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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
23 February 2006 (23.02.2006)

PCT

(10) International Publication Number
WO 2006/019701 A2

(51) International Patent Classification:
H04L 12/56 (2006.01)

(21) International Application Number:
PCT/US2005/024592

(22) International Filing Date: 12 July 2005 (12.07.2005)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
10/910,194 2 August 2004 (02.08.2004) US

(71) Applicant *(for all designated States except US)*: **CISCO TECHNOLOGY, INC.** [US/US]; 170 West Tasman Drive, San Jose, CA 95134 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **HALL, Michael, Lee, Jr.** [US/US]; 9822 Mandeville Circle, Austin, TX 78750-2855 (US). **WILEY, Kevin, L.** [US/US]; 518 Arbors Circle, Austin, TX 78621 (US). **HOSSAIN, Munawar** [US/US]; 7405 Fireoak Drive, Austin, TX 78759 (US). **SIRRIANNI, Joseph, M.** [US/US]; 1314 Fall Creek Loop, Cedar Park, TX 78613 (US).

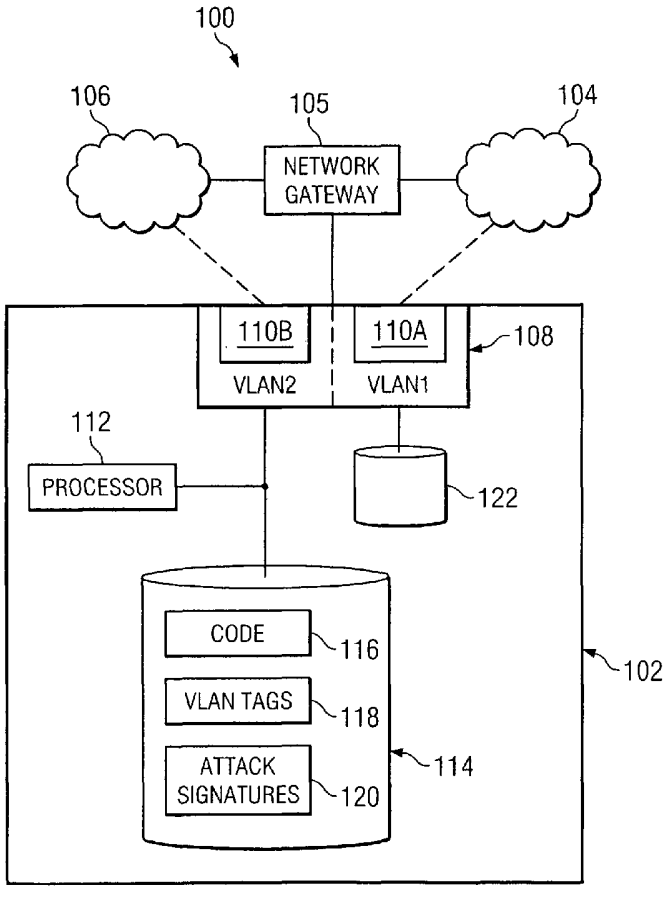
(74) Agent: **SHOWALTER, Barton, E.**; Baker Botts, L.L.P., 2001 Ross Avenue, Suite 600, Dallas, TX 75201 (US).

(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, NG, 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, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, NL, PL, PT,

[Continued on next page]

(54) Title: INLINE INTRUSION DETECTION USING A SINGLE PHYSICAL PORT



(57) Abstract: In accordance with one embodiment of the present invention, a method for inline intrusion detection includes receiving a packet at a physical interface of an intrusion detection system. The packet is tagged with a first VLAN identifier associated with an external network. The network further includes buffering the packet at the physical interface, communicating a copy of the packet to a processor, and analyzing the copy of the packet at the processor to determine whether the packet includes an attack signature. The method also includes communicating a reply message from the processor to the interface indicating whether the packet includes an attack signature. If the packet does not contain an attack signature the buffered copy of the packet is retagged with a second VLAN identifier associated with a protected network and re-tagged packet is communicated to the protected network.

