

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
10 November 2005 (10.11.2005)

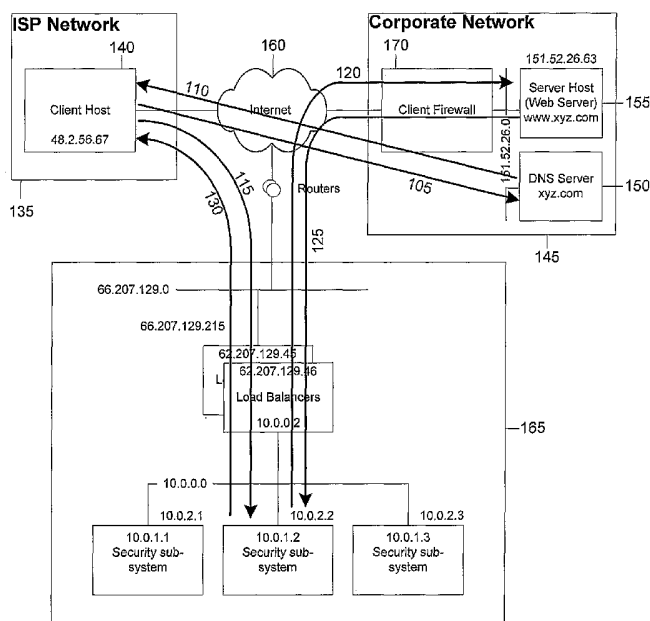
PCT

(10) International Publication Number
WO 2005/107296 A2

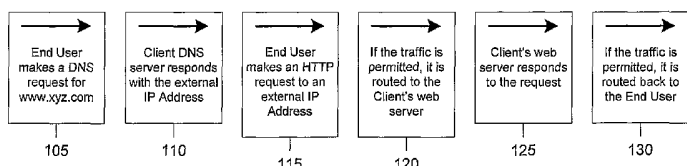
- (51) International Patent Classification⁷: **H04Q 7/28**
- (21) International Application Number: PCT/US2005/011899
- (22) International Filing Date: 8 April 2005 (08.04.2005)
- (25) Filing Language: English
- (26) Publication Language: English
- (30) Priority Data:
60/563,437 19 April 2004 (19.04.2004) US
10/918,171 13 August 2004 (13.08.2004) US
- (71) Applicant (for all designated States except US): **VIGILANTMINDS, INC.** [US/US]; 4736 Penn Avenue, Suite 321, Pittsburgh, PA 15224 (US).
- (71) Applicants and
- (72) Inventors: **DINELLO, Brian** [US/US]; 82 Duncan Station Road, McKeesport, PA 15135 (US). **GRAY, Donald, II.** [US/US]; 30 Knox Avenue, Monessen, PA 15062 (US).
- (74) Agents: **SINGER, James, M.** et al.; Pepper Hamilton LLP, 500 Grant Street, 50th Floor, Pittsburgh, PA 15219 (US).
- (81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.
- (84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI,

[Continued on next page]

(54) Title: NETWORK SECURITY SYSTEM



(57) Abstract: Methods and systems for preventing unacceptable communication requests from being transmitted to a network-accessible service are disclosed. A domain name server for a local network including a network-accessible service returns an address for a network security system remote from the local network in response to a request for the address of the network-accessible service. The network security system processes communication requests directed to the network-accessible service to determine whether the communication request is a network intrusion attempt. If so, the network security system performs a network intrusion prevention technique, such as discarding the communication request, generating an alert or message or storing at least a portion of the communication request. Otherwise, the network security system forwards the communication request to the network-accessible service. A firewall on the local network may discard requests destined for the network-accessible service unless the source address equals a public address of the network security system.



WO 2005/107296 A2



FR, GB, GR, HU, IE, IS, IT, LT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Declarations under Rule 4.17:

- as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii)) for the following designations AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VC, VN, YU, ZA, ZM, ZW, ARIPO patent (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT,

BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)

- as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii)) for all designations
- as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii)) for all designations

Published:

- without international search report and to be republished upon receipt of that report

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

NETWORK SECURITY SYSTEM

RELATED APPLICATIONS AND CLAIM OF PRIORITY

[0001] This application claims priority to and incorporates by reference in its entirety U.S. Provisional Application Serial No. 60/563,437, entitled "Network Security System" and filed April 19, 2004 and U.S. Application Serial No. 10/918,171 filed August 13, 2004 entitled "Network Security System".

TECHNICAL FIELD

[0002] The present application is directed to intrusion detection for computer-based systems. More particularly, the present application is directed to methods and systems for inhibiting intrusion attempts originating from a networked client host from reaching a networked server host.

BACKGROUND

[0003] Computer networks provide connectivity between computing devices on local networks and/or remote networks. A connection between two remote networks typically occurs through a communications network such as the Internet. Communications over the Internet pass through a series of communication links and routers/switches, many of which are located within third-party networks that are also interconnected with the Internet. Thus, communications between two remote networks across the Internet are typically "open" because neither the sender nor the receiver controls the path that the communications traffic travels from source to destination. Rather, the path is controlled by the various providers and devices located on the Internet itself.

[0004] The connectivity between remote networks can be used to allow a client host to utilize a network-accessible service provided by a remote server host. Common network-accessible services include but are not limited to Finger, Echo, SMTP, Telnet, SSH, FTP, DNS, HTTP and HTTPS as well as those services utilizing IP Protocol 50, ICMP, TCP/IP and UDP.

[0005] Because private networks are connected to an open system such as the Internet, security is of great concern when communicating with other private networks via network-accessible services. Often, network administrators install firewall devices, intrusion detection devices, intrusion prevention devices and/or other buffers on a local area network ("LAN") in order to screen and/or filter incoming and/or outgoing content from the local network. Alternatively, system administrators can install firewall, intrusion detection, or intrusion prevention software on a local host within a LAN in order to screen and/or filter incoming and/or outgoing content from the local host. This can require the network administrator and/or the system administrator to install complex and costly equipment and/or software in order to ensure that the local network and/or local host is protected.

[0006] Exemplary network security systems are described in U.S. Patent No. 6,687,831 to *Albaugh et al.*; U.S. Patent No. 6,654,882 to *Froutan et al.*; U.S. Patent No. 6,321,336 to *Applegate et al.*; U.S. Patent No. 5,892,903 to *Klaus*; and U.S. Patent No. 5,557,752 to *Smaha et al.* However, each of these network security systems requires the installation of costly and/or complex equipment and/or software.

[0007] What are needed are improved methods and systems for inhibiting intrusion attempts directed at network-accessible services.

SUMMARY

[0008] Before the present methods, systems and materials are described, it is to be understood that this invention is not limited to the particular methodologies, systems and materials described, as these may vary. It is also to be understood that the terminology used in the description is for the purpose of describing the particular versions or embodiments only, and is not intended to limit the scope of the invention which will be limited only by the appended claims.

[0009] It must also be noted that as used herein and in the appended claims, the singular forms “a,” “an,” and “the” include plural references unless the context clearly dictates otherwise. Thus, for example, reference to a “communication request” is a reference to one or more communications requests and equivalents thereof known to those skilled in the art, and so forth. Unless defined otherwise, all technical and scientific terms used herein have the same meanings as commonly understood by one of ordinary skill in the art. Although any methods, materials, and devices similar or equivalent to those described herein can be used in the practice or testing of embodiments of the invention, the preferred methods, materials, and devices are now described. All publications mentioned herein are incorporated by reference. Nothing herein is to be construed as an admission that the invention is not entitled to antedate such disclosure by virtue of prior invention.

[0010] In an embodiment, a system provides protection against intrusion attempts directed at network-accessible services and methods covering the initiation of the use of the system and the perfection of the intrusion protection provided by the system through a demonstrative base-lining process.

[0011] In an embodiment, the system includes one or more networks, network devices and computing devices that provide firewall, intrusion detection and/or intrusion

prevention protection for a server host on a private network that provides network-accessible service(s) through a connection to an open communications network such as the Internet from intrusion attempts initiated by a client host on a private network connected to an open communications network such as the Internet.

[0012] In an embodiment, the system includes one or more networks, network devices and computing devices that provide firewall, intrusion detection and/or intrusion prevention protection for a client host on a private network connected to an open communications network such as the Internet from intrusion attempts initiated by a server host on a private network that provides network-accessible service(s) through a connection to an open communications network such as the Internet.

