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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
5 August 2010 (05.08.2010)

PCT

(10) International Publication Number
WO 2010/087845 A1

(51) International Patent Classification:
H04W 28/10 (2009.01) *H04B 7/26* (2006.01)
H04W 12/08 (2009.01)

(21) International Application Number:
PCT/US2009/032573

(22) International Filing Date:
30 January 2009 (30.01.2009)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant *(for all designated States except US)*: **HEWLETT-PACKARD DEVELOPMENT COMPANY, L.P.** [US/US]; 20555 S.H. 249, Huston, Texas 77070 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **KRELL, Sherry** [US/US]; Hewlett-Packard Company, 8000 Foothills Blvd., Roseville, California 95747 (US). **BALLESTEROS, Rebecca M.** [US/US]; Hewlett-Packard Company, 8000 Foothills Blvd., Roseville, California 95747 (US). **COWHAM, Adrian** [US/US]; Hewlett-Packard Company, 8000 Foothills Blvd., Roseville, California 95747 (US). **GREEN, John M.** [US/US]; Hewlett-Packard Company, 8000 Foothills Blvd., Roseville, California 95747 (US).

(74) Agents: **LEE, Denise A.** et al.; Hewlett-Packard Company, Intellectual Property Administration, P.O Box 272400, Mail Stop 35, Fort Collins, Colorado 80527-2400 (US).

[Continued on next page]

(54) Title: DYNAMICALLY APPLYING A CONTROL POLICY TO A NETWORK

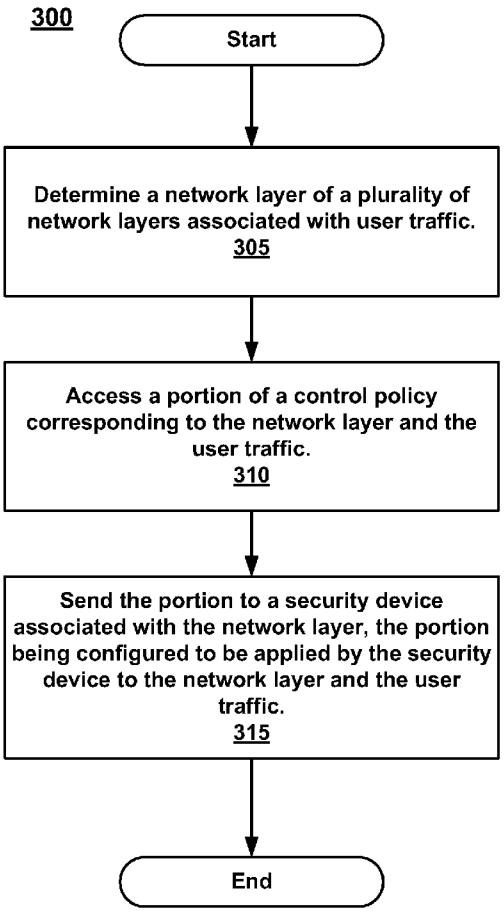

FIG. 3

(57) Abstract: A method [300] of dynamically applying a control policy to a network is described. A network layer of a plurality of network layers associated with user traffic is determined [305]. A portion of a control policy corresponding to the network layer and the user traffic is accessed [310]. Then, the portion is sent to a security device associated with the network layer, the portion being configured to be applied by the security device to the network layer and the user traffic [315].

WO 2010/087845 A1

(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, BR, BW, BY, BZ, CA, CH, 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, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, 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, 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, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, SE, SI, SK, 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 the identity of the inventor (Rule 4.17(i))*

— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))*

Published:

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

DYNAMICALLY APPLYING A CONTROL POLICY TO A NETWORK

FIELD

[0001] The field of the present invention relates to computing systems. More particularly, embodiments of the present invention relate to network security management.

BACKGROUND

[0002] Technological advances have led to the use of increasingly larger and complex networks with an ever increasing number of network systems as an integral part of organizational operations. Many network systems routinely receive, process and/or store data of a sensitive and/or confidential nature. Users are often provided with access to a network via external network access points to retrieve and/or exchange data with network systems within the network. The increased use of such external network access points has in many cases rendered networks increasingly vulnerable to attacks by malicious users.

[0003] Attacks on networks are growing in frequency and sophistication. The sensitive nature of data that is routinely stored in such networks often attracts malicious users or hackers that seek to gain access to the sensitive data and/or confidential data. In some cases, malicious users seek access to networks and network systems with the intention of corrupting the network and/or network systems. Examples of mechanisms that are often used by malicious users to inflict damage on a network include, but are not limited to, viruses, worms, spiders, crawlers and Trojans.

[0004] The increasing frequency of attacks on networks has often lead to an increase on the demands made on network administrators to find methods that are more efficient to protect the network from these attacks.

BRIEF DESCRIPTION OF THE DRAWINGS

[0005] The accompanying drawings, which are incorporated in and form a part of this specification, illustrate embodiments of the present technology for a system for dynamically applying a user access control policy to a network and, together with the description, serve to explain principles discussed below:

[0006] Figure 1 is a block diagram of an example network in which an example system for dynamically applying a control policy to a network may be implemented, in accordance with embodiments of the present technology.

[0007] Figure 2 is a block diagram of an example system for dynamically applying a control policy to a network, in accordance with embodiments of the present technology.

[0008] Figure 3 is a flowchart of an example method for dynamically applying a control policy to a network, in accordance with embodiments of the present technology.

[0009] Figure 4 is a diagram of an example computer system used for dynamically applying a control policy to a network, in accordance with embodiments of the present technology.

[0010] Figure 5 is a flowchart of an example method for dynamically applying a control policy to a network, in accordance with embodiments of the present technology.

[0011] The drawings referred to in this description should not be understood as being drawn to scale unless specifically noted.

DESCRIPTION OF EMBODIMENTS

[0012] Reference will now be made in detail to embodiments of the present technology, examples of which are illustrated in the accompanying drawings. While the present technology will be described in conjunction with various embodiment(s), it will be understood that they are not intended to limit the present technology to these embodiments. On the contrary, the present technology is intended to cover alternatives, modifications and equivalents, which may be included within the spirit and scope of the various embodiments as defined by the appended claims.

[0013] Furthermore, in the following detailed description, numerous specific details are set forth in order to provide a thorough understanding of embodiment of the present technology. However, embodiments of the present technology may be practiced without these specific details. In other instances, well known methods, procedures, components, and circuits have not been described in detail as not to unnecessarily obscure aspects of the present embodiments.

[0014] Unless specifically stated otherwise as apparent from the following discussions, it is appreciated that throughout the present detailed description, discussions utilizing terms such as "determining", "accessing", "sending", "detecting", "continuing", "identifying", "utilizing", or the like, refer to the actions and processes of a computer system, or similar electronic computing device. The computer system or similar electronic computing device manipulates and transforms data represented as physical

(electronic) quantities within the computer system's registers and memories into other data similarly represented as physical quantities within the computer system memories or registers or other such information storage, transmission, or display devices. Embodiments of the present technology are also well suited to the use of other computer systems such as, for example, optical and mechanical computers.

