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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
1 October 2015 (01.10.2015)

WIPO | PCT

(10) International Publication Number
WO 2015/147793 A1

(51) International Patent Classification:
H04L 12/855 (2013.01)

(21) International Application Number:
PCT/US2014/031640

(22) International Filing Date:
25 March 2014 (25.03.2014)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant: **HEWLETT-PACKARD DEVELOPMENT COMPANY, L.P.** [US/US]; 11445 Compaq Center Drive W., Houston, Texas 77070 (US).

(72) Inventor: **WACKERLY, Shaun**; 8000 Foothills Blvd., Roseville, California 95747 (US).

(74) Agents: **KINCAID, David K.** et al.; Hewlett-Packard Company, Intellectual Property Adminsitration, 3404 E. Harmony Road, Mail Stop 35, Fort Collins, Colorado 80528 (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, IR, IS, JP, KE, KG, 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, SA, 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, KM, 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))*

WO 2015/147793 A1

(54) Title: TRANSMITTING NETWORK TRAFFIC IN ACCORDANCE WITH NETWORK TRAFFIC RULES

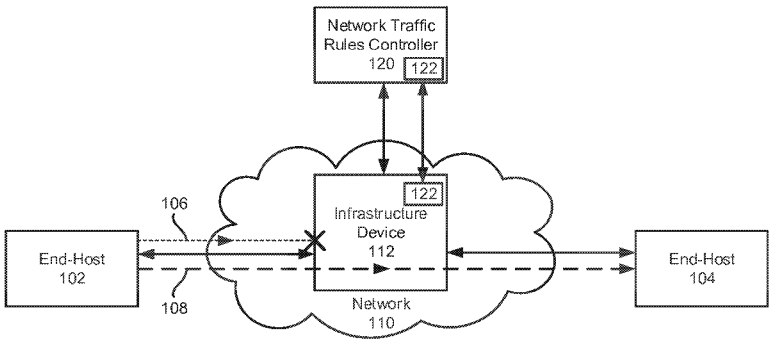

FIG. 1

(57) Abstract: In an example implementation according to aspects of the present disclosure, a method may include identifying, by a computing system, an infrastructure device and an end-host device within a network. The method may further include disseminating, by the computing system, network traffic rules to the infrastructure device, the network traffic rules to route network traffic between end-host devices through the infrastructure device. Further, the network traffic transmitted from a first end-host device to a second end-host device is passed through the infrastructure device to the second end-host device in accordance with the network traffic rules, and network traffic transmitted from the first end-host device to the infrastructure device is blocked by the infrastructure device in accordance with the network traffic rules.

TRANSMITTING NETWORK TRAFFIC IN ACCORDANCE WITH NETWORK TRAFFIC RULES

BACKGROUND

[0001] Computing devices, such as laptops, desktops, mobile phones, tablets, and the like often utilize resources including services, data, and applications within an electronic communication network. Consequently, networks of these computing devices have grown in size and complexity. These networks may include various infrastructure devices, such as switches, routers, hubs, and the like, which connect to and provide the network for the computing devices.

BRIEF DESCRIPTION OF THE DRAWINGS

[0002] The following detailed description references the drawings, in which:

[0003] FIG. 1 illustrates a block diagram of a system for transmitting network traffic in accordance with network traffic rules according to examples of the present disclosure;

[0004] FIG. 2 illustrates a block diagram of a system for transmitting network traffic in accordance with network traffic rules according to examples of the present disclosure;

[0005] FIG. 3 illustrates a flow diagram of a method for transmitting network traffic in accordance with network traffic rules according to examples of the present disclosure; and

[0006] FIG. 4 illustrates a flow diagram of a method for transmitting network traffic in accordance with network traffic rules according to examples of the present disclosure.

DETAILED DESCRIPTION

[0007] Electronic communication networks may include a variety of devices, including networked end-host devices (*e.g.*, a user computing device) and networked infrastructure devices (*e.g.*, network switches, routers, hubs, etc.). Through the network, these interconnected devices communicate by transmitting and receiving data packets. For example, a first end-host device may transmit a

data packet to a second end-host device through an infrastructure device such as a network switch designed to forward the data packets accordingly.

[0008] To direct the network packets appropriately, network infrastructure devices have addressing schemes such as MAC addresses, IP/IPv6 addresses, and the like for communications purposes. The networking infrastructure devices may support a variety of services that may not need to interact with the networked end-host devices. However, the addressing schemes may still be visible to end-hosts. Consequently, the networked infrastructure devices may be vulnerable to security attacks from the networked end-host devices with which they are allowed to communicate. By attacking the network infrastructure, a malicious end-host may deny services and/or snoop network packets from other networked end-hosts connected to the network.

[0009] Previously, network administrators attempted to block end-host communication to specific infrastructure devices by creating network traffic routing rules through manual administrator configuration. This can be a time consuming, costly, and complex endeavor because it depends on the network administrator to reflect network configuration and architecture changes in one part of the network by changing the network traffic routing rules through manual administrator configuration for the entire network's configuration as soon as those changes occur. Failure to implement the manual changes to the rules results in network venerability and insecurity. Consequently, a network administrator needs to be available to update the network traffic routing rules whenever such changes occur, which may be very frequently in large and/or complex networks.

[0010] Various implementations are described below by referring to several examples of techniques for transmitting network traffic in accordance with network traffic rules. In an example implementation according to aspects of the present disclosure, a method may include identifying, by a computing system, an infrastructure device and an end-host device within a network. The method may further include disseminating, by the computing system, network traffic rules to the infrastructure device, the network traffic rules to route network traffic between end-host devices through the infrastructure device. Further, the network traffic transmitted from a first end-host device to a second end-host device is passed

through the infrastructure device to the second end-host device in accordance with the network traffic rules, and network traffic transmitted from the first end-host device to the infrastructure device is blocked by the infrastructure device in accordance with the network traffic rules.

