(54) Title: INTEGRATED SECURITY GATEWAY APPARATUS AND OPERATING METHOD THEREOF

(57) Abstract: A networking system is associated with an integrated security gateway for integrating virtual private networking, firewall, and network monitoring functions. A duplicate of a received packet is provided to a network monitoring system connected thereto or included therein so as to detect all kinds of intrusions and attacks to a virtual private network and the integrated security gateway itself. And, by implementing a variety of functions and services in the network monitoring system, the networking system can enjoy almost complete security.
INTEGRATED SECURITY GATEWAY APPARATUS
AND OPERATING METHOD THEREOF

TECHNICAL FIELD

The present invention relates to a networking system for wide-area networking; and, more particularly, to an integrated security gateway apparatus and an operating method thereof employed in a networking system, wherein the integrated security gateway apparatus is interposed between an internal network and an external network, for integrating a virtual private networking and firewall and intrusion detection functions.

BACKGROUND ART

Businesses today are faced with supporting a broader variety of communications among a wider range of corporate branches even as they seek to reduce the cost of their communications infrastructure. Employees are looking to access the resources of their corporate intranets as they take to the road or telecommute. And also, business partners are joining together in extra-nets to share business information. In this environment, private computer networks come in all forms and are put to many purposes.

Fig. 1 shows an example of a conventional private computer network using dedicated leased lines or packet-based networks to connect corporate branches through routers. One of the most disadvantageous features of this solution is that such private computer networking does not provide the flexibility required for quickly creating new partner links or supporting project teams in the field.

On the other hand, the corporate branches can enjoy the security of the private computer network via access control and encryption, while taking advantage of the economies of scale and built-in management facilities of
large public networks. For example, a point-to-point tunneling protocol (PPTP) that encapsulates other protocol for transmission over an IP (Internet Protocol) network is used to create a VPN (Virtual Private Network) within the public Internet. The VPN allows a network manager to connect corporate remote branch sites and/or project teams to the corporate main branch economically and provides remote access to employees, which reduces in-house requirements for equipment and support. That is, an Internet-based VPN uses an open, distributed infrastructure of the Internet to transmit data between the corporate branches.

Since each of the corporate branches is connected to the Internet in the Internet-based VPN, information can be exchanged between VPN users and Internet users. This information exchange presents a challenge to protect information located on the corporate branches from unauthorized access by the Internet users and from unauthorized export by the VPN users. For example, hackers have been able to erase files or disks, cancel programs, retrieve sensitive information, and even introduce computer viruses, e.g., Trojan horses, and/or worms into the corporate main branch.

A firewall is a technique for keeping a network secure. The firewall is gaining the popularity to separate corporate public resources, e.g., DMZ (Demilitarized Zone) servers including a corporate public web server, mail server, etc., from a corporate internal network as well as to give the VPN users access to the Internet in a secure fashion.

Fig. 2 shows an example of a conventional internet-based VPN 200 using the Internet 230 to connect VPN branches 210 and 220 through VPN proxies 260 and 270, firewalls 280 and 290, and routers 240 and 250. Each of the firewalls 280 and 290 is coupled to corresponding one of the VPN proxies 260 and 270, and to corresponding one
of corporate DMZ servers 214 and 224. The VPN proxies 260 and 270 generally perform encryption and decryption to protect data against eavesdropping and tampering by unauthorized parties.

Each of the firewalls 280 and 290 receives an incoming packet from the corresponding router 240 or 250 and checks whether the incoming packet could be sent to the VPN branches 210 and 220, and the DMZ servers 214 and 224 by using a predetermined rule. For example, the firewalls 280 and 290 check whether the incoming packet is from a valid domain or an IP address, i.e., an identified external resource.

Referring to Figs. 3A and 3B, there are provided other conventional Internet-based VPNs, each of which further comprises an IDS (Intrusion Detection System) 370 interposed between a router 340 and a firewall 350 or an IDS 380 between a VPN branch 310 and a VPN proxy 360. Except that the IDS 370 or 380 is inserted, the VPNs 301 and 302 in Figs. 3A and 3B are substantially identical to the VPN 200 in Fig. 2. The IDSs 370 and 380 perform real-time intrusion detection into the VPN branch 310 by including an intrusion pattern database and an expert system, which can be implemented by software or hardware.

The IDSs 370 and 380 perform functions of a traffic control, real-time monitoring and intrusion detection, intrusion blocking, and intrusion analysis and reporting. In Fig. 3A, since the IDS 370 is interposed between the router 340 and the firewall 350, the IDS 370 can detect an intrusion into the firewall 350 or the VPN branch 310. However, in this case, the IDS 370 itself could be attacked by an external intruder. On the contrary, in Fig. 3B, since the IDS 380 is interposed between the VPN branch 310 and the VPN proxy 360, the intrusion detection is done only for a packet that is passed through the firewall 350. That is, the IDS 380 cannot detect an intrusion exactly because the firewall 350 drops packets
that are not accepted. Therefore, the external intruder can attack the firewall 350 or the VPN branch 310 and abuse network resources continuously.

Furthermore, because the VPN proxy 360, the firewall 350, and the IDS 370 or 380 are constructed separately, a security hole problem tends to frequently occur as well as costly installation.

DISCLOSURE OF INVENTION

It is, therefore, an object of the present invention to provide an integrated security gateway for integrating virtual private networking and firewall functions and an operating method thereof.

Another object of the present invention is to provide an integrated security gateway for integrating intrusion detection functions as well as virtual private networking and firewall functions and an operating method thereof.

In accordance with one aspect of the present invention, there is provided an integrated security gateway apparatus interfacing with an internal network and an external network for blocking a selected packet from one of the internal network and the external network, the apparatus comprising: a packet duplicating module for receiving and duplicating an incoming packet from said one of the internal and external networks; a server complex, which is coupled to the packet duplicating module through a port complex, for analyzing the duplicated packet; and an inspection engine, which is connected to the packet duplicating module and to the server complex via the port complex, for inspecting whether or not the incoming packet corresponds to the selected packet to be blocked based on the analysis result and selectively blocking the incoming packet depending on the inspection result.

In accordance with another aspect of the present
invention, there is provided a networking system consisting of at least one internal network and an external network, comprising: an integrated security gateway interfacing with said at least one internal network and said external network, for blocking a selected packet from said at least one internal network and said external network; and black zone servers, which are coupled to the integrated security gateway for analyzing the duplicated packet.

In accordance with yet another aspect of the present invention, there is provided a method for blocking a selected packet from one of an internal network and an external network in an integrated security gateway apparatus interfacing with the internal and external networks, wherein the integrated security gateway apparatus includes a packet duplicating module for duplicating an incoming packet and an inspection engine, the method comprising the steps of: a) receiving a message packet from a server complex; b) determining whether or not the message packet containing information to be used in the blocking the incoming packet which corresponds to the selected packet, wherein the incoming packet is transmitted from said one of the internal network and the external network; c) determining a type of an attack depending on the message if the packet has the message; and, otherwise, dropping the packet; d) setting access deny time to the incoming packet; e) setting an attacker's address; f) setting a destination address to be attacked by the attacker through the incoming packet; g) determining whether or not there is a session connected to the destination address; h) disconnecting the session, if there is the session connected to the destination address; i) setting a timer to the incoming packet depending on the access deny time, if there is no the session connected to the destination address; and j) denying a connection from the attacker to
the destination address and vice versa by blocking the incoming packet.

BRIEF DESCRIPTION OF DRAWINGS

The above and other objectives and features of the present invention will become apparent from the following description of embodiments given in conjunction with the accompanying drawings, in which:

Fig. 1 is a schematic diagram of a conventional private computer network using dedicated leased lines or packet-based networks.