[0013] In an embodiment, the system provides intrusion protection for a plurality of client hosts and multiple server hosts providing network-accessible service(s) limited only by the number of public IP addresses available to the service provider hosting the system.

[0014] The system, in conjunction with the methods, may permit the protection of a client host on a private network connected to an open communications network such as the Internet or a server host providing network-accessible service(s) on a private network connected to an open communications network such as the Internet with no hardware or software installation required on the client host, client private network, server host or server private network.

[0015] Through execution of the invented method of initiating protection of a server host providing network-accessible service(s) on a private network connected to an open communications network such as the Internet, the system may intercept the traffic between the client host and server host by having a domain name server, which provides authoritative responses for the server host, advertise the public IP address of the system as the actual public IP address of the server host.

[0016] In an embodiment, the system does not store the intercepted traffic other than to process the traffic. The system may examine the traffic in real time such that communications between the client host and the server host providing the network-accessible service(s) are not perceptibly delayed. In this embodiment, the system is used for many or all network-accessible services, such as interactive network-accessible services.

[0017] The system is capable of providing intrusion protection for any common interactive network-accessible service(s) including but not limited to Finger, Echo, SMTP, Telnet, SSH, FTP, DNS, HTTP, and HTTPS as well as those services utilizing IP Protocol 50, ICMP, TCP/IP, and UDP.

BRIEF DESCRIPTION OF THE DRAWINGS

[0018] Aspects, features, benefits and advantages of the embodiments will be apparent with regard to the following description and accompanying drawings where:

[0019] FIG. 1 is a network diagram depicting an overview of an exemplary physical flow of communication requests from a client host to a server host and communication responses from a server host to a client host through an embodiment of a security system;

[0020] FIG. 2 is a process diagram depicting an exemplary logic flow of communication requests from a client host to a server host through a security system;

[0021] FIG. 3 is a process diagram depicting an exemplary logic flow of communication responses from a server host through a security system;

[0022] FIG. 4 is a process diagram depicting an exemplary method for initiating protection of a server host;

[0023] FIG. 5 is a network diagram depicting an exemplary physical flow of communication requests from a client host to a server host and communication responses from a server host to a client;

[0024] FIG. 6 is a process diagram depicting an exemplary method for configuring a security system to provide protection of a server host;

[0025] FIG. 7 is a process diagram depicting an exemplary logic flow of communication requests from a client host to a server host through a security system;

[0026] FIG. 8 is a process diagram depicting an exemplary logic flow of communication responses from a server host to a client host through the security system; and

[0027] FIG. 9 is a process diagram depicting an exemplary method for refining the configuration of a security system through a demonstrative base-lining process.

DETAILED DESCRIPTION

[0028] Embodiments of the present invention include methods and systems for inhibiting or preventing intrusion attempts from occurring between a client host on a private network connected to an open communications network such as the Internet and a server host providing network-accessible service(s) on a private network connected to the open communications network. In an embodiment, the present invention may prevent intrusion attempts without the need for substantial additional computer software or hardware devices on the private networks, the client host or the server host.

[0029] FIGs. 1-3 illustrate an exemplary communication process between a client host **140** on a private network connected to an open communications network such as the Internet **160** and a server host **155** providing network-accessible service(s) on a private network connected to the open communications network **160**. The client host **140** may be part of a first private network such as an Internet service provider (ISP) network **135**. The server host **155** may be a web server that is part of a second private network such as a corporate network **145**.

[0030] In order to communicate with a network-accessible service on the server host 155, the client host 140 may transmit a request 105 (step 205 in FIG. 2) to an authoritative domain name server 150 for the server host 155 to resolve its public IP address. The authoritative domain name server 150 may respond 110 (step 210 in FIG. 2) with a public IP address (e.g., 66.207.129.215 in FIG. 1) for a separate security system or network 165 assigned to protect the server host 155 providing the network-accessible service instead of, as is typically done, the true public IP address of the server host 155 (e.g., 151.52.26.63 in FIG. 1).

[0031] The client host 140 may then transmit its communication request 115 (step 215 in FIG. 2). The communication request 115 (step 215 in FIG. 2) is transmitted to the security system 165 because of the IP address provided by the DNS server. The security system 165 may perform a series of processing steps (220 in FIG. 2) to determine whether the communication request 115 is an intrusion attempt. If the communication request 115 is determined to be non-intrusive, the security system 165 may forward the communication request 120 (step 225 in FIG. 2) to the network-accessible service on the server host 155. The client firewall 170 permits the communication request (step 230 in FIG. 2) to enter the corporate network 145 because it comes from a public IP address of the security system 165. The server host 155 then receives the communication request 120 (step 235 in FIG. 2).

[0032] The server host 155 may perform any necessary processing and generate a response 125 to the forwarded communication request 120, if required. If generated, the response 125 may first be sent to the security system 165 (step 305 in FIG. 3) since the forwarded communication request 120 originated from the security system 165. The security system 165 may receive the response 125 (step 310 in FIG. 3) and perform a series of processing steps (315 in FIG. 3) designed to determine whether the response 125 is an

intrusion attempt. If the response 125 is determined to be non-intrusive, the security system 165 may then forward the response 130 (step 320 in FIG. 3) to the client host 140, which processes the response 130, 325. In an embodiment, the server host 155 transmits the response 125 directly to the client host 140.

[0033] In an embodiment, some or all of the processing steps performed by the security system 165 between the original communication request 115 and the forwarded communication request 120 and/or between the response 125 and the forwarded response 130 occur in real time without storing the communications requests 115 and 120 or the responses 125 and 130 other than as required for real time processing. Thus, the security system 165 may permit interactivity between the client host 140 and server host 155 without any perceptible delay in communication between the two systems. This allows the security system 165 to be used for providing intrusion protection to interactive and/or batch network-accessible services, including but not limited to Finger, Echo, SMTP, Telnet, SSH, FTP, DNS, HTTP and HTTPS, as well as those services utilizing IP Protocol 50, ICMP, TCP/IP and UDP.

[0034] In an alternate embodiment, the devices of the security system 165 may be located on the corporate network 145. In such an embodiment, the devices of the security system 165 perform the series of processing steps (220 in FIG. 2) to determine whether the communication request 115 is an intrusion attempt and forward the communication request 120 (steps 225 and 230 in FIG. 2) to the network-accessible service on the server host 155 if the communication request 115 is non-intrusive. Likewise, the devices of the security system 165 may perform the series of processing steps (315 in FIG. 3) to determine whether the response 125 is an intrusion attempt and forward the response 130 (step 320 in FIG. 3) to the client host 140 via the communications network 160 if the response 130 is non-intrusive.

[0035] In an alternate embodiment, the devices of the security system 165 are located on the client network 135. In such an embodiment, the devices of the security system 165 perform the series of processing steps 220 to determine whether the communication request 115 is an intrusion attempt and forward the communication request 120 (steps 225 and 230 in FIG. 2) via the communications network 160 to the network-accessible service on the server host 155 if the communication request 115 is non-intrusive. Likewise, the devices of the security system 165 may perform the series of processing steps (315 in FIG. 3) to determine whether the response 125 is an intrusion attempt and forward the response 130, (step 320 in FIG. 3) to the client host 140 if the response 130 is non-intrusive.

[0036] In an embodiment, the security system 165 may maintain an event log of the requests 115 and responses 125 that pass through the security system 165. In an embodiment, the event log may maintain only a partial copy of a request 115 or a response 125.

[0037] FIGs. 1 and 4 illustrate a method of configuring the security system 165 to initiate network intrusion protection of a server host 155 providing network-accessible service(s), and the resultant configuration within the server host 155. Initially, an owner of a server host 155 providing a network-accessible service(s) may contact 405 a service provider hosting the security system 165 to provide network intrusion protection. The owner may communicate (step 410) the public IP address, IP protocol(s) and IP port(s) of the server host 155 to the service provider. The service provider may assign (step 415) a public IP address within the public network segment of the security system 165 (e.g., 66.207.129.215 in FIG. 1) to accept communication requests for and/or responses from the specified server host 155. The service provider may execute (step 420) the "Internal Host Setup Process" upon the security system, as shown in FIG. 6 and described in more detail below, to configure the

security system **165** to perform intrusion protection for the specified server host **155** and its network-accessible services.

