

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

NETSKOPE, INC.,
Petitioner,

v.

FORTINET, INC.,
Patent Owner.

IPR2023-00459
Patent 10,084,825 B1

Before JAMES P. CALVE, THOMAS L. GIANNETTI, and
STEPHEN E. BELISLE, *Administrative Patent Judges*.

CALVE, *Administrative Patent Judge*.

DECISION
Granting Institution of *Inter Partes* Review
35 U.S.C. § 314

I. BACKGROUND

Netskope, Inc. (“Petitioner”) filed a petition requesting an *inter partes* review of claims 1–7 and 10–31 (the “challenged claims”) of U.S. Patent No. 10,084,825 (“the ’825 patent”) (Ex. 1001). Paper 2, 1 (“Pet.”). Fortinet, Inc. (“Patent Owner”) timely filed a Preliminary Response. Paper 6 (“Prelim. Resp.”).

We have authority to determine whether to institute an *inter partes* review. *See* 35 U.S.C. § 314 (2018); 37 C.F.R. § 42.4(a) (2022) (“The Board institutes the trial on behalf of the Director.”). An *inter partes* review may not be instituted “unless . . . the information presented in the petition . . . shows that there is a reasonable likelihood that the petitioner would prevail with respect to at least 1 of the claims challenged in the petition.” 35 U.S.C. § 314(a). Upon consideration of the evidence and arguments in the record, we determine that the information presented shows a reasonable likelihood that Petitioner would prevail with respect to at least one of the challenged claims. We therefore grant institution of an *inter partes* review.

A. *Related Proceedings*

The parties identify the following proceeding involving the ’825 patent: *Netskope, Inc. v. Fortinet, Inc.*, No. 3:22-cv-01852-TLT (N.D. Cal.). Pet. 2; Paper 3, 2.

Petitioner identifies the following, co-pending *inter partes* review proceedings in which Petitioner challenges other patents of Patent Owner: IPR2022-01587, IPR2023-00030, IPR2023-00175, IPR2023-00456, IPR2023-00457, and IPR2023-00458. Pet. 2.

B. Real Parties in Interest

Petitioner identifies Netskope, Inc. as the real party in interest. Pet. 1.
Patent Owner identifies Fortinet, Inc. as the real party in interest. Paper 3, 2.

C. The '825 Patent (Ex. 1001)

The '825 patent describes methods of performing security operations on network traffic passing through a cooperative security fabric (CSF) of network security appliances that coordinate their security operations to avoid redundant security operations. Ex. 1001, 1:26–29, 1:64–2:16, 2:46–58.

Figure 1 is reproduced below to depicts such a CSF network topology.

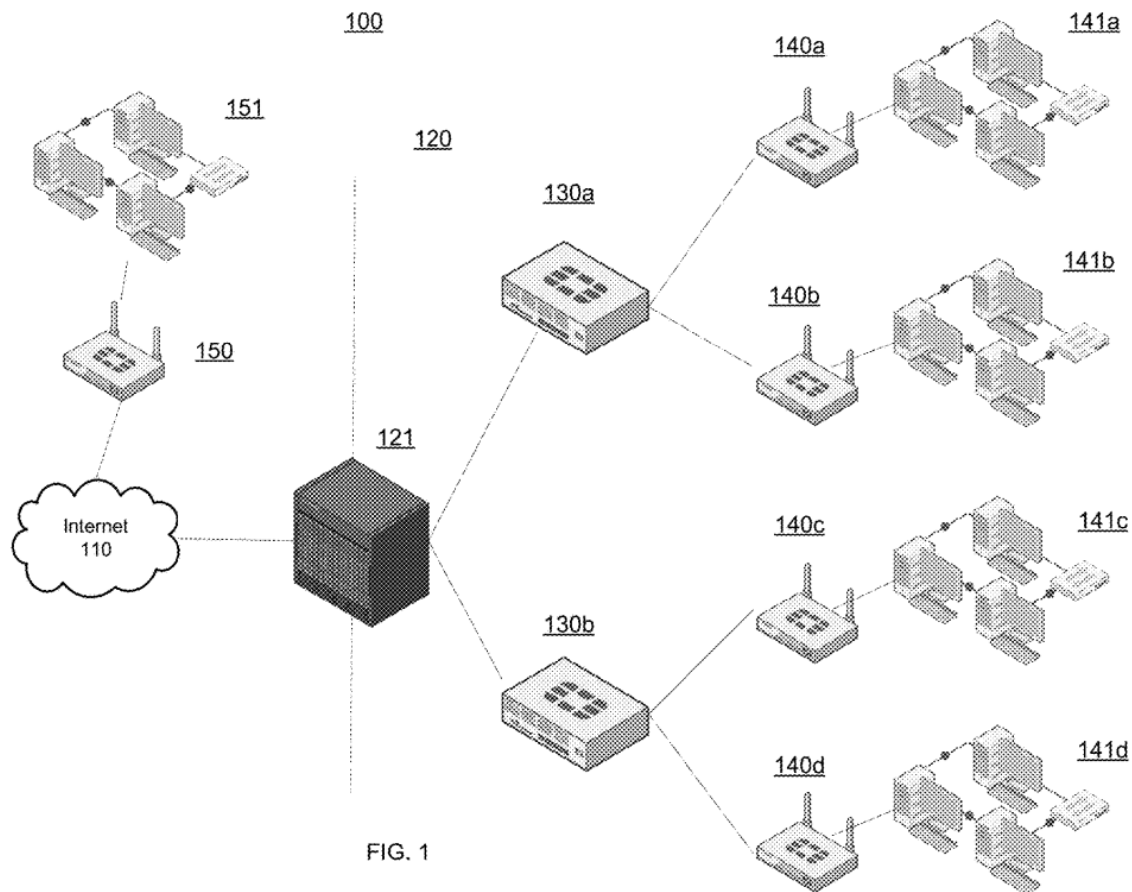


Figure 1 illustrates private network 120 connected to Internet 120 by root network security appliance 121. Ex. 1001, 4:58–67, 5:10–18.

Each subnet 141a–d connects to a subnet network security appliance 140a–d and scans traffic transmitted to and from the subnets for malware, viruses, or high risk network accesses based on network policies. Ex. 1001, 5:19–25. Middle network security appliances 130a, b connect root network security appliance 121 to subnet network security appliances 140a–d and inspect network traffic based on local security policies. Ex. 1001, 5:26–31.

“[T]he root, middle and subnet network security appliances form a cooperative security fabric that coordinates operations among members and avoids redundant operations even when local policies define the same operations” as illustrated in Figure 2, reproduced below. Ex. 1001, 5:44–48.

