



**(12) DEMANDE DE BREVET CANADIEN
CANADIAN PATENT APPLICATION**

(13) A1

(86) Date de dépôt PCT/PCT Filing Date: 2018/09/11
(87) Date publication PCT/PCT Publication Date: 2019/03/21
(85) Entrée phase nationale/National Entry: 2020/03/05
(86) N° demande PCT/PCT Application No.: US 2018/050450
(87) N° publication PCT/PCT Publication No.: 2019/055407
(30) Priorité/Priority: 2017/09/12 (US15/702,338)

(51) Cl.Int./Int.Cl. *H04L 29/06* (2006.01),
G06F 15/16 (2006.01), *H04L 29/08* (2006.01)

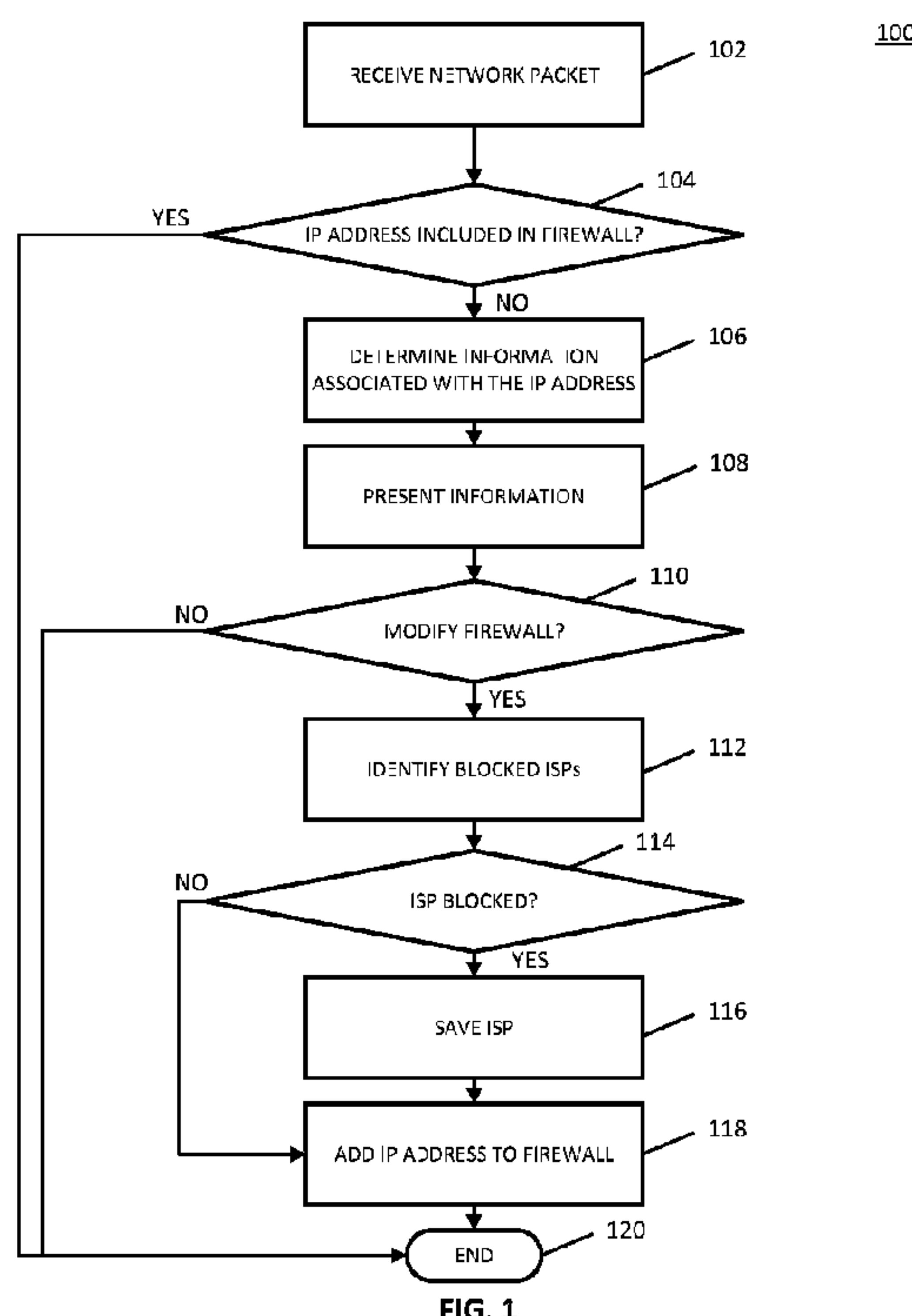
(71) Demandeurs/Applicants:
SYNERGEX GROUP, US;
TAYLOR, WAYNE, US;
PHAM HOLDINGS INC., US

(72) Inventeur/Inventor:
PHAM, THIEN VAN, US

(74) Agent: GOWLING WLG (CANADA) LLP

(54) Titre : PROCEDES, SYSTEMES, ET SUPPORTS, PERMETTANT D'AJOUTER DES ADRESSES IP A DES PARE-FEU

(54) Title: METHODS, SYSTEMS, AND MEDIA FOR ADDING IP ADDRESSES TO FIREWALLS



(57) Abrégé/Abstract:

Methods, systems, and media for adding IP addresses to firewalls are provided. In some embodiments, the method comprises: receiving a network packet that includes an external IP address associated with an external device, wherein the external device is a device not protected by a firewall; determining whether the external IP address is included in a group of IP addresses maintained by the firewall; determining whether to add the external IP address to the group of IP addresses; identifying an Internet Service Provider (ISP) associated with the external IP address; determining whether the ISP is included in a group of ISPs maintained by the firewall; and in response to determining that the ISP is not included in the group of ISPs maintained by the firewall, adding the external IP address to the group of IP addresses and adding the ISP to the group of ISPs.

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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
21 March 2019 (21.03.2019)



(10) International Publication Number
WO 2019/055407 A1

(51) International Patent Classification:

H04L 29/06 (2006.01) H04L 29/08 (2006.01)
G06F 15/16 (2006.01)

(21) International Application Number:

PCT/US2018/050450

(22) International Filing Date:

11 September 2018 (11.09.2018)

(25) Filing Language:

English

(26) Publication Language:

English

(30) Priority Data:

15/702,338 12 September 2017 (12.09.2017) US

(71) Applicants: **SYNERGEX GROUP** [US/US]; 19 Cobb Island Drive, Greenwich, CT 06830 (US). **TAYLOR, Wayne** [US/US]; 2117 East Teakwood Place, Chandler, AZ 85249 (US). **PHAM HOLDINGS INC.** [US/US]; 9227 24th Court SE, Lacey, WA 98513 (US).

(72) Inventor: **PHAM, Thien, Van**; 9227 24th Court SE, Lacey, WA 98513 (US).

