(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
20 June 2013 (20.06.2013)

W I P O | P C T

(10) International Publication Number
WO 2013/089935 A1

(51) International Patent Classification:
H04L 12/56 (2006.01) *H04L 12/22* (2006.01)
H04L 12/24 (2006.01) *H04L 9/00* (2006.01)

(21) International Application Number:
PCT/US20 12/063249

(22) International Filing Date:
2 November 2012 (02.1 1.2012)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
13/323,816 12 December 201 1 (12. 12.201 1) US

(71) Applicant *(for all designated States except US):* **MCAFEE, INC.** [US/US]; 2821 Mission College Blvd., Santa Clara, CA 95054 (US).

(72) Inventors; and
(71) Applicants *(for US only):* **ALLISON, Tylor** [US/US]; 241 Rutherford Road, Stillwater, MN 55082 (US). **KARLES, Michael, J.** [US/US]; 14991 Williamsburg Ct., Eden Prairie, MN 55347 (US).

(74) Agent: **HUBBARD, William, M.;** Wong, Cabello, Lutsch, Rutherford, & Brucculeri L.L.P., 20333 Tomball Parkway, Suite 600, Houston, TX 77070 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available):* AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available):* ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Declarations under Rule 4.17:

— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.1 7(H))*

— *as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.1 7(in))*

[Continued on next page]

(54) Title: VPN SUPPORT IN A LARGE FIREWALL CLUSTER

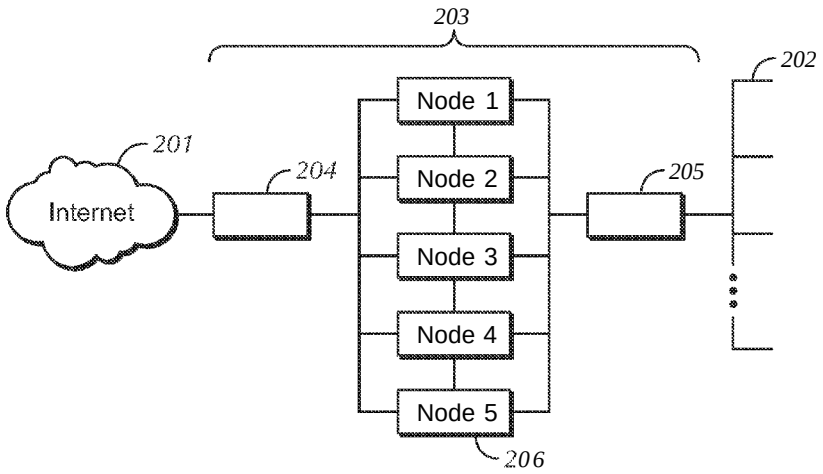

FIG. 2

(57) Abstract: A firewall cluster comprises three or more firewall processing nodes, at least one of which is operable to establish a Virtual Private Network (VPN) network connection. A node is further operable to share VPN state information with two or more receiving nodes by sending broadcast message to the two or more nodes. Shared VPN state information in various embodiments includes encryption keys for a VPN session or security policy information identifying what data should encrypted. Shared VPN state information is used to route VPN connections traffic to a primary node, or to provide for reassignment of VPN processing in the firewall for load balancing or failover.

WO 2013/089935 A1

Published:

— *with international search report (Art. 21(3))*

VPN SUPPORT IN A LARGE FIREWALL CLUSTER

Field of the Invention

The invention relates generally to firewall operation, and more specifically in one embodiment to VPN support in a large firewall cluster.

Limited Copyright Waiver

Background

Computers are valuable tools in large part for their ability to communicate with other computer systems and retrieve information over computer networks. Networks typically comprise an interconnected group of computers, linked by wire, fiber optic, radio, or other data transmission means, to provide the computers with the ability to transfer information from computer to computer. The Internet is perhaps the best-known computer network, and enables millions of people to access millions of other computers such as by viewing web pages, sending e-mail, or by performing other computer-to-computer communication.

