

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

NETSKOPE, INC.,
Petitioner,

v.

FORTINET, INC.,
Patent Owner.

Case No. IPR2023-00459
U.S. Patent No. 10,084,825

PATENT OWNER'S NOTICE OF APPEAL

Office of the General Counsel
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, Virginia 22313-1450

Notice is hereby given, pursuant to 37 C.F.R. § 90.2(a) and 35 U.S.C. §§ 141(c), 142, and 319, that Patent Owner Fortinet, Inc. (“Patent Owner”) appeals to the United States Court of Appeals for the Federal Circuit from the Final Written Decision of the Patent Trial and Appeal Board in Case No. IPR2023-00459, entered August 19, 2024 (Paper No. 33) (attached as Exhibit A). This notice is timely filed within 63 days of the issuance of the Final Written Decision. For the limited purpose of providing the Director with the information specified in 37 C.F.R. § 90.2(a)(3)(ii), Patent Owner indicates that the issues on appeal may include, but are not limited to, the following:

1. Whether the PTAB erred in finding that Petitioner has shown by a preponderance of the evidence that claims 1-7 and 10-31 of U.S. Patent No. 10,084,825 (“the ’825 Patent”) are unpatentable;
2. Whether the PTAB erred in finding that Petitioner has shown by a preponderance of the evidence that claims 1-5, 12, 15, 16, 21, 22, and 27 of the ’825 Patent are unpatentable under 35 U.S.C. § 103 as obvious in view of U.S. Pat. App. Pub. No. 2007/0204018 A1 (“Chandra”) alone;
3. Whether the PTAB erred in finding that Petitioner has shown by a preponderance of the evidence that claims 6, 7, 17, 18, 23, 24, 28, and 29 of the ’825 Patent are unpatentable under 35 U.S.C. § 103 as obvious in view of Chandra and U.S. Pat. App. Pub. No. 2014/0282843 A1 (“Buruganahalli”);
4. Whether the PTAB erred in finding that Petitioner has shown by a preponderance of the evidence that claims 10 and 11 of the ’825 Patent are

unpatentable under 35 U.S.C. § 103 as obvious in view of Chandra and U.S. Pat. App. Pub. No. 2009/0144818 A1 (“Kumar”);

5. Whether the PTAB erred in finding that Petitioner has shown by a preponderance of the evidence that claims 13, 14, 19, 20, 25, 26, 30, and 31 of the ’825 Patent are unpatentable under 35 U.S.C. § 103 as obvious in view of Chandra and U.S. Pat. App. Pub. No. 2017/0093917 A1 (“Chandra-2”);
6. Whether the PTAB erred in finding that Petitioner has shown by a preponderance of the evidence that claims 1-5, 10-12, 15, 16, 21, 22, and 27 of the ’825 Patent are unpatentable under 35 U.S.C. § 103 as obvious in view of U.S. Pat. App. Pub. No. 2008/0134332 A1 (“Keohane”) alone;
7. Whether the PTAB erred in finding that Petitioner has shown by a preponderance of the evidence that claims 6, 7, 17, 18, 23, 24, 28, 29 of the ’825 Patent are unpatentable under 35 U.S.C. § 103 as obvious in view of Keohane and Buruganahalli;
8. Whether the PTAB erred in finding that Petitioner has shown by a preponderance of the evidence that claim 10 of the ’825 Patent is unpatentable under 35 U.S.C. § 103 as obvious in view of Keohane and Kumar;
9. Whether the PTAB erred in finding that Petitioner has shown by a preponderance of the evidence that claims 13, 14, 19, 20, 25, 26, 30, and 31 of the ’825 Patent are unpatentable under 35 U.S.C. § 103 as obvious in view of Keohane and Chandra-2;
10. Whether the PTAB erred in all other prior interlocutory and underlying orders, decisions, rulings, findings and opinions decided adversely to Patent Owner, including procedural orders, discovery orders, or other findings and determinations.

Simultaneous with this submission and in accordance with 37 C.F.R. § 90.2(a), a copy of this Notice of Appeal is being filed with the Director of the United States Patent and Trademark Office, filed with the Patent Trial and Appeal Board, and served upon Petitioner in accordance with 37 C.F.R. § 42.6(e). In

addition, this Notice of Appeal, along with the required docketing fees, is being filed with the Clerk's Office for the United States Court of Appeal for the Federal Circuit in accordance with Fed. Cir. R. 15(a)(1).

Respectfully submitted,

Dated: October 21, 2024

By: /s/ James M. Glass

James M. Glass
jimglass@quinnemanuel.com
QUINN EMANUEL URQUHART &
SULLIVAN, LLP
51 Madison Ave, 22nd Floor
New York, New York 10010
Tel: (212) 849-7000
Fax: (212) 849-7100

Counsel for Patent Owner

CERTIFICATE OF FILING

The undersigned hereby certifies that, in addition to being filed electronically via PTAB P-TACTS, the foregoing document was filed by Express Mail on October 21, 2024, with the Director of the United States Patent and Trademark Office, at the following address:

Director of the United States Patent and Trademark Office
c/o Office of the General Counsel
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, Virginia 22313-1450.

CERTIFICATE OF FILING

The undersigned hereby certifies that a true and correct copy of the foregoing document was filed electronically by CM/ECF on October 21, 2024, with the Clerk's Office of the United States Court of Appeals for the Federal Circuit.

CERTIFICATE OF SERVICE

The undersigned hereby certifies that a copy of the foregoing document was served on October 21, 2024, by email at the following addresses:

millikan-ptab@perkinscoie.com

tehranchi-ptab@perkinscoie.com

Netskope-FortinetIPRTeam@perkinscoie.com

Dated: October 21, 2024

By: /s/ James M. Glass
James M. Glass
jimglass@quinnemanuel.com
QUINN EMANUEL URQUHART &
SULLIVAN, LLP
51 Madison Ave, 22nd Floor
New York, New York 10010
Tel: (212) 849-7000
Fax: (212) 849-7100

Counsel for Patent Owner

EXHIBIT A

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*.

JUDGMENT
Final Written Decision
Determining All Challenged Claims Unpatentable
35 U.S.C. § 318(a)

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 (“Pet.”), 1. Fortinet, Inc. (“Patent Owner”) timely filed a Preliminary Response. Paper 6. Applying the standard in 35 U.S.C. § 314(a), we instituted an *inter partes* review of all challenged claims on all grounds asserted in the Petition. Paper 10 (“Decision”).

After we instituted trial, Patent Owner filed a Patent Owner Response. Paper 18 (“PO Resp.”). Petitioner filed a Reply to Patent Owner’s Response. Paper 22 (“Reply”). Patent Owner filed a Sur-reply to Petitioner’s Reply. Paper 29 (“Sur-reply”).

An oral hearing was held on June 21, 2024, and a copy of the transcript was entered in the record. Paper 32 (“Tr.”).

We have jurisdiction pursuant to 35 U.S.C. § 6. This Decision is a Final Written Decision under 35 U.S.C. § 318(a) (2018) and 37 C.F.R. § 42.73 (2020) as to the patentability of the claims on which we instituted trial. Petitioner bears the burden of proving unpatentability of the challenged claims. *Dynamic Drinkware, LLC v. Nat’l Graphics, Inc.*, 800 F.3d 1375, 1378 (Fed. Cir. 2015). To prevail, Petitioner must prove unpatentability by a preponderance of the evidence. *See* 35 U.S.C. § 316(e); 37 C.F.R. § 42.1(d).

For reasons that follow, we determine that Petitioner has shown by a preponderance of the evidence that claims 1–7 and 10–31 of the ’825 patent are unpatentable.

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 (Patent Owner's Mandatory Notices), 2. Petitioner identifies the following *inter partes* review proceedings that challenge 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

The '825 patent describes methods to coordinate security operations performed on network traffic by network security appliances participating in a cooperative security fabric ("CSF") shown in Figure 1, reproduced below.