Overview of Discussion

[0015] Embodiments in accordance with the present technology pertain to a system for dynamically applying an identity-based security policy across all layers of a network. As a user's traffic moves across the network, embodiments of the present technology apply a centralized security policy for a user to each layer of the network. For example, a user's switch security policy would be applied as the user's traffic enters a switch. In another example, the user's network firewall security policy would be applied as the user's traffic enters a firewall.

[0016] This method of applying an identity-based security policy allows a network administrator to configure a centrally managed security policy that applies to all layers of a network. The network administrator may easily deploy the appropriate portion of the security policy to all of the corresponding security devices coupled with an associated network layer. Thus, a single security policy for a user may be applied across multiple network layers.

Managing Security in a Network

[0017] Figure 1 is a block diagram representation of an example of a network 100 where one embodiment of a system 132 for dynamically applying a user access control policy may be implemented is shown. The example network 100 generally includes first, second and third network switch systems 102, 104, 106, a network administrator system 108, a network management system 110, first, second and third server systems 112, 114, 116, and first, second, third and fourth threat assessment systems 118, 120, 122, 124. An external system 128, such as a laptop, is communicatively coupled with network 100.

[0018] First, second and third network switch systems 102, 104, 106 are communicatively coupled with each other and generally communicatively coupled with network 100. Each of first, second and third network switch systems 102, 104, 106, respectively, includes a plurality of data ports 1, 2, 3, 4, 5, 6. Communicative coupling is established between first network switch system 102 and second network switch system 104 via a communication channel between data port 6 of first network switch system 102 and data port 2 of second network switch system 104. Communicative coupling is established between second network switch system 104 and third network switch system 106 via a communication channel between data port 1 of second network switch system 104 and data port 6 of third network switch system 106.

[0019] In one embodiment, one or more network switch systems 102, 104, 106 includes one or more edge interconnect data ports. Data port 1 of first network switch

system 102 is communicatively coupled with external system 128 and is an example of an edge interconnect data port. In one embodiment, one or more network switch systems are configured as edge interconnect network switch systems where the data ports 1, 2, 3, 4, 5, 6 are all configured as edge interconnect data ports.

[0020] In one embodiment, one or more network switch systems 102, 104, 106 includes an embedded threat assessment system in the form of a switch based trap system. The switch based trap system is configured to detect one or more selected data anomalies and raises a data anomaly event upon detection of the one of the selected data anomalies. In one embodiment, the switch based trap system issues an anomaly notification to network management system 110 upon detection of one of the selected data anomalies. In one embodiment, the switch based trap system issues an anomaly notification to network administrator system 108 upon detection of one of the selected data anomalies. In one embodiment, the switch based trap system is a virus throttling (VT) system.

[0021] In one embodiment, one or more data ports, 1, 2, 3, 4, 5, 6 of one or more of network switch systems 102, 104, 106 are configured as mirror source ports. In one embodiment, one or more data ports 1, 2, 3, 4, 5, 6 of one or more network switch systems 102, 104, 106 are configured as mirror destination ports. In one embodiment, one or more data ports 1, 2, 3, 4, 5, 6 of one or more network switch systems 102, 104, 106 are configured as local mirror source ports. In one embodiment, one or more data ports 1, 2, 3, 4, 5, 6 of one or more network switch systems 102, 104, 106 are configured

as local mirror destination ports. In one embodiment, one or more data ports 1, 2, 3, 4, 5, 6 of one or more network switch systems 102, 104, 106 are configured as remote mirror source ports. In one embodiment, one or more data ports 1, 2, 3, 4, 5, 6 of one or more network switch systems 102, 104, 106 are configured as remote mirror destination ports.

[0022] While network switch systems having six data ports have been described, network switch systems used in a network may have a fewer or a greater number of data ports. For example, many network switch systems have well over 100 data ports. Also, while a number of different types of network switch systems having the described configurations and/or features have been described, the network switch systems may be configured using alternative network switch system configurations and/or features. Furthermore, while a network has been described as having three network switch systems, a fewer or greater number of network switch systems may be used.

[0023] Threat assessment systems 118, 120, 122, 124 generally monitor network data to identify data anomalies that may pose a security threat to network 100 and evaluate any identified data anomalies. In one embodiment, threat assessment system 118, 120, 122, 124 implements mitigation actions in response to the detection of a data anomaly that may pose a potential security threat to network 100. There are a number of different types of threat assessment systems 118, 120, 122, 124 available for use in network 100. Examples of such threat assessment systems 118, 120, 122, 124, include but are not limited to, intrusion detection systems (IDS), intrusion prevention systems (IPS), unified threat management (UTM) systems and firewall systems (FW). In an example network

100, first and third threat assessment systems 118 and 122, respectively, are intrusion detection systems (IDS), second threat assessment system 120 is an intrusion prevention system (IPS), and fourth threat assessment system 124 is a unified threat management (UTM) system.

[0024] First and second threat assessment systems 118 and 120, respectively, are communicatively coupled with network 100 via first network switch system 102 and third and fourth threat assessment systems 122 and 124, respectively, are communicatively coupled to network 100 via second and third network switch systems 104 and 106, respectively. More specifically, first threat assessment system 118 is communicatively coupled with network 100 via a communication channel between first threat assessment system 118 and data port 2 of first network switch system 102. Second threat assessment system 120 is communicatively coupled with network 100 via a communication channel between second threat assessment system 120 and data port 5 of first network switch system 102. Third threat assessment system 122 is communicatively coupled with network 100 via a communication channel between third threat assessment system 122 and data port 6 of second network switch system 104. Fourth threat assessment system 124 is communicatively coupled with network 100 via a communication channel between fourth threat assessment system 124 and data port 5 of third network switch system 106.

[0025] In one embodiment, one or more threat assessment systems 118, 120, 122, 124 issues an anomaly event notification to network administrator system 108 upon the detection of selected data anomalies. In one embodiment, one or more threat assessment

systems 118, 120, 122, 124 issues an evaluation notification to network administrator system 108 upon completion of an evaluation of a detected data anomaly. In one embodiment, one or more threat assessment systems 118, 120, 122, 124 issues an anomaly event notification to network management system 110 upon the detection of a data anomaly. In one embodiment, one or more threat assessment systems 118, 120, 122, 124 issues an evaluation notification to network management system 110 upon completion of an evaluation of a detected data anomaly.

[0026] While a number of different types of threat assessment systems have been described, other types of threat assessment systems may be used. Also, while a network has been described as having four threat assessment systems, a fewer or greater number of threat assessment systems may be used. Furthermore, while a particular network configuration has been described for the threat assessment systems, alternative network configurations may be employed.

[0027] In one embodiment, upon the detection of selected data anomalies by network management system 110, network management system 110 issues a data anomaly assessment request to a selected threat assessment system 118, 120, 122, 124 to provide an assessment of the detected data anomaly. In one embodiment, upon the detection of selected data anomalies by network management system 110, network management system 110 issues a data mirroring command to a selected network system to mirror network data associated with the detected data anomaly to a selected threat assessment system 118, 120, 122, 124. In one embodiment, upon the detection of selected data

anomalies by network management system 110, network management system 110 identifies the threat type posed by the detected network data anomaly, identifies a threat assessment system 118, 120, 122, 124 that specializes in the evaluation of an identified threat type and issues a data mirroring command to a selected network system to mirror network data associated with the data anomaly to the identified threat assessment system 118, 120, 122, 124.