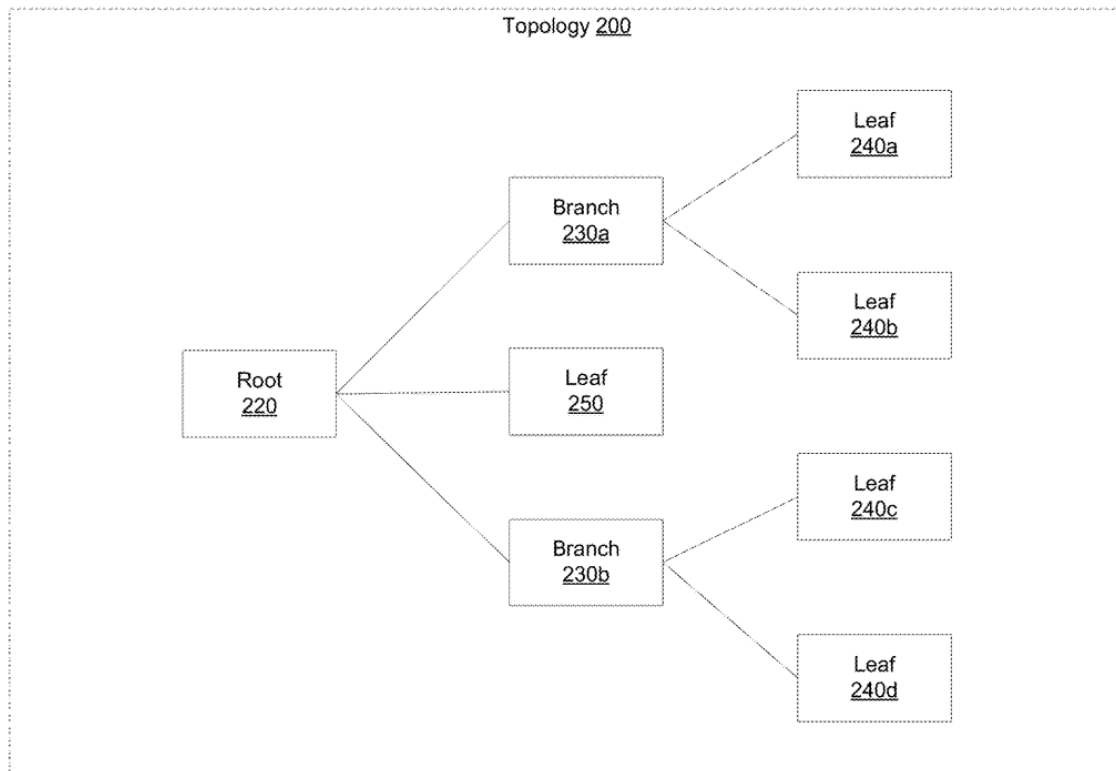


FIG. 2

Figure 2 shows a topology 200 of a cooperative security fabric that consists of the network security appliances of Figure 1. Ex. 1001, 5:50–51.

Root node 220 corresponds to root network security appliance 121 in Figure 1 and acts in a wide area network (WAN) role that connects a private network to other networks or the Internet. Ex. 1001, 5:52–56. Branch nodes 230a, 230b correspond to middle network security appliances 130a, 130b and connect other network security appliances within the private network. *Id.* at 5:60–64. Leaf nodes 240a–d are network security appliances that connect endpoint devices, which are sources or destinations of network traffic such as personal computers, servers, laptops, and printers. *Id.* at 6:1–9. Root nodes and leaf nodes are edge nodes where network traffic enters and leaves the CSF *Id.* at 6:9–12.

To cooperate with other members of a CSF, a member node adds one or more flags (e.g., a single bit flag, a collection of bit fields) to a network packet after the member node inspects the packet and transmits the network packet to another member node at the next hop. Ex. 1001, 6:28–34. When the member node at the next hop receives the network packet, the member node checks if the network packet carries a flag. If so, the member node skips the operations that are reported via the flag as having been executed by the previous member node. *Id.* at 6:34–43.

A flag may be added to the first packet of a session to indicate one or more network security operations (e.g., antivirus scanning, content filtering, antispam, data leak prevention) were performed by the transmitting member node. As a result, subsequent member nodes do not need to execute these operations again. Ex. 1001, 7:5–16, 7:33–44. If a flag is not present in an incoming packet, it means that the member node is the first member of the CSF to receive the incoming packet. *Id.* at 7:26–28.

D. Challenged Claims

Claims 1, 15, 21, and 27 are independent. Claims 2–7 and 10–14 depend from claim 1. Claims 16–20 depend from claim 15. Claims 22–26 depend from claim 21. Claims 28–31 depend from claim 27. Ex. 1001, 10:58–14:59. Claim 1 is reproduced below with Petitioner’s annotations added to identify each limitation (Pet. 22–37 (*see* Ground 1 contentions)).

1[pre] A method comprising:

1[a] 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;

1[b] 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;

1[c] when the network traffic is determined to have been transmitted from the second network security appliance:

1[d][i] determining, by the first network security appliance, one or more network security operations that are executed by the second network security appliance;

1[d][ii] 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

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

Ex. 1001, 10:58–11:17.

E. Asserted Grounds of Unpatentability

Petitioner asserts that the challenged claims are unpatentable on the following eight grounds (Pet. 3–4):

Ground	Challenged Claim(s)	35 U.S.C. §	Reference(s)
1	1–5, 12, 15, 16, 21, 22, 27	103 ¹	Chandra ²
2	6, 7, 17, 18, 23, 24, 28, 29	103	Chandra, Buruganahalli ³
3	10, 11	103	Chandra, Kumar ⁴
4	13, 14, 19, 20, 25, 26, 30, 31	103	Chandra, Chandra-2 ⁵
5	1–5, 10–12, 15, 16, 21, 22, 27	103	Keohane ⁶
6	6, 7, 17, 18, 23, 24, 28, 29	103	Keohane, Buruganahalli
7	10	103	Keohane, Kumar
8	13, 14, 19, 20, 25, 26, 30, 31	103	Keohane, Chandra-2

Petitioner relies on a Declaration of Dr. Michael Franz. Ex. 1002.

Patent Owner relies on a Declaration of Dr. John Black Jr. Ex. 2001.

¹ The Leahy-Smith America Invents Act (“AIA”) revised 35 U.S.C. § 103 effective on March 16, 2013. Because the ’825 patent has an effective filing date after March 16, 2013, we use the AIA version of 35 U.S.C. § 103.

² US 2007/0204018 A1, published Aug. 30, 2007 (Ex. 1004, “Chandra”).

³ US 2014/0282843 A1, published Sept. 18, 2014 (Ex. 1005, “Buruganahalli”).

⁴ US 2009/0144818 A1, published June 4, 2009 (Ex. 1006, “Kumar”).

⁵ US 2017/0093917 A1, published Mar. 30, 2017 (Ex. 1007, “Chandra-2”).

⁶ US 2008/0134332 A1, published June 5, 2008 (Ex. 1008, “Keohane”).

II. DISCUSSION

A. *Level of Ordinary Skill in the Art*

The parties substantially agree on the level of ordinary skill in the art. Petitioner asserts that a skilled artisan “would have had at least a B.S. degree in computer science, computer engineering, or electrical engineering (or equivalent experience) and . . . at least two years’ practical experience with computer networking and computer security.” Pet. 19. Patent Owner asserts that a skilled artisan “would have had a Bachelor of Science degree in electrical engineering and/or computer science, and two years of work or research experience in the fields of network and data security, or a Master’s degree in electrical engineering and/or computer science and one year of work or research experience in related fields.” Prelim. Resp. 8. Patent Owner asserts that its positions would be the same under either proposal. *Id.* We adopt Patent Owner’s proposal as more consistent with the prior art and the ’825 patent. Our decision would be the same under either formulation.

B. *Claim Interpretation*

We interpret claims “using the same claim construction standard that would be used to construe the claims in a civil action [held] under 35 U.S.C. 282(b).” 37 C.F.R. § 42.100(b). Under this standard, we construe claims “in accordance with the ordinary and customary meaning of such claim as understood by one of ordinary skill in the art and the prosecution history pertaining to the patent.” *Id.* We construe the claims only to the extent necessary to determine whether to institute *inter partes* review. *See Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co.*, 868 F.3d 1013, 1017 (Fed. Cir. 2017). The parties agree that the claims should be given their ordinary and customary meaning. Pet. 19; Prelim. Resp. 8–9.

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.*

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.

C. Principles of Law

A patent claim is unpatentable under 35 U.S.C. § 103 if differences between the claimed subject matter and the prior art are such that the subject matter, as a whole, would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. 35 U.S.C. § 103; *KSR Int’l Co. v. Teleflex Inc.*, 550 U.S. 398, 406 (2007). “The combination of familiar elements according to known methods is likely to be obvious when it does no more than yield predictable results.” *KSR*, 550 U.S. at 416. Similarly, “if a technique has been used to improve one device, and a person of ordinary skill in the art would recognize that it would improve similar devices in the same way, using the technique is obvious unless its actual application is beyond his or her skill.” *Id.* at 417.

The question of obviousness is resolved based on underlying factual determinations including: (1) the scope and content of the prior art; (2) any differences between the claimed subject matter and the prior art; (3) the level of ordinary skill in the art; and (4) when in evidence, objective evidence of non-obviousness. *Graham v. John Deere Co.*, 383 U.S. 1, 17–18 (1966). Neither party presents any objective evidence of non-obviousness at this stage of the proceeding.