Fig. 2 shows a schematic diagram of an Internet-based VPN (virtual private networking);

Figs. 3A and 3B offer schematic diagrams of conventional and other Internet-based VPNs;

Fig. 4 illustrates a schematic diagram of a VPN employing an integrated security gateway apparatus in accordance with the present invention;

Fig. 5 provides a hardware block diagram of the integrated security gateway apparatus in Fig. 4;

Fig. 6 shows a functional block diagram of the integrated security gateway apparatus in Fig. 4;

Figs. 7A and 7B depict flow charts for explaining an operating method of the integrated security gateway apparatus in Fig. 4;

Fig. 8 exemplifies a schematic block diagram of an integrated security gateway apparatus in accordance with a second embodiment of the present invention;

Figs. 9A and 9B present flow charts for explaining an operating method of the integrated security gateway apparatus in Fig. 8;

Fig. 10 demonstrates a schematic block diagram of an integrated security gateway apparatus in accordance with a third embodiment of the present invention;

Figs. 11A and 11B give flow charts for explaining an operating method of the integrated security gateway.
apparatus in Fig. 10;

Fig. 12 shows a schematic block diagram of an integrated security gateway apparatus in accordance with a fourth embodiment of the present invention;

Figs. 13A and 13B are flow charts for explaining an operating method of the integrated security gateway apparatus in Fig. 12;

Fig. 14 illustrates a schematic block diagram of an integrated security gateway apparatus in accordance with a fifth embodiment of the present invention;

Fig. 15 provides a schematic block diagram of an integrated security gateway apparatus in accordance with a sixth embodiment of the present invention;

Figs. 16A and 16B depict flow charts for explaining an operating method of the integrated security gateway apparatus in Fig. 15;

Fig. 17 exemplifies a schematic block diagram of a built-in security unit employed in the integrated security gateway apparatus of Fig. 4 in accordance with the present invention;

Figs. 18A and 18B present flow charts for explaining an operating method of the built-in security unit in Fig. 17;

Fig. 19 shows a flow chart for explaining an intrusion detection process in accordance with the present invention;

Fig. 20 offers a structure of a communication packet transmitted from BZ servers to the integrated security gateway apparatus in accordance with the present invention;

Figs. 21A and 21B show flow charts for explaining in detail a method for performing an anti-virus function and an intrusion detection function in accordance with the present invention; and

Fig. 22 presents flow charts for explaining in detail a method for performing a noxious site blocking
function in accordance with the present invention.

BEST MODE FOR CARRYING OUT THE INVENTION

Referring to Fig. 4, there is provided a schematic diagram of a VPN (Virtual Private Network) employing an integrated security gateway in accordance with the present invention. The VPN 400 is comprised of a plurality of internal networks, each of which is connected to an external network such as the Internet 450 via a router 440. For the sake of simplicity, only one internal network 410 is shown in Fig. 4.

The internal network 410 is connected to the router 440 through the inventive integrated security gateway apparatus 420 to which a "demilitarized zone (DMZ)" server 414 and a "black zone (BZ)" server 430 are connected. The DMZ server 414 is a web server and/or a mail server. The internal network 410 may be a local area network (LAN). In Fig. 4, the internal network 410 is illustrated as including a server computer 411 and two client computers 412 and 413 only, for the sake of simplicity.

The integrated security gateway apparatus 420 protects the internal network 410 from outsiders. It also prevents unauthorized transmission of data/information stored in the internal network computers 411 to 413 to outside.

The integrated security gateway apparatus 420 protects the DMZ server 414 from an attack through the external network 450.

The integrated security gateway apparatus 420 provides data encryption and decryption for which variable encryption and decryption rules can be applied, depending on IP (Internet Protocol) addresses or ports. A key to data encryption and decryption can be established or updated in the integrated security gateway apparatus 420 by a well-known external input device, e.g.,
a smart card.

The integrated security gateway apparatus 420 provides a packet filtering function by employing a stateful inspection, i.e., by inspecting the state of a current input packet with respect to the state of a previous input packet in an application. And, a number of filtering rules can be applied depending on the IP addresses or the ports. The integrated security gateway apparatus 420 performs a static packet filtering function, i.e., a checking operation on the input packets under a predetermined filtering rule.

The integrated security gateway apparatus 420 performs a URL (Uniform Resource Locator) filtering function in a restrictive mode in which selected packets are to be passed or in a permissive mode in which all the packets except for a selected few are to be passed. The integrated security gateway apparatus 420 also performs a packet contents filtering functions.

The integrated security gateway apparatus 420 provides a virtual session for a UDP (User Datagram Protocol) application to solve a security problem associated with connectionless packet transfer. The virtual session contains and updates UDP connection information dynamically.

The integrated security gateway apparatus 420 generates a session for only a permitted RPC (Remote Procedure Call) service in which a port number of a packet source is changed dynamically and performs ICMP (Internet Control Message Protocol) redirect blocking, IP source routing blocking, and static routing functions. The integrated security gateway apparatus 420 provides an NAT (network address translation) function.

The BZ server 430, coupled to the integrated security gateway apparatus 420 acts as an IDS (Intrusion Detection System), performing traffic control, real-time monitoring, intrusion detection, intrusion blocking, and
intrusion analysis and reporting functions. As will be described below, the BZ server 430 is invisible to the users of the internal network 410 and the external network 450 so as to maximize the security of the VPN 400. In other words, the integrated security gateway apparatus 420 duplicates all the incoming packets from the internal network 410, the DMZ server 414, and the external network 450 and sends them to the BZ server 430. Then, the BZ server 430 analyzes each of the duplicated packets from the integrated security gateway apparatus 420 and reports its analysis result to the integrated security gateway apparatus 420, so that the integrated security gateway apparatus 420 can process each of the incoming packets depending on the analysis result.

The BZ server 430 may act as an anti-virus system for blocking packets infected with virus and/or as a blocking system for blocking packets from noxious web sites.

It may be a hub to which the IDS, the anti-virus system and/or the site blocking system may be coupled, so that intrusion protection, virus checking and/or site blocking functions can be performed.

The integrated security gateway apparatus 420 may include a built-in BZ server at which the duplicated packets are analyzed.

Fig. 5 provides a hardware block diagram of an embodiment of the integrated security gateway apparatus 420 in Fig. 4. As shown in Fig. 5, the integrated security gateway apparatus 420 includes a firewall processor 10, three network interface cards 20, 21, and 22, a BZ port 23, a first memory 30, a key memory 40, and an I/O (input/output) interface card 50, all connected to a first bus 1. The integrated security gateway apparatus 420 further includes a VPN processor 60, a crypto-coprocessor 70, and a second memory 80, all connected to a second bus 2 which in turn is connected to the first
bus 1 through a bus bridge 3.

Each of the network interface cards 20, 21, and 22 includes a LAN (local area network) connector, a Rx (receiving) buffer, and a Tx (transmitting) buffer, which are not shown in Fig. 5. The network interface cards 20, 21, and 22 are used to interface with the internal network 410, the DMZ server 414, and the external network 450 in Fig. 4, respectively. The network interface cards 20, 21, and 22 are designed to meet the Institute of Electrical and Electronics Engineers (IEEE) standard 802.3 titled "Carrier Sense Multiple Access with Collision Detection (CSMA/CD) access method and Physical layer specifications." It can be appreciated, however, that the network interface cards 20, 21, and 22 designed to work with other medium access techniques or standards could be used in the present invention.

The Rx buffer is used to store incoming packets received from the internal network 410, the DMZ server 414, or the external network 450 until the incoming packets can be processed by the processor 10 or 60.

The Tx buffer is used to store outgoing packets until the outgoing packets can be sent to the internal network 410, the DMZ server 414, or and the external network 450.

The BZ port 23 is used to interface with the BZ server 430. Similar to the network interface cards 20, 21, and 22, the BZ port 23 includes a LAN (local area network) connector, a Rx (receiving) buffer, and a Tx (transmitting) buffer, which are not shown in Fig. 5.

Each of the firewall processor 10 and the VPN processor 60 can be a dedicated high performance microprocessor. Any microprocessor capable of operating at a speed required to implement the functions as described above and will be described in detail below is appropriate.

