PTO/AIA/80 (07-12)
Approved for use through 11/30/2014. OMB 0651-0035
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE

POWER OF ATTORNEY TO PROSECUTE APPLICATIONS BEFORE THE USPTO

I hereby revoke all previous powers of attorney given in the application identified in the attached statement under 37 CFR 3.73(c).

I hereby appoint:

■ Practitioners associated with Customer Number: 22907

OR

☐ Practitioner(s) named below (if more than ten patent practitioners are to be named, then a customer number must be used):

Name	Registration Number	Name	Registration Number

As attorney(s) or agent(s) to represent the undersigned before the United States Patent and Trademark Office (USPTO) in connection with any and all patent applications assigned only to the undersigned according to the USPTO assignment records or assignments documents attached to this form in accordance with 37 CFR 3.73(c).

Please change the correspondence address for the application identified in the attached statement under 37 CFR 3.73(c) to:

☑ The address associated with Customer Number: 22907

OR

☐

Firm or Individual Name			
Address			
City		State	Zip
Country			
Telephone		Email	

Assignee Name and Address: Centripetal Networks, Inc.
41378 Raspberry Drive
Leesburg, VA 20176-7826

A copy of this form, together with a statement under 37 CFR 3.73(c) (Form PTO/AIA/96 or equivalent) is required to be Filed in each application in which this form is used. The statement under 37 CFR 3.73(c) may be completed by one of The practitioners appointed in this form, and must identify the application in which this Power of Attorney is to be filed.

SIGNATURE of Assignee of Record

The individual whose signature and title is supplied below is authorized to act on behalf of the assignee

Signature	/Steven Rogers/	Date	
Name	Steven Rogers	Telephone	(571) 252-5082
Title	Chief Executive Officer		

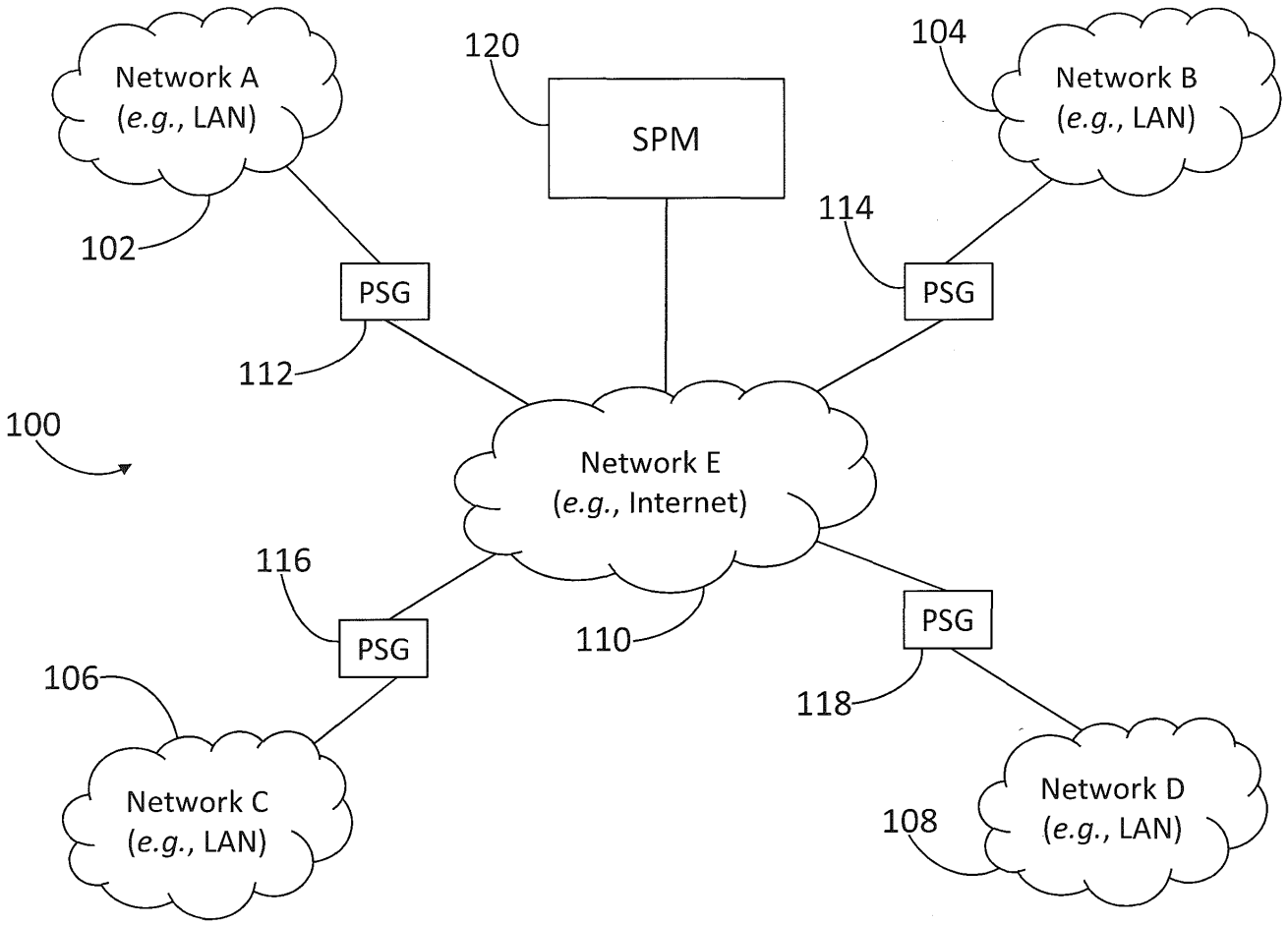

Network A
(e.g., LAN)
120
SPM
104
Network B
(e.g., LAN)
102
114
PSG
PSG
112
100
Network E
(e.g., Internet)
116
PSG
110
PSG
106
118
Network C
(e.g., LAN)
Network D
(e.g., LAN)
108

FIG. 1

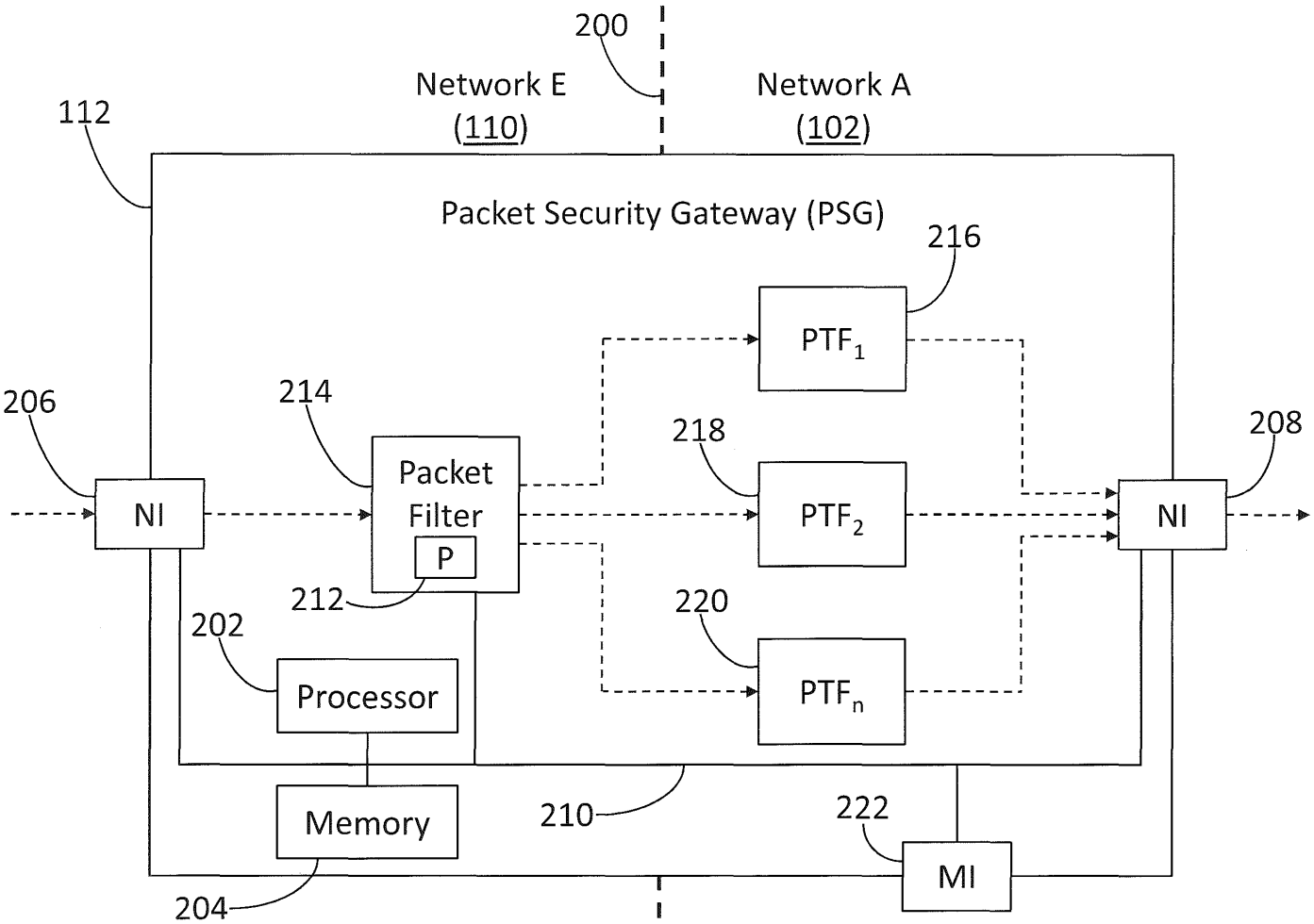
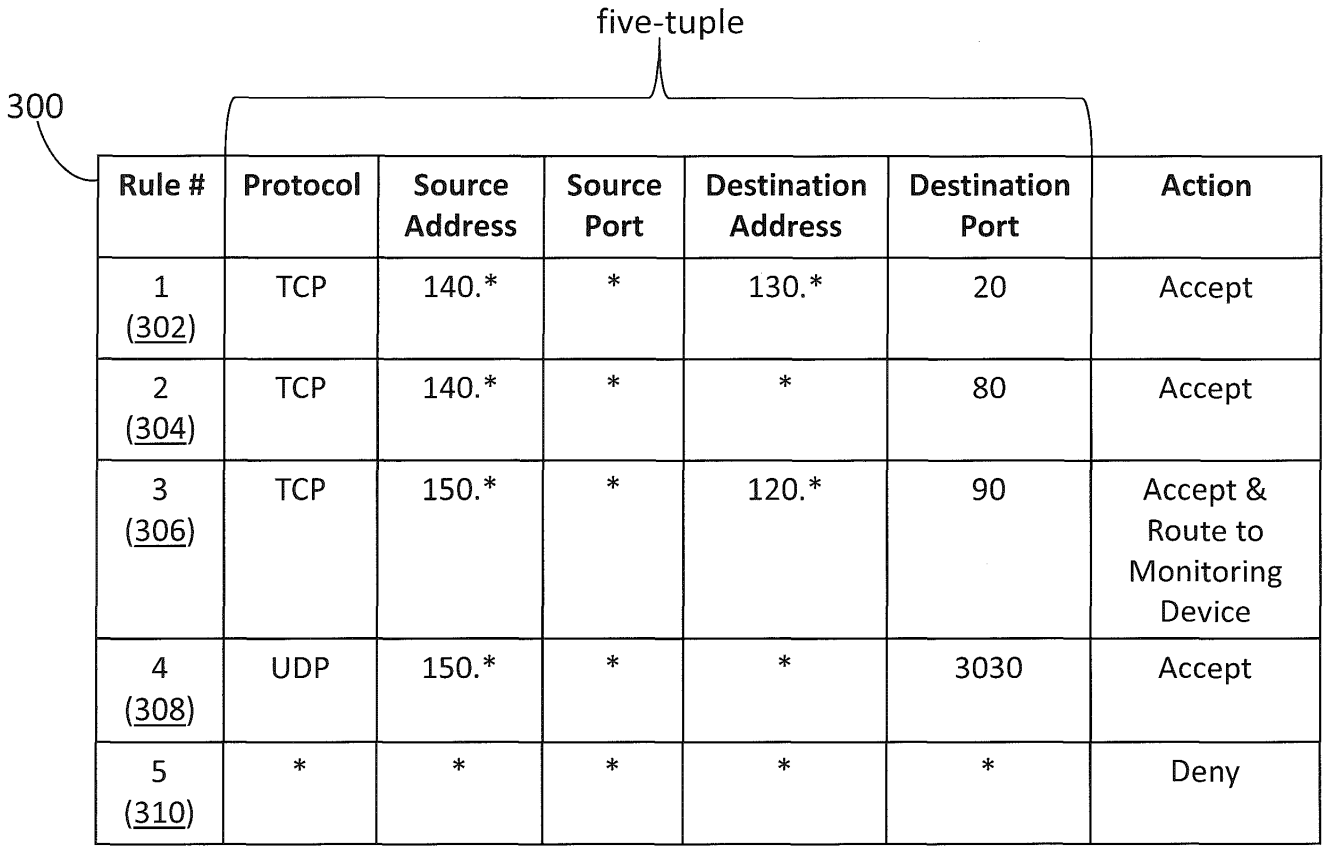

200
Network E
(110)
Network A
(102)
112
Packet Security Gateway (PSG)
216
PTF1
206
214
Packet
Filter
P
218
PTF2
208
NI
NI
212
220
202
Processor
PTFn
Memory
210
222
MI
204

FIG. 2



Rule #	Protocol	Source Address	Source Port	Destination Address	Destination Port	Action
1 (302)	TCP	140.*	*	130.*	20	Accept
2 (304)	TCP	140.*	*	*	80	Accept
3 (306)	TCP	150.*	*	120.*	90	Accept & Route to Monitoring Device
4 (308)	UDP	150.*	*	*	3030	Accept
5 (310)	*	*	*	*	*	Deny

FIG. 3

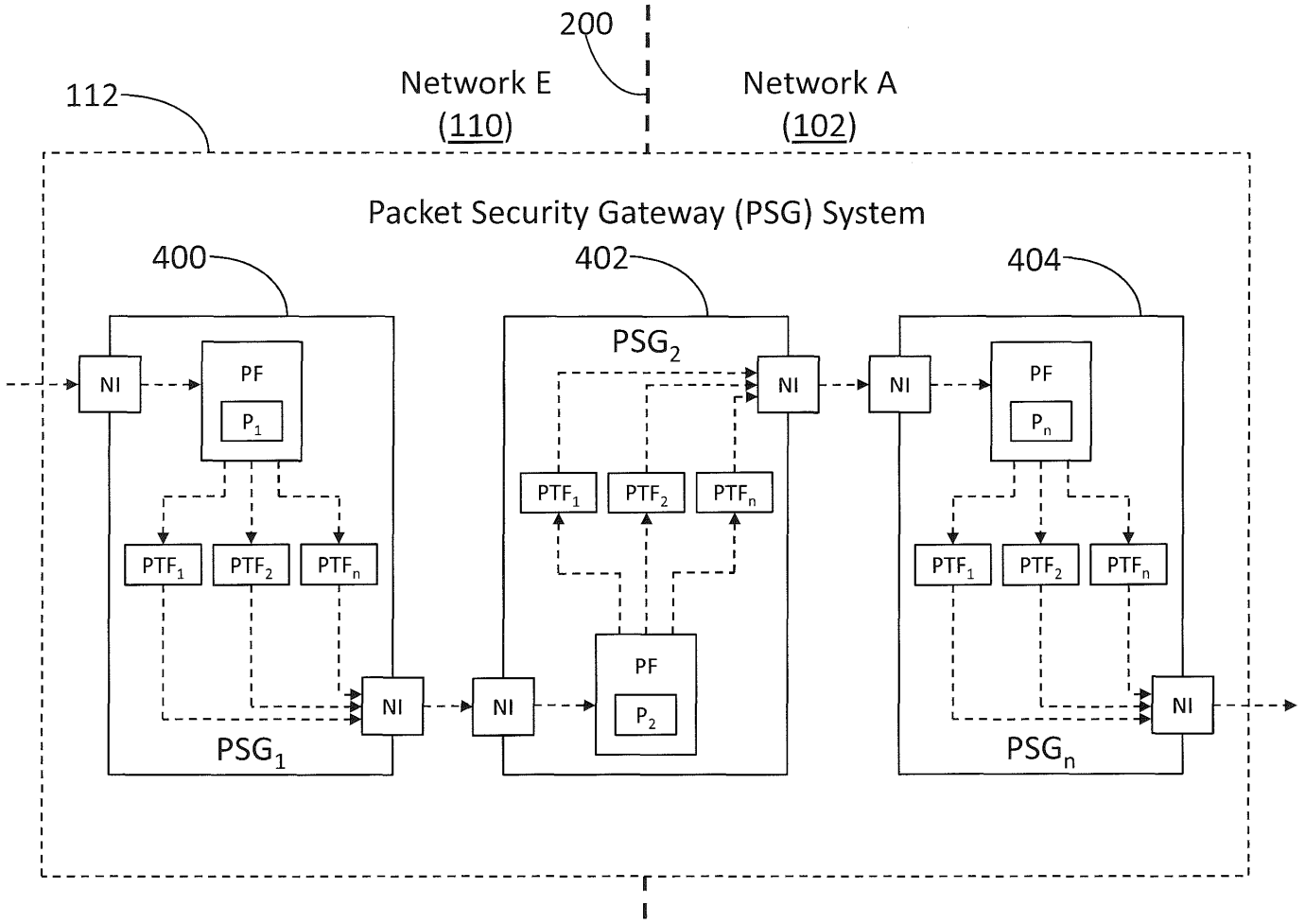

200
Network E
(110)
Network A
(102)
112
Packet Security Gateway (PSG) System
400
402
404
NI
PF
P1
PTF1
PTF2
PTFn
PSG2
Pn
P2
PSG1
PSGn

FIG. 4

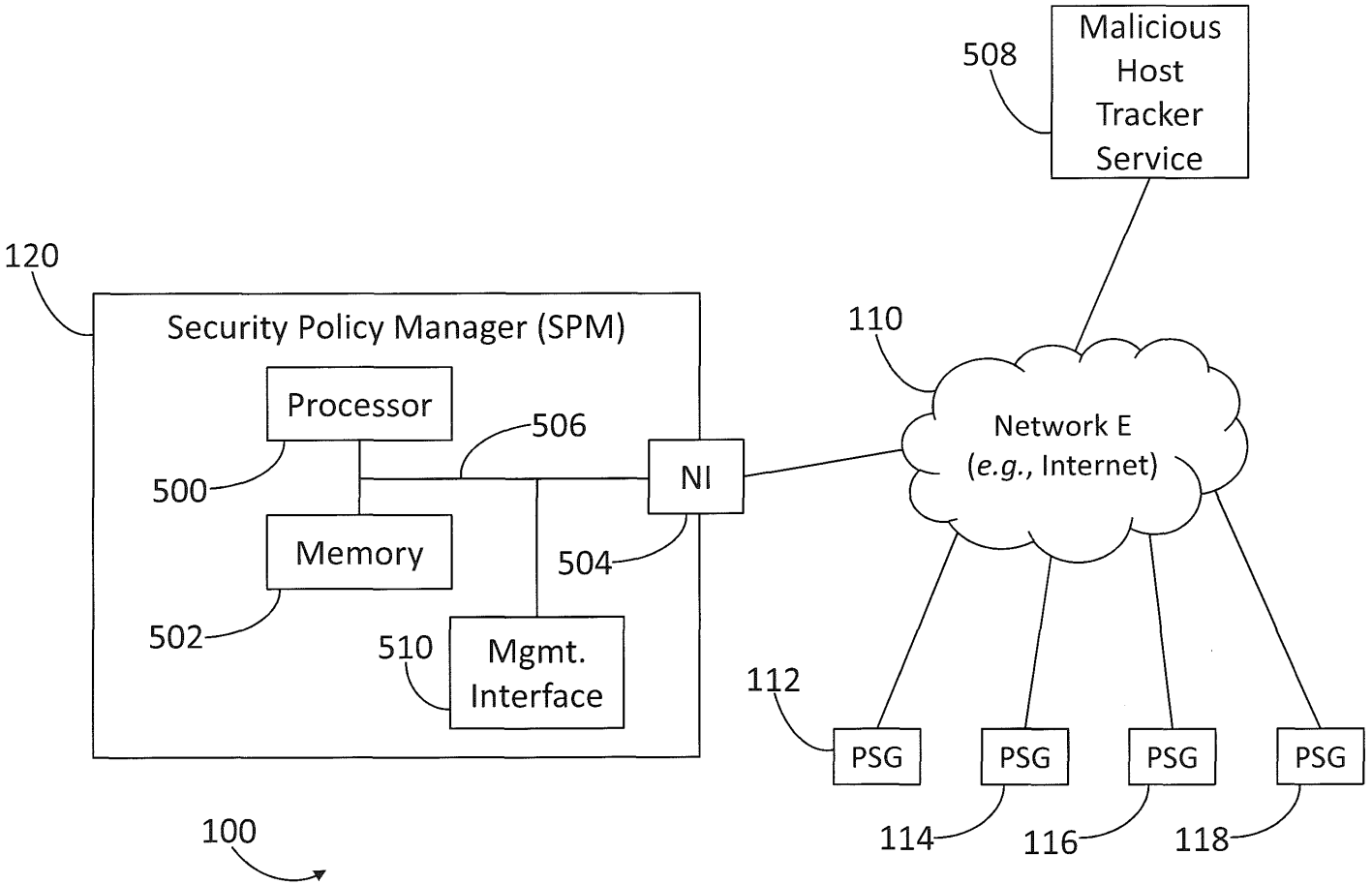

Malicious
Host
Tracker
Service
508
120
Security Policy Manager (SPM)
Processor
506
500
NI
110
Network E
(e.g., Internet)
Memory
504
502
510
Mgmt.
Interface
112
PSG
PSG
PSG
PSG
114
116
118
100

FIG. 5

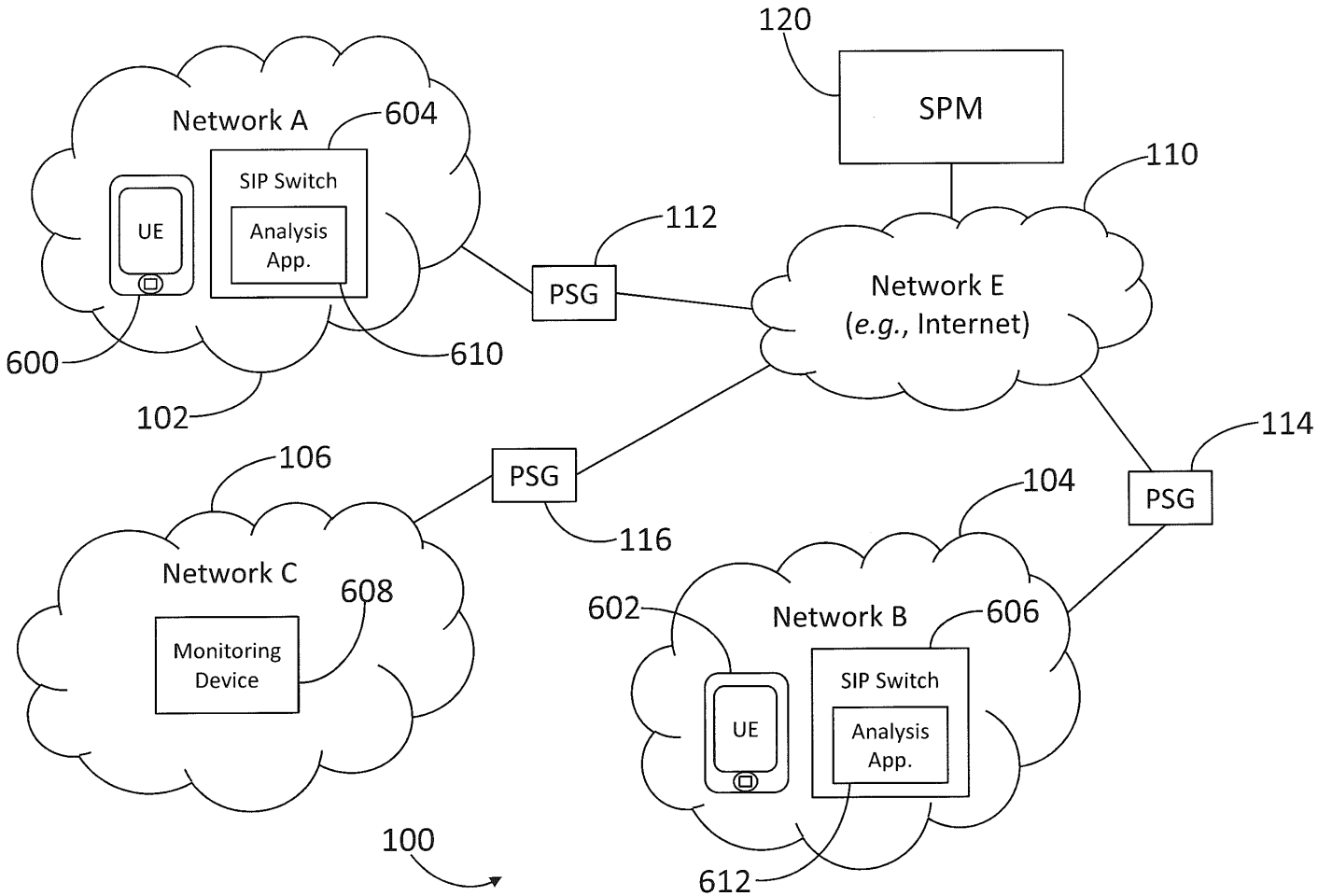

120
SPM
Network A
604
SIP Switch
UE
Analysis App.
112
PSG
110
Network E
(e.g., Internet)
600
610
102
106
PSG
114
PSG
104
116
Network C
608
Monitoring Device
602
Network B
606
SIP Switch
UE
Analysis App.
100
612

FIG. 6

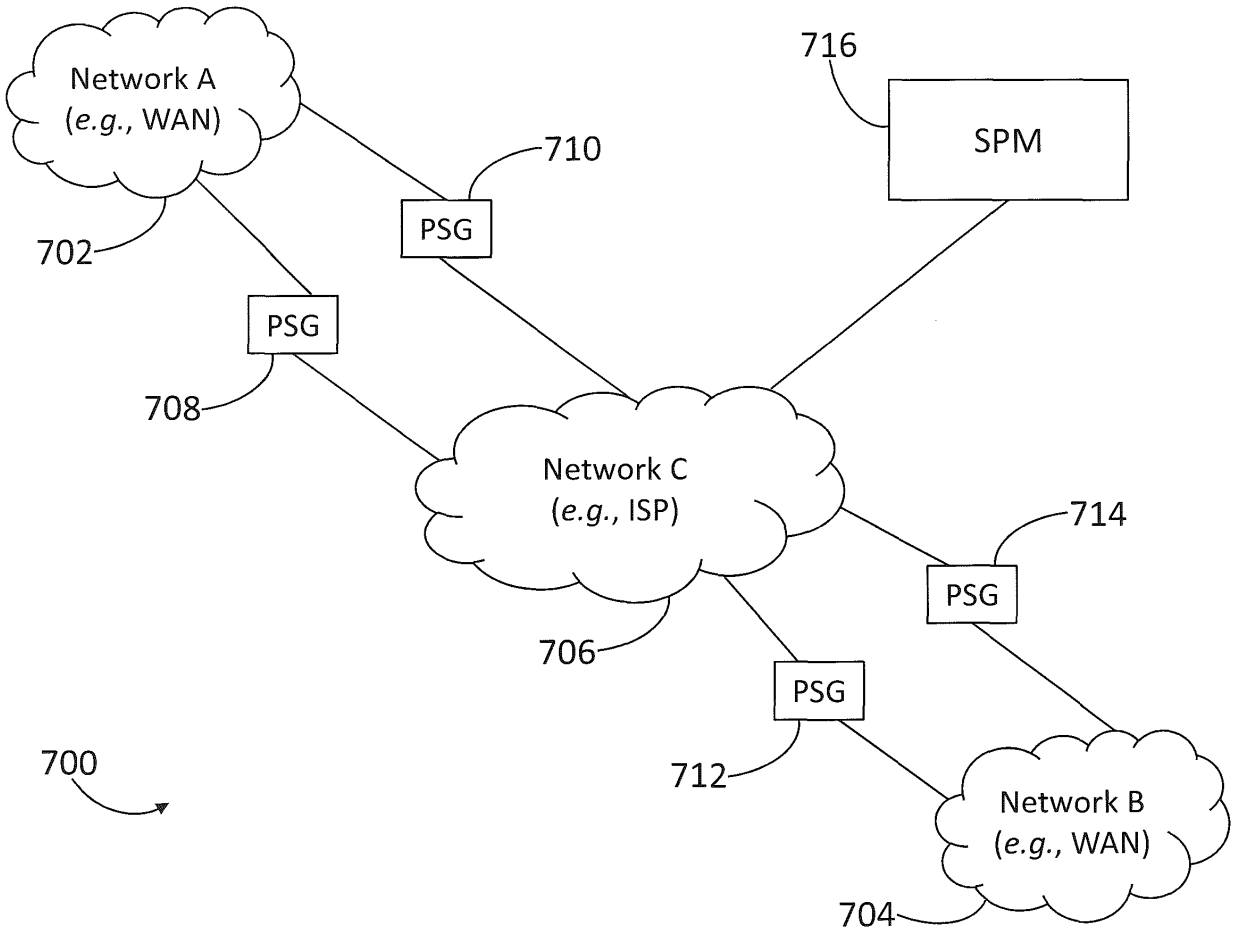

Network A
(e.g., WAN)
702
PSG
710
716
SPM
PSG
708
Network C
(e.g., ISP)
706
PSG
714
PSG
712
Network B
(e.g., WAN)
704
700

FIG. 7

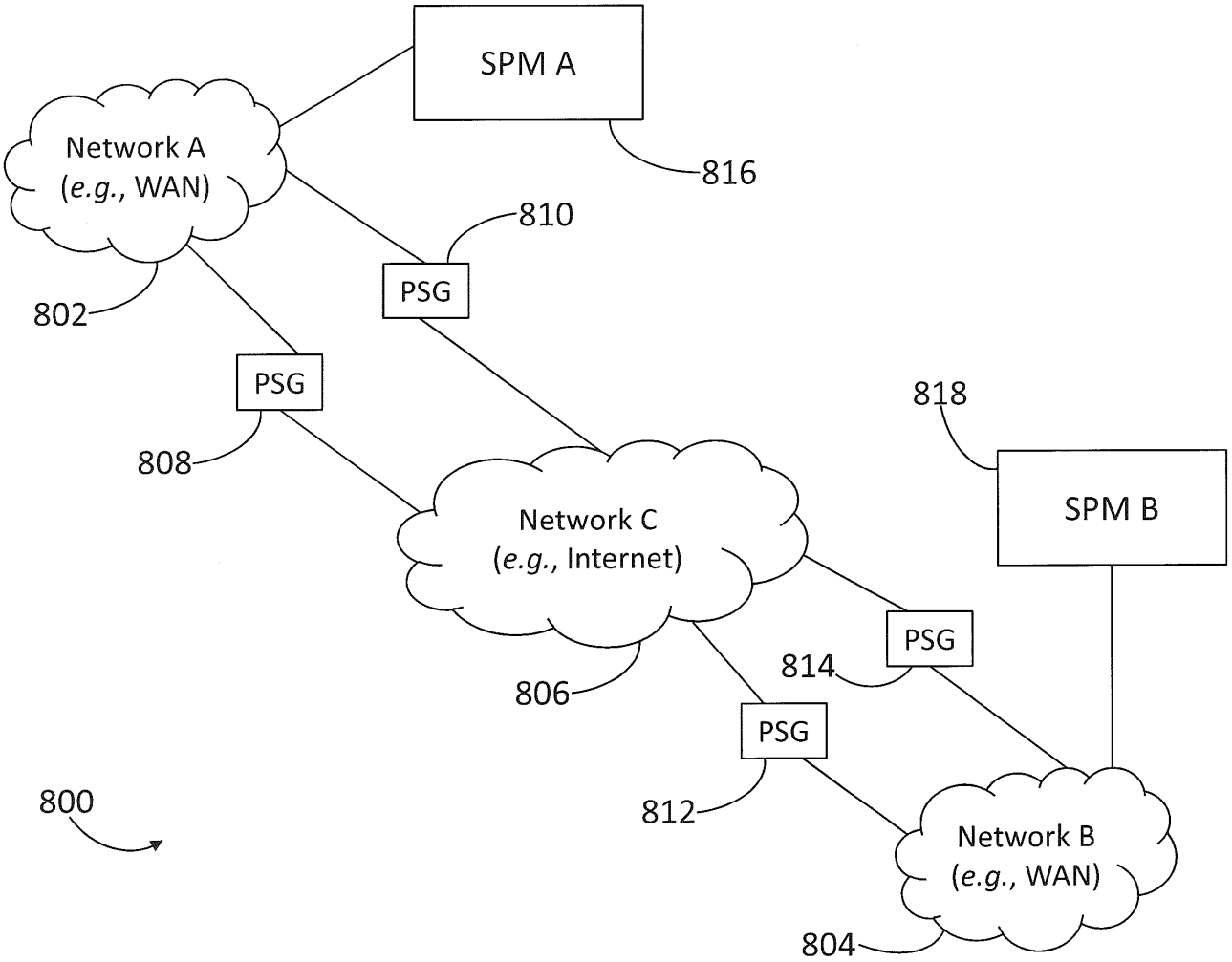

SPM A
816
Network A
(e.g., WAN)
810
802
PSG
PSG
808
818
SPM B
Network C
(e.g., Internet)
PSG
814
806
PSG
812
800
Network B
(e.g., WAN)
804

FIG. 8

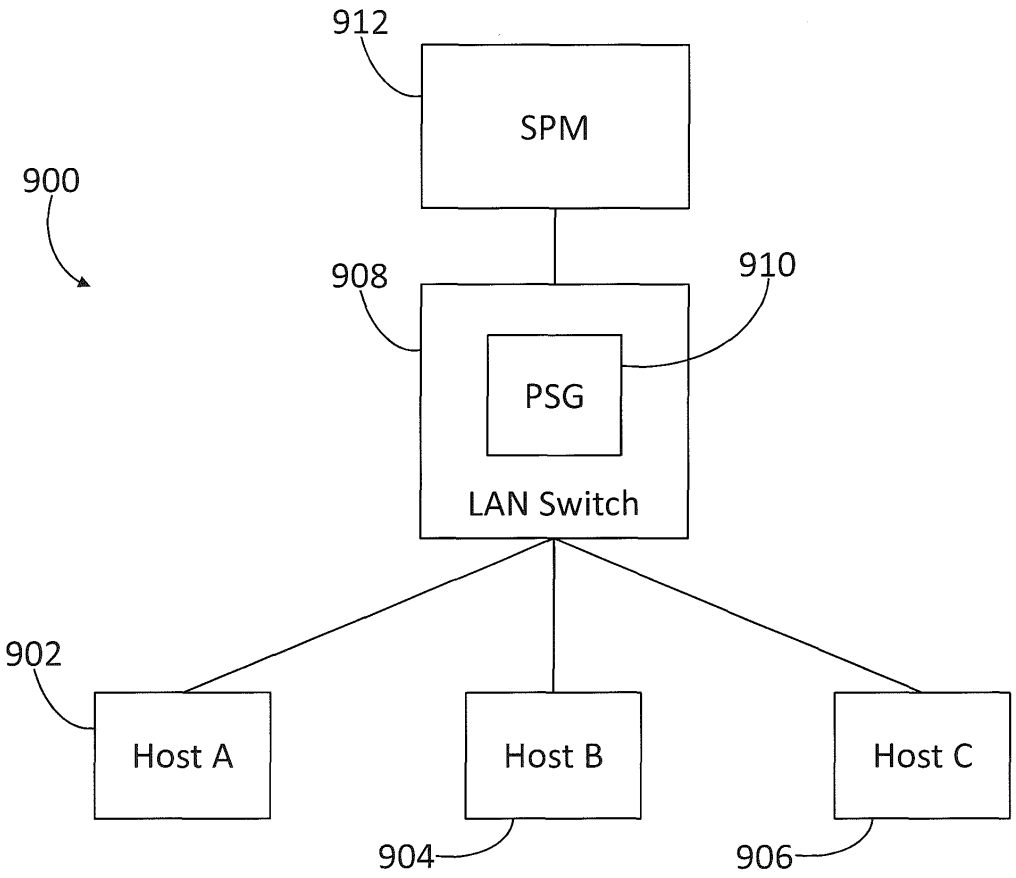

912
SPM
900
908
910
PSG
LAN Switch
902
Host A
Host B
Host C
904
906

FIG. 9

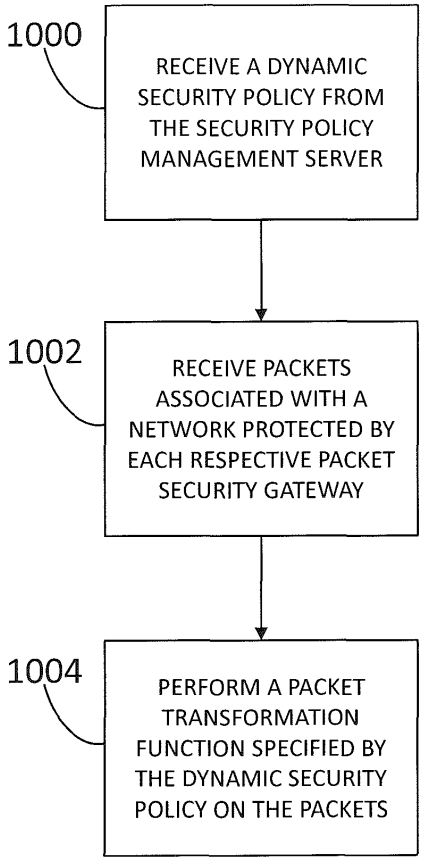

1000
RECEIVE A DYNAMIC SECURITY POLICY FROM THE SECURITY POLICY MANAGEMENT SERVER
1002
RECEIVE PACKETS ASSOCIATED WITH A NETWORK PROTECTED BY EACH RESPECTIVE PACKET SECURITY GATEWAY
1004
PERFORM A PACKET TRANSFORMATION FUNCTION SPECIFIED BY THE DYNAMIC SECURITY POLICY ON THE PACKETS

FIG. 10

Electronic Patent Application Fee Transmittal	
Application Number:	
Filing Date:	
Title of Invention:	Methods and Systems for Protecting a Secured Network
First Named Inventor/Applicant Name:	Steven Rogers
Filer:	William Eugene Wooten/leatrice sims
Attorney Docket Number:	007742.00017
Filed as Large Entity	

Utility under 35 USC 111(a) Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Utility application filing	1011	1	390	390
Utility Search Fee	1111	1	620	620
Utility Examination Fee	1311	1	250	250
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Miscellaneous:				
		Total in USD ($)		**1260**

Electronic Acknowledgement Receipt

EFS ID:	14041123
Application Number:	13657010
International Application Number:	
Confirmation Number:	2390
Title of Invention:	Methods and Systems for Protecting a Secured Network
First Named Inventor/Applicant Name:	Steven Rogers
Customer Number:	22907
Filer:	William Eugene Wooten/leatrice sims
Filer Authorized By:	William Eugene Wooten
Attorney Docket Number:	007742.00017
Receipt Date:	22-OCT-2012
Filing Date:	
Time Stamp:	14:18:55
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$1260
RAM confirmation Number	624
Deposit Account	190733
Authorized User	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)

1	Application Data Sheet	ADS.pdf	1396050 953297f73f56a1410f98b433a2a5ee16714de9c8	no	6
Warnings:					
Information:					
2		application.pdf	227280 d98586775a81bc70ebeaac5284ae12cdfc8b9eb2	yes	37
	Multipart Description/PDF files in .zip description				
	Document Description		**Start**	**End**	
	Specification		1	30	
	Claims		31	36	
	Abstract		37	37	
Warnings:					
Information:					
3	Oath or Declaration filed	DEC.pdf	541372 d8bc0ff94c825ae8d74b9072b395ba2026be0318	no	1
Warnings:					
Information:					
4	Oath or Declaration filed	declaration.pdf	2414375 1b7072d7d2d887d8359cef6c8e201fa5b79549fc	no	1
Warnings:					
Information:					
5	Assignee showing of ownership per 37 CFR 3.73.	373b.pdf	163547 b4d19e0a381ad2d40adbfed567643f3a1b7e751d	no	2
Warnings:					
Information:					
6	Power of Attorney	poa.pdf	2649391 ddfc36155a7100c549e54dcacd4db23293ababa09	no	1
Warnings:					
Information:					
7	Drawings-only black and white line drawings	figures.pdf	164350 4cb3657620b137a8df3150955c7be70f968314ec	no	10
Warnings:					
Information:					

8	Fee Worksheet (SB06)	fee-info.pdf	32756 bf596a3db66790fd22d640675cf34a6a057ef514	no	2
Warnings:					
Information:					
			Total Files Size (in bytes):	7589121	

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PTO/AIA/14 (08-12)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	007742.00017
	Application Number	
Title of Invention	METHODS AND SYSTEMS FOR PROTECTING A SECURED NETWORK	

The application data sheet is part of the provisional or nonprovisional application for which it is being submitted. The following form contains the bibliographic data arranged in a format specified by the United States Patent and Trademark Office as outlined in 37 CFR 1.76.
This document may be completed electronically and submitted to the Office in electronic format using the Electronic Filing System (EFS) or the document may be printed and included in a paper filed application.

Secrecy Order 37 CFR 5.2

☐ Portions or all of the application associated with this Application Data Sheet may fall under a Secrecy Order pursuant to 37 CFR 5.2 (Paper filers only. Applications that fall under Secrecy Order may not be filed electronically.)

Inventor Information:

Inventor 1 Remove

Legal Name

Prefix	Given Name	Middle Name	Family Name	Suffix
	Steven		Rogers	

Residence Information (Select One) ◉ US Residency ○ Non US Residency ○ Active US Military Service

City	Leesburg	State/Province	VA	Country of Residence	US

Mailing Address of Inventor:

Address 1	c/o Centripetal Networks, Inc.
Address 2	41378 Raspberry Drive

City	Leesburg	State/Province	VA
Postal Code	20176-7826	Country	US

Inventor 2 Remove

Legal Name

Prefix	Given Name	Middle Name	Family Name	Suffix
	Sean		Moore	

Residence Information (Select One) ◉ US Residency ○ Non US Residency ○ Active US Military Service

City	Hollis	State/Province	NH	Country of Residence	US

Mailing Address of Inventor:

Address 1	c/o Centripetal Networks, Inc.
Address 2	41378 Raspberry Drive

City	Leesburg	State/Province	VA
Postal Code	20176-7826	Country	US

All Inventors Must Be Listed - Additional Inventor Information blocks may be generated within this form by selecting the **Add** button. Add

Correspondence Information:

Enter either Customer Number or complete the Correspondence Information section below.
For further information see 37 CFR 1.33(a).

PTO/AIA/14 (08-12)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	007742.00017
	Application Number	
Title of Invention	METHODS AND SYSTEMS FOR PROTECTING A SECURED NETWORK	

☐ An Address is being provided for the correspondence Information of this application.			
Customer Number	22907		
Email Address		Add Email	Remove Email

Application Information:

Title of the Invention	METHODS AND SYSTEMS FOR PROTECTING A SECURED NETWORK		
Attorney Docket Number	007742.00017	**Small Entity Status Claimed**	☒
Application Type	Nonprovisional		
Subject Matter	Utility		
Suggested Class (if any)		**Sub Class (if any)**	
Suggested Technology Center (if any)			
Total Number of Drawing Sheets (if any)		**Suggested Figure for Publication (if any)**	

Publication Information:

☐ Request Early Publication (Fee required at time of Request 37 CFR 1.219)
☐ **Request Not to Publish.** I hereby request that the attached application not be published under 35 U.S.C. 122(b) and certify that the invention disclosed in the attached application **has not and will not** be the subject of an application filed in another country, or under a multilateral international agreement, that requires publication at eighteen months after filing.

Representative Information:

Representative information should be provided for all practitioners having a power of attorney in the application. Providing this information in the Application Data Sheet does not constitute a power of attorney in the application (see 37 CFR 1.32).
Either enter Customer Number or complete the Representative Name section below. If both sections are completed the customer Number will be used for the Representative Information during processing.

Please Select One:	◉ Customer Number	○ US Patent Practitioner	○ Limited Recognition (37 CFR 11.9)
Customer Number	22907		

Domestic Benefit/National Stage Information:

This section allows for the applicant to either claim benefit under 35 U.S.C. 119(e), 120, 121, or 365(c) or indicate National Stage entry from a PCT application. Providing this information in the application data sheet constitutes the specific reference required by 35 U.S.C. 119(e) or 120, and 37 CFR 1.78.

Prior Application Status			Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	007742.00017
	Application Number	
Title of Invention	METHODS AND SYSTEMS FOR PROTECTING A SECURED NETWORK	

Additional Domestic Benefit/National Stage Data may be generated within this form by selecting the **Add** button. Add

Foreign Priority Information:

This section allows for the applicant to claim benefit of foreign priority and to identify any prior foreign application for which priority is not claimed. Providing this information in the application data sheet constitutes the claim for priority as required by 35 U.S.C. 119(b) and 37 CFR 1.55(a).

Remove

Application Number	Country i	Filing Date (YYYY-MM-DD)	Priority Claimed
			(•) Yes ( ) No

Additional Foreign Priority Data may be generated within this form by selecting the **Add** button. Add

Authorization to Permit Access:

☐ Authorization to Permit Access to the Instant Application by the Participating Offices

If checked, the undersigned hereby grants the USPTO authority to provide the European Patent Office (EPO), the Japan Patent Office (JPO), the Korean Intellectual Property Office (KIPO), the World Intellectual Property Office (WIPO), and any other intellectual property offices in which a foreign application claiming priority to the instant patent application is filed access to the instant patent application. See 37 CFR 1.14(c) and (h). This box should not be checked if the applicant does not wish the EPO, JPO, KIPO, WIPO, or other intellectual property office in which a foreign application claiming priority to the instant patent application is filed to have access to the instant patent application.

In accordance with 37 CFR 1.14(h)(3), access will be provided to a copy of the instant patent application with respect to: 1) the instant patent application-as-filed; 2) any foreign application to which the instant patent application claims priority under 35 U.S.C. 119(a)-(d) if a copy of the foreign application that satisfies the certified copy requirement of 37 CFR 1.55 has been filed in the instant patent application; and 3) any U.S. application-as-filed from which benefit is sought in the instant patent application.

In accordance with 37 CFR 1.14(c), access may be provided to information concerning the date of filing this Authorization.

Applicant Information:

Providing assignment information in this section does not substitute for compliance with any requirement of part 3 of Title 37 of CFR to have an assignment recorded by the Office.

PTO/AIA/14 (08-12)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	007742.00017
	Application Number	
Title of Invention	METHODS AND SYSTEMS FOR PROTECTING A SECURED NETWORK	

Applicant 1

If the applicant is the inventor (or the remaining joint inventor or inventors under 37 CFR 1.45), this section should not be completed. The information to be provided in this section is the name and address of the legal representative who is the applicant under 37 CFR 1.43; or the name and address of the assignee, person to whom the inventor is under an obligation to assign the invention, or person who otherwise shows sufficient proprietary interest in the matter who is the applicant under 37 CFR 1.46. If the applicant is an applicant under 37 CFR 1.46 (assignee, person to whom the inventor is obligated to assign, or person who otherwise shows sufficient proprietary interest) together with one or more joint inventors, then the joint inventor or inventors who are also the applicant should be identified in this section.

Remove

◯ Assignee	◯ Legal Representative under 35 U.S.C. 117
◯ Person to whom the inventor is obligated to assign.	◯ Person who shows sufficient proprietary interest

If applicant is the legal representative, indicate the authority to file the patent application, the inventor is:

Name of the Deceased or Legally Incapacitated Inventor :

If the Assignee is an Organization check here. ☒

Organization Name	Centripetal Networks, Inc.		
Mailing Address Information:			
Address 1	41378 Raspberry Drive		
Address 2			
City	Leesburg	**State/Province**	VA
Country [i]	US	Postal Code	20176-7826
Phone Number		Fax Number	
Email Address			

Additional Applicant Data may be generated within this form by selecting the Add button. Add

Signature:

Remove

NOTE: This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4 for signature requirements and certifications

Signature	/William E. Wooten/			Date (YYYY-MM-DD)	2012-10-22
First Name	William	Last Name	Wooten	Registration Number	60049

Additional Signature may be generated within this form by selecting the Add button. Add

PTO/AIA/14 (08-12)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	007742.00017
	Application Number	
Title of Invention	METHODS AND SYSTEMS FOR PROTECTING A SECURED NETWORK	

This collection of information is required by 37 CFR 1.76. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 23 minutes to complete, including gathering, preparing, and submitting the completed application data sheet form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

METHODS AND SYSTEMS FOR PROTECTING A SECURED NETWORK

BACKGROUND

[1] The TCP/IP network protocols (*e.g.*, the Transmission Control Protocol (TCP) and the Internet Protocol (IP)) were designed to build large, resilient, reliable, and robust networks. Such protocols, however, were not originally designed with security in mind. Subsequent developments have extended such protocols to provide for secure communication between peers (*e.g.*, Internet Protocol Security (IPsec)), but the networks themselves remain vulnerable to attack (*e.g.*, Distributed Denial of Service (DDoS) attacks).

[2] Most existing approaches to protecting such networks are reactive rather than proactive. While reactive approaches may identify the source of an attack and assist in subsequent mitigation efforts, in most instances, the attack will have already been successfully launched.

[3] Proactive solutions, however, have often been deemed untenable due to an inability to scale to larger networks. A significant challenge associated with building a scalable proactive solution is the need to filter substantially all network traffic at a high resolution. In a large network, where traffic volumes may be enormous, the time required to provide high resolution filtering has traditionally been thought to render a proactive solution infeasible.

SUMMARY

[4] The following presents a simplified summary in order to provide a basic understanding of some aspects of the disclosure. It is neither intended to identify key or critical elements of the disclosure nor to delineate the scope of the disclosure. The following summary merely presents some concepts in a simplified form as a prelude to the description below.

[5] Aspects of this disclosure relate to protecting a secured network. In some embodiments, one or more packet security gateways are associated with a security policy management server. At each of the packet security gateways, a dynamic security policy may be received from the security policy management server, packets associated with a network protected by the packet security gateway may be received, and at least one of multiple packet transformation

functions specified by the dynamic security policy may be performed on the packets. Performing the at least one of multiple packet transformation functions specified by the dynamic security policy on the packets may include performing at least one packet transformation function other than forwarding or dropping the packets.

[6] In some embodiments, two or more of the packet security gateways may be configured in series such that packets forwarded from a first of the packet security gateways are received by a second of the packet security gateways. In some embodiments, the dynamic security policy may include two rules requiring sequential execution. A first of the packet security gateways may perform a packet transformation function specified by one of the rules on the packets and a second of the packet security gateways may subsequently perform a packet transformation function specified by the other of the rules on packets received from the first packet security gateway.

[7] In some embodiments, the dynamic security policy may include a rule specifying a set of network addresses for which associated packets should be dropped and a rule specifying that all packets associated with network addresses outside the set should be forwarded. Additionally or alternatively, the dynamic security policy may include a rule specifying a set of network addresses for which associated packets should be forwarded and a rule specifying that all packets associated with network addresses outside the set should be dropped. In some embodiments, the security policy management server may receive information associated with one or more Voice over Internet Protocol (VoIP) sessions and the set of network addresses for which associated packets should be forwarded may be created or altered utilizing the information associated with the one or more VoIP sessions.

[8] In some embodiments, the packet security gateways may receive three or more dynamic security policies from the security policy management server. A first of the dynamic security policies may specify a first set of network addresses for which packets should be forwarded. A second of the dynamic security policies may be received after the first and may specify a second set of network addresses, which includes more network addresses than the first set, for which packets should be forwarded. A third of the dynamic security policies may be received after the second and may specify a third set of network addresses, which

includes more network addresses than the second set, for which packets should be forwarded.

[9] In some embodiments, the dynamic security policy may include two rules that each specify a set of network addresses. The dynamic security policy may specify that packets associated with the first set of network addresses should be placed in a first forwarding queue and packets associated with the second set of network addresses should be placed in a second forwarding queue. The first forwarding queue may have a different queueing policy, for example, a higher forwarding rate, than the second forwarding queue.

[10] In some embodiments, the dynamic security policy may include a rule specifying a set of network addresses and an additional parameter. The packet transformation function specified by the dynamic security policy may include routing packets that fall within the specified set and match the additional parameter to a network address different from a destination network address specified by the packets. In some embodiments, the additional parameter may be a Session Initiation Protocol (SIP) Uniform Resource Identifier (URI). The network address different from the destination network address may correspond to a device configured to copy information contained within the packets and forward the packets to the destination network address specified by the packets.

[11] In some embodiments, the packet transformation function may forward the packets into the network protected by the packet security gateway. In some embodiments, the packet transformation function may forward the packets out of the network protected by the packet security gateway. In some embodiments, the packet transformation function may forward the one or more packets to an IPsec stack having an IPsec security association corresponding to the packets. In some embodiments, the packet transformation function may drop the packets.

[12] In some embodiments, the dynamic security policy may include multiple rules. One of the rules may specify the packet transformation function. In some embodiments, one of the rules may specify a five-tuple of values selected from packet header information. The five-tuple may specify one or more protocol types, one or more IP source addresses, one or more source ports, one or more IP destination addresses, and one or more destination ports. In

some embodiments, one of the rules may specify a Differentiated Service Code Point (DSCP) that maps to a DSCP field in an IP header of one of the packets.

[13] In some embodiments, one of the packet security gateways may operate in a network layer transparent manner. For example, the packet security gateway may send and receive traffic at a link layer using an interface that is not addressed at the network layer and simultaneously perform the packet transformation function at the network layer. Additionally or alternatively, the packet security gateway may include a management interface having a network layer address. Access to the management interface may be secured at the application level.

[14] In some embodiments, the dynamic security policy may include a rule generated based, at least in part, on a list of known network addresses associated with malicious network traffic. In some embodiments, the list of known network addresses associated with malicious network traffic may be received from a subscription service that aggregates information associated with malicious network traffic.

[15] In some embodiments, the packets associated with the network protected by the packet security gateway may originate within the network protected by the packet security gateway and may be destined for a network distinct from the network protected by the packet security gateway. Additionally or alternatively, the packets associated with the network protected by the packet security gateway may originate within a network distinct from the network protected by the packet security gateway and may be destined for a host within the network protected by the packet security gateway.

[16] In some embodiments, one of the packet security gateways may be located at each boundary between a protected network associated with the security policy management server and an unprotected network.

[17] Other details and features will be described in the sections that follow.

BRIEF DESCRIPTION OF THE DRAWINGS

[18] The present disclosure is pointed out with particularity in the appended claims. Features of the disclosure will become more apparent upon a review of this disclosure in its entirety, including the drawing figures provided herewith.

[19] Some features herein are illustrated by way of example, and not by way of limitation, in the figures of the accompanying drawings, in which like reference numerals refer to similar elements.

[20] FIG. 1 illustrates an exemplary network environment in which one or more aspects of the disclosure may be implemented.

[21] FIG. 2 illustrates an exemplary packet security gateway.

[22] FIG. 3 illustrates an exemplary dynamic security policy.

[23] FIG. 4 illustrates an exemplary configuration of multiple packet security gateways in series.

[24] FIG. 5 illustrates an exemplary security policy management server.

[25] FIG. 6 illustrates an exemplary network environment for implementing a monitoring service.

[26] FIG. 7 illustrates an exemplary network environment that includes a secured network having multiple boundaries with unsecured networks.

[27] FIG. 8 illustrates an exemplary network environment that includes multiple distinct secured networks.

[28] FIG. 9 illustrates an exemplary secure LAN environment.

[29] FIG. 10 illustrates an exemplary method for protecting a secured network.

DETAILED DESCRIPTION

[30] In the following description of various illustrative embodiments, reference is made to the accompanying drawings, which form a part hereof, and in which is shown, by way of illustration, various embodiments in which aspects of the disclosure may be practiced. It is to be understood that other embodiments may be utilized, and structural and functional modifications may be made, without departing from the scope of the present disclosure.

[31] Various connections between elements are discussed in the following description. These connections are general and, unless specified otherwise, may be direct or indirect, wired or wireless. In this respect, the specification is not intended to be limiting.

[32] FIG. 1 illustrates an exemplary network environment in which one or more aspects of the disclosure may be implemented. Referring to FIG. 1, network environment **100** may include networks A – E **102**, **104**, **106**, **108**, and **110**. One or more networks within network environment **100** may be a Local Area Network (LAN) or a Wide Area Network (WAN). Such a LAN or WAN may be associated, for example, with an organization (*e.g.*, a company, university, enterprise, or government agency). For example, networks A – D **102**, **104**, **106**, and **108** may be LANs, any combination of which may be associated with one or more organizations. One or more networks within network environment **100** may interface with one or more other networks within network environment **100**. For example, network environment **100** may include a WAN that interfaces one or more LANs within network environment **100** or network environment **100** may include one or more Internet Service Providers (ISPs) that interface one or more LANs or WANs within network environment **100** via the Internet. For example, network E **110** may comprise the Internet and may interface networks A – D **102**, **104**, **106**, and **108**.

[33] As used herein, a packet security gateway includes any computing device configured to receive packets and perform a packet transformation function on the packets. Optionally, a packet security gateway may further be configured to perform one or more additional functions as described herein. As used herein, a security policy management server includes any computing device configured to communicate a dynamic security policy to a packet security gateway. Optionally, a security policy management server may further be configured to perform one or more additional functions as described herein. As used herein,

a dynamic security policy includes any rule, message, instruction, file, data structure, or the like that specifies criteria corresponding to one or more packets and identifies a packet transformation function to be performed on packets corresponding to the specified criteria. Optionally, a dynamic security policy may further specify one or more additional parameters as described herein.

[34] Network environment **100** may include one or more packet security gateways and one or more security policy management servers. For example, network environment **100** may include packet security gateways **112**, **114**, **116**, and **118**, and security policy management server **120**. One or more security policy management servers may be associated with a protected network. For example, networks A – D **102**, **104**, **106**, and **108** may each be distinct LANs associated with a common organization and may each form part of a protected network associated with security policy management server **120**. Many network protocols route packets dynamically, and thus the path a given packet may take cannot be readily predicted. Accordingly it may be advantageous to locate a packet security gateway at each boundary between a protected network and an unprotected network. For example, packet security gateway **112** may be located at the boundary between network A **102** and network E **110**. Similarly, packet security gateway **114** may be located at the boundary between network B **104** and network E **110**; packet security gateway **116** may be located at the boundary between network C **106** and network E **110**; and packet security gateway **118** may be located at the boundary between network D **108** and network E **110**. As will be described in greater detail below, each of one or more packet security gateways associated with a security policy management server may be configured to receive a dynamic security policy from the security policy management server, receive packets associated with a network protected by the packet security gateway, and perform a packet transformation function specified by the dynamic security policy on the packets. For example, each of packet security gateways **112**, **114**, **116**, and **118** may be configured to receive a dynamic security policy from security policy management server **120**. Each of packet security gateways **112**, **114**, **116**, and **118** may also be configured to receive packets respectively associated with networks A – D **102**, **104**, **106**, and **108**. Each of packet security gateways **112**, **114**, **116**, and **118** may further be configured to perform a packet transformation function specified by the dynamic security policy received from security policy

management server **120** on the packets respectively associated with networks A – D **102**, **104**, **106**, and **108**.

[35] FIG. 2 illustrates an exemplary packet security gateway according to one or more aspects of the disclosure. Referring to FIG. 2, as indicated above, packet security gateway **112** may be located at network boundary **200** between network A **102** and network E **110**. Packet security gateway **112** may include processor **202**, memory **204**, network interfaces **206** and **208**, packet filter **214**, and management interface **222**. Processor **202**, memory **204**, network interfaces **206** and **208**, packet filter **214**, and management interface **222** may be interconnected via data bus **210**. Network interface **206** may connect packet security gateway **112** to network E **110**. Similarly, network interface **208** may connect packet security gateway **112** to network A **102**. Memory **204** may include one or more program modules that when executed by processor **202**, configure packet security gateway **112** to perform various functions as described herein.

[36] Packet security gateway **112** may be configured to receive a dynamic security policy from security policy management server **120**. For example, packet security gateway **112** may receive dynamic security policy **212** from security policy management server **120** via management interface **222** (*i.e.*, out-of-band signaling) or network interface **206** (*i.e.*, in-band signaling). Packet security gateway **112** may include one or more packet filters or packet discriminators, or logic for implementing one or more packet filters or packet discriminators. For example, packet security gateway **112** may include packet filter **214**, which may be configured to examine information associated with packets received by packet security gateway **112** and forward the packets to one or more packet transformation functions based on the examined information. For example, packet filter **214** may examine information associated with packets received by packet security gateway **112** (*e.g.*, packets received from network E **110** via management interface **222** or network interface **206**) and forward the packets to one or more of packet transformation functions 1 – N **216**, **218**, and **220** based on the examined information.

[37] As will be described in greater detail below, dynamic security policy **212** may include one or more rules and the configuration of packet filter **214** may be based on one or more of the

rules included in dynamic security policy **212**. For example, dynamic security policy **212** may include one or more rules specifying that packets having specified information should be forwarded to packet transformation function **216**, while all other packets should be forwarded to packet transformation function **218**. Packet transformation functions 1 – N **216**, **218**, and **220** may be configured to perform one or more functions on packets they receive from packet filter **214**. For example, packet transformation functions 1 – N **216**, **218**, and **220** may be configured to forward packets received from packet filter **214** into network A **102**, forward packets received from packet filter **214** to an IPsec stack having an IPsec security association corresponding to the packets, or drop packets received from packet filter **214**. In some embodiments, one or more of packet transformation functions 1 – N **216**, **218**, and **220** may be configured to drop packets by sending the packets to a local "infinite sink" (*e.g.*, the /dev/null device file in a UNIX/LINUX system).

[38] In some embodiments, packet security gateway **112** may be configured in a network layer transparent manner. For example, packet security gateway **112** may be configured to utilize one or more of network interfaces **206** and **208** to send and receive traffic at the link layer. One or more of network interfaces **206** and **208**, however, may not be addressed at the network layer. Because packet filter **214** and packet transformation functions 1 – N **216**, **218**, and **220** operate at the network layer, PSG **112** may still perform packet transformation functions at the network layer. By operating in a network layer transparent manner, packet security gateway **112** may insulate itself from network attacks (*e.g.*, DDoS attacks) launched at the network layer because attack packets cannot be routed to the network interfaces **206** and **208**. In some embodiments, packet security gateway **112** may include management interface **222**. Management interface **222** may be addressed at the network level in order to provide packet security gateway **112** with network level addressability. Access to management interface **222** may be secured, for example, at the application level by using a service such as SSH, or secured at the transport level using, *e.g.*, TLS, or secured at the network level by attaching it to a network with a separate address space and routing policy from network A **102** and network E **110**, or secured at the link level, *e.g.*, using the IEEE 802.1X framework, etc.

[39] The flows illustrated by Figure 2 are merely exemplary and show packets that originate within a network distinct from network A **102** and are destined for a host within network A **102** in order to simplify the illustration. Packet security gateway **112** may be configured to receive and filter packets that originate within a network other than network A **102** (*e.g.*, networks B – E **104**, **106**, **108**, or **110**) and are destined for a host within network A **102**, as well as packets that originate within network A **102** destined for a network distinct from network A **102** (*e.g.*, network B – D **104**, **106**, **108**, or **110**). That is, packet security gateway **112** may be configured to filter and perform one or more packet transformation functions on packets flowing in either direction and may thus be utilized, for example, to both protect network A **102** from malicious network traffic and to prevent malicious network traffic from leaving network A **102**.

[40] FIG. 3 illustrates an exemplary dynamic security policy in accordance with one or more embodiments. Referring to FIG. 3, dynamic security policy **300** may include rules 1 – 5 **302**, **304**, **306**, **308**, and **310**. Each rule may specify criteria and one or more packet transformation functions that should be performed for packets associated with the specified criteria. The specified criteria may take the form of a five-tuple of values selected from packet header information, specifying a protocol type of the data section of the IP packet (*e.g.*, TCP, UDP, ICMP, or any other protocol), one or more source IP addresses, one or more source port values, one or more destination IP addresses, and one or more destination ports. For example, rule 1 **302** may specify that IP packets containing TCP packets, originating from a source IP address that begins with 140, having any source port, destined for an IP address that begins with 130, and destined for port 20 should have an accept packet transformation function (*e.g.*, the identity function) performed on them. Similarly, rule 2 **304** may specify that IP packets containing TCP packets, originating from a source IP address that begins with 140, having any source port, destined for any IP address, and destined for port 80 should have an accept packet transformation function performed on them; rule 3 **306** may specify that IP packets containing TCP packets, originating from a source IP address that begins with 150, having any source port, destined for any IP address that begins with 120, and destined for port 90 should have an accept packet transformation function performed on them; rule 4 **308** may specify that IP packets containing UDP packets, originating from a source IP address that begins with 150, having any source port,

destined for any IP address, and destined for port 3030 should have an accept packet transformation function performed on them; and rule 5 **310** may specify that IP packets containing any data, originating from any source IP address, having any source port, destined for any IP address, and destined for any port should have a deny packet transformation function performed on them. One or more rules included in dynamic security policy **300** may be specified in IP version 4 or IP version 6.

[41] As will be described in greater detail below, dynamic security policy **300** may include one or more rules that specify a packet transformation function other than forwarding (accepting or allowing) or dropping (denying) a packet. For example, rule 3 **306** may specify that IP packets containing TCP packets, originating from a source IP address that begins with 150, having any source port, destined for any IP address that begins with 120, and destined for port 90 should not only have an accept packet transformation function performed on them, but should also be routed to a monitoring device.

[42] One or more rules within dynamic security policy **300** may be required to execute in a specific order. For example, it may be required that rule 5 **310** be executed last. Because rule 5 **310** specifies that any packet should have a deny packet transformation function performed on it, if it were executed before a rule specifying an accept packet transformation function (*e.g.*, one or more of rules 1 – 4 **302**, **304**, **306**, or **308**), no packets matching the criteria specified by the rule specifying the accept packet transformation function would pass through a packet security gateway implementing dynamic security policy **300**. Similarly, two or more rules within dynamic security policy **300** may specify overlapping criteria and different packet transformation functions. In such cases, the order-of-application of the rules may determine which rule is applied to a packet that would match the two or more rules. Such rules may be merged together or otherwise transformed into a different set of rules without overlapping criteria, which may produce the same result as the original set of rules, when applied to any packet.

[43] A dynamic security policy may utilize the combination of one or more rules to create policies for governing packets within a network environment or effectuating one or more services within a network environment. For example, a dynamic security policy may

include one or more rules, the combination of which may effectuate a blocklist service within a network environment. A dynamic security policy that effectuates a blocklist service within a network environment may include one or more rules specifying criteria (*e.g.*, a set of network addresses) for which associated packets should be blocked, dropped, or denied, and at least one rule specifying that all packets outside the specified block sets should be forwarded, accepted, or allowed. Such a dynamic security policy may be constructed by including one or more rules specifying criteria (*e.g.*, a set of network addresses) for which associated packets should be dropped, and a wildcard rule, designated to be executed last, and specifying that all packets should be allowed. One or more dynamic security policies that effectuate a blocklist service may be utilized to implement one or more Virtual Private Networks (VPNs).

[44] A dynamic security policy may also include one or more rules, the combination of which may effectuate an allowlist service within a network environment. A dynamic security policy that effectuates an allowlist service within a network environment may include one or more rules specifying criteria (*e.g.*, a set of network addresses) for which associated packets should be forwarded, allowed, or accepted, and at least one rule specifying that all packets outside the specified allow sets should be blocked, denied, or dropped. Such a dynamic security policy may be constructed by including one or more rules specifying criteria (*e.g.*, a set of network addresses) for which associated packets should be forwarded, and a wildcard rule, designated to be executed last, and specifying that all packets should be blocked. For example, dynamic security policy **300** includes rules 1 – 4 **302**, **304**, **306**, and **308**, each of which specifies a set of network addresses for which packets should be allowed, and rule 5 **310** which specifies that all packets should be dropped. Thus, if rules 1 – 5 **302**, **304**, **306**, **308**, and **310** are executed in order, dynamic security policy **300** will effectuate an allowlist service.

[45] A dynamic security policy may also include one or more rules, the combination of which may effectuate a VoIP firewall service within a network environment. As will be discussed in greater detail below, a security policy management server may receive information associated with VoIP sessions. For example, a security policy management server may receive information associated with VoIP sessions from one or more softswitches (*e.g.*,

H.323 softswitches, SIP IP Multimedia Subsystem (IMS) softswitches) or session border controllers when a VoIP session is initialized or set up. In order to allow packets associated with such a VoIP session within a network protected by one or more packet security gateways associated with the security policy management server, the security policy management server may utilize the received information associated with the VoIP sessions to construct one or more rules for allowing the packets associated with the VoIP session. When the VoIP session is terminated or torn down, the softswitch or session border controller may notify the security policy management server, which may create or alter one or more rules to reflect the termination of the VoIP session (*e.g.*, to deny future packets which may match criteria previously associated with the VoIP session).

[46] A dynamic security policy may also include one or more rules or rule sets, the combination of which may effectuate a phased restoration service within a network environment. Such a phased restoration service may be used in the event of a network attack (*e.g.*, a DDoS attack). When an attack occurs a network may be overwhelmed with network traffic and be unable to route all or any of the traffic. In the event of such an attack, it may be beneficial to utilize a dynamic security policy which effectuates a phased restoration service. Such a dynamic security policy may include one or more rules or rule sets configured for execution in time-shifted phases. Each of the rules or rule sets may specify progressively larger sets of network addresses. For example, a dynamic security policy may include three rules or rule sets which may be configured for execution in time-shifted phases. A first of the rules or rule sets may specify a relatively small set of network addresses for which packets should be forwarded (*e.g.*, network addresses corresponding to mission critical network devices). A second of the rules or rule sets may specify a relatively larger set of network addresses for which packets should be forwarded (*e.g.*, network addresses corresponding to trusted network devices). A third of the rules or rule sets may specify an even larger set of network addresses for which packets should be forwarded (*e.g.*, network addresses corresponding to all network devices that would be allowed under ordinary circumstances). The dynamic security policy may specify that the rules or rule sets should be implemented in time-shifted phases. That is, the dynamic security policy may specify that the first rule or rule set should be executed first, and that the second rule or rule set should be executed at a time after the time at which the first rule or rule set is executed, and the third rule or rule set should be

executed at a time after the time at which the second rule or rule set is executed. Such a dynamic security policy may assist a network in recovering from an attack, by allowing the network to isolate itself from the attack or recover in a controlled manner.

[47] A dynamic security policy may also include one or more rules, the combination of which may effectuate an enqueueing service within a network environment. A dynamic security policy that effectuates an enqueueing service may include one or more rules that specify sets of network addresses and packet transformation functions that queue packets in one or more queues corresponding to the sets. These queues may then be serviced at varying rates. For example, a dynamic security policy may include two rules, each of which specify a set of network addresses. A first of the rules may specify that packets corresponding to its specified set should be queued in a first forwarding queue. A second of the rules may specify that packets corresponding to its specified set should be queued in a second forwarding queue. The first forwarding queue may be serviced at a higher forwarding rate than the second forwarding queue. Such an enqueueing service may be utilized during or following a network attack, or generally to provide prioritized service to critical network devices (*e.g.*, when network resources are strained). In some embodiments, one or more rules contained within a dynamic security policy may include an arbitrary selector which may correspond to one or more parameters or fields associated with a packet. For example, a dynamic security policy rule may include a Differentiated Service Code Point (DSCP) selector that corresponds to a DSCP field in an IP header. Thus, two packets having different values within the specified DSCP field may correspond to two distinct rules within a dynamic security policy and have different packet transformation functions performed on them. For example, two otherwise identical packets having different values within the specified DSCP field may be queued in two different forwarding queues that have different forwarding rates, and may thus receive differentiated service.

[48] A dynamic security policy may also include one or more rules, the combination of which may effectuate a multi-dimensional routing service or a multi-dimensional switching service within a network environment. For example, in some embodiments, a dynamic security policy may include one or more rules that specify a set of network addresses and an additional parameter. Such rules may further specify a packet transformation function

configured to route packets within the specified set of network addresses that match the additional parameter to a network address distinct from the packets' respective destination network addresses. For example, the packet transformation function may be configured to encapsulate such packets (*e.g.*, as described by Internet Engineering Task Force (IETF) Request For Comment (RFC) 2003) with an IP header specifying a network address different from their respective destination addresses. The packets may then be routed to the network address specified by the encapsulating IP header, which may correspond to a network device configured to utilize such packets or data contained within them, strip the IP header from the packets, and forward the packets to their respective destination addresses. In some embodiments, the packet transformation function may be configured to alter or modify the destination address of the packets, which may then be routed to the altered or modified destination address. Additionally or alternatively, the packet transformation function may be configured to assign such packets to a particular Layer-2 VLAN (*e.g.*, as described by IEEE 802.1Q). The packets may then be switched to another device on the same VLAN, which may or may not be on the IP-layer path that the packet would have taken if it were routed according to the packet's destination IP address instead of being switched through the VLAN.

[49] As will be described in greater detail below, in some embodiments a dynamic security policy may include one or more rules, the combination of which may effectuate an implementation of a multi-dimensional routing service for performing a monitoring service within a network environment. For example, a dynamic security policy may include one or more rules that specify a set of network addresses (*e.g.*, a set of network addresses from which a call that is to be monitored is expected to originate within) and an additional parameter (*e.g.*, a SIP URI corresponding to a caller to be monitored). As indicated above, such rules may further specify a packet transformation function configured to route or switch packets within the specified set of network addresses that match the additional parameter (*e.g.*, the SIP URI) to a network address corresponding to a monitoring device. The network address corresponding to the monitoring device may be different from the packets' destination network address (*e.g.*, an address corresponding to the called party or a softswitch associated with the called party). For example, the packet transformation function may be configured to encapsulate the packets with an IP header specifying the

network address corresponding to the monitoring device. The packets may then be routed (or rerouted) to the monitoring device, which may be configured to copy the packets or data contained within them (*e.g.*, for subsequent review by a law enforcement or national security authority), strip the IP header from them, and then forward the packets to their destination address (*e.g.*, the address corresponding to the called party or softswitch associated with the called party).

[50] As indicated above, a significant challenge associated with building a scalable proactive solution for protecting a secured network, is the need to filter substantially all network traffic at a high resolution. Filtering traffic at a high resolution often requires the use of many rules. In a large network, where traffic volumes may be enormous, the time required to provide high resolution filtering (*e.g.*, the time required to apply a large number of rules to a large volume of traffic) has traditionally been thought to render proactive network protection solutions infeasible. This concern may be particularly acute in network environments that utilize low-latency applications (*e.g.*, VoIP).

[51] Recent advances in packet filtering technology have reduced the time required to apply large rule sets to network traffic. For example, U.S. Patent Application Publication Nos. 2006/0195896 and 2006/0248580 to Fulp et al., and U.S. Patent Application Publication No. 2011/0055916 to Ahn, describe advanced packet filtering technologies, and are each incorporated by reference herein in their entireties.

[52] One approach to providing high resolution filtering, while reducing the number of rules applied to network traffic, may be utilized when a dynamic security policy is combinatorially complete. For example, a dynamic security policy may be configured to allow bi-directional communication between a set of N internal hosts $\{I_1, I_2, \ldots, I_N\}$ within a protected network and a set of M external hosts $\{E_1, E_2, \ldots, E_M\}$ outside the protected network. To enable communications between the internal hosts and the external hosts, the dynamic security policy may be constructed to include a set of rules containing each possible combination of internal hosts and external hosts (*e.g.*,$\{\{I_1, E_1\}, \{I_1, E_2\}, \ldots \{I_1, E_M\}, \{I_2, E_1\}, \{I_2, E_2\}, \ldots \{I_2, E_M\}, \ldots, \{I_N, E_1\}, \{I_N, E_2\}, \ldots \{I_N, E_M\}\}$), each of the rules being associated with an allow packet transformation function. Such a dynamic security

policy would have N*M rules for allowing communication between the internal hosts and the external hosts that originate from one of the internal hosts and are destined for one of the external hosts, and an additional N*M rules for allowing communications between the internal hosts and the external hosts that originate from one of the external hosts and are destined for one of the internal hosts. An equivalent result may be achieved, however, by constructing two smaller dynamic security policies: a first dynamic security policy that includes rules specifying the N internal hosts (*e.g.*, $\{\{I_1\}, \{I_2\}, \ldots, \{I_N\}\}$), each rule being associated with an accept packet transformation function; and a second dynamic security policy that includes rules specifying the M external hosts (*e.g.*, $\{\{E_1\}, \{E_2\}, \ldots, \{E_M\}\}$), each rule being associated with an accept packet transformation function. Such a construct of dynamic security policies may be implemented using a system of packet security gateways configured in series.

[53] FIG. 4 illustrates an exemplary configuration of multiple packet security gateways connected in series. Referring to FIG. 4, packet security gateway **112** may include one or more packet security gateways configured in series. For example, packet security gateway **112** may include packet security gateways 1 – N **400**, **402**, and **404**. Packet security gateways 1 – N **400**, **402**, and **404** may be configured so that packets forwarded by packet security gateway 1 **400** are received by packet security gateway 2 **402**, and packets forwarded by packet security gateway 2 **402** are received by the next packet security gateway in the series, all the way through packet security gateway N **404**. Each of packet security gateways 1 – N **400**, **402**, and **404** may include a packet filter, similar to packet filter **214** described above with respect to FIG. 2, and one or more packet transformation functions, similar to packet transformation functions 1 – N **216**, **218**, and **220** described above with respect to FIG. 2. Packet security gateways 1 – N **400**, **402**, and **404** may be utilized to implement a construct of dynamic security policies similar to that described above.

[54] For example, packet security gateway 1 **400** may be configured to implement P_1, which may include rules specifying M external hosts (*e.g.*, $\{\{E_1\}, \{E_2\}, \ldots, \{E_M\}\}$), each rule being associated with an accept packet transformation function. Packet security gateway 2 **402** may be configured to implement P_2, which may include rules specifying N internal hosts

(*e.g.*, $\{\{I_1\}, \{I_2\}, \ldots, \{I_N\}\}$), each rule being associated with an accept packet transformation function. A packet received by packet security gateway **112** may be initially received via packet security gateway 1 **400**'s network interface. Packet security gateway 1 **400** may apply one or more of the rules in P_1 to the received packet until the packet matches criteria specified by a rule in P_1, at which point packet security gateway 1 **400** may perform a packet transformation function specified by the rule on the packet. For example, a packet may be received by packet security gateway **112** that originates from external host E_5 (*e.g.*, a host within network E **110**) and is destined for internal host I_7 (*e.g.*, a host within network A **102**). Packet security gateway 1 **400** may apply one or more of the rules in P_1 (*e.g.*, $\{\{E_1\}, \{E_2\}, \ldots, \{E_M\}\}$) to the received packet and the received packet may match the criteria specified by one of the rules in P_1 (*e.g.*, $\{\{E_5\}$). The rule may specify that an accept packet transformation function should be performed, and packet security gateway 1 **400** may utilize one or more of its packet transformation functions to perform the accept packet transformation function on the packet and forward the packet to packet security gateway 2 **402**. Packet security gateway 2 **402** may apply one or more of the rules in P_2 (*e.g.*, $\{\{I_1\}, \{I_2\}, \ldots, \{I_N\}\}$) to the packet and the packet may match the criteria specified by one of the rules in P_2 (*e.g.*, $\{\{I_7\}$). The rule may specify that an accept packet transformation function should be performed, and packet security gateway 2 **402** may utilize one or more of its packet transformation functions to perform the accept packet transformation function on the packet and forward the packet to network A **102**.

[55] It will be appreciated that utilizing multiple packet security gateways in series to implement dynamic security policy constructs may increase performance and decrease memory resource requirements. For example, in the described scenario packet security gateway 1 **400** may have only been required to compare the packet to five rules and packet security gateway 2 **402** may have only been required to compare the packet to seven rules. In a worst case scenario, packet security gateway 1 **400** may have only been required to compare the packet to M rules and packet security gateway 2 **402** may have only been required to compare the packet to N rules. Moreover, the series configuration may enable packet security gateway 1 **400** to begin implementing P_1 with respect to a subsequently received packet, while packet security gateway 2 **402** simultaneously implements P_2 with respect to the packet forwarded by packet security gateway 1 **400**. Furthermore, the memory

requirements for this scenario with packet security gateways in series may be comparable to M+N, whereas originally the combinatorially complete set of rules contained in a single packet security gateway may have required memory comparable to N*M.

[56] FIG. 5 illustrates an exemplary security policy management server. Referring to FIG. 5, security policy management server **120** may include processor **500**, memory **502**, and network interface **504**. One or more of processor **500**, memory **502**, and network interface **504** may be interconnected via data bus **506**. Network interface **504** may interface security policy management server **120** with network E **110**. Memory **502** may include one or more program modules that when executed by processor **500**, configure security policy management server **120** to perform functions described herein. It will be appreciated that as used herein the term "server" designates one or more computing devices configured to perform one or more functions described herein. The term "server" should not be construed to imply that a client/server relationship (*e.g.*, a relationship in which a request is received from a client and then serviced by a server) necessarily exists.

[57] Security policy management server **120** may be configured to communicate one or more dynamic security policies to one or more packet security gateways within network environment **100**. For example, security policy management server **120** may communicate one or more dynamic security policies stored in memory **502** to one or more of packet security gateways **112**, **114**, **116**, and **118**. For example, security policy management server **120** may be configured to communicate one or more dynamic security policies to one or more of packet security gateways **112**, **114**, **116**, and **118** on a periodic basis, under specified network conditions, whenever security policy management server **120** receives a new dynamic security policy, whenever a dynamic security policy stored on security policy management server **120** is changed or altered, or in response to a request from one or more of packet security gateways **112**, **114**, **116**, and **118**.

[58] Security policy management server **120** may also be configured to provide one or more administrators associated with security policy management server **120** with management interface **510**. For example, security policy management server **120** may be configured to provide one or more administrators with a Graphical User Interface (GUI) or Command

Line Interface (CLI). An administrator of security policy management server **120** may utilize security policy management server **120**'s management interface **510** to configure security policy management server **120**. For example, an administrator may configure security policy management server **120** in order to associate security policy management server **120** with one or more of packet security gateways **112**, **114**, **116**, and **118**. An administrator of security policy management server **120** may also utilize security policy management server **120**'s management interface **510** to construct one or more dynamic security policies or to load one or more dynamic security policies into security policy management server **120**'s memory **502**. For example, an administrator associated with security policy management server **120** may manually construct one or more dynamic security policies offline and then utilize security policy management server **120**'s management interface **510** to load such dynamic security policies into security policy management server **120**'s memory **502**.

[59] In some embodiments, security policy management server **120** may be configured to add, remove, or alter one or more dynamic security policies stored in memory **502** based on information received from one or more devices within network environment **100**. For example, security policy management server **120**'s memory **502** may include a dynamic security policy having one or more rules that specify a list of network addresses known to be associated with malicious network traffic. Security policy management server **120** may be configured to automatically create or alter one or more of such rules as new network addresses associated with malicious network traffic are determined. For example, security policy management server **120** may receive updates (*e.g.* as part of a subscription) from malicious host tracker service **508**. Malicious host tracker service **508** may aggregate information associated with malicious network traffic and updates received from malicious host tracker service **508** may include one or more network addresses that have been determined to be associated with malicious network traffic. Security policy management server **120** may be configured to create or alter one or more rules included within a dynamic security policy associated with malicious host tracker service **508** to block traffic associated with the network addresses received from malicious host tracker service **508**. Additionally or alternatively, as indicated above, security policy management server **120** may be configured to create or alter one or more dynamic security policies, or one or more rules

included in one or more dynamic security policies, to account for VoIP sessions being initiated or terminated by a network device within network environment **100**.

[60] As indicated above, a dynamic security policy may include one or more rules, the combination of which may effectuate an implementation of a multi-dimensional routing service for performing a monitoring service within a network environment. FIG. 6 illustrates an exemplary network environment for implementing a monitoring service in accordance with one or more embodiments. Referring to FIG. 6, a user of network environment **100** (*e.g.*, a law enforcement or national security authority) may desire to obtain a copy of packets associated with one or more VoIP sessions (*e.g.*, sessions associated with SIP URI exampleuser@exampledomain.com) within network environment **100**. Because many SIP-signaled services are designed to address sessions dynamically, it may not be possible to determine, prior to a session being set up, a particular network address and port from which packets should be copied. Moreover, due to privacy concerns, regulators may require that only packets associated with the specified VoIP sessions (*e.g.*, sessions associated with SIP URI exampleuser@exampledomain.com) be copied.

[61] For example, a user associated with SIP URI exampleuser@exampledomain.com may utilize User Equipment (UE) **600** within network A **102** to place a VoIP call to a user utilizing UE **602** within network B **104**. SIP switch **604** may be utilized by an operator of network A **102** for switching SIP signals within network A **102**. Similarly, SIP switch **606** may be utilized by an operator of network B **104** for switching SIP signals within network B **104**. One or more of SIP switches **604** and **606** may include an analysis application configured to monitor SIP signals and publish SIP messages associated with specified users to one or more subscribers. For example, the operator of network A **102** may have installed analysis application **610** on SIP switch **604** (*e.g.*, accessed via a SIP IMS Service Control (ISC) interface associated with SIP switch **604**) and configured analysis application **610** to search for and publish SIP messages associated with SIP URI exampleuser@exampledomain.com to security policy management server **120**. Similarly, the operator of network B **104** may have installed analysis application **612** on SIP switch **606** and configured analysis application **612** to publish SIP messages associated with SIP URI exampleuser@exampledomain.com to security policy management server **120**.

[62] When the user associated with SIP URI exampleuser@exampledomain.com utilizes UE **600** to place a VoIP call to the user utilizing UE **602**, analysis application **610** may detect one or more SIP signaling messages associated with the call (*e.g.*, SIP signaling messages for setting up the call) and publish the messages to security policy management server **120**. Security policy management server **120** may extract one or more network addresses and port numbers from the SIP signaling messages (*e.g.*, a network address and port number utilized by UE **600** for placing the VoIP call to UE **602**). Security policy management server **120** may utilize the extracted network addresses and port numbers to create a new dynamic security policy or alter one or more rules within an existing dynamic security policy. For example, security policy management server **120** may construct a new dynamic security policy that includes a rule specifying one of the extracted network addresses and port numbers, as well as a packet transformation function configured to route associated packets to monitoring device **608**. Security policy management server **120** may communicate the new or modified dynamic security policy to packet security gateway **112**.

[63] When packets associated with the VoIP call between UE **600** and UE **602** are received by packet security gateway **112**, packet filter **214** may identify the packets as matching the criteria specified by the dynamic security policy received from security policy management server **120** (*e.g.*, packets addressed to or from the extracted address and port number) and may perform the packet transformation function configured to route the packets to monitoring device **608**. For example, the packet transformation function configured to route the packets to monitoring device **608** may be packet transformation function 2 **218**. When packet transformation function 2 **218** receives the packets from packet filter **214**, it may encapsulate them with an IP header having an address corresponding to monitoring device **608** and may then forward them to network E **110**. Once forwarded, the packets may be routed based on the address specified by the encapsulating header, and may thus be communicated to monitoring device **608**. When the packets are received by monitoring device **608**, monitoring device **608** may copy the packets or data contained within them, and strip the encapsulating header from them. Monitoring device **608** may then forward the packets, without the encapsulating header, to network E **110**. Network E **110** may receive the packets forwarded by monitoring device **608** and may route them based on their destination address (*e.g.*, to UE **602**).

[64] In some embodiments, packet security gateway **112** may be configured to perform multiple packet transformation functions on the packets associated with the VoIP call between UEs **600** and **602**. For example, packet filter **214** may identify the packets as matching the criteria specified by the dynamic security policy received from security policy management server **120** and may forward the packets to packet transformation functions 1 **216** and 2 **218**. Packet transformation function 1 **216** may be configured to forward the packets to their destination address (*e.g.*, to UE **602**) and packet transformation function 2 **218** may be configured to encapsulate the packets (or a copy of the packets) with an IP header having an address corresponding to monitoring device **608** and then forward the encapsulated packets to network E **110**. Once forwarded, the encapsulated packets may be routed based on the address specified by the encapsulating header, and may thus be communicated to monitoring device **608**, which may store the packets or data contained within them for subsequent review or analysis (*e.g.*, by a law enforcement or national security authority). In such embodiments, it may not be necessary for monitoring device **608** to strip the encapsulating header from the packets or route them based on their destination address (*e.g.*, to UE **602**) because packet transformation function 1 **216** may have already forwarded the packets to their destination address (*e.g.*, to UE **602**).

[65] It will be appreciated that SIP switch **604**'s analysis application **610** may similarly detect SIP signaling associated with the termination of the VoIP call between UE **600** and UE **602** and may publish the SIP messages to security policy management server **120**. Security policy management server **120** may utilize one or more network addresses and port numbers within the messages to construct a new dynamic security policy or modify one or more rules within an existing dynamic security policy and communicate the new or modified dynamic security policy to packet security gateway **112** in order to ensure that future packets associated with the network address and port number but not associated with SIP URI exampleuser@exampledomain.com are not routed to monitoring device **608**. Security policy management server **120** may communicate any dynamic security policy constructed or modified based on SIP messages to any of multiple packet security gateways (*e.g.*, packet security gateways **114** and **116**) within network environment **100** in order to ensure that all packets associated with the VoIP call between UE **600** and UE **602** are forwarded to monitoring device **608**.

[66] FIG. 7 illustrates an exemplary network environment that includes a secured network having multiple boundaries with unsecured networks in which one or more embodiments may be implemented. Network environment **700** may include networks A – C **702**, **704**, and **706**. Networks A **702** and B **704** may be a LAN or WAN associated with an organization (*e.g.*, a company, university, enterprise, or government agency). One or more networks within network environment **700** may interface with one or more other networks within network environment **700**. For example, the organizations associated with networks A **702** and B **704** may subscribe to an ISP to provide interconnectivity between their respective networks or allow public access to their respective networks (*e.g.*, via the Internet). Each of networks A **702** and B **704** may be connected to network C **706**, which may be the ISP's network. The ISP may desire to offer an interconnection service between networks A **702** and B **704**, but may also want to enforce one or more dynamic security policies with respect to traffic traversing network C **706**.Accordingly, one or more packet security gateways may be located at each boundary between network A **702** and network C **706**, and each boundary between network B **704** and network C **706**. For example, packet security gateway **708** and packet security gateway **710** may be respectively located at first and second boundaries between networks A **702** and C **706**. Similarly, packet security gateways **712** and **714** may be respectively located at first and second boundaries between networks B **704** and C **706**. Each of packet security gateways **708**, **710**, **712**, and **714** may be associated with security policy management server **716**.

[67] Security policy management server **716** may maintain one or more dynamic security policies configured for protecting network C **706**, and may be managed by the ISP associated with network C **706**. Security policy management server **716** may ensure that each of packet security gateways **708**, **710**, **712**, and **714** protect each of their respective boundaries with network C **706** in a uniform manner. For example, security policy management server **716** may be configured to communicate one or more dynamic security policies it maintains to each of packet security gateways **708**, **710**, **712**, and **714** on a periodic basis, in response to being directed to by a network operator associated with network environment **700**, in response to detected network conditions (*e.g.*, an attack or high resource utilization), or in response to a request from one or more of packet security gateways **708**, **710**, **712**, or **714**.

[68] In some embodiments, security policy management server **716** may be configured to communicate different dynamic security policies to one or more of packet security gateways **708**, **710**, **712**, and **714** based on, for example, their respective locations within network environment **700**. For example, security policy management server **716** may be configured to implement one or more anti-spoofing techniques (*e.g.*, ingress filtering or Best Current Practice (BCP) 38, as described by Internet Engineering Task Force (IETF) Request For Comment (RFC) 2827) with respect to network environment **700**. Effective implementation of such techniques may require that a dynamic security policy be based on the location at which it is being implemented. For example, a dynamic security policy that implements ingress filtering may comprise one or more rules that filter based on a packet's source address, identifying packets having source addresses that could not possibly have originated from a network downstream of the ingress filtering point (*e.g.*, packets having spoofed source addresses). Such rules may vary depending on the boundary point for which they are implemented (*e.g.*, a packet for one boundary may be properly identified as spoofed, yet a packet having the same source address may be legitimate traffic at a different boundary point). Accordingly, security policy management server **716** may be configured to communicate different dynamic security policies to one or more of packet security gateways **708**, **710**, **712**, and **714** based on their respective locations within network environment **700**. For example, security policy management server **716** may communicate a dynamic security policy to packet security gateways **708** and **710** that includes one or more rules for performing ingress filtering for network A **702** (*e.g.*, for identifying packets having source addresses that could not have originated within network A **702**) and a different dynamic security policy to packet security gateways **712** and **714** that includes one or more rules for performing ingress filtering for network B **704** (*e.g.*, for identifying packets having source addresses that could not have originated within network B **704**).

[69] It will be appreciated that by maintaining uniform dynamic security policies at each boundary between networks A **702** and C **706**, as well as at each boundary between networks B **704** and C **706**, security policy management server **716** and packet security gateways **708**, **710**, **712**, and **714** may aid the ISP associated with network C **706** in protecting network C **706** from network attacks.

[70] FIG. 8 illustrates an exemplary network environment that includes multiple distinct secured networks in which one or more embodiments may be implemented. Referring to FIG. 8, network environment **800** may include networks A **802**, B **804**, and C **806**. Each of networks A **802** and B **804** may interface with network C **806** at multiple boundaries within network environment **800**. Packet security gateways **808** and **810** may be respectively located at first and second boundaries between networks A **802** and C **806**. Similarly, packet security gateways **812** and **814** may be respectively located at first and second boundaries between networks B **804** and C **806**.

[71] Network A **802** and B **804** may both be associated with a common organization (*e.g.*, a company, university, enterprise, or government agency), or may each be associated with a distinct organization. In the former case, the common organization may desire to utilize one or more dynamic security policies with respect to network A **802** and one or more different dynamic security policies with respect to network B **804**. In the latter case, an organization associated with network A **802** may desire to utilize one or more dynamic security policies with respect to network A **802** and a different organization associated with network B **804** may desire to utilize one or more different dynamic security policies with respect to network B **804**. Network environment **800** may include security policy management servers A **816** and B **818**. Security policy management server A **816** may be associated with network A **802** and may maintain one or more dynamic security policies configured for protecting network A **802**. Similarly, security policy management server B **818** may be associated with network B **804** and may maintain one or more dynamic security policies configured for protecting network B **804**.

[72] Packet security gateways **808** and **810** may be associated with security policy management server A **816**. Similarly, packet security gateways **812** and **814** may be associated with security policy management server B **818**. Security policy management server A **816** may ensure that packet security gateways **808** and **810** protect each of their respective boundaries with network C **806** in a uniform manner. For example, security policy management server A **816** may be configured to communicate one or more dynamic security policies it maintains to packet security gateways **808** and **810** on a periodic basis, in response to being directed to by a network operator associated with network A **802**, in response to detected

network conditions (*e.g.*, an attack or high resource utilization), or in response to a request from packet security gateway **808** or **810**. Similarly, security policy management server B **818** may ensure that packet security gateways **812** and **814** protect each of their respective boundaries with network C **806** in a uniform manner. For example, security policy management server B **818** may be configured to communicate one or more dynamic security policies it maintains to packet security gateways **812** and **814** on a periodic basis, in response to being directed to by a network operator associated with network B **804**, in response to detected network conditions (*e.g.*, an attack or high resource utilization), or in response to a request from packet security gateway **812** or **814**. By utilizing distinct security policy management servers (*e.g.*, security policy management servers A **816** and B **818**), one or more operators associated with distinct networks (*e.g.*, networks A **802** and B **804**) may maintain uniform dynamic security policies at each boundary of their respective networks, while simultaneously enabling different dynamic security policies to be maintained for each network. Similarly, by utilizing distinct security policy management servers (*e.g.*, security policy management servers A **816** and B **818**), one or more operators associated with a single organization that desires to maintain distinct networks (*e.g.*, networks A **802** and B **804**) may maintain uniform dynamic security policies at each boundary of their distinct networks, while simultaneously enabling different dynamic security policies to be maintained for each network.

[73] FIG. 9 illustrates an exemplary secure LAN environment protected in accordance with one or more aspects of the disclosure. Referring to FIG. 9, network environment **900** may be a LAN, including hosts A **902**, B **904**, and C **906**. It may also include LAN switch **908**. LAN switch **908** may be configured to switch network traffic (*e.g.*, packets) between one or more of hosts A **902**, B **904**, and C **906**. For example, LAN switch **908** may include a switching matrix configured to switch packets received from one or more of hosts A **902**, B **904**, and C **906** to one or more of hosts A **902**, B **904**, and C **906**. LAN switch **908** may be associated with packet security gateway **910**, and network environment **900** may include security policy management server **912**.

[74] In some embodiments, packet security gateway **910** may be embedded within LAN switch **908**. Alternatively, packet security gateway **910** may be a device distinct from LAN switch

908, and LAN switch **908** may be configured to route network traffic through packet security gateway **910** (*e.g.*, by modifying LAN switch **908**'s switching matrix). Packet security gateway **910** may be configured to receive one or more dynamic security policies from security policy management server **912**. The dynamic security policies received from security policy management server **912** may include one or more rules specifying criteria associated with one or more of hosts A **902**, B **904**, and C **906**, and may further specify one or more packet transformation functions to be performed on packets matching the specified criteria. Packet security gateway **910** may identify packets matching one or more of the criteria specified by the rules and may perform the associated packet transformation functions on the identified packets. By utilizing packet security gateway **910** within network environment **900**, an operator of network environment **900** may be able to protect network environment **900** from network attacks, as well as implement one or more services (*e.g.*, blocklist service, allowlist service, VoIP firewall service, phased restoration service, enqueueing service, multi-dimensional routing service, or monitoring service) within network environment **900**. Network environment **900** may include multiple LAN switches with embedded or associated packet security gateways, each of the packet security gateways configured to receive one or more dynamic security policies from security policy management server **912**.

[75] FIG. 10 illustrates an exemplary method for protecting a secured network in accordance with one or more embodiments. The steps may be performed at each of one or more packet security gateways associated with a security policy management server. For example, each of packet security gateways **112**, **114**, **116**, and **118** may be associated with security policy management server **120**, and the steps may be performed at each of packet security gateways **112**, **114**, **116**, and **118**. At step **1000**, a dynamic security policy is received from the security policy management server. For example, packet security gateway **112** may receive dynamic security policy **300** from security policy management server **120**. At step **1002**, packets associated with a network protected by each respective packet security gateway are received. For example, packet security gateway **112** may receive UDP packets from a device within network E **110** having an address that begins with 150 and that are destined for port 3030 of a device within network A **102**. At step **1004**, a packet transformation function specified by the dynamic security policy is performed on the

packets. For example, rule **308** of dynamic security policy **300** may specify that packets using the UDP protocol, coming from a source address that begins with 150, having any source port, destined for any address, and destined for port 3030 should have an accept packet transformation function performed on them, packet filter **214** may identify the UDP packets received from the device within network E **110** as matching the criteria specified by rule **308**, packet transformation function 1 **216** may be configured to forward packets, and packet security gateway **112** may utilize packet transformation function 1 **216** to perform the accept packet transformation function specified by rule **308** on the UDP packets received from the device within network E **110**.

[76] The functions and steps described herein may be embodied in computer-usable data or computer-executable instructions, such as in one or more program modules, executed by one or more computers or other devices to perform one or more functions described herein. Generally, program modules include routines, programs, objects, components, data structures, etc. that perform particular tasks or implement particular abstract data types when executed by one or more processors in a computer or other data processing device. The computer-executable instructions may be stored on a computer-readable medium such as a hard disk, optical disk, removable storage media, solid state memory, RAM, etc. As will be appreciated, the functionality of the program modules may be combined or distributed as desired in various embodiments. In addition, the functionality may be embodied in whole or in part in firmware or hardware equivalents, such as integrated circuits, application-specific integrated circuits (ASICs), field programmable gate arrays (FPGA), and the like. Particular data structures may be used to more effectively implement one or more aspects of the disclosure, and such data structures are contemplated to be within the scope of computer executable instructions and computer-usable data described herein.

[77] Although not required, one of ordinary skill in the art will appreciate that various aspects described herein may be embodied as a method, an apparatus, or as one or more computer-readable media storing computer-executable instructions. Accordingly, those aspects may take the form of an entirely hardware embodiment, an entirely software embodiment, an entirely firmware embodiment, or an embodiment combining software, hardware, and firmware aspects in any combination.