D. Ground 1: Alleged Obviousness Over Chandra

Petitioner asserts that claims 1–5, 12, 15, 16, 21, 22, and 27 are unpatentable under 35 U.S.C. § 103 over Chandra. Pet. 3, 19–46.

1. Chandra (Ex. 1004)

Chandra tags data packets with labels to indicate actions performed on the data packet by transmitting customer edge (CE) 208. This information allows receiving CE 214 to determine other actions to perform on the data packet as depicted in Figure 2, which is reproduced in part below.

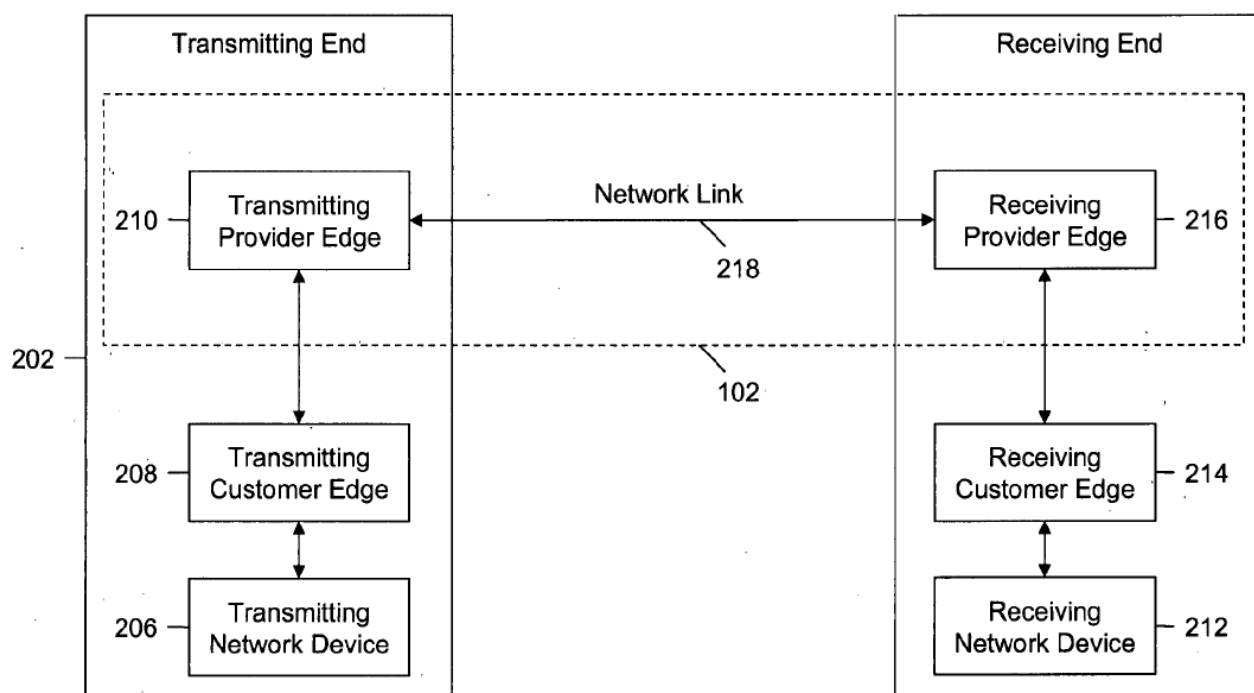


Figure 2 shows transmitting CE 208 and receiving CE 214 as security-based devices located at the edges of their respective customer networks. Ex. 1004 ¶ 30. Transmitting CE 208 and receiving CE 214 register with one another and exchange CE labels. Then, when receiving CE 214 receives a data packet, it pops off the tagged CE label, identifies a first set of actions performed by transmitting CE 208, and performs non-redundant security actions on the data packet. *Id.* ¶¶ 33–37, 46–48, 51, 52, Figs. 6, 7.

Transmitting CE 208 and receiving CE 214 authenticate each other before exchanging CE labels that they use for tagging data packets that are transmitted between them. Ex. 1004 ¶ 34. After exchanging CE labels, the CE labels are registered as a transmitting end set of labels at transmitting CE 208 and as a receiving end set of labels at receiving CE 214. *Id.* In various embodiments, the transmitting and receiving labels are the same. *Id.*

Transmitting CE 208 uses the registered transmitting end set of labels to tag a data packet with a CE label that indicates a first set of actions that it performed on the data packet. Ex. 1004 ¶ 35. The registered receiving end set of labels is used by receiving CE 214 to determine the first set of actions that transmitting CE 208 performed on the data packet and then determine a second, non-redundant set of actions to perform on the data packet before transmitting the data packet to a receiving network device 212. *Id.*

Receiving CE 214 stores CE labels that it receives from transmitting CE 208 in a table of registered labels, such as the table reproduced below.

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
. . .		

The table of receiving end set labels above is registered and stored by receiving CE 214 so receiving CE 214 can determine if a data packet was sent by transmitting CE 208. A data packet with label 1256 indicates the data packet was sent by transmitting CE 208, which performed the security actions corresponding to rules A and B so receiving CE 214 does not have to perform these actions as redundant actions. Ex. 1004 ¶¶ 52, 53.

2. *Independent Claim 1*

a. *1[pre]: “A method comprising:”*

Petitioner contends that Chandra discloses a method that obviates redundant actions by tagging a data packet with a label to indicate that a first set of actions was performed on the data packet at the transmitting end. Pet. 22 (citing Ex. 1004 ¶ 18). This contention, which Patent Owner does not contest at this stage, is supported by record evidence.

b. *1[a]: “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;”*

Petitioner contends that Chandra discloses a receiving CE 214 that receives data packets over LAN 102 or a virtual private network that are private networks, and CE 214 may be a “security-based device” such as a firewall or Intrusion Detection System (IDS) that a skilled artisan would know is a network security appliance. Pet. 22–26 (citing Ex. 1004 ¶¶ 4–7, 21, 30, 58–68, Figs. 2, 8; Ex. 1001, 4:16–18, 4:65–67, 5:1–2; Ex. 1002 ¶¶ 65–68). Petitioner asserts that Chandra has a network security appliance “participating in a cooperative security fabric (CSF)” and “receiving . . . network traffic that is to be inspected” as receiving CE 214 cooperating with transmitting CE 208 to coordinate the security actions that they perform on network traffic. Petitioner asserts that these transmitting and receiving CEs authenticate one other and exchange CE labels to coordinate security actions and obviate redundant actions performed on tagged data packet network traffic, e.g., by removing a tagged CE label in a data packet to identify a first set of actions performed. Pet. 26–28 (citing Ex. 1004 ¶¶ 18–20, 24–26, 30, 32–34, 37, 46; Ex. 1001, 1:64–68, 5:45–47, 6:18–20; Ex. 1002 ¶¶ 69, 70).

c. Chandra's alleged lack of bidirectional fabric

Patent Owner argues that Chandra lacks a “fabric,” “whose ordinary meaning requires a topology that processes *bidirectional* communications” because Chandra discloses a two-node tunnel that processes *unidirectional* communication only. Prelim. Resp. 16. Patent Owner asserts, “Chandra discloses that its receiving CE (214) and transmitting CE (208) are two nodes that can only process traffic in one direction.” *Id.* at 17. Patent Owner argues that transmitting data from CE 208 via unidirectional tunnel 218 to receiving CE 214 is not a “fabric.” *Id.* at 17–18. These arguments are unavailing based on our construction of “fabric” and the following.