(74) Agent: **BYRNE, Matthew, T.** et al.; Byrne Poh LLP, 11 Broadway, Suite 760, New York, NY 10004 (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,

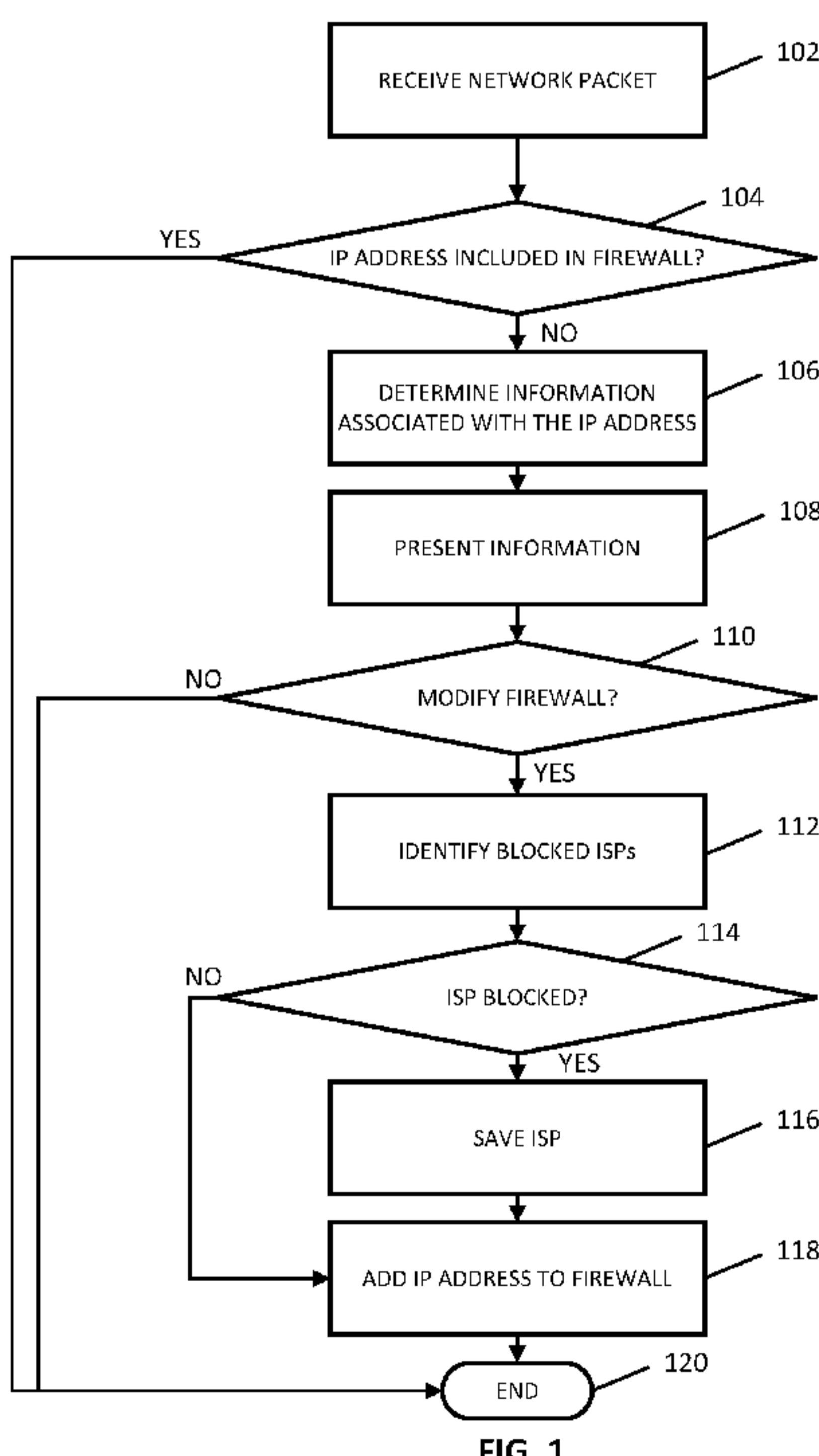
CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, 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, ST, 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).

Published:

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

(54) Title: METHODS, SYSTEMS, AND MEDIA FOR ADDING IP ADDRESSES TO FIREWALLS



(57) Abstract: Methods, systems, and media for adding IP addresses to firewalls are provided. In some embodiments, the method comprises: receiving a network packet that includes an external IP address associated with an external device, wherein the external device is a device not protected by a firewall; determining whether the external IP address is included in a group of IP addresses maintained by the firewall; determining whether to add the external IP address to the group of IP addresses; identifying an Internet Service Provider (ISP) associated with the external IP address; determining whether the ISP is included in a group of ISPs maintained by the firewall; and in response to determining that the ISP is not included in the group of ISPs maintained by the firewall, adding the external IP address to the group of IP addresses and adding the ISP to the group of ISPs.

METHODS, SYSTEMS, AND MEDIA FOR ADDING IP ADDRESSES TO FIREWALLS

Cross-Reference to Related Applications

[0001] This application claims the benefit of United States Patent Application No. 15/702,338, filed September 12, 2017, which is hereby incorporated by reference herein in its entirety.

Technical Field

[0002] The disclosed subject matter relates to methods, systems, and media for adding IP addresses to firewalls.

Background

[0003] Devices, such as servers, frequently use firewalls to protect the devices from malicious users, such as hackers, and viruses. To protect a device, a firewall can identify Internet Protocol (IP) addresses of devices that are not allowed access to the device and blocks incoming and/or outgoing data from being received from and/or transmitted to devices associated with blocked IP addresses. However, it can be difficult to determine whether an IP address should be blocked by a firewall.

[0004] Accordingly, it is desirable to provide new methods, systems, and media for adding IP addresses to firewalls.

Summary

[0005] Methods, systems, and media for adding IP addresses to firewalls are provided. In accordance with some embodiments of the disclosed subject matter, a method for adding IP addresses to firewalls is provided, the method comprising: receiving a network packet that includes an external IP address associated with an external device, wherein the external device is a device not protected by a firewall; determining whether the external IP address is included in a group of IP addresses maintained by the firewall that are either blocked from receiving data from an internal device protected by the firewall or allowed to receive data from an internal device protected by the firewall; in response to determining that the external IP address is not included

in the group of IP addresses, determining whether to add the external IP address to the group of IP addresses; in response to determining that the external IP address is to be added to the group of IP addresses, identifying an Internet Service Provider (ISP) associated with the external IP address; determining whether the ISP is included in a group of ISPs maintained by the firewall; and in response to determining that the ISP is not included in the group of ISPs maintained by the firewall, adding the external IP address to the group of IP addresses and adding the ISP to the group of ISPs.

[0006] In accordance with some embodiments of the disclosed subject matter, a system for adding IP addresses to firewalls are provided, the system comprising: a hardware processor that is programmed to: receive a network packet that includes an external IP address associated with an external device, wherein the external device is a device not protected by a firewall; determine whether the external IP address is included in a group of IP addresses maintained by the firewall that are either blocked from receiving data from an internal device protected by the firewall or allowed to receive data from an internal device protected by the firewall; in response to determining that the external IP address is not included in the group of IP addresses, determine whether to add the external IP address to the group of IP addresses; in response to determining that the external IP address is to be added to the group of IP addresses, identify an Internet Service Provider (ISP) associated with the external IP address; determine whether the ISP is included in a group of ISPs maintained by the firewall; and in response to determining that the ISP is not included in the group of ISPs maintained by the firewall, add the external IP address to the group of IP addresses and adding the ISP to the group of ISPs.

