

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

NETSKOPE, INC.,

Petitioner,

v.

FORTINET, INC.,

Patent Owner.

PTAB Case No. IPR2023-00459

Patent No. 10,084,825 B2

PETITIONER'S DEMONSTRATIVES FOR ORAL ARGUMENT

Netskope, Inc. v. Fortinet, Inc.

IPR2023-00459

Patent 10,084,825 B2

Claims 1-7 and 10-31

Petitioner Netskope's Demonstratives

Oral Hearing
June 21, 2024

Overview

1. The Board Correctly Construed “Fabric”
2. Patent Owner’s Proposed Construction Is Wrong
3. The Prior Art Discloses a Cooperative Security Fabric

Overview

- 1. The Board Correctly Construed “Fabric”**
2. Patent Owner’s Proposed Construction Is Wrong
3. The Prior Art Discloses a Cooperative Security Fabric

1. The Board Correctly Construed “Fabric”

Board’s Construction of “Fabric”

“a network topology such as the physical structure of a switch or network”

1. The Board Correctly Construed “Fabric”

Board’s Construction of “Fabric”

“a network topology such as the physical structure of a switch or network”

Institution Decision

Nonetheless, we provide the following guidance for the meaning of “fabric,” in claims 1, 15, 21, and 27 to assist the parties in the upcoming trial, and encourage the parties to address this term at the appropriate stages of the trial. At this stage of the proceeding, based on the current record, we interpret “fabric” as “a network topology such as the physical structure of a switch or network.” This is consistent with an ordinary, customary meaning. Ex. 2003, 3 (defining a “fabric” as “[a] descriptive term referring to the physical structure of a switch or network.”) (cited in Prelim. Resp. 12).

This meaning is consistent with Patent Owner’s assertion that “fabric” is an “interconnected topology” in “enterprise networks.” Prelim. Resp. 10. Patent Owner’s declarant, Dr. Black, testifies that “[a]s enterprise networks became larger and larger, a complex, interconnected topology known as a ‘fabric’ was developed to handle the management of such networks.” Ex. 2001 ¶ 44 (cited in Prelim. Resp. 10). Dr. Black testifies that “a fabric of network devices (such as switches or access points for each subnetwork) was developed to manage network traffic between subnetworks, and to and from the Internet.” *Id.*

1. The Board Correctly Construed “Fabric”

Board’s Construction of “Fabric”

“a network topology such as the physical structure of a switch or network”

Institution Decision

This meaning is consistent with the ’825 patent, which describes a private *network 120 topology* of computers and servers coupled together by a local area network (LAN) or a wireless LAN. Ex. 1001, 5:3–9, Fig. 1. “FIG. 2 shows a *topology 200 of a cooperative security fabric* that consists of network security appliances of FIG. 1.” *Id.* at 5:50–51 (emphasis added). Root node 220 corresponds to network security appliance 121 and acts as a wide area network (WAN) role in topology 200 to connect a private network to other networks or the Internet. *Id.* at 5:52–56. It is the outermost network security appliance of the cooperative security fabric. *Id.* at 5:52–55.

The ’825 patent defines “connected” or “coupled” as not limited to a direct connection or coupling so devices may be coupled via intermediate media or devices, and information can pass between them without sharing any physical connection between them. Ex. 1001, 4:43–53.

Patent Owner argues that Keohane is unidirectional and not a “fabric.” Prelim. Resp. 21–23. As discussed for Ground 1, a “fabric” does not require bidirectional communications under an ordinary, customary meaning of fabric as a topology of network connections as Keohane teaches. Ex. 1008 ¶¶ 22–32. Claim 1 only requires communication in one direction as well.

1. The Board Correctly Construed “Fabric”

Board’s Construction of “Fabric”

“a network topology such as the physical structure of a switch or network”

‘825 Patent

Systems and methods for coordinating security operations among members of a cooperative security fabric (CSF) are provided. According to one embodiment, a first network security appliance of a CSF receives incoming network traffic and determines whether the network traffic has been transmitted from a second network security appliance based on a flag carried by one or more packets of the network traffic. If the incoming network traffic is from the second network security appliance, the first network security appliance determines network security operations that are executed by the second network security appliance and then determines local network security operations. The first network security appliance executes the local network security operations on the network traffic.

Therefore, there is a need for a cooperative security fabric (CSF) that may coordinate operations performed on network traffic to avoid or reduce redundant operations among members of the CSF.

‘825 at Abstract;1:64-67

1. The Board Correctly Construed “Fabric”

Board’s Construction of “Fabric”

“a network topology such as the physical structure of a switch or network”

‘825 Patent

1. A method comprising:

receiving, by a first network security appliance of a private network that is participating in a cooperative security fabric (CSF), network traffic that is to be inspected by the first network security appliance;

determining, by the first network security appliance, whether the network traffic has been transmitted from a second network security appliance that is participating in the CSF based on a flag carried by one or more packets of the network traffic;

when the network traffic is determined to have been transmitted from the second network security appliance:

determining, by the first network security appliance, one or more network security operations that are executed by the second network security appliance;

determining, by the first network security appliance, one or more local network security operations that are to be executed by the first network security appliance based on the one or more network security operations that are executed by the second network security appliance, including skipping, by the first network security appliance, the one or more network security operations that are executed by the second network security appliance; and

executing, by the first network security appliance, the one or more local operations on the network traffic.

1. The Board Correctly Construed “Fabric”

Board’s Construction of “Fabric”

“a network topology such as the physical structure of a switch or network”

- PO does not dispute that Chandra and Keohane disclose a “CSF” under the Board’s interpretation

‘825 Patent

1. A method comprising:

receiving, by a first network security appliance of a private network that is participating in a cooperative security fabric (CSF), network traffic that is to be inspected by the first network security appliance;

determining, by the first network security appliance, whether the network traffic has been transmitted from a second network security appliance that is participating in the CSF based on a flag carried by one or more packets of the network traffic;

when the network traffic is determined to have been transmitted from the second network security appliance:

determining, by the first network security appliance, one or more network security operations that are executed by the second network security appliance;

determining, by the first network security appliance, one or more local network security operations that are to be executed by the first network security appliance based on the one or more network security operations that are executed by the second network security appliance, including skipping, by the first network security appliance, the one or more network security operations that are executed by the second network security appliance; and

executing, by the first network security appliance, the one or more local operations on the network traffic.

Overview

1. The Board Correctly Construed “Fabric”
- 2. Patent Owner’s Proposed Construction Is Wrong**
3. The Prior Art Discloses a Cooperative Security Fabric

2. Patent Owner’s Proposed Construction Is Wrong

Board’s Construction of “Fabric”	Patent Owner’s Proposed Construction of “Cooperative Security Fabric”
“a network topology such as the physical structure of a switch or network”	“a topology of network security appliances that cooperate to inspect incoming and outgoing traffic along multiple interconnected paths”

2. Patent Owner’s Proposed Construction Is Wrong

Board’s Construction of “Fabric”	Patent Owner’s Proposed Construction of “Cooperative Security Fabric”
“a network topology such as the physical structure of a switch or network”	“a topology of network security appliances that cooperate to inspect <u>incoming and outgoing</u> traffic along multiple interconnected paths”

Patent Owner argues that Keohane is unidirectional and not a “fabric.” Prelim. Resp. 21–23. As discussed for Ground 1, a “fabric” does not require bidirectional communications under an ordinary, customary meaning of fabric as a topology of network connections as Keohane teaches. Ex. 1008 ¶¶ 22–32. Claim 1 only requires communication in one direction as well.

ID at 30

2. Patent Owner's Proposed Construction Is Wrong – Incoming/Outgoing

'825 Patent

1. A method comprising:

receiving, by a first network security appliance of a private network that is participating in a cooperative security fabric (CSF), network traffic that is to be inspected by the first network security appliance;
determining, by the first network security appliance, whether the network traffic has been transmitted from a second network security appliance that is participating in the CSF based on a flag carried by one or more packets of the network traffic;

2. Patent Owner's Proposed Construction Is Wrong – Incoming/Outgoing

'825 Patent

1. A method comprising:
receiving, by a first network security appliance of a private network that is participating in a cooperative security fabric (CSF), network traffic that is to be inspected by the first network security appliance;
determining, by the first network security appliance, whether the network traffic has been transmitted from a second network security appliance that is participating in the CSF based on a flag carried by one or more packets of the network traffic;

'825 Patent

Therefore, there is a need for a cooperative security fabric (CSF) that may coordinate operations performed on network traffic to avoid or reduce redundant operations among members of the CSF.

1:64-67

'825 Patent

Systems and methods for coordinating security operations among members of a cooperative security fabric (CSF) are provided. According to one embodiment, a first network security appliance of a CSF receives incoming network traffic and determines whether the network traffic has been transmitted from a second network security appliance based on a flag carried by one or more packets of the network traffic. If the incoming network traffic is from the second network security appliance, the first network security appliance determines network security operations that are executed by the second network security appliance and then determines local network security operations. The first network security appliance executes the local network security operations on the network traffic.

2:3-19

2. Patent Owner’s Proposed Construction Is Wrong

Board’s Construction of “Fabric”	Patent Owner’s Proposed Construction of “Cooperative Security Fabric”
“a network topology such as the physical structure of a switch or network”	“a topology of network security appliances that cooperate to inspect incoming and outgoing traffic along <u>multiple interconnected paths</u> ”

2. Patent Owner's Proposed Construction Is Wrong – Multiple Interconnected Paths

'825 Patent

1. A method comprising:

receiving, by a first network security appliance of a private network that is participating in a cooperative security fabric (CSF), network traffic that is to be inspected by the first network security appliance;

determining, by the first network security appliance, whether the network traffic has been transmitted from a second network security appliance that is participating in the CSF based on a flag carried by one or more packets of the network traffic;

when the network traffic is determined to have been transmitted from the second network security appliance:

determining, by the first network security appliance, one or more network security operations that are executed by the second network security appliance;

determining, by the first network security appliance, one or more local network security operations that are to be executed by the first network security appliance based on the one or more network security operations that are executed by the second network security appliance, including skipping, by the first network security appliance, the one or more network security operations that are executed by the second network security appliance; and

executing, by the first network security appliance, the one or more local operations on the network traffic.