[0028] Network management system 110 generally manages network operations including network security operations. In one embodiment, network management system 110 includes a network immunity management system where the network immunity management system generally manages network security operations. In one embodiment, network management system 110 is a network immunity management (NIM) system type of network management system that generally manages network security operations. Additional types of network management systems are used to manage other types of network operations. In one embodiment, network management system 110 includes an embedded threat assessment system. In one embodiment, the embedded threat assessment system is a network behavior anomaly detection (NBAD) system. Network management system 110 is communicatively coupled with network 100 via second network switch 104. More specifically, network management system 110 is communicatively coupled with network 100 via a communication channel between network management system 110 and data port 5 of second network switch system 104. Network management system 110 will be described in greater detail with reference to FIG. 2 below.

[0029] Network administrator 130 generally manages network operations including network security operations via network administrator system 108. Network administrator system 108 is communicatively coupled with network 100 via third network switch 106. More specifically, network administrator system 108 is communicatively coupled with network 100 via a communication channel between network administrator system 108 and data port 1 of third network switch system 106.

[0030] In one embodiment, network administrator 130 is provided with the option of manually defining and/or amending security policies via network administrator system 108. In one embodiment, anomaly notifications are received at network administrator system 108. In one embodiment, network administrator 130 is provided with the option of selectively manually enforcing selected security polices via network administrator system 108. In one embodiment, network administrator 130 is provided with the option of selectively manually implementing one or more mitigation responses to selected data anomalies via network administrator system 108. In one embodiment, network administrator 130 is provided with the option of configuring selected network systems via network administrator system 108.

[0031] In one embodiment, network administrator 130 is provided with the option of configuring individual network switch systems 102, 104, 106 via network administrator system 108. In one embodiment, network administrator 130 is provided with the option of configuring individual data ports 1, 2, 3, 4, 5, 6 of individual network switch systems 102, 104, 106 via network administrator system 108. In one embodiment, network

administrator 130 is provided with the option of configuring individual data ports 1, 2, 3, 4, 5, 6 as mirror source data ports and as mirror destination data ports via network administrator system 108. In one embodiment, network administrator 130 is provided with the option of configuring individual data ports 1, 2, 3, 4, 5, 6 as local mirror source data ports and as local mirror destination data ports via network administrator system 108. In one embodiment, network administrator 130 is provided with the option of configuring individual data ports 1, 2, 3, 4, 5, 6, as remote mirror source data ports and as remote mirror destination data ports via network administrator system 108. While a number of different network administrations functions that may be performed by network administrator 130 via network administrator system 108 have been described, other network administrations functions may also be performed by network administrator 130 via network administrator system 108.

[0032] First server system 112 is communicatively coupled with network 100 via third network switch 106 and second and third server systems 114 and 116, respectively, are communicatively coupled with network 100 via second network switch 104. More specifically, first server system 112 is communicatively coupled with network 100 via a communication channel between first server system 112 and data port 3 of third network switch system 106. Second server system 114 is communicatively coupled with network 100 via a communication channel between second server system 114 and data port 3 of second network switch system 104. Third server system 116 is communicatively coupled with network 100 via a communication channel between third server system 116 and data port 4 of second network switch system 104. In the example network 100, first server

system 112 handles data requiring a relatively low level of network security while second and third server systems 114 and 116, respectively, handle relatively sensitive financial data and require a relatively higher level of network security. While one network configuration including specific types of server systems configured within the network in a particular manner have been described, other types of server systems may be used in a network. Also, while one network configuration of server systems has been described alternative network configurations may be used. Furthermore, while three servers have been described as a part of the network, a fewer or greater number of servers may be used.

[0033] A user 126 has used external system 128, such as a laptop, to establish communicative coupling with network 100. External system 128 has established communicative coupling with network 100 via a communication channel established between external system 128 and data port 1 of first network switch system 102. Data port 1 is an edge interconnect data port. A user as used in the description includes human users as well as automated agents. One example of such an automated agent is a bot.

[0034] In one embodiment, communication channels established between network systems within network 100 are wireless communication channels. In one embodiment, communication channels established between network systems within network 100 are wired communication channels. In one embodiment, communication channels established between network systems within network 100 are a combination of wireless communication channels and wired communication channels.

[0035] In one embodiment, communication channels established between external system 128 and network 100 are via wireless communication channels. In one embodiment, communication channels established between external system 128 and network 100 are via wired communication channels. In one embodiment, communication channels established between external system 128 and network 100 are via a combination of wireless communication channels and wired communication channels.

[0036] While one particular configuration of network 100 where one embodiment of managing security in network 100 may be implemented has been described, embodiments of managing security in a network may be implemented in networks having alternative configurations. Furthermore, embodiments of managing security in a network may be implemented in networks including a fewer or greater number of types of network systems and including a fewer or greater number of the described network systems.

Example Architecture of a System for Dynamically Applying a User Access Control Policy to a Network

[0037] Figure 2 is a block diagram of an example system 132 for dynamically applying a user access control policy to network 100, in accordance with embodiments of the present technology. System 132 is coupled with, wired and/or wirelessly, network 100. System 132 includes network layer locator 205, control policy accessor 240, control policy sender 250, and data store 230. Embodiments of the present technology may further include user traffic detector 260 and user identifier 265.

[0038] In one embodiment, network layers 210a, 210b, 210c, and 210n… (210a-210n…) comprise a plurality of network layers 215 within network 100. One network layer may be a firewall layer, while another network layer may be a layer upon which a user 270 logs in. In another embodiment, a network layer may represent network switches 102, 104, 106. Each network layer accommodates user traffic. User traffic refers to one or more actions user 270 performs on one of the plurality of network layers 215.

[0039] In one embodiment, data store 230 is internal to system 132. In another embodiment, data store 230 may be coupled with, wired or wirelessly, and external to system 132. Data store 230 is configured for storing a control policy 235 that may be divided into portions 245a, 245b, 245c, and 245n… (245a-245n…). Each network layer of plurality of network layers 215 has a specific portion related thereto. Additionally, it is appreciated that there may be more or less portions than the number of network layers within network 100. In one embodiment, data store 230 is configured for storing a plurality of control policies, including control policy 235.

[0040] In one embodiment, control policy 235 comprises at least one access restriction instruction associated with user 270 and user traffic 225b and the network layer 210b upon which user traffic 225b is operating. While only one access restriction instruction is described herein, it is understood that control policy 235 may contain more than one access restriction instruction. An access restriction instruction may include a description

regarding instructions limiting a user's access to a certain network layer within a network.

[0041] In one embodiment, an access restriction instruction may be a network location restriction for user 270. For example, the access restriction instruction may indicate that user 270 is only permitted access to a portion of network layer 210b, such as ports 5 and 6 of the ports 1, 2, 3, 4, 5, and 6. In another embodiment, an access restriction instruction may be a network bandwidth restriction. For example, the access restriction instruction may indicate that user 270 is only permitted to use a pre-specified amount of bandwidth on network layer 210b. In one embodiment, an access restriction instruction may be a duration restriction for user 270. For example, the access restriction instruction may indicate that user 270 is only permitted access to network layer 210b via port 1 for two minutes at a time.