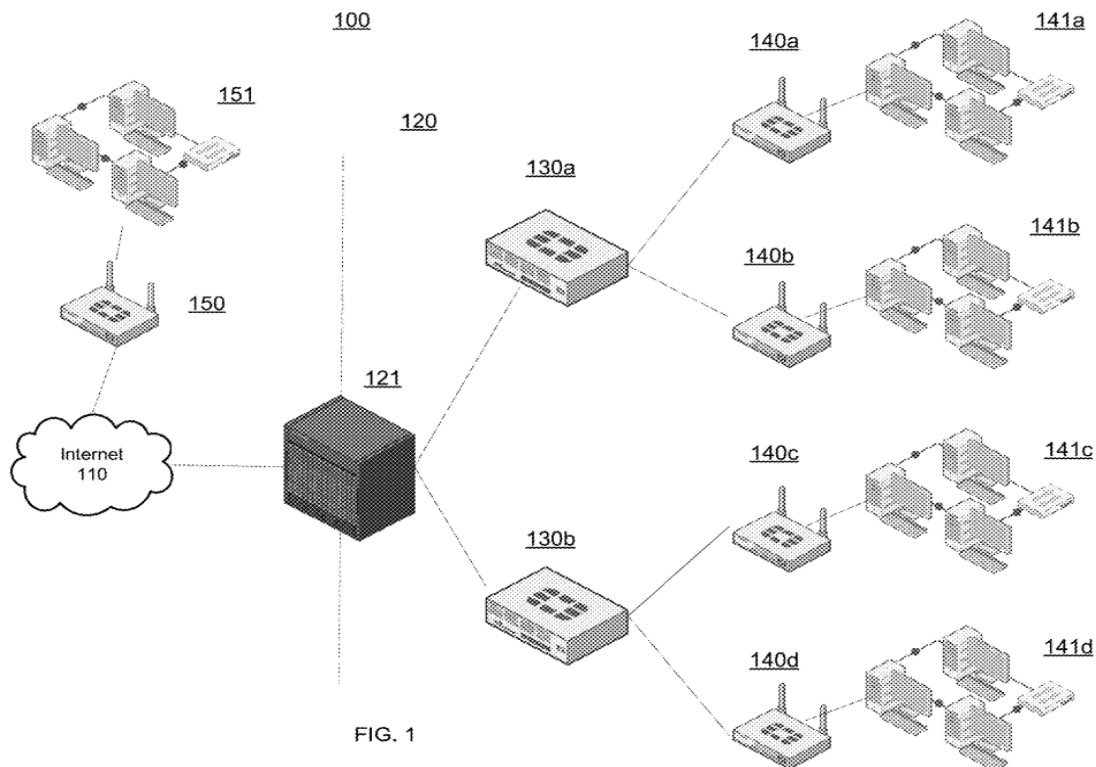


Figure 1 illustrates private network 120 connected to Internet 110 by root network security appliance 121 at the edge of network 120. Ex. 1001, 4:58–67, 5:10–18. Each of subnets 141a–d connects to a subnet network security appliance 140a–d that scans traffic sent to each subnet for malware, viruses, and high risk network accesses based on network policies. *Id.* at 5:19–25. Middle network security appliances 130a, 130b connect edge root network security appliance 121 to subnet network security appliances 140a–d and inspect network traffic based on local security policies. *Id.* at 5:26–31. “[R]oot, 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 shown in Figure 2, which is reproduced below. *Id.* at 2:29–31, 5:44–48.

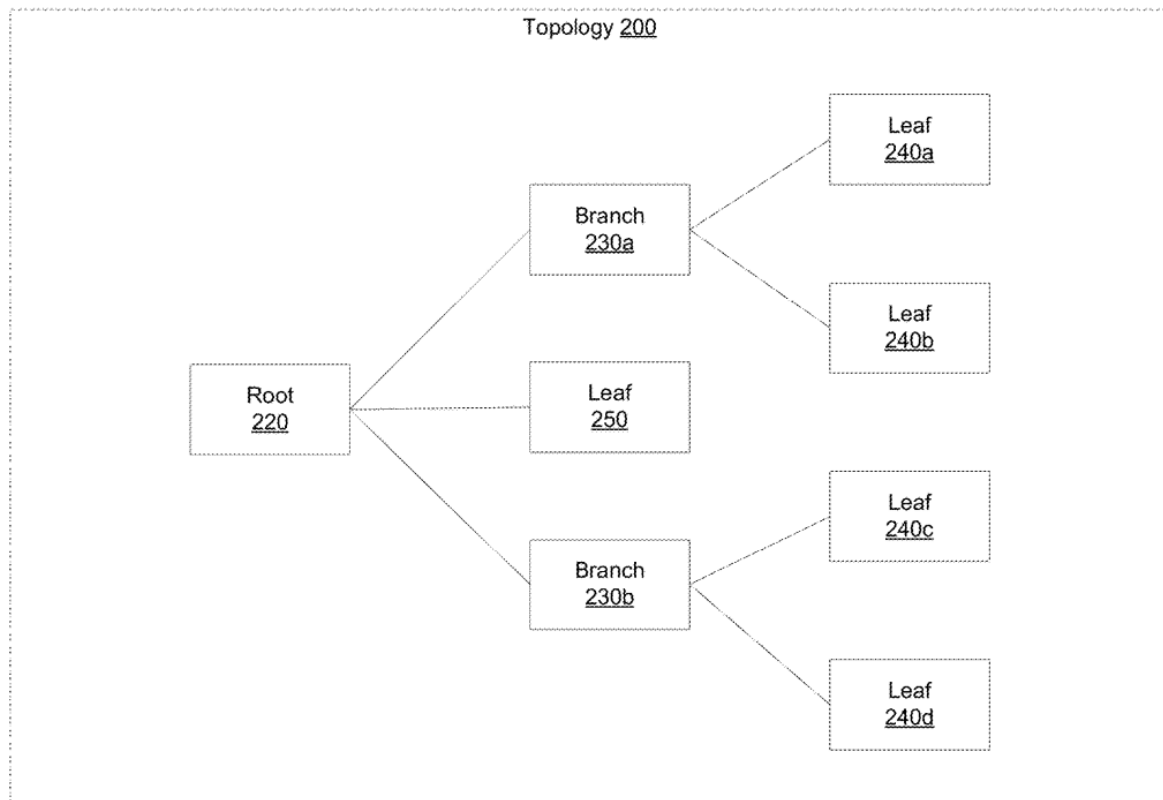


FIG. 2

Figure 2 shows 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 and acts in a wide area network (“WAN”) role that connects private network 120 to other networks or the Internet. *Id.* at 5:52–56. Branch nodes 230a, 230b correspond to middle network security appliances 130a, 130b that connect other network security appliances within the private network. *Id.* at 5:60–64. Leaf nodes 240a–240d, 250 are network security appliances that connect to endpoint devices that are sources or destinations of network traffic, such as personal computers, servers, laptops, and printers. *Id.* at 6:1–9 (describes leaf nodes as elements 250a–250d). The root and the 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 identify network security operations (e.g., antivirus scanning, content filtering, antispam, data leak prevention) performed by the transmitting member node. As a result, subsequent member nodes do not need to execute these operations again. *Id.* at 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.

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; *see* Pet. 100–101 (claims listing).

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 Declarations of Dr. Michael Franz. Ex. 1002; Ex. 1019.

Patent Owner relies on a Declaration of Dr. John Black Jr. Ex. 2004.

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.” PO Resp. 3. 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, but our decision would be the same under either formulation.

B. Claim Interpretation

We interpret the claims “using the same claim construction standard that would be used to construe the claim in a civil action under 35 U.S.C. 282(b).” 37 C.F.R. § 42.100(b). Under that standard, words of a claim are generally given their ordinary and customary meaning as understood by a person of ordinary skill in the art at the time of the invention. *Phillips v. AWH Corp.*, 415 F.3d 1303, 1312 (Fed. Cir. 2005) (en banc). We construe the claims only to the extent necessary to reach our final written decision. *See Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co.*, 868 F.3d 1013, 1017 (Fed. Cir. 2017) (“[W]e need only construe terms ‘that are in controversy, and only to the extent necessary to resolve the controversy.’”).