Chandra's network topology 100 allows network security appliances to exchange network traffic and perform non-redundant security checks on network traffic to form a cooperative security fabric. Ex. 1002 ¶¶ 2, 18–20, 24–43, Figs. 1–4; Pet. 19–28. Network 102 is a communication medium for network devices 104 so “data [can] be transmitted from one network device to another network device,” which may include personal computers, servers, and mobile phones. Ex. 1004 ¶ 21. This description indicates network 102 supports *bidirectional* communication between network devices 104 as does the statement that “*a network device from network devices 104 can transmit data, while another network device from network devices 104 can receive data.*” *Id.* ¶ 23 (emphasis added). Network topology 100 is not limited to a certain number or type of network devices 104. *Id.* ¶ 22. Figure 2 depicts network link 218 as bidirectional. Claim 1 recites a first network security appliance “receiving” network traffic that is to be inspected by the first network security appliance. Claim 1 does not require the first network security appliance to transmit network traffic. Ex. 1001, 10:59–11:17.

The plain language of claim 1 covers network traffic in one direction. A first network security device *receives* network traffic for inspection and determines if the received network traffic was transmitted by a second network security appliance. . Ex. 1001, 10:59–11:17. Patent Owner does not dispute that Chandra’s transmitting CE 208 and receiving CE 214 perform these claimed activities. *See* Prelim. Resp. 16–18.

- d. *1[b]: “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;”*

Petitioner contends that Chandra discloses a first network security appliance (receiving CE 214) that determines whether the network traffic that it receives was transmitted from a second network security appliance (transmitting CE 208) that is participating in the CSF. Petitioner asserts that receiving CE 214 checks if a data packet received from transmitting CE 208 is tagged with a CE label that was exchanged and registered as a “receiving end set of labels” so the receiving CE 214 can identify the network traffic as being transmitted by transmitting CE 208 in the same CSF as claimed. Pet. 28–32 (citing Ex. 1004 ¶¶ 31–35, 37, 47–49, CE label table, Figs. 2, 6, 7; Ex. 1001, 6:28–34, 6:54–59, 6:65–67; Ex. 1002 ¶¶ 76, 77).

Patent Owner argues that the CE label “provides no information about whether the transmitting CE participated in the same CSF as the receiving CE” and “merely indicates whether security operations were performed by the transmitting CE [but the CE label] does *not* include any indication that the transmitting CE (208) is participating in the same CSF as the receiving CE (214).” Prelim Resp. 18–19.

Dr. Black testifies, “the CE label only indicates that certain security operations were performed by the transmitting CE. There is no indication that the transmitting CE is participating in the same CSF as the receiving CE.” Ex. 2001 ¶ 63. Dr. Black testifies that the ’825 patent describes the CSF member nodes determining whether traffic comes from a member node based on the flag carried by the incoming packet because “the flag is set to indicate that the network packet is transmitted from a member node [of a CSF].” *Id.* ¶ 64.

We find Patent Owner’s and Dr. Black’s arguments and testimony to be unavailing because Chandra discloses that transmitting and receiving CEs *register their CE labels* with one another, *after authenticating* themselves to one another as participants in a CSF, so receiving CE 214 can determine that network traffic was transmitted by transmitting CE 208 participating in the same CSF based on the registered CE labels. Ex. 1004 ¶¶ 32–43, Figs. 2–4.

The registered transmitting and receiving end sets of labels indicate to the receiving CE 214 that the network traffic was transmitted by transmitting CE 208 in the same CSF *for distributed enforcement of rules* to coordinate actions and reduce redundancy. Ex. 1004 ¶¶ 18–20, 30–43, Figs. 2–4.

At step 304, receiving end 204 receives the data packet from transmitting end 202. The data packet is tagged with the CE label indicating the first set of actions performed on the data packet at transmitting CE 208. At step 306, receiving CE 214 identifies the CE label. *This CE label is present in the registered receiving end set of labels, and therefore, can be recognized by receiving CE 214.*

Ex. 1004 ¶ 37 (emphasis added); *id.* ¶¶ 38–43, 46, 47, Figs. 4, 6.

The registered CE label indicates the network traffic was transmitted by transmitting CE 208 in the same CSF as receiving CE 204 as claimed.

Just as a “flag is set to indicate that the network packet is transmitted from a member node [of a CSF]” in claim 1 (*see* Prelim. Resp. 19; Ex. 1001, 6:65–7:4), transmitting CE 208 adds end set labels registered with receiving CE 214 to tag (flag) a data packet and indicate that transmitting CE 208 performed a first set of actions as part of the cooperative CSF that it formed with receiving CE 214 (Ex. 1004 ¶¶ 34–43, Figs. 2–4).

Transmitting CE 208 tags data packets with a registered end set of labels. Receiving CE 214 recognizes the registered labels of the data packet as being from transmitting CE 208 in the same CSF. Ex. 1004 ¶ 43.

We reproduce a table of registered CE labels from Chandra below.

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
...		

Pet. 31. The table of CE labels above are registered by a transmitting and a receiving CE. The CE labels are rules that the transmitting CE may perform before sending a data packet to the receiving CE. Receiving CE 214 uses the table to identify CE labels in a data packet as being sent by transmitting CE 208 in the same CSF as receiving CE 214 for the distributed enforcement of rules. Label 1256 indicates transmitting CE performed actions for rules A and B on a data packet. Ex. 1004 ¶¶ 32–43; Pet. 31 (reproducing CE table).

At this stage, based on the evidence and arguments, we conclude that Petitioner has provided sufficient evidence at this stage to establish that Chandra discloses element 1[b].

- e. *1[c]: “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 appliance;”*

Petitioner contends that Chandra discloses a receiving CE determining “the first set of actions performed on the data packet at transmitting CE 208” by determining network traffic was transmitted by transmitting CE 214 in the CSF and the security operations performed. Pet. 32–33 (citing Ex. 1004 ¶¶ 32, 46, 48, Fig. 6 (step 604); Ex. 1002 ¶¶ 78, 79). This contention, which Patent Owner does not contest at this stage, is supported by record evidence.

- f. *1[d][i]: “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,”*

Petitioner contends that Chandra also discloses that receiving CE 214 (first network security appliance) determines operations to execute based on the security operation actions previously performed by transmitting CE 208 (the second network security appliance). Pet. 34–35 (citing Ex. 1004 ¶¶ 18, 32, 46, Fig. 6; Ex. 1002 ¶ 82). These contentions, which Patent Owner does not contest at this stage, are supported by record evidence. After receiving CE 214 and transmitting CE 208 exchange labels, the receiving set of labels is registered at receiving CE 214 and used to determine a first set of actions performed at transmitting CE 208 so a second set of non-redundant actions can be performed at receiving CE 214. Ex. 1004 ¶¶ 31–43, 46, Figs. 2–4, 6.

- g. *1[d][ii]: “including skipping, by the first network security appliance, the one or more network security operations that are executed by the second network security appliance;”*

Petitioner contends that Chandra discloses the receiving CE (the first network security appliance) not performing (skipping) the network security operations that were executed by the transmitting CE (the second network security appliance) so the second set of actions performed by receiving CE 214 includes only non-redundant actions not performed by transmitting CE 208. Pet. 35–36 (citing Ex. 1004 ¶¶ 37, 46, 53; Ex. 1002 ¶¶ 83, 85). These contentions, which Patent Owner does not contest at this stage, are supported by record evidence. Receiving CE 214 determines a non-redundant set of actions to perform based on a first set of actions. Ex. 1004 ¶¶ 30–46, Fig. 6.

- h. *1[e]: “and executing, by the first network security appliance, the one or more local operations on the network traffic.”*

Petitioner contends that Chandra discloses executing the second set of actions on the data packet as one or more local operations at receiving CE 214. Pet. 36–37 (citing Ex. 1004 ¶ 46; Ex. 1002 ¶ 85). These contentions, which Patent Owner does not contest at this stage, are supported by record evidence.

On this record, we find that Petitioner has established a reasonable likelihood that claim 1 is unpatentable over Chandra.

3. *Dependent Claims 2–5 and 12*

Petitioner asserts that Chandra determines a second set of actions at receiving CE 214 based on local network policies (Rules A–E) and performs those actions that transmitting CE 208 did not perform as recited in claim 2. Pet. 37–38 (citing Ex. 1004 ¶¶ 18, 35, 37, 53; Ex. 1002 ¶ 89).