2. Patent Owner's Proposed Construction Is Wrong – Multiple Interconnected Paths

'825 Patent

1. A method comprising:

receiving, by a first network security appliance of a private network that is participating in a cooperative security fabric (CSF), network traffic that is to be inspected by the first network security appliance;

determining, by the first network security appliance, whether the network traffic has been transmitted from a second network security appliance that is participating in the CSF based on a flag carried by one or more packets of the network traffic;

when the network traffic is determined to have been transmitted from the second network security appliance:

determining, by the first network security appliance, one or more network security operations that are executed by the second network security appliance;

determining, by the first network security appliance, one or more local network security operations that are to be executed by the first network security appliance based on the one or more network security operations that are executed by the second network security appliance, including skipping, by the first network security appliance, the one or more network security operations that are executed by the second network security appliance; and

executing, by the first network security appliance, the one or more local operations on the network traffic.

'825 Patent

In a large network, many network security appliances may be deployed at different locations within the network. Network traffic transmitted to/from the network may go through multiple network security appliances along a path within the network. Usually, a network security appliance may be

1:33-37

2. Patent Owner’s Proposed Construction Is Wrong

Board’s Construction of “Fabric”	Patent Owner’s Proposed Construction of “Cooperative Security Fabric”
“a network topology such as the physical structure of a switch or network”	“a topology of network security appliances that cooperate to inspect incoming and outgoing traffic along multiple interconnected paths”

PO’s Additional “Hidden” Limitations

- 1. “CSF” **cannot** inspect internal network traffic, i.e., traffic from one part of the network to another. (POR, 20; Black Depo. Tr., 33:11-15.)
- 2. “CSF” only processes traffic transmitted **from the Internet** into the network and from the network **to the Internet**. (POR, 20; Black Depo. Tr., 70:10-13.)
- 3. “CSF” requires **three or more** interconnected security appliances. (Black Depo. Tr., 19:2-7.)
- 4. “CSF” **cannot be “a single thread.”** (POR, 12.)

2. Patent Owner's Proposed Construction Is Wrong – Internal Network Traffic

Patent Owner Reply

virtual private network.”); Ex. 2004, ¶59. Again, the '825 patent does not describe that its CSF inspects internal network traffic—instead, the '825 patent is concerned with and directed to “downstream network traffic that is transmitted from the Internet 110 to a subnet,” or “upstream network traffic that is transmitted from [a] subnet ... to the Internet.” Ex. 1001, 5:32-36. And such traffic does not include VPN traffic, which is considered to be internal traffic. Ex. 2004, ¶60.

POR at 20

Patent Owner Expert

Q. So in -- under your construction of a CSF, can a CSF process internal traffic?

A. No, at least not in the '825. It doesn't ever process traffic that is strictly internal. It's neither ingoing nor outgoing traffic.

Black Depo. Tr. at 33:11-15

Patent Owner Sur-reply

not supported by the evidence. POPR 10. Not true. Patent Owner's construction requires that cooperative inspection of incoming and outgoing traffic, as established by the intrinsic and extrinsic evidence—whether or not it *also* inspects internal traffic is simply not within the scope of the claims.

Sur-reply at 7.

2. Patent Owner's Proposed Construction Is Wrong – Only Internet Traffic

Patent Owner Reply

virtual private network.”); Ex. 2004, ¶59. Again, the '825 patent does not describe that its CSF inspects internal network traffic—instead, the '825 patent is concerned with and directed to “downstream network traffic that is transmitted from the Internet 110 to a subnet,” or “upstream network traffic that is transmitted from [a] subnet ... to the Internet.” Ex. 1001, 5:32-36. And such traffic does not include VPN traffic, which is considered to be internal traffic. Ex. 2004, ¶60.

POR at 20

Patent Owner Expert

A. Right. So the CSF is not directed toward finding insider attacks. We typically call that an insider attack, if somebody within the network is the attacker. And those do occur in real life, you have insider attacks.

So the CSF is directed toward testing information coming from external sources on the Internet into the root node and then into -- or the reverse, leaving the internal network and going out.

Patent Owner Sur-reply

whether a CSF could perform other tasks. Ex. 1018, 70:5-13. Dr. Black's testimony also did not limit CSF to inspecting Internet-only traffic. *Id.*, 32:1-

Sur-reply at 20

2. Patent Owner's Proposed Construction Is Wrong – Three or More Appliances

Patent Owner Reply

A. So in the '825 patent, the fabric is of the so-called network security appliances. And there I would say that the word "fabric" is used to describe several, I would say three or more of these NSAs, these network security appliances, that are all interconnected via multiple paths.

Black Depo. Tr. at 19:2-7

Provisional

[00026] According to one embodiment CSF 100 can be dynamically constructed and maintained in a recursive way based on the downstream-upstream relationships defined by the hierarchical interconnection of the network security devices within the private network. For example, NSD 1 102, having no parent, may initially represent a CSF containing only one member. The other NSDs 104a-i, having one or more upstream NSDs, may join the CSF to which its parent belongs as described further below. Once CSF 100 stabilizes, the root node, i.e., NSD 1 102, has full information regarding CSF 100.

Provisional, ¶32

downstream node/NSD from sending queries to its upstream node/NSD. In general, when an upstream NSD queries a downstream NSD, the query is passed from the forward daemon of the upstream NSD (which may be referred to herein as an "uplevel daemon") to the backend daemon of an intermediate NSD, if any (which may be referred to herein as a "downlevel daemon") and ultimately to the destination NSD. When the query reaches the destination

2. Patent Owner's Proposed Construction Is Wrong – Cannot Be a Single Thread

Patent Owner Reply

have cables weaving ... through buildings.” Ex. 2005, 7:25-8:8. Yet according to Petitioner, just two computers connected via cable—a single “thread” in the clothing analogy—would qualify as a “fabric.” Petitioner’s position runs against common sense: a single thread is not a fabric. Ex. 2004,

POR at 12

Provisional

[00026] According to one embodiment CSF 100 can be dynamically constructed and maintained in a recursive way based on the downstream-upstream relationships defined by the hierarchical interconnection of the network security devices within the private network. For example, NSD 1 102, having no parent, may initially represent a CSF containing only one member. The other NSDs 104a-i, having one or more upstream NSDs, may join the CSF to which its parent belongs as described further below. Once CSF 100 stabilizes, the root node, i.e., NSD 1 102, has full information regarding CSF 100.

Provisional

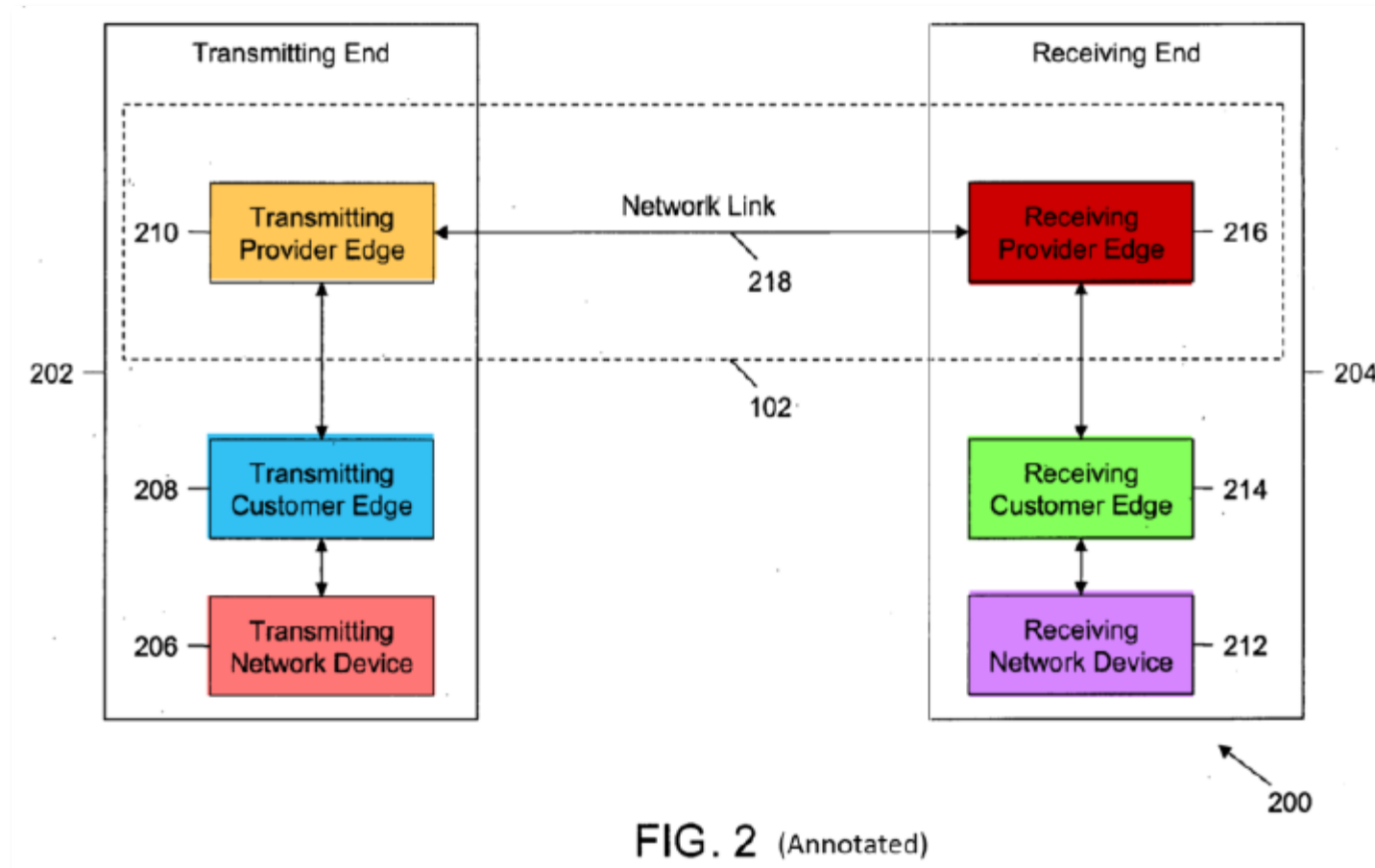
1. A method comprising:
dynamically constructing a cooperative security fabric (CSF) of a plurality of network security devices deployed within a protected network in a form of a tree, having a plurality of nodes, including a root node, one or more intermediate nodes and one or more leaf nodes, based on hierarchical interconnections among the plurality of network security devices by determining a relative upstream or downstream relationship among each network security device of the plurality of network security devices, wherein each node of a plurality of nodes within the CSF represents a network security device of the plurality of network security devices and each node of the CSF, except the root node and the one or more leaf nodes, includes both a parent node and one or more child nodes;

Overview

1. The Board Correctly Construed “Fabric”
2. Patent Owner’s Proposed Construction Is Wrong
- 3. The Prior Art Discloses a Cooperative Security Fabric**

3. The Prior Art Discloses a CSF - Chandra

PO does not dispute that Chandra discloses a “CSF” under the Board’s interpretation.