[0011] In some implementations, the network infrastructure devices are protected from malicious network traffic from end-host devices. Moreover, the techniques described herein reduce the time, costs, and complexity associated with manual network traffic routing rules configuration maintenance. These and other advantages will be apparent from the description that follows.

[0012] FIG. 1 illustrates a block diagram of a system for transmitting network traffic in accordance with network traffic rules according to examples of the present disclosure. FIG. 1 includes particular components, modules, etc. according to various examples. However, in different implementations, more, fewer, and/or other components, modules, arrangements of components/modules, etc. may be used according to the teachings described herein. In addition, various components, modules, etc. described herein may be implemented as one or more software modules, hardware modules, special-purpose hardware (e.g., application specific hardware, application specific integrated circuits (ASICs), embedded controllers, hardwired circuitry, etc.), or some combination of these.

[0013] As shown in FIG. 1, a network traffic rules controller 120 is communicatively coupled to an infrastructure device 112, which is also communicatively coupled to end-hosts 102 and 104 within a network 110. It should be noted that the network 110 may include all of the devices shown, as well as additional devices.

[0014] It should be understood that the network traffic rules controller 120 may be a computing system such as any appropriate type of computing device, including for example smartphones, tablets, desktops, laptops, workstations, servers, smart monitors, smart televisions, digital signage, scientific instruments, retail point of sale devices, video walls, imaging devices, peripherals, or the like, or any combination or portion thereof.

[0015] The network traffic rules controller 120 may include a processing resource that represents generally any suitable type or form of processing unit or

units capable of processing data or interpreting and executing instructions. The instructions may be stored on a non-transitory tangible computer-readable storage medium, such as a memory resource, or on a separate device, or on any other type of volatile or non-volatile memory that stores instructions to cause a programmable processor to perform the techniques described herein. Alternatively or additionally, the network traffic rules controller 120 may include dedicated hardware, such as one or more integrated circuits, Application Specific Integrated Circuits (ASICs), Application Specific Special Processors (ASSPs), Field Programmable Gate Arrays (FPGAs), or any combination of the foregoing examples of dedicated hardware, for performing the techniques described herein. In some implementations, multiple processors may be used, as appropriate, along with multiple memories and/or types of memory. In other examples, the network traffic rules controller 120 may include modules or engines made up of hardware and/or software to execute programmatic instructions to perform the processes and methods described herein.

[0016] The network 110 represents generally hardware components and computers interconnected by communications channels that allow sharing of resources and information. The network 110 may include one or more of a cable, wireless, fiber optic, or remote connection via a telecommunication link, an infrared link, a radio frequency link, or any other connectors or systems that provide electronic communication. The network 110 may include, at least in part, an Intranet, the internet, or a combination of both. The network 110 may also include intermediate proxies, routers, switches, load balancers, and the like, such as infrastructure device 112. The paths followed by the network 110 among the end-hosts 102 and 104, the infrastructure device 112, and the network traffic rules controller 120 as depicted in FIG. 1 represent the logical communication paths between these devices, not necessarily the physical paths between the devices. In examples, the network 110 may be a software defined network or the like.

[0017] The network traffic rules controller 120 generates network traffic rules 122 to route network traffic between the end-hosts 102 and 104 through the infrastructure device 112 and then disseminates the network traffic rules 122 to the infrastructure device 112. In examples, the network traffic rules controller 120 also

identifies devices connected to the network, including at least the infrastructure device 112 and the end-hosts 102 and 104. Identifying the infrastructure device and/or the end-hosts within the network may be based, in part or in whole, on the internet protocol (IP) address, media access control (MAC) address, other addressing scheme, traffic type, and/or application function of the device. Additional devices may also be detected. In examples, the network traffic rules controller 120 may periodically (such as once a day, every hour, every few seconds, or any other appropriate interval) or continuously attempt to identify changes to the infrastructure devices and/or end-host devices, such as the modification, addition, or removal of infrastructure and/or end-host devices.

[0018] In an example, the network traffic rules controller 120 may also include functionality to act as a software defined networking controller such as to enable the control plane to communicate with the data plane, using, for example, OpenFlow or another similar mechanism.

[0019] The infrastructure device 112, which may include a network switch, router, hub, or other similar network appliance, transmits network traffic transmitted or sent from one of the end-hosts to another of the end-hosts while refusing network traffic transmitted from one of the end-hosts to the infrastructure device 112 in accordance with the network traffic rules 122. For example, network traffic sent by the end-host 102 to the end-host 104 is sent through the infrastructure device 112 to the end-host 104 in accordance with the network traffic rules 122. In FIG. 1, this is depicted by the dashed line 108 showing network traffic sent from end-host 102 to the end-host 104 through the infrastructure device 112. In other examples, network traffic may be logged or recorded by the infrastructure device (or an appropriate attached device) but allowed to be received by the infrastructure device. This allows for flexibility and post-mortem analysis if a breach occurs. The network traffic may also be redirected to an analysis engine elsewhere in the network and the network traffic may be then allowed or denied by the infrastructure device based on an analysis performed by the analysis engine.

[0020] In an example, network traffic transmitted from one of the end-host devices to another of the end-host devices is passed through the infrastructure device based at least in part on a media access control (MAC) address. In this

case, the infrastructure device 112 stores a MAC address forwarding or routing table to forward or route the network traffic appropriately. Similarly, network traffic transmitted from one of the end-host devices to another of the end-host devices is passed through the infrastructure device based at least in part on an internet protocol (IP) address. In this case, the infrastructure device 112 stores an IP address forwarding or routing table to forward or route the network traffic appropriately.

[0021] The infrastructure device 112 may also deny, refuse, or drop network traffic based on an application type. For example, if network traffic is related to a certain type of application, it may be refused by the infrastructure device 112. Other type of network traffic may also be denied, dropped, or refused in accordance with the network traffic rules 122. In examples, the network traffic rules 122 may be applied at the application layer, presentation layer, session layer, transport layer, network layer, data link layer, and/or physical layer, as appropriate.