Petitioner also contends that Chandra determines a second set of actions that could be redundant in claim 3. Petitioner asserts that Chandra executes a third set of actions when the network traffic is not transmitted by a transmitting CE (second network security appliance) as specified by local policies in claim 4 and indicates by the CE label (flag) the first set of actions that have been performed by the transmitting CE in claim 5. Petitioner also asserts that a skilled artisan would have found it obvious that the packet in which a flag was carried was a first packet of a session in claim 12. Pet. 39–44 (citing Ex. 1004 ¶¶ 18, 31, 47, 48, 53, Fig. 7; Ex. 1002 ¶¶ 93, 95, 96, 100, 101). These contentions, which Patent Owner does not contest at this stage, are supported by record evidence.

On this record, we find that Petitioner has established a reasonable likelihood that claims 2–5 and 12 are unpatentable over Chandra.

4. Independent Claims 15, 21, and 27; Claims 16 and 22

Petitioner asserts that Chandra discloses limitations of claims 15, 16, 21, 22, and 27. Pet. 44–46 (citing contentions for claims 1–3 and 5). These contentions, which Patent Owner does not contest at this stage, are supported by record evidence such as a second set of actions being redundant or also non-redundant actions and a flag indicates executed network operations.

On this record, we find that Petitioner has established a reasonable likelihood that claims 15, 16, 21, 22, and 27 are unpatentable over Chandra.

E. Ground 2: Alleged Obviousness Over Chandra and Buruganahalli

Petitioner asserts that claims 6, 7, 17, 18, 23, 24, 28, and 29 are unpatentable under 35 U.S.C. § 103 over Chandra and Buruganahalli. Pet. 4, 46–58.

1. *Buruganahalli (Ex. 1005)*

Buruganahalli coordinates security actions among network security devices by using a metadata tag carried by network traffic 28 to indicate the actions performed by previous network security devices. This determination ensures subsequent devices do not perform the same actions on network data 28. Ex. 1005 ¶¶ 26–30. Figure 2, reproduced below, depicts this network.

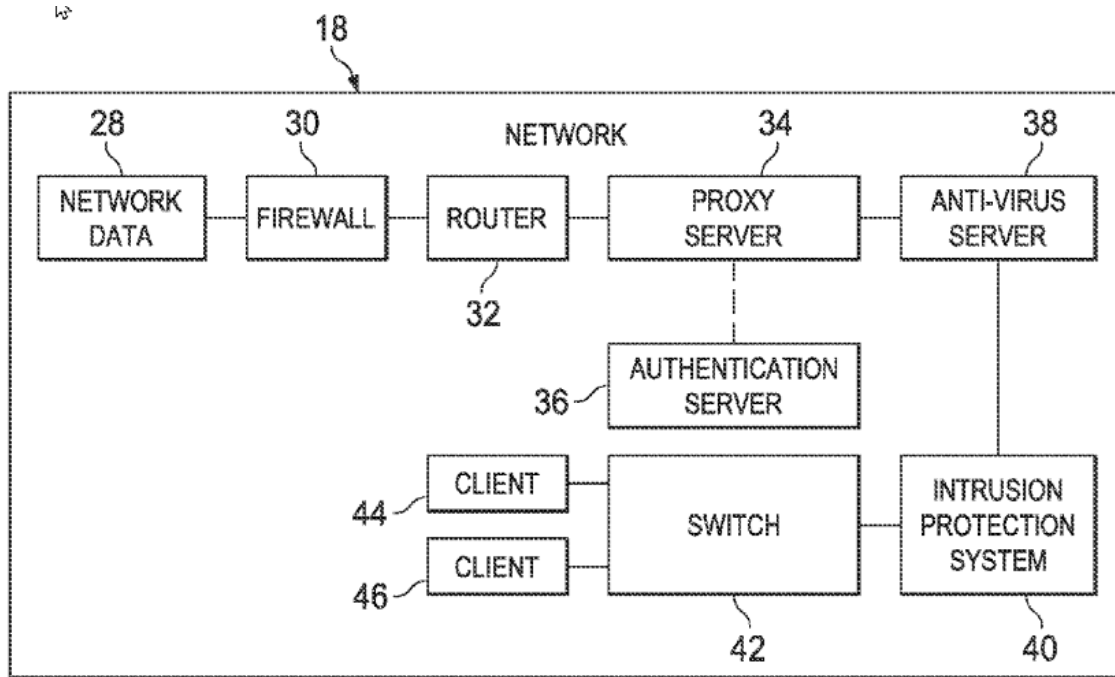


FIG. 2

Figure 2 depicts network data 28 processed by firewall 30, router 32, proxy server 34, anti-virus server 38, and intrusion protection system 40. Each device ensures that network data 38 satisfies certain criteria and does not include malicious content. Ex. 1005 ¶¶ 19–26. Unlike known networks where a network device performs the processing on network data 28 all over again, Buruganahalli allows a network device to use the results of processing performed by a previous network device through which network data 28 has traveled to process the data without repeating actions. *Id.* ¶¶ 26–30.

“The use of processing by the previous network device allows the network device to process the data without having to repeat actions already performed by the previous network device.” Ex. 1005 ¶ 27. As network data 28 is forwarded to the next network device in the route for processing, the next network device may analyze a metadata tag added by the previous network device to obtain information about network data 28. *Id.* ¶ 28. By receiving a metadata tag with information about network data 28, a network device may avoid reprocessing the network data in the same way. *Id.*

2. *Motivation to combine*

Petitioner contends that a skilled artisan would have been motivated to combine the teachings of Chandra and Buruganahalli with a reasonable expectation of success because both references disclose network security devices that coordinate actions to reduce redundancy. Pet. 50. Petitioner contends that Chandra discloses network security devices as transmitting CE and receiving CE that coordinate their security operations using labels, and Buruganahalli discloses network devices in a data path that coordinate their operations using a metadata tag carried by data packets. *Id.* (citing Ex. 1004, Abstract, ¶ 30; Ex. 1005 ¶¶ 27, 28). Petitioner asserts that a skilled artisan looking to improve Chandra would have considered the complementary disclosures of Buruganahalli. *Id.* These contentions, which Patent Owner does not contest at this stage, are supported by record evidence. *See* Prelim. Resp. 20. Metadata tags would improve Chandra by allowing a transmitting CE to identify security operations that it performed on a data packet to a receiving CE *and other network devices* that receive the data packet to reduce redundancy across various network devices and improve efficiency as Buruganahalli teaches. Ex. 1005 ¶¶ 27–30; *see KSR*, 550 U.S. at 417.

3. *Claims 6, 17, 23, and 28*

Petitioner contends that Buruganahalli discloses a network device that updates a metadata tag (flag) to indicate analysis performed on network data by the device and transmits the network traffic and updated flag to the next network device participating in the CSF to coordinate their actions and to reduce redundancies. Pet. 50–56 (citing Ex. 1005 ¶¶ 27, 28, 32, 38, 40, 44, 46, 48, Figs. 2, 3, 8; Ex. 1004 ¶¶ 24, 28, 56, 58, Figs. 2, 8; Ex. 1002 ¶¶ 121, 122, 127–130). Petitioner contends that a skilled artisan would have added Buruganahalli’s tag updating to Chandra’s label updating so a receiving CE would benefit from knowing what actions were performed by a previous CE in a *multi-CE* data path situation and which CE performed them. *Id.* at 54 (citing Ex. 1004 ¶ 28). These contentions, which Patent Owner does not contest at this stage, are supported by record evidence. On this record, we find that Petitioner has established a reasonable likelihood that claims 6, 17, 23, and 28 are unpatentable over Chandra and Buruganahalli.

4. *Claims 7, 18, 24, and 29*

Petitioner contends that Buruganahalli discloses that the last network device to receive network data before sending the data outside the network (or any device) may remove the metadata tag before transmitting it. Pet. 57–58 (citing Ex. 1005 ¶¶ 29, 47; Ex. 1002 ¶ 134). Petitioner contends that a skilled artisan would have incorporated this technique into Chandra to keep the network’s labeling mechanism private so that malicious devices do not intercept and exploit it. These contentions, which Patent Owner does not contest at this stage, are supported by record evidence. On this record, we find that Petitioner has established a reasonable likelihood that claims 7, 18, 24, and 29 are unpatentable over Chandra and Buruganahalli.