Reply, 6-7

3. The Prior Art Discloses a CSF - Chandra

Chandra also discloses a “CSF” under PO’s construction.

Notably, Chandra describes what happens when traffic comes from the Internet—however, in that embodiment, there is no cooperation between multiple network security appliances, as claimed. Ex. 2004, ¶94. Rather, all of Chandra’s “actions” are performed by just the “receiving customer edge.” Specifically, Chandra discloses that, “when receiving CE 214 receives a data packet from the Internet, it performs actions corresponding to rules regarding such data packets.” *Id.*, ¶53; *see also* ¶77 (“[R]eceiving end can identify a data packet from the Internet as insecure, and perform rigorous actions on it.”). As

POR, 36-37

3. The Prior Art Discloses a CSF - Chandra

Chandra also discloses a “CSF” under PO’s construction.

’825 Patent – Claim 4

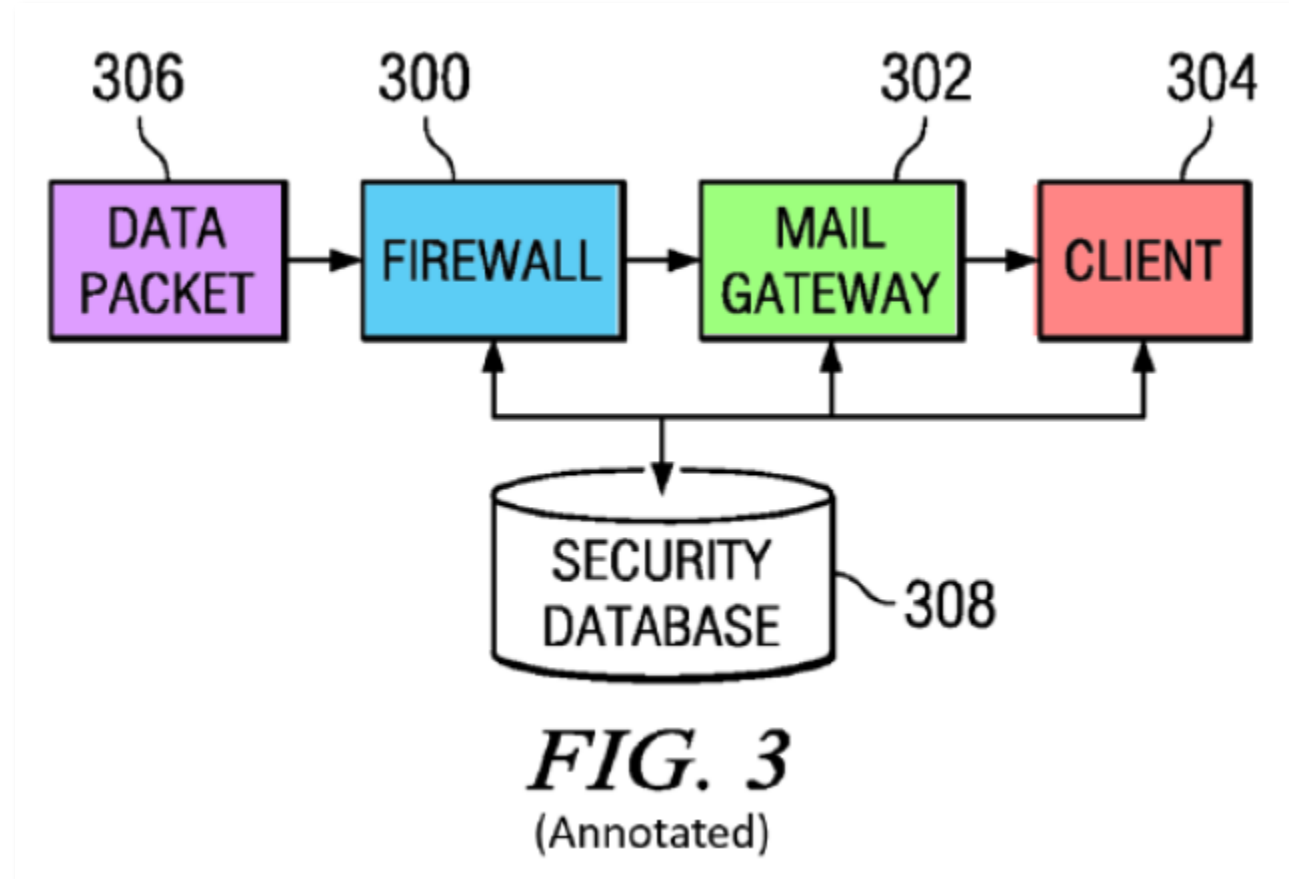
Notably, Chandra describes what happens when traffic comes from the Internet—however, in that embodiment, there is no cooperation between multiple network security appliances, as claimed. Ex. 2004, ¶94. Rather, all of Chandra’s “actions” are performed by just the “receiving customer edge.” Specifically, Chandra discloses that, “when receiving CE 214 receives a data packet from the Internet, it performs actions corresponding to rules regarding such data packets.” *Id.*, ¶53; see also ¶77 (“[R]eceiving end can identify a data packet from the Internet as insecure, and perform rigorous actions on it.”). As

POR, 36-37

4. The method of claim 1, further comprising when the network traffic is not transmitted from the second network security appliance, executing, by the first network security appliance, one or more local network security operations specified by one or more local policies.

3. The Prior Art Discloses a CSF - Keohane

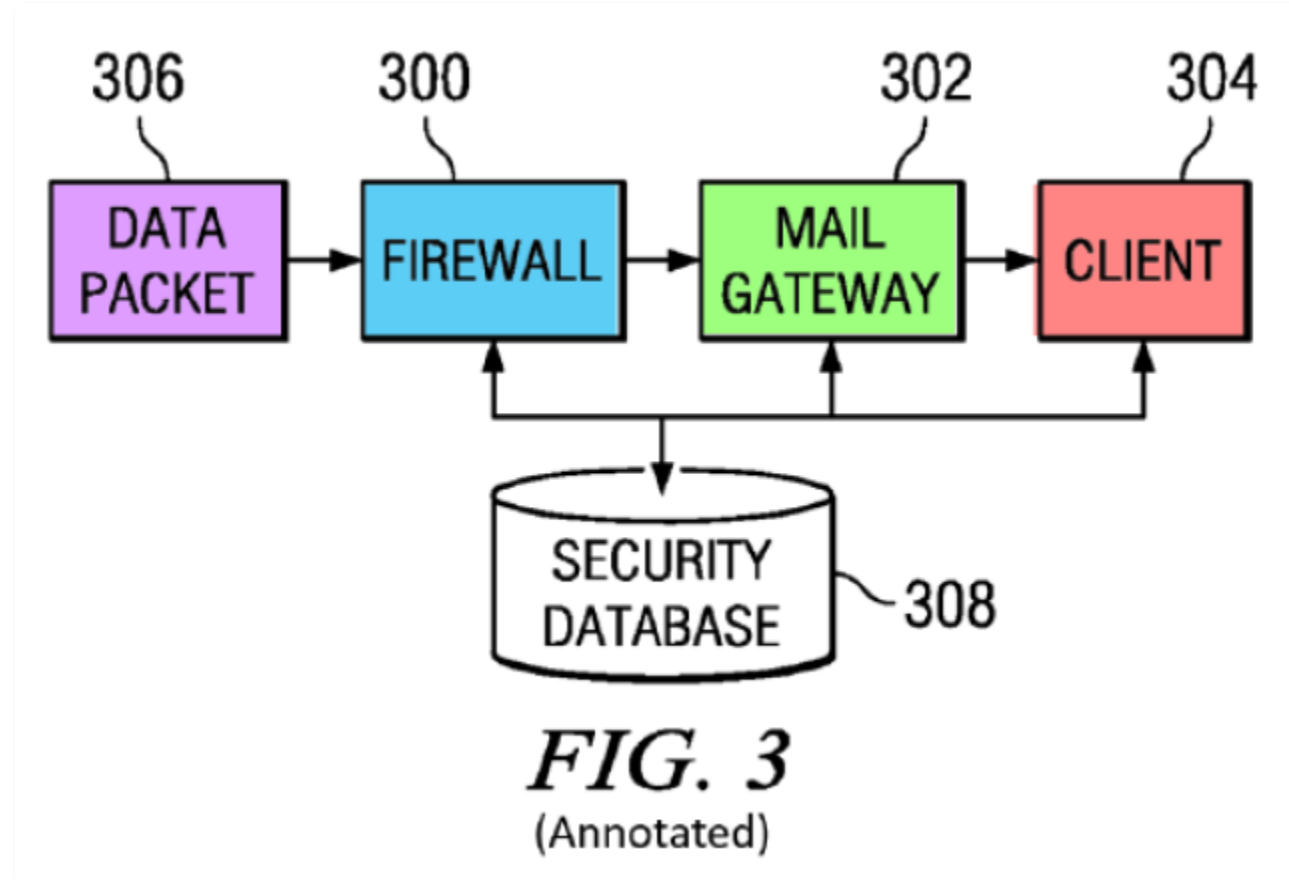
PO does not dispute that Keohane discloses a “CSF” under the Board’s interpretation.