But, because the size of the Internet is so large and Internet users are so diverse in their interests, it is not uncommon for malicious users or pranksters to attempt to communicate with other users' computers in a manner that poses a danger to the other users. For example, a hacker may attempt to log in to a corporate computer to steal, delete, or change information. Computer viruses or Trojan horse programs may be distributed to other computers, or unknowingly downloaded or

executed by large numbers of computer users. Further, computer users within an organization such as a corporation may on occasion attempt to perform unauthorized network communications, such as running file sharing programs or transmitting corporate secrets from within the corporation's network to the Internet.

For these and other reasons, many corporations, institutions, and even home users use a network firewall or similar device between their local network and the Internet. The firewall is typically a computerized network device that inspects network traffic that passes through it, permitting passage of desired network traffic based on a set of rules.

Firewalls perform their filtering functions by observing communication packets, such as TCP/IP or other network protocol packets, and examining characteristics such as the source and destination network addresses, what ports are being used, and the state or history of the connection. Some firewalls also examine packets traveling to or from a particular application, or act as a proxy device by processing and forwarding selected network requests between a protected user and external networked computers.

The firewall typically controls the flow of network information by monitoring connections between various ports, sockets, and protocols, such as by examining the network traffic in a firewall. Rules based on socket, port, application, and other information are used to selectively filter or pass data, and to log network activity. Firewall rules are typically configured to identify certain types of network traffic that are to be prohibited or that should have certain other restrictions applied, such as blocking traffic on ports known to be used for file sharing programs while virus scanning any received over a traditional FTP port, blocking certain applications or users from performing some tasks while allowing others to perform such tasks, and blocking traffic based on known attack patterns such as repeated queries to different ports from a common IP address. Firewalls can also be configured to permit certain types of traffic, such as to allow encrypted traffic so that a remote system can communicate with a VPN or Virtual Private Network behind the firewall.

But, the ability of a firewall to manage such connections when distributed across multiple computer systems is limited in that knowledge of a connection is typically stored only in the system handling the connection. Improved firewall distribution in a cluster is therefore desired.

Summary

In one example embodiment, a firewall cluster comprises three or more firewall processing nodes, at least one of which is operable to establish a Virtual Private Network (VPN) network connection. A node is further operable to share VPN state information with two or more receiving nodes by sending broadcast message to the two or more nodes.

Shared VPN state information in various embodiments includes encryption keys for a VPN session or security policy information identifying what data should encrypted. Shared VPN state information is used to route VPN connections traffic to a primary node, or to provide for reassignment of VPN processing in the firewall for load balancing or failover.

Brief Description of the Figures

Figure 1 shows an example network including a firewall, as may be used to practice some embodiments of the invention.

Figure 2 shows an example network including a firewall cluster comprising multiple firewall nodes, consistent with an example embodiment of the invention.

Figure 3 shows an example network including a distributed firewall having VPN support, consistent with an example embodiment of the invention.

Detailed Description

In the following detailed description of example embodiments of the invention, reference is made to specific examples by way of drawings and illustrations. These examples are described in sufficient detail to enable those skilled

in the art to practice the invention, and serve to illustrate how the invention may be applied to various purposes or embodiments. Other embodiments of the invention exist and are within the scope of the invention, and logical, mechanical, electrical, and other changes may be made without departing from the subject or scope of the present invention. Features or limitations of various embodiments of the invention described herein, however essential to the example embodiments in which they are incorporated, do not limit the invention as a whole, and any reference to the invention, its elements, operation, and application do not limit the invention as a whole but serve only to define these example embodiments. The following detailed description does not, therefore, limit the scope of the invention, which is defined only by the appended claims.

Figure 1 illustrates a typical computer network environment, including a public network such as the Internet at 101, a private network 102, and a computer network device operable to provide firewall and intrusion protection functions shown at 103. In this particular example, the computer network device 103 is positioned between the Internet and the private network, and regulates the flow of traffic between the private network and the public network.