WO 2006/019701 A2

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 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.

INLINE INTRUSION DETECTION USING A SINGLE PHYSICAL PORT

TECHNICAL FIELD OF THE INVENTION

The present invention relates generally to the field of network security, and more particularly to inline intrusion detection using a single physical port.

BACKGROUND OF THE INVENTION

Intrusion detection systems (IDSs) generally operate in one of two modes. In "promiscuous" mode, the IDS monitors incoming network traffic to determine whether a particular pattern characteristic of an intrusion can be observed. In "inline" mode, network traffic is scanned by the IDS to determine whether it contains a hostile signature. If a hostile signature is detected, the IDS prevents the network from receiving the traffic. Generally, inline IDSs have two physical ports, one coupled to the outside network and one coupled to the protected network. On the other hand, IDSs operating in promiscuous mode only need one physical port to receive network traffic.

SUMMARY OF THE INVENTION

In accordance with one embodiment of the present invention, a method for inline intrusion detection includes receiving a packet at a physical interface of an intrusion detection system. The packet is tagged with a first VLAN identifier associated with an external network. The network further includes buffering the packet at the physical interface, communicating a copy of the packet to a processor, and analyzing the copy of the packet at the processor to determine whether the packet

includes an attack signature. The method also includes communicating a reply message from the processor to the interface indicating whether the packet includes an attack signature. If the packet does not contain an attack signature the buffered copy of the packet is re-tagged with a second VLAN identifier associated with a protected network and re-tagged packet is communicated to the protected network.

In accordance with another embodiment of the present invention, an intrusion detection system includes an interface operable to receive a packet that is tagged with a first VLAN identifier associated with an external network. The interface is further operable to buffer the packet at the interface, communicate a copy of the packet to a processor, and re-tag the packet with a second VLAN identifier associated with a protected network. The intrusion detection system is also operable to communicate the packet to the protected network. The processor is operable to analyze the copy of the packet to determine if it includes an attack signature and communicate a reply message to the interface indicating whether the packet includes an attack signature. The interface re-tags and communicates the packet only if the reply message indicates that the packet does not include an attack signature.

Important technical advantages of certain embodiments of the present invention include inline intrusion detection using a single port. This allows single-port intrusion detection systems that may have been used for monitoring to be adapted for use as inline systems. Furthermore, it may provide a lower cost

alternative to multiple-port devices used for inline intrusion detection.

Other important technical advantages of certain embodiments of the present invention include more efficient use of memory and bus resources in an inline system. Re-tagging packets with a VLAN identifier can be performed at the physical interface. Thus, in contrast with systems that operate at higher layers, such as firewalls, certain embodiments of the present invention allow a packet to be buffered and re-tagged without having to be processed and returned by a processor. This reduces the amount of packet communication between the interface and the processor.

Additional technical advantages of the present invention will be readily apparent to one skilled in the art from the following figures, descriptions, and claims. Moreover, while specific advantages have been enumerated above, various embodiments may include all, some, or none of the enumerated advantages.

BRIEF DESCRIPTION OF THE DRAWINGS

For a more complete understanding of the present invention and its advantages, reference is now made to the following description, taken in conjunction with the accompanying drawings, in which:

FIGURE 1 illustrates an inline intrusion detection system using a single physical port; and

FIGURE 2 illustrates a flow chart showing an example method of operation for the inline intrusion detection system of FIGURE 1.

DETAILED DESCRIPTION OF EXAMPLE EMBODIMENTS OF THE INVENTION

FIGURE 1 illustrates a computer system 100 that includes an inline intrusion detection system (IDS) 102 between an external network 104 and a protected network 106. Generally, IDS 102 receives information from external network 104 and analyzes the information to determine whether the information includes a signature that is characteristic of a network attack or other hostile action. If an attack is detected, IDS 102 does not send the information to protected network 106. Otherwise, IDS 102 communicates the information to protected network 106.