The first memory 30 is used to store the packets,
an OS (operating system), OS parameters, pre-defined parameters, IP addresses, and etc. The first memory 30 includes several types of high-speed memory devices such as a DIMM (dual in-line memory module) type 64-512 Mbytes SDRAM (Synchronous Dynamic Random Access Memory) and a flash type 4-8 Mbytes ROM (Read only Memory). The first memory 30 further stores instructions for controlling actions to be taken on the incoming and outgoing packets. These instructions include a predetermined set of criteria based upon the fields of the incoming packets and other information such as the time of day at which the incoming packet was sent or received, and the state of the session. Such criteria can be implemented by inspecting the fields of the incoming packets, by reference to external data such as a connection status and the time of day and by reference to pre-defined tables or other information stored in the first memory 30. The application of the criteria leads one or several pre-defined actions to be taken on the incoming packets.

The VPN processor 60 performs a tunneling function using the IPSec (Internet Protocol Security) protocol, data encryption/decryption, and packet authentication. It should be appreciated that the VPN processor 60 and the firewall processor 10 can be implemented by a single microprocessor or by a multiplicity of microprocessors in the present invention.

The crypto-coprocessor 70 is used to perform a computation function for the data encryption/decryption and packet authentication. Preferably, the crypto-coprocessor 70 is implemented by an ASIC (Application-Specific Integrated Circuit) supporting an algorithm for the data encryption and hash functions for the packet authentication employed in the VPN 400 of the present invention.

The second memory 80 is used to store the packets transferred from the first memory 30 through the bus
bridge 3, and encryption and decryption rules for each IP address and port.

The key memory 40 is used to store the key for encryption/decryption and includes a SRAM (Static Random Access Memory) type memory device. The key memory 40 is coupled to a battery 41 for protection in a stoppage of electric current.

The I/O interface card 50 is coupled to an IC card reader 51 and a console connector 52 via an I/O bus 4.

Fig. 6 shows a functional block diagram of the integrated security gateway apparatus 420 in Fig. 4. In one embodiment, these modules except for the BZ port 23 connected to the BZ server 430 are program instruction modules stored in the first memory 30 and executed by the processors 10, 60, and 70. The connections shown in Fig. 6 refer to software instructions or hardware instructions or both, depending on the particular physical implementation of the invention.

The integrated security gateway apparatus 420 also includes a packet duplicating module 610 and an inspection engine 620. Further included are a rule storage 630, a session table 640, and an action module 650 in the integrated security gateway apparatus 420. The action module 650 contains a number of modules, e.g., a decryption module 652, an encryption module 654, a URL/contents filtering module 656, and an NAT (Network Address Translation) module 658.

The packet duplicating module 610 is coupled to the network interface cards 20, 21, and 22 of Fig. 5 to receive incoming packets from the internal network 410, the DMZ server 414, and the external network 450, respectively. The packet duplicating module 610 is coupled to the inspection engine 620 to transfer the received packets thereto. On the other hand, the packet duplicating module 610 duplicates the received packets and transfers them to the BZ server 430 through the BZ
port 23.

The rule storage 630 is used to store instructions for inspection rules.

The session table 640 is used to store session information for states of the sessions.

The inspection engine 620 inspects the fields of the packets from the packet duplicating module 610, by using the inspection rules retrieved in the rule storage unit 630 and passes them to one of the action modules 652 to 658 to execute appropriate operations on the packets or to abandon the packets.

On the other hand, the inspection engine 620 retrieves the session corresponding to each packet in the session table 640 and extracts IP header information and TCP (Transmission Control Protocol) header information to refer and update the session status.

The decryption module 652 performs the decryption function on each packet whose a source is another VPN branch (not shown) connected to the external network 450.

The encryption module 654 performs the encryption function on each outgoing packet whose a destination is another VPN branch (not shown) connected to the external network 450.

The URL/contents filtering module 656 performs typical URL/contents filtering functions to prevent access to a predetermined group of URLs and to drop the packet containing noxious contents.

The NAT module 658 performs a typical NAT function, e.g., by processing a proxy address resolution protocol to translate source and destination addresses between the internal network 410 and the external network 450.

The operation of the integrated security gateway apparatus 420 as shown in Figs. 4 to 6 will be discussed in detail below in connection with Figs. 7A and 7B, but it should be understood that other embodiments can be proposed without departing the range of the present
invention. Each of the operations, actions, or functions can be implemented as program instructions or modules, hardware, e.g., ASIC or other circuitry, ROMs, etc., or some combinations thereof.

Referring to Fig. 7A, at step S701, when the packet is received by the packet duplicating module 610, it is transferred to the inspection engine 620.

At step S702, the packet received via one of the network interface cards 20, 21, and 22 is duplicated and transferred to the BZ server 430 through the BZ port 23, and then the procedure proceeds to step S703.

At step S703, the inspection engine 620 checks whether the packet is encrypted. If the packet is encrypted, the procedure proceeds to step S704; and, otherwise, the procedure proceeds to step S705.

At step S704, the packet is decrypted at the decryption module 652, and then the procedure proceeds to step S705.

At step S705, the inspection engine 620 retrieves rule and session information corresponding to the packet in the rule storage unit 630 and the session table unit 640, and then the procedure proceeds to step S706.

At step S706, the inspection engine 620 determines whether the packet is to be denied depending on the retrieved rule and the session information. If the packet is to be denied, the procedure proceeds to step S707; and, otherwise, the procedure proceeds to step S708.

At step S707, the inspection engine 620 abandons the packet and then the procedure is terminated.

At step S708, the inspection engine 620 extracts packet information and updates the session information in the session table unit 640, and then the procedure proceeds to step S709.

At step S709, the inspection engine 620 determines whether a packet content filtering is required. If the packet contents filtering is required, the procedure
proceeds to step S710; and, otherwise, the procedure proceeds to step S711 of Fig. 7B through a tap A.

At step S710, the URL/contents filtering module 656 performs contents filtering for the packet, and then the procedure proceeds to step S711.

At step S711, the inspection engine 620 determines whether the NAT is required. If the NAT is required, the procedure proceeds to step S712; and, otherwise, the procedure proceeds to step S713.

At step S712, the NAT module 658 performs the NAT function on the packet, and then the procedure proceeds to step S713.

At step S713, the inspection engine 620 determines whether the encryption is required. If the encryption is required, the procedure proceeds to step S714; and, otherwise, the procedure proceeds to step S715.

At step S714, the packet is encrypted at the encryption module 662, and then the procedure proceeds to step S715.

At step S715, the inspection engine 620 determines whether the packet is to be forwarded to outside. If the packet is to be forwarded, the procedure proceeds to step S716; and, if the packet is to be processed within the integrated security gateway apparatus 420, the procedure proceeds to step S718.

At step S716, the inspection engine 620 checks a corresponding port, and then the procedure proceeds to step S717.

At step S717, the inspection engine 620 forwards the packet to the corresponding port via the corresponding network interface card, e.g., the network interface card 20 connected to the internal network 410, and then the procedure is terminated.

At step S718, the inspection engine 620 processes a predetermined processing, e.g., updating a list of the blocked URLs stored at the rule storage unit 630, and
then the procedure proceeds to step S719.

At step S719, the inspection engine 620 forwards the processing result to the destination of the packet through the network interface card 20, 21, and 22.

As described above, the duplicated incoming packet is provided to the BZ server 430 connected to or included in the integrated security gateway apparatus 420 so as to detect all kinds of intrusions and attacks to the internal network 410 and the integrated security gateway apparatus 420 itself.

Furthermore, by implementing a variety of functions and services in the BZ server 430, the VPN 400 of the present invention can enjoy almost complete security.

Fig. 8 exemplifies a schematic block diagram of an integrated security gateway apparatus in accordance with a second embodiment of the present invention. It is noted that the packet duplicating module 610 and the inspection engine 620 are the functional modules as described above; and a hub module 810, a port complex 820, and a server complex 830 are hardware modules. Actually, the hub module 810 and the BZ port complex 820 of the hardware modules are included in the integrated security gateway apparatus of the second embodiment. The port complex 820 includes four BZ ports 822 to 828, while the server complex 830 includes four auxiliary security servers 832 to 838. The server complex 830 serves the same functions of the BZ server 430.