[0022] However, if the end-host 102 sends network traffic directly to the infrastructure device 112, that network traffic is denied, refused, and/or dropped by the infrastructure device 112 in accordance with the network traffic rules 122. As shown by the dotted line 106 in FIG. 1, the network traffic is refused by the infrastructure device 112. This prevents unauthorized, potentially harmful network traffic from being received by the infrastructure device 112, which could then potentially infect other devices within the network 110. Similarly, if any other end-host (such as end-host 104) sends network traffic directly to any of the infrastructure devices (such as infrastructure device 112), the traffic is denied by the infrastructure device or treated as otherwise described herein.

[0023] In other examples, such as shown in FIG. 2 and discussed below, the network 110 may include a second infrastructure device. More particularly, FIG. 2 illustrates a block diagram of a system for transmitting network traffic in accordance with network traffic rules 122 according to examples of the present disclosure.

[0024] FIG. 2 includes particular components, modules, etc. according to various examples. However, in different implementations, more, fewer, and/or other components, modules, arrangements of components/modules, etc. may be used according to the teachings described herein. In addition, various components,

modules, etc. described herein may be implemented as one or more software modules, hardware modules, special-purpose hardware (e.g., application specific hardware, application specific integrated circuits (ASICs), embedded controllers, hardwired circuitry, etc.), or some combination of these.

[0025] As shown in FIG. 2, a network traffic rules controller 220 is communicatively coupled to infrastructure devices 212 and 214, which are communicatively coupled together and also to end-hosts 202 and 204 within a network 210. It should be noted that the network 210 may include all of the devices shown, as well as additional devices.

[0026] It should be understood that the network traffic rules controller 220 may be a computing system such as any appropriate type of computing device, including for example smartphones, tablets, desktops, laptops, workstations, servers, smart monitors, smart televisions, digital signage, scientific instruments, retail point of sale devices, video walls, imaging devices, peripherals, or the like, or any combination or portion thereof.

[0027] The network traffic rules controller 220 may include a processing resource that represents generally any suitable type or form of processing unit or units capable of processing data or interpreting and executing instructions. The instructions may be stored on a non-transitory tangible computer-readable storage medium, such as a memory resource, or on a separate device, or on any other type of volatile or non-volatile memory that stores instructions to cause a programmable processor to perform the techniques described herein. Alternatively or additionally, the network traffic rules controller 120 may include dedicated hardware, such as one or more integrated circuits, Application Specific Integrated Circuits (ASICs), Application Specific Special Processors (ASSPs), Field Programmable Gate Arrays (FPGAs), or any combination of the foregoing examples of dedicated hardware, for performing the techniques described herein. In some implementations, multiple processors may be used, as appropriate, along with multiple memories and/or types of memory. In other examples, the network traffic rules controller 220 may include modules or engines made up of hardware and/or software to execute programmatic instructions to perform the processes and methods described herein.

[0028] The network 210 represents generally hardware components and computers interconnected by communications channels that allow sharing of resources and information. The network 210 may include one or more of a cable, wireless, fiber optic, or remote connection via a telecommunication link, an infrared link, a radio frequency link, or any other connectors or systems that provide electronic communication. The network 210 may include, at least in part, an Intranet, the internet, or a combination of both. The network 210 may also include intermediate proxies, routers, switches, load balancers, and the like, such as infrastructure devices 212 and 214. The paths followed by the network 210 among the end-hosts 202 and 204, the infrastructure devices 212 and 214, and the network traffic rules controller 220 as depicted in FIG. 2 represent the logical communication paths between these devices, not necessarily the physical paths between the devices. In examples, the network 210 may be a software defined network or the like.

[0029] The network traffic rules controller 220 generates network traffic rules to route network traffic between the end-hosts 202 and 204 through the infrastructure devices 212 and 214 and then disseminates the network traffic rules to the infrastructure devices 212 and 214. In examples, the network traffic rules controller 220 also identifies devices connected to the network, including at least the infrastructure devices 212 and 214 and the end-hosts 202 and 204. Identifying the infrastructure device and/or the end-hosts within the network may be based, in part or in whole, on the internet protocol (IP) address, media access control (MAC) address, other addressing schemes, traffic type, and/or application function of the device. Additional devices may also be detected. In examples, the network traffic rules controller 220 may periodically (such as once a day, every hour, every few seconds, or any other appropriate interval) or continuously attempt to identify changes to the infrastructure devices and/or end-host devices, such as the modification, addition, or removal of infrastructure and/or end-host devices.

[0030] In an example, the network traffic rules controller 220 may also include functionality to act as a software defined networking controller such as to enable the control plane to communicate with the data plane, using, for example, OpenFlow or another similar mechanism.

[0031] The infrastructure devices 212 and 214, which may include network switches, routers, hubs, and/or other similar network appliance, transmit network traffic transmitted or sent from one of the end-hosts to another of the end-hosts while refusing network traffic transmitted from one of the end-hosts to the infrastructure devices 212 and 214 in accordance with the network traffic rules. For example, network traffic sent by the end-host 202 to the end-host 204 is sent through the infrastructure devices 212 and 214 to the end-host 204 in accordance with the network traffic rules. In FIG. 2, this is depicted by the dashed line 208 showing network traffic sent from end-host 202 to the end-host 204 through the infrastructure devices 212 and 214.

[0032] In an example, network traffic transmitted from one of the end-host devices to another of the end-host devices is passed through the infrastructure devices based at least in part on a media access control (MAC) address. In this case, the infrastructure devices 212 and/or 214 store a MAC address forwarding or routing table(s) to forward or route the network traffic appropriately. Similarly, network traffic transmitted from one of the end-host devices to another of the end-host devices is passed through the infrastructure devices based at least in part on an internet protocol (IP) address. In this case, the infrastructure devices 212 and/or 214 store an IP address forwarding or routing table(s) to forward and/or route the network traffic appropriately.