Reply, 7-9

3. The Prior Art Discloses a CSF - Keohane

Keohane also discloses a “CSF” under PO’s construction.



Reply, 20-22

3. The Prior Art Discloses a CSF - Keohane

Keohane also discloses a “CSF” under PO’s construction.

Keohane. As Dr. Black explained, in order to have multiple paths even though all appliances are in a single line, as is the case in Keohane, traffic would have to be able to enter *the network* via multiple nodes. Ex. 1018, 23:15-22 (“It could be if traffic can enter, let’s say, the middle one in that line and then go left and out, but it could also enter the middle and then go right. As long as there are separate paths that the traffic can follow, then yes. But if the traffic

Sur-reply, 13

gateway 302 only receives traffic from firewall 300. Petitioner points to Keohane’s “signature[s]” but those signatures *only* “indicate[] that a previous security action has been performed on the data packet.” Ex. 1008 at Abstract.

Sur-reply, 14-15

2004, ¶138. This is because the very purpose of a signature is to authenticate that a message truly came from a certain sender—in Keohane’s case, the signature *also* authenticates which security actions were performed by the sender. *Id.*; Ex. 1008, ¶34. If a signature could be easily altered, then the

POR, 57

Reply, 20-22

3. The Prior Art Discloses a CSF - Keohane

Keohane also discloses a “CSF” under PO’s construction.

unidirectional path. Ex. 2004, ¶121. Keohane also only describes inspecting incoming network traffic—there is no disclosure that Keohane’s Mail Gateway and Firewall cooperate to inspect outgoing network traffic. *Id.*

POR, 50

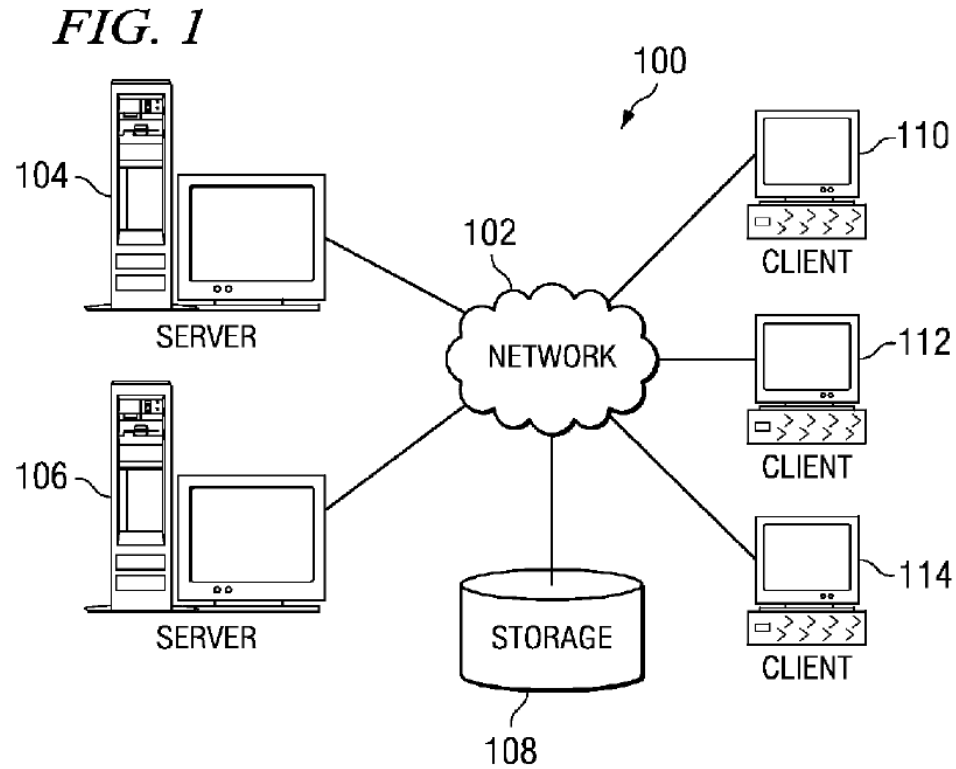
Patent Owner argues that Keohane is unidirectional and not a “fabric.” Prelim. Resp. 21–23. As discussed for Ground 1, a “fabric” does not require bidirectional communications under an ordinary, customary meaning of fabric as a topology of network connections as Keohane teaches. Ex. 1008 ¶¶ 22–32. Claim 1 only requires communication in one direction as well.

ID, 30

Reply, 20-22

3. The Prior Art Discloses a CSF - Keohane

Keohane also discloses a “CSF” under PO’s construction.



[0023] In the depicted example, server 104 and server 106 connect to network 102 along with storage unit 108. In addition, clients 110, 112, and 114 connect to network 102. These clients 110, 112, and 114 may be, for example, personal computers or network computers. In the depicted example, server 104 provides data, such as boot files, operating system images, and applications to clients 110, 112, and 114. Clients 110, 112, and 114 are clients to server 104 in this example. These clients and servers may include software and/or hardware used to perform security actions to remove malware from data packets received by them. Further, network 102 also includes devices such as routers, gateways, and firewalls that may have software/hardware to perform security actions with respect to malware. Network data processing system 100 may include additional servers, clients, and other devices not shown.

Chandra – “local network policies” (Claims 2, 4, 15)

Transmitting CE labels			
	Label	Rules	Receiving CE
	1256	Rules A and B	Address of receiving CE 214
	1257	Rules C and D	Address of receiving CE 214
	<untagged>	Rule E	Address of receiving CE 214
Receiving CE labels	...		
	Label	Rules	Transmitting CE
	1256	Rules A and B	Address of transmitting CE 208
	1257	Rules C and D	Address of transmitting CE 208
	<untagged>	Rule E	Address of transmitting CE 208
	...		

Chandra CE Labels

Pet., 37-38; Reply, 23-24

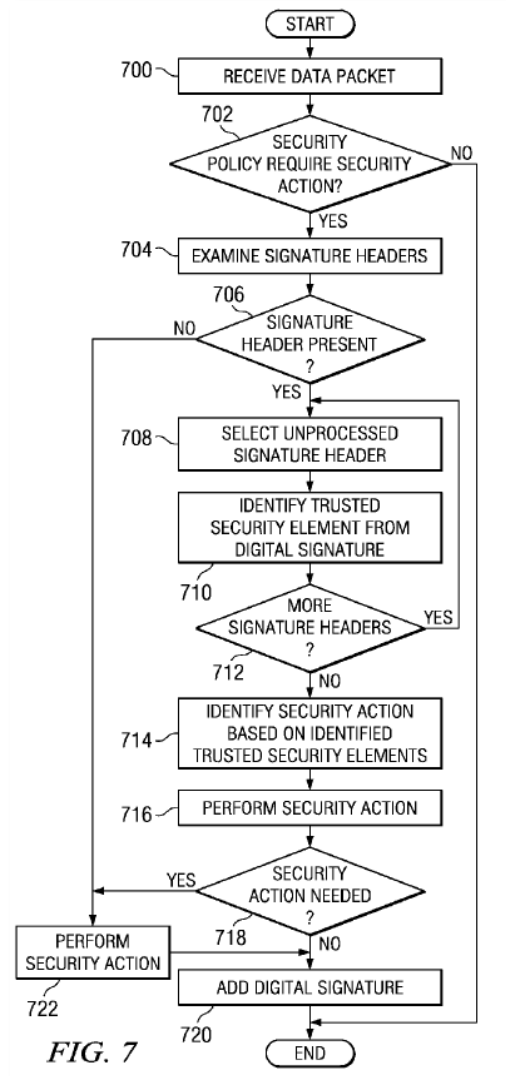
Chandra – “a first packet of a session” (Claim 12)

Transmitting CE labels			
	Label	Rules	Receiving CE
	1256	Rules A and B	Address of receiving CE 214
	1257	Rules C and D	Address of receiving CE 214
Receiving CE labels	<untagged>	Rule E	Address of receiving CE 214
	...		
Receiving CE labels			
	Label	Rules	Transmitting CE
	1256	Rules A and B	Address of transmitting CE 208
	1257	Rules C and D	Address of transmitting CE 208
Receiving CE labels	<untagged>	Rule E	Address of transmitting CE 208
	...		