[0007] In accordance with some embodiments of the disclosed subject matter, a non-transitory computer-readable medium containing computer executable instructions that, when executed by a processor, cause the processor to perform a method for adding IP addresses to firewalls is provided. The method comprises: receiving a network packet that includes an external IP address associated with an external device, wherein the external device is a device not protected by a firewall; determining whether the external IP address is included in a group of IP addresses maintained by the firewall that are either blocked from receiving data from an internal device protected by the firewall or allowed to receive data from an internal device protected by the firewall; in response to determining that the external IP address is not included in the group of IP addresses, determining whether to add the external IP address to the group of

IP addresses; in response to determining that the external IP address is to be added to the group of IP addresses, identifying an Internet Service Provider (ISP) associated with the external IP address; determining whether the ISP is included in a group of ISPs maintained by the firewall; and in response to determining that the ISP is not included in the group of ISPs maintained by the firewall, adding the external IP address to the group of IP addresses and adding the ISP to the group of ISPs.

[0008] In accordance with some embodiments of the disclosed subject matter, a system for adding IP addresses to firewalls is provided, the system comprising: means for receiving a network packet that includes an external IP address associated with an external device, wherein the external device is a device not protected by a firewall; means for determining whether the external IP address is included in a group of IP addresses maintained by the firewall that are either blocked from receiving data from an internal device protected by the firewall or allowed to receive data from an internal device protected by the firewall; in response to determining that the external IP address is not included in the group of IP addresses, means for determining whether to add the external IP address to the group of IP addresses; in response to determining that the external IP address is to be added to the group of IP addresses, means for identifying an Internet Service Provider (ISP) associated with the external IP address; means for determining whether the ISP is included in a group of ISPs maintained by the firewall; and in response to determining that the ISP is not included in the group of ISPs maintained by the firewall, means for adding the external IP address to the group of IP addresses and adding the ISP to the group of ISPs.

[0009] In some embodiments, determining whether to add the external IP address to the group of IP addresses is based on input received via a user interface.

[0010] In some embodiments, the system further comprises means for causing the user interface to be presented, wherein the user interface indicates the external IP address and the ISP associated with the external IP address.

[0011] In some embodiments, the system further comprises means for identifying geographic information associated with the external IP address, wherein determining whether to add the external IP address to the group of IP addresses is based on the geographic information associated with the external IP address.

[0012] In some embodiments, the system further comprises means for causing a user interface to be presented that indicates a number of network packets that have been blocked that are associated with the external IP address.

[0013] In some embodiments, the system further comprises means for adding the external IP address to a group of IP addresses associated with the firewall that are blocked from transmitting data to the internal device.

Brief Description of the Drawings

[0014] Various objects, features, and advantages of the disclosed subject matter can be more fully appreciated with reference to the following detailed description of the disclosed subject matter when considered in connection with the following drawings, in which like reference numerals identify like elements.

[0015] FIG. 1 shows an example of a process for adding an IP address to a firewall in accordance with some embodiments of the disclosed subject matter.

[0016] FIG. 2 shows a schematic diagram of an illustrative system suitable for adding IP addresses to a firewall in accordance with some embodiments of the disclosed subject matter.

[0017] FIG. 3 shows a detailed example of hardware that can be used in a server and/or a user device of FIG. 2 in accordance with some embodiments of the disclosed subject matter.

[0018] FIG. 4A shows an example of a user interface for blocking an IP address in accordance with some embodiments of the disclosed subject matter.

[0019] FIG. 4B shows an example of a user interface for presenting aggregated information relating to blocked IP addresses in accordance with some embodiments of the disclosed subject matter.

[0020] FIG. 5 shows an example of a user interface for presenting aggregated information relating to received network packets in accordance with some embodiments of the disclosed subject matter.

Detailed Description

[0021] In accordance with various embodiments, mechanisms (which can include methods, systems, and media) for adding IP addresses to firewalls are provided.

[0022] In some embodiments, the mechanisms described herein can receive a network packet from a device and can determine whether an Internet Protocol (IP) address associated with the received network packet is to be blocked by a firewall. For example, in some embodiments, the mechanisms can determine whether an IP address is included in a list of IP addresses that are to be blocked by a firewall. Additionally, in some embodiments, the mechanisms can add an IP address or an Internet Service Provider (ISP) associated with an IP address to a list of IP addresses or ISPs blocked by a firewall. In some such embodiments, the mechanisms can determine information associated with an IP address based on a network packet. For example, the mechanisms can determine an ISP associated with an IP address and/or can determine geographic information associated with the IP address, and can add the IP address and/or the ISP to one or more lists of IP addresses and/or ISPs that are to be blocked by the firewall.

[0023] In some embodiments, the mechanisms can determine whether to block a particular IP address or an ISP associated with the particular IP address based on any suitable information. For example, in some embodiments, the mechanisms can determine that a particular IP address or an ISP associated with the particular IP address is to be added to a list of blocked IP addresses or blocked ISPs based on an explicit indication from a user (e.g., a user associated with administration of the firewall or of a device protected by the firewall), such as via a user interface, as shown in and described below in connection with FIG. 4A. Additionally, in some embodiments, the mechanisms can allow a user to unblock a blocked IP address and/or a blocked ISP, for example, via a user interface, as shown in and described below in connection with FIG. 4B.

[0024] In some embodiments, the mechanisms can present aggregated information relating to received network packets. For example, in some embodiments, the mechanisms can cause a user interface that includes a listing of received network packets to be presented. In some such embodiments, each entry in a list of received network packets can indicate an external IP address associated with a network packet (e.g., an IP address associated with a device not protected by the firewall that is attempting to connect to a device protected by the firewall, and/or any other suitable device), an internal IP address associated with the network packet (e.g., an IP address of a device protected by the firewall, and/or any other suitable device), an ISP

corresponding to the external IP address associated with the network packet, and/or any other suitable information.

[0025] Turning to FIG. 1, an example 100 of a process for adding IP addresses to a firewall in accordance with some embodiments of the disclosed subject matter is shown. In some embodiments, blocks of process 100 can be executed on any suitable device, such as a firewall 212 as shown in and described below in connection with FIG. 2.

[0026] Process 100 can begin by receiving a network packet at 102. In some embodiments, the network packet can be received from any suitable device and can include any suitable information. For example, in some embodiments, the network packet can indicate a date and time the network packet was received, an internal IP address and port, an external IP address and port, a size of the network packet, and/or any other suitable information.

[0027] At 104, process 100 can determine whether an IP address included in the network packet received at 102 is included in a list or a group of IP addresses maintained by a firewall. Note that, in some embodiments, such a list or a group of IP addresses can be maintained by a firewall in any suitable manner. For example, in some embodiments, a list or a group of IP addresses can include inbound rules and/or outbound rules that indicate whitelisted IP addresses of external devices. As a more particular example, in some embodiments, an inbound rule can indicate IP addresses of external devices that are allowed to connect to devices protected by the firewall and an outbound rule can indicate IP addresses of external devices allowed to be connected to by devices protected by the firewall, and/or any other suitable information. As another example, in some embodiments, a list or a group of IP addresses can include inbound rules and/or outbound rules that indicate blacklisted IP addresses of external devices. As a more particular example, in some embodiments, an inbound rule can indicate IP addresses of external devices that are blocked from connected to devices protected by the firewall and an outbound rule can indicate IP addresses of external devices blocked from being connected to by devices protected by the firewall, and/or any other suitable information. Note that, in some embodiments, an inbound rule and/or an outbound rule can additionally or alternatively include internal IP addresses (e.g., IP addresses corresponding to devices protected by the firewall) that are allowed to communicate with external devices and/or blocked from communicating with external devices. In some embodiments, a rule can act as both an inbound rule and an outbound rule – i.e., by blocking both inbound and outbound traffic. In some embodiments, a rule can be

both a whitelisting rule and a blacklisting rule – e.g., by allowing certain external IP addresses while blocking other external IP addresses.