The network device 103 is in various embodiments a firewall device, and intrusion protection device, or functions as both. A firewall device or module within the network device provides various network flow control functions, such as inspecting network packets and dropping or rejecting network packets that meet a set of firewall filtering rules. As described previously, firewalls typically perform their filtering functions by observing communication packets, such as TCP/IP or other network protocol packets, and examining characteristics such as the source and destination network addresses, what ports are being used, and the state or history of the connection. Some firewalls also examine packets to determine what application has established the connection, or act as a proxy device by processing and forwarding selected network requests between a protected user and external networked computers. Firewalls often use "signatures" or other characteristics of undesired

traffic to detect and block traffic that is deemed harmful or that is otherwise undesired.

Firewalls typically use sets of rules to filter traffic, such that what happens with any particular element of network data is dependent on how the rule set applies to that particular data. For example a rule blocking all traffic to port 6346 will block incoming traffic bound for that port on a server within the protected network, but will not block other data going to the same server on a different port number. Similarly, a rule blocking traffic originating from a file sharing program such as Shareaza will use patterns in the traffic to block Shareaza traffic on port 6346, but allow other traffic on port 6346.

But, in an environment where a firewall is implemented as a system distributed across multiple computers or nodes, such as in a large or complex system, the ability of multiple nodes to share a connection is limited by each node's information regarding the connection, such as socket information, application information, user information, and the like regarding the connection. Some embodiments of the invention therefore share information, such as Virtual Private Network or VPN connection data, with other nodes in the firewall. Because only one node handles each connection at one time, sharing information between nodes provides the cluster the ability to load balance by moving connection responsibility between nodes, to manage failure of a node in the cluster by moving its connections to another node, and to perform other such functions.

In one such example, a firewall or intrusion protection system is implemented as a cluster or connected group of nodes that share processing traffic flowing through the firewall. Figure 2 shows a network with a distributed firewall, as may be used to practice some embodiments of the invention. Here, a network such as the Internet 201 is coupled to an internal network 202 by a firewall, 203. The firewall 203 comprises an incoming traffic module 204 and an outgoing traffic module 205 that can perform functions such as load balancing and other firewall management

functions. The firewall or intrusion protection rules are applied in firewall nodes 206, which are connected to one another by network connections as shown.

Here the five nodes shown each comprise a separate computer system running an instance of firewall or related software, operable to apply rules to traffic to selectively permit or block traffic flowing between the Internet 201 and the internal network 202. In an alternate embodiment, some nodes such as nodes 1, 2, and 3 execute a firewall application, while other nodes such as 4 and 5 execute an intrusion protection system (IPS) application. The nodes 204 and 205 are responsible for performing functions such as load balancing traffic routed to the firewall nodes 206, ensuring that the nodes are able to work together efficiently to provide higher throughput capability than a single node.

When a computer wishes to communicate with a Virtual Private Network or VPN, it typically uses an encrypted connection to ensure that the communicated data remains private. An example of such a VPN configuration is shown in Figure 3, as may be used to practice some embodiments of the invention. Here, a central office 301 has a corporate computer system, which is connected to the Internet 302 via a firewall 303. The firewall prevents unauthorized access to the home office's computer servers and corporate data, while allowing desired data such as email and web traffic to flow through.

In this example, the home office has also configured a Virtual Private Network or VPN that allows computer systems at regional offices 304 and mobile or home office users at 305 to access the corporate network through the firewall while preserving data security. This is achieved by authenticating the remote user, such as the regional office 304 or remote users, to the home office, and establishing a secure or encrypted connection over which data can be exchanged. Authentication can use passwords, digital certificates, biometrics, secure token codes, or other such mechanisms to ensure that the remote user attempting to connect to the home office is a known and authorized party. Encryption of the established link, such as IPSec, SSL/TLS, or other encryption mechanisms are typically employed to ensure that the

various systems on the Internet 302 through which traffic may pass cannot intercept and read the company's confidential information.