[0033] The infrastructure devices 212 and 214 may also deny, refuse, or drop network traffic based on an application type. For example, if network traffic is related to a certain type of application, it may be refused by the infrastructure devices 212 and 214. Other type of network traffic may also be denied, dropped, or refused in accordance with the network traffic rules. In examples, the rules may be applied at the application layer, presentation layer, session layer, transport layer, network layer, data link layer, and/or physical layer, as appropriate. In other examples, network traffic may be logged or recorded by the infrastructure device (or an appropriate attached device) but allowed to be received by the infrastructure device. This allows for flexibility and post-mortem analysis if a breach occurs. The network traffic may also be redirected to an analysis engine elsewhere in the

network and the network traffic may be then allowed or denied by the infrastructure device based on an analysis performed by the analysis engine.

[0034] However, if the end-host 202 sends network traffic directly to the infrastructure device 212, for example, that network traffic is denied, refused, and/or dropped or otherwise treated as discussed herein by the infrastructure device 212 in accordance with the network traffic rules. As shown by the dotted line 206 in FIG. 2, the network traffic is refused by the infrastructure device 212. This prevents unauthorized, potentially harmful network traffic from being received by the infrastructure device 212, which could then potentially infect other devices (such as infrastructure device 214) within the network 210. Similarly, if any other end-host (such as end-host 204) sends network traffic directly to any of the infrastructure devices (such as infrastructure device 212 and/or infrastructure device 214), the traffic may be denied by the infrastructure device.

[0035] FIG. 3 illustrates a flow diagram of a method 300 for transmitting network traffic in accordance with network traffic rules according to examples of the present disclosure. The method 300 may be executed by a computing system or a computing device such as the network traffic rules controller 120 and/or 220 of FIGs. 1 and 2 respectively. In one example, method 300 may include: identifying an infrastructure device and an end-host device within a network (block 302); and disseminating network traffic rules to the infrastructure device, the rules to route network traffic between end-host devices through the infrastructure device while preventing the end-host devices form communicating directly with the infrastructure device (block 304).

[0036] At block 302, the method 300 includes identifying an infrastructure device and an end-host device within a network. For example, a computing system (*e.g.*, the network traffic rules controller 120 of FIG. 1 and the network traffic rules controller 220 of FIG. 2) identifies an infrastructure device (*e.g.*, infrastructure device 112 of FIG. 1 and infrastructure devices 212 and 214 of FIG. 2) and an end-host device (*e.g.*, end-hosts 102 and 104 of FIG. 1 and end-hosts 202 and 204 of FIG. 2) within a network (*e.g.*, network 110 of FIG. 1 and network 210 of FIG. 2).

[0037] Identifying the infrastructure device and/or the end-host device within the network may be based, in part or in whole, on the internet protocol (IP) address,

media access control (MAC) address, traffic type, and/or application function of the device. Additional devices may also be detected. In examples, the network traffic rules controller 120 may periodically (such as once a day, every hour, every few seconds, or any other appropriate interval) or continuously attempt to identify changes to the infrastructure devices and/or end-host devices, such as the modification, addition, or removal of infrastructure and/or end-host devices. The method continues to block 304.

[0038] At block 304, the method 300 includes disseminating network traffic rules to the infrastructure device, the rules to route network traffic between end-host devices through the infrastructure device while preventing the end-host devices from communicating directly with the infrastructure device. For example, the computing system (*e.g.*, the network traffic rules controller 120 of FIG. 1 or the network traffic rules controller of FIG. 2) disseminates network traffic rules to the infrastructure device, the network traffic rules to route network traffic between end-host devices through the infrastructure device. In this example, network traffic transmitted from a first end-host device to a second end-host device is passed through the infrastructure device to the second end-host device in accordance with the network traffic rules. However, network traffic transmitted from the first end-host device to the infrastructure device is blocked by the infrastructure device in accordance with the network traffic rules, thus preventing the first end-host device from communicating directly with the infrastructure device.

[0039] In examples, the network traffic rules may be disseminated in a variety of ways. For instance, the network traffic rules may be disseminated manually. The network traffic rules may also be disseminated automatically and may occur in response to a network change (*i.e.*, the addition, removal, or reconfiguration of an infrastructure device). In this way, the network may remain up-to-date by automatically receiving the network traffic rules as soon as a change occurs.

[0040] Additional processes also may be included. For example, the method 300 may include generating, by a computing system, the set of network traffic rules prior to disseminating the set of network traffic rules to the infrastructure device. The method 300 may also include identifying, by the computing system, additional infrastructure devices and end-host devices within the network.

[0041] It should be understood that the processes depicted in FIG. 3 represent illustrations, and that other processes may be added or existing processes may be removed, modified, or rearranged without departing from the scope and spirit of the present disclosure. It should also be understood that the processes depicted in FIG. 3 may be implemented as programmatic instructions stored on a non-transitory computer-readable storage medium that, when executed by a processing resource of a computing system, cause the processing resource to perform the processes described herein.

[0042] FIG. 4 illustrates a flow diagram of a method 400 for transmitting network traffic in accordance with network traffic rules according to examples of the present disclosure. The method 400 may be executed by a computing system or a computing device such as the network traffic rules controller 120 and/or 220 of FIGs. 1 and 2 respectively. In one example, method 400 may include: identifying an infrastructure device and end-host devices within a software defined network (block 402); generating network traffic rules to route network traffic between the end-host devices through the infrastructure device (block 404); and disseminating network traffic rules to the infrastructure device, the rules to route network traffic between end-host devices through the infrastructure device while preventing the end-host devices form communicating directly with the infrastructure device (block 406).