[0042] In one embodiment, each network layer 210a-210n… has a security device 255a coupled therewith. In one embodiment, one or more of the security devices 255a, 255b, 255c, and 255n… is an access control device. The access control device functions to enforce a pre-defined level for a user's network layer.

[0043] As will be described herein, embodiments of the present technology provide for the administration of an identity-based control policy across multiple layers of a network. Using well-known networking authentication/authorization protocol, system 132 sends control policy information to security devices to enforce a pre-defined access level for a

user on the network. System 132 intelligently determines what portion of the control policy, depending on the network layer at which a user is operating, should be given to the security device. Additionally, system 132 allows updates of control policies to be dynamically applied as the user moves around the network.

Example Operation of Network Security System

[0044] More generally, in embodiments in accordance with the present technology, system 132 is utilized to dynamically share a single control policy across multiple network layers. This allows a network administrator to configure a centrally managed control policy that applies to all layers of a network. Additionally, the network administrator may easily deploy the appropriate portion of the control policy to each of the corresponding security devices on the network.

[0045] Referring to Figure 2, in one embodiment, user traffic detector 260 detects user traffic. For example, user traffic detector 260 may detect user traffic 225b and user traffic 225n… Referring still to Figure 2, in one embodiment, network layer locator 205 determines a network layer of a plurality of network layers associated with user traffic. For example, network layer locater 205 may determine that user traffic 225b is occurring at switch 204. Switch 204 comprises network layer 210b. Therefore, network layer locator 205 determines that network layer 210b is associated with user traffic 225b.

[0046] In one embodiment, determining a network layer associated with user traffic is performed while the user traffic is entering network layer. However, in another

embodiment, determining a network layer associated with user traffic is performed after the user traffic has entered the network layer.

[0047] In one embodiment, determining a network layer associated with user traffic comprises identifying a user creating the user traffic. For example, user 270 may be responsible for user traffic 225b. Part of determining the network layer associated with user traffic 225 includes identifying that user 270 is responsible for user traffic 225b. In one embodiment, identifying user 270 may include mapping user 270 to an associated network address via technology known in the field.

[0048] Referring to Figure 2, in one embodiment, once the network layer upon which user traffic is operating is determined, then control policy accessor 240 accesses a portion of the control policy corresponding to network layer 210b and user traffic 225b. For example, a portion of a control policy corresponds to a network layer and user traffic when that portion's access restriction instruction thereon refers to network layer 210b and user traffic 225b.

[0049] Referring still to Figure 2, in one embodiment, control policy sender 250 sends the accessed portion 245b to a security device associated with network layer 210b. For example, in Figure 2, security device 255b is coupled with network layer 210b. Portion 245b is configured to be applied to network layer 210b and user traffic 225b security device 255b. Thus, security device 255b may then apply portion 245b of control policy 235 to network layer 210b and user traffic 225b.

[0050] In one embodiment, system 132 provides that portion 245b is automatically sent to security device 255b. In another embodiment, system 132 provides that portion 245b is sent to security device 255b in response to instructions from an administrator of network 100, such as administrator 130.

[0051] In one embodiment, the network layer locator 205, control policy accessor 240, and control policy sender 250 function continuously while user traffic is still be detected. For example, while user traffic 225b is still being detected by user traffic detector 260, then network layer locator 205 continues to determine network layer 210b associated with user traffic 225b, control policy accessor 240 continues to access portion 245b corresponding to network layer 210b and user traffic 225b, and control policy sender 250 continues to send portion 245b to security device 255b. Finally, security device 255b continues to apply portion 245b to network layer 210b and user traffic 225b.

[0052] Referring now to 300 of Figure 3, a flowchart of an example computer-implemented method for dynamically applying a control policy to a network, in accordance with embodiments of the present technology is shown.

[0053] Referring to 305 of Figure 3 and as described herein, in one embodiment of the present technology, network layer 210b, of plurality of network layers 215, that is associated with user traffic 225b is determined. Referring now to 310 of Figure 3 and as

described herein, in one embodiment portion 245b of control policy 235 corresponding to network layer 210b and user traffic 225 is accessed.

[0054] Referring to 315 of Figure 3 and as described herein, in one embodiment, portion 245b is sent to security device 255b associated with network layer 210b. Portion 245b is configured to be applied by security device 255b to network layer 210b and user traffic 225b.

Example Computer System Environment

[0055] Figure 4 illustrates an example computer system 400 used in accordance with embodiments of the present technology. It is appreciated that system 400 of Figure 4 is an example only and that embodiments of the present technology can operate on or within a number of different computer systems including general purpose networked computer systems, embedded computer systems, routers, switches, server devices, user devices, various intermediate devices/artifacts, stand alone computer systems, and the like. As shown in Figure 4, computer system 400 of Figure 4 is well adapted to having peripheral computer readable media 402 such as, for example, a compact disc, and the like coupled therewith.

[0056] System 400 of Figure 4 includes an address/data bus 404 for communicating information, and a processor 406A coupled to bus 404 for processing information and instructions. As depicted in Figure 4, system 400 is also well suited to a multi-processor environment in which a plurality of processors 406A, 406B, and 406C are present.

Conversely, system 400 is also well suited to having a single processor such as, for example, processor 406A. Processors 406A, 406B, and 406C may be any of various types of microprocessors. System 400 also includes data storage features such as a computer usable volatile memory 408, e.g. random access memory (RAM), coupled to bus 404 for storing information and instructions for processors 406A, 406B, and 406C.

[0057] System 400 also includes computer usable non-volatile memory 410, e.g. read only memory (ROM), coupled to bus 404 for storing static information and instructions for processors 406A, 406B, and 406C. Also present in system 400 is a data storage unit 412 (e.g., a magnetic or optical disk and disk drive) coupled to bus 404 for storing information and instructions. System 400 also includes an optional alpha-numeric input device 614 including alphanumeric and function keys coupled to bus 404 for communicating information and command selections to processor 406A or processors 406A, 406B, and 406C. System 400 also includes an optional cursor control device 416 coupled to bus 404 for communicating user input information and command selections to processor 406A or processors 406A, 406B, and 406C. System 400 also includes an optional display device 418 coupled to bus 404 for displaying information.

[0058] Referring still to Figure 4, optional display device 418 of Figure 4 may be a liquid crystal device, cathode ray tube, plasma display device or other display device suitable for creating graphic images and alpha-numeric characters recognizable to a user. Optional cursor control device 416 allows the computer user to dynamically signal the movement of a visible symbol (cursor) on a display screen of display device 418. Many

implementations of cursor control device 416 are known in the art including a trackball, mouse, touch pad, joystick or special keys on alpha-numeric input device 414 capable of signaling movement of a given direction or manner of displacement. Alternatively, it will be appreciated that a cursor can be directed and/or activated via input from alpha-numeric input device 414 using special keys and key sequence commands.

[0059] System 400 is also well suited to having a cursor directed by other means such as, for example, voice commands. System 400 also includes an I/O device 420 for coupling system 400 with external entities.