[0028] Note that, in some embodiments, an inbound rule and/or an outbound rule can specify one or more ports or programs that are allowed to connect with devices protected by the firewall or that are blocked from connecting with devices protected by the firewall. Additionally or alternatively, in some embodiments, an inbound rule and/or an outbound rule can include a scope that indicates a particular IP address or a range of IP addresses that are allowed access to devices protected by the firewall or that are blocked from accessing devices protected by the firewall.

[0029] In some embodiments, process 100 can determine whether an IP address associated with a received network packet is included in a list of IP addresses (e.g., a list associated with an inbound rule, a list associated with an outbound rule, and/or any other suitable list or group) in any suitable manner. For example, in some embodiments, process 100 can determine whether an external IP address associated with a received network packet is included in an inbound rule that indicates blocked IP addresses, an inbound rule that indicates allowed IP addresses, an outbound rule that indicates blocked IP addresses, an outbound rule that indicates allowed IP addresses, and/or included in any other suitable group.

[0030] If, at 104, process 100 determines that an IP address is included in one or more lists maintained by the firewall (“yes” at 104), process 100 can end at 120.

[0031] If, at 104, process 100 determines that the IP address is not included in one or more lists maintained by the firewall (“no” at 104), process 100 can determine information associated with the IP address at 106. In some embodiments, process 100 can determine any suitable information. For example, in some embodiments, process 100 can determine an Internet Service Provider (ISP) associated with an external IP address corresponding to a network packet, a geographic location associated with the external IP address (e.g., a latitude and/or a longitude, and/or any other suitable geographic information), a domain associated with the external IP address, and/or any other suitable information. In some embodiments, process 100 can determine the information associated with the IP address using any suitable technique or combination of techniques. For example, in some embodiments, process 100 can query a database, such as a database stored in a memory of the firewall and/or of a device protected by the firewall (e.g., memory 304 of firewall 212 and/or memory 304 of server(s) 202 as described

below in connection with FIGS. 2 and 3, and/or any other suitable memory). As another example, in some embodiments, process 100 can connect to an online IP address translator. As a more particular example, in some embodiments, process 100 can transmit the IP address to an online IP address translator and can receive information associated with the IP address in response to the transmitted query.

[0032] At 108, process 100 can present information to a user, such as, for example, a user associated with administration of the firewall. FIG. 4A shows an example 400 of a user interface for presenting information associated with a received network packet. As illustrated, in some embodiments, user interface 400 can include information 402, which can include, for example, a date or a time the network packet was received, an external IP address and port, an internal IP address and port, a communication protocol, an ISP name associated with the external IP address, geographic information associated with the external IP address, a directionality of the network packet (e.g., whether the destination of the network packet is a device protected by the firewall or a device not protected by the firewall), and/or a domain name associated with the external IP address. In some embodiments, user interface 400 can include a selectable input 404 to block the external IP address associated with the network packet. In some such embodiments, selection of input 404 can cause the external IP address to be added to firewall rules that indicate IP addresses not allowed to communicate with devices protected by the firewall (e.g., server(s) 202 as shown in and described below in connection with FIG. 2). Additionally, in some embodiments, user interface 400 can include selectable inputs to view a page corresponding to the external IP address, view a page corresponding to the domain associated with the external IP address, and/or view a page corresponding to the ISP associated with the external IP address. In some embodiments, user interface 400 can include a domain preview 406 that shows a web page corresponding to the domain. For example, in instances where the domain is “www.domainA.com,” domain preview 406 can show the web page that corresponds to “www.domainA.com.”

[0033] Note that, in some embodiments, process 100 can additionally present aggregated information that indicates IP addresses and/or ISPs that have been blocked by the firewall. Turning to FIG. 4B, an example 450 of a user interface for showing aggregated information in accordance with some embodiments of the disclosed subject matter is shown. As illustrated, in some embodiments, user interface 450 can include information about IP addresses and/or ISPs

that have been blocked by the firewall, for example, in response to a user of user interface 400 indicating that a particular IP address or ISP is to be blocked. In some embodiments, user interface 450 can include a list of blocked IP addresses, and each entry, such as entry 452, can indicate a name of an ISP associated with a blocked IP address, a geographic location associated with the blocked IP address, and/or a domain name associated with the blocked IP address. In some embodiments, selection of entry 452 can allow a user of user interface 450 to change a status of entry 452, for example, by unblocking a blocked IP address or ISP.

[0034] Returning to FIG. 1, at 110, process 100 can determine whether the firewall is to be modified. In some embodiments, process 100 can determine whether the firewall is to be modified based on any suitable information. For example, in some embodiments, process 100 can determine whether the firewall is to be modified based on whether a user of user interface 400 has indicated that an IP address associated with the received network packet or an ISP associated with the IP address is to be blocked. As a more particular example, in some embodiments, a user of user interface 400 can indicate that an external IP address associated with the received network packet is to be blocked and/or that an ISP associated with the external IP address is to be blocked. As another more particular example, in some embodiments, a user of user interface 400 can indicate that an external IP address associated with the received network packet is to be allowed and/or that an ISP associated with the external IP address is to be allowed. As yet another more particular example, in some embodiments, a user of user interface 400 can indicate that an internal IP address associated with the received network packet is to be blocked in any suitable manner (e.g., blocked from communicating with all external devices not protected by the firewall, blocked from communicating with an external device associated with the external IP address, blocked from communicating with external devices associated with the external ISP, and/or blocked in any other suitable manner).

[0035] As another example, in some embodiments, process 100 can determine that an IP address is to be blocked based on the port number associated with the IP address. As a more particular example, in some embodiments, process 100 can determine that an IP address is to be blocked based on the port number of the network packet corresponding to a particular activity, such as file transfer, web browsing, remote printing, and/or any other suitable activity. As yet another example, in some embodiments, process 100 can determine that an IP address is to be blocked based on a type of protocol associated with the network packet (e.g., Transmission

Control Protocol, User Datagram Protocol, and/or any other suitable protocol). As still another example, in some embodiments, process 100 can determine that an IP address is to be blocked based on any other suitable information, such as a domain associated with an external IP address, a geographic location associated with the external IP address, and/or any other suitable information.

[0036] At 112, process 100 can identify one or more ISPs that are blocked by the firewall. For example, in some embodiments, the blocked ISPs can include ISPs associated with previously blocked external IP addresses. In some embodiments, process 100 can identify the one or more blocked ISPs using any suitable information and using any suitable technique(s). For example, in some embodiments, process 100 can retrieve a list of blocked ISPs stored in memory of the firewall and/or of a device protected by the firewall (e.g., memory 304 of firewall 212 and/or memory 304 of server(s) 202, as described below in connection with FIGS. 2 and 3). In some embodiments, the blocked ISPs can include ISPs blocked by inbound rules and/or outbound rules, as described above.

[0037] At 114, process 100 can determine whether the ISP associated with the external IP address is included in a list of allowed or blocked ISPs.