[0043] At block 402, the method 400 includes identifying an infrastructure device and end-host devices within a software defined network. For example, a computing system (*e.g.*, the network traffic rules controller 120 of FIG. 1 and the network traffic rules controller 220 of FIG. 2) identifies an infrastructure device (*e.g.*, infrastructure device 112 of FIG. 1 and infrastructure devices 212 and 214 of FIG. 2) and end-host devices (*e.g.*, end-hosts 102 and 104 of FIG. 1 and end-hosts 202 and 204 of FIG. 2) within a software defined network (*e.g.*, network 110 of FIG. 1 and network 210 of FIG. 2).

[0044] In examples, the network traffic rules controller 120 may periodically or continuously attempt to identify changes to the infrastructure devices and/or end-host devices, such as the modification, addition, or removal of infrastructure and/or end-host devices. Additional devices may also be detected. In examples, the

network traffic rules controller 120 may periodically (such as once a day, every hour, every few seconds, or any other appropriate interval) or continuously attempt to identify changes to the infrastructure devices and/or end-host devices, such as the modification, addition, or removal of infrastructure and/or end-host devices. The method continues to block 404.

[0045] At block 404, the method 400 includes generating network traffic rules to route network traffic between the end-host devices through the infrastructure device. For example, a computing system (*e.g.*, the network traffic rules controller 120 of FIG. 1 and the network traffic rules controller of FIG. 2) generates network traffic rules to route network traffic between the end-host devices through the infrastructure device.

[0046] Generating the network traffic rules may include a network traffic rules controller as discussed regarding FIGs. 1 and 2 automatically generating the network traffic rules. For example, the network traffic rules controller may generate a rule specifying that all network traffic from an end-host with an Ethernet header specifying a destination MAC address as the MAC address of an infrastructure device be blocked or dropped. Similarly, the network traffic rules controller may generate a rule specifying that all network traffic from an end-host with an Ethernet header specifying a destination IP address as the IP address of an infrastructure device be blocked or dropped. The rules may be generated individually based on the type , address, and/or location of a particular infrastructure device, and the rules may differ from one infrastructure device to another infrastructure device. In examples, the rules may also be manually programed programmed such as by a network administrator. In examples, the network traffic rules may also include infrastructure devices within a certain proximity, address range, type, or feature set as the infrastructure to which the rules are disseminated. For instance, each infrastructure device may want to only protect access to devices which are within a three network hops or on the same subnet, so as to reduce the number of network traffic rules on a per-device basis. The network traffic rules controller would still be aware of the remaining infrastructure devices, in examples.

[0047] It should also be understood that the rules may include exceptions, such as for trusted end-hosts. For example, a trusted end-host device may be enabled

to communicate directly with an infrastructure device, such as for management purposes. In this way, the trusted end-host device may be treated like another infrastructure device that may communicate with some of all of the other infrastructure devices within the network. The method continues to block 406.

[0048] At block 406, the method 400 includes disseminating network traffic rules to the infrastructure device, the rules to route network traffic between end-host devices through the infrastructure device while preventing the end-host devices from communicating directly with the infrastructure device. For example, the computing system (*e.g.*, the network traffic rules controller 120 of FIG. 1 or the network traffic rules controller 220 of FIG. 2) disseminates network traffic rules to the infrastructure device, the network traffic rules to route network traffic between end-host devices through the infrastructure device. In this example, network traffic transmitted from a first end-host device to a second end-host device is passed through the infrastructure device to the second end-host device in accordance with the network traffic rules. However, network traffic transmitted from the first end-host device to the infrastructure device is blocked by the infrastructure device in accordance with the network traffic rules, thus preventing the first end-host device from communicating directly with the infrastructure device.

[0049] In examples, the network traffic rules may be disseminated in a variety of ways. For instance, the network traffic rules may be disseminated manually. The network traffic rules may also be disseminated automatically and may occur in response to a network change (*i.e.*, the addition, removal, or reconfiguration of an infrastructure device). In this way, the network may remain up-to-date by automatically receiving the network traffic rules as soon as a change occurs.

[0050] Additional processes also may be included, and it should be understood that the processes depicted in FIG. 4 represent illustrations, and that other processes may be added or existing processes may be removed, modified, or rearranged without departing from the scope and spirit of the present disclosure. It should also be understood that the processes depicted in FIG. 4 may be implemented as programmatic instructions stored on a non-transitory computer-readable storage medium that, when executed by a processing resource of a

computing system, cause the processing resource to perform the processes described herein.

[0051] It should be emphasized that the above-described examples are merely possible examples of implementations and set forth for a clear understanding of the present disclosure. Many variations and modifications may be made to the above-described examples without departing substantially from the spirit and principles of the present disclosure. Further, the scope of the present disclosure is intended to cover any and all appropriate combinations and sub-combinations of all elements, features, and aspects discussed above. All such appropriate modifications and variations are intended to be included within the scope of the present disclosure, and all possible claims to individual aspects or combinations of elements or steps are intended to be supported by the present disclosure.

WHAT IS CLAIMED IS:

1. A method, comprising:

identifying, by a computing system, an infrastructure device and an end-host device within a network; and

disseminating, by the computing system, network traffic rules to the infrastructure device, the network traffic rules to route network traffic between end-host devices through the infrastructure device,

wherein network traffic transmitted from a first end-host device to a second end-host device is passed through the infrastructure device to the second end-host device in accordance with the network traffic rules, and

wherein network traffic transmitted from the first end-host device to the infrastructure device is blocked by the infrastructure device in accordance with the network traffic rules.

2. The method of claim 1, further comprising:

generating, by a computing system, the set of network traffic rules prior to disseminating the set of network traffic rules to the infrastructure device.

3. The method of claim 1, further comprising,

identifying, by the computing system, additional infrastructure devices and end-host devices within the network.

4. The method of claim 1, wherein identifying additional infrastructure devices and end-host devices within the network occurs periodically.

5. The method of claim 1, wherein identifying the infrastructure device and an end-host device within the network is based in part on at least one of an internet protocol (IP) address, a media access control (MAC) address, and an application function.