[0060] Referring still to Figure 4, various other components are depicted for system 400. Specifically, when present, an operating system 422, applications 424, modules 426, and data 428 are shown as typically residing in one or some combination of computer usable volatile memory 408, e.g. random access memory (RAM), and data storage unit 412. However, it is appreciated that in some embodiments, operating system 422 may be stored in other locations such as on a network or on a flash drive; and that further, operating system 422 may be accessed from a remote location via, for example, a coupling to the internet. In one embodiment, the present invention, for example, is stored as an application 424 or module 426 in memory locations within RAM 408 and memory areas within data storage unit 412.

[0061] Computing system 400 is only one example of a suitable computing environment and is not intended to suggest any limitation as to the scope of use or

functionality of embodiments of the present technology. Neither should the computing environment 400 be interpreted as having any dependency or requirement relating to any one or combination of components illustrated in the example computing system 400.

[0062] Embodiments of the present technology may be described in the general context of computer-executable instructions, such as program modules, being executed by a computer. Generally, program modules include routines, programs, objects, components, data structures, etc., that perform particular tasks or implement particular abstract data types. Embodiments of the present technology may also be practiced in distributed computing environments where tasks are performed by remote processing devices that are linked through a communications network. In a distributed computing environment, program modules may be located in both local and remote computer-storage media including memory-storage devices.

[0063] Figure 5 is a flowchart of an example method for dynamically applying a control policy to a network, in accordance with embodiments of the present technology. In one embodiment, process 500 is carried out by processors and electrical components under the control of computer readable and computer executable instructions. The computer readable and computer executable instructions reside, for example, in data storage features such as computer usable volatile and non-volatile memory. However, the computer readable and computer executable instructions may reside in any type of computer readable medium. In one embodiment, process 500 is performed by system 132 of Figure 2.

[0064] Referring to 505 of Figure 5, in one embodiment, user traffic 225b on network 100 is detected. Referring to 510 of Figure 5, in one embodiment, network layer 210b of plurality of network layers 215 upon which user traffic 225b is operating is determined. In one embodiment, determining comprises identifying user 270 associated with user traffic 225b.

[0065] Referring to 515 of Figure 5, in one embodiment, portion 245b of control policy 235 corresponding to network layer 210b and user traffic 225b is accessed. Referring to 520 of Figure 5, in one embodiment, portion 245b is sent to a control device associated with network layer 210b. Portion 245b is configured to be applied by the control device to network layer 210b and user traffic 225b.

[0066] Thus, embodiments of the present technology enable the administration of an identity-based control policy across multiple layers of a network. Control policies may be dynamically applied as a user moves around the network. Additionally, this centralized control policy may be applied to the user at the network level, regardless of where or how the user connects to the network.

[0067] Although the subject matter has been described in a language specific to structural features and/or methodological acts, it is to be understood that the subject matter defined in the appended claims is not necessarily limited to the specific features or

acts described above. Rather, the specific features and acts described above are disclosed as example forms of implementing the claims.

CLAIMS

What is claimed is:

1. A computer implemented method [300] of dynamically applying a control policy to a network, said method [300] comprising:

determining [305] a network layer of a plurality of network layers associated with user traffic;

accessing [310] a portion of a control policy corresponding to said network layer and said user traffic; and

sending [315] said portion to a security device associated with said network layer, said portion being configured to be applied by said security device to said network layer and said user traffic.

2. The method [300] of Claim 1, further comprising:

detecting said user traffic.

3. The method [300] of Claim 2, further comprising:

continuing said determining, said accessing, and said sending while said user traffic is being detected.

4. The method [300] of Claim 1, further comprising:

determining a network layer of a plurality of network layers associated with user traffic as said user traffic enters said network layer.

5. The method [300] of Claim 1, further comprising:

determining a network layer of a plurality of network layers associated with user traffic after said user traffic enters said network layer.

6. The method [300] of Claim 1, further comprising:

automatically sending said portion to a security device associated with said network layer, said portion being configured to be applied by said security device to said user traffic and said network layer.

7. The method [300] of Claim 1, further comprising:

in response to instructions from an administrator of said network, sending said portion of said network to a security device associated with said network layer, said portion being configured to be applied by said security device to said user traffic and said network layer.

8. The method [300] of Claim 1, wherein said determining comprises:

identifying a user associated with said user traffic.

9. The method [300] of Claim 1, further comprising:

utilizing an access control device as said security device.

10. A system [132] for dynamically applying a control policy to a network [100], said system [132] comprising:

a network layer locator [205] configured for determining a network layer of a plurality of network layers associated with user traffic;

a data store [230] configured for storing a control policy;

a control policy accessor [240] configured for accessing a portion of said control policy corresponding to said network layer and said user traffic; and

a control policy sender [250] configured for sending said portion to a security device associated with said network layer, said portion being configured to be applied by said security device to said network layer and said user traffic.

11. The system [132] of Claim 10, further comprising:

a user traffic detector [260] configured for detecting user traffic on a network [100].

12. The system [132] of Claim 10, wherein said data store [230] is configured for storing a plurality of control policies.

13. The system [132] of Claim 10, further comprising:

a user identifier [265] configured for identifying a user associated with said user traffic.

14. The system [132] of Claim 10, wherein said security device is an access control device.

15. A computer usable storage medium comprising instructions that when executed cause a computer system to perform a method [500] of dynamically applying a control policy to a network, said method comprising:

detecting [505] user traffic on a network;

determining [510] a network layer of a plurality of network layers upon which said user traffic is operating;

accessing [515] a portion of a control policy corresponding to said network layer and said user traffic; and

sending [520] said portion to a control device associated with said network layer, said portion being configured to be applied by said access control device to said network layer and said user traffic.