[78] As described herein, the various methods and acts may be operative across one or more computing servers and one or more networks. The functionality may be distributed in any manner, or may be located in a single computing device (e.g., a server, a client computer, etc.).

[79] Aspects of the disclosure have been described in terms of illustrative embodiments thereof. Numerous other embodiments, modifications, and variations within the scope and spirit of the appended claims will occur to persons of ordinary skill in the art from a review of this disclosure. For example, one of ordinary skill in the art will appreciate that the steps illustrated in the illustrative figures may be performed in other than the recited order, and that one or more steps illustrated may be optional.

What is claimed is:

1. A method, comprising:

at each of one or more packet security gateways associated with a security policy management server:

receiving a dynamic security policy from the security policy management server;

receiving packets associated with a network protected by each respective packet security gateway; and

performing, on a packet by packet basis, at least one of multiple packet transformation functions specified by the dynamic security policy on the packets, wherein performing the at least one of multiple packet transformation functions specified by the dynamic security policy on the packets comprises performing at least one packet transformation function other than forwarding or dropping the packets.

2. The method of claim 1, wherein the one or more packet security gateways comprise at least two packet security gateways configured in series such that packets forwarded from a first of the at least two packet security gateways are received by a second of the at least two packet security gateways.

3. The method of claim 2, wherein the dynamic security policy comprises at least two rules, a second of the at least two rules being required to execute subsequent to a first of the at least two rules, and wherein, for the at least two packet security gateways configured in series, performing the at least one of multiple packet transformation functions specified by the dynamic security policy on the packets comprises: performing, by the first of the at least two packet security gateways, a first packet transformation function specified by the first of the at least two rules; and performing, by the second of the at least two packet security gateways, a second packet transformation function specified by the second of the at least two rules.

4. The method of claim 1, wherein the dynamic security policy comprises at least one rule specifying a set of network addresses for which associated packets should be dropped and at least one rule specifying that all packets associated with network addresses outside the set should be forwarded.

5. The method of claim 1, wherein the dynamic security policy comprises at least one rule specifying a set of network addresses for which associated packets should be forwarded and at least one rule specifying that all packets associated with network addresses outside the set should be dropped.

6. The method of claim 5, further comprising receiving, by the security policy management server, information associated with a Voice over Internet Protocol (VoIP) session, and wherein the at least one rule specifying the set of network addresses for which associated packets should be forwarded is one of created and altered by the security policy management server utilizing the information associated with the one or more VoIP sessions.

7. The method of claim 5, wherein receiving the dynamic security policy from the security policy management server comprises receiving at least three dynamic security policies from the security policy management server, a first of the at least three dynamic security policies being received at a first time and specifying a first set of network addresses for which packets should be forwarded, a second of the at least three dynamic security policies being received at a second time after the first time and specifying a second set of network addresses for which packets should be forwarded that includes more network addresses than the first set of network addresses, and a third of the at least three dynamic security policies being received at a third time after the second time and specifying a third set of network addresses for which packets should be forwarded that includes more network addresses than the second set of network addresses.

8. The method of claim 1, wherein the dynamic security policy comprises at least two rules, a first of the at least two rules specifying a first set of network addresses, a second of the at least two rules specifying a second set of network addresses, and wherein the dynamic

security policy specifies that packets associated with the first set of network addresses should be placed in a first forwarding queue and packets associated with the second set of network addresses should be placed in a second forwarding queue, the first forwarding queue having a higher forwarding rate than the second forwarding queue.

9. The method of claim 1, wherein the dynamic security policy comprises at least one rule specifying a set of network addresses and an additional parameter, and wherein performing the at least one of multiple packet transformation functions specified by the dynamic security policy on the packets comprises routing at least one of the packets that falls within the set of network addresses and matches the additional parameter to a network address different from a destination network address specified by the at least one of the packets.

10. The method of claim 9, wherein the additional parameter comprises a Session Initiation Protocol (SIP) Uniform Resource Identifier (URI), wherein the network address different from the destination network address specified by the at least one of the packets corresponds to a network device configured to copy information contained in the at least one of the packets and forward the at least one of the packets to the destination network address specified by the at least one of the packets, and wherein routing the at least one of the packets that falls within the set of network addresses and matches the additional parameter to a network address different from the destination network address specified by the at least one of the packets comprises encapsulating the at least one of the packets that falls within the set of network addresses and matches the additional parameter with a header containing the network address different from the destination network address specified by the at least one of the packets.

11. The method of claim 1, wherein the at least one of the multiple packet transformation functions comprises at least one of forwarding the packets into the network protected by the packet security gateway, forwarding the packets out of the network protected by the packet security gateway, forwarding the packets to an Internet Protocol Security (IPsec) stack having an IPsec security association corresponding to the packets, and dropping the packets.

12. The method of claim 1, wherein the dynamic security policy comprises a plurality of rules, and wherein at least one of the rules specifies a five-tuple, the five-tuple specifying one or more protocols, one or more IP source addresses, one or more source port values, one or more IP destination addresses, and one or more destination port values.

13. The method of claim 1, wherein the dynamic security policy comprises a plurality of rules, and wherein at least one of the rules specifies a Differentiated Service Code Point (DSCP) selector that maps to a DSCP field in an Internet Protocol (IP) header of the packets.

14. The method of claim 1, wherein at least one of the one or more packet security gateways operates in a network layer transparent manner by sending and receiving traffic at a link layer using an interface that is not addressed at the network layer and performing the at least one of the multiple packet transformation functions at the network layer.

15. The method of claim 14, wherein the at least one of the one or more packet security gateways includes a management interface having a network layer address, and wherein access to the management interface is secured at at least one of an application level, a link level, and a transport level.

16. The method of claim 1, wherein the dynamic security policy comprises one or more rules generated based, at least in part, on a list of known network addresses associated with malicious network traffic that is received from a subscription service that aggregates information associated with malicious network traffic.

17. The method of claim 1, wherein at least two of the one or more packet security gateways receive dynamic security policies from the security policy management server that include one or more rules specifying source addresses that correspond to spoofed network addresses, and wherein at least one of the dynamic security policies specifies different source addresses that correspond to spoofed network addresses than at least another one of the dynamic security policies.

18. The method of claim 1, wherein at least one of the one or more packet security gateways is located at each boundary between a protected network associated with the security policy management server and an unprotected network.

19. A system, comprising:

a security policy management server; and

one or more packet security gateways associated with the security policy management server, wherein each of the one or more packet security gateways is configured to:

receive a dynamic security policy from the security policy management server;

receive packets associated with a network protected by each respective packet security gateway; and

perform, on a packet by packet basis, at least one of multiple packet transformation functions specified by the dynamic security policy on the packets, wherein each of the one or more packet security gateways is configured to perform the at least one of multiple packet transformation functions specified by the dynamic security policy on the packets by performing at least one packet transformation function other than forwarding or dropping the packets.

20. One or more non-transitory computer-readable media having instructions stored thereon, that when executed by one or more computers, cause the one or more computers to:

at each of one or more packet security gateways associated with a security policy management server:

receive a dynamic security policy from the security policy management server;

receive packets associated with a network protected by each respective packet security gateway; and

perform, on a packet by packet basis, at least one of multiple packet transformation functions specified by the dynamic security policy on the packets, wherein each of the one or more packet security gateways is configured to perform

the at least one of multiple packet transformation functions specified by the dynamic security policy on the packets by performing at least one packet transformation function other than forwarding or dropping the packets.

ABSTRACT

Methods and systems for protecting a secured network are presented. For example, one or more packet security gateways may be associated with a security policy management server. At each packet security gateway, a dynamic security policy may be received from the security policy management server, packets associated with a network protected by the packet security gateway may be received, and at least one of multiple packet transformation functions specified by the dynamic security policy may be performed on the packets. Performing the at least one of multiple packet transformation functions specified by the dynamic security policy on the packets may include performing at least one packet transformation function other than forwarding or dropping the packets.

PTO/AIA/01 (06-12)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE

DECLARATION (37 CFR 1.63) FOR UTILITY OR DESIGN APPLICATION USING AN APPLICATION DATA SHEET (37 CFR 1.76)

Title of Invention	METHODS AND SYSTEMS FOR PROTECTING A SECURED NETWORK

As the below named inventor, I hereby declare that:

This declaration is directed to:

- [x] The attached application, or
- [ ] United States application or PCT international application number _____ filed on _____.

The above-identified application was made or authorized to be made by me.

I believe that I am the original inventor or an original joint inventor of a claimed invention in the application.

I hereby acknowledge that any willful false statement made in this declaration is punishable under 18 U.S.C. 1001 by fine or imprisonment of not more than five (5) years, or both.

WARNING:

Petitioner/applicant is cautioned to avoid submitting personal information in documents filed in a patent application that may contribute to identity theft. Personal information such as social security numbers, bank account numbers, or credit card numbers (other than a check or credit card authorization form PTO-2038 submitted for payment purposes) is never required by the USPTO to support a petition or an application. If this type of personal information is included in documents submitted to the USPTO, petitioners/applicants should consider redacting such personal information from the documents before submitting them to the USPTO. Petitioner/applicant is advised that the record of a patent application is available to the public after publication of the application (unless a non-publication request in compliance with 37 CFR 1.213(a) is made in the application) or issuance of a patent. Furthermore, the record from an abandoned application may also be available to the public if the application is referenced in a published application or an issued patent (see 37 CFR 1.14). Checks and credit card authorization forms PTO-2038 submitted for payment purposes are not retained in the application file and therefore are not publicly available.

LEGAL NAME OF INVENTOR

Inventor: Sean Moore Date (Optional): 01-Oct-2012

Signature: Sean Moore

Note: An application data sheet (PTO/SB/14 or equivalent), including naming the entire inventive entity, must accompany this form or must have been previously filed. Use an additional PTO/AIA/01 form for each additional inventor.

PTO/AIA/01 (06-12)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE

DECLARATION (37 CFR 1.63) FOR UTILITY OR DESIGN APPLICATION USING AN APPLICATION DATA SHEET (37 CFR 1.76)

Title of Invention	METHODS AND SYSTEMS FOR PROTECTING A SECURED NETWORK

As the below named inventor, I hereby declare that:

This declaration is directed to:

- [■] The attached application, or
- [ ] United States application or PCT international application number _____ filed on _____.

The above-identified application was made or authorized to be made by me.

I believe that I am the original inventor or an original joint inventor of a claimed invention in the application.

I hereby acknowledge that any willful false statement made in this declaration is punishable under 18 U.S.C. 1001 by fine or imprisonment of not more than five (5) years, or both.

WARNING:

Petitioner/applicant is cautioned to avoid submitting personal information in documents filed in a patent application that may contribute to identity theft. Personal information such as social security numbers, bank account numbers, or credit card numbers (other than a check or credit card authorization form PTO-2038 submitted for payment purposes) is never required by the USPTO to support a petition or an application. If this type of personal information is included in documents submitted to the USPTO, petitioners/applicants should consider redacting such personal information from the documents before submitting them to the USPTO. Petitioner/applicant is advised that the record of a patent application is available to the public after publication of the application (unless a non-publication request in compliance with 37 CFR 1.213(a) is made in the application) or issuance of a patent. Furthermore, the record from an abandoned application may also be available to the public if the application is referenced in a published application or an issued patent (see 37 CFR 1.14). Checks and credit card authorization forms PTO-2038 submitted for payment purposes are not retained in the application file and therefore are not publicly available.

LEGAL NAME OF INVENTOR

Inventor: Steven Rogers _____ Date (Optional): _____

Signature: _____

Note: An application data sheet (PTO/SB/14 or equivalent), including naming the entire inventive entity, must accompany this form or must have been previously filed. Use an additional PTO/AIA/01 form for each additional inventor.

PTO/SB/96 (01-09)
Approved for use through 02/28/2009. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

STATEMENT UNDER 37 CFR 3.73(b)

Applicant/Patent Owner: Washington University

Application No./Patent No.: 12/845,516 Filed/Issue Date: July 28, 2010

Titled: RECOMBINANT ALPHAVIRUS-BASED VECTORS WITH REDUCED INHIBITION OF CELLULAR MACROMOLECULAR SYNTHESIS

Washington University , a university
(Name of Assignee) (Type of Assignee, e.g., corporation, partnership, university, government agency, etc.

states that it is:

1. ☐ the assignee of the entire right, title, and interest in;

2. ☐ an assignee of less than the entire right, title, and interest in
(The extent (by percentage) of its ownership interest is _____ %); or

3. ☒ the assignee of an undivided interest in the entirety of (a complete assignment from one of the joint inventors was made)

the patent application/patent identified above, by virtue of either:

A. ☒ An assignment from the inventor(s) of the patent application/patent identified above. The assignment was recorded in the United States Patent and Trademark Office at Reel 009686, Frame 0436, or for which a copy therefore is attached.

OR

B. ☐ A chain of title from the inventor(s), of the patent application/patent identified above, to the current assignee as follows:

1. From: _____ To: _____
The document was recorded in the United States Patent and Trademark Office at
Reel _____, Frame _____, or for which a copy thereof is attached.

2. From: _____ To: _____
The document was recorded in the United States Patent and Trademark Office at
Reel _____, Frame _____, or for which a copy thereof is attached.

3. From: _____ To: _____
The document was recorded in the United States Patent and Trademark Office at
Reel _____, Frame _____, or for which a copy thereof is attached.

☐ Additional documents in the chain of title are listed on a supplemental sheet(s).

☐ As required by 37 CFR 3.73(b)(1)(i), the documentary evidence of the chain of title from the original owner to the assignee was, or concurrently is being, submitted for recordation pursuant to 37 CFR 3.11.

[NOTE: A separate copy (*i.e.*, a true copy of the original assignment document(s)) must be submitted to Assignment Division in accordance with 37 CFR Part 3, to record the assignment in the records of the USPTO. See MPEP 302.08]

The undersigned (whose title is supplied below) is authorized to act on behalf of the assignee.

Signature	10/10/2012 Date
Jon Kratochvil Printed or Typed Name	Business Dev. Director Title

PTO/SB/96 (01-09)
Approved for use through 02/28/2009 OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

STATEMENT UNDER 37 CFR 3.73(b)

Applicant/Patent Owner: Novartis Vaccines and Diagnostics, Inc.

Application No./Patent No.: 12/845,516 Filed/Issue Date: July 28, 2010

Titled: RECOMBINANT ALPHAVIRUS-BASED VECTORS WITH REDUCED INHIBITION OF CELLULAR MACROMOLECULAR SYNTHESIS

Novartis Vaccines and Diagnostics, Inc. , a corporation

(Name of Assignee) (Type of Assignee, e.g., corporation, partnership, university, government agency, etc.

states that it is:

1. ☐ the assignee of the entire right, title, and interest in;

2. ☐ an assignee of less than the entire right, title, and interest in
(The extent (by percentage) of its ownership interest is _____ %); or

3. ☒ the assignee of an undivided interest in the entirety of (a complete assignment from one of the joint inventors was made)

the patent application/patent identified above, by virtue of either:

A. ☐ An assignment from the inventor(s) of the patent application/patent identified above. The assignment was recorded in the United States Patent and Trademark Office at Reel _____, Frame _____, or for which a copy therefore is attached.

OR

B. ☒ A chain of title from the inventor(s), of the patent application/patent identified above, to the current assignee as follows:

1. From: DUBENSKY, POLO, and BELLI To: Chiron Corporation

The document was recorded in the United States Patent and Trademark Office at
Reel 009686, Frame 0421, or for which a copy thereof is attached.

2. From: Chiron Corporation To: Novartis Vaccines and Diagnostics, Inc.

The document was recorded in the United States Patent and Trademark Office at
Reel 022262, Frame 0395, or for which a copy thereof is attached.

3. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at
Reel _____, Frame _____, or for which a copy thereof is attached.

☐ Additional documents in the chain of title are listed on a supplemental sheet(s).

☒ As required by 37 CFR 3.73(b)(1)(i), the documentary evidence of the chain of title from the original owner to the assignee was, or concurrently is being, submitted for recordation pursuant to 37 CFR 3.11.

[NOTE: A separate copy (*i.e.*, a true copy of the original assignment document(s)) must be submitted to Assignment Division in accordance with 37 CFR Part 3, to record the assignment in the records of the USPTO. See MPEP 302.08]

The undersigned (whose title is supplied below) is authorized to act on behalf of the assignee.

Regina Bautista 10/16/12

Signature Date

Regina Bautista Attorney-in-fact

Printed or Typed Name Title

PTO/AIA/80 (07-12)
Approved for use through 11/30/2014. OMB 0651-0035
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE

POWER OF ATTORNEY TO PROSECUTE APPLICATIONS BEFORE THE USPTO

I hereby revoke all previous powers of attorney given in the application identified in the attached statement under 37 CFR 3.73(c).

I hereby appoint:

■ Practitioners associated with Customer Number: 22907

OR

☐ Practitioner(s) named below (if more than ten patent practitioners are to be named, then a customer number must be used):

Name	Registration Number	Name	Registration Number

As attorney(s) or agent(s) to represent the undersigned before the United States Patent and Trademark Office (USPTO) in connection with any and all patent applications assigned only to the undersigned according to the USPTO assignment records or assignments documents attached to this form in accordance with 37 CFR 3.73(c).

Please change the correspondence address for the application identified in the attached statement under 37 CFR 3.73(c) to:

☑ The address associated with Customer Number: 22907

OR

☐

Firm or Individual Name			
Address			
City		State	Zip
Country			
Telephone		Email	

Assignee Name and Address: Centripetal Networks, Inc.
41378 Raspberry Drive
Leesburg, VA 20176-7826

A copy of this form, together with a statement under 37 CFR 3.73(c) (Form PTO/AIA/96 or equivalent) is required to be Filed in each application in which this form is used. The statement under 37 CFR 3.73(c) may be completed by one of The practitioners appointed in this form, and must identify the application in which this Power of Attorney is to be filed.

SIGNATURE of Assignee of Record

The individual whose signature and title is supplied below is authorized to act on behalf of the assignee

Signature	/Steven Rogers/	Date	
Name	Steven Rogers	Telephone	(571) 252-5082
Title	Chief Executive Officer		

PTO/SB/96 (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

STATEMENT UNDER 37 CFR 3.73(b)

Applicant/Patent Owner: Steven Rogers et al.

Application No./Patent No.: 13/657,010 Filed/Issue Date: October 22, 2012

Titled: Methods and Systems for Protecting a Secured Network

Centripetal Networks, Inc. , a corporation

(Name of Assignee) (Type of Assignee, e.g., corporation, partnership, university, government agency, etc.

states that it is:

1. ☒ the assignee of the entire right, title, and interest in;

2. ☐ an assignee of less than the entire right, title, and interest in (The extent (by percentage) of its ownership interest is _____ %); or

3. ☐ the assignee of an undivided interest in the entirety of (a complete assignment from one of the joint inventors was made)

the patent application/patent identified above, by virtue of either:

A. ☒ An assignment from the inventor(s) of the patent application/patent identified above. The assignment was recorded in the United States Patent and Trademark Office at Reel _____, Frame _____, or for which a copy therefore is attached.

OR

B. ☐ A chain of title from the inventor(s), of the patent application/patent identified above, to the current assignee as follows:

1. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at

Reel _____, Frame _____, or for which a copy thereof is attached.

2. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at

Reel _____, Frame _____, or for which a copy thereof is attached.

3. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at

Reel _____, Frame _____, or for which a copy thereof is attached.

☐ Additional documents in the chain of title are listed on a supplemental sheet(s).

☒ As required by 37 CFR 3.73(b)(1)(i), the documentary evidence of the chain of title from the original owner to the assignee was, or concurrently is being, submitted for recordation pursuant to 37 CFR 3.11.

[NOTE: A separate copy (*i.e.*, a true copy of the original assignment document(s)) must be submitted to Assignment Division in accordance with 37 CFR Part 3, to record the assignment in the records of the USPTO. See MPEP 302.08]

The undersigned (whose title is supplied below) is authorized to act on behalf of the assignee.

/William E. Wooten/ 10-23-2012

Signature Date

William E. Wooten Attorney of Record

Printed or Typed Name Title

Privacy Act Statement

The **Privacy Act of 1974 (P.L. 93-579)** requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (*i.e.*, GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Electronic Acknowledgement Receipt

EFS ID:	14055117
Application Number:	13657010
International Application Number:	
Confirmation Number:	2390
Title of Invention:	METHODS AND SYSTEMS FOR PROTECTING A SECURED NETWORK
First Named Inventor/Applicant Name:	Steven Rogers
Customer Number:	22907
Filer:	William Eugene Wooten/Leatrice sims
Filer Authorized By:	William Eugene Wooten
Attorney Docket Number:	007742.00017
Receipt Date:	23-OCT-2012
Filing Date:	
Time Stamp:	15:47:02
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Power of Attorney	poa.pdf	2649391 ddfc36155a7100c549e54dcacd4db23293abaa09	no	1
Warnings:					
Information:					

2	CRF Statement Paper and CRF are the same	373b.pdf	421664 44d14f41b9e8b738efb26dfb688f9c9d46a49adb	no	2

Warnings:	
Information:	
Total Files Size (in bytes):	3071055

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:	)	Confirmation No. 2390
	)	
Steven ROGERS et al.	)	Group Art No. TBD
	)	
Serial No: 13/657,010	)	Examiner: TBD
	)	
Filed: October 22, 2012	)	Docket No. 007742.00017
	)	
For: **Methods and Systems for Protecting a Secured Network**	)	

REQUEST FOR REFUND

U.S. Patent and Trademark Office
Randolph Building
401 Dulany Street
Alexandria, VA 22314

Sir:

Upon filing the above-identified application via the United States Patent and Trademark Office's EFS-web filing system on October 22, 2012, Applicants' representative mistakenly paid fees for Large Entity status in the amount of $1260. As indicated in the Application Data Sheet, however, Applicants are entitled to small entity status. Accordingly, Applicants hereby respectfully request a refund for the difference between Large Entity and Small Entity fees in the amount of $630.00 be credited to our Deposit Account 19-0733.

Respectfully submitted,

BANNER & WITCOFF, LTD.

Date: November 6, 2012

By: /William E. Wooten/
William E. Wooten
Registration No. 60,049

Banner & Witcoff, Ltd.
1100 13th St., NW
Washington, DC 20005-4051
Telephone: (202) 824-3000
Facsimile: (202) 824-3001

Electronic Acknowledgement Receipt

EFS ID:	14156673
Application Number:	13657010
International Application Number:	
Confirmation Number:	2390
Title of Invention:	METHODS AND SYSTEMS FOR PROTECTING A SECURED NETWORK
First Named Inventor/Applicant Name:	Steven Rogers
Customer Number:	22907
Filer:	William Eugene Wooten/Leatrice Sims
Filer Authorized By:	William Eugene Wooten
Attorney Docket Number:	007742.00017
Receipt Date:	06-NOV-2012
Filing Date:	
Time Stamp:	10:26:28
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Refund Request	REQUEST_for_REFUND.pdf	78543 d2bd4732baf575b701234d6611c6a02630b2168f	no	1

Warnings:	
Information:	

Total Files Size (in bytes):	78543

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:	)	Confirmation No. 2390
Steven ROGERS et al.	)	Group Art No. TBD
Serial No: 13/657,010	)	Examiner: TBD
Filed: October 22, 2012	)	Docket No. 007742.00017
For: **Methods and Systems for Protecting a Secured Network**	)	

2012 NOV -6 P 4:34

REQUEST FOR REFUND

U.S. Patent and Trademark Office
Randolph Building
401 Dulany Street
Alexandria, VA 22314

Sir:

Upon filing the above-identified application via the United States Patent and Trademark Office's EFS-web filing system on October 22, 2012, Applicants' representative mistakenly paid fees for Large Entity status in the amount of $1260. As indicated in the Application Data Sheet, however, Applicants are entitled to small entity status. Accordingly, Applicants hereby respectfully request a refund for the difference between Large Entity and Small Entity fees in the amount of $630.00 be credited to our Deposit Account 19-0733.

Respectfully submitted,

BANNER & WITCOFF, LTD.

Date: November 6, 2012

By: /William E. Wooten/
William E. Wooten
Registration No. 60,049

Banner & Witcoff, Ltd.
1100 13th St., NW
Washington, DC 20005-4051
Telephone: (202) 824-3000
Facsimile: (202) 824-3001

Electronic Patent Application Fee Transmittal

Application Number:	
Filing Date:	
Title of Invention:	Methods and Systems for Protecting a Secured Network
First Named Inventor/Applicant Name:	Steven Rogers
Filer:	William Eugene Wooten/leatrice sims
Attorney Docket Number:	007742.00017

Filed as Large Entity

Utility under 35 USC 111(a) Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Utility application filing	1011	1	390	390
Utility Search Fee	1111	1	620	620
Utility Examination Fee	1311	1	250	250
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				

Adjustment date: 11/13/2012 SDIRETA1 13657010
10/23/2012 INTEFSW 00000624 190733
01 FC:1011 390.00 CR
02 FC:1111 620.00 CR
03 FC:1311 250.00 CR

11/13/2012 SDIRETA1 00000004 190733 13657010
01 FC:4011 98.00 DA
02 FC:2111 310.00 DA
03 FC:2311 125.00 DA

PATENT APPLICATION FEE DETERMINATION RECORD

Substitute for Form PTO-875

Application or Docket Number: 13/657,010

APPLICATION AS FILED - PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA	SMALL ENTITY RATE($)	SMALL ENTITY FEE($)	OR	OTHER THAN SMALL ENTITY RATE($)	OTHER THAN SMALL ENTITY FEE($)
BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A	98		N/A	
SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A	310		N/A	
EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A	125		N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	20 minus 20 =	*	x 31 =	0.00	OR		
INDEPENDENT CLAIMS (37 CFR 1.16(h))	3 minus 3 =	*	x 125 =	0.00			
APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).			0.00			
MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))				0.00			
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL	533		TOTAL	

APPLICATION AS AMENDED - PART II

		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	SMALL ENTITY RATE($)	SMALL ENTITY ADDITIONAL FEE($)	OR	OTHER THAN SMALL ENTITY RATE($)	OTHER THAN SMALL ENTITY ADDITIONAL FEE($)
AMENDMENT A	Total (37 CFR 1.16(i))	*	Minus	**	=	x =		OR	x =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x =		OR	x =	
	Application Size Fee (37 CFR 1.16(s))									
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	SMALL ENTITY RATE($)	SMALL ENTITY ADDITIONAL FEE($)	OR	OTHER THAN SMALL ENTITY RATE($)	OTHER THAN SMALL ENTITY ADDITIONAL FEE($)
AMENDMENT B	Total (37 CFR 1.16(i))	*	Minus	**	=	x =		OR	x =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x =		OR	x =	
	Application Size Fee (37 CFR 1.16(s))									
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".
*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".
The "Highest Number Previously Paid For" (Total or Independent) is the highest found in the appropriate box in column 1.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING or 371(c) DATE	GRP ART UNIT	FIL FEE REC'D	ATTY.DOCKET.NO	TOT CLAIMS	IND CLAIMS
13/657,010	10/22/2012	2431	533	007742.00017	20	3

CONFIRMATION NO. 2390

22907
BANNER & WITCOFF, LTD.
1100 13th STREET, N.W.
SUITE 1200
WASHINGTON, DC 20005-4051

FILING RECEIPT

OC000000057768609

Date Mailed: 11/28/2012

Receipt is acknowledged of this non-provisional patent application. The application will be taken up for examination in due course. Applicant will be notified as to the results of the examination. Any correspondence concerning the application must include the following identification information: the U.S. APPLICATION NUMBER, FILING DATE, NAME OF APPLICANT, and TITLE OF INVENTION. Fees transmitted by check or draft are subject to collection. Please verify the accuracy of the data presented on this receipt. **If an error is noted on this Filing Receipt, please submit a written request for a Filing Receipt Correction. Please provide a copy of this Filing Receipt with the changes noted thereon. If you received a "Notice to File Missing Parts" for this application, please submit any corrections to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections**

Inventor(s)
Steven Rogers, Leesburg, VA;
Sean Moore, Hollis, NH;

Applicant(s)
Centripetal Networks, Inc., Leesburg, VA

Assignment For Published Patent Application
CENTRIPETAL NETWORKS, INC., Leesburg, VA

Power of Attorney: The patent practitioners associated with Customer Number 22907

Domestic Applications for which benefit is claimed - None.
A proper domestic benefit claim must be provided in an Application Data Sheet in order to constitute a claim for domestic benefit. See 37 CFR 1.76 and 1.78.

Foreign Applications for which priority is claimed (You may be eligible to benefit from the **Patent Prosecution Highway** program at the USPTO. Please see http://www.uspto.gov for more information.) - None.
Foreign application information must be provided in an Application Data Sheet in order to constitute a claim to foreign priority. See 37 CFR 1.55 and 1.76.

If Required, Foreign Filing License Granted: 11/23/2012
The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 13/657,010**
Projected Publication Date: 04/24/2014
Non-Publication Request: No
Early Publication Request: No
** **SMALL ENTITY** **

Title

METHODS AND SYSTEMS FOR PROTECTING A SECURED NETWORK

Preliminary Class

726

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

Since the rights granted by a U.S. patent extend only throughout the territory of the United States and have no effect in a foreign country, an inventor who wishes patent protection in another country must apply for a patent in a specific country or in regional patent offices. Applicants may wish to consider the filing of an international application under the Patent Cooperation Treaty (PCT). An international (PCT) application generally has the same effect as a regular national patent application in each PCT-member country. The PCT process **simplifies** the filing of patent applications on the same invention in member countries, but **does not result** in a grant of "an international patent" and does not eliminate the need of applicants to file additional documents and fees in countries where patent protection is desired.

Almost every country has its own patent law, and a person desiring a patent in a particular country must make an application for patent in that country in accordance with its particular laws. Since the laws of many countries differ in various respects from the patent law of the United States, applicants are advised to seek guidance from specific foreign countries to ensure that patent rights are not lost prematurely.

Applicants also are advised that in the case of inventions made in the United States, the Director of the USPTO must issue a license before applicants can apply for a patent in a foreign country. The filing of a U.S. patent application serves as a request for a foreign filing license. The application's filing receipt contains further information and guidance as to the status of applicant's license for foreign filing.

Applicants may wish to consult the USPTO booklet, "General Information Concerning Patents" (specifically, the section entitled "Treaties and Foreign Patents") for more information on timeframes and deadlines for filing foreign patent applications. The guide is available either by contacting the USPTO Contact Center at 800-786-9199, or it can be viewed on the USPTO website at http://www.uspto.gov/web/offices/pac/doc/general/index.html.

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, http://www.stopfakes.gov. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4158).

LICENSE FOR FOREIGN FILING UNDER

Title 35, United States Code, Section 184

Title 37, Code of Federal Regulations, 5.11 & 5.15

GRANTED

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where the conditions for issuance of a license have been met, regardless of whether or not a license may be required as

set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

This license is to be retained by the licensee and may be used at any time on or after the effective date thereof unless it is revoked. This license is automatically transferred to any related applications(s) filed under 37 CFR 1.53(d). This license is not retroactive.

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national security or the export of technical data. Licensees should apprise themselves of current regulations especially with respect to certain countries, of other agencies, particularly the Office of Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR 121-128)); the Bureau of Industry and Security, Department of Commerce (15 CFR parts 730-774); the Office of Foreign AssetsControl, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

NOT GRANTED

No license under 35 U.S.C. 184 has been granted at this time, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" DOES NOT appear on this form. Applicant may still petition for a license under 37 CFR 5.12, if a license is desired before the expiration of 6 months from the filing date of the application. If 6 months has lapsed from the filing date of this application and the licensee has not received any indication of a secrecy order under 35 U.S.C. 181, the licensee may foreign file the application pursuant to 37 CFR 5.15(b).

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
13/657,010	10/22/2012	Steven Rogers	007742.00017

CONFIRMATION NO. 2390

22907
BANNER & WITCOFF, LTD.
1100 13th STREET, N.W.
SUITE 1200
WASHINGTON, DC 20005-4051

POA ACCEPTANCE LETTER

OC000000057776326

Date Mailed: 11/28/2012

NOTICE OF ACCEPTANCE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 10/22/2012.

The Power of Attorney in this application is accepted. Correspondence in this application will be mailed to the above address as provided by 37 CFR 1.33.

/ygenet/

Office of Data Management, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101

PTO/SB/08a (01-10)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	13657010
Filing Date	2012-10-22
First Named Inventor	Steven ROGERS
Art Unit	2431
Examiner Name	TBD
Attorney Docket Number	007742.00017

U.S.PATENTS

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Patent citation information please click the Add button.

U.S.PATENT APPLICATION PUBLICATIONS

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20060195896		2006-08-31	Fulp et al.	
	2	20060248580		2006-11-02	Fulp et al.	
	3	20110055916		2011-03-03	Ahn	

If you wish to add additional U.S. Published Application citation information please click the Add button.

FOREIGN PATENT DOCUMENTS

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							☐

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13657010
	Filing Date	2012-10-22
	First Named Inventor	Steven ROGERS
	Art Unit	2431
	Examiner Name	TBD
	Attorney Docket Number	007742.00017

If you wish to add additional Foreign Patent Document citation information please click the Add button

NON-PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1	John Kindervag; "Build Security Into Your Network's DNA: The Zero Trust Network Architecture"; Forrester Research Inc.; November 5, 2010; pps. 1-26.	☐
	2	Palo Alto Networks; "Designing A Zero Trust Network With Next-Generation Firewalls"; pps. 1-10; last viewed on October 21, 2012.	☐

If you wish to add additional non-patent literature document citation information please click the Add button

EXAMINER SIGNATURE

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13657010
	Filing Date	2012-10-22
	First Named Inventor	Steven ROGERS
	Art Unit	2431
	Examiner Name	TBD
	Attorney Docket Number	007742.00017

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☐ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

☐ See attached certification statement.

☐ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/William E. Wooten/	Date (YYYY-MM-DD)	2012-12-13
Name/Print	William E. Wooten	Registration Number	60,049

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Electronic Acknowledgement Receipt

EFS ID:	14464198
Application Number:	13657010
International Application Number:	
Confirmation Number:	2390
Title of Invention:	METHODS AND SYSTEMS FOR PROTECTING A SECURED NETWORK
First Named Inventor/Applicant Name:	Steven Rogers
Customer Number:	22907
Filer:	William Eugene Wooten/Debra Barnes
Filer Authorized By:	William Eugene Wooten
Attorney Docket Number:	007742.00017
Receipt Date:	13-DEC-2012
Filing Date:	22-OCT-2012
Time Stamp:	16:53:11
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Information Disclosure Statement (IDS) Form (SB08)	IDS.pdf	66083 bb72462094b67e69421988175c6725fd370c1ac9	no	4
Warnings:					
Information:					

This is not an USPTO supplied IDS fillable form	
Total Files Size (in bytes):	66083

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

Electronic Acknowledgement Receipt

EFS ID:	14464630
Application Number:	13657010
International Application Number:	
Confirmation Number:	2390
Title of Invention:	METHODS AND SYSTEMS FOR PROTECTING A SECURED NETWORK
First Named Inventor/Applicant Name:	Steven Rogers
Customer Number:	22907
Filer:	William Eugene Wooten/Debra Barnes
Filer Authorized By:	William Eugene Wooten
Attorney Docket Number:	007742.00017
Receipt Date:	13-DEC-2012
Filing Date:	22-OCT-2012
Time Stamp:	17:11:28
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Non Patent Literature	Reference1.pdf	14884866 b8fa9c6427f7a4618ad56395e84e0e6c39a79c25	no	11
Warnings:					
Information:					

2	Non Patent Literature	Reference2.pdf	4197520 85383f438184454e1563ef5631526cff2fd0348b	no	27

Warnings:	
Information:	
Total Files Size (in bytes):	19082386

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PTO/SB/08a (01-10)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	13657010
Filing Date	2012-10-22
First Named Inventor	Steven ROGERS
Art Unit	2438
Examiner Name	Lynch, Sharon S.
Attorney Docket Number	007742.00017

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	6226372	B1	2001-05-01	Beebe et al.	

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] ¡	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1	1677484	EP	A2	2006-07-05	MICROSOFT CORPORATION		☐

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13657010
	Filing Date	2012-10-22
	First Named Inventor	Steven ROGERS
	Art Unit	2438
	Examiner Name	Lynch, Sharon S.
	Attorney Docket Number	007742.00017

	1	Copy of ISR for PCT/US2013/057502 dated November 7, 2013.	☐

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**		
	Application Number	13657010
	Filing Date	2012-10-22
	First Named Inventor	Steven ROGERS
	Art Unit	2438
	Examiner Name	Lynch, Sharon S.
	Attorney Docket Number	007742.00017

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☐ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

☐ See attached certification statement.

☐ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/William E. Wooten/	Date (YYYY-MM-DD)	2013-12-02
Name/Print	William E. Wooten	Registration Number	60049

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

PATENT COOPERATION TREATY

From the INTERNATIONAL SEARCHING AUTHORITY

PCT

To:
Wright, Bradley
BANNER & WITCOFF, LTD.
1100 13th Street, N.W. Suite 1200
Washington, DC 20005-4051
ETATS-UNIS D'AMERIQUE

NOTIFICATION OF TRANSMITTAL OF THE INTERNATIONAL SEARCH REPORT AND THE WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY, OR THE DECLARATION

(PCT Rule 44.1)

Applicant's or agent's file reference 007742.00023	Date of mailing *(day/month/year)* 7 November 2013 (07-11-2013) **FOR FURTHER ACTION** See paragraphs 1 and 4 below
International application No. PCT/US2013/057502	International filing date *(day/month/year)* 30 August 2013 (30-08-2013)
Applicant CENTRIPETAL NETWORKS, INC.	

1. [X] The applicant is hereby notified that the international search report and the written opinion of the International Searching Authority have been established and are transmitted herewith.

   Filing of amendments and statement under Article 19:
   The applicant is entitled, if he so wishes, to amend the claims of the International Application (see Rule 46):

   When? The time limit for filing such amendments is normally two months from the date of transmittal of the International Search Report.

   Where? Directly to the International Bureau of WIPO, 34 chemin des Colombettes 1211 Geneva 20, Switzerland, Facsimile No.: (41-22) 338.82.70

   For more detailed instructions, see *PCT Applicant's Guide*, International Phase, paragraphs 9.004 - 9.011.

2. [ ] The applicant is hereby notified that no international search report will be established and that the declaration under Article 17(2)(a) to that effect and the written opinion of the International Searching Authority are transmitted herewith.

3. [ ] **With regard to any protest** against payment of (an) additional fee(s) under Rule 40.2, the applicant is notified that:

   [ ] the protest together with the decision thereon has been transmitted to the International Bureau together with any request to forward the texts of both the protest and the decision thereon to the designated Offices.

   [ ] no decision has been made yet on the protest; the applicant will be notified as soon as a decision is made.

4. **Reminders**

   The applicant may submit comments on an informal basis on the written opinion of the International Searching Authority to the International Bureau. The International Bureau will send a copy of such comments to all designated Offices unless an international preliminary examination report has been or is to be established. Following the expiration of 30 months from the priority date, these comments will also be made available to the public.

   Shortly after the expiration of **18 months** from the priority date, the international application will be published by the International Bureau. If the applicant wishes to avoid or postpone publication, a notice of withdrawal of the international application, or of the priority claim, must reach the International Bureau before completion of the technical preparations for international publication (Rules 90*bis*.1 and 90*bis*.3).

   Within **19 months** from the priority date, but only in respect of some designated Offices, a demand for international preliminary examination must be filed if the applicant wishes to postpone the entry into the national phase **until 30 months** from the priority date (in some Offices even later); otherwise, the applicant must, **within 20 months** from the priority date, perform the prescribed acts for entry into the national phase before those designated Offices.

   In respect of other designated Offices, the time limit of **30 months** (or later) will apply even if no demand is filed within 19 months.

   For details about the applicable time limits, Office by Office, see www.wipo.int/pct/en/texts/time_limits.html and the *PCT Applicant's Guide*, National Chapters.

Name and mailing address of the International Searching Authority European Patent Office, P.B. 5818 Patentlaan 2 NL-2280 HV Rijswijk Tel. (+31-70) 340-2040 Fax: (+31-70) 340-3016	Authorized officer VINCI, Rossana Tel: +31 (0)70 340-2812

NOV 12 2013

Form PCT/ISA/220 (July 2010)

PATENT COOPERATION TREATY

PCT

INTERNATIONAL SEARCH REPORT

(PCT Article 18 and Rules 43 and 44)

Applicant's or agent's file reference	**FOR FURTHER ACTION**	see Form PCT/ISA/220 as well as, where applicable, item 5 below.
007742.00023		
International application No.	International filing date *(day/month/year)*	(Earliest) Priority Date *(day/month/year)*
PCT/US2013/057502	30 August 2013 (30-08-2013)	22 October 2012 (22-10-2012)
Applicant		
CENTRIPETAL NETWORKS, INC.		

This international search report has been prepared by this International Searching Authority and is transmitted to the applicant according to Article 18. A copy is being transmitted to the International Bureau.

This international search report consists of a total of 3 sheets.

[X] it is also accompanied by a copy of each prior art document cited in this report.

1. **Basis of the report**
   a. With regard to the **language**, the international search was carried out on the basis of:
      [X] the international application in the language in which it was filed
      [ ] a translation of the international application into _____, which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1(b))
   b. [ ] This international search report has been established taking into account the **rectification of an obvious mistake** authorized by or notified to this Authority under Rule 91 (Rule 43.6*bis*(a)).
   c. [ ] With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, see Box No. I.

2. [ ] **Certain claims were found unsearchable** (See Box No. II)

3. [ ] **Unity of invention is lacking** (see Box No III)

4. With regard to the **title,**
   [X] the text is approved as submitted by the applicant
   [ ] the text has been established by this Authority to read as follows:

5. With regard to the **abstract,**
   [X] the text is approved as submitted by the applicant
   [ ] the text has been established, according to Rule 38.2, by this Authority as it appears in Box No. IV. The applicant may, within one month from the date of mailing of this international search report, submit comments to this Authority

6. With regard to the **drawings,**
   a. the figure of the **drawings** to be published with the abstract is Figure No. 1
      [ ] as suggested by the applicant
      [X] as selected by this Authority, because the applicant failed to suggest a figure
      [ ] as selected by this Authority, because this figure better characterizes the invention
   b. [ ] none of the figures is to be published with the abstract

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2013/057502

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L29/06
ADD.

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 1 677 484 A2 (MICROSOFT CORP [US]) 5 July 2006 (2006-07-05) paragraphs [0011], [0017] - [0019]	1-20
X	US 6 226 372 B1 (BEEBE TODD [US] ET AL) 1 May 2001 (2001-05-01) column 3, line 38 - column 4, line 32; claims 1-11	1-20

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
30 October 2013	07/11/2013

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Veen, Gerardus

Form PCT/ISA/210 (second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/US2013/057502

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 1677484 A2	05-07-2006	CN 1777179 A	24-05-2006
		EP 1677484 A2	05-07-2006
		JP 4914052 B2	11-04-2012
		JP 2006146891 A	08-06-2006
		KR 20060056231 A	24-05-2006
		US 2006129808 A1	15-06-2006
		US 2009172774 A1	02-07-2009
US 6226372 B1	01-05-2001	AU 1950301 A	18-06-2001
		US 6226372 B1	01-05-2001
		US 2001014150 A1	16-08-2001
		WO 0143343 A1	14-06-2001

Form PCT/ISA/210 (patent family annex) (April 2005)

PATENT COOPERATION TREATY

From the
INTERNATIONAL SEARCHING AUTHORITY

To:

see form PCT/ISA/220

PCT

WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY
(PCT Rule 43*bis*.1)

Date of mailing
(day/month/year) see form PCT/ISA/210 (second sheet)

Applicant's or agent's file reference
see form PCT/ISA/220

FOR FURTHER ACTION
See paragraph 2 below

International application No.	International filing date *(day/month/year)*	Priority date *(day/month/year)*
PCT/US2013/057502	30.08.2013	22.10.2012

International Patent Classification (IPC) or both national classification and IPC
INV. H04L29/06

Applicant
CENTRIPETAL NETWORKS, INC.

1. This opinion contains indications relating to the following items:

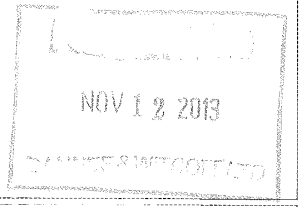
- ☒ Box No. I Basis of the opinion
- ☐ Box No. II Priority
- ☐ Box No. III Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- ☐ Box No. IV Lack of unity of invention
- ☒ Box No. V Reasoned statement under Rule 43*bis*.1(a)(i) with regard to novelty, inventive step and industrial applicability; citations and explanations supporting such statement
- ☐ Box No. VI Certain documents cited
- ☐ Box No. VII Certain defects in the international application
- ☐ Box No. VIII Certain observations on the international application

2. **FURTHER ACTION**

If a demand for international preliminary examination is made, this opinion will usually be considered to be a written opinion of the International Preliminary Examining Authority ("IPEA") except that this does not apply where the applicant chooses an Authority other than this one to be the IPEA and the chosen IPEA has notifed the International Bureau under Rule 66.1*bis*(b) that written opinions of this International Searching Authority will not be so considered.

If this opinion is, as provided above, considered to be a written opinion of the IPEA, the applicant is invited to submit to the IPEA a written reply together, where appropriate, with amendments, before the expiration of 3 months from the date of mailing of Form PCT/ISA/220 or before the expiration of 22 months from the priority date, whichever expires later.

For further options, see Form PCT/ISA/220.



Name and mailing address of the ISA:	Date of completion of this opinion	Authorized Officer
European Patent Office P.B. 5818 Patentlaan 2 NL-2280 HV Rijswijk - Pays Bas Tel. +31 70 340 - 2040 Fax: +31 70 340 - 3016	see form PCT/ISA/210	Veen, Gerardus Telephone No. +31 70 340-3811

Form PCT/ISA/237 (Cover Sheet) (July 2009)

Box No. I Basis of the opinion

1. With regard to the **language**, this opinion has been established on the basis of:

   ☒ the international application in the language in which it was filed

   ☐ a translation of the international application into , which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1 (b)).

2. ☐ This opinion has been established taking into account the **rectification of an obvious mistake** authorized by or notified to this Authority under Rule 91 (Rule 43bis.1(a))

3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, this opinion has been established on the basis of a sequence listing filed or furnished:

   a. (means)

   ☐ on paper

   ☐ in electronic form

   b. (time)

   ☐ in the international application as filed

   ☐ together with the international application in electronic form

   ☐ subsequently to this Authority for the purposes of search

4. ☐ In addition, in the case that more than one version or copy of a sequence listing has been filed or furnished, the required statements that the information in the subsequent or additional copies is identical to that in the application as filed or does not go beyond the application as filed, as appropriate, were furnished.

5. Additional comments:

Box No. V Reasoned statement under Rule 43*bis*.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Yes:	Claims	
	No:	Claims	1-20
Inventive step (IS)	Yes:	Claims	
	No:	Claims	1-20
Industrial applicability (IA)	Yes:	Claims	1-20
	No:	Claims	

2. Citations and explanations

see separate sheet

Re Item V

Reasoned statement with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1 The following documents are referred to:

D1 EP 1 677 484 A2 (MICROSOFT CORP [US]) 5 July 2006 (2006-07-05)

D2 US 6 226 372 B1 (BEEBE TODD [US] ET AL) 1 May 2001 (2001-05-01)

2 The present application does not meet the criteria of Article 33(2) PCT, because the subject-matter of claims 1-20 is not new.

2.1 In the words of independent claim 1, D1 discloses:

'A method (column 4, line 13), comprising:

at each of one or more packet security gateways (c.4, l.16, 'enforcement engine') associated with a security policy management server (c.4, l.15, 'policy server'):

receiving a dynamic security policy from the security policy management server (c.4, l.16-19);

receiving packets associated with a network protected by each respective packet security gateway; and

performing, on a packet by packet basis, at least one of multiple packet transformation functions specified by the dynamic security policy on the packets (c.4, l.19-20, 'enforcing the security policies'), wherein performing the at least one of multiple packet transformation functions specified by the dynamic security policy on the packets comprises performing at least one packet transformation function other than forwarding or dropping the packets (c.5, l.30-36)'.

Claim 1 is thus not new (Art. 33(2) PCT).

2.2 The same reasoning applies, mutatis mutandis, to independent claims 19 and 20 which are, therefore, also not new.

2.3 Dependent claims 2-18 do not contain any features which, in combination with the features of the claims to which they refer, meet the requirements of the PCT in respect of novelty and inventive step, see D1, D2 and the corresponding citations in the search report.

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 677 484 A2

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
05.07.2006 Bulletin 2006/27

(51) Int Cl.:
H04L 29/06 *(2006.01)*

(21) Application number: **05110420.6**

(22) Date of filing: **07.11.2005**

(84) Designated Contracting States:
AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IS IT LI LT LU LV MC NL PL PT RO SE SI SK TR
Designated Extension States:
AL BA HR MK YU

(30) Priority: **19.11.2004 US 993688**

(71) Applicant: **MICROSOFT CORPORATION**
Redmond, Washington 98052-6399 (US)

(72) Inventors:
- **Paleologu, Emanuel,**
  cO Microsoft Corporation
  Redmond,
  WA 98052 (US)
- **Youngblut, Eric E.,**
  c/o Microsoft Corporation
  Redmond,
  WA 98052 (US)
- **Ivanov, Maxim A.,**
  c/o Microsoft Corporation
  Redmond,
  WA 98052 (US)
- **Nagampalli, Narasimha Rao S.S.,**
  c/o Microsoft Corp
  Redmond,
  WA 98052 (US)
- **Sheth, Sachin C.,**
  c/o Microsoft Corporation
  Redmond,
  WA 98052 (US)
- **Koti, Shirish R.,**
  c/o Microsoft Corporation
  Redmond,
  WA 98052 (US)
- **Lin, Yun,**
  c/o Microsoft Corporation
  Redmond,
  WA 98052 (US)

(74) Representative: **Schuster, Thomas**
Grünecker, Kinkeldey,
Stockmair & Schwanhäusser
Anwaltssozietät
Maximilianstrasse 58
D-80538 München (DE)

(54) Method and system for distributing security policies

(57) A method and system for distributing and enforcing security policies is provided. A firewall agent executing at a host computer system that is to be protected receives security policies for the enforcement engines responsible for enforcing the security policies on the host computer system. A security policy has rules that each provide a condition and action to be performed when the condition is satisfied. A rule also has a rule type that is used by the distribution system to identify the security components that are responsible for enforcing the rules. To distribute the security policies that have been received at a host computer system, the firewall agent identifies to which enforcement engine a rule applies based in part on rule type. The firewall agent then distributes the rule to the identified enforcement engine, which then enforces the rule.

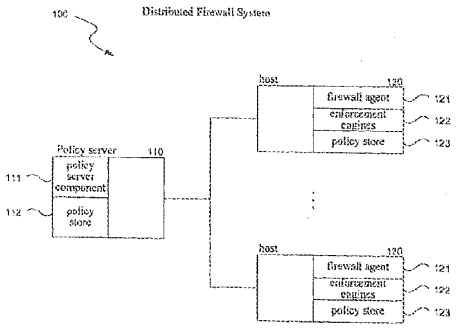


FIG. 1

EP 1 677 484 A2

Description

TECHNICAL FIELD

[0001] The described technology relates generally to systems that prevent the exploitation of vulnerabilities of computer systems.

BACKGROUND

[0002] Although the Internet has had great successes in facilitating communications between computer systems and enabling electronic commerce, the computer systems connected to the Internet have been under almost constant attack by hackers seeking to disrupt their operation. Many of the attacks seek to exploit vulnerabilities of software systems including application programs or other computer programs executing on those computer systems. Developers of software systems and administrators of computer systems of an enterprise go to great effort and expense to identify and remove vulnerabilities. Because of the complexity of software systems, however, it is virtually impossible to identify and remove all vulnerabilities before software systems are released. After a software system is released, developers can become aware of vulnerabilities in various ways. A party with no malicious intent may identify a vulnerability and may secretly notify the developer so the vulnerability can be removed before a hacker identifies and exploits it. If a hacker identifies a vulnerability first, the developer may not learn of the vulnerability until it is exploited—sometimes with disastrous consequences.

[0003] Regardless of how a developer finds out about a vulnerability, the developer typically develops and distributes to system administrators "patches" or updates to the software system that remove the vulnerability. If the vulnerability has not yet been exploited (e.g., might not be known to hackers), then a developer can design, implement, test, and distribute a patch in a disciplined way. If the vulnerability has already been widely exposed, then the developer may rush to distribute a patch without the same care that is used under normal circumstances. When patches are distributed to the administrators of the computer systems, they are responsible for scheduling and installing the patches to remove the vulnerabilities.

[0004] Unfortunately, administrators often delay the installation of patches to remove vulnerabilities for various reasons. When a patch is installed, the software system and possibly the computer system on which it is executing may need to be shut down and restarted. If the vulnerability is in a software system that is critical to the success of an organization, then the administrator needs to analyze the tradeoffs of keeping the software system up and running with its associated risk of being attacked and of shutting down a critical resource of the enterprise to install the patch. Some administrators may delay the installation of the patch because they fear that, because of a hasty distribution, it might not be properly tested and have unintended side effects. If the patch has an unintended side effect, then the software system, the computer system, or some other software component that is impacted by the patch may be shut down by the patch itself. Administrators need to factor in the possibility of an unintended side effect when deciding whether to install a patch. These administrators may delay installing a patch until experience by others indicates that there are no serious unintended side effects.

[0005] Intrusion detection systems have been developed that can be used to identify whether an attempt is being made to exploit a known vulnerability that has not yet been patched. These intrusion detection systems can be used to prevent exploitations of newly discovered vulnerabilities for which patches have not yet been developed or installed. These intrusion detection systems may define a "signature" for each way a vulnerability can be exploited. For example, if a vulnerability can be exploited by sending a certain type of message with a certain attribute, then the signature for that exploitation would specify that type and attribute. When a security enforcement event occurs, such as the receipt of a message, the intrusion detection system checks its signatures to determine whether any match the security enforcement event. If so, the intrusion detection system may take action to prevent the exploitation, such as dropping the message.

[0006] Signatures for newly discovered exploitations of vulnerabilities can be created in different ways. Developers of intrusion detection systems may create and distribute new signatures when they become aware of new exploitations. An administrator can then install the new signatures to prevent the exploitation. A developer may not, however, provide signatures for all known exploitations. For example, the vulnerability may be in a special-purpose application program that the developer does not support. To prevent exploitation of such a vulnerability, intrusion detection systems may allow administrators to create their own signatures.

[0007] A set of one or more signatures may be considered a security policy. Developers of intrusion detection systems may provide various security policies. For example, a developer may provide one security policy that defines signatures of vulnerabilities of an operating system and many other security policies that are specific to an application or a class of applications. Similarly, an administrator may define a security policy that is specific to custom applications used by the enterprise.

[0008] Because intrusions can occur at various points within an operating system or an application, intrusion detection systems have been developed to detect and prevent exploitation of vulnerabilities at each of these points. For example, an intrusion detection system may be developed to prevent exploitation of vulnerabilities that can be detected at the network layer of a communication protocol, and another intrusion detection system may be developed to prevent exploitation of vulnerabilities that can be detected when a file is accessed. Each

developer of an intrusion detection system can provide their own implementation and security policies that need to be distributed to each computer system to be protected. In addition, any updates to the implementation or security policies also need to be distributed to the computer systems to be protected.

[0009] The distribution and updating of security policies for an enterprise with a large number of computer systems can be a complex and time-consuming task. Each security policy needs to be provided to each computer system and then to the appropriate intrusion detection system that is installed on the computer system. Since the developers of intrusion detection systems typically develop their systems independent of each other, each intrusion detection system may have a proprietary mechanism for defining and distributing security policies. A system administrator of an enterprise may need to be aware of each of these mechanisms to use the intrusion detection system effectively.

[0010] It would be desirable to have a mechanism that would provide a uniform way to distribute security policies received at a computer system to components responsible for enforcing the security policies.

SUMMARY

[0011] A method and system for distributing and enforcing security policies is provided. A distributed firewall system includes a policy server component, firewall agents, and enforcement engines. A firewall agent executing at a host computer system that is to be protected receives from the policy server component security policies for the enforcement engines responsible for enforcing the security policies on the host computer system. A security policy has rules that each provide a condition and action to be performed when the condition is satisfied. A rule also has a rule type (also referred to as a security type) that is used by the firewall agent to identify the enforcement engines that are responsible for enforcing the rules. The firewall agent may distribute the security policies to enforcement engines executing in user mode and in kernel mode. The enforcement engines may provide a layered approach to security enforcement. To distribute the security policies that have been received at a host computer system, the firewall agent identifies to which enforcement engine a rule applies based in part on rule type. The firewall agent then distributes the rule to the identified enforcement engine, which then enforces the rule.

BRIEF DESCRIPTION OF THE DRAWINGS

[0012] Figure 1 is a block diagram that illustrates the distributed firewall system in one embodiment.

[0013] Figure 2 is a block diagram that illustrates the components of the portions of the distributed firewall system executing on a host computer system in one embodiment.

[0014] Figure 3 is a flow diagram that illustrates the processing of the distribute policy component of the firewall agent in one embodiment.

[0015] Figure 4 is a flow diagram that illustrates the processing of the flow manager component in one embodiment.

[0016] Figure 5 is a flow diagram that illustrates the processing of an enforcement engine for a specific layer in one embodiment.

DETAILED DESCRIPTION

[0017] A method and system for distributing and enforcing security policies is provided. A distributed firewall system includes a policy server component, firewall agents, and enforcement engines. A firewall agent executing at a host computer system that is to be protected receives from a policy server security policies for the enforcement engines responsible for enforcing the security policies on the host computer system. A security policy has an execution scope and associated rules. An execution scope defines the attributes of a process or application to which the associated rules are to be applied. A rule provides a condition and action to be performed when the condition is satisfied. A rule also has a rule type (also referred to as a security type) that is used by the firewall agent to identify the enforcement engines that are responsible for enforcing the rules. The firewall agent may distribute the security policies to enforcement engines executing in user mode and in kernel mode. The enforcement engines may provide a layered approach to a distributed firewall. For example, enforcement engines may be installed on a host computer system to prevent intrusions at various layers of the ISO 7-layer reference model. The network layer, the transport layer, and the session layer may each have an enforcement engine that is developed to detect attempted intrusions at that layer. To distribute the security policies that have been received at a host computer system, the firewall agent identifies to which enforcement engine a rule applies based in part on rule type. The firewall agent then distributes the rule to the identified enforcement engine, which then enforces the rule. Upon receiving a rule, an enforcement engine may distribute the rule to its subcomponents as appropriate. For example, the firewall agent may distribute all rules destined for kernel-mode enforcement engines to a single kernel-mode security component that then distributes the rules to the enforcement engines. In this way, the distributed firewall system provides a single mechanism for distributing rules of security policies to the enforcement engines providing different layers of protection for a host computer system.

[0018] In one embodiment, a security policy includes rules that specify conditions, actions, and optionally exceptions. For example, a rule may indicate that an application may not receive messages on any network port other than port 80. The condition of the rule may be satisfied when a message is received on a network port

other than port 80, and the action may result in the message being discarded. As another example, a rule may indicate that when an application attempts to send a message on network port 80, authorization is to be solicited from a user of the computing system on which the rule is enforced. The rules may be categorized into rule or security types based on their behavior. For example, rules with a network security type may be directed to security enforcement for network traffic. Each security type may have its own security component for enforcing rules of that security type. Languages for specifying security policies is described in U.S. Patent Application No. 10/882,438, entitled "Languages for Expressing Security Policies" and filed on July 1, 2004, which is hereby incorporated by reference.

[0019] The condition, action, and exception of the rules may be specified as expressions. A rule may be semantically expressed as "IF conditions THEN actions EXCEPT exceptions." Conditions of a rule are expressions of circumstances under which security enforcement actions of the rule are to be performed. An action is an expression of activity to be performed when the condition is satisfied. A rule may have multiple actions. An exception is an expression of when the actions may not be performed even though the condition is satisfied. A condition may be either static or dynamic. A static condition is one which refers, for example, to a hard-coded list of files. A dynamic condition is one which, for example, performs a query to determine a list of files matching a provided criterion. Security enforcement actions may include allowing a request that caused the security enforcement event, denying the request, soliciting input from a user, notifying the user, and so on. Other rule constructs are also possible. As an example, an "else" construct could be added to perform alternate actions when a condition is false.

[0020] Figure 1 is a block diagram that illustrates the distributed firewall system in one embodiment. An enterprise may have a network system 100 that includes a policy server computer system 110 and host computer systems 120. A system administrator uses a policy server component 111 of the policy server computer system to prepare and distribute security policies stored in a security policy store 112 to the host computer systems. Each host computer system includes a firewall agent 121, enforcement engines 122, and a policy store 123. The firewall agent provides a central mechanism through which a host computer system receives and distributes security policies to the enforcement engines of that host computer system. Upon receiving a security policy from the policy server computer system, the firewall agent of a host computer system stores the security policy in the policy store. The firewall agent then processes the security policies on a rule-by-rule basis and provides the rules to the appropriate enforcement engine. The firewall agent may combine various security policies, order the rules of the security policies, and dynamically notify the enforcement engines of changes to security policies or system configurations that will affect the enforcement of the security policies. Such combining, ordering, and notifying is described in U.S. Patent Application No. 10/966,800, entitled "Method and System for Merging Security Policies" and filed on October 14, 2004, which is hereby incorporated by reference. The enforcement engines then enforce the rules by applying them to network events. The enforcement engines may provide various type of security enforcement. An enforcement engine may detect an attempt to perform a certain behavior and block the attempt. For example, an application that is infected with a virus may attempt to delete certain files of the operating system. A security engine executing in the same process space as the application may detect and block the attempt to delete the file. A security engine for performing behavior blocking is described in U.S. Patent Application No. 10/832,798, entitled "A Method and System for Enforcing a Security Policy via a Security Virtual Machine" and filed on April 27, 2004, which is hereby incorporated by reference. The enforcement engines may be adapted to apply rules to network events of various protocols, such as IP, ICMP, TCP, FTP, DNS, HTTP, RPC, and so on. Techniques preventing exploitation of vulnerabilities are described in U.S. Patent Application No. 10/955,963, entitled "Method and System for Filtering Communications to Prevent Exploitation of a Software Vulnerability" and filed on September 30, 2004, which is hereby incorporated by reference.

[0021] Figure 2 is a block diagram that illustrates the components of the distributed firewall system executing on a host computer system in one embodiment. The host computer system includes firewall agent components 220, kernel-mode components 230, and application user-mode components 240. The firewall agent components include a receive policy component 221, a parse policy component 222, and a distribute policy component 223. The firewall agent components also include a policy store 224 and a configuration manager 225. The receive policy component receives security policies provided by the policy server computer system and stores the policies in the policy store. The parse policy component retrieves the policies from the policy store and converts them to a lower-level language for processing by the enforcement engines. The distribute policy component receives the parsed security policies and distributes the rules of the security policies to the appropriate enforcement engines. The configuration manager provides configuration information for use in determining which rules should be distributed to which enforcement engines based on the current configuration of the host computer system.

[0022] The kernel-mode components include enforcement engines 231, flow manager components 233, and protocol hooks 234. The components may be layered from layer 0 to layer N, which may correspond to various layers of the ISO 7-layer reference model. Each layer may have an associated protocol hook, flow manager, and enforcement engine that is specific to the layer, parses network events specific to that layer, and enforces the

rules provided by the firewall agent to that layer. The rules for each layer are stored in a rule store 232 that may be specific for that layer. The flow manager components are responsible for intercepting network events and invoking the corresponding enforcement engine to enforce the rules. Each flow manager component receives network events from the corresponding protocol hook that is responsible for detecting network events at the corresponding layer. The application user-mode components may be provided as a dynamic link library that links into an application for providing layered security in a manner that is similar in overall architecture to the kernel-mode components.

[0023] The computing device on which the distribution system is implemented may include a central processing unit, memory, input devices (e.g., keyboard and pointing devices), output devices (e.g., display devices), and storage devices (e.g., disk drives). The memory and storage devices are computer-readable media that may contain instructions that implement the distribution system. In addition, the data structures and message structures may be stored or transmitted via a data transmission medium, such as a signal on a communications link. Various communication links may be used, such as the Internet, a local area network, a wide area network, a point-to-point dial-up connection, a cell phone network, and so on.

[0024] The distribution system may be implemented in various operating environments that include personal computers, server computers, hand-held or laptop devices, multiprocessor systems, microprocessor-based systems, programmable consumer electronics, digital cameras, network PCs, minicomputers, mainframe computers, distributed computing environments that include any of the above systems or devices, and so on. The host computer systems may be cell phones, personal digital assistants, smart phones, personal computers, programmable consumer electronics, digital cameras, and so on.

[0025] The distribution system may be described in the general context of computer-executable instructions, such as program modules, executed by one or more computers or other devices. Generally, program modules include routines, programs, objects, components, data structures, and so on that perform particular tasks or implement particular abstract data types. Typically, the functionality of the program modules may be combined or distributed as desired in various embodiments.

[0026] Figure 3 is a flow diagram that illustrates the processing of the distribute policy component of the firewall agent in one embodiment. Upon receiving policies from the parse policy component, the component identifies the enforcement engines to which the rules apply and distributes the rules to the identified enforcement engines. In blocks 301-307, the component loops selecting the security policies. In block 301, the component selects the next security policy. In decision block 302, if all the security policies have already been selected, then the component completes, else the component continues at block 303. In blocks 303-307, the component loops processing each rule within the selected security policy. In block 303, the component selects the next rule of the selected security policy. In decision block 304, if all the rules of the selected security policy have already been selected, then the component loops to block 301 to select the next security policy, else the component continues at block 305. In block 305, the component identifies the rule type (or security type) of the selected security rule. In block 306, the component identifies the enforcement engine that is responsible for enforcing the rules of the identified rule type. In block 307, the component provides the selected rule to the identified component and then loops to block 303 to select the next rule of the selected security policy.

[0027] Figure 4 is a flow diagram that illustrates the processing of the flow manager component in one embodiment. The flow manager component is passed a network event and invokes the appropriate enforcement engine for processing the network event. The flow manager component may be implemented as a separate flow manager for each layer that processes network events only for that layer or may be implemented as a single flow manager component that process network events for all layers. In this illustrated embodiment, the flow manager component processes all network events for all layers. In decision blocks 401-403, the component identifies the layer to which a network event applies. The component then invokes the associated enforcement engine for that layer in blocks 411-413. The component then completes. The flow manager may maintain a separate flow for each network connection. The enforcement engines and flow managers may be specific to the layer and the protocol implemented by the layer. For example, when a connection uses the Transmission Control Protocol ("TCP") or the User Datagram Protocol ("UDP") at the packet layer, the flow manager invokes the enforcement engine that is appropriate for the protocol. The invoked enforcement engines may instantiate data structures for tracking state information from one invocation to the next. Each application that is protected by user-mode enforcement engine may also have a flow manager with a separate flow for each connection.

[0028] Figure 5 is a flow diagram that illustrates the processing of an enforcement engine for a specific layer in one embodiment. The enforcement engine, which is a component of the distributed firewall system, is provided a network event, identifies the rules to apply to the event, determines whether the conditions of the rules are satisfied, and if so, performs the action associated with the rule. In blocks 501-504, the component loops selecting each rule associated with the layer of the enforcement engine. In block 501, the component selects the next rule. In decision block 502, if all the rules have already been selected, then the component completes, else the component continues at block 503. In decision block 503, if the condition of the rule is satisfied, then the component continues at block 504, else the component loops to block

501 to select the next rule. In block 504, the component performs the action associated with the rule and then loops to block 501 to select the next rule. Each enforcement engine may be adapted to process the network events and rules that are appropriate to its layer. For example, an enforcement engine for the network layer may parse network packets and enforce rules related to the network packets. An enforcement engine for the application layer may detect unauthorized attempts to access or modify files relating to that application.

[0029] From the foregoing, it will be appreciated that specific embodiments of the distributed firewall system have been described herein for purposes of illustration, but that various modifications may be made without deviating from the spirit and scope of the invention. Accordingly, the invention is not limited except as by the appended claims.

Claims

1. A method in a computer system for distributing rules of security policies to enforcement engines for enforcing the security policies, the method comprising:

   providing at the computer system enforcement engines that implement different layers of security enforcement;
   receiving and storing at the computer system security policies having rules, each rule having a rule type;
   under control of a firewall agent executing on the computer system,
   retrieving the stored security policies; and
   for rules of a retrieved security policy,
   identifying an enforcement engine to which a rule applies based on the rule type of the rule; and
   providing the rule to the identified enforcement engine; and under control of the enforcement engines, enforcing the rules provided to the enforcement engine by the firewall agent,
   wherein the firewall agent provides a mechanism for distributing the rules to multiple enforcement engines of the computer system.

2. The method of claim 1 wherein the security policies are received from policy computer system that distributes the security policies for multiple computer systems.

3. The method of claim 1 wherein the enforcement engines provide a layered firewall.

4. The method of claim 1 wherein the enforcement engines include a behavior blocking security component.

5. The method of claim 1 wherein an enforcement engine includes subcomponents and wherein upon being provided with a rule, the enforcement engine provides the rule to a subcomponent.

6. The method of claim 1 wherein at least one enforcement engine executes in kernel mode and at least one enforcement engine executes in user mode.

7. The method of claim 1 wherein the firewall agent includes a user-mode subcomponent and a kernel-mode subcomponent, and the user-mode subcomponent distributes rules to the kernel-mode subcomponent for providing the rules to enforcement engines that execute in kernel mode.

8. The method of claim 1 wherein a flow manager component intercepts network events at the various layers and invokes an enforcement engine associated with a layer to enforce the rules for that layer.

9. The method of claim 8 wherein a single flow manager component handles network events from multiple layers.

10. The method of claim 8 wherein a flow manager component handles network events from only one layer.

11. The method of claim 1 wherein enforcement engines provide for security at various layers of a network protocol stack.

12. The method of claim 11 wherein layers of different enforcement engines are used for different connections.

13. A computer system architecture for distributing security policies, the architecture comprising:

   a policy server computer system for establishing security policies, the security policies having rules with rule types, and for providing the security policies to host computer systems for enforcement of the security policies at the host computer systems; and
   multiple host computer systems that include:

      enforcement engines for enforcing a type of security at the host computer system; and
      a firewall agent that receives the security policies from the policy server computer system, identifies the enforcement engine to which the rules apply based on rule type and enforcement engine type, and provides the rules to the identified enforcement engines for enforcement of the security policies.

14. The computer system architecture of claim 13 wherein the enforcement engines are layered so that when one enforcement engine determines that the rules provided to it do not to apply to a network event, another enforcement engine determines whether the rules provided to it apply to the network event.

15. The computer system architecture of claim 14 wherein the layers include a protocol interception hook and an enforcement engine.

16. The computer system architecture of claim 13 wherein the firewall agent distributes rules to enforcement engines executing in user mode.

17. The computer system architecture of claim 13 wherein the firewall agent distributes rules to enforcement engines executing in kernel mode.

18. The computer system architecture of claim 13 wherein the enforcement engines are layered and including a flow manager component that handles network events at each layer and invokes an enforcement engine of the layer to enforce the rules of that layer on the network event.

19. The computer system architecture of claim 18 wherein the flow manager component handles network events for multiple layers.

20. The computer system architecture of claim 18 wherein the flow manager component handles network events for a single layer.

21. A host computer system for distributing rules of security policies to enforcement engines for enforcing the security policies of the host computer system, comprising:

multiple enforcement engines that implement different layers of firewall security enforcement at the host computer system by receiving and enforcing rules of security policies;
a component that receives at the host computer system security policies having rules, each rule having a rule type; and
a component that identifies enforcement engines to which a rule applies based on the rule type of the rule and that provides the rule to the identified security component;
wherein a mechanism is provided for distributing the rules to the layered enforcement engines of the host computer system.

22. The computer system of claim 21 wherein the security policies are received from a policy computer system that distributes the security policies for multiple host computer systems.

23. The computer system of claim 21 wherein the enforcement engine includes a behavior blocking security component.

24. The computer system of claim 21 wherein an enforcement engine includes subcomponents and wherein upon being provided with a rule, the enforcement engine provides the rule to a subcomponent.

25. The computer system of claim 21 wherein at least one enforcement engine executes in kernel mode and at least one enforcement engine executes in user mode.

26. The computer system of claim 21 wherein the component that provides the rules to the enforcement engines includes a user-mode subcomponent and a kernel-mode subcomponent, and the user-mode subcomponent distributes rules to the kernel-mode subcomponent for providing the rules to enforcement engine that execute in kernel mode.

27. The computer system of claim 21 including a flow manager component that intercepts network events at the various layers and invokes an enforcement engine associated with a layer to enforce the rules for that layer.

28. The computer system of claim 27 wherein a single flow manager component handles network events from multiple layers.

29. The computer system of claim 27 wherein a flow manager component handles network events from only one layer.

30. A computer-readable medium containing instructions for controlling a host computer system to distribute security policies to enforcement engines for enforcing the security policies, by a method comprising:

receiving and storing at the host computer system security policies having rules, each rule having a rule type;
under control of a firewall agent executing on the host computer system,
retrieving the stored security policies; and
for rules of a retrieved security policy,
identifying an enforcement engine to which a rule applies based on the rule type of the rule; and
providing the rule to the identified enforcement engine; and under control of the enforcement engines, enforcing the rules provided to the enforcement engines by the distribution component.

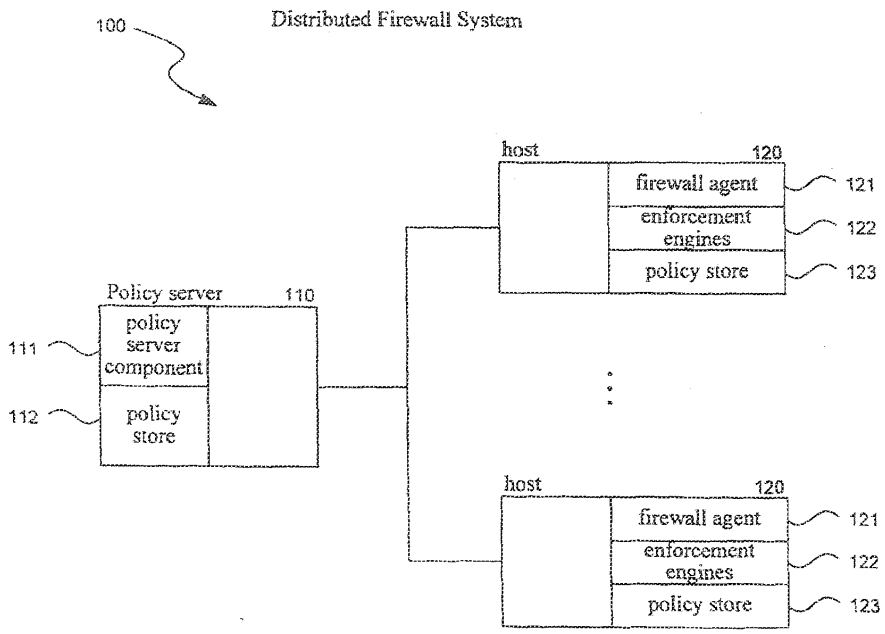

100
Distributed Firewall System
host
120
firewall agent
121
enforcement engines
122
policy store
123
Policy server
110
111
policy server component
112
policy store
host
120
firewall agent
121
enforcement engines
122
policy store
123

FIG. 1

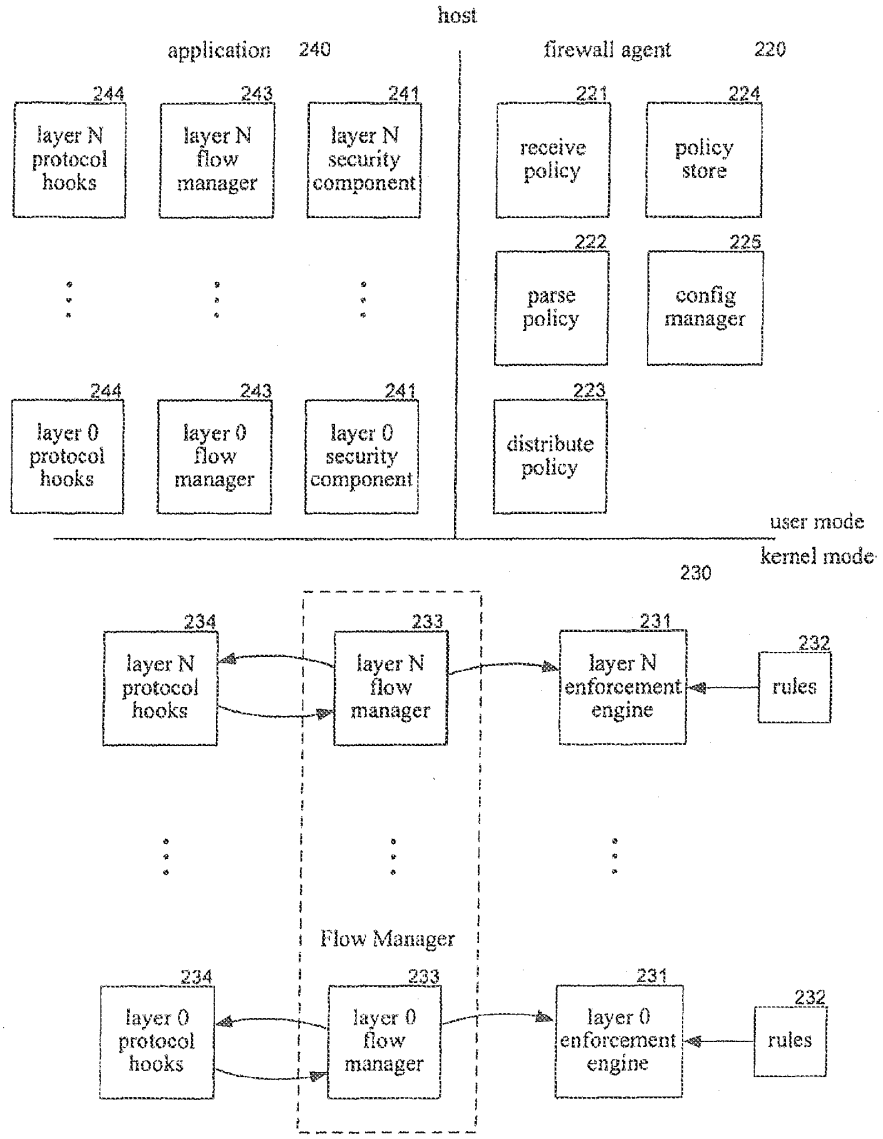


FIG. 2

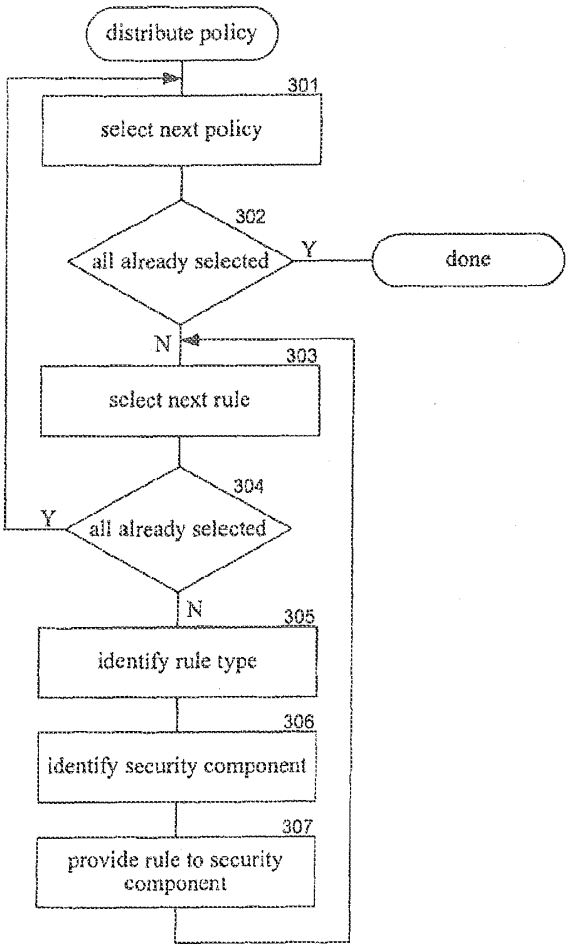


FIG. 3

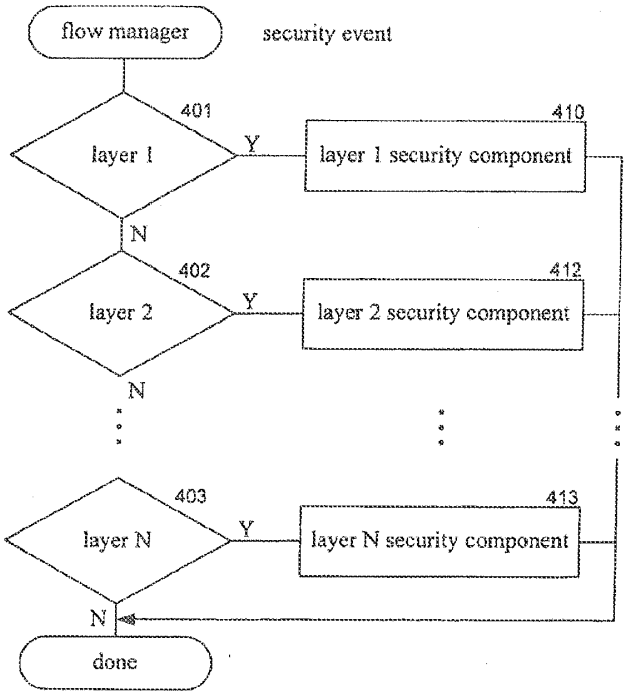


FIG. 4

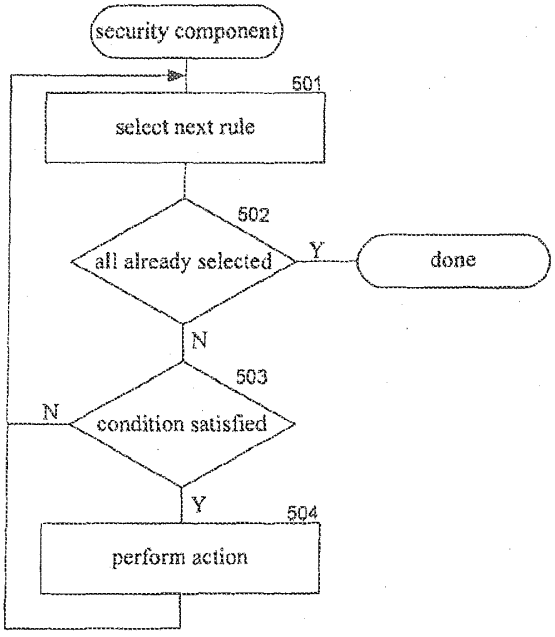


FIG. 5

Electronic Acknowledgement Receipt

EFS ID:	17538107
Application Number:	13657010
International Application Number:	
Confirmation Number:	2390
Title of Invention:	METHODS AND SYSTEMS FOR PROTECTING A SECURED NETWORK
First Named Inventor/Applicant Name:	Steven Rogers
Customer Number:	22907
Filer:	William Eugene Wooten/Debra Barnes
Filer Authorized By:	William Eugene Wooten
Attorney Docket Number:	007742.00017
Receipt Date:	02-DEC-2013
Filing Date:	22-OCT-2012
Time Stamp:	14:26:50
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Information Disclosure Statement (IDS) Form (SB08)	IDS17.pdf	612283 8256b8ce2ce3a13ff2f8f6369a854620a535891f	no	4

Warnings:	
Information:	

2	Non Patent Literature	ISR.pdf	880948 0876fa4b43caa8e36f97b28c2dbd6d79293272b4	no	8
Warnings:					
Information:					
3	Foreign Reference	EP1677484.PDF	4757932 f0ee7f33d05de0bdb80b5b1e458c01571ce1576d	no	12
Warnings:					
Information:					
		Total Files Size (in bytes):	6251163		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re the Application of:		Atty. Docket No.:	007742.00017
Steven ROGERS *et al.*			
Serial No.:	13/657,010	Group Art Unit:	2438
Filed:	October 22, 2012	Examiner:	Lynch, Sharon S.
For:	METHODS AND SYSTEMS FOR PROTECTING A SECURED NETWORK	Confirmation No.:	2390

PRELIMINARY AMENDMENT

Mail Stop Amendment
Commissioner for Patents
Randolph Building
401 Dulany Street
Alexandria, VA 22314

Dear Sir:

This paper is a preliminary amendment.

Please enter the following:

Amendments to the Claims are reflected in the Listing of Claims, which begins at page 2 of this paper.

Remarks begin at page 8 of this paper.

If any fees are required or if an overpayment is made, the Commissioner is authorized to debit or credit Deposit Account No. 19-0733, accordingly.

This Listing of Claims will replace all prior versions and listings of claims in the application:

Listing of the Claims:

1. (Original) A method, comprising:

at each of one or more packet security gateways associated with a security policy management server:

receiving a dynamic security policy from the security policy management server;

receiving packets associated with a network protected by each respective packet security gateway; and

performing, on a packet by packet basis, at least one of multiple packet transformation functions specified by the dynamic security policy on the packets, wherein performing the at least one of multiple packet transformation functions specified by the dynamic security policy on the packets comprises performing at least one packet transformation function other than forwarding or dropping the packets.

2. (Original) The method of claim 1, wherein the one or more packet security gateways comprise at least two packet security gateways configured in series such that packets forwarded from a first of the at least two packet security gateways are received by a second of the at least two packet security gateways.

3. (Original) The method of claim 2, wherein the dynamic security policy comprises at least two rules, a second of the at least two rules being required to execute subsequent to a first of the at least two rules, and wherein, for the at least two packet security gateways configured in series, performing the at least one of multiple packet transformation functions specified by the dynamic security policy on the packets comprises: performing, by the first of the at least two packet security gateways, a first packet transformation function specified by the first of the at least two rules; and performing, by the second of the at least two packet security gateways, a second packet transformation function specified by the second of the at least two rules.

4. (Original) The method of claim 1, wherein the dynamic security policy comprises at least one rule specifying a set of network addresses for which associated packets should be dropped and at least one rule specifying that all packets associated with network addresses outside the set should be forwarded.

5. (Original) The method of claim 1, wherein the dynamic security policy comprises at least one rule specifying a set of network addresses for which associated packets should be forwarded and at least one rule specifying that all packets associated with network addresses outside the set should be dropped.

6. (Original) The method of claim 5, further comprising receiving, by the security policy management server, information associated with a Voice over Internet Protocol (VoIP) session, and wherein the at least one rule specifying the set of network addresses for which associated packets should be forwarded is one of created and altered by the security policy management server utilizing the information associated with the one or more VoIP sessions.

7. (Original) The method of claim 5, wherein receiving the dynamic security policy from the security policy management server comprises receiving at least three dynamic security policies from the security policy management server, a first of the at least three dynamic security policies being received at a first time and specifying a first set of network addresses for which packets should be forwarded, a second of the at least three dynamic security policies being received at a second time after the first time and specifying a second set of network addresses for which packets should be forwarded that includes more network addresses than the first set of network addresses, and a third of the at least three dynamic security policies being received at a third time after the second time and specifying a third set of network addresses for which packets should be forwarded that includes more network addresses than the second set of network addresses.

8. (Original) The method of claim 1, wherein the dynamic security policy comprises at least two rules, a first of the at least two rules specifying a first set of network addresses, a second of the at least two rules specifying a second set of network addresses, and wherein the

dynamic security policy specifies that packets associated with the first set of network addresses should be placed in a first forwarding queue and packets associated with the second set of network addresses should be placed in a second forwarding queue, the first forwarding queue having a higher forwarding rate than the second forwarding queue.

9. (Original) The method of claim 1, wherein the dynamic security policy comprises at least one rule specifying a set of network addresses and an additional parameter, and wherein performing the at least one of multiple packet transformation functions specified by the dynamic security policy on the packets comprises routing at least one of the packets that falls within the set of network addresses and matches the additional parameter to a network address different from a destination network address specified by the at least one of the packets.

10. (Original) The method of claim 9, wherein the additional parameter comprises a Session Initiation Protocol (SIP) Uniform Resource Identifier (URI), wherein the network address different from the destination network address specified by the at least one of the packets corresponds to a network device configured to copy information contained in the at least one of the packets and forward the at least one of the packets to the destination network address specified by the at least one of the packets, and wherein routing the at least one of the packets that falls within the set of network addresses and matches the additional parameter to a network address different from the destination network address specified by the at least one of the packets comprises encapsulating the at least one of the packets that falls within the set of network addresses and matches the additional parameter with a header containing the network address different from the destination network address specified by the at least one of the packets.

11. (Original) The method of claim 1, wherein the at least one of the multiple packet transformation functions comprises at least one of forwarding the packets into the network protected by the packet security gateway, forwarding the packets out of the network protected by the packet security gateway, forwarding the packets to an Internet Protocol

Security (IPsec) stack having an IPsec security association corresponding to the packets, and dropping the packets.

12. (Original) The method of claim 1, wherein the dynamic security policy comprises a plurality of rules, and wherein at least one of the rules specifies a five-tuple, the five-tuple specifying one or more protocols, one or more IP source addresses, one or more source port values, one or more IP destination addresses, and one or more destination port values.

13. (Original) The method of claim 1, wherein the dynamic security policy comprises a plurality of rules, and wherein at least one of the rules specifies a Differentiated Service Code Point (DSCP) selector that maps to a DSCP field in an Internet Protocol (IP) header of the packets.

14. (Original) The method of claim 1, wherein at least one of the one or more packet security gateways operates in a network layer transparent manner by sending and receiving traffic at a link layer using an interface that is not addressed at the network layer and performing the at least one of the multiple packet transformation functions at the network layer.

15. (Original) The method of claim 14, wherein the at least one of the one or more packet security gateways includes a management interface having a network layer address, and wherein access to the management interface is secured at at least one of an application level, a link level, and a transport level.

16. (Original) The method of claim 1, wherein the dynamic security policy comprises one or more rules generated based, at least in part, on a list of known network addresses associated with malicious network traffic that is received from a subscription service that aggregates information associated with malicious network traffic.

17. (Original) The method of claim 1, wherein at least two of the one or more packet security gateways receive dynamic security policies from the security policy management server that include one or more rules specifying source addresses that correspond to spoofed network

addresses, and wherein at least one of the dynamic security policies specifies different source addresses that correspond to spoofed network addresses than at least another one of the dynamic security policies.

18. (Original) The method of claim 1, wherein at least one of the one or more packet security gateways is located at each boundary between a protected network associated with the security policy management server and an unprotected network.

19. (Original) A system, comprising:

a security policy management server; and

one or more packet security gateways associated with the security policy management server, wherein each of the one or more packet security gateways is configured to:

receive a dynamic security policy from the security policy management server;

receive packets associated with a network protected by each respective packet security gateway; and

perform, on a packet by packet basis, at least one of multiple packet transformation functions specified by the dynamic security policy on the packets, wherein each of the one or more packet security gateways is configured to perform the at least one of multiple packet transformation functions specified by the dynamic security policy on the packets by performing at least one packet transformation function other than forwarding or dropping the packets.

20. (Original) One or more non-transitory computer-readable media having instructions stored thereon, that when executed by one or more computers, cause the one or more computers to:

at each of one or more packet security gateways associated with a security policy management server:

receive a dynamic security policy from the security policy management server;

receive packets associated with a network protected by each respective packet security gateway; and

perform, on a packet by packet basis, at least one of multiple packet transformation functions specified by the dynamic security policy on the packets, wherein each of the one or more packet security gateways is configured to perform the at least one of multiple packet transformation functions specified by the dynamic security policy on the packets by performing at least one packet transformation function other than forwarding or dropping the packets.

21. (New) A method, comprising:

at each of one or more packet security gateways associated with a security policy management server:

receiving a dynamic security policy from the security policy management server;

receiving packets associated with a network protected by each respective packet security gateway; and

performing, on a packet by packet basis, at least one of multiple packet transformation functions specified by the dynamic security policy on the packets, wherein performing the at least one of multiple packet transformation functions specified by the dynamic security policy on the packets comprises dropping a portion of the packets and forwarding a portion of the packets toward their respective destinations.

22. (New) The method of claim 21, wherein at least one of the one or more packet security gateways or the security policy management server is associated with an organization distinct from an organization associated with the network protected by each respective packet security gateway, the method comprising operating, by the organization distinct from the organization associated with the network protected by each respective packet security gateway, the at least one of the one or more packet security gateways or the security policy management server.

REMARKS

By the instant preliminary amendment, claims 21 and 22 are added. No new matter has been added. Upon entry of this paper, claims 1-22 will be pending in the instant application. Applicants respectfully request consideration of the application and allowance of all pending claims.

If any fees are required or an overpayment is made, the Commissioner is authorized to debit or credit Deposit Account No. 19-0733, accordingly.

Respectfully submitted,

BANNER & WITCOFF, LTD.

Date: February 12, 2014

By: /William E. Wooten/
William E. Wooten
Registration No. 60,049

Banner & Witcoff, Ltd.
1100 13th Street NW, Suite 1200
Washington, DC 20005-4051
Telephone: (202) 824-3000
Facsimile: (202) 824-3001

Electronic Patent Application Fee Transmittal

Application Number:	13657010
Filing Date:	22-Oct-2012
Title of Invention:	METHODS AND SYSTEMS FOR PROTECTING A SECURED NETWORK
First Named Inventor/Applicant Name:	Steven Rogers
Filer:	William Eugene Wooten
Attorney Docket Number:	007742.00017

Filed as Small Entity

Utility under 35 USC 111(a) Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Claims in excess of 20	2202	2	40	80
Independent Claims in Excess of 3	2201	1	210	210
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension-of-Time:				
Miscellaneous:				
		Total in USD ($)		**290**

Electronic Acknowledgement Receipt	
EFS ID:	18184740
Application Number:	13657010
International Application Number:	
Confirmation Number:	2390
Title of Invention:	METHODS AND SYSTEMS FOR PROTECTING A SECURED NETWORK
First Named Inventor/Applicant Name:	Steven Rogers
Customer Number:	22907
Filer:	William Eugene Wooten
Filer Authorized By:	
Attorney Docket Number:	007742.00017
Receipt Date:	12-FEB-2014
Filing Date:	22-OCT-2012
Time Stamp:	12:59:01
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$290
RAM confirmation Number	9047
Deposit Account	190733
Authorized User	
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows: Charge any Additional Fees required under 37 C.F.R. Section 1.16 (National application filing, search, and examination fees) Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)	

Charge any Additional Fees required under 37 C.F.R. Section 1.19 (Document supply fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.20 (Post Issuance fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.21 (Miscellaneous fees and charges)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Preliminary Amendment	Prelim.pdf	130086 df698b19df96bd9d861cf4bdaeef9c42c2805d3e	no	8
Warnings:					
Information:					
2	Fee Worksheet (SB06)	fee-info.pdf	31915 89a32bf5b7a3e9ceff565c58a7d9abfd5a9cec97	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	162001		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

<u>New Applications Under 35 U.S.C. 111</u>
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

<u>National Stage of an International Application under 35 U.S.C. 371</u>
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

<u>New International Application Filed with the USPTO as a Receiving Office</u>
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

Electronic Acknowledgement Receipt

EFS ID:	18184740
Application Number:	13657010
International Application Number:	
Confirmation Number:	2390
Title of Invention:	METHODS AND SYSTEMS FOR PROTECTING A SECURED NETWORK
First Named Inventor/Applicant Name:	Steven Rogers
Customer Number:	22907
Filer:	William Eugene Wooten
Filer Authorized By:	
Attorney Docket Number:	007742.00017
Receipt Date:	12-FEB-2014
Filing Date:	22-OCT-2012
Time Stamp:	12:59:01
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$290
RAM confirmation Number	9047
Deposit Account	190733
Authorized User	
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows: Charge any Additional Fees required under 37 C.F.R. Section 1.16 (National application filing, search, and examination fees) Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)	

Charge any Additional Fees required under 37 C.F.R. Section 1.19 (Document supply fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.20 (Post Issuance fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.21 (Miscellaneous fees and charges)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Preliminary Amendment	Prelim.pdf	130086 df698b19df96bd9d861cf4bdaeef9c42c2805d3e	no	8
Warnings:					
Information:					
2	Fee Worksheet (SB06)	fee-info.pdf	31915 89a32bf5b7a3e9ceff565c58a7d9abfd5a9cec97	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	162001		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PTO/SB/06 (09-11)
Approved for use through 1/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875	Application or Docket Number 13/657,010	Filing Date 10/22/2012	☐ To be Mailed

ENTITY: ☐ LARGE ☒ SMALL ☐ MICRO

APPLICATION AS FILED – PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA	RATE ($)	FEE ($)
☒ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A	**390**
☒ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A	**620**
☒ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A	**250**
TOTAL CLAIMS (37 CFR 1.16(i))	20 minus 20 =	* 0	x $31 =	**0**
INDEPENDENT CLAIMS (37 CFR 1.16(h))	3 minus 3 =	* 0	x $125 =	**0**
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).			
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))				
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL	**630**

APPLICATION AS AMENDED – PART II

AMENDMENT	**02/12/2014**	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	* 22	Minus	** 20	= 2	x $40 =	80
	Independent (37 CFR 1.16(h))	* 4	Minus	***3	= 1	x $210 =	210
	☐ Application Size Fee (37 CFR 1.16(s))						
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						
						TOTAL ADD'L FEE	**290**

AMENDMENT		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	*	Minus	**	=	x $ =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x $ =	
	☐ Application Size Fee (37 CFR 1.16(s))						
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						
						TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".
*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".
The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

LDRC
/SUSAN HAY/

PTO/SB/06 (09-11)
Approved for use through 1/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875	Application or Docket Number 13/657,010	Filing Date 10/22/2012	☐ To be Mailed

ENTITY: ☐ LARGE ☒ SMALL ☐ MICRO

APPLICATION AS FILED – PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA	RATE ($)	FEE ($)
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*	X $ =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*	X $ =	
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).			
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))				
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL	

APPLICATION AS AMENDED – PART II

AMENDMENT	02/19/2014	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	* 94	Minus	** 20	= 74	X $40 =	2960
	Independent (37 CFR 1.16(h))	* 8	Minus	***3	= 5	X $210 =	1050
	☐ Application Size Fee (37 CFR 1.16(s))						
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						
						TOTAL ADD'L FEE	**4010**

AMENDMENT		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	*	Minus	**	=	X $ =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	X $ =	
	☐ Application Size Fee (37 CFR 1.16(s))						
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						
						TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".
*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".
The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

LIE
/JAMES MASON/

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
13/657,010	10/22/2012	Steven Rogers	007742.00017

CONFIRMATION NO. 2390

22907
BANNER & WITCOFF, LTD.
1100 13th STREET, N.W.
SUITE 1200
WASHINGTON, DC 20005-4051

PUBLICATION NOTICE

OC000000068005253

Title:METHODS AND SYSTEMS FOR PROTECTING A SECURED NETWORK

Publication No.US-2014-0115654-A1
Publication Date:04/24/2014

NOTICE OF PUBLICATION OF APPLICATION

The above-identified application will be electronically published as a patent application publication pursuant to 37 CFR 1.211, et seq. The patent application publication number and publication date are set forth above.

The publication may be accessed through the USPTO's publically available Searchable Databases via the Internet at www.uspto.gov. The direct link to access the publication is currently http://www.uspto.gov/patft/.

The publication process established by the Office does not provide for mailing a copy of the publication to applicant. A copy of the publication may be obtained from the Office upon payment of the appropriate fee set forth in 37 CFR 1.19(a)(1). Orders for copies of patent application publications are handled by the USPTO's Office of Public Records. The Office of Public Records can be reached by telephone at (703) 308-9726 or (800) 972-6382, by facsimile at (703) 305-8759, by mail addressed to the United States Patent and Trademark Office, Office of Public Records, Alexandria, VA 22313-1450 or via the Internet.

In addition, information on the status of the application, including the mailing date of Office actions and the dates of receipt of correspondence filed in the Office, may also be accessed via the Internet through the Patent Electronic Business Center at www.uspto.gov using the public side of the Patent Application Information and Retrieval (PAIR) system. The direct link to access this status information is currently http://pair.uspto.gov/. Prior to publication, such status information is confidential and may only be obtained by applicant using the private side of PAIR.

Further assistance in electronically accessing the publication, or about PAIR, is available by calling the Patent Electronic Business Center at 1-866-217-9197.