1. “cooperative security fabric” or “CSF”

a. Petitioner’s contentions

Petitioner asserts that a “cooperative security *fabric*” is “devices that form a network topology and work together to coordinate security operations among them.” Reply 1, 3, 4. Petitioner agrees that a “fabric” is “a network topology such as the physical structure of a switch or network.” *Id.* at 2 (citing Decision 9, 28). Petitioner asserts a “fabric” is “a network topology,” “cooperative” is “marked by a willingness and ability to work with others” (Ex. 1013), and “security” is “measures taken to guard against espionage or sabotage, crime, attack, or escape.” *Id.* at 4 (citing Ex. 1013; Ex. 1014).

b. Patent Owner’s arguments

Patent Owner argues, “the plain meaning of the term ‘fabric’ ‘requires network nodes that process bidirectional communications’” (PO Resp. 10), and a CSF is “a topology of network security appliances that cooperate to inspect incoming and outgoing traffic along multiple interconnected paths” (*id.* at 13, 20). Patent Owner argues that “a ‘fabric’ topology consists of multiple paths to and from endpoints” so the cabling resembles interwoven threads in a piece of cloth that is a “fabric.” *Id.* at 14–15 (citing Ex. 2004 ¶¶ 48, 49; Ex. 2005, 7:25–8:8). Patent Owner argues that a “cooperative security fabric” includes different paths of network appliances so network traffic transmitted to/from the network may go through multiple network security appliances along a path within the network. *Id.* at 15 (citing Ex. 1001, 1:33–37; Ex. 2004 ¶¶ 50, 52). Patent Owner argues that Figure 2 of the ’825 patent depicts a cooperative security fabric of three different paths through the network. *Id.* at 16–17. We find Patent Owner’s arguments unavailing, and belied by the intrinsic evidence, as discussed below.

c. *Analysis*

Although Patent Owner argues that a CSF has bidirectional traffic, claims 1, 15, 21, and 27 recite methods in which a first network security appliance of a CSF receives network traffic to inspect, determines whether the traffic was transmitted from a second network security appliance that executed security operations on the traffic, determines network security operations for the first network security appliance to execute based on any security operations executed by the second network security appliance, and executes operations on the traffic. Ex. 1001, 10:58–11:17, 12:31–60, 13:20–47, 14:13–37. As claimed, network traffic may travel in one direction from a second network security appliance to a first network security appliance.

The '825 patent describes unidirectional traffic as “one embodiment” of the CSF. A first network security appliance receives *incoming* network traffic and determines if the *incoming* network traffic is transmitted from a second network security appliance based on the source address of the traffic and determines operations that the second network security appliance executed. Ex. 1001, 2:48–56. In this embodiment, traffic travels in a single *incoming* direction between network security appliances. Tr. 30:22–31:18.

The '825 patent also describes the “cooperation” in a CSF as “[t]he network packet carrying the flag is transmitted to another member node *at the next hop.*” Ex. 1001, 6:28–34 (emphasis added); *id.* at 8:3–8. Traffic always flows from one hop to a next hop along the same path between root 220 at the edge of the network and each particular endpoint (leaf) shown in Figure 2 below. Traffic does not flow along different interconnected paths when it travels from root 220 to an endpoint leaf 240a–240d, 250 as Patent Owner asserts is required of a CSF. PO Resp. 13–15.

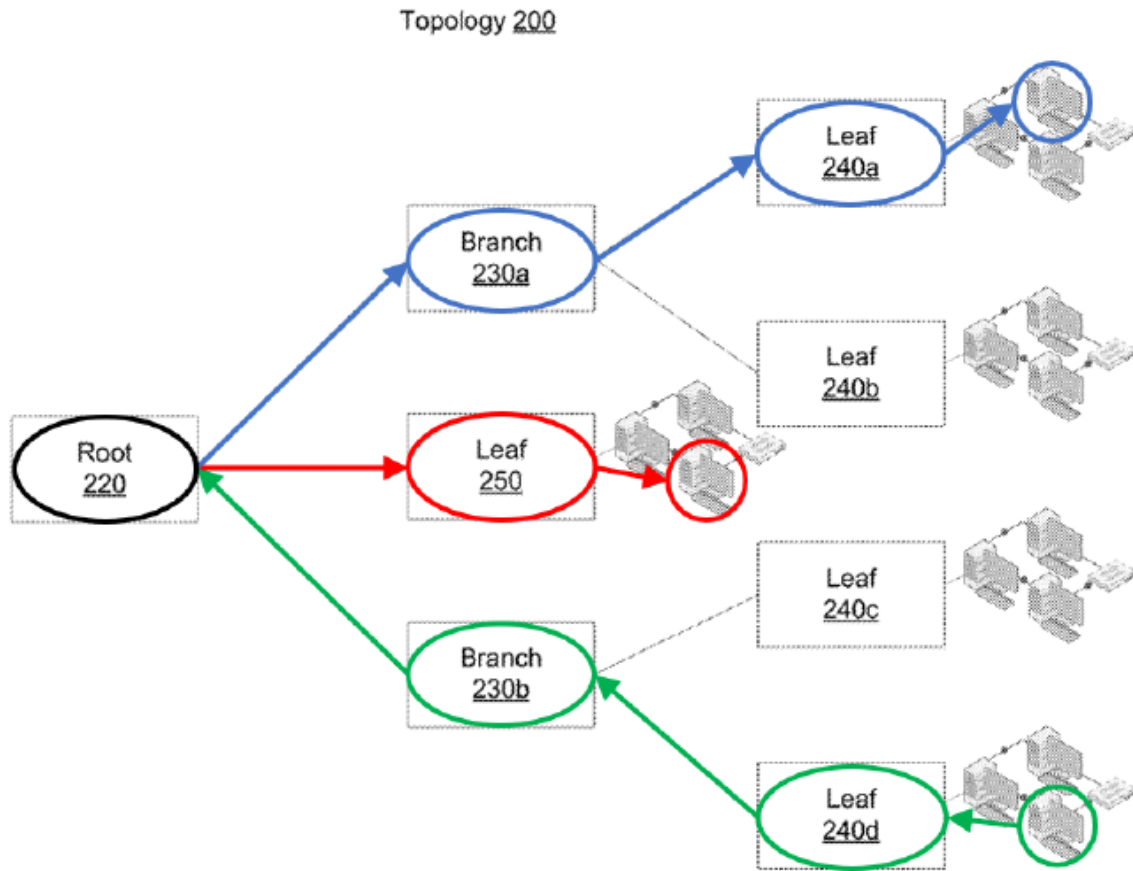


Figure 2 is “an exemplary topology of a cooperative security fabric (CSF)” with Patent Owner’s annotation of network traffic paths. Ex. 1001, 2:29–31; PO Resp. 16. Traffic travels along a single path from root 220 to branch 230a to leaf 240a to the blue end node. Traffic travels along a single path from root 220 to leaf 250 to the red end node. Traffic from the green node travels along a single path to leaf 240d to branch 230b to root 220.

Network security appliances only *cooperate* along a single red, green, or blue path to inspect traffic between an endpoint and root node 220. They do not cooperate with appliances on different colored paths. A node only determines operations performed by the previous node along the same green, red, or blue path. Ex. 1001, 7:33–35, Fig. 3 (step 304). This “fabric” is only single paths that start at root 220 at the edge of the network. *Id.* at 5:55–56.

d. Conclusion

We interpret “cooperative security fabric” to mean “a network topology of devices that coordinate their efforts to inspect network traffic.”

C. Principles of Law

A patent claim is unpatentable under 35 U.S.C. § 103 if differences between the claimed invention and the prior art are such that the invention, 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 the claimed invention 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: 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. 19–46.

1. *Chandra*

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.