In this embodiment, the hub module 810 simultaneously transmits packets duplicated in the packet duplicating module 610 to each of the auxiliary security servers 832 to 838 through the corresponding BZ port 822, 824, 826, or 828. In this case, the auxiliary security servers 832 to 838 may act as one of an IDS system, an anti-virus system, and a site blocking system. Otherwise, each of the auxiliary security servers 832 to 838 may act as a different system. For example, the auxiliary
security server 832 acts as the IDS system, the auxiliary security server 834 serves as the anti-virus system, the auxiliary security server 836 acts as the site blocking system, and the auxiliary security server 838 serves as another security system.

The auxiliary security servers 832 to 838 are process the same duplicated packet at the same time so that total load of the server complex 830 can be dramatically reduced.

Figs. 9A and 9B present flow charts for explaining an operating method of the integrated security gateway apparatus in Fig. 8.

At step S902, when a packet is received by the packet duplicating module 610, it is transferred to the inspection engine 620.

At step S904, the inspection engine 620 checks whether the packet is encrypted. If the packet is encrypted, the procedure proceeds to step S906; and, otherwise, the procedure goes to step S908.

At step S906, the packet is decrypted at the decryption module 652, and then procedure proceeds to step S908.

At step S908, the inspection engine 620 determines whether a session exists on the packet depending on session information retrieved from the session table unit 640. If the session exists on the packet, the procedure proceeds to step S914; and, otherwise, the procedure goes to step S910.

At step S910, the inspection engine 620 determines whether a rule exists on the packet depending on rule information retrieved from the rule storage unit 630. If the rule does not exist on the packet, the procedure proceeds to step S932 of Fig. 9B through a tap B; and, otherwise, the procedure goes to step S912.

At step S912, the inspection engine 620 creates a session to the packet, and the procedure proceeds to step
At step S914, the inspection engine 620 determines whether the packet is to be denied depending on the retrieved rule and the session information. If the packet is to be denied, the procedure proceeds to step S932 of Fig. 7B through the tap B; and, otherwise, the procedure goes to step S916.

At step S916, the inspection engine 620 determines whether the NAT is required. If the NAT is required, the procedure proceeds to step S918; and, otherwise, the procedure goes to step S920 of Fig. 9B through a tap A.

At step S918, the NAT module 658 performs the NAT function on the packet, and then the procedure proceeds to step S920 through the tap A.

At step S920 of Fig. 9B, the inspection engine 620 extracts packet information and updates the session information in the session table 640, and then the procedure proceeds to step S922 and step S932. In case that the procedure proceeds to step S922 through PATH 2, the inspection engine 620 processes the packet; and, in case that the procedure goes to step S932 through PATH 1, the packet duplicating module 610 duplicates the packet in order to perform subsequent processes on the duplicated packet. Therefore, it should be understood and interpreted that the PATH 1 is a virtual branch for the purpose of explaining the operating method, so that the process of the packet and the duplication thereof may be occurred at the same time in the inventive integrated security gateway apparatus.

At step S922, the inspection engine 620 determines whether a packet content filtering is required. If the packet contents filtering is required, the procedure proceeds to step S924; and, otherwise, the procedure goes to step S926.

At step S924, the URL/contents filtering module 656 performs contents filtering on the packet, and then the
procedure proceeds to step S926.

At step S926, the inspection engine 620 determines whether the encryption is required. If the encryption is required, the procedure proceeds to step S928; and, otherwise, the procedure proceeds to step S930.

At step S928, the packet is encrypted at the encryption module 654, and the procedure proceeds to step S930.

At step S930, the inspection engine 620 forwards the packet to its destination via the corresponding network interface card 20, 21, or 22, and then the procedure is terminated.

At step S932, the packet duplicating module 610 determines whether a BZ port exists. If the BZ port exists, the procedure proceeds to step S936; and, otherwise, the procedure goes to step S934.

At step S934, the inspection engine 620 abandons the packet and then the procedure is terminated.

At step S936, the packet duplicating module 610 duplicates the packet with the same number of the BZ ports 822 to 828, and then the procedure proceeds to step S938.

At step S938, the packet duplicating module 610 forwards the duplicated packet to the auxiliary security server complex 830 through the hub module 810 and the BZ port complex 820, and then the procedure is terminated.

Fig. 10 demonstrates a schematic block diagram of an integrated security gateway apparatus in accordance with a third embodiment of the present invention. It is noted that the packet duplicating module 610, the inspection engine 620, and a load balancing module 1000 are functional modules. Alternatively, the load balancing module 1000 may be implemented by a hardware. Similar to Fig. 8, a BZ port complex 1010 and a server complex 1020 are hardware modules. As described above, the server complex 1020 serves the same functions of the
BZ server 430. The BZ port complex 1010 includes four BZ ports 1012 to 1018, while the server complex 1020 includes four auxiliary security servers 1022 to 1028.

In this embodiment, the servers 1022 to 1028 perform the same function. That is, all the auxiliary security servers 1022 to 1028 act as one of the IDS system, the anti-virus system, and the site blocking system. The load balancing module 1000 transmits a duplicated packet from the packet duplicating module 610 to the auxiliary security servers 1022 to 1028 through the BZ port complex 1010, depending on the load of each server 1022 to 1028. Such scheme may be used in enhancing a specific function of the IDS, anti-virus, and site blocking functions according to the security policy.

Figs. 11A and 11B give flow charts for explaining an operating method of the integrated security gateway apparatus in Fig. 10.

Since steps S1102 to S1130 of Figs. 11A and 11B perform the same operations of steps S902 to S930 of Figs. 9A and 9B, the description for step S1102 to S1130 will be omitted herein, for the sake of simplicity.

At step S1132 of Fig. 11B, the packet duplicating module 610 checks a session to the packet, and then the procedure proceeds to step S1134.

At step S1134, the load balancing module 1000 determines one of the BZ ports 1012 to 1028 for transmitting the packet, and then the procedure proceeds to step S1136.

At step S1136, the packet duplicating module 610 duplicates the packet to transmit it to the load balancing module 1000, and then the procedure proceeds to step S1138.

At step S1138, the load balancing module 1000 forwards the duplicated packet to one of the auxiliary security servers 1022 to 1028 depending on the load of each server, and then the procedure is terminated.
Fig. 12 shows a schematic block diagram of an integrated security gateway apparatus in accordance with a fourth embodiment of the present invention. It is noted that the structure of the integrated security gateway apparatus in Fig. 12 is identical to that of the integrated security gateway apparatus in Fig. 10, except for a traffic control module 1200. The traffic control module 1200 may be implemented by software or hardware. The traffic control module 1200 is connected to a server complex 1220 through a port complex 1210. The server complex 1220 includes four auxiliary security servers 1222 to 1228; and the port complex 1210 includes BZ ports 1212 to 1218.

In general, each of users connected to the internal network 410 performs various works at the same time so that packets having various protocols exist on the internal network 410. The role of the traffic control module 1200 is to collect packets having an identical protocol among the duplicated packets from the packet duplicating module 610 and to send the identical protocol packets to the port complex 1210 depending on the priority of protocol predetermined by the network management policy or the security policy of the integrated security gateway apparatus. It is noted that the integrated security gateway apparatus in Fig. 12 may include one BZ port only, instead of the port complex 1210. Such case, a hub module or a load balancing module is disposed between the BZ port and the server complex 1220.

Fig. 13A and 13B are flow charts for explaining an operating method of the integrated security gateway apparatus in Fig. 12.

Since steps S1302 to S1330 of Figs. 13A and 13B perform the same operations of steps S902 to S930 of Figs. 9A and 9B, the description for step S1302 to S1330 will be omitted herein, for the sake of simplicity.
At step S1332 of Fig. 13B, the inspection engine 620 analyzes a service of the packet and transmits the analyzed result to the packet duplicating module 610.

At step S1334, the traffic control module 1200 determines a BZ port among the BZ ports 1212 to 1218 depending on a load of each of the auxiliary security servers 1222 to 1228 to transmit the packet to the server complex 1220, and then the procedure proceeds to step S1336.

At step S1336, the packet duplicating module 610 duplicates the packet to transmit it to the traffic control module 1200, and then the procedure proceeds to step S1338.

At step S1338, the traffic control module 1200 forwards the duplicated packet to one of the auxiliary security servers 1222 to 1228 via the determined BZ port of the port complex 1210, and the procedure is terminated.