Office of Data Managment, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101

PTO/SB/08a (01-10)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**		
	Application Number	13657010
	Filing Date	2012-10-22
	First Named Inventor	Steven Rogers
	Art Unit	2438
	Examiner Name	K. W. Chang
	Attorney Docket Number	007742.00017

U.S.PATENTS						Remove
Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					
If you wish to add additional U.S. Patent citation information please click the Add button.						Add

U.S.PATENT APPLICATION PUBLICATIONS						Remove
Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20030123456	A1	2003-07-03	Denz et al.	
	2	20070083924	A1	2007-04-12	Lu	
If you wish to add additional U.S. Published Application citation information please click the Add button.						Add

FOREIGN PATENT DOCUMENTS							Remove	
Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							☐
If you wish to add additional Foreign Patent Document citation information please click the Add button							Add	

NON-PATENT LITERATURE DOCUMENTS	Remove

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13657010
	Filing Date	2012-10-22
	First Named Inventor	Steven Rogers
	Art Unit	2438
	Examiner Name	K. W. Chang
	Attorney Docket Number	007742.00017

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1	International Search Report off International Application No. PCT/US2014/023286, dated June 24, 2014.	☐

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**		
	Application Number	13657010
	Filing Date	2012-10-22
	First Named Inventor	Steven Rogers
	Art Unit	2438
	Examiner Name	K. W. Chang
	Attorney Docket Number	007742.00017

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☐ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

☐ See attached certification statement.

☐ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/William E. Wooten/	Date (YYYY-MM-DD)	2014-06-25
Name/Print	William E. Wooten	Registration Number	60049

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Electronic Acknowledgement Receipt

EFS ID:	19408936
Application Number:	13657010
International Application Number:	
Confirmation Number:	2390
Title of Invention:	METHODS AND SYSTEMS FOR PROTECTING A SECURED NETWORK
First Named Inventor/Applicant Name:	Steven Rogers
Customer Number:	22907
Filer:	William Eugene Wooten/Rocko Bund
Filer Authorized By:	William Eugene Wooten
Attorney Docket Number:	007742.00017
Receipt Date:	25-JUN-2014
Filing Date:	22-OCT-2012
Time Stamp:	15:10:01
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Non Patent Literature	NPL-ISR_dated_24-6-14774230_16806852.PDF	519073 8f3879c91d1dd61cd1a7d73ef98e5330996 4ad85	no	9
Warnings:					
Information:					

2	Information Disclosure Statement (IDS) Form (SB08)	Information_Disclosure_Statement_Fillable_PDF_16807080.PDF	612179 dde8b6f012435b7bc2aa864212cecf5c066ec413	no	4
Warnings:					
Information:					
			Total Files Size (in bytes):	1131252	

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PATENT COOPERATION TREATY

From the INTERNATIONAL SEARCHING AUTHORITY

To:
Wright, Bradley C.
BANNER & WITCOFF, LTD.
1100 13th Street, N.W. Suite 1200
Washington, DC 20005-4051
ETATS-UNIS D'AMERIQUE

PCT

NOTIFICATION OF TRANSMITTAL OF THE INTERNATIONAL SEARCH REPORT AND THE WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY, OR THE DECLARATION

(PCT Rule 44.1)

Applicant's or agent's file reference 007742.00030	Date of mailing *(day/month/year)* 24 June 2014 (24-06-2014)
International application No. PCT/US2014/023286	**FOR FURTHER ACTION** See paragraphs 1 and 4 below
Applicant CENTRIPETAL NETWORKS, INC.	International filing date *(day/month/year)* 11 March 2014 (11-03-2014)

1. [X] The applicant is hereby notified that the international search report and the written opinion of the International Searching Authority have been established and are transmitted herewith.

   Filing of amendments and statement under Article 19:
   The applicant is entitled, if he so wishes, to amend the claims of the International Application (see Rule 46):

   When? The time limit for filing such amendments is normally two months from the date of transmittal of the International Search Report.

   Where? Directly to the International Bureau of WIPO, 34 chemin des Colombettes 1211 Geneva 20, Switzerland, Fascimile No.: (41-22) 338.82.70

   For more detailed instructions, see *PCT Applicant's Guide*, International Phase, paragraphs 9.004 - 9.011.

2. [ ] The applicant is hereby notified that no international search report will be established and that the declaration under Article 17(2)(a) to that effect and the written opinion of the International Searching Authority are transmitted herewith.

3. [ ] **With regard to any protest** against payment of (an) additional fee(s) under Rule 40.2, the applicant is notified that:

   [ ] the protest together with the decision thereon has been transmitted to the International Bureau together with any request to forward the texts of both the protest and the decision thereon to the designated Offices.

   [ ] no decision has been made yet on the protest; the applicant will be notified as soon as a decision is made.

4. **Reminders**

   The applicant may submit comments on an informal basis on the written opinion of the International Searching Authority to the International Bureau. The International Bureau will send a copy of such comments to all designated Offices unless an international preliminary examination report has been or is to be established. Following the expiration of 30 months from the priority date, these comments will also be made available to the public.

   Shortly after the expiration of **18 months** from the priority date, the international application will be published by the International Bureau. If the applicant wishes to avoid or postpone publication, a notice of withdrawal of the international application, or of the priority claim, must reach the International Bureau before completion of the technical preparations for international publication (Rules 90*bis*.1 and 90*bis*.3).

   Within **19 months** from the priority date, but only in respect of some designated Offices, a demand for international preliminary examination must be filed if the applicant wishes to postpone the entry into the national phase **until 30 months** from the priority date (in some Offices even later); otherwise, the applicant must, **within 20 months** from the priority date, perform the prescribed acts for entry into the national phase before those designated Offices.

   In respect of other designated Offices, the time limit of **30 months** (or later) will apply even if no demand is filed within 19 months.

   For details about the applicable time limits, Office by Office, see www.wipo.int/pct/en/texts/time_limits.html and the *PCT Applicant's Guide*, National Chapters.

Name and mailing address of the International Searching Authority	Authorized officer	
European Patent Office, P.B. 5818 Patentlaan 2 NL-2280 HV Rijswijk Tel. (+31-70) 340-2040 Fax: (+31-70) 340-3016	ROTHENBüCHER, Anita Tel: +31 (0)70 340-9872	JUN 24 2014 BANNER & WITCOFF LTD

Form PCT/ISA/220 (July 2010)

PATENT COOPERATION TREATY

PCT

INTERNATIONAL SEARCH REPORT

(PCT Article 18 and Rules 43 and 44)

Applicant's or agent's file reference	**FOR FURTHER ACTION**	see Form PCT/ISA/220 as well as, where applicable, item 5 below.
007742.00030		
International application No.	International filing date *(day/month/year)*	(Earliest) Priority Date *(day/month/year)*
PCT/US2014/023286	11 March 2014 (11-03-2014)	12 March 2013 (12-03-2013)
Applicant		
CENTRIPETAL NETWORKS, INC.		

This international search report has been prepared by this International Searching Authority and is transmitted to the applicant according to Article 18. A copy is being transmitted to the International Bureau.

This international search report consists of a total of 3 sheets.

[X] It is also accompanied by a copy of each prior art document cited in this report.

1. **Basis of the report**
   a. With regard to the **language,** the international search was carried out on the basis of:
      [X] the international application in the language in which it was filed
      [ ] a translation of the international application into _____, which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1(b))
   b. [ ] This international search report has been established taking into account the **rectification of an obvious mistake** authorized by or notified to this Authority under Rule 91 (Rule 43.6*bis*(a)).
   c. [ ] With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, see Box No. I.

2. [ ] **Certain claims were found unsearchable** (See Box No. II)

3. [ ] **Unity of invention is lacking** (see Box No III)

4. With regard to the **title,**
   [X] the text is approved as submitted by the applicant
   [ ] the text has been established by this Authority to read as follows:

5. With regard to the **abstract,**
   [X] the text is approved as submitted by the applicant
   [ ] the text has been established, according to Rule 38.2, by this Authority as it appears in Box No. IV. The applicant may, within one month from the date of mailing of this international search report, submit comments to this Authority

6. With regard to the **drawings,**
   a. the figure of the **drawings** to be published with the abstract is Figure No. 2
      [ ] as suggested by the applicant
      [X] as selected by this Authority, because the applicant failed to suggest a figure
      [ ] as selected by this Authority, because this figure better characterizes the invention
   b. [ ] none of the figures is to be published with the abstract

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2014/023286

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L29/06
ADD.

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2003/123456 A1 (DENZ PETER R [US] ET AL) 3 July 2003 (2003-07-03) paragraphs [03.7], [0008], [0025] - [0027]	1-20
X	US 2007/083924 A1 (LU HONGQIAN K [US]) 12 April 2007 (2007-04-12) paragraphs [0054] - [0055]	1-20

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
13 June 2014	24/06/2014

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Veen, Gerardus

1

Form PCT/ISA/210 (second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/US2014/023286

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2003123456 A1	03-07-2003	NONE	
US 2007083924 A1	12-04-2007	NONE	

PATENT COOPERATION TREATY

From the
INTERNATIONAL SEARCHING AUTHORITY

To:

see form PCT/ISA/220

PCT

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY
(PCT Rule 43*bis*.1)

Date of mailing
(day/month/year) see form PCT/ISA/210 (second sheet)

Applicant's or agent's file reference
see form PCT/ISA/220

FOR FURTHER ACTION
See paragraph 2 below

International application No.	International filing date *(day/month/year)*	Priority date *(day/month/year)*
PCT/US2014/023286	11.03.2014	12.03.2013

International Patent Classification (IPC) or both national classification and IPC
INV. H04L29/06

Applicant
CENTRIPETAL NETWORKS, INC.

1. This opinion contains indications relating to the following items:

- ☒ Box No. I Basis of the opinion
- ☐ Box No. II Priority
- ☐ Box No. III Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- ☐ Box No. IV Lack of unity of invention
- ☒ Box No. V Reasoned statement under Rule 43*bis*.1(a)(i) with regard to novelty, inventive step and industrial applicability; citations and explanations supporting such statement
- ☐ Box No. VI Certain documents cited
- ☐ Box No. VII Certain defects in the international application
- ☒ Box No. VIII Certain observations on the international application

2. **FURTHER ACTION**

If a demand for international preliminary examination is made, this opinion will usually be considered to be a written opinion of the International Preliminary Examining Authority ("IPEA") except that this does not apply where the applicant chooses an Authority other than this one to be the IPEA and the chosen IPEA has notifed the International Bureau under Rule 66.1*bis*(b) that written opinions of this International Searching Authority will not be so considered.

If this opinion is, as provided above, considered to be a written opinion of the IPEA, the applicant is invited to submit to the IPEA a written reply together, where appropriate, with amendments, before the expiration of 3 months from the date of mailing of Form PCT/ISA/220 or before the expiration of 22 months from the priority date, whichever expires later.

For further options, see Form PCT/ISA/220.

Name and mailing address of the ISA:	Date of completion of this opinion	Authorized Officer
European Patent Office P.B. 5818 Patentlaan 2 NL-2280 HV Rijswijk - Pays Bas Tel. +31 70 340 - 2040 Fax: +31 70 340 - 3016	see form PCT/ISA/210	Veen, Gerardus Telephone No. +31 70 340-3811

Form PCT/ISA/237 (Cover Sheet) (July 2009)

Box No. I Basis of the opinion

1. With regard to the **language**, this opinion has been established on the basis of:

   ☒ the international application in the language in which it was filed

   ☐ a translation of the international application into , which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1 (b)).

2. ☐ This opinion has been established taking into account the **rectification of an obvious mistake** authorized by or notified to this Authority under Rule 91 (Rule 43bis.1(a))

3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, this opinion has been established on the basis of a sequence listing filed or furnished:

   a. (means)

      ☐ on paper

      ☐ in electronic form

   b. (time)

      ☐ in the international application as filed

      ☐ together with the international application in electronic form

      ☐ subsequently to this Authority for the purposes of search

4. ☐ In addition, in the case that more than one version or copy of a sequence listing has been filed or furnished, the required statements that the information in the subsequent or additional copies is identical to that in the application as filed or does not go beyond the application as filed, as appropriate, were furnished.

5. Additional comments:

Box No. V Reasoned statement under Rule 43*bis*.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Yes:	Claims	
	No:	Claims	1-20
Inventive step (IS)	Yes:	Claims	
	No:	Claims	1-20
Industrial applicability (IA)	Yes:	Claims	1-20
	No:	Claims	

2. Citations and explanations

see separate sheet

Box No. VIII Certain observations on the international application

The following observations on the clarity of the claims, description, and drawings or on the question whether the claims are fully supported by the description, are made:

see separate sheet

Re Item V

Reasoned statement with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

The following documents are referred to:

D1 US 2003/123456 A1 (DENZ PETER R [US] ET AL) 3 July 2003 (2003-07-03)

D2 US 2007/083924 A1 (LU HONGQIAN K [US]) 12 April 2007 (2007-04-12)

1 The present application does not meet the criteria of Article 33(2) PCT, because the subject-matter of claims 1-20 is not new.

1.1 Independent claim 1 (as far as it is clear, see **Item VIII**) defines a method for filtering a packet, the method having two stages:

1) in the first stage, a first operation ('operator') is performed upon the packet, based on a first header field value;

2) in the second stage, a second operation ('transformation') is performed upon the packet, based on a second header field value.

Moreover, these two steps are interrelated in the sense that the criteria, with which the second header field value is compared during the second stage, are determined during the first stage.

Such a method is also disclosed in D1 (see the passages cited in the search report).

Present claim 1 is thus not new according to Art. 33(2) PCT.

1.2 The same reasoning applies, mutatis mutandis, to independent claims 11 and 20 which are, therefore, also not new.

1.3 Dependent claims 2-10 and 12-19 do not appear to contain any features which, in combination with the features of the claims to which they refer, meet the requirements of the PCT in respect of novelty and inventive step, see D1, D2 and the corresponding references cited in the search report.

1.4 It is further noted that a reasoning based on D2 would lead to very similar conclusions.

Re Item VIII

Certain observations on the international application

2 Claims 1-20 do not meet the requirements of Article 6 PCT for, at least, the following reasons:

- in claim 1, the expressions 'header field' and 'application header field', and especially how they differ from each other, are not clear;

- a similar remark applies to the expressions 'operator' and 'packet transformation function', respectively.

Similar observations apply to independent claims 11 and 20.

PTO/SB/08a (01-10)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	13657010
Filing Date	2012-10-22
First Named Inventor	Steven Rogers
Art Unit	2438
Examiner Name	K. W. Chang
Attorney Docket Number	007742.00017

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1	1313290	EP	A1	2003-05-21	Stonesoft Corp		☐
	2	2005046145	WO	A1	2005-05-19	Ericsson Telefon Ab L M		☐

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13657010
	Filing Date	2012-10-22
	First Named Inventor	Steven Rogers
	Art Unit	2438
	Examiner Name	K. W. Chang
	Attorney Docket Number	007742.00017

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1	ISR off International Application No. PCT/US2013/072566, dated March 24, 2014.	☐

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**		
	Application Number	13657010
	Filing Date	2012-10-22
	First Named Inventor	Steven Rogers
	Art Unit	2438
	Examiner Name	K. W. Chang
	Attorney Docket Number	007742.00017

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☐ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

☐ See attached certification statement.

☐ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/William E. Wooten/	Date (YYYY-MM-DD)	2014-06-27
Name/Print	William E. Wooten	Registration Number	60049

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Espacenet

Bibliographic data: EP1313290 (A1) — 2003-05-21

A personal firewall with location dependent functionality

No documents available for this priority number.

Inventor(s): SYVAENNE TUOMO [FI] ± (SYVAENNE, TUOMO)

Applicant(s): STONESOFT CORP [FI] ± (STONESOFT CORPORATION)

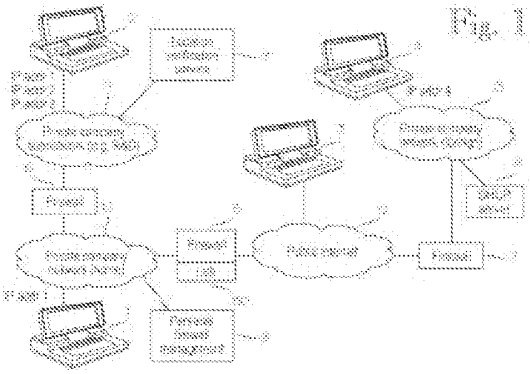
Classification: **- international:** ***H04L29/06;*** (IPC1-7): H04L29/06
- cooperative: **H04L63/0227**; **H04L63/0263**; **H04L63/107**

Application number: EP20020102581 20021114

Priority number (s): US20010988356 20011119

Also published as: EP1313290 (B1) US2003097590 (A1) US7325248 (B2) DE60216218 (T2) AT346446 (T)

Abstract of EP1313290 (A1)



A computer device is provided with a local security mechanism, a personal firewall, for protecting the computer device from attacks from a foreign network, in addition to or instead of a firewall in the internal network which protects the computer when connected to a home network. The personal firewall is provided with different sets of security rules for the home network and foreign networks. The personal firewall is arranged to detect its current location, i.e. determine to which network it is connected to at each particular moment. The personal firewall activates one of the given sets of security rules according to the detected current location of the computer device, i.e. the personal firewall automatically uses the security rules predefined for the network to which the computer device is connected at each particular moment.; Upon detecting a change in the location, the personal firewall immediately adapts to use security rules predefined for the new location.

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 313 290 A1

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
21.05.2003 Bulletin 2003/21

(51) Int Cl.7: **H04L 29/06**

(21) Application number: **02102581.2**

(22) Date of filing: **14.11.2002**

(84) Designated Contracting States:
AT BE BG CH CY CZ DE DK EE ES FI FR GB GR IE IT LI LU MC NL PT SE SK TR
Designated Extension States:
AL LT LV MK RO SI

(30) Priority: **19.11.2001 US 988356**

(71) Applicant: **Stonesoft Corporation**
00210 Helsinki (FI)

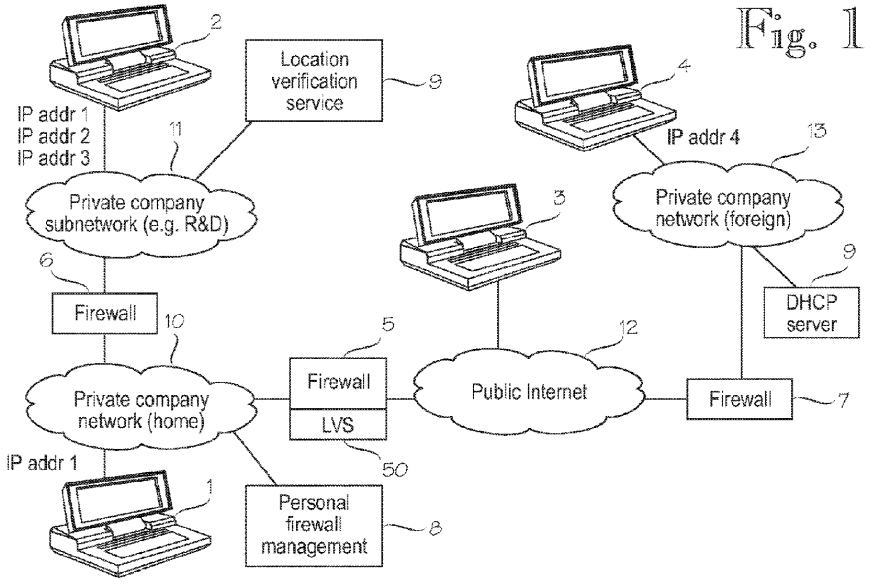
(72) Inventor: **Syvänne, Tuomo**
Fin-01450, Vantaa (FI)

(74) Representative: **Äkräs, Tapio Juhani**
Kolster Oy Ab,P.O. Box 148,
Iso Roobertinkatu 23
00121 Helsinki (FI)

(54) A personal firewall with location dependent functionality

(57) A computer device is provided with a local security mechanism, a personal firewall, for protecting the computer device from attacks from a foreign network, in addition to or instead of a firewall in the internal network which protects the computer when connected to a home network. The personal firewall is provided with different sets of security rules for the home network and foreign networks. The personal firewall is arranged to detect its current location, i.e. determine to which network it is connected to at each particular moment. The personal firewall activates one of the given sets of security rules according to the detected current location of the computer device, i.e. the personal firewall automatically uses the security rules predefined for the network to which the computer device is connected at each particular moment. Upon detecting a change in the location, the personal firewall immediately adapts to use security rules predefined for the new location.

Fig. 1



EP 1 313 290 A1

Printed by Jouve, 75001 PARIS (FR)

Description

Field of the Invention

[0001] The present invention relates to network security and, more particularly, to personal firewalls.

Background of the Invention

[0002] Traditionally, a firewall is considered as a set of components forming a gateway between two or more networks. Thus, a firewall has been a gateway which operates at the same time as a connector and a separator between the networks in a sense that the firewall keeps track of the traffic that passes through it from one network to another and restricts connections and packets that are defined as unwanted by the administrator of the system. Physically a firewall is a machine with appropriate software to do the tasks assigned to it. It can be a router, a personal computer (PC), or any other device that can be used for such purposes. Although firewalls are mostly used to connect Local Area Networks (LANs), i.e. internal networks, to the Internet and to protect against attackers or undesired traffic in general, they may also be used to separate and connect different segments of internal network for security purposes. The advantages of having a firewall are numerous. A firewall secures the network and can be used as a tool for monitoring the traffic especially from the outside to the inside of the network guarded by a firewall. Because all traffic intended for the internal network must pass through the firewall, most of the network security actions and policies can be concentrated in this particular point. This is of course a cost and administrative advantage.

[0003] Nowadays, laptop computers and other portable computer devices are widely used. While outside the internal network, the laptop cannot make benefit of the protection provided by the conventional "gateway-type" firewall. Therefore, approaches to improve security of a client located in a foreign network (a public network or an internal network of a foreign organisation) have been proposed. These approaches are based on protecting the laptop itself by means of a local security mechanism, called a personal firewall herein, installed in the laptop (in addition to or instead of a firewall in an internal network, which protects the computers connected to the internal network). The personal firewall may be implemented as software installed in the computer device, or as a separate electronic device connected to the computer device.

[0004] European patent application EP 0 952 715 discloses a firewall security device connected to an external communication port of a computer device. The incoming communications stream to the computer device from e.g. public networks is passed through the firewall security device. The firewall device applies standard security measures, thereby protecting the computer device.

[0005] There is a particular need for such protection by means of a personal firewall if the laptop is allowed to have a remote access, e.g. make a VPN (Virtual Private Network) connection to company network while being connected to a foreign network. In order to improve security of the VPN connections, one prior art solution is to enforce a protection level of a laptop, when a VPN tunnel to a company network is created. This means for example that, during a VPN connection, the IP address forwarding is not allowed, or that any connection attempts to the laptop are denied.

[0006] Clearly this is not enough, since the laptop must be protected as soon as it is connected to a foreign network, not only during a VPN connection. The laptops are often used by non-technical people, which increases the risk of overlooking security aspects. Laptops contain sensitive material, such as customer emails. If a laptop is unprotected, when connected to a foreign network, even for a short period of time, there is a risk of getting infected by a hostile application. Such application can be activated later, when the laptop is connected to an internal network and offer inside help for attacks.

[0007] Thus, there is a need to protect the laptop by means of a personal firewall always when the laptop is connected to a foreign network. However, when the laptop is connected to a company internal network, such personal firewall may unduly prevent some essential traffic. For example, the personal firewall should allow use of a laptop at home (internal) network and access to all services, such as disk-share. In a home network even non-IP protocols are sometimes used. Therefore, it is not feasible to have a personal firewall running at all times, at least not with the same configuration, since the protection needs in an internal network are different from those in a foreign network.

[0008] Some of the current solutions allow changing the set of rules used in the personal firewall, that is, they allow the user of the laptop to use different rule sets when connected to the internal network and when connected to a foreign network. However this is a manual operation. Since manual action is required, there is a high risk that operation is not done. Risk is even higher if the end user does not fully understand the need of a firewall.

Summary of the Invention

[0009] An object of the invention is to improve the security and flexibility of a personal firewall. The object is achieved by the invention disclosed in the attached independent claims. Preferred embodiments are disclosed in the attached dependent claims.

[0010] A computer device which can be connected to a home network (such as an internal network of a company or other organisation where the user is employed) and to a foreign network (such as a public network or an internal network of a foreign organisation) is provided with a local security mechanism, called a personal fire-

wall herein, for protecting the computer device from attacks from a foreign network, in addition to or instead of a firewall in the internal network which protects the computer when connected to the internal network. The personal firewall is provided with different sets of security rules, at least one set of rules for the home network and at least one set of rules for foreign networks. In its simplest form, the set of rules for the home network contains no restrictions for the communication or use of service in the home network. The personal firewall is arranged to detect its current location, i.e. to determine the network to which it is connected at each particular moment. The personal firewall activates one of the given sets of security rules according to the detected current location of the computer device, i.e. the personal firewall automatically uses the security rules predefined for the network to which the computer device is connected at each particular moment. Upon detecting a change in the location, the personal firewall immediately adapts to use security rules predefined for the new location. A benefit of the invention is that the protection of a personal firewall is always enabled at the correct level, depending on the current location. On the other hand, when the computer device is located in the home network, a lower level of protection, or no protection at all, can be automatically provided by the personal firewall, so that the communication and services are not unduly restricted in the home network. Thus, the automated location-dependent management of different sets of rules offers optimal protection in different networks, while not unduly restricting operation in the home network.

[0011] The current location of the computer device is preferably determined on the basis of a currently used IP address of the computer device. This is based on the common practice that a computer device has a different IP address, either a fixed address or a dynamic address, in different networks. The IP address can thereby be utilized for identifying the current network and the location of the computer device.

[0012] However, there are situations where the IP address fails to indicate current location of the computer device. Therefore, in an embodiment of the invention, the current location determined on the basis of the current IP address of the computer device is verified by carrying out an additional location verification procedure with a predetermined network element. In a still further embodiment of the invention, availability of said predetermined network element related to the current IP address is checked. The predetermined network element is such that it responses only if the computer device is located in the network in which it is assumed to be on the basis of the current IP address. If the predetermined network element responses and identifies itself properly, the current location determined based on the current IP address is considered to be verified. Otherwise the computer device determines that the current IP address fails to indicate current location of the computer device. The additional verification process makes it even possible to automatically create a secured tunnel, such as a VPN tunnel to a home network even if the computer device uses the same IP address in the current location as in the internal (home) network. The present invention offers benefits even with stand alone personal firewalls wherein the security rules can be defined locally by the user, although the use of these rules is automated and location-dependent. However, more advantages are achieved when the basic invention is used with a central management of personal firewalls.

[0013] According to an aspect of the invention, security rules are defined, updated and distributed centrally by a centralized rule-based server. Especially the updating of the rules is challenging, because the rule updates must be applied as soon as possible, and therefore the process of updating rules in the personal firewalls must be automated. Updating of rules by push method from the centralized rule base server is not a sufficient option in this case. Use of DHCP (Dynamic Host Configuration Protocol), frequent travelling and the fact that at times the laptop may not be connected to any network makes it next to impossible for the centralized management to initiate contacts with the personal firewalls in the computer devices, because there is no way for the centralized management to know the IP address the computer device is using at a given moment. Therefore, according to an aspect of the invention, the personal firewall is configured to periodically query the availability of updated security rules from the centralized management. The queries should only be made, while the computer device is located in the home network, or optionally, when the computer device has a remote access (e.g. VPN connection) to the home network while being located in a foreign network. In other words, also the updating process is dependent on the current location of the computer device in a similar manner as the selection of the active rules, and similar methods can be utilized for determining the current location.

[0014] According to another aspect of the invention, log files containing information of a status and usage of resources of the computer device are handled in a centralized management location. This enables personnel aware of security aspects to verify whether there have been any attacks against the computer device or not. To that end, the personal firewall sends the log files to the central management, such as to a centralized log server, when the computer device is located in the home network. However, when the computer device is disconnected from the home network, the log files are collected and stored locally in the firewall. In order to enable central handling of the log files, the personal firewall transfers the collected log files to the central log server when such is available. This is performed automatically, whenever the computer device is located in, or optionally, connected to the home network. Again, the handling of the log files in the personal firewall is automated and location dependent in a way similar to the selection of active rules, and similar methods can be used for de-

termining the current location of the computer device.

[0015] The present invention allows use of a computer device in a home (internal) network and access to all services, such as disc-share, and even use of non-IP protocols, which are often denied in foreign networks.

Brief description of the drawings

[0016] Preferred embodiments of the invention will now be described with reference to the attached drawings, in which

Figure 1 is a schematic block diagram of an exemplary network configuration where the present invention can be applied;
Figure 2 shows an exemplary protocol stack of a computer device containing a personal firewall according to the present invention,
Figure 3 illustrates exemplary selection rules and a security rule basis, and the association therebetween,
Figure 4 is a flow diagram illustrating a location-dependent rule base selection according to an embodiment of the invention;
Figures 5 and 6 are flow diagrams illustrating the location verification procedure according to an embodiment of the invention;
Figures 7 and 8 are flow diagrams illustrating the rule base updating according to an embodiment of the invention; and
Figure 9 is a flow diagram illustrating the handling of log files according to an embodiment of the invention.

Preferred embodiments of the invention

[0017] The present invention can be applied in personal firewalls in any computer device which can be moved and connected to different networks. Typically such devices are portable computer devices, such as laptop computers, PDAs, communicators, smart phones, intelligent telecommunication devices, etc. In the following illustrative embodiments of the invention, a laptop computer is used as an example of suitable computer devices.

[0018] Figure 1 shows a schematic block diagram of an exemplary network configuration. The configuration is shown only to facilitate the understanding and description of the present invention. The present invention is not intended to be restricted to any particular network configuration. Further, in order to improve clarity, only network elements which are somehow involved with the present invention are shown in Figure 1.

[0019] As illustrated in Figure 1, private local networks 10 and 13 are coupled to a public network, such as the Internet 12 via firewalls 5 and 7, respectively. Naturally, the coupling between the private networks and the public Internet 12 may include also routers and Internet service providers (ISPs not shown in Figure 1). As is well known in the art, private networks 10 and 13 may be, for example, company networks, such as local area networks (LANs) which connect users and resources, such as workstations, servers, printers and the like of the company. A private internal network may also consist of several sub-networks separated by internal firewalls. In the exemplary network configuration shown in Figure 1, the private company sub-network 11 is connected via a firewall 6 to the private local network 10. Such a sub-network 11 may be, for example, a dedicated network for a specific department of the organisation, such as the research and development (R&D) department which must have a restrictive access and higher protection level compared with other part of the company network. Sub-networks of the company, such as the local networks of organisation headquarters and branch offices may be interconnected by secure connections, such as virtual private network (VPN).

[0020] As already described above, the firewalls 5, 6 and 7 are gateways which operate at the same time as connectors and separators between the networks in a sense that the firewall keeps track of the traffic that passes through it from one network to another and restricts connections and packets that are defined as unwanted by the administrator of the system. Physically a firewall is a machine with appropriate software to perform the task assigned to it. It can be a router, a personal computer (PC), or whatever that can be used for such purposes.

[0021] However, the firewalls between the networks, or the implementations thereof, are not relevant to the present invention.

[0022] The present invention relates to protecting of the computer device, e.g. laptop itself, by means of a local security mechanism, called a personal firewall herein, installed on the laptop in addition to or instead of a firewall in a private network. The personal firewall may be implemented as software installed and run in the computer device, which is a preferred embodiment, or as a separate electronic device connected to the computer device. In Figure 1, the laptops 1, 2, 3 and 4 illustrate laptops provided with a personal firewall.

[0023] Figure 2 illustrates the basic principle of a personal firewall installed in a laptop. Physical and network layers 200 refer to all protocols and physical connections required for transferring protocol data units (PDUs) of the upper layers. The upper layers 200 include applications and any transmission protocols employed, such as Internet protocol (IP) transmission control protocol (TCP), NetPEUI, IPX, etc. Basically the personal firewall protection layer 201 operates in a manner analogue to a firewall between networks. More particularly, the personal firewall protection layer 201 operates at the same time as a connector and a separator between the underlying layers and the upper layer in a sense that the personal firewall keeps track of the traffic that passes through it from underlying layers to the upper layers, and

vice versa, and restricts connections and packets that are defined as unwanted according to the security rules used. The personal firewall protection layer 201 is implemented or controlled by a personal firewall application 203 run in the laptop. In a preferred embodiment of the invention, the personal firewall application 203 carries out the location detection and the location-dependent functions described below, such as the selection of the active rule base according to the current location of the laptop. However, it should be appreciated that the present invention is not intended to be restricted to any specific practical implementation of the personal firewall.

[0024] In accordance with the principles of the present invention, the personal firewall has different sets of rules for the home network (such as the private company network 10) and foreign network, such as the public Internet 12, or the foreign private network 13, or a network of another department of the company. It is not relevant to the present invention what kind of security rules are applied, but some examples are given in Figure 3. For example, a rule base 301 for the foreign company network may list as allowed connections of protocols: hypertext transfer protocol (http), secured http (Https), domain name service (DNS), single message transfer protocol (SMTP) and a VPN connection with IPsec. In the preferred embodiment of the invention these rules are exclusive, in other words, other protocols and connections are denied and blocked by the personal firewall. For a default network, which may be the public Internet 12, the rule base 302 is similar to the rule base 301, except that the SMTP protocol is no longer allowed. For the home network 10, a rule base 300 is defined. The allowed protocols include, in addition to the http, https and the SMTP, also other transmission protocols, such as NetBEUI and IPX. The rule base 300 also allows a disc-share for predefined servers using NetBIOS. Other protocols and connections are denied. It is also possible that the rule base 300 allows all protocols and connections in the home network. Since the home network is protected by a company firewall, the use of a personal firewall in the home network may be regarded as unnecessary. However, the company firewall gives protection only against attacks from the outside of the home network, and the use of a personal firewall protection may be necessary for protecting against attacks from within the home network.

[0025] The different rule bases could be activated manually by a user. However, according to the basic principle of the present invention, the personal firewall automatically selects and activates the proper rule base according to the current location of the laptop.

[0026] Figure 4 is a flow diagram illustrating the selection of the rule base according to one embodiment of the present invention. The simplest way to determine the current location of the laptop is to do it on the basis of the currently used IP address only. This is possible in the cases where the laptop has a different IP address, either a fixed or a dynamic address, in different networks. As is well known in the art, a part of the IP address identifies the network, and can thus be used for detecting the current network of the laptop. The personal firewall may, for example, contain information on the IP address space of home network, and optionally, foreign networks, or a list of addresses available for the laptop in the home network.

[0027] When the current IP address of the laptop matches to a given address space or a list of addresses of the home network 10, for example, it can be assumed that the laptop is located in the home network 10 and the rule base 300 of the home network 10 is used. Thus, the current IP address is used as a selection rule for activating the rule base 300. However, there is some uncertainty in determining the location based on the current IP address only, and some approaches to overcome this problem are described with reference to further embodiments of the invention below.

[0028] Referring again to the generic flow diagram shown in Figure 4, the current IP address of the laptop is firstly determined in the step 401. The current IP address may be obtained simply by asking for it from the operating system of the laptop by means of using IP configuration routine. The current location of the laptop is monitored constantly, and therefore the personal firewall may be configured to periodically query the current IP address from the operating system. More preferably, the operating system of the laptop may be configured to inform any changes in the IP address to the personal firewall, and therefore a need for query the IP address time-to-time can be avoided. The step 401 may also include verification of the location determined based on the IP address by a verification procedure described below. In step 402, the personal firewall compares the current IP address with the current IP address stored in the personal firewall. If the IP address has not changed, the present active rule base can be maintained. However, if the IP address has changed, the personal firewall checks whether the new IP address matches to any IP address space or IP address belonging to one of the networks on the selection rule list in the personal firewall (step 403). If the new IP address does not belong to any of the networks on the selection rule list, the personal firewall considers the current network an unidentified network, and a default rule base 302 is selected (step 404). If the network cannot be identified and the default rule base must be used, it is normally assumed that the laptop is in a potentially hostile environment, most likely in the public Internet 12. Therefore, the default rule base is typically defined to provide the maximum protection needed. If the new IP address belongs to one of the networks defined on the selection rule list in step 403, it means that the network has been identified and a rule base linked to the identified network (or the corresponding selection rule) is selected and activated (step 405). In the simplest implementation, the selection rules include only the home network of the laptop and the cor-

responding IP address space or list of addresses . If the current IP address belongs to the home network, the rule base 300 of the home network 10 is used. Otherwise the rule base 310 for foreign network or the default rule base 302 is used. In a more complicated implementation, there are selection rules (i.e. IP addresses and associated rule bases) also for at least one foreign network and/or different segments of the home network 10.

[0029] In the examples described above there are two or more rule bases which are enabled or disabled on the basis of the current location of the laptop. However, there are also alternative ways to implement different rule bases. One alternative is to provide only one rule base in which the rules are enabled and disabled in different combinations on the basis of the current location of the laptop.

[0030] As noted above, there are situations where the location (the current network) determined on the basis of the current IP address is uncertain, i.e. the IP address fails to indicate the current location of the laptop. If the IP address does not match the current network, use of the Internet protocol (IP) to attack against the laptop is not likely, and one may reason that in that case a personal firewall does not need to be used. However, there is still a possibility that there is an attack using other protocols, such NetBEUI or IPX. By detecting the situation where the IP address of the laptop is not an IP address of the current network, it is possible to block such protocols while in foreign networks. Further, NAT (network address translation) and private IP addresses are frequently used. This means that the same IP address is in use in several networks. In that case it is not enough to trust IP address information only when determining the location of the laptop. It is even possible that while being connected to a hostile network, the DHCP (dynamic host configuration protocol) gives familiar IP address to make it easier to attack the laptop. Basically, the DHCP enables individual computers on a network to connect to a DHCP server, such as the server 9 in Figure 1, and be assigned a dynamic IP address of the current network.

[0031] Thus, according to an aspect of the invention, in addition to the detection of location based on the current IP address described above, a further location verification procedure is carried out with a predetermined network element, which is preferably reachable only from the location to be verified. More generally, the network element is selected in such a way that it responses to the verification request only if the request originates from the location (i.e. the network) to be verified. Preferably, the specific network element is provided with a location verification service supporting the verification according to the invention. The verification procedure requires that the verification method be specified for the personal firewall, preferably at the same time as the different locations are specified. In other words, the methods to verify the location are specified for the personal firewall in the initial configuration, for example. It is also possible that the verification methods are updated or changed by means of the updating procedure described below, in a manner similar to other security rules.

[0032] A generic location verification procedure according to one embodiment of the invention is described with reference to Figures 5 and 6. Firstly, the current location is determined on the basis of the currently used IP address as described above (step 501). Next, the personal firewall selects a predetermined network element that should be available for verification from the determined current location (step 502). Then the personal firewall sends to the selected network element a request to send a response with some data proving the identity of the network element (step 503). Referring now to Figure 6, the verifying network element receives the verification request (step 601) from a personal firewall. Then, either always in response to the verification request or only if predetermined requirements are met, the network element sends the response with the required identity data to the personal firewall (step 602). Referring again to Figure 5, the personal firewall waits for a response (step 504), and if no response is received (preferably within a predetermined period of time), the location determined on the basis of the current IP address is rejected, and the location is determined to be unknown (step 505). In that case, a default location and an associated rule base, such as the rule base 302, can be used.

[0033] However, if the response is received from the network element in the step 504, the personal firewall verifies the identity of the network element on the basis of the received identity data, e.g. by comparing the received identity data with identity data stored in the personal firewall (step 506). If the verification of the identity is unsuccessful (step 507), the procedure proceeds to the step 505 described above. However, if the verification of the identity of the network element is successful, also the location of the laptop determined on the basis of the current IP address has been successfully verified and can be accepted.

[0034] Additionally, it is possible that one IP address is included in more than one selection rule in the personal firewall. In that case, if the verification of the laptop being located in a first network indicated by the current IP address fails, it is checked if the laptop is located in a second network indicated by the current IP address. There are various ways to implement the generic location verification procedure described above. The simplest way to implement the location verification service is to probe some known (known to the personal firewall) element. For example, it is possible to ask the MAC address of the known network element located in the home network and having a known IP address. The network element returns the MAC address in response, and if the AMC address is the one that it is assumed to be (e. g. matches with a MAC address stored in the personal firewall), it is verified that the laptop is located in the home network. If the MAC address is not the correct one, the laptop is determined to be outside the internal

network.

[0035] One possible implementation is that the location verification service is implemented in such network element in an internal network which can be reached only from inside the internal network. For example, the firewall protecting the internal network, such as firewall 5 in Figure 1, may be configured to discard all connections from outside the internal network to this network element. If the personal firewall is able to reach this specific network element, it is verified that the personal firewall resides inside the internal network. Otherwise the personal firewall resides outside the internal network. There may be a plurality of such location verification services in a plurality of internal networks or sub-networks, and if the personal firewall cannot reach any of them, then it is assumed to be outside this plurality of internal networks or sub-networks.

[0036] The location verification service may be incorporated into the network firewall, such as the location verification service 50 in the firewall 5 in Figure 1. For example, verification requests only from the direction of the internal network (such as home network 10) may be responded by the location verification service 50. This implementation is rather straightforward, since the present firewalls are readily capable of detecting from which direction, that is, from which interface, a data packet is coming from.

[0037] In any case it is preferred that the personal firewall communicates with the location verification service by using some cryptographically strong method, such as public key encryption. For example SSL can be used. The certainty of the location verification can be further improved by setting the TTL (time-to-live) field in the location verification request to a relatively low value, so that the request is capable of reaching only a nearby location verification service. The TTL value is decremented each time the verification request passes through a router connecting different networks or network segments. If the TTL value is set to, for example, a zero value the verification request is not able to pass through a router to a different network or a network segment.

[0038] The use of additional location verification makes it even possible to automatically create a VPN tunnel to the home network even if the current location (a foreign network) is using the same IP address as in the internal network.

[0039] All the embodiments described above are effective both in standalone computers and in centrally managed computers. The central management of personal firewalls enables a uniform protection level in all computer devices using the private network. One feature of the central management is that preferably all of the personal firewalls have essentially similar security rules. It should also be possible to update these. It is preferable that rule updates are applied in the personal firewalls as soon as possible after they have been made in the central management. Because it is not sufficient to rely on the manual updating by the user, the process of updating the rules must be automated. However, distribution of the updated rules by a push transmission from the central management is not a sufficient option in a case where the personal firewalls can move from one network to another. Therefore, according to an aspect of the invention, the personal firewalls are arranged to periodically query the availability of updated rules from the central management. An updating procedure according to one embodiment of the invention is described with reference to Figures 7 and 8.

[0040] Firstly, a personal firewall measures a predetermined updating period, which can be any period of time, preferably one day or a few days (step 701). In step 702, the personal firewall checks whether the updating period has expired, and if not, the procedure returns to the step 701. When the updating period has expired, the personal firewall checks whether the current location of the laptop is in the home network (step 703) or in another subnetwork of the same company. The location determination is preferably based on the methods described above. If the current location is in the home network, the process proceeds directly to the step 705. However, if the current location is not in the home network, the personal firewall waits for the laptop to return to or establish a connection (e.g. VPN) to the home network (step 704), before proceeding to the step 705. In the step 705, the personal firewall sends a rule update query to the central management, such as the personal firewall management server 8 in Figure 1. Referring now to Figure 8, the personal firewall management 8 receives the rule update query from the personal firewall (step 801) and sends updated rules, if there are any, to the personal firewall (step 802). Referring again to Figure 7, the personal firewall checks whether the reply received from the personal firewall management 8 contains rule updatings (step 706), and if not, the process returns to the step 701 to measure the next updating period. However, if rule updatings have been received, the personal firewall updates the relevant rule bases stored in the laptop (step 707).

[0041] It is also preferable that the logs relating to the communication transactions of the laptop are handled in a central location. Since the laptops are frequently disconnected from the home network, logs must be collected locally. In order to enable central handling, the logs must be transferred to a central log server, such as the personal firewall management 8, when such is available. This should take place automatically when the computer device provided with a personal firewall is connected to the home network. Figure 9 illustrates log handling according to one embodiment of the invention.

[0042] Firstly, the personal firewall creates a log file each time the laptop is involved with a communication transaction, such as an Internet session (step 91). Then the personal firewall determines the current location of the laptop, preferably based on the location determining methods described above (steps 92 and 93). If the lo-

cation of the laptop is in the home network or in another subnetwork of the same company, the personal firewall sends the log file to the central log server 8 immediately (step 94). However, if the current location of the laptop is not in the home network, the process proceeds to the step 95, where the log file is stored locally. Similarly, a number of log files is collected locally while the laptop is disconnected from the home network. When the personal firewall next time detects that the computer device is relocated in the home network, it sends the collected log files to the central log server 8. Optionally, the personal firewall may also send the collected log files to the personal firewall management 8 when the laptop has established a (e.g. VPN) connection to the home network.

[0043] It is apparent for those skilled in the art that the illustrative embodiments described are only examples and that various modifications can be made within the scope and spirit of the invention as defined in the appended claims.

Claims

1. A method of controlling a personal firewall in a client computer, said method comprising
   providing said personal firewall with at least one set of security rules to be used when said client computer is connected to a home network of said client computer, and at least one set of security rules to be used when said client computer is connected to foreign networks,
   monitoring the current location of said client computer based on an Internet Protocol (IP) address currently used by said client computer, and
   automatically selecting one of said sets of security rules by said personal firewall according to said current location of said client computer.

2. A method according to claim 1, wherein
   said step of providing comprises providing said client computer with said set of security rules in form of at least two rule bases,
   said step of selecting comprises enabling one of said rule bases at a time according to the current location of said client computer.

3. A method according to claim 1, wherein
   said step of providing comprises providing said client computer with said set of security rules in form of one rule base, and
   said step of selecting comprises enabling and disabling rules in said one rule base in different combinations according to the current location of said client computer.

4. A method according to claim 1, wherein said step of monitoring comprises
   storing in said client computer an IP address space of said home network,
   comparing the current IP address of said client computer with said IP address space, and
   if the current IP address of said client computer matches said IP address space, determining said personal firewall to be located in said home network.

5. A method according to any one of claims 1, 2 or 3, wherein said step of monitoring comprises
   storing in said client computer a list of IP addresses of said home network,
   comparing the current IP address of said client computer with said list of IP addresses, and
   if the current IP address of said client computer matches one of said addresses on said list, determining said client computer to be located in said home network.

6. A method according to any one of claims 1, 2 or 3, comprising
   verifying the current location determined on the basis of the current IP address of said client computer by carrying out a location verification procedure with a predetermined network element.

7. A method according to claim 6, wherein said step of verifying comprises
   checking availability of said predetermined network element related to the current IP address, said predetermined network element responding only if said client computer is located in the network in which it is assumed to be on the basis of the current IP address,
   verifying the current location determined based on said current IP address, if said predetermined network element responses with a specific identity data.

8. A method according to claim 7, wherein said specific identity data is a Media Access Control (MAC) address of said predetermined network element.

9. A method of managing a personal firewall in a client computer, comprising
   storing in said personal firewall at least one set of security rules to be used when said client computer is connected to a home network of said client computer, and at least one set of security rules to be used when said client computer is connected to foreign networks,
   storing updated sets of security rules, if any, in a centralized unit in said home network of said client computer,
   configuring said personal firewall to periodically query the availability of said updated sets of security rules from said centralized rule base server

when being located in said home network, or when having a remote access to said home network while being located in a foreign network, and

loading said updated sets of security rules from said centralized rule base server to said personal firewall in response to said query, if such updated sets of security rules are available.

10. A method according to claim 9, comprising

monitoring the current location of said client computer based on an Internet Protocol (IP) address currently used by said client computer, and

automatically activating said periodical query, when the current location of said client computer is in said home network.

11. A method according to claim 9, comprising

monitoring the current location of said client computer based on an Internet Protocol (IP) address currently used by said client computer,

sending log files to a centralized log server from said personal firewall, when the current location of said client computer is in said home network, said log files containing information on communication transactions in said client computer,

collecting log files locally at said personal firewall, when the current location of said client computer is not in said home network, and

transferring said locally collected log files from said personal firewall to said centralized log server, when said client computer is connected to said home network.

12. A computer terminal, comprising

a personal firewall provided with at least one set of security rules to be used when said computer terminal is connected to a home network of said computer terminal, and at least one set of security rules to be used when said computer terminal is connected to foreign networks,

said personal firewall having a mechanism monitoring the current location of said computer terminal based on an Internet Protocol (IP) address currently used by said computer terminal, and

said personal firewall having a mechanism automatically selecting one of said sets of security rules by said personal firewall according to said current location of said computer terminal.

13. A computer terminal according to claim 12, further comprising

a mechanism verifying the current location determined on the basis of the current IP address of said computer terminal by carrying out a location verification procedure with a predetermined network element.

14. A computer-readable medium, containing a computer software which, when executed in a computer device, causes the computer device to provide a personal firewall routine comprising

storing at least one set of security rules to be used when said computer device is connected to a home network of said computer device, and at least one set of security rules to be used when said computer device is connected to foreign networks,

monitoring the current location of said computer device based on an Internet Protocol (IP) address currently used by said computer device, and

automatically selecting one of said sets of security rules by said personal firewall according to said current location of said computer device.

15. A computer-readable medium according to claim 14, said personal firewall routine further comprising

verifying the current location determined on the basis of the current IP address of said client computer by carrying out a location verification procedure with a predetermined network element

16. A computer device, comprising a personal firewall routine configured to store security rules for a home network of said computer device, and for foreign networks,

periodically query the availability of updated security rules from a centralized rule base server in said home network of said computer device when said computer device is located in said home network, and

download said updated security rules from said centralized rule base server, if such updated security rules are available in said centralized rule base server.

17. A computer device according to claim 16, said personal firewall routine being further configured to

activate said periodical query also when said computer device has a remote access to said home network while being located in a foreign network.

18. A computer device, comprising a personal firewall routine configured to

send log files to a centralized log server, when a current location of said computer device is in a home network of said computer device, said log files containing information on communication transactions in said computer device,

collect log files locally in said computer device, when the current location of said client device is not in said home network,

transfer said locally collected log files to said centralized log server, when said computer device is reconnected to said home network.

19. A computer-readable medium, containing computer software which, when executed in a computer de-

vice, causes the computer device to provide a personal firewall routine comprising

storing security rules for a home network of said computer device, and for foreign networks,

periodically querying the availability of updated security rules from a centralized rule base server in said home network of said computer device when said computer device is located in said home network, and

downloading said updated security rules from said centralized rule base server, if such updated security rules are available in said centralized rule base server.

20. A computer-readable medium, containing computer software which, when executed in a computer device, causes the computer device to provide a personal firewall routine comprising

sending log files to a centralized log server, when a current location of said computer device is in a home network of said computer device, said log files containing information on communication transactions in said computer device,

collecting log files locally in said computer device, when the current location of said client device is not in said home network,

transferring said locally collected log files to said centralized log server, when said computer device is reconnected to said home network.

21. A computer program comprising program code means for performing all the steps of any one of claims 1 to 11 when the program is run on a computer.

Fig. 1

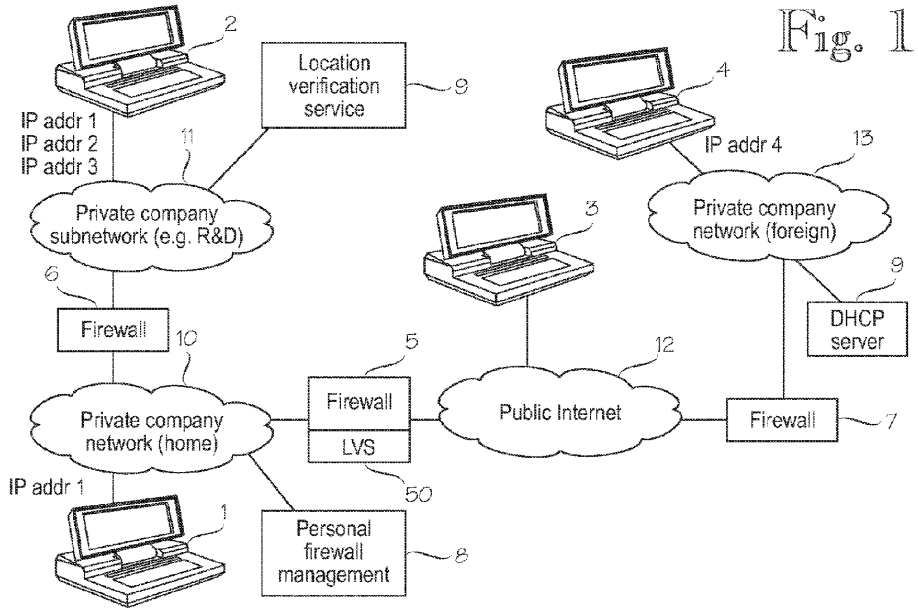


Fig. 2

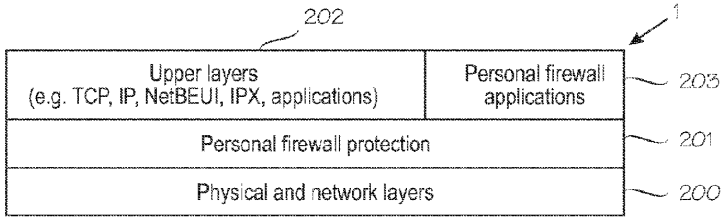


Fig. 3

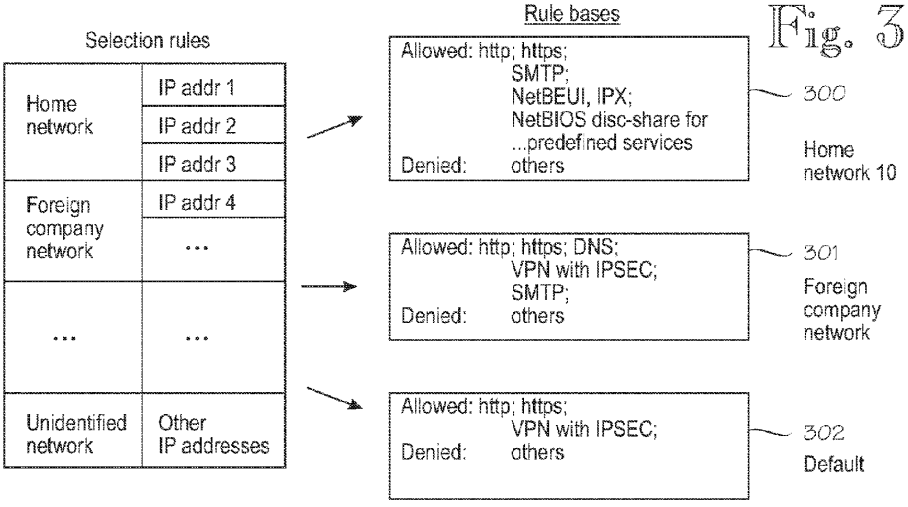


Fig. 4

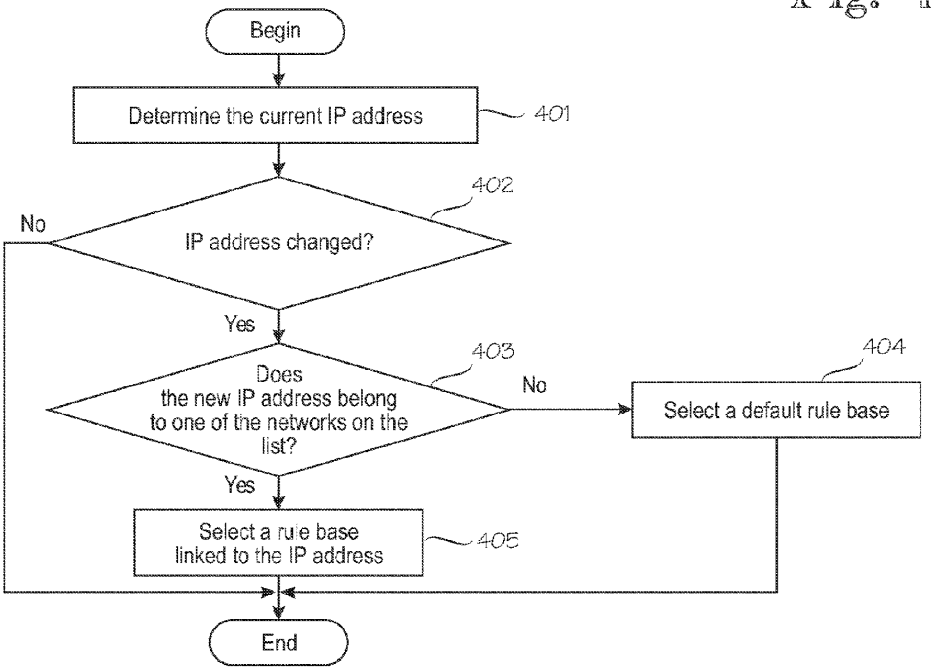


Fig. 9

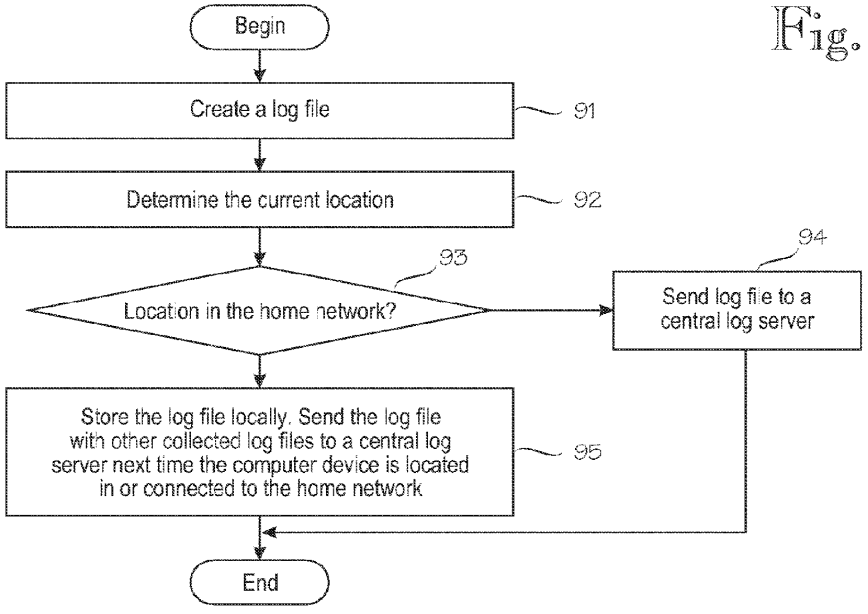


Fig. 5

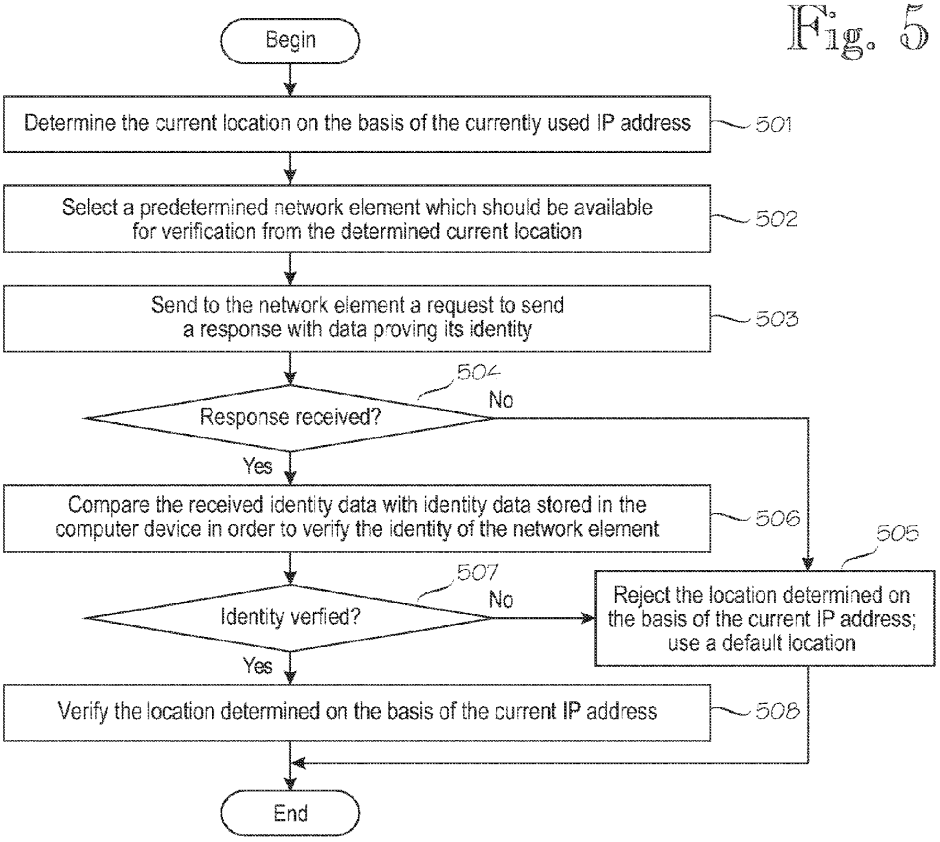


Fig. 6

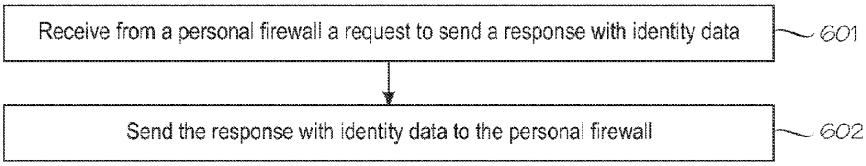


Fig. 8

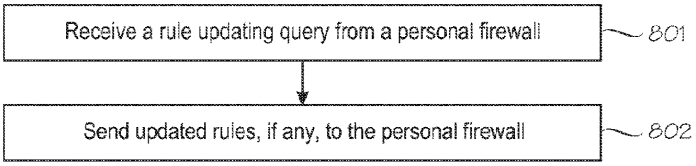
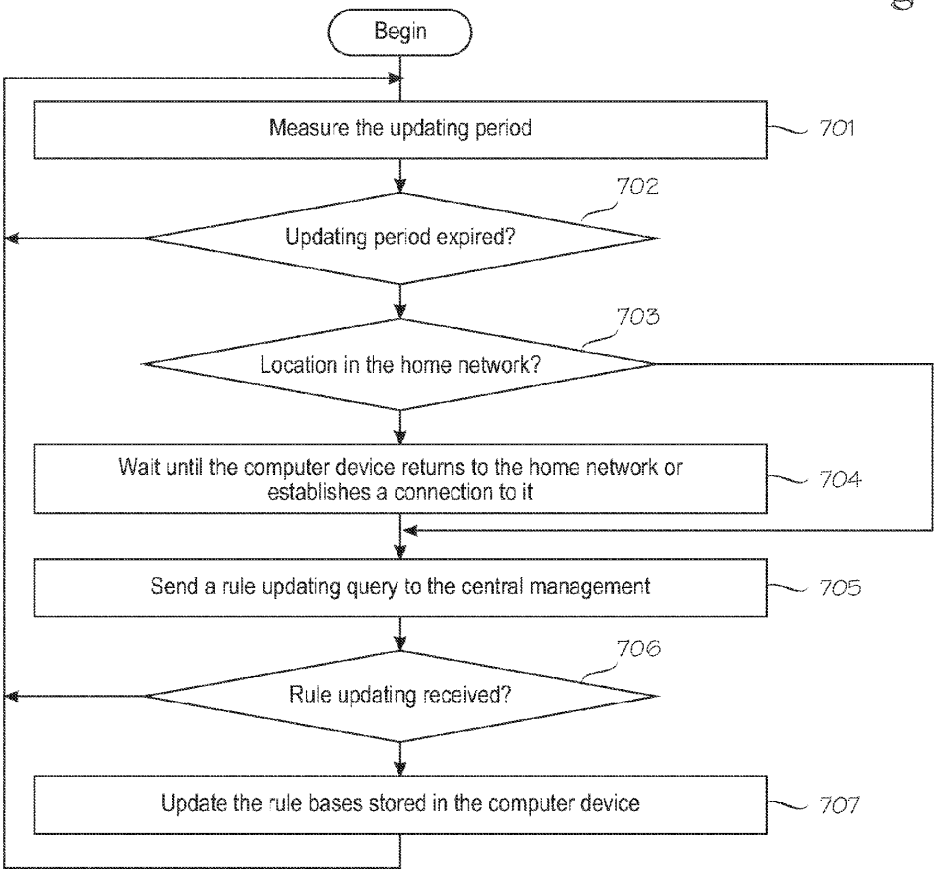


Fig. 7



European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 02 10 2581

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.7)
A	EP 0 854 621 A (AT & T CORP) 22 July 1998 (1998-07-22) * page 4, line 28 - line 47 * ---	1-21	H04L29/06
A	US 6 158 008 A (OWENS LESLIE DALE ET AL) 5 December 2000 (2000-12-05) * claim 1 * -----	1-21	

TECHNICAL FIELDS SEARCHED (Int.Cl.7)

H04L

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
THE HAGUE	14 March 2003	Veen, G

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 02 10 2581

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

14-03-2003

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0854621 A	22-07-1998	US 6233686 B1	15-05-2001
		CA 2226814 A1	17-07-1998
		EP 0854621 A1	22-07-1998
		JP 10229418 A	25-08-1998
US 6158008 A	05-12-2000	WO 9921339 A1	29-04-1999

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82

Espacenet

Bibliographic data: WO2005046145 (A1) — 2005-05-19

ADAPTABLE NETWORK BRIDGE

No documents available for this priority number.

Inventor(s): HALEN JOACIM ± (HALEN, JOACIM)

Applicant(s): ERICSSON TELEFON AB L M [SE] ± (TELEFONAKTIEBOLAGET LM ERICSSON (PUBL))

Classification: **- international:** ***H04L12/24; H04L12/46; H04L12/56;***
(IPC1-7): H04L12/46; H04L12/56
- cooperative: **H04L12/4625**; **H04L41/0893**; **H04L41/0896**; **H04L45/04**; **H04L45/56**; **H04L45/66**; **H04L49/351**

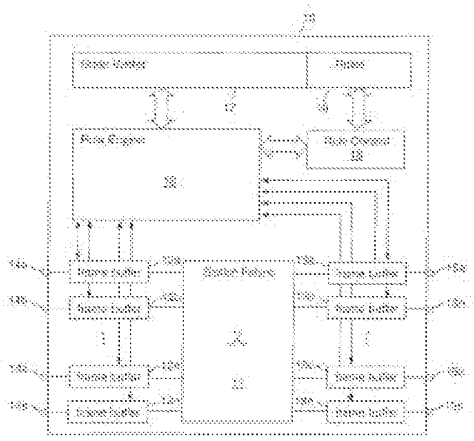
Application number: WO2004SE01611 20041105

Priority number (s): US20030517737P 20031106 ; US20040977724 20041029

Also published as: US2005111434 (A1) US7672318 (B2) JP2007534219 (A) JP4323523 (B2) EP1683313 (A1) more

Abstract of WO2005046145 (A1)

An adaptable network bridge such as an Ethernet bridge (10) includes a Rule Engine (16) that processes data frames according to a set of switching rules. Each switching rule identifies a type of frame to which the rule applies, and how the type of frame is to be processed. The bridge also includes means (18) for dynamically adding, subtracting, or modifying the switching rules in response to changes in the bridge's state information, or changes in context information. If the bridge includes a plurality of input/output ports (14, 15), the Rule Engine (16) may include a plurality of sets of switching rules, with each set of switching rules being applicable to a different port in the bridge. In this way, different network providers can share the same equipment, but have different network behavior.



(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
19 May 2005 (19.05.2005)

PCT

(10) International Publication Number
WO 2005/046145 A1

(51) International Patent Classification[7]: H04L 12/56, 12/46

(21) International Application Number:
PCT/SE2004/001611

(22) International Filing Date:
5 November 2004 (05.11.2004)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

60/517,737	6 November 2003 (06.11.2003)	US
10/977,724	29 October 2004 (29.10.2004)	US

(71) Applicant: **TELEFONAKTIEBOLAGET LM ERICSSON (publ)** [SE/SE]; S-164 83 Stockholm (SE).

(72) Inventor: **HALEN, Joacim**; Anhaltsvägen 8, S-191 40 Sollentuna (SE).

(74) Agent: **KARIN BOESTAD et al.**; Ericsson AB, Patent Unit Core Networks Kista, S-164 80 Stockholm (SE).

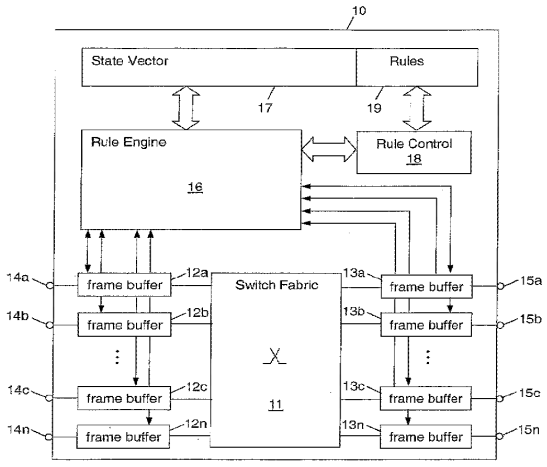
(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*
— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: ADAPTABLE NETWORK BRIDGE



(57) Abstract: An adaptable network bridge such as an Ethernet bridge (10) includes a Rule Engine (16) that processes data frames according to a set of switching rules. Each switching rule identifies a type of frame to which the rule applies, and how the type of frame is to be processed. The bridge also includes means (18) for dynamically adding, subtracting, or modifying the switching rules in response to changes in the bridge's state information, or changes in context information. If the bridge includes a plurality of input/output ports (14, 15), the Rule Engine (16) may include a plurality of sets of switching rules, with each set of switching rules being applicable to a different port in the bridge. In this way, different network providers can share the same equipment, but have different network behavior.

WO 2005/046145 A1

ADAPTABLE NETWORK BRIDGE

CROSS-REFERENCE TO RELATED APPLICATIONS

This nonprovisional application claims priority under 35 U.S.C. § 119(e) on U.S. Provisional Application No. 60/517,737 entitled, *Programmable Bridge*, filed November 6, 2003, the disclosure of which is incorporated herein in its entirety.

BACKGROUND OF THE INVENTION

Technical Field of the Invention

The present invention relates generally to digital communication systems. More particularly, and not by way of limitation, the invention is directed to an adaptable network bridge having a Rule Engine that simplifies adapting the bridge to dynamically changing conditions.

Description of Related Art

Ethernet is a layer-2 packet-based transmission protocol that is primarily used in local area networks (LANs). Ethernet is the common name for the Institute of Electrical and Electronics Engineers (IEEE) 802.3 industry specification. Data is transmitted in Ethernet frames. Each frame includes a preamble with 64 bits utilized for synchronization. A Start of Frame Delimiter (SFD), a destination address, a source address, and a length/type identifier follow the preamble. Media Access Control (MAC) client data, together with a Packet Assembler/Disassembler (PAD) may vary in length from 46 to 1500 bytes (octets). A Frame Check Sequence (FCS) adds four more octets. Higher-level protocols reside in the content part of the frame. The frame size is counted from the destination address to the FCS, inclusive, and thus may vary between 64 and 1518 octets, not including a Virtual Local Area Network (VLAN) tag, which adds 4 octets.

Today most packet-based networks are built on Ethernet technology, as it is a cheap and reliable technology with good performance. Ethernet has been used in office networks for a long time and is now used to build Wide Area Networks (WANs) as well as small networks in homes. The communications

industry is now expanding the use of Ethernet to what is called "Public Ethernet" where millions of users are connected in the same network. Unfortunately, Ethernet does not scale to such large networks due to flooding of broadcasted messages. Some solutions have been proposed, but these solutions require modifications to the existing standards if they are to be implemented on standard equipment.

Ethernet bridging is a way to connect networks together to form a larger network. The standard for bridging is ANSI/IEEE 802.1d, which is hereby incorporated by reference herein. A bridge is a way to connect two separate network segments together in a protocol-independent way. Packets are forwarded based on Ethernet address, rather than IP address. Since forwarding is done at Layer 2, all protocols can go transparently through a bridge.

There are basically two approaches to adding new functionality to Ethernet bridges (and other Ethernet equipment as well): standardization thru IEEE, or proprietary solutions, which make the equipment non-standard. Adding new functionality and behavior to IEEE 802.1d MAC bridges, better known as Ethernet switches (or other Ethernet equipment), is a difficult and time-consuming process without any guarantees of success. Each new function must be proposed to and scrutinized by an IEEE standardization group (an existing working group or a new group has to be accepted and established). If one is lucky, the proposed function is accepted and added to the standard. However, since each new function requires a change in the standard, there is reluctance to add new functions. If the proposal is rejected, one is limited to a proprietary solution on non-standard equipment. The members of the standardization groups come from different vendors and other organizations, and although they are supposed to act in the interest of IEEE and the entire community, they may also act on agendas from their own organization/company that might be in conflict with the proposed functionality, thereby turning it down. It should also be noted that if a new function is added to the standard, it is then up to the different vendors to add the standardized functionality. A feature may be standardized but not made mandatory.

The proprietary approach also has its drawbacks. For example,

programmable network processors have been available for some time, and bridges may be purchased off the shelf containing programmable network processors. Proprietary solutions can be implemented on these. However, these network processors are vendor specific, and the solution will only work on that network processor or processor family. The solution will not be portable, and it will not be possible to run it on other vendors' equipment. Additionally, programming a network processor is done at a very low level, basically in assembly language, and the programming model is hard, requiring special skill. It should also be noted that a proprietary solution will make the equipment non-standard, and customers are more reluctant to buy non-standard equipment. There might also be inter-operational problems with other equipment.

SUMMARY OF THE INVENTION

The present invention is an adaptable network bridge having a Rule Engine that simplifies the adaptation of the bridge to dynamically changing conditions related, for example, to network conditions and user context. Simplicity is achieved by specifying how data frames should be processed and switched in terms of switching rules. Flexibility is achieved by enabling dynamic loading and updating of rules in the bridge via a protocol. In addition, one bridge may generate or modify rules for loading at another, neighboring, bridge. In a preferred embodiment, the bridge is an Ethernet bridge.

Thus, in one aspect, the invention is directed to an adaptable network bridge that includes a Rule Engine that processes data frames according to a set of switching rules. Each switching rule identifies a type of frame to which the rule applies, and how the type of frame is to be processed. The bridge also includes means for dynamically modifying the switching rules. In particular, the rules may be dynamically loaded and updated, for example, in response to changes in the bridge's state information, or changes in context information. In another embodiment, the bridge includes a plurality of input/output ports, and the Rule Engine includes a plurality of sets of switching rules, wherein each set of switching rules is applicable to a different port in the bridge.

In one aspect the rules are forced on the switch by external units such as a

Network Management System (NMS).

In a further aspect, a switch generates or modifies rules that are forced on other switches.

In yet another aspect, the invention is directed to a method of processing and switching Ethernet frames in an adaptable Ethernet bridge. The method includes the steps of defining a set of switching rules for the adaptable Ethernet bridge; receiving a given frame in the bridge; determining whether any of the rules are applicable to the given frame; and upon determining that one of the rules is applicable to the given frame, processing and switching the frame according to the applicable rule. The switching rules may be dynamically added, subtracted, or modified, for example, in response to changes in state or context information.

An important aspect of the invention is how the extended state vector can be utilized in new ways in the switching process. The switching process can be controlled and adapted in new ways allowing completely new ways to control networks.

BRIEF DESCRIPTION OF THE DRAWINGS

In the following, the essential features of the invention will be described in detail by showing preferred embodiments, with reference to the figures of the attached drawings.

FIG. 1 is a simplified block diagram of a Rule Engine utilized in the adaptable network bridge of the present invention;

FIG. 2 is a sequence diagram illustrating the steps of a process performed by the Rule Engine; and

FIG. 3 is an illustration of a network of adaptable Ethernet bridges controlled by a Network Management System (NMS).

DETAILED DESCRIPTION OF THE INVENTION

In the following description, for purposes of explanation and not limitation, specific details are set forth, such as particular embodiments, circuits, signal formats etc. in order to provide a thorough understanding of the present invention. It will be apparent to one skilled in the art that the present invention may be

practiced in other embodiments that depart from these specific details.

In existing Ethernet bridges, there are two identifiable phases in the switching process. In the first phase, parts of the frame header are checked for specific information. For example, the destination address of each frame may be checked against a forwarding table, priority bits, VLAN tags, and the like. In the second phase, different actions are taken within the bridge depending on the result of this check. For example, the frame may be sent to the port pointed to in the forwarding table, or the frame may be sent to all ports except the originating port, and so on. These steps characterize a process in which a frame is put through a filter that selects the action to take. Another important element is that the bridge stores and retrieves information in the form of a simple state vector in a forwarding table (i.e., memory), which the bridge is using in the process. However, the different parts of this process are fixed and may not be altered.

The present invention is based on a generalization of this switching process that adds several new key aspects to switching, enabling new ways of adapting and controlling the switching process as well as new ways to control Ethernet networks. The invention provides an adaptable Ethernet bridge having a Rule Engine that simplifies the addition or modification of functionality within the bridge. One of the purposes of the adaptable bridge is to provide a simple solution whereby anyone with reasonable skill can implement and add new functionality in a standardized way on standard equipment. Simplicity is achieved by specifying how Ethernet frames should be processed and switched in terms of switching rules. Flexibility is achieved by enabling dynamic loading and updating, inspection, and prioritization of rules in bridges via a protocol.

The generalized switching process consists of the Rule Engine processing Ethernet frames by applying the switching rules. A switching rule encapsulates a specific switching behavior that describes the filter and action processes together with the state vector. A switching rule thus consists of three parts:

1) A filter function that can filter any part or parts of a frame. The purpose of the filter is to decide if the rule is applicable to a given frame. In other words, the filter works as a predicate function on frames. In this decision process information in the state vector may be used.

2) An action function that describes how a frame header (or the entire frame) should be transformed and how the frame should be switched, i.e. to which port or ports the frame should be sent. In this process the action function may alter the state vector.

3) A state vector that the filter function and the action function can use in the switching process.

The switching rule can also contain other information such as version, priority specification, vendor information, and the like.

The state vector is an abstraction of several parts:

1) A local memory for a rule or a set of rules where rule-specific data can be stored and altered. Specific "management rules" make it possible to access that data from, for example, a management system.

2) A global bridge memory where bridge-specific data applicable to and accessible by all rules can be stored and altered. One example is the port-forwarding table.

3) Access to a set of bridge resources that can be implemented as library functions. Some examples are a function to retrieve the source port of the frame processed, a function that provides timestamps, counters and timers, and functions that describe the traffic flows and load in the bridge. The invention is not limited to these examples; other functions may be identified by those skilled in the art.

A switching rule describes the types of frames that match the rule and how these frames should be processed (e.g., switched or transformed before switching). Each incoming frame is checked against the set of rules stored in the bridge. If a rule matches, the frame is processed and switched according to the specification in the rule. If no rule matches the frame, a default rule may be utilized, or the frame may be dropped.

With the concept of rules, the switching process is defined as a simple and understandable programming model. Standardizing rule language and making it possible to dynamically load new rules in a bridge also makes it possible to add new functionality, adapting standard equipment to the needs at hand. If some functionality becomes obsolete, that functionality can be removed by removing the

rule or set of rules implementing it.

A powerful extension is to allow different rule sets to be valid for different ports enabling, for example, different network providers to share the same hardware but have different network behavior. Different embodiments of this extension include: a rules control mechanism that selects and prioritizes available rule sets based on port, time of day, load, and the like. Alternatively, this kind of information may be described in the filter functions, and the Rule Engine tries all rules until it finds a match.

Yet another powerful extension is to allow rules that monitor the state vector instead of being matched against Ethernet frames. That is, the filter function monitors the state vector, and when some condition is fulfilled, the action function is invoked. The monitoring process can be implemented by regularly processing these rules in the Rule Engine or in a separate Rule Engine.

Note that allowing the filter and action functions to have access to a state vector that goes beyond the forwarding table provides new and powerful ways to process and switch frames.

FIG. 1 is a simplified block diagram of an exemplary embodiment of the dynamically adaptable network bridge 10 of the present invention. The adaptable bridge includes many of the same components as existing bridges such as switch fabric 11, frame buffers 12a-12n and 13a-13n, and ports 14a-14n and 15a-15n. In addition, however, the adaptable bridge includes a Rule Engine 16, which replaces the implementation of some or all protocols. The adaptable bridge also includes a state vector memory 17 accessible by the Rule Engine, a rule control function 18, and a rules memory 19 accessible by the Rule Engine through the rule control function. Collectively, these new bridge components enable the adaptable bridge to receive and store rules from external units, store a state vector which may be dependent on external sources, and store rules that are imposed on other bridges.

Hybrid designs having both a Rule Engine and some of the protocols of existing bridges may also be implemented. The Rule Engine has processing capabilities, that is, the Rule Engine can (1) apply the filter function to a frame and calculate the result; (2) apply the action function if the rule matches; (3) access

the state vector; and (4) access the other resources of the switch. A frame entering the adaptable bridge through an input port such as port 14a and frame buffer 12a is acted upon by switching rules in the Rule Engine 16, including the filter function, action function, and state vector. The result is a calculated result frame, which is outputted through switch fabric 11, and an appropriate frame buffer and output port such as frame buffer 13a and output port 15a.

The rule control function 18 adds and removes rules dynamically, and orders or prioritizes THE set of rules. The rule control function may be implemented as protocols and secured against unwanted manipulation by using well known techniques intended for that purpose, for example, using digital signatures and encryption. Additionally, the rule control function may include a mechanism to transform (or translate) switching rules in human-readable form to an efficient form understandable by the Rule Engine 16.

The mechanisms to access different bridge resources and state information (i.e., state vectors), mechanisms to access library functions, and a protocol for externally accessing the state information are important parts of the adaptable bridge. The bridge resources and state information may be accessed via, for example, an Application Programming Interface (API). The protocol for externally accessing the state information may be implemented as a set of rules. The state of the bridge can affect switching rules dynamically, that is, a rule can behave differently depending on the current state. For example, frames can be switched differently depending on time of day, traffic pattern, traffic load, and the like. This behavior can also be controlled externally by, for example, a network management system (NMS).

FIG. 2 is a sequence diagram illustrating the steps of a method of processing an Ethernet frame by the Rule Engine 16. The process starts at step 21 and moves to step 22 where, for each incoming Ethernet frame, the port-specific rules associated with the Source Port are merged with the rules shared among all ports of the bridge (this merge can be done in advance by the priority module as a ordered list). The rules in the list are then tested to determine whether the frame matches the rule. This process begins at step 23, where a determination is made whether there are any more rules left to test. If not, and all

the rules have been tested, the frame is dropped at step 24. However, in the case of the first rule, there are rules left to test, so the method moves to step 25 where the filter function of the first rule in the list is applied to the frame. The filter function uses the information found in the frame together with the current state vector to determine whether the frame matches the rule. The filter function is a predicate, so the result at step 26 will be either true (the frame matches the rule) or false (the frame does not match the rule). If the result is false, the rule is discarded at step 27, and the method returns to step 23 where the test is performed on the next rule in the list.

The remainder of the rules are then tested until either no rules are left and the frame is dropped at step 24, or there is a match at step 26, and the method moves to step 28 where the action function of the rule is applied to the frame. The action function may use the library functions, the information in the frame, and the state vector to transform (or modify) the frame. In this process, the action function can use functions to modify the state vector. For example, a counter may be incremented, which counts the number of frames containing a specific high-level protocol coming from the port. At step 29, the action function determines the destination port or ports and sends the (possibly transformed) frame to the determined port or ports. The method then ends at step 30.

Another important aspect of the invention not shown in the sequence diagram is that other resources or modules in the bridge may continuously monitor and change the state vector in parallel. An extended Rule Engine, to the one described, may then invoke rules that, instead of being matched against Ethernet frames, monitor the state vector. When one or more predefined criteria are fulfilled (determined by the filter function), the action function generates new frames containing new rules to be sent to the bridge itself or to nearby bridges altering their behavior.

FIG. 3 is an illustration of a network 35 of adaptable Ethernet bridges controlled by a Network Management System (NMS) 36. The NMS monitors the state in the bridges and issues rules that adapt the behavior of certain bridges accordingly. For example, if $Bridge_{11}$ becomes heavily loaded with traffic, the NMS may issue a rule that will move some traffic from associated bridges (i.e.,

$Bridge_{21}$ – $Bridge_{23}$) to $Bridge_{12}$. For example, the rule may move every third frame or frames carrying a particular protocol to $Bridge_{12}$. Context information may also be added to the state vector, thereby allowing context to influence switching. Context information may contain, but is not limited to, information about traffic load in nearby bridges, forecasts or predictions of expected traffic, and the like. This feature is of particular interest in a mobile environment.

The NMS 36 is shown connected to the network by a dotted line because the adaptable bridges may automatically generate specific context rules and distribute them to nearby bridges as users move around in the network. When bridges automatically generate rules to other bridges (and to themselves), a self-managed network can be implemented in which bridges exchange rules dynamically. This capability can be used, for example, to setup a particular flow-path, distribute traffic during heavy load, or automatically redirect traffic in the case of network failures. For example, if Bridge11 receives a flow of high priority frames when it is already heavily loaded with traffic, it can issue a rule or set of rules to Bridge22 that move the flow to Bridge12 instead.

An Ethernet bridge is working in "wire-speed" and therefore it is desirable that the bridge introduce as little delay as possible. Adding a Rule Engine and basing the switching on rules may increase the delay. However, a number of techniques and mechanisms can be used to make the Rule Engine more efficient:

1) Filter functions can be tested in parallel, and a priority module can select the matching rule with highest priority. These computations can be performed because the filter functions are pure predicates, i.e. they contain no side effects.

2) Filter functions will in most cases be a conjunction (or disjunction) of comparisons. These can be directly mapped onto a pipelined matrix of comparison modules in hardware.

3) A similar pipelined hardware matrix realizing the language constructs used in the action functions can be implemented.

4) Some parts of the state vector, for example library functions reflecting bridge context and resources, can be implemented in hardware such as registers, thereby providing "instant" access to them.

In the preferred embodiment, the rule language used to describe the filter

and action functions is not a general purpose programming language. A programming language should only have the necessary constructs and mechanisms needed to express the solutions to the problems in the specified domain. If the language is too powerful, as a general-purpose language, it is possible to express an infinite loop (accidentally or on purpose) thereby increasing the delay to infinity. The preferred switching rule language, therefore, is a language primarily restricted to the domain of Ethernet switching (layer 2), with language constructs expressing the mechanisms used in the switching process. However, language constructs that are useful for other purposes like network management, constructs related to exchange of new rules, and so on, that are not in conflict with the basic requirements may also be included.

The present invention provides several advantages. The Ethernet standards can be implemented as switching rule sets, and as the standards evolve, the rule sets are updated. These updated rule sets can then easily be loaded into an adaptable network bridge. The rule sets can be vendor-independent and, for example, published by IEEE. Today, each vendor decides which protocols (standards) to support in a bridge, and unless the vendor issues an update whenever the standard is updated, users have to buy a new bridge if they need to follow the new standard.

In the present invention, the "programming language" of rules may be standardized thereby enabling anyone to add new functionality, as a switching rule, to any bridge with a Rule Engine. These rules can then be updated or removed if necessary. A proprietary solution can also be implemented as a rule or set of rules and loaded in any bridge with a Rule Engine. If a user later wants to use another solution, the rule set is simply replaced with a new rule set. It will be much less expensive to implement new functionality because, in most cases, the user only has to write some software in the form of a set of rules.

The present invention also greatly increases flexibility in networks because each bridge can be loaded with its own rule set down to the individual port level. The invention also provides the ability to adapt the functionality on each port based on time, user demands, service agreements, and the like. For example, different operators can share the same physical bridge (network) and provide

different services to their respective users.

Some examples of functionality that can be implemented with switching rules include the following:

1) Broadcast tunnels. It is simple to implement broadcast tunnels necessary for building Public Ethernet Networks.

2) Distributed router functionality added to a set of bridges.

3) Simple firewall functionality.

4) User adapted services on the port level.

5) Authentication and security mechanisms on the port level that are transparent to users.

6) Self-managed networks or semi-self managed networks.

This list is not intended to be exhaustive, and other functions may also be implemented with switching rules and loaded into any adaptable bridge with a Rule Engine.

As shown by the above examples, the state of the dynamically adaptable bridge can be utilized in the switching process to enable entirely new functionality and to provide new ways to use bridges in networks.

Although preferred embodiments of the present invention have been illustrated in the accompanying drawings and described in the foregoing Detailed Description, it is understood that the invention is not limited to the embodiments disclosed, but is capable of numerous rearrangements, modifications, and substitutions without departing from the scope of the invention. The specification contemplates any all modifications that fall within the scope of the invention defined by the following claims.

WHAT IS CLAIMED IS:

1. A dynamically adaptable network bridge comprising:

a Rule Engine that processes data frames according to a set of switching rules, wherein each switching rule identifies a type of frame to which the rule applies, and how the type of frame is to be processed; and

means for dynamically modifying the switching rules.

2. The dynamically adaptable network bridge of claim 1 wherein the means for dynamically modifying the switching rules includes a protocol for dynamically loading and updating the switching rules.

3. The dynamically adaptable network bridge of claim 1, wherein each switching rule includes a filter function for determining whether a given rule is applicable to a given frame.

4. The dynamically adaptable network bridge of claim 3, wherein each switching rule also includes an action function for specifying changes to the given frame's header and how the given frame should be switched.

5. The dynamically adaptable network bridge of claim 1, wherein each switching rule includes a state vector utilized for processing the type of frames to which each rule applies.

6. The dynamically adaptable network bridge of claim 5, wherein the state vector includes an abstraction of a local memory for storing rule-specific data for each switching rule.

7. The dynamically adaptable network bridge of claim 6, wherein specific management rules enable the Rule Engine to access the rule-specific data for each switching rule.

8. The dynamically adaptable network bridge of claim 6, wherein the state vector also includes an abstraction of a global bridge memory for storing bridge-specific data applicable to and accessible by all the switching rules.

9. The dynamically adaptable network bridge of claim 8, wherein the bridge-specific data includes a port-forwarding table.

10. The dynamically adaptable network bridge of claim 8, wherein the state vector also includes a set of library functions that implement bridge resources.

11. The dynamically adaptable network bridge of claim 10, wherein the set of library functions are selected from a group consisting of:

a function that retrieves a source port of a processed frame;

a function that provides timestamps;

a function that describes traffic flows in the bridge; and

a function that indicates the traffic load in the bridge.

12. The dynamically adaptable network bridge of claim 3, wherein the given frame is processed in accordance with the given rule if the filter function determines that the given rule is applicable to the given frame, and the given frame is dropped if the filter function determines that there is no rule applicable to the given frame.

13. The dynamically adaptable network bridge of claim 1, wherein the bridge includes a plurality of input/output ports, and the Rule Engine includes a plurality of sets of switching rules, wherein each set of switching rules is applicable to a different port in the bridge.

14. The dynamically adaptable network bridge of claim 1, wherein the bridge is an Ethernet bridge.

15. The dynamically adaptable network bridge of claim 1, wherein the means for dynamically modifying the switching rules includes a protocol that dynamically adds, subtracts, and modifies the switching rules.

16. The dynamically adaptable network bridge of claim 1, further comprising means for prioritizing rules within the set of switching rules.

17. The dynamically adaptable network bridge of claim 1, further comprising means for accessing state information for the bridge, wherein a given rule causes a given frame to be processed differently when the state information changes.

18. The dynamically adaptable network bridge of claim 17, wherein the given rule processes the given frame differently, depending on traffic load in the bridge.

19. The dynamically adaptable network bridge of claim 17, further comprising a port for receiving rules from a Network Management System (NMS), wherein the NMS monitors the state information for a plurality of adaptable bridges in a network, and issues rules that adapt the behavior of the bridge to optimize network performance.

20. The dynamically adaptable network bridge of claim 17, wherein the state information includes context information, wherein a given rule causes a given frame to be processed differently when the context information changes.

21. The dynamically adaptable network bridge of claim 1, wherein the bridge is one of a plurality of adaptable bridges in a network, and the bridge further comprises means for generating specific context rules and distributing the context rules to other adaptable bridges in the network.

22. A method of processing and switching data frames in an adaptable network bridge, said method comprising the steps of:

defining a set of switching rules for the adaptable bridge;

receiving a given frame in the bridge;

determining whether any of the rules are applicable to the given frame; and

upon determining that one of the rules is applicable to the given frame, processing and switching the frame according to the applicable rule.

23. The method of claim 22, further comprising dynamically adding, subtracting, and modifying the switching rules.

24. The method of claim 23, further comprising accessing state information for the bridge, wherein the step of dynamically adding, subtracting, and modifying the switching rules is performed in response to a change in the state information.

25. The method of claim 24, wherein the bridge is one of a plurality of adaptable bridges in a network, and the method further comprises the steps of:

receiving a new or modified switching rule from a Network Management System (NMS), wherein the NMS monitors the state information for a plurality of adaptable bridges in a network, and issues rules that adapt the behavior of the bridge to optimize network performance; and

processing and switching frames according to the new or modified switching rule received from the NMS.

26. The method of claim 24, further comprising adding context information to the state information, wherein the step of dynamically adding, subtracting, and modifying the switching rules is performed in response to a change in the context information.

27. The method of claim 22, wherein the bridge is one of a plurality of adaptable bridges in a network, and the method further comprises the steps of:

generating specific context rules; and

distributing the context rules to other adaptable bridges in the network.