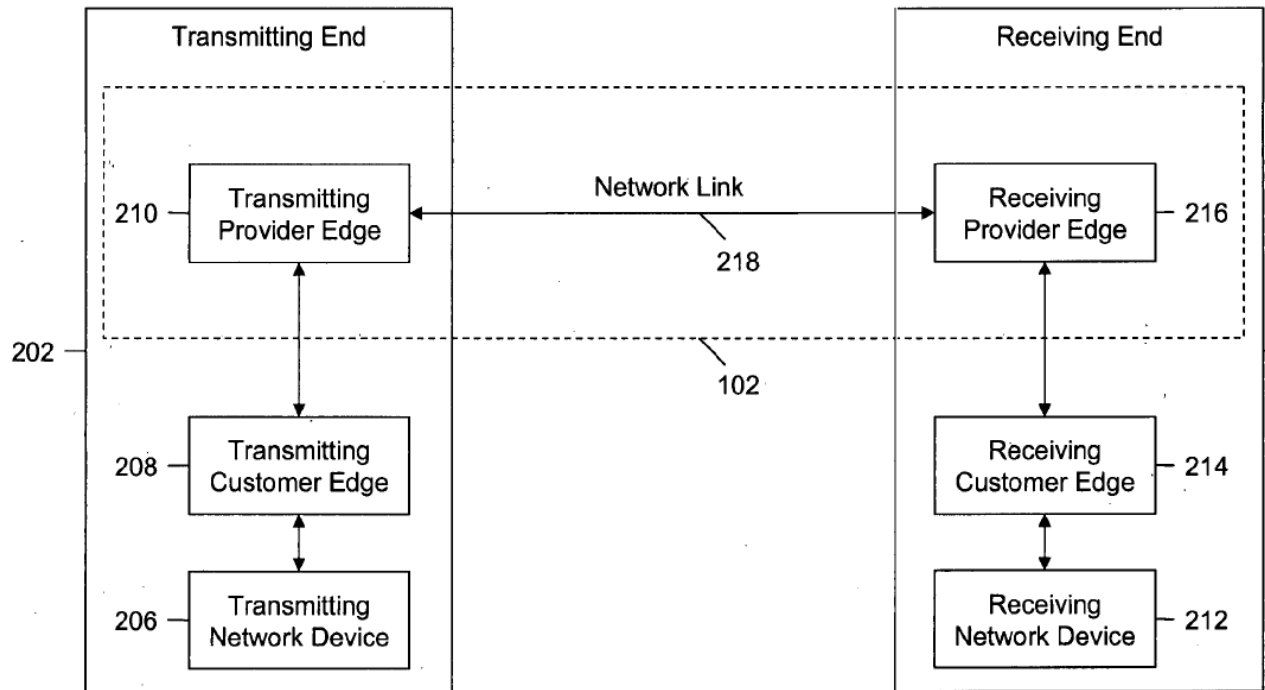


Figure 2 shows transmitting CE 208 and receiving CE 214 as security-based devices connected to transmitting and receiving provider edge (“PE”) 210, 216 at the edges of their networks. Ex. 1004 ¶ 30. Transmitting CE 208 and receiving CE 214 register with one another and exchange CE labels. When receiving CE 214 subsequently 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. *Id.* ¶ 34.

After the CE labels are exchanged, 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. Ex. 1004 ¶ 34. 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 receiving end set of labels is registered and stored by receiving CE 214 in a table shown above so receiving CE 214 can determine if a data packet was sent by transmitting CE 208. Ex. 1004 ¶¶ 34, 35, 52. 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. Thus, receiving CE 214 does not perform these security actions in order to avoid performing redundant security actions. *Id.* ¶¶ 52, 53.

2. *Independent Claim 1*

a. *1[pre]: “A method comprising:”*

(1) *Petitioner’s contentions*

Petitioner contends that Chandra discloses a method that obviates redundant actions by tagging data packets with a label to indicate a first set of actions performed on the data packet. Pet. 22 (citing Ex. 1004 ¶ 18).

(2) *Patent Owner’s arguments*

Patent Owner does not contest Petitioner’s assertions that Chandra discloses element 1[pre]. *See generally* PO Resp.; Sur-reply.

(3) *Conclusion*

Based on the parties’ contentions and record evidence, we determine that Chandra discloses element 1[pre] by a preponderance of evidence to the extent the preamble is limiting.

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;”*

(1) *Petitioner’s contentions*

Petitioner asserts that Chandra uses receiving CE 214, which is a security-based device such as Intrusion Detection Systems or firewalls, to perform network security operations and coordinate security actions with other appliances to receive and inspect data packets in network traffic. Pet. 22–23 (citing Ex. 1004 ¶ 30, Fig. 2; Ex. 1001, 4:16–18; Ex. 1002 ¶ 65). Petitioner asserts that Chandra implemented the receiving CE in a private network 102 like a local network or virtual private network (“VPN”). *Id.* at 23–26 (citing Ex. 1004 ¶¶ 4–7, 21, 58–68, Fig. 8; Ex. 1001, 4:65–67 (a VPN is a private network), 5:1–2, Fig. 1; Ex. 1002 ¶¶ 67, 68).

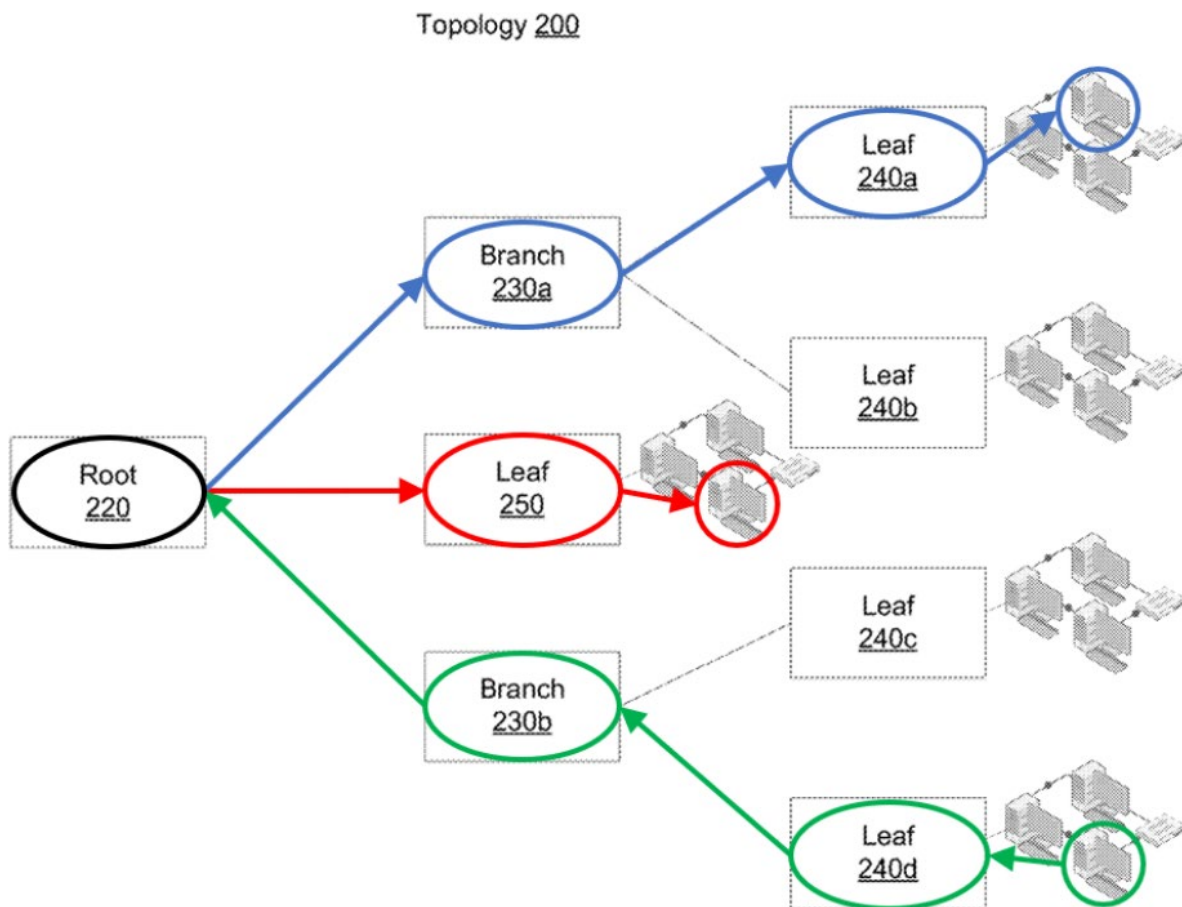
Petitioner contends that Chandra's receiving CE 214 participates in a cooperative security fabric (CSF) by cooperating with transmitting CE 208 to coordinate security actions performed on network traffic by authenticating each other and exchanging labels used to coordinate security actions to allow coordinated enforcement of rules that helped to obviate redundant operations similar to the '825 patent's description of coordinating operations of a CSF among members to avoid redundant operations. Pet. 26–27 (citing Ex. 1004 ¶¶ 18–20, 24–26, 30, 33, 34; Ex. 1001, 1:64–68, 5:45–47, 6:18–20; Ex. 1002 ¶¶ 69, 70). Petitioner contends that receiving CE 214 does so by receiving network traffic (tagged data packets) from receiving provider edge (PE) 216, removing the tagged CE label, and comparing the CE label tagged on the data packet with the registered receiving end set of labels to identify the first set of actions. *Id.* at 27–28 (citing Ex. 1004 ¶¶ 32, 37, 46).