Chandra CE Labels

Reply, 23-24

Keohane – “a first packet of a session” (Claim 12)

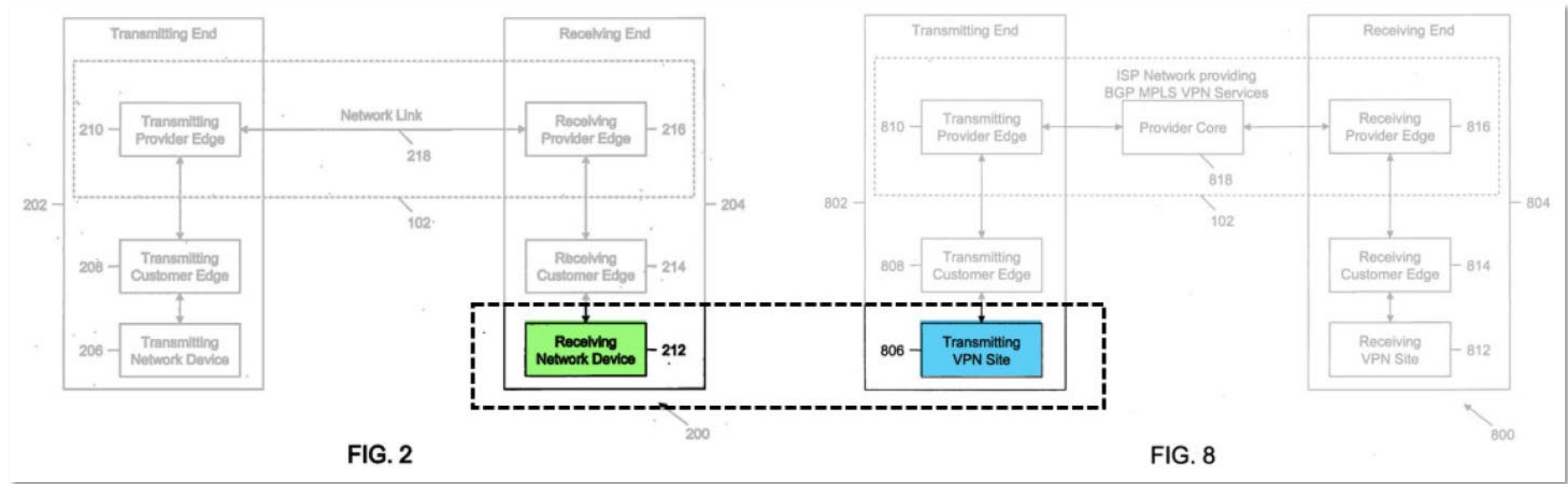


Chandra

[0028] Further, system **200** includes a CE and a PE associated with each network device from network devices **104**, in accordance with an embodiment of the present invention. It should be noted that a CE is not limited to be associated with only a single network device from network devices **104**. A plurality of such network devices can be associated with a single CE. Further, it should also be noted that a plurality of such CEs can be associated with a single PE.

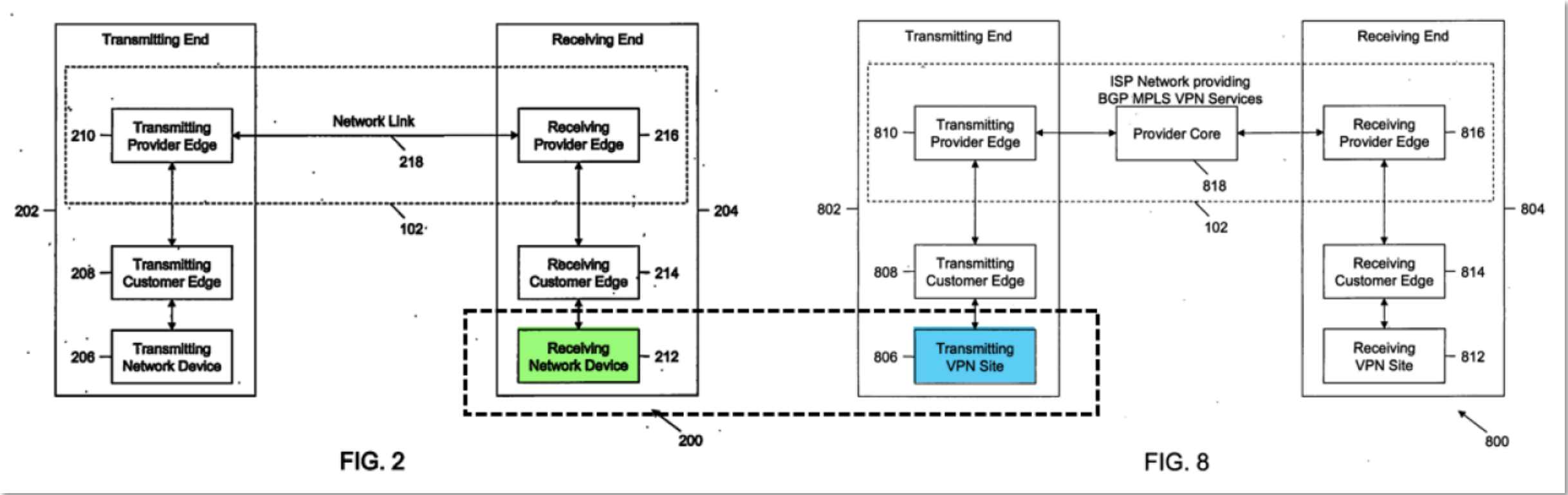
Chandra – “next network appliance” and “next network appliance participating in a CSF”
(Claims 6, 7, 17, 18, 23, 24, 28, 29)

Chandra Figs 2 and 8 (redrawn and annotated)



Chandra – “next network appliance” and “next network appliance participating in a CSF”
(Claims 6, 7, 17, 18, 23, 24, 28, 29)

Chandra Figs 2 and 8 (redrawn and annotated)



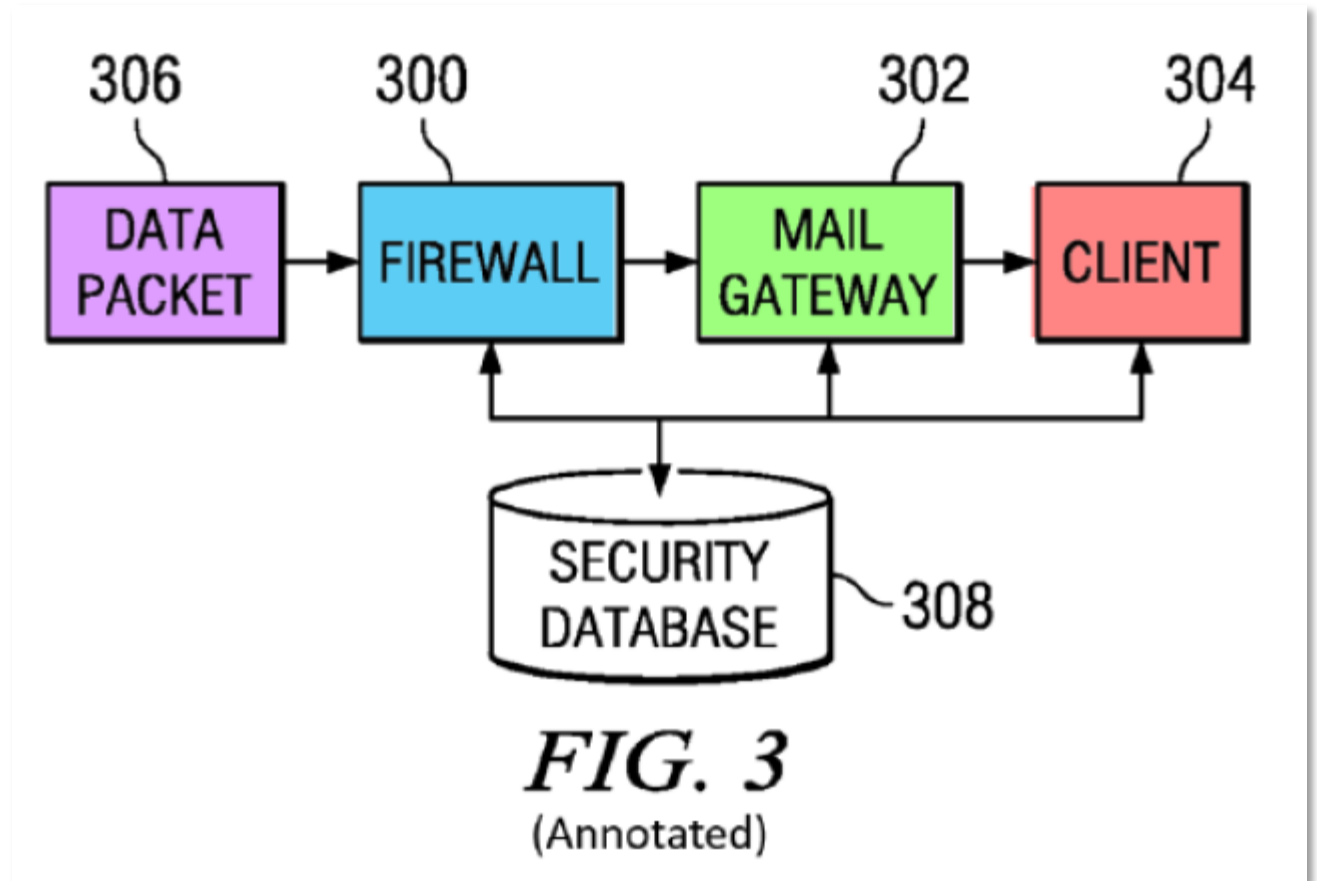
Keohane – “next network appliance” and “next network appliance participating in a CSF” (Claims 6, 7, 17, 18, 23, 24, 28, 29)

The phrase “network appliance” generally refers to a specialized or dedicated device for use on a network in virtual or physical form. Some network appliances are implemented as general-purpose computers with appropriate software configured for the particular functions to be provided by the network appliance; others include custom hardware (e.g., one or more custom Application Specific Integrated Circuits (ASICs)). Examples of functionality that