But, because the firewall 303 is configured to control traffic between the home office and external users, it is typically configured to manage or be aware of VPN traffic. For example, the firewall may permit access to a VPN server to which a remote user authenticates, and then permit only certain TCP destination port and IP protocol IDs that match expected VPN traffic. For example, some VPN servers uses TCP destination port 1723 to receive VPN traffic, and IP protocol ID 47 to identify VPN packets, and the firewall is configured to allow this traffic to the VPN server.

Other firewall examples include firewall monitoring of VPN data to ensure that undesirable data is not brought into the home office 301 from remote users, such as a virus being transferred from a home computer to the home office network computers. This involves inspecting incoming decrypted packets in the firewall, and encrypting any outgoing VPN traffic before being sent to a remote location. In such examples, the firewall performs encryption functions such as by using IPSec encryption keys on the data, in coordination with the VPN server. In some examples the firewall includes a VPN server, simplifying interaction between the VPN and firewall. In one such example, the firewall shares the VPN server's encryption keys and can decrypt and inspect traffic flowing through the firewall before forwarding the encrypted traffic to a remote computer. In another firewall example, encrypted communication is passed unfiltered to a specific port on the central office's separate VPN server using technologies such as IPSec, or is handled via proxy in the firewall via technologies such as SSL.

In firewall example such as the distributed firewall of Figure 2, managing a firewall having an integrated VPN can be challenging in that VPN session information will be generated local to a specific node 206 handling the connection. Should the node fail, or should the connection be transferred to another node such as for load balancing, the new node will desirably have connection state information

regarding the connection such as IPSec keys and security policy information indicating what packets should be encrypted.

For these reasons, various embodiments of the invention include VPN state sharing across nodes in a distributed firewall, such as by sending state update information to the other nodes in the firewall. In one such embodiment, the state is sent from the primary node or the node originating the VPN connection to each of the other nodes in the firewall, and an acknowledgment is received in the originating node or in the primary node.

In other embodiments, such a system of send/acknowledge messages is replaced by a multicast or broadcast system of state sharing, in which the state is distributed to each node in the firewall cluster. In a more detailed example, no acknowledgment is sent from the receiving nodes in the firewall cluster, but the primary node distributes all state updates and numbers or otherwise orders the updates, so that if a node misses an update it can be identified and resolved.

For example, if a new IPSec connection is initiated in distributed firewall 206 of Figure 2, the primary node negotiates and establishes the session before the connection is handed off to another node. The primary node further sends state information regarding the connection to each of the other nodes in a broadcast or multicast message, along with a serialized message tag such as a message number.

The receiving nodes then receive the message and compare the message number to the expected next message number to ensure that all messages have been received. For example, a node that has received messages 1, 2, and 3, and then receives message 6, will know that it has missed messages 4 and 5. The receiving node can then request these messages be re-sent from the primary node, and have a high probability that all messages have been received.

In a more detailed example, a window or range such as 32 message numbers is used to number messages in a round-robin fashion, such that the primary node buffers and numbers messages numbered 1-32 before restarting with message 1 again. A receiving node therefore has a window of 32 received messages in which to request

and receive any missing messages before the primary node will overwrite the buffer storing sent messages with a new message, after which the missing message will be resolved by re-sending the entire connection state database.

Such a method of distributing connection state information for distributed connections such as an IPSec VPN connection reduce the number of messages that would need to be sent between nodes from a node-to-node receive/acknowledge state distribution method, especially in environments where IPSec or other VPN session keys are updated several times per hour and many VPN sessions are running on the same firewall.

The state information shared with the distributed firewall nodes also includes IPSec policy updates in some embodiments, so that any secondary node handling IPSec traffic knows that the traffic is to be encrypted as part of an IPSec session before being sent to the external network. In further examples, this IPSec policy update includes an identifier of the node handling the specific IPSec connection, or simply designates that the connection is an IPSec connection and the node knows that all IPSec traffic is handled by a designated node such as the primary node.