(2) *Patent Owner's arguments*

Patent Owner argues that “Ground 1 fails to establish that Chandra discloses a ‘cooperative security fabric’ whose plain meaning is ‘a topology of network security appliances that cooperate to inspect incoming and outgoing traffic along multiple interconnected paths.’” PO Resp. 35. Patent Owner argues that “the claimed CSF requires inspection of incoming and outgoing traffic, but in Chandra, both the transmitting and receiving device are *within the same network*.” *Id.* Patent Owner asserts, “the transmitting and receiving CE only process internal network 102 communication and thus do not ‘cooperate to inspect incoming and outgoing traffic,’ which is part of the plain meaning of ‘cooperative security fabric.’” *Id.* at 36. Patent Owner argues that traffic is inspected on each end by a transmitting and a receiving CE rather than multiple network security appliances. *Id.* at 38.

(3) *Analysis*

We agree with Petitioner that “the claims only require two appliances and traffic to go from one appliance to the other.” Reply 11. Nothing in the claims or element 1[a] requires network traffic to originate from outside the private network or the CSF. Dr. Black testifies that the background of the ’825 patent describes a need for a CSF to coordinate operations performed on network traffic that is “transmitted to/from the network” to avoid or reduce redundant operations among members of the CSF” (Ex. 2004 ¶¶ 44, 50), but Dr. Black describes the claimed network fabric and CSF entirely in the context of controlling network traffic transmitted *within the enterprise network topology 200* as illustrated in Figure 2 of the ’825 patent (*id.* ¶ 52), which we discussed in Section II.B.1. *supra* and reproduce again below.



In Figure 2, Patent Owner annotates paths taken by network traffic *within* network topology 200 comprising root 220, branches 230a, 230b, and leaves 240a–d, 250 *within* network 200. PO Resp. 16–17; Ex. 2004 ¶ 52.

In addition, Chandra’s network 102 is “a collection of individual networks, interconnected with each other and functioning as a single large network.”⁷ Ex. 1004 ¶ 21. Network 102 can include LANs, WANs, and/or MANs. *Id.* As a result, network devices 104 located in different networks of network 102 transmit to one another via edge network links 218 within this internetwork of networks 102. *Id.* ¶¶ 8, 9, 21–30, Figs. 1, 2; Pet. 22–26.

Transmitting and receiving CEs 208, 214 are security-based devices at the edges of different networks in network 102 to control incoming network traffic sent between transmitting and receiving network devices 206, 212 located in different networks. Ex. 1004 ¶ 30. A plurality of CEs can be associated with a single PE to receive incoming network traffic from a transmitting CE. Ex. 1004 ¶ 28. Thus, network traffic is transmitted from network devices 104 connected to a plurality of CEs that connect to other CEs via edge network link 218 and to other network devices 104 connected to those CEs “along multiple interconnected paths” (*see id.* ¶¶ 28–30) that satisfies Patent Owner’s definition of CSF (PO Resp. 13). The sending and receiving CEs “constitute multiple cooperating network security appliances” contrary to Patent Owner’s arguments (PO Resp. 38), as do CEs 208, 214.

⁷ The term “Internet” is “[s]hort for Internetwork” and means “[a] set of computer networks that may be dissimilar and are joined together by means of gateways that handle data transfer and conversion of messages from the sending networks’ protocols to those of the receiving network.” *Microsoft Computer Dictionary, Fifth Edition* 281 (Microsoft Press 2002) (Ex. 3001); Ex. 1008 ¶ 24 (Internet is worldwide collection of networks and gateways).

(4) *Conclusion*

Based on the parties' contentions and evidence, we agree with and adopt Petitioner's analysis that Chandra discloses or suggests element 1[a]. Accordingly, we determine Petitioner has demonstrated by a preponderance of evidence that Chandra discloses or suggests element 1[a].

- c. *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) *Petitioner's contentions*

Petitioner asserts that Chandra discloses a receiving CE (first network security appliance) that determines whether network traffic was transmitted from a transmitting CE (second network security appliance) by using a label (flag) carried by the traffic. Pet. 28. Petitioner asserts that the transmitting and receiving CEs authenticate each other and exchange labels to coordinate their security operations so receiving CE 214 recognizes CE labels in traffic sent from transmitting CE 208. *Id.* (citing Ex. 1004 ¶¶ 31–35, 47, Fig. 2). Petitioner asserts that transmitting CE 208 tags packets of network traffic received from network device 206 with a CE label to indicate a first set of actions performed and the tagged network traffic travels from transmitting CE 208 to transmitting PE 210 to receiving PE 216 to receiving PT 216 and then to receiving CE 214, which checks if the data packet was tagged with a CE label from the registered set of labels exchanged with the transmitting CE (the second security appliance participating in the CSF). *Id.* at 28–32 (citing Ex. 1004 ¶¶ 31, 32, 37, 46–49, 52, Figs. 2, 6, 7; Ex. 1001, 6:28–34, 6:54–59, 6:65–67; Ex. 1002 ¶¶ 76, 77).

(2) *Patent Owner's arguments*

Patent Owner does not contest Petitioner's assertions that Chandra discloses and suggests element 1[b]. *See generally* PO Resp.; Sur-reply.

(3) *Conclusion*

Based on the parties' contentions and evidence, we agree with and adopt Petitioner's undisputed analysis that Chandra discloses or suggests element 1[b]. Accordingly, we determine Petitioner has demonstrated by a preponderance of evidence that Chandra discloses or suggests element 1[b].

- d. *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 security appliance;*

(1) *Petitioner's contentions*

Petitioner contends that Chandra discloses that once a receiving CE determines a data pack of network traffic was sent from a transmitting CE participating in the CSF, it determines the security operations performed by the transmitting CE on the data packet at transmitting CE 208. Pet. 32–33 (citing Ex. 1004 ¶¶ 32, 46, Fig. 6; Ex. 1002 ¶ 78).

(2) *Patent Owner's arguments*

Patent Owner does not contest Petitioner's assertions that Chandra discloses and suggests element 1[c]. *See generally* PO Resp.; Sur-reply.

(3) *Conclusion*

Based on the parties' contentions and evidence, we agree with and adopt Petitioner's undisputed analysis that Chandra discloses or suggests element 1[c]. Accordingly, we determine Petitioner has demonstrated by a preponderance of evidence that Chandra discloses or suggests element 1[c].

- e. 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,*

(1) Petitioner's contentions

Petitioner asserts that the receiving CE determines a second set of local actions to perform based on the actions performed by the transmitting CE. Pet. 34–35 (citing Ex. 1004 ¶¶ 18, 32, 46, Fig. 6; Ex. 1002 ¶ 82).

(2) Patent Owner's arguments

Patent Owner does not contest Petitioner's assertions that Chandra discloses and suggests element 1[d][i]. *See generally* PO Resp.; Sur-reply.