28. The method of claim 22, wherein the bridge is an Ethernet bridge.

5

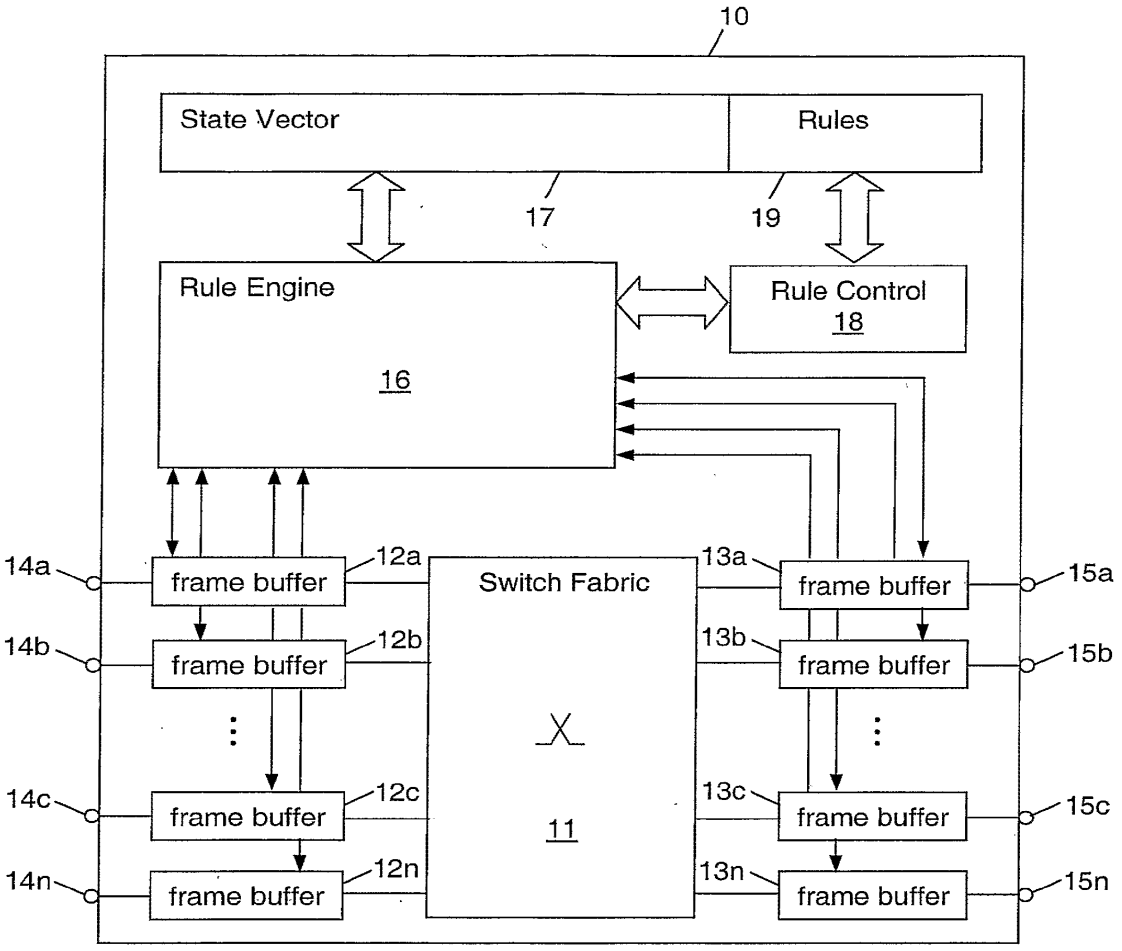


FIG. 1

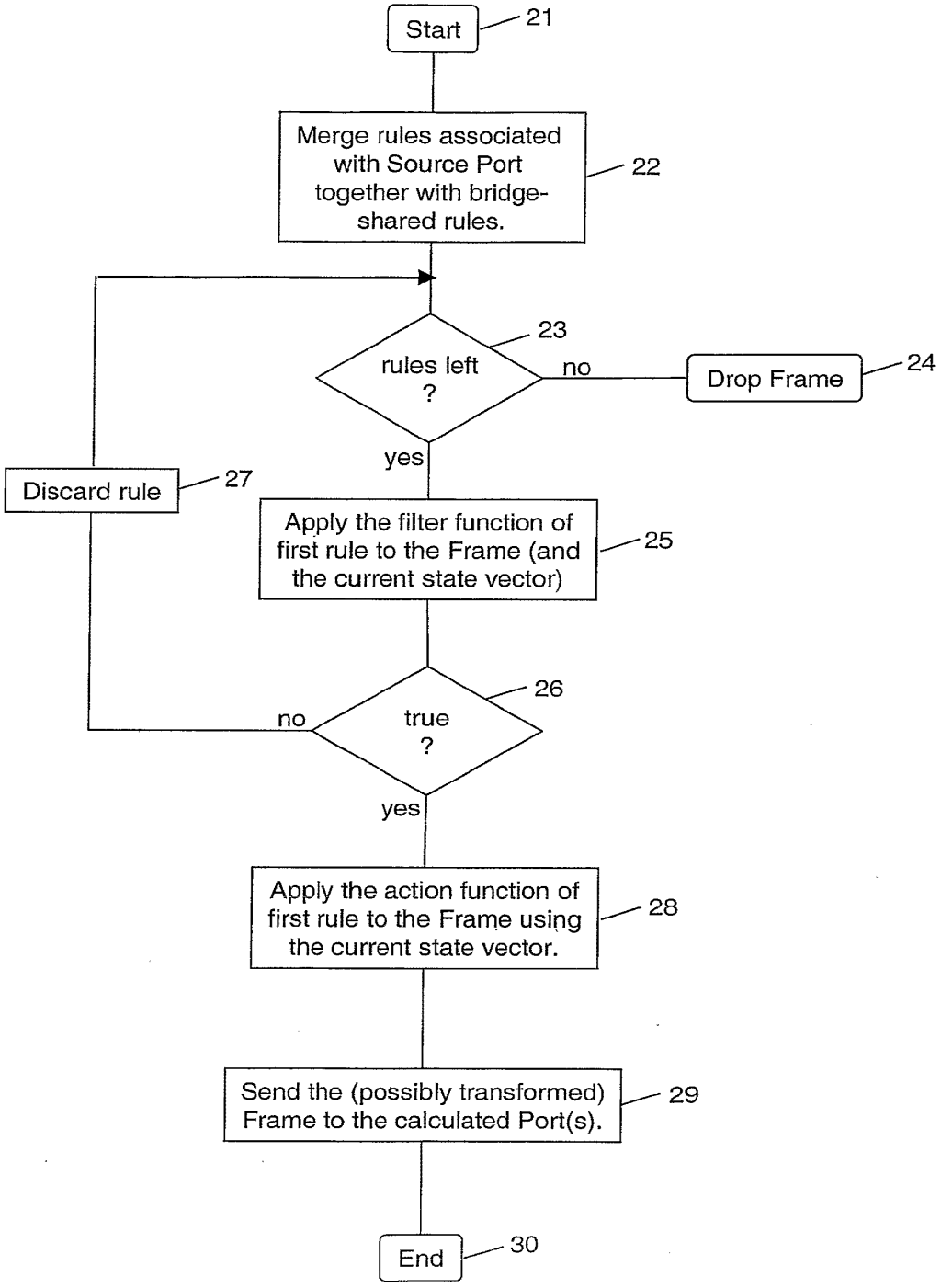


FIG. 2

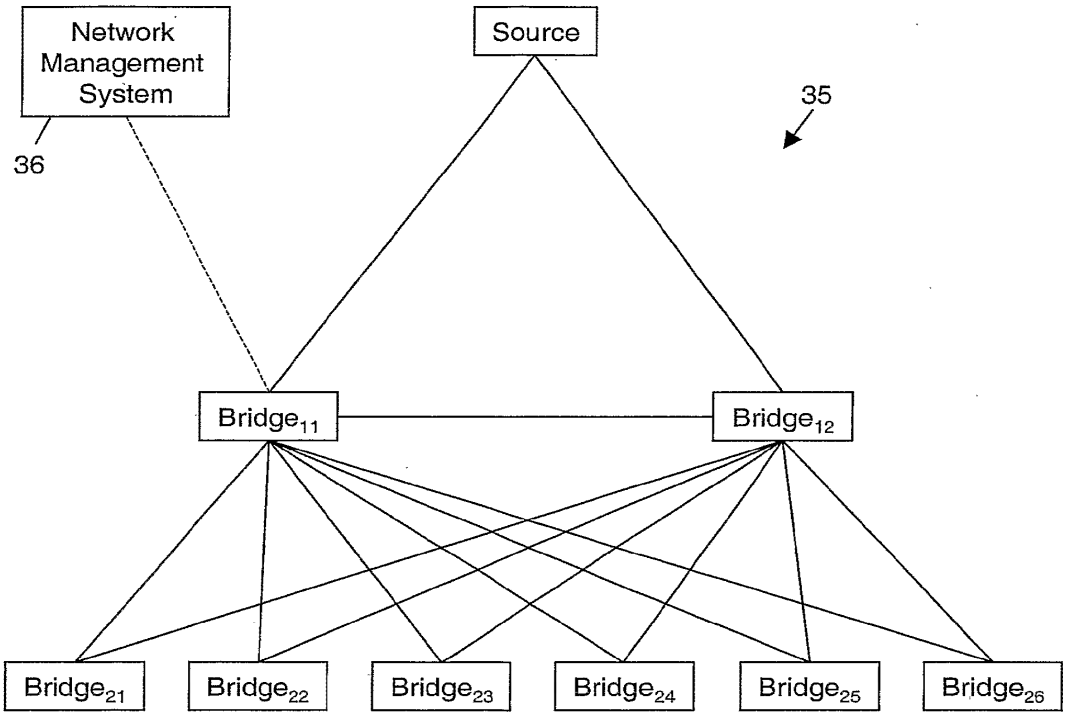


FIG. 3

INTERNATIONAL SEARCH REPORT

International Application No
[redacted]T/SE2004/001611

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L12/56 H04L12/46

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal, WPI Data, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5 790 554 A (PITCHER ET AL) 4 August 1998 (1998-08-04) abstract column 1, line 15 - column 1, line 67 column 2, line 39 - column 3, line 25 column 3, line 48 - column 4, line 42 column 4, line 60 - column 8, line 4 column 8, line 24 - column 8, line 26; claims 1,2,14,22,28; figures 2,3 ----- -/--	1-5, 12-20, 22-25, 27,28

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
21 March 2005	31/03/2005
Name and mailing address of the ISA European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Authorized officer Todorut, C

Form PCT/ISA/210 (second sheet) (January 2004)

INTERNATIONAL SEARCH REPORT

International Application No
T/SE2004/001611

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 5 396 493 A (SUGIYAMA ET AL) 7 March 1995 (1995-03-07) abstract column 1, line 63 - column 3, line 11 column 4, line 11 - column 4, line 51 column 5, line 67 - column 6, line 39; claims 1,17; figures 1-4	1-28
X	WO 00/56024 A (BROADCOM CORPORATION; KADAMBI, SHIRI; AMBE, SHEKHAR; KALKUNTE, MOHAN;) 21 September 2000 (2000-09-21) abstract	1-4,22, 23
A	page 53, line 12 - page 65, line 21; claims 1,2	5-21, 24-28
A	US 2003/123387 A1 (JACKSON ANDREW LLOYD 'GB!) 3 July 2003 (2003-07-03) abstract column 1, paragraph 2 - column 1, paragraph 9 column 2, paragraph 16 - column 3, paragraph 25; claims 1,6,9; figure 4	1-28
A	US 5 959 976 A (KUO ET AL) 28 September 1999 (1999-09-28) abstract column 1, line 5 - column 2, line 40 column 3, line 8 - column 3, line 18 column 5, line 56 - column 6, line 10; claim 1; figures 3-5	1-28
A	EP 0 508 886 A (DIGITAL EQUIPMENT CORPORATION) 14 October 1992 (1992-10-14) abstract column 1, line 40 - column 3, line 54 column 4, line 45 - column 5, line 16 column 5, line 55 - column 6, line 53; claims 1,23; figures 5-8	1-28
A	US 5 515 376 A (MURTHY ET AL) 7 May 1996 (1996-05-07) abstract column 6, line 1 - column 9, line 21	1-28

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
/SE2004/001611

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5790554 A	04-08-1998	NONE	
US 5396493 A	07-03-1995	JP 6224918 A	12-08-1994
		KR 9614983 B1	23-10-1996
WO 0056024 A	21-09-2000	US 2001043611 A1	22-11-2001
		AU 3529500 A	04-10-2000
		AU 3752000 A	04-10-2000
		AU 4325800 A	04-10-2000
		EP 1161817 A2	12-12-2001
		EP 1169809 A2	09-01-2002
		EP 1159805 A2	05-12-2001
		WO 0056024 A2	21-09-2000
		WO 0056011 A2	21-09-2000
		WO 0056013 A2	21-09-2000
		US 6707817 B1	16-03-2004
		US 6810037 B1	26-10-2004
		US 6850521 B1	01-02-2005
		US 6707818 B1	16-03-2004
		US 2004174898 A1	09-09-2004
		US 2005047411 A1	03-03-2005
		US 2002039365 A1	04-04-2002
		AU 5442700 A	12-12-2000
		AU 5586400 A	12-12-2000
		AU 5737300 A	31-01-2001
		AU 6334400 A	22-01-2001
		EP 1181791 A1	27-02-2002
		EP 1181792 A1	27-02-2002
		EP 1212867 A2	12-06-2002
		EP 1192767 A2	03-04-2002
		WO 0072533 A1	30-11-2000
		WO 0102965 A2	11-01-2001
		WO 0072531 A1	30-11-2000
		WO 0101724 A2	04-01-2001
		US 2002093974 A1	18-07-2002
		US 2002186705 A1	12-12-2002
		US 6813268 B1	02-11-2004
		US 6735679 B1	11-05-2004
		US 6792500 B1	14-09-2004
		US 6842457 B1	11-01-2005
		US 6430188 B1	06-08-2002
		US 6859454 B1	22-02-2005
		US 2004170176 A1	02-09-2004
		US 2005036488 A1	17-02-2005
		US 2002031090 A1	14-03-2002
US 2003123387 A1	03-07-2003	NONE	
US 5959976 A	28-09-1999	NONE	
EP 0508886 A	14-10-1992	DE 69217103 D1	13-03-1997
		DE 69217103 T2	21-08-1997
		EP 0508886 A1	14-10-1992
		JP 5114905 A	07-05-1993
		US 5515513 A	07-05-1996
US 5515376 A	07-05-1996	EP 0710415 A1	08-05-1996
		JP 3335358 B2	15-10-2002

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
/SE2004/001611

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5515376 A		JP 9500774 T	21-01-1997
		WO 9503659 A1	02-02-1995
		US 5610905 A	11-03-1997
		US 6545982 B1	08-04-2003

Form PCT/ISA/210 (patent family annex) (January 2004)

Electronic Acknowledgement Receipt

EFS ID:	19436677
Application Number:	13657010
International Application Number:	
Confirmation Number:	2390
Title of Invention:	METHODS AND SYSTEMS FOR PROTECTING A SECURED NETWORK
First Named Inventor/Applicant Name:	Steven Rogers
Customer Number:	22907
Filer:	William Eugene Wooten/Rocko Bund
Filer Authorized By:	William Eugene Wooten
Attorney Docket Number:	007742.00017
Receipt Date:	27-JUN-2014
Filing Date:	22-OCT-2012
Time Stamp:	14:39:01
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Non Patent Literature	NPL-ISR_16812867.PDF	1078548 bb0e661dcbcde2c2213fee0b75d5c81ce10349c9	no	9
Warnings:					
Information:					

2	Information Disclosure Statement (IDS) Form (SB08)	Information_Disclosure_Statement_Fillable_PDF_16811329.PDF	612199 1d0f13d993ad40f41f74abaff1de33f0dfebe84c	no	4
Warnings:					
Information:					
A U.S. Patent Number Citation or a U.S. Publication Number Citation is required in the Information Disclosure Statement (IDS) form for autoloading of data into USPTO systems. You may remove the form to add the required data in order to correct the Informational Message if you are citing U.S. References. If you chose not to include U.S. References, the image of the form will be processed and be made available within the Image File Wrapper (IFW) system. However, no data will be extracted from this form. Any additional data such as Foreign Patent Documents or Non Patent Literature will be manually reviewed and keyed into USPTO systems.					
3	Foreign Reference	EP1313290A1_16689905.PDF	1181323 0d673c0a51b64a7a9da6dec238ebe98d483c6031	no	18
Warnings:					
Information:					
4	Foreign Reference	WO2005046145_16811218.PDF	1189526 12556d88fc51d8167206348609ca3e7c4e53943b	no	27
Warnings:					
Information:					
		Total Files Size (in bytes):	4061596		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

<u>New Applications Under 35 U.S.C. 111</u>
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

<u>National Stage of an International Application under 35 U.S.C. 371</u>
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

<u>New International Application Filed with the USPTO as a Receiving Office</u>
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PATENT COOPERATION TREATY

From the INTERNATIONAL SEARCHING AUTHORITY

To:
Wright, Bradley C.
BANNER & WITCOFF, LTD.
1100 13th Street, N.W. Suite 1200
Washington, DC 20005-4051
ETATS-UNIS D'AMERIQUE

PCT

NOTIFICATION OF TRANSMITTAL OF THE INTERNATIONAL SEARCH REPORT AND THE WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY, OR THE DECLARATION

(PCT Rule 44.1)

Applicant's or agent's file reference 007742.00025	Date of mailing *(day/month/year)* 24 March 2014 (24-03-2014) **FOR FURTHER ACTION** See paragraphs 1 and 4 below
International application No. PCT/US2013/072566	International filing date *(day/month/year)* 2 December 2013 (02-12-2013)
Applicant CENTRIPETAL NETWORKS, INC.	

1. [X] The applicant is hereby notified that the international search report and the written opinion of the International Searching Authority have been established and are transmitted herewith.

   Filing of amendments and statement under Article 19:
   The applicant is entitled, if he so wishes, to amend the claims of the International Application (see Rule 46):

   When? The time limit for filing such amendments is normally two months from the date of transmittal of the International Search Report.

   Where? Directly to the International Bureau of WIPO, 34 chemin des Colombettes 1211 Geneva 20, Switzerland, Fascimile No.: (41-22) 338.82.70

   For more detailed instructions, see *PCT Applicant's Guide*, International Phase, paragraphs 9.004 - 9.011.

2. [ ] The applicant is hereby notified that no international search report will be established and that the declaration under Article 17(2)(a) to that effect and the written opinion of the International Searching Authority are transmitted herewith.

3. [ ] **With regard to any protest** against payment of (an) additional fee(s) under Rule 40.2, the applicant is notified that:

   [ ] the protest together with the decision thereon has been transmitted to the International Bureau together with any request to forward the texts of both the protest and the decision thereon to the designated Offices.

   [ ] no decision has been made yet on the protest; the applicant will be notified as soon as a decision is made.

4. **Reminders**

   The applicant may submit comments on an informal basis on the written opinion of the International Searching Authority to the International Bureau. The International Bureau will send a copy of such comments to all designated Offices unless an international preliminary examination report has been or is to be established. Following the expiration of 30 months from the priority date, these comments will also be made available to the public.

   Shortly after the expiration of **18 months** from the priority date, the international application will be published by the International Bureau. If the applicant wishes to avoid or postpone publication, a notice of withdrawal of the international application, or of the priority claim, must reach the International Bureau before completion of the technical preparations for international publication (Rules 90*bis*.1 and 90*bis*.3).

   Within **19 months** from the priority date, but only in respect of some designated Offices, a demand for international preliminary examination must be filed if the applicant wishes to postpone the entry into the national phase **until 30 months** from the priority date (in some Offices even later); otherwise, the applicant must, **within 20 months** from the priority date, perform the prescribed acts for entry into the national phase before those designated Offices.

   In respect of other designated Offices, the time limit of **30 months** (or later) will apply even if no demand is filed within 19 months.

   For details about the applicable time limits, Office by Office, see www.wipo.int/pct/en/texts/time_limits.html and the *PCT Applicant's Guide*, National Chapters.

Name and mailing address of the International Searching Authority European Patent Office, P.B. 5818 Patentlaan 2 NL-2280 HV Rijswijk Tel. (+31-70) 340-2040 Fax: (+31-70) 340-3016	Authorized officer ROTHENBÜCHER, Anita Tel: +31 (0)70 340-9872

RECEIVED
MAR 28 2014
BANNER & WITCOFF, LTD.

Form PCT/ISA/220 (July 2010)

PATENT COOPERATION TREATY

PCT

INTERNATIONAL SEARCH REPORT

(PCT Article 18 and Rules 43 and 44)

Applicant's or agent's file reference	FOR FURTHER ACTION	see Form PCT/ISA/220 as well as, where applicable, item 5 below.
007742.00025		
International application No.	International filing date *(day/month/year)*	(Earliest) Priority Date *(day/month/year)*
PCT/US2013/072566	2 December 2013 (02-12-2013)	11 January 2013 (11-01-2013)
Applicant		
CENTRIPETAL NETWORKS, INC.		

This international search report has been prepared by this International Searching Authority and is transmitted to the applicant according to Article 18. A copy is being transmitted to the International Bureau.

This international search report consists of a total of 4 sheets.

[X] It is also accompanied by a copy of each prior art document cited in this report.

1. **Basis of the report**
   a. With regard to the **language,** the international search was carried out on the basis of:
      [X] the international application in the language in which it was filed
      [ ] a translation of the international application into _____, which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1(b))
   b. [ ] This international search report has been established taking into account the **rectification of an obvious mistake** authorized by or notified to this Authority under Rule 91 (Rule 43.6*bis*(a)).
   c. [ ] With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, see Box No. I.

2. [ ] **Certain claims were found unsearchable** (See Box No. II)

3. [ ] **Unity of invention is lacking** (see Box No III)

4. With regard to the **title,**
   [X] the text is approved as submitted by the applicant
   [ ] the text has been established by this Authority to read as follows:

5. With regard to the **abstract,**
   [X] the text is approved as submitted by the applicant
   [ ] the text has been established, according to Rule 38.2, by this Authority as it appears in Box No. IV. The applicant may, within one month from the date of mailing of this international search report, submit comments to this Authority

6. With regard to the **drawings,**
   a. the figure of the **drawings** to be published with the abstract is Figure No. 2
      [ ] as suggested by the applicant
      [X] as selected by this Authority, because the applicant failed to suggest a figure
      [ ] as selected by this Authority, because this figure better characterizes the invention
   b. [ ] none of the figures is to be published with the abstract

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2013/072566

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L29/06
ADD.

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 1 313 290 A1 (STONESOFT CORP [FI]) 21 May 2003 (2003-05-21) abstract paragraph [0010] paragraph [0022] paragraph [0024] paragraph [0029] paragraph [0040] paragraph [0025] ----- -/--	1-24

[X] Further documents are listed in the continuation of Box C. [X] See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
14 March 2014	24/03/2014

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Oliveira, Joel

Form PCT/ISA/210 (second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2013/072566

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 2005/046145 A1 (ERICSSON TELEFON AB L M [SE]) 19 May 2005 (2005-05-19) abstract page 3, line 14 - line 28 page 4, line 10 - line 11 page 5, line 10 page 5, line 23 - line 32 page 7, line 2 - line 8 page 7, line 30 - page 8, line 8 page 11, line 20 - line 25	1-24
A	US 2011/055916 A1 (AHN DAVID K [US]) 3 March 2011 (2011-03-03) paragraph [0017] paragraph [0021] - paragraph [0022]	1-24

1

Form PCT/ISA/210 (continuation of second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/US2013/072566

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 1313290 A1	21-05-2003	AT 346446 T	15-12-2006
		DE 60216218 T2	08-03-2007
		EP 1313290 A1	21-05-2003
		US 2003097590 A1	22-05-2003
WO 2005046145 A1	19-05-2005	CN 1879361 A	13-12-2006
		EP 1683313 A1	26-07-2006
		JP 4323523 B2	02-09-2009
		JP 2007534219 A	22-11-2007
		US 2005111434 A1	26-05-2005
		WO 2005046145 A1	19-05-2005
US 2011055916 A1	03-03-2011	AU 2010297968 A1	22-03-2012
		EP 2471218 A2	04-07-2012
		US 2011055916 A1	03-03-2011
		US 2014007216 A1	02-01-2014
		WO 2011038420 A2	31-03-2011

PATENT COOPERATION TREATY

From the
INTERNATIONAL SEARCHING AUTHORITY

To:

see form PCT/ISA/220

PCT

WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY
(PCT Rule 43*bis*.1)

Date of mailing
(day/month/year) see form PCT/ISA/210 (second sheet)

Applicant's or agent's file reference
see form PCT/ISA/220

FOR FURTHER ACTION
See paragraph 2 below

International application No.	International filing date *(day/month/year)*	Priority date *(day/month/year)*
PCT/US2013/072566	02.12.2013	11.01.2013

International Patent Classification (IPC) or both national classification and IPC
INV. H04L29/06

Applicant
CENTRIPETAL NETWORKS, INC.

1. This opinion contains indications relating to the following items:

- ☒ Box No. I Basis of the opinion
- ☐ Box No. II Priority
- ☐ Box No. III Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- ☐ Box No. IV Lack of unity of invention
- ☒ Box No. V Reasoned statement under Rule 43*bis*.1(a)(i) with regard to novelty, inventive step and industrial applicability; citations and explanations supporting such statement
- ☐ Box No. VI Certain documents cited
- ☐ Box No. VII Certain defects in the international application
- ☐ Box No. VIII Certain observations on the international application

2. **FURTHER ACTION**

If a demand for international preliminary examination is made, this opinion will usually be considered to be a written opinion of the International Preliminary Examining Authority ("IPEA") except that this does not apply where the applicant chooses an Authority other than this one to be the IPEA and the chosen IPEA has notifed the International Bureau under Rule 66.1*bis*(b) that written opinions of this International Searching Authority will not be so considered.

If this opinion is, as provided above, considered to be a written opinion of the IPEA, the applicant is invited to submit to the IPEA a written reply together, where appropriate, with amendments, before the expiration of 3 months from the date of mailing of Form PCT/ISA/220 or before the expiration of 22 months from the priority date, whichever expires later.

For further options, see Form PCT/ISA/220.

Name and mailing address of the ISA:	Date of completion of this opinion	Authorized Officer: BANNER & WITCOFF, LTD.
European Patent Office P.B. 5818 Patentlaan 2 NL-2280 HV Rijswijk - Pays Bas Tel. +31 70 340 - 2040 Fax: +31 70 340 - 3016	see form PCT/ISA/210	Oliveira, Joel Telephone No. +31 70 340-3334

Form PCT/ISA/237 (Cover Sheet) (July 2009)

Box No. I Basis of the opinion

1. With regard to the **language**, this opinion has been established on the basis of:

   ☒ the international application in the language in which it was filed

   ☐ a translation of the international application into , which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1 (b)).

2. ☐ This opinion has been established taking into account the **rectification of an obvious mistake** authorized by or notified to this Authority under Rule 91 (Rule 43bis.1(a))

3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, this opinion has been established on the basis of a sequence listing filed or furnished:

   a. (means)

      ☐ on paper

      ☐ in electronic form

   b. (time)

      ☐ in the international application as filed

      ☐ together with the international application in electronic form

      ☐ subsequently to this Authority for the purposes of search

4. ☐ In addition, in the case that more than one version or copy of a sequence listing has been filed or furnished, the required statements that the information in the subsequent or additional copies is identical to that in the application as filed or does not go beyond the application as filed, as appropriate, were furnished.

5. Additional comments:

Box No. V Reasoned statement under Rule 43*bis*.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Yes:	Claims	2, 3, 6-9, 11, 13, 14, 17-22, 24
	No:	Claims	1, 4, 5, 10, 12, 15, 16, 23
Inventive step (IS)	Yes:	Claims	
	No:	Claims	1-24
Industrial applicability (IA)	Yes:	Claims	1-24
	No:	Claims	

2. Citations and explanations

see separate sheet

Re Item V

Reasoned statement with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

Reference is made to the following documents:

D1 EP 1 313 290 A1 (STONESOFT CORP [FI]) 21 May 2003 (2003-05-21)

D2 WO 2005/046145 A1 (ERICSSON TELEFON AB L M [SE]) 19 May 2005 (2005-05-19)

D3 US 2011/055916 A1 (AHN DAVID K [US]) 3 March 2011 (2011-03-03)

1 The present application does not meet the criteria of Article 33(2) PCT, because the subject-matter of claims **1, 12 and 23** is not new.

1.1 **D1** discloses a method comprising, at a network protection device **(abstract)**:

receiving a first rule set **(paragraph [0010], column3 lines 4-7)**;

receiving a second rule set **(paragraph [0010], column3 lines 4-7)**;

preprocessing the first rule set and the second rule set **(considered to be implicit from paragraphs [0010], [0013], [0040]: when a new set of rules is made available it must be made certain that they do not contain errors which could stop the filtering of the firewall)**;

configuring the network protection device to process packets in accordance with the first rule set **(paragraph [0010], column3 lines 13-18)**;

receiving packets **(column 6 lines 23-26)**;

processing a first portion of the packets in accordance with the first rule set **(paragraphs [0010], [0020])**;

reconfiguring the network protection device to process packets in accordance with the second rule set **(paragraphs [0010], [0024])**; and

processing a second portion of the packets in accordance with the second rule set **(paragraphs [0010], [0024])**.

1.2 The same reasoning applies, mutatis mutandis, to the subject-matter of the corresponding independent apparatus and computer-readable media claims **12 and 23**, which therefore are also considered not new.

1.3 Dependent claims **2-11, 13-22 and 24** do not contain any features which, in combination with the features of any claim to which they refer, meet the requirements of the PCT in respect of novelty (for claims **4, 5, 10, 15, 16**) and/or inventive step (for claims **2, 3, 6, 7, 8, 9, 11, 13, 14, 17, 18, 19, 20, 21, 22, 24**) see passages cited in the Search Report.

Doc code: IDS
Doc description: Information Disclosure Statement (IDS) Filed

PTO/SB/08a (01-10)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**		
	Application Number	13657010
	Filing Date	2012-10-22
	First Named Inventor	Steven Rogers
	Art Unit	2438
	Examiner Name	K. W. Chang
	Attorney Docket Number	007742.00017

U.S.PATENTS						Remove
Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					
If you wish to add additional U.S. Patent citation information please click the Add button.						Add

U.S.PATENT APPLICATION PUBLICATIONS						Remove
Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20060048142		2006-03-02	Roese et al.	
	2	20100011434		2010-01-14	Kay	
If you wish to add additional U.S. Published Application citation information please click the Add button.						Add

FOREIGN PATENT DOCUMENTS								Remove
Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1	2385676	EP	A1	2011-11-09	Alcatel Lucent		☐
	2	2498442	EP	A1	2012-09-12	Openet Telecom Ltd		☐

EFS Web 2.1.17

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13657010
	Filing Date	2012-10-22
	First Named Inventor	Steven Rogers
	Art Unit	2438
	Examiner Name	K. W. Chang
	Attorney Docket Number	007742.00017

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1	ISR off International Application No. PCT/US2014/027723, dated June 26, 2014.	☐
	2	""SBIR Case Study: Centripetal Networks Subtitle: How CNI Leveraged DHS S&T SBIR Funding to Launch a Successful Cyber Security Company, Cyber Security Division, 2012 Principal Investigators' Meeting"; Sean Moore, October 10, 2012.	☐
	3	"Control Plane Policing Implementation Best Practices"; Cisco Systems; March 13, 2013; <https://web.archive.org/web/20130313135143/http:www.cisco.com/web/about/security/intelligence/coppwp_gs.html>	☐

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**		
	Application Number	13657010
	Filing Date	2012-10-22
	First Named Inventor	Steven Rogers
	Art Unit	2438
	Examiner Name	K. W. Chang
	Attorney Docket Number	007742.00017

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☐ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

☐ See attached certification statement.

☐ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/William E. Wooten/	Date (YYYY-MM-DD)	2014-07-03
Name/Print	William E. Wooten	Registration Number	60049

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Espacenet

Bibliographic data: EP2385676 (A1) — 2011-11-09

Method for adapting security policies of an information system infrastructure

Inventor(s): CUPPENS FREDERIC [FR]; CUPPENS NORA [FR]; DUBUS SAMUEL [FR]; KANOUN WAEL [FR] ± (CUPPENS, FREDERIC, ; CUPPENS, NORA, ; DUBUS, SAMUEL, ; KANOUN, WAEL)

Applicant(s): ALCATEL LUCENT [FR]; INST TELECOM TELECOM BRETAGNE [FR] ± (ALCATEL LUCENT, ; INSTITUT TELECOM - TELECOM BRETAGNE)

Classification: **- international:** ***G06F21/57; H04L29/06***
- cooperative: **G06F21/577**; **H04L63/1408**; **H04L63/1433**; **H04L63/20**; H04L63/1441

Application number: EP20100290250 20100507

Priority number (s): EP20100290250 20100507

Also published as: US2013111548 (A1) KR20130005301 (A) JP2013525927 (A) WO2011138417 (A1) CN102934122 (A)

Abstract of EP2385676 (A1)

The present invention refers to a method for adapting security policies of an information system infrastructure in function of attacks wherein it comprises the steps of: - storing potential attacks and their associated risks in a data repository (125); - storing curative security policies (128) in response of the potential attacks in a data repository; - monitoring (101) entering contents representing data streams of the information system; - detecting (129) at least one attack in the information system; - assessing a success probability parameter (132) of the at least one detected attack and its associated cost impact parameter (133); -

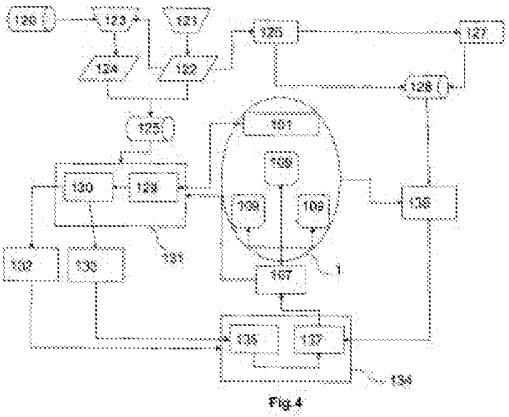


Fig 4

assessing an activation impact parameter (136) of at least one curative security policy in response to the at least one detected attack and its associated cost impact parameter; - deciding of the activation or deactivation (134) of a curative security policy in function of the success probability parameter of the, at least one, detected attack, of the activation impact parameter of at least one curative security policy and of the cost impact parameters of both the detected at least one attack and the at least one curative security policy.

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 2 385 676 A1

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
09.11.2011 Bulletin 2011/45

(51) Int Cl.:
H04L 29/06 *(2006.01)* ***G06F 21/00*** *(2006.01)*

(21) Application number: **10290250.9**

(22) Date of filing: **07.05.2010**

(84) Designated Contracting States:
AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO SE SI SK SM TR
Designated Extension States:
BA ME RS

(71) Applicants:
- **Alcatel Lucent**
  75008 Paris (FR)
- **Institut Télécom - Télécom Bretagne**
  29238 BREST cedex 3 (FR)

(72) Inventors:
- **Cuppens, Frédéric**
  29238 Brest Cedex 3 (FR)
- **Cuppens, Nora**
  29238 Brest Cedex 3 (FR)
- **Dubus, Samuel**
  91620 Nozay (FR)
- **Kanoun, Wael**
  91620 Nozay (FR)

(74) Representative: **Croonenbroek, Thomas Jakob et al**
Cabinet Innovincia
11, avenue des Tilleuls
74200 Thonon-les-Bains (FR)

(54) Method for adapting security policies of an information system infrastructure

(57) The present invention refers to a method for adapting security policies of an information system infrastructure in function of attacks wherein it comprises the steps of:
- storing potential attacks and their associated risks in a data repository (125);
- storing curative security policies (128) in response of the potential attacks in a data repository;
- monitoring (101) entering contents representing data streams of the information system;
- detecting (129) at least one attack in the information system;
- assessing a success probability parameter (132) of the at least one detected attack and its associated cost impact parameter (133);
- assessing an activation impact parameter (136) of at least one curative security policy in response to the at least one detected attack and its associated cost impact parameter;
- deciding of the activation or deactivation (134) of a curative security policy in function of the success probability parameter of the, at least one, detected attack, of the activation impact parameter of at least one curative security policy and of the cost impact parameters of both the detected at least one attack and the at least one curative security policy.

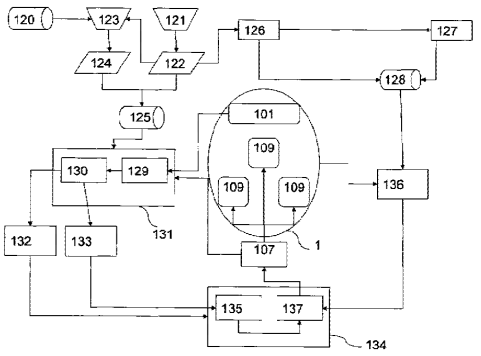


Fig.4

EP 2 385 676 A1

Description

[0001] The present invention relates to the field of information system protection and more precisely to the management of security policy in function of attacks undergone or being undergone by the information system.

[0002] Infrastructures of information systems need to be protected from harmful attacks leading to malicious events such as intrusions, data thefts, viruses or worms...

[0003] Due to the potential number of alerts generated by the existing attack detection systems with large information system infrastructures, it becomes impossible for operators to assess in real-time the risk of an attack and to decide of the suitable response to apply in response to the attack. Thus, automatic deployment of formally defined operational security policies starts to be considered in the protection of telecommunication and information infrastructures.

[0004] Fig.1 represents an example of such automatic protection of the state of the art.

[0005] The first step 101 corresponds to the detection of attacks toward the monitored information system which leads to the creation of elementary alerts (102). An alert correlation is then processed (103) to define correlated alerts (104) that are sent to a policy instantiation engine (105) to activate the appropriate security rules (106). These rules are sent to a policy decision point (107) which generates the configuration scripts (108) which are then used to configure policy enforcement points (109). Said policy enforcement points (109) are located in the information system 1 and apply the security rules in response to the detected attacks.

[0006] Such configuration of automatic policy activation suffers from drawbacks. Indeed, it is based only on correlated alerts and the number of correlated alerts may reach a very large number (up to thousands within a single day with large system) which would lead to thousands of security policy activations. Moreover, the deactivation of said security policies is not taken into account in the configurations of the state of the art such that a security policy may remain activated even if its impact on the users of the information system 1 is worth than the impact of the attack.

SUMMARY OF THE INVENTION

[0007] One object of the present invention is therefore to overcome the precited drawbacks of the state of the art and offer a method that allow to dynamically trig security policy activations only when it is necessary by taking into account a plurality of parameters influencing the activation decision and by defining a method that allow the deactivation of a security policy when it is necessary.

[0008] This is achieved by a method for adapting security policies of an information system infrastructure in function of attacks wherein it comprises the steps of:

- storing potential attacks and their associated risks in a data repository;
- storing curative security policies in response of the potential attacks in a data repository;
- monitoring entering contents representing data streams of the information system;
- detecting at least one attack in the information system;
- assessing a success probability parameter of the at least one detected attack and its associated cost impact parameter;
- assessing an activation impact parameter of at least one curative security policy in response to the at least one detected attack and its associated cost impact parameter;
- deciding of the activation or deactivation of a curative security policy in function of the success probability parameter of the, at least one, detected attack, of the activation impact parameter of at least one curative security policy and of the cost impact parameters of both the detected at least one attack and the at least one curative security policy.

[0009] According to another aspect of the invention, the step of storing potential attacks and their associated risks in a data repository comprises the steps of:

- defining the information system topology and attack detection signatures;
- defining a risk analysis of the information system that identifies potential attack objectives;
- specifying attack models to reach the identified attack objectives;
- storing said attack models in a data repository.

[0010] According to a further aspect of the invention, the step of storing curative security policies in response of the potential attacks in a data repository comprises:

- specifying at least one attack context;
- specifying curative security policies corresponding to the specified at least one attack context;
- storing said curative security policies in a data repository.

[0011] According to an additional aspect of the present invention, the step of assessing a success probability parameter of the at least one detected attack and its associated cost impact parameter comprises:

- generating attack strategy graphs based on the stored attack models and the detected at least one attack;
- assessing the probability for the attack to reach its objective;
- assessing the impact of the attack objective on the system security level and on the system quality of service (QoS) level;
- assessing the associated cost impact parameter of

the attack objective;

[0012] According to another aspect of the present invention, the step of assessing an activation impact parameter of at least one curative security policy in response to the at least one detected attack and its associated cost impact parameter is based on the stored curative security policies and the state of the monitored information system.

[0013] According to a further aspect of the invention, the step of deciding of the activation or deactivation of a curative security policy in function of the success probability parameter of the, at least one, detected attack, of the activation impact parameter of at least one curative security policy and of the cost impact parameters of both the detected at least one attack and the at least one curative security policy is applied dynamically based on the evolution of the state of the monitored system.

[0014] According to an additional aspect of the invention, the cost impact parameters comprise:

- a quality of service (QoS) impact and,
- a security level degradation impact.

[0015] The present invention also refers to a monitoring and protecting equipment comprising:

- at least one data repository for:
  - storing potential attacks and their associated risks;
  - storing curative security policies in response of the potential attacks;
- processing means for:
  - monitoring entering contents representing data streams of the information system;
  - detecting at least one attack in the information system;
  - assessing a success probability parameter of the detected at least one attack and its associated cost impact parameter;
  - assessing at least one activation impact parameter of at least one curative security policy in response to the at least one detected attack and its associated cost impact parameter;
  - deciding of the activation of a curative security policy in function of the success probability parameter of the at least one detected attack, of the activation impact parameter of at least one curative security policy and of the cost impact parameters of both the at least oneattack and the at least one curative policy,
  - activating at least one curative security policy.

[0016] The present invention also refers to a monitoring and protecting equipment comprising:

- at least one data repository for:
  - storing potential attacks and their associated risks;
  - storing curative security policies in response of the potential attacks;
- processing means for:
  - monitoring entering contents representing data streams of the information system;
  - detecting at least one attack in the information system;
  - assessing a success probability parameter of the detected at least one attack and its associated cost impact parameter;
  - assessing at least one activation impact parameter of at least one curative security policy in response to the at least one detected attack and its associated cost impact parameter;
  - deciding of the deactivation of a curative security policy in function of the success probability parameter of the at least one detected attack, of the activation impact parameter of at least one curative security policy and of the cost impact parameters of both the at least one attack and the at least one curative policy,
  - deactivating at least one curative security policy.

BRIEF DESCRIPTION OF THE DRAWINGS

[0017]

FIG.**1** is a synoptic diagram of the different steps of a protective method for launching security policies against attacks of an information system according to the state of the art;

FIG.**2** is a synoptic diagram of the different steps of a protective method for adapting security policies of an information system infrastructure against attacks according to the present invention;

FIG.**3** is a diagram of an example of attack graph comprising the different attack steps and the objectives associated with these attacks;

FIG.4 is a synoptic diagram of the different steps of a detailed protective method for adapting security policies of an information system infrastructure against attacks according to the present invention;

DETAILED DESCRIPTION OF THE INVENTION

[0018] As used herein, the term "attack" refers to an event in a system that transgress the normal authorized usage of the system or exploits deliberately or accidentally a vulnerability in the system as for example a network scanning, a password cracking, a sending of malicious email (also called spam), a sending of a malformed internet protocol (IP) packet... Moreover, the expression

attack with respect to an information system refers to attacks initiated from outside or inside of the information system (usually from an attacker machine) and directed toward said information system in order to produce dysfunctionings in said system.

[0019] As used herein, the term "SIP" refers to the acronym session Internet protocol.

[0020] As used herein, the term "IP" refers to the acronym Internet protocol.

[0021] As used herein, the term "QoS" refers to the acronym quality of service.

[0022] The embodiments of the present invention refer to a method for activating and deactivating security policies in order to protect an information system against malicious attacks wherein not only impacts of the attacks but also the success likelihood for the attack to reach its objective and impacts of security policies are taken into account in the activation/deactivation decision in order to minimize the impact, and in particular the cost, of attacks on the users of the information system.

[0023] Fig.2 represents the general steps of the method for adapting the protection of the information system 1.

[0024] Step 110 refers to the specification and the storing in a data repository of potential attacks and their associated risks. This first step allows to provide attack models that define the strategy and the objectives of the possible attacks.

[0025] Step 111 refers to specification and storing in a data repository of the foreseen security policies to apply in response to the possible attacks defined in the previous step.

[0026] Step 112 refers to the monitoring of entering content of the information system 1 corresponding to data streams and the attacks detection.

[0027] Step 113 refers to the assessment of a success probability of detected attacks and the cost impact associated with these attacks. Such assessment is achieved based on the attack models stored in step 110 and the attacks detected in step 112.

[0028] Step 114 refers to the assessment of the impact of an activation of a curative security policy in response to a detected attack and the cost impact associated with this activation. Such assessment is achieved based on the security policies stored in step 111 and the state of the monitored information system 1.

[0029] Step 115 refers to the decision of activating or deactivating a curative security policy in function of the assessments achieved in steps 113 and 114. Such decision corresponds to the comparison of the cumulative impacts of both the attack and the curative security policy on the information system 1.

[0030] The activation or deactivation decided in step 115 is then applied in step 116.

[0031] Moreover, it has to be noted that the steps 110 and 111 are preliminary steps which can be achieved offline whereas the steps 112, 113, 114, 115, 116 are dynamic steps which are achieved online such that any modification of the information system is taken into account in real time to decide of the activation or the deactivation of security policies.

[0032] Thus, the present invention, thanks to the assessments of both the attack consequences and the consequences of the activation of a security policy allows to determine if it is worthy to activate a curative security policy and when said policy is activated to determine if it is worthy to keep this policy activated in function of the evolution of the information system and the impact of this policy on said information system.

[0033] As described above, an attack is an event occurring in a system. In practice, an attack comprises different levels (or steps) that lead to the objective of the attack as described in fig.3 where an example of attack graph aimed at hacking a voice over internet protocol (VoIP) system is described.

[0034] The first level 201 corresponds to the sending of an email (malicious email or spam) toward a victim machine. Then the below (or next) levels represent the different steps to reach the objectives (213, 214, 215 and 216). The second level 202 refers to the gain of a remote shell in the victim machine (corresponding to the opening by the user of the malicious link or attachment of the email). The third level 203 corresponds to a bot (robot) infection which is the installation of a malicious software bot capable of simulating human activity that uses the remote shell. The bot can wait for future orders from the attacker to execute. As represented in fig.3, several remote shells and several corresponding bot infections may be develop in parallel in the information system.

[0035] The next level 204 corresponds to the discovery of the session initial protocol (SIP) discovery which is a scanning of the system (or network) to discover machines (computers in general) or servers using SIP protocol. Such attack may be done by a bot.

[0036] From this step, the attack may use two different ways depending on its objective.

[0037] The first way leads to step 205 which refers to the SIP fingerprinting which consists of identifying the type and the version of the software (operating systems, softphones, servers, etc...) installed on the SIP entities discovered at the previous level (204). This level may also be performed by a bot.

[0038] From step 205, the attack may have two different ways again, one leading to the objective of spam over IP (SPIT) 213 and comprising two levels, a discovery of the active users which is a scanning to determine the users of the VoIP system and which may be performed by a bot and a direct call 209 referring to a call to the victim user (by a bot) to perform spam over IP (SPIT).

[0039] The other possibility from level 205 is the discovery of the media access control (MAC) address of potential victim machines 207 (which may be performed by a bot).

[0040] The next step 208 is then the address resolution protocol (ARP) poisoning which forces the traffic (e.g. the established calls) between two victim users to pass through one bot. The attacker may then have access to

all the traffic between both victim users. This leads either to a step of sniff audio 211 to sniff the audio packets transmitted between both users or a step of inject audio 212 to inject audio packets in the transmission between both users for altering the established call. The corresponding respective objectives being the conversation tapping 214 and the conversation injection 215.

[0041] From level 204 the second attack solution consists in a server flooding 210 wherein the bots flood the main server of the VoIP system to cause a denial of service (DoS) which is the objective 216.

[0042] It has to be noted that the closer to the objective is the attack, the higher the probability to reach the objective. Thus, when a spam (level 201) is detected, it is generally not worth activating a security policy as the probability for the attack to reach one of the objectives (213, 214, 215 or 216) is still low whereas if the server is flooded (level 210) for example, then the probability of reaching the objective 216 is very high.

[0043] The graphs such as presented in fig.3 are achieved automatically based on attack models stored in data repository and are used in the assessment of the impact of an attack and its probability to reach its objective as described previously.

[0044] In order to better understand the different steps of the invention, a detailed configuration of a possible embodiment of the invention will now be described based on fig.4, it refers to a more detailed presentation of the organization presented in fig.2.

[0045] Step 120 corresponds to the storing in a data repository of the information system topology and the attack or intrusion detection signatures (IDS). Step 121 is a risk analysis for the monitored system which is conducted by an expert to identify potential attack objectives 122. Based on these attack objectives and the system topology (stored in step 120), attack models are specified (by an expert) 123 as well as an attack context specification 126. Attack models such as presented in fig.4 are then set up 124 and stored as elementary models in a data repository 125.

[0046] On the other hand, the specification of attack contexts 126 allows to specify response contexts 127. For each identified attack context an appropriate response context is specified with the associated security rules. Said security rules and attack contexts are stored as security policies in a data repository 128. Said security policies refer, for example, to firewall activation, authentication request activation or user account blocking or any actions allowing to cure the information system or reduce the impact of the attack. Based on the stored attack models and security policies to apply in response to each attack, the automatic and dynamic part of the invention may be implemented.

[0047] The information system 1 is monitored by intrusion detection systems (IDS) 101 which correspond to any types of sensors capable of detecting an attack and of generating and sending alerts. Said sensors may be made of specific electronic devices (micro-controllers, application specific integrated systems (ASICs)...) or in an information technology (IT) environment, it may simply be a software run by a computer, a server or a router.

[0048] The alerts sent by the IDS are then aggregated 129 in an online correlation engine 131 which uses these aggregated alerts and the attack models stored in a data repository to generate attack graphs such as presented in fig.3. The generated graphs are used, on one hand, for the assessment of the probability for the attack to reach its objective 132 and, on the other hand, for the assessment of the impact of the attack 133.

[0049] The determination of the probability to reach the objective corresponds to the success likelihood for an attack to reach an objective. Thus, the success likelihood level of each attainable objective (predefined in the attack graph) of the attack is calculated. This level shows how close the attack is with respect to its objective.

[0050] The attack impact assessment corresponds to the determination of the impact of the attack on the security and the quality of service (QoS) of the information system 1. This gathers the impact on the confidentiality, the integrity and the availability and any parameters influencing the using of the information system 1. Such assessment is also based on the state of the information system 1.

[0051] The results of both assessments are then sent to a policy instantiation engine (PIE) 134 where the cumulative impact of the attacks is determined.

[0052] Besides, in the same way as the assessment of the impact of the attacks, an assessment of the impact of the curative security policies which can be used in response of the attacks 136 is done based on the stored security policies. Again, impact on both the security and the QoS of the information system as well as as the state of said system are taken into account in the assessment. The results of the assessment are also transmitted to the PIE 134 where the cumulative impact of the curative security policies is determined.

[0053] The policy instantiation engine 134 receives the assessments corresponding on one side of the attack impact and on the other side of the curative security policy impact which are processed respectively by an attack handler module 135 and a response handler module 137. For each type of impact, at least one metric is defined, and in the general case, a plurality of metrics corresponding to different aspects of the impact (on security, on QoS...) are defined and the assessed value of all these impact contributions are added (practically by integrated their value over time).

[0054] Based on both cumulative impacts computed by the attack handler module and the response handler module as well as the probability for the attack to reach its objective (also called success likelihood) and the state of the monitored information system 1, the PIE 134 determines if curative security policies have to be activated or deactivated.

[0055] Different activation/deactivation rules may be used, for example, a security policy may be activated if

the success likelihood reached a given threshold, or if the attack impact reach a predetermined threshold. It can also be a combination of both (activation if the attack impact and the success likelihood reach given thresholds).

[0056] In general, a response policy must be activated when:

- the detected threat violated the security and operational policies and,
- the success likelihood (calculated dynamically, considering the attack progress and the state of the monitored system) of the threat exceeds a predefined threshold and,
- the impact of the threat exceeds a predefined threshold, and is greater than the cost of the associated response policy.

[0057] In the same way, if the success likelihood goes below a given threshold or the response impact goes over a predefined threshold or a combination of both, an activated security policy have to be deactivated. Such case may occur if the impact of a response policy induced more drawbacks than advantages with respect to the initial attack or if the risks associated with the attack have been dismissed or eradicated.

[0058] The order or command of activating or deactivating a security policy is then sent to response policy deployment point (PDP) 107 (also called policy decision point) wherein each security rule of a response policy is converted into scripts to configure the policy enforcement points (PEP) 109 which are located within the information system 1 and which are used to enforce the security policies (firewall activation or configuration, intrusion prevention systems activations, account permissions or access modifications...). The online steps (comprising the online correlation engine 131, the attack objective probability assessment 132, the attack impact assessment, the attack response assessment 136, the policy instantiation engine 134, the policy deployment point and the policy enforcement point) may be achieved by programs or software run by a computer or a server. Said online steps use the stored elements of the data repositories (attack model data repository 125 and response policy data repository 128) to determine dynamically the necessity of activation/deactivation of response security policy in function of the detected attacks and of the state of the monitored information system 1.

[0059] Thus, the present invention allows to provide a dynamic assessment of the impact of an attack as well as the impact of the security policy to apply in response to the attack providing therefore an optimized efficiency of the use of a security policy. Moreover, the idea of determining conditions for deactivating a security policy allows to improve the reactivity of the information system protection and to avoid an unnecessary degraded use of the information system. Indeed, security policy usually correspond to a degraded mode that limits the effects of the attack but also reduces the capacity of said information system and may disturb and affect the users of the information system leading to a loss of productivity or a reduction of quality of service (QoS) for the company using the information system.

Claims

1. Method for adapting security policies of an information system infrastructure in function of attacks wherein it comprises the steps of:

   - storing potential attacks and their associated risks in a data repository;
   - storing curative security policies in response of the potential attacks in a data repository;
   - monitoring entering contents representing data streams of the information system;
   - detecting at least one attack in the information system;
   - assessing a success probability parameter of the at least one detected attack and its associated cost impact parameter;
   - assessing an activation impact parameter of at least one curative security policy in response to the at least one detected attack and its associated cost impact parameter;
   - deciding of the activation or deactivation of a curative security policy in function of the success probability parameter of the, at least one, detected attack, of the activation impact parameter of at least one curative security policy and of the cost impact parameters of both the detected at least one attack and the at least one curative security policy.

2. Method for adapting security policies of an information system infrastructure in accordance with claim 1 wherein the step of storing potential attacks and their associated risks in a data repository comprises the steps of:

   - defining the information system topology and attack detection signatures;
   - defining a risk analysis of the information system that identifies potential attack objectives;
   - specifying attack models to reach the identified attack objectives;
   - storing said attack models in a data repository.

3. Method for adapting security policies of an information system infrastructure in accordance with claim 1 or 2 wherein the step of storing curative security policies in response of the potential attacks in a data repository comprises:

   - specifying at least one attack context;

- specifying curative security policies corresponding to the specified at least one attack context;
- storing said curative security policies in a data repository.

4. Method for adapting security policies of an information system infrastructure in accordance with one of the previous claims wherein the step of assessing a success probability parameter of the at least one detected attack and its associated cost impact parameter comprises:

- generating attack strategy graphs based on the stored attack models and the detected at least one attack;
- assessing the probability for the attack to reach its objective;
- assessing the impact of the attack objective on the system security level and on the system quality of service (QoS) level;
- assessing the associated cost impact parameter of the attack objective;

5. Method for adapting security policies of an information system infrastructure in accordance with one of the previous claims wherein the step of assessing an activation impact parameter of at least one curative security policy in response to the at least one detected attack and its associated cost impact parameter is based on the stored curative security policies and the state of the monitored information system.

6. Method for adapting security policies of an information system infrastructure in accordance with one of the previous claims wherein the step of deciding of the activation or deactivation of a curative security policy in function of the success probability parameter of the, at least one, detected attack, of the activation impact parameter of at least one curative security policy and of the cost impact parameters of both the detected at least one attack and the at least one curative security policy is applied dynamically based on the evolution of the state of the monitored system.

7. Method for adapting security policies of an information system infrastructure in accordance with one of the previous claims wherein the cost impact parameters comprise:

- a quality of service (QoS) impact and,
- a security level degradation impact.

8. Monitoring and protecting equipment comprising:

- at least one data repository for:
  - storing potential attacks and their associated risks;
  - storing curative security policies in response of the potential attacks;
- processing means for:
  - monitoring entering contents representing data streams of the information system;
  - detecting at least one attack in the information system;
  - assessing a success probability parameter of the detected at least one attack and its associated cost impact parameter;
  - assessing at least one activation impact parameter of at least one curative security policy in response to the at least one detected attack and its associated cost impact parameter;
  - deciding of the activation of a curative security policy in function of the success probability parameter of the at least one detected attack, of the activation impact parameter of at least one curative security policy and of the cost impact parameters of both the at least one attack and the at least one curative policy,
  - activating at least one curative security policy.

9. Monitoring and protecting equipment comprising:

- at least one data repository for:
  - storing potential attacks and their associated risks;
  - storing curative security policies in response of the potential attacks;
- processing means for:
  - monitoring entering contents representing data streams of the information system;
  - detecting at least one attack in the information system;
  - assessing a success probability parameter of the detected at least one attack and its associated cost impact parameter;
  - assessing at least one activation impact parameter of at least one curative security policy in response to the at least one detected attack and its associated cost impact parameter;
  - deciding of the deactivation of a curative security policy in function of the success probability parameter of the at least one detected attack, of the activation impact parameter of at least one curative security pol-

icy and of the cost impact parameters of both the at least one attack and the at least one curative policy
- deactivating at least one curative security policy.

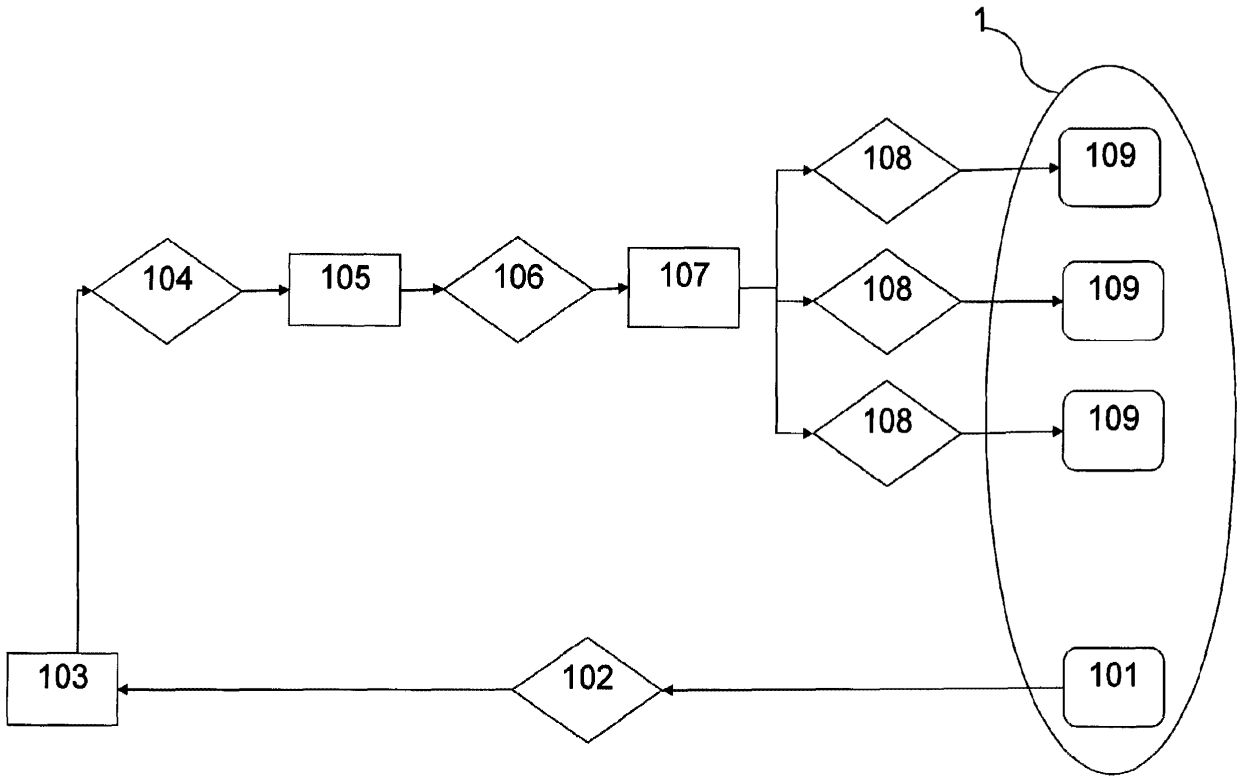


Fig.1

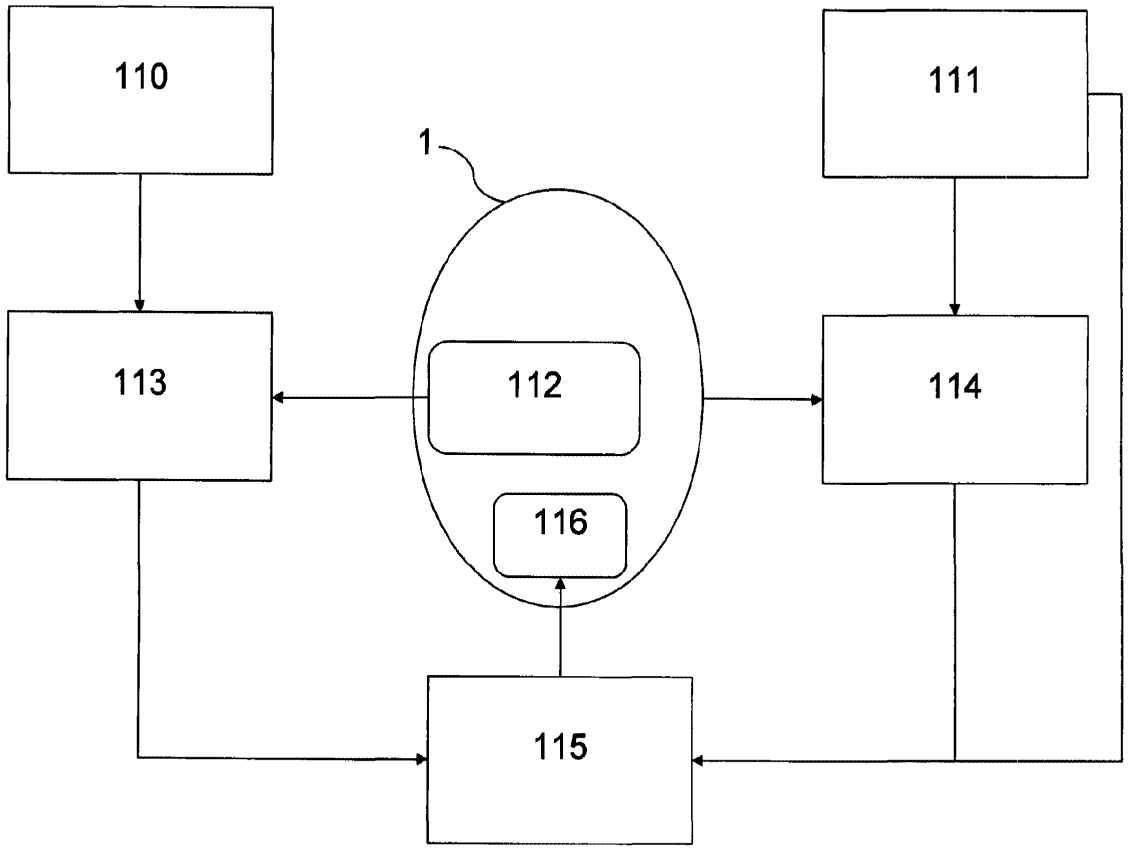


Fig.2

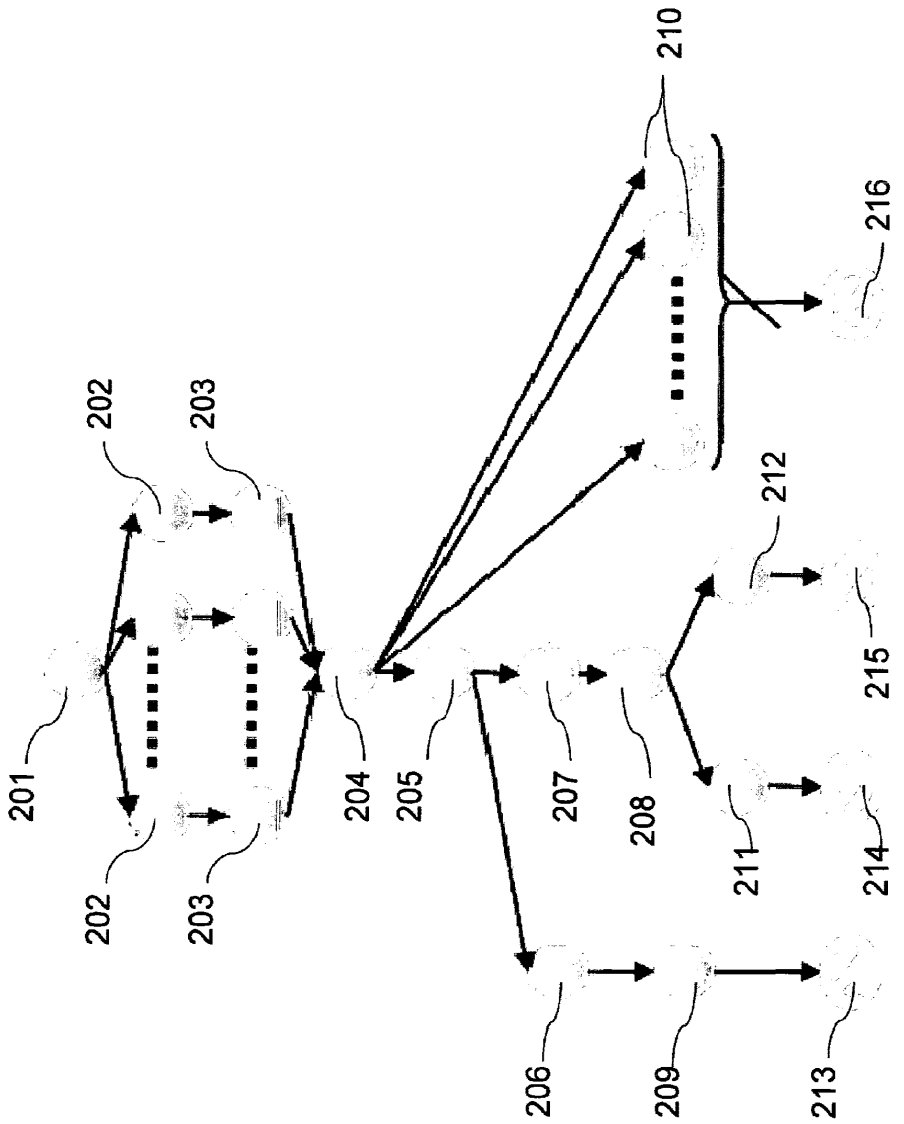


Fig.3

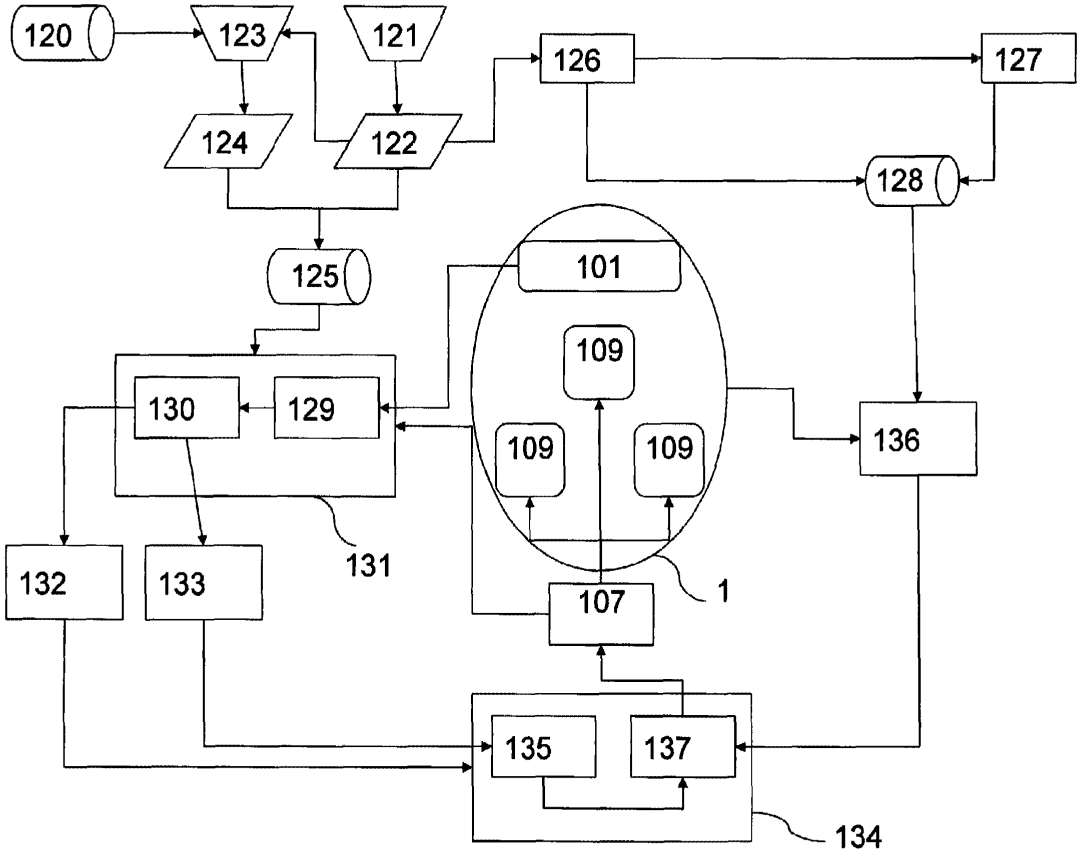

120
123
121
126
127
124
122
128
125
101
109
130
129
109
109
136
131
132
133
1
107
135
137
134

Fig.4

Europäisches Patentamt
European Patent Office
Office européen des brevets

EUROPEAN SEARCH REPORT

Application Number
EP 10 29 0250

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (IPC)
X	WO 2004/015908 A2 (ALPHATECH INC [US]; KREIDL O PATRICK [US]; FRAZIER TIFFANY [US]) 19 February 2004 (2004-02-19) * abstract; figures 1-6; tables I, II * * paragraphs [0006], [0008], [0013] * * paragraphs [0021] - [0023] * * paragraphs [0037] - [0039] * * paragraphs [0052], [0053], [0062] * * paragraphs [0067], [0069], [0072] * * paragraphs [0073], [0076] * * paragraphs [0088] - [0110] * -----	1-9	INV. H04L29/06 G06F21/00
X	KANOUN W ET AL: "Success Likelihood of Ongoing Attacks for Intrusion Detection and Response Systems" COMPUTATIONAL SCIENCE AND ENGINEERING, 2009. CSE '09. INTERNATIONAL CONFERENCE ON, IEEE, PISCATAWAY, NJ, USA, 29 August 2009 (2009-08-29), pages 83-91, XP031543989 ISBN: 978-1-4244-5334-4 * abstract; figures 3,6,7 * * page 83, left-hand column, line 1 - right-hand column, line 37 * * page 84, left-hand column, line 42 - right-hand column, line 2 * * page 84, right-hand column, line 44 - page 85, left-hand column, line 15 * * page 87, left-hand column, line 35 - right-hand column, line 19 * -----	1-9	TECHNICAL FIELDS SEARCHED (IPC) H04L G06F G06N
A	WO 2007/027131 A2 (TELIASONERA AB [SE]; ENDERSZ VIKTOR [SE]) 8 March 2007 (2007-03-08) * figure 1 * * page 4, line 29 - page 8, line 34 * -----	1-9	
	-/--		

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
Munich	21 October 2010	Schossmaier, Klaus

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

Europäisches Patentamt
European Patent Office
Office européen des brevets

EUROPEAN SEARCH REPORT

Application Number
EP 10 29 0250

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (IPC)
A	MIGUEL JOHN: "COMPOSITE COST/BENEFIT/RISK ANALYSIS METHODOLOGY" COMPUTER SECURITY: A GLOBAL CHALLENGE; PROCEEDINGS / PROCEEDINGS OF THE IFIP INTERNATIONAL CONFERENCE ON COMPUTER SECURITY,, 1 January 1984 (1984-01-01), pages 307-311, XP009139953 ISBN: 978-0-444-87618-8 * the whole document * -----	1-9	
			TECHNICAL FIELDS SEARCHED (IPC)

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
Munich	21 October 2010	Schossmaier, Klaus

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

4

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 10 29 0250

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

21-10-2010

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 2004015908 A2	19-02-2004	AU 2003278706 A1	25-02-2004
		CA 2495147 A1	19-02-2004
		EP 1535422 A2	01-06-2005
WO 2007027131 A2	08-03-2007	NONE	

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82

Bibliographic data: EP2498442 (A1) — 2012-09-12

Methods, systems and devices for the detection and prevention of malware within a network

Inventor(s): RIESCHICK GARY [US]; DUNNE CAMERON ROSS [IE]; MCNAMEE ALAN [IE]; HOGAN JOE [IE] ± (RIESCHICK, GARY, ; DUNNE, CAMERON ROSS, ; MCNAMEE, ALAN, ; HOGAN, JOE)

Applicant(s): OPENET TELECOM LTD [IE] ± (OPENET TELECOM LTD)

Classification: **- international:** ***H04L12/24; H04L29/06; H04W12/08; H04W12/12;*** *H04W24/00; H04W88/16*
- cooperative: **H04L63/1441**; **H04W12/08**; **H04W12/12**; H04L63/1408; H04W88/16

Application number: EP20120158921 20120309

Priority number (s): US201161451775P 20110311 ; US201113159710 20110614

Also published as: US2012233656 (A1) US8726376 (B2)

Abstract of EP2498442 (A1)

Methods, systems and devices examine data flows in a communication system control network for known malware threats and suspicious properties typically associated with malware threats. A policy management system inside the control network accesses a user repository and a charging network, and performs pattern matching and/or observed behavior detection methods to determine if the data flows carry content (e.g., malware) that poses a security risk to network or wireless devices. The policy management system generates policy rules based on user preferences and risk-level. The policy management system sends the generated policy rules to a gateway/PCEF, which blocks the data flows, allows the data flows, or restricts the data flow based on the policy rules.

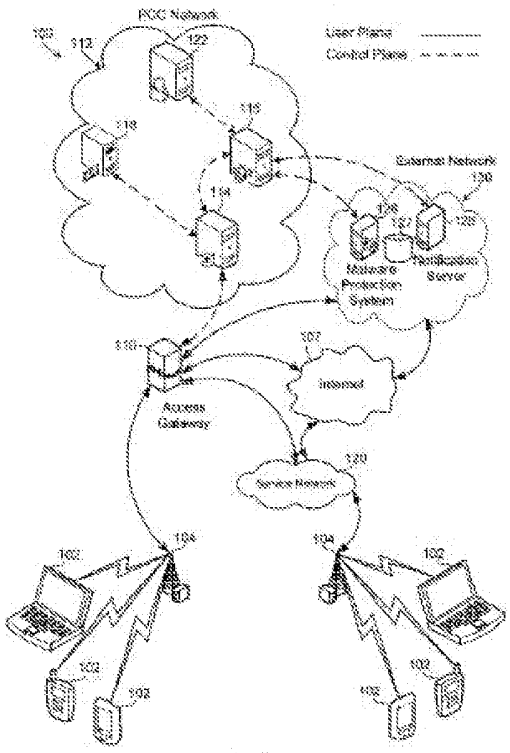

PCC Network
User Plane
Control Plane
External Network
Network Protection System
Identification Server
Internet
Access Gateway
Service Network

FIG. 2

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 2 498 442 A1

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
12.09.2012 Bulletin 2012/37

(21) Application number: **12158921.2**

(22) Date of filing: **09.03.2012**

(51) Int Cl.:
H04L 12/24 *(2006.01)* ***H04L 29/06*** *(2006.01)*
H04W 12/08 *(2009.01)* ***H04W 12/12*** *(2009.01)*
H04W 24/00 (2009.01) *H04W 88/16 (2009.01)*

(84) Designated Contracting States:
AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO RS SE SI SK SM TR
Designated Extension States:
BA ME

(30) Priority: **11.03.2011 US 201161451775 P**
14.06.2011 US 201113159710

(71) Applicant: **Openet Telecom Ltd.**
12 Dublin (IE)

(72) Inventors:
- **Rieschick, Gary**
  Louisburg, KS Kansas KS 66053 (US)
- **Dunne, Cameron Ross**
  County Kildare (IE)
- **McNamee, Alan**
  Dublin, 9 (IE)
- **Hogan, Joe**
  County Dublin (IE)

(74) Representative: **Kelly, Madeleine**
FRKelly
27 Clyde Road
Ballsbridge
Dublin 4 (IE)

(54) Methods, systems and devices for the detection and prevention of malware within a network

(57) Methods, systems and devices examine data flows in a communication system control network for known malware threats and suspicious properties typically associated with malware threats. A policy management system inside the control network accesses a user repository and a charging network, and performs pattern matching and/or observed behavior detection methods to determine if the data flows carry content (e.g., malware) that poses a security risk to network or wireless devices. The policy management system generates policy rules based on user preferences and risk-level. The policy management system sends the generated policy rules to a gateway/PCEF, which blocks the data flows, allows the data flows, or restricts the data flow based on the policy rules.

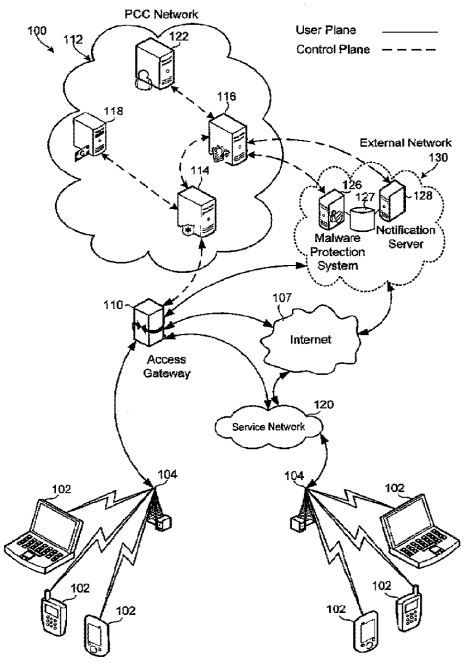


FIG. 2

EP 2 498 442 A1

Description

BACKGROUND

[0001] Recent advances in wireless and mobile technologies enable mobile-device users to access the Internet at any time and in any place. Internet usage habits are changing and many new types of Internet-enabled devices are emerging to meet the evolving user demands and changing Internet-usage habits. Many of these new and emerging Internet-enabled wireless devices use custom and/or non-traditional operating systems and access the Internet through mobile data networks. Further, many of these devices include powerful processors capable of executing third-party application software downloaded from digital application distribution platforms (e.g., Apple Inc.'s App Store, etc.). The emergence these new technologies and wireless devices presents additional security challenges for the telecommunications networks, mobile data networks and to the new wireless devices themselves.

[0002] Today, malicious software (herein "malware") may be used by thieves and hackers to steal confidential information, launch attacks on web servers and to flood networks with spam. Recently, there have been many high-profile cases of confidential customer information being stolen from businesses, and private wireless device users being subjected to online financial and identity thefts. Perhaps even more significantly, there has recently been an increase in wireless devices being infected by malware that forces the wireless device to participate in malicious activities without the user's knowledge or consent, causing users to incur higher usage-charges and leaving them vulnerable to potential legal actions. Recent press reports indicate this problem is increasing at an alarming rate. The emergence of these new types of Internet-enabled devices is likely to exacerbate these problems, as current malware detection and prevention techniques are ineffective at preventing or removing malware from wireless devices, especially the new breed of Internet-enabled wireless devices that have custom and/or non-traditional operating systems.

[0003] Further, the growth in popularity of application distribution platforms (herein "app ecosystems") allows wireless device users to more readily download third party software and execute the downloaded software with full administrative privileges on the mobile device. Such downloaded applications may be sourced from many different sources, such as email attachments, instant messaging systems, and device-to-device transfers. The emergence of app ecosystems presents additional security challenges that are distinct from the traditional security challenges presented by a malicious page being displayed within web browsers which could be managed by implementing a sandbox model.

[0004] Current malware detection and prevention techniques typically involve installing a protective software client application onto a traditional Internet-enabled device, such as a desktop computer or a laptop computer. Thus, current techniques aim to prevent malware by protecting user-level devices (e.g., laptops) rather than providing a comprehensive solution that can eliminate malware from within the network. Further, since many of the new and emerging Internet-enabled wireless devices do not have traditional operating systems, they cannot effectively employ existing malware detection and prevention techniques. As these new Internet-enabled devices grow in popularity, so will the importance of detecting and preventing malware from within the network.

SUMMARY

[0005] The various embodiments provide methods, systems and devices for receiving from one or more communication system control network components data flow parameters identifying characteristics of a data flow, performing a detection method to determine if the data flow carries malicious content, generating restrictive policy rules in response to determining the data flow carries malicious content, generating non-restrictive policy rules in response to determining the data flow does not carry malicious content, and pushing the generated policy rules to a communication system gateway configured to control the flow of packet-based data between a wireless device and an external network. In various embodiments, generating restrictive policy rules in response to determining the data flow carries malicious content includes generating restrictive policy rules that instruct the gateway to block the data flow and/or to block future data flows originating from the wireless device. The data flow may originate from a wireless device or an Internet server.

[0006] Various embodiment methods, systems and devices may perform charging operations that charge subscriber accounts for data flows allowed by the gateway and not charge subscriber accounts for the data flows blocked by the gateway.

[0007] Pattern matching detection methods may be performed in embodiment methods, systems and devices to determine if the data flow carries content that is a security risk. In an embodiment, pattern matching detection methods may be performed by comparing identified binary-file characteristic information with a binary-file characteristic of a known malware type to determine if the data flow carries content having binary-file characteristics of known malware, which may include comparing the identified binary-file characteristic information with a binary-file characteristic of a spam-sending Internet bot.

[0008] The embodiments include servers configured to implement the various methods through software programming, systems implementing such servers, and non-transitory computer-readable storage media on which are stored server-executable instructions implementing the various methods.

BRIEF DESCRIPTION OF THE DRAWINGS

[0009] The accompanying drawings, which are incorporated herein and constitute part of this specification, illustrate exemplary aspects of the invention, and, together with the general description given above and the detailed description given below, serve to explain features of the invention.

[0010] FIG. 1 is a communication system block diagram illustrating network components of a communication system having a third generation partnership project (3GPP), evolved packet core (EPC) architecture suitable for use in the various embodiments.

[0011] FIG. 2 is a communication system block diagram illustrating network components and of an example communication-system having a policy and charging control (PCC) network in accordance with the various embodiments.

[0012] FIG. 3A is a communication system block diagram illustrating example communications between logical components in an example control network and an external network.

[0013] FIG. 3B is an communication system block diagram illustrating example communications between a malware protection system and external networks in accordance with various embodiments.

[0014] FIG. 4A is a process flow diagram illustrating an example method for receiving signaling flows and enforcing policy rules on the signaling flows in accordance with various embodiments.

[0015] FIG. 4B is a process flow diagram illustrating an example policy management system method for receiving parameters from a gateway and generating rules in accordance with the various embodiments.

[0016] FIG. 5 is a process flow diagram illustrating an example pattern matching detection method in accordance with an embodiment.

[0017] FIGs. 6A and 6B are process flow diagrams illustrating example observed behavior detection methods in accordance with various embodiments.

[0018] FIG. 7 is a component block diagram of a server suitable for use with an embodiment.

DETAILED DESCRIPTION

[0019] The various embodiments will be described in detail with reference to the accompanying drawings. Wherever possible, the same reference numbers will be used throughout the drawings to refer to the same or like parts. References made to particular examples and implementations are for illustrative purposes, and are not intended to limit the scope of the invention or the claims.

[0020] The word "exemplary" is used herein to mean "serving as an example, instance, or illustration." Any implementation described herein as "exemplary" is not necessarily to be construed as preferred or advantageous over other implementations.

[0021] As used herein, the terms "mobile device," "wireless device" and "user equipment (UE)" may be used interchangeably and refer to any one of various cellular telephones, smart-phones (e.g., iPhone®), personal data assistants (PDA's), palm-top computers, laptop computers, wireless electronic mail receivers (e.g., the Blackberry® and Treo® devices), VoIP phones, multimedia/Internet enabled cellular telephones, and similar electronic devices capable of sending and receiving wireless communication signals. A wireless device may include a programmable processor and memory.

[0022] As used herein, the term "bot" is used to refer to software applications that emulate human online-activity by automatically performing tasks typically performed by human computer users.

[0023] As used herein, the phrase "malware protection system" is used to refer to any system configured to detect, prevent and/or remove malware such as computer viruses, computer worms, Trojan horses, bots, spyware, adware, etc. Thus, a malware protection system may include a malware prevention system, a malware detection system, a malware removal system, or any other system that assists the detection, prevention and/or removal of malware, as well as combinations of such systems.

[0024] A number of different cellular and mobile communication services and standards are available or contemplated in the future, all of which may implement and benefit from the various embodiments. Such services and standards include, e.g., 3rd generation partnership project (3GPP), long term evolution (LTE) systems, 3rd generation wireless mobile communication technology (3G), 4th generation wireless mobile communication technology (4G), global system for mobile communications (GSM), universal mobile telecommunications system (UMTS), 3GSM, general packet radio service (GPRS), code division multiple access (CDMA) systems (e.g., cdmaone, CDMA2000TM), worldwide interoperability for microwave access (WiMAX), enhanced data rates for GSM evolution (EDGE), advanced mobile phone system (AMPS), digital AMPS (IS-136/TDMA), evolution-data optimized (EV-DO), digital enhanced cordless telecommunications (DECT), and integrated digital enhanced network (iden). Each of these technologies involves the transmission and reception of signaling and content messages. It should be understood that any references to terminology and/or technical details related to an individual standard or technology are for illustrative purposes only and are not intended to limit the scope of the claims to a particular broadcast communication system or technology unless specifically recited in the claim language.

[0025] As discussed above, Internet usage habits are changing and many new types of Internet-enabled devices are emerging to meet evolving user demands. The emergence of these devices presents new security challenges that cannot be addressed by existing antivirus/malware detection and removal systems. For example, current malware detection and prevention techniques attempt to prevent malware by protecting user-level devic-

es (e.g., laptops) rather than from within the network. Since many new and emerging Internet-enabled devices do not having traditional operating systems, current malware detection and prevention techniques cannot efficiently detect or prevent malware.

[0026] The various embodiments provide a comprehensive security solution for detecting and preventing malware from within a mobile data network. The various embodiments protect mobile devices from becoming infected with malicious software (malware) and protect Internet servers and network components from attacks (e.g., denial of service attacks) and inconveniences (e.g., spam) caused by malware. The various embodiments detect both known and yet-to-be identified security threats by performing pattern matching and observed behavior detection methods. Various embodiments monitor network traffic for suspicious content or activities to detect malware and block suspicious data flows from within the network.

[0027] Various embodiments provide methods for detecting and preventing malware from within a data network by combining a policy management component, which has a global or near global view of network traffic and transactions, with a malware system detection component configured to recognize malware based upon patterns within the network traffic and transactions. The various embodiments may operate exclusively within the network and support any type of Internet device.

[0028] The various embodiments may detect transmissions of known and unknown malware in real time as the network patterns emerge. Various embodiments may enable defensive and ameliorative actions, such as modifying the transmissions of the malware or transmission generated by malware, which may include throttling malware transmissions. Various embodiments may prevent the transmission of malware once it has been detected. Various embodiments may alert wireless device users of detected malware. Various embodiments may alert telecommunications network operators of detected malware so they can take corrective actions and/or warn targets of an attack.

The various embodiments may include machine learning mechanisms to enable the malware protection system to learn about malware-generated transmissions and recognize malware patterns as they develop. Such machine learning capabilities may include tracking or correlating network activity levels of recognized threats as well as details of suspicious activities not yet recognized as threatening. Various embodiments may store user-specific malware detection (e.g., patterns in network traffic that occurred while a malware event was underway) and prevention information (e.g., countermeasures that proved effective in responding to a malware event), which may be used by the malware protection system for the detection and prevention of future malware events. Various embodiments may map specific malware threats identified to users of the network. Malware threats may be identified using any suitable mechanism, including the use of IP addresses.

[0029] The various embodiments may push client software capable of exchanging malware and security information with a control network to wireless devices. The malware and security information may include report details generated by the client, alerts generated by the system, instructions from the system to the client that relate to a specific threat to the client, and/or instructions that instruct the wireless device to change its behavior. In an embodiment, the malware and security information may include instructions that instruct a first application executing on the wireless device to cause a second application executing on the wireless device to change its behavior.

[0030] The various embodiments may detect spam by recognizing network traffic with certain characteristics, which may include destination information, protocols, and/or payload content. The various embodiments may protect networks by preventing wireless devices from being used as a source of malware attacks. Various embodiments may detect denial of service attacks by recognizing rapid increases in traffic addressed to a single or related destination from multiple sources. Various embodiments may prevent spam and denial of service attacks by throttling or blocking suspected malicious traffic.

[0031] The various embodiments may reduce the need for network operators to augment capacity and provide network congestion relief. The various embodiments may send detection and prevention information to telecommunications network operators, wireless devices and/or malware systems in real time.

[0032] The various embodiments may be implemented within a variety of mobile communication systems, an example of which is illustrated in FIG. 1. Wireless devices 102 may be configured to send and receive voice, data and control signals to and from a service network 36 (and ultimately the Internet) using a variety of communication systems/technologies (e.g., GPRS, UMTS, LTE, cdmaOne, CDMA2000™, etc). For example, general packet radio service (GPRS) data transmitted from a wireless device 102 is received by a base transceiver station (BTS) 12 and sent to a base station controller (BSC) and/or packet control unit (PCU) component (BSC/PCU) 18. Code division multiple access (CDMA) data transmitted from a wireless device 102 is received by a base transceiver station 12 and sent to a base station controller (BSC) and/or point coordination function (PCF) component (BSC/PCF) 22. Universal mobile telecommunications system (UMTS) data transmitted from a wireless device 102 is received by a NodeB 14 and sent to a radio network controller (RNC) 20. Long term evolution (LTE) data transmitted from a wireless device 102 is received by an eNodeB 16 and sent directly to a serving gateway (SGW) 28 located within the EPC 40.

[0033] The BSC/PCU 18, RNC 20 and BSC/PCF 22 components process the GPRS, UMTS and CDMS data, respectively, and send the processed data to a node within the EPC 40. More specifically, the BSC/PCU 18 and

RNC 20 units send the processed data to a serving GPRS support node (SGSN) 24 and the BSC/PCF 22 sends the processed data to a packet data serving node (PDSN) and/or high rate packet data serving gateway (HSGW) component (PDSN/HSGW) 30. The PDSN/HSGW 30 may act as a connection point between the radio access network and the IP based PCEF/PGW 32. The SGSN 24 is responsible for routing the data within a particular geographical service area and may send signaling (control plane) information (e.g., information pertaining to call set-up, security, authentication, etc.) to a mobility management entity (MME) 26. The MME may request user and subscription information from a home subscriber server (HSS) 42, perform various administrative tasks (e.g., user authentication, enforcement of roaming restrictions, etc), select a SGW 28 and send administrative and/or authorization information to the SGSN 24.

[0034] Upon receiving the authorization information from the MME 26 (e.g., authentication complete, identifier of a selected SGW, etc.), the SGSN 24 sends the GPRS/UMTS data to a selected SGW 28. The SGW 28 stores information about the data (e.g., parameters of the IP bearer service, network internal routing information, etc.) and forwards user data packets to a policy control enforcement function (PCEF) and/or packet data network gateway (PGW) 32. The PCEF/ PGW 32 sends signaling information (control plane) to a policy control rules function 34. The PCRF 34 accesses subscriber databases, creates a set of intelligent policy rules and performs other specialized functions (e.g., interacts with online/offline charging systems, application functions, etc.) and sends the intelligent policy rules to the PCEF/ PGW 32 for enforcement. The PCEF/ PGW 32 implements the policy rules to control the bandwidth, the quality of service and the characteristics of the data, services and flows being communicated between the service network 36 and the end users.

[0035] FIG. 2 illustrates various logical components in an example communication system 100 suitable for implementing the various embodiments. Wireless devices 102 may be configured to communicate via cellular telephone network, a radio access network (e.g., UTRAN, RAN, etc.), WiFi network, WiMAX network, and/or other well known technologies (e.g., GPRS, UMTS, LTE, cdmaOne, CDMA2000TM). Wireless devices 102 may be configured to transmit and receive voice, data and control signals to and from a base station (e.g., base transceiver station, NodeB, eNodeB, etc.) 104, which may be coupled to a controller (e.g., cellular base station, radio network controller, service gateway, etc.) operable to communicate the voice, data, and control signals between mobile devices and to other network destinations. The base station 104 may communicate with an access gateway 110, which serves as the primary point of entry and exit of wireless device traffic and connects the wireless devices 102 to their immediate service provider and/or packet data networks (PDNs). The access gateway 110 may be a part of the policy control and charging network 112 or external to the policy control and charging network 112, and may include one or more of a controller, a gateway, a serving gateway (SGW), a packet data network gateway (PGW), an evolved packet data gateway (ePDG), a packet data serving node (PDSN), a serving general packet radio service support node (SGSN), a policy and charging enforcement function (PCEF), or any combination of the features/functions provided thereof. The access gateway 110 may be implemented in a single computing device or in many computing devices, either within a single network or across a wide area network, such as the Internet.

[0036] The access gateway 110 may forward the voice, data, and control signals to other network components as user data packets, provide connectivity to external packet data networks, manage and store contexts (e.g. network internal routing information, etc.) and act as an anchor between different technologies (e.g., 3GPP and non-3GPP systems). The access gateway 110 may also coordinate the transmission and reception of data to and from the Internet 107, and the transmission and reception of voice, data and control information to and from an external service network 120 connected to the Internet 107 and other base stations 104 and wireless devices 102. The access gateway 110 may also route control/signaling information to a policy and charging control (PCC) network 112, which may be a part of an implementation of an evolved packet core (EPC)/long term evolution (LTE) architecture.

[0037] The PCC network 112 may include a gateway and/or policy and charging enforcement function (PCEF) 114 component for controlling the flow of Internet protocol (IP) data between mobile devices 102 and external networks (e.g., Internet 107, service network 120, etc.). The gateway/PCEF 114 may contain a deep packet inspection (DPI) component (not illustrated) configured to obtain additional application-level information about a particular IP data flow and provide the information to other components in the PCC network 112. In various embodiments, the gateway/PCEF 114 may be integrated with, or a part of, the access gateway 110, either within the PCC network 112 or outside of the PCC network 112.

[0038] The policy and charging control network 112 may also include a policy management system 116, a charging system 118 and a user repository 122. The policy management system 116 may communicate with a malware protection system 126 and a notification server 128 in a network (External Network) 130 outside the telecommunications provider network. The notification server 128 may be configured to receive requests from the policy management system 116 (e.g., PCRF) and send messages to mobile devices 102 using various technologies/mechanisms, such as email, short message service (SMS) texts, instant messaging (IM) systems, interactive voice response (IVR) systems. The notification server 128 may also send messages in a mobile device-specific format, which may be unique to each mobile device type. The notification server 128 may choose

a communications technology/mechanism on a case-by-case basis. For example, the notification server 128 may choose a communications technology/mechanism depending on the user's preferences and/or mobile device type. Messages may be sent through the Internet 107 or the access gateway 110. In an embodiment, the notification server 128 may send messages to a client application running on the mobile devices 102 (e.g., via the Internet 107, access gateway 110, etc.), which may send a response to the notification server 128 for forwarding to the policy management system 116.

[0039] In an embodiment, the notification server 128 may be configured to send messages to mobile devices 102 "in-band" or "out-of-band." The in-band notifications may use the same communication mechanism used for receiving message and the out-of-band notifications may use a different communication mechanism than that used for receiving message. For example, if a user is browsing web pages and receives an in-band notification, then the notification may appear as a new web page.

[0040] The malware protection system 126 may be a dedicated malware system or server, which is sometime referred to herein as a "malware expert system." The malware protection system 126 may be implemented within one or a number of dedicated servers located within the communication network 100, or within one or a number of dedicated servers located external from but with communication links to the communication network 100 (as illustrated). In a further embodiment, some or all elements of the malware protection system 126 functionality may be implemented within a server performing another network function, such as the policy management system 116, a charging system 118 or a user repository 122.

[0041] The malware protection system 126 may maintain a repository of known security risks, gather real-time information regarding emerging security/malware threats, identify security/malware threats by monitoring traffic within the communication network 100, and generate security/malware threat counter-measures. Such security/malware threat counter-measures may include malware removal software and/or malware repair software. In an embodiment, the malware protection system 126 may be configured to generate security/malware threat counter-measures, malware removal software and/or malware repair software in a format specific to each mobile device 102 type. The mobile device formats may be defined by configuration or determined in real time by the policy control system 116, or by the malware protection system 126 based on information received in real time from the policy control system 116.

[0042] The malware protection system 126 may also include a local malware prevention memory or database 127 for each policy management system 116. Likewise, the policy management system 116 may include a local policy management memory (not illustrated), which may be populated by the policy management system 116, the malware protection system 126, or both. In an embodiment, the malware protection system 126 may push data to the policy management memory of the policy management system 116. In an embodiment, the policy management system 116 may periodically request information from the malware protection system 126 and populate the policy management memory with the received information.

[0043] FIG. 3 A is a system architecture diagram illustrating communications between logical components in an example control network 150 (e.g., PCC network) and an external network 155. FIG. 3 illustrates that the control network 150 may include one or more components for providing a policy and charging enforcement function (PCEF) 114, a policy management system 116, a charging system 118, and a user repository 122. The gateway/PCEF 114 may be a part of, or perform operations typically associated with, a gateway GPRS support node (GGSN), a packet data network gateway (PGW), an access gateway 110, or other similar components. In an embodiment, the policy management system 116 may include a policy and charging rules function (PCRF). In an embodiment, the charging system 118 may include an off-line charging system (OFCS) and an on-line charging system (OCS). In an embodiment, the user repository 122 may include a subscriber profile repository (SPR).

[0044] The gateway/PCEF 114 may serve as the primary enforcement point, as a gateway and as a router providing a routing mechanism between the Internet and the radio infrastructure/radio access network. The gateway/PCEF 114 may receive signaling flows and use information contained therein to select an optimal route for a particular type of communication, session, or quality of service (QoS). The gateway/PCEF 114 may also enforce various policies on the received flows, which may include querying, coordinating and/or adjusting various network resources based on a set of policy rules provided by the policy management system 116.

[0045] The policy management system 116 may identify appropriate policy rules for a given situation and send the identified policy rules to the gateway/PCEF 114 for enforcement. Each policy rule may govern the services, quality of service (QoS) and/or bandwidth that are made available to a particular subscriber in a particular data call and/or session. The policy rules may also govern when certain services are made accessible to the subscriber (e.g. weekdays from 9AM to 5PM, etc.) and how long the subscriber may access to those services (e.g., 15 minutes at a time, a total of two hours, etc.). The policy rules may further govern whether specific IP data flows should be "blocked," "allowed" or "allowed with constraints," based on current and potential security risks/malware threats, as discussed in further detail below.

[0046] In an embodiment, the policy management system 116 may generate, compile and select a set of business, technology and security rules that define the policies that are to be enforced. In doing so, the policy management system 116 may communicate with the user repository 122 and/or the charging system 118. The user

repository 112 may store subscriber information (e.g., customer IDs, preferences, subscription levels, etc.) and user-specific information, such as details of a user's subscription to malware prevention services and historical details of a user's exposure to specific malware threats. The charging system 118 may store information pertaining to how much wireless data is being used by a wireless subscriber and information pertaining to whether the subscriber has sufficient funds/credits/access units to receive a requested service/flow. The policy management system 116 may use the information stored by the user repository 122 and charging system 118 to identify potential security risks/malware threats and user preferences for responding to identified security risks/malware threats and make rule decisions based on a combination of the risk/threat and user preference. The policy management system 116 may make the rule decisions on a per-subscriber, per-session and/or per-service basis. For example, the policy management system 116 may use subscriber information (e.g., subscriber's city of residence), the current usage parameters (e.g., day of week, time of day, peak hours, etc.) and the subscriber's service level (e.g., Gold, Bronze, etc.) in conjunction with identified security risks (e.g., known virus, irregular usage patterns, etc.) and user preferences to generate and/or select one or more rules or rule groups, which are pushed to the gateway/PCEF 114 for enforcement.

[0047] The policy management system 116 may also communicate with external systems 155, such as a malware protection system 126 and a notification server 128. As mentioned above, the malware protection system 126 may maintain a repository of known malware threats, gather information regarding emerging malware threats, identify current and potential malware threats and generate malware threat counter-measures, malware removal software and/or malware repair software to neutralize the security threats. The policy management system 116 may send information to the malware protection system 126 to aid in the malware prevention operations. Likewise, the malware protection system 126 may send security related information to the policy management system 116 to aid in the rule making decisions/operations.

[0048] FIG. 3B is a system architecture diagram illustrating communications between policy management systems and malware protection systems. Specifically, FIG. 3B illustrates that the malware protection system 126 may receive information from the policy management system 116, and share information with other policy management systems (e.g., policy management systems 166) or external antivirus/malware protection systems (e.g., malware detection system 162).

[0049] In an embodiment, the policy management system 116 may provide malware detection feedback to the malware protection system 126. In an embodiment, the malware detection feedback may include detection rate information extracted from the IP data flows. The detection rate information may identify the detection rates of known malware threats and include additional parameters (e.g., wireless device type, location of a wireless device, etc.) readily accessible to components within the control network (e.g., policy management system 116, gateway/PCEF 114, etc.). These communication system control network components are generally unavailable to external services and servers (e.g., antivirus servers, malware detection systems, etc.). Such additional parameters may be carried by the IP data flows, extracted by the gateway/PCEF 114 and/or the policy management system 116 and sent to the malware protection system 126. The malware protection system 126 may then use this information to update its malware protection services (e.g., to update lists, generate new prevention software, etc.).

[0050] In an embodiment, the policy management system 116 may send the malware protection system 126 information relating to IP data flows with suspicious characteristics. This information may be used by the malware protection system 126 to identify emerging and unidentified malware threats that are not yet prevalent enough to be known to the malware protection system 126. The malware protection system 126 may also use this information to develop preemptive or preventative countermeasures for the identified malware threats.

[0051] In an embodiment, the policy management system 116 may send malware protection system sample data extracted from IP traffic flows within the detection feedback, which the malware protection system 126 may use for analyzing the malware threats.

[0052] In an embodiment, the malware protection system 126 can subsequently share information received from the policy management system 116 with other policy management systems (e.g., policy management systems 166) in other mobile data networks (e.g., roaming/home networks, external networks, etc.) and/or with independent malware protection systems (e.g., malware detection system 162) operating in private data networks, such as corporate networks, etc.

[0053] FIG. 4A illustrates an example gateway/PCEF method 400 for receiving signaling flows and enforcing policy rules on the signaling flows in accordance with the various embodiments. This embodiment method 400 may be implemented in a server configured with server-executable instructions configured to cause the server to perform the operations of the method steps. In step 402, the gateway/PCEF may receive a data flow originating from, or destined for, a wireless device. In step 406, the gateway/PCEF may examine the data flows and/or the network traffic, identify key characteristics of the data flows and/or network traffic, generate parameters based on the key characteristics and send the generated parameters to a policy managements system for analysis. In step 408, the gateway/PCEF may receive one or more policy rules from the policy management system. In step 410, the gateway/PCEF may use the received policy rules to enforce the various policies discussed above, such as blocking, restricting, or allowing

the data flow to be sent to, or received from, a wireless device.

[0054] FIG. 4B illustrates an example policy management system method 450 for receiving parameters from a gateway/PCEF and generating/selecting rules in accordance with the various embodiments. In step 452, the policy management system may receive parameters generated by the gateway/PCEF. In step 454, the policy management system may use the received parameters to determine if the data flows carry content (e.g., malware) that poses a security risk to network and/or wireless devices. For example, the policy management system may use the parameters to perform pattern matching detection methods or observed behavior detection methods to determine if the data flow carries malicious content or is otherwise a security risk. The policy management system may retrieve information from a local memory and/or request/receive information from external memories/systems/servers (e.g., user repository, charging system, a malware protection system, etc.) that may be used to determine if the data flows carry content (e.g., malware) associated with a potential or known security risk. In step 456, the policy management system may generate/select policy rules based on determining the data flows carry content that poses a "known risk," a "potential risk," or "no risk." In step 458, the policy management system may send the generated/selected policy rules to the gateway/PCEF for enforcement.

[0055] As mentioned above, the policy management system may retrieve information from a local memory as well as from external memories/systems/servers. In an embodiment, the policy management system may first access the local memory before requesting information from the external memories/systems/servers to reduce latency and improve efficiency. In an embodiment, if the local memory identifies the data flow as carrying a potential security risk, the policy management system may forgo accessing the external memories/systems/servers and generate rules based on the information in the local memory. This reduces latency and improves efficiency because fewer operations and external communications are required to make intelligent policy rule decisions.

[0056] FIG. 5 illustrates an example pattern matching detection method 500, which may be performed by the policy management system to determine if an IP data flow carries content (e.g., malware) that poses a security risk. In step 502, the policy management system may receive parameters identifying certain key characteristics of the IP data flows and/or network traffic. In step 504, the policy management system may examine the parameters to identify/extract information that may be used to determine if the data flow carries content that poses an unacceptable security risk to a wireless device, the network, or both. For example, in step 504, the policy management system may extract binary-file characteristic information, uniform resource locator (URL) information (e.g., from the HTTP-headers of IP packets), IP address information and/or simple mail transfer protocol (SMTP) information (e.g., from SMTP headers/bodies of outgoing emails) from the received parameters.

[0057] In determination step 506, the policy management system may compare the extracted binary-file characteristic information with binary-file characteristics of known malware types (e.g., bots, viruses, worms, Trojan Horses, etc.) to determine if the data flow carries content having binary-file characteristics of known malware (e.g., bots, viruses, worms, Trojan Horses, etc). If the policy management system determines that the data flow carries content that has binary-file characteristics in common with known malware (i.e., determination step 506 = "Yes"), in step 550, the policy management system may generate restrictive policies rules (e.g., "block content," "allow with constraints," etc.) based on the severity of the risk and push the generated rules to the gateway/PCEF. In an embodiment, the policy management system may generate restrictive policy rules that instruct the gateway/PCEF to block the IP data flow upon determining that an IP data flow carries content having binary-file characteristics of known malware threats (e.g., viruses, Trojan Horses, etc.).

[0058] If the policy management system determines that the data flow does not carry content having binary-file characteristics of known malware types (i.e., determination step 506 = "No"), in determination step 510, the policy management system may compare extracted URL information against a list of URLs known to be under attack (e.g., denial-of-service attack, etc.) to determine if the destination of data flow content is a server under attack. If the policy management system determines that the data flow carries or is likely to carry content destined for a server under attack (i.e., determination step 510 = "Yes"), in step 550, the policy management system may generate policy rules (e.g., "block content," "allow with constraints," etc.) based on various factors (e.g., severity of the risk, subscriber's usage history, subscription level, likelihood request is genuine, etc.) and push the generated rules to the gateway/PCEF. In an embodiment, the policy management system may generate an "allow with constraints" rule upon determining that the IP data flow represents a malware threat (e.g., carries content destined for a server under attack), but does not contain a binary that is a malware threat (e.g., carries content having binary-file characteristics of known malware). In an embodiment, the policy management system may generate rules that include constraints that set an upper threshold on the rate of IP data flows and/or introduce an artificial latency to the IP data flow. In this manner, the policy management system may generate intelligent policy rules to prevent attacks on servers, in real time and from within the network, without shutting off all communications to a particular Internet site.