[0038] The service provider may then communicate (step **425**) the assigned public IP address (66.207.129.215) to the owner of the server host **155**. The owner of the server host **155** may update (step **430**) the configuration of its domain name server **150** such that the "A" record for the server host **155** indicates the service provider provisioned public IP address (66.207.129.215) rather than the public IP address of the server host **155** (e.g., 151.52.26.63 in FIG. 1). The nature of the domain name server infrastructure dictates that this change will propagate (step **435**) through the entire communications network **160** within a specified time period, such as 72 hours.

[0039] In an embodiment, the owner of the server host **155** may configure a perimeter firewall **170** to restrict inbound network traffic with a destination address corresponding to the public IP address of the server host **155** (e.g., 151.52.26.63) to traffic having a source address corresponding to the public IP address assigned by the security system **165** (step **440**). Such an embodiment may provide a heightened level of network intrusion protection.

[0040] By providing network intrusion protection between the client host **140** and the server host **155**, the security system **165** inhibits or prevents viruses, worms, directed intrusion attempts and other malicious traffic from reaching and/or being delivered from the server host **155**. In addition, by being loosely coupled with both the private network **135** of the client host **140** and the private network **145** of the server host **155** through an open communications network **160**, the security system **165** may provide network intrusion protection for multiple client hosts **140** belonging to multiple private networks **135** and multiple server hosts **155** belonging to multiple private networks **145** simultaneously. As

such, economies of scale may be achieved since no additional devices or computing software are required on the client host **140**, the client host's private network **135**, the server host **155** or the server host's private network **145**.

[0041] FIG. 5 illustrates a detailed network diagram of an embodiment of a security system **165** and the packet translations that occur when the security system **165** is used to provide intrusion protection between a client host on a first private network connected to an open communications network such as the Internet and a server host providing network-accessible service(s) on a second private network connected to the open communications network. The client host **505** is part of a first private network such as an ISP network **510** connected to an open communications network **515**. The first private network may include network devices, such as routers, firewalls, proxies, etc., that connect the client host **505** to the ISP network **510**. These network devices may perform address translations, routing and/or other communication techniques and functions. Regardless of the intermediary network devices and intermediary network processing, the client host **505** may be reachable via a public IP address (e.g., 48.2.56.67 in FIG. 5). The public IP address may allow the client host **505** to communicate over the open communications network **515**.

[0042] The server host **525** may be part of a second private network, such as a corporate network **520** connected to the open communications network **515**. The second private network may include network devices, such as routers, firewalls, proxies, etc., that connect the server host **525** to the corporate network **520**. These network devices may perform address translations, routing and/or other communication techniques and functions. Regardless of the intermediary network devices and intermediary network processing, the server host **525** may be reachable via a public IP address (e.g., 151.52.26.63 in FIG. 5). The public IP address may allow the server host **525** to communicate over the open communications network **515**.

[0043] FIGs. 5 and 6 illustrate a method of configuring the security system 165 to initiate network intrusion protection of a server host 525 providing network-accessible service(s) and the resultant configuration within the security system 165. The security system 165 may be part of a private network connected to an open communications network such as the Internet 515. Referring to FIG. 5, the security system may have a private network that includes a public network segment 535 having a plurality of public IP addresses and an internal network segment 545 having a plurality of private IP addresses. In an embodiment, the public IP addresses may include a public IP address associated with the public IP address of a server host 525. One public IP address (e.g., 66.207.129.215 in FIG. 5) may provide network intrusion protection for the server host 525. Accordingly, a one-to-one relationship may exist between a public IP address of the server host 525 (e.g., 151.52.26.63 in FIG. 5) and the assigned public IP address (66.207.129.215).

[0044] The private IP addresses for use on the private network segment 545 within the security system may be assigned a private IP address 605 (e.g., 10.0.2.1, 10.0.2.2 and 10.0.2.3 550 may each be assigned to a security sub-system 555 within the security system 165). As such, a one-to-many relationship may exist between the public IP address (66.207.129.215) and the private IP addresses 550 (10.0.2.1, 10.0.2.2 and 10.0.2.3).

[0045] Within the security system 165, the assigned public IP address (66.207.129.215) may exist as a virtual IP address assigned to and shared between IP network load balancers 540. The load balancers 540 may provide address translation and routing between the public network segment 535 within the security system 165 and the private network segment 545 within the security system. More specifically, the network load balancers 540 may perform 610 network address translation and routing between the virtual

public IP address (66.207.129.215) and the private IP addresses **550** (10.0.2.1, 10.0.2.2 and 10.0.2.3).

[0046] The security system **165** may include the above described network communications framework and a security sub-system **555**. The security sub-system **555** may include computing devices that perform load-balancing and failover protection. The computing devices may be configured with multiple computer software programs, referred to herein as “modules,” which provide network firewall functionality, network intrusion prevention (IPS) functionality and/or network intrusion detection (IDS) functionality.

[0047] Each computing device may operate in one of two modes: passive and active. When the computing devices are passive, no network intrusion prevention functionality is performed. However, network intrusion protection may still be realized through the network firewall module and the intrusion detection module. When the computing devices are active, full network intrusion protection may be provided including network intrusion prevention. Each assigned private IP address **550** (10.0.2.1, 10.0.2.2 and 10.0.2.3) may be assigned **615** to a particular security sub-system **555** computing device.

[0048] The network firewall modules of the security sub-system **555** may perform TCP/IP layer 3 network traffic filtering based on, for example, source and/or destination IP addresses, source and/or destination TCP/IP ports, and IP protocols. The network firewall modules may further perform **620** network address translation between private IP addresses. In addition, a firewall module may be implemented as an Ethernet router device. In other words, the firewall module may perform “inbound” and “outbound” processing using, for example, two Ethernet network interface controllers that route traffic between “inbound” and “outbound” interfaces. As such, the firewall module may perform “inbound” processing, including filtering and network address translation; “outbound” processing, including filtering

and network address translation; and additional "in between" processing, including forwarding IP packets to an intrusion prevention module for examination.

[0049] Each firewall module of each computing device within the security sub-system may be configured **620** to allow communication requests using the specified IP protocol(s), and/or TCP/IP port(s) for the protected network-accessible service(s) provided by the protected server host **525**. In addition, each firewall module of each computing device may be configured **620** to perform network address translation between an assigned private IP address (e.g., 10.0.2.2) **550** and the public IP address (151.52.26.63) of the protected server host **525**.

[0050] In an embodiment, if the firewall module receives an IP packet that does not meet its filtering criteria for allowed network traffic, the IP packet is discarded. In an embodiment, the discard event is logged. In an alternate embodiment, at least a portion of the IP packet is saved. In an embodiment, an alert is sent to a system administrator or a network administrator. In an embodiment, a message is transmitted to the sender of the IP packet.

[0051] The network intrusion prevention module of the security sub-system **555** may perform, for example, TCP/IP layer 3 through TCP/IP layer 7 packet examinations. The network intrusion prevention module may reassemble IP packets that have been fragmented, whether intentionally to mask the contents of the IP packet or because of IP packet size limitations within any of the network devices through which the IP packet traversed. The network intrusion prevention module may then examine characteristics of the IP packet including, for example, various packet header values and/or the contents of the packet data payload. These characteristics and packet data payload may then be compared with a database of known network intrusion attempt signatures. If a match exists, the mode (passive v. active) of the computing device on which the network intrusion prevention module resides may determine how the IP packet is handled **625**. If the computing device is passive, the

matched IP packet may not be discarded. However, the fact that the IP packet would have been discarded had the computing device been active and data including, for example, at least a partial copy of the IP packet header and IP packet data payload may be logged. If the computing device is active, the matched IP packet may be discarded. Moreover, the fact that the IP packet was discarded and data including, for example, at least a partial copy of the IP packet header and IP packet data payload may be logged. If a match does not exist, the IP packet may be forwarded to its destination.

[0052] The network intrusion detection module of the security sub-system **555** may similarly be capable of performing, for example, TCP/IP layer 3 through TCP/IP layer 7 packet examinations. The network intrusion detection module may first reassemble IP packets that have been fragmented, whether intentionally to mask the contents of the IP packet or because of IP packet size limitations within any of the network devices through which the IP packet traversed. The network intrusion detection module may then examine characteristics of the IP packet including, for example, various packet header values and/or the contents of the packet data payload. This examination may occur because the intrusion detection module “listens” to all IP traffic traversing the routed Ethernet interface of the computing device. These characteristics and packet data payload may be compared with a database of known network intrusion attempt signatures. If a match exists, the fact that the IP packet was matched and data including, for example, at least a partial copy of the IP packet header and/or the IP packet data payload may be logged. If a match does not exist, the IP packet may be permitted to continue toward its destination.