6. A system, comprising:

an infrastructure device within a network; and

a network traffic rules controller communicatively coupled to the infrastructure device, the network traffic rules controller to generate network traffic rules to route network traffic between end-host devices through the infrastructure device and to disseminate the network traffic rules to the infrastructure device,

the infrastructure device to, in accordance with the network traffic rules, transmit network traffic transmitted from one of the end-host devices to another of the end-host devices and refuse network traffic transmitted from one of the end-host devices to the infrastructure device.

7. The system of claim 6, further comprising:

a second infrastructure device within the network and communicatively coupled to the infrastructure device, the second infrastructure device to transmit network traffic transmitted from one of the end-host devices to another of the end host devices through the infrastructure device and to refuse network traffic transmitted from one of the end-host devices to the second infrastructure device.

8. The system of claim 7, where network traffic transmitted from the one of the end-host devices to the second infrastructure device is refused by the infrastructure device.

9. The system of claim 6, wherein network traffic transmitted from one of the end-host devices to another of the end-host devices is passed through the infrastructure device based at least in part on a media access control (MAC) address.

10. The system of claim 9, wherein the infrastructure device stores a MAC address forwarding table.

11. The system of claim 6, wherein network traffic transmitted from one of the end-host devices to another of the end-host devices is passed through the infrastructure device based at least in part on an internet protocol (IP) address.

12. The system of claim 11, wherein the infrastructure device stores an IP address forwarding table.

13. The system of claim 7, wherein network traffic transmitted from one of the end-host devices to the second infrastructure device is refused by the second infrastructure device based in part on an application traffic type.

14. The system of claim 6, wherein the network traffic rules controller identifies devices connected to the network, including at least the infrastructure device and the end-host devices.

15. A non-transitory computer-readable storage medium storing instructions that, when executed by a processor, cause the processor to:

identify an infrastructure device and end-host devices within a software defined network;

generate network traffic rules to route network traffic between end-host devices through the infrastructure device; and

disseminate the network traffic rules to the infrastructure device,

wherein network traffic transmitted from a first end-host device is passed through the infrastructure device to a second end-host device in accordance with the network traffic rules, and

wherein network traffic transmitted from the first end-host device to the infrastructure device is blocked by the infrastructure device in accordance with the network traffic rules.

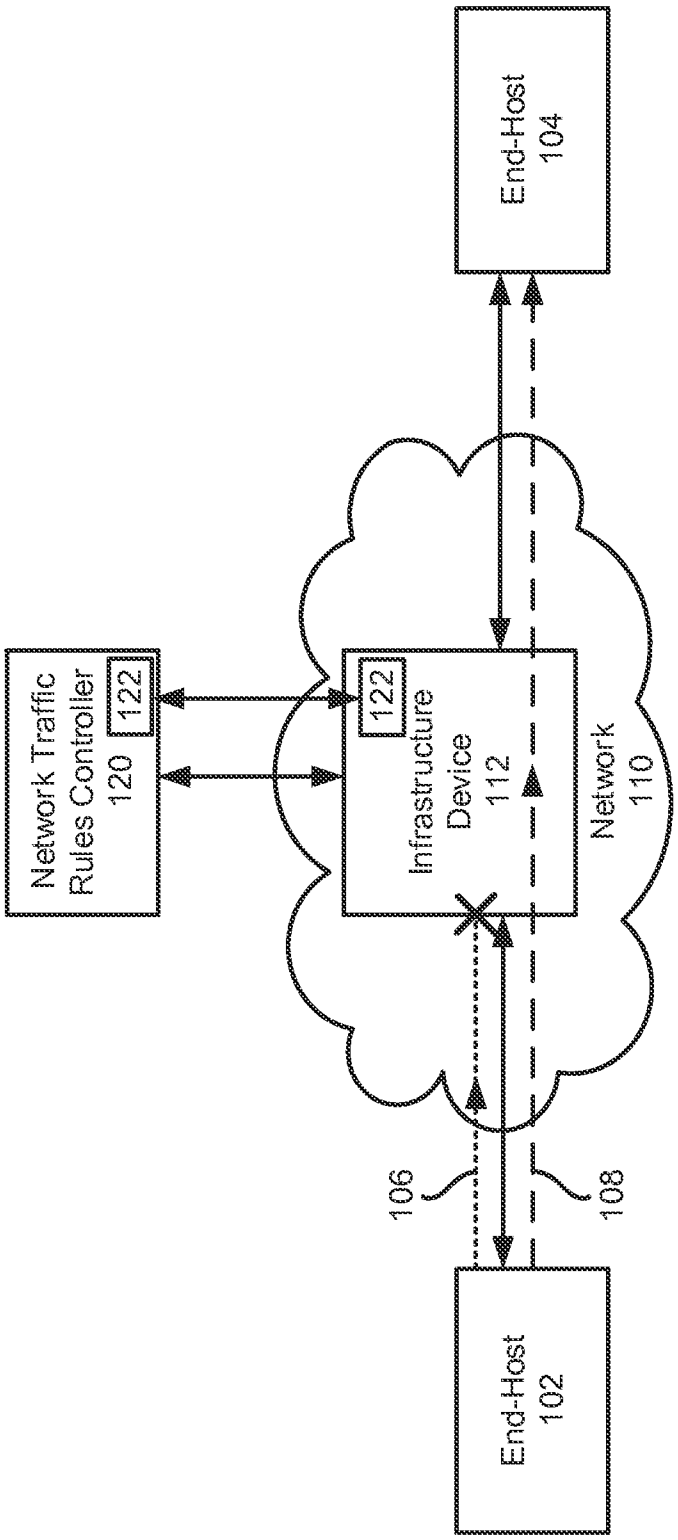
End-Host
104
Network Traffic
Rules Controller
120
122
122
Infrastructure
Device
112
Network
110
106
108
End-Host
102