[0059] If the policy management system determines that the data flow does not carry content destined for a server under attack (i.e., determination step 510 = "No"), in determination step 512, the policy management system may compare SMTP information of emails carried

by a data-flow with known spam heuristics (e.g., incorrect SMTP headers, origin IP address blacklisting, email not relayed, message body contains blacklisted keywords, message attachment scanning using Optical Character Recognition (OCR) techniques, Artificial Intelligence (AI) based methods such as Bayesian filtering, or any combination of these) to determine if the emails originate from a spam-sending bot. If the policy management system determines that the data-flow carries an email that originates from a spam-sending bot (i.e., determination step 512 = "Yes"), in step 550, the policy management system may generate restrictive policy rules that block or restrict the data flow and push the generated rules to the gateway/PCEF for enforcement. In an embodiment, the policy management system may generate an "allow with constraints" rule upon determining that the IP data flow carries content from a known spam bot. In this manner, the policy management system may generate intelligent policy rules to reduce spam, in real time and from within the network, without filtering desired emails/communications.

[0060] If the policy management system determines that the IP data flow does not carry an email that originates from a spam-sending bot (i.e., determination step 512 = "No"), in determination step 514, the policy management system may compare the IP address information with a list of known offender IP addresses to determine if the IP data flow originates from, or is destined for, a mobile device that is compromised (e.g., infected with malware, a virus, etc.) or blacklisted (e.g., known to intentionally engage in malicious activities). If the policy management system determines that the IP address information is associated with an IP address in the list of known offender IP addresses (i.e., determination step 514 = "Yes), in step 550, the policy management system may generate policy rules that block or restrict the data flow and push the generated rules to the gateway/PCEF for enforcement. In an embodiment, the policy management system may generate an "allow with constraints" rule upon determining that the IP data flow carries content originating from, or destined for, a mobile device that is compromised or blacklisted. In this manner, the policy management system may generate intelligent policy rules to prevent the wireless device, a network server, or both from engaging in malicious activities, without blocking all the services/communications between a wireless device and a network component.

[0061] If the policy management system determines that the IP address information is not associated with an IP address in the list of known offender IP addresses (i.e., determination step 514 = "No"), in determination step 516, the policy management system may compare the URL information to a list of known offender network addresses (e.g., URLs) to determine if the data flow is destined for a website/server known to engage in malicious activities. If the policy management system determines that the URL information is associated with a URL in the list of known offender URLs (i.e., determination step 516 = "Yes"), in step 550, the policy management system may generate restrictive policy rules and push the generated rules to the gateway/PCEF for enforcement. In an embodiment, the policy management system may generate an "allow with constraints" rule upon determining that the IP data flow carries content destined for a website/server known to engage in malicious activities, without blocking all access to the website/server.

[0062] If the policy management system determines that the URL information is not associated with a URL in the list of known offender URLs (i.e., determination step 516 = "No"), in step 560, the policy management system may generate rules to allow the flow, or perform additional operations (e.g., observed behavior detection methods) to determine if the data flow carries content (e.g., malware) that poses a security risk to a wireless device, network server, or both.

[0063] In an embodiment, the policy management system may perform observed behavior detection methods to determine if the data flow carries content (e.g., malware) that may be harmful or a security risk to the network/wireless devices. The policy management system may perform the observed behavior detection methods instead of, or in addition to, the pattern matching detection methods discussed above. Observed behavior detection methods allow the policy management system to detect emerging and yet-unidentified security risks (e.g., malware threats) that are not yet prevalent enough to be known to the malware protection system or third party antivirus/security systems. The observed behavior detection methods may exploit the policy management system's access to the control network information to monitor IP data flows for suspicious characteristics and to identify security risks. For example, the policy management system may access information stored in a user repository and/or charging system in a control network to identify and neutralize security risks that cannot be identified or neutralized by systems that do not have access to user/charging information (e.g., components outside the control network).

[0064] FIGs. 6A-6B illustrate example observed behavior detection methods that may be performed by the policy management system to determine if an IP data flow is a security risk/malware threat. Performing the observed behavior oriented detection methods may include monitoring a number of data flows matching a specific behavior and/or detecting an unexpected rise in a number of requests matching a defined behavior from a specific wireless device. The specific and defined behaviors may include any of the behaviors described below, including unexpected rise in requests, requests to a specific port 80 of a specific IP address, increases in HTTP requests to a specific URL, unexpected rise in requests to a single destination, unexpected rise in outbound emails and/or DNS queries, etc.

[0065] FIG. 6A illustrates an example observed behavior detection method 600 for determining if an IP data flow carries content that may contribute to a denial of

service attack. In step 602, the policy management system may receive parameters identifying certain key characteristics of the IP data flows and/or network traffic. In step 604, the policy management system may analyze the parameters and update memories, counters and/or threshold values used to monitor sudden and unexpected rises in requests to a single destination. These counters may be used to store running totals, averages, and/or maximum values for one or more different time periods (e.g., the total number of requests to a destination IP address in the last 24 hours, or the average number of requests to a destination IP address per month). Therefore, the counters can be used to store or derive request rates. The counters may be specific to the user, or they may be generalized across groups of users. Therefore, a sudden and unexpected rise in requests to a single destination can be defined in terms of a counter value surpassing a pre-defined rate. This predefined rate can be expressed in terms of the counters (e.g., a sudden and unexpected rise can be defined as the current rate being greater than a tripling of the maximum hourly rate ever experienced). The associated thresholds may be defined as constants, or in terms of the counters (e.g., a threshold can be defined as a quadrupling of the maximum hourly rate ever experienced). Thus, there can be a sudden and unexpected rise in the number of requests to a single destination, but it may not exceed a threshold. In step 606, the policy management system may monitor the number of requests by performing IP level and application level monitoring operations. IP level monitoring operations may include monitoring requests to a specific port 80 of a specific IP address. Application level monitoring operations may include monitoring increases in HTTP requests to a specific URL. In determination step 608, the policy management system may determine if there has been a sudden and unexpected rise in requests to a single destination. This determination may be based upon a counter value surpassing a pre-defined rate, as described previously. If the policy management system determines that there has not been a sudden and unexpected rise in requests to a particular address (i.e., determination step 608 = "No"), in step 612, the policy management system may generate policy rules and push the generated rules to the gateway/PCEF. If the policy management system determines that there has been a sudden and unexpected rise in requests to a single destination (i.e., determination step 608 = "Yes"), in determination step 610, the policy management system may determine if the rise in requests exceeds a predetermined threshold. If the rise in requests does not exceed the predetermined threshold (i.e., determination step 610 = "No"), in step 612, the policy management system may generate policy rules and push the generated rules to the gateway/PCEF. If the rise in requests exceeds the predetermined threshold (i.e., determination step 610 = "Yes"), the policy management system may conclude that a denial of service attack is emerging, and in step 614, register the destination as being under attack, generate restrictive policy rules to block or limit current and future flows from accessing the registered destination, and push the generated rules to the gateway/PCEF for implementation.

[0066] FIG. 6B illustrates an example observed behavior detection method 650 for determining if an IP data flow carries content from spam engines. In step 652, the policy management system may receive parameters identifying certain key characteristics of the IP data flows and/or network traffic from a gateway/PCEF. In step 654, the policy management system may analyze the parameters and update local databases and/or counters with information that may be used to monitor sudden rises in outbound emails and/or sudden rises in domain name system (DNS) queries for mail exchanger (MX) records by a single mobile device. In step 656, the policy management system may monitor the number of outbound emails and/or DNS queries by performing IP-level and application-level monitoring operations. IP-level monitoring operations performed by the policy management system may include monitoring/counting the number of requests by a specific mobile device to port 25 of different IP addresses. Application-level monitoring operations may include monitoring the number of SMTP requests being sent directly to an email recipient's SMTP server from a single mobile device. The IP-level and application-level monitoring operations may be used to identify data flows carrying content originating from a spam engine because "well-behaved" email clients generally send all their outbound email via a single SMTP server, whereas spam engines typically send outbound emails directly to the email recipient's SMTP server.

[0067] In determination step 658, the policy management system may determine if there has been a sudden and unexpected rise in outbound emails and/or in domain name system (DNS) queries for mail exchanger (MX) records by a single mobile device. This determination may be based upon a counter value surpassing a pre-defined rate, as described previously. If the policy management system determines that there has not been a sudden and unexpected rise in outbound emails/queries (i.e., determination step 658 = "No"), in step 662, the policy management system may generate policy rules and push the rules to the gateway/PCEF. If the policy management system determines that there has been a sudden and unexpected rise in outbound emails and/or in domain name system (DNS) queries (i.e., determination step 658 = "Yes"), in determination step 660, the policy management system may determine if the rise in requests exceeds a predetermined threshold. If the rise exceeds the predetermined threshold (i.e., determination step 660 = "Yes"), in step 664, the policy management system may identify the data flow as carrying content from a spam engine, register the spam engine (e.g., update a spam engine list in memory, etc.), generate restrictive policy rules to block or limit data flows originating from the spam engine, and push the rules to the gateway/PCEF for enforcement. If the rise does not exceed the

predetermined threshold (i.e., determination step 660 = "No"), in step 664, the policy management system may generate policy rules (e.g., allow, allow with constraints, etc.) and push the rules to the gateway/PCEF.

[0068] As mentioned above, the policy management system may perform detection methods (e.g., pattern matching, observed behavior, etc.) and generate restrictive policy rules based on the type of malware detected. For example, the policy management system may generate a "block" rule if an IP data flow carries content having binary-file characteristics of known malware threats (e.g., viruses, Trojan Horses, etc.) and an "allow with constraints" rule if the IP data flow represents a malware threat, but does not contain a binary that is a malware threat (e.g., the IP data flow is part of a denial of service attack, the IP data flow originates from a spam bot, etc.). The "allow with constraints" rule may define requirements (i.e., constraints) for allowing certain IP data flows to pass through the gateway/PCEF. For example, the constraints may require the gateway/PCEF to introduce an artificial latency to certain IP data flows or to set an upper threshold on certain IP data flow rates.

[0069] The "allow with constraints" type rules, and the constraints they impose, allow the policy management system to customize each rule to the preferences of a particular subscriber, wireless device type or type value, network component or network client. For example, the policy management system may access user preference parameters that define which constraints are to be used in various situations, as well as the actions, conditions and variables (e.g., risk levels, thresholds, data usage levels, costs, etc.) associated with each constraint. In an embodiment, a unique/separate set of user preference parameters may be maintained for each wireless subscriber, device, device type, network component, or client. In this manner telecommunications network operators and their customers may customize responses to malware events, which may be implemented automatically and in real time, consistent with the type of threat and how the network operator and/or customer prefers to respond. For example, some organizations cannot to afford to shut off all requests for service during a denial of service attack, and thus would prefer constraints on the volume or data rates imposed on incoming service requests.

[0070] In an embodiment, the constraints imposed by the policy management system may be proportional to a malware threat or threat-level as determined by the malware protection system or specified by an operator. Methods for determining a malware threat-level within malware protection system are disclosed herein. In an embodiment, the constraints imposed by the policy management system may become progressively more restrictive or constrained, in real-time, as a malware threat or threat-level rises as determined by malware protection system, an operator or other systems configured to identify the threat level.

[0071] User preference parameters may define the actions and conditions associated with each constraint in "allow with constraints" type rules. Thus, the user preference parameters may be used by the policy management system to generate policy rules that instruct the gateway/PCEF to perform several different types of operations (i.e., actions) as well as set conditions for performing those actions. For example, the policy management system may access the user preference parameters to determine that the correct course of action (i.e., the correct rule) for the gateway/PCEF upon the detection of low-risk malware is to send an alert message to the wireless device without blocking the IP data flow. Likewise, the user preference parameters may be used by the policy management system to generate rules that instruct the gateway/PCEF to block the current IP data flow and all future IP data flows until the malware has been manually removed from the mobile device.

[0072] In an embodiment, the policy management system may perform quarantining operations by storing details of IP data flows, aggregated details of the IP data flows, or sequestering the actual content of the IP data flows, that were allowed, constrained, or blocked. The policy management system may store source information, destination information and time information for each IP data flow that is constrained. For example, the policy management system may track the number of IP data flows containing infected binaries within a predetermined time period (e.g., within the last month) and store the number value in a memory. The policy management system may also store emails deemed to be spam. This information may be stored such that a wireless device user whose mobile device is associated with these IP data flows may subsequently view the quarantining details. In an embodiment, the policy management system may be configured to receive messages from the wireless device user that trigger further quarantining actions (e.g., removing a stored IP data flow, un-quarantining stored IP data flow, etc.). For example, the user may send the policy management system a message to reclassify an email as not spam, in which case the email may be pushed to the mobile device by the policy management system. In an embodiment, the user may classify the IP data flow in a manner that causes the policy management system to allow delivery of future similar IP data flows.

[0073] In the various embodiments, user preference parameters may be generated from information from a subscriber account in the user repository, by interacting with the user (e.g., via SMS messages sent through the notification server 126, etc.) to determine his/her preferences in real-time, by using contextual information (e.g., roaming in third party network, home network, etc.), or any combination thereof. For example, a wireless device user may upload user preference parameters to the user repository that instructs the policy management system to send an alert to the user's wireless device warning of potential risks if the wireless device is not roaming in a third-party mobile data network and to block the current IP data flow and all future IP data flows if the wireless

device is roaming in a third-party mobile data network. In this manner, cost conscientious users may prevent a potential malware program from accessing online services while roaming in an expensive third-party mobile data network.

[0074] In an embodiment, the user preference parameters may be based on a malware threat model. The malware threat model may be defined in terms of multiple independent factors, such as the probability of infection, the type of infection, the severity of the threat posed by the infection, and the difficulty associated with removing the infection. These factors may be weighted and combined to produce an overall threat level. The user may then specify his/her preference in terms of this overall threat level. Alternatively, the user may specify his/her preference in terms of one of the factors within the threat model (e.g., a user may be willing to be exposed to a type of infection that installs Adware, whereas he/she may not be willing to be exposed to a type of infection that corrupts or destroys data stored on the wireless device).

[0075] In an embodiment, the policy management system and/or gateway/PCEF may be configured to charge users/subscribers differently for the IP data flows depending on the actions. For example, a user/subscriber may not be charged for any IP data flows that were blocked by the gateway.

[0076] In an embodiment, a malware prevention and removal client (MPRC) software application may be pushed to the wireless devices. The policy management system may, upon determining that an IP data flow is associated with a malware threat, notify the malware protection system of the wireless device's identity and the detected malware. The malware protection system may then update, or instruct, the MPRC to take preventative, recovery, or removal actions specific to the wireless device type or type value and the detected malware threat. For example, the malware protection system may instruct the MPRC to disable the wireless device's data capabilities and/or isolate the mobile device from the mobile data network until the malware is removed or is otherwise no longer a threat. In an embodiment, the policy management system may send a notification based on the status of the user's subscription to the malware prevention service.

[0077] As discussed above with reference to FIG. 3, the policy management system may exchange information with both a user repository and a charging system. In an embodiment, the policy management system may directly charge the subscription accounts of beneficiaries (e.g., wireless device users, web servers, telecommunication clients, etc.) of the above mentioned malware detection/prevention services by sending a charging message to deduct funds from each subscriber's service account. For example, the policy management system may send a charge message to charge a wireless device user's wireless subscription account each time malware is detected and/or removed from the user's wireless device.

[0078] The policy management system may support multiple different charging models to support any required business models. The charging models may include providing the above mentioned services free-of-charge, charging on an annual basis, on a pay-as-you-consume basis, or any combination thereof. If the services are charged on an annual basis, the policy management system may determine the status of the users' annual subscriptions (e.g., last time payment was made, account status, subscription level, etc.) by accessing the user repository and sending charging messages to the charging system to charge the customers as required. If the services are charged on a pay-as-you-consume basis, the policy management system may send a charging request to the charging system each time the service is provided (e.g., each time a message is send waning of potential malware). In an embodiment, each service may be charged separately. For example, the policy management system may send charging messages to the charging system annually for the detection services and send charging messages to the charging system each time malware is removed.

[0079] In an embodiment, the policy management system may be configured to automatically adapt to a network wide stance if the detection of malware indicates that the network is under attack. The adaption of the network wide stance may be in stages, such that the network-wide protections are progressive. In an embodiment, the policy management system may change and/or bulk push policies/rules into the network if the network the detection of malware indicates that the network is under attack. Policies/rules may be pushed to network elements upon detection of a new malware threat or upon a malware threat level achieving a predefined threshold such that the network adopts an "under attack" pre-defined configuration. The initiation of such "under attack" responses or configuration may be based on the detection of malware and/or policy counters exceeding a predefined threshold number or instances of attack.

[0080] The various embodiments and logical components may be implemented on any of a variety of commercially available server devices, such as the server 700 illustrated in FIG. 7. Such a server 700 typically includes a processor 701 coupled to volatile memory 702 and a large capacity nonvolatile memory, such as a disk drive 703. The server 700 may also include a floppy disc drive, compact disc (CD) or DVD disc drive 706 coupled to the processor 701. The server 700 may also include network access ports 704 coupled to the processor 701 for establishing data connections with a network 705, such as a local area network coupled to other broadcast system computers and servers.

[0081] The processor 701 may be any programmable microprocessor, microcomputer or multiple processor chip or chips that can be configured by software instructions (applications) to perform a variety of functions, including the functions of the various embodiments described below. Multiple processors 701 may be provided,

such as one processor dedicated to wireless communication functions and one processor dedicated to running other applications. Typically, software applications may be stored in the internal memory 702, 703 before they are accessed and loaded into the processor 701. The processor 701 may include internal memory sufficient to store the application software instructions.

[0082] The foregoing method descriptions and the process flow diagrams are provided merely as illustrative examples and are not intended to require or imply that the steps of the various embodiments must be performed in the order presented. As will be appreciated by one of skill in the art the order of steps in the foregoing embodiments may be performed in any order. Words such as "thereafter," "then," "next," etc. are not intended to limit the order of the steps; these words are simply used to guide the reader through the description of the methods. Further, any reference to claim elements in the singular, for example, using the articles "a," "an" or "the" is not to be construed as limiting the element to the singular.

[0083] The various illustrative logical blocks, modules, circuits, and algorithm steps described in connection with the embodiments disclosed herein may be implemented as electronic hardware, computer software, or combinations of both. To clearly illustrate this interchangeability of hardware and software, various illustrative components, blocks, modules, circuits, and steps have been described above generally in terms of their functionality. Whether such functionality is implemented as hardware or software depends upon the particular application and design constraints imposed on the overall system. Skilled artisans may implement the described functionality in varying ways for each particular application, but such implementation decisions should not be interpreted as causing a departure from the scope of the present invention.

[0084] The hardware used to implement the various illustrative logics, logical blocks, modules, and circuits described in connection with the aspects disclosed herein may be implemented or performed with a general purpose processor, a digital signal processor (DPC), an application specific integrated circuit (ASIC), a field programmable gate array (FPGA) or other programmable logic device, discrete gate or transistor logic, discrete hardware components, or any combination thereof designed to perform the functions described herein. A general-purpose processor may be a microprocessor, but, in the alternative, the processor may be any conventional processor, controller, microcontroller, or state machine. A processor may also be implemented as a combination of computing devices, e.g., a combination of a DPC and a microprocessor, a plurality of microprocessors, one or more microprocessors in conjunction with a DPC core, or any other such configuration. Alternatively, some steps or methods may be performed by circuitry that is specific to a given function.

[0085] In one or more exemplary aspects, the functions described may be implemented in hardware, software, firmware, or any combination thereof. If implemented in software, the functions may be stored on or transmitted over as one or more instructions or code on a non-transitory computer-readable medium. The steps of a method or algorithm disclosed herein may be embodied in a processor-executable software module which may reside on a non-transitory computer-readable storage medium. Non-transitory computer-readable storage media may be any available media that may be accessed by a computer (e.g., a server) or processor of a computer or server. By way of example, and not limitation, non-transitory computer-readable media may include RAM, ROM, EEPROM, CD-ROM or other optical disk storage, magnetic disk storage or other magnetic storage devices, or any other storage medium that may be used to store desired program code in the form of processor-executable instructions or data structures and that may be accessed by a computer. Disk and disc, as used herein, includes compact disc (CD), laser disc, optical disc, digital versatile disc (DVD), floppy disk, and blu-ray disc where disks usually reproduce data magnetically, while discs reproduce data optically with lasers. Combinations of the above should also be included within the scope of non-transitory computer-readable media. Additionally, the operations of a method or algorithm may reside as one or any combination or set of codes and/or instructions on a non-transitory machine readable medium and/or computer-readable medium, which may be incorporated into a computer program product.

[0086] The preceding description of the disclosed embodiments is provided to enable any person skilled in the art to make or use the present invention. Various modifications to these embodiments will be readily apparent to those skilled in the art, and the generic principles defined herein may be applied to other embodiments without departing from the scope of the invention. Thus, the present invention is not intended to be limited to the embodiments shown herein but is to be accorded the widest scope consistent with the following claims and the principles and novel features disclosed herein.

Claims

1. A communication method, comprising:

   receiving in a server from one or more communication system control network components data flow parameters identifying characteristics of a data flow;

   performing in the server a detection method to determine if the data flow carries malicious content;

   generating restrictive policy rules in response to determining the data flow carries malicious content;

   generating non-restrictive policy rules in response to determining the data flow does not

carry malicious content; and
pushing the generated policy rules to a communication system gateway configured to control a flow of packet-based data between a wireless device and an external network.

2. The method of claim 1, wherein generating restrictive policy rules in response to determining the data flow carries malicious content comprises generating restrictive policy rules based on a subscriber's usage history and a subscription level.

3. The method of claim 1, wherein generating restrictive policy rules in response to determining the data flow carries malicious content comprises generating constraints that are proportional to a threat-level associated with the malicious content and generating restrictive policy rules that impose the generated constraints on the communication system gateway.

4. The method of claim 1, further comprising transmitting malware detection feedback to a network component in a second external network.

5. The method of claim 1, further comprising interacting with a wireless device user to determine user preferences in real-time via alert messages sent through a notification server to receive user preference parameters.

6. The method of claim 1, wherein the data flow originates from the wireless device, and generating restrictive policy rules in response to determining the data flow carries malicious content comprises generating restrictive policy rules that instruct the communication system gateway to block future data flows originating from the wireless device.

7. The method of claim 1, wherein performing a detection method to determine if the data flow carries content that is a security risk comprises performing a pattern matching detection method.

8. The method of claim 7, wherein:

receiving in a server from one or more communication system control network components data flow parameters identifying characteristics of a data flow comprises receiving parameters identifying binary-file characteristic information; and
performing a pattern matching detection method comprises comparing the identified binary-file characteristic information with a binary-file characteristic of a known malware type to determine if the data flow carries content having binary-file characteristics of known malware.

9. The method of claim 7, wherein:

receiving in a server from one or more communication system control network components data flow parameters identifying characteristics of a data flow comprises receiving parameters identifying source and destination information; and
performing in the server a pattern matching detection method comprises comparing the identified source and destination information against a list of known offender sources and destinations to determine if the data flow originates from a wireless device known to engage in malicious activity and if the data flow is destined for a website/server known to engage in malicious activities.

10. The method of claim 7, wherein:

receiving in a server from one or more communication system control network components data flow parameters identifying characteristics of a data flow comprises receiving parameters identifying destination information; and
performing in the server a pattern matching detection method comprises comparing the identified destination information against a list of destinations known to be under attack to determine if a destination of the data flow is a network server under attack.

11. The method of claim 7, wherein:

receiving in a server from one or more communication system control network components data flow parameters identifying characteristics of a data flow comprises receiving parameters identifying messaging information; and
performing in the server a pattern matching detection method comprises comparing the identified messaging information with spam heuristics.

12. The method of claim 1, wherein performing in the server a detection method to determine if the data flow carries content that is a security risk comprises performing a behavior oriented detection method.

13. The method of claim 12, wherein performing a behavior oriented detection method comprises accessing information stored in one of a user repository of a control network and a charging system of a control network.

14. The method of claim 12, wherein performing a behavior oriented detection method comprises updating a counter value to monitor a number of data flows

matching a specific behavior.

15. The method of claim 12, wherein performing a behavior oriented detection method comprises performing monitoring operations in order to detect an unexpected rise in a number of requests matching a defined behavior from a specific wireless device.

16. A server, comprising:

a memory; and
a processor coupled to the memory, wherein the processor is configured with processor-executable instructions to perform operations comprising:

receiving data flow parameters identifying characteristics of a data flow;
performing a detection method to determine if the data flow carries malicious content;
generating restrictive policy rules in response to determining the data flow carries malicious content;
generating non-restrictive policy rules in response to determining the data flow does not carry malicious content; and
pushing the generated policy rules to a communication system gateway configured to control a flow of packet-based data between a wireless device and an external network.

17. A non-transitory computer readable medium having stored thereon processor-executable software instructions configured to cause a processor to perform operations comprising:

receiving from one or more communication system control network components data flow parameters identifying characteristics of a data flow;
performing a detection method to determine if the data flow carries malicious content;
generating restrictive policy rules in response to determining the data flow carries malicious content;
generating non-restrictive policy rules in response to determining the data flow does not carry malicious content; and
pushing the generated policy rules to a communication system gateway configured to control a flow of packet-based data between a wireless device and an external network.

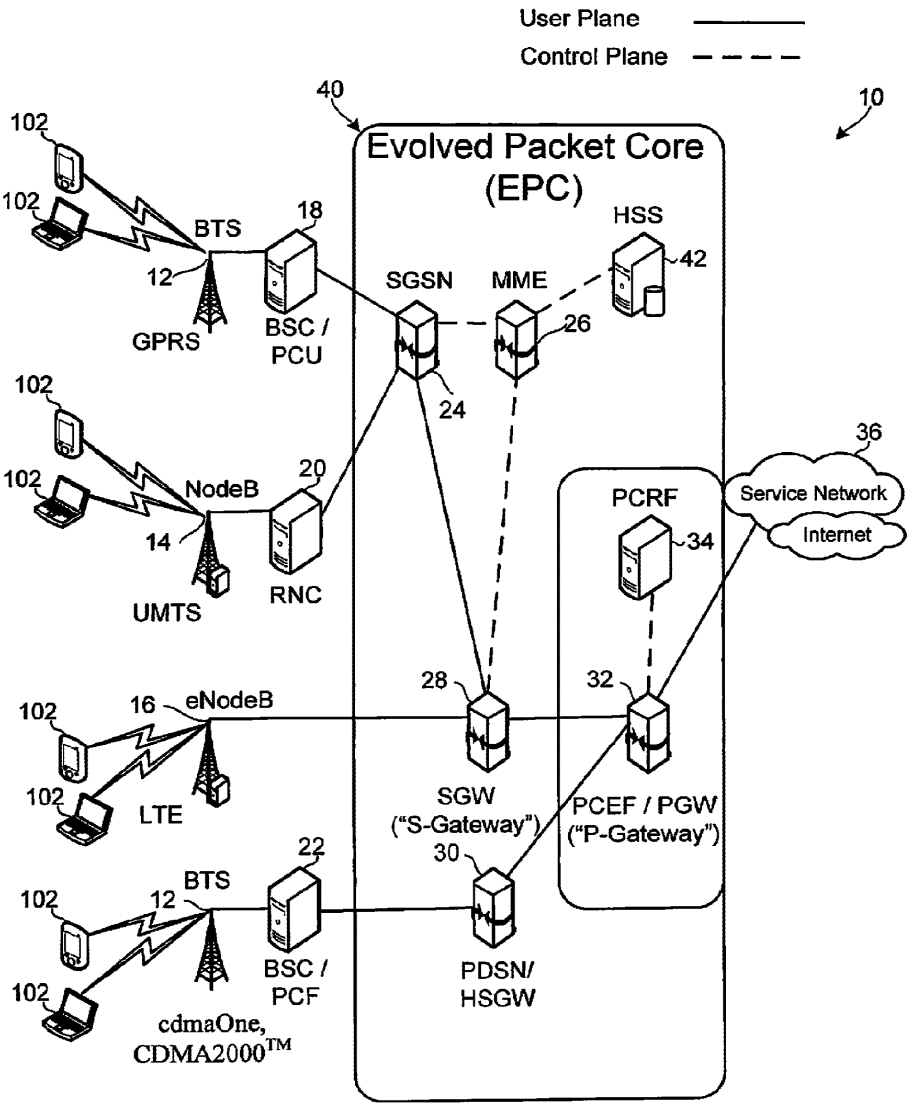


FIG. 1

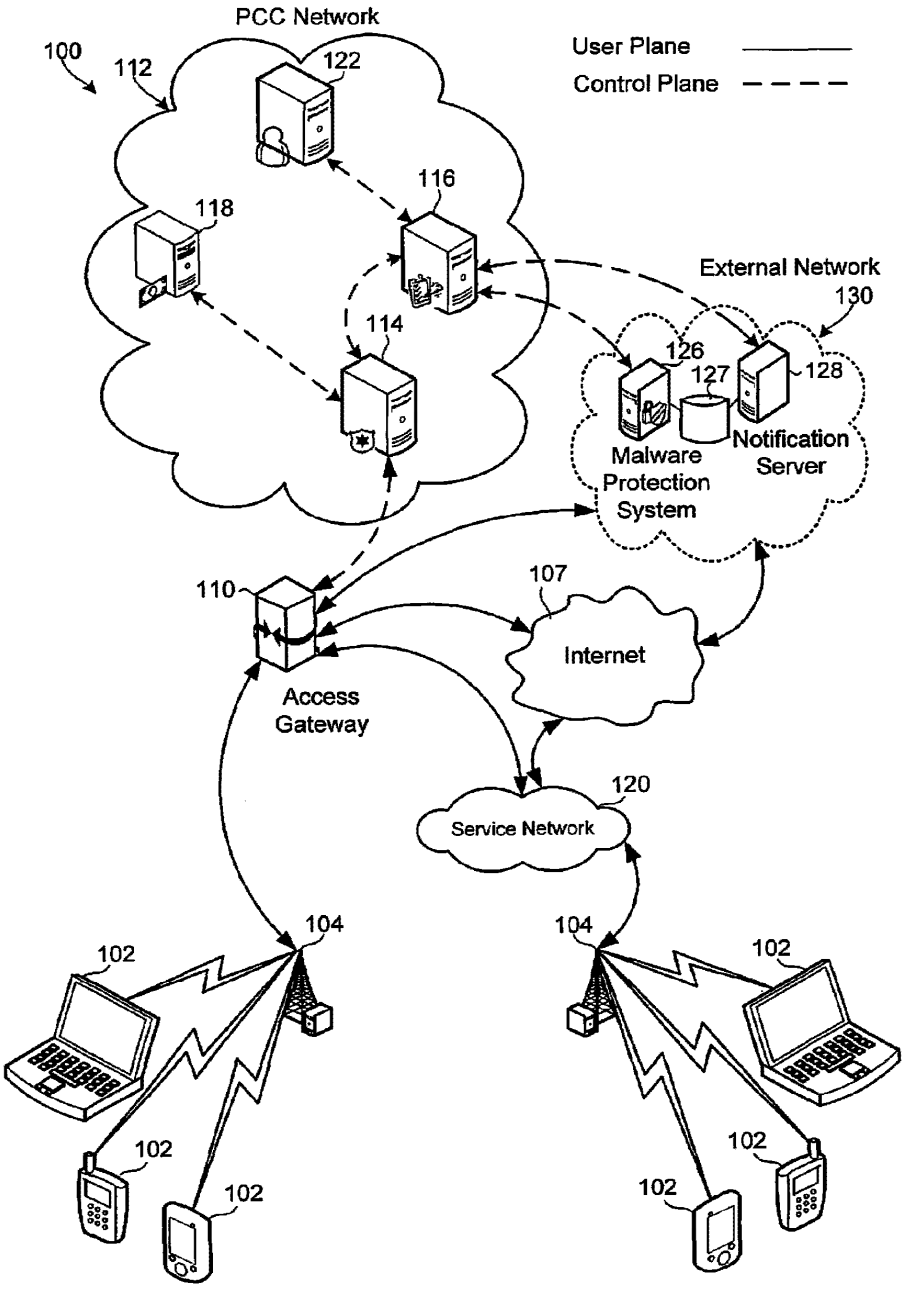


FIG. 2

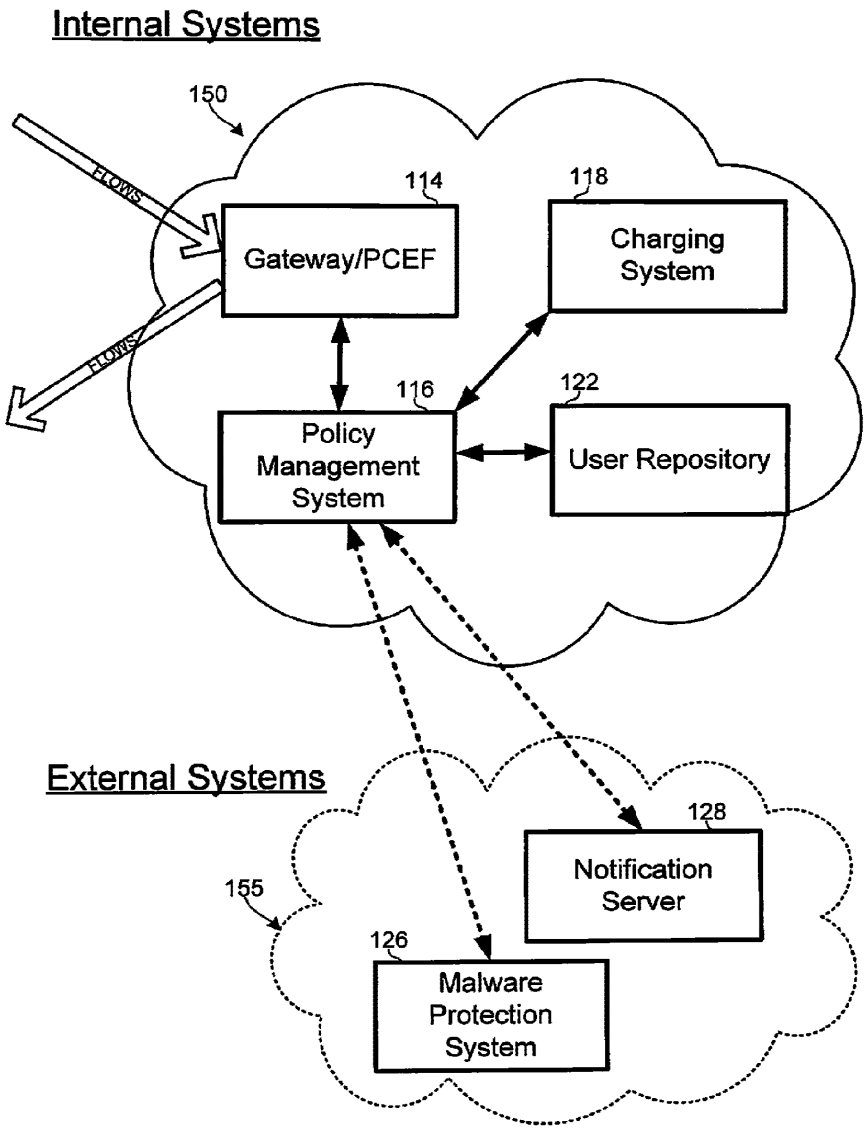


FIG. 3A

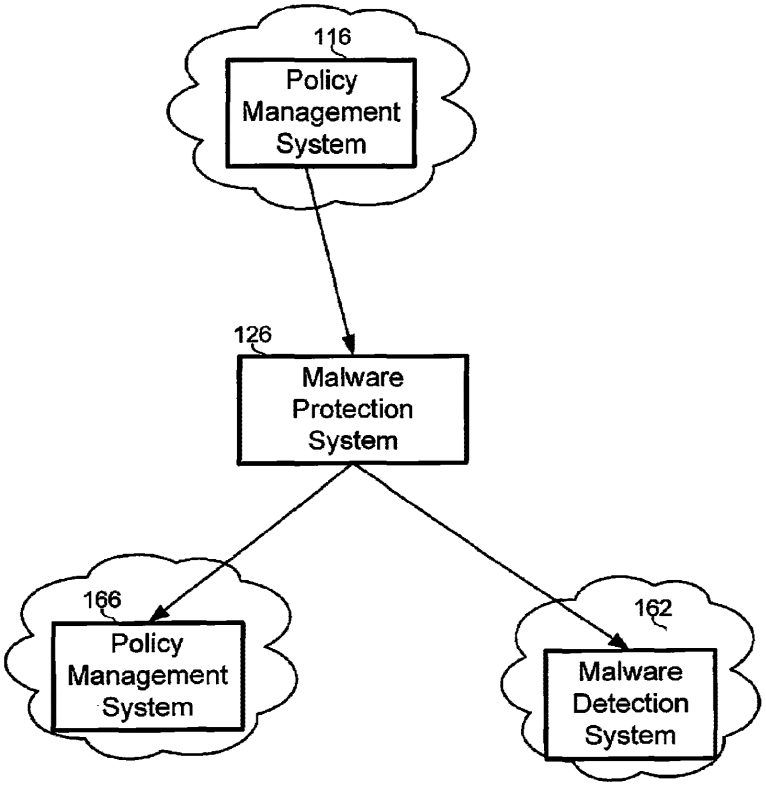


FIG. 3B

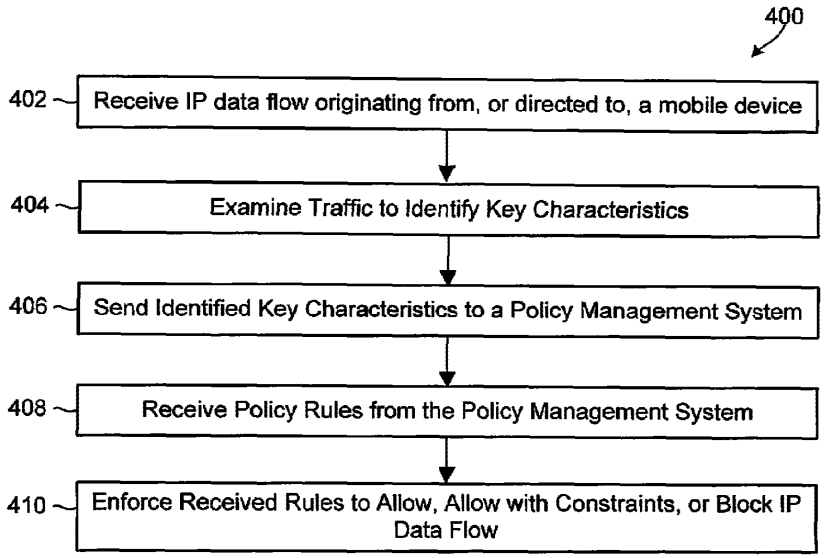


FIG. 4A

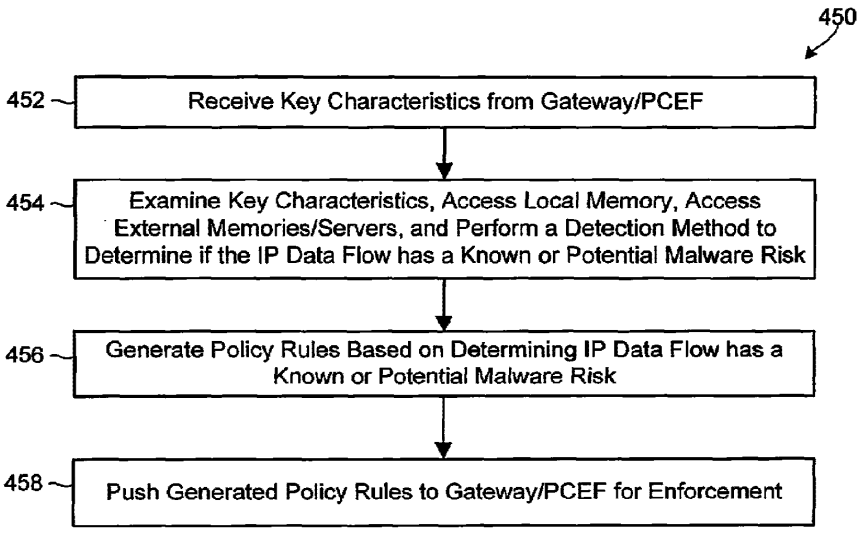


FIG. 4B

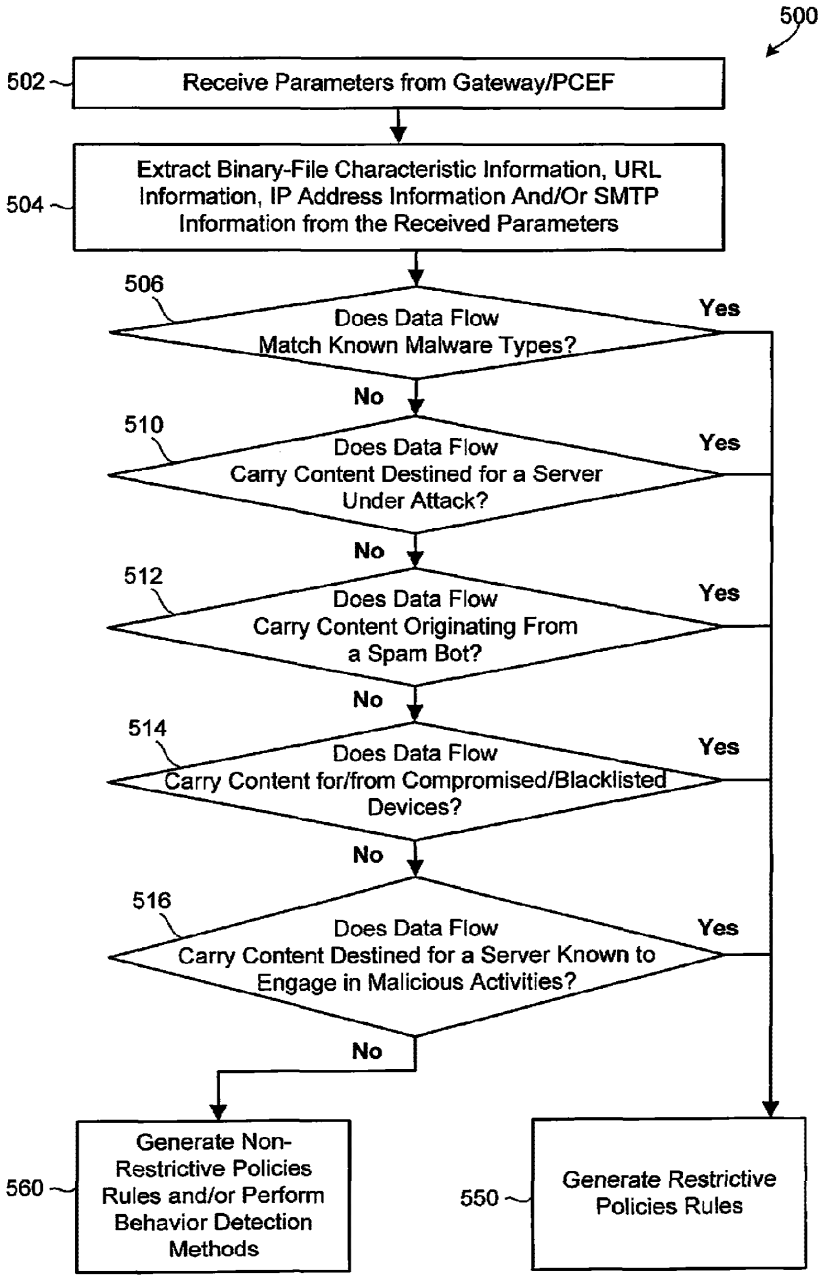


FIG. 5

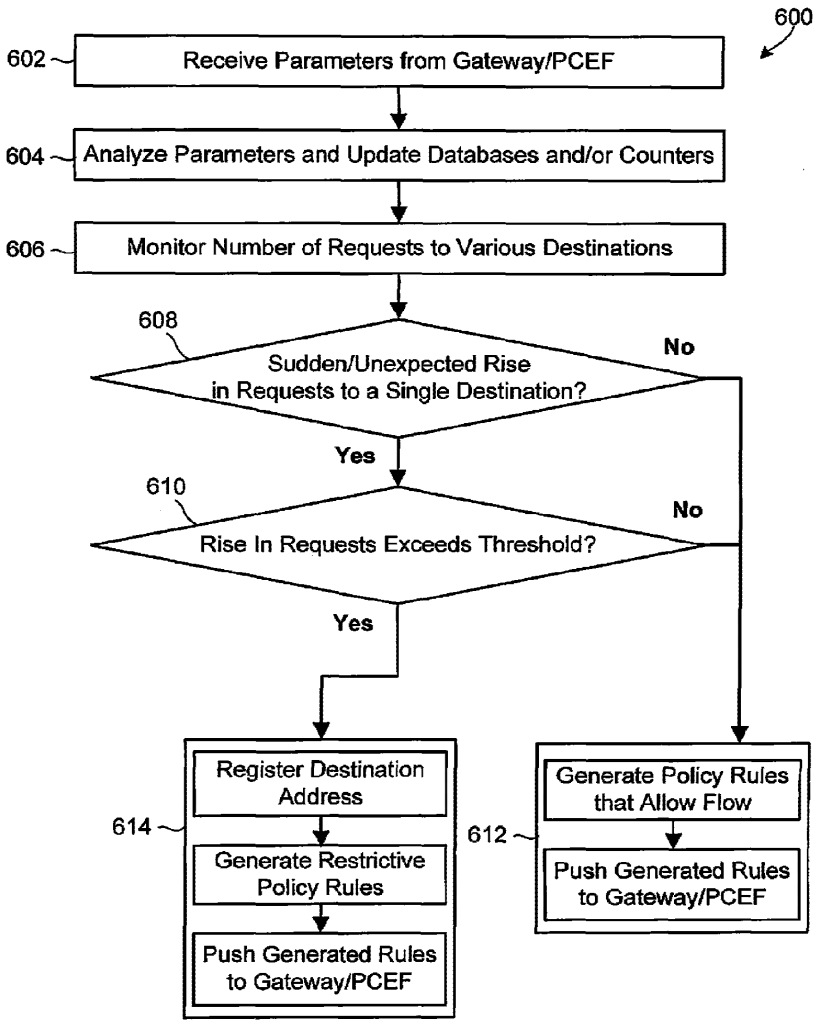


FIG. 6A

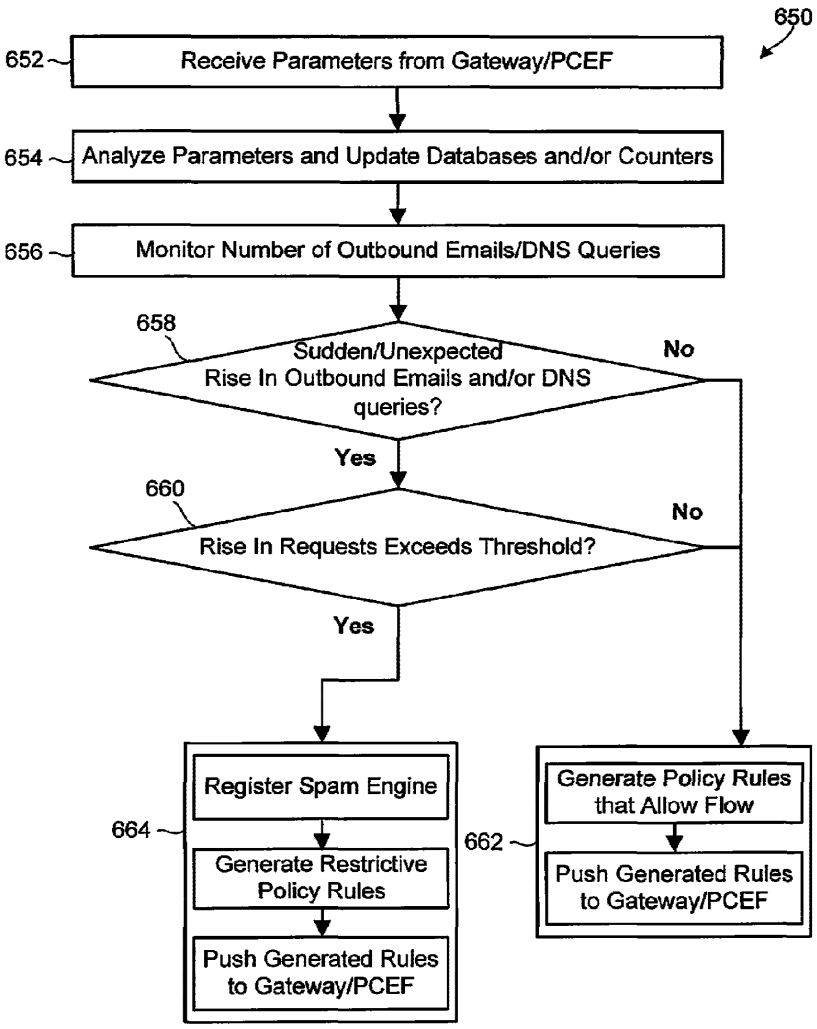


FIG. 6B

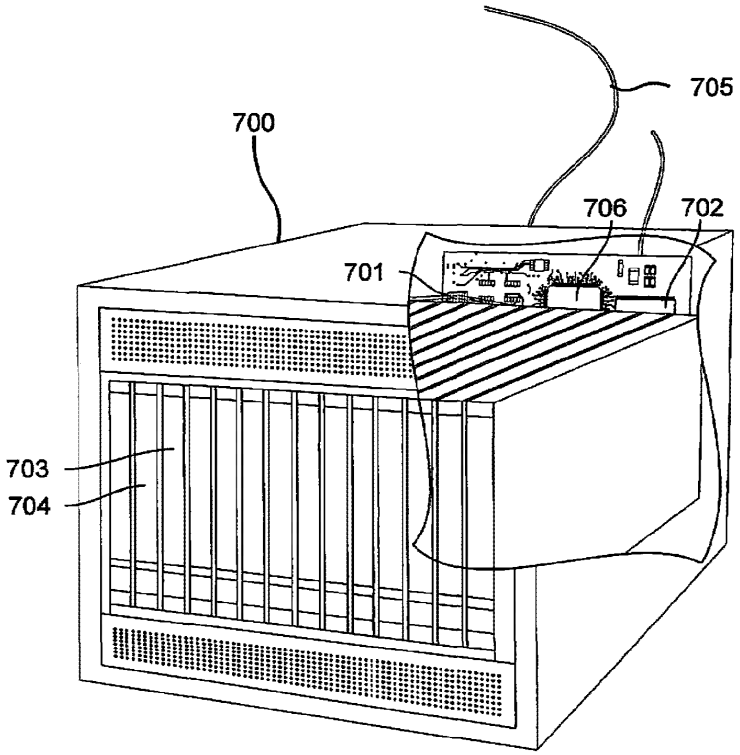


FIG. 7

Europäisches Patentamt
European Patent Office
Office européen des brevets

EUROPEAN SEARCH REPORT

Application Number
EP 12 15 8921

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (IPC)
X	WO 2009/132700 A1 (ERICSSON TELEFON AB L M [SE]; STENFELT JOHN [SE]) 5 November 2009 (2009-11-05) * page 6, lines 4-10 * * page 8, lines 6-10 * * page 15, line 25 - page 17, line 16 * * page 17, lines 29-31 * * claim 12; figures 1,4 *	1-17	INV. H04L12/24 H04L29/06 H04W12/08 H04W12/12 ADD. H04W24/00 H04W88/16
X	US 2004/193912 A1 (LI HONG C [US] ET AL) 30 September 2004 (2004-09-30) * paragraphs [0024], [0039] - [0041] * * figure 3 *	1-17	
A	US 2007/006309 A1 (HERBERT HOWARD C [US] ET AL SMITH NED M [US] ET AL) 4 January 2007 (2007-01-04) * paragraph [0026]; figure 2 *	1-17	
			TECHNICAL FIELDS SEARCHED (IPC) H04L H04W

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
Munich	20 June 2012	Pajatakis, Emmanouil

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 12 15 8921

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

20-06-2012

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 2009132700 A1	05-11-2009	EP 2304915 A1	06-04-2011
		US 2011041182 A1	17-02-2011
		WO 2009132700 A1	05-11-2009
US 2004193912 A1	30-09-2004	CN 1768518 A	03-05-2006
		DE 112004000428 B4	26-11-2009
		DE 112004000428 T5	09-02-2006
		GB 2412540 A	28-09-2005
		JP 2006521598 A	21-09-2006
		JP 2009187587 A	20-08-2009
		KR 20050118223 A	15-12-2005
		TW I253571 B	21-04-2006
		US 2004193912 A1	30-09-2004
		WO 2004095801 A1	04-11-2004
US 2007006309 A1	04-01-2007	TW I323102 B	01-04-2010
		US 2007006309 A1	04-01-2007
		WO 2007002875 A1	04-01-2007

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82

Electronic Acknowledgement Receipt

EFS ID:	19486945
Application Number:	13657010
International Application Number:	
Confirmation Number:	2390
Title of Invention:	METHODS AND SYSTEMS FOR PROTECTING A SECURED NETWORK
First Named Inventor/Applicant Name:	Steven Rogers
Customer Number:	22907
Filer:	William Eugene Wooten/Rocko Bund
Filer Authorized By:	William Eugene Wooten
Attorney Docket Number:	007742.00017
Receipt Date:	03-JUL-2014
Filing Date:	22-OCT-2012
Time Stamp:	10:09:24
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Non Patent Literature	NPL-ISR_dated_260614_16818779.PDF	744984 e1ca96f7cd5b5a2fa2cccc54367d9a3ea7ad69bc	no	11
Warnings:					
Information:					

2	Non Patent Literature	NPL-Moore_16818826.PDF	1932721 7f7362dd6ca63b62d069e3a66279ca0175c2da98	no	9
Warnings:					
Information:					
3	Non Patent Literature	NPL-Cisco_16818946.PDF	2472590 e14c692da0b6acaa6bb75cbae061bdd60efaea86	no	26
Warnings:					
Information:					
4	Information Disclosure Statement (IDS) Form (SB08)	Information_Disclosure_Statement_Fillable_PDF_16819437.PDF	612609 0d71342d63eb7d9b23c1d95a71cff32b4919cbe1	no	4
Warnings:					
Information:					
5	Foreign Reference	EP2385676A1_16818890.PDF	780191 b81189390d037dff528b0afcc8f407a761e32de5	no	17
Warnings:					
Information:					
6	Foreign Reference	EP2498442A1_16818909.PDF	1749069 e86e61d1c020da22685c864e51bdf4c636777f30	no	28
Warnings:					
Information:					
		Total Files Size (in bytes):	8292164		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

<u>New Applications Under 35 U.S.C. 111</u>
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

<u>National Stage of an International Application under 35 U.S.C. 371</u>
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

<u>New International Application Filed with the USPTO as a Receiving Office</u>
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PATENT COOPERATION TREATY

From the INTERNATIONAL SEARCHING AUTHORITY

To:
Wright, Bradley C.
BANNER & WITCOFF, LTD.
1100 13th Street, N.W. Suite 1200
Washington, DC 20005-4051
ETATS-UNIS D'AMERIQUE

PCT

NOTIFICATION OF TRANSMITTAL OF THE INTERNATIONAL SEARCH REPORT AND THE WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY, OR THE DECLARATION

(PCT Rule 44.1)

Applicant's or agent's file reference 007742.00031	Date of mailing *(day/month/year)* 26 June 2014 (26-06-2014) **FOR FURTHER ACTION** See paragraphs 1 and 4 below
International application No. PCT/US2014/027723	International filing date *(day/month/year)* 14 March 2014 (14-03-2014)
Applicant CENTRIPETAL NETWORKS, INC.	

1. [X] The applicant is hereby notified that the international search report and the written opinion of the International Searching Authority have been established and are transmitted herewith.

   Filing of amendments and statement under Article 19:
   The applicant is entitled, if he so wishes, to amend the claims of the International Application (see Rule 46):

   When? The time limit for filing such amendments is normally two months from the date of transmittal of the International Search Report.

   Where? Directly to the International Bureau of WIPO, 34 chemin des Colombettes 1211 Geneva 20, Switzerland, Fascimile No.: (41-22) 338.82.70

   For more detailed instructions, see *PCT Applicant's Guide,* International Phase, paragraphs 9.004 - 9.011.

2. [ ] The applicant is hereby notified that no international search report will be established and that the declaration under Article 17(2)(a) to that effect and the written opinion of the International Searching Authority are transmitted herewith.

3. [ ] **With regard to any protest** against payment of (an) additional fee(s) under Rule 40.2, the applicant is notified that:

   [ ] the protest together with the decision thereon has been transmitted to the International Bureau together with any request to forward the texts of both the protest and the decision thereon to the designated Offices.

   [ ] no decision has been made yet on the protest; the applicant will be notified as soon as a decision is made.

4. **Reminders**

The applicant may submit comments on an informal basis on the written opinion of the International Searching Authority to the International Bureau. The International Bureau will send a copy of such comments to all designated Offices unless an international preliminary examination report has been or is to be established. Following the expiration of 30 months from the priority date, these comments will also be made available to the public.

Shortly after the expiration of **18 months** from the priority date, the international application will be published by the International Bureau. If the applicant wishes to avoid or postpone publication, a notice of withdrawal of the international application, or of the priority claim, must reach the International Bureau before completion of the technical preparations for international publication (Rules 90*bis*.1 and 90*bis*.3).

Within **19 months** from the priority date, but only in respect of some designated Offices, a demand for international preliminary examination must be filed if the applicant wishes to postpone the entry into the national phase **until 30 months** from the priority date (in some Offices even later); otherwise, the applicant must, **within 20 months** from the priority date, perform the prescribed acts for entry into the national phase before those designated Offices.

In respect of other designated Offices, the time limit of **30 months** (or later) will apply even if no demand is filed within 19 months.

For details about the applicable time limits, Office by Office, see www.wipo.int/pct/en/texts/time_limits.html and the *PCT Applicant's Guide*, National Chapters.

Name and mailing address of the International Searching Authority European Patent Office, P.B. 5818 Patentlaan 2 NL-2280 HV Rijswijk Tel. (+31-70) 340-2040 Fax: (+31-70) 340-3016	Authorized officer GOTTAR, Chantal Tel: +49 (0)89 2399-3203

Form PCT/ISA/220 (July 2010)

PATENT COOPERATION TREATY

PCT

INTERNATIONAL SEARCH REPORT

(PCT Article 18 and Rules 43 and 44)

Applicant's or agent's file reference	**FOR FURTHER ACTION**	see Form PCT/ISA/220 as well as, where applicable, item 5 below.
007742.00031		
International application No.	International filing date *(day/month/year)*	(Earliest) Priority Date *(day/month/year)*
PCT/US2014/027723	14 March 2014 (14-03-2014)	15 March 2013 (15-03-2013)
Applicant		
CENTRIPETAL NETWORKS, INC.		

This international search report has been prepared by this International Searching Authority and is transmitted to the applicant according to Article 18. A copy is being transmitted to the International Bureau.

This international search report consists of a total of 4 sheets.

[X] It is also accompanied by a copy of each prior art document cited in this report.

1. **Basis of the report**
   a. With regard to the **language,** the international search was carried out on the basis of:
      [X] the international application in the language in which it was filed
      [ ] a translation of the international application into _____, which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1(b))
   b. [ ] This international search report has been established taking into account the **rectification of an obvious mistake** authorized by or notified to this Authority under Rule 91 (Rule 43.6*bis*(a)).
   c. [ ] With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, see Box No. I.

2. [ ] **Certain claims were found unsearchable** (See Box No. II)

3. [ ] **Unity of invention is lacking** (see Box No III)

4. With regard to the **title,**
   [X] the text is approved as submitted by the applicant
   [ ] the text has been established by this Authority to read as follows:

5. With regard to the **abstract,**
   [X] the text is approved as submitted by the applicant
   [ ] the text has been established, according to Rule 38.2, by this Authority as it appears in Box No. IV. The applicant may, within one month from the date of mailing of this international search report, submit comments to this Authority

6. With regard to the **drawings,**
   a. the figure of the **drawings** to be published with the abstract is Figure No. 1
      [X] as suggested by the applicant
      [ ] as selected by this Authority, because the applicant failed to suggest a figure
      [ ] as selected by this Authority, because this figure better characterizes the invention
   b. [ ] none of the figures is to be published with the abstract

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2014/027723

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L29/06
ADD.

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
EPO-Internal, WPI Data, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2006/048142 A1 (ROESE JOHN J [US] ET AL) 2 March 2006 (2006-03-02) figures 1-4 paragraph [0002] - paragraph [0027] paragraph [0037] - paragraph [0042] paragraph [0046] - paragraph [0058] ----- -/--	1-20

[X] Further documents are listed in the continuation of Box C.

[X] See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
13 June 2014	26/06/2014

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Olaechea, Javier

1

Form PCT/ISA/210 (second sheet) (April 2005)

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	Sean Moore: "SBIR Case Study: Centripetal Networks Subtitle: How CNI Leveraged DHS S&T SBIR Funding to Launch a Successful Cyber Security Company Cyber Security Division 2012 Principal Investigators' Meeting 10-October-2012", , 10 October 2012 (2012-10-10), XP055122227, Retrieved from the Internet: URL:http://www.dhs.gov/sites/default/files/publications/csd-day-2-04-sbir-centripetal-price.pdf [retrieved on 2014-06-06] the whole document	1-20
A	EP 2 385 676 A1 (ALCATEL LUCENT [FR]; INST TELECOM TELECOM BRETAGNE [FR]) 9 November 2011 (2011-11-09) paragraph [0044] - paragraph [0059]	1-20
A	EP 2 498 442 A1 (OPENET TELECOM LTD [IE]) 12 September 2012 (2012-09-12) paragraph [0053] - paragraph [0079]	1-20
A	Cisco: "Control Plane Policing Implementation Best Practices", , 13 March 2013 (2013-03-13), XP002725728, Retrieved from the Internet: URL:https://web.archive.org/web/20130313135143/http://www.cisco.com/web/about/security/intelligence/coppwp_gs.html [retrieved on 2014-06-12] the whole document	1-20
A	US 2010/011434 A1 (KAY RONY [US]) 14 January 2010 (2010-01-14) paragraph [0034] - paragraph [0045]	1-20

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/US2014/027723

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2006048142 A1	02-03-2006	NONE	
EP 2385676 A1	09-11-2011	CN 102934122 A	13-02-2013
		EP 2385676 A1	09-11-2011
		JP 2013525927 A	20-06-2013
		KR 20130005301 A	15-01-2013
		US 2013111548 A1	02-05-2013
		WO 2011138417 A1	10-11-2011
EP 2498442 A1	12-09-2012	EP 2498442 A1	12-09-2012
		US 2012233656 A1	13-09-2012
US 2010011434 A1	14-01-2010	NONE	

Form PCT/ISA/210 (patent family annex) (April 2005)

PATENT COOPERATION TREATY

From the
INTERNATIONAL SEARCHING AUTHORITY

To:

see form PCT/ISA/220

PCT

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY
(PCT Rule 43*bis*.1)

Date of mailing
(day/month/year) see form PCT/ISA/210 (second sheet)

Applicant's or agent's file reference
see form PCT/ISA/220

FOR FURTHER ACTION
See paragraph 2 below

International application No.	International filing date *(day/month/year)*	Priority date *(day/month/year)*
PCT/US2014/027723	14.03.2014	15.03.2013

International Patent Classification (IPC) or both national classification and IPC
INV. H04L29/06

Applicant
CENTRIPETAL NETWORKS, INC.

1. This opinion contains indications relating to the following items:

- ☒ Box No. I Basis of the opinion
- ☐ Box No. II Priority
- ☐ Box No. III Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- ☐ Box No. IV Lack of unity of invention
- ☒ Box No. V Reasoned statement under Rule 43*bis*.1(a)(i) with regard to novelty, inventive step and industrial applicability; citations and explanations supporting such statement
- ☐ Box No. VI Certain documents cited
- ☒ Box No. VII Certain defects in the international application
- ☐ Box No. VIII Certain observations on the international application

2. **FURTHER ACTION**

If a demand for international preliminary examination is made, this opinion will usually be considered to be a written opinion of the International Preliminary Examining Authority ("IPEA") except that this does not apply where the applicant chooses an Authority other than this one to be the IPEA and the chosen IPEA has notifed the International Bureau under Rule 66.1*bis*(b) that written opinions of this International Searching Authority will not be so considered.

If this opinion is, as provided above, considered to be a written opinion of the IPEA, the applicant is invited to submit to the IPEA a written reply together, where appropriate, with amendments, before the expiration of 3 months from the date of mailing of Form PCT/ISA/220 or before the expiration of 22 months from the priority date, whichever expires later.

For further options, see Form PCT/ISA/220.

Name and mailing address of the ISA:	Date of completion of this opinion	Authorized Officer
European Patent Office D-80298 Munich Tel. +49 89 2399 - 0 Fax: +49 89 2399 - 4465	see form PCT/ISA/210	Olaechea, Javier Telephone No. +49 89 2399-8233

Form PCT/ISA/237 (Cover Sheet) (July 2009)

Box No. I Basis of the opinion

1. With regard to the **language**, this opinion has been established on the basis of:

   ☒ the international application in the language in which it was filed

   ☐ a translation of the international application into , which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1 (b)).

2. ☐ This opinion has been established taking into account the **rectification of an obvious mistake** authorized by or notified to this Authority under Rule 91 (Rule 43bis.1(a))

3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, this opinion has been established on the basis of a sequence listing filed or furnished:

   a. (means)

      ☐ on paper

      ☐ in electronic form

   b. (time)

      ☐ in the international application as filed

      ☐ together with the international application in electronic form

      ☐ subsequently to this Authority for the purposes of search

4. ☐ In addition, in the case that more than one version or copy of a sequence listing has been filed or furnished, the required statements that the information in the subsequent or additional copies is identical to that in the application as filed or does not go beyond the application as filed, as appropriate, were furnished.

5. Additional comments:

Box No. V Reasoned statement under Rule 43*bis*.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Yes:	Claims	
	No:	Claims	1-20
Inventive step (IS)	Yes:	Claims	
	No:	Claims	1-20
Industrial applicability (IA)	Yes:	Claims	1-20
	No:	Claims	

2. Citations and explanations

see separate sheet

Box No. VII Certain defects in the international application

The following defects in the form or contents of the international application have been noted:

see separate sheet

Re Item V

Reasoned statement with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1 Reference is made to the following document:

D1 US 2006/048142 A1 (ROESE JOHN J [US] ET AL) 2 March 2006 (2006-03-02)

D2 Sean Moore: "SBIR Case Study: Centripetal Networks Subtitle: How CNI Leveraged DHS S&T SBIR Funding to Launch a Successful Cyber Security Company Cyber Security Division 2012 Principal Investigators' Meeting 10-October-2012", , 10 October 2012 (2012-10-10), XP055122227, Retrieved from the Internet: URL:http://www.dhs.gov/sites/default/files/publications/csd-day-2-04-sbir-centripetal-price.pdf [retrieved on 2014-06-06]

D3 Cisco: "Control Plane Policing Implementation Best Practices", , 13 March 2013 (2013-03-13), XP002725728, Retrieved from the Internet: URL:https://web.archive.org/web/20130313135143/http://www.cisco.com/web/about/security/intelligence/coppwp_gs.html [retrieved on 2014-06-12]

2 The present application does not meet the criteria of Article 33(1) PCT, because the subject-matter of claims 1, 11 and 16 is not new in the sense of Article 33(2) PCT.

2.1 The document D1 discloses (the references in parentheses applying to this document) in terms of claim 1:

A method, comprising:

at a computing platform comprising at least one processor, memory, and communication interface (*network device in Figures 1 and 2*):

receiving, via the communication interface, a plurality of packets (paragraph 55; *traffic is received by the network device*);
responsive to a determination that an overload condition has occurred in one or more networks associated with the computing platform, applying, by the processor and to at least some of the plurality of packets, a first group of packet-filtering rules that comprises at least one five-tuple indicating a first set of packets that should be allowed to continue toward their respective destinations, wherein applying the first group of packet-filtering rules includes allowing at least a first portion of the plurality of packets that fall within the first set of packets to continue toward their respective destinations (paragraphs 24, 56 and table in pages 9-10; *in response to an attack trigger, a rule set is activated by the network device, said rule set including disabling all traffic excluding the management traffic, RR1*); and

responsive to a determination that the overload condition has been mitigated to a first degree, applying, to at least some of the plurality of packets, a second group of packet-filtering rules that comprises at least one five-tuple indicating a second set of packets that should be allowed to continue toward their respective destinations, wherein applying the second group of packet-filtering rules includes allowing at least a second portion of the plurality of packets that fall within the second set of packets to continue toward their respective destinations, and wherein the second group of packet-filtering rules is less restrictive than the first group of packet-filtering rules (paragraph 24; *upon detection of a new triggering condition, a less restrictive set of filtering rules is implemented by the networking device*).

Since all the features of claim 1 are known in combination from document D1, the subject-matter of claim 1 is not new (Article 33(2) PCT). Therefore, claim 1 is not allowable (Article 33(1) PCT).

2.2 The same reasoning applies, mutatis mutandis, to the subject-matter of the corresponding independent claims 11 and 16, which therefore are also considered not new (Article 33(2) PCT).

2.3 Furthermore, it is noted that the disclosure of document D2 (see page 4) would also render the subject-matter of claims 1, 11 and 16 not new or at least not inventive.

3 None of the dependent claims 2-10, 12-15 and 17-20 contain additional features which lead the subject-matter to be both new and inventive (see documents D1-D3 and the corresponding passages cited in the search report).

Re Item VII

Certain defects in the international application

The independent claims are not in the two-part form in accordance with Rule 6.3(b) PCT, which in the present case would be appropriate, with those features known in combination from the prior art being placed in the preamble (Rule 6.3(b)(i) PCT) and with the remaining features being included in the characterising part (Rule 6.3(b)(ii) PCT).

The features of the claims are not provided with reference signs placed in parentheses (Rule 6.2(b) PCT).

The description is not in conformity with the claims as required by Rule 5.1(a)(iii) PCT.

Contrary to the requirements of Rule 5.1(a)(ii) PCT, the relevant background art disclosed in the documents D1-D3 is not mentioned in the description, nor are these documents identified therein.

PTO/SB/08a (01-10)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**		
	Application Number	13657010
	Filing Date	2012-10-22
	First Named Inventor	Steven Rogers
	Art Unit	2438
	Examiner Name	Chang, Kenneth W.
	Attorney Docket Number	007742.00017

U.S.PATENTS						Remove
Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	7721084		2010-05-18	Salminen et al.	
	2	7684400		2010-03-23	Govindarajan et al.	
If you wish to add additional U.S. Patent citation information please click the Add button.						Add
U.S.PATENT APPLICATION PUBLICATIONS						Remove
Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20120113987	A1	2012-05-10	Riddoch et al.	
	2	20110270956	A1	2011-11-03	McDysan et al.	
	3	20100211678	A1	2010-08-19	McDysan et al.	
	4	20050117576		2005-06-02	McDysan et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13657010
	Filing Date	2012-10-22
	First Named Inventor	Steven Rogers
	Art Unit	2438
	Examiner Name	Chang, Kenneth W.
	Attorney Docket Number	007742.00017

	5	20040151155	A1	2004-08-05	Jouppi	
	6	20030212900	A1	2003-11-13	Liu et al.	
	7	20030188192	A1	2003-10-02	Tang et al.	
	8	20120264443	A1	2012-10-18	Ng et al.	
	9	20130059527	A1	2013-03-07	HASESAKA et al.	

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							☐

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1		☐

If you wish to add additional non-patent literature document citation information please click the Add button Add

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13657010
	Filing Date	2012-10-22
	First Named Inventor	Steven Rogers
	Art Unit	2438
	Examiner Name	Chang, Kenneth W.
	Attorney Docket Number	007742.00017

EXAMINER SIGNATURE			
Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**		
	Application Number	13657010
	Filing Date	2012-10-22
	First Named Inventor	Steven Rogers
	Art Unit	2438
	Examiner Name	Chang, Kenneth W.
	Attorney Docket Number	007742.00017

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☐ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

☐ See attached certification statement.

☐ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/William E. Wooten/	Date (YYYY-MM-DD)	2014-09-09
Name/Print	William E. Wooten	Registration Number	60049

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Electronic Acknowledgement Receipt

EFS ID:	20086683
Application Number:	13657010
International Application Number:	
Confirmation Number:	2390
Title of Invention:	METHODS AND SYSTEMS FOR PROTECTING A SECURED NETWORK
First Named Inventor/Applicant Name:	Steven Rogers
Customer Number:	22907
Filer:	William Eugene Wooten
Filer Authorized By:	
Attorney Docket Number:	007742.00017
Receipt Date:	09-SEP-2014
Filing Date:	22-OCT-2012
Time Stamp:	14:35:21
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Information Disclosure Statement (IDS) Form (SB08)	IDS.pdf	612539 1826f43d3505977ff882364a61d14b72fa0f4271	no	5
Warnings:					
Information:					

Total Files Size (in bytes):	612539

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/657,010	10/22/2012	Steven Rogers	007742.00017	2390

22907 7590 10/21/2014

BANNER & WITCOFF, LTD.
1100 13th STREET, N.W.
SUITE 1200
WASHINGTON, DC 20005-4051

EXAMINER	
CHANG, KENNETH W	
ART UNIT	**PAPER NUMBER**
2438	
MAIL DATE	**DELIVERY MODE**
10/21/2014	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

PTOL-90A (Rev. 04/07)

Office Action Summary	Application No. 13/657,010	Applicant(s) ROGERS ET AL.	
	Examiner KENNETH CHANG	Art Unit 2438	AIA (First Inventor to File) Status No

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTHS FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *10/22/2012*.

☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

4)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims*

5)☒ Claim(s) *1-22* is/are pending in the application.

5a) Of the above claim(s) _____ is/are withdrawn from consideration.

6)☐ Claim(s) _____ is/are allowed.

7)☒ Claim(s) *1-6,8,9 and 11-22* is/are rejected.

8)☒ Claim(s) *7 and 10* is/are objected to.

9)☐ Claim(s) _____ are subject to restriction and/or election requirement.

* If any claims have been determined allowable, you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to PPHfeedback@uspto.gov.

Application Papers

10)☐ The specification is objected to by the Examiner.

11)☒ The drawing(s) filed on *10/22/2012* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

Certified copies:

a)☐ All b)☐ Some** c)☐ None of the:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

** See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☒ Information Disclosure Statement(s) (PTO/SB/08a and/or PTO/SB/08b) Paper No(s)/Mail Date *12/13/2012, 12/02/2013, 06/25/2014, 06/27/2014, 07/03/2014, and 09/09/2014*.

3) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .

4) ☐ Other: _____.

DETAILED ACTION

1. This first non-final action is in response to applicants' filing on 10/22/2012.

Claims 1-22 are pending and have been considered as follows.

Notice of Pre-AIA or AIA Status

2. The present application is being examined under the pre-AIA first to invent provisions.

Drawings

3. The drawings filed on 10/22/2012 are accepted.

Information Disclosure Statement

4. The information disclosure statements (IDS) submitted on 12/13/2012, 12/02/2013, 06/25/2014, 06/27/2014, 07/03/2014, and 09/09/2014 have been placed in the application file, and the information referred therein has been considered as to the merits.

Claim Rejections - 35 USC § 102

5. The following is a quotation of the appropriate paragraphs of pre-AIA 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

6. **Claims 1, 11, 12, 14, 15, and 18-21** are rejected under pre-AIA 35 U.S.C. 102(b) as being anticipated by Iyer et al. (US 20050138204 A1, hereinafter **Iyer**).

As to Claim 1:

Iyer discloses a method **(e.g. method for configuration and management of virtual private networks Iyer [0002])**, comprising:

- at each of one or more packet security gateways **(e.g. policy enforcers Iyer [0045]-[0046]; [0126]; where Applicants define in the originally filed Specification on page 6 at paragraph [33]: "*As used herein, a packet security gateway includes any computing device configured to receive packets and perform a packet transformation function on the packets*")** associated with a security policy management server **(e.g. policy server defining managing network services and policies for the organization Iyer [0045])**:
- receiving a dynamic security policy **(e.g. define network policy, firewall policy for policy enforcers in different locations Iyer [0045]; [0046]; [0060]; [0062]; modified policy [0076]; [0086])** from the security policy management server **(e.g. policy server includes management module Iyer [0062])**;
- receiving packets associated with a network protected **(e.g. network traffic [0087]-[0089]; receiving traffic flow of packets [0103]; incoming packets [0126])** by each respective packet security gateway **(e.g. policy enforcer [0126])**; and
- performing, on a packet by packet basis **(e.g. packet policies enforced Iyer [0126])**, at least one of multiple packet transformation functions **(e.g. performing IPSec security and authentication functions, decode protocols in packets,**

buffers packets based on policies being enforced, provide bandwidth shaping services to the packets Iyer [0126]) specified by the dynamic security policy **(e.g. policy settings stored in the policy database [0126])** on the packets, wherein performing the at least one of multiple packet transformation functions specified by the dynamic security policy on the packets comprises performing at least one packet transformation function **(e.g. performing IPSec security and authentication functions, decode protocols in packets, buffers packets based on policies being enforced, provide bandwidth shaping services to the packets Iyer [0126]; storing packet 5-tuple values in stream table, such as source IP, destination IP, source port, destination port, protocol number of incoming packet [0127]; processing the packets based on the policy rules [0128])** other than forwarding or dropping the packets.

As to Claim 11:

Iyer discloses the method of claim 1, wherein the at least one of the multiple packet transformation functions comprises at least **one of** forwarding the packets into the network protected by the packet security gateway **(e.g. forwarding the packets by policy enforcer to local network protected Iyer [0043]; [0126])**, forwarding the packets out of the network protected by the packet security gateway, forwarding the packets to an Internet Protocol Security (IPsec) stack having an IPsec security association corresponding to the packets, and dropping the packets **(e.g. drop the packets based on the policies being enforced Iyer [0126])**.

As to Claim 12:

Iyer discloses the method of claim 1, wherein the dynamic security policy comprises a plurality of rules **(e.g. network policies are a set of rules Iyer [0045]; [0128])**, and wherein at least one of the rules specifies a five-tuple **(e.g. incoming packets are matched against stream table in enforcing policies Iyer [0127])**, the five-tuple specifying one or more protocols **(e.g. protocol number Iyer [0127])**, one or more IP source addresses **(e.g. source IP Iyer [0127])**, one or more source port values **(e.g. source port Iyer [0127])**, one or more IP destination addresses **(e.g. destination IP Iyer [0127])**, and one or more destination port values **(e.g. destination port Iyer [0127]) (e.g. performing IPSec security and authentication functions, decode protocols in packets, buffers packets based on policies being enforced, provide bandwidth shaping services to the packets Iyer [0126]; storing packet 5-tuple values in stream table, such as source IP, destination IP, source port, destination port, protocol number of incoming packet [0127]; processing the packets based on the policy rules [0128])**.

As to Claim 14:

Iyer discloses the method of claim 1, wherein at least one of the one or more packet security gateways operates in a network layer transparent manner **(e.g. policy is enforced on policy enforces in different locations transparently Iyer [0060]; [0076])** by sending and receiving traffic at a link layer using an interface **(e.g. common gateway interface Iyer [0073]; [0118])** that is not addressed at the network layer and performing the at least one of the multiple packet transformation functions at the

network layer **(e.g. performing IPSec security and authentication functions, decode protocols in packets, buffers packets based on policies being enforced, provide bandwidth shaping services to the packets Iyer [0126])**.

As to Claim 15:

Iyer discloses the method of claim 14, wherein the at least one of the one or more packet security gateways **(e.g. policy enforcers Iyer [0070])** includes a management interface **(e.g. interactive user interface Iyer [0070])** having a network layer address **(e.g. access to wizard is web-based using network administrator's personal computer Iyer [0070]; [0071])**, and wherein access to the management interface is secured at at least one of an application level **(e.g. authentication for access to administrative functions Iyer [0045]; [0053]; login [0078]; [0121])**, a link level, and a transport level.

As to Claim 18:

Iyer discloses the method of claim 1, wherein at least one of the one or more packet security gateways **(e.g. policy enforcer is an edge device coupled to private network Iyer [0008]; [0046]; [0056])** is located at each boundary **(e.g. FIG. 1)** between a protected network associated with the security policy management server and an unprotected network **(e.g. public network, public Internet Iyer [0043]; [0045])**.

As to Claim 19:

Iyer discloses a system **(e.g. FIG. 1 Iyer [0002])**, comprising:

- a security policy management server **(e.g. policy server defining managing network services and policies for the organization Iyer [0045])**; and
- one or more packet security gateways **(e.g. policy enforcers Iyer [0045]-[0046]; [0126]; where Applicants define in the originally filed Specification on page 6 at paragraph [33]: "*As used herein, a packet security gateway includes any computing device configured to receive packets and perform a packet transformation function on the packets*")** associated with the security policy management server **(e.g. managed by policy server Iyer [0046])**, wherein each of the one or more packet security gateways is configured to:
- receive a dynamic security policy **(e.g. define network policy, firewall policy for policy enforcers in different locations Iyer [0045]; [0046]; [0060]; [0062]; modified policy [0076]; [0086])** from the security policy management server **(e.g. policy server includes management module Iyer [0062])**;
- receive packets associated with a network protected **(e.g. network traffic [0087]-[0089]; receiving traffic flow of packets [0103]; incoming packets [0126])** by each respective packet security gateway **(e.g. policy enforcer [0126])**; and
- perform, on a packet by packet basis **(e.g. packet policies enforced Iyer [0126])**, at least one of multiple packet transformation functions **(e.g. performing IPSec security and authentication functions, decode protocols in packets,**

buffers packets based on policies being enforced, provide bandwidth shaping services to the packets Iyer [0126]) specified by the dynamic security policy **(e.g. policy settings stored in the policy database [0126])** on the packets, wherein each of the one or more packet security gateways is configured to perform the at least one of multiple packet transformation functions specified by the dynamic security policy on the packets by performing at least one packet transformation function **(e.g. policy enforcer performs IPSec security and authentication functions, decode protocols in packets, buffers packets based on policies being enforced, provide bandwidth shaping services to the packets Iyer [0126]; storing packet 5-tuple values in stream table, such as source IP, destination IP, source port, destination port, protocol number of incoming packet [0127]; processing the packets based on the policy rules [0128])** other than forwarding or dropping the packets.

As to Claim 20:

Iyer discloses one or more non-transitory computer-readable media **(e.g. policy routers' memory Iyer [0047]; devices' memory [0056])** having instructions stored **(e.g. IPSec engine, policy engine, classification engine, module Iyer [0126])** thereon, that when executed by one or more computers **(e.g. router Iyer [0047]; device [0056])**, cause the one or more computers to:

- at each of one or more packet security gateways **(e.g. policy enforcers Iyer [0045]-[0046]; [0126]; where Applicants define in the originally filed Specification on page 6 at paragraph [33]: "*As used herein, a packet***

***security gateway includes any computing device configured to receive packets and perform a packet transformation function on the packets*")** associated with a security policy management server **(e.g. policy server defining managing network services and policies for the organization lyer [0045])**:

- receive a dynamic security policy **(e.g. define network policy, firewall policy for policy enforcers in different locations lyer [0045]; [0046]; [0060]; [0062]; modified policy [0076]; [0086])** from the security policy management server **(e.g. policy server includes management module lyer [0062])**;
- receive packets associated with a network protected **(e.g. network traffic [0087]-[0089]; receiving traffic flow of packets [0103]; incoming packets [0126])** by each respective packet security gateway **(e.g. policy enforcer [0126])**; and
- perform, on a packet by packet basis **(e.g. packet policies enforced lyer [0126])**, at least one of multiple packet transformation functions **(e.g. performing IPSec security and authentication functions, decode protocols in packets, buffers packets based on policies being enforced, provide bandwidth shaping services to the packets lyer [0126])** specified by the dynamic security policy **(e.g. policy settings stored in the policy database [0126])** on the packets, wherein each of the one or more packet security gateways is configured to perform the at least one of multiple packet transformation functions specified by the dynamic security policy on the packets by performing at least one packet

transformation function **(e.g. policy enforcer performs IPSec security and authentication functions, decode protocols in packets, buffers packets based on policies being enforced, provide bandwidth shaping services to the packets Iyer [0126]; storing packet 5-tuple values in stream table, such as source IP, destination IP, source port, destination port, protocol number of incoming packet [0127]; processing the packets based on the policy rules [0128])** other than forwarding or dropping the packets.

As to Claim 21:

Iyer discloses a method **(e.g. method for configuration and management of virtual private networks Iyer [0002])**, comprising:

- at each of one or more packet security gateways **(e.g. policy enforcers Iyer [0045]-[0046]; [0126]; where Applicants define in the originally filed Specification on page 6 at paragraph [33]: "*As used herein, a packet security gateway includes any computing device configured to receive packets and perform a packet transformation function on the packets*")** associated with a security policy management server **(e.g. policy server defining managing network services and policies for the organization Iyer [0045])**:
- receiving a dynamic security policy **(e.g. define network policy, firewall policy for policy enforcers in different locations Iyer [0045]; [0046]; [0060]; [0062]; modified policy [0076]; [0086])** from the security policy management server **(e.g. policy server includes management module Iyer [0062])**;

- receiving packets associated with a network protected **(e.g. network traffic [0087]-[0089]; receiving traffic flow of packets [0103]; incoming packets [0126])** by each respective packet security gateway **(e.g. policy enforcer [0126])**; and
- performing, on a packet by packet basis **(e.g. packet policies enforced lyer [0126])**, at least one of multiple packet transformation functions **(e.g. performing IPSec security and authentication functions, decode protocols in packets, buffers packets based on policies being enforced, provide bandwidth shaping services to the packets lyer [0126])** specified by the dynamic security policy **(e.g. policy settings stored in the policy database lyer [0126])** on the packets, wherein performing the at least one of multiple packet transformation functions specified by the dynamic security policy on the packets comprises dropping a portion of the packets **(e.g. policy enforcer drops packets based on the policies being enforced lyer [0126])** and forwarding a portion of the packets **(e.g. packet forwarding module forwards the packets based on the policies being enforced lyer [0126])** toward their respective destinations **(e.g. destination IP address lyer [0139])**.

Claim Rejections - 35 USC § 103

7. The following is a quotation of pre-AIA 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which

> said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8. This application currently names joint inventors. In considering patentability of the claims under pre-AIA 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of pre-AIA 35 U.S.C. 103(c) and potential pre-AIA 35 U.S.C. 102(e), (f) or (g) prior art under pre-AIA 35 U.S.C. 103(a).

9. **Claims 2 and 3** are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over **Iyer** in view of **Ahn** (US 20110055916 A1, IDS submitted 12/13/2012).

As to Claim 2:

Iyer discloses the method of claim 1, but does not specifically disclose:

- wherein the one or more packet security gateways comprise at least two packet security gateways *configured in series* such *that packets forwarded* from a first of the at least two packet security gateways *are received by a second* of the at least two packet security gateways.

However, the analogous art **Ahn** does disclose wherein the one or more packet security gateways comprise at least two packet security gateways **(e.g. plural firewall processors [0021]; in separate firewalls [0025])** configured in series **(e.g. pipelined manner [0021])** such that packets forwarded from a first of the at least two packet

security gateways are received by a second **(e.g. FIG. 2; FIG. 3; FIG. 4; [0021]; [0023])** of the at least two packet security gateways. **Iyer** and **Ahn** are analogous art because they are from the same field of endeavor in policy rule processing of network packets.

- (e.g. see **Ahn**, "FIG. 2 is a block diagram illustrating an exemplary pipelined approach where rules and different subsets are distributed across plural firewall processors for processing packets in a pipelined manner… Because the rules in different subsets are distributed across plural processors in a pipeline manner, packet filtering efficiency is improved over a single-processor approach because the different processors can simultaneously apply rules to different packets" **[0021]**; see also "In yet another embodiment, rule subset identifier/rule sorter 106 may distribute the grouped, sorted rules across firewall processors such that a combination of pipelined and function parallel processing techniques are used. FIG. 5 illustrates an example where firewalls 500, 502, 504, and 506 each include separate processors 508, 510, 512, and 514 for applying their respective packet filters" **[0025]**).

At the time of applicants' invention, it would have been obvious to one of ordinary skill in the art, having the teachings of **Iyer** and **Ahn** before him or her, to modify the firewall policy enforcer system of **Iyer** with the teachings of **Ahn** to include *wherein the one or more packet security gateways comprise at least two packet security gateways configured in series such that packets forwarded from a first of the at least two packet security gateways are received by a second of the at least two packet security gateways* as claimed because **Iyer**'s policy enforcer system already provides centralized

management of policy enforcers with network processing functions **(Iyer [0045]-[0046]; [0126]-[0128])** which could be configured in a pipelined manner for processing packets **(Ahn [0021]; [0025])**. The suggestion/motivation for doing so would have been to improve packet filtering efficiency and achieve greater performance **(Ahn [0006]; [0021])**. Therefore, it would have been obvious to combine **Iyer** and **Ahn** to obtain the invention as specified in the instant claim(s).

As to Claim 3:

Iyer in view of **Ahn** discloses the method of claim 2, wherein the dynamic security policy comprises at least two rules **(e.g. network policies are set of rules Iyer [0045])**, a second of the at least two rules being required to execute subsequent **(e.g. sequence processing of one rule at a time Iyer [0087])** to a first of **(e.g. first rule Iyer [0087])** the at least two rules, and wherein, for the at least two packet security gateways configured in series **(e.g. pipelined manner Ahn [0021])**, performing the at least one of multiple packet transformation functions specified by the dynamic security policy on the packets comprises: performing, by the first of the at least two packet security gateways **(e.g. policy enforcer performs Iyer [0086])**, a first packet transformation function **(e.g. firewall policy rule for spam blocking, URL blocking Iyer [0088]; based on policy rule, policy enforcer processes packet stream with IPSec, or bandwidth [0128])** specified by the first of the at least two rules; and performing, by the second of the at least two packet security gateways, a second packet transformation function **(e.g. bandwidth shaping service to the packets or decoding protocols used in the packets Iyer [0126])** specified by the second of the at least two rules. The Examiner

supplies the same rationale for the combination of references **Iyer** and **Ahn** as in Claim 2 above.

10. **Claims 4 and 9** are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over **Iyer** in view of **Afek et al.** (US 20060212572 A1, hereinafter **Afek**).

As to Claim 4:

Iyer discloses the method of claim 1, but does not specifically disclose:

- at least one rule specifying a set of network addresses for which associated packets should be dropped and at least one rule specifying that all packets associated with network addresses outside the set should be forwarded.

However, the analogous art **Afek** does disclose at least one rule **(e.g. blacklist of network addresses [0021]; [0084]; [0088])** specifying a set of network addresses for which associated packets should be dropped **(e.g. blocked and discarded [0089])** and at least one rule specifying that all packets associated with network addresses outside the set **(e.g. instruction for guard device to forward the packets with addresses not found on blacklist [0088])** should be forwarded. **Iyer** and **Afek** are analogous art because they are from the same field of endeavor in coordinated processing of network packets.

- (e.g. see **Afek**, "After traffic has been diverted, guard device 28 intercepts all diverted packets, at packet interception step 52. Guard device 28 looks up the source address or subnetwork source address of each packet on the blacklist, at a blacklist look-up step 64. Guard device 28 determines whether the address of the packet is on the blacklist, at an address check step 66. If the address of the

packet is not found on the blacklist, the guard device forwards the packet on its-normal path to its intended destination address, at a forward packet step 68" **[0088]**; see also "On the other hand, if the address of the packet is found on the blacklist, guard device 28 blocks the further transmission of the packet, at a block step 70. Typically, the guard device simply discards the blocked packet" **[0089]**).

At the time of applicants' invention, it would have been obvious to one of ordinary skill in the art, having the teachings of **Iyer** and **Afek** before him or her, to modify the firewall policy enforcer system of **Iyer** with the teachings of **Afek** to include *at least one rule specifying a set of network addresses for which associated packets should be dropped and at least one rule specifying that all packets associated with network addresses outside the set should be forwarded* as claimed because **Iyer**'s policy enforcer system already provides centralized management of policy enforcers with network processing functions including forwarding and dropping packets **(Iyer [0045]-[0046]; [0126]-[0128])** which could be implemented by a blacklist of network addresses **(Afek [0088]; [0089])**. The suggestion/motivation for doing so would have been to provide monitoring of sources of packets for anomalous traffic patterns and enable more complete blocking of blacklisted sources **(Afek [0006]; [0084])**. Therefore, it would have been obvious to combine **Iyer** and **Afek** to obtain the invention as specified in the instant claim(s).

As to Claim 9:

Iyer discloses the method of claim 1, but does not specifically disclose:

- at least one rule specifying a set of network addresses and an additional parameter, and routing at least one of the packets that falls within the set of

network addresses and matches the additional parameter to a network address different from a destination network address specified by the at least one of the packets.

However, the analogous art **Afek** does disclose at least one rule specifying a set of network addresses **(e.g. designated network addresses [0007]; blacklist of packet addresses [0088])** and an additional parameter **(e.g. content or statistical property of the traffic packet [0007]; information about packet [0093])**, and routing at least one of the packets **(e.g. initiate diversion of traffic to one or more guard devices [0095])** that falls within the set of network addresses **(e.g. blacklist of source addresses [0088]; [0095])** and matches the additional parameter **(e.g. [0007]; matches recorded packet statistical information [0093])** to a network address different from **(e.g. traffic diverted and forwarded to guard device [0088]; [0093]; [0095])** a destination network address specified by the at least one of the packets. **Iyer** and **Afek** are analogous art because they are from the same field of endeavor in coordinated processing of network packets.

- (e.g. see **Afek**, “a network protected with the network guard system designates a set of network addresses (such as IP addresses) assigned to the network as "trap" addresses. These trap addresses are assigned to one or more guard devices, but otherwise are not used by other elements of the network. When a packet addressed to such a trap address enters the protected network, the packet is forwarded to the assigned guard device, which analyzes the traffic. The guard device may determine that the traffic from a given source address is

suspicious, based on the content or statistical properties of the traffic, for example. The guard device may then block or otherwise filter incoming traffic from the suspicious source address, to reduce the likelihood of servers within the protected area of a network becoming infected with a worm" **[0007]**; see also "After traffic has been diverted, guard device 28 intercepts all diverted packets, at packet interception step 52. Guard device 28 looks up the source address or subnetwork source address of each packet on the blacklist, at a blacklist look-up step 64. Guard device 28 determines whether the address of the packet is on the blacklist, at an address check step 66" **[0088]**; see also "When a packet addressed to a trap address enters protected area 30, the packet is received by one of routers 22, at a router receipt step 94. The router forwards the packet to a guard device, at a forwarding step 96. At an analysis step 98, the guard device analyzes the packet to determine whether it is indicative of worm activity. For example, the guard device may perform a statistical analysis on packets received from the same source or subnetwork source address, using information about the packet just received, combined with information about previously-received packets recorded in a statistical repository, as described hereinbelow with reference to step 102" **[0093]**; see also "the guard device initiates diversion of traffic from the source address to one or more guard devices for screening, but not necessarily blocking. Alternatively or additionally, when a worm has been identified, the guard device initiates diversion of all traffic entering the protected area of the network (including traffic from addresses other than the infected

source address) to one or more guard devices for screening and possible blocking" **[0095]**).

At the time of applicants' invention, it would have been obvious to one of ordinary skill in the art, having the teachings of **Iyer** and **Afek** before him or her, to modify the firewall policy enforcer system of **Iyer** with the teachings of **Afek** to include *at least one rule specifying a set of network addresses and an additional parameter, and routing at least one of the packets that falls within the set of network addresses and matches the additional parameter to a network address different from a destination network address specified by the at least one of the packets* as claimed because **Iyer**'s policy enforcer system already provides centralized management of policy enforcers with network processing functions including forwarding and dropping packets **(Iyer [0045]-[0046]; [0126]-[0128])** which could be based on a blacklist of network addresses and recorded packet content properties **(Afek [0007]; [0088]; [0089]; [0093]; [0095])**. The suggestion/motivation for doing so would have been to provide monitoring of sources of packets for anomalous traffic patterns and enable more complete blocking of blacklisted sources **(Afek [0006]; [0084])**. Therefore, it would have been obvious to combine **Iyer** and **Afek** to obtain the invention as specified in the instant claim(s).

11. **Claim 5** is rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over **Iyer** in view of **Barkan** (US 20100296441 A1).

As to Claim 5:

Iyer discloses the method of claim 1, but does not specifically disclose:

- wherein the dynamic security policy comprises at least one rule specifying a set of network addresses for which associated packets should be forwarded and at least one rule specifying that all packets associated with network addresses outside the set should be dropped.

However, the analogous art **Afek** does disclose wherein the dynamic security policy comprises at least one rule specifying **(e.g. white listing allowed addresses [0191])** a set of network addresses for which associated packets should be forwarded **(e.g. allow only packets to and from known white listed addresses [0191])** and at least one rule specifying that all packets associated with network addresses outside the set should be dropped **(e.g. block all traffic not from white listed addresses [0190]; [0191])**. **Iyer** and **Barkan** are analogous art because they are from the same field of endeavor in coordinated processing of network packets.

- (e.g. see **Barkan**, "In another embodiment a remote site 50 with a fast Internet connection acts as a proxy of STA 14. Incoming and outgoing packets are forwarded between STA 14 and remote site 50" **[0159]**; see also "In another method, laptop 11 allow only packets to and from known servers such as trusted server 50 (i.e., white listing the allowed addresses)" **[0191]**).

At the time of applicants' invention, it would have been obvious to one of ordinary skill in the art, having the teachings of **Iyer** and **Barkan** before him or her, to modify the firewall policy enforcer system of **Iyer** with the teachings of **Barkan** to include *wherein the dynamic security policy comprises at least one rule specifying a set of network addresses for which associated packets should be forwarded and at least one rule*

specifying that all packets associated with network addresses outside the set should be dropped as claimed because **Iyer**'s policy enforcer system already provides centralized management of policy enforcers with network processing functions including forwarding and dropping packets **(Iyer [0045]-[0046]; [0126]-[0128])** which could be implemented by a white listing of allowed network addresses **(Barkan [0159]; [0191])**. The suggestion/motivation for doing so would have been to protect privacy in tunneling sensitive traffic to a trusted network **(Barkan [0189])**. Therefore, it would have been obvious to combine **Iyer** and **Barkan** to obtain the invention as specified in the instant claim(s).

12. **Claim 6** is rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over **Iyer** in view of **Barkan** as applied to claim 5 above, and further in view of **Maes** (US 20080072307 A1).

As to Claim 6:

Iyer in view of **Barkan** discloses the method of claim 5, but does not specifically disclose:

- receiving, by the security policy management server, information associated with a Voice over Internet Protocol (VoIP) session, and wherein the at least one rule specifying the set of network addresses for which associated packets should be forwarded is one of created and altered by the security policy management server utilizing the information associated with the one or more VoIP sessions.

However, the analogous art **Maes** does disclose receiving, by the security policy management server, information **(e.g. stored session information by Web server**

[0023]) associated with a Voice over Internet Protocol (VoIP) session **(e.g. session information such as voice packets [0024]; [0026]; in VoIP data [0005])**, and wherein the at least one rule specifying the set of network addresses **(e.g. session data table with appropriate address of participant devices are stored [0023])** for which associated packets should be forwarded **(e.g. allow streaming media packets such as VoIP [0005]; packet arriving at firewall checked against session data table [0024])** is one of created and altered by the security policy management server utilizing the information **(e.g. packet arriving at the firewall from the authorized address of the participant device is checked against session information data table [0024])** associated with the one or more VoIP sessions **(e.g. interactive multimedia session [0026])**. **Iyer**, **Barkan**, and **Maes** are analogous art because they are from the same field of endeavor in coordinated processing of network packets.

- (e.g. see **Maes**, "This can be useful to allow streaming media such as VoIP data to pass through the firewall without weakening firewall policies" **[0005]**; see also "In embodiments without a gateway, the session information can be written to the session data table by the participant on the secure side of the firewall, here the Web server 114. The stored session information can include information such as the appropriate address of the participant device 102 and Web server 114 for the communications, the port of the firewall 110 through which the communications will occur (the communications path), and a session identifier. The session information also can include other appropriate session information such as an active status of the session, a lifetime, etc" **[0023]**; see also "Once the session

information is stored in the session data table, any packet arriving at the firewall can be checked against the session data table to determine whether the packet should be allowed through the firewall. This authorization can be in addition to any other determination as known in the art for authorizing communications to pass through a firewall. For example, a packet arriving at the firewall from the authorized address of the participant device 102 to the authorized port for an active session will be checked against the session information in the session data table, whereby the firewall will find the relevant session information and allow the packet to pass through the firewall to the authorized address of the Web server 114" **[0024]**; see also "Allowing the firewall to access the session information and security policy allows the firewall to act as a security policy enforcer for the enterprise. This can be advantageous for protocols such as the Session Initialization Protocol (SIP), which is a standard for initiating, modifying, and terminating an interactive session that involves multimedia elements such as video, voice, and instant messaging. In typical use, SIP sessions are streams of RTP packets, with RTP being the carrier for the actual voice or video content" **[0026]**).