(3) Conclusion

Based on the parties' contentions and evidence, we agree with and adopt Petitioner's undisputed analysis that Chandra discloses or suggests element 1[d][i], and we determine that Petitioner has demonstrated by a preponderance of evidence Chandra discloses or suggests element 1[d][i].

- f. 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;*

(1) Petitioner's contentions

Petitioner asserts that Chandra's receiving CE skips network security operations that were executed by the transmitting CE and performing non-redundant actions. Pet. 35–36 (citing Ex. 1004 ¶¶ 37, 53; Ex. 1002 ¶ 83).

(2) Patent Owner's arguments

Patent Owner does not contest Petitioner's assertions that Chandra discloses and suggests element 1[d][ii]. *See generally* PO Resp.; Sur-reply.

(3) *Conclusion*

Based on the parties' contentions and evidence, we agree with and adopt Petitioner's undisputed analysis that Chandra discloses or suggests element 1[d][ii], and we determine that Petitioner has demonstrated by a preponderance of evidence Chandra discloses or suggests element 1[d][ii].

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

(1) *Petitioner's contentions*

Petitioner asserts that Chandra's receiving CE executes a second set of local actions (operations). Pet. 36–37 (citing Ex. 1004 ¶ 46; Ex. 1002 ¶ 85).

(2) *Patent Owner's arguments*

Patent Owner does not contest Petitioner's assertions that Chandra discloses and suggests element 1[e]. *See generally* PO Resp.; Sur-reply.

(3) *Conclusion*

Based on the parties' contentions and evidence, we agree with and adopt Petitioner's undisputed analysis that Chandra discloses or suggests element 1[e], and we determine that Petitioner has demonstrated by a preponderance of evidence Chandra discloses or suggests element 1[e].

h. *Conclusion*

We determine that Petitioner has established by a preponderance of evidence that claim 1 is unpatentable over Chandra.

3. *Independent Claims 15, 21, and 27*

a. *Petitioner's contentions*

Petitioner asserts that Chandra disclosed elements of claims 15, 21, and 27 for the reasons provided in its contentions for elements of claims 1–3 and 5, which it incorporates by reference. Pet. 44–46.

b. Patent Owner's arguments

Patent Owner argues that Chandra does not disclose a “cooperative security fabric” for the same reasons as claim 1. *See* PO Resp. 35–38.

c. Analysis

We determine that Chandra discloses a cooperative security fabric as discussed in Section II.D.2.b. *supra* for element 1[a].

d. Conclusion

Based on the parties' contentions and evidence, we agree with and adopt Petitioner's analysis that Chandra discloses or suggests claims 15, 21, and 27, and we determine that Petitioner has established by a preponderance of evidence that claims 15, 21, and 27 are unpatentable over Chandra.

4. *Claim 2: wherein said determining [of element 1[d][ii]] further comprises determining, by the first network security appliance, one or more network security operations that are to be executed by the first network security appliance except the one or more network security operations that are executed by the second network security appliance based on local network policies.*

a. Petitioner's contentions

Petitioner asserts that Chandra's receiving CE determines actions to perform that were not executed by a transmitting CE based on local network policies. Pet. 37–38 (citing Ex. 1004 ¶¶ 18, 35, 37, 53; Ex. 1002 ¶¶ 89, 90).

b. Patent Owner's arguments

Patent Owner argues that “Chandra never states that the second set of actions is determined according to a policy that is local to the receiving CE.” PO Resp. 39 (“Chandra discloses that actions are performed according to a *global* policy, or at least, a policy that is shared by endpoints.”). Patent Owner asserts that Chandra uses global labels and rules. *Id.* at 39–40.

c. Analysis

The '825 patent describes root, middle, and subnet network security appliances being configured with local policies that control the operations that they perform on network traffic. Ex. 1001, 5:26–31, 5:40–43. These CSF member nodes execute local network security operations based on policies that are configured at each node. *Id.* at 8:3–15, Fig. 3 (step 306).

We find that Chandra configures a receiving CE with a set of local policies as registered, locally-stored labels and rules that control the security operations it performs on network traffic. Ex. 1004 ¶¶ 34–46, 50–56, Figs. 2–6; *see* Pet. 38; Reply 23–24. The local rules determine security actions that a receiving CE performs on network traffic. Ex. 1004 ¶¶ 34–46, 50–56.

Even if Chandra's VPN network 102 also provides a global policy, Chandra discloses that the locally-stored table of CE labels and rules takes precedence over such global policies to control operations of a receiving CE and avoid redundancy. Ex. 1004 ¶¶ 18, 34–46, 50–56. If a global security policy requires CEs to perform Rules A–D, local rules stored at a receiving CE override the global policy and require a receiving CE to perform Rules C and D if the receiving CE determines the transmitting CE already performed Rules A and B. *Id.* ¶¶ 18, 37, 53; *see* Ex. 1001, 8:3–8 (a node may override CSF rules based on local policies). Chandra's local rules also may require a receiving CE to perform redundant actions or no actions. Ex. 1004 ¶ 18.

d. Conclusion

Based on the parties' contentions and evidence, we agree with and adopt Petitioner's analysis that Chandra discloses or suggests claim 2, and we determine Petitioner has established by a preponderance of evidence that claim 2 is unpatentable over Chandra.

5. *Dependent Claims 3–5, 16, and 22*

a. *Petitioner’s contentions*

Petitioner asserts that Chandra discloses that a receiving CE (first network security appliance) determines actions to take that a transmitting CE (second network security appliance) already performed as recited in claim 3. Pet. 39–40 (citing Ex. 1004 ¶ 18 (redundant actions); Ex. 1002 ¶ 93).

Petitioner asserts that Chandra discloses that a receiving CE performs a third set of local action specified by a local policy when it receives a data packet that was not transmitted by a transmitting CE as recited in claim 4. Pet. 40–42 (citing Ex. 1004 ¶¶ 47, 48, 53, Fig. 7; Ex. 1002 ¶¶ 95, 96).

Petitioner contends that Chandra discloses that a transmitting CE performs a first set of actions on a data packet and tags the data packet with a CE label, which is a flag, to indicate the network security operations that it performed as recited in claims 5, 16, and 22. Pet. 43 (citing Ex. 1004 ¶ 31), 45–46 (citing contentions for claim 5 for claims 16 and 22).

b. *Patent Owner’s arguments*

Patent Owner does not argue claims 3–5, 16, and 22 separate from challenging their independent claims. *See generally* PO Resp.; Sur-reply.

c. *Conclusion*

Based on the parties’ contentions and evidence, we agree with and adopt Petitioner’s undisputed analysis that Chandra discloses or suggests claims 3–5, 16, and 22, and we determine Petitioner has established by a preponderance of evidence that those claims are unpatentable over Chandra.

6. *Claim 12: wherein the one or more packets in which the flag is carried comprises a first packet of a session.*

a. *Petitioner's contentions*

Petitioner asserts that Chandra fails to disclose a flag carried in a first session packet, but this feature would have been obvious because TCP/IP is the most common internet protocol used to establish connections between a client and server before data can be sent, and the sequence starts by opening a connection, and it would have been obvious to send a flag(s) in the first packet to set up the connection. Pet. 43–44 (citing Ex. 1002 ¶¶ 100, 101).

b. *Patent Owner's arguments*

Patent Owner asserts that Petitioner provides no rationale to include Chandra's labels in a first packet of a session rather than any other packet. PO Resp. 41 ("Including flags in the first packet may be sufficient, but that does not explain *why* a POSITA would do so in the first place."). Patent Owner asserts that Chandra requires labels to be exchanged between a transmitting CE and receiving CE before a data packet is received so the flag is not received until several other transmissions have occurred. *Id.* at 42.

c. *Analysis*

We agree with Petitioner that a skilled artisan would have wanted to transmit flags in a first session packet because security appliances need to receive flags to perform security operations on packets. Reply 24. A skilled artisan would have understood that the sooner a receiving CE obtains a flag listing security operations that were performed, the sooner it can process the data packets for network security actions that avoid redundant operations. *DyStar Textilfarben GmbH & Co. Deutschland KG v. C.H. Patrick Co.*, 464 F.3d 1356, 1368 (Fed. Cir. 2006) (an implicit motivation exists when an "improvement" makes a process faster or more efficient); Ex. 1019 ¶ 56.