FIG. 1

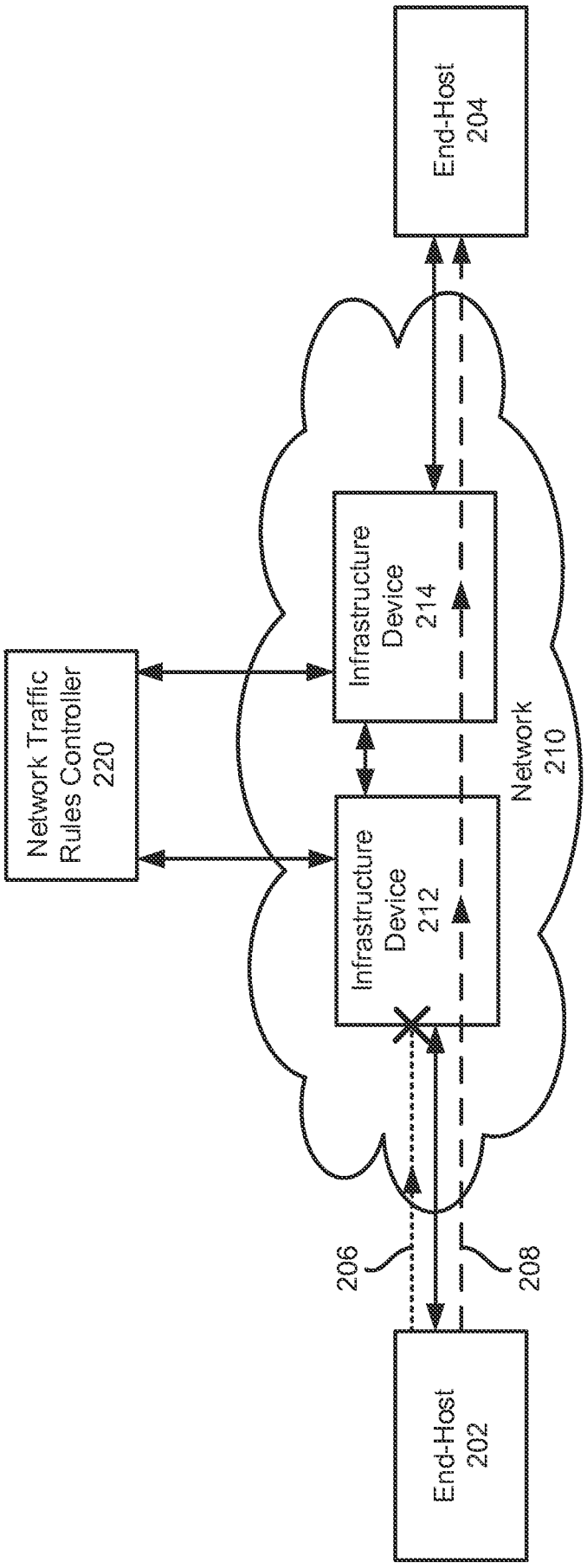
End-Host
204
Infrastructure
Device
214
Network Traffic
Rules Controller
220
Network
210
Infrastructure
Device
212
206
208
End-Host
202

FIG. 2

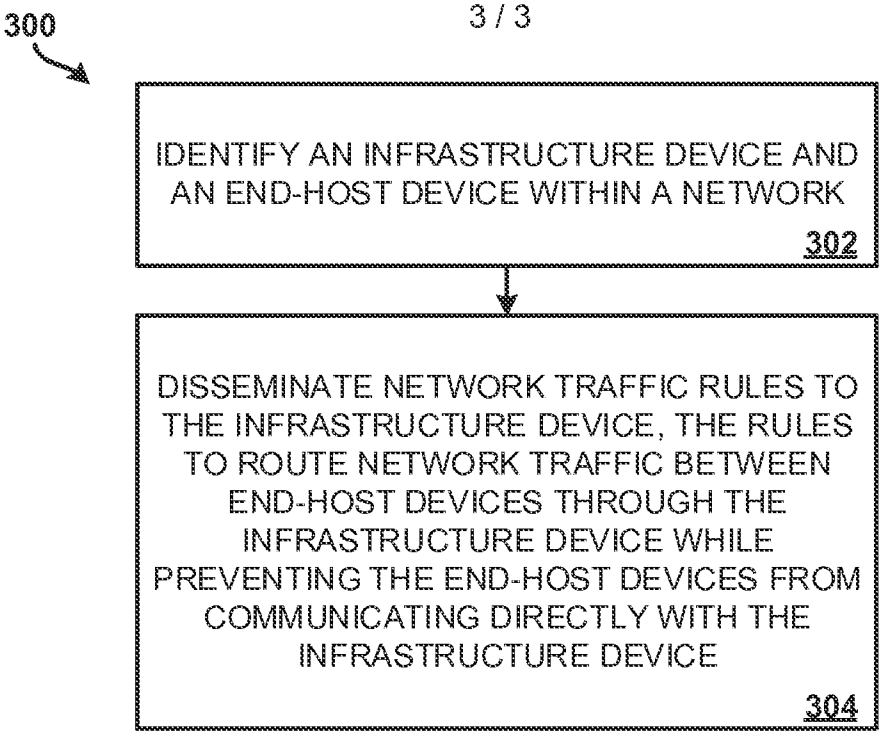
300
IDENTIFY AN INFRASTRUCTURE DEVICE AND AN END-HOST DEVICE WITHIN A NETWORK
302
DISSEMINATE NETWORK TRAFFIC RULES TO THE INFRASTRUCTURE DEVICE, THE RULES TO ROUTE NETWORK TRAFFIC BETWEEN END-HOST DEVICES THROUGH THE INFRASTRUCTURE DEVICE WHILE PREVENTING THE END-HOST DEVICES FROM COMMUNICATING DIRECTLY WITH THE INFRASTRUCTURE DEVICE
304