F. Ground 3: Alleged Obviousness Over Chandra and Kumar

Petitioner asserts that claims 10 and 11 are unpatentable under 35 U.S.C. § 103 over Chandra and Kumar. Pet. 4, 58–62.

1. Kumar (Ex. 1006)

Kumar discloses a method in which sending node 20 and receiving node 60 establish an authentication session in which sending node 20 uses a unique client ID and session key from a receiving node 60 to create a digital signature and security tag to insert into an outgoing packet. Kumar discloses that receiving node 60 authenticates the security tag by recreating the digital signature and comparing the result to the digital signature contained in the security tag. Ex. 1006 ¶¶ 31–33, 36, 38, 45, 46, 49, 50, Abstract. Kumar teaches that an authentic security tag indicates the packet was transmitted from an approved sending node 20 and may be passed on. *Id.* ¶ 55.

2. Motivation to combine

Petitioner contends that a skilled artisan would have been motivated to incorporate Kumar’s combination of the two well-known techniques of authenticating another party in a communication with digital signatures and inserting additional information into packet headers of a data stream so that “downstream” devices can decode the data stream. Petitioner contends that a skilled artisan would have used the traditional technique taught by Kumar of inserting such additional information into packet headers because this technique has the advantage that no payloads need to be altered. Pet. 59. Petitioner contends that a skilled artisan would have been motivated to incorporate these well-known techniques into Chandra to secure data packets that are transmitted between network devices because these techniques often were used predictably and reliably. Pet. 59 (citing Ex. 1002 ¶ 137).

3. *Claims 10 and 11*

Petitioner contends that Kumar teaches that a transmitting device can use a client ID, session key, and public key to create a digital signature and a security tag to insert into a data packet. Petitioner asserts that a skilled artisan would use digital signatures in Chandra to authenticate a source as trusted and data as untampered (claim 10) and insert a security flag into an IP header field (claim 11) to avoid having to modify the payload. Pet. 60–62 (citing Ex. 1006 ¶¶ 36, 38, 45, 46–50, 53; Ex. 1004 ¶¶ 30, 32, 33, Abstract; Ex. 1002 ¶¶ 140, 141, 143–145). These contentions, which Patent Owner does not contest at this stage, are supported by record evidence.

On this record, we find that Petitioner has established a reasonable likelihood that claims 10 and 11 are unpatentable over Chandra and Kumar.

G. Ground 4: Alleged Obviousness Over Chandra and Chandra-2

Petitioner asserts that claims 13, 14, 19, 20, 25, 26, 30, and 31 are unpatentable under 35 U.S.C. § 103 over Chandra and Chandra-2. Pet. 4, 62–64.

1. *Chandra-2 (Ex. 1007)*

Chandra-2 describes techniques for managing online behavior tracking policies to ensure that communications between a client and web server comply with pertinent privacy regulations. Ex. 1007 ¶ 15.

2. *Motivation to combine*

Petitioner asserts that a skilled artisan would have performed each of Chandra-2’s well-known security operations in Chandra⁷ to expand the range of operations for predictable results. Pet. 62–63.

⁷ We treat Petitioner’s reference to Keohane as a clerical error as the caption and table of grounds list Chandra and Chandra-2 for Ground 4. Pet. 4, 62.

3. *Claims 13, 19, 25, and 30*

Petitioner contends that Chandra-2 describes a network “security device” that provides “logging.” Pet. 63 (citing Ex. 1007 ¶ 23). Petitioner asserts that a skilled artisan would have known network traffic logging is a widely used security operation especially important for forensic analysis after a vulnerability or breach is discovered. Petitioner asserts that a skilled artisan would have found it obvious that “logging” by a network security device such as Chandra’s CE might include “network traffic logging” as in claims 13, 19, 25, and 30 to expand its range of operations. *Id.* at 62–63 (citing Ex. 1002 ¶ 149). Dr. Franz testifies that network traffic logging is well-known and would have been obvious to perform with Chandra’s security devices for predictable results to provide a broader range of operations. Ex. 1002 ¶¶ 146–149. These contentions, which Patent Owner does not contest at this stage, are supported by record evidence.

4. *Claims 14, 20, 26, and 31*

Petitioner contends that Chandra-2 describes network security devices as providing antivirus, intrusion prevention (IPS), content filtering, data leak protection (DLP), antispam, antispyware, reputation-based protections, network access control, load balancing, vulnerability management, traffic shaping, and content filtering in claims 14, 20, 26, and 31. Petitioner asserts that a skilled artisan would have found it obvious to perform these well-known operations at Chandra’s CE to expand its operations. Pet. 62–64 (citing Ex. 1007 ¶¶ 23, 24; Ex. 1001, 9:23–26; Ex. 1002 ¶¶ 149, 151). Dr. Franz testifies that these operations are well known and would have been obvious to perform. Ex. 1002 ¶ 151. These contentions, which Patent Owner does not contest at this stage, are supported by record evidence.

On this record, we find that Petitioner has established a reasonable likelihood that claims 13, 14, 19, 20, 25, 26, 30, and 31 are unpatentable over Chandra and Chandra-2.

H. Ground 5: Alleged Obviousness over Keohane

Petitioner contends that claims 1–5, 10–12, 15, 16, 21, 22, and 27 are unpatentable under 35 U.S.C. § 103 over Keohane. Pet. 4, 64–90.

1. Keohane (Ex. 1008)

Keohane describes a network that eliminates costly and inefficient redundancy of scanning data packets by determining whether a signature of a trusted security element is present in a data packet header. Ex. 1008 ¶¶ 9, 11, 12. Figure 1, reproduced below, depicts such a processing system 100.

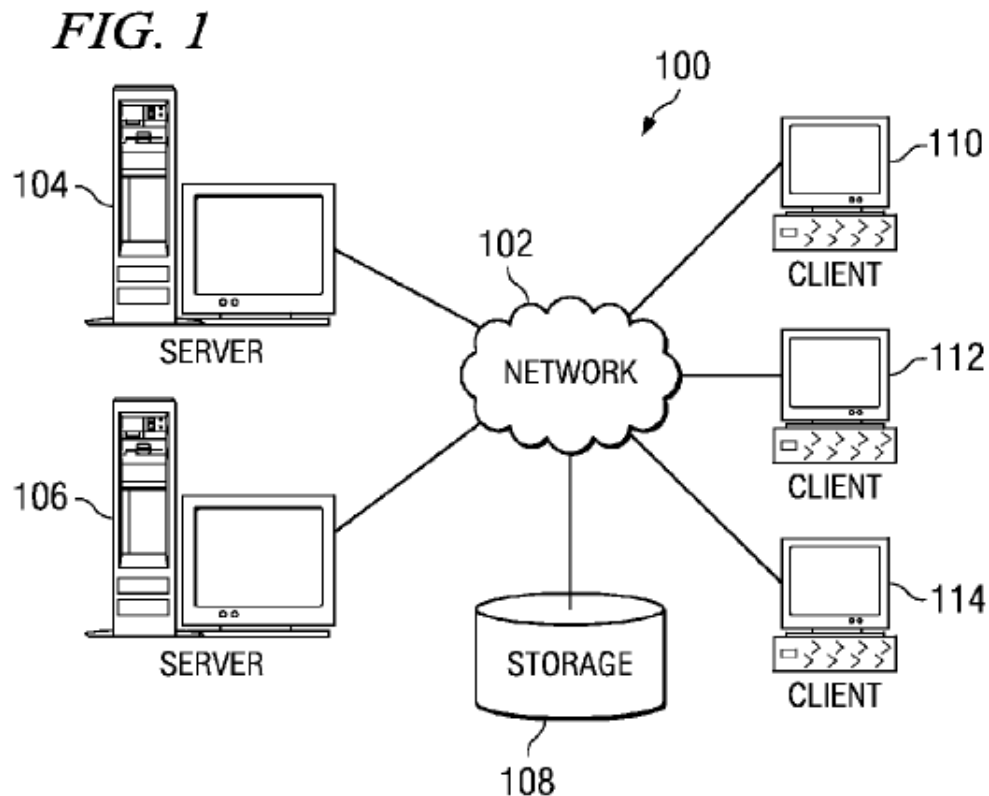


Figure 1 depicts network 102 that comprises routers, gateways, and firewalls that perform security actions to identify malware. Ex. 1008 ¶ 23.