The authentication and exchange of CE labels used to tag data packets occurs before a session to transmit data packet so the first session packet can include such flags/labels. Reply 24 (citing Ex. 1004 ¶ 34); *cf.* PO Resp. 42.

d. Conclusion

Based on the parties' contentions and evidence, we agree with and adopt Petitioner's analysis that Chandra discloses or suggests claim 12, and we determine Petitioner has established by a preponderance of evidence that claim 12 is unpatentable over Chandra.

E. Ground 2: 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 the combination of Chandra and Buruganahalli. Pet. 46–58.

1. Buruganahalli

Buruganahalli coordinates security actions among network security devices (firewall 30, router 32, proxy server 34, and anti-virus server 38) so they do not perform the same actions on network data. Ex. 1005 ¶¶ 26–30. To avoid a network device reprocessing network data 28, Buruganahalli's network devices use the results of processing network data 28 by previous network devices 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. When network data 28 is forwarded to the next network device for processing, the network device may analyze a metadata tag added by the previous network device to obtain information about network data 28 and avoid processing the network data in the same way. *Id.* ¶ 28.

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

a. *Motivation to combine*

(1) *Petitioner's contentions*

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 they both disclose network security devices that coordinate actions to reduce redundancy. Pet. 50. Petitioner asserts that Chandra discloses network security devices, such as a transmitting CE and a 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, and Buruganahalli's complementary teachings would improve Chandra similarly. *Id.* (citing Ex. 1004, Abstr., ¶ 30; Ex. 1005 ¶¶ 27, 28). Petitioner asserts that a skilled artisan would have added Buruganahalli's ability to update metadata tag data to Chandra so each device did not have to add its own label to indicate the actions it performed on data packets, which would increase the time taken by the next device to read and process a packet, increase latency, and use more space to store labels along the data path. *Id.* at 53 (citing Ex. 1002 ¶ 122).

(2) *Patent Owner's arguments*

Patent Owner does not contest Petitioner's assertions that it would have been obvious to combine complementary teachings of Buruganahalli and Chandra to improve Chandra. *See generally* PO Resp.; Sur-reply.

(3) *Conclusion*

We determine that Petitioner has established by a preponderance of evidence that a skilled artisan would have been motivated to combine the teachings of Buruganahalli and Chandra with a reasonable expectation of success, and we agree with and adopt Petitioner's analysis.

- b. 6[a]/17[a]/23[a]/28[a]: “The method of claim [1/15/21/27], further comprising: updating, by the first network security appliance, the flag to indicate the network security operations executed by the first network security appliance;”

(1) *Petitioner’s contentions*

Petitioner contends that Buruganahalli discloses network devices that updated metadata tags (flags) to indicate actions performed by the network devices. Pet. 51. Petitioner asserts that Figure 3 of Buruganahalli depicts network devices 50, 52, 54 connected in network 18, and network device 52 received network data 58 from network device 54 with network data 58 that included metadata tag 64. *Id.* at 51–53 (citing Ex. 1005 ¶¶ 32, 38, 40, Fig. 3; Ex. 1002 ¶ 121). Petitioner asserts that analysis module 66 of network device 52 analyzed this data and added or updated fields in metadata tag 64 by tag module 60 to form metadata tag 64. *Id.* at 52–53 (citing same).

(2) *Patent Owner’s arguments*

Patent Owner argues that Buruganahalli processes packets along a single sequence of network devices 54, 52, 50, which is not part of a “fabric” because there are not multiple paths to traverse. PO Resp. 42–43. Patent Owner argues that adding these network devices to Chandra does not add a network appliance participating in a CSF. *Id.* at 43 (citing Ex. 2004 ¶ 106).

(3) *Analysis*

As discussed in Section II.B.1. *supra*, a “cooperative security fabric” is “a network topology of devices that coordinate their efforts to inspect network traffic.” Patent Owner’s arguments for multiple paths are not commensurate with the claim scope or a CSF because two network security appliances can form a CSF by coordinating their security operations along a single path or fiber, *as claimed*. Ex. 1001, 2:48–58, 6:28–43, Fig. 2.

Buruganahalli's topology of devices 50, 52, 54 coordinates security operations that they perform on network data 58 sent from network device 54 to network device 52 to network device 50 from one hop to the next hop. Ex. 1005 ¶¶ 30–32, 34–36, 38–40, 46–48, Fig. 3. We agree with Petitioner that it would have been obvious to update Chandra's metadata tag for a multi-CE path to indicate actions taken, as Buruganahalli teaches, to reduce latency and resource waste. Pet. 53–54 (citing Ex. 1002 ¶¶ 122, 125 (citing Ex. 1004 ¶ 28)). Dr. Franz testifies it would have been obvious to arrange Chandra's different network security appliance CEs in series so that traffic passed through multiple CEs that performed different security functions in a CSF before reaching a receiving PE, as Chandra and Buruganahalli teach or suggest. Ex. 1019 ¶ 60 (citing Ex. 1004 ¶¶ 28, 30; Ex. 1002 ¶¶ 122, 125). Patent Owner's argument that the CEs are not in series does not address Petitioner's contention that it would have been obvious to place them in series, as Buruganahalli discloses, to perform different security operations on network traffic. Pet. 54; Ex. 1019 ¶ 60; *Cf.* Sur-reply 20–21.

Petitioner contends that Chandra's system also transmits data packets with updated labels to devices in an extended virtual private network (VPN) shown in Figure 8. Pet. 54. Petitioner asserts it was well known to connect a private network of a remote company site to another network such as an enterprise network using a VPN tunnel, and it would have been obvious to attach the VPN in Figure 8 to a private network as an extension of Figure 2's private network. Pet. 54–56. Petitioner contends that, in such instances, a receiving CE would transmit data packets with the updated label to a receiving device in an extended network using the transmitting and receiving end configurations shown in Figures 2 and 8 of Chandra. *Id.* at 54.

We agree with Petitioner that a skilled artisan would have been motivated to connect Chandra's Figure 2 private network to Chandra's Figure 8 VPN network to extend enterprise network communications so the next device in the extended VPN network would be "a next network appliance participating in the CSF" as claimed. Pet. 54–56; Reply 26–27 (citing Ex. 1019 ¶ 61). We also agree with Dr. Franz who testifies:

Contrary to the PO's assertion that "Petitioner...provides no rationale for why a POSITA would modify Chandra by combining Figures 2 and 8, or explain why a POSITA would reasonably expect it to succeed (POR, 45)," I provided ample reasons why a POSITA would have found it obvious that the VPN in Chandra's Figure 8 could be attached as an extension to the private network in Chandra's Figure 2 as illustrated below. In fact, I provided an example of a widely circulated official publication by the U.S. National Security Agency containing a reference architecture that recommended cascading multiple VPN solutions for added security. (Franz. Decl. ¶¶126-130.)

Ex. 1019 ¶ 62 (citing Ex. 1002 ¶¶ 126–130).

(4) *Conclusion*

Based on the parties' contentions and evidence, we agree with and adopt Petitioner's analysis, and we determine the combination of Chandra and Buruganahalli discloses or suggests elements 6[a]/17[a]/23[a]/28[a].

- c. 6[b]/17[b]/23[b]/28[b]: "*and transmitting, by the first network security network appliance, the network traffic with the updated flag to a next network appliance participating in the CSF.*"

(1) *Petitioner's contentions*

Petitioner contends that Buruganahalli discloses network device 52 transmitting network traffic to a network device 50, which is a next network appliance participating in the CSF. Pet. 53–54 (citing Ex. 1005 ¶¶ 27, 44, 46, 48).