[0038] If, at 114, process 100 determines that the ISP is included in a list of ISPs (“yes” at 114), at 116, process 100 can add the ISP associated with the external IP address to a list stored in memory (e.g., memory 304 of firewall 212, memory 304 of server(s) 202, and/or any other suitable location), such as the list of blocked ISPs described above in connection with block 112.

[0039] If, at 114, process 100 determines that the ISP is not included in the list of blocked ISPs (“no” at 114), process 100 can proceed to 118.

[0040] At 118, process 100 can add the IP address to any suitable lists associated with and/or maintained by the firewall. For example, in some embodiments, process 100 can add an external IP address to an inbound rules list that indicates IP addresses blocked from connecting to devices protected by the firewall. As another example, in some embodiments, process 100 can add an IP address to an outbound rules list that indicates IP addresses blocked from being connected to by devices protected by the firewall. As yet another example, in some embodiments, process 100 can add an external IP address to an inbound rules list that indicates IP addresses allowed to connect to devices protected by the firewall. As still another example, in

some embodiments, process 100 can add an external IP address to an outbound rules list that indicates IP addresses allowed to be connected to by devices protected by the firewall. Note that, in some embodiments, process 100 can add an internal IP address associated with a received network packet to any suitable lists associated with and/or maintained by the firewall, such as inbound rules that indicate blocked IP addresses, outbound rules that indicate blocked IP addresses, inbound rules that indicate allowed IP addresses, outbound rules that indicate allowed IP addresses, and/or any other suitable lists or rules.

[0041] Note that, in some embodiments, process 100 can cause any suitable information to be presented to a user, such as a user associated with administration of the firewall. For example, as shown in user interface 500 of FIG. 5, process 100 can present information corresponding to an aggregation of network packets that have been received. As illustrated, in some embodiments, user interface 500 can include a listing of network packets that have been received, and can include individual entries, such as entry 502. As shown, entry 502 can include any suitable information, such as a date and a time that a network packet was received, an external IP address associated with the network packet, an internal IP address associated with the network packet, a geographic location associated with the network packet, an ISP name corresponding to the external IP address associated with the network packet, a domain name associated with the external IP address of the network packet, and/or any other suitable information. Additionally, as shown in user interface 500, entry 502 can indicate a number of network packets received corresponding to a blocked IP address that have been blocked by the firewall previously over any suitable time frame (e.g., total packets in the past week, total packets in the past month, and/or a number of packets blocked over any other suitable time frame).

[0042] Process 100 can end at 120.

[0043] Turning to FIG. 2, an example 200 of hardware for adding IP addresses to firewalls that can be used in accordance with some embodiments of the disclosed subject matter is shown. As illustrated, hardware 200 can include one or more servers 202, a communication network 204, one or more user devices 206, such as user devices 208 and 210, and/or a firewall 212.

[0044] Server(s) 202 can be any suitable server(s) for storing data or providing services to devices, such as user devices 206. For example, in some embodiments, server(s) 202 can store

media content, such as videos, television programs, movies, live-streamed media content, audio content, and/or any other suitable media content. As another example, in some embodiments, server(s) 202 can be associated with a web site or service that provides any suitable service(s), such as an online database, an online retailer, and/or any other suitable type of service. In some embodiments, server(s) 202 can be protected by firewall 212, as described above in connection with FIG. 1.

[0045] Communication network 204 can be any suitable combination of one or more wired and/or wireless networks in some embodiments. For example, communication network 204 can include any one or more of the Internet, an intranet, a wide-area network (WAN), a local-area network (LAN), a wireless network, a digital subscriber line (DSL) network, a frame relay network, an asynchronous transfer mode (ATM) network, a virtual private network (VPN), and/or any other suitable communication network. User devices 206 can be connected by one or more communications links to communication network 204 that can be linked via one or more communications links to server(s) 202. The communications links can be any communications links suitable for communicating data among user devices 206 and server(s) 202 such as network links, dial-up links, wireless links, hard-wired links, any other suitable communications links, or any suitable combination of such links. In some embodiments, communication via communication network 204 can be through transmitted network packets corresponding to any suitable type of communication protocol, such as Transmission Control Protocol (TCP), User Datagram Protocol (UDP), and/or any other suitable protocol.

[0046] User devices 206 can include any one or more user devices suitable for communicating with server(s) 202. For example, in some embodiments, user devices 206 can include a mobile device, such as a mobile phone, a tablet computer, a wearable computer, a laptop computer, a vehicle (e.g., a car, a boat, an airplane, or any other suitable vehicle) information and/or entertainment system, and/or any other suitable mobile device. As another example, in some embodiments, user devices 206 can include a non-mobile device, such as a television, a projector device, a game console, desktop computer, and/or any other suitable non-mobile device.

[0047] Firewall 212 can be any suitable device for protecting server(s) 202. For example, in some embodiments, firewall 212 can be a device that stores and maintains lists of external IP addresses allowed to connect to and/or blocked from connecting to user devices 206.

As another example, in some embodiments, firewall 212 can store and maintain lists of external IP addresses allowed to be connected to and/or blocked from being connected to by user devices 206. As yet another example, in some embodiments, firewall 212 can store and maintain lists of internal IP addresses that are to be blocked from communicating with external devices not protected by firewall 212 and/or lists of internal IP addresses that are allowed to communicate with external devices not protected by firewall 212. Note that, although firewall 212 is shown as a device separate from server(s) 202, in some embodiments, firewall 212 can be combined with any of server(s) 202.

[0048] Although server(s) 202 is illustrated as one device, the functions performed by server(s) 202 can be performed using any suitable number of devices in some embodiments. For example, in some embodiments, multiple devices can be used to implement the functions performed by server(s) 202.

[0049] Although two user devices 208 and 210 are shown in FIG. 2 to avoid over-complicating the figure, any suitable number of user devices, and/or any suitable types of user devices, can be used in some embodiments.

[0050] Server(s) 202 and user devices 206 can be implemented using any suitable hardware in some embodiments. For example, in some embodiments, devices 202 and 206 can be implemented using any suitable general purpose computer or special purpose computer. For example, a mobile phone may be implemented using a special purpose computer. Any such general purpose computer or special purpose computer can include any suitable hardware. For example, as illustrated in example hardware 300 of FIG. 3, such hardware can include hardware processor 302, memory and/or storage 304, an input device controller 306, an input device 308, display/audio drivers 310, display and audio output circuitry 312, communication interface(s) 314, an antenna 316, and a bus 318.

[0051] Hardware processor 302 can include any suitable hardware processor, such as a microprocessor, a micro-controller, digital signal processor(s), dedicated logic, and/or any other suitable circuitry for controlling the functioning of a general purpose computer or a special purpose computer in some embodiments. In some embodiments, hardware processor 302 can be controlled by a computer program stored in memory and/or storage 304 of a firewall device (e.g., such as firewall 212). For example, in some embodiments, the computer program can cause hardware processor 302 to identify information associated with an IP address and, based on the

information, determine whether to add the IP address to a list of blocked IP addresses maintained by firewall 212.

[0052] Memory and/or storage 304 can be any suitable memory and/or storage for storing programs, data, media content, and/or any other suitable information in some embodiments. For example, memory and/or storage 304 can include random access memory, read-only memory, flash memory, hard disk storage, optical media, and/or any other suitable memory.