[0053] Referring to FIG. 5, a communication request **560** may be transmitted from a client host **505** with a public IP address (e.g., 48.2.56.67 as in FIG. 5). The communication request **560** may be directed, by the end-user of the client host **505**, to a protected network-accessible service provided by a server host **525** with a public IP address (e.g., 151.52.26.63

as in FIG. 5). The security system may intercept the request because of the special configuration of the domain name server that provides authoritative responses for the server host **525**. As such, this communication request **560** has a source IP address equal to the public IP address of the client host (48.2.56.67) and a destination IP address equal to the public IP address assigned for the protection of the server host **525** to the security system (e.g., 66.207.129.215 as in FIG. 5).

[0054] Referring to FIG. 7, the network load balancers **540** of the security system may receive **705** the communication request **560**. The network load balancers **540** may translate the destination IP address to one of the private IP addresses **710** assigned for the protection of the server host **525** to a specific computing device within the security system's security sub-system **555** (e.g., 10.0.2.2 as in FIG. 5). The communication request **565** may then be routed **715** to the specific computing device within the security sub-system.

[0055] The computing device may perform intrusion protection processing including, for example, the firewall module **720** making a determination **725** of whether the communication request **565** is permitted based on the firewall module's filtering criteria. If the communication request **565** is not permitted, the fact that it is not permitted may be logged **770**, and the communication request may be discarded **775**. In an alternate embodiment, the computing device generates an alert if the request **565** is not permitted. In an alternate embodiment, the computing device generates a message to the sender if the request **565** is not permitted. In an alternate embodiment, the computing device saves at least a portion of the communication request **565** if the request is not permitted.

[0056] If the communication request **565** is permitted, it may be presented to the intrusion prevention module **730** for examination. The intrusion prevention module may determine **735** whether the communication request **565** is permitted based on whether or not

it matches one of a plurality of intrusion prevention signatures. If the communication request 565 matches an intrusion prevention signature, the fact that it matched and data including, for example, at least a partial copy of the communication request's IP packet header and/or the IP packet data payload may be logged 780. A determination 785 of the operating mode of the current security sub-system computing device may be made. If the current computing device is active, the communication request 565 may be discarded 790. Alternately, at least a portion of the communication request 565 may be saved. Alternately or additionally, an alert and/or a message may be generated. If the current computing device is passive, the communication request 565 may be allowed to pass to the "outside" interface of the routed Ethernet connection maintained by the firewall module of the security sub-system 555.

[0057] During the traversal of the routed Ethernet interface, the intrusion detection module 740 may examine the communication request 565 to determine 745 whether the communication request matches one of a plurality of intrusion detection signatures. If the communication request 565 matches an intrusion detection signature, the fact that it matched and data including, for example, at least a partial copy of the communication request's IP packet header and IP packet data payload may be logged 795. If the communication request 565 was not discarded during the prior processing, upon reaching the "outside" interface of the routed Ethernet connection, the firewall module may translate 750 the source IP address of the communication request to the private IP addresses assigned for the protection of the server host 525 to the current computing device within the security system's security sub-system 555 (10.0.2.2).

[0058] The firewall module may then translate 755 the destination IP address of the communication request to the public IP address of the protected server host 525 (151.52.26.63). The computing device may then route the communication request to the

network load balancers **540**, which may translate **765** the source IP address of the communication request **570** to the public IP addresses assigned for the protection of the server host **525** to the security system (66.207.129.215). The communication request **575** may then be routed normally through the open network **515** to the protected server host **525**.

[0059] Referring to FIG. 5, a response **595** to a previous communication request **575** may be transmitted from a protected server host **525** having an IP address (e.g., 151.52.26.63). The response **595** may be directed towards the security system with a destination IP address of, for example, 66.207.129.215. This may occur because the communication request **575** originated from the security system **165**. As such, the response **595** may have a source IP address equal to the IP address of the server host **525** (151.52.26.63) and a destination IP address equal to the public IP address assigned for the protection of the server host **525** to the security system **165** (66.207.129.215).

[0060] Referring to FIG. 8, the network load balancers **540** of the security system may receive **805** the response **595** and may translate **810** its destination IP address to one of the private IP addresses assigned for the protection of the server host **525** to a specific computing device within the security system's security sub-system **555** (e.g., 10.0.2.2). The response **590** may be routed **815** to the specific computing device.

[0061] The computing device may perform intrusion protection processing including, for example, the firewall module **820** making a determination **825** of whether the response **590** is permitted based on the firewall module's filtering criteria. If the response **590** is not permitted, the fact that it is not permitted may be logged **870**, and the response may be discarded **875**. In an alternate embodiment, the computing device generates an alert if the response **590** is not permitted. In an alternate embodiment, the computing device generates a

message to the sender if the response 590 is not permitted. In an alternate embodiment, the computing device saves at least a portion of the response 590 if it is not permitted.

[0062] If the response 590 is permitted, it may be presented to the intrusion prevention module 830 for examination. The intrusion prevention module may determine 835 whether the response 590 is permitted based on whether or not it matches one of a plurality of intrusion prevention signatures. If the response 590 matches an intrusion prevention signature, the fact that it matched and data including, for example, at least a partial copy of the response's IP packet header and/or the IP packet data payload may be logged 880. A determination 885 of the operating mode of the current security sub-system computing device may be made. If the current computing device is active, the response 590 may be discarded 890. Alternately, at least a portion of the response 590 may be saved. Alternately or additionally, an alert and/or a message may be generated. If the current computing device is passive, the response 590 may be allowed to pass to the "outside" interface of the routed Ethernet connection maintained by the firewall module of the security sub-system 555.

[0063] During the traversal of the routed Ethernet interface, the intrusion detection module 840 may examine the response 590 to determine 845 whether the response matches one of a plurality of intrusion detection signatures. If the response 590 matches an intrusion detection signature, the fact that it matched and data including, for example, at least a partial copy of the response's IP packet header and IP packet data payload may be logged 895. If the response 590 was not discarded during the prior processing, upon reaching the "outside" interface of the routed Ethernet connection, the firewall module may translate 850 the source IP address of the response to the private IP addresses assigned for the protection of the server host 525 to the current computing device within the security system's security sub-system 555 (10.0.2.2).

[0064] The firewall module may then translate **855** the destination IP address of the response to the public IP address of the client host **505** (48.2.56.67). The computing device may then route the response **585** to the network load balancers **540**, which may translate **865** the source IP address of the response to the public IP addresses assigned for the protection of the server host **525** to the security system (66.207.129.215). The response **580** may then be routed normally through the open network **515** to the client host **505**.

[0065] FIGs. 1 and 9 illustrate a method of utilizing the security system **165** to refine and/or perfect the network intrusion protection of a server host **155** providing network-accessible service(s) and the resultant configuration within embodiments of the security system **165**. The service provider may perform **905** the Initial Host Setup method, as shown in FIG. 6, to provide network intrusion protection to a server host **155** providing a network-accessible service(s). After this initial setup, the computing device within the security subsystem of the security system **165** may operate in passive mode. Communication requests and responses to communication requests may then be allowed to flow **910** through the security system **165**. The security system may log **915** all potential network intrusion attempts directed at the protected network-accessible service(s) that would have been blocked had the security system been configured in active mode. In addition, the owner of the protected server host **155** may review the logs **920** to determine potential false positives (i.e., communication requests and responses that the security system **165** determines to be intrusion attempts that are not actually intrusion attempts). The service provider may adjust **925** the intrusion prevention signatures and/or intrusion detection signatures (combined, the network intrusion attempt signatures) to eliminate or reduce the occurrence of such false positives. This learning process may iterate until the owner of the protected server host **155** is comfortable with the actions that would be performed by the security system when operating

in active mode. Upon reaching this comfort level, the service provider may configure 930 the computing device within the security sub-system to operate in active mode in order to provide a heightened level of network intrusion protection to the server host 155.

[0066] It is to be understood that the invention is not limited in its application to the details of construction and to the arrangements of the components set forth in this description or illustrated in the drawings. The invention is capable of other embodiments and of being practiced and carried out in various ways. Hence, it is to be understood that the phraseology and terminology employed herein are for the purpose of description and should not be regarded as limiting.

[0067] As such, those skilled in the art will appreciate that the conception upon which this disclosure is based may readily be utilized as a basis for the designing of other structures, methods, and systems for carrying out the several purposes of the present invention. It is important, therefore, that the description be regarded as including such equivalent constructions insofar as they do not depart from the spirit and scope of the present invention.