’825 patent, 4:1-8

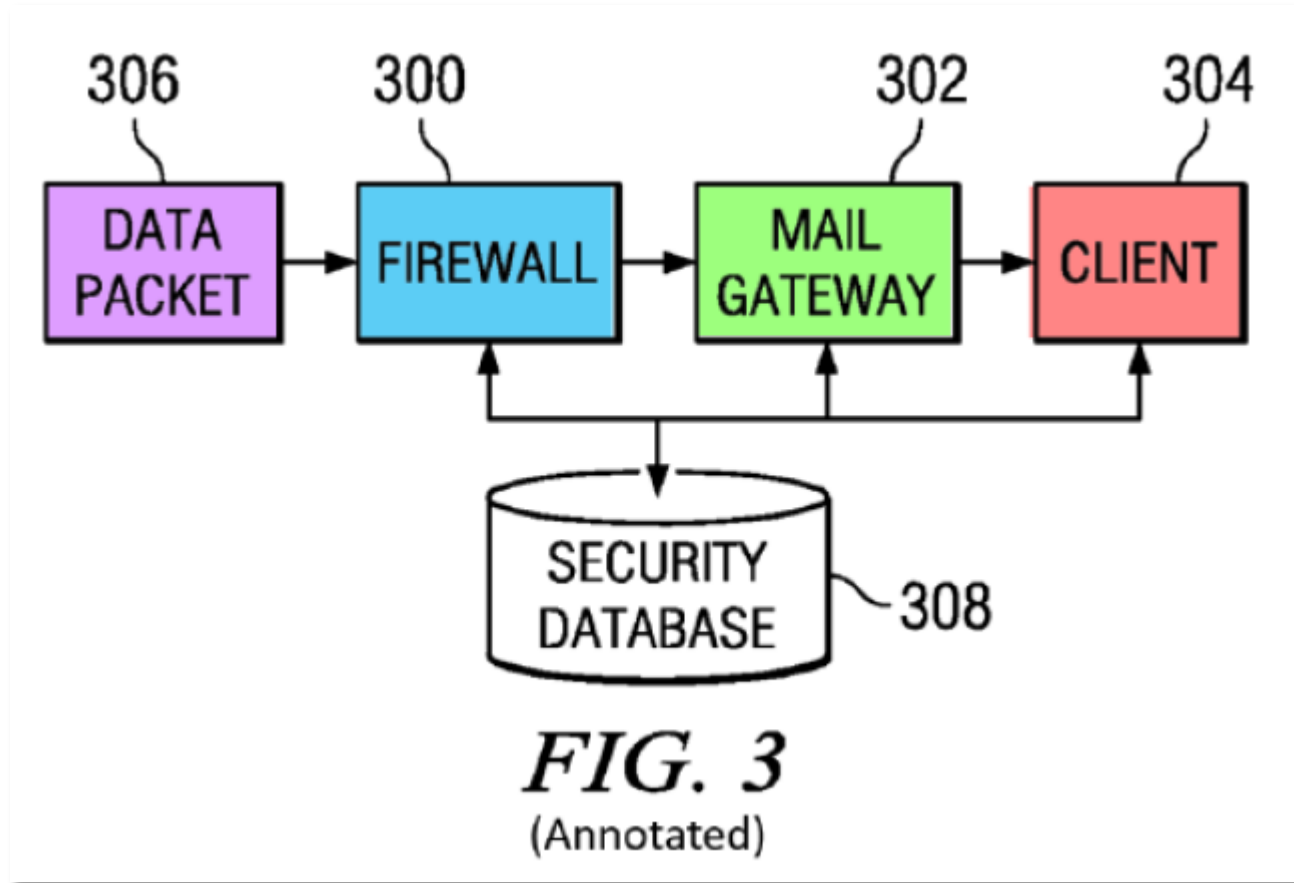
[0023] In the depicted example, server 104 and server 106 connect to network 102 along with storage unit 108. In addition, clients 110, 112, and 114 connect to network 102. These clients 110, 112, and 114 may be, for example, personal computers or network computers. In the depicted example,

Keohane, ¶23



Keohane Fig. 3 (annotated)

Keohane – “not transmitted from the second network security appliance” (Claim 4)



Keohane Fig. 3 (annotated)

a digital signature.” Ex. 1008, ¶¶34-35. However, a POSITA would have understood that a purpose of a digital signature is to prevent tampering. Ex. 2004, ¶138. This is because the very purpose of a signature is to authenticate that a message truly came from a certain sender—in Keohane’s case, the signature also authenticates which security actions were performed by the sender. *Id.*; Ex. 1008, ¶34. If a signature could be easily altered, then the POR at 57

Keohane – updating flags (Claims 6, 17, 23, 28)

Keohane

[0038] In these examples, the determination of what security actions have been taken may be identified by a code in the signature. For example, a code of “01” or “policy 1” may indicate that the source of the data packet is a trusted source. A code of “02” or “policy 2” may indicate that a virus scan has been performed by the trusted element. The codes may also indicate particular types of scanning mechanisms that were used to scan the data packet. These codes may be located at firewall **300**, mail gateway **302**, and client **304**.

Franz Rebuttal Declaration

72. To the contrary, updating the signature could still ensure that the signature indicated a secure source, as long as all the security appliances along the data paths were previously authenticated with each other. The whole point about a CSF is that it is collaborative and the participants trust each other. It would be obvious that the CSF participants could use a common pre-shared cryptographic key to prevent non-members from tampering with the signature while each of the CSF members would be able to decrypt, update, and then re-encrypt the signature. Keohane’s signatures contained codes indicating what security actions were performed and whether the source of the data packet was a secure source. (Keohane ¶38, Franz, ¶174, 186-87.) The signature could be easily updated to modify the codes or add more codes in the same signature.

Keohane – removing flags (Claims 7, 18, 24, 29)

Keohane

[0038] In these examples, the determination of what security actions have been taken may be identified by a code in the signature. For example, a code of “01” or “policy 1” may indicate that the source of the data packet is a trusted source. A code of “02” or “policy 2” may indicate that a virus scan has been performed by the trusted element. The codes may also indicate particular types of scanning mechanisms that were used to scan the data packet. These codes may be located at firewall **300**, mail gateway **302**, and client **304**.

Franz Rebuttal Declaration ¶73

(POR, 60.) However, while Keohane was not so limited, it would be obvious for a POSITA to implement a version of Keohane where the client only ever received data packets from an upstream network security appliance participating in the CSF and performed no security actions of its own. This would be the obvious configuration in an enterprise network in which clients would be connecting to the enterprise’s networking infrastructure. As I explained in my opening declaration, in this situation where the client “was not one of the network devices that could read and utilize the [flag] to cooperate network operations (Franz, ¶231)”, it would be obvious to remove the signature for reasons provided in my Opening Declaration (Franz, ¶230-31) because the signature lost its purpose of authenticating the source and record previous security actions.

Background: '825 Patent

What is claimed is:

1. A method comprising:

receiving, by a first network security appliance of a private network that is participating in a cooperative security fabric (CSF), network traffic that is to be inspected by the first network security appliance;

determining, by the first network security appliance, whether the network traffic has been transmitted from a second network security appliance that is participating in the CSF based on a flag carried by one or more packets of the network traffic;

when the network traffic is determined to have been transmitted from the second network security appliance:

determining, by the first network security appliance, one or more network security operations that are executed by the second network security appliance;

determining, by the first network security appliance, one or more local network security operations that are to be executed by the first network security appliance based on the one or more network security operations that are executed by the second network security appliance, including skipping, by the first network security appliance, the one or more network security operations that are executed by the second network security appliance; and

executing, by the first network security appliance, the one or more local operations on the network traffic.