[0053] Input device controller 306 can be any suitable circuitry for controlling and receiving input from one or more input devices 308 in some embodiments. For example, input device controller 306 can be circuitry for receiving input from a touchscreen, from a keyboard, from a mouse, from one or more buttons, from a voice recognition circuit, from a microphone, from a camera, from an optical sensor, from an accelerometer, from a temperature sensor, from a near field sensor, and/or any other type of input device.

[0054] Display/audio drivers 310 can be any suitable circuitry for controlling and driving output to one or more display/audio output devices 312 in some embodiments. For example, display/audio drivers 310 can be circuitry for driving a touchscreen, a flat-panel display, a cathode ray tube display, a projector, a speaker or speakers, and/or any other suitable display and/or presentation devices.

[0055] Communication interface(s) 314 can be any suitable circuitry for interfacing with one or more communication networks, such as network 204 as shown in FIG. 2. For example, interface(s) 314 can include network interface card circuitry, wireless communication circuitry, and/or any other suitable type of communication network circuitry.

[0056] Antenna 316 can be any suitable one or more antennas for wirelessly communicating with a communication network (e.g., communication network 204) in some embodiments. In some embodiments, antenna 316 can be omitted.

[0057] Bus 318 can be any suitable mechanism for communicating between two or more components 302, 304, 306, 310, and 314 in some embodiments.

[0058] Any other suitable components can be included in hardware 300 in accordance with some embodiments.

[0059] In some embodiments, at least some of the above described blocks of the process of FIG. 1 can be executed or performed in any order or sequence not limited to the order and sequence shown in and described in connection with the figure. Also, some of the above blocks

of FIG. 1 can be executed or performed substantially simultaneously where appropriate or in parallel to reduce latency and processing times. Additionally or alternatively, some of the above described blocks of the process of FIG. 1 can be omitted.

[0060] In some embodiments, any suitable computer readable media can be used for storing instructions for performing the functions and/or processes herein. For example, in some embodiments, computer readable media can be transitory or non-transitory. For example, non-transitory computer readable media can include media such as non-transitory forms of magnetic media (such as hard disks, floppy disks, and/or any other suitable magnetic media), non-transitory forms of optical media (such as compact discs, digital video discs, Blu-ray discs, and/or any other suitable optical media), non-transitory forms of semiconductor media (such as flash memory, electrically programmable read-only memory (EPROM), electrically erasable programmable read-only memory (EEPROM), and/or any other suitable semiconductor media), any suitable media that is not fleeting or devoid of any semblance of permanence during transmission, and/or any suitable non-transitory tangible media. As another example, transitory computer readable media can include signals on networks, in wires, conductors, optical fibers, circuits, any suitable media that is fleeting and devoid of any semblance of permanence during transmission, and/or any suitable intangible media.

[0061] Accordingly, methods, systems, and media for adding IP addresses to firewalls are provided.

[0062] Although the invention has been described and illustrated in the foregoing illustrative embodiments, it is understood that the present disclosure has been made only by way of example, and that numerous changes in the details of implementation of the invention can be made without departing from the spirit and scope of the invention, which is limited only by the claims that follow. Features of the disclosed embodiments can be combined and rearranged in various ways.

What is claimed is:

1. A method for adding Internet Protocol (IP) addresses to firewalls, comprising:
 - receiving a network packet that includes an external IP address associated with an external device, wherein the external device is a device not protected by a firewall;
 - determining whether the external IP address is included in a group of IP addresses maintained by the firewall that are either blocked from receiving data from an internal device protected by the firewall or allowed to receive data from an internal device protected by the firewall;
 - in response to determining that the external IP address is not included in the group of IP addresses, determining whether to add the external IP address to the group of IP addresses;
 - in response to determining that the external IP address is to be added to the group of IP addresses, identifying an Internet Service Provider (ISP) associated with the external IP address;
 - determining whether the ISP is included in a group of ISPs maintained by the firewall; and
 - in response to determining that the ISP is not included in the group of ISPs maintained by the firewall, adding the external IP address to the group of IP addresses and adding the ISP to the group of ISPs.
2. The method of claim 1, wherein determining whether to add the external IP address to the group of IP addresses is based on input received via a user interface.
3. The method of claim 2, further comprising causing the user interface to be presented, wherein the user interface indicates the external IP address and the ISP associated with the external IP address.
4. The method of claim 1, further comprising identifying geographic information associated with the external IP address, wherein determining whether to add the external IP address to the group of IP addresses is based on the geographic information associated with the external IP address.

5. The method of claim 1, further comprising causing a user interface to be presented that indicates a number of network packets that have been blocked that are associated with the external IP address.

6. The method of claim 1, further comprising adding the external IP address to a group of IP addresses associated with the firewall that are blocked from transmitting data to the internal device.

7. A system for adding Internet Protocol (IP) addresses to firewalls, the system comprising:

a hardware processor that is programmed to:

receive a network packet that includes an external IP address associated with an external device, wherein the external device is a device not protected by a firewall;

determine whether the external IP address is included in a group of IP addresses maintained by the firewall that are either blocked from receiving data from an internal device protected by the firewall or allowed to receive data from an internal device protected by the firewall;

in response to determining that the external IP address is not included in the group of IP addresses, determine whether to add the external IP address to the group of IP addresses;

in response to determining that the external IP address is to be added to the group of IP addresses, identify an Internet Service Provider (ISP) associated with the external IP address;

determine whether the ISP is included in a group of ISPs maintained by the firewall; and

in response to determining that the ISP is not included in the group of ISPs maintained by the firewall, add the external IP address to the group of IP addresses and adding the ISP to the group of ISPs.

8. The system of claim 7, wherein determining whether to add the external IP address to the group of IP addresses is based on input received via a user interface.

9. The system of claim 8, wherein the hardware processor is further programmed to cause the user interface to be presented, wherein the user interface indicates the external IP address and the ISP associated with the external IP address.

10. The system of claim 7, wherein the hardware processor is further programmed to identify geographic information associated with the external IP address, wherein determining whether to add the external IP address to the group of IP addresses is based on the geographic information associated with the external IP address.

11. The system of claim 7, wherein the hardware processor is further programmed to cause a user interface to be presented that indicates a number of network packets that have been blocked that are associated with the external IP address.

12. The system of claim 7, wherein the hardware processor is further programmed to add the external IP address to a group of IP addresses associated with the firewall that are blocked from transmitting data to the internal device.

13. A non-transitory computer-readable medium containing computer executable instructions that, when executed by a processor, cause the processor to perform a method for adding Internet Protocol (IP) addresses to firewalls, the method comprising:

receiving a network packet that includes an external IP address associated with an external device, wherein the external device is a device not protected by a firewall;

determining whether the external IP address is included in a group of IP addresses maintained by the firewall that are either blocked from receiving data from an internal device protected by the firewall or allowed to receive data from an internal device protected by the firewall;

in response to determining that the external IP address is not included in the group of IP addresses, determining whether to add the external IP address to the group of IP addresses;

in response to determining that the external IP address is to be added to the group of IP addresses, identifying an Internet Service Provider (ISP) associated with the external IP address;

determining whether the ISP is included in a group of ISPs maintained by the firewall; and

in response to determining that the ISP is not included in the group of ISPs maintained by the firewall, adding the external IP address to the group of IP addresses and adding the ISP to the group of ISPs.