At the time of applicants' invention, it would have been obvious to one of ordinary skill in the art, having the teachings of **Iyer**, **Barkan**, and **Maes** before him or her, to modify the combination of **Iyer** and **Barkan** with the teachings of **Maes** to include *receiving, by the security policy management server, information associated with a Voice over Internet Protocol (VoIP) session, and w**h**erein the at least one rule specifying the set of network*

addresses for which associated packets should be forwarded is one of created and altered by the security policy management server utilizing the information associated with the one or more VoIP sessions as claimed because **Iyer**'s policy enforcer system already provides centralized management of policy enforcers with network processing functions including forwarding **(Iyer [0045]-[0046]; [0126]-[0128])** which could be based upon relevant session information of authorized addresses of participant devices in active voice, VoIP, multimedia sessions **(Maes [0005]; [0023]; [0024]; [0026])**. The suggestion/motivation for doing so would have been to allow protocols of various levels to pass through a firewall including streaming VoIP data without weakening firewall policies **(Maes [0005])**. Therefore, it would have been obvious to combine **Iyer** and **Maes** to obtain the invention as specified in the instant claim(s).

13. **Claim 8** is rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over **Iyer** in view of Kumar et al. (US 20050141537 A1, hereinafter **Kumar**).

As to Claim 8:

Iyer discloses the method of claim 1, but does not specifically disclose:

- a first of the at least two rules specifying a first set of network addresses, a second of the at least two rules specifying a second set of network addresses, and wherein the dynamic security policy specifies that packets associated with the first set of network addresses should be placed in a first forwarding queue and packets associated with the second set of network addresses should be placed in a second forwarding queue, the first forwarding queue having a higher forwarding rate than the second forwarding queue.

However, the analogous art **Kumar** does disclose a first of the at least two rules specifying a first set of network addresses **(e.g. frame forwarding policy for MAC addresses with higher priority [0019])**, a second of the at least two rules specifying a second set of network addresses **(e.g. frame forwarding policy for MAC addresses with lower priority [0019])**, and wherein the dynamic security policy specifies that packets associated with the first set of network addresses should be placed in a first forwarding queue **(e.g. higher priority frames are placed into corresponding ingress queue [0019])** and packets associated with the second set of network addresses should be placed in a second forwarding queue **(e.g. lower priority frames based on MAC addresses are placed into other ingress queue [0019])**, the first forwarding queue having a higher forwarding rate **(e.g. higher priority forwarding and processing [0019])** than the second forwarding queue. **Iyer** and **Kumar** are analogous art because they are from the same field of endeavor in coordinated processing of network packets.

- (e.g. see **Kumar**, "The Ethernet processing engine 100 forwards frames or packets based on the MAC addresses contained in the frames. The process of frame forwarding involves determining what MAC addresses connect to which ports on the network device. When a frame arrives at a port on the network device, the frame is placed into one of the port's ingress queues. Each of the ingress queues contains frames to be forwarded and typically each of the ingress queues corresponds to a different priority or service level. The network device processes and forwards frames with higher priority before processing and

> forwarding frames with lower priority. As the ingress queues are serviced and a frame is pulled off of an ingress queue, the network device determines if, how, and where to forward the frame. Typically, the network device determines which of the egress ports the frame is to be forwarded on and also determines the forwarding policies. These determinations are preferably made simultaneously by independent components of the Ethernet processing engine 100" **[0019]**).

At the time of applicants' invention, it would have been obvious to one of ordinary skill in the art, having the teachings of **Iyer** and **Kumar** before him or her, to modify the firewall policy enforcer system of **Iyer** with the teachings of **Kumar** to include *a first of the at least two rules specifying a first set of network addresses, a second of the at least two rules specifying a second set of network addresses, and wherein the dynamic security policy specifies that packets associated with the first set of network addresses should be placed in a first forwarding queue and packets associated with the second set of network addresses should be placed in a second forwarding queue, the first forwarding queue having a higher forwarding rate than the second forwarding queue* as claimed because **Iyer**'s policy enforcer system already provides centralized management of policy enforcers with network processing functions including forwarding and dropping packets based on network addresses **(Iyer [0045]-[0046]; [0126]-[0128])** which could include prioritized queue processing based on frame addresses **(Kumar [0019])**. The suggestion/motivation for doing so would have been to provide certain quality of service levels of treatment for ingress packets **(Kumar [0017])**. Therefore, it would have been

obvious to combine **Iyer** and **Kumar** to obtain the invention as specified in the instant claim(s).

14. **Claim 13** is rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over **Iyer** in view of Chen et al. (US 20030142681 A1, hereinafter **Chen**).

As to Claim 13:

Iyer discloses the method of claim 1, wherein the dynamic security policy comprises a plurality of rules **(e.g. network policies are a set of rules Iyer [0045]; [0128])**, but does not specifically disclose:

- wherein at least one of the rules specifies a Differentiated Service Code Point (DSCP) selector that maps to a DSCP field in an Internet Protocol (IP) header of the packets.

However, the analogous art **Chen** does disclose wherein at least one of the rules specifies a Differentiated Service Code Point (DSCP) selector **(e.g. Diff-Serv boundary node, edge router [0007])** that maps to a DSCP field **(e.g. aggregates packets having same DSCPs code point header values [0007])** in an Internet Protocol (IP) header of the packets. **Iyer** and **Chen** are analogous art because they are from the same field of endeavor in coordinated processing of network packets.

- (e.g. see **Chen**, "In operation, the TOS field (i.e., the DS byte) is set by Diff-Serv capable network interface cards, routers and switches, and is used to differentiate between traffic flow which belongs to different service classes. Diff-Serv operates at network layer (or layer 3). If each network utilizes IP as a common network layer protocol, the data packet scheme and quality of Service

(QoS) parameters operate across different networks. DiffServ QoS specifications are recognizable by routers and switches, or any device which may read the IP header and DS byte. The DS byte contains a DS code point, and a tag which specifies the forwarding Per-Hop Behavior (PHB) for the DS byte. PHB is the forwarding treatment which is applied to a specific class of traffic, based on criteria defined in the Diff-Serv field. Routers and switches use PHBs to determine priorities for servicing various traffic flows. In this case, a PHB might specify routing precedence, or it may include other performance characteristics, such as query servicing or management policy" **[0006]**; see also "When data packets enter the network, they pass through a Diff-Serv boundary node (i.e., an edge router or edge node), and then pass through a Diff-Serv core node (i.e., a core router). If the data packets are unclassified, the edge router handles and assigns each packet to a "behavior aggregate". Here, a behavior aggregate is a collection of packets having the same DSCPs (DS code points, i.e., header values) which are members of the same DSCP group and cross a link in a particular direction, where the DSCP group is a set of related DSCPs which select the same PHB group" **[0007]**).

At the time of applicants' invention, it would have been obvious to one of ordinary skill in the art, having the teachings of **Iyer** and **Chen** before him or her, to modify the firewall policy enforcer system of **Iyer** with the teachings of **Chen** to include *wherein at least one of the rules specifies a Differentiated Service Code Point (DSCP) selector that maps to a DSCP field in an Internet Protocol (IP) header of the packets* as claimed

because **Iyer**'s policy enforcer system provides centralized management of policy enforcers with network processing functions including forwarding and dropping packets based on network addresses **(Iyer [0045]-[0046]; [0126]-[0128])** which could include a Diff-Serv boundary node to handle quality of service parameters such as DSCP packet header values **(Chen [0006]; [0007])**. The suggestion/motivation for doing so would have been to provide differentiated service classes of forwarding treatment based on defined criteria **(Chen [0006])**. Therefore, it would have been obvious to combine **Iyer** and **Chen** to obtain the invention as specified in the instant claim(s).

15. **Claim 16** is rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over **Iyer** in view of Van Der Merwe et al. (US 20100082811 A1, hereinafter **Van Der Merwe**).

As to Claim 16:

Iyer discloses the method of claim 1, but does not specifically disclose:

- wherein the dynamic security policy comprises one or more rules generated based, at least in part, on a list of known network addresses associated with malicious network traffic that is received from a subscription service that aggregates information associated with malicious network traffic.

However, the analogous art **Van Der Merwe** does disclose wherein the dynamic security policy comprises one or more rules **(e.g. blacklist generated from received malicious network sources [0042]; [0043])** generated based, at least in part, on a list of known network addresses **(e.g. addresses of sources of unwanted data traffic [0003]; [0005]; [0006])** associated with malicious network traffic **(e.g. unwanted traffic**

sources [0006]; malicious traffic source [0043]) that is received from a subscription service **(e.g. network service for customers [0028])** that aggregates information associated **(e.g. raw blacklists acquired from reputation systems [0030])** with malicious network traffic. **Iyer** and **Van Der Merwe** are analogous art because they are from the same field of endeavor in coordinated processing of network packets.

- (e.g. see **Van Der Merwe**, "Blacklists may be derived, for example, from e-mail spam logs, firewall logs, databases from anti-spyware software, and databases from anti-virus software. Blacklists may also contain user-specified entries" **[0022]**; see also "Herein, a customer refers to an end-user of network services. A customer, for example, may operate user system US1 150. A user system operated by a customer is also referred to as a customer user system" **[0028]**; see also "In FIG. 2(a), a set of raw blacklists 202 is acquired from reputation systems RS1 130-RS3 134 as input to traffic filter system TFS 140. Additional raw blacklists may also be inputted by the network administrator. A raw blacklist refers to a blacklist which has not been processed by traffic filter system 140. In step 204, TFS 140 consolidates the multiple raw blacklists into a single list of unwanted traffic sources, referred to herein as a consolidated raw blacklist" **[0030]**; see also "FIG. 2(c) shows a flowchart of steps for generating a customer blacklist for a specific customer. Network blacklist 216 and a customer whitelist 234 (for a specific customer) are acquired as input into TFS 140… In general, since customer whitelist 234 may be different for different specific customers, customer blacklist 248 may be different for different specific customers. A

customer blacklist is associated with a customer system" **[0042]**; see also "For example, network blacklist 216 may be updated in response to a network attack by a malicious traffic source" **[0043]**).

At the time of applicants' invention, it would have been obvious to one of ordinary skill in the art, having the teachings of **Iyer** and **Van Der Merwe** before him or her, to modify the firewall policy enforcer system of **Iyer** with the teachings of **Van Der Merwe** to include *wherein the dynamic security policy comprises one or more rules generated based, at least in part, on a list of known network addresses associated with malicious network traffic that is received from a subscription service that aggregates information associated with malicious network traffic* as claimed because **Iyer**'s policy enforcer system provides centralized management of policy enforcers with network processing functions including forwarding and dropping packets based on network addresses **(Iyer [0045]-[0046]; [0126]-[0128])** included in generated blacklists of malicious traffic sources for network service customers **(Van Der Merwe [0022]; [0028]; [0030]; [0042]; [0043])**. The suggestion/motivation for doing so would have been to provide a customer specific blacklist that is different for specific customers **(Van Der Merwe [0004]; [0042])**. Therefore, it would have been obvious to combine **Iyer** and **Van Der Merwe** to obtain the invention as specified in the instant claim(s).

16. **Claim 17** is rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over **Iyer** in view of Nguyen et al. (US 20110088092 A1, hereinafter **Nguyen**).

As to Claim 17:

Iyer discloses the method of claim 1, wherein at least two of the one or more packet security gateways receive dynamic security policies **(e.g. define network policy, firewall policy for policy enforcers in different locations Iyer [0045]; [0046]; [0060]; [0062]; modified policy [0076]; [0086])** from the security policy management server, but does not specifically disclose:

- one or more rules specifying source addresses that correspond to spoofed network addresses, and wherein at least one of the dynamic security policies specifies different source addresses that correspond to spoofed network addresses than at least another one of the dynamic security policies.

However, the analogous art **Nguyen** does disclose one or more rules specifying source addresses **(e.g. list of mac addresses, source IP [0027])** that correspond to spoofed network addresses **(e.g. spoofed address detected [0027]; multiple source IP addresses identified as suspicious hosts [0028])**, and wherein at least one of the dynamic security policies **(e.g. traffic summery information [0015]; [0027]; hash map [0028])** specifies different source addresses **(e.g. multiple varying source IP addresses [0028])** that correspond to spoofed network addresses **(e.g. spoofed host source [0027]; [0028])** than at least another one of the dynamic security policies. **Iyer** and **Nguyen** are analogous art because they are from the same field of endeavor in coordinated processing of network packets.

- (e.g. see **Nguyen**, "In another example, the source MAC address of the suspicious host is compared to a list of MAC addresses of known routers in the

network. The spoof condition is expected where the source MAC address of the suspicious host appears on the list" **[0012]**; see also "Network management server 30 may be further configured to inspect and analyze traffic summary information collected by one or more traffic data collectors and to detect network address spoofing activities in network system 100 based on the analysis of the traffic summary information" **[0015]**; see also "the traffic summary information includes the source MAC address, the source IP address, and the default initial TTL. The traffic summary information may be inspected and each source MAC address, source IP, and the associated default initial TTL value from the traffic summary information may be tracked, for example using a hash map. The tracking function may be performed by a spoofing detection engine, which may be implemented on the network management server 30. The spoofing detection engine may identify a suspicious host, for example, using the hash map" **[0027]**; see also "The suspicious host may be identified. In one embodiment, a source MAC address that is associated with multiple varying source IP addresses are identified as suspicious hosts. Using the exemplary hash map, the source MAC address of Host 44 (i.e., 00:00:00:00:00:0C) is associated with three different source IP addresses. As such, the source MAC address 00:00:00:00:00:0C is identified as a suspicious host. The spoofing detection engine may determine whether the suspicious host generated spoofed traffic while considering one or more false positive conditions" **[0028]**).

At the time of applicants' invention, it would have been obvious to one of ordinary skill in the art, having the teachings of **Iyer** and **Nguyen** before him or her, to modify the firewall policy enforcer system of **Iyer** with the teachings of **Nguyen** to include *one or more rules specifying source addresses that correspond to spoofed network addresses, and wherein at least one of the dynamic security policies specifies different source addresses that correspond to spoofed network addresses than at least another one of the dynamic security policies* as claimed because **Iyer**'s policy enforcer system provides centralized management of policy enforcers with network processing functions including forwarding and dropping packets based on network addresses **(Iyer [0045]-[0046]; [0126]-[0128])** which could be identified as spoofed source IP addresses **(Nguyen [0012]; [0015]; [0027]; [0028])**. The suggestion/motivation for doing so would have been to protect against malicious attacks by identifying and locating malicious hosts by detecting network address spoofing activities in the network **(Nguyen [0006]; [0036])**. Therefore, it would have been obvious to combine **Iyer** and **Nguyen** to obtain the invention as specified in the instant claim(s).

17. **Claim 22** is rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over **Iyer** in view of **Brustoloni** (US 20030035370 A1).

As to Claim 22:

Iyer discloses the method of claim 21, but does not specifically disclose:

- wherein at least one of the one or more packet security gateways or the security policy management server is associated with an organization distinct from an organization associated with the network protected by each respective packet

security gateway, and operating, by the organization distinct from the organization associated with the network protected by each respective packet security gateway, the at least one of the one or more packet security gateways or the security policy management server.

However, the analogous art **Brustoloni** does disclose wherein at least **one of** the one or more packet security gateways **(e.g. devices designated as server profile enforcement (SPE) units [0014])** or the security policy management server is associated with an organization distinct from **(e.g. ISP deploys SPE units for remuneration by subscribing site [0022]; [0023]; [0024])** an organization associated with the network protected **(e.g. subscriber server site and network [0022]; [0028])** by each respective packet security gateway **(e.g. access gateway includes SPE responder [0022])**, and operating, by the organization **(e.g. ISP deploys SPE units implemented in access gateways which perform ingress filtering to determine source address of packets arriving [0014])** distinct from the organization associated with the network protected by **(e.g. SPE subscriber [0014])** each respective packet security gateway, the at least one of the one or more packet security gateways **(e.g. ISP SPE units implemented in access gateways which perform ingress filtering to determine source address of packets arriving [0014])** or the security policy management server. **Iyer** and **Brustoloni** are analogous art because they are from the same field of endeavor in coordinated processing of network packets.

- (e.g. see **Brustoloni**, “To provide SPE service, an ISP deploys devices designated as SPE units, typically implemented in the ISP's access gateways.

Alternatively, SPE units can be implemented in IP service switches or as stand-alone devices. An ISP installs in its SPE units the profiles of the SPE subscribers. The SPE units perform ingress filtering, previously described, to determine whether the source address of a packet arriving on an access link is properly associated with the port on which the packet has arrived… Additionally, the SPE units filter packets destined or belonging to a connection to an SPE subscriber" **[0014]**; see also "Although only a single access gateway 103 is shown in FIG. 1, it should be appreciated that an ISP will have at least one such access gateway associated with each of its likely multiple points of presence (PoPs)" **[0021]**; see also "Server 107, a subscribing site of the SPE service, is connected over an access link to ISP 106 through an access gateway 108, which includes an SPE responder 109, to be described later. Other non-subscribing sites, such as server 110 may be connected to the same access gateway 108, or to other PoPs of ISP 106 that are not shown in FIG. 1" **[0022]**; see also "For providing the filtering service for a server site, the ISP receives from the subscribing server site remuneration of some type, monetary or otherwise" **[0023]**; see also "Enforcement of TCP congestion-avoidance prevents a malicious client from flooding the network or a server with TCP packets. Unlike limiting the transmission rate to some predetermined value, enforcement of congestion-avoidance provides dynamic and scalable throttling of each client's packets" **[0028]**).

At the time of applicants' invention, it would have been obvious to one of ordinary skill in the art, having the teachings of **Iyer** and **Brustoloni** before him or her, to modify the firewall policy enforcer system of **Iyer** with the teachings of **Brustoloni** to include *wherein at least one of the one or more packet security gateways or the security policy management server is associated with an organization distinct from an organization associated with the network protected by each respective packet security gateway, and operating, by the organization distinct from the organization associated with the network protected by each respective packet security gateway, the at least one of the one or more packet security gateways or the security policy management server* as claimed because **Iyer**'s policy enforcer system provides centralized management of policy enforcers with network processing functions including forwarding and dropping packets based on network addresses **(Iyer [0045]-[0046]; [0126]-[0128])** which could be implemented as a subscriber service offered by an ISP organization **(Brustoloni [0014]; [0021]; [0022]; [0023]; [0028])**. The suggestion/motivation for doing so would have been to provide a filtering service for a subscriber in exchange for remuneration of some type **(Brustoloni [0013]; [0023])**. Therefore, it would have been obvious to combine **Iyer** and **Brustoloni** to obtain the invention as specified in the instant claim(s).

Allowable Subject Matter

18. **Claims 7 and 10** are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Conclusion

19. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a. **Kellum** (US 20010039624 A1) is cited for teaching a protected system with filter/guard functions to process incoming data packet flows.

b. **Bruton, III et al.** (US 20030145225 A1) is cited for teaching an intrusion detection system that provides filtering and attack signature packet processing.

c. **Roese et al.** (US 20060048142 A1) is cited for teaching a system for policy enforcement of rule sets that are responsive to network event triggers.

20. Any inquiry concerning this communication or earlier communications from the examiner should be directed to KENNETH CHANG whose telephone number is (571)270-7530. The examiner can normally be reached on Monday-Friday 10:30am-7:30pm (Alt. Friday off).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Taghi T. Arani can be reached on 571-272-3787. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic

Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/KENNETH CHANG/
Examiner, Art Unit 2438
10/17/14

Notice of References Cited	Application/Control No. 13/657,010	Applicant(s)/Patent Under Reexamination ROGERS ET AL.	
	Examiner KENNETH CHANG	Art Unit 2438	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-2001/0039624 A1	11-2001	Kellum, Charles W.	713/201
*	B	US-2003/0035370 A1	02-2003	Brustoloni, Jose?apos, C.	370/229
*	C	US-2003/0142681 A1	07-2003	Chen et al.	370/401
*	D	US-2003/0145225 A1	07-2003	Bruton et al.	713/201
*	E	US-2005/0138204 A1	06-2005	Iyer et al.	709/242
*	F	US-2005/0141537 A1	06-2005	Kumar et al.	370/429
*	G	US-2006/0048142 A1	03-2006	Roese et al.	717/176
*	H	US-2006/0212572 A1	09-2006	Afek et al.	709/225
*	I	US-2008/0072307 A1	03-2008	Maes, Stephane H.	726/12
*	J	US-2010/0082811 A1	04-2010	Van Der Merwe et al.	709/225
*	K	US-2010/0296441 A1	11-2010	Barkan, Elad	370/328
*	L	US-2011/0088092 A1	04-2011	Nguyen et al.	726/22
	M	US-			

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13657010	ROGERS ET AL.
	Examiner	Art Unit
	KENNETH CHANG	2438

CPC- SEARCHED		
Symbol	Date	Examiner

CPC COMBINATION SETS - SEARCHED		
Symbol	Date	Examiner

US CLASSIFICATION SEARCHED			
Class	Subclass	Date	Examiner
726	1	10/17/2014	KC

SEARCH NOTES		
Search Notes	Date	Examiner
Searched Inventors' Names and Assignee on eDan and EAST.	10/17/2014	KC
Searched IEEE Xplore Database online.	10/17/2014	KC
Completed Limited Classified Search on EAST USPAT, PGPUB, and EPO databases with Keywords combined with Classes/Subclasses 726/3,6,11,12,13,14,15,16,17,22,23,24,25, 713/1,100,150,151,152,153,154,155,166,167,168, and 709/201,203,217,218,219,220,223,224,225,226,227,228,229,230,231,238 ,239,240,242,244,245.	10/17/2014	KC
Keywords Searched: gateway, policy, policies, packet, traffic, rule, address$10, source, destination, network, ip, internet protocol, security, secure, supervis$9, protect$9, ids, intrusion, dos, denial of service, filter$9, processing, algorithm, function, ipsec, ip security, internet protocol security, discard$9, block$6, drop$5, forward$9, allow$8.	10/17/2014	KC

INTERFERENCE SEARCH			
US Class/ CPC Symbol	US Subclass / CPC Group	Date	Examiner

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**		
	Application Number	13657010
	Filing Date	2012-10-22
	First Named Inventor	Steven Rogers
	Art Unit	2438
	Examiner Name	K. W. Chang
	Attorney Docket Number	007742.00017

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
/K.C./	1	1313290	EP	A1	2003-05-21	Stonesoft Corp		☐
/K.C./	2	2005046145	WO	A1	2005-05-19	Ericsson Telefon Ab L M		☐

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

EFS Web 2.1.17 ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.C./

Receipt date: 06/27/2014	Application Number	13657010 13657010 - GAU: 2438
INFORMATION DISCLOSURE STATEMENT BY APPLICANT	Filing Date	2012-10-22
(Not for submission under 37 CFR 1.99)	First Named Inventor	Steven Rogers
	Art Unit	2438
	Examiner Name	K. W. Chang
	Attorney Docket Number	007742.00017

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
/K.C./	1	ISR off International Application No. PCT/US2013/072566, dated March 24, 2014.	☐

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature	/Kenneth Chang/	Date Considered	10/18/2014

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.C./

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

BIB DATA SHEET

CONFIRMATION NO. 2390

SERIAL NUMBER	FILING or 371(c) DATE RULE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
13/657,010	10/22/2012	726	2438	007742.00017

APPLICANTS
CENTRIPETAL NETWORKS, INC., Leesburg, VA

INVENTORS
Steven Rogers, Leesburg, VA;
Sean Moore, Hollis, NH;

**** CONTINUING DATA ***************************

**** FOREIGN APPLICATIONS ***************************

**** IF REQUIRED, FOREIGN FILING LICENSE GRANTED **** ** SMALL ENTITY **
11/23/2012

Foreign Priority claimed ☐ Yes ☑ No 35 USC 119(a-d) conditions met ☐ Yes ☑ No Verified and Acknowledged /KENNETH W CHANG/ Examiner's Signature	☐ Met after Allowance Initials	STATE OR COUNTRY	SHEETS DRAWINGS	TOTAL CLAIMS	INDEPENDENT CLAIMS
		VA	10	20	3

ADDRESS

BANNER & WITCOFF, LTD.
1100 13th STREET, N.W.
SUITE 1200
WASHINGTON, DC 20005-4051
UNITED STATES

TITLE

METHODS AND SYSTEMS FOR PROTECTING A SECURED NETWORK

FILING FEE RECEIVED		
823	FEES: Authority has been given in Paper No._____ to charge/credit DEPOSIT ACCOUNT No._____ for following:	☐ All Fees ☐ 1.16 Fees (Filing) ☐ 1.17 Fees (Processing Ext. of time) ☐ 1.18 Fees (Issue) ☐ Other _____ ☐ Credit

BIB (Rev. 05/07).

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**		
	Application Number	13657010
	Filing Date	2012-10-22
	First Named Inventor	Steven Rogers
	Art Unit	2438
	Examiner Name	Chang, Kenneth W.
	Attorney Docket Number	007742.00017

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
/K.C./	1	7721084		2010-05-18	Salminen et al.	
/K.C./	2	7684400		2010-03-23	Govindarajan et al.	

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
/K.C./	1	20120113987	A1	2012-05-10	Riddoch et al.	
	2	20110270956	A1	2011-11-03	McDysan et al.	
	3	20100211678	A1	2010-08-19	McDysan et al.	
	4	20050117576		2005-06-02	McDysan et al.	

EFS Web 2.1.17

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.C./

Receipt date: 09/09/2014	Application Number	13657010 13657010 - GAU: 2438
INFORMATION DISCLOSURE STATEMENT BY APPLICANT	Filing Date	2012-10-22
(Not for submission under 37 CFR 1.99)	First Named Inventor	Steven Rogers
	Art Unit	2438
	Examiner Name	Chang, Kenneth W.
	Attorney Docket Number	007742.00017

/K.C./	5	20040151155	A1	2004-08-05	Jouppi	
	6	20030212900	A1	2003-11-13	Liu et al.	
	7	20030188192	A1	2003-10-02	Tang et al.	
	8	20120264443	A1	2012-10-18	Ng et al.	
	9	20130059527	A1	2013-03-07	HASESAKA et al.	

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							☐

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1		☐

If you wish to add additional non-patent literature document citation information please click the Add button Add

EFS Web 2.1.17

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.C./

Receipt date: 09/09/2014	Application Number	13657010 13657010 - GAU: 2438
INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**	Filing Date	2012-10-22
	First Named Inventor	Steven Rogers
	Art Unit	2438
	Examiner Name	Chang, Kenneth W.
	Attorney Docket Number	007742.00017

EXAMINER SIGNATURE			
Examiner Signature	/Kenneth Chang/	Date Considered	10/18/2014

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

EFS Web 2.1.17 ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.C./

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L29	26	713/1,100,150,151,152,153,154,155,166,167,168.CCLS. AND L26	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/20 02:26
L28	54	709/201,203,217,218,219,220,223,224,225,226,227,228,229,230,231,238,239,240,242,244,245.CCLS. AND L26	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/20 02:26
L27	31	726/3,6,11,12,13,14,15,16,17,22,23,24,25.CCLS. AND L26	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/20 02:26
L26	198	(gateway) same (policy or policies) same (packet or traffic) and (rule) same (address$10) with (source or destination or network or ip or internet protocol) same (security or secure or protect$9 or ids or intrusion or dos or denial of service) and (server or manager or managing or supervis$9) and (set or list) and (function or algorithm or filter$9 or processing) same (ipsec or ip security or internet protocol security)	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/20 02:26
L25	24976	713/1,100,150,151,152,153,154,155,166,167,168.CCLS.	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/20 02:26
L24	125386	709/201,203,217,218,219,220,223,224,225,226,227,228,229,230,231,238,239,240,242,244,245.CCLS.	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/20 02:26
L22	26093	726/3,6,11,12,13,14,15,16,17,22,23,24,25.CCLS.	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/20 02:24
L18	1	"20030035370".pn.	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/20 01:42
L17	1	"20050135375".pn.	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/20 01:39
L16	1	"20110088092".pn.	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/20 00:40
L15	69	(spoof$5) with (address$5) with (network or source) with (policy or policies or rule)	US-PGPUB;	ADJ	ON	2014/10/20 00:28

			USPAT; EPO			
L14	209	(spoof$5) with (address$5) with (network or source) same (policy or policies or rule)	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/20 00:28
L13	1	"20100082811".pn.	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/20 00:08
L12	1	"20080279200".pn.	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/19 23:51
L11	5	(blacklist$5 or black list$9) with (addresses) with (paid or pay)	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/19 23:46
L10	5	(blacklist$5 or black list$9) with (addresses) with (provider) with (subscription or subscribing or subscriber)	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/19 23:42
L9	55	(blacklist$5 or black list$9) with (addresses) with (provider) with (service)	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/19 23:41
L8	15	(blacklist$5 or black list$9) with (addresses) with (subscription or subscriber or subscribing) with (service)	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/19 23:38
L7	222	(blacklist$5 or black list$9) with (addresses) same (subscription or subscriber or subscribing or customer)	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/19 23:38
L6	2	(blacklist$5 or black list$9) with (addresses) with (discard$9 or block$6 or drop$5) with (packet) same (subscription or subscriber or subscribing or customer)	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/19 23:38
L5	3	(differentiat$10 service code point select$5 or dscp select$5 or Diff-Serv Code Point) same (header or heading) same (traffic or packet) same (policy or policies or rule)	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/19 22:48
L4	26	(differentiat$10 service code point select$5 or dscp select$5 or Diff-Serv Code Point) same (header or heading) same (traffic or packet)	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/19 22:47
L3	10	(differentiat$10 service code point select$5 or dscp select$5) same (header or heading) same (traffic or packet)	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/19 22:47
L1	34	(forward$9) with (packet) same (queue or group or buffer$5) same (priority) same (faster or higher) same (policy or policies or whitelist$5 or white list$8)	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/19 21:56

S40	11	(discard$10 or block$5 or drop$5) and (forward$9 or allow$8) with (packet) with (address$5) same (policy or policies or whitelist$5 or white list$8) same (voip or voice over ip or voice over internet protocol) same (call or session or traffic or connection)	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/19 20:32
S39	12	(discard$10 or block$5 or drop$5) and (forward$9 or allow$8) with (packet) with (address$5) same (policy or policies or whitelist$5 or white list$8) same (voip or voice over ip or voice over internet protocol)	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/19 20:32
S38	223	(discard$10 or block$5 or drop$5) and (forward$9 or allow$8) with (packet) with (address$5) same (policy or policies or whitelist$5 or white list$8) and (voip or voice over ip or voice over internet protocol)	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/19 20:31
S37	21	(discard$10 or block$5 or drop$5) and (forward$9 or allow$8) with (packet) with (address$5) with (whitelist$9 or white list$5)	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/19 20:07
S36	5	(discard$10 or block$5 or drop$5) and (forward$9 or allow$8) with (packet) with (address$5) with (whitelist$9 or white list$5) with (only)	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/19 20:07
S35	5	(addresses) with (ip or internet protocol or source) with (discard$9 or block$6 or drop$5) with (packet) and (forward$9 or allow$8) with (packet) with (address$5) with (whitelist$9 or white list$5) with (only)	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/19 20:05
S34	15	(addresses) with (ip or internet protocol or source) with (discard$9 or block$6 or drop$5) with (packet) and (forward$9 or allow$8) with (outside or otherwise or address$5) with (packet) with (address$5) with (whitelist$9 or white list$5)	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/19 20:04
S33	12	(blacklist$5 or black list$9) with (addresses) with (ip or internet protocol or source) with (discard$9 or block$6 or drop$5) with (packet) and (forward$9 or allow$8) with (outside or otherwise or address$5) with (packet) with (address$5) with (blacklist$5 or black list$9)	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/19 18:28
S32	19	(blacklist$5 or black list$9) with (addresses) with (ip or internet protocol or source) with (discard$9 or block$6 or drop$5) with (packet) and (forward$9 or allow$8) with (outside or otherwise or address$5) with (packet) with (address$5)	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/19 18:28
S31	1	(blacklist$5 or black list$5) with (address$9) with increas$9 with (policy or policies)	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/19 18:26
S30	546	(set or list$5) with (addresses) with (ip or internet protocol or source) with (discard$9 or block$6 or drop$5) with (packet) and (forward$9 or allow$8) with (outside or otherwise or address$5) with (packet) with (address$5)	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/19 18:24
S29	705	(set or list$5) with (addresses) with (ip or internet protocol or source) with (discard$9 or block$6 or drop$5) same (packet) and (forward$9 or allow$8) with (outside or otherwise or address$5) same (packet) with (address$5)	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/19 18:24
S28	1857	(set or list$5) with (addresses) with (ip or internet protocol or source) same (discard$9 or block$6 or drop$5) same (packet) and (forward$9 or allow$8) with (outside or otherwise or address$5) same (packet) same (address$5)	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/19 18:24
S27	8993	(set or list$5) with (addresses) with (ip or internet protocol or source) same (discard$9 or block$6 or drop$5)	US-PGPUB;	ADJ	ON	2014/10/19 18:23

			USPAT; EPO			
S26	74	(gateway) same (policy or policies) same (packet or traffic) and (rule) same (function or algorithm or filter$9 or processing) same (ipsec or ip security or internet protocol security) and (security or secure or protect$9 or ids or intrusion or dos or denial of service) and (server or manager or managing or supervis$9) same (policy or policies) and (address$10) with (source or destination or network or ip or internet protocol)	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/19 15:35
S25	9	(gateway) same (policy or policies) same (packet or traffic) and (rule) same (address$10) with (source or destination or network or ip or internet protocol) same (function or algorithm or filter$9 or processing) same (ipsec or ip security or internet protocol security) and (security or secure or protect$9 or ids or intrusion or dos or denial of service) and (server or manager or managing or supervis$9) same (policy or policies) and (pipelin$5 or parallel$5)	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/19 15:25
S24	28	(gateway) same (policy or policies) same (packet or traffic) and (rule) same (address$10) with (source or destination or network or ip or internet protocol) same (function or algorithm or filter$9 or processing) same (ipsec or ip security or internet protocol security) and (security or secure or protect$9 or ids or intrusion or dos or denial of service) and (server or manager or managing or supervis$9) same (policy or policies)	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/19 15:25
S23	198	(gateway) same (policy or policies) same (packet or traffic) and (rule) same (address$10) with (source or destination or network or ip or internet protocol) same (security or secure or protect$9 or ids or intrusion or dos or denial of service) and (server or manager or managing or supervis$9) and (set or list) and (function or algorithm or filter$9 or processing) same (ipsec or ip security or internet protocol security)	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/19 15:24
S22	253	(gateway) same (policy or policies) same (packet or traffic) and (rule) same (address$10) with (source or destination or network or ip or internet protocol) same (security or secure or protect$9 or ids or intrusion or dos or denial of service) and (server or manager or managing or supervis$9) and (set or list) and (function or algorithm or filter$9 or processing) and (ipsec or ip security or internet protocol security)	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/19 15:23
S21	252	(gateway) same (policy or policies) same (packet or traffic) and (rule) same (address$10) with (source or destination or network or ip or internet protocol) same (security or secure or protect$9 or ids or intrusion or dos or denial of service) and (server or manager or managing or supervis$9) and (set or list) and (function or algorithm or filter$9 or processing) and (ipsec or ip security)	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/19 15:23
S20	534	(gateway) same (policy or policies) same (packet or traffic) and (rule) same (address$10) with (source or destination or network or ip or internet protocol) same (security or secure or protect$9 or ids or intrusion or dos or denial of service) and (server or manager or managing or supervis$9) and (set or list) and (function or algorithm or filter$9 or processing)	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/19 00:19
S19	534	(gateway) same (policy or policies) same (packet or traffic) and (rule) same (address$10) with (source or destination or network or ip or internet protocol) same (security or secure or protect$9 or ids or intrusion or dos or denial of service) and (server or manager or managing or supervis$9) and (set or list)	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/19 00:18
S18	551	(gateway) same (policy or policies) same (packet or traffic) and (rule) same (address$10) with (source or destination or network or ip or internet protocol) same (security or secure or protect$9 or ids or intrusion or dos or denial of service) and (server or manager or managing or supervis$9)	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/19 00:18
S17	570	(gateway) same (policy or policies) same (packet or traffic) and (rule) same (address$10) with (source or destination or network or ip or internet protocol) same (security or secure or protect$9 or ids or intrusion or dos or denial of service)	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/19 00:18
S16	1430	(gateway) same (policy or policies) same (packet or traffic) and (rule) same (address$10) with (source or destination or network or ip or internet protocol) and (security or secure or protect$9 or ids or intrusion or dos or denial of service)	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/19 00:17
S15	3295	(gateway) same (policy or policies) same (packet or traffic) and (rule) and (address$10) with (source or destination or network or ip or internet protocol) and (security or secure or protect$9 or ids or intrusion or dos or denial of service)	US-PGPUB; USPAT;	ADJ	ON	2014/10/19 00:16

			EPO			
S14	3686	(gateway) same (policy or policies) same (packet or traffic) and (rule) and (address$10) with (source or destination or network or ip or internet protocol)	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/19 00:15
S13	4415	(gateway) same (policy or policies) same (packet or traffic) and (rule)	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/19 00:14
S12	7	("20120113987" | "20060195896" | "7684400" | "20060248580" | "20110055916" | "0000000" | "20110270956" | "20130059527" | "20100011434" | "20120264443" | "6226372" | "20040151155" | "20030212900" | "20050117576" | "20060048142" | "20030188192" | "7721084" | "20030123456" | "20070083924" | "20100211678").PN. and (gateway) and (policy or policies)	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/19 00:12
S11	17	S7 and (gateway) and (policy or policies)	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/19 00:05
S10	17	S6 and (gateway) and (policy or policies)	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/19 00:05
S9	7	S8 and (gateway) and (policy or policies)	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/19 00:03
S8	20	("20050071655" | "20040098618" | "20090038008" | "7975059" | "6715084" | "20060143709" | "20010020255" | "20020066034" | "20040148520" | "20060143688" | "20090037682" | "20120167120" | "20020078382" | "20040128543" | "20020162026" | "20040044912" | "8214900" | "20020083175" | "20030145225" | "20030204632").PN.	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/19 00:01
S7	54	("20060173992" | "20030084329" | "20030035370" | "20010042200" | "20020133721" | "20030023733" | "20060095965" | "20060230444" | "20020073155" | "20030233328" | "20060212524" | "20070180510" | "7536715" | "20060212572" | "20020198956" | "20040199793" | "20030126468" | "20050050338" | "20040073800" | "20060050719" | "20050262556" | "20040049574" | "20030101260" | "20020198956" | "20030035370" | "20040190522" | "20070157316" | "20050182950" | "20020073337" | "20030145225" | "20040117624" | "20040128538" | "20040148520" | "20070056030" | "20040004941" | "20030061514" | "20030014665" | "20060193470" | "20080176536" | "7409712" | "20020133721" | "20020166063" | "20030204632" | "20060137012" | "7574740" | "20050086502" | "7331060" | "20030023733" | "20050278415" | "20020178378" | "20030101260" | "20070180511" | "20020162026" | "20050037733" | "20050039104" | "7702739" | "20010042200" | "20020073337" | "20030145225" | "20040117624" | "20050180416" | "20020083175" | "20060048142").PN.	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/18 23:56
S6	53	("20060173992" | "20030084329" | "20030035370" | "20040128538" | "20010042200" | "20060230444" | "20020073155" | "20030233328" | "20060212524" | "20070180510" | "7536715" | "20060212572" | "20020178378" | "20040199793" | "20030126468" | "20050050338" | "20060095965" | "20060050719" | "20050262556" | "20040049574" | "20030101260" | "20040073800" | "20020198956" | "20040190522" | "20070157316" | "20050182950" | "20040117624" | "20040148520" | "20070056030" | "20040004941" | "20030061514" | "20030014665" | "20060193470" | "20080176536" | "7409712" | "20020133721" | "20020166063" | "20030204632" | "20060137012" | "7574740" | "20050086502" | "7331060" | "20030023733" | "20070180511" | "20020162026" | "20050037733" | "20050039104" | "7702739" | "20020073337" | "20030145225" | "20050180416" | "20020083175" | "20060048142").PN.	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/18 23:55
S5	3	(centripetal networks).as.	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/18 14:50

S4	95	(moore adj3 sean).in.	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/18 14:49
S3	443	(rogers adj3 steven).in.	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/18 14:49
S2	5511	726/1.CCLS.	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/18 14:49
S1	19	("20120113987" | "20060195896" | "7684400" | "20060248580" | "20110055916" | "0000000" | "20110270956" | "20130059527" | "20100011434" | "20120264443" | "6226372" | "20040151155" | "20030212900" | "20050117576" | "20060048142" | "20030188192" | "7721084" | "20030123456" | "20070083924" | "20100211678").PN.	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/18 14:49

10/ 20/ 2014 2:28:30 AM
C:\ Users\ kchang3\ Documents\ EAST\ Workspaces\ 13657010_APP.wsp

SEARCH RESULTS

You searched for: policy gateway packet filter central server packet rule set

5 Results returned

Research on the Defense Against ARP Spoofing Attacks Based on Winpcap
Wenjian Xing ; Yunlan Zhao ; Tonglei Li
Education Technology and Computer Science (ETCS), 2010 Second International Workshop on
Volume: 1
DOI: 10.1109/ETCS.2010.75
Publication Year: 2010 , Page(s): 762 - 765
Cited by: Papers (1)
IEEE CONFERENCE PUBLICATIONS

A redirection-based defense mechanism against flood-type attacks in large-scale ISP networks
Hamano, T. ; Suzuki, R. ; Ikegawa, T. ; Ichikawa, H.
Communications, 2004 and the 5th International Symposium on Multi-Dimensional Mobile Communications Proceedings. The 2004 Joint Conference of the 10th Asia-Pacific Conference on
Volume: 2
DOI: 10.1109/APCC.2004.1391773
Publication Year: 2004 , Page(s): 543 - 547 vol.2
Cited by: Papers (1) | Patents (7)
IEEE CONFERENCE PUBLICATIONS

Tuple Based Approach for Anomalies Detection within Firewall Filtering Rules
Benelbahri, M.A. ; Bouhoula, A.
Computers and Communications, 2007. ISCC 2007. 12th IEEE Symposium on
DOI: 10.1109/ISCC.2007.4381486
Publication Year: 2007 , Page(s): 63 - 70
Cited by: Papers (3)
IEEE CONFERENCE PUBLICATIONS

Adaptive optimization of packet filtering **devices performance ensuring a conflict-free network configuration**
Maiolini, G. ; Cignini, L. ; Baiocchi, A.
INFOCOM Workshops 2008, IEEE
DOI: 10.1109/INFOCOM.2008.4544614
Publication Year: 2008 , Page(s): 1 - 6
IEEE CONFERENCE PUBLICATIONS

IEEE Standard for Broadband over Power Line Networks: Medium Access Control and Physical Layer Specifications

IEEE Std 1901-2010
DOI: 10.1109/IEEESTD.2010.5678772
Publication Year: 2010 , Page(s): 1 - 1586
Cited by: Papers (1)
IEEE STANDARDS

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**		
	Application Number	13657010
	Filing Date	2012-10-22
	First Named Inventor	Steven Rogers
	Art Unit	2438
	Examiner Name	K. W. Chang
	Attorney Docket Number	007742.00017

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
/K.C./	1	20060048142		2006-03-02	Roese et al.	
/K.C./	2	20100011434		2010-01-14	Kay	

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
/K.C./	1	2385676	EP	A1	2011-11-09	Alcatel Lucent		☐
/K.C./	2	2498442	EP	A1	2012-09-12	Openet Telecom Ltd		☐

EFS Web 2.1.17

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.C./

Receipt date: 07/03/2014	Application Number	13657010 13657010 - GAU: 2438
INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**	Filing Date	2012-10-22
	First Named Inventor	Steven Rogers
	Art Unit	2438
	Examiner Name	K. W. Chang
	Attorney Docket Number	007742.00017

If you wish to add additional Foreign Patent Document citation information please click the Add button **Add**

NON-PATENT LITERATURE DOCUMENTS **Remove**

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
/K.C./	1	ISR off International Application No. PCT/US2014/027723, dated June 26, 2014.	☐
/K.C./	2	""SBIR Case Study: Centripetal Networks Subtitle: How CNI Leveraged DHS S&T SBIR Funding to Launch a Successful Cyber Security Company, Cyber Security Division, 2012 Principal Investigators' Meeting"; Sean Moore, October 10, 2012.	☐
/K.C./	3	"Control Plane Policing Implementation Best Practices"; Cisco Systems; March 13, 2013; <https://web.archive.org/web/20130313135143/http:www.cisco.com/web/about/security/intelligence/coppwp_gs.html>	☐

If you wish to add additional non-patent literature document citation information please click the Add button **Add**

EXAMINER SIGNATURE

Examiner Signature	/Kenneth Chang/	Date Considered	10/18/2014

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.C./

Receipt date: 12/02/2013

13657010 - GAU: 2438

Doc code: IDS

Doc description: Information Disclosure Statement (IDS) Filed

PTO/SB/08a (01-10)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**		
	Application Number	13657010
	Filing Date	2012-10-22
	First Named Inventor	Steven ROGERS
	Art Unit	2438
	Examiner Name	~~Lynch, Charon C.~~ Kenneth Chang
	Attorney Docket Number	007742.00017

U.S.PATENTS						Remove
Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
/K.C./	1	6226372	B1	2001-05-01	Beebe et al.	
If you wish to add additional U.S. Patent citation information please click the Add button.						Add

U.S.PATENT APPLICATION PUBLICATIONS						Remove
Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					
If you wish to add additional U.S. Published Application citation information please click the Add button.						Add

FOREIGN PATENT DOCUMENTS								Remove
Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
/K.C./	1	1677484	EP	A2	2006-07-05	MICROSOFT CORPORATION		☐
If you wish to add additional Foreign Patent Document citation information please click the Add button								Add

NON-PATENT LITERATURE DOCUMENTS			Remove
Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]

EFS Web 2.1.17

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.C./

Receipt date: 12/02/2013	Application Number	13657010 13657010 - GAU: 2438
INFORMATION DISCLOSURE STATEMENT BY APPLICANT	Filing Date	2012-10-22
	First Named Inventor	Steven ROGERS
(Not for submission under 37 CFR 1.99)	Art Unit	2438
	Examiner Name	~~Lynch, Sharon S.~~ Kenneth Chang
	Attorney Docket Number	007742.00017

/K.C./	1	Copy of ISR for PCT/US2013/057502 dated November 7, 2013.	☐

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature	/Kenneth Chang/	Date Considered	10/18/2014

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.C./

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13657010	ROGERS ET AL.
	Examiner	**Art Unit**
	KENNETH CHANG	2438

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	10/20/2014								
	1	✓								
	2	✓								
	3	✓								
	4	✓								
	5	✓								
	6	✓								
	7	O								
	8	✓								
	9	✓								
	10	O								
	11	✓								
	12	✓								
	13	✓								
	14	✓								
	15	✓								
	16	✓								
	17	✓								
	18	✓								
	19	✓								
	20	✓								
	21	✓								
	22	✓								

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**		
	Application Number	13657010
	Filing Date	2012-10-22
	First Named Inventor	Steven Rogers
	Art Unit	2438
	Examiner Name	K. W. Chang
	Attorney Docket Number	007742.00017

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
/K.C./	1	20030123456	A1	2003-07-03	Denz et al.	
/K.C./	2	20070083924	A1	2007-04-12	Lu	

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							☐

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

EFS Web 2.1.17 ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.C./

Receipt date: 06/25/2014	Application Number	13657010 13657010 - GAU: 2438
INFORMATION DISCLOSURE STATEMENT BY APPLICANT	Filing Date	2012-10-22
	First Named Inventor	Steven Rogers
	Art Unit	2438
(Not for submission under 37 CFR 1.99)	Examiner Name	K. W. Chang
	Attorney Docket Number	007742.00017

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
/K.C./	1	International Search Report off International Application No. PCT/US2014/023286, dated June 24, 2014.	☐

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature	/Kenneth Chang/	Date Considered	10/18/2014

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.C./

Doc code: IDS

Doc description: Information Disclosure Statement (IDS) Filed

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99**)		
	Application Number	13657010
	Filing Date	2012-10-22
	First Named Inventor	Steven ROGERS
	Art Unit	~~2438~~ 2438
	Examiner Name	~~TBD~~ Kenneth Chang
	Attorney Docket Number	007742.00017

U.S.PATENTS						
Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Patent citation information please click the Add button.

U.S.PATENT APPLICATION PUBLICATIONS						
Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
/K.C./	1	20060195896		2006-08-31	Fulp et al.	
	2	20060248580		2006-11-02	Fulp et al.	
	3	20110055916		2011-03-03	Ahn	

If you wish to add additional U.S. Published Application citation information please click the Add button.

FOREIGN PATENT DOCUMENTS								
Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							☐

EFS Web 2.1.17

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.C./

Receipt date: 12/13/2012	Application Number	13657010 13657010 - GAU: 2438
INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99**)	Filing Date	2012-10-22
	First Named Inventor	Steven ROGERS
	Art Unit	~~2494~~ 2438
	Examiner Name	~~TBD~~ Kenneth Chang
	Attorney Docket Number	007742.00017

If you wish to add additional Foreign Patent Document citation information please click the Add button

NON-PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
/K.C./	1	John Kindervag; "Build Security Into Your Network's DNA: The Zero Trust Network Architecture"; Forrester Research Inc.; November 5, 2010; pps. 1-26.	☐
/K.C./	2	Palo Alto Networks; "Designing A Zero Trust Network With Next-Generation Firewalls"; pps. 1-10; last viewed on October 21, 2012.	☐

If you wish to add additional non-patent literature document citation information please click the Add button

EXAMINER SIGNATURE

Examiner Signature	/Kenneth Chang/	Date Considered	10/18/2014

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.C./

PTO/SB/08a (01-10)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	13657010
Filing Date	2012-10-22
First Named Inventor	Steven ROGERS
Art Unit	2438
Examiner Name	Chang, Kenneth W.
Attorney Docket Number	007742.00017

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	7539186	B2	2009-05-26	Aerrabotu et al.	
	2	7710885	B2	2010-05-04	Ilnicki et al.	
	3	8856926	B2	2014-10-07	Narayanaswamy et al.	

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							☐

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13657010
	Filing Date	2012-10-22
	First Named Inventor	Steven ROGERS
	Art Unit	2438
	Examiner Name	Chang, Kenneth W.
	Attorney Docket Number	007742.00017

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1	REUMANN, John et al., "Adaptive Packet Filters," Department of Electrical Engineering and Computer Science, The University of Michigan, Ann Arbor, MI, IEEE, 2001.	☐
	2	GREENWALD, Michael et al., "Designing an Academic Firewall: Policy, Practice, and Experience with SURF," Department of Computer Science, Stanford University, Stanford, CA, IEEE, Proceedings of SNDSS, 1996.	☐

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**		
	Application Number	13657010
	Filing Date	2012-10-22
	First Named Inventor	Steven ROGERS
	Art Unit	2438
	Examiner Name	Chang, Kenneth W.
	Attorney Docket Number	007742.00017

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☐ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

☐ See attached certification statement.

☒ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/William E. Wooten/	Date (YYYY-MM-DD)	2014-11-25
Name/Print	William E. Wooten	Registration Number	60049

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Electronic Patent Application Fee Transmittal	
Application Number:	13657010
Filing Date:	22-Oct-2012
Title of Invention:	METHODS AND SYSTEMS FOR PROTECTING A SECURED NETWORK
First Named Inventor/Applicant Name:	Steven Rogers
Filer:	William Eugene Wooten
Attorney Docket Number:	007742.00017
Filed as Large Entity	

Utility under 35 USC 111(a) Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
Submission- Information Disclosure Stmt	1806	1	180	180
		Total in USD ($)		**180**

Electronic Acknowledgement Receipt

EFS ID:	20802774
Application Number:	13657010
International Application Number:	
Confirmation Number:	2390
Title of Invention:	METHODS AND SYSTEMS FOR PROTECTING A SECURED NETWORK
First Named Inventor/Applicant Name:	Steven Rogers
Customer Number:	22907
Filer:	William Eugene Wooten
Filer Authorized By:	
Attorney Docket Number:	007742.00017
Receipt Date:	25-NOV-2014
Filing Date:	22-OCT-2012
Time Stamp:	18:29:38
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$180
RAM confirmation Number	5772
Deposit Account	190733
Authorized User	
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows: Charge any Additional Fees required under 37 C.F.R. Section 1.16 (National application filing, search, and examination fees) Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)	

Charge any Additional Fees required under 37 C.F.R. Section 1.19 (Document supply fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.20 (Post Issuance fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.21 (Miscellaneous fees and charges)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Information Disclosure Statement (IDS) Form (SB08)	IDS.pdf	612555 524f5d7c5c683d3f3c5f3ec298d7b2f4b3debb5a	no	4
Warnings:					
Information:					
2	Non Patent Literature	NPL1.pdf	507671 6740bd120958939e87fc90a8262baad96e26f861	no	5
Warnings:					
Information:					
3	Non Patent Literature	NPL2.pdf	1464667 f99fa81447cc68e17deee719d658cdb0a3edfb87	no	14
Warnings:					
Information:					
4	Fee Worksheet (SB06)	fee-info.pdf	30336 344f33e9119a11af48332aea3b422796f7b75559	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	2615229		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

<u>New Applications Under 35 U.S.C. 111</u>
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

<u>National Stage of an International Application under 35 U.S.C. 371</u>
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

<u>New International Application Filed with the USPTO as a Receiving Office</u>
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

Doc code: IDS
Doc description: Information Disclosure Statement (IDS) Filed

PTO/SB/08a (01-10)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**		
	Application Number	13657010
	Filing Date	2012-10-22
	First Named Inventor	Steven ROGERS
	Art Unit	2438
	Examiner Name	Chang, Kenneth W.
	Attorney Docket Number	007742.00017

U.S.PATENTS						Remove
Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					
If you wish to add additional U.S. Patent citation information please click the Add button.						Add

U.S.PATENT APPLICATION PUBLICATIONS						Remove
Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20090172800	A1	2009-07-02	Wool	
	2	20080005795	A1	2008-01-03	Acharya et al.	
If you wish to add additional U.S. Published Application citation information please click the Add button.						Add

FOREIGN PATENT DOCUMENTS							Remove	
Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							☐
If you wish to add additional Foreign Patent Document citation information please click the Add button							Add	

NON-PATENT LITERATURE DOCUMENTS	Remove

EFS Web 2.1.17

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13657010
	Filing Date	2012-10-22
	First Named Inventor	Steven ROGERS
	Art Unit	2438
	Examiner Name	Chang, Kenneth W.
	Attorney Docket Number	007742.00017

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1		☐

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**		
	Application Number	13657010
	Filing Date	2012-10-22
	First Named Inventor	Steven ROGERS
	Art Unit	2438
	Examiner Name	Chang, Kenneth W.
	Attorney Docket Number	007742.00017

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☐ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

☐ See attached certification statement.

☒ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/William E. Wooten/	Date (YYYY-MM-DD)	2015-02-18
Name/Print	William E. Wooten	Registration Number	60049

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Electronic Patent Application Fee Transmittal

Application Number:	13657010
Filing Date:	22-Oct-2012
Title of Invention:	METHODS AND SYSTEMS FOR PROTECTING A SECURED NETWORK
First Named Inventor/Applicant Name:	Steven Rogers
Filer:	William Eugene Wooten
Attorney Docket Number:	007742.00017

Filed as Small Entity

Filing Fees for Utility under 35 USC 111(a)

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
Submission- Information Disclosure Stmt	2806	1	90	90
		Total in USD ($)		**90**

Electronic Acknowledgement Receipt

EFS ID:	21534066
Application Number:	13657010
International Application Number:	
Confirmation Number:	2390
Title of Invention:	METHODS AND SYSTEMS FOR PROTECTING A SECURED NETWORK
First Named Inventor/Applicant Name:	Steven Rogers
Customer Number:	22907
Filer:	William Eugene Wooten
Filer Authorized By:	
Attorney Docket Number:	007742.00017
Receipt Date:	18-FEB-2015
Filing Date:	22-OCT-2012
Time Stamp:	19:11:41
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$90
RAM confirmation Number	14499
Deposit Account	190733
Authorized User	
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows: Charge any Additional Fees required under 37 C.F.R. Section 1.16 (National application filing, search, and examination fees) Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)	

Charge any Additional Fees required under 37 C.F.R. Section 1.19 (Document supply fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.20 (Post Issuance fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.21 (Miscellaneous fees and charges)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Information Disclosure Statement (IDS) Form (SB08)	IDS.pdf	612224 95729e319a5f4b5d675d5fc67c1e53cc61b1f7f2	no	4
Warnings:					
Information:					
2	Fee Worksheet (SB06)	fee-info.pdf	30668 ab6ba0cad94dba82f040b5df7ba258cccd5b0e2d	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	642892		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

<u>New Applications Under 35 U.S.C. 111</u>
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

<u>National Stage of an International Application under 35 U.S.C. 371</u>
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

<u>New International Application Filed with the USPTO as a Receiving Office</u>
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re the Application of:		Atty. Docket No.:	007742.00017
Steven ROGERS *et al.*			
Serial No.:	13/657,010	Group Art Unit:	2438
Filed:	October 22, 2012	Examiner:	Chang, Kenneth W.
For:	METHODS AND SYSTEMS FOR PROTECTING A SECURED NETWORK	Confirmation No.:	2390

AMENDMENT UNDER 37 C.F.R. § 1.111

Mail Stop Amendment
Commissioner for Patents
Randolph Building
401 Dulany Street
Alexandria, VA 22314

Dear Sir:

In response to the Non-Final Office Action dated October 21, 2014, please enter the following:

Amendments to the Claims reflected in the Listing of Claims, which begins at page 2 of this paper; and

Remarks, which begin at page 31 of this paper.

Applicant hereby petitions for any applicable extension of time that may be required. If any fees are required or if an overpayment is made, the Commissioner is authorized to debit or credit Deposit Account No. 19-0733, accordingly.

This Listing of Claims will replace all prior versions and listings of claims in the application.

Listing of the Claims:

1. (Currently Amended) A method, comprising:

at each packet security gateway of one or more packet security gateways associated with a security policy management server:

receiving a plurality of dynamic security ~~policy~~ policies from the security policy management server, wherein receiving the plurality of dynamic security policies comprises:

receiving at least one rule specifying a set of network addresses for which associated packets should be forwarded and at least one rule specifying that all packets associated with network addresses outside the set of network addresses for which packets should be forwarded should be dropped;

receiving, at a first time, a dynamic security policy specifying a first set of network addresses for which packets should be forwarded;

receiving, at a second time, a dynamic security policy specifying a second set of network addresses for which packets should be forwarded; and

receiving, at a third time, a dynamic security policy specifying a third set of network addresses for which packets should be forwarded, the second time being after the first time, the third time being after the second time, the second set of network addresses including more network addresses than the first set of network addresses, and the third set of network addresses including more network addresses than the second set of network addresses;

receiving packets associated with a network protected by ~~each respective~~the packet security gateway; and

performing, on a packet by packet basis, at least one of multiple packet transformation functions specified by the plurality of dynamic security ~~policy~~ policies on the packets associated with the network protected by the packet security gateway, wherein performing the at least one of the multiple packet transformation functions specified by the plurality of dynamic security ~~policy~~ policies on the

packets comprises performing at least one packet transformation function other than forwarding or dropping the packets.

2. (Currently Amended) The method of claim 1, wherein the one or more packet security gateways comprise at least two packet security gateways configured in series ~~such that packets forwarded from a first of the at least two packet security gateways are received by a second of the at least two packet security gateways~~, the method comprising:

forwarding, by a first of the at least two packet security gateways and to a second of the at least two packet security gateways, a portion of the packets; and

receiving, by the second of the at least two packet security gateways and from the first of the at least two packet security gateways, the portion of the packets.

3. (Currently Amended) The method of claim 2, wherein [[the]] a dynamic security policy of the plurality of dynamic security policies comprises at least two rules, a second of the at least two rules being ~~required~~ configured to execute ~~subsequent to~~after a first of the at least two rules, ~~and wherein, for the at least two packet security gateways configured in series, performing the at least one of multiple packet transformation functions specified by the dynamic security policy on the packets comprises~~the method comprising:

performing, by the first of the at least two packet security gateways, a ~~first~~ packet transformation function specified by the first of the at least two rules; and

performing, by the second of the at least two packet security gateways, a ~~second~~ packet transformation function specified by the second of the at least two rules.

4. (Currently Amended) The method of claim 1, wherein receiving the plurality of dynamic security ~~policy~~ policies comprises receiving at least one rule specifying a set of network addresses for which associated packets should be dropped and at least one rule specifying that all packets associated with network addresses outside the set of network addresses for which associated packets should be dropped should be forwarded.

5. (Canceled)

6. (Currently Amended) The method of claim [[5]] 1, ~~further~~ comprising:

receiving, by the security policy management server, information associated with a Voice over Internet Protocol (VoIP) session[[,]]; and

~~wherein the at least one rule specifying the set of network addresses for which associated packets should be forwarded is one of created and altered~~creating or altering, by the security policy management server ~~utilizing~~ and based on the information associated with the ~~one or more~~ VoIP ~~sessions~~session, the at least one rule specifying the set of network addresses for which associated packets should be forwarded.

7. (Canceled)

8. (Currently Amended) The method of claim 1, wherein the plurality of dynamic security ~~policy~~ policies ~~comprises at least two rules, a first of the at least two rules specifying a first set of network addresses, a second of the at least two rules specifying a second set of network addresses, and wherein the dynamic security policy specifies~~ specify that a first portion of the packets ~~associated with the first set of network addresses~~ should be placed in a first forwarding queue and a second portion of the packets ~~associated with the second set of network addresses~~ should be placed in a second forwarding queue, the first forwarding queue having a higher forwarding rate than the second forwarding queue, the method comprising:

placing, by the one or more packet security gateways, the first portion of the packets in the first forwarding queue; and

placing, by the one or more packet security gateways, the second portion of the packets in the second forwarding queue.

9. (Currently Amended) The method of claim 1, wherein receiving the plurality of dynamic security ~~policy~~ policies comprises receiving at least one rule specifying ~~a set of network addresses and an additional~~ a parameter, ~~and wherein performing the at least one of multiple packet transformation functions specified by the dynamic security policy on the packets comprises~~the method comprising routing, by the one or more packet security gateways, at least one packet of the packets that ~~falls within the set of network addresses and~~ matches the

~~additional~~ parameter to a network address different from a destination network address specified by the at least one ~~of the packets~~packet.

10. (Currently Amended) The method of claim 9, wherein the ~~additional~~ parameter comprises a Session Initiation Protocol (SIP) Uniform Resource Identifier (URI), wherein the network address different from the destination network address specified by the at least one ~~of the packets~~packet corresponds to a network device configured to copy information contained in the at least one ~~of the packets~~packet and forward the at least one ~~of the packets~~packet to the destination network address specified by the at least one ~~of the packets~~packet, and wherein routing the at least one ~~of the packets that falls within the set of network addresses and matches the additional parameter to a network address different from the destination network address specified by the at least one of the packets~~packet comprises encapsulating the at least one ~~of the packets that falls within the set of network addresses and matches the additional parameter~~packet with a header containing the network address different from the destination network address specified by the at least one ~~of the packets~~packet.

11. (Currently Amended) The method of claim 1, wherein performing the at least one of the multiple packet transformation functions comprises at least one of forwarding the packets into the network protected by the packet security gateway, forwarding the packets out of the network protected by the packet security gateway, forwarding the packets to an Internet Protocol Security (IPsec) stack having an IPsec security association corresponding to the packets, [[and]] or dropping the packets.

12. (Currently Amended) The method of claim 1, wherein receiving the plurality of dynamic security ~~policy~~ policies comprises ~~a plurality of rules, and wherein~~ receiving at least one ~~of the rules specifies~~rule comprising a five-tuple~~, the five-tuple~~ specifying one or more protocols, one or more ~~IP~~ Internet Protocol (IP) source addresses, one or more source port values, one or more IP destination addresses, and one or more destination port values.

13. (Currently Amended) The method of claim 1, wherein receiving the plurality of dynamic security ~~policy~~ policies comprises ~~a plurality of rules, and wherein~~ receiving at least one ~~of~~

~~the rules specifies~~rule comprising a Differentiated Service Code Point (DSCP) selector that maps to a DSCP field in an Internet Protocol (IP) header of the packets.

14. (Currently Amended) The method of claim 1, ~~wherein~~ comprising operating, by at least one of the one or more packet security gateways, ~~operates~~ in a network layer transparent manner by sending and receiving traffic at a link layer using an interface that is not addressed at the network layer and performing the at least one of the multiple packet transformation functions at the network layer.

15. (Currently Amended) The method of claim 14, wherein the at least one of the one or more packet security gateways includes a management interface having a network layer address, ~~and wherein~~the method comprising securing access to the management interface ~~is secured~~ at at least one of an application level, a link level, [[and]] or a transport level.

16. (Currently Amended) The method of claim 1, ~~wherein the dynamic security policy comprises one or more rules generated based, at least in part, on a list of known network addresses associated with malicious network traffic that is received~~comprising:

receiving, by the security policy management server and from a subscription service that aggregates information associated with malicious network traffic, a list of network addresses known to be associated with malicious network traffic; and

generating, by the security policy management server and based at least in part on the list, one or more rules included in the plurality of dynamic security policies.

17. (Currently Amended) The method of claim 1, ~~wherein~~ comprising receiving, by at least two of the one or more packet security gateways ~~receive dynamic security policies~~and from the security policy management server, ~~that include~~ one or more rules specifying source addresses that correspond to spoofed network addresses, [[and]] wherein at least one rule of the ~~dynamic security policies~~one or more rules specifies different source addresses ~~that correspond to spoofed network addresses~~ than at least another ~~one of the dynamic security policies~~rule of the one or more rules.

18. (Currently Amended) The method of claim 1, ~~wherein~~ comprising locating at least one of the one or more packet security gateways ~~is located~~ at each boundary between a protected network associated with the security policy management server and an unprotected network.

19. (Currently Amended) A system, comprising:

a security policy management server; and

one or more packet security gateways associated with the security policy management server, wherein each packet security gateway of the one or more packet security gateways is configured to:

receive a plurality of dynamic security ~~policy~~ policies from the security policy management server;

receive at least one rule specifying a set of network addresses for which associated packets should be forwarded and at least one rule specifying that all packets associated with network addresses outside the set of network addresses for which packets should be forwarded should be dropped;

receive, at a first time, a dynamic security policy specifying a first set of network addresses for which packets should be forwarded;

receive, at a second time, a dynamic security policy specifying a second set of network addresses for which packets should be forwarded;

receive, at a third time, a dynamic security policy specifying a third set of network addresses for which packets should be forwarded, the second time being after the first time, the third time being after the second time, the second set of network addresses including more network addresses than the first set of network addresses, and the third set of network addresses including more network addresses than the second set of network addresses;

receive packets associated with a network protected by ~~each respective~~the packet security gateway; and

perform, on a packet by packet basis, at least one of multiple packet transformation functions specified by the plurality of dynamic security ~~policy~~ policies on the packets associated with the network protected by the packet security gateway, wherein each of the one or more packet security gateways is configured to

perform the at least one of the multiple packet transformation functions specified by the plurality of dynamic security ~~policy~~ policies on the packets by performing at least one packet transformation function other than forwarding or dropping the packets.

20. (Currently Amended) One or more non-transitory computer-readable media having instructions stored thereon, that when executed ~~by one or more computers~~, cause ~~the one or more computers to: at~~ each packet security gateway of one or more packet security gateways associated with a security policy management server to:

receive a plurality of dynamic security ~~policy~~ policies from the security policy management server;

receive at least one rule specifying a set of network addresses for which associated packets should be forwarded and at least one rule specifying that all packets associated with network addresses outside the set of network addresses for which packets should be forwarded should be dropped;

receive, at a first time, a dynamic security policy specifying a first set of network addresses for which packets should be forwarded;

receive, at a second time, a dynamic security policy specifying a second set of network addresses for which packets should be forwarded;

receive, at a third time, a dynamic security policy specifying a third set of network addresses for which packets should be forwarded, the second time being after the first time, the third time being after the second time, the second set of network addresses including more network addresses than the first set of network addresses, and the third set of network addresses including more network addresses than the second set of network addresses;

receive packets associated with a network protected by ~~each respective~~the packet security gateway; and

perform, on a packet by packet basis, at least one of multiple packet transformation functions specified by the plurality of dynamic security ~~policy~~ policies on the packets associated with the network protected by the packet security gateway, wherein each of the one or more packet security gateways is configured to perform the at least one of the multiple packet transformation functions specified by the plurality of dynamic security

~~policy~~ policies on the packets by performing at least one packet transformation function other than forwarding or dropping the packets.

21-22. (Canceled)

23. (New) The system of claim 19, wherein:

the one or more packet security gateways comprise at least two packet security gateways configured in series;

a first of the at least two packet security gateways being configured to forward a portion of the packets to a second of the at least two packet security gateways; and

the second of the at least two packet security gateways being configured to receive the portion of the packets from the first of the at least two packet security gateways.

24. (New) The system of claim 23, wherein:

a dynamic security policy of the plurality of dynamic security policies comprises at least two rules, a second of the at least two rules being configured to execute after a first of the at least two rules;

the first of the at least two packet security gateways is configured to perform a packet transformation function specified by the first of the at least two rules; and

the second of the at least two packet security gateways is configured to perform a packet transformation function specified by the second of the at least two rules.

25. (New) The system of claim 19, wherein each packet security gateway of the one or more packet security gateways is configured to receive at least one rule specifying a set of network addresses for which associated packets should be dropped and at least one rule specifying that all packets associated with network addresses outside the set of network addresses for which associated packets should be dropped should be forwarded.

26. (New) The system of claim 19, wherein the security policy management server is configured to:

receive information associated with a Voice over Internet Protocol (VoIP) session; and

at least one of create or alter, based on the information associated with the VoIP session, the at least one rule specifying the set of network addresses for which associated packets should be forwarded.

27. (New) The system of claim 19, wherein:

the plurality of dynamic security policies specify that a first portion of the packets should be placed in a first forwarding queue and a second portion of the packets should be placed in a second forwarding queue, the first forwarding queue having a higher forwarding rate than the second forwarding queue; and

the one or more packet security gateways are configured to:

place the first portion of the packets in the first forwarding queue; and

place the second portion of the packets in the second forwarding queue.

28. (New) The system of claim 19, wherein:

the plurality of dynamic security policies comprises at least one rule specifying a parameter; and

the one or more packet security gateways are configured to route at least one packet of the packets that matches the parameter to a network address different from a destination network address specified by the at least one packet.

29. (New) The system of claim 28, wherein:

the parameter comprises a Session Initiation Protocol (SIP) Uniform Resource Identifier (URI);

the network address different from the destination network address specified by the at least one packet corresponds to a network device configured to copy information contained in the at least one packet and forward the at least one packet to the destination network address specified by the at least one packet; and

the one or more packet security gateways are configured to encapsulate the at least one packet with a header containing the network address different from the destination network address specified by the at least one packet.

30. (New) The system of claim 19, wherein each packet security gateway of the one or more packet security gateways is configured to at least one of forward the packets into the network protected by the packet security gateway, forward the packets out of the network protected by the packet security gateway, forward the packets to an Internet Protocol Security (IPsec) stack having an IPsec security association corresponding to the packets, or drop the packets.

31. (New) The system of claim 19, wherein each packet security gateway of the one or more packet security gateways is configured to receive at least one rule comprising a five-tuple specifying one or more protocols, one or more Internet Protocol (IP) source addresses, one or more source port values, one or more IP destination addresses, and one or more destination port values.

32. (New) The system of claim 19, wherein each packet security gateway of the one or more packet security gateways is configured to receive at least one rule comprising a Differentiated Service Code Point (DSCP) selector that maps to a DSCP field in an Internet Protocol (IP) header of the packets.

33. (New) The system of claim 19, wherein at least one of the one or more packet security gateways is configured to operate in a network layer transparent manner by sending and receiving traffic at a link layer using an interface that is not addressed at the network layer and performing the at least one of the multiple packet transformation functions at the network layer.

34. (New) The system of claim 33, wherein the at least one of the one or more packet security gateways includes a management interface having a network layer address, and wherein the

at least one of the one or more packet security gateways is configured to secure access to the management interface at at least one of an application level, a link level, or a transport level.

35. (New) The system of claim 19, wherein the security policy management server is configured to:

receive, from a subscription service that aggregates information associated with malicious network traffic, a list of network addresses known to be associated with malicious network traffic; and

generate, based at least in part on the list, one or more rules included in the plurality of dynamic security policies.

36. (New) The system of claim 19, wherein:

at least two of the one or more packet security gateways are configured to receive, from the security policy management server, one or more rules specifying source addresses that correspond to spoofed network addresses; and

at least one rule of the one or more rules specifies different source addresses than at least another rule of the one or more rules.

37. (New) The system of claim 19, wherein at least one of the one or more packet security gateways is located at each boundary between a protected network associated with the security policy management server and an unprotected network.

38. (New) The one or more non-transitory computer-readable media of claim 20, wherein the one or more packet security gateways comprise at least two packet security gateways configured in series, and wherein the instructions, when executed, cause:

a first of the at least two packet security gateways to forward a portion of the packets to a second of the at least two packet security gateways; and

the second of the at least two packet security gateways to receive the portion of the packets from the first of the at least two packet security gateways.

39. (New) The one or more non-transitory computer-readable media of claim 38, wherein a dynamic security policy of the plurality of dynamic security policies comprises at least two rules, a second of the at least two rules being configured to execute after a first of the at least two rules, and wherein the instructions, when executed, cause:

the first of the at least two packet security gateways to perform a packet transformation function specified by the first of the at least two rules; and

the second of the at least two packet security gateways to perform a packet transformation function specified by the second of the at least two rules.

40. (New) The one or more non-transitory computer-readable media of claim 20, wherein the instructions, when executed, cause each packet security gateway of the one or more packet security gateways to receive at least one rule specifying a set of network addresses for which associated packets should be dropped and at least one rule specifying that all packets associated with network addresses outside the set of network addresses for which associated packets should be dropped should be forwarded.

41. (New) The one or more non-transitory computer-readable media of claim 20, wherein the instructions, when executed, cause the security policy management server to:

receive information associated with a Voice over Internet Protocol (VoIP) session; and

at least one of create or alter, based on the information associated with the VoIP session, the at least one rule specifying the set of network addresses for which associated packets should be forwarded.

42. (New) The one or more non-transitory computer-readable media of claim 20, wherein the plurality of dynamic security policies specify that a first portion of the packets should be placed in a first forwarding queue and a second portion of the packets should be placed in a second forwarding queue, the first forwarding queue having a higher forwarding rate than the second forwarding queue, and wherein the instructions, when executed, cause the one or more packet security gateways to:

place the first portion of the packets in the first forwarding queue; and

place the second portion of the packets in the second forwarding queue.

43. (New) The one or more non-transitory computer-readable media of claim 20, wherein the plurality of dynamic security policies comprises at least one rule specifying a parameter, and wherein the instructions, when executed, cause the one or more packet security gateways to route at least one packet of the packets that matches the parameter to a network address different from a destination network address specified by the at least one packet.

44. (New) The one or more non-transitory computer-readable media of claim 43, wherein the parameter comprises a Session Initiation Protocol (SIP) Uniform Resource Identifier (URI), wherein the network address different from the destination network address specified by the at least one packet corresponds to a network device configured to copy information contained in the at least one packet and forward the at least one packet to the destination network address specified by the at least one packet, and wherein the instructions, when executed, cause the one or more packet security gateways to encapsulate the at least one packet with a header containing the network address different from the destination network address specified by the at least one packet.

45. (New) The one or more non-transitory computer-readable media of claim 20, wherein the instructions, when executed, cause each packet security gateway of the one or more packet security gateways to at least one of forward the packets into the network protected by the packet security gateway, forward the packets out of the network protected by the packet security gateway, forward the packets to an Internet Protocol Security (IPsec) stack having an IPsec security association corresponding to the packets, or drop the packets.

46. (New) The one or more non-transitory computer-readable media of claim 20, wherein the instructions, when executed, cause each packet security gateway of the one or more packet security gateways to receive at least one rule comprising a five-tuple specifying one or more protocols, one or more Internet Protocol (IP) source addresses, one or more source port values, one or more IP destination addresses, and one or more destination port values.

47. (New) The one or more non-transitory computer-readable media of claim 20, wherein the instructions, when executed, cause each packet security gateway of the one or more packet security gateways to receive at least one rule comprising a Differentiated Service Code Point (DSCP) selector that maps to a DSCP field in an Internet Protocol (IP) header of the packets.

48. (New) The one or more non-transitory computer-readable media of claim 20, wherein the instructions, when executed, cause at least one packet security gateway of the one or more packet security gateways to operate in a network layer transparent manner by sending and receiving traffic at a link layer using an interface that is not addressed at the network layer and performing the at least one of the multiple packet transformation functions at the network layer.

49. (New) The one or more non-transitory computer-readable media of claim 48, wherein the at least one of the one or more packet security gateways includes a management interface having a network layer address, and wherein the instructions, when executed, cause the at least one packet security gateway of the one or more packet security gateways to secure access to the management interface at at least one of an application level, a link level, or a transport level.

50. (New) The one or more non-transitory computer-readable media of claim 20, wherein the instructions, when executed, cause the security policy management server to:

receive, from a subscription service that aggregates information associated with malicious network traffic, a list of network addresses known to be associated with malicious network traffic; and

generate, based at least in part on the list, one or more rules included in the plurality of dynamic security policies.

51. (New) The one or more non-transitory computer-readable media of claim 20, wherein the instructions, when executed, cause at least two of the one or more packet security gateways to receive, from the security policy management server, one or more rules specifying source

addresses that correspond to spoofed network addresses, at least one rule of the one or more rules specifying different source addresses than at least another rule of the one or more rules.

52. (New) The one or more non-transitory computer-readable media of claim 20, wherein at least one of the one or more packet security gateways is located at each boundary between a protected network associated with the security policy management server and an unprotected network.

53. (New) A method, comprising:

at each of one or more packet security gateways associated with a security policy management server:

receiving, from the security policy management server, a dynamic security policy comprising at least one rule specifying a set of network addresses and a Session Initiation Protocol (SIP) Uniform Resource Identifier (URI);

receiving packets associated with a network protected by the packet security gateway; and

performing, on the packets, on a packet by packet basis, at least one packet transformation function of multiple packet transformation functions specified by the dynamic security policy, wherein performing the at least one packet transformation function comprises:

encapsulating at least one packet of the packets that falls within the set of network addresses and matches the SIP URI with a header containing a network address that is different from a destination network address specified by the at least one packet and that corresponds to a network device configured to copy information contained in the at least one packet and to forward the at least one packet to the destination network address; and

routing the at least one packet to the network address that is different from the destination network address.

54. (New) The method of claim 53, wherein the one or more packet security gateways comprise at least two packet security gateways configured in series, the method comprising:

forwarding, by a first of the at least two packet security gateways, a portion of the packets to a second of the at least two packet security gateways; and

receiving, by the second of the at least two packet security gateways, the portion of the packets from the first of the at least two packet security gateways.

55. (New) The method of claim 54, wherein the dynamic security policy comprises at least two rules, a second of the at least two rules being configured to execute after a first of the at least two rules, the method comprising:

performing, by the first of the at least two packet security gateways, a packet transformation function specified by the first of the at least two rules; and

performing, by the second of the at least two packet security gateways, a packet transformation function specified by the second of the at least two rules.

56. (New) The method of claim 53, wherein receiving the dynamic security policy comprises receiving at least one rule specifying a set of network addresses for which associated packets should be dropped and at least one rule specifying that all packets associated with network addresses outside the set of network addresses for which associated packets should be dropped should be forwarded.

57. (New) The method of claim 53, comprising:

receiving, by the security policy management server, information associated with a Voice over Internet Protocol (VoIP) session; and

creating or altering, by the security policy management server and based on the information associated with the VoIP session, the at least one rule specifying the set of network addresses.

58. (New) The method of claim 53, wherein the dynamic security policy specifies that a first portion of the packets should be placed in a first forwarding queue and a second portion of the packets should be placed in a second forwarding queue, the first forwarding queue having a higher forwarding rate than the second forwarding queue, the method comprising:

placing, by the one or more packet security gateways, the first portion of the packets in the first forwarding queue; and

placing, by the one or more packet security gateways, the second portion of the packets in the second forwarding queue.

59. (New) The method of claim 53, wherein performing the at least one packet transformation function comprises at least one of forwarding the packets into the network protected by the packet security gateway, forwarding the packets out of the network protected by the packet security gateway, forwarding the packets to an Internet Protocol Security (IPsec) stack having an IPsec security association corresponding to the packets, or dropping the packets.

60. (New) The method of claim 53, wherein receiving the dynamic security policy comprises receiving at least one rule comprising a five-tuple specifying one or more protocols, one or more Internet Protocol (IP) source addresses, one or more source port values, one or more IP destination addresses, and one or more destination port values.

61. (New) The method of claim 53, wherein receiving the dynamic security policy comprises receiving at least one rule comprising a Differentiated Service Code Point (DSCP) selector that maps to a DSCP field in an Internet Protocol (IP) header of the packets.

62. (New) The method of claim 53, comprising operating, by at least one of the one or more packet security gateways, in a network layer transparent manner by sending and receiving traffic at a link layer using an interface that is not addressed at the network layer and performing the at least one packet transformation function at the network layer.

63. (New) The method of claim 62, wherein the at least one of the one or more packet security gateways includes a management interface having a network layer address, the method comprising securing access to the management interface at at least one of an application level, a link level, or a transport level.

64. (New) The method of claim 53, comprising:

receiving, by the security policy management server and from a subscription service that aggregates information associated with malicious network traffic, a list of network addresses known to be associated with malicious network traffic; and

generating, by the security policy management server and based at least in part on the list, one or more rules included in the dynamic security policy.

65. (New) The method of claim 53, comprising receiving, by at least two of the one or more packet security gateways and from the security policy management server, one or more rules specifying source addresses that correspond to spoofed network addresses, wherein at least one rule of the one or more rules specifies different source addresses than at least another rule of the one or more rules.

66. (New) The method of claim 53, comprising locating at least one of the one or more packet security gateways at each boundary between a protected network associated with the security policy management server and an unprotected network.

67. (New) A system, comprising:

a security policy management server; and

one or more packet security gateways associated with the security policy management server, wherein each packet security gateway of the one or more packet security gateways is configured to:

receive, from the security policy management server, a dynamic security policy comprising at least one rule specifying a set of network addresses and a Session Initiation Protocol (SIP) Uniform Resource Identifier (URI);

receive packets associated with a network protected by the packet security gateway;

perform, on the packets, on a packet by packet basis, at least one packet transformation function of multiple packet transformation functions specified by the dynamic security policy;

encapsulate at least one packet of the packets that falls within the set of network addresses and matches the SIP URI with a header containing a network

address that is different from a destination network address specified by the at least one packet and that corresponds to a network device configured to copy information contained in the at least one packet and to forward the at least one packet to the destination network address; and

route the at least one packet to the network address that is different from the destination network address.

68. (New) The system of claim 67, wherein:

the one or more packet security gateways comprise at least two packet security gateways configured in series;

a first of the at least two packet security gateways being configured to forward a portion of the packets to a second of the at least two packet security gateways; and

the second of the at least two packet security gateways being configured to receive the portion of the packets from the first of the at least two packet security gateways.

69. (New) The system of claim 68, wherein:

the dynamic security policy comprises at least two rules, a second of the at least two rules being configured to execute after a first of the at least two rules;

the first of the at least two packet security gateways is configured to perform a packet transformation function specified by the first of the at least two rules; and

the second of the at least two packet security gateways is configured to perform a packet transformation function specified by the second of the at least two rules.

70. (New) The system of claim 67, wherein each packet security gateway of the one or more packet security gateways is configured to receive at least one rule specifying a set of network addresses for which associated packets should be dropped and at least one rule specifying that all packets associated with network addresses outside the set of network addresses for which associated packets should be dropped should be forwarded.

71. (New) The system of claim 67, wherein the security policy management server is configured to:

receive information associated with a Voice over Internet Protocol (VoIP) session; and

at least one of create or alter, based on the information associated with the VoIP session, the at least one rule specifying the set of network addresses.

72. (New) The system of claim 67, wherein:

the dynamic security policy specifies that a first portion of the packets should be placed in a first forwarding queue and a second portion of the packets should be placed in a second forwarding queue, the first forwarding queue having a higher forwarding rate than the second forwarding queue; and

the one or more packet security gateways are configured to:

place the first portion of the packets in the first forwarding queue; and

place the second portion of the packets in the second forwarding queue.

73. (New) The system of claim 67, wherein each packet security gateway of the one or more packet security gateways is configured to at least one of forward the packets into the network protected by the packet security gateway, forward the packets out of the network protected by the packet security gateway, forward the packets to an Internet Protocol Security (IPsec) stack having an IPsec security association corresponding to the packets, or drop the packets.

74. (New) The system of claim 67, wherein each packet security gateway of the one or more packet security gateways is configured to receive at least one rule comprising a five-tuple specifying one or more protocols, one or more Internet Protocol (IP) source addresses, one or more source port values, one or more IP destination addresses, and one or more destination port values.

75. (New) The system of claim 67, wherein each packet security gateway of the one or more packet security gateways is configured to receive at least one rule comprising a Differentiated Service Code Point (DSCP) selector that maps to a DSCP field in an Internet Protocol (IP) header of the packets.

76. (New) The system of claim 67, wherein at least one of the one or more packet security gateways is configured to operate in a network layer transparent manner by sending and receiving traffic at a link layer using an interface that is not addressed at the network layer and performing the at least one packet transformation function at the network layer.

77. (New) The system of claim 76, wherein the at least one of the one or more packet security gateways includes a management interface having a network layer address, and wherein the at least one of the one or more packet security gateways is configured to secure access to the management interface at at least one of an application level, a link level, or a transport level.

78. (New) The system of claim 67, wherein the security policy management server is configured to:

receive, from a subscription service that aggregates information associated with malicious network traffic, a list of network addresses known to be associated with malicious network traffic; and

generate, based at least in part on the list, one or more rules included in the dynamic security policy.

79. (New) The system of claim 67, wherein:

at least two of the one or more packet security gateways are configured to receive, from the security policy management server, one or more rules specifying source addresses that correspond to spoofed network addresses; and

at least one rule of the one or more rules specifies different source addresses than at least another rule of the one or more rules.

80. (New) The system of claim 67, wherein at least one of the one or more packet security gateways is located at each boundary between a protected network associated with the security policy management server and an unprotected network.

81. (New) One or more non-transitory computer-readable media having instructions stored thereon, that when executed, cause each packet security gateway of one or more packet security gateways associated with a security policy management server to:

receive, from the security policy management server, a dynamic security policy comprising at least one rule specifying a set of network addresses and a Session Initiation Protocol (SIP) Uniform Resource Identifier (URI);

receive packets associated with a network protected by the packet security gateway;

perform, on the packets, on a packet by packet basis, at least one packet transformation function of multiple packet transformation functions specified by the dynamic security policy;

encapsulate at least one packet of the packets that falls within the set of network addresses and matches the SIP URI with a header containing a network address that is different from a destination network address specified by the at least one packet and that corresponds to a network device configured to copy information contained in the at least one packet and to forward the at least one packet to the destination network address; and

route the at least one packet to the network address that is different from the destination network address.

82. (New) The one or more non-transitory computer-readable media of claim 81, wherein the one or more packet security gateways comprise at least two packet security gateways configured in series, and wherein the instructions, when executed, cause:

a first of the at least two packet security gateways to forward a portion of the packets to a second of the at least two packet security gateways; and

the second of the at least two packet security gateways to receive the portion of the packets from the first of the at least two packet security gateways.

83. (New) The one or more non-transitory computer-readable media of claim 82, wherein the dynamic security policy comprises at least two rules, a second of the at least two rules being configured to execute after a first of the at least two rules, and wherein the instructions, when executed, cause:

the first of the at least two packet security gateways to perform a packet transformation function specified by the first of the at least two rules; and

the second of the at least two packet security gateways to perform a packet transformation function specified by the second of the at least two rules.

84. (New) The one or more non-transitory computer-readable media of claim 81, wherein the instructions, when executed, cause each packet security gateway of the one or more packet security gateways to receive at least one rule specifying a set of network addresses for which associated packets should be dropped and at least one rule specifying that all packets associated with network addresses outside the set of network addresses for which associated packets should be dropped should be forwarded.

85. (New) The one or more non-transitory computer-readable media of claim 81, wherein the instructions, when executed, cause the security policy management server to:

receive information associated with a Voice over Internet Protocol (VoIP) session; and

at least one of create or alter, based on the information associated with the VoIP session, the at least one rule specifying the set of network addresses.

86. (New) The one or more non-transitory computer-readable media of claim 81, wherein the dynamic security policy specifies that a first portion of the packets should be placed in a first forwarding queue and a second portion of the packets should be placed in a second forwarding queue, the first forwarding queue having a higher forwarding rate than the second forwarding queue, and wherein the instructions, when executed, cause the one or more packet security gateways to:

place the first portion of the packets in the first forwarding queue; and

place the second portion of the packets in the second forwarding queue.

87. (New) The one or more non-transitory computer-readable media of claim 81, wherein the instructions, when executed, cause each packet security gateway of the one or more packet security gateways to at least one of forward the packets into the network protected by the

packet security gateway, forward the packets out of the network protected by the packet security gateway, forward the packets to an Internet Protocol Security (IPsec) stack having an IPsec security association corresponding to the packets, or drop the packets.

88. (New) The one or more non-transitory computer-readable media of claim 81, wherein the instructions, when executed, cause each packet security gateway of the one or more packet security gateways to receive at least one rule comprising a five-tuple specifying one or more protocols, one or more Internet Protocol (IP) source addresses, one or more source port values, one or more IP destination addresses, and one or more destination port values.

89. (New) The one or more non-transitory computer-readable media of claim 81, wherein the instructions, when executed, cause each packet security gateway of the one or more packet security gateways to receive at least one rule comprising a Differentiated Service Code Point (DSCP) selector that maps to a DSCP field in an Internet Protocol (IP) header of the packets.

90. (New) The one or more non-transitory computer-readable media of claim 81, wherein the instructions, when executed, cause at least one packet security gateway of the one or more packet security gateways to operate in a network layer transparent manner by sending and receiving traffic at a link layer using an interface that is not addressed at the network layer and performing the at least one packet transformation function at the network layer.

91. (New) The one or more non-transitory computer-readable media of claim 90, wherein the at least one of the one or more packet security gateways includes a management interface having a network layer address, and wherein the instructions, when executed, cause the at least one packet security gateway of the one or more packet security gateways to secure access to the management interface at at least one of an application level, a link level, or a transport level.

92. (New) The one or more non-transitory computer-readable media of claim 81, wherein the instructions, when executed, cause the security policy management server to:

receive, from a subscription service that aggregates information associated with malicious network traffic, a list of network addresses known to be associated with malicious network traffic; and

generate, based at least in part on the list, one or more rules included in the dynamic security policy.

93. (New) The one or more non-transitory computer-readable media of claim 81, wherein the instructions, when executed, cause at least two of the one or more packet security gateways to receive, from the security policy management server, one or more rules specifying source addresses that correspond to spoofed network addresses, at least one rule of the one or more rules specifying different source addresses than at least another rule of the one or more rules.

94. (New) The one or more non-transitory computer-readable media of claim 81, wherein at least one of the one or more packet security gateways is located at each boundary between a protected network associated with the security policy management server and an unprotected network.

95. (New) A method, comprising:

communicating, by a security policy management server and to a packet security gateway located at a first boundary of a network protected by the security policy management server, a first dynamic security policy, the first dynamic security policy comprising one or more rules based on the first boundary;

communicating, by the security policy management server and to a packet security gateway located at a second boundary of the network, a second dynamic security policy, the second dynamic security policy comprising one or more rules based on the second boundary that differ from the one or more rules based on the first boundary;

performing, by the packet security gateway located at the first boundary, at least one of multiple packet transformation functions specified by the first dynamic security policy on a plurality of packets associated with the network that correspond to one or more criteria specified by the one or more rules based on the first boundary; and

performing, by the packet security gateway located at the second boundary, at least one of multiple packet transformation functions specified by the second dynamic security policy on a plurality of packets associated with the network that correspond to one or more criteria specified by the one or more rules based on the second boundary.

96. (New) The method of claim 95, wherein:

the first boundary comprises a boundary between the network protected by the security policy management server and a first network that interfaces with the network protected by the security policy management server;

the second boundary comprises a boundary between the network protected by the security policy management server and a second network that interfaces with the network protected by the security policy management server;

the one or more criteria specified by the one or more rules based on the first boundary comprise one or more criteria based on a set of source network addresses for the first network;

the one or more criteria specified by the one or more rules based on the second boundary comprise one or more criteria based on a set of source network addresses for the second network;

performing the at least one of the multiple packet transformation functions specified by the first dynamic security policy comprises dropping at least one packet, received from the first network, comprising a spoofed source address; and

performing the at least one of the multiple packet transformation functions specified by the second dynamic security policy comprises dropping at least one packet, received from the second network, comprising a different spoofed source address.

97. (New) A system, comprising:

a security policy management server;

a first packet security gateway, located at a first boundary of a network protected by the security policy management server, and configured to:

receive, from the security policy management server, a first dynamic security policy, the first dynamic security policy comprising one or more rules based on the first boundary; and

perform, at least one of multiple packet transformation functions specified by the first dynamic security policy on a plurality of packets that correspond to one or more criteria specified by the one or more rules based on the first boundary; and

a second packet security gateway, located at a second boundary of a network protected by the security policy management server, and configured to:

receive, from the security policy management server, a second dynamic security policy, the second dynamic security policy comprising one or more rules based on the second boundary that differ from the one or more rules based on the first boundary; and

perform at least one of multiple packet transformation functions specified by the second dynamic security policy on a plurality of packets that correspond to one or more criteria specified by the one or more rules based on the second boundary.

98. (New) The system of claim 97, wherein:

the first boundary comprises a boundary between the network protected by the security policy management server and a first network that interfaces with the network protected by the security policy management server;

the second boundary comprises a boundary between the network protected by the security policy management server and a second network that interfaces with the network protected by the security policy management server;

the one or more criteria specified by the one or more rules based on the first boundary comprise one or more criteria based on a set of source network addresses for the first network;

the one or more criteria specified by the one or more rules based on the second boundary comprise one or more criteria based on a set of source network addresses for the second network;

the first packet security gateway is configured to drop at least one packet received from the first network based on a determination that the at least one packet received from the first network comprises a spoofed source address; and

the second packet security gateway is configured to drop at least one packet received from the second network based on a determination that the at least one packet received from the second network comprises a different spoofed source address.

99. (New) One or more non-transitory computer-readable media having instructions stored thereon that when executed cause:

a security policy management server to communicate, to a packet security gateway located at a first boundary of a network protected by the security policy management server, a first dynamic security policy, the first dynamic security policy comprising one or more rules based on the first boundary;

the security policy management server to communicate, to a packet security gateway located at a second boundary of the network, a second dynamic security policy, the second dynamic security policy comprising one or more rules based on the second boundary that differ from the one or more rules based on the first boundary;

the packet security gateway located at the first boundary to perform at least one of multiple packet transformation functions specified by the first dynamic security policy on a plurality of packets associated with the network that correspond to one or more criteria specified by the one or more rules based on the first boundary; and

the packet security gateway located at the second boundary to perform at least one of multiple packet transformation functions specified by the second dynamic security policy on a plurality of packets associated with the network that correspond to one or more criteria specified by the one or more rules based on the second boundary.

100. (New) The one or more non-transitory computer-readable media of claim 99, wherein:

the first boundary comprises a boundary between the network protected by the security policy management server and a first network that interfaces with the network protected by the security policy management server;

the second boundary comprises a boundary between the network protected by the security policy management server and a second network that interfaces with the network protected by the security policy management server;

the one or more criteria specified by the one or more rules based on the first boundary comprise one or more criteria based on a set of source network addresses for the first network;

the one or more criteria specified by the one or more rules based on the second boundary comprise one or more criteria based on a set of source network addresses for the second network; and

the instructions, when executed, cause:

the packet security gateway located at the first boundary to drop at least one packet received from the first network based on a determination that the at least one packet received from the first network comprises a spoofed source address; and

the packet security gateway located at the second boundary to drop at least one packet received from the second network based on a determination that the at least one packet received from the second network comprises a different spoofed source address.

REMARKS

The Office Action dated October 21, 2014 ("Office Action"), has been reviewed and these remarks are responsive thereto. By this paper, claims 1-4, 6, and 8-20 have been amended, claims 5, 7, 21, and 22 have been canceled, and claims 23-100 have been added. No new matter has been added. Upon entry of this amendment, claims 1-4, 6, 8-20, and 23-100 will be pending in this application. Reconsideration and allowance of the instant application are respectfully requested.

Rejections Under 35 U.S.C. §§ 102 & 103

Claims 1, 11, 12, 14, 15, and 18-21 stand rejected under 35 U.S.C. § 102(b) as being anticipated by U.S. Patent Application Publication No. 2005/0138204 to Iyer et al. ("Iyer"). **Claims 2 and 3** stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Iyer in view of U.S. Patent Application Publication No. 2011/0055916 to Ahn ("Ahn"). **Claims 4 and 9** stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Iyer in view of U.S. Patent Application Publication No. 2006/0212572 to Afek et al. ("Afek"). **Claim 5** stands rejected under 35 U.S.C. § 103(a) as being unpatentable over Iyer in view of U.S. Patent Application Publication No. 2010/0296441 to Barkan ("Barkan"). **Claim 6** stands rejected under 35 U.S.C. § 103(a) as being unpatentable over Iyer in view of Barkan and further in view of U.S. Patent Application Publication No. 2008/0072307 to Maes ("Maes"). **Claim 8** stands rejected under 35 U.S.C. § 103(a) as being unpatentable over Iyer in view of U.S. Patent Application Publication No. 2005/0141537 to Kumar et al. ("Kumar"). **Claim 13** stands rejected under 35 U.S.C. § 103(a) as being unpatentable over Iyer in view of U.S. Patent Application Publication No. 2003/0142681 to Chen et al. ("Chen"). **Claim 16** stands rejected under 35 U.S.C. § 103(a) as being unpatentable over Iyer in view of U.S. Patent Application Publication No. 2010/0082811 to Van Der Merwe et al. ("Van Der Merwe"). **Claim 17** stands rejected under 35 U.S.C. § 103(a) as being unpatentable over Iyer in view of U.S. Patent Application Publication No. 2011/0088092 to Nguyen et al. ("Nguyen"). **Claim 22** stands rejected under 35 U.S.C. § 103(a) as being unpatentable over Iyer in view of U.S. Patent Application Publication No. 2003/0035370 to Brustoloni ("Brustoloni").

The rejections of claims 5, 21, and 22 are moot due to their cancelation herein. With respect to claims 1-4, 6, 8, 9, and 11-20 and without acquiescing to the propriety of their rejections, Applicant requests reconsideration in light of the amendments made herein.

As indicated below, Applicant appreciates the indication of allowable subject matter in claims 7 and 10. In accordance with the indication of allowable subject matter, independent claim 1 has been amended to recite the features of original claims 5 and 7, independent claims 19 and 20 have been amended to recite features similar to those recited by amended claim 1, and claim 5 has been canceled. Claims 2-4, 6, 8, 9, and 11-18 depend from independent claim 1 and recite additional features. Accordingly, it is respectfully submitted that claims 1-4, 6, 8, 9, and 11-20 are in condition for allowance.

Allowable Subject Matter

Claims 7 and 10 stand objected to as being dependent upon a rejected base claim; however, the Office Action indicates that they would be allowable if rewritten in independent form, including all of the limitations of their base claim and any intervening claims.

As indicated above, Applicant appreciates the indication of allowable subject matter. In accordance with the indication of allowable subject matter, independent claim 1 has been amended to recite the features of original claims 5 and 7, independent claims 19 and 20 have been amended to recite features similar to those recited by amended claim 1, and claims 5 and 7 have been canceled. Claims 2-4, 6, and 8-18 depend from independent claim 1 and recite additional features. Accordingly, it is respectfully submitted that claims 1-4, 6, and 8-20 are in condition for allowance.

New Claims

Claims 23-100 have been added. Support for claims 23-100 is found in the instant specification. No new matter has been added.

In accordance with the indication of allowable subject matter, independent claim 53 recites the features of original claims 1, 9, and 10, and independent claims 67 and 81 recite features similar to those recited by claim 53. Claims 23-37 depend from independent claim 19 and recite additional features. Claims 38-52 depend from independent claim 20 and recite additional features. Claims 54-66 depend from independent claim 53 and recite additional features. Claims 68-80 depend from independent claim 67 and recite additional features. Claims 82-94 depend from independent claim 81 and recite additional features. Accordingly, it is respectfully submitted that claims 23-94 are in condition for allowance.

Independent claim 95 recites, among other features, "communicating, by the security policy management server and to a packet security gateway located at a second boundary of the network, a second dynamic security policy, the second dynamic security policy comprising one or more rules based on the second boundary that differ from the one or more rules based on the first boundary."

Iyer fails to disclose, teach, or suggest these recited features.