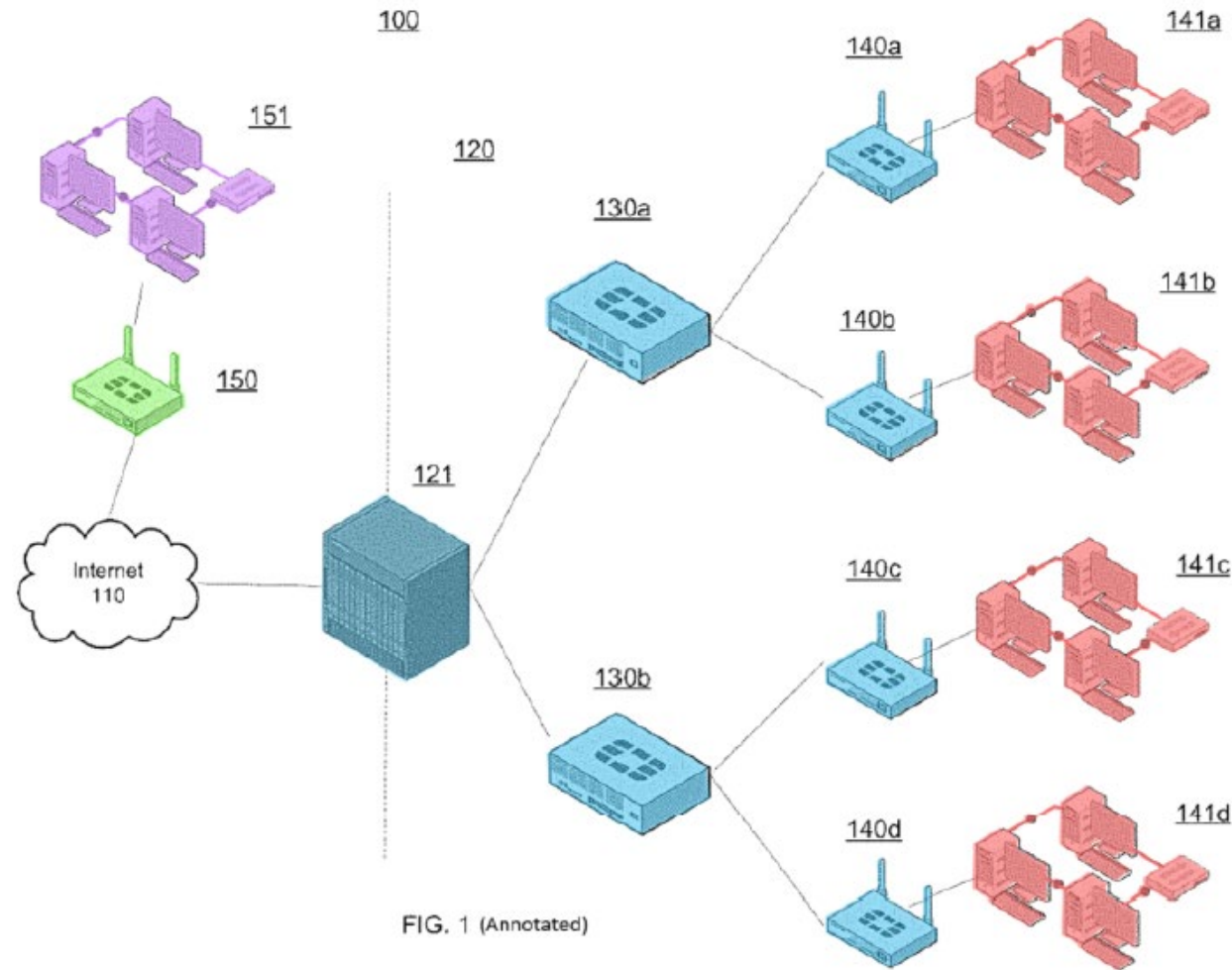
'825 patent

PETITIONER'S DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

Background: the '825 Patent

subnet 151

subnet network
security appliance 150



network security
appliances 121, 130a and
130b, 140a-140d

subnets 141a-141d

Background: '825 Patent

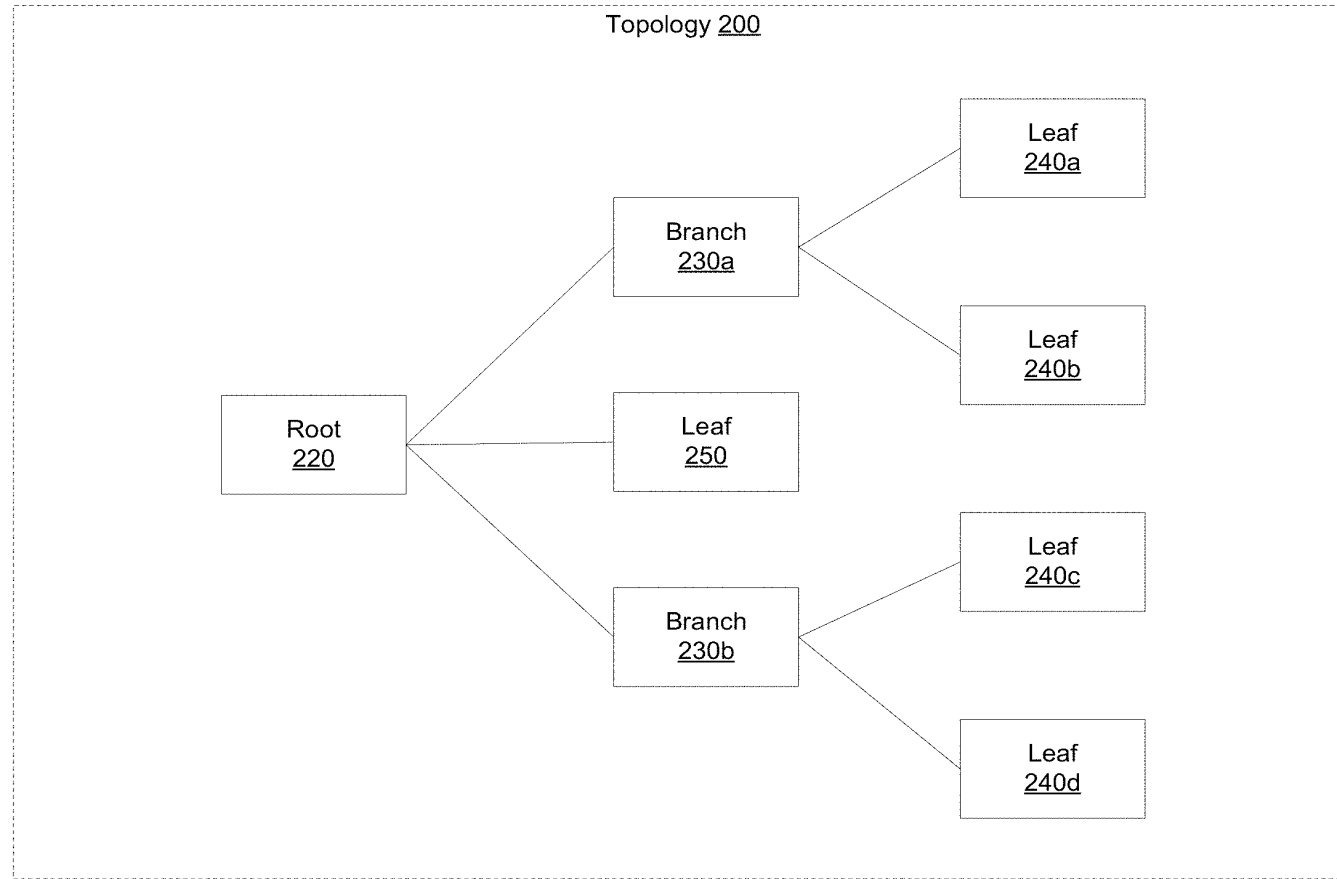
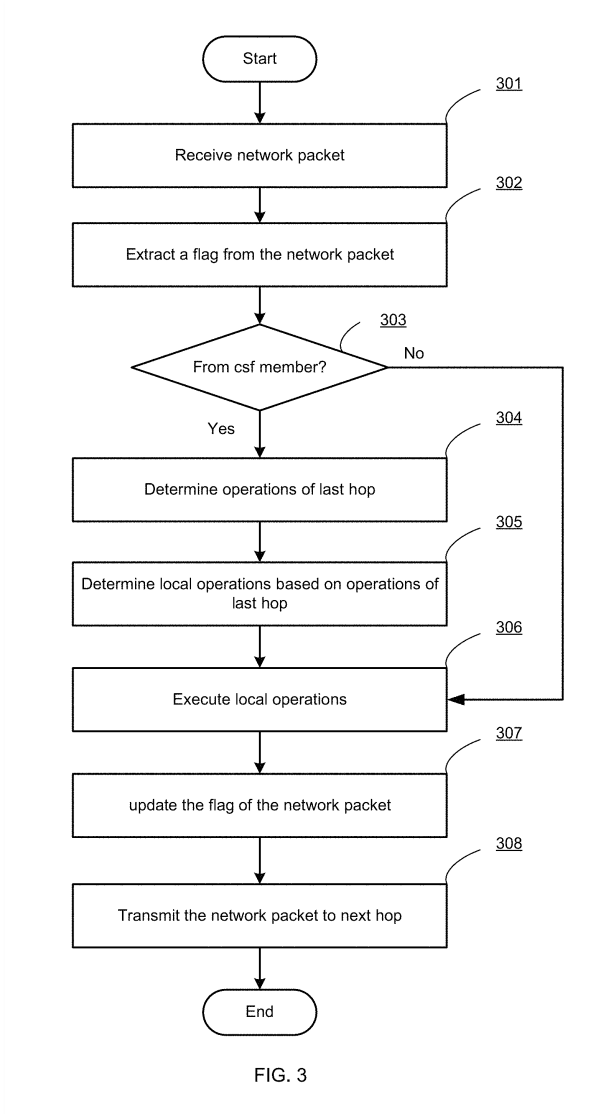


FIG. 2

'825 patent

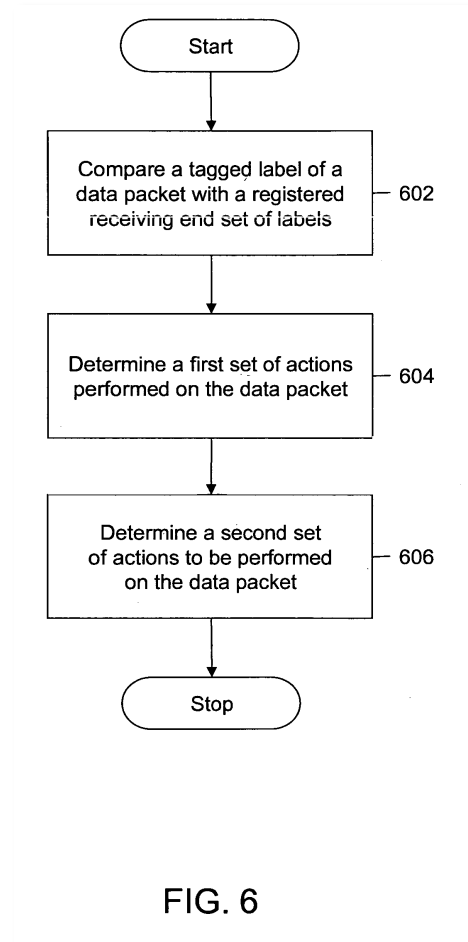
PETITIONER'S DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