2. *Independent Claim 1*

a. *1[pre]*

Petitioner asserts that Keohane discloses a method for screening data packets. Pet. 69 (citing Ex. 1008, Abstract). This contention, which Patent Owner does not contest at this stage, is supported by evidence of record.

b. *1[a]*

Petitioner contends that Keohane discloses mail gateway 302 as a first network security appliance of a private network that receives data packet 306 from firewall 300 and performs and coordinates security actions such as scanning data packets for viruses as part of a CSF. Petitioner asserts that Keohane's gateway and other participating appliances insert a signature into a data packet. Petitioner asserts that the signature indicates the data packet is from a trusted source, and it identifies security actions taken based on a code included in the signature. Petitioner asserts that coordinating security actions this way allows the system to avoid redundant actions and save time. Pet. 69–74 (citing Ex. 1008 ¶¶ 11, 22–24, 32, 35–38, 53, Figs. 1, 3, 7; Ex. 1009; Ex. 1001, 5:45–47; Ex. 1002 ¶¶ 160, 161, 163, 164, 167).

Patent Owner argues that Keohane does not disclose a “fabric” that processes bidirectional communications, and it only processes traffic in one direction (i.e., as unidirectional communication). Prelim. Resp. 21. Patent Owner argues that Keohane only handles traffic that originates from outside the network and flows in one direction to firewall 300, then to gateway 302, and then to client 304. *Id.* at 22–23.

Patent Owner's arguments are unavailing given our interpretation of a “fabric” of a CSF as a network topology that connects network devices to perform security actions, as discussed above, and the following.

Keohane describes a *network 102 topology* of communications links between various devices and computers connected together in network data processing system 100. Ex. 1008 ¶ 22. Clients 111–114 may be personal or network computers that may include software and/or hardware. *Id.* ¶ 23. Figure 3 is reproduced below to illustrate this multi-level security system.

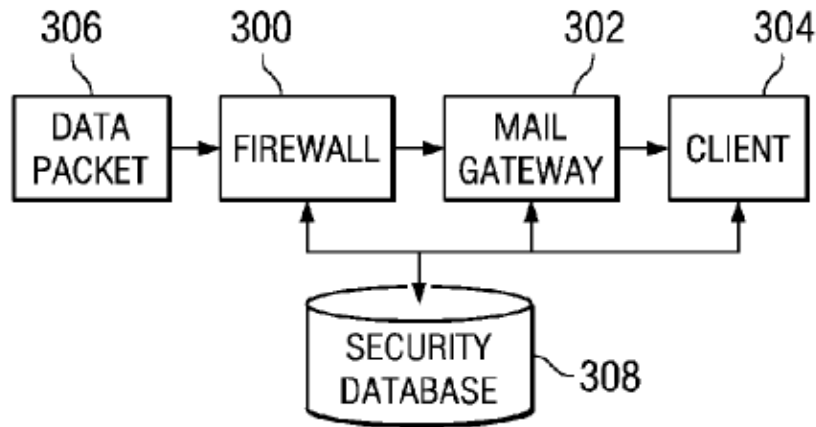


FIG. 3

Figure 3 depicts firewall 300, mail gateway 302, and client 304 that perform multiple levels of cooperative network security actions on data packets to prevent the introduction of malware. Ex. 1008 ¶ 33. Firewall 300 determines whether a data pack originates from a trusted source and if so, adds a signature to the data packet to indicate source verification was done. *Id.* ¶¶ 32–34. When mail gateway 302 receives data packet 306, it looks for a signature from a trusted security element such as a firewall, mail gateway, or router, performs a virus scan, and adds a signature to data packet 306 to indicate a virus scan was performed. *Id.* ¶¶ 34–36. Client 304 examines data packet 306 for signatures to indicate the data packet is from a trusted source and no viruses were found. Client may perform additional security actions such as scanning for spyware to save time and resources and avoid unneeded redundancy in scanning data packet 306. *Id.* ¶ 37.

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.

c. 1[b]

Petitioner contends that Keohane’s mail gateway 302 determines if a received data packet 306 includes a digital signature from a trusted security element in its header to indicate the data packet is transmitted from a second network security appliance in the CSF. Keohane’s gateway 302 also looks for a flag (e.g., a *code such as “01” or “02”*) to indicate the actions taken on the packet by a transmitting entity. Pet. 74–76 (citing Ex. 1008 ¶¶ 32, 34, 35, 38, 54, Fig. 7; Ex. 1001, 6:28–34, 6:54–59, 6:65–67; Ex. 1002 ¶ 171).

Patent Owner argues that Keohane’s “signature” indicates a security action was performed on a data packet but gives no information about a node or whether it participates in a CSF. Prelim. Resp. 23–24. Patent Owner argues that member nodes of a CSF check whether an incoming packet is from another member node based on a flag that indicates the network packet is from a member node. *Id.* at 24–25. These arguments are unavailing.

Keohane’s multilevel security system of network security appliances of firewall 300, mail gateway 302, and client 304 is configured to perform security actions as a CSF. It uses the same set of security policy or rules to determine which security action is taken by a transmitting device of the CSF. A firewall or gateway adds a signature to a data packet to indicate a trusted source, and packet codes identify actions taken so redundant actions are avoided by other devices. Ex. 1008 ¶¶ 23, 33–37, 53–55, Figs. 1, 3, 7.

Signatures are added to data packet 306 to indicate the packet is sent by a trusted security element of the CSF, the action performed, and the result (no viruses were found). Ex. 1008 ¶ 37. When client device 304 receives a data packet 306 with signatures from firewall 300 and mail gateway 302, it recognizes, based on the signatures, that the packet is from trusted devices in the CSF. Then, client 304 only performs an anti-spyware scan because mail gateway 302 performed a virus scan to reduce the time and resources used to process the data packet and unneeded redundancy. *Id.* If mail gateway 302 performs both virus and spyware scans and so indicates by signature in the data packet, “client 304 would take[] no action as the security action”

Keohane uses codes as flags in signatures to indicate the source of the data packet is a trusted source in the same CSF and to identify the security action that was performed. Ex. 1008 ¶ 38. A code of “01” or “policy 1” may indicate the source of the data packet is a trusted source. *Id.* A code of “02” or “policy 2” may indicate a virus scan was performed by the trusted element. *Id.*

d. 1[c], 1[d][i], and 1[d][ii]

Petitioner asserts that Keohane’s mail gateway 302 uses a signature in data packet 306 received from firewall 300 to determine firewall 300 of the CSF performed a security action before transmitting data packet 306 to mail gateway 302. Petitioner asserts that mail gateway 302 identifies the security action performed and determines a security action that was not performed (e.g., a virus scan). Petitioner contends that client device 304 determines a security action performed by mail gateway and a security action it needs to perform based on signatures in the data packet. Pet. 76–79 (citing Ex. 1008 ¶¶ 12, 32–38, 40, 54, 55, 58, Figs. 3, 7; Ex. 1002 ¶¶ 171, 173, 174).

e. 1[e]

Petitioner contends that Keohane's security elements execute local operations on a network traffic data packet based on the previous security action performed on the data packet by other devices in the CSF. Petitioner asserts that a signature added to the data packet by a trusted security element is used to identify the security action performed. Pet. 79 (citing Ex. 1008 ¶¶ 11, 36, 37; Ex. 1002 ¶ 180). These contentions, which Patent Owner does not contest at this stage, are supported by record evidence.