Iyer is directed to "a ***unified*** policy management system" that aggregates, abstracts, and shares "reachability information" between endpoints in a VPN tunnel. *See* Iyer, ¶ [0007] (emphasis added). Nowhere does Iyer disclose, teach, or suggest "communicating, by the security policy management server and to a packet security gateway located at a second boundary of the network, a second dynamic security policy, the second dynamic security policy comprising ***one or more rules based on the second boundary that differ from the one or more rules based on the first boundary***," as recited by claim 95.

Without acquiescing to the propriety of any of the alleged combinations of Iyer and Ahn, Iyer and Afek, Iyer and Barkan, Iyer, Barkan, and Maes, Iyer and Kumar, Iyer and Chen, Iyer and Van Der Merwe, Iyer and Nguyen, or Iyer and Brustoloni, Ahn, Afek, Barkan, Maes, Kumar, Chen, Van Der Merwe, Nguyen, and Brustoloni fail to cure the above-noted deficiencies of Iyer. Accordingly, claim 95 distinguishes over any alleged combination of Iyer, Ahn, Afek, Barkan, Maes, Kumar, Chen, Van Der Merwe, Nguyen, and Brustoloni.

Independent claims 97 and 99, while different in scope, recite features similar to those discussed above with respect to claim 95 and similarly distinguish over any alleged combination of Iyer, Ahn, Afek, Barkan, Maes, Kumar, Chen, Van Der Merwe, Nguyen, and Brustoloni.

Claim 96 depends from independent claim 95 and recites additional features. Claim 98 depends from independent claim 97 and recites additional features. Claim 100 depends from independent claim 99 and recites additional features. Accordingly, each of dependent claims 96, 98, and 100 is allowable over any alleged combination of Iyer, Ahn, Afek, Barkan, Maes, Kumar, Chen, Van Der Merwe, Nguyen, and Brustoloni for the same reasons as its respective base claim and further in view of the various novel and non-obvious features recited therein.

[CONCLUSION AND SIGNATURE FOLLOW ON SEPARATE PAGE]

CONCLUSION

If any fees are required or an overpayment is made, the Commissioner is authorized to debit or credit Deposit Account No. 19-0733, accordingly.

All rejections having been addressed, Applicant respectfully submits that the instant application is in condition for allowance and respectfully solicits prompt notification of the same.

The Examiner is invited to call the undersigned at (202) 824-3270 to resolve any outstanding issues.

Respectfully submitted,

BANNER & WITCOFF, LTD.

Dated: February 19, 2015

By: /William E. Wooten/
William E. Wooten
Registration No. 60,049

Banner & Witcoff, Ltd.
1100 13th Street NW, Suite 1200
Washington, D.C. 20005-4051
Telephone: (202) 824-3000
Facsimile: (202) 824-3001

PTO/AIA/22 (03-13)
Approved for use through 7/31/2016. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

PETITION FOR EXTENSION OF TIME UNDER 37 CFR 1.136(a)	Docket Number (Optional) 007742.00017
Application Number 13/657,010	Filed October 22, 2012
For METHODS AND SYSTEMS FOR PROTECTING A SECURED NETWORK	
Art Unit 2438	Examiner Chang, Kenneth W.

This is a request under the provisions of 37 CFR 1.136(a) to extend the period for filing a reply in the above-identified application.

The requested extension and fee are as follows (check time period desired and enter the appropriate fee below):

		Fee	Small Entity Fee	Micro Entity Fee	
☑	One month (37 CFR 1.17(a)(1))	$200	$100	$50	$ 100
☐	Two months (37 CFR 1.17(a)(2))	$600	$300	$150	$
☐	Three months (37 CFR 1.17(a)(3))	$1,400	$700	$350	$
☐	Four months (37 CFR 1.17(a)(4))	$2,200	$1,100	$550	$
☐	Five months (37 CFR 1.17(a)(5))	$3,000	$1,500	$750	$

☑ Applicant asserts small entity status. See 37 CFR 1.27.

☐ Applicant certifies micro entity status. See 37 CFR 1.29.
Form PTO/SB/15A or B or equivalent must either be enclosed or have been submitted previously.

☐ A check in the amount of the fee is enclosed.

☐ Payment by credit card. Form PTO-2038 is attached.

☑ The Director has already been authorized to charge fees in this application to a Deposit Account.

☑ The Director is hereby authorized to charge any fees which may be required, or credit any overpayment, to Deposit Account Number 19-0733.

☑ Payment made via EFS-Web.

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

I am the

☐ applicant.

☑ attorney or agent of record. Registration number 60,049.

☐ attorney or agent acting under 37 CFR 1.34. Registration number _____.

/William E. Wooten/	February 19, 2015
Signature	Date
William E. Wooten	(202) 824-3000
Typed or printed name	Telephone Number

NOTE: This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4 for signature requirements and certifications. Submit multiple forms if more than one signature is required, see below*.

☑ * Total of 1 forms are submitted.

Privacy Act Statement

The **Privacy Act of 1974 (P.L. 93-579)** requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (*i.e.*, GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Electronic Patent Application Fee Transmittal

Application Number:	13657010
Filing Date:	22-Oct-2012
Title of Invention:	METHODS AND SYSTEMS FOR PROTECTING A SECURED NETWORK
First Named Inventor/Applicant Name:	Steven Rogers
Filer:	William Eugene Wooten
Attorney Docket Number:	007742.00017

Filed as Small Entity

Filing Fees for Utility under 35 USC 111(a)

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Claims in excess of 20	2202	74	40	2960
Independent Claims in Excess of 3	2201	5	210	1050
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Extension - 1 month with $0 paid	2251	1	100	100
Miscellaneous:				
		Total in USD ($)		**4110**

Electronic Acknowledgement Receipt	
EFS ID:	21549475
Application Number:	13657010
International Application Number:	
Confirmation Number:	2390
Title of Invention:	METHODS AND SYSTEMS FOR PROTECTING A SECURED NETWORK
First Named Inventor/Applicant Name:	Steven Rogers
Customer Number:	22907
Filer:	William Eugene Wooten
Filer Authorized By:	
Attorney Docket Number:	007742.00017
Receipt Date:	19-FEB-2015
Filing Date:	22-OCT-2012
Time Stamp:	22:01:52
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$4110
RAM confirmation Number	7708
Deposit Account	190733
Authorized User	
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows: Charge any Additional Fees required under 37 C.F.R. Section 1.16 (National application filing, search, and examination fees) Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)	

Charge any Additional Fees required under 37 C.F.R. Section 1.19 (Document supply fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.20 (Post Issuance fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.21 (Miscellaneous fees and charges)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Amendment/Req. Reconsideration-After Non-Final Reject	Amendment.pdf	218483 1ddd2914be66cb6ca1b335f7c18ac082ea6e6cea	no	34
Warnings:					
Information:					
2	Extension of Time	EOT.pdf	163638 3dd4ee38df4287584bccf5895c5e3a5590f6f137	no	2
Warnings:					
Information:					
3	Fee Worksheet (SB06)	fee-info.pdf	33902 68759ecb4b7057790f5efd84f5da6705f2f7c5cd	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	416023		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re the Application of:		Atty. Docket No.:	007742.00017
Steven ROGERS *et al.*			
Serial No.:	13/657,010	Group Art Unit:	2438
Filed:	October 22, 2012	Examiner:	Chang, Kenneth W.
For:	METHODS AND SYSTEMS FOR PROTECTING A SECURED NETWORK	Confirmation No.:	2390

REFUND REQUEST

Commissioner for Patents
Randolph Building
401 Dulany Street
Alexandria, VA 22314

Dear Sir:

Applicant's undersigned representative mistakenly paid the $180 fee (fee code 1806) prescribed by 37 C.F.R. § 1.17(p) for the filing of an information disclosure statement under 37 C.F.R. § 1.97 on November 25, 2014, instead of the appropriate $90 small-entity-status fee (fee code 2806). Accordingly, Applicant respectfully requests that the mistaken overpayment of $90 be credited to Deposit Account No. 19-0733.

Respectfully submitted,

BANNER & WITCOFF, LTD.

Dated: February 20, 2015

By: /William E. Wooten/
William E. Wooten
Registration No. 60,049

Banner & Witcoff, Ltd.
1100 13th Street NW, Suite 1200
Washington, D.C. 20005-4051
Telephone: (202) 824-3000
Facsimile: (202) 824-3001

Electronic Acknowledgement Receipt

EFS ID:	21549847
Application Number:	13657010
International Application Number:	
Confirmation Number:	2390
Title of Invention:	METHODS AND SYSTEMS FOR PROTECTING A SECURED NETWORK
First Named Inventor/Applicant Name:	Steven Rogers
Customer Number:	22907
Filer:	William Eugene Wooten
Filer Authorized By:	
Attorney Docket Number:	007742.00017
Receipt Date:	20-FEB-2015
Filing Date:	22-OCT-2012
Time Stamp:	06:31:16
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Refund Request	Request.pdf	93701 945f38a0092c18706e7c359a6ea855485228a0f9	no	1
Warnings:					
Information:					

Total Files Size (in bytes):	93701

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re the Application of:		Atty. Docket No.:	007742.00017
Steven ROGERS *et al.*			
Serial No.:	13/657,010	Group Art Unit:	2438
Filed:	October 22, 2012	Examiner:	Chang, Kenneth W.
For:	METHODS AND SYSTEMS FOR PROTECTING A SECURED NETWORK	Confirmation No.:	2390

REFUND REQUEST

Commissioner for Patents
Randolph Building
401 Dulany Street
Alexandria, VA 22314

Dear Sir:

Applicant's undersigned representative mistakenly paid the $180 fee (fee code 1806) prescribed by 37 C.F.R. § 1.17(p) for the filing of an information disclosure statement under 37 C.F.R. § 1.97 on November 25, 2014, instead of the appropriate $90 small-entity-status fee (fee code 2806). Accordingly, Applicant respectfully requests that the mistaken overpayment of $90 be credited to Deposit Account No. 19-0733.

Respectfully submitted,

BANNER & WITCOFF, LTD.

Dated: February 20, 2015

By: /William E. Wooten/
William E. Wooten
Registration No. 60,049

Banner & Witcoff, Ltd.
1100 13th Street NW, Suite 1200
Washington, D.C. 20005-4051
Telephone: (202) 824-3000
Facsimile: (202) 824-3001

Electronic Patent Application Fee Transmittal

Application Number:	13657010
Filing Date:	22-Oct-2012
Title of Invention:	METHODS AND SYSTEMS FOR PROTECTING A SECURED NETWORK
First Named Inventor/Applicant Name:	Steven Rogers
Filer:	William Eugene Wooten
Attorney Docket Number:	007742.00017

Filed as Large Entity

Utility under 35 USC 111(a) Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Adjustment date: 03/04/2015 SDIRETA1
11/26/2014 INTEFSW 00005772 190733 13657010
01 FC:1806 180.00 CR

03/04/2015 SDIRETA1 00000004 190733 13657010
01 FC:2806 90.00 DA

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
Submission- Information Disclosure Stmt	1806	1	180	180
		Total in USD ($)		**180**

Doc code: IDS
Doc description: Information Disclosure Statement (IDS) Filed

PTO/SB/08a (01-10)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**		
	Application Number	13657010
	Filing Date	2012-10-22
	First Named Inventor	Steven ROGERS
	Art Unit	2438
	Examiner Name	Chang, Kenneth W.
	Attorney Docket Number	007742.00017

U.S.PATENTS						Remove
Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	8806638	B1	2014-08-12	Mani	
	2	6611875	B1	2003-08-26	Chopra et al.	
If you wish to add additional U.S. Patent citation information please click the Add button.						Add

U.S.PATENT APPLICATION PUBLICATIONS						Remove
Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20090328219	A1	2009-12-31	Narayanaswamy	
	2	20120240135	A1	2012-09-20	Risbood et al.	
	3	20120314617	A1	2012-12-13	Erichsen et al.	
	4	20030097590	A1	2003-05-22	Syvanne	
If you wish to add additional U.S. Published Application citation information please click the Add button.						Add
FOREIGN PATENT DOCUMENTS						Remove

EFS Web 2.1.17

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13657010
	Filing Date	2012-10-22
	First Named Inventor	Steven ROGERS
	Art Unit	2438
	Examiner Name	Chang, Kenneth W.
	Attorney Docket Number	007742.00017

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							☐

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1		☐

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**		
	Application Number	13657010
	Filing Date	2012-10-22
	First Named Inventor	Steven ROGERS
	Art Unit	2438
	Examiner Name	Chang, Kenneth W.
	Attorney Docket Number	007742.00017

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☐ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

☐ See attached certification statement.

☒ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/William E. Wooten/	Date (YYYY-MM-DD)	2015-03-13
Name/Print	William E. Wooten	Registration Number	60049

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Electronic Patent Application Fee Transmittal

Application Number:	13657010
Filing Date:	22-Oct-2012
Title of Invention:	METHODS AND SYSTEMS FOR PROTECTING A SECURED NETWORK
First Named Inventor/Applicant Name:	Steven Rogers
Filer:	William Eugene Wooten
Attorney Docket Number:	007742.00017

Filed as Small Entity

Filing Fees for Utility under 35 USC 111(a)

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
Submission- Information Disclosure Stmt	2806	1	90	90
		Total in USD ($)		**90**

Electronic Acknowledgement Receipt

EFS ID:	21758052
Application Number:	13657010
International Application Number:	
Confirmation Number:	2390
Title of Invention:	METHODS AND SYSTEMS FOR PROTECTING A SECURED NETWORK
First Named Inventor/Applicant Name:	Steven Rogers
Customer Number:	22907
Filer:	William Eugene Wooten
Filer Authorized By:	
Attorney Docket Number:	007742.00017
Receipt Date:	13-MAR-2015
Filing Date:	22-OCT-2012
Time Stamp:	02:58:53
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$90
RAM confirmation Number	7063
Deposit Account	190733
Authorized User	
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows: Charge any Additional Fees required under 37 C.F.R. Section 1.16 (National application filing, search, and examination fees) Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)	

Charge any Additional Fees required under 37 C.F.R. Section 1.19 (Document supply fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.20 (Post Issuance fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.21 (Miscellaneous fees and charges)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Information Disclosure Statement (IDS) Form (SB08)	IDS.pdf	612419 b82245386dc72ff107f8813261f424f55c8958da	no	4
Warnings:					
Information:					
2	Fee Worksheet (SB06)	fee-info.pdf	30669 b424f50f43b42cfdf32f0a7a1c2b1eb139e63480	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	643088		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

NOTICE OF ALLOWANCE AND FEE(S) DUE

22907 7590 04/08/2015
BANNER & WITCOFF, LTD.
1100 13th STREET, N.W.
SUITE 1200
WASHINGTON, DC 20005-4051

EXAMINER	
CHANG, KENNETH W	
ART UNIT	PAPER NUMBER
2438	

DATE MAILED: 04/08/2015

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/657,010	10/22/2012	Steven Rogers	007742.00017	2390

TITLE OF INVENTION: METHODS AND SYSTEMS FOR PROTECTING A SECURED NETWORK

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	$480	$0	$0	$480	07/08/2015

THE APPLICATION IDENTIFIED ABOVE HAS BEEN EXAMINED AND IS ALLOWED FOR ISSUANCE AS A PATENT. PROSECUTION ON THE MERITS IS CLOSED. THIS NOTICE OF ALLOWANCE IS NOT A GRANT OF PATENT RIGHTS. THIS APPLICATION IS SUBJECT TO WITHDRAWAL FROM ISSUE AT THE INITIATIVE OF THE OFFICE OR UPON PETITION BY THE APPLICANT. SEE 37 CFR 1.313 AND MPEP 1308.

THE ISSUE FEE AND PUBLICATION FEE (IF REQUIRED) MUST BE PAID WITHIN THREE MONTHS FROM THE MAILING DATE OF THIS NOTICE OR THIS APPLICATION SHALL BE REGARDED AS ABANDONED. THIS STATUTORY PERIOD CANNOT BE EXTENDED. SEE 35 U.S.C. 151. THE ISSUE FEE DUE INDICATED ABOVE DOES NOT REFLECT A CREDIT FOR ANY PREVIOUSLY PAID ISSUE FEE IN THIS APPLICATION. IF AN ISSUE FEE HAS PREVIOUSLY BEEN PAID IN THIS APPLICATION (AS SHOWN ABOVE), THE RETURN OF PART B OF THIS FORM WILL BE CONSIDERED A REQUEST TO REAPPLY THE PREVIOUSLY PAID ISSUE FEE TOWARD THE ISSUE FEE NOW DUE.

HOW TO REPLY TO THIS NOTICE:

I. Review the ENTITY STATUS shown above. If the ENTITY STATUS is shown as SMALL or MICRO, verify whether entitlement to that entity status still applies.

If the ENTITY STATUS is the same as shown above, pay the TOTAL FEE(S) DUE shown above.

If the ENTITY STATUS is changed from that shown above, on PART B - FEE(S) TRANSMITTAL, complete section number 5 titled "Change in Entity Status (from status indicated above)".

For purposes of this notice, small entity fees are 1/2 the amount of undiscounted fees, and micro entity fees are 1/2 the amount of small entity fees.

II. PART B - FEE(S) TRANSMITTAL, or its equivalent, must be completed and returned to the United States Patent and Trademark Office (USPTO) with your ISSUE FEE and PUBLICATION FEE (if required). If you are charging the fee(s) to your deposit account, section "4b" of Part B - Fee(s) Transmittal should be completed and an extra copy of the form should be submitted. If an equivalent of Part B is filed, a request to reapply a previously paid issue fee must be clearly made, and delays in processing may occur due to the difficulty in recognizing the paper as an equivalent of Part B.

III. All communications regarding this application must give the application number. Please direct all communications prior to issuance to Mail Stop ISSUE FEE unless advised to the contrary.

IMPORTANT REMINDER: Utility patents issuing on applications filed on or after Dec. 12, 1980 may require payment of maintenance fees. It is patentee's responsibility to ensure timely payment of maintenance fees when due.

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), to: Mail **Mail Stop ISSUE FEE**
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
or Fax (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

22907 7590 04/08/2015
BANNER & WITCOFF, LTD.
1100 13th STREET, N.W.
SUITE 1200
WASHINGTON, DC 20005-4051

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission
I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being facsimile transmitted to the USPTO (571) 273-2885, on the date indicated below.

(Depositor's name)
(Signature)
(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/657,010	10/22/2012	Steven Rogers	007742.00017	2390

TITLE OF INVENTION: METHODS AND SYSTEMS FOR PROTECTING A SECURED NETWORK

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	$480	$0	$0	$480	07/08/2015

EXAMINER	ART UNIT	CLASS-SUBCLASS
CHANG, KENNETH W	2438	726-001000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).
- ❑ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.
- ❑ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list
(1) The names of up to 3 registered patent attorneys or agents OR, alternatively,
(2) The name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.
1 _____
2 _____
3 _____

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document has been filed for recordation as set forth in 37 CFR 3.11. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE (B) RESIDENCE: (CITY and STATE OR COUNTRY)

Please check the appropriate assignee category or categories (will not be printed on the patent) : ❑ Individual ❑ Corporation or other private group entity ❑ Government

4a. The following fee(s) are submitted:
- ❑ Issue Fee
- ❑ Publication Fee (No small entity discount permitted)
- ❑ Advance Order - # of Copies _____

4b. Payment of Fee(s): **(Please first reapply any previously paid issue fee shown above)**
- ❑ A check is enclosed.
- ❑ Payment by credit card. Form PTO-2038 is attached.
- ❑ The director is hereby authorized to charge the required fee(s), any deficiency, or credits any overpayment, to Deposit Account Number _____ (enclose an extra copy of this form).

5. **Change in Entity Status** (from status indicated above)
- ❑ Applicant certifying micro entity status. See 37 CFR 1.29 — NOTE: Absent a valid certification of Micro Entity Status (see forms PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.
- ❑ Applicant asserting small entity status. See 37 CFR 1.27 — NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.
- ❑ Applicant changing to regular undiscounted fee status. — NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

NOTE: This form must be signed in accordance with 37 CFR 1.31 and 1.33. See 37 CFR 1.4 for signature requirements and certifications.

Authorized Signature _____ Date _____

Typed or printed name _____ Registration No. _____

PTOL-85 Part B (10-13) Approved for use through 10/31/2013. OMB 0651-0033 U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/657,010	10/22/2012	Steven Rogers	007742.00017	2390

22907 7590 04/08/2015

BANNER & WITCOFF, LTD.
1100 13th STREET, N.W.
SUITE 1200
WASHINGTON, DC 20005-4051

EXAMINER	
CHANG, KENNETH W	

ART UNIT	PAPER NUMBER
2438	

DATE MAILED: 04/08/2015

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)
(Applications filed on or after May 29, 2000)

The Office has discontinued providing a Patent Term Adjustment (PTA) calculation with the Notice of Allowance.

Section 1(h)(2) of the AIA Technical Corrections Act amended 35 U.S.C. 154(b)(3)(B)(i) to eliminate the requirement that the Office provide a patent term adjustment determination with the notice of allowance. See Revisions to Patent Term Adjustment, 78 Fed. Reg. 19416, 19417 (Apr. 1, 2013). Therefore, the Office is no longer providing an initial patent term adjustment determination with the notice of allowance. The Office will continue to provide a patent term adjustment determination with the Issue Notification Letter that is mailed to applicant approximately three weeks prior to the issue date of the patent, and will include the patent term adjustment on the patent. Any request for reconsideration of the patent term adjustment determination (or reinstatement of patent term adjustment) should follow the process outlined in 37 CFR 1.705.

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Customer Service Center of the Office of Patent Publication at 1-(888)-786-0101 or (571)-272-4200.

OMB Clearance and PRA Burden Statement for PTOL-85 Part B

The Paperwork Reduction Act (PRA) of 1995 requires Federal agencies to obtain Office of Management and Budget approval before requesting most types of information from the public. When OMB approves an agency request to collect information from the public, OMB (i) provides a valid OMB Control Number and expiration date for the agency to display on the instrument that will be used to collect the information and (ii) requires the agency to inform the public about the OMB Control Number's legal significance in accordance with 5 CFR 1320.5(b).

The information collected by PTOL-85 Part B is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450. Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Examiner-Initiated Interview Summary	Application No.	Applicant(s)	
	13/657,010	ROGERS ET AL.	
	Examiner	Art Unit	
	KENNETH CHANG	2438	

All participants (applicant, applicant's representative, PTO personnel):

(1) *KENNETH CHANG*. (3)_____.

(2) *WILLIAM WOOTEN*. (4)_____.

Date of Interview: *26 March 2015*.

Type: ☒ Telephonic ☐ Video Conference
☐ Personal [copy given to: ☐ applicant ☐ applicant's representative]

Exhibit shown or demonstration conducted: ☐ Yes ☒ No.
If Yes, brief description: _____.

Issues Discussed ☐101 ☐112 ☐102 ☐103 ☒Others
(For each of the checked box(es) above, please describe below the issue and detailed description of the discussion)

Claim(s) discussed: *19,53,67,81,95,97 and 99*.

Identification of prior art discussed: *N/A*.

Substance of Interview
(For each issue discussed, provide a detailed description and indicate if agreement was reached. Some topics may include: identification or clarification of a reference or a portion thereof, claim interpretation, proposed amendments, arguments of any applied references etc...)

To expedite prosecution, the Examiner made contact with applicants' attorney of record William Wooten (Reg. No. 60,049). Attorney Wooten indicated applicants' authorization to amend claims 19, 53, 67, 81, 95, 97, and 99 to place the application in condition for allowance.

Applicant recordation instructions: It is not necessary for applicant to provide a separate record of the substance of interview.

Examiner recordation instructions: Examiners must summarize the substance of any interview of record. A complete and proper recordation of the substance of an interview should include the items listed in MPEP 713.04 for complete and proper recordation including the identification of the general thrust of each argument or issue discussed, a general indication of any other pertinent matters discussed regarding patentability and the general results or outcome of the interview, to include an indication as to whether or not agreement was reached on the issues raised.

☐ Attachment

/KENNETH CHANG/ Examiner, Art Unit 2438	

Notice of Allowability	Application No. 13/657,010	Applicant(s) ROGERS ET AL.	
	Examiner KENNETH CHANG	Art Unit 2438	AIA (First Inventor to File) Status No

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *the filing on 02/19/2015*.
   ☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on_____.
2. ☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.
3. ☒ The allowed claim(s) is/are *1-4,6,8-20 and 23-100*. As a result of the allowed claim(s), you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to PPHfeedback@uspto.gov .
4. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   Certified copies:
   a) ☐ All b) ☐ Some *c) ☐ None of the:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).
6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☒ Notice of References Cited (PTO-892)
2. ☒ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date 11/25/14, 02/18/15, 03/13/15
3. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
4. ☒ Interview Summary (PTO-413), Paper No./Mail Date *03/26/2015* .
5. ☒ Examiner's Amendment/Comment
6. ☒ Examiner's Statement of Reasons for Allowance
7. ☐ Other _____.

/KENNETH CHANG/
Examiner, Art Unit 2438

DETAILED ACTION

1. This Examiner's Amendment and Reasons for Allowance is in response to the Examiner initiated telephone interview on 03/26/2015.

2. The text of those sections of Title 35 U.S. Code not included in this section can be found in the prior office action.

3. The prior office actions are incorporated herein by reference. In particular, the observations with respect to claim language, and response to previously presented arguments.

Information Disclosure Statement

4. The information disclosure statements (IDS) submitted on 11/25/2014, 02/18/2015, and 03/13/2015 have been placed in the application file, and the information referred therein has been considered as to the merits.

Allowable Subject Matter

5. **Claims 1-4, 6, 8-20, and 23-100** are allowed over the prior art through this Examiner's Amendment.

EXAMINER'S AMENDMENT

6. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with applicants' attorney of record William Wooten (Reg. No. 60,049) on March 26,

2015. Attorney Wooten indicated applicants' authorization to amend claims 19, 53, 67, 81, 95, 97, and 99 to place the application in condition for allowance.

7. Please Enter the Following EXAMINER'S AMENDMENT:

Replace Claim 19 with the following:

19. A system, comprising:

a security policy management server; and

one or more packet security gateways associated with the security policy management server, wherein each packet security gateway of the one or more packet security gateways **[[is]]** **comprises computer hardware and logic** configured to **cause the packet security gateway to**:

receive a plurality of dynamic security policies from the security policy management server;

receive at least one rule specifying a set of network addresses for which associated packets should be forwarded and at least one rule specifying that all packets associated with network addresses outside the set of network addresses for which packets should be forwarded should be dropped;

receive, at a first time, a dynamic security policy specifying a first set of network addresses for which packets should be forwarded;

receive, at a second time, a dynamic security policy specifying a second set of network addresses for which packets should be forwarded;

receive, at a third time, a dynamic security policy specifying a third set of network addresses for which packets should be forwarded, the second time being after the first

time, the third time being after the second time, the second set of network addresses including more network addresses than the first set of network addresses, and the third set of network addresses including more network addresses than the second set of network addresses;

receive packets associated with a network protected by the packet security gateway; and

perform, on a packet by packet basis, at least one of multiple packet transformation functions specified by the plurality of dynamic security policies on the packets associated with the network protected by the packet security gateway, wherein each of the one or more packet security gateways is configured to perform the at least one of the multiple packet transformation functions specified by the plurality of dynamic security policies on the packets by performing at least one packet transformation function other than forwarding or dropping the packets.

Replace Claim 53 with the following:

53. A method, comprising:

at each of one or more packet security gateways associated with a security policy management server:

receiving, from the security policy management server, a dynamic security policy comprising at least one rule specifying a set of network addresses and a Session Initiation Protocol (SIP) Uniform Resource Identifier (URI);

receiving packets associated with a network protected by the packet security gateway; and

performing, on the packets, on a packet by packet basis, at least one packet transformation function of multiple packet transformation functions specified by the dynamic security policy, wherein performing the at least one packet transformation function comprises:

encapsulating at least one packet of the packets that falls within the set of network addresses and matches the SIP URI with a header containing a network address that is different from a destination network address specified by the at least one packet and that corresponds to a network device configured to copy information contained in the at least one packet and to forward the at least one packet to the destination network address; and

routing**, based on the header,** the at least one packet to the network address that is different from the destination network address.

Replace Claim 67 with the following:

67. A system, comprising:

a security policy management server; and

one or more packet security gateways associated with the security policy management server, wherein each packet security gateway of the one or more packet security gateways **[[is]] comprises computer hardware and logic** configured to **cause the packet security gateway to**:

receive, from the security policy management server, a dynamic security policy comprising at least one rule specifying a set of network addresses and a Session Initiation Protocol (SIP) Uniform Resource Identifier (URI);

receive packets associated with a network protected by the packet security gateway;

perform, on the packets, on a packet by packet basis, at least one packet transformation function of multiple packet transformation functions specified by the dynamic security policy;

encapsulate at least one packet of the packets that falls within the set of network addresses and matches the SIP URI with a header containing a network address that is different from a destination network address specified by the at least one packet and that corresponds to a network device configured to copy information contained in the at least one packet and to forward the at least one packet to the destination network address; and

route**, based on the header,** the at least one packet to the network address that is different from the destination network address.

Replace Claim 81 with the following:

81. One or more non-transitory computer-readable media having instructions stored thereon, that when executed, cause each packet security gateway of one or more packet security gateways associated with a security policy management server to:

receive, from the security policy management server, a dynamic security policy comprising at least one rule specifying a set of network addresses and a Session Initiation Protocol (SIP) Uniform Resource Identifier (URI);

receive packets associated with a network protected by the packet security gateway;

perform, on the packets, on a packet by packet basis, at least one packet transformation function of multiple packet transformation functions specified by the dynamic security policy;

encapsulate at least one packet of the packets that falls within the set of network addresses and matches the SIP URI with a header containing a network address that is different from a destination network address specified by the at least one packet and that corresponds to a network device configured to copy information contained in the at least one packet and to forward the at least one packet to the destination network address; and

route**, based on the header,** the at least one packet to the network address that is different from the destination network address.

Replace Claim 95 with the following:

95. A method, comprising:

communicating, by a security policy management server and to a packet security gateway located at a first boundary of a network protected by the security policy

management server, a first dynamic security policy, the first dynamic security policy comprising one or more rules based on the first boundary;

communicating, by the security policy management server and to a packet security gateway located at a second boundary of the network, a second dynamic security policy, the second dynamic security policy comprising one or more rules based on the second boundary that differ from the one or more rules based on the first boundary;

performing, by the packet security gateway located at the first boundary, at least one of multiple packet transformation functions specified by the first dynamic security policy on a plurality of packets associated with the network that correspond to one or more criteria specified by the one or more rules based on the first boundary**, wherein performing the at least one of the multiple packet transformation functions specified by the first dynamic security policy comprises dropping one or more of the plurality of packets associated with the network that correspond to the one or more criteria specified by the one or more rules based on the first boundary**; and

performing, by the packet security gateway located at the second boundary, at least one of multiple packet transformation functions specified by the second dynamic security policy on a plurality of packets associated with the network that correspond to one or more criteria specified by the one or more rules based on the second boundary**, wherein performing the at least one of the multiple packet transformation functions specified by the second dynamic security policy comprises dropping one or more of the plurality of packets associated with the network that**

correspond to the one or more criteria specified by the one or more rules based on the second boundary.

Replace Claim 97 with the following:

97. A system, comprising:

a security policy management server;

a first packet security gateway, located at a first boundary of a network protected by the security policy management server, **[[and]]** **comprising computer hardware and logic** configured to **cause the first packet security gateway to**:

receive, from the security policy management server, a first dynamic security policy, the first dynamic security policy comprising one or more rules based on the first boundary; **[[and]]**

perform, at least one of multiple packet transformation functions specified by the first dynamic security policy on a plurality of packets that correspond to one or more criteria specified by the one or more rules based on the first boundary; and

drop one or more of the plurality of packets associated with the network that correspond to the one or more criteria specified by the one or more rules based on the first boundary; and

a second packet security gateway, located at a second boundary of a network protected by the security policy management server, **[[and]]** **comprising computer hardware and logic** configured to **cause the second packet security gateway to**:

receive, from the security policy management server, a second dynamic security policy, the second dynamic security policy comprising one or more rules based on the second boundary that differ from the one or more rules based on the first boundary; **[[and]]**

perform at least one of multiple packet transformation functions specified by the second dynamic security policy on a plurality of packets that correspond to one or more criteria specified by the one or more rules based on the second boundary**; and**

drop one or more of the plurality of packets associated with the network that correspond to the one or more criteria specified by the one or more rules based on the second boundary.

Replace Claim 99 with the following:

99. One or more non-transitory computer-readable media having instructions stored thereon that when executed cause:

a security policy management server to communicate, to a packet security gateway located at a first boundary of a network protected by the security policy management server, a first dynamic security policy, the first dynamic security policy comprising one or more rules based on the first boundary;

the security policy management server to communicate, to a packet security gateway located at a second boundary of the network, a second dynamic security

policy, the second dynamic security policy comprising one or more rules based on the second boundary that differ from the one or more rules based on the first boundary;

the packet security gateway located at the first boundary **[[to]]** **to:**

perform at least one of multiple packet transformation functions specified by the first dynamic security policy on a plurality of packets associated with the network that correspond to one or more criteria specified by the one or more rules based on the first boundary; and

drop one or more of the plurality of packets associated with the network that correspond to the one or more criteria specified by the one or more rules based on the first boundary; and

the packet security gateway located at the second boundary **[[to]]** **to:**

perform at least one of multiple packet transformation functions specified by the second dynamic security policy on a plurality of packets associated with the network that correspond to one or more criteria specified by the one or more rules based on the second boundary**; and**

drop one or more of the plurality of packets associated with the network that correspond to the one or more criteria specified by the one or more rules based on the second boundary.

Examiner's Statement for Reasons of Allowance

8. The following is an examiner's statement of reasons for allowance:

In interpreting the currently amended claims in light of the specification, the Examiner finds the claimed invention to be patentably distinct from the prior art of record.

Amended independent **Claims 1, 19, 20, 53, 67, 81, 95, 97, and 99** are allowed in view of this Examiner's Amendment and for the reasons argued by Applicants in the Remarks filed 02/19/2015 which are persuasive. **Claims 2-4, 6, 8-18, 23-52, 54-66, 68-80, 82-94, 96, 98, and 100** depend upon one of the allowed independent claims above and are allowed by virtue of their dependencies.

Although the closest prior art **Iyer et al. (US 20050138204 A1)** taught "*a method comprising: at each of one or more packet security gateways* **(e.g. policy enforcers Iyer [0045]-[0046]; [0126])** *associated with a security policy management server* **(e.g. policy server defining managing network services and policies for the organization Iyer [0045])**: *receiving a dynamic security policy* **(e.g. define network policy, firewall policy for policy enforcers in different locations Iyer [0045]; [0046]; [0060]; [0062]; modified policy [0076]; [0086])** *from the security policy management server* **(e.g. policy server includes management module Iyer [0062])**; *receiving packets associated with a network protected* **(e.g. network traffic [0087]-[0089]; receiving traffic flow of packets [0103]; incoming packets [0126])** *by each respective packet security gateway* **(e.g. policy enforcer [0126])**; *and performing, on a packet by packet basis* **(e.g. packet policies enforced Iyer [0126])**, *at least one of*

multiple packet transformation functions **(e.g. performing IPSec security and authentication functions, decode protocols in packets, buffers packets based on policies being enforced, provide bandwidth shaping services to the packets Iyer [0126])** *specified by the dynamic security policy* **(e.g. policy settings stored in the policy database [0126])** *on the packets, wherein performing the at least one of multiple packet transformation functions specified by the dynamic security policy on the packets comprises performing at least one packet transformation function* **(e.g. performing IPSec security and authentication functions, decode protocols in packets, buffers packets based on policies being enforced, provide bandwidth shaping services to the packets Iyer [0126]; storing packet 5-tuple values in stream table, such as source IP, destination IP, source port, destination port, protocol number of incoming packet [0127]; processing the packets based on the policy rules [0128])** *other than forwarding or dropping the packets*",

None of the prior art of record teaches individually or in combination the limitations listed below as recited in Applicants' independent claims:

- [Claim 1] "***receiving, at a first time, a dynamic security policy specifying a first set of network addresses for which packets should be forwarded; receiving, at a second time, a dynamic security policy specifying a second set of network addresses for which packets should be forwarded; and receiving, at a third time, a dynamic security policy specifying a third set of network addresses for which packets should be forwarded, the second time being after the first time, the third time being after the second time, the***

second set of network addresses including more network addresses than the first set of network addresses, and the third set of network addresses including more network addresses than the second set of network addresses";

- [Claim 19] "***to cause the packet security gateway to: receive, at a first time, a dynamic security policy specifying a first set of network addresses for which packets should be forwarded; receive, at a second time, a dynamic security policy specifying a second set of network addresses for which packets should be forwarded; receive, at a third time, a dynamic security policy specifying a third set of network addresses for which packets should be forwarded, the second time being after the first time, the third time being after the second time, the second set of network addresses including more network addresses than the first set of network addresses, and the third set of network addresses including more network addresses than the second set of network addresses***";
- [Claim 20] "***cause each packet security gateway of one or more packet security gateways associated with a security policy management server to: receive, at a first time, a dynamic security policy specifying a first set of network addresses for which packets should be forwarded; receive, at a second time, a dynamic security policy specifying a second set of network addresses for which packets should be forwarded; receive, at a third time, a dynamic security policy specifying a third set of network addresses for***

which packets should be forwarded, the second time being after the first time, the third time being after the second time, the second set of network addresses including more network addresses than the first set of network addresses, and the third set of network addresses including more network addresses than the second set of network addresses";

- [Claim 53] "***at each of one or more packet security gateways associated with a security policy management server: receiving, from the security policy management server, a dynamic security policy comprising at least one rule specifying a set of network addresses and a Session Initiation Protocol (SIP) Uniform Resource Identifier (URI)***";
- [Claim 53] "***encapsulating at least one packet of the packets that falls within the set of network addresses and matches the SIP URI with a header containing a network address that is different from a destination network address specified by the at least one packet and that corresponds to a network device configured to copy information contained in the at least one packet and to forward the at least one packet to the destination network address***; ***and routing, based on the header, the at least one packet to the network address that is different from the destination network address***";
- [Claim 67] "***configured to cause the packet security gateway to: receive***, from the security policy management server, a dynamic security policy

comprising at least one rule ***specifying a set of network addresses and a Session Initiation Protocol (SIP) Uniform Resource Identifier (URI)***";

- [Claim 67] "***encapsulate at least one packet of the packets that falls within the set of network addresses and matches the SIP URI with a header containing a network address that is different from a destination network address specified by the at least one packet and that corresponds to a network device configured to copy information contained in the at least one packet and to forward the at least one packet to the destination network address; and route, based on the header, the at least one packet to the network address that is different from the destination network address***";
- [Claim 81] "***receive, from the security policy management server, a dynamic security policy comprising at least one rule specifying a set of network addresses and a Session Initiation Protocol (SIP) Uniform Resource Identifier (URI)***";
- [Claim 81] "***encapsulate at least one packet of the packets that falls within the set of network addresses and matches the SIP URI with a header containing a network address that is different from a destination network address specified by the at least one packet and that corresponds to a network device configured to copy information contained in the at least one packet and to forward the at least one packet to the destination network address; and route, based on the header, the at least one packet to the network address that is different from the destination network address***";

- [Claim 95] "***performing, by the packet security gateway located at the first boundary, at least one of multiple packet transformation functions specified by the first dynamic security policy on a plurality of packets associated with the network that correspond to one or more criteria specified by the one or more rules based on the first boundary, wherein performing the at least one of the multiple packet transformation functions specified by the first dynamic security policy comprises dropping one or more of the plurality of packets associated with the network that correspond to the one or more criteria specified by the one or more rules based on the first boundary***";
- [Claim 95] "***performing, by the packet security gateway located at the second boundary, at least one of multiple packet transformation functions specified by the second dynamic security policy on a plurality of packets associated with the network that correspond to one or more criteria specified by the one or more rules based on the second boundary, wherein performing the at least one of the multiple packet transformation functions specified by the second dynamic security policy comprises dropping one or more of the plurality of packets associated with the network that correspond to the one or more criteria specified by the one or more rules based on the second boundary***";
- [Claim 97] "***a first packet security gateway, located at a first boundary of a network protected by the security policy management server, comprising***

computer hardware and logic configured to cause the first packet security gateway ***to: perform, at least one of multiple packet transformation functions specified by the first dynamic security policy on a plurality of packets that correspond to one or more criteria specified by the one or more rules based on the first boundary***; ***and a second packet security gateway, located at a second boundary of a network protected by the security policy management server,*** comprising computer hardware and logic configured to cause the second packet security gateway ***to: perform at least one of multiple packet transformation functions specified by the second dynamic security policy on a plurality of packets that correspond to one or more criteria specified by the one or more rules based on the second boundary***";

- [Claim 99] "the security policy management server to communicate, to a packet security gateway located at a second boundary of the network, a second dynamic security policy, ***the second dynamic security policy comprising one or more rules based on the second boundary that differ from the one or more rules based on the first boundary***";
- [Claim 99] "***the packet security gateway located at the first boundary to: perform at least one of multiple packet transformation functions specified by the first dynamic security policy on a plurality of packets associated with the network that correspond to one or more criteria specified by the one or more rules based on the first boundary***; ***and the packet security***

gateway located at the second boundary to: perform at least one of multiple packet transformation functions specified by the second dynamic security policy on a plurality of packets associated with the network that correspond to one or more criteria specified by the one or more rules based on the second boundary".

The **closest** prior art made of record and cited consisted of the following references.

Kellum (US 20010039624 A1) disclosed a system and method for providing external data-signal isolation, and signal-level information-preserving-data-transformations, to enable safe, operationally efficient, information sharing between protected information systems and networks and external, potentially hostile, information systems and networks which neutralizes any imbedded hostile executable codes such as viruses that may be in data-signals incoming from the external systems and networks. The system and method prevent un-transformed external data-signals from entering protected systems and/or networks using an intermediate screen which is a computer hardware device. The intermediate screen (which may be implemented as a network of systems) is deployed between the protected systems and external systems and is used to process all incoming signals from the external system to obtain transformed data sets from which information is extracted before it is passed to the protected system. The incoming signals all remain confined in the intermediate screen.

Brustoloni et al. (US 20030035370 A1) disclosed an ISP system that determines whether packets destined to that site conform to a profile provided to the ISP by that site. The profile, indicates, for example, what protocols are allowed by the

server, and, for each such protocol, what destination port numbers or message types are allowed, a maximum transmission rate, the maximum number of allowed connections a client may have, and whether to enforce congestion-avoidance. This server profile enforcement (SPE) automatically thwarts denial of service attacks from attackers that send packets to the subscribing server from that ISP using connections or having packet characteristics that do not conform to the acceptable characteristics specified in the profile. SPE is generally performed by an SPE unit, which can be incorporated in the access gateways of an ISP that supports the service. Packets may also be forwarded in multiple classes of service depending upon the type of traffic from which they originate. Multiple classes of service allow the method to be effective even if deployed only by select ISPs.

Chen et al. (US 20030142681 A1) disclosed a method for distributing and conditioning IP traffic for mobile networks based on differentiated services, wherein edge/border routers are only required to maintain QoS profiles for related mobile stations. A new IP address or a new service level subscription or service level agreement of an mobile station is only sent to related edge/border routers. As a result, unnecessary IP traffic is significantly reduced. The routers in accordance with methods of the invention disregard the contents of an IP payload and therefore all of the IP addresses that a mobile station may posse. A mobile station is permitted to enter into a domain and obtain a desired quality of service (e.g., Gold or Standard service) without the need to maintain the service while moving through the domain.

Bruton et al. (US 20030145225 A1) disclosed a method providing intrusion event filtering and/or generic attack signature processing. These services are integrated into a system or server that is the potential target of attack, or alternatively may be implemented in a network device. Filtering may be provided using sensitivity levels and suspicion levels. Generic attack signatures describe relatively broad classes of intrusions. Intrusion detection policy information may be used to direct the actions to be taken upon detecting an attack.

Iyer et al. (US 20050138204 A1) disclosed a unified policy management system for an organization including a central policy server and remotely situated policy enforcers. A central database and policy enforcer databases storing policy settings are configured as LDAP databases adhering to a hierarchical object oriented structure. Such structure allows the policy settings to be defined in an intuitive and extensible fashion. Changes in the policy settings made at the central policy server are automatically transferred to the policy enforcers for updating their respective databases. Each policy enforcer collects and transmits health and status information in a predefined log format and transmits it to the policy server for efficient monitoring by the policy server. For further efficiencies, the policy enforcement functionalities of the policy enforcers are effectively partitioned so as to be readily implemented in hardware. The system also provides for dynamically routed VPNs where VPN membership lists are automatically created and shared with the member policy enforcers. Updates to such membership lists are also automatically transferred to remote VPN clients. The system further provides for fine grain access control of the traffic in the VPN by allowing

definition of firewall rules within the VPN. In addition, policy server and policy enforcers may be configured for high availability by maintaining a backup unit in addition to a primary unit. The backup unit become active upon failure of the primary unit.

Kumar et al. (US 20050141537 A1) disclosed an Ethernet system and method for auto-learning of MAC addresses and lexicographic lookup of hardware databases are disclosed. An Ethernet network device includes a hardware MAC address database containing MAC address entries and a hardware MAC address learning engine in communication with the hardware MAC address database and configured to receive an unresolved source MAC address to be learned and to record the unresolved source MAC address in the hardware MAC address database in a corresponding MAC address entry. The Ethernet network device may also include a hardware lexicographic lookup engine configured to perform hardware lookups of MAC address entries in the hardware MAC address database and to interface with a management application program interface (API) for management of the Ethernet network device.

Roese et al. (US 20060048142 A1) disclosed a system and method for rapidly responding to triggering events or activities in a network system. The system includes a policy enforcement function, a policy manager function, and one or more network devices of the network system. The policy enforcement function includes one or more installed policy sets and/or policy enforcement rule sets suitably responsive to triggering events or activities. Upon detection of a trigger, the policy manager function analyzes the trigger and selects one or more appropriate policy sets and/or policy enforcement rule sets deemed to be responsive to the trigger. Each set has a unique rapid response

identifier. The policy manager function signals for implementation of the one or more policy and/or rule sets, based on one or more rapid response identifiers, which are enforced through the policy enforcement function. The policy enforcement function may be a part of one or more of the one or more network infrastructure devices for implementing the policy change. The system and method enable rapid response to a detected trigger (which might be a manual input) by pre-installing responsive policy and/or rule sets first and then generating and transmitting the unique rapid response identifier(s) corresponding to one or more selected policy and/or rule sets for implementation.

Afek et al. (US 20060212572 A1) disclosed a method for screening packet-based communication traffic. At least a first data packet, sent over a network from a source address to a destination address, is received. A determination is made, by analyzing the first data packet, that the first data packet was generated by a worm. In response to the determination, a second data packet sent over the network from the source address is blocked.

Maes (US 20080072307 A1) disclosed a method where information is established between two parties, including a negotiated port to be used in the path of network traffic between those two parties. A firewall then can be informed by the party "behind" the firewall of traffic that will take place between addresses for the two parties on that port. When a service or application is involved (as an end point or as a third party, for example), the service or application can log the information for the firewall as described elsewhere herein. Further, using the view of the application log, the logging

party can be outside the firewall. In such a case, the first device or an application outside the firewall may log a session. If authorized to do so, such as by policy enforcement on such requests, the firewall may then let this traffic through.

Van Der Merwe et al. (US 20100082811 A1) disclosed a method using a customer blacklist that is generated from a network blacklist and a customer whitelist. The network blacklist comprises a list of Internet Protocol (IP) addresses identifying unwanted traffic sources. The customer whitelist comprises a list of IP addresses identifying wanted traffic sources for a specific customer. The customer blacklist is generated by removing from the network blacklist any IP address that is also on the customer whitelist.

Barkan (US 20100296441 A1) disclosed a method for providing a wireless Internet connection to WiFi-enabled devices (STAs) comprising: wirelessly connecting a first STA to the Internet through a first AP with a first SSID; remaining connected to the first Access Point (AP), the first STA creates a software-based wireless AP with a second SSID for wirelessly connecting other STAs to the Internet through the first STA. A software module running on the first STA allows a second STA a wide access to the Internet only if the second STA has a copy of the software module running installed and active therein. A method for configuring STAs to connect to a wireless network, comprising: a customer first connects a STA by wire to its network; a software on the STA copies to the STA the security information gained through the wired connection, thus setting the security parameters for the STA.

Nguyen et al. (US 20110088092 A1) disclosed a method for detection of network address spoofing and false positive avoidance in a network is described herein. The network may include one or more hosts and a network management system. The network management system may identify a suspicious host in the network. A condition indicative of network address spoofing by the suspicious host may be detected. It may be determined whether the spoofing condition is expected in normal traffic of the network. In response to a determination that the spoofing condition is expected, it is determined that the suspicious host generated normal traffic.

However, the prior art of record, taken by itself or in any combination, **do not** anticipate or make obvious the invention of the present application and in particular the claim features listed above.

9. Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

10. The prior art made of record and not relied upon is considered pertinent to applicants' disclosure.

a. **Mizuno et al., ("A New Remote Configurable Firewall System for Home-use Gateways", January 2005, Second IEEE Consumer Communications and Networking Conference, pp. 599-601)** is cited for

disclosing a remote-configurable firewall system that allows users to configure policies and notifies them when the home-gateway is under attack.

b. **Duade et al. (US 20040088542 A1)** is cited for disclosing a VPN network system with a gateway device that manages routing and forwarding processes.

c. **Blaisdell et al. (US 20080235755 A1)** is cited for disclosing a method and system for propagating security policies and rules to network components.

d. **Ou (US 20100132027 A1)** is cited for disclosing a network boundary interface device that enables policy configuration by network administrators.

11. Any inquiry concerning this communication or earlier communications from the examiner should be directed to KENNETH CHANG whose telephone number is (571)270-7530. The examiner can normally be reached on Monday-Friday 10:30am-7:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Taghi T. Arani can be reached on 571-272-3787. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a

USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/KENNETH CHANG/
Examiner, Art Unit 2438
03/26/15

Examiner-Initiated Interview Summary	Application No.	Applicant(s)	
	13/657,010	ROGERS ET AL.	
	Examiner	Art Unit	
	KENNETH CHANG	2438	

All participants (applicant, applicant's representative, PTO personnel):

(1) *KENNETH CHANG*. (3)_____.

(2) *WILLIAM WOOTEN*. (4)_____.

Date of Interview: *26 March 2015*.

Type: ☒ Telephonic ☐ Video Conference
☐ Personal [copy given to: ☐ applicant ☐ applicant's representative]

Exhibit shown or demonstration conducted: ☐ Yes ☒ No.
If Yes, brief description: _____.

Issues Discussed ☐101 ☐112 ☐102 ☐103 ☒Others
(For each of the checked box(es) above, please describe below the issue and detailed description of the discussion)

Claim(s) discussed: *19,53,67,81,95,97 and 99*.

Identification of prior art discussed: *N/A*.

Substance of Interview
(For each issue discussed, provide a detailed description and indicate if agreement was reached. Some topics may include: identification or clarification of a reference or a portion thereof, claim interpretation, proposed amendments, arguments of any applied references etc...)

To expedite prosecution, the Examiner made contact with applicants' attorney of record William Wooten (Reg. No. 60,049). Attorney Wooten indicated applicants' authorization to amend claims 19, 53, 67, 81, 95, 97, and 99 to place the application in condition for allowance.

Applicant recordation instructions: It is not necessary for applicant to provide a separate record of the substance of interview.

Examiner recordation instructions: Examiners must summarize the substance of any interview of record. A complete and proper recordation of the substance of an interview should include the items listed in MPEP 713.04 for complete and proper recordation including the identification of the general thrust of each argument or issue discussed, a general indication of any other pertinent matters discussed regarding patentability and the general results or outcome of the interview, to include an indication as to whether or not agreement was reached on the issues raised.

☐ Attachment

/KENNETH CHANG/ Examiner, Art Unit 2438	

Notice of References Cited	Application/Control No. 13/657,010	Applicant(s)/Patent Under Reexamination ROGERS ET AL.	
	Examiner KENNETH CHANG	Art Unit 2438	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-2004/0088542 A1	05-2004	Daude et al.	713/156
*	B	US-2008/0235755 A1	09-2008	Blaisdell et al.	726/1
*	C	US-2010/0132027 A1	05-2010	Ou, Shukong	726/11
	D	US-			
	E	US-			
	F	US-			
	G	US-			
	H	US-			
	I	US-			
	J	US-			
	K	US-			
	L	US-			
	M	US-			

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	Mizuno et al., A New Remote Configurable Firewall System for Home-use Gateways, January 2005, Second IEEE Consumer Communications and Networking Conference, pp. 599-601
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**		
	Application Number	13657010
	Filing Date	2012-10-22
	First Named Inventor	Steven ROGERS
	Art Unit	2438
	Examiner Name	Chang, Kenneth W.
	Attorney Docket Number	007742.00017

U.S.PATENTS						Remove
Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
/K.C./	1	8806638	B1	2014-08-12	Mani	
/K.C./	2	6611875	B1	2003-08-26	Chopra et al.	
If you wish to add additional U.S. Patent citation information please click the Add button.						Add

U.S.PATENT APPLICATION PUBLICATIONS						Remove
Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
/K.C./	1	20090328219	A1	2009-12-31	Narayanaswamy	
	2	20120240135	A1	2012-09-20	Risbood et al.	
	3	20120314617	A1	2012-12-13	Erichsen et al.	
	4	20030097590	A1	2003-05-22	Syvanne	
If you wish to add additional U.S. Published Application citation information please click the Add button.						Add

FOREIGN PATENT DOCUMENTS	Remove

EFS Web 2.1.17

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.C./

Receipt date: 03/13/2015	Application Number	13657010 13657010 - GAU: 2438
INFORMATION DISCLOSURE STATEMENT BY APPLICANT	Filing Date	2012-10-22
(Not for submission under 37 CFR 1.99)	First Named Inventor	Steven ROGERS
	Art Unit	2438
	Examiner Name	Chang, Kenneth W.
	Attorney Docket Number	007742.00017

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							☐

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1		☐

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature	/Kenneth Chang/	Date Considered	03/26/2015

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.C./

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13657010	ROGERS ET AL.
	Examiner	**Art Unit**
	KENNETH CHANG	2438

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	10/20/2014	03/26/2015							
1	1	✓	=							
2	2	✓	=							
3	3	✓	=							
4	4	✓	=							
	5	✓	-							
5	6	✓	=							
	7	O	-							
6	8	✓	=							
7	9	✓	=							
8	10	O	=							
9	11	✓	=							
10	12	✓	=							
11	13	✓	=							
12	14	✓	=							
13	15	✓	=							
14	16	✓	=							
15	17	✓	=							
16	18	✓	=							
17	19	✓	=							
33	20	✓	=							
	21	✓	-							
	22	✓	-							
18	23		=							
19	24		=							
20	25		=							
21	26		=							
22	27		=							
23	28		=							
24	29		=							
25	30		=							
26	31		=							
27	32		=							
28	33		=							
29	34		=							
30	35		=							
31	36		=							

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13657010	ROGERS ET AL.
	Examiner	**Art Unit**
	KENNETH CHANG	2438

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	10/20/2014	03/26/2015							
32	37		=							
34	38		=							
35	39		=							
36	40		=							
37	41		=							
38	42		=							
39	43		=							
40	44		=							
41	45		=							
42	46		=							
43	47		=							
44	48		=							
45	49		=							
46	50		=							
47	51		=							
48	52		=							
49	53		=							
50	54		=							
51	55		=							
52	56		=							
53	57		=							
54	58		=							
55	59		=							
56	60		=							
57	61		=							
58	62		=							
59	63		=							
60	64		=							
61	65		=							
62	66		=							
63	67		=							
64	68		=							
65	69		=							
66	70		=							
67	71		=							
68	72		=							

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13657010	ROGERS ET AL.
	Examiner	**Art Unit**
	KENNETH CHANG	2438

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	10/20/2014	03/26/2015							
69	73		=							
70	74		=							
71	75		=							
72	76		=							
73	77		=							
74	78		=							
75	79		=							
76	80		=							
77	81		=							
78	82		=							
79	83		=							
80	84		=							
81	85		=							
82	86		=							
83	87		=							
84	88		=							
85	89		=							
86	90		=							
87	91		=							
88	92		=							
89	93		=							
90	94		=							
91	95		=							
92	96		=							
93	97		=							
94	98		=							
95	99		=							
96	100		=							

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13657010	ROGERS ET AL.
	Examiner	**Art Unit**
	KENNETH CHANG	2438

CPC						
Symbol					**Type**	**Version**
H04L		63	/	0218	F	2013-01-01
H04L		63	/	0263	I	2013-01-01
H04L		63	/	20	I	2013-01-01
			/			
			/			
			/			
			/			
			/			
			/			
			/			
			/			
			/			
			/			
			/			

CPC Combination Sets							
Symbol					**Type**	**Set**	**Ranking**	**Version**
			/					
			/					

(Assistant Examiner)	(Date)	**Total Claims Allowed:** 96	
/KENNETH CHANG/ Examiner.Art Unit 2438	03/26/2015	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	4

U.S. Patent and Trademark Office

Part of Paper No. 20150320

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13657010	ROGERS ET AL.
	Examiner	**Art Unit**
	KENNETH CHANG	2438

US ORIGINAL CLASSIFICATION		INTERNATIONAL CLASSIFICATION									
CLASS	SUBCLASS	CLAIMED					NON-CLAIMED				
		H	0	4	L	29 / 06 (2006.01.01)					
CROSS REFERENCE(S)											
CLASS	SUBCLASS (ONE SUBCLASS PER BLOCK)										

(Assistant Examiner)	(Date)	Total Claims Allowed: 96	
/KENNETH CHANG/ Examiner.Art Unit 2438	03/26/2015	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	4

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13657010	ROGERS ET AL.
	Examiner	**Art Unit**
	KENNETH CHANG	2438

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original
1	1	15	17	28	33	45	49	61	65	77	81	93	97		
2	2	16	18	29	34	46	50	62	66	78	82	94	98		
3	3	17	19	30	35	47	51	63	67	79	83	95	99		
4	4	33	20	31	36	48	52	64	68	80	84	96	100		
	5		21	32	37	49	53	65	69	81	85				
5	6		22	34	38	50	54	66	70	82	86				
	7	18	23	35	39	51	55	67	71	83	87				
6	8	19	24	36	40	52	56	68	72	84	88				
7	9	20	25	37	41	53	57	69	73	85	89				
8	10	21	26	38	42	54	58	70	74	86	90				
9	11	22	27	39	43	55	59	71	75	87	91				
10	12	23	28	40	44	56	60	72	76	88	92				
11	13	24	29	41	45	57	61	73	77	89	93				
12	14	25	30	42	46	58	62	74	78	90	94				
13	15	26	31	43	47	59	63	75	79	91	95				
14	16	27	32	44	48	60	64	76	80	92	96				

(Assistant Examiner)	(Date)	**Total Claims Allowed:** 96	
/KENNETH CHANG/ Examiner.Art Unit 2438	03/26/2015	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	4

Receipt date: 11/25/2014

Doc code: IDS

Doc description: Information Disclosure Statement (IDS) Filed

13657010 - GAU: 2438

PTO/SB/08a (01-10)

Approved for use through 07/31/2012. OMB 0651-0031

U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**		
	Application Number	13657010
	Filing Date	2012-10-22
	First Named Inventor	Steven ROGERS
	Art Unit	2438
	Examiner Name	Chang, Kenneth W.
	Attorney Docket Number	007742.00017

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
/K.C./	1	7539186	B2	2009-05-26	Aerrabotu et al.	
	2	7710885	B2	2010-05-04	Ilnicki et al.	
	3	8856926	B2	2014-10-07	Narayanaswamy et al.	

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							☐

EFS Web 2.1.17

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.C./

Receipt date: 11/25/2014	Application Number	13657010 13657010 - GAU: 2438
INFORMATION DISCLOSURE STATEMENT BY APPLICANT	Filing Date	2012-10-22
(Not for submission under 37 CFR 1.99)	First Named Inventor	Steven ROGERS
	Art Unit	2438
	Examiner Name	Chang, Kenneth W.
	Attorney Docket Number	007742.00017

If you wish to add additional Foreign Patent Document citation information please click the Add button **Add**

NON-PATENT LITERATURE DOCUMENTS **Remove**

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
/K.C./	1	REUMANN, John et al., "Adaptive Packet Filters," Department of Electrical Engineering and Computer Science, The University of Michigan, Ann Arbor, MI, IEEE, 2001.	☐
/K.C./	2	GREENWALD, Michael et al., "Designing an Academic Firewall: Policy, Practice, and Experience with SURF," Department of Computer Science, Stanford University, Stanford, CA, IEEE, Proceedings of SNDSS, 1996.	☐

If you wish to add additional non-patent literature document citation information please click the Add button **Add**

EXAMINER SIGNATURE

Examiner Signature	/Kenneth Chang/	Date Considered	02/24/2015

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

EFS Web 2.1.17 ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.C./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**		
	Application Number	13657010
	Filing Date	2012-10-22
	First Named Inventor	Steven ROGERS
	Art Unit	2438
	Examiner Name	Chang, Kenneth W.
	Attorney Docket Number	007742.00017

U.S.PATENTS						Remove
Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					
If you wish to add additional U.S. Patent citation information please click the Add button.						Add

U.S.PATENT APPLICATION PUBLICATIONS						Remove
Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
/K.C./	1	20090172800	A1	2009-07-02	Wool	
/K.C./	2	20080005795	A1	2008-01-03	Acharya et al.	
If you wish to add additional U.S. Published Application citation information please click the Add button.						Add

FOREIGN PATENT DOCUMENTS								Remove
Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							☐
If you wish to add additional Foreign Patent Document citation information please click the Add button								Add

NON-PATENT LITERATURE DOCUMENTS	Remove

EFS Web 2.1.17

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.C./

Receipt date: 02/18/2015	Application Number	13657010 13657010 - GAU: 2438
INFORMATION DISCLOSURE STATEMENT BY APPLICANT	Filing Date	2012-10-22
	First Named Inventor	Steven ROGERS
	Art Unit	2438
(Not for submission under 37 CFR 1.99)	Examiner Name	Chang, Kenneth W.
	Attorney Docket Number	007742.00017

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1		☐

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature	/Kenneth Chang/	Date Considered	02/24/2015

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.C./

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

BIB DATA SHEET

CONFIRMATION NO. 2390

SERIAL NUMBER	FILING or 371(c) DATE RULE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
13/657,010	10/22/2012	726	2438	007742.00017

APPLICANTS
CENTRIPETAL NETWORKS, INC., Leesburg, VA

INVENTORS
Steven Rogers, Leesburg, VA;
Sean Moore, Hollis, NH;

** **CONTINUING DATA** **********

** **FOREIGN APPLICATIONS** **********

** **IF REQUIRED, FOREIGN FILING LICENSE GRANTED** ** SMALL ENTITY **
11/23/2012

Foreign Priority claimed ☐ Yes ☑ No 35 USC 119(a-d) conditions met ☐ Yes ☑ No Verified and Acknowledged /KENNETH W CHANG/ Examiner's Signature	☐ Met after Allowance Initials	STATE OR COUNTRY	SHEETS DRAWINGS	TOTAL CLAIMS	INDEPENDENT CLAIMS
		VA	10	20	3

ADDRESS

BANNER & WITCOFF, LTD.
1100 13th STREET, N.W.
SUITE 1200
WASHINGTON, DC 20005-4051
UNITED STATES

TITLE

METHODS AND SYSTEMS FOR PROTECTING A SECURED NETWORK

FILING FEE RECEIVED		
4833	FEES: Authority has been given in Paper No._____ to charge/credit DEPOSIT ACCOUNT No._____ for following:	☐ All Fees ☐ 1.16 Fees (Filing) ☐ 1.17 Fees (Processing Ext. of time) ☐ 1.18 Fees (Issue) ☐ Other _____ ☐ Credit

SEARCH RESULTS

You searched for: gateways network security rule policy

13 Results returned

Network Security Policies: **Verification, Optimization and Testing**
Al-Shaer, E.
Network Operations and Management Symposium, 2006. NOMS 2006. 10th IEEE/IFIP
DOI: 10.1109/NOMS.2006.1687592
Publication Year: 2006 , Page(s): 584
Cited by: Papers (1)
IEEE CONFERENCE PUBLICATIONS

Efficient Algorithms for Dynamic Detection and Resolution of IPSec/VPN Security Policy **Conflicts**
Niksefat, S. ; Sabaei, M.
Advanced Information Networking and Applications (AINA), 2010 24th IEEE International Conference on
DOI: 10.1109/AINA.2010.99
Publication Year: 2010 , Page(s): 737 - 744
Cited by: Papers (1)
IEEE CONFERENCE PUBLICATIONS

A method for moving rules **in a** network **with multiple packet filters**
Mothersole, I. ; Reed, M.J.
Computer Science and Electronic Engineering Conference (CEEC), 2011 3rd
DOI: 10.1109/CEEC.2011.5995823
Publication Year: 2011 , Page(s): 45 - 49
IEEE CONFERENCE PUBLICATIONS

Modeling and verification of IPSec and VPN security policies
Hamed, H. ; Al-Shaer, E. ; Marrero, W.
Network Protocols, 2005. ICNP 2005. 13th IEEE International Conference on
DOI: 10.1109/ICNP.2005.25
Publication Year: 2005
Cited by: Papers (24) | Patents (2)
IEEE CONFERENCE PUBLICATIONS

Adaptive optimization of packet filtering devices performance ensuring a conflict-free network **configuration**
Maiolini, G. ; Cignini, L. ; Baiocchi, A.
INFOCOM Workshops 2008, IEEE
DOI: 10.1109/INFOCOM.2008.4544614
Publication Year: 2008 , Page(s): 1 - 6
IEEE CONFERENCE PUBLICATIONS

A new remote configurable firewall system for home-use gateways
Mizuno, S. ; Matsuura, K. ; Yamada, Kohji ; Takahashi, K.
Consumer Communications and Networking Conference, 2005. CCNC. 2005 Second IEEE
DOI: 10.1109/CCNC.2005.1405247
Publication Year: 2005 , Page(s): 599 - 601
Cited by: Papers (4) | Patents (7)
IEEE CONFERENCE PUBLICATIONS

On Optimal Firewall Rule Ordering
El-Alfy, E.-S.M. ; Selim, S.Z.
Computer Systems and Applications, 2007. AICCSA '07. IEEE/ACS International Conference on
DOI: 10.1109/AICCSA.2007.370727
Publication Year: 2007 , Page(s): 819 - 824
Cited by: Papers (2)
IEEE CONFERENCE PUBLICATIONS

Novel disjoint graph based algorithm for multi-field range-based packet classification
Yuke Wang ; Yun Zhang ; Tiyan Tang ; Krishnamurthy, A. ; Damm, G. ; Bou-Diab, B.
Communications, 2004 IEEE International Conference on
Volume: 2
DOI: 10.1109/ICC.2004.1312672
Publication Year: 2004 , Page(s): 1108 - 1112 Vol.2
Cited by: Papers (1)
IEEE CONFERENCE PUBLICATIONS

Automatic Conflict Analysis and Resolution of Traffic Filtering Policy for Firewall and Security Gateway
Ferraresi, S. ; Pesic, S. ; Trazza, L. ; Baiocchi, A.
Communications, 2007. ICC '07. IEEE International Conference on
DOI: 10.1109/ICC.2007.220
Publication Year: 2007 , Page(s): 1304 - 1310
Cited by: Papers (3)
IEEE CONFERENCE PUBLICATIONS

Real-Time Security Exercises on a Realistic Interdomain Routing Experiment Platform
Yue Li ; Liljenstam, M. ; Liu, J.
Principles of Advanced and Distributed Simulation, 2009. PADS '09. ACM/IEEE/SCS 23rd Workshop on
DOI: 10.1109/PADS.2009.12
Publication Year: 2009 , Page(s): 54 - 63
Cited by: Patents (1)
IEEE CONFERENCE PUBLICATIONS

ODYSSEY: Policy-Driven Anonymizer for Handheld Wireless Devices Privacy
Gaspard, C. ; Kayssi, A. ; Chehab, A
Innovations in Information Technology, 2006
DOI: 10.1109/INNOVATIONS.2006.301891
Publication Year: 2006 , Page(s): 1 - 5
IEEE CONFERENCE PUBLICATIONS

The new European regulatory environment for telecommunications-implications for service management and its security
Maillot, D. ; Olnes, J. ; Spilling, P
Communications, 1995. ICC '95 Seattle, 'Gateway to Globalization', 1995 IEEE International Conference on
Volume: 1
DOI: 10.1109/ICC.1995.525148
Publication Year: 1995 , Page(s): 110 - 116 vol.1
Cited by: Papers (1)
IEEE CONFERENCE PUBLICATIONS

A novel approach for checking route oscillation of BGP
Ziying Hu ; Jun Zhang
Digital Avionics Systems Conference, 2009. DASC '09. IEEE/AIAA 28th
DOI: 10.1109/DASC.2009.5347423
Publication Year: 2009 , Page(s): 7.B.4-1 - 7.B.4-6
IEEE CONFERENCE PUBLICATIONS

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L9	34	H04L63/20.CPC. AND (gateway) same (policy or policies) same (packet or traffic) and (rule) same (address$10) with (source or destination or network or ip or internet protocol) same (security or secure or protect$9 or ids or intrusion or dos or denial of service) and (server or manager or managing or supervis$9) and (set or list) and (function or algorithm or filter$9 or processing or rout$9) and (edge or boundary or boundaries or border$5) with network	US-PGPUB; USPAT; EPO	ADJ	ON	2015/03/26 17:38
L8	51	H04L63/20.CPC. AND (gateway) same (policy or policies) same (packet or traffic) and (rule) same (address$10) with (source or destination or network or ip or internet protocol) same (security or secure or protect$9 or ids or intrusion or dos or denial of service) and (server or manager or managing or supervis$9) and (set or list) and (function or algorithm or filter$9 or processing or rout$9) and (edge or boundary or boundaries or border$5)	US-PGPUB; USPAT; EPO	ADJ	ON	2015/03/26 17:38
L7	96	H04L63/20.CPC. AND (gateway) same (policy or policies) same (packet or traffic) and (rule) same (address$10) with (source or destination or network or ip or internet protocol) same (security or secure or protect$9 or ids or intrusion or dos or denial of service) and (server or manager or managing or supervis$9) and (set or list) and (function or algorithm or filter$9 or processing or rout$9)	US-PGPUB; USPAT; EPO	ADJ	ON	2015/03/26 17:37
L6	8	H04L63/0218.CPC. AND (gateway) same (policy or policies) same (packet or traffic) and (rule) same (address$10) with (source or destination or network or ip or internet protocol) same (security or secure or protect$9 or ids or intrusion or dos or denial of service) and (server or manager or managing or supervis$9) and (set or list) and (function or algorithm or filter$9 or processing or encapsul$9)	US-PGPUB; USPAT; EPO	ADJ	ON	2015/03/26 17:36
L5	12	(US-20060212572-$ or US-20030145225-$ or US-20060048142-$ or US-20010039624-$ or US-20050138204-$ or US-20100296441-$ or US-20080072307-$ or US-20050141537-$ or US-20030142681-$ or US-20100082811-$ or US-20030035370-$ or US-20110088092-$).did.	US-PGPUB	ADJ	ON	2015/03/26 17:35
S107	6	("20030097590" | "20090328219" | "20120240135" | "20120314617" | "6611875" | "8806638").PN.	US-PGPUB; USPAT; EPO	ADJ	ON	2015/03/26 14:52
S90	96	H04L63/20.CPC. AND (gateway) same (policy or policies) same (packet or traffic) and (rule) same (address$10) with (source or destination or network or ip or internet protocol) same (security or secure or protect$9 or ids or intrusion or dos or denial of service) and (server or manager or managing or supervis$9) and (set or list) and (function or algorithm or filter$9 or processing or rout$9 or encapsul$9)	US-PGPUB; USPAT; EPO	ADJ	ON	2015/03/26 12:26
S88	8	H04L63/0218.CPC. AND (gateway) same (policy or policies) same (packet or traffic) and (rule) same (address$10) with (source or destination or network or ip or internet protocol) same (security or secure or protect$9 or ids or intrusion or dos or denial of service) and (server or manager or managing or supervis$9) and (set or list) and (function or algorithm or filter$9 or processing or rout$9)	US-PGPUB; USPAT; EPO	ADJ	ON	2015/03/26 12:22
S87	67	H04L63/0263.CPC. AND (gateway) same (policy or policies) same (packet or traffic) and (rule) same (address$10) with (source or destination or network or ip or internet protocol) same (security or secure or protect$9 or ids or intrusion or dos or denial of service) and (server or manager or managing or supervis$9) and (set or list) and (function or algorithm or filter$9 or processing or rout$9)	US-PGPUB; USPAT; EPO	ADJ	ON	2015/03/26 12:22
S86	67	H04L63/0263.CPC. AND (gateway) same (policy or policies) same (packet or traffic) and (rule) same (address$10) with (source or destination or network or ip or internet protocol) same (security or secure or protect$9 or ids or intrusion or dos or denial of service) and (server or manager or managing or supervis$9) and (set or list) and (function or algorithm or filter$9 or processing)	US-PGPUB; USPAT; EPO	ADJ	ON	2015/03/26 12:11
S85	96	H04L63/20.CPC. AND (gateway) same (policy or policies) same (packet or traffic) and (rule) same	US-	ADJ	ON	2015/03/26

		(address$10) with (source or destination or network or ip or internet protocol) same (security or secure or protect$9 or ids or intrusion or dos or denial of service) and (server or manager or managing or supervis$9) and (set or list) and (function or algorithm or filter$9 or processing)	US-PGPUB; USPAT; EPO			12:11
S84	8	H04L63/0218.CPC. AND (gateway) same (policy or policies) same (packet or traffic) and (rule) same (address$10) with (source or destination or network or ip or internet protocol) same (security or secure or protect$9 or ids or intrusion or dos or denial of service) and (server or manager or managing or supervis$9) and (set or list) and (function or algorithm or filter$9 or processing)	US-PGPUB; USPAT; EPO	ADJ	ON	2015/03/26 12:11
S83	1680	H04L63/0263.CPC.	US-PGPUB; USPAT; EPO	ADJ	ON	2015/03/26 12:04
S82	5918	H04L63/20.CPC.	US-PGPUB; USPAT; EPO	ADJ	ON	2015/03/26 12:04
S81	655	H04L63/0218.CPC.	US-PGPUB; USPAT; EPO	ADJ	ON	2015/03/26 12:04
S80	6	("20030097590" | "20090328219" | "20120240135" | "20120314617" | "6611875" | "8806638").PN.	US-PGPUB; USPAT; EPO	ADJ	ON	2015/03/14 21:26
S79	34	(SIP or session initiat$9 protocol) with (URI or uniform resourse) with (header or heading) same (network address$9)	US-PGPUB; USPAT; EPO	ADJ	ON	2015/03/14 21:20
S78	1202	(SIP or session initiat$9 protocol) with (URI or uniform resourse) with (header or heading)	US-PGPUB; USPAT; EPO	ADJ	ON	2015/03/14 21:20
S77	1806	(SIP or session initiat$9 protocol) same (URI or uniform resourse) same (header or heading)	US-PGPUB; USPAT; EPO	ADJ	ON	2015/03/14 21:19
S76	114	(network with transparent$5 with layer) same address$9 same (link$9) and (secure or security or attack$9)	US-PGPUB; USPAT; EPO	ADJ	ON	2015/02/24 14:01
S75	171	(network with transparent$5 with layer) same address$9 same (link$9)	US-PGPUB; USPAT; EPO	ADJ	ON	2015/02/24 14:00
S74	539	(network with transparent$5 with layer) same address$9	US-PGPUB; USPAT; EPO	ADJ	ON	2015/02/24 14:00
S73	2	("20080005795" | "20090172800").PN.	US-PGPUB; USPAT; EPO	ADJ	ON	2015/02/24 13:49
S72	3	("7539186" | "7710885" | "8856926").PN.	US-PGPUB; USPAT;	ADJ	ON	2015/02/24 13:48

			EPO			
S71	66	H04L63/0263.CPC. AND (gateway) same (policy or policies) same (packet or traffic) and (rule) same (address$10) with (source or destination or network or ip or internet protocol) same (security or secure or protect$9 or ids or intrusion or dos or denial of service) and (server or manager or managing or supervis$9) and (set or list) and (function or algorithm or filter$9 or processing)	US-PGPUB; USPAT; EPO	ADJ	ON	2015/02/24 11:54
S70	88	H04L63/20.CPC. AND (gateway) same (policy or policies) same (packet or traffic) and (rule) same (address$10) with (source or destination or network or ip or internet protocol) same (security or secure or protect$9 or ids or intrusion or dos or denial of service) and (server or manager or managing or supervis$9) and (set or list) and (function or algorithm or filter$9 or processing)	US-PGPUB; USPAT; EPO	ADJ	ON	2015/02/24 11:54
S69	8	H04L63/0218.CPC. AND (gateway) same (policy or policies) same (packet or traffic) and (rule) same (address$10) with (source or destination or network or ip or internet protocol) same (security or secure or protect$9 or ids or intrusion or dos or denial of service) and (server or manager or managing or supervis$9) and (set or list) and (function or algorithm or filter$9 or processing)	US-PGPUB; USPAT; EPO	ADJ	ON	2015/02/24 11:54
S68	1654	H04L63/0263.CPC.	US-PGPUB; USPAT; EPO	ADJ	ON	2015/02/24 11:54
S67	5709	H04L63/20.CPC.	US-PGPUB; USPAT; EPO	ADJ	ON	2015/02/24 11:54
S66	647	H04L63/0218.CPC.	US-PGPUB; USPAT; EPO	ADJ	ON	2015/02/24 11:53
S65	1	"20140115654".pn.	US-PGPUB; USPAT; EPO	ADJ	ON	2015/02/24 11:53
S64	26	713/1,100,150,151,152,153,154,155,166,167,168.CCLS. AND S61	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/20 02:26
S63	54	709/201,203,217,218,219,220,223,224,225,226,227,228,229,230,231,238,239,240,242,244,245.CCLS. AND S61	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/20 02:26
S62	31	726/3,6,11,12,13,14,15,16,17,22,23,24,25.CCLS. AND S61	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/20 02:26
S61	198	(gateway) same (policy or policies) same (packet or traffic) and (rule) same (address$10) with (source or destination or network or ip or internet protocol) same (security or secure or protect$9 or ids or intrusion or dos or denial of service) and (server or manager or managing or supervis$9) and (set or list) and (function or algorithm or filter$9 or processing) same (ipsec or ip security or internet protocol security)	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/20 02:26
S60	24976	713/1,100,150,151,152,153,154,155,166,167,168.CCLS.	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/20 02:26
S59	125386	709/201,203,217,218,219,220,223,224,225,226,227,228,229,230,231,238,239,240,242,244,245.CCLS.	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/20 02:26

S58	26093	726/3,6,11,12,13,14,15,16,17,22,23,24,25.CCLS.	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/20 02:24
S57	1	"20030035370".pn.	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/20 01:42
S56	1	"20050135375".pn.	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/20 01:39
S55	1	"20110088092".pn.	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/20 00:40
S54	69	(spoof$5) with (address$5) with (network or source) with (policy or policies or rule)	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/20 00:28
S53	209	(spoof$5) with (address$5) with (network or source) same (policy or policies or rule)	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/20 00:28
S52	1	"20100082811".pn.	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/20 00:08
S51	1	"20080279200".pn.	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/19 23:51
S50	5	(blacklist$5 or black list$9) with (addresses) with (paid or pay)	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/19 23:46
S49	5	(blacklist$5 or black list$9) with (addresses) with (provider) with (subscription or subscribing or subscriber)	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/19 23:42
S48	55	(blacklist$5 or black list$9) with (addresses) with (provider) with (service)	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/19 23:41
S47	15	(blacklist$5 or black list$9) with (addresses) with (subscription or subscriber or subscribing) with (service)	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/19 23:38
S46	222	(blacklist$5 or black list$9) with (addresses) same (subscription or subscriber or subscribing or customer)	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/19 23:38
S45	2	(blacklist$5 or black list$9) with (addresses) with (discard$9 or block$6 or drop$5) with (packet) same (subscription or subscriber or subscribing or customer)	US-PGPUB;	ADJ	ON	2014/10/19 23:38

			USPAT; EPO			
S44	3	(differentiat$10 service code point select$5 or dscp select$5 or Diff-Serv Code Point) same (header or heading) same (traffic or packet) same (policy or policies or rule)	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/19 22:48
S43	26	(differentiat$10 service code point select$5 or dscp select$5 or Diff-Serv Code Point) same (header or heading) same (traffic or packet)	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/19 22:47
S42	10	(differentiat$10 service code point select$5 or dscp select$5) same (header or heading) same (traffic or packet)	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/19 22:47
S41	34	(forward$9) with (packet) same (queue or group or buffer$5) same (priority) same (faster or higher) same (policy or policies or whitelist$5 or white list$8)	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/19 21:56
S40	11	(discard$10 or block$5 or drop$5) and (forward$9 or allow$8) with (packet) with (address$5) same (policy or policies or whitelist$5 or white list$8) same (voip or voice over ip or voice over internet protocol) same (call or session or traffic or connection)	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/19 20:32
S39	12	(discard$10 or block$5 or drop$5) and (forward$9 or allow$8) with (packet) with (address$5) same (policy or policies or whitelist$5 or white list$8) same (voip or voice over ip or voice over internet protocol)	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/19 20:32
S38	223	(discard$10 or block$5 or drop$5) and (forward$9 or allow$8) with (packet) with (address$5) same (policy or policies or whitelist$5 or white list$8) and (voip or voice over ip or voice over internet protocol)	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/19 20:31
S37	21	(discard$10 or block$5 or drop$5) and (forward$9 or allow$8) with (packet) with (address$5) with (whitelist$9 or white list$5)	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/19 20:07
S36	5	(discard$10 or block$5 or drop$5) and (forward$9 or allow$8) with (packet) with (address$5) with (whitelist$9 or white list$5) with (only)	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/19 20:07
S35	5	(addresses) with (ip or internet protocol or source) with (discard$9 or block$6 or drop$5) with (packet) and (forward$9 or allow$8) with (packet) with (address$5) with (whitelist$9 or white list$5) with (only)	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/19 20:05
S34	15	(addresses) with (ip or internet protocol or source) with (discard$9 or block$6 or drop$5) with (packet) and (forward$9 or allow$8) with (outside or otherwise or address$5) with (packet) with (address$5) with (whitelist$9 or white list$5)	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/19 20:04
S33	12	(blacklist$5 or black list$9) with (addresses) with (ip or internet protocol or source) with (discard$9 or block$6 or drop$5) with (packet) and (forward$9 or allow$8) with (outside or otherwise or address$5) with (packet) with (address$5) with (blacklist$5 or black list$9)	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/19 18:28
S32	19	(blacklist$5 or black list$9) with (addresses) with (ip or internet protocol or source) with (discard$9 or block$6 or drop$5) with (packet) and (forward$9 or allow$8) with (outside or otherwise or address$5) with (packet) with (address$5)	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/19 18:28

S31	1	(blacklist$5 or black list$5) with (address$9) with increas$9 with (policy or policies)	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/19 18:26
S30	546	(set or list$5) with (addresses) with (ip or internet protocol or source) with (discard$9 or block$6 or drop$5) with (packet) and (forward$9 or allow$8) with (outside or otherwise or address$5) with (packet) with (address$5)	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/19 18:24
S29	705	(set or list$5) with (addresses) with (ip or internet protocol or source) with (discard$9 or block$6 or drop$5) same (packet) and (forward$9 or allow$8) with (outside or otherwise or address$5) same (packet) with (address$5)	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/19 18:24
S28	1857	(set or list$5) with (addresses) with (ip or internet protocol or source) same (discard$9 or block$6 or drop$5) same (packet) and (forward$9 or allow$8) with (outside or otherwise or address$5) same (packet) same (address$5)	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/19 18:24
S27	8993	(set or list$5) with (addresses) with (ip or internet protocol or source) same (discard$9 or block$6 or drop$5)	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/19 18:23
S26	74	(gateway) same (policy or policies) same (packet or traffic) and (rule) same (function or algorithm or filter$9 or processing) same (ipsec or ip security or internet protocol security) and (security or secure or protect$9 or ids or intrusion or dos or denial of service) and (server or manager or managing or supervis$9) same (policy or policies) and (address$10) with (source or destination or network or ip or internet protocol)	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/19 15:35
S25	9	(gateway) same (policy or policies) same (packet or traffic) and (rule) same (address$10) with (source or destination or network or ip or internet protocol) same (function or algorithm or filter$9 or processing) same (ipsec or ip security or internet protocol security) and (security or secure or protect$9 or ids or intrusion or dos or denial of service) and (server or manager or managing or supervis$9) same (policy or policies) and (pipelin$5 or parallel$5)	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/19 15:25
S24	28	(gateway) same (policy or policies) same (packet or traffic) and (rule) same (address$10) with (source or destination or network or ip or internet protocol) same (function or algorithm or filter$9 or processing) same (ipsec or ip security or internet protocol security) and (security or secure or protect$9 or ids or intrusion or dos or denial of service) and (server or manager or managing or supervis$9) same (policy or policies)	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/19 15:25
S23	198	(gateway) same (policy or policies) same (packet or traffic) and (rule) same (address$10) with (source or destination or network or ip or internet protocol) same (security or secure or protect$9 or ids or intrusion or dos or denial of service) and (server or manager or managing or supervis$9) and (set or list) and (function or algorithm or filter$9 or processing) same (ipsec or ip security or internet protocol security)	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/19 15:24
S22	253	(gateway) same (policy or policies) same (packet or traffic) and (rule) same (address$10) with (source or destination or network or ip or internet protocol) same (security or secure or protect$9 or ids or intrusion or dos or denial of service) and (server or manager or managing or supervis$9) and (set or list) and (function or algorithm or filter$9 or processing) and (ipsec or ip security or internet protocol security)	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/19 15:23
S21	252	(gateway) same (policy or policies) same (packet or traffic) and (rule) same (address$10) with (source or destination or network or ip or internet protocol) same (security or secure or protect$9 or ids or intrusion or dos or denial of service) and (server or manager or managing or supervis$9) and (set or list) and (function or algorithm or filter$9 or processing) and (ipsec or ip security)	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/19 15:23
S20	534	(gateway) same (policy or policies) same (packet or traffic) and (rule) same (address$10) with (source or destination or network or ip or internet protocol) same (security or secure or protect$9 or ids or intrusion or dos or denial of service) and (server or manager or managing or supervis$9) and (set or list) and (function or algorithm or filter$9 or processing)	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/19 00:19
S19	534	(gateway) same (policy or policies) same (packet or traffic) and (rule) same (address$10) with (source or destination or network or ip or internet protocol) same (security or secure or protect$9 or ids or	US-PGPUB;	ADJ	ON	2014/10/19 00:18

		intrusion or dos or denial of service) and (server or manager or managing or supervis$9) and (set or list)	USPAT; EPO			
S18	551	(gateway) same (policy or policies) same (packet or traffic) and (rule) same (address$10) with (source or destination or network or ip or internet protocol) same (security or secure or protect$9 or ids or intrusion or dos or denial of service) and (server or manager or managing or supervis$9)	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/19 00:18
S17	570	(gateway) same (policy or policies) same (packet or traffic) and (rule) same (address$10) with (source or destination or network or ip or internet protocol) same (security or secure or protect$9 or ids or intrusion or dos or denial of service)	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/19 00:18
S16	1430	(gateway) same (policy or policies) same (packet or traffic) and (rule) same (address$10) with (source or destination or network or ip or internet protocol) and (security or secure or protect$9 or ids or intrusion or dos or denial of service)	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/19 00:17
S15	3295	(gateway) same (policy or policies) same (packet or traffic) and (rule) and (address$10) with (source or destination or network or ip or internet protocol) and (security or secure or protect$9 or ids or intrusion or dos or denial of service)	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/19 00:16
S14	3686	(gateway) same (policy or policies) same (packet or traffic) and (rule) and (address$10) with (source or destination or network or ip or internet protocol)	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/19 00:15
S13	4415	(gateway) same (policy or policies) same (packet or traffic) and (rule)	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/19 00:14
S12	7	("20120113987" | "20060195896" | "7684400" | "20060248580" | "20110055916" | "0000000" | "20110270956" | "20130059527" | "20100011434" | "20120264443" | "6226372" | "20040151155" | "20030212900" | "20050117576" | "20060048142" | "20030188192" | "7721084" | "20030123456" | "20070083924" | "20100211678").PN. and (gateway) and (policy or policies)	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/19 00:12
S11	17	S7 and (gateway) and (policy or policies)	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/19 00:05
S10	17	S6 and (gateway) and (policy or policies)	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/19 00:05
S9	7	S8 and (gateway) and (policy or policies)	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/19 00:03
S8	20	("20050071655" | "20040098618" | "20090038008" | "7975059" | "6715084" | "20060143709" | "20010020255" | "20020066034" | "20040148520" | "20060143688" | "20090037682" | "20120167120" | "20020078382" | "20040128543" | "20020162026" | "20040044912" | "8214900" | "20020083175" | "20030145225" | "20030204632").PN.	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/19 00:01
S7	54	("20060173992" | "20030084329" | "20030035370" | "20010042200" | "20020133721" | "20030023733" | "20060095965" | "20060230444" | "20020073155" | "20030233328" | "20060212524" | "20070180510" | "7536715" | "20060212572" | "20020198956" | "20040199793" | "20030126468" | "20050050338" | "20040073800" | "20060050719" | "20050262556" | "20040049574" | "20030101260" | "20020198956" | "20030035370" | "20040190522" | "20070157316" | "20050182950" | "20020073337" | "20030145225" | "20040117624" | "20040128538" | "20040148520" | "20070056030" | "20040004941" | "20030061514" | "20030014665" | "20060193470" | "20080176536" | "7409712" | "20020133721" | "20020166063" | "20030204632" | "20060137012" | "7574740" | "20050086502" | "7331060" | "20030023733" |	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/18 23:56

		"20050278415" | "20020178378" | "20030101260" | "20070180511" | "20020162026" | "20050037733" | "20050039104" | "7702739" | "20010042200" | "20020073337" | "20030145225" | "20040117624" | "20050180416" | "20020083175" | "20060048142").PN.				
S6	53	("20060173992" | "20030084329" | "20030035370" | "20040128538" | "20010042200" | "20060230444" | "20020073155" | "20030233328" | "20060212524" | "20070180510" | "7536715" | "20060212572" | "20020178378" | "20040199793" | "20030126468" | "20050050338" | "20060095965" | "20060050719" | "20050262556" | "20040049574" | "20030101260" | "20040073800" | "20020198956" | "20040190522" | "20070157316" | "20050182950" | "20040117624" | "20040148520" | "20070056030" | "20040004941" | "20030061514" | "20030014665" | "20060193470" | "20080176536" | "7409712" | "20020133721" | "20020166063" | "20030204632" | "20060137012" | "7574740" | "20050086502" | "7331060" | "20030023733" | "20070180511" | "20020162026" | "20050037733" | "20050039104" | "7702739" | "20020073337" | "20030145225" | "20050180416" | "20020083175" | "20060048142").PN.	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/18 23:55
S5	3	(centripetal networks).as.	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/18 14:50
S4	95	(moore adj3 sean).in.	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/18 14:49
S3	443	(rogers adj3 steven).in.	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/18 14:49
S2	5511	726/1.CCLS.	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/18 14:49
S1	19	("20120113987" | "20060195896" | "7684400" | "20060248580" | "20110055916" | "0000000" | "20110270956" | "20130059527" | "20100011434" | "20120264443" | "6226372" | "20040151155" | "20030212900" | "20050117576" | "20060048142" | "20030188192" | "7721084" | "20030123456" | "20070083924" | "20100211678").PN.	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/18 14:49

EAST Search History (Interference)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L3	4	((gateway) AND (policy or policies) AND (packet or traffic or frame) AND (rule) AND (boundary or boundaries or edge or border$5) AND (rule) AND (drop$9 or discard$9)).CLM.	US-PGPUB; USPAT; UPAD	ADJ	ON	2015/03/26 17:27
L2	1	((gateway) AND (policy or policies) AND (packet or traffic or frame) AND (rule) AND (boundary or boundaries or edge or border$5) AND (rule) AND (drop$9 or discard$9) AND (first) AND (second)).CLM.	US-PGPUB; USPAT; UPAD	ADJ	ON	2015/03/26 17:17
S106	1	((gateway) AND (policy or policies) AND (packet or traffic or frame) AND (rule) AND (address$10) AND (source or destination or ip or internet protocol) AND (security or secure or protect$9 or ids or intrusion or dos or denial of service) AND (server or manager or managing or supervis$9) AND (encapsu$9) AND (routing or route or routed) AND protect$9 AND network$9 AND (URI or uniform resource)).CLM.	US-PGPUB; USPAT; UPAD	ADJ	ON	2015/03/26 12:34
S102	1	((gateway) AND (policy or policies) AND (packet or traffic or frame) AND (rule) AND (address$10) AND (source or destination or ip or internet protocol) AND (security or secure or protect$9 or ids or intrusion or dos or	US-PGPUB; USPAT;	ADJ	ON	2015/03/26 12:27

		denial of service) AND (server or manager or managing or supervis$9) AND (encapsu$9) AND (routing or route or routed) AND network$9 AND (URI or uniform resource)).CLM.	UPAD			
S101	1	((gateway) AND (policy or policies) AND (packet or traffic or frame) AND (rule) AND (address$10) AND (source or destination or ip or internet protocol) AND (security or secure or protect$9 or ids or intrusion or dos or denial of service) AND (server or manager or managing or supervis$9) AND (encapsu$9) AND (routing or route or routed) AND network$9 AND (SIP or session initia$9 protocol)).CLM.	US-PGPUB; USPAT; UPAD	ADJ	ON	2015/03/26 12:27
S100	1	((gateway) AND (policy or policies) AND (packet or traffic or frame) AND (rule) AND (address$10) AND (source or destination or ip or internet protocol) AND (security or secure or protect$9 or ids or intrusion or dos or denial of service) AND (server or manager or managing or supervis$9) AND (set or list) AND (encapsu$9) AND (routing or route or routed) AND network$9 AND (SIP or session initia$9 protocol)).CLM.	US-PGPUB; USPAT; UPAD	ADJ	ON	2015/03/26 12:26
S99	2	((gateway) AND (policy or policies) AND (packet or traffic or frame) AND (rule) AND (address$10) AND (source or destination or ip or internet protocol) AND (security or secure or protect$9 or ids or intrusion or dos or denial of service) AND (server or manager or managing or supervis$9) AND (set or list) AND (function or algorithm or filter$9 or processing) AND (routing or route or routed) AND network$9 AND (SIP or session initia$9 protocol)).CLM.	US-PGPUB; USPAT; UPAD	ADJ	ON	2015/03/26 12:23
S97	3	((gateway) AND (policy or policies) AND (packet or traffic or frame) AND (rule) AND (address$10) AND (source or destination or ip or internet protocol) AND (security or secure or protect$9 or ids or intrusion or dos or denial of service) AND (server or manager or managing or supervis$9) AND (set or list) AND (function or algorithm or filter$9 or processing) AND (forward$9 or drop$9) AND network$9 AND dynamic$9).CLM.	US-PGPUB; USPAT; UPAD	ADJ	ON	2015/03/26 12:17
S96	9	((gateway) AND (policy or policies) AND (packet or traffic or frame) AND (rule) AND (address$10) AND (source or destination or ip or internet protocol) AND (security or secure or protect$9 or ids or intrusion or dos or denial of service) AND (server or manager or managing or supervis$9) AND (set or list) AND (function or algorithm or filter$9 or processing) AND (forward$9 or drop$9) AND network$9 AND (set or list$9 or group$9 or subset)).CLM.	US-PGPUB; USPAT; UPAD	ADJ	ON	2015/03/26 12:16
S95	9	((gateway) AND (policy or policies) AND (packet or traffic or frame) AND (rule) AND (address$10) AND (source or destination or ip or internet protocol) AND (security or secure or protect$9 or ids or intrusion or dos or denial of service) AND (server or manager or managing or supervis$9) AND (set or list) AND (function or algorithm or filter$9 or processing) AND (forward$9 or drop$9) AND network$9 AND (set or list$9)).CLM.	US-PGPUB; USPAT; UPAD	ADJ	ON	2015/03/26 12:16

3/ 26/ 2015 5:41:19 PM
C:\ Users\ kchang3\ Documents\ EAST\ Workspaces\ 13657010_APP.wsp

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13657010	ROGERS ET AL.
	Examiner	Art Unit
	KENNETH CHANG	2438

CPC- SEARCHED		
Symbol	Date	Examiner
H04L63/0218	2/24/2015	KC
H04L63/20	2/24/2015	KC
H04L63/0263	2/24/2015	KC
H04L63/20	3/26/2015	KC
H04L63/0263	3/26/2015	KC
H04L63/0218	3/26/2015	KC

CPC COMBINATION SETS - SEARCHED		
Symbol	Date	Examiner

US CLASSIFICATION SEARCHED			
Class	Subclass	Date	Examiner
726	1	10/17/2014	KC

SEARCH NOTES		
Search Notes	Date	Examiner
Searched Inventors' Names and Assignee on eDan and EAST.	10/17/2014	KC
Searched IEEE Xplore Database online.	10/17/2014	KC
Completed Limited Classified Search on EAST USPAT, PGPUB, and EPO databases with Keywords combined with Classes/Subclasses 726/3,6,11,12,13,14,15,16,17,22,23,24,25, 713/1,100,150,151,152,153,154,155,166,167,168, and 709/201,203,217,218,219,220,223,224,225,226,227,228,229,230,231,238 ,239,240,242,244,245.	10/17/2014	KC
Keywords Searched: gateway, policy, policies, packet, traffic, rule, address$10, source, destination, network, ip, internet protocol, security, secure, supervis$9, protect$9, ids, intrusion, dos, denial of service, filter$9, processing, algorithm, function, ipsec, ip security, internet protocol security, discard$9, block$6, drop$5, forward$9, allow$8.	10/17/2014	KC
Consulted with QAS Beatriz Prieto regarding 101 claim compliance in view of 2014 Interim Guidance on Patent Subject Matter Eligibility.	3/13/2015	KC

/KENNETH CHANG/ Examiner, Art Unit 2438	

SEARCH NOTES		
Search Notes	**Date**	**Examiner**
Updated Limited Classified Search in CPC on EAST USPAT, PGPUB, and EPO databases with Keywords in H04L63/0218, H04L63/0263, and H04L63/20.	3/26/2015	KC
Updated Keywords: set, list, edge, boundary, boundaries, border$5, encapsul$9, rout$9.	3/26/2015	KC
Updated NPL search on IEEE Xplore Database online.	3/26/2015	KC
Interference Search Completed on USPAT, UPAD, and US-PGPUB with claim language search. See EAST SEARCH HISTORY for interference searches.	3/26/2015	KC

INTERFERENCE SEARCH			
US Class/ CPC Symbol	**US Subclass / CPC Group**	**Date**	**Examiner**
	((gateway) AND (policy or policies) AND (packet or traffic or frame) AND (rule) AND (address$10) AND (source or destination or ip or internet protocol) AND (security or secure or protect$9 or ids or intrusion or dos or denial of service) AND (server or manager or managing or supervis$9) AND (set or list) AND (function or algorithm or filter$9 or processing) AND (forward$9 or drop$9) AND network$9 AND (set or list$9)).CLM.	3/26/2015	KC
	((gateway) AND (policy or policies) AND (packet or traffic or frame) AND (rule) AND (address$10) AND (source or destination or ip or internet protocol) AND (security or secure or protect$9 or ids or intrusion or dos or denial of service) AND (server or manager or managing or supervis$9) AND (set or list) AND (function or algorithm or filter$9 or processing) AND (forward$9 or drop$9) AND network$9 AND (set or list$9 or group$9 or subset)).CLM.	3/26/2015	KC
	((gateway) AND (policy or policies) AND (packet or traffic or frame) AND (rule) AND (address$10) AND (source or destination or ip or internet protocol) AND (security or secure or protect$9 or ids or intrusion or dos or denial of service) AND (server or manager or managing or supervis$9) AND (set or list) AND (function or algorithm or filter$9 or processing) AND (forward$9 or drop$9) AND network$9 AND dynamic$9).CLM.	3/26/2015	KC
	((gateway) AND (policy or policies) AND (packet or traffic or frame) AND (rule) AND (address$10) AND (source or destination or ip or internet protocol) AND (security or secure or protect$9 or ids or intrusion or dos or denial of service) AND (server or manager or managing or supervis$9) AND (set or list) AND (function or algorithm or filter$9 or processing) AND (routing or route or routed) AND network$9 AND (SIP or session initia$9 protocol)).CLM.	3/26/2015	KC

/KENNETH CHANG/ Examiner, Art Unit 2438	

INTERFERENCE SEARCH			
US Class/ CPC Symbol	**US Subclass / CPC Group**	**Date**	**Examiner**
	((gateway) AND (policy or policies) AND (packet or traffic or frame) AND (rule) AND (address$10) AND (source or destination or ip or internet protocol) AND (security or secure or protect$9 or ids or intrusion or dos or denial of service) AND (server or manager or managing or supervis$9) AND (set or list) AND (encapsu$9) AND (routing or route or routed) AND network$9 AND (SIP or session initia$9 protocol)).CLM.	3/26/2015	KC
	((gateway) AND (policy or policies) AND (packet or traffic or frame) AND (rule) AND (address$10) AND (source or destination or ip or internet protocol) AND (security or secure or protect$9 or ids or intrusion or dos or denial of service) AND (server or manager or managing or supervis$9) AND (encapsu$9) AND (routing or route or routed) AND network$9 AND (SIP or session initia$9 protocol)).CLM.	3/26/2015	KC
	((gateway) AND (policy or policies) AND (packet or traffic or frame) AND (rule) AND (address$10) AND (source or destination or ip or internet protocol) AND (security or secure or protect$9 or ids or intrusion or dos or denial of service) AND (server or manager or managing or supervis$9) AND (encapsu$9) AND (routing or route or routed) AND network$9 AND (URI or uniform resource)).CLM.	3/26/2015	KC
	((gateway) AND (policy or policies) AND (packet or traffic or frame) AND (rule) AND (address$10) AND (source or destination or ip or internet protocol) AND (security or secure or protect$9 or ids or intrusion or dos or denial of service) AND (server or manager or managing or supervis$9) AND (encapsu$9) AND (routing or route or routed) AND protect$9 AND network$9 AND (URI or uniform resource)).CLM.	3/26/2015	KC
	((gateway) AND (policy or policies) AND (packet or traffic or frame) AND (rule) AND (boundary or boundaries or edge or border$5) AND (rule) AND (drop$9 or discard$9) AND (first) AND (second)).CLM.	3/26/2015	KC
	((gateway) AND (policy or policies) AND (packet or traffic or frame) AND (rule) AND (boundary or boundaries or edge or border$5) AND (rule) AND (drop$9 or discard$9)).CLM.	3/26/2015	KC

/KENNETH CHANG/ Examiner, Art Unit 2438	

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), to: Mail **Mail Stop ISSUE FEE**
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
or Fax (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

22907 7590 04/08/2015
BANNER & WITCOFF, LTD.
1100 13th STREET, N.W.
SUITE 1200
WASHINGTON, DC 20005-4051

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission
I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being facsimile transmitted to the USPTO (571) 273-2885, on the date indicated below.