Fig. 14 illustrates a schematic block diagram of an integrated security gateway apparatus in accordance with a fifth embodiment of the present invention. As shown in Fig. 14, a switching module 1400 is included in the integrated security gateway apparatus. A port complex 1410 includes four BZ ports 1412 to 1418; and a server complex 1420 includes an auxiliary server 1422, a site blocking server 1424, an anti-virus server 1426, and an intrusion detecting server 1428. That is, the server complex 1420 includes servers having different functions to each other.

In this embodiment, the integrated security gateway apparatus analyzes duplicated packets and transmits each of the duplicated packets, by using the switching module 1400, to corresponding server of the server complex 1420 according to a protocol of each packet.

For example, if the packet is e-mail, the packet uses POP 3 (Post Office Protocol 3) so that it is possible that the packet was infected with a virus. Such
case, the switching module 1400 transmits the packet to the anti-virus server 1426 through the BZ port 1416. Since the packet is processed according to its protocol, the performance of the server complex 1420 can be increased.

Fig. 15 provides a schematic block diagram of an integrated security gateway apparatus in accordance with a sixth embodiment of the present invention. As shown in Fig. 15, the packet duplicating module 610 is coupled to a hub module 1500. The hub module 1500 is connected to two BZ ports 1522 and 1524 of a port complex 1520. Also, the hub module 1500 is connected to two BZ ports 1526 and 1528 of the port complex 1520 through a load balancing module 1510. The BZ port 1522 connected to an anti-virus server 1532; the BZ port 1524 is to a site blocking server 1534; the BZ port 1526 is to an intrusion detecting server 1536; and the BZ port 1528 is to an intrusion detecting server 1538. That is, the load balancing module 1510 is connected to servers performing the same function. In this case, it is possible to prevent the lowering of the processing speed and the overload at specific servers, e.g., the intrusion detecting servers 1536 and 1538, connected to the load balancing module 1510, depending on the security policy.

Fig. 16A and 16B depict flow charts for explaining an operating method of the integrated security gateway apparatus in Fig. 15.

Since steps S1602 to S1630 of Figs. 16A and 16B perform the same operations of steps S902 to S930 of Figs. 9A and 9B, the description for step S1602 to S1630 will be omitted herein, for the sake of simplicity.

At step S1632 of Fig. 16B, the inspection engine 620 checks the setting of the BZ ports 1522 to 1528, and the procedure proceeds to step S1634. That is, each of the BZ ports 1522 to 1528 is connected to one of the servers 1532 to 1538.
At step S1634, the load balancing module 1510 determines whether a load balancing is required for the packet. If the load balancing is required, the procedure proceeds to step S1636; and, otherwise, the procedure goes to step S1640.

At step S1636, the packet duplicating module 610 checks a session of the packet, and the procedure proceeds to step S1638.

At step S1638, the packet duplicating module 610 selects one of the BZ ports to the session of the packet, and the procedure proceeds to step S1640.

At step S1640, the packet duplicating module 610 duplicates the packet to transmit it to the hub module 1500, and the procedure proceeds to step S1642.

At step S1642, the hub module 1500 forwards the packet to the BZ ports 1522 and 1524 and the load balancing module 1510. The, the load balancing module 1510 forwards the packet to one of the BZ ports 1526 and 1528, depending on the load of the intrusion detecting servers 1536 and 1538.

Fig. 17 exemplifies a schematic block diagram of a built-in security unit employed in the integrated security gateway apparatus 420 of Fig. 4 in accordance with the present invention. As shown in Fig. 17, the built-in security unit 1700 comprises a network interface module 1710, a TCP/IP protocol stack module 1720, a first memory 1730, a processing module 1740, and a second memory 1750. The built-in security unit 1700 is used in the integrated security gateway apparatus 420 instead of the BZ port 23. The built-in security unit 1700 may be implemented in the form of a card capable of being inserted on a slot provided in the integrated security gateway apparatus 420.

The network interface module 1710 includes a LAN connector, a Rx buffer, and a Tx buffer and is connected to the first bus 1. The network interface module 1710
operates in promiscuous mode and receives duplicated packets from the packet duplicating module 610. The TCP/IP protocol stack module 1720 transforms the state of the duplicated packets from physical layer to application layer. The duplicated packets from the packet duplicating module 610 are transmitted to the first memory 1730 through the TCP/IP protocol stack module 1720, thereby being stored on the first memory 1730 in application layer state. The first memory 1730 may be implemented by a DRAM (Direct Random Access Memory). The first memory 1730 receives the duplicated packets and transmits it to the processing module 1740. The second memory 1750 stores information and acts as the BZ server 430. The processing module 1740 processes the duplicated packets and transmits the processed result to the processor 10 or 60, in order to take action on the packets.

Figs. 18A and 18B present flow charts for explaining an operating method of the built-in security unit 1700 in Fig. 17.

Since steps S1802 to S1830 of Figs. 18A and 18B perform the same operations of steps S902 to S930 of Figs. 9A and 9B, the description for step S1802 to S1830 will be omitted herein, for the sake of simplicity.

At step S1832 of Fig. 18B, the processing module 1740 analyzes a service type of the duplicated packet, and the procedure proceeds to step S1834.

At step S1834, the processing module 1740 determines whether pattern information exists on the second memory 1750, wherein the pattern information includes attack and virus patterns. If the pattern information exists on the second memory 1750, the procedure proceeds to step S1836; and, otherwise, the procedure returns to step S1802.

At step S1836, the processing module 1740 compares the duplicated packet with the pattern information on the
second memory 1750, and the procedure proceeds to step S1838.

At step S1838, the processing module 1740 takes action on the packet depending on the comparison result, and the procedure is terminated. The action includes a session blocking, an alarm, a log, and the like.

Fig. 19 shows a flow chart for explaining an intrusion detection process in accordance with the present invention.

At step S1902, the inspection engine 620 receives a packet, and the procedure proceeds to step S1904.

At step S1904, the inspection engine 620 determines whether the packet is transmitted from the BZ server 430, the server complex 830, 1020, 1220, 1420, or 1530, or the built-in security unit 1700. That is, the inspection engine 620 determines whether the packet has an IDS message. If the packet has the IDS message, the procedure proceeds to step S1908; and, otherwise, the procedure goes to step S1906.

At step S1906, the inspection engine 620 drops the packet, and the procedure is terminated.

At step S1908, the inspection engine 620 determines the type of an attack for a current packet to be processed therein depending on the IDS message, and procedure proceeds to step S1910.

At step S1910, the inspection engine 620 sets access deny time to the current packet, and the procedure proceeds to step S1912.

At step S1912, the inspection engine 620 sets an address of an attacker, and the procedure proceeds to step S1914.

At step S1914, the inspection engine 620 sets a destination address to be attacked, and the procedure proceeds to step S1916.

At step S1916, the inspection engine 620 determines whether there is a session connected to the destination
address. If there is the session connected to the destination address, the procedure proceeds to the step S1918; and, otherwise, the procedure goes to step S1920.

At step S1918, the inspection engine 620 disconnects the session, and the procedure proceeds to step S1920.

At step S1920, the inspection engine 620 sets a timer to the current packet depending on the access deny time, and the procedure proceeds to step S1922.

At step S1922, the inspection engine 620 denies a connection from the attacker to the destination address and vice versa, and the procedure proceeds to step S1924.

At step S1924, the inspection engine 620 determines whether the access deny time has been passed. If the access deny time has been passed, the procedure proceeds to step S1926; and, otherwise, the procedure returns to step S1922.

At step S1926, the inspection engine 620 releases the timer, and the procedure proceeds to step S1928.

At step S1928, the inspection engine 620 permits a connection from the attacker to the destination and vice versa, and the procedure is terminated.

Fig. 20 offers a structure of a communication packet transmitted from the BZ server 430, the server complex 830, 1020, 1220, 1420, or 1530, or the built-in security unit 1700 to the inspection engine 620 in accordance with the present invention. The communication packet includes various fields. The fields includes a source IP, a destination IP, a source port, a destination port, a protocol, a filer, a risk, a hackcode1, a hackcode2, a lasting time, and a description, and are not limited thereto.