CLAIMS

What is claimed is:

1. A method of preventing unacceptable communication requests from reaching a local network, comprising:

receiving, by a domain name server on a local network, an address request from a client device for a network address of a computing device on the local network;

transmitting, by the domain name server, an address for a network security system to the client device;

receiving, by the network security system, a communication request from the client device containing information destined for the computing device;

determining whether the communication request is permitted; and

if the communication request is permitted, forwarding the communication request from the network security system to the computing device.

2. The method of claim 1 wherein the network security system is remote from both the local network and the client device.

3. The method of claim 1 wherein determining whether the communication request is permitted is performed in real time.

4. The method of claim 1 wherein determining whether the communication request is permitted comprises performing traffic filtering based on one or more of the following:

a source address for the communication request;

a destination address for the communication request;

a source port for the communication request;
a destination port for the communication request; and
a protocol for the communication request.

5. The method of claim 1 wherein determining whether the communication request is permitted comprises performing network address translation.

6. The method of claim 1 wherein determining whether the communication request is permitted comprises:

examining the communication request, wherein the communication request comprises one or more packets;

examining characteristics for the communication request, wherein the characteristics include one or more of a header for each packet and packet data for the communication request;

comparing the characteristics with information stored in a database containing known network intrusion attempt signatures; and

if the characteristics match a known network intrusion attempt signature, performing a network intrusion prevention technique.

7. The method of claim 6 wherein performing a network intrusion prevention technique comprises:

storing at least a partial copy of the packet; and

storing a designation that the characteristics matched the known network intrusion attempt signature.

8. The method of claim 6 wherein performing a network intrusion prevention technique comprises at least one of discarding the packet, generating an alert, and generating a message to the client device.

9. The method of claim 1, further comprising:
transmitting, by the computing device, a response to the communication request;
receiving the response at the network security system;
determining whether the response is permitted; and
if the response is permitted, forwarding the response from the network security system to the client device.

10. The method of claim 9 wherein determining whether the response is permitted comprises performing traffic filtering based on one or more of the following:

- a source address for the response;
- a destination address for the response;
- a source port for the response;
- a destination port for the response; and
- a protocol for the response.

11. The method of claim 9 wherein determining whether the response is permitted comprises performing network address translation.

12. The method of claim 9 wherein determining whether the response is permitted comprises:

examining the response, wherein the response comprises one or more packets;

examining characteristics for the response, wherein the characteristics include one or more of a header for each packet and packet data for the response;

comparing the characteristics with information stored in a database containing known network intrusion attempt signatures; and

if the characteristics match a known network intrusion attempt signature, performing a network intrusion prevention technique.

13. The method of claim 12 wherein performing a network intrusion prevention technique comprises:

storing at least a partial copy of the packet; and

storing a designation that the characteristics matched the known network intrusion attempt signature.

14. The method of claim 12 wherein performing a network intrusion prevention technique comprises discarding the packet.

15. The method of claim 12 wherein performing a network intrusion prevention technique comprises generating an alert.

16. The method of claim 12 wherein performing a network intrusion prevention technique comprises generating a message to the computing device.

17. The method of claim 1, further comprising:
transmitting, by the computing device, a response to the communication request; and
receiving the response at the client device.
18. A method for performing network security, comprising:
receiving, by a local network, a request from a client device for a network destination address for a computing device on the local network;
transmitting a public address for a network security system to the client device in response to the request, wherein the network security system is remote from the local network and the client device;
receiving a packet at the network security system, wherein the packet has a source address equal to an address for the client device, a destination address equal to the public address for the network security system, a packet header, and packet data;
determining whether the packet is permitted;
if the packet is permitted:
translating the destination address for the packet to an address for the computing device,
translating the source address for the packet to the public address for the network security system, and
transmitting the packet to the translated destination address; and
if the packet is not permitted, performing a network intrusion prevention technique.

19. The method of claim 18 wherein determining whether the packet is permitted comprises:

translating the source address for the packet to the public address for the network security system;

translating the destination address for the packet to a private address for the network security system;

transmitting the packet to the destination address;

examining characteristics for the packet, wherein the characteristics include one or more of the packet header and the packet data;

comparing the characteristics with information stored in a database containing known network intrusion attempt signatures;

if the characteristics match a known network intrusion attempt signature, designating that the packet is not permitted; and

if the characteristics do not match any known network intrusion attempt signature:

translating the source address for the packet to the private address for the network security system,

translating the destination address for the packet to the public address for the network security system,

transmitting the packet to the translated destination address, and

designating that the packet is permitted.

20. The method of claim 18 wherein performing a network intrusion prevention technique comprises one or more of the following:

discarding the packet;

generating an alert;
generating a message to the client device;
storing a designation that the packet is not permitted; and
storing at least a portion of the packet in a database.

21. A system for preventing unacceptable communication requests from reaching a network-accessible service, comprising:

one or more servers, wherein each server has a public address associated with a network-accessible service and a private address; and

one or more security sub-systems, wherein each security sub-system has a private address;

wherein each server includes software that instructs the server to receive a communication request having a destination address intended for the network-accessible service at the public address and to translate the destination address of the communication request to the private address of a security sub-system;

wherein each security sub-system includes software that instructs the security sub-system to analyze communication requests received from a server and to forward the communication request to the network-accessible service, via a server, only if the communication request meets predetermined criteria; and

wherein each server further includes software that instructs the server to translate the destination address of criteria-meeting communication requests to an address for the network-accessible service.

22. The system of claim 21 wherein the servers and the security sub-systems are remote from the network-accessible service.

23. A system for preventing unacceptable communication requests from reaching a network-accessible service, the system comprising:

a network security system operably connected to a communication network;

and

a server network operably connected to the communication network;

wherein the network security system and server network are remote from each other;

wherein the network security system has a public network address, wherein the server network includes a firewall and a network-accessible service, wherein the network-accessible service has a network address, and wherein the firewall discards communication requests having a destination address equal to the network address of the network-accessible service and a source address that is not equal to the public network address of the network security system.

24. A system for preventing unacceptable communication requests from reaching a network-accessible service, the system comprising:

a server network that server network includes a domain name server, a server host, and a firewall, wherein the server host includes a network-accessible service; and

a network security system in remote communication with the server network via a communication network, wherein the network security system includes one or more load-balancing servers and one or more security sub-systems;

wherein if the domain name server receives a request from a remote client host for a network address for the network-accessible service, the domain name server transmits a network address for a load-balancing server associated with the network-accessible service to the client host.

25. The system of claim 24 wherein the network security subsystem receives a client communication request for the network-accessible service from the client host, analyzes the client communication request, and transmits the client communication request to the network-accessible service if the client communication request is permitted.

26. The system of claim 24 wherein the network security subsystem receives a response from the network-accessible service, analyzes the response, and transmits the response to the client host if the response is permitted.