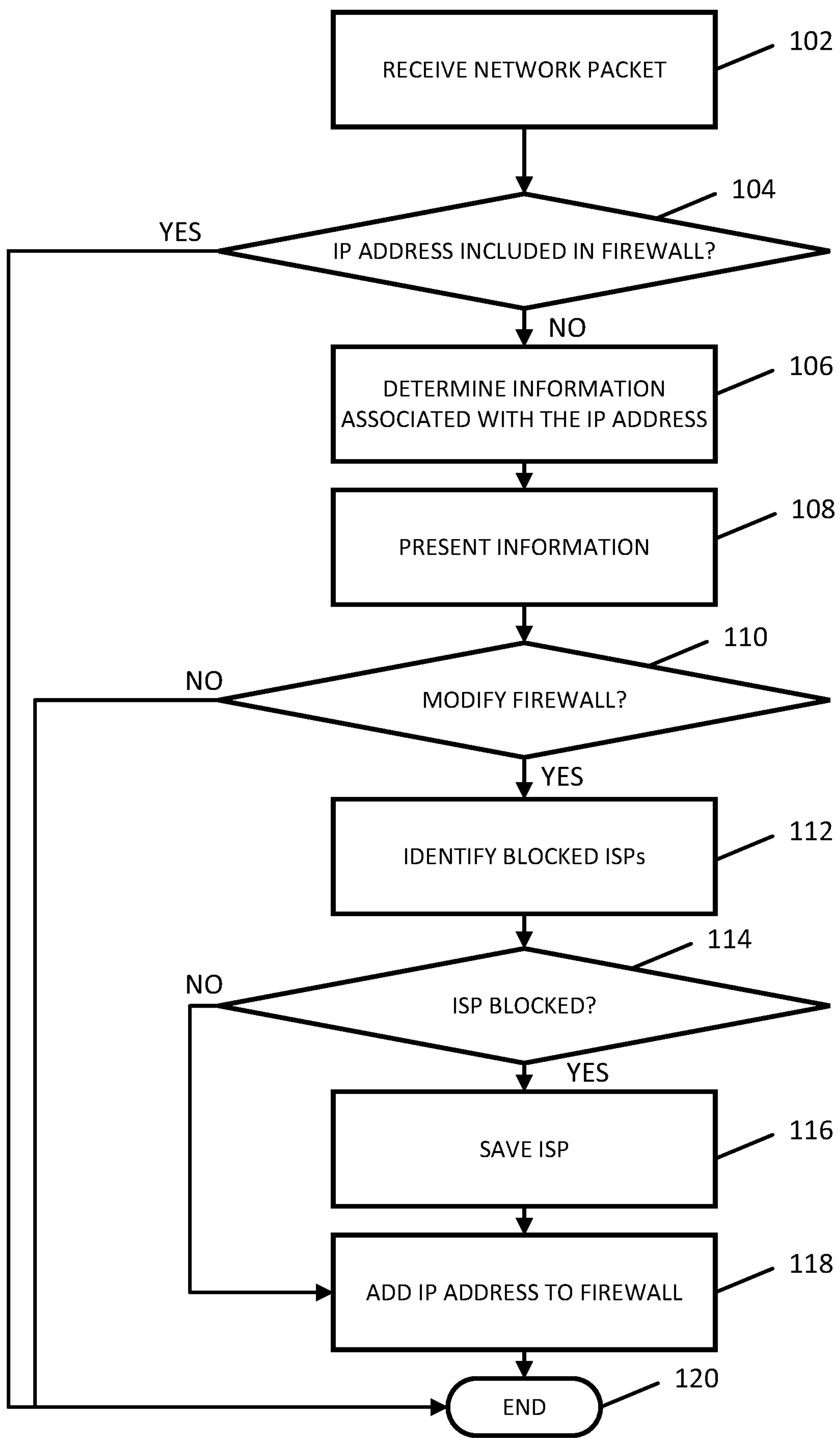
14. The non-transitory computer-readable medium of claim 13, wherein determining whether to add the external IP address to the group of IP addresses is based on input received via a user interface.

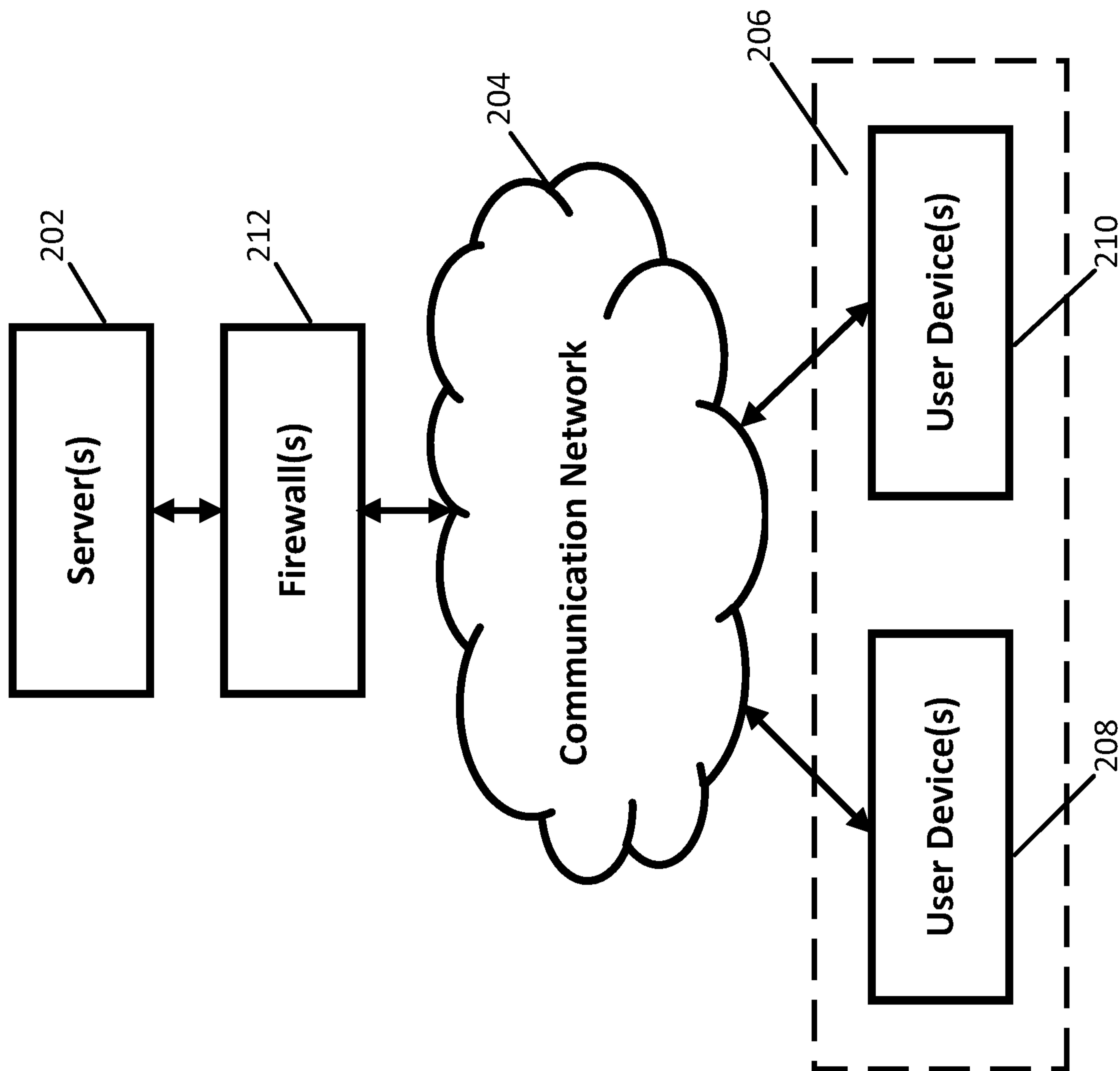
15. The non-transitory computer-readable medium of claim 14, wherein the method further comprises causing the user interface to be presented, wherein the user interface indicates the external IP address and the ISP associated with the external IP address.