FIG. 3

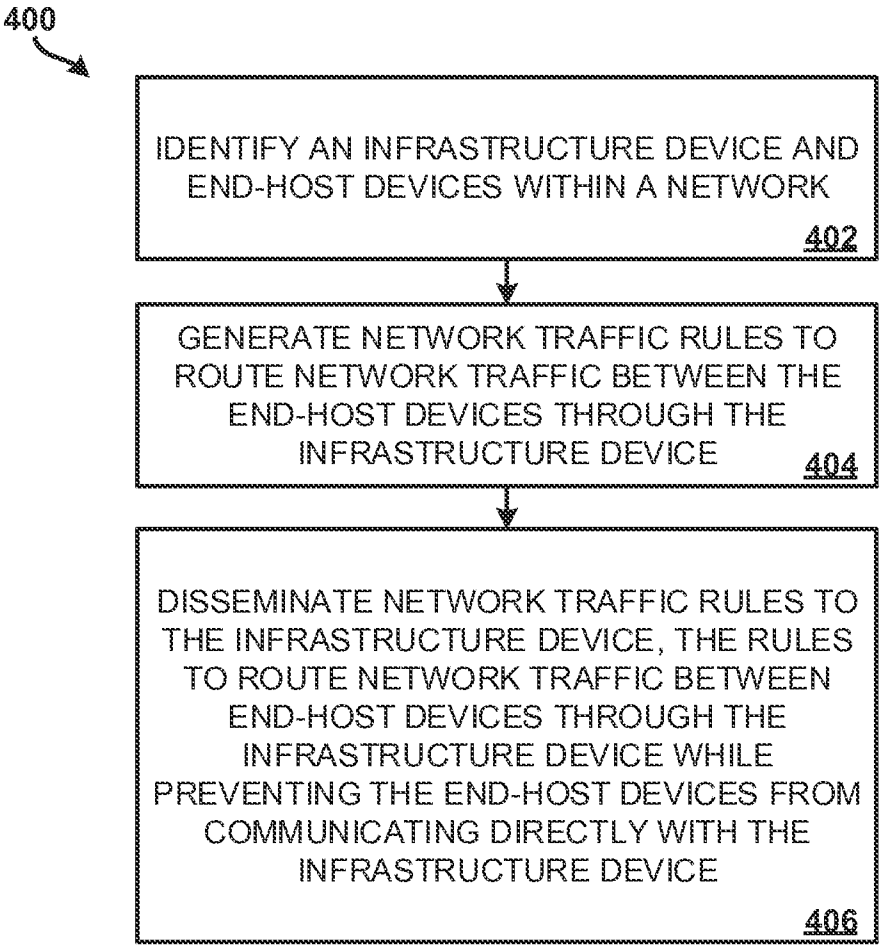
400
IDENTIFY AN INFRASTRUCTURE DEVICE AND END-HOST DEVICES WITHIN A NETWORK
402
GENERATE NETWORK TRAFFIC RULES TO ROUTE NETWORK TRAFFIC BETWEEN THE END-HOST DEVICES THROUGH THE INFRASTRUCTURE DEVICE
404
DISSEMINATE NETWORK TRAFFIC RULES TO THE INFRASTRUCTURE DEVICE, THE RULES TO ROUTE NETWORK TRAFFIC BETWEEN END-HOST DEVICES THROUGH THE INFRASTRUCTURE DEVICE WHILE PREVENTING THE END-HOST DEVICES FROM COMMUNICATING DIRECTLY WITH THE INFRASTRUCTURE DEVICE
406

FIG. 4

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2014/031640

A. CLASSIFICATION OF SUBJECT MATTER

H04L 12/855(2013.01)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)
H04L 12/855; G06F 15/173; H04L 9/32; G06F 12/14; H04L 12/56; G06F 21/00; G06F 21/22

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: network, traffic, rules, controller, switch, router, host, block, IP, MAC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2013-0070762 A1 (ROBERT EDWARD ADAMS et al.) 21 March 2013 See paragraphs [0006], [0069], [0076]-[0077], [0084], [0098], [0101]; and figures 8-9, 10D.	1-4,6-12,14-15
Y		5,13
Y	US 2013-0054784 A1 (NAVINDRA YADAV et al.) 28 February 2013 See paragraphs [0036]-[0040]; and figure 1.	5,13
A		1-4,6-12,14-15
A	US 2012-0311664 A1 (CRAIG T. ELROD et al.) 06 December 2012 See paragraphs [0016], [0019], [0024]; and figure 1B.	1-15
A	US 2008-0189769 A1 (MARTIN CASADO et al.) 07 August 2008 See paragraphs [0012], [0022], [0055]; and figures 1-2.	1-15
A	US 2007-0192862 A1 (VINCENT VERMEULEN et al.) 16 August 2007 See paragraphs [0004]-[0006]; and figure 1.	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 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
08 December 2014 (08.12.2014)	**11 December 2014 (11.12.2014)**

Name and mailing address of the ISA/KR
International Application Division
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
KIM, Seong Woo
Telephone No. +82-42-481-3348

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.
PCT/US2014/031640

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2013-0070762 A1	21/03/2013	AU 2012-312587 A1	03/04/2014
		EP 2748974 A1	02/07/2014
		KR 10-2014-0060583 A	20/05/2014
		WO 2013-043604 A1	28/03/2013
US 2013-0054784 A1	28/02/2013	US 08688828 B2	01/04/2014
		US 2014-156840 A1	05/06/2014
US 2012-0311664 A1	06/12/2012	US 08255996 B2	28/08/2012
		US 08615785 B2	24/12/2013
		US 2007-157306 A1	05/07/2007
US 2008-0189769 A1	07/08/2008	WO 2008-095010 A1	07/08/2008
US 2007-0192862 A1	16/08/2007	CN 101411156 A	15/04/2009
		CN 101411156 B	20/04/2011
		EP 1745631 A1	24/01/2007
		MX PA06013129 A	28/02/2007
		RU 2006-143768 A	20/06/2008
		US 2010-0223669 A1	02/09/2010
		WO 2005-112390 A1	24/11/2005