Background: '825 Patent

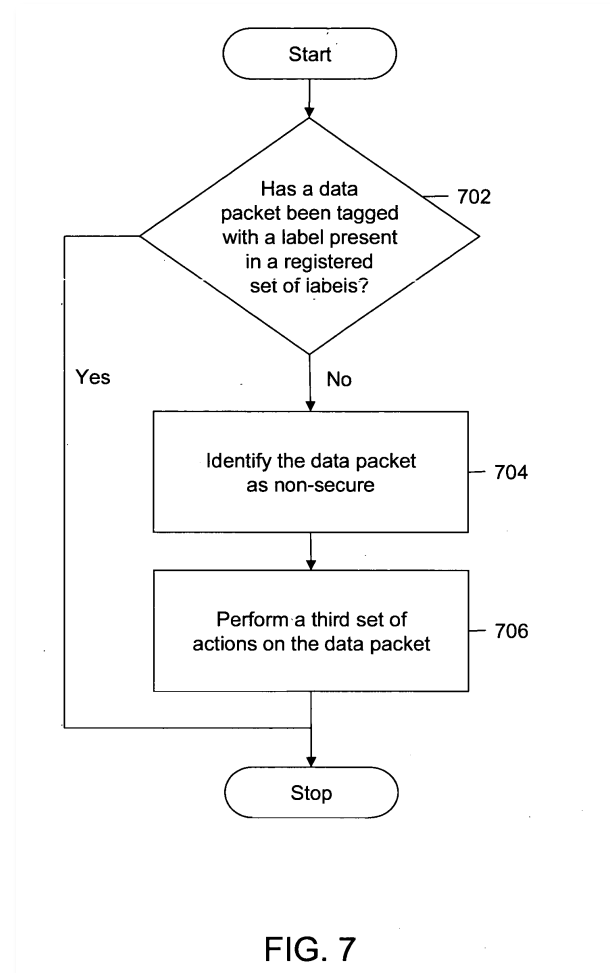


'825 patent

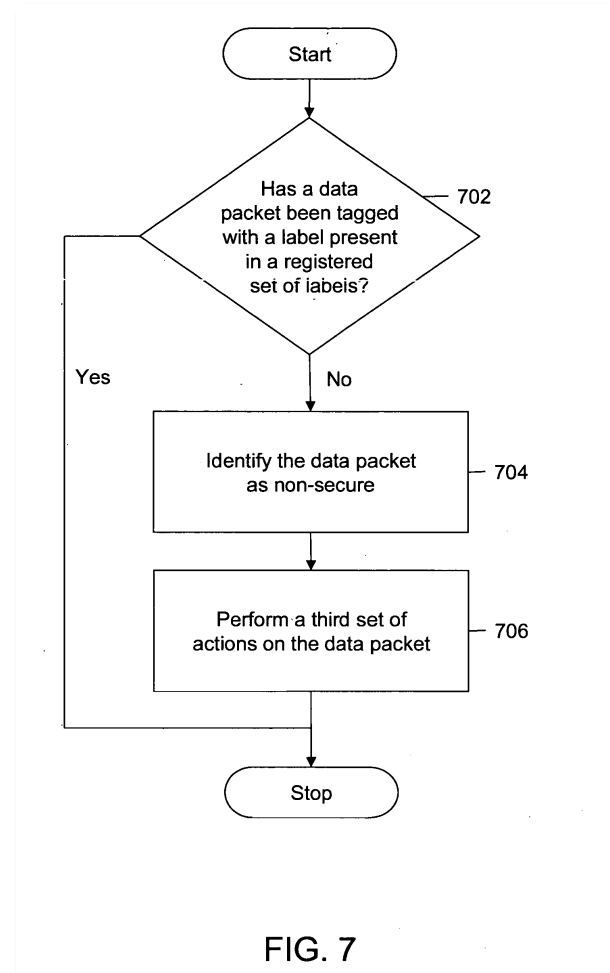
PETITIONER'S DEMONSTRATIVE EXHIBIT – NOT EVIDENCE



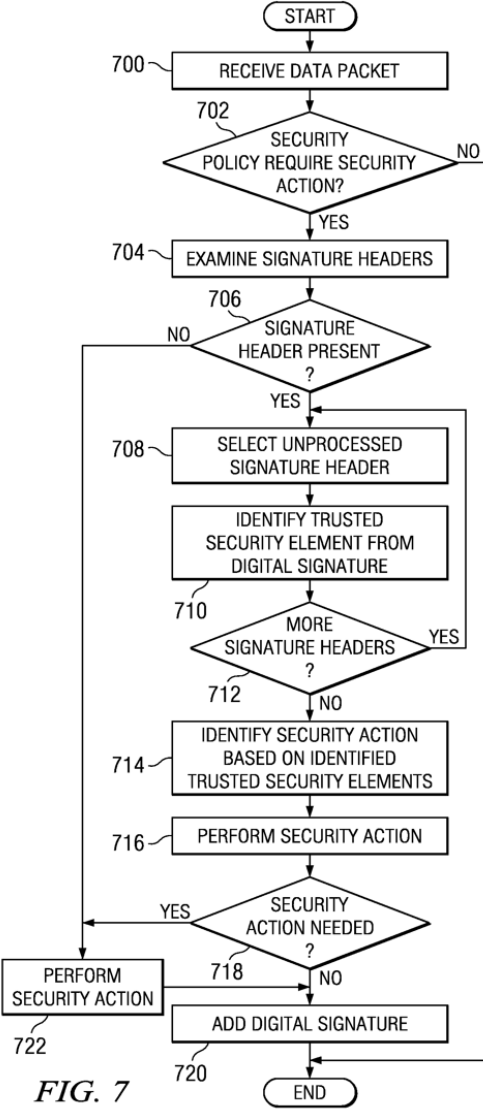
Chandra



Chandra



Chandra



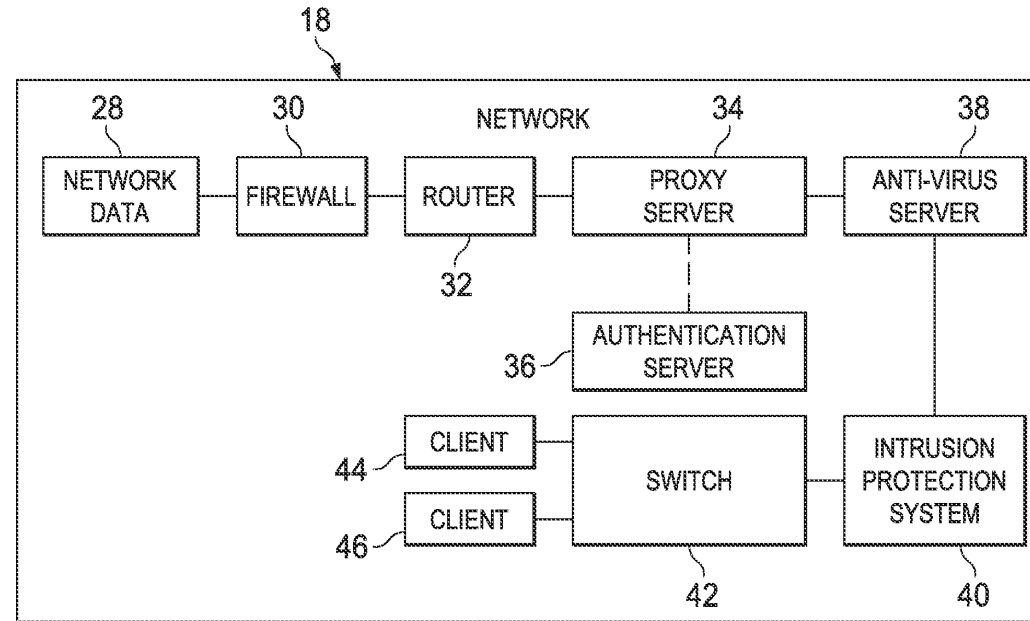
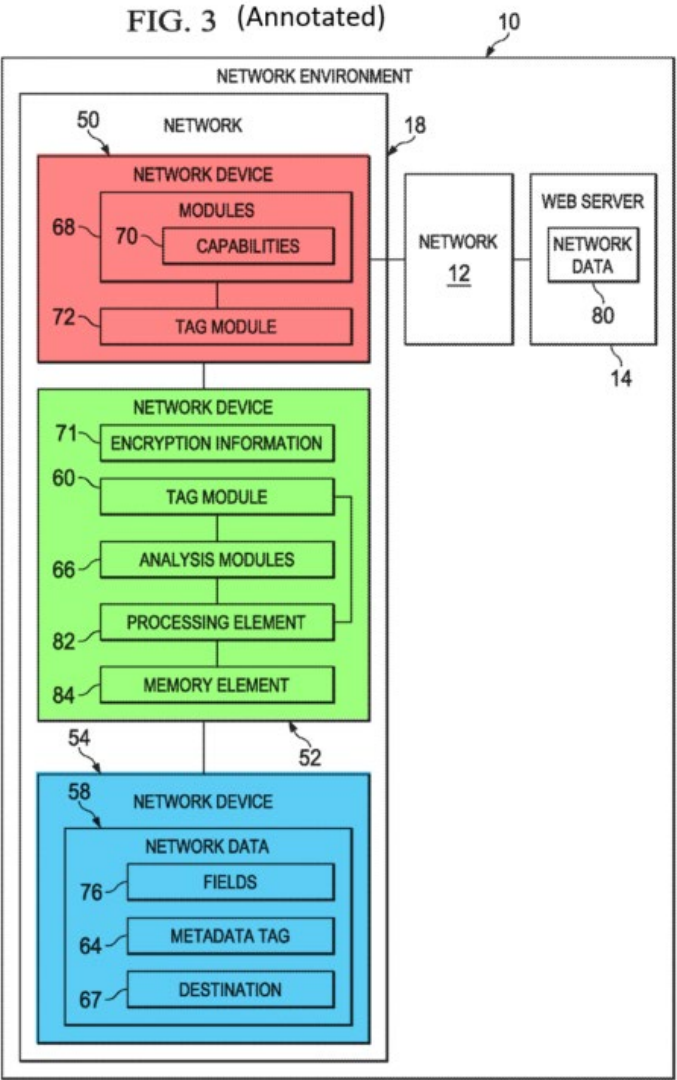


FIG. 2



CERTIFICATE OF SERVICE

The undersigned hereby certifies that a true copy of the foregoing PETITIONER'S DEMONSTRATIVES FOR ORAL ARGUMENT was served in its entirety this 18th day of June, 2024 by electronic mail on the Patent Owner via its attorneys of record:

James M. Glass - jimglass@quinnemanuel.com
John T. McKee - johnmckee@quinnemanuel.com
Quincy Lu - quincylu@quinnemanuel.com
Andrew M. Holmes - drewholmes@quinnemanuel.com
Ognjen Zivojnovic - ogizivojnovic@quinnemanuel.com
Razmig H. Messerian - razmesserian@quinnemanuel.com
Sean Gloth - seangloth@quinnemanuel.com
Quinn Emanuel Urquhart & Sullivan LLP
51 Madison Ave, 22nd Floor
New York, New York 10010

Dated: June 18, 2024

Respectfully submitted,

Perkins Coie LLP
1201 Third Avenue Suite 4900
Seattle, WA 98101-3099

/Meghan Bright/

Meghan Bright
Patent Paralegal