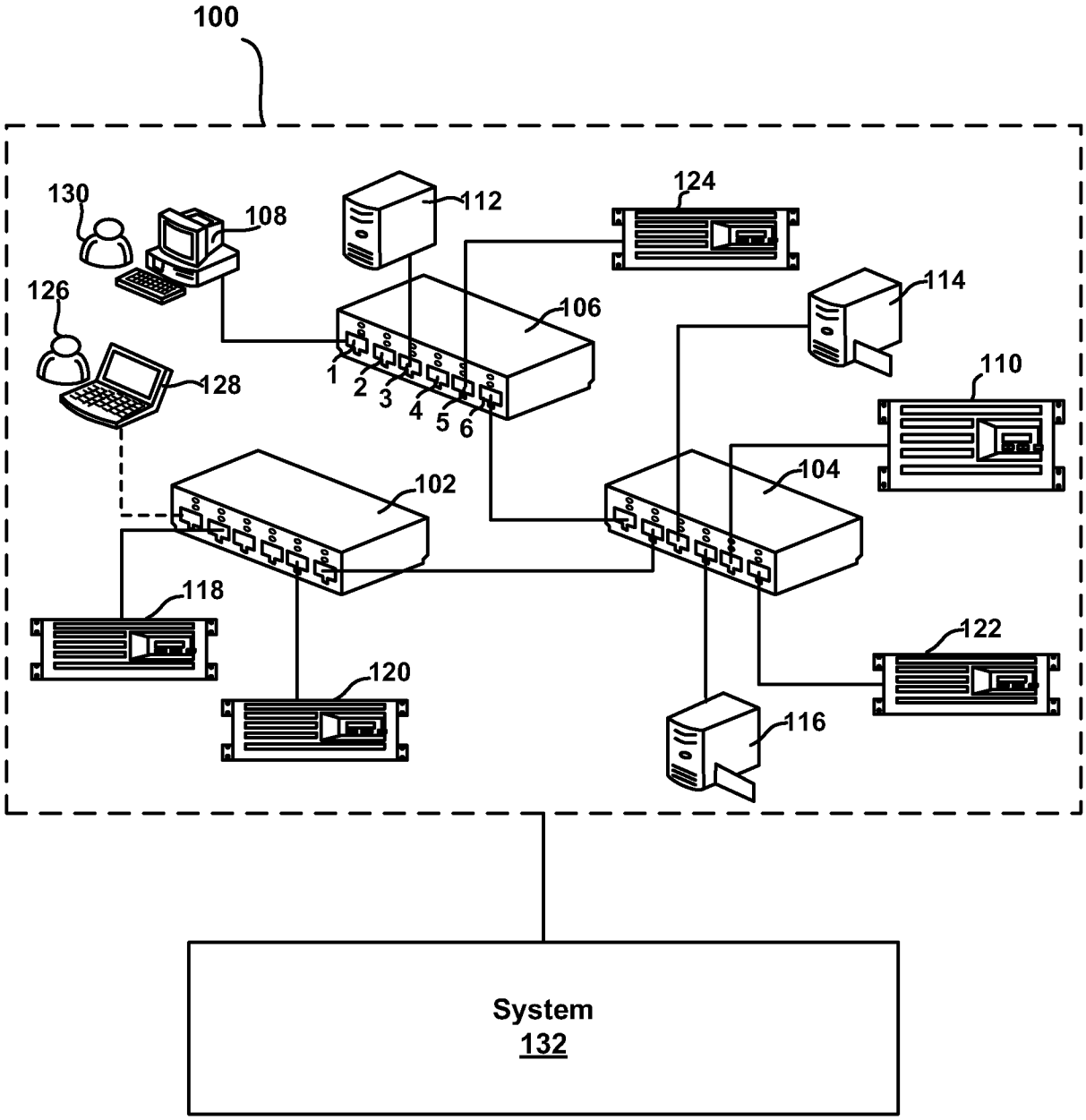
100
130
108
112
124
126
106
114
128
1
2
3
4
5
6
110
102
104
118
122
120
116
System
132

FIG. 1

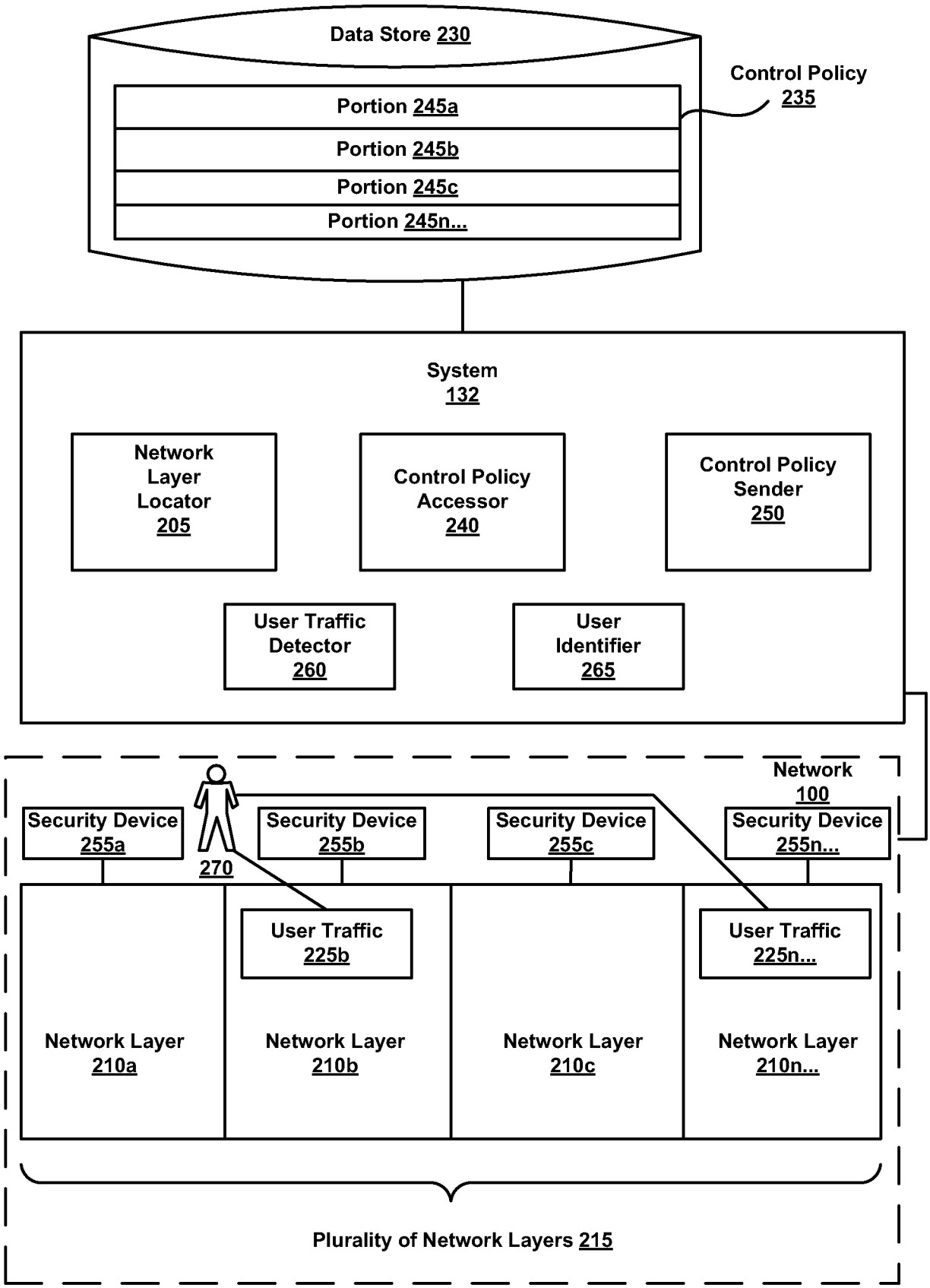
Data Store 230
Portion 245a
Portion 245b
Portion 245c
Portion 245n...
Control Policy 235
System 132
Network Layer Locator 205
Control Policy Accessor 240
Control Policy Sender 250
User Traffic Detector 260
User Identifier 265
Network 100
Security Device 255a
Security Device 255b
Security Device 255c
Security Device 255n...
270
User Traffic 225b
User Traffic 225n...
Network Layer 210a
Network Layer 210b
Network Layer 210c
Network Layer 210n...
Plurality of Network Layers 215