External network 104 may include any collection of networked communication devices exchanging information. Networked communication devices may include hubs, routers, switches, gateways, personal computers, telephones, or any other device that can exchange information. Devices in external network 104 may exchange information in the form of packets, cells, frames, segments, or other portions of data (collectively referred to as "packets"). External network 104 may use any suitable medium or media of transmission, including wireline, wireless, or optical connections. Devices in external network 104 may communicate with one another using any number of suitable protocols, such as asynchronous transfer mode (ATM), transport control protocol / Internet protocol (TCP/IP), synchronous optical network (SONET), or Ethernet. External network 104 may also include the Internet.

Protected network 106 represents any collection of communication devices communicating in any suitable

manner. In particular, protected network 106 may include any of the devices and communication media discussed in conjunction with external network 104. Protected network 106 may also use one or more suitable communication protocols, such as the ones described above. In particular, protected network 106 supports the use of virtual local area networks (VLANs). A VLAN is a logical separation created between devices that share a physical network, so that devices on one VLAN cannot communicate with one another using the existing physical connections between the devices except through suitable network bridging hardware and/or software. VLANs are described in IEEE specification 802.1q.

Network gateway 105 represents any suitable hardware and/or software that communicates traffic received from external network 106 to protected network 106 and IDS 102. Traffic received from external network 106 is automatically tagged with an identifier for a first VLAN. Protected network 106 is configured to be on a second VLAN, so that it does not recognize traffice tagged with the identifier of the first VLAN. Thus, even though network gateway 105 may replicate the information to all of its ports, such as might take place in a network hub, the traffic will not be recognized by protected network 106 unless tagged with the proper VLAN identifier. Network gateway 105 includes a monitoring port that replicates the contents of incoming network traffic for IDS 102.

IDS 102 is an inline security system that receives traffic from external network 104, analyzes the traffic to determine if it contains an attack signature or other indication of hostile action, and prevents hostile

information from reaching protected network 106. In the depicted embodiment, IDS 102 includes an interface 108, a processor 112, and a memory 114. Processor 112 may be any hardware and/or software components suitable for processing information, such as microprocessors, microcontrollers, or digital signal processors (DSPs).

Memory 114 is any suitable form of information storage, which may include magnetic media, optical media, removable media, local storage, remote storage, or other suitable component. In the depicted embodiment, memory 114 stores code 116, VLAN tags 118, and attack signatures 120. Code 116 is executed by processor 112 to perform any suitable task associated with IDS 102. VLAN tags 118 are stored identifiers associated respectively with external network 104 and protected network 106. Attack signatures 120 are recognized patterns of information that indicate that an incoming packet represents a hostile action directed at protected network 106. Processor 112 compares information to attack signatures 120 to detect attacks.

Interface 108 represents a physical connection allowing communication between IDS 102 and devices on protected network 106 and external network 104. Communications with interface 102 take place at layer 2 of the Open Systems Interconnect (OSI) model. Interface 108 supports VLAN trunking. VLAN trunking allows interface 108 to recognize and communicate with multiple VLANs, each identified by a particular VLAN tag. Interface 108 therefore effectively includes multiple logical ports, each associated with a particular VLAN. Interface 108 may tag packets and change existing tags

appropriately so that a packet is communicated to a particular VLAN.

In the depicted embodiment, interface 108 establishes a first VLAN for external network 104 and a second VLAN for protected network 106. Thus, interface 108 has two logical ports 110A and 110B. Information received from external network 104 is tagged with the VLAN tag associated with the first VLAN network, so it is not recognized by protected network 106. Once the information is determined to be safe for protected network 106, interface 106 may re-tag the information with the tag of the second VLAN. This effectively communicates information to protected network 106 using logical port 110B, even though interface 108 only includes one physical connection.