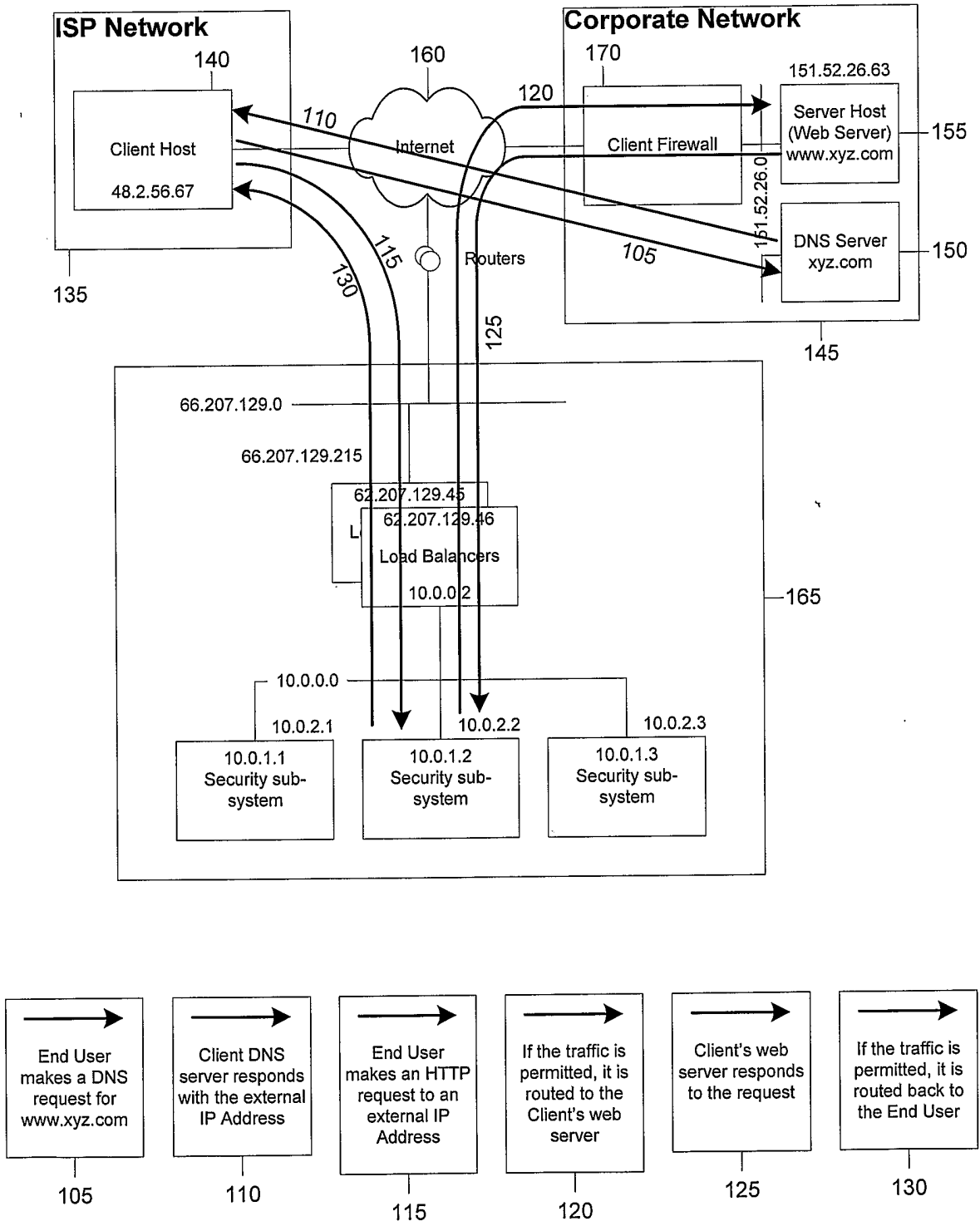


FIG. 1

2/9

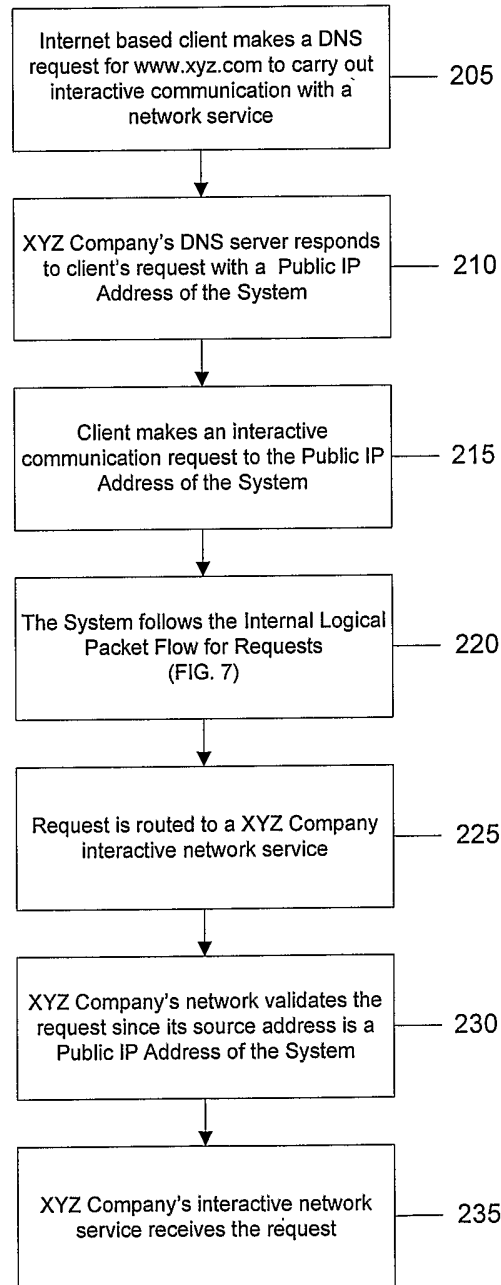


FIG. 2

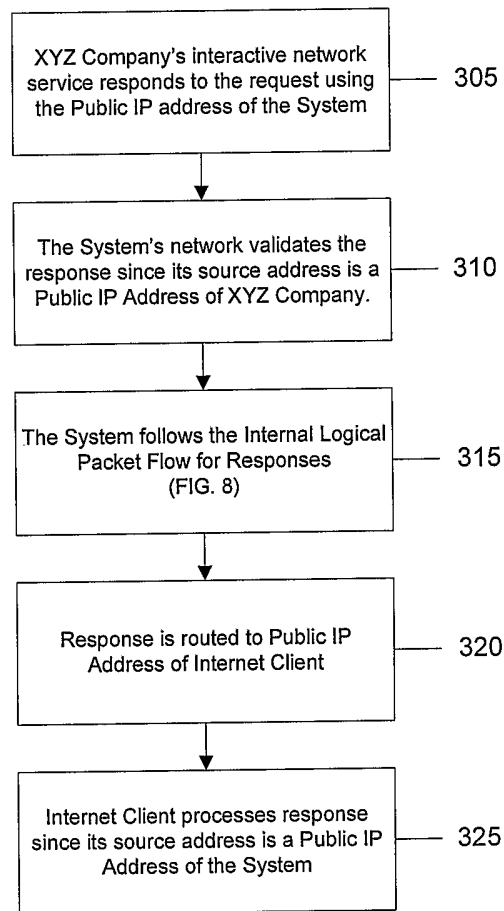


FIG. 3

4/9