FIG. 2

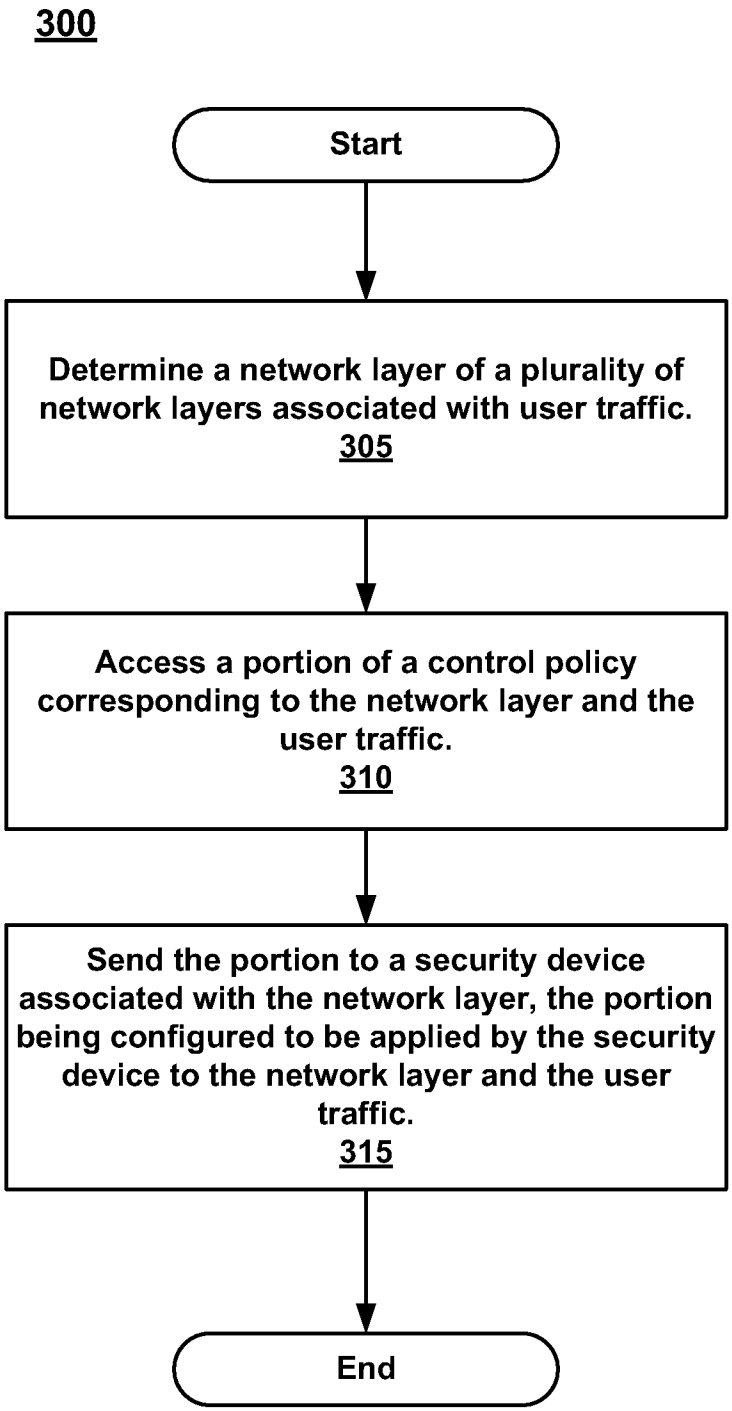
300
Start
Determine a network layer of a plurality of network layers associated with user traffic.
305
Access a portion of a control policy corresponding to the network layer and the user traffic.
310
Send the portion to a security device associated with the network layer, the portion being configured to be applied by the security device to the network layer and the user traffic.
315
End

FIG. 3

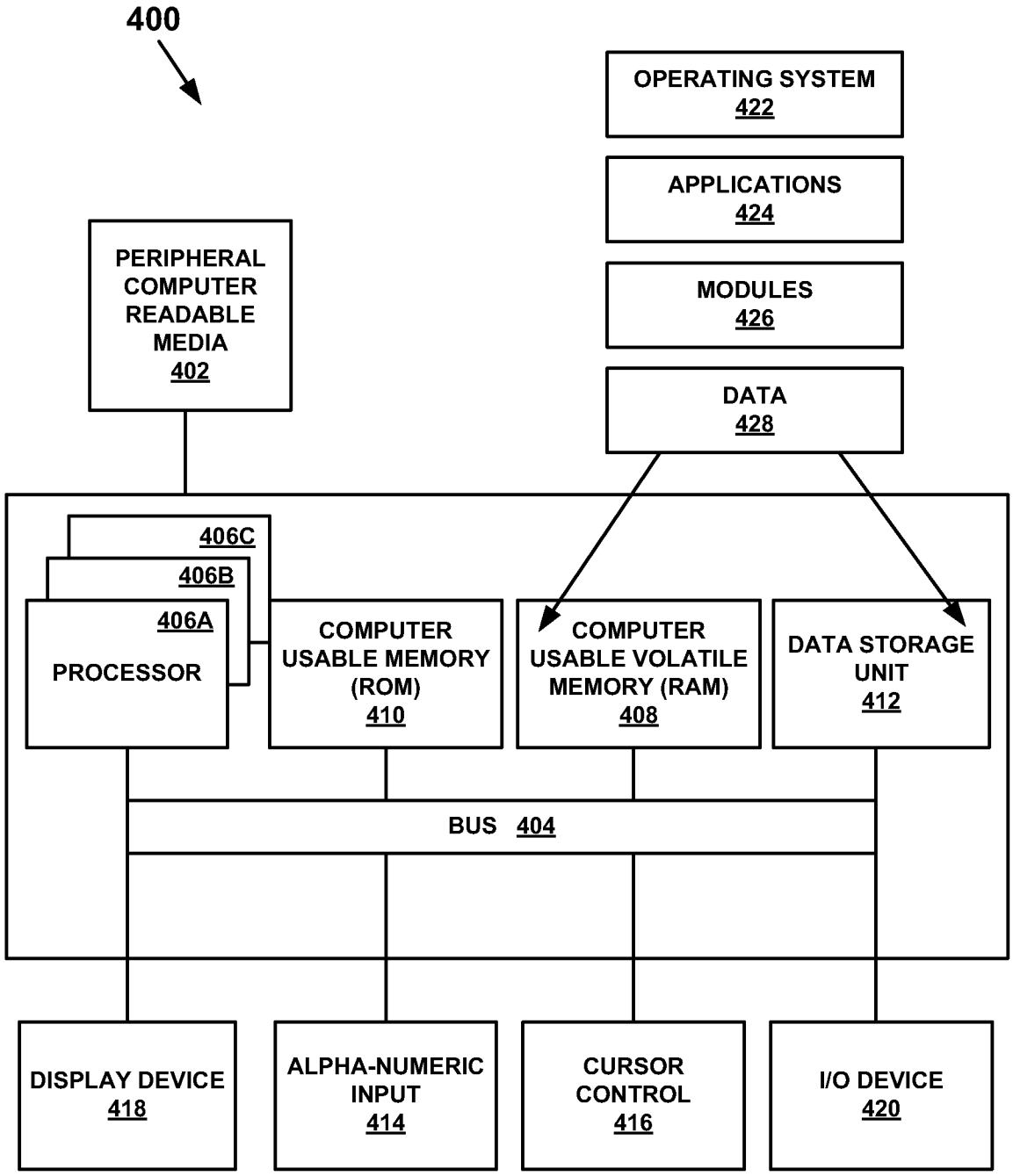
400
OPERATING SYSTEM
422
APPLICATIONS
424
MODULES
426
DATA
428
PERIPHERAL COMPUTER READABLE MEDIA
402
406C
406B
406A
PROCESSOR
COMPUTER USABLE MEMORY (ROM)
410
COMPUTER USABLE VOLATILE MEMORY (RAM)
408
DATA STORAGE UNIT
412
BUS 404
DISPLAY DEVICE
418
ALPHA-NUMERIC INPUT
414
CURSOR CONTROL
416
I/O DEVICE
420