Interface 108 also includes a buffer 122. Buffer 122 represents local information storage at interface 108. Buffer 122 may include any suitable form of information storage, such as magnetic media, flash memory, optical media, or other type of information storage medium. Buffer 122 stores incoming information from external network 104 while the information is processed by components of IDS 102. In a particular embodiment, buffer 122 retains a copy of incoming traffic while the traffic is being analyzed by processor 112 to determine whether the incoming information is hostile.

In one example of a mode of operation, network gateway 105 receives traffic from network and tags the traffic with a first VLAN identifier. Network gateway 105 may then broadcast the traffic to all of its ports or may communicate it to IDS 102 only. Protected network 106 is configured to recognize only information on a

second VLAN, so even if the packet is broadcast to protected network 106, it will not be recognized. IDS 102 receives the traffic at interface 108 and buffers the traffic in buffer 122. IDS 102 communicates a copy of the packet to processor 112, which analyzes the traffic to determine whether it includes an attack signature. Processor 112 then returns a message to IDS 102 indicating whether the packet includes an attack signature or not. If the packet includes an attack signature, then IDS 102 discards the packet from buffer 112. Otherwise, IDS 102 may re-tag the packet with a second VLAN identifier and communicate the packet back to network gateway 105, which in turn communicates the packet to protected network 106.

One technical advantage of certain embodiments of the present invention is the opportunity to conserve memory and bus resources in IDS 102. Since VLAN re-tagging may be performed at interface 108, interface 108 does not require additional processing resources to move a packet from one VLAN to another. Conversely, network protection systems that operate at higher layers, such as firewalls, typically require network address translation or other similar adjustments to packet header information. Such systems must forward a packet to the appropriate processing resource using an internal bus, and then receive a returned packet suitably modified for communication to the network protected by these systems. In contrast to these conventional systems, interface 108 may receive a reply message, which may be as short as a single bit, that indicates whether or not the packet should be communicated to protected network 106. Thus, IDS 102 may use less internal bus resources and also

reduce the load of buffer 122, which need not store both incoming packets and packets returned by processor 112.

FIGURE 2 is a flow chart 200 illustrating an example method of operation for IDS 102. IDS 102 receives a packet tagged for a first VLAN at step 202. IDS 102 buffer the packet at interface 108 at step 204. Interface 108 communicates a copy of the packet to processor 112 at step 206.

Processor 112 analyzes the packet by comparing the packet to attack signatures 120 at step 208. If an attack signature is detected at decision step 210, then processor 112 sends an alert to interface 108 at step 212. Interface 108 then discards the packet from buffer 122 at step 214. If an attack signature is not detected, processor 112 sends an OK message to interface 108 at step 216. Interface 108 re-tags the packet with the identifier for the second VLAN associated with protected network 106 at step 218. Interface 108 then communicates the packet to protected network 106 at step 220. The method may be repeated as long as there are incoming packets, as shown by decision step 220.

Although the present invention has been described with several embodiments, a myriad of changes, variations, alterations, transformations, and modifications may be suggested to one skilled in the art, and it is intended that the present invention encompass such changes, variations, alterations, transformations, and modifications as fall within the scope of the appended claims.

WHAT IS CLAIMED IS:

1. A method for inline intrusion detection, comprising:

receiving a packet at a physical interface of an intrusion detection system, wherein the packet is tagged with a first VLAN identifier associated with an external network;

buffering the packet at the physical interface;

communicating a copy of the packet to a processor;

analyzing the copy of the packet at the processor to determine whether the packet includes an attack signature;

communicating a reply message from the processor to the interface indicating whether the packet includes an attack signature; and

if the packet does not contain an attack signature:

re-tagging the buffered copy of the packet with a second VLAN identifier associated with a protected network; and

communicating the re-tagged packet to the protected network.

2. The method of Claim 1, further comprising:

receiving the packet from the external network at a network gateway;

tagging the packet with the first VLAN identifier at the network gateway; and

communicating the packet to the interface.

3. The method of Claim 2, wherein the step of communicating the re-tagged packet to the protected network comprises:

communicating the re-tagged packet to a first port of the network gateway; and

communicating the re-tagged packet to the protected network using a second port of the network gateway.