The source IP field represents to an attacker's IP address; the destination IP field is to an IP address of destination; the source port field is to a port number of the attacker; the destination port field is to a port
number of the destination; the protocol field is to an attack protocol; the filter field is to an action for attack; the risk field is to a risk for the attack; the hackcode1 and hackcode2 are to the type of the attack; the lasting time is to an access deny time; and the description is to a description for the attack.

Figs. 21A and 21B show flow charts for explaining in detail a method for performing an anti-virus function and an intrusion detection function in accordance with the present invention.

At step S2102 of Fig. 21A, the inventive integrated security gateway apparatus receives an incoming packet from the internal network or the external network, and the procedure proceeds to step S2104.

At step S2104, the inventive integrated security gateway apparatus duplicates the incoming packet, and the procedure proceeds to step S2106. In this time, the incoming packet is transmitted to its destination.

At step S2106, the inventive integrated security gateway transmits the duplicated packet to the BZ server performing an anti-virus function or the server complex serving as the BZ server (hereinafter, referred to the anti-virus server), and the procedure proceeds to step S2108.

At step S2108, the anti-virus server collects the duplicated packets from the inventive integrated security gateway apparatus to produce an assembled message, and the procedure proceeds to step S2110.

At step S2110, the anti-virus server determines whether the packet collection is completed. If the packet collection is completed, the procedure proceeds to step S2112; and, otherwise, the procedure returns to step S2108.

At step S2112, the anti-virus server checks that a virus exists in the assembled message with reference to virus information stored on a virus database 2100. The
virus database is provided in the anti-virus server.

At step S2114, the anti-virus server determines whether the assembled message is infected with the virus. If the assembled message is infected with the virus, the procedure proceeds to step S2118; and, otherwise, the procedure goes to step S2116.

At step S2116, the anti-virus server drops the duplicated packets, and the procedure is terminated.

At step S2118, the anti-virus server determines whether it is possible to cure the virus depending on the virus information. If it is possible to cure the virus, the procedure proceeds to step S2122; and, otherwise, the procedure goes to step S2120.

At step S2120, the anti-virus server deletes a portion of the assembled message, which is infected with the virus, and the procedure proceeds to step S2124.

At step S2122, the anti-virus server cures the virus, and the procedure proceeds to step S2124.

At step S2124, the anti-virus server determines whether a session corresponding to the assembled message exists. If the session exists, the procedure proceeds to step S2126. Otherwise, the procedure goes to step S2128 of Fig. 21B through a tap A.

At step S2126, the anti-virus server deletes the session, and the procedure is terminated.

At step S2128, the anti-virus server determines whether an integrated center exists. The integrated center may be provided in case that a plurality of integrated security gateway apparatus is employed in a VPN and controls the operations of the integrated security gateway apparatus. If the integrated center exists, the procedure proceeds to step S2136; and, otherwise, the procedure goes to step S2130.

At step S2130, the anti-virus server determines whether the intrusion detection system exists. If the intrusion detection system exists, the procedure proceeds
to step S2132; and, otherwise, the procedure goes to step S2134.

At step S2132, the anti-virus server transmits a warning message to the intrusion detection system, and the procedure proceeds to step S2138. The warning message includes information related to the virus.

At step S2134, the anti-virus server transmits the warning message to the inventive integrated security gateway apparatus, and the procedure proceeds to step S2138.

At step S2136, the anti-virus server transmits the warning message to the integrated center, and the procedure proceeds to step S2138.

At step S2138, the anti-virus server identifies a service type of the assembled message, and the procedure proceeds to step S2140.

At step S2140, the anti-virus server determines whether the assembled message uses an SMTP (simple mail transfer protocol). If the assembled message uses the SMTP, the procedure proceeds to step S2142; and, otherwise, the procedure proceeds to step S2144.

At step S2142, the anti-virus server deletes a service session corresponding to the assembled message, and the procedure proceeds to step S2144.

At step S2144, the anti-virus server transmits a result message related to the deletion, and the procedure is terminated.

At step S2148, the anti-virus server determines whether a mail session exists. If the mail session exists, the procedure proceeds to step S2152; and, otherwise, the procedure goes to step S2150.

At step S2150, the anti-virus server transmits a warning mail to a mail receiver account, and the procedure is terminated.

At step S2152, the anti-virus server inserts a warning message in a last portion of the assembled
message, i.e., a mail to be forwarded to the mail receiver, and the procedure is terminated.

Fig. 22 presents flow charts for explaining in detail a method for performing a noxious site blocking function in accordance with the present invention.

At step S2202, the inventive integrated security receives an incoming packet from the internal network or the external network, and the procedure proceeds to step S2204.

At step S2204, the inventive integrated security gateway apparatus compares a destination address of the incoming packet with noxious site addresses stored in a built-in database 2200, and the procedure proceeds to step S2206. The built-in database 2200 is provided in the inventive security gateway apparatus.

At step S2206, the inventive integrated security gateway apparatus determines whether the destination address corresponds to one of the noxious site addresses. If the destination address corresponds to one of the noxious site addresses, the procedure proceeds to step S2208; and, otherwise, the procedure goes to step S2212.

At step S2208, the inventive integrated security gateway apparatus transmits a warning packet to a user, and the procedure proceeds to step S2210. The warning packet includes a warning message and uses an HTTP (HyperText Transfer Protocol).

At step S2210, the inventive integrated security gateway apparatus deletes a session corresponding to the destination address, and the procedure is terminated.

At step S2212, the inventive integrated security gateway apparatus hold a communication between the destination address and an origination address of the incoming packet, and the procedure proceeds to step S2214. In other words, the incoming packet is transmitted to its destination.

At step S2214, the inventive integrated security
gateway apparatus duplicates the incoming packet, and the
procedure proceeds to step S2216.

At step S2216, the inventive integrated security
gateway apparatus transmits the duplicated packet to a
server for performing a noxious site blocking function
(hereinafter, referred to a noxious site blocking server),
and the procedure proceeds to step S2218.

At step S2218, the noxious site blocking server
receives the duplicated packet and compares the
destination address of the duplicated packet with noxious
site addresses stored on a noxious sites database 2210,
and the procedure proceeds to step S2220. The noxious
sites database 2210 is provided in the noxious site
blocking server.

At step S2220, the noxious site blocking server
determines whether the destination address corresponds to
one of the noxious site addresses stored on the database
2210. If the destination address corresponds to one of
the noxious site addresses, the procedure proceeds to
step S2226; and, otherwise, the procedure goes to step
S2222.

At step S2222, the noxious site blocking server
maintains a session related to the destination address,
and the procedure proceeds to step S2224.

At step S2224, the noxious site blocking server
permits a communication related to the destination
address and notifies the permission result to the
inventive integrated security gateway apparatus, and the
procedure is terminated.

At step S2226, the noxious site blocking server
transmits a warning packet including a warning message to
the user, and the procedure proceeds to step S2228.

At step S2228, the noxious site blocking server
deletes the session related to the destination address
and notifies the deletion result to the inventive
integrated security gateway apparatus, and the procedure
proceeds to step S2230.

At step S2230, the inventive integrated security gateway apparatus updates the noxious site addresses on the built-in database 2200 with reference to the deletion result, and the procedure is terminated.

While there has been described and illustrated various embodiments of the present invention, it will be apparent to those skilled in the art that variations and modifications are possible without deviating from the broad principles and teachings of the present invention which should be limited solely by the scope of the claims appended hereto.
CLAIMS:

1. An integrated security gateway apparatus interfacing with an internal network and an external network for blocking a selected packet from one of the internal network and the external network, the apparatus comprising:

   a packet duplicating module for receiving and duplicating an incoming packet from said one of the internal and external networks;

   a server complex, which is coupled to the packet duplicating module through a port complex, for analyzing the duplicated packet; and

   an inspection engine, which is connected to the packet duplicating module and to the server complex via the port complex, for inspecting whether or not the incoming packet corresponds to the selected packet to be blocked based on the analysis result and selectively blocking the incoming packet depending on the inspection result,

   wherein the server complex includes a plurality of servers for serving one of an intrusion detection function, an anti-virus function, and a noxious site blocking function, and

   the port complex includes a same number of black zone ports as said servers, each of the black zone ports being connected to one of said servers.