In a more complex example a TCP session or other connection can be broken in two, such as where a load balancer on the server or central office side of the firewall reassigns part of a connection using certain protocols for load balancing. For example, a user may initiate a TCP session with distributed firewall node 1, while the FTP connection is handled on the central office side of the firewall by keeping a control session on node 1 but the data session on node 2. Here, node 1 publishes primary connection information to the other nodes in the firewall using a method such as those described above, so the secondary connection to node 2 is recognized and passed back to the external user.

In a more detailed example, the secondary node 2 handling the data connection forwards all traffic it receives in the session back to node 1 so that the FTP proxy on node 1 can manage the connection back to the external user in one example, so that the node handling the primary connection is the single node that

exchanges FTP session data with the external user. This is done so that an FTP proxy managed by node 1 can process both the control and the data sessions in the FTP connection, despite the connection's sessions being split among nodes 1 and 2 on the central office side of the firewall.

These examples illustrate how sharing state information regarding a Virtual Private Network or VPN in a distributed firewall cluster can be used to provide for improved firewall performance, enabling transferring of VPN responsibility between nodes such as for node balancing or failover. It also illustrates how a multicast security policy update with message serialization can be used to reduce the demand placed upon node-to-node connections in the distributed firewall, while ensuring that all nodes have up-to-date copies of the security policy.

Although specific embodiments have been illustrated and described herein, it will be appreciated by those of ordinary skill in the art that any arrangement which is calculated to achieve the same purpose may be substituted for the specific embodiments shown. This application is intended to cover any adaptations or variations of the example embodiments of the invention described herein. It is intended that this invention be limited only by the claims, and the full scope of equivalents thereof.

Claims

1. A method of operating a firewall cluster, comprising:

establishing a Virtual Private Network (VPN) network connection in a firewall cluster having three or more firewall processing nodes; and

sharing VPN state information with two or more receiving nodes by sending broadcast message to the two or more nodes

2. The method of operating a firewall cluster of claim 1, further comprising serializing the broadcast message such that the two or more receiving nodes can identify missing received messages.

3. The method of operating a firewall cluster of claim 1, wherein the VPN state information comprises encryption keys.

4. The method of operating a firewall cluster of claim 1, wherein the VPN state information comprises security policy information identifying what data should encrypted.

5. The method of operating a firewall cluster of claim 1, further comprising using VPN state information to route VPN connections traffic to a primary node.

6. The method of operating a firewall cluster of claim 5, wherein the primary node shares VPN state information with other nodes in the firewall cluster.

7. The method of operating a firewall cluster of claim 1, wherein the distributed firewall uses VPN state information to assign a new node to handle VPN connections to provide load balancing or failover.

8. A distributed firewall cluster, comprising:

three or more firewall processing nodes, at least one of which is operable to establish a Virtual Private Network (VPN) network connection, at least one of which is further operable to share VPN state information with two or more receiving nodes by sending broadcast message to the two or more nodes.

9. The distributed firewall cluster of claim 8, wherein the broadcast message is serialized such that the two or more receiving nodes can identify missing received messages.

10. The distributed firewall cluster of claim 8, wherein the VPN state information comprises encryption keys.

11. The distributed firewall cluster of claim 8, wherein the VPN state information comprises security policy information identifying what data should encrypted.

12. The distributed firewall cluster of claim 8, wherein at least one firewall processing node is further operable to use VPN state information to route VPN connections traffic to a primary node.

13. The distributed firewall cluster of claim 12, the primary node operable to share VPN state information with other nodes in the firewall cluster.

14. The distributed firewall cluster of claim 8, wherein the distributed firewall uses VPN state information to assign a new node to handle VPN connections to provide load balancing or failover.