FIG. 4

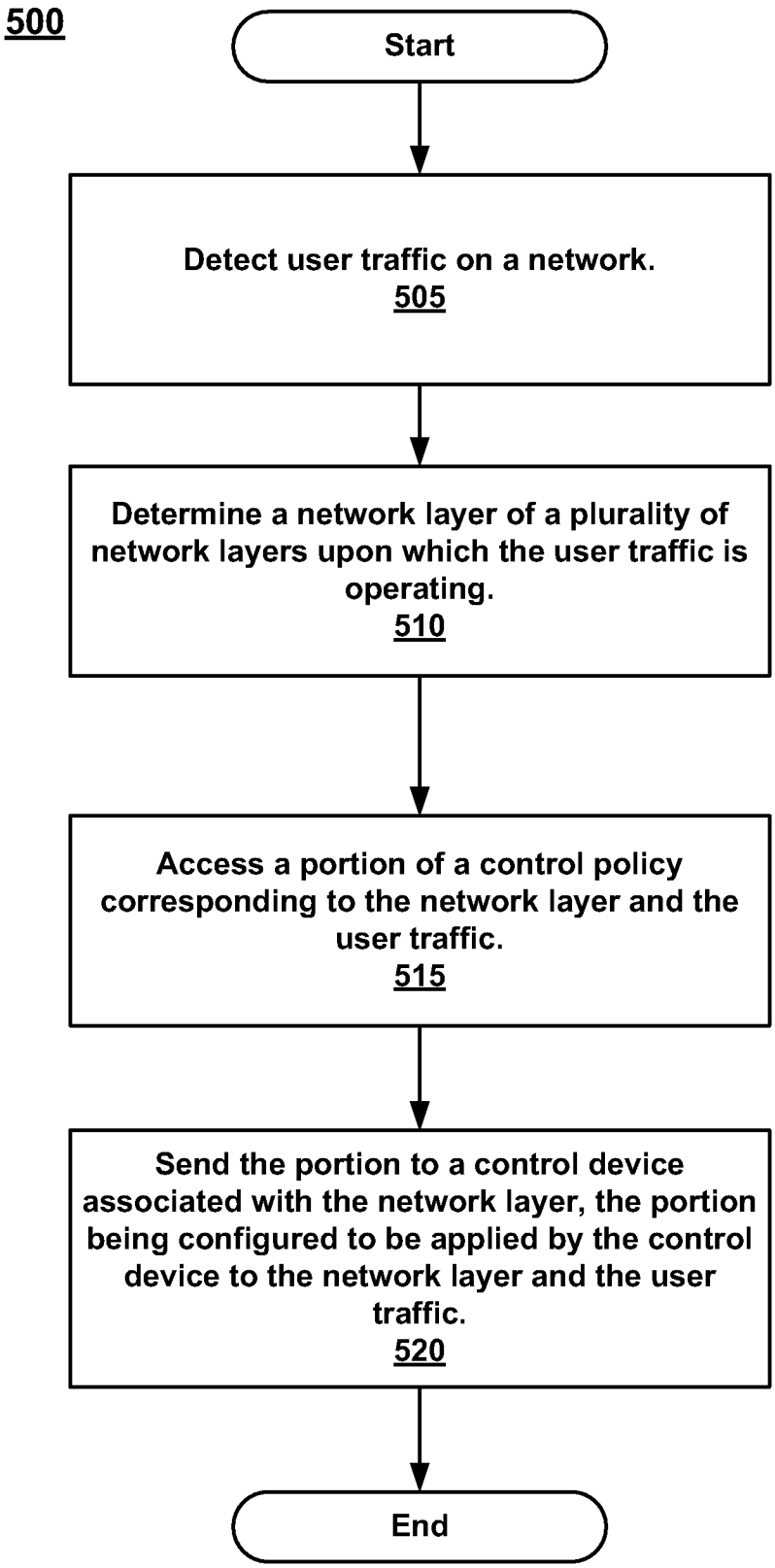
500
Start
Detect user traffic on a network.
505
Determine a network layer of a plurality of network layers upon which the user traffic is operating.
510
Access a portion of a control policy corresponding to the network layer and the user traffic.
515
Send the portion to a control device associated with the network layer, the portion being configured to be applied by the control device to the network layer and the user traffic.
520
End

FIG. 5

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2009/032573

A. CLASSIFICATION OF SUBJECT MATTER

H04W 28/10(2009.01)i, H04W 12/08(2009.01)i, H04B 7/26(2006.01)i

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 G06F

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 since 1975
Japanese Utility models and applications for Utility Models since 1975

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
eKIPASS(KIPO internal) & keywords: "dynamic","firewall, securit*","intrusion","identi*"

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X Y A	US 2005-0108568 A1 (RICHARD BUSSIERE et al.) 19 May 2005 See the abstract; claims 1-3; and figures 1-2.	1-2, 8, 10-11, 13, 15 6-7, 9, 14 3-5, 12
Y A	US 2008-0092223 A1 (DEEPINDER SETIA et al.) 17 April 2008 See the abstract; claim 1; paragraphs [0026]; and figure 4.	6-7, 9, 14 1-5, 8, 10-13, 15
A	US 2005-0027837 A1 (JOHN J. ROESE et al.) 03 February 2005 See the abstract; claim 1; and figure 1.	1-15
A	US 2007-0199061 A1 (ERIC BYRES et al.) 23 August 2007 See the abstract; claim 1; and figure 5.	1-15

☐ 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
19 OCTOBER 2009 (19.10.2009)	**20 OCTOBER 2009 (20.10.2009)**

Name and mailing address of the ISA/KR
Korean Intellectual Property Office
Government Complex-Daejeon, 139 Seonsa-ro, Seo-gu, Daejeon 302-701, Republic of Korea
Facsimile No. 82-42-472-7140

Authorized officer
JUNG, Sung Yun
Telephone No. 82-42-481-8483

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/US2009/032573

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2005-0108568 A1	19.05.2005	EP 1682985 A2	26.07.2006
		US 07581249 B2	25.08.2009
		WO 2005-050364 A2	02.06.2005
		WO 2005-050364 A3	02.06.2005
US 2008-0092223 A1	17.04.2008	None	
US 2005-00027837 A1	03.02.2005	AU 2004-262261 A1	06.07.2004
		CN 1860467 A	08.11.2006
		EP 1652103 A2	03.05.2006
		JP 2007-500396 A	11.01.2007
		KR 10-2006-0029191 A	04.04.2006
		US 07526541 B2	28.04.2009
		WO 2005-013034 A2	10.02.2005
US 2007-0199061 A1	23.08.2007	None	