4. The method of Claim 2, wherein communicating the packet to the interface comprises:

generating a copy of the packet for each of a plurality of ports of the network gateway, wherein one of the ports is coupled to the interface; and

communicating one of the copies of the packet from each of the ports.

5. The method of Claim 1, wherein the size of the reply message is less than the size of the packet.

6. Logic embodied in a computer-readable medium operable to perform the steps of:

receiving a packet at a physical interface of an intrusion detection system, wherein the packet is tagged with a first VLAN identifier associated with an external network;

buffering the packet at the physical interface;

communicating a copy of the packet to a processor;

analyzing the copy of the packet at the processor to determine whether the packet includes an attack signature;

communicating a reply message from the processor to the interface indicating whether the packet includes an attack signature; and

if the packet does not contain an attack signature:

re-tagging the buffered copy of the packet with a second VLAN identifier associated with a protected network; and

communicating the re-tagged packet to the protected network.

7. The logic of Claim 6, further operable to perform the steps of:

receiving the packet from the external network at a network gateway;

tagging the packet with the first VLAN identifier at the network gateway; and

communicating the packet to the interface.

8. The logic of Claim 7, wherein the step of communicating the re-tagged packet to the protected network comprises:

communicating the re-tagged packet to a first port of the network gateway; and

communicating the re-tagged packet to the protected network using a second port of the network gateway.

9. The logic of Claim 7, wherein the step of communicating the packet to the interface comprises:

generating a copy of the packet for each of a plurality of ports of the network gateway, wherein one of the ports is coupled to the interface; and

communicating one of the copies of the packet from each of the ports.

10. The logic of Claim 6, wherein the size of the reply message is less than the size of the packet.

11. A system, comprising:

means for receiving a packet at a physical interface of an intrusion detection system, wherein the packet is tagged with a first VLAN identifier associated with an external network;

means for buffering the packet at the physical interface;

means for communicating a copy of the packet to a processsor, wherein the processor is operable to analyze the copy of the packet at the processor to determine whether the packet includes an attack signature;

means for communicating a reply message from the processor to the interface indicating whether the packet includes an attack signature; and

means for re-tagging the buffered copy of the packet with a second VLAN identifier associated with a protected network if the packet does not contain an attack signature; and

means for communicating the re-tagged packet to the protected network.

12. The system of Claim 11, further comprising:

means for receiving the packet from the external network at a network gateway;

means for tagging the packet with the first VLAN identifier at the network gateway; and

means for communicating the packet to the interface.

13. An intrusion detection system, comprising:

an interface operable to:

receive a packet, wherein the packet is tagged with a first VLAN identifier associated with an external network;

buffer the packet at the interface;

communicate a copy of the packet to a processor;

re-tag the packet with a second VLAN identifier associated with a protected network; and

communicate the packet to the protected network; and

the processor operable to:

analyze the copy of the packet to determine if it includes an attack signature; and

communicate a reply message to the interface indicating whether the packet includes an attack signature, wherein the interface re-tags and communicates the packet only if the reply message indicates that the packet does not include an attack signature.

14. The system of Claim 13, further comprising a network gateway operable to:

receive the packet from the external network;

tag the packet with the first VLAN identifier at the network gateway; and

communicate the packet to the interface.

15. The system of Claim 14, wherein:

the interface is further operable to communicate the re-tagged packet to a first port of the network gateway; and

the network gateway is further operable to communicate the re-tagged packet to the protected network using a second port of the network gateway.

16. The system of Claim 14, wherein the network gateway is further operable to:

generate a copy of the packet for each of a plurality of ports of the network gateway, wherein one of the ports is coupled to the interface; and

communicate one of the copies of the packet from each of the ports.