2. The apparatus of Claim 1, further comprising a hub module disposed between the packet duplicating module and the port complex, for simultaneously transmitting the duplicated packet to said servers through the port complex.

3. The apparatus of Claim 2, wherein the hub module is implemented by software program.
4. The apparatus of Claim 1, further comprising a load balancing module disposed between the packet duplicating module and the port complex, for transmitting the duplicated packet to each of said servers through the packet complex, depending on the load of each of said servers.

5. The apparatus of Claim 4, wherein the load balancing module is implemented by software program.

6. The apparatus of Claim 1, further comprising a traffic control module disposed between the packet duplicating module and the port complex, for collecting packets having an identical protocol among duplicated packets from the packet duplicating module and transmitting the identical protocol packets to each of said servers, depending on a predetermined priority of protocols.

7. The apparatus of Claim 6, wherein the traffic control module is implemented by software program.

8. The apparatus of Claim 2, further comprising a load balancing module disposed between the hub module and at least two black zone ports of the port complex, for transmitting the duplicated packet to each of said at least two black zone servers depending on the load of each of said at least two black zone servers.

9. The apparatus of Claim 8, wherein at least two of said black zone ports are connected to corresponding servers of the server complex serving same functions.

10. The apparatus of Claim 8, wherein the load balancing module is implemented by software program.
11. The apparatus of Claim 1, further comprising a switching module disposed between the packet duplicating module and the port complex, for enabling each of said servers to serve a different function to each other.

12. The apparatus of Claim 11, wherein the duplicated packet is transmitted to one of said servers depending on a function to be taken on the duplicated packet.

13. The apparatus of Claim 1, further comprising a TCP/IP (Transmission Control Protocol/Internet Protocol) protocol stack for transforming a layer of the duplicated packet from a physical layer to an application layer.

14. The apparatus of Claim 1, further comprising encrypting/decrypting means for encrypting the incoming packet if the incoming packet is from the internal network to the external network and decrypting otherwise.

15. The apparatus of Claim 14, wherein the encrypting/decrypting means uses different keys depending on a source and a destination of the incoming packet.

16. The apparatus of Claim 1, wherein the packet duplicating module and the inspection engine are implemented by software program.

17. The apparatus of Claim 1, wherein the analysis result is transmitted from the server complex to the inspection engine in the form of a message packet having information to be used in the blocking the incoming packet.

18. A networking system consisting of at least one internal network and an external network, comprising:
   an integrated security gateway interfacing with
said at least one internal network and said external network, for blocking a selected packet from said at least one internal network and said external network; and
black zone servers, which are coupled to the integrated security gateway for analyzing the duplicated packet,

wherein the integrated security gateway includes:
a packet duplicating module for receiving and duplicating an incoming packet from said at least one internal network and said external network; and
an inspection engine, which is connected to the packet duplicating module and to the black zone servers, for inspecting whether or not the incoming packet corresponds to the selected packet to be blocked based on the analysis result from the black zone servers and selectively blocking the incoming packet depending on the inspection result.

19. The system of Claim 18, wherein the black zone servers are connected to the packet duplicating module.

20. The system of Claim 19, wherein each of the black zone servers serves one of an intrusion detection function, an anti-virus function, and a noxious site blocking function.

21. The system of Claim 19, wherein the integrated security gateway includes a hub module disposed between the packet duplicating module and the black zone servers, for simultaneously transmitting the duplicated packet to each of the black zone servers.

22. The system of Claim 21, wherein the hub module is implemented by software program.

23. The system of Claim 19, wherein the integrated
security gateway includes a load balancing module disposed between the packet duplicating module and the black zone servers, for transmitting the duplicated packet to each of the black zone servers depending on the load of each of the black zone servers.

24. The system of Claim 23, wherein the load balancing module is implemented by software program.

25. The system of Claim 19, wherein the integrated security gateway includes a traffic control module disposed between the packet duplicating module and the black zone servers, for collecting packets having an identical protocol among duplicated packets from the packet duplicating module and transmitting the identical protocol packets to each of the black zone servers depending on a predetermined priority of protocols.

26. The system of Claim 25, wherein the traffic control module is implemented by software program.

27. The system of Claim 21, wherein the integrated security gateway further includes a load balancing module disposed between the hub module and at least two black zone servers of the black zone servers, for transmitting the duplicated packet to each of said at least two black zone servers depending on the load of each of said at least two black zone servers.

28. The system of Claim 27, wherein each of said at least two black zone servers serves a same function.

29. The system of Claim 27, wherein the load balancing module is implemented by software program.

30. The system of Claim 19, wherein the integrated
security gateway includes a switching module disposed between the packet duplicating module and the black zone servers, for enabling each of the black zone servers to serve a different function to each other.

31. The system of Claim 30, wherein the duplicated packet is transmitted to one of the black zone servers depending on a function to be taken on the duplicated packet.

32. The system of Claim 19, wherein the integrated security gateway includes encrypting/decrypting means for encrypting the incoming packet if the incoming packet is from the internal network to the external network and decrypting otherwise.

33. The system of Claim 32, wherein the encrypting/decrypting means uses different keys depending on a source and a destination of the incoming packet.

34. The system of Claim 18, wherein the analysis result is transmitted from the server complex to the inspection engine in the form of a message packet having information to be used in the blocking the incoming packet.

35. A method for blocking a selected packet from one of an internal network and an external network in an integrated security gateway apparatus interfacing with the internal and external networks, wherein the integrated security gateway apparatus includes a packet duplicating module for duplicating an incoming packet and an inspection engine, the method comprising the steps of:
   a) receiving a message packet from a server complex;
   b) determining whether or not the message packet containing information to be used in the blocking the
incoming packet which corresponds to the selected packet, wherein the incoming packet is transmitted from said one of the internal network and the external network;
c) determining a type of an attack depending on the message if the packet has the message; and, otherwise, dropping the packet;
d) setting access deny time to the incoming packet;
e) setting an attacker's address;
f) setting a destination address to be attacked by the attacker through the incoming packet;
g) determining whether or not there is a session connected to the destination address;
h) disconnecting the session, if there is the session connected to the destination address;
i) setting a timer to the incoming packet depending on the access deny time, if there is no the session connected to the destination address; and
j) denying a connection from the attacker to the destination address and vice versa by blocking the incoming packet.

36. The method of Claim 35, further comprising the steps of:
k) determining whether or not the access deny time has been passed; and
l) releasing the timer, if the access deny time has been passed; and, otherwise, returning to the step j).

37. The method of Claim 35, wherein the server complex includes a plurality of servers, each of which serves one of an intrusion detection function, an anti-virus function, and a noxious site blocking function.

38. The method of Claim 36, further comprising, before the step a), the steps of:
duplicating the incoming packet; and
-41-
transmitting the duplicated packet to the server complex,

wherein the duplicating and the transmitting steps are carried out at the packet duplicating module.

39. The method of Claim 38, further comprising, after the transmitting step, the steps of:

- receiving the duplicated packet;
- performing on the duplicated packet the intrusion detection, anti-virus, and noxious blocking functions to analyze the packet; and
- transmitting the message packet containing information according to the analysis result to the inspection engine,

wherein the receiving, the performing, and transmitting steps are carried out at the server complex.
Fig. 1
(Prior Art)

Dedicated leased lines/Packet-based Networks
Fig. 2
(Prior Art)
Fig. 7B

A

S711
NAT?

Yes
S712
NAT

No
S713
Encryption?

Yes
S714
Packet Encryption

No
S715
Forwarding?

Yes
S716
Check Port

No
S718
Processing

Forward Result

S719

S717
Forward Packet

End
Fig. 9B

A

Extract Packet Information

PATH2

Contents Filtering Required?

Yes

S924

Contents Filtering

No

S922

Encryption?

Yes

S928

Packet Encryption

No

S930

Forwarding

B

PATH1

Black Zone Port?

Yes

S936

Duplicate Packet

No

S932

S934

Abandon Packet

C

S938

Forwarding

End
Fig. 11A

Start

Receive Packet ~ S1102

Encrypted?