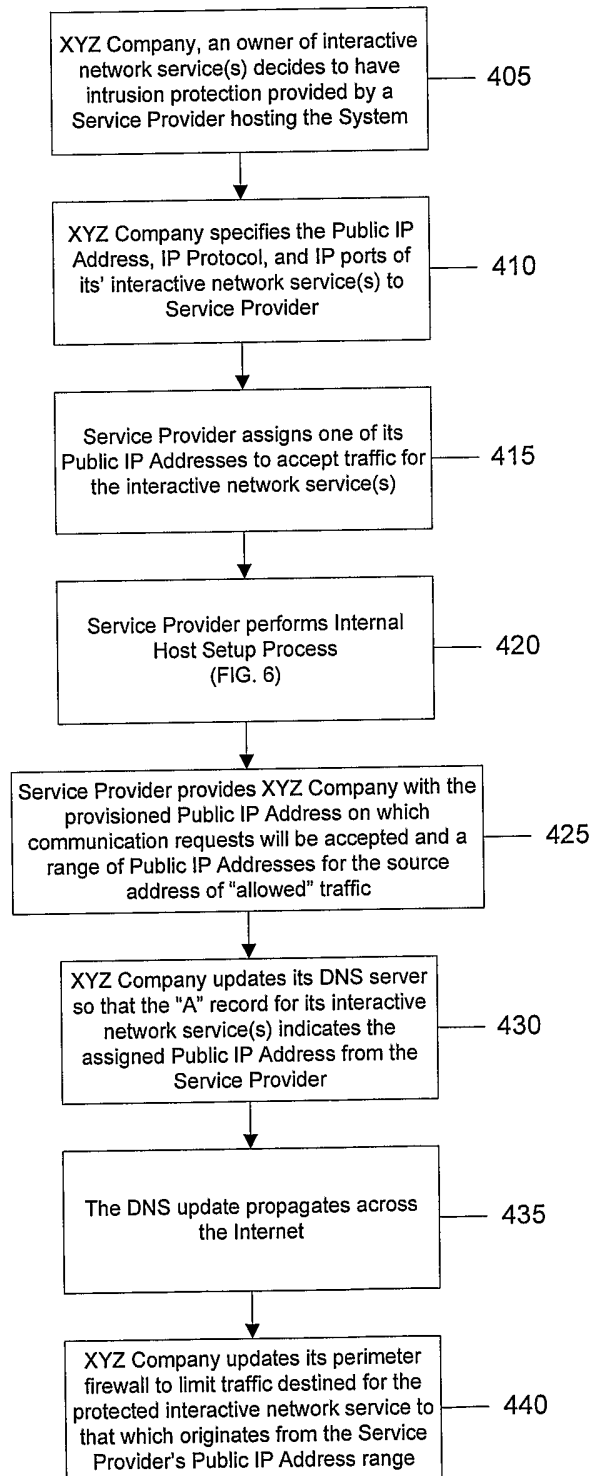


FIG. 4

5/9

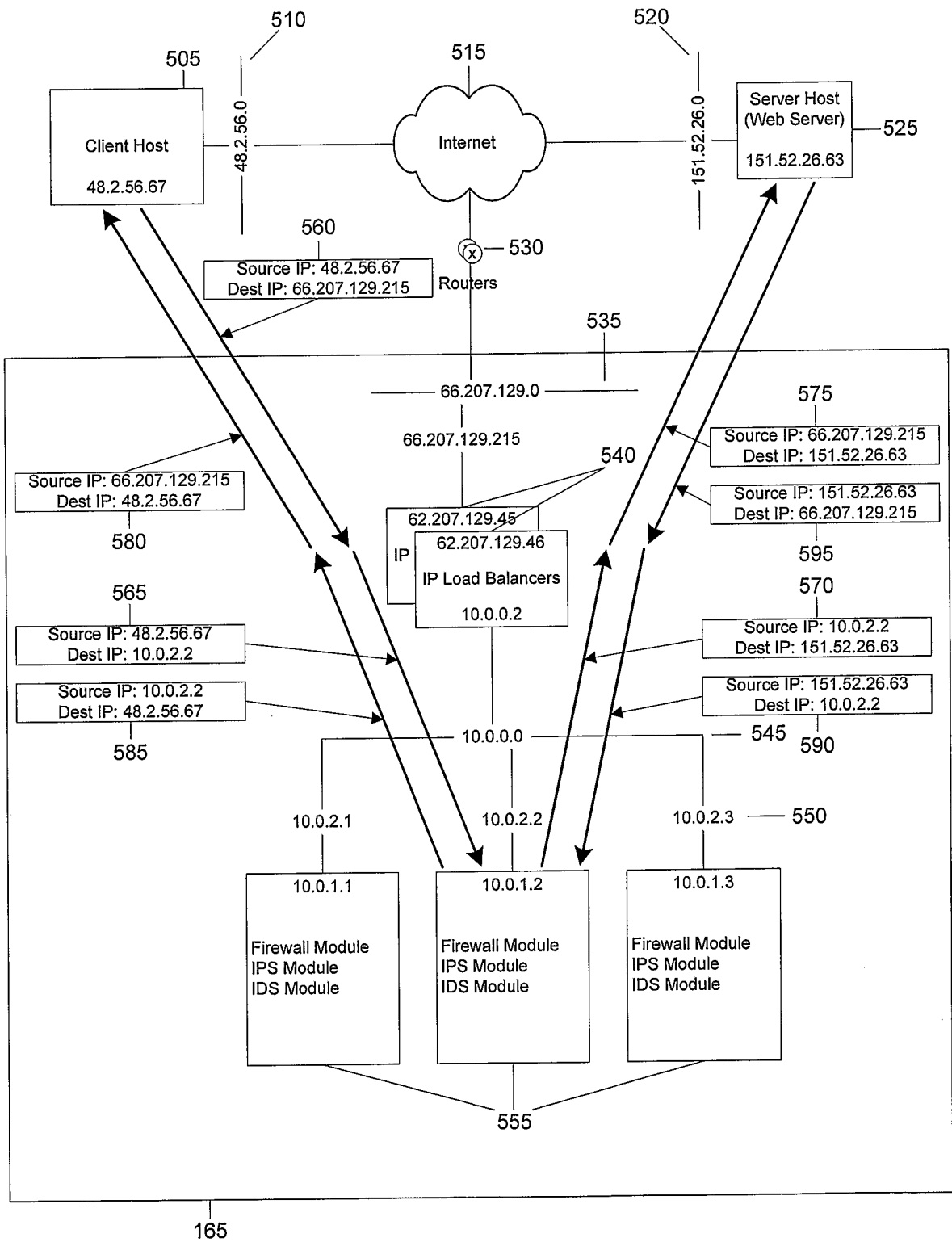


FIG. 5

6/9

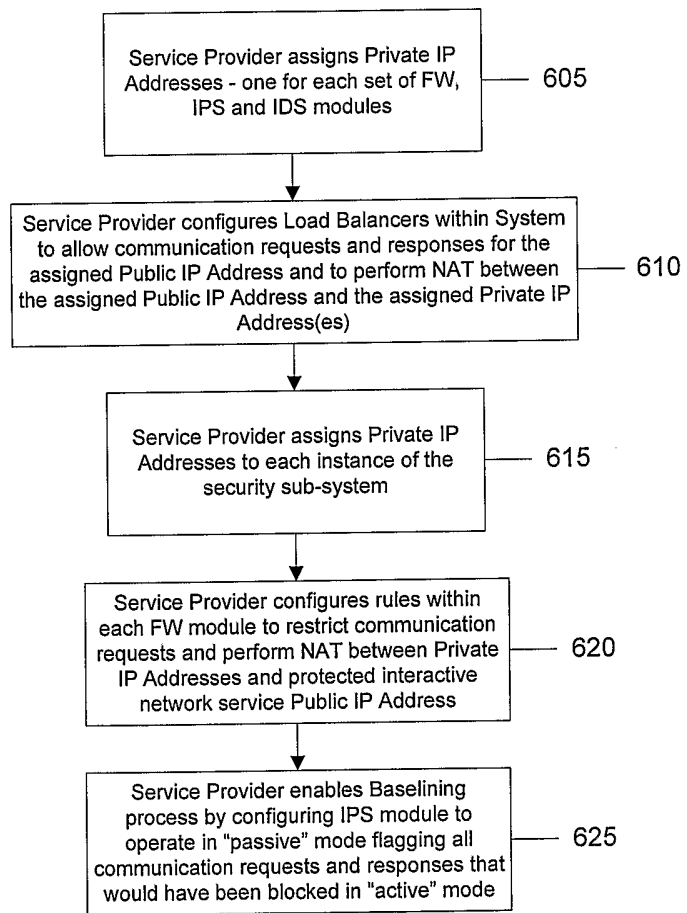