On this record, we find that Petitioner has established a reasonable likelihood that claim 1 is unpatentable over Keohane.

3. Dependent claims 2–5 and 10–12

Petitioner provides detailed contentions showing that claims 2–5 and 10–12 are obvious over Keohane. Pet. 79–88 (citing Ex. 1008 ¶¶ 12, 32, 34–38, 40, 53, 54, 56; Ex. 1002 ¶¶ 185–187, 191, 192, 196, 197, 200, 203, 204). These contentions, which Patent Owner does not contest at this stage, are supported by record evidence. On this record, we find that Petitioner has established a reasonable likelihood that claims 2–5 and 10–12 are unpatentable over Keohane.

4. Independent Claims 15, 21, 27; dependent claims 16, 22

Petitioner asserts that Keohane discloses the limitations of claims 15, 21, and 27 and dependent claims 16 and 22 by relying on its contentions for similar limitations of claim 1 and limitations in claims 2 and 5. Pet. 88–90. These contentions, which Patent Owner does not contest at this stage, are supported by record evidence. On this record, we find that Petitioner has established a reasonable likelihood that claims 15, 16, 21, 22, and 27 are unpatentable over Keohane.

I. Ground 6: Alleged Obviousness Over Keohane, Buruganahalli

Petitioner asserts that claims 6, 7, 17, 18, 23, 24, 28, and 29 are unpatentable under 35 U.S.C. § 103 over Keohane and Buruganahalli. Pet. 4, 90–96.

1. Motivation to combine

Petitioner asserts that a skilled artisan would consider complementary teachings of Buruganahalli to use metadata tags in data packets in Keohane to coordinate the operations of multiple network devices in a data path and avoid redundant actions as both references teach is desirable. Pet. 90–91.

2. Claims 6, 17, 23, and 28

Petitioner asserts that a skilled artisan would update metadata tags in Keohane, as Buruganahalli teaches, for claims 6, 17, 23, and 28 to indicate the analysis performed on network data by a device and reduce redundancy. Petitioner asserts that a skilled artisan would include this feature in Keohane so a security element does not have to add a signature to indicate the actions it performed thereby obviating the need for each device to read and process multiple signatures. Pet. 91–94 (citing 1005 ¶¶ 27, 32, 38, 40, 44, 48, Fig. 3; Ex. 1002 ¶¶ 222, 223, 226). These contentions, which Patent Owner does not contest at this stage, are supported by record evidence.

3. Claims 7, 18, 24, and 29

Petitioner asserts that a skilled artisan would remove metadata tags from network data before sending the data to “undesired network devices” in claims 7, 18, 24, and 29 to protect the network’s labeling mechanism. Pet. 94–96 (citing 1005 ¶¶ 29, 46–48, Fig. 3; Ex. 1002 ¶, 231). This contention, which Patent Owner does not contest at this stage, is supported by record evidence.

On this record, we find that Petitioner has established a reasonable likelihood that claims 6, 7, 17, 18, 23, 24, 28, and 29 are unpatentable over Keohane and Buruganahalli.

J. Ground 7: Alleged Obviousness over Keohane and Kumar

Petitioner asserts that claim 10 is unpatentable under 35 U.S.C. § 103 over Keohane and Kumar. Pet. 4, 96–97.

1. Motivation to combine

Petitioner contends that a skilled artisan would combine Kumar’s source authentication method of using a digital signature to create a security tag that is inserted into a data packet with Keohane to authenticate that the signature is associated with a trusted security element and to improve digital signature source authentication. Pet. 96–97 (citing Ex. 1006 ¶¶ 36, 49, 50, 54; Ex. 1002 ¶¶ 233, 236, 237). These contentions, which Patent Owner does not contest at this stage, are supported by record evidence.

2. Claim 10

Petitioner contends that Keohane discloses a flag associated with or comprising a signature of a transmitting security element so that a receiving security element can authenticate the sending element. Pet. 96. Petitioner asserts that Kumar teaches that a transmitting device can use a client ID, session key, or public key to create a digital signature that can be used to create a security tag that is inserted into a data packet so that a receiving device can recreate the digital signature to authenticate the security tag. *Id.* at 96–97. Petitioner asserts a skilled artisan would have incorporated this common source authentication into Keohane to authenticate the signature as associated with a trusted transmitting security element. *Id.* (citing Ex. 1006 ¶¶ 36, 45, 46, 49, 50; Ex. 1008 ¶ 54; Ex. 1002 ¶¶ 233, 236, 237).

On this record, we find that Petitioner has established a reasonable likelihood that claim 10 is unpatentable over Keohane and Kumar.

K. Ground 8: Alleged Obviousness over Keohane and Chandra-2

Petitioner contends that claims 13, 14, 19, 20, 25, 26, 30, and 31 are unpatentable under 35 U.S.C. § 103 over Keohane and Chandra-2. Pet. 4, 97–99.

1. Motivation to combine

Petitioner asserts that a skilled artisan would have been motivated to include Chandra’s well-known, commonly implemented security operations into Keohane to expand Keohane’s range of operations to yield predictable results. Pet. 97–98. This contention, which Patent Owner does not contest at this stage, is supported by record evidence.

2. Claims 13, 19, 25, and 30

Petitioner asserts that Chandra-2 discloses a network security device that provides logging, and a skilled artisan would have found network traffic logging obvious because it is well-known to use it for forensic analysis after a vulnerability or breach is found. Petitioner asserts a skilled artisan would have found it obvious to perform network traffic logging in Keohane. Pet. 98 (citing Ex. 1007 ¶ 23; Ex. 1002 ¶ 241). These contentions, which Patent Owner does not contest at this stage, are supported by record evidence.

3. Claims 14, 20, 26, and 31

Petitioner contends that Chandra-2 discloses a network security device that performs antivirus, intrusion prevention (IPS), content filtering, data leak protection (DLP), antispam, antispymware, reputation-based protections, network access control, load balancing, vulnerability management, traffic shaping, and content filtering as in claims 14, 20, 26, and 31. Pet. 98–99.

Petitioner asserts that the '825 patent recognizes that DLP and IPS are well known. Pet. 99. Petitioner contends that a skilled artisan would have found it obvious that Keohane's security elements could perform any or all of these well-known operations. *Id.* at 99. These contentions, which Patent Owner does not contest at this stage, are supported by record evidence. *See id.* at 98–99 (citing Ex. 1007 ¶¶ 23, 24; Ex. 1002 ¶ 243; Ex. 1001, 9:23–26).

On this record, we find that Petitioner has established a reasonable likelihood that claims 13, 14, 19, 20, 25, 26, 30, and 31 are unpatentable over Keohane and Chandra-2.

III. CONCLUSION

For the reasons discussed above, we are persuaded that Petitioner has demonstrated a reasonable likelihood of prevailing in establishing that at least one of claims 1–7 and 10–31 of the '825 patent is unpatentable.

IV. ORDER

In consideration of the foregoing, it is hereby:

ORDERED that *inter partes* review of the '825 patent is hereby instituted as to claims 1–7 and 10–31 on all grounds set forth in the Petition; and

FURTHER ORDERED that pursuant to 35 U.S.C. § 314(c) and 37 C.F.R. § 42.4, notice is hereby given of the institution of a trial on the grounds of unpatentability authorized above; the trial commences on the entry date of this decision.

IPR2023-00459
Patent 10,084,825 B1

For PETITIONER:

Thomas Millikan
Babak Tehranchi
PERKINS COIE LLP
millikan-ptab@perkinscoie.com
tehranchi-ptab@perkinscoie.com

For PATENT OWNER:

James Glass
John McKee
Quincy Lu
Andrew Holmes
Ognjen Zivojnovic
QUINN EMANUEL URQUHART & SULLIVAN LLP
jimglass@quinnemanuel.com
johnmckee@quinnemanuel.com
quincylu@quinnemanuel.com
drewholmes@quinnemanuel.com
ogizivojnovic@quinnemanuel.com