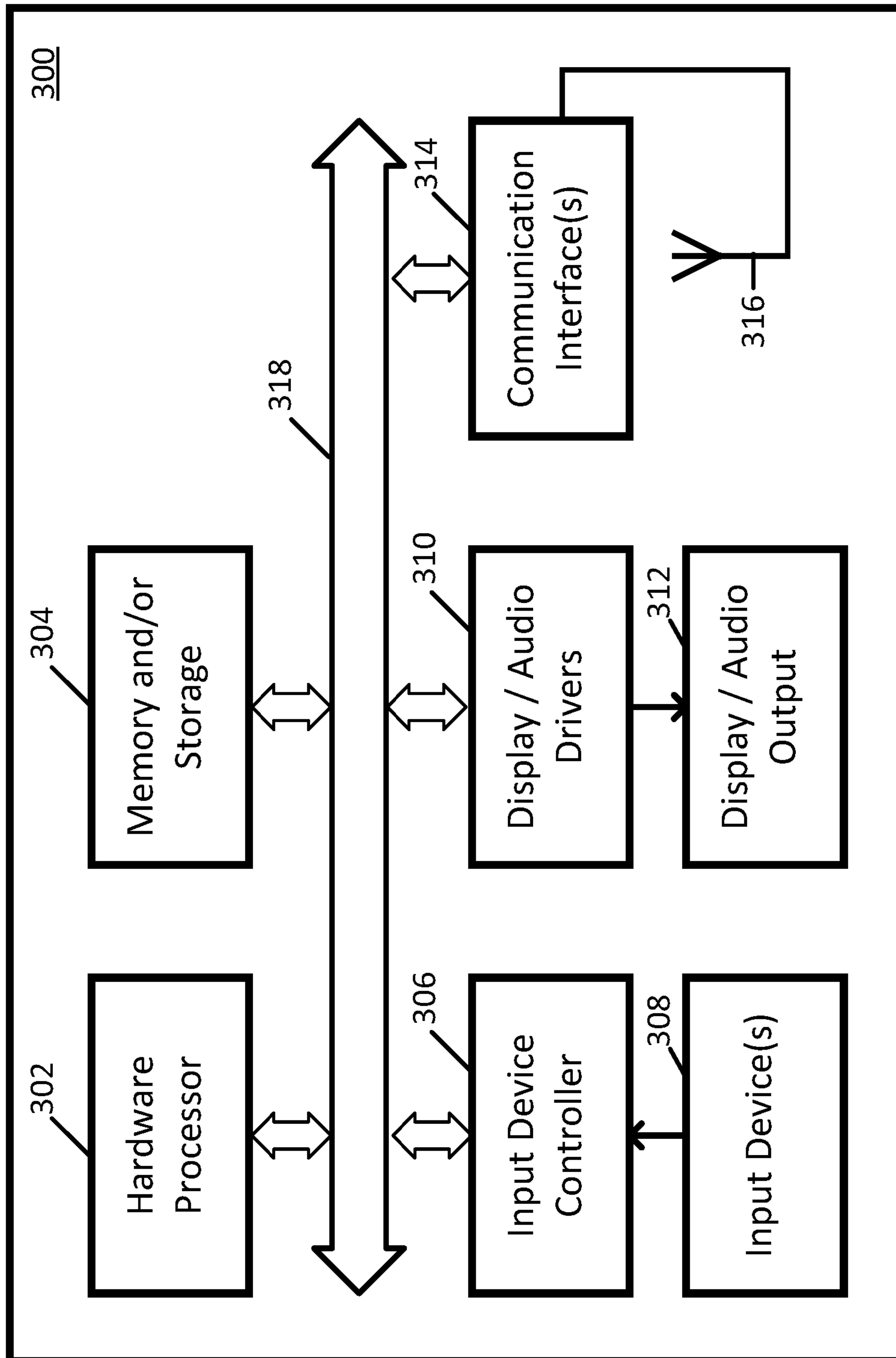
16. The non-transitory computer-readable medium of claim 13, wherein the method further comprises identifying geographic information associated with the external IP address, wherein determining whether to add the external IP address to the group of IP addresses is based on the geographic information associated with the external IP address.

17. The non-transitory computer-readable medium of claim 13, wherein the method further comprises causing a user interface to be presented that indicates a number of network packets that have been blocked that are associated with the external IP address.

18. The non-transitory computer-readable medium of claim 13, wherein the method further comprises adding the external IP address to a group of IP addresses associated with the firewall that are blocked from transmitting data to the internal device.

100**FIG. 1**

200**FIG. 2**

**FIG. 3**

Time:	8/3/17 9:39:23 AM	Protocol:	UDP	400
Internal IP Address:	192.168.1.117:56686	ISP:	ISP NAME A	402
External IP Address:	75.75.75.75:53	Location:	Arlington, US	
Direction:	Inbound	Domain:	domain.net	404
<input type="button" value="VIEW IP"/> <input type="button" value="VIEW DOMAIN"/> <input type="button" value="BLOCK"/>				406
DOMAIN PREVIEW				

FIG. 4A

Double click on an ISP to block or unblock. Once blocked, communications to ISP servers are closed. Some ISPs require a connection to complete a task. You can quickly allow by unblocking the ISP and then block the ISP when you think it is done.

450

<u>STATUS</u>	<u>ISP</u>	<u>CITY, COUNTRY</u>	<u>IP ADDRESS</u>	<u>DOMAIN</u>
Blocked	ISP NAME A	Chicago, US	185.167.110.164	domainA.com
Blocked	ISP NAME A	Chicago, US	185.167.110.162	domainA.com
Blocked	ISP NAME A	Chicago, US	185.167.110.160	domainA.com
Blocked	ISP NAME B	Paris, France	207.137.142.89	domainB.com
Blocked	ISP NAME C	Arlington, US	178.13.62.153	domainC.com
Blocked	ISP NAME D	San Jose, US	192.151.77.130	domainD.com

452

FIG. 4B

500

<u>TIME</u>	<u>SOURCE</u>	<u>DESTINATION</u>	<u>LOCATION</u>	<u>ISP</u>	<u>DOMAIN</u>	<u># BLOCKED</u>
1:04 PM	172.31.98.111:5153	8.8.8.53	Chicago, US	ISP NAME A	domainA.com	1
1:05 PM	172.31.98.111:1252	8.8.4.4:80	Chicago, US	ISP NAME A	domainA.com	10
1:06 PM	172.31.98.111:5288	23.40.17.2:443	Paris, France	ISP NAME B	domainB.com	0
1:07 PM	172.31.98.111:1277	172.45.3.194:80	Arlington, US	ISP NAME C	domainC.com	2
1:08 PM	172.31.98.111:1251	13.215.3.4:1900	San Jose, US	ISP NAME D	domainD.com	4

FIG. 5




FIG. 1