FIG. 6

7/9

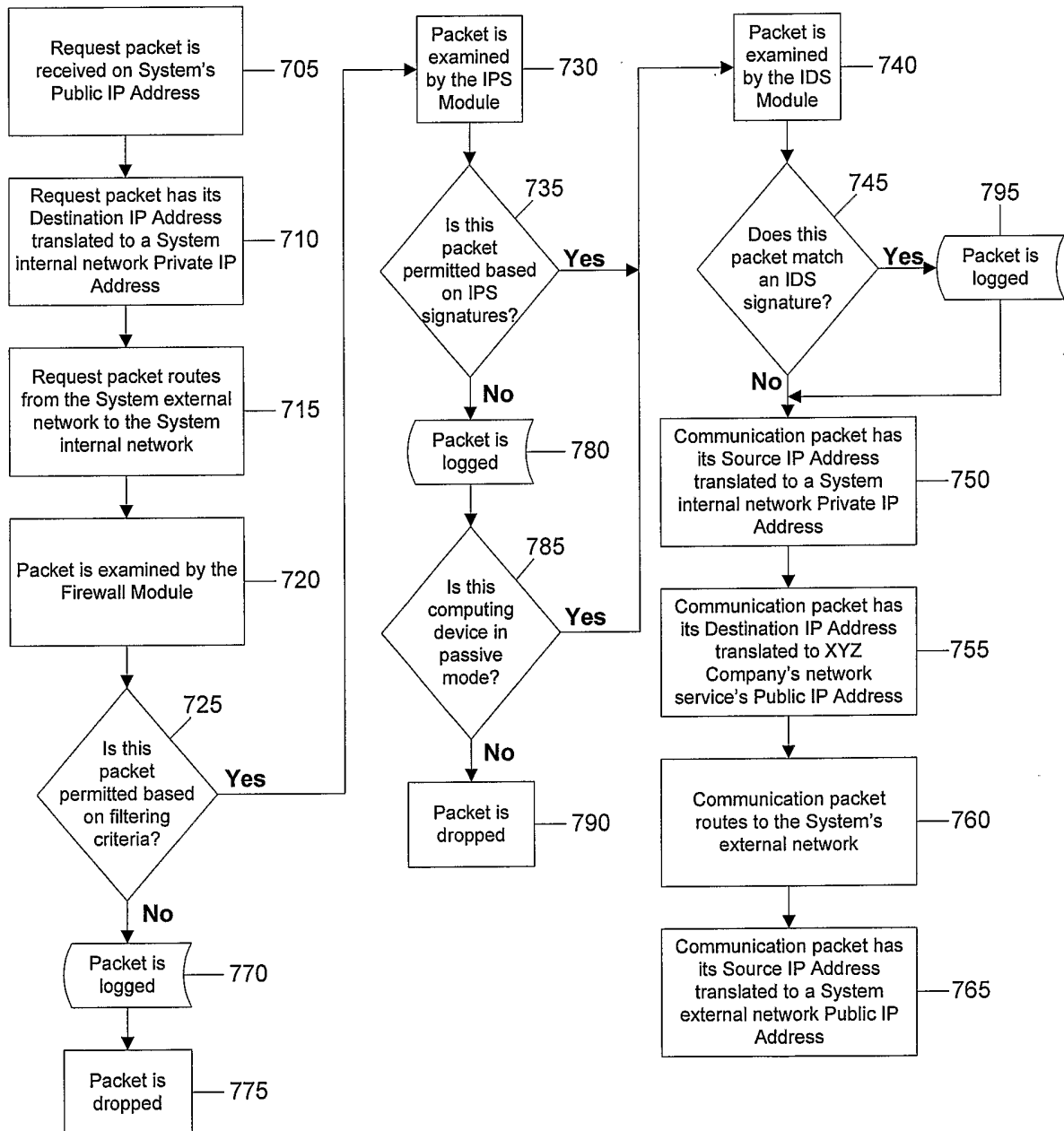


FIG. 7

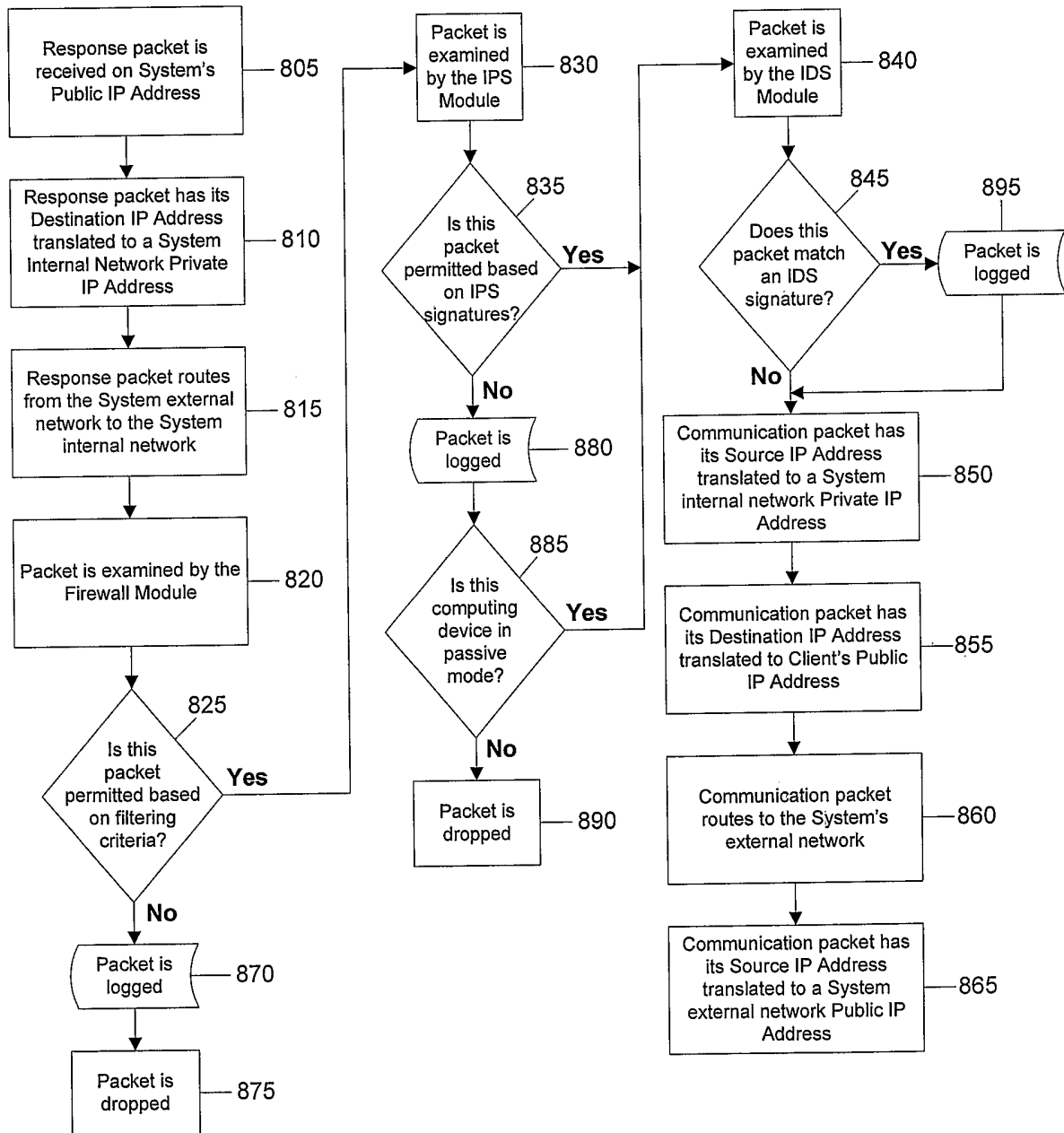


FIG. 8

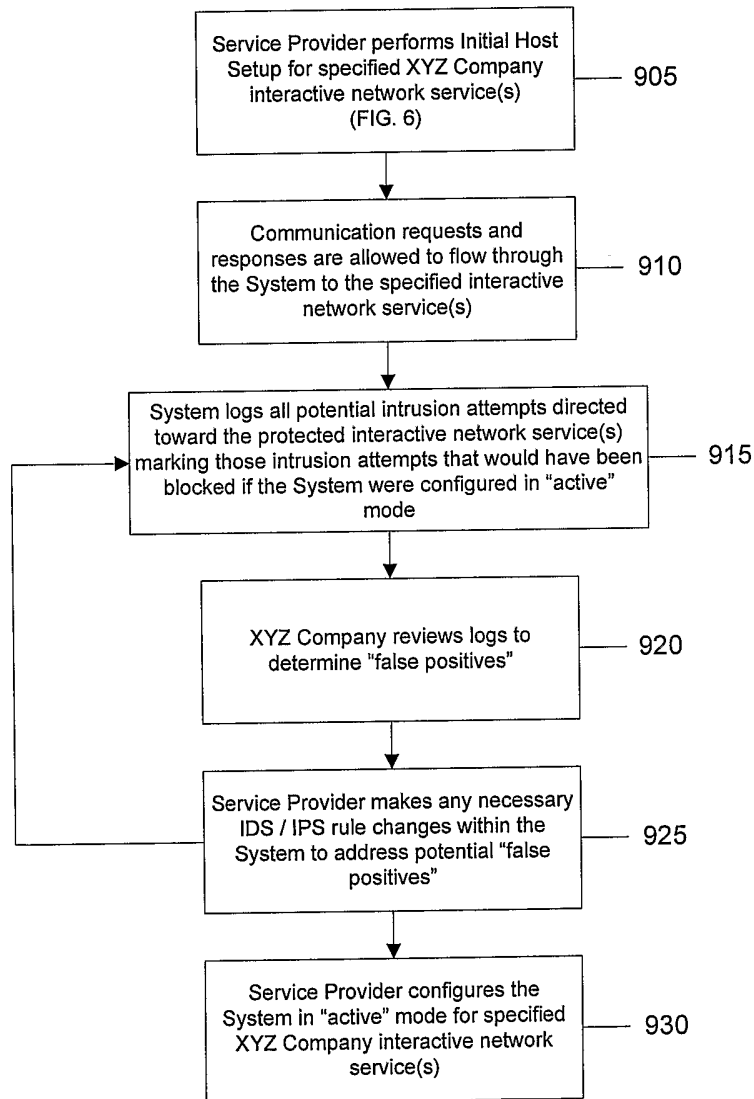


FIG. 9