Yes ~ S1104

Packet Decryption ~ S1106

No

Session?

Yes S1108

No

Rule?

Yes ~ S1110

Create Session ~ S1112

Denied?

Yes ~ S1114

No

NAT?

Yes ~ S1116

NAT ~ S1118

No

A B
Fig. 11B

A

Extract Packet Information \( \rightarrow \) S1120

PATH2

Contents Filtering Required ?

Yes \( \rightarrow \) S1124

Contents Filtering

No \( \rightarrow \) S1126

Encryption ?

Yes \( \rightarrow \) S1128

Packet Encryption

No \( \rightarrow \) S1130

Forwarding

B

Check Session \( \rightarrow \) S1132

Determine BZ Port \( \rightarrow \) S1134

Duplicate Packet \( \rightarrow \) S1136

Forwarding \( \rightarrow \) S1138

End
Fig. 12
Fig. 13A

1. Start
2. Receive Packet (S1302)
3. Encrypted? (S1304)
   - Yes: Packet Decryption (S1306)
   - No: Proceed to next step
4. Session? (S1308)
   - No: Proceed to Rule (S1310)
   - Yes: Proceed to Create Session (S1312)
5. Rule? (S1310)
   - Yes: Proceed to Create Session (S1312)
   - No: Proceed to the next step
6. Denied? (S1314)
   - Yes: Proceed to NAT? (S1316)
   - No: Proceed to the next step
7. NAT? (S1316)
   - Yes: NAT (S1318)
   - No: Proceed to the next step

A and B
Fig. 13B

A

Extract Packet Information S1320

PATH2

Contents Filtering Required ?

Yes

Contents Filtering

S1322

No

Encryption ?

Yes

Packet Encryption S1328

S1326

No

Forwarding S1330

B

PATH1

S1324

S1332

Analyze Service

Determine BZ Port S1334

Duplicate Packet S1336

Forwarding S1338

End
Fig. 15
Fig. 16A

Start

Receive Packet

Encrypted?

Yes → Packet Decryption

No → Session?

Yes → Create Session

No → Rule?

Yes → Create Session

No → Denied?

Yes → NAT

No → NAT

A → B
Fig. 16B

A

Extract Packet Information

PATH2

S1622

Contents Filtering Required

Yes

Contents Filtering

S1624

No

S1626

Encryption

Yes

Packet Encryption

S1628

No

Forwarding

S1630

B

Check BZ Port Setting

S1632

No

Load Balancing required?

Yes

S1634

Check Session

S1636

Select BZ Port for the Session

S1638

Duplicate Packet

S1640

Forwarding

End
Fig. 18B

A
Extract Packet Information S1820

PATH2
Contents Filtering Required ?
Yes S1822
No

PATH1
Contents Filtering
S1824

S1826
Encryption ?
Yes S1828
No Forwarding S1830

B
Analyze Service
S1832

C
Pattern Information ?
No
Yes S1836

Compare Pattern
S1838

Write Action

End
Fig. 19

Start

S1902 ~ Receive Packet

No ~ S1904

IDS Message ~

Yes ~

S1908 ~ Determine type of Attack

S1910 ~ Set Access Deny Time

S1912 ~ Set Address of Attacker

S1914 ~ Set Destination Address

Drop Packet ~ S1906

S1920 ~ Set Timer

No ~

Deny Connection ~ S1922

Timeout ~ S1924

No ~

Yes ~

Release Timer ~ S1926

Permit Connection ~ S1928

End

S1916 ~

Session ~

Yes ~

Disconnect ~ S1918
### Fig. 20

<table>
<thead>
<tr>
<th>Source IP</th>
<th>Destination IP</th>
<th>Source Port</th>
<th>Destination Port</th>
<th>Protocol</th>
<th>Filter</th>
<th>Risk</th>
<th>Reserved</th>
<th>Hack Code 1</th>
<th>Hack Code 2</th>
<th>Lasting Time</th>
<th>Reserved</th>
<th>Destination Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>4byte</td>
<td>4byte</td>
<td>2byte</td>
<td>2byte</td>
<td>1byte</td>
<td>1byte</td>
<td>1byte</td>
<td>2byte</td>
<td>2byte</td>
<td>4byte</td>
<td>24byte</td>
<td>100byte</td>
<td></td>
</tr>
</tbody>
</table>

148byte
Fig. 21B

A

S2130

Intrusion Detection System?

Yes

S2132

Transmit Warning Message

No

S2134

Transmit Warning Message

A

S2128

Integrated Center?

Yes

S2136

Transmit Warning Message

No

S2138

Identify Service Type

S2140

SMTP?

No

Delete Service Session

S2142

Yes

Mail Session?

No

Transmit Result Message

S2144

Yes

Transmit Warning Mail

S2150

Insert Warning Message

S2152

B

End
Fig. 22

Start

Receive Packet

S2202

Built-in Database

Compare Destination Address

S2204

No

S2206

Noxious Site?

Yes

S2208

Transmit Warning Packet

Delete Session

S2210

A

Hold Communication

S2212

Duplicate Packet

S2214

Transmit Duplicated Packet

S2216

Compare Destination Address

S2218

No

Maintain Session

S2222

Yes

Transmit Warning Packet

S2226

Noxious Sites Database

2210

Permit Communication

S2224

Delete Session

S2228

Update Built-in Database

S2230

A

End
### A. CLASSIFICATION OF SUBJECT MATTER

IPC7 H04L 12/00   H04L 9/00   H04L 12/66   G06F 11/00

According to International Patent Classification (IPC) or to both national classification and IPC.

### B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC7 H04L 12/00   H04L 9/00   H04L 12/66   G06F 11/00

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

KOREAN PATENTS AND APPLICATIONS FOR INVENTIONS SINCE 1975
KOREAN UTILITY MODELS AND APPLICATIONS FOR UTILITY MODELS SINCE 1975

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

### C. DOCUMENTS CONSIDERED TO BE RELEVANT

<table>
<thead>
<tr>
<th>Category</th>
<th>Citation of document, with indication, where appropriate, of the relevant passages</th>
<th>Relevant to claim No.</th>
</tr>
</thead>
<tbody>
<tr>
<td>E. X</td>
<td>KR 2001-0112633 A (FUTURE SYSTEMS INC.) 20 DECEMBER 2001</td>
<td>1 - 34</td>
</tr>
<tr>
<td>A</td>
<td>JP 2001-160828 A (MATSUSHITA ELECTRIC CO. LTD.) 12 JUNE 2001</td>
<td>1, 18, 35</td>
</tr>
<tr>
<td>A</td>
<td>US 6,189,104 B1 (HARRIS CORP.) 13 FEBRUARY 2001</td>
<td>1, 18, 35</td>
</tr>
<tr>
<td>A</td>
<td>US 5,864,683 A (SECURE COMPUTING CORP.) 26 JANUARY 1999</td>
<td>1, 18, 35</td>
</tr>
<tr>
<td>A</td>
<td>JP 11-205388 A (HITACHI LTD.) 30 JULY 1999</td>
<td>1, 18, 35</td>
</tr>
</tbody>
</table>

- Further documents are listed in the continuation of Box C.
- See patent family annex.

- * Special categories of cited documents:
  - "A" document defining the general state of the art which is not considered to be of particular relevance
  - "E" earlier application or patent but published on or after the international filing date
  - "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of citation or other special reason (as specified)
  - "O" document referring to an oral disclosure, use, exhibition or other means
  - "P" document published prior to the international filing date but later than the priority date claimed

- Other document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
- "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
- "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
- "&" document member of the same patent family

Date of the actual completion of the international search
27 AUGUST 2002 (27.08.2002)

Date of mailing of the international search report
27 AUGUST 2002 (27.08.2002)

Name and mailing address of the ISA/KR
Korean Intellectual Property Office
920 Dunsan-dong, Seo-gu, Daejeon 302-701, Republic of Korea

Facsimile No. 82-42-472-7140

Authorized officer
HWANG, Eun Taek
Telephone No. 82-42-481-5688

Form PCT/ISA/210 (second sheet) (July 1998)