15. A machine-readable article of manufacture with instructions stored thereon, the instructions when executed operable to cause a computerized system to:

establish a Virtual Private Network (VPN) network connection in a firewall cluster having three or more firewall processing nodes; and

share VPN state information with two or more receiving nodes by sending broadcast message to the two or more nodes

16. The machine-readable article of manufacture of claim 15, the instructions when executed operable to cause a computerized system to serialize the broadcast message such that the two or more receiving nodes can identify missing received messages.

17. The machine-readable article of manufacture of claim 15, wherein the VPN state information comprises at least one of encryption keys or security policy information identifying what data should encrypted.

18. The machine-readable article of manufacture of claim 15, the instructions when executed operable to cause a computerized system to use VPN state information to route VPN connections traffic to a primary node.

19. The machine-readable article of manufacture of claim 18, wherein the primary node shares VPN state information with other nodes in the firewall cluster.

20. The machine-readable article of manufacture of claim 15, wherein the distributed firewall uses VPN state information to assign a new node to handle VPN connections to provide load balancing or failover.

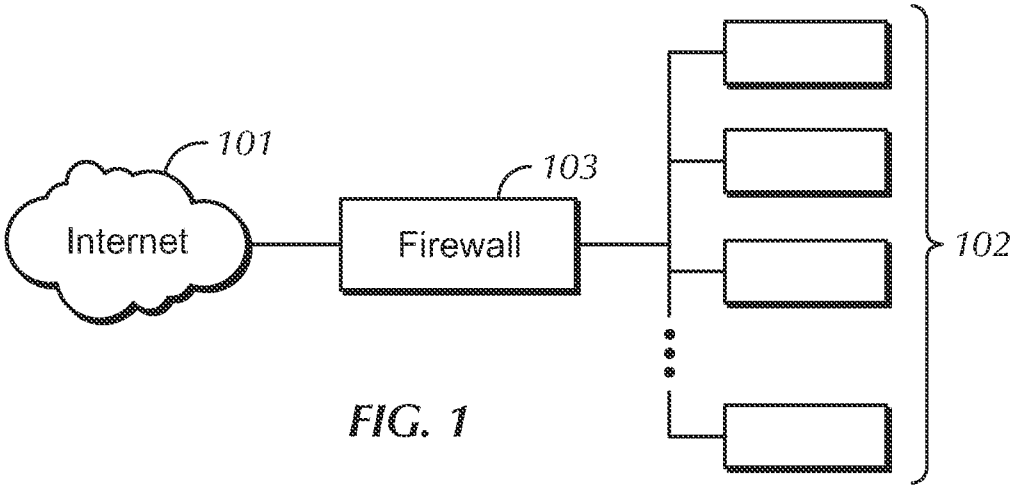
101
Internet
103
Firewall
102

FIG. 1

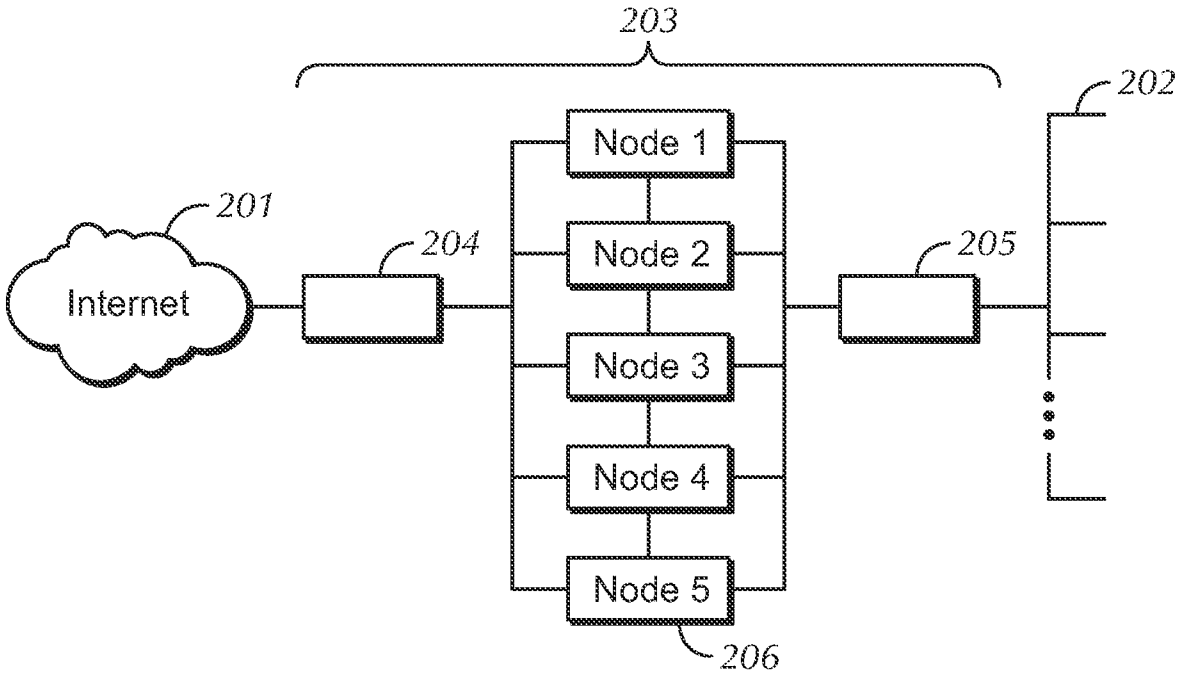
203
202
Node 1
201
204
Node 2
205
Internet
Node 3
Node 4
Node 5
206

FIG. 2

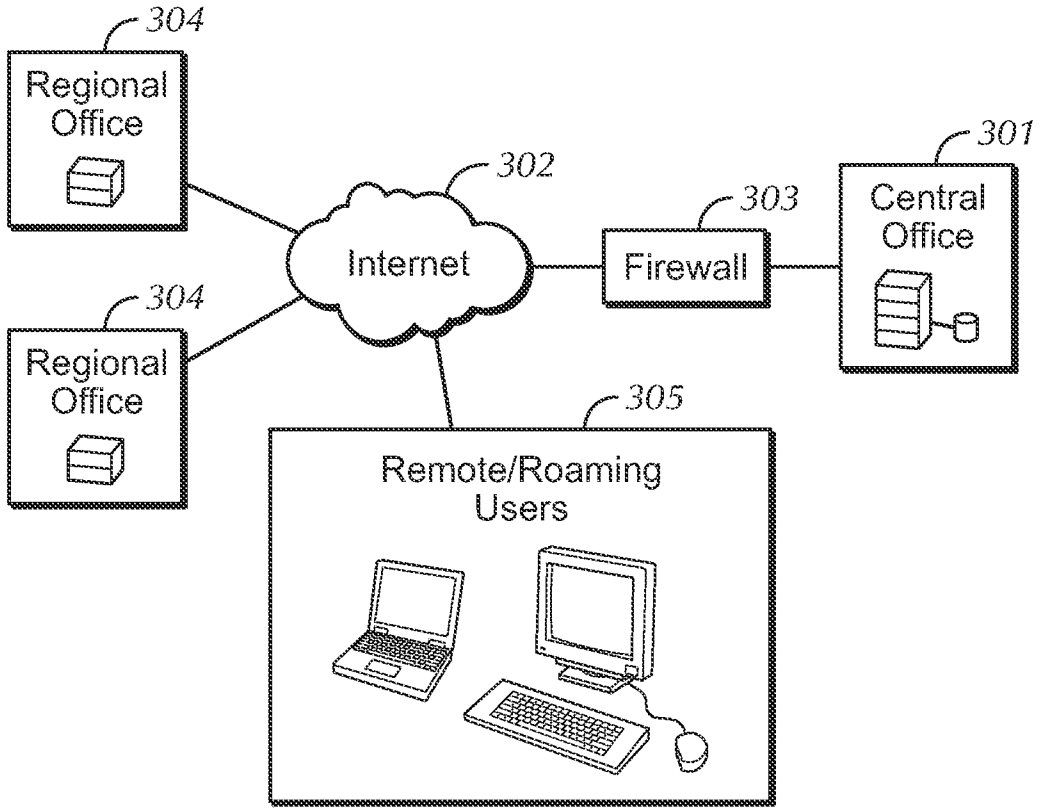
304
Regional Office
302
Internet
303
Firewall
301
Central Office
304
Regional Office
305
Remote/Roaming Users