17. The system of Claim 13, wherein the size of the reply message is less than the size of the packet.

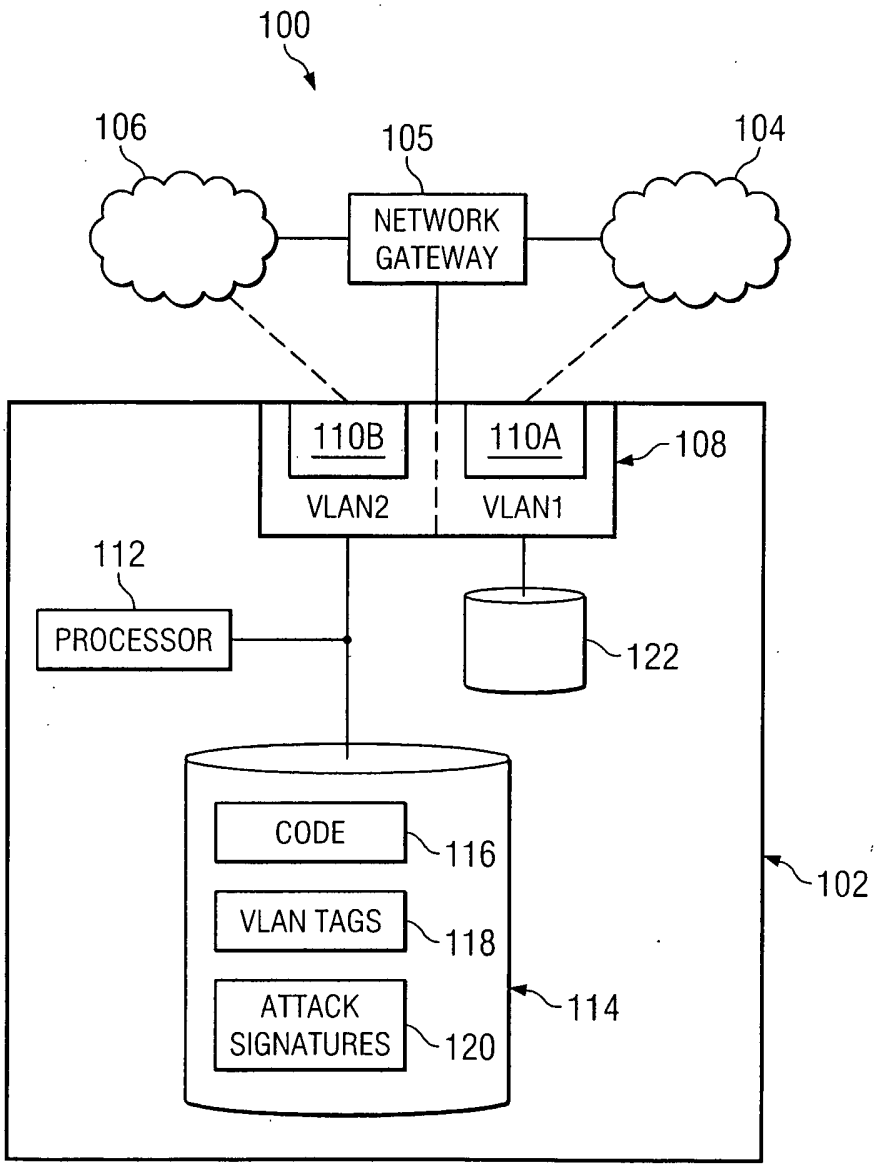
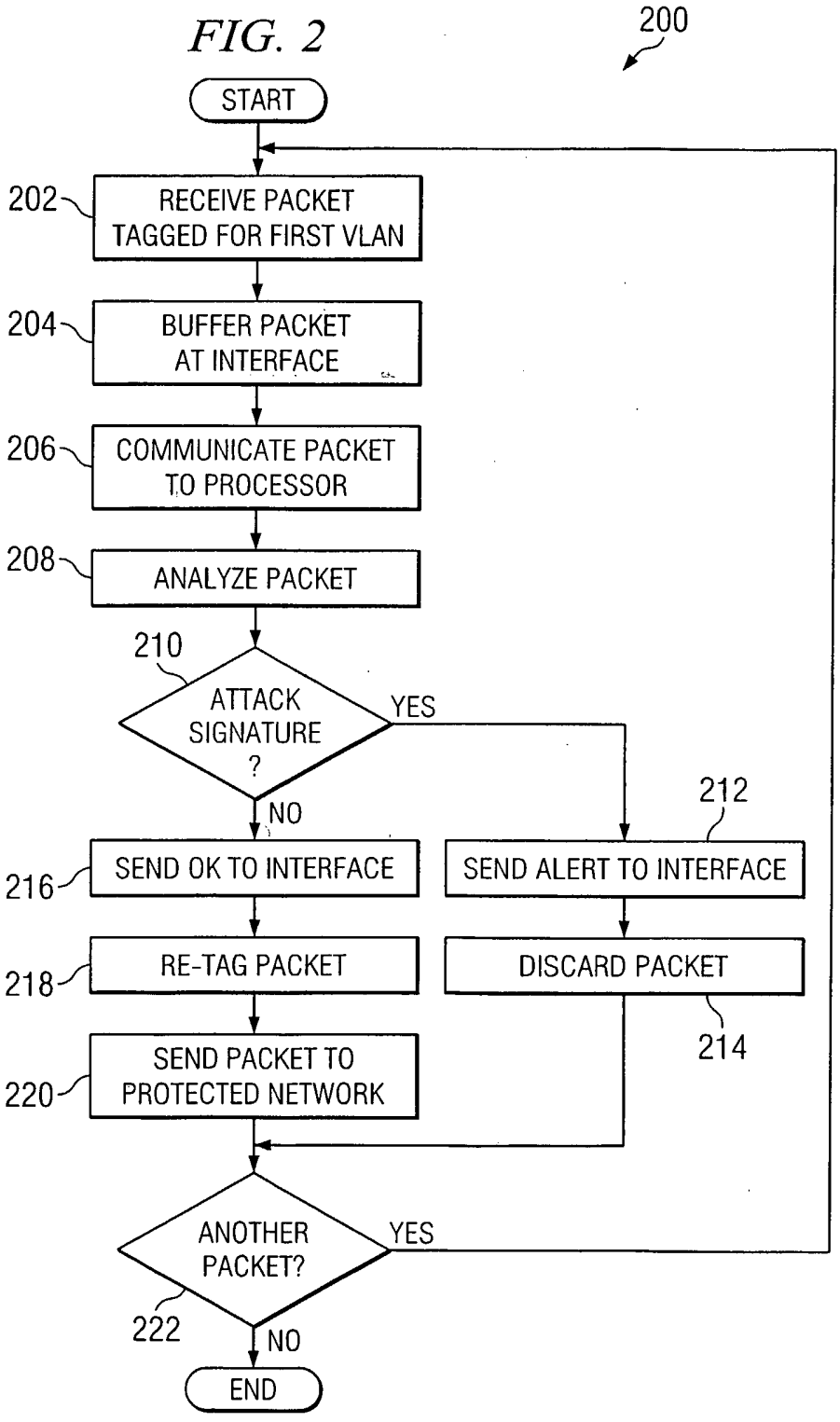

100
106
105
104
NETWORK GATEWAY
110B
110A
108
VLAN2
VLAN1
112
PROCESSOR
122
CODE
116
VLAN TAGS
118
ATTACK SIGNATURES
120
114
102

FIG. 1

FIG. 2


200
START
202
RECEIVE PACKET TAGGED FOR FIRST VLAN
204
BUFFER PACKET AT INTERFACE
206
COMMUNICATE PACKET TO PROCESSOR
208
ANALYZE PACKET
210
ATTACK SIGNATURE ?
YES
NO
212
SEND ALERT TO INTERFACE
DISCARD PACKET
214
216
SEND OK TO INTERFACE
218
RE-TAG PACKET
220
SEND PACKET TO PROTECTED NETWORK
ANOTHER PACKET?
YES
222
NO
END