(Depositor's name)
(Signature)
(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/657,010	10/22/2012	Steven Rogers	007742.00017	2390

TITLE OF INVENTION: METHODS AND SYSTEMS FOR PROTECTING A SECURED NETWORK

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	$480	$0	$0	$480	07/08/2015

EXAMINER	ART UNIT	CLASS-SUBCLASS
CHANG, KENNETH W	2438	726-001000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).
- ☐ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.
- ☐ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list
(1) The names of up to 3 registered patent attorneys or agents OR, alternatively,
(2) The name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.

1 Banner & Witcoff, Ltd.
2
3

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document has been filed for recordation as set forth in 37 CFR 3.11. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE: Centripetal Networks, Inc.
(B) RESIDENCE: (CITY and STATE OR COUNTRY): Herndon, Virginia

Please check the appropriate assignee category or categories (will not be printed on the patent) : ☐ Individual ☒ Corporation or other private group entity ☐ Government

4a. The following fee(s) are submitted:
- ☒ Issue Fee
- ☐ Publication Fee (No small entity discount permitted)
- ☐ Advance Order - # of Copies _____

4b. Payment of Fee(s): **(Please first reapply any previously paid issue fee shown above)**
- ☐ A check is enclosed.
- ☐ Payment by credit card. Form PTO-2038 is attached.
- ☒ The director is hereby authorized to charge the required fee(s), any deficiency, or credits any overpayment, to Deposit Account Number 19-0733 (enclose an extra copy of this form).

5. **Change in Entity Status** (from status indicated above)
- ☐ Applicant certifying micro entity status. See 37 CFR 1.29
  NOTE: Absent a valid certification of Micro Entity Status (see forms PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.
- ☒ Applicant asserting small entity status. See 37 CFR 1.27
  NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.
- ☐ Applicant changing to regular undiscounted fee status.
  NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

NOTE: This form must be signed in accordance with 37 CFR 1.31 and 1.33. See 37 CFR 1.4 for signature requirements and certifications.

Authorized Signature /William E. Wooten/ Date April 28, 2015

Typed or printed name William E. Wooten Registration No. 60,049

PTOL-85 Part B (10-13) Approved for use through 10/31/2013. OMB 0651-0033 U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re the Application of:		Atty. Docket No.:	007742.00017
Steven ROGERS *et al.*			
Serial No.:	13/657,010	Group Art Unit:	2438
Filed:	October 22, 2012	Examiner:	Chang, Kenneth W.
For:	METHODS AND SYSTEMS FOR PROTECTING A SECURED NETWORK	Confirmation No.:	2390

COMMENTS ON STATEMENT OF REASONS FOR ALLOWANCE

Mail Stop *Issue Fee*
Commissioner for Patents
Randolph Building
401 Dulany Street
Alexandria, VA 22314

Dear Sir:

In brief response to the Statement of Reasons for Allowance, Applicant respectfully submits that the quoted excerpts are not the full claim language and are not necessarily the only reasons for distinguishing the claims from the cited references. To the extent there is any deviation between the quoted excerpts and the language of the claims, Applicant submits that the language of the claims will control.

Respectfully submitted,

BANNER & WITCOFF, LTD.

Dated: April 28, 2015

By: /William E. Wooten/
William E. Wooten
Registration No. 60,049

Banner & Witcoff, Ltd.
1100 13th Street NW, Suite 1200
Washington, D.C. 20005-4051
Telephone: (202) 824-3000
Facsimile: (202) 824-3001

Electronic Patent Application Fee Transmittal

Application Number:	13657010
Filing Date:	22-Oct-2012
Title of Invention:	METHODS AND SYSTEMS FOR PROTECTING A SECURED NETWORK
First Named Inventor/Applicant Name:	Steven Rogers
Filer:	William Eugene Wooten
Attorney Docket Number:	007742.00017

Filed as Small Entity

Filing Fees for Utility under 35 USC 111(a)

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Utility Appl Issue Fee	2501	1	480	480

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension-of-Time:				
Miscellaneous:				
		Total in USD ($)		**480**

Electronic Acknowledgement Receipt

EFS ID:	22194486
Application Number:	13657010
International Application Number:	
Confirmation Number:	2390
Title of Invention:	METHODS AND SYSTEMS FOR PROTECTING A SECURED NETWORK
First Named Inventor/Applicant Name:	Steven Rogers
Customer Number:	22907
Filer:	William Eugene Wooten
Filer Authorized By:	
Attorney Docket Number:	007742.00017
Receipt Date:	28-APR-2015
Filing Date:	22-OCT-2012
Time Stamp:	17:04:00
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$480
RAM confirmation Number	4202
Deposit Account	190733
Authorized User	WOOTEN, WILLIAM E.
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows: Charge any Additional Fees required under 37 C.F.R. Section 1.16 (National application filing, search, and examination fees) Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)	

Charge any Additional Fees required under 37 C.F.R. Section 1.19 (Document supply fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.20 (Post Issuance fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.21 (Miscellaneous fees and charges)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Issue Fee Payment (PTO-85B)	IssueFeeTransmittal.pdf	173543 b280d5c876b4fe7ae9b3d79affa63f253c347b39	no	1
Warnings:					
Information:					
2	Post Allowance Communication - Incoming	Remarks.pdf	21034 e4f8d46868dacfe8d82247a7585cb7957aadf1ce	no	1
Warnings:					
Information:					
3	Fee Worksheet (SB06)	fee-info.pdf	30556 3602feeb33080826eaae74d18ee9d47d60b82c43	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	225133		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

<u>New Applications Under 35 U.S.C. 111</u>
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

<u>National Stage of an International Application under 35 U.S.C. 371</u>
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

<u>New International Application Filed with the USPTO as a Receiving Office</u>
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PTO/SB/30EFS (07-14)
Approved for use through 07/31/2016. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

REQUEST FOR CONTINUED EXAMINATION(RCE)TRANSMITTAL
(Submitted Only via EFS-Web)

Application Number	13657010	Filing Date	2012-10-22	Docket Number (if applicable)	007742.00017	Art Unit	2438
First Named Inventor	Steven ROGERS			Examiner Name	Chang, Kenneth W.		

This is a Request for Continued Examination (RCE) under 37 CFR 1.114 of the above-identified application.
Request for Continued Examination (RCE) practice under 37 CFR 1.114 does not apply to any utility or plant application filed prior to June 8, 1995, to any international application that does not comply with the requirements of 35 U.S.C. 371, or to any design application. The Instruction Sheet for this form is located at WWW.USPTO.GOV.

SUBMISSION REQUIRED UNDER 37 CFR 1.114

Note: If the RCE is proper, any previously filed unentered amendments and amendments enclosed with the RCE will be entered in the order in which they were filed unless applicant instructs otherwise. If applicant does not wish to have any previously filed unentered amendment(s) entered, applicant must request non-entry of such amendment(s).

☐ Previously submitted. If a final Office action is outstanding, any amendments filed after the final Office action may be considered as a submission even if this box is not checked.

☐ Consider the arguments in the Appeal Brief or Reply Brief previously filed on _____

☐ Other _____

☒ Enclosed

☐ Amendment/Reply

☒ Information Disclosure Statement (IDS)

☐ Affidavit(s)/ Declaration(s)

☐ Other _____

MISCELLANEOUS

☐ Suspension of action on the above-identified application is requested under 37 CFR 1.103(c) for a period of months _____
(Period of suspension shall not exceed 3 months; Fee under 37 CFR 1.17(i) required)

☐ Other _____

FEES

☒ **The RCE fee under 37 CFR 1.17(e) is required by 37 CFR 1.114 when the RCE is filed.**
The Director is hereby authorized to charge any underpayment of fees, or credit any overpayments, to Deposit Account No 190733

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT REQUIRED

☒ Patent Practitioner Signature

☐ Applicant Signature

PTO/SB/30EFS (07-14)
Approved for use through 07/31/2016. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Signature of Registered U.S. Patent Practitioner			
Signature	/William E. Wooten/	Date (YYYY-MM-DD)	2015-06-19
Name	William E. Wooten	Registration Number	60049

This collection of information is required by 37 CFR 1.114. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

PTO/SB/08a (01-10)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	13657010
Filing Date	2012-10-22
First Named Inventor	Steven ROGERS
Art Unit	2438
Examiner Name	Chang, Kenneth W.
Attorney Docket Number	007742.00017

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	7478429	B2	2009-01-13	Lyon	
	2	7818794	B2	2010-10-19	Wittman	
	3	8935785	B2	2015-01-13	Pandrangi	

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							☐

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13657010
	Filing Date	2012-10-22
	First Named Inventor	Steven ROGERS
	Art Unit	2438
	Examiner Name	Chang, Kenneth W.
	Attorney Docket Number	007742.00017

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1		☐

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**		
	Application Number	13657010
	Filing Date	2012-10-22
	First Named Inventor	Steven ROGERS
	Art Unit	2438
	Examiner Name	Chang, Kenneth W.
	Attorney Docket Number	007742.00017

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☐ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☒ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

☐ See attached certification statement.

☒ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☐ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/William E. Wooten/	Date (YYYY-MM-DD)	2015-06-19
Name/Print	William E. Wooten	Registration Number	60049

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Electronic Patent Application Fee Transmittal

Application Number:	13657010
Filing Date:	22-Oct-2012
Title of Invention:	METHODS AND SYSTEMS FOR PROTECTING A SECURED NETWORK
First Named Inventor/Applicant Name:	Steven Rogers
Filer:	William Eugene Wooten
Attorney Docket Number:	007742.00017

Filed as Small Entity

Filing Fees for Utility under 35 USC 111(a)

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Petition Fee-37CFR 1.17(h) (Group II)	2464	1	70	70
Request for Continued Examination	2801	1	600	600
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Miscellaneous:				
		Total in USD ($)		**670**

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

Decision Date : June 19, 2015

In re Application of :

Steven Rogers

DECISION ON PETITION
UNDER CFR 1.313(c)(2)

Application No : 13657010

Filed : 22-Oct-2012

Attorney Docket No : 007742.00017

This is an electronic decision on the petition under 37 CFR 1.313(c)(2), filed June 19, 2015 , to withdraw the above-identified application from issue after payment of the issue fee.

The petition is **GRANTED.**

The above-identified application is withdrawn from issue for consideration of a submission under 37 CFR 1.114 (request for continued examination). See 37 CFR 1.313(c)(2).

Petitioner is advised that the issue fee paid in this application cannot be refunded. If, however, this application is again allowed, petitioner may request that it be applied towards the issue fee required by the new Notice of Allowance.

Telephone inquiries concerning this decision should be directed to the Patent Electronic Business Center (EBC) at 866-217-9197.

This application file is being referred to Technology Center AU 2438 for processing of the request for continuing examination under 37 CFR 1.114 .

Office of Petitions

Electronic Acknowledgement Receipt

EFS ID:	22691279
Application Number:	13657010
International Application Number:	
Confirmation Number:	2390
Title of Invention:	METHODS AND SYSTEMS FOR PROTECTING A SECURED NETWORK
First Named Inventor/Applicant Name:	Steven Rogers
Customer Number:	22907
Filer:	William Eugene Wooten
Filer Authorized By:	
Attorney Docket Number:	007742.00017
Receipt Date:	19-JUN-2015
Filing Date:	22-OCT-2012
Time Stamp:	20:45:13
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$670
RAM confirmation Number	5917
Deposit Account	190733
Authorized User	WOOTEN, WILLIAM E.
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows: Charge any Additional Fees required under 37 C.F.R. Section 1.16 (National application filing, search, and examination fees) Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)	

Charge any Additional Fees required under 37 C.F.R. Section 1.19 (Document supply fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.20 (Post Issuance fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.21 (Miscellaneous fees and charges)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Petition automatically granted by EFS	petition-request.pdf	31524 62a9b6ee7dd6dfd070d2356878f1135f4da500cf	no	2
Warnings:					
Information:					
2	Request for Continued Examination (RCE)	RCE.pdf	1349861 e3e0fbb7ab0e1708c651959d682c22bbe8a30a1b	no	3
Warnings:					
Information:					
3	Quick Path Information Disclosure Statement	QPIDS.pdf	166620 7a2bcc9cc9c6337dd8a69e833ad2be0c93b55553	no	2
Warnings:					
Information:					
4	Information Disclosure Statement (IDS) Form (SB08)	IDS.pdf	612048 57d73a31cf30e434c0a379269aa61fc38f281ef1	no	4
Warnings:					
Information:					
5	Fee Worksheet (SB06)	fee-info.pdf	32395 69dd328aa8cdb2fb5f7e92f19ea6e8f540b7f442	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	2192448		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

Doc Code: PET.AUTO Document Description: Petition automatically granted by EFS-Web	PTO/SB/140 U.S. Patent and Trademark Office Department of Commerce

Electronic Petition Request	**PETITION TO WITHDRAW AN APPLICATION FROM ISSUE AFTER PAYMENT OF THE ISSUE FEE UNDER 37 CFR 1.313(c)**
Application Number	13657010
Filing Date	22-Oct-2012
First Named Inventor	Steven Rogers
Art Unit	2438
Examiner Name	KENNETH CHANG
Attorney Docket Number	007742.00017
Title	METHODS AND SYSTEMS FOR PROTECTING A SECURED NETWORK

An application may be withdrawn from issue for further action upon petition by the applicant. To request that the Office withdraw an application from issue, applicant must file a petition under this section including the fee set forth in § 1.17(h) and a showing of good and sufficient reasons why withdrawal of the application from issue is necessary.

APPLICANT HEREBY PETITIONS TO WITHDRAW THIS APPLICATION FROM ISSUE UNDER 37 CFR 1.313(c).

A grantable petition requires the following items:
(1) Petition fee; and
(2) One of the following reasons:
(a) Unpatentability of one or more claims, which must be accompanied by an unequivocal statement that one or more claims are unpatentable, an amendment to such claim or claims, and an explanation as to how the amendment causes such claim or claims to be patentable;
(b) Consideration of a request for continued examination in compliance with § 1.114 (for a utility or plant application only); or
(c) Express abandonment of the application. Such express abandonment may be in favor of a continuing application, but not a CPA under 37 CFR 1.53(d).

Petition Fee

(●)	Small Entity
( )	Micro Entity
( )	Regular Undiscounted

Reason for withdrawal from issue

◯ One or more claims are unpatentable ◉ Consideration of a request for continued examination (RCE) (List of Required Documents and Fees) ◯ Applicant hereby expressly abandons the instant application (any attorney/agent signing for this reason must have power of attorney pursuant to 37 CFR 1.32(b)).
RCE request,submission, and fee. ☐ I certify, in accordance with 37 CFR 1.4(d)(4) that : The RCE request ,submission, and fee have already been filed in the above-identified application on ☒ Are attached.
THIS PORTION MUST BE COMPLETED BY THE SIGNATORY OR SIGNATORIES I certify, in accordance with 37 CFR 1.4(d)(4) that I am: ◉ An attorney or agent registered to practice before the Patent and Trademark Office who has been given power of attorney in this application. ◯ An attorney or agent registered to practice before the Patent and Trademark Office, acting in a representative capacity. ◯ A sole inventor ◯ A joint inventor; I certify that I am authorized to sign this submission on behalf of all of the inventors as evidenced by the power of attorney in the application ◯ A joint inventor; all of whom are signing this e-petition

Signature	/William E. Wooten/
Name	William E. Wooten
Registration Number	60049

Electronic Patent Application Fee Transmittal

Application Number:	13657010
Filing Date:	22-Oct-2012
Title of Invention:	METHODS AND SYSTEMS FOR PROTECTING A SECURED NETWORK
First Named Inventor/Applicant Name:	Steven Rogers
Filer:	William Eugene Wooten
Attorney Docket Number:	007742.00017

Filed as Small Entity

Filing Fees for Utility under 35 USC 111(a)

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
Submission- Information Disclosure Stmt	2806	1	90	90
		Total in USD ($)		**90**

Electronic Acknowledgement Receipt

EFS ID:	22691319
Application Number:	13657010
International Application Number:	
Confirmation Number:	2390
Title of Invention:	METHODS AND SYSTEMS FOR PROTECTING A SECURED NETWORK
First Named Inventor/Applicant Name:	Steven Rogers
Customer Number:	22907
Filer:	William Eugene Wooten
Filer Authorized By:	
Attorney Docket Number:	007742.00017
Receipt Date:	19-JUN-2015
Filing Date:	22-OCT-2012
Time Stamp:	20:46:14
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$90
RAM confirmation Number	5926
Deposit Account	190733
Authorized User	WOOTEN, WILLIAM E.
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows: Charge any Additional Fees required under 37 C.F.R. Section 1.16 (National application filing, search, and examination fees) Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)	

Charge any Additional Fees required under 37 C.F.R. Section 1.19 (Document supply fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.20 (Post Issuance fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.21 (Miscellaneous fees and charges)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Fee Worksheet (SB06)	fee-info.pdf	30668 8d5da0860f409476142b33270bba2581d92bd7e0	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	30668		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PTO/SB/08a (03-15)
Approved for use through 07/31/2016. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**		
	Application Number	13657010
	Filing Date	2012-10-22
	First Named Inventor	Steven ROGERS
	Art Unit	2438
	Examiner Name	Chang, Kenneth W.
	Attorney Docket Number	007742.00017

U.S.PATENTS						Remove
Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	8004994	B1	2011-08-23	Darisi et al.	
If you wish to add additional U.S. Patent citation information please click the Add button.						Add

U.S.PATENT APPLICATION PUBLICATIONS						Remove
Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20030154297	A1	2003-08-14	Suzuki et al.	
	2	20060114899	A1	2006-06-01	Toumura et al.	
	3	20110185055	A1	2011-07-28	Nappier et al.	
	4	20120331543	A1	2012-12-27	Bostrom et al.	
	5	20130254766	A1	2013-09-26	Zuo et al.	
If you wish to add additional U.S. Published Application citation information please click the Add button.						Add

FOREIGN PATENT DOCUMENTS	Remove

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13657010
	Filing Date	2012-10-22
	First Named Inventor	Steven ROGERS
	Art Unit	2438
	Examiner Name	Chang, Kenneth W.
	Attorney Docket Number	007742.00017

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							☐

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1		☐

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**		
	Application Number	13657010
	Filing Date	2012-10-22
	First Named Inventor	Steven ROGERS
	Art Unit	2438
	Examiner Name	Chang, Kenneth W.
	Attorney Docket Number	007742.00017

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☐ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☒ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

☐ See attached certification statement.

☒ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☐ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/William E. Wooten/	Date (YYYY-MM-DD)	2015-07-23
Name/Print	William E. Wooten	Registration Number	60049

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Electronic Patent Application Fee Transmittal

Application Number:	13657010
Filing Date:	22-Oct-2012
Title of Invention:	METHODS AND SYSTEMS FOR PROTECTING A SECURED NETWORK
First Named Inventor/Applicant Name:	Steven Rogers
Filer:	William Eugene Wooten
Attorney Docket Number:	007742.00017

Filed as Small Entity

Filing Fees for Utility under 35 USC 111(a)

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
Submission- Information Disclosure Stmt	2806	1	90	90
		Total in USD ($)		**90**

Electronic Acknowledgement Receipt

EFS ID:	23011217
Application Number:	13657010
International Application Number:	
Confirmation Number:	2390
Title of Invention:	METHODS AND SYSTEMS FOR PROTECTING A SECURED NETWORK
First Named Inventor/Applicant Name:	Steven Rogers
Customer Number:	22907
Filer:	William Eugene Wooten
Filer Authorized By:	
Attorney Docket Number:	007742.00017
Receipt Date:	23-JUL-2015
Filing Date:	22-OCT-2012
Time Stamp:	23:37:07
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$90
RAM confirmation Number	7303
Deposit Account	190733
Authorized User	WOOTEN, WILLIAM E.
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows: Charge any Additional Fees required under 37 C.F.R. Section 1.16 (National application filing, search, and examination fees) Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)	

Charge any Additional Fees required under 37 C.F.R. Section 1.19 (Document supply fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.20 (Post Issuance fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.21 (Miscellaneous fees and charges)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Information Disclosure Statement (IDS) Form (SB08)	IDS.pdf	1035152 9c0b74a513ed34b7a31cfbe4f7304b4b72797bd5	no	4
Warnings:					
Information:					
2	Fee Worksheet (SB06)	fee-info.pdf	30668 3c2d2255ec44630f282f79ad79cdc6332e0bd054	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	1065820		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/657,010	10/22/2012	Steven Rogers	007742.00017	2390

22907 7590 07/24/2015

BANNER & WITCOFF, LTD.
1100 13th STREET, N.W.
SUITE 1200
WASHINGTON, DC 20005-4051

EXAMINER	
CHANG, KENNETH W	

ART UNIT	PAPER NUMBER
2438	

MAIL DATE	DELIVERY MODE
07/24/2015	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Supplemental Notice of Allowability	Application No. 13/657,010	Applicant(s) ROGERS ET AL.	
	Examiner KENNETH CHANG	Art Unit 2438	AIA (First Inventor to File) Status No

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *the QPIDS request and IDS filed 06/19/2015*.
   ☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on_____.
2. ☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.
3. ☒ The allowed claim(s) is/are *1-4,6,8-20 and 23-100*. As a result of the allowed claim(s), you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to PPHfeedback@uspto.gov .
4. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   Certified copies:
   a) ☐ All b) ☐ Some *c) ☐ None of the:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).
6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☒ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date 06/19/2015
3. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
4. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____ .
5. ☐ Examiner's Amendment/Comment
6. ☐ Examiner's Statement of Reasons for Allowance
7. ☐ Other _____.

/KENNETH CHANG/
Examiner, Art Unit 2438

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	13657010
Filing Date	2012-10-22
First Named Inventor	Steven ROGERS
Art Unit	2438
Examiner Name	Chang, Kenneth W.
Attorney Docket Number	007742.00017

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
/K.C./	1	7478429	B2	2009-01-13	Lyon	
	2	7818794	B2	2010-10-19	Wittman	
	3	8935785	B2	2015-01-13	Pandrangi	

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2]	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							☐

Ltrs wdtz rtz ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.C./

Receipt date: 06/19/2015	Application Number	13657010	13657010 - GAU: 2438
INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**	Filing Date	2012-10-22	
	First Named Inventor	Steven ROGERS	
	Art Unit	2438	
	Examiner Name	Chang, Kenneth W.	
	Attorney Docket Number	007742.00017	

If you wish to add additional Foreign Patent Document citation information please click the Add button			Add
NON-PATENT LITERATURE DOCUMENTS			Remove
Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1		☐
If you wish to add additional non-patent literature document citation information please click the Add button			Add

EXAMINER SIGNATURE			
Examiner Signature	/Kenneth Chang/	Date Considered	07/22/2015

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.C./

PTO/SB/08a (03-15)
Approved for use through 07/31/2016. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**		
	Application Number	13657010
	Filing Date	2012-10-22
	First Named Inventor	Steven ROGERS
	Art Unit	2438
	Examiner Name	Chang, Kenneth W.
	Attorney Docket Number	007742.00017

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	6317837	B1	2001-11-13	Kenworthy	
	2	8306994	B2	2012-11-06	Kenworthy	

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20020049899	A1	2002-04-25	Kenworthy	
	2	20060136987	A1	2006-06-22	Okuda	
	3	20060146879	A1	2006-07-06	Anthias et al.	
	4	20070240208	A1	2007-10-11	Yu et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13657010
	Filing Date	2012-10-22
	First Named Inventor	Steven ROGERS
	Art Unit	2438
	Examiner Name	Chang, Kenneth W.
	Attorney Docket Number	007742.00017

	5	20100242098	A1	2010-09-23	Kenworthy	
	6	20130061294	A1	2013-03-07	Kenworthy	

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							☐

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1	Communication Relating to the Results of the Partial International Search for International App. No. PCT/ US2015/024691, dated July 10, 2015.	☐
	2	International Preliminary Report on Patentability for International App. No. PCT/US2013/072566, dated July 23, 2015.	☐

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

EFS Web 2.1.17

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13657010
	Filing Date	2012-10-22
	First Named Inventor	Steven ROGERS
	Art Unit	2438
	Examiner Name	Chang, Kenneth W.
	Attorney Docket Number	007742.00017

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**		
	Application Number	13657010
	Filing Date	2012-10-22
	First Named Inventor	Steven ROGERS
	Art Unit	2438
	Examiner Name	Chang, Kenneth W.
	Attorney Docket Number	007742.00017

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☐ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

☐ See attached certification statement.

☐ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/William E. Wooten/	Date (YYYY-MM-DD)	2015-07-24
Name/Print	William E. Wooten	Registration Number	60049

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

PATENT COOPERATION TREATY

From the INTERNATIONAL SEARCHING AUTHORITY

PCT

To:
Wright, Bradley C.
BANNER & WITCOFF, LTD.
1100 13th Street, N.W. Suite 1200
Washington, DC 20005-4051
ETATS-UNIS D'AMERIQUE

INVITATION TO PAY ADDITIONAL FEES AND, WHERE APPLICABLE, PROTEST FEE

(PCT Article 17(3)(a) and Rule 40.1 and 40.2(e))

Applicant's or agent's file reference 007742.00043	Date of mailing *(day/month/year)* 10 July 2015 (10-07-2015) **PAYMENT DUE** within **ONE MONTH** from the above date of mailing
International application No. PCT/US2015/024691	International filing date *(day/month/year)* 7 April 2015 (07-04-2015)
Applicant CENTRIPETAL NETWORKS, INC.	

1. This International Searching Authority

(i) considers that there are 3 *(number of)* inventions claimed in the international application covered by the claims indicated on an extra sheet:

(ii) therefore considers that **the international application does not comply with the requirements of unity of invention** (Rules 13.1, 13.2 and 13.3) for the reasons indicated on an extra sheet:

(iii) [X] has carried out a partial international search (see Annex) [ ] will establish the international search report on those parts of the international application which relate to the invention first mentioned in claims Nos.:

see extra sheet

(iv) will establish the international search report on the other parts of the international application only if, and to the extent to which, additional fees are paid.

2. Consequently, the applicant is hereby **invited to pay,** within the time limit indicated above, the amount indicated below:

EUR 1.875,00	x	2	=	EUR 3.750,00
Fee per additional invention		number of additional inventions		currency/total amount of additional fees

3. The applicant is informed that, according to Rule 40.2(c), **the payment of any additional fee may be made under protest,** i.e., a reasoned statement to the effect that the international application complies with the requirement of unity of invention or that the amount of the required additional fee is excessive, where applicable, subject to the payment of a protest fee.

Where the applicant pays additional fees under protest, the applicant is hereby invited, within the time limit indicated above, to pay a protest fee (Rule 40.2(e)) in the amount of EUR 865,00 *(currency/amount)*

Where the applicant has not, within the time limit indicated above, paid the required protest fee, the protest will be considered not to have been made and the International Searching Authority will so declare.

4. [ ] Claim(s) Nos. _____ have been found to be unsearchable under Article 17(2)(b) because of defects under Article 17(2)(a) and therefore have not been included with any invention.

Name and mailing address of the International Searching Authority	Authorized officer	
European Patent Office, P.B. 5818 Patentlaan 2 NL-2280 HV Rijswijk Tel. (+31-70) 340-2040 Fax: (+31-70) 340-3016	BARRIO BARANANO, Ainhoa Tel: +49 (0)89 2399-8621	RECEIVED JUL 21 2015 BANNER & WITCOFF LTD

Form PCT/ISA/206 (April 2005)
Registered Mail

INVITATION TO PAY ADDITIONAL FEES

International application No.
PCT/US2015/024691

This International Searching Authority found multiple (groups of) inventions in this international application, as follows:

1. claims: 1-9

A method for packet filtering based on application-layer packet header information

---

2. claims: 10-18

A method for selective packet digest logging

---

3. claims: 19, 20

A method for security policy update and management

The lack of unity becomes apparent a posteriori, i.e. for the following reasoning document D1 (US20060136987) is taken into account. From this prior art document what is known is a method comprising a security policy management server ("the controller 13 provides the identifying rule and the processing rule" in paragraph [0093]; "the controller may delete from the identifying rule/processing rule setting table the identifying rule and the processing rule which have not been accessed for a predetermined time." in paragraph [0036]) as claimed in claim 1. These features are the only features common to all the groups of inventions.
With the reference to the prior art document D1:
The third group yields the potential special technical feature of receiving, by a security policy management server and from a computing device, a security update comprising a set of network addresses; updating, one or more rules; receiving, from a different computing device, a security update comprising a different set of network addresses; determining that the different set of network addresses includes at least a portion of network addresses included in the set of network addresses; and responsive to that identifying the at least a portion of network addresses included in the set of network addresses, at least one of the one or more rules stored in the memory that specifies a range of network addresses comprising the at least a portion of network addresses; and updating the at least one of the one or more rules to include one or more other network addresses included in the different set of network addresses, hence solving the objective problem of how to manage security policies based on information received from different sources comprising overlapping network addresses.
Moreover, the first and second invention have further common features, which are also disclosed in document D1 as shown in the following. From document D1 what is further known is:
receiving ("receive the identifying rule and the processing rule from another communication apparatus" in paragraph [0040]), by each of a plurality of packet security gateways associated with a security policy management server and from the security policy management server ("the controller 13 provides the identifying rule and the processing rule" in paragraph [0093]; "while the notifying destination of the notifying

message (identifying rule and the processing rule) 740 is made the router 100C in FIG. 8, the gateway apparatus, a switch, and a management system (not shown) may be made a notifying destination." in paragraph [0095]), a dynamic security policy ("receive the identifying rule and the processing rule from another communication apparatus" in paragraph [0040]; "the controller may delete from the identifying rule/processing rule setting table the identifying rule and the processing rule which have not been accessed for a predetermined time." in paragraph [0036]) that includes at least one rule specifying a packet transformation function to be performed on packets

receiving, by a packet security gateway of the plurality of packet security gateways, packets associated with a network protected by the packet security gateway ("received packet" in the abstract);

identifying, by the packet security gateway, from amongst the packets associated with the network protected by the packet security gateway, and on a packet-by-packet basis, one or more packets ("identify a protocol type of a communication packet transmitted/received by a device" in paragraph [0028]); and

performing, by the packet security gateway and on a packet-by-packet basis, the packet transformation function on each of the one or more packets ("to automatically set the processing rule of the packet" in paragraph [0028]; "the processing policy may include a policy concerning at least one of a service quality class, filtering, and routing of the packet." in paragraph [0029]) as claimed in claim 1. These features are the only features common to the first two groups of inventions.

With the reference to the prior art document D1:

The first group yields the potential special technical feature of using application-layer packet-header information as the packet identification at the gateway, hence solving the objective problem of how to improve the scalability issues in high resolution filtering.

The second group yields the potential special technical feature of using a packet digest logging function to the identified packets, hence solving the objective problem of how to enable security awareness information in a network.

Consequently, neither the objective problems underlying the subjects of the three claimed inventions, nor the solutions as defined by the special technical features described allow for the link of a common inventive concept to be established between said inventions in the meaning of Rule 13.2 PCT. In conclusion, the three groups of claims are not linked by a single general inventive concept. The application hence does not meet the requirements of unity of invention as defined in Rule 13.1 PCT.

Annex to Form PCT/ISA/206
COMMUNICATION RELATING TO THE RESULTS OF THE PARTIAL INTERNATIONAL SEARCH

International Application No
PCT/US2015/024691

1. The present communication is an Annex to the invitation to pay additional fees (Form PCT/ISA/206). It shows the results of the international search established on the parts of the international application which relate to the invention first mentioned in claims Nos.:
see 'Invitation to pay additional fees'
2. This communication is not the international search report which will be established according to Article 18 and Rule 43.

3. If the applicant does not pay any additional search fees, the information appearing in this communication will be considered as the result of the international search and will be included as such in the international search report.

4. If the applicant pays additional fees, the international search report will contain both the information appearing in this communication and the results of the international search on other parts of the international application for which such fees will have been paid.

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2006/136987 A1 (OKUDA MASATO [JP]) 22 June 2006 (2006-06-22) paragraph [0028] - paragraph [0030]; figures 1,21 paragraphs [0033], [0036], [0040], [0093], [0095], [0135]	1-9
X	US 2007/240208 A1 (YU MING-CHE [TW] ET AL) 11 October 2007 (2007-10-11) abstract paragraphs [0021], [0024] - paragraph [0026] paragraph [0033] - paragraph [0036] paragraph [0039] - paragraph [0040]	1-9
A	US 2006/146879 A1 (ANTHIAS TEFCROS [US] ET AL) 6 July 2006 (2006-07-06) paragraph [0074] - paragraph [0076] paragraph [0112] - paragraph [0119] paragraphs [0207], [0208], [0240]	1-9
A	US 8 306 994 B2 (KENWORTHY STACY [US]) 6 November 2012 (2012-11-06) abstract; figures 4,6 column 2 - column 4 column 6 - column 9	1-9

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

1

Patent Family Annex

Information on patent family members

International Application No
PCT/US2015/024691

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2006136987 A1	22-06-2006	JP 2006174350 A	29-06-2006
		US 2006136987 A1	22-06-2006
US 2007240208 A1	11-10-2007	NONE	
US 2006146879 A1	06-07-2006	CN 101099345 A	02-01-2008
		EP 1834453 A2	19-09-2007
		US 2006146879 A1	06-07-2006
		WO 2006073740 A2	13-07-2006
US 8306994 B2	06-11-2012	US 6317837 B1	13-11-2001
		US 2002049899 A1	25-04-2002
		US 2010242098 A1	23-09-2010
		US 2013061294 A1	07-03-2013

European Patent Organisation

Account details

N° 3 338 800 00 (BLZ 700 800 00)
Commerzbank
Promenadeplatz 7
D-80273 München
SWIFT Code: DRESDEFF700
IBAN: DE20 7008 0000 0333 880000
BIC: DRESDEFF

PATENT COOPERATION TREATY

From the INTERNATIONAL BUREAU

PCT

NOTIFICATION CONCERNING TRANSMITTAL OF COPY OF INTERNATIONAL PRELIMINARY REPORT ON PATENTABILITY (CHAPTER I OF THE PATENT COOPERATION TREATY)
(PCT Rule 44bis.1(c))

To:

WRIGHT, Bradley C.
1100 13th Street, N.W.
Suite 1200
Washington, District of Columbia 20005-4051
ETATS-UNIS D'AMERIQUE

Date of mailing *(day/month/year)*	
23 July 2015 (23.07.2015)	

Applicant's or agent's file reference	IMPORTANT NOTICE
007742.00025	

International application No.	International filing date *(day/month/year)*	Priority date *(day/month/year)*
PCT/US2013/072566	02 December 2013 (02.12.2013)	11 January 2013 (11.01.2013)

Applicant: CENTRIPETAL NETWORKS, INC.

The International Bureau transmits herewith a copy of the international preliminary report on patentability (Chapter I of the Patent Cooperation Treaty)

The International Bureau of WIPO
34, chemin des Colombettes
1211 Geneva 20, Switzerland

Facsimile No. +41 22 338 82 70

Authorized officer
Simin Baharlou

e-mail: pt09.pct@wipo.int

Form PCT/IB/326 (January 2004)

PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY REPORT ON PATENTABILITY

(Chapter I of the Patent Cooperation Treaty)

(PCT Rule 44*bis*)

Applicant's or agent's file reference 007742.00025	**FOR FURTHER ACTION**	See item 4 below
International application No. PCT/US2013/072566	International filing date *(day/month/year)* 02 December 2013 (02.12.2013)	Priority date *(day/month/year)* 11 January 2013 (11.01.2013)
International Patent Classification (8th edition unless older edition indicated) See relevant information in Form PCT/ISA/237		
Applicant CENTRIPETAL NETWORKS, INC.		

1. This international preliminary report on patentability (Chapter I) is issued by the International Bureau on behalf of the International Searching Authority under Rule 44 *bis*.1(a).

2. This REPORT consists of a total of 5 sheets, including this cover sheet.

   In the attached sheets, any reference to the written opinion of the International Searching Authority should be read as a reference to the international preliminary report on patentability (Chapter I) instead.

3. This report contains indications relating to the following items:

☒	Box No. I	Basis of the report
☐	Box No. II	Priority
☐	Box No. III	Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
☐	Box No. IV	Lack of unity of invention
☒	Box No. V	Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
☐	Box No. VI	Certain documents cited
☐	Box No. VII	Certain defects in the international application
☐	Box No. VIII	Certain observations on the international application

4. The International Bureau will communicate this report to designated Offices in accordance with Rules 44*bis*.3(c) and 93*bis*.1 but not, except where the applicant makes an express request under Article 23(2), before the expiration of 30 months from the priority date (Rule 44*bis* .2).

	Date of issuance of this report 14 July 2015 (14.07.2015)
The International Bureau of WIPO 34, chemin des Colombettes 1211 Geneva 20, Switzerland Facsimile No. +41 22 338 82 70	Authorized officer Simin Baharlou e-mail: pt09.pct@wipo.int

Form PCT/IB/373 (January 2004)

PATENT COOPERATION TREATY

From the
INTERNATIONAL SEARCHING AUTHORITY

To:

see form PCT/ISA/220

PCT

WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY
(PCT Rule 43*bis*.1)

Date of mailing
(day/month/year) see form PCT/ISA/210 (second sheet)

Applicant's or agent's file reference
see form PCT/ISA/220

FOR FURTHER ACTION
See paragraph 2 below

International application No.	International filing date *(day/month/year)*	Priority date *(day/month/year)*
PCT/US2013/072566	02.12.2013	11.01.2013

International Patent Classification (IPC) or both national classification and IPC
INV. H04L29/06

Applicant
CENTRIPETAL NETWORKS, INC.

1. This opinion contains indications relating to the following items:

- ☒ Box No. I Basis of the opinion
- ☐ Box No. II Priority
- ☐ Box No. III Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- ☐ Box No. IV Lack of unity of invention
- ☒ Box No. V Reasoned statement under Rule 43*bis*.1(a)(i) with regard to novelty, inventive step and industrial applicability; citations and explanations supporting such statement
- ☐ Box No. VI Certain documents cited
- ☐ Box No. VII Certain defects in the international application
- ☐ Box No. VIII Certain observations on the international application

2. **FURTHER ACTION**

If a demand for international preliminary examination is made, this opinion will usually be considered to be a written opinion of the International Preliminary Examining Authority ("IPEA") except that this does not apply where the applicant chooses an Authority other than this one to be the IPEA and the chosen IPEA has notifed the International Bureau under Rule 66.1*bis*(b) that written opinions of this International Searching Authority will not be so considered.

If this opinion is, as provided above, considered to be a written opinion of the IPEA, the applicant is invited to submit to the IPEA a written reply together, where appropriate, with amendments, before the expiration of 3 months from the date of mailing of Form PCT/ISA/220 or before the expiration of 22 months from the priority date, whichever expires later.

For further options, see Form PCT/ISA/220.

Name and mailing address of the ISA:	Date of completion of this opinion	Authorized Officer
European Patent Office P.B. 5818 Patentlaan 2 NL-2280 HV Rijswijk - Pays Bas Tel. +31 70 340 - 2040 Fax. +31 70 340 - 3016	see form PCT/ISA/210	Oliveira, Joel Telephone No. +31 70 340-3334

Form PCT/ISA/237 (Cover Sheet) (July 2009)

Box No. I Basis of the opinion

1. With regard to the **language**, this opinion has been established on the basis of:

   ☑ the international application in the language in which it was filed

   ☐ a translation of the international application into , which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1 (b)).

2. ☐ This opinion has been established taking into account the **rectification of an obvious mistake** authorized by or notified to this Authority under Rule 91 (Rule 43bis.1(a))

3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, this opinion has been established on the basis of a sequence listing filed or furnished:

   a. (means)

      ☐ on paper

      ☐ in electronic form

   b. (time)

      ☐ in the international application as filed

      ☐ together with the international application in electronic form

      ☐ subsequently to this Authority for the purposes of search

4. ☐ In addition, in the case that more than one version or copy of a sequence listing has been filed or furnished, the required statements that the information in the subsequent or additional copies is identical to that in the application as filed or does not go beyond the application as filed, as appropriate, were furnished.

5. Additional comments:

Box No. V Reasoned statement under Rule 43*bis*.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Yes:	Claims	2, 3, 6-9, 11, 13, 14, 17-22, 24
	No:	Claims	1, 4, 5, 10, 12, 15, 16, 23
Inventive step (IS)	Yes:	Claims	
	No:	Claims	1-24
Industrial applicability (IA)	Yes:	Claims	1-24
	No:	Claims	

2. Citations and explanations

see separate sheet

Re Item V

Reasoned statement with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

Reference is made to the following documents:

D1 EP 1 313 290 A1 (STONESOFT CORP [FI]) 21 May 2003 (2003-05-21)

D2 WO 2005/046145 A1 (ERICSSON TELEFON AB L M [SE]) 19 May 2005 (2005-05-19)

D3 US 2011/055916 A1 (AHN DAVID K [US]) 3 March 2011 (2011-03-03)

1 The present application does not meet the criteria of Article 33(2) PCT, because the subject-matter of claims **1, 12 and 23** is not new.

1.1 **D1** discloses a method comprising, at a network protection device **(abstract)**:

receiving a first rule set **(paragraph [0010], column3 lines 4-7)**;

receiving a second rule set **(paragraph [0010], column3 lines 4-7)**;

preprocessing the first rule set and the second rule set **(considered to be implicit from paragraphs [0010], [0013], [0040]: when a new set of rules is made available it must be made certain that they do not contain errors which could stop the filtering of the firewall)**;

configuring the network protection device to process packets in accordance with the first rule set **(paragraph [0010], column3 lines 13-18)**;

receiving packets **(column 6 lines 23-26)**;

processing a first portion of the packets in accordance with the first rule set **(paragraphs [0010], [0020])**;

reconfiguring the network protection device to process packets in accordance with the second rule set **(paragraphs [0010], [0024])**; and

processing a second portion of the packets in accordance with the second rule set **(paragraphs [0010], [0024])**.

1.2 The same reasoning applies, mutatis mutandis, to the subject-matter of the corresponding independent apparatus and computer-readable media claims **12 and 23**, which therefore are also considered not new.

1.3 Dependent claims **2-11, 13-22 and 24** do not contain any features which, in combination with the features of any claim to which they refer, meet the requirements of the PCT in respect of novelty (for claims **4, 5, 10, 15, 16**) and/or inventive step (for claims **2, 3, 6, 7, 8, 9, 11, 13, 14, 17, 18, 19, 20, 21, 22, 24)** see passages cited in the Search Report.

Electronic Acknowledgement Receipt

EFS ID:	23018436
Application Number:	13657010
International Application Number:	
Confirmation Number:	2390
Title of Invention:	METHODS AND SYSTEMS FOR PROTECTING A SECURED NETWORK
First Named Inventor/Applicant Name:	Steven Rogers
Customer Number:	22907
Filer:	William Eugene Wooten
Filer Authorized By:	
Attorney Docket Number:	007742.00017
Receipt Date:	24-JUL-2015
Filing Date:	22-OCT-2012
Time Stamp:	15:26:42
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Information Disclosure Statement (IDS) Form (SB08)	IDS.pdf	1035482 084bb5213460456a3fa29f03e21bf9ce8b4546d4	no	5
Warnings:					
Information:					

2	Non Patent Literature	NPL1.pdf	815786 eb48aa2043fa84c9e8370fe50f66417815b641ca	no	6
Warnings:					
Information:					
3	Non Patent Literature	NPL2.pdf	4664429 f85b52c4383706df599c6d06af9ca94e83f98034	no	6
Warnings:					
Information:					
			Total Files Size (in bytes):	6515697	

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

Electronic Acknowledgement Receipt

EFS ID:	22691279
Application Number:	13657010
International Application Number:	
Confirmation Number:	2390
Title of Invention:	METHODS AND SYSTEMS FOR PROTECTING A SECURED NETWORK
First Named Inventor/Applicant Name:	Steven Rogers
Customer Number:	22907
Filer:	William Eugene Wooten
Filer Authorized By:	
Attorney Docket Number:	007742.00017
Receipt Date:	19-JUN-2015
Filing Date:	22-OCT-2012
Time Stamp:	20:45:13
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$670
RAM confirmation Number	5917
Deposit Account	190733
Authorized User	WOOTEN, WILLIAM E.
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows: Charge any Additional Fees required under 37 C.F.R. Section 1.16 (National application filing, search, and examination fees) Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)	

Electronic Patent Application Fee Transmittal

Application Number:	13657010
Filing Date:	22-Oct-2012
Title of Invention:	METHODS AND SYSTEMS FOR PROTECTING A SECURED NETWORK
First Named Inventor/Applicant Name:	Steven Rogers
Filer:	William Eugene Wooten
Attorney Docket Number:	007742.00017

Filed as Small Entity

Filing Fees for Utility under 35 USC 111(a)

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Petition Fee-37CFR 1.17(h) (Group II)	2464	1	70	70
Request for Continued Examination	2801	1	600	600
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				

Adjustment date: 07/20/2015 SDIBETA1
06/22/2015 INTEFGU 00005917 190733 13657010
02 FC:2801 600.00 CR

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/657,010	10/22/2012	Steven Rogers	007742.00017	2390

22907 7590 08/11/2015

BANNER & WITCOFF, LTD.
1100 13th STREET, N.W.
SUITE 1200
WASHINGTON, DC 20005-4051

EXAMINER
CHANG, KENNETH W

ART UNIT	PAPER NUMBER
2438	

MAIL DATE	DELIVERY MODE
08/11/2015	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES DEPARTMENT OF COMMERCE
U.S. Patent and Trademark Office
Address : COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450

APPLICATION NO./ CONTROL NO.	FILING DATE	FIRST NAMED INVENTOR / PATENT IN REEXAMINATION	ATTORNEY DOCKET NO.
13/657,010	22 October, 2012	ROGERS ET AL.	007742.00017

BANNER & WITCOFF, LTD.
1100 13th STREET, N.W.
SUITE 1200
WASHINGTON, DC 20005-4051

EXAMINER	
KENNETH CHANG	
ART UNIT	**PAPER**
2438	20150728

DATE MAILED:

Please find below and/or attached an Office communication concerning this application or proceeding.

Commissioner for Patents

The IDS filed 07/23/15 and the IDS filed 07/24/15 fail to comply with 37 CFR 1.97 because they are filed after payment of the issue fee. They will be considered upon timely filing of a subsequent QPIDS request or Request for Continued Examination.

/JOSNEL JEUDY/
Primary Examiner, Art Unit 2438

PTO-90C (Rev.04-03)

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	ISSUE DATE	PATENT NO.	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/657,010	09/15/2015	9137205	007742.00017	2390

22907 7590 08/26/2015

BANNER & WITCOFF, LTD.
1100 13th STREET, N.W.
SUITE 1200
WASHINGTON, DC 20005-4051

ISSUE NOTIFICATION

The projected patent number and issue date are specified above.

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)
(application filed on or after May 29, 2000)

The Patent Term Adjustment is 198 day(s). Any patent to issue from the above-identified application will include an indication of the adjustment on the front page.

If a Continued Prosecution Application (CPA) was filed in the above-identified application, the filing date that determines Patent Term Adjustment is the filing date of the most recent CPA.

Applicant will be able to obtain more detailed information by accessing the Patent Application Information Retrieval (PAIR) WEB site (http://pair.uspto.gov).

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Application Assistance Unit (AAU) of the Office of Data Management (ODM) at (571)-272-4200.

APPLICANT(s) (Please see PAIR WEB site http://pair.uspto.gov for additional applicants):

Steven Rogers, Leesburg, VA;
Sean Moore, Hollis, NH;
CENTRIPETAL NETWORKS, INC., Leesburg, VA

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re the Application of:		Atty. Docket No.:	007742.00017
Steven ROGERS *et al.*			
Serial No.:	13/657,010	Group Art Unit:	2438
Filed:	October 22, 2012	Examiner:	Chang, Kenneth W.
For:	METHODS AND SYSTEMS FOR PROTECTING A SECURED NETWORK	Confirmation No.:	2390

AMENDMENT UNDER 37 C.F.R. § 1.111

Mail Stop Amendment
Commissioner for Patents
Randolph Building
401 Dulany Street
Alexandria, VA 22314

Dear Sir:

In response to the Non-Final Office Action dated October 21, 2014, please enter the following:

Amendments to the Claims reflected in the Listing of Claims, which begins at page 2 of this paper; and

Remarks, which begin at page 31 of this paper.

Applicant hereby petitions for any applicable extension of time that may be required. If any fees are required or if an overpayment is made, the Commissioner is authorized to debit or credit Deposit Account No. 19-0733, accordingly.

This Listing of Claims will replace all prior versions and listings of claims in the application.

Listing of the Claims:

1. (Currently Amended) A method, comprising:

at each packet security gateway of one or more packet security gateways associated with a security policy management server:

receiving a plurality of dynamic security ~~policy~~ policies from the security policy management server, wherein receiving the plurality of dynamic security policies comprises:

receiving at least one rule specifying a set of network addresses for which associated packets should be forwarded and at least one rule specifying that all packets associated with network addresses outside the set of network addresses for which packets should be forwarded should be dropped;

receiving, at a first time, a dynamic security policy specifying a first set of network addresses for which packets should be forwarded;

receiving, at a second time, a dynamic security policy specifying a second set of network addresses for which packets should be forwarded; and

receiving, at a third time, a dynamic security policy specifying a third set of network addresses for which packets should be forwarded, the second time being after the first time, the third time being after the second time, the second set of network addresses including more network addresses than the first set of network addresses, and the third set of network addresses including more network addresses than the second set of network addresses;

receiving packets associated with a network protected by ~~each respective~~the packet security gateway; and

performing, on a packet by packet basis, at least one of multiple packet transformation functions specified by the plurality of dynamic security ~~policy~~ policies on the packets associated with the network protected by the packet security gateway, wherein performing the at least one of the multiple packet transformation functions specified by the plurality of dynamic security ~~policy~~ policies on the

packets comprises performing at least one packet transformation function other than forwarding or dropping the packets.

2. (Currently Amended) The method of claim 1, wherein the one or more packet security gateways comprise at least two packet security gateways configured in series ~~such that packets forwarded from a first of the at least two packet security gateways are received by a second of the at least two packet security gateways~~, the method comprising:

forwarding, by a first of the at least two packet security gateways and to a second of the at least two packet security gateways, a portion of the packets; and

receiving, by the second of the at least two packet security gateways and from the first of the at least two packet security gateways, the portion of the packets.

3. (Currently Amended) The method of claim 2, wherein [[the]] a dynamic security policy of the plurality of dynamic security policies comprises at least two rules, a second of the at least two rules being ~~required~~ configured to execute ~~subsequent to~~after a first of the at least two rules, ~~and wherein, for the at least two packet security gateways configured in series, performing the at least one of multiple packet transformation functions specified by the dynamic security policy on the packets comprises~~the method comprising:

performing, by the first of the at least two packet security gateways, a ~~first~~ packet transformation function specified by the first of the at least two rules; and

performing, by the second of the at least two packet security gateways, a ~~second~~ packet transformation function specified by the second of the at least two rules.

4. (Currently Amended) The method of claim 1, wherein receiving the plurality of dynamic security ~~policy~~ policies comprises receiving at least one rule specifying a set of network addresses for which associated packets should be dropped and at least one rule specifying that all packets associated with network addresses outside the set of network addresses for which associated packets should be dropped should be forwarded.

5. (Canceled)

6. (Currently Amended) The method of claim [[5]] 1, ~~further~~ comprising:

receiving, by the security policy management server, information associated with a Voice over Internet Protocol (VoIP) session[[,]]; and

~~wherein the at least one rule specifying the set of network addresses for which associated packets should be forwarded is one of created and altered~~creating or altering, by the security policy management server ~~utilizing~~ and based on the information associated with the ~~one or more~~ VoIP ~~sessions~~session, the at least one rule specifying the set of network addresses for which associated packets should be forwarded.

7. (Canceled)

8. (Currently Amended) The method of claim 1, wherein the plurality of dynamic security ~~policy~~ policies ~~comprises at least two rules, a first of the at least two rules specifying a first set of network addresses, a second of the at least two rules specifying a second set of network addresses, and wherein the dynamic security policy specifies~~ specify that a first portion of the packets ~~associated with the first set of network addresses~~ should be placed in a first forwarding queue and a second portion of the packets ~~associated with the second set of network addresses~~ should be placed in a second forwarding queue, the first forwarding queue having a higher forwarding rate than the second forwarding queue, the method comprising:

placing, by the one or more packet security gateways, the first portion of the packets in the first forwarding queue; and

placing, by the one or more packet security gateways, the second portion of the packets in the second forwarding queue.

9. (Currently Amended) The method of claim 1, wherein receiving the plurality of dynamic security ~~policy~~ policies comprises receiving at least one rule specifying ~~a set of network addresses and an additional~~ a parameter, ~~and wherein performing the at least one of multiple packet transformation functions specified by the dynamic security policy on the packets comprises~~the method comprising routing, by the one or more packet security gateways, at least one packet of the packets that ~~falls within the set of network addresses and~~ matches the

~~additional~~ parameter to a network address different from a destination network address specified by the at least one ~~of the packets~~packet.

10. (Currently Amended) The method of claim 9, wherein the ~~additional~~ parameter comprises a Session Initiation Protocol (SIP) Uniform Resource Identifier (URI), wherein the network address different from the destination network address specified by the at least one ~~of the packets~~packet corresponds to a network device configured to copy information contained in the at least one ~~of the packets~~packet and forward the at least one ~~of the packets~~packet to the destination network address specified by the at least one ~~of the packets~~packet, and wherein routing the at least one ~~of the packets that falls within the set of network addresses and matches the additional parameter to a network address different from the destination network address specified by the at least one of the packets~~packet comprises encapsulating the at least one ~~of the packets that falls within the set of network addresses and matches the additional parameter~~packet with a header containing the network address different from the destination network address specified by the at least one ~~of the packets~~packet.

11. (Currently Amended) The method of claim 1, wherein performing the at least one of the multiple packet transformation functions comprises at least one of forwarding the packets into the network protected by the packet security gateway, forwarding the packets out of the network protected by the packet security gateway, forwarding the packets to an Internet Protocol Security (IPsec) stack having an IPsec security association corresponding to the packets, [[and]] or dropping the packets.

12. (Currently Amended) The method of claim 1, wherein receiving the plurality of dynamic security ~~policy~~ policies comprises ~~a plurality of rules, and wherein~~ receiving at least one ~~of the rules specifies~~rule comprising a five-tuple~~, the five-tuple~~ specifying one or more protocols, one or more ~~IP~~ Internet Protocol (IP) source addresses, one or more source port values, one or more IP destination addresses, and one or more destination port values.

13. (Currently Amended) The method of claim 1, wherein receiving the plurality of dynamic security ~~policy~~ policies comprises ~~a plurality of rules, and wherein~~ receiving at least one ~~of~~

~~the rules specifies~~rule comprising a Differentiated Service Code Point (DSCP) selector that maps to a DSCP field in an Internet Protocol (IP) header of the packets.

14. (Currently Amended) The method of claim 1, ~~wherein~~ comprising operating, by at least one of the one or more packet security gateways, ~~operates~~ in a network layer transparent manner by sending and receiving traffic at a link layer using an interface that is not addressed at the network layer and performing the at least one of the multiple packet transformation functions at the network layer.

15. (Currently Amended) The method of claim 14, wherein the at least one of the one or more packet security gateways includes a management interface having a network layer address, ~~and wherein~~the method comprising securing access to the management interface ~~is secured~~ at at least one of an application level, a link level, [[and]] or a transport level.

16. (Currently Amended) The method of claim 1, ~~wherein the dynamic security policy comprises one or more rules generated based, at least in part, on a list of known network addresses associated with malicious network traffic that is received~~comprising:

receiving, by the security policy management server and from a subscription service that aggregates information associated with malicious network traffic, a list of network addresses known to be associated with malicious network traffic; and

generating, by the security policy management server and based at least in part on the list, one or more rules included in the plurality of dynamic security policies.

17. (Currently Amended) The method of claim 1, ~~wherein~~ comprising receiving, by at least two of the one or more packet security gateways ~~receive dynamic security policies~~and from the security policy management server, ~~that include~~ one or more rules specifying source addresses that correspond to spoofed network addresses, [[and]] wherein at least one rule of the ~~dynamic security policies~~one or more rules specifies different source addresses ~~that correspond to spoofed network addresses~~ than at least another ~~one of the dynamic security policies~~rule of the one or more rules.

18. (Currently Amended) The method of claim 1, ~~wherein~~ comprising locating at least one of the one or more packet security gateways ~~is located~~ at each boundary between a protected network associated with the security policy management server and an unprotected network.

19. (Currently Amended) A system, comprising:

a security policy management server; and

one or more packet security gateways associated with the security policy management server, wherein each packet security gateway of the one or more packet security gateways is configured to:

receive a plurality of dynamic security ~~policy~~ policies from the security policy management server;

receive at least one rule specifying a set of network addresses for which associated packets should be forwarded and at least one rule specifying that all packets associated with network addresses outside the set of network addresses for which packets should be forwarded should be dropped;

receive, at a first time, a dynamic security policy specifying a first set of network addresses for which packets should be forwarded;

receive, at a second time, a dynamic security policy specifying a second set of network addresses for which packets should be forwarded;

receive, at a third time, a dynamic security policy specifying a third set of network addresses for which packets should be forwarded, the second time being after the first time, the third time being after the second time, the second set of network addresses including more network addresses than the first set of network addresses, and the third set of network addresses including more network addresses than the second set of network addresses;

receive packets associated with a network protected by ~~each respective~~the packet security gateway; and

perform, on a packet by packet basis, at least one of multiple packet transformation functions specified by the plurality of dynamic security ~~policy~~ policies on the packets associated with the network protected by the packet security gateway, wherein each of the one or more packet security gateways is configured to

perform the at least one of the multiple packet transformation functions specified by the plurality of dynamic security ~~policy~~ policies on the packets by performing at least one packet transformation function other than forwarding or dropping the packets.

20. (Currently Amended) One or more non-transitory computer-readable media having instructions stored thereon, that when executed ~~by one or more computers~~, cause ~~the one or more computers to: at~~ each packet security gateway of one or more packet security gateways associated with a security policy management server to:

receive a plurality of dynamic security ~~policy~~ policies from the security policy management server;

receive at least one rule specifying a set of network addresses for which associated packets should be forwarded and at least one rule specifying that all packets associated with network addresses outside the set of network addresses for which packets should be forwarded should be dropped;

receive, at a first time, a dynamic security policy specifying a first set of network addresses for which packets should be forwarded;

receive, at a second time, a dynamic security policy specifying a second set of network addresses for which packets should be forwarded;

receive, at a third time, a dynamic security policy specifying a third set of network addresses for which packets should be forwarded, the second time being after the first time, the third time being after the second time, the second set of network addresses including more network addresses than the first set of network addresses, and the third set of network addresses including more network addresses than the second set of network addresses;

receive packets associated with a network protected by ~~each respective~~the packet security gateway; and

perform, on a packet by packet basis, at least one of multiple packet transformation functions specified by the plurality of dynamic security ~~policy~~ policies on the packets associated with the network protected by the packet security gateway, wherein each of the one or more packet security gateways is configured to perform the at least one of the multiple packet transformation functions specified by the plurality of dynamic security

~~policy~~ policies on the packets by performing at least one packet transformation function other than forwarding or dropping the packets.

21-22. (Canceled)

23. (New) The system of claim 19, wherein:

the one or more packet security gateways comprise at least two packet security gateways configured in series;

a first of the at least two packet security gateways being configured to forward a portion of the packets to a second of the at least two packet security gateways; and

the second of the at least two packet security gateways being configured to receive the portion of the packets from the first of the at least two packet security gateways.

24. (New) The system of claim 23, wherein:

a dynamic security policy of the plurality of dynamic security policies comprises at least two rules, a second of the at least two rules being configured to execute after a first of the at least two rules;

the first of the at least two packet security gateways is configured to perform a packet transformation function specified by the first of the at least two rules; and

the second of the at least two packet security gateways is configured to perform a packet transformation function specified by the second of the at least two rules.

25. (New) The system of claim 19, wherein each packet security gateway of the one or more packet security gateways is configured to receive at least one rule specifying a set of network addresses for which associated packets should be dropped and at least one rule specifying that all packets associated with network addresses outside the set of network addresses for which associated packets should be dropped should be forwarded.

26. (New) The system of claim 19, wherein the security policy management server is configured to:

receive information associated with a Voice over Internet Protocol (VoIP) session; and

at least one of create or alter, based on the information associated with the VoIP session, the at least one rule specifying the set of network addresses for which associated packets should be forwarded.

27. (New) The system of claim 19, wherein:

the plurality of dynamic security policies specify that a first portion of the packets should be placed in a first forwarding queue and a second portion of the packets should be placed in a second forwarding queue, the first forwarding queue having a higher forwarding rate than the second forwarding queue; and

the one or more packet security gateways are configured to:

place the first portion of the packets in the first forwarding queue; and

place the second portion of the packets in the second forwarding queue.

28. (New) The system of claim 19, wherein:

the plurality of dynamic security policies comprises at least one rule specifying a parameter; and

the one or more packet security gateways are configured to route at least one packet of the packets that matches the parameter to a network address different from a destination network address specified by the at least one packet.

29. (New) The system of claim 28, wherein:

the parameter comprises a Session Initiation Protocol (SIP) Uniform Resource Identifier (URI);

the network address different from the destination network address specified by the at least one packet corresponds to a network device configured to copy information contained in the at least one packet and forward the at least one packet to the destination network address specified by the at least one packet; and

the one or more packet security gateways are configured to encapsulate the at least one packet with a header containing the network address different from the destination network address specified by the at least one packet.

30. (New) The system of claim 19, wherein each packet security gateway of the one or more packet security gateways is configured to at least one of forward the packets into the network protected by the packet security gateway, forward the packets out of the network protected by the packet security gateway, forward the packets to an Internet Protocol Security (IPsec) stack having an IPsec security association corresponding to the packets, or drop the packets.

31. (New) The system of claim 19, wherein each packet security gateway of the one or more packet security gateways is configured to receive at least one rule comprising a five-tuple specifying one or more protocols, one or more Internet Protocol (IP) source addresses, one or more source port values, one or more IP destination addresses, and one or more destination port values.

32. (New) The system of claim 19, wherein each packet security gateway of the one or more packet security gateways is configured to receive at least one rule comprising a Differentiated Service Code Point (DSCP) selector that maps to a DSCP field in an Internet Protocol (IP) header of the packets.

33. (New) The system of claim 19, wherein at least one of the one or more packet security gateways is configured to operate in a network layer transparent manner by sending and receiving traffic at a link layer using an interface that is not addressed at the network layer and performing the at least one of the multiple packet transformation functions at the network layer.

34. (New) The system of claim 33, wherein the at least one of the one or more packet security gateways includes a management interface having a network layer address, and wherein the

at least one of the one or more packet security gateways is configured to secure access to the management interface at at least one of an application level, a link level, or a transport level.

35. (New) The system of claim 19, wherein the security policy management server is configured to:

receive, from a subscription service that aggregates information associated with malicious network traffic, a list of network addresses known to be associated with malicious network traffic; and

generate, based at least in part on the list, one or more rules included in the plurality of dynamic security policies.

36. (New) The system of claim 19, wherein:

at least two of the one or more packet security gateways are configured to receive, from the security policy management server, one or more rules specifying source addresses that correspond to spoofed network addresses; and

at least one rule of the one or more rules specifies different source addresses than at least another rule of the one or more rules.

37. (New) The system of claim 19, wherein at least one of the one or more packet security gateways is located at each boundary between a protected network associated with the security policy management server and an unprotected network.

38. (New) The one or more non-transitory computer-readable media of claim 20, wherein the one or more packet security gateways comprise at least two packet security gateways configured in series, and wherein the instructions, when executed, cause:

a first of the at least two packet security gateways to forward a portion of the packets to a second of the at least two packet security gateways; and

the second of the at least two packet security gateways to receive the portion of the packets from the first of the at least two packet security gateways.

39. (New) The one or more non-transitory computer-readable media of claim 38, wherein a dynamic security policy of the plurality of dynamic security policies comprises at least two rules, a second of the at least two rules being configured to execute after a first of the at least two rules, and wherein the instructions, when executed, cause:

the first of the at least two packet security gateways to perform a packet transformation function specified by the first of the at least two rules; and

the second of the at least two packet security gateways to perform a packet transformation function specified by the second of the at least two rules.

40. (New) The one or more non-transitory computer-readable media of claim 20, wherein the instructions, when executed, cause each packet security gateway of the one or more packet security gateways to receive at least one rule specifying a set of network addresses for which associated packets should be dropped and at least one rule specifying that all packets associated with network addresses outside the set of network addresses for which associated packets should be dropped should be forwarded.

41. (New) The one or more non-transitory computer-readable media of claim 20, wherein the instructions, when executed, cause the security policy management server to:

receive information associated with a Voice over Internet Protocol (VoIP) session; and

at least one of create or alter, based on the information associated with the VoIP session, the at least one rule specifying the set of network addresses for which associated packets should be forwarded.

42. (New) The one or more non-transitory computer-readable media of claim 20, wherein the plurality of dynamic security policies specify that a first portion of the packets should be placed in a first forwarding queue and a second portion of the packets should be placed in a second forwarding queue, the first forwarding queue having a higher forwarding rate than the second forwarding queue, and wherein the instructions, when executed, cause the one or more packet security gateways to:

place the first portion of the packets in the first forwarding queue; and

place the second portion of the packets in the second forwarding queue.

43. (New) The one or more non-transitory computer-readable media of claim 20, wherein the plurality of dynamic security policies comprises at least one rule specifying a parameter, and wherein the instructions, when executed, cause the one or more packet security gateways to route at least one packet of the packets that matches the parameter to a network address different from a destination network address specified by the at least one packet.

44. (New) The one or more non-transitory computer-readable media of claim 43, wherein the parameter comprises a Session Initiation Protocol (SIP) Uniform Resource Identifier (URI), wherein the network address different from the destination network address specified by the at least one packet corresponds to a network device configured to copy information contained in the at least one packet and forward the at least one packet to the destination network address specified by the at least one packet, and wherein the instructions, when executed, cause the one or more packet security gateways to encapsulate the at least one packet with a header containing the network address different from the destination network address specified by the at least one packet.

45. (New) The one or more non-transitory computer-readable media of claim 20, wherein the instructions, when executed, cause each packet security gateway of the one or more packet security gateways to at least one of forward the packets into the network protected by the packet security gateway, forward the packets out of the network protected by the packet security gateway, forward the packets to an Internet Protocol Security (IPsec) stack having an IPsec security association corresponding to the packets, or drop the packets.

46. (New) The one or more non-transitory computer-readable media of claim 20, wherein the instructions, when executed, cause each packet security gateway of the one or more packet security gateways to receive at least one rule comprising a five-tuple specifying one or more protocols, one or more Internet Protocol (IP) source addresses, one or more source port values, one or more IP destination addresses, and one or more destination port values.

47. (New) The one or more non-transitory computer-readable media of claim 20, wherein the instructions, when executed, cause each packet security gateway of the one or more packet security gateways to receive at least one rule comprising a Differentiated Service Code Point (DSCP) selector that maps to a DSCP field in an Internet Protocol (IP) header of the packets.

48. (New) The one or more non-transitory computer-readable media of claim 20, wherein the instructions, when executed, cause at least one packet security gateway of the one or more packet security gateways to operate in a network layer transparent manner by sending and receiving traffic at a link layer using an interface that is not addressed at the network layer and performing the at least one of the multiple packet transformation functions at the network layer.

49. (New) The one or more non-transitory computer-readable media of claim 48, wherein the at least one of the one or more packet security gateways includes a management interface having a network layer address, and wherein the instructions, when executed, cause the at least one packet security gateway of the one or more packet security gateways to secure access to the management interface at at least one of an application level, a link level, or a transport level.

50. (New) The one or more non-transitory computer-readable media of claim 20, wherein the instructions, when executed, cause the security policy management server to:

receive, from a subscription service that aggregates information associated with malicious network traffic, a list of network addresses known to be associated with malicious network traffic; and

generate, based at least in part on the list, one or more rules included in the plurality of dynamic security policies.

51. (New) The one or more non-transitory computer-readable media of claim 20, wherein the instructions, when executed, cause at least two of the one or more packet security gateways to receive, from the security policy management server, one or more rules specifying source

addresses that correspond to spoofed network addresses, at least one rule of the one or more rules specifying different source addresses than at least another rule of the one or more rules.

52. (New) The one or more non-transitory computer-readable media of claim 20, wherein at least one of the one or more packet security gateways is located at each boundary between a protected network associated with the security policy management server and an unprotected network.

53. (New) A method, comprising:

at each of one or more packet security gateways associated with a security policy management server:

receiving, from the security policy management server, a dynamic security policy comprising at least one rule specifying a set of network addresses and a Session Initiation Protocol (SIP) Uniform Resource Identifier (URI);

receiving packets associated with a network protected by the packet security gateway; and

performing, on the packets, on a packet by packet basis, at least one packet transformation function of multiple packet transformation functions specified by the dynamic security policy, wherein performing the at least one packet transformation function comprises:

encapsulating at least one packet of the packets that falls within the set of network addresses and matches the SIP URI with a header containing a network address that is different from a destination network address specified by the at least one packet and that corresponds to a network device configured to copy information contained in the at least one packet and to forward the at least one packet to the destination network address; and

routing the at least one packet to the network address that is different from the destination network address.

54. (New) The method of claim 53, wherein the one or more packet security gateways comprise at least two packet security gateways configured in series, the method comprising:

forwarding, by a first of the at least two packet security gateways, a portion of the packets to a second of the at least two packet security gateways; and

receiving, by the second of the at least two packet security gateways, the portion of the packets from the first of the at least two packet security gateways.

55. (New) The method of claim 54, wherein the dynamic security policy comprises at least two rules, a second of the at least two rules being configured to execute after a first of the at least two rules, the method comprising:

performing, by the first of the at least two packet security gateways, a packet transformation function specified by the first of the at least two rules; and

performing, by the second of the at least two packet security gateways, a packet transformation function specified by the second of the at least two rules.

56. (New) The method of claim 53, wherein receiving the dynamic security policy comprises receiving at least one rule specifying a set of network addresses for which associated packets should be dropped and at least one rule specifying that all packets associated with network addresses outside the set of network addresses for which associated packets should be dropped should be forwarded.

57. (New) The method of claim 53, comprising:

receiving, by the security policy management server, information associated with a Voice over Internet Protocol (VoIP) session; and

creating or altering, by the security policy management server and based on the information associated with the VoIP session, the at least one rule specifying the set of network addresses.

58. (New) The method of claim 53, wherein the dynamic security policy specifies that a first portion of the packets should be placed in a first forwarding queue and a second portion of the packets should be placed in a second forwarding queue, the first forwarding queue having a higher forwarding rate than the second forwarding queue, the method comprising:

placing, by the one or more packet security gateways, the first portion of the packets in the first forwarding queue; and

placing, by the one or more packet security gateways, the second portion of the packets in the second forwarding queue.

59. (New) The method of claim 53, wherein performing the at least one packet transformation function comprises at least one of forwarding the packets into the network protected by the packet security gateway, forwarding the packets out of the network protected by the packet security gateway, forwarding the packets to an Internet Protocol Security (IPsec) stack having an IPsec security association corresponding to the packets, or dropping the packets.

60. (New) The method of claim 53, wherein receiving the dynamic security policy comprises receiving at least one rule comprising a five-tuple specifying one or more protocols, one or more Internet Protocol (IP) source addresses, one or more source port values, one or more IP destination addresses, and one or more destination port values.

61. (New) The method of claim 53, wherein receiving the dynamic security policy comprises receiving at least one rule comprising a Differentiated Service Code Point (DSCP) selector that maps to a DSCP field in an Internet Protocol (IP) header of the packets.

62. (New) The method of claim 53, comprising operating, by at least one of the one or more packet security gateways, in a network layer transparent manner by sending and receiving traffic at a link layer using an interface that is not addressed at the network layer and performing the at least one packet transformation function at the network layer.

63. (New) The method of claim 62, wherein the at least one of the one or more packet security gateways includes a management interface having a network layer address, the method comprising securing access to the management interface at at least one of an application level, a link level, or a transport level.

64. (New) The method of claim 53, comprising:

receiving, by the security policy management server and from a subscription service that aggregates information associated with malicious network traffic, a list of network addresses known to be associated with malicious network traffic; and

generating, by the security policy management server and based at least in part on the list, one or more rules included in the dynamic security policy.

65. (New) The method of claim 53, comprising receiving, by at least two of the one or more packet security gateways and from the security policy management server, one or more rules specifying source addresses that correspond to spoofed network addresses, wherein at least one rule of the one or more rules specifies different source addresses than at least another rule of the one or more rules.

66. (New) The method of claim 53, comprising locating at least one of the one or more packet security gateways at each boundary between a protected network associated with the security policy management server and an unprotected network.

67. (New) A system, comprising:

a security policy management server; and

one or more packet security gateways associated with the security policy management server, wherein each packet security gateway of the one or more packet security gateways is configured to:

receive, from the security policy management server, a dynamic security policy comprising at least one rule specifying a set of network addresses and a Session Initiation Protocol (SIP) Uniform Resource Identifier (URI);

receive packets associated with a network protected by the packet security gateway;

perform, on the packets, on a packet by packet basis, at least one packet transformation function of multiple packet transformation functions specified by the dynamic security policy;

encapsulate at least one packet of the packets that falls within the set of network addresses and matches the SIP URI with a header containing a network

address that is different from a destination network address specified by the at least one packet and that corresponds to a network device configured to copy information contained in the at least one packet and to forward the at least one packet to the destination network address; and

route the at least one packet to the network address that is different from the destination network address.

68. (New) The system of claim 67, wherein:

the one or more packet security gateways comprise at least two packet security gateways configured in series;

a first of the at least two packet security gateways being configured to forward a portion of the packets to a second of the at least two packet security gateways; and

the second of the at least two packet security gateways being configured to receive the portion of the packets from the first of the at least two packet security gateways.

69. (New) The system of claim 68, wherein:

the dynamic security policy comprises at least two rules, a second of the at least two rules being configured to execute after a first of the at least two rules;

the first of the at least two packet security gateways is configured to perform a packet transformation function specified by the first of the at least two rules; and

the second of the at least two packet security gateways is configured to perform a packet transformation function specified by the second of the at least two rules.

70. (New) The system of claim 67, wherein each packet security gateway of the one or more packet security gateways is configured to receive at least one rule specifying a set of network addresses for which associated packets should be dropped and at least one rule specifying that all packets associated with network addresses outside the set of network addresses for which associated packets should be dropped should be forwarded.

71. (New) The system of claim 67, wherein the security policy management server is configured to:

receive information associated with a Voice over Internet Protocol (VoIP) session; and

at least one of create or alter, based on the information associated with the VoIP session, the at least one rule specifying the set of network addresses.

72. (New) The system of claim 67, wherein:

the dynamic security policy specifies that a first portion of the packets should be placed in a first forwarding queue and a second portion of the packets should be placed in a second forwarding queue, the first forwarding queue having a higher forwarding rate than the second forwarding queue; and

the one or more packet security gateways are configured to:

place the first portion of the packets in the first forwarding queue; and

place the second portion of the packets in the second forwarding queue.

73. (New) The system of claim 67, wherein each packet security gateway of the one or more packet security gateways is configured to at least one of forward the packets into the network protected by the packet security gateway, forward the packets out of the network protected by the packet security gateway, forward the packets to an Internet Protocol Security (IPsec) stack having an IPsec security association corresponding to the packets, or drop the packets.

74. (New) The system of claim 67, wherein each packet security gateway of the one or more packet security gateways is configured to receive at least one rule comprising a five-tuple specifying one or more protocols, one or more Internet Protocol (IP) source addresses, one or more source port values, one or more IP destination addresses, and one or more destination port values.

75. (New) The system of claim 67, wherein each packet security gateway of the one or more packet security gateways is configured to receive at least one rule comprising a Differentiated Service Code Point (DSCP) selector that maps to a DSCP field in an Internet Protocol (IP) header of the packets.

76. (New) The system of claim 67, wherein at least one of the one or more packet security gateways is configured to operate in a network layer transparent manner by sending and receiving traffic at a link layer using an interface that is not addressed at the network layer and performing the at least one packet transformation function at the network layer.

77. (New) The system of claim 76, wherein the at least one of the one or more packet security gateways includes a management interface having a network layer address, and wherein the at least one of the one or more packet security gateways is configured to secure access to the management interface at at least one of an application level, a link level, or a transport level.

78. (New) The system of claim 67, wherein the security policy management server is configured to:

receive, from a subscription service that aggregates information associated with malicious network traffic, a list of network addresses known to be associated with malicious network traffic; and

generate, based at least in part on the list, one or more rules included in the dynamic security policy.

79. (New) The system of claim 67, wherein:

at least two of the one or more packet security gateways are configured to receive, from the security policy management server, one or more rules specifying source addresses that correspond to spoofed network addresses; and

at least one rule of the one or more rules specifies different source addresses than at least another rule of the one or more rules.

80. (New) The system of claim 67, wherein at least one of the one or more packet security gateways is located at each boundary between a protected network associated with the security policy management server and an unprotected network.

81. (New) One or more non-transitory computer-readable media having instructions stored thereon, that when executed, cause each packet security gateway of one or more packet security gateways associated with a security policy management server to:

receive, from the security policy management server, a dynamic security policy comprising at least one rule specifying a set of network addresses and a Session Initiation Protocol (SIP) Uniform Resource Identifier (URI);

receive packets associated with a network protected by the packet security gateway;

perform, on the packets, on a packet by packet basis, at least one packet transformation function of multiple packet transformation functions specified by the dynamic security policy;

encapsulate at least one packet of the packets that falls within the set of network addresses and matches the SIP URI with a header containing a network address that is different from a destination network address specified by the at least one packet and that corresponds to a network device configured to copy information contained in the at least one packet and to forward the at least one packet to the destination network address; and

route the at least one packet to the network address that is different from the destination network address.

82. (New) The one or more non-transitory computer-readable media of claim 81, wherein the one or more packet security gateways comprise at least two packet security gateways configured in series, and wherein the instructions, when executed, cause:

a first of the at least two packet security gateways to forward a portion of the packets to a second of the at least two packet security gateways; and

the second of the at least two packet security gateways to receive the portion of the packets from the first of the at least two packet security gateways.

83. (New) The one or more non-transitory computer-readable media of claim 82, wherein the dynamic security policy comprises at least two rules, a second of the at least two rules being configured to execute after a first of the at least two rules, and wherein the instructions, when executed, cause:

the first of the at least two packet security gateways to perform a packet transformation function specified by the first of the at least two rules; and

the second of the at least two packet security gateways to perform a packet transformation function specified by the second of the at least two rules.

84. (New) The one or more non-transitory computer-readable media of claim 81, wherein the instructions, when executed, cause each packet security gateway of the one or more packet security gateways to receive at least one rule specifying a set of network addresses for which associated packets should be dropped and at least one rule specifying that all packets associated with network addresses outside the set of network addresses for which associated packets should be dropped should be forwarded.

85. (New) The one or more non-transitory computer-readable media of claim 81, wherein the instructions, when executed, cause the security policy management server to:

receive information associated with a Voice over Internet Protocol (VoIP) session; and

at least one of create or alter, based on the information associated with the VoIP session, the at least one rule specifying the set of network addresses.

86. (New) The one or more non-transitory computer-readable media of claim 81, wherein the dynamic security policy specifies that a first portion of the packets should be placed in a first forwarding queue and a second portion of the packets should be placed in a second forwarding queue, the first forwarding queue having a higher forwarding rate than the second forwarding queue, and wherein the instructions, when executed, cause the one or more packet security gateways to:

place the first portion of the packets in the first forwarding queue; and

place the second portion of the packets in the second forwarding queue.

87. (New) The one or more non-transitory computer-readable media of claim 81, wherein the instructions, when executed, cause each packet security gateway of the one or more packet security gateways to at least one of forward the packets into the network protected by the

packet security gateway, forward the packets out of the network protected by the packet security gateway, forward the packets to an Internet Protocol Security (IPsec) stack having an IPsec security association corresponding to the packets, or drop the packets.

88. (New) The one or more non-transitory computer-readable media of claim 81, wherein the instructions, when executed, cause each packet security gateway of the one or more packet security gateways to receive at least one rule comprising a five-tuple specifying one or more protocols, one or more Internet Protocol (IP) source addresses, one or more source port values, one or more IP destination addresses, and one or more destination port values.

89. (New) The one or more non-transitory computer-readable media of claim 81, wherein the instructions, when executed, cause each packet security gateway of the one or more packet security gateways to receive at least one rule comprising a Differentiated Service Code Point (DSCP) selector that maps to a DSCP field in an Internet Protocol (IP) header of the packets.

90. (New) The one or more non-transitory computer-readable media of claim 81, wherein the instructions, when executed, cause at least one packet security gateway of the one or more packet security gateways to operate in a network layer transparent manner by sending and receiving traffic at a link layer using an interface that is not addressed at the network layer and performing the at least one packet transformation function at the network layer.

91. (New) The one or more non-transitory computer-readable media of claim 90, wherein the at least one of the one or more packet security gateways includes a management interface having a network layer address, and wherein the instructions, when executed, cause the at least one packet security gateway of the one or more packet security gateways to secure access to the management interface at at least one of an application level, a link level, or a transport level.

92. (New) The one or more non-transitory computer-readable media of claim 81, wherein the instructions, when executed, cause the security policy management server to:

receive, from a subscription service that aggregates information associated with malicious network traffic, a list of network addresses known to be associated with malicious network traffic; and

generate, based at least in part on the list, one or more rules included in the dynamic security policy.

93. (New) The one or more non-transitory computer-readable media of claim 81, wherein the instructions, when executed, cause at least two of the one or more packet security gateways to receive, from the security policy management server, one or more rules specifying source addresses that correspond to spoofed network addresses, at least one rule of the one or more rules specifying different source addresses than at least another rule of the one or more rules.

94. (New) The one or more non-transitory computer-readable media of claim 81, wherein at least one of the one or more packet security gateways is located at each boundary between a protected network associated with the security policy management server and an unprotected network.

95. (New) A method, comprising:

communicating, by a security policy management server and to a packet security gateway located at a first boundary of a network protected by the security policy management server, a first dynamic security policy, the first dynamic security policy comprising one or more rules based on the first boundary;

communicating, by the security policy management server and to a packet security gateway located at a second boundary of the network, a second dynamic security policy, the second dynamic security policy comprising one or more rules based on the second boundary that differ from the one or more rules based on the first boundary;

performing, by the packet security gateway located at the first boundary, at least one of multiple packet transformation functions specified by the first dynamic security policy on a plurality of packets associated with the network that correspond to one or more criteria specified by the one or more rules based on the first boundary; and

performing, by the packet security gateway located at the second boundary, at least one of multiple packet transformation functions specified by the second dynamic security policy on a plurality of packets associated with the network that correspond to one or more criteria specified by the one or more rules based on the second boundary.

96. (New) The method of claim 95, wherein:

the first boundary comprises a boundary between the network protected by the security policy management server and a first network that interfaces with the network protected by the security policy management server;

the second boundary comprises a boundary between the network protected by the security policy management server and a second network that interfaces with the network protected by the security policy management server;

the one or more criteria specified by the one or more rules based on the first boundary comprise one or more criteria based on a set of source network addresses for the first network;

the one or more criteria specified by the one or more rules based on the second boundary comprise one or more criteria based on a set of source network addresses for the second network;

performing the at least one of the multiple packet transformation functions specified by the first dynamic security policy comprises dropping at least one packet, received from the first network, comprising a spoofed source address; and

performing the at least one of the multiple packet transformation functions specified by the second dynamic security policy comprises dropping at least one packet, received from the second network, comprising a different spoofed source address.

97. (New) A system, comprising:

a security policy management server;

a first packet security gateway, located at a first boundary of a network protected by the security policy management server, and configured to:

receive, from the security policy management server, a first dynamic security policy, the first dynamic security policy comprising one or more rules based on the first boundary; and

perform, at least one of multiple packet transformation functions specified by the first dynamic security policy on a plurality of packets that correspond to one or more criteria specified by the one or more rules based on the first boundary; and

a second packet security gateway, located at a second boundary of a network protected by the security policy management server, and configured to:

receive, from the security policy management server, a second dynamic security policy, the second dynamic security policy comprising one or more rules based on the second boundary that differ from the one or more rules based on the first boundary; and

perform at least one of multiple packet transformation functions specified by the second dynamic security policy on a plurality of packets that correspond to one or more criteria specified by the one or more rules based on the second boundary.

98. (New) The system of claim 97, wherein:

the first boundary comprises a boundary between the network protected by the security policy management server and a first network that interfaces with the network protected by the security policy management server;

the second boundary comprises a boundary between the network protected by the security policy management server and a second network that interfaces with the network protected by the security policy management server;

the one or more criteria specified by the one or more rules based on the first boundary comprise one or more criteria based on a set of source network addresses for the first network;

the one or more criteria specified by the one or more rules based on the second boundary comprise one or more criteria based on a set of source network addresses for the second network;

the first packet security gateway is configured to drop at least one packet received from the first network based on a determination that the at least one packet received from the first network comprises a spoofed source address; and

the second packet security gateway is configured to drop at least one packet received from the second network based on a determination that the at least one packet received from the second network comprises a different spoofed source address.

99. (New) One or more non-transitory computer-readable media having instructions stored thereon that when executed cause:

a security policy management server to communicate, to a packet security gateway located at a first boundary of a network protected by the security policy management server, a first dynamic security policy, the first dynamic security policy comprising one or more rules based on the first boundary;

the security policy management server to communicate, to a packet security gateway located at a second boundary of the network, a second dynamic security policy, the second dynamic security policy comprising one or more rules based on the second boundary that differ from the one or more rules based on the first boundary;

the packet security gateway located at the first boundary to perform at least one of multiple packet transformation functions specified by the first dynamic security policy on a plurality of packets associated with the network that correspond to one or more criteria specified by the one or more rules based on the first boundary; and

the packet security gateway located at the second boundary to perform at least one of multiple packet transformation functions specified by the second dynamic security policy on a plurality of packets associated with the network that correspond to one or more criteria specified by the one or more rules based on the second boundary.

100. (New) The one or more non-transitory computer-readable media of claim 99, wherein:

the first boundary comprises a boundary between the network protected by the security policy management server and a first network that interfaces with the network protected by the security policy management server;

the second boundary comprises a boundary between the network protected by the security policy management server and a second network that interfaces with the network protected by the security policy management server;

the one or more criteria specified by the one or more rules based on the first boundary comprise one or more criteria based on a set of source network addresses for the first network;

the one or more criteria specified by the one or more rules based on the second boundary comprise one or more criteria based on a set of source network addresses for the second network; and

the instructions, when executed, cause:

the packet security gateway located at the first boundary to drop at least one packet received from the first network based on a determination that the at least one packet received from the first network comprises a spoofed source address; and

the packet security gateway located at the second boundary to drop at least one packet received from the second network based on a determination that the at least one packet received from the second network comprises a different spoofed source address.

REMARKS

The Office Action dated October 21, 2014 ("Office Action"), has been reviewed and these remarks are responsive thereto. By this paper, claims 1-4, 6, and 8-20 have been amended, claims 5, 7, 21, and 22 have been canceled, and claims 23-100 have been added. No new matter has been added. Upon entry of this amendment, claims 1-4, 6, 8-20, and 23-100 will be pending in this application. Reconsideration and allowance of the instant application are respectfully requested.

Rejections Under 35 U.S.C. §§ 102 & 103

Claims 1, 11, 12, 14, 15, and 18-21 stand rejected under 35 U.S.C. § 102(b) as being anticipated by U.S. Patent Application Publication No. 2005/0138204 to Iyer et al. ("Iyer"). **Claims 2 and 3** stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Iyer in view of U.S. Patent Application Publication No. 2011/0055916 to Ahn ("Ahn"). **Claims 4 and 9** stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Iyer in view of U.S. Patent Application Publication No. 2006/0212572 to Afek et al. ("Afek"). **Claim 5** stands rejected under 35 U.S.C. § 103(a) as being unpatentable over Iyer in view of U.S. Patent Application Publication No. 2010/0296441 to Barkan ("Barkan"). **Claim 6** stands rejected under 35 U.S.C. § 103(a) as being unpatentable over Iyer in view of Barkan and further in view of U.S. Patent Application Publication No. 2008/0072307 to Maes ("Maes"). **Claim 8** stands rejected under 35 U.S.C. § 103(a) as being unpatentable over Iyer in view of U.S. Patent Application Publication No. 2005/0141537 to Kumar et al. ("Kumar"). **Claim 13** stands rejected under 35 U.S.C. § 103(a) as being unpatentable over Iyer in view of U.S. Patent Application Publication No. 2003/0142681 to Chen et al. ("Chen"). **Claim 16** stands rejected under 35 U.S.C. § 103(a) as being unpatentable over Iyer in view of U.S. Patent Application Publication No. 2010/0082811 to Van Der Merwe et al. ("Van Der Merwe"). **Claim 17** stands rejected under 35 U.S.C. § 103(a) as being unpatentable over Iyer in view of U.S. Patent Application Publication No. 2011/0088092 to Nguyen et al. ("Nguyen"). **Claim 22** stands rejected under 35 U.S.C. § 103(a) as being unpatentable over Iyer in view of U.S. Patent Application Publication No. 2003/0035370 to Brustoloni ("Brustoloni").

The rejections of claims 5, 21, and 22 are moot due to their cancelation herein. With respect to claims 1-4, 6, 8, 9, and 11-20 and without acquiescing to the propriety of their rejections, Applicant requests reconsideration in light of the amendments made herein.

As indicated below, Applicant appreciates the indication of allowable subject matter in claims 7 and 10. In accordance with the indication of allowable subject matter, independent claim 1 has been amended to recite the features of original claims 5 and 7, independent claims 19 and 20 have been amended to recite features similar to those recited by amended claim 1, and claim 5 has been canceled. Claims 2-4, 6, 8, 9, and 11-18 depend from independent claim 1 and recite additional features. Accordingly, it is respectfully submitted that claims 1-4, 6, 8, 9, and 11-20 are in condition for allowance.

Allowable Subject Matter

Claims 7 and 10 stand objected to as being dependent upon a rejected base claim; however, the Office Action indicates that they would be allowable if rewritten in independent form, including all of the limitations of their base claim and any intervening claims.

As indicated above, Applicant appreciates the indication of allowable subject matter. In accordance with the indication of allowable subject matter, independent claim 1 has been amended to recite the features of original claims 5 and 7, independent claims 19 and 20 have been amended to recite features similar to those recited by amended claim 1, and claims 5 and 7 have been canceled. Claims 2-4, 6, and 8-18 depend from independent claim 1 and recite additional features. Accordingly, it is respectfully submitted that claims 1-4, 6, and 8-20 are in condition for allowance.

New Claims

Claims 23-100 have been added. Support for claims 23-100 is found in the instant specification. No new matter has been added.

In accordance with the indication of allowable subject matter, independent claim 53 recites the features of original claims 1, 9, and 10, and independent claims 67 and 81 recite features similar to those recited by claim 53. Claims 23-37 depend from independent claim 19 and recite additional features. Claims 38-52 depend from independent claim 20 and recite additional features. Claims 54-66 depend from independent claim 53 and recite additional features. Claims 68-80 depend from independent claim 67 and recite additional features. Claims 82-94 depend from independent claim 81 and recite additional features. Accordingly, it is respectfully submitted that claims 23-94 are in condition for allowance.

Independent claim 95 recites, among other features, "communicating, by the security policy management server and to a packet security gateway located at a second boundary of the network, a second dynamic security policy, the second dynamic security policy comprising one or more rules based on the second boundary that differ from the one or more rules based on the first boundary."

Iyer fails to disclose, teach, or suggest these recited features.

Iyer is directed to "a ***unified*** policy management system" that aggregates, abstracts, and shares "reachability information" between endpoints in a VPN tunnel. *See* Iyer, ¶ [0007] (emphasis added). Nowhere does Iyer disclose, teach, or suggest "communicating, by the security policy management server and to a packet security gateway located at a second boundary of the network, a second dynamic security policy, the second dynamic security policy comprising ***one or more rules based on the second boundary that differ from the one or more rules based on the first boundary***," as recited by claim 95.

Without acquiescing to the propriety of any of the alleged combinations of Iyer and Ahn, Iyer and Afek, Iyer and Barkan, Iyer, Barkan, and Maes, Iyer and Kumar, Iyer and Chen, Iyer and Van Der Merwe, Iyer and Nguyen, or Iyer and Brustoloni, Ahn, Afek, Barkan, Maes, Kumar, Chen, Van Der Merwe, Nguyen, and Brustoloni fail to cure the above-noted deficiencies of Iyer. Accordingly, claim 95 distinguishes over any alleged combination of Iyer, Ahn, Afek, Barkan, Maes, Kumar, Chen, Van Der Merwe, Nguyen, and Brustoloni.

Independent claims 97 and 99, while different in scope, recite features similar to those discussed above with respect to claim 95 and similarly distinguish over any alleged combination of Iyer, Ahn, Afek, Barkan, Maes, Kumar, Chen, Van Der Merwe, Nguyen, and Brustoloni.

Claim 96 depends from independent claim 95 and recites additional features. Claim 98 depends from independent claim 97 and recites additional features. Claim 100 depends from independent claim 99 and recites additional features. Accordingly, each of dependent claims 96, 98, and 100 is allowable over any alleged combination of Iyer, Ahn, Afek, Barkan, Maes, Kumar, Chen, Van Der Merwe, Nguyen, and Brustoloni for the same reasons as its respective base claim and further in view of the various novel and non-obvious features recited therein.

[CONCLUSION AND SIGNATURE FOLLOW ON SEPARATE PAGE]

CONCLUSION

If any fees are required or an overpayment is made, the Commissioner is authorized to debit or credit Deposit Account No. 19-0733, accordingly.

All rejections having been addressed, Applicant respectfully submits that the instant application is in condition for allowance and respectfully solicits prompt notification of the same.

The Examiner is invited to call the undersigned at (202) 824-3270 to resolve any outstanding issues.

Respectfully submitted,

BANNER & WITCOFF, LTD.

Dated: February 19, 2015

By: /William E. Wooten/
William E. Wooten
Registration No. 60,049

Banner & Witcoff, Ltd.
1100 13th Street NW, Suite 1200
Washington, D.C. 20005-4051
Telephone: (202) 824-3000
Facsimile: (202) 824-3001

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re U.S. Patent No. 9,137,205	)	Serial No.: 13/657,010
	)	
Inventors: Steven Rogers, et al.	)	Filed: October 22, 2012
	)	
Issue Date: September 15, 2015	)	Attorney Docket No. 007742.00017

For: **METHODS AND SYSTEMS FOR PROTECTING A SECURED NETWORK**

REQUEST FOR CERTIFICATE OF CORRECTION

U.S. Patent and Trademark Office
Customer Service Window
Randolph Building, Mail Stop: Certificate of Correction Branch
401 Dulany Street
Alexandria, VA 22314

Sir:

Pursuant to 35 U.S.C. § 254 and 37 C.F.R. § 1.322, Applicant requests the issuance of a Certificate of Correction in the above-identified patent. A copy of PTO Form 1050 is appended. The complete Certificate of Correction involves 1 page.

The mistake identified in the appended Form occurred through no fault of the Applicant, as clearly disclosed by the records of the application, which matured into this patent. Enclosed for your convenience is a copy of the Amendment After Non-Final Rejection as filed on 02/19/2015, showing mark-up in original claims 2, 6, and 9 (issued claims 2, 5 and 7, respectively).

Issuance of the Certificate of Correction containing the correction is respectfully requested. Since this change is necessitated through no fault of the Applicant, no fee is believed to be associated with this request. Nonetheless, should the Patent and Trademark Office determine that a fee is required, please charge our Deposit Account No. 19-0733.

Respectfully submitted,

BANNER & WITCOFF, LTD.

Dated: January 11, 2016

By: /Bradley C. Wright/
Bradley C. Wright
Registration No. 38,061

Banner & Witcoff, Ltd.
1100 13th Street, N.W., Suite 1200
Washington, D.C. 20005-4051
(202) 824-3000

UNITED STATES PATENT AND TRADEMARK OFFICE

CERTIFICATE OF CORRECTION

PATENT NO.: **9,137,205**

DATED: September 15, 2015

INVENTORS: Steven Rogers, et al.

It is certified that an error appears in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

In Column 20, Claim 2, Line 56
Please delete “in series the” and replace with --in series, the--.

In Column 21, Claim 5, Line 15
Please delete “comprising;” and replace with --comprising:--.

In Column 21, Claim 7, Line 39
Please delete “specifying” and replace with --specifying a parameter,--.

Mailing Address of Sender:

Banner & Witcoff, Ltd.
1100 13th Street, N.W., Suite 1200
Washington, DC 20005-4051

U.S. PAT. NO

No. of add'l copies
@ $0.50 per page

FORM PTO 1050 (Rev.2-93)

Electronic Acknowledgement Receipt

EFS ID:	24584739
Application Number:	13657010
International Application Number:	
Confirmation Number:	2390
Title of Invention:	METHODS AND SYSTEMS FOR PROTECTING A SECURED NETWORK
First Named Inventor/Applicant Name:	Steven Rogers
Customer Number:	22907
Filer:	Bradley C. Wright/Marcie Burkhart
Filer Authorized By:	Bradley C. Wright
Attorney Docket Number:	007742.00017
Receipt Date:	11-JAN-2016
Filing Date:	22-OCT-2012
Time Stamp:	14:22:36
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Request for Certificate of Correction	CoC_Evidence_17645252.PDF	1588663 a774994e018a4b318bf6d285305f9fc74dd84840	no	34
Warnings:					
Information:					

2	Request for Certificate of Correction	Request_for_Certificate_of_Correction_-_PTO_error_17667937.pdf	27090 cfe539d4dfcb3254b7b1ea758fda9830c2b7b30e	no	2
Warnings:					
Information:					
			Total Files Size (in bytes):	1615753	

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

UNITED STATES PATENT AND TRADEMARK OFFICE

CERTIFICATE OF CORRECTION

PATENT NO. : 9,137,205 B2
APPLICATION NO. : 13/657010
DATED : September 15, 2015
INVENTOR(S) : Steven Rogers et al.

It is certified that error appears in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

In the Claims:

In Column 20, Claim 2, Line 56
Please delete "in series the" and replace with --in series, the--.

In Column 21, Claim 5, Line 15
Please delete "comprising;" and replace with --comprising:--.

In Column 21, Claim 7, Line 39
Please delete "specifying" and replace with --specifying a parameter,--.

Signed and Sealed this
Nineteenth Day of April, 2016

Michelle K. Lee

Michelle K. Lee
Director of the United States Patent and Trademark Office