FIG. 3

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2012/063249

A. CLASSIFICATION OF SUBJECT MATTER

H04L 12/56(2006.01)i, H04L 12/24(2006.01)1, H04L 12/22(2006.01)1, H04L 9/00(2006.01)1

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 12/56; G06F 15/16; H04L 29/00; H04L 9/00

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

Korean utility models and applications for utility models
Japanese utility models and applications for utility models

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

eKOMPASS(KIPO internal) & Keywords: firewall, cluster, VPN, and similar terms.

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 02-15514 A2 (CYBER IQ SYSTEMS) 21 February 2002 See abstract, figure 1 and claims 12,14.	1-20
A	US 6772226 B1 (B0MMAREDDY; SATISH et al.) 03 August 2004 See abstract, figure 1 and column 3 line 66-column 4 line 50.	1-20
A	US 2007-0294754 A1 (AMIT FINKELSTEIN et al.) 20 December 2007 See abstract, figure 1 and paragraphs [0001] ,[0005]-[0008] .	1-20
A	US 2003-0018914 A1 (LEBIN CHENG et al.) 23 January 2003 See abstract, figure 1 and claims 1,8.	1-20
A	US 6880089 B1 (SATISH BOMMAREDDY et al.) 12 April 2005 See abstract and column 2 line 65-column 5 line 48.	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 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
26 DECEMBER 2012 (26. 12.2012)	**27 DECEMBER 2012 (27.12.2012)**

Name and mailing address of the ISA/KR

Korean Intellectual Property Office
189 Cheongsa-ro, Seo-gu, Daejeon Metropolitan City, 302-701, Republic of Korea

Facsimile No. 82-42-472-7140

Authorized officer

HA, Eun Ju

Telephone No. 82-42-481-5707

Form PCT/ISA/210 (second sheet) (My 2009)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.
PCT/US2012/063249

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 02-15514 A2	21.02.2002	AU 2001-84854 A1	25.02,2002
		CA 2419400 A1	21.02,2002
		CA 2419400 C	11.01,2011
		DE 60138915 D1	16.07,2009
		EP 1342344 A2	10.09,2003
		EP 1342344 B1	03.06.2009
		JP 04-361270 B2	21.08,2009
		JP 2004-507169 A	04.03,2004
		JP 2004-507169 T	04.03,2004
		JP 4361270 B2	11.11,2009
		US 6772226 B1	03.08.2004
		WO 02-15514 A3	21.02,2002
US 6772226 B1	03.08.2004	AU 2001-84854 A1	25.02,2002
		CA 2419400 A1	21.02,2002
		CA 2419400 C	11.01.2011
		DE 60138915 D1	16.07,2009
		EP 1342344 A2	10.09,2003
		EP 1342344 B1	03.06.2009
		JP 04-361270 B2	21.08,2009
		JP 2004-507169 A	04.03,2004
		JP 2004-507169 T	04.03,2004
		JP 4361270 B2	11.11,2009
		WO 02-15514 A2	21.02.2002
		wo 02-15514 A3	21.02,2002
US 2007-0294754 A1	20.12.2007	None	
US 2003-0018914 A1	23.01.2003	US 7107609 B2	12.09.2006
US 6880089 B1	12.04.2005	None	