Petitioner asserts it would have been obvious to use Buruganahalli's tag updating in Chandra to update a label by a receiving CE and transmit it to the next network appliance in the CSF because Chandra discloses multiple CEs associated with a single PE, and a multi-CE data path would benefit from label updates indicating actions taken by a previous CE. Pet. 53–54 (citing Ex. 1004 ¶ 28). Petitioner also asserts it would have been obvious to combine Chandra's Figure 2 network with its Figure 8 VPN. *Id.* at 54–56 (citing Ex. 1004 ¶¶ 24, 56, 58, Figs. 2, 8; Ex. 1002 ¶¶ 127–130).

(2) *Patent Owner's arguments*

Patent Owner argues that Petitioner provides no rationale to combine the embodiments in Figures 2 and 8 of Chandra or demonstrate a reasonable expectation of success. PO Resp. 45. Patent Owner argues that CEs have to authenticate and exchange labels before data is sent so adding extra CEs would require an exponential increase in the exchange of data. *Id.* at 45–46.

(3) *Analysis*

As discussed above, Petitioner provided reasons to modify Chandra to combine Figure 2 and 8 networks. Pet. 54–56; Reply 26–27 (citing Ex. 1019 ¶ 61). We agree with Dr. Franz's testimony that a skilled artisan would have cascaded VPNs to enhance security with a reasonable expectation of success (Ex. 1019 ¶ 62). CEs apply a common label set locally. Ex. 1004 ¶¶ 27–35.

(4) *Conclusion*

Based on the parties' contentions and evidence, we agree with and adopt Petitioner's analysis that Chandra and Buruganahalli disclose or suggest elements 6[b]/17[b]/23[b]/28[b], and we determine that Petitioner has demonstrated by a preponderance of evidence that Chandra and Buruganahalli disclose or suggests elements 6[b]/17[b]/23[b]/28[b].

d. Conclusion

We determine that Petitioner has established by a preponderance of evidence that claims 6, 17, 23, and 28 are unpatentable over the combination of Chandra and Buruganahalli.

3. *Claims 7, 18, 24, and 29: “further comprising: removing, by the first network security appliance, the flag from the network traffic; and transmitting, by the first network security network appliance, the network traffic without the flag to a next network appliance.”*

a. Petitioner’s contentions

Petitioner contends that Buruganahalli discloses a network device that removes a metadata tag carried by network data before sending data to the next device. Pet. 57 (citing Ex. 1005 ¶¶ 29, 47; Ex. 1002 ¶ 134). Petitioner asserts that a skilled artisan would have been motivated to combine this teaching with Chandra to keep the network’s labeling mechanism private, prevent malicious devices from intercepting the data packet and exploiting the labeling mechanism as Buruganahalli teaches, and prevent compatibility issues with proprietary tags. *Id.* at 57–58 (citing Ex. 1002 ¶ 134).

b. Patent Owner’s arguments

Patent Owner does not contest Petitioner’s assertions that claims 7, 18, 24, and 29 are unpatentable over Chandra and Buruganahalli. *See generally* PO Resp.; Sur-reply.

c. Conclusion

Based on the parties’ contentions and evidence, we agree with and adopt Petitioner’s undisputed analysis that Chandra and Buruganahalli disclose or suggest claims 7, 18, 24, and 29, and we determine Petitioner has established by a preponderance of evidence that claims 7, 18, 24, and 29 are unpatentable over the combination of Chandra and Buruganahalli.

F. Ground 3: Obviousness over Chandra and Kumar

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

1. Kumar

Kumar discloses sending node 20 and receiving node 60 establishing an authentication session in which sending node 20 uses a client ID and session key from receiving node 60 to create a digital signature and security tag to insert into an outgoing packet, and 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, Abstr. An authentic security tag indicates the packet was transmitted from an approved sending node 20. *Id.* ¶ 55.

2. Motivation to combine

a. Petitioner’s contentions

Petitioner contends that a skilled artisan would have been motivated to add Kumar’s 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 into Chandra so “downstream” devices can decode the data stream. Pet. 59 (citing Ex. 1002 ¶ 137). Petitioner also asserts that a skilled artisan would have used Kumar’s traditional technique of inserting such additional information into packet headers because this technique has the advantage that no payloads need to be altered. *Id.* In addition, Petitioner asserts 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. *Id.*

b. Patent Owner's arguments

Patent Owner does not contest Petitioner's assertions that a skilled artisan would have been motivated to combine the teachings of Chandra and Kumar as asserted by Petitioner. *See generally* PO Resp.; Sur-reply.

c. Conclusion

Based on the parties' contentions and record evidence, we determine that Petitioner has established by a preponderance of evidence that a skilled artisan would have combined teachings of Chandra and Kumar as asserted.

3. Claims 10 and 11

a. Petitioner's contentions

Petitioner asserts that Kumar's transmitting device can use a client ID, session key, and public key to create a digital signature and security tag to insert into a packet. Petitioner asserts that a skilled artisan would have used digital signatures in Chandra to authenticate a source as trusted and data as untampered (claim 10) and insert a security flag in an IP header (claim 11) to avoid modifying payloads. Pet. 60–62 (citing Ex. 1006 ¶¶ 36, 38, 45, 46–50, 53; Ex. 1004 ¶¶ 30, 32, 33, Abstr.; Ex. 1002 ¶¶ 140, 141, 143–145).

b. Patent Owner's arguments

Patent Owner does not contest the assertions that claims 10 and 11 are unpatentable over Chandra and Kumar. *See* PO Resp. 47; Sur-reply.

c. Conclusion

Based on the parties' contentions and evidence, we agree with and adopt Petitioner's undisputed analysis that Chandra and Kuman disclose or suggest claims 10 and 11, and we determine that Petitioner has established by a preponderance of evidence that claims 10 and 11 are unpatentable over the combination of Chandra and Kumar.

G. Ground 4: Obviousness over Chandra and Chandra-2

Petitioner asserts the unpatentability of claims 13, 14, 19, 20, 25, 26, 30, and 31 under 35 U.S.C. § 103 over the combination of Chandra and Chandra-2. Pet. 62–64.

1. Chandra-2

Chandra-2 manages online behavior to ensure that communications between a client and server comply with privacy regulations. Ex. 1007 ¶ 15.

2. Motivation to combine

a. Petitioner’s contentions

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

b. Patent Owner’s arguments

Patent Owner does not contest Petitioner’s assertions that a skilled artisan would have been motivated to combine the teachings of Chandra and Chandra-2 as asserted by Petitioner. *See generally* PO Resp.; Sur-reply.

c. Conclusion

Based on the parties’ contentions and record evidence, we determine that Petitioner has established that a skilled artisan would have been motivated to combine the teachings of Chandra and Chandra-2 as asserted.

3. Claims 13, 14, 19, 20, 25, 26, 30, and 31

a. Petitioner’s contentions

Petitioner asserts that Chandra-2’s network security device provides “logging” that a skilled artisan would have known is a widely used security operation especially important for forensic analysis after a vulnerability or a breach is discovered. Pet. 63 (citing Ex. 1007 ¶ 23).

Petitioner asserts that a skilled artisan would have found it obvious that “logging” by a network security device such as Chandra’s CE would include “network traffic logging” as recited in claims 13, 19, 25, and 30 to expand its range of security 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 predictably with Chandra’s security devices to provide a broader range of security operations. Ex. 1002 ¶¶ 146–149.

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 as recited in claims 14, 20, 26, and 31, and a skilled artisan would have found it obvious to perform these well-known operations at Chandra’s CE to expand its security 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.

b. Patent Owner’s arguments

Patent Owner does not contest Petitioner’s assertions regarding claims 13, 14, 19, 20, 25, 26, 30, and 31. *See* PO Resp. 47; Sur-reply.

c. Conclusion

Based on the parties’ contentions and evidence, we agree with and adopt Petitioner’s undisputed analysis that Chandra and Chandra-2 disclose or suggest claims 13, 14, 19, 20, 25, 26, 30, and 31, and we determine that Petitioner has established by a preponderance of evidence that claims 13, 14, 19, 20, 25, 26, 30, and 31 are unpatentable over of Chandra and Chandra-2.

H. Ground 5: 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. 64–90.

1. Keohane

Keohane describes a network 102 topology that includes a multi-level security system as shown in Figure 3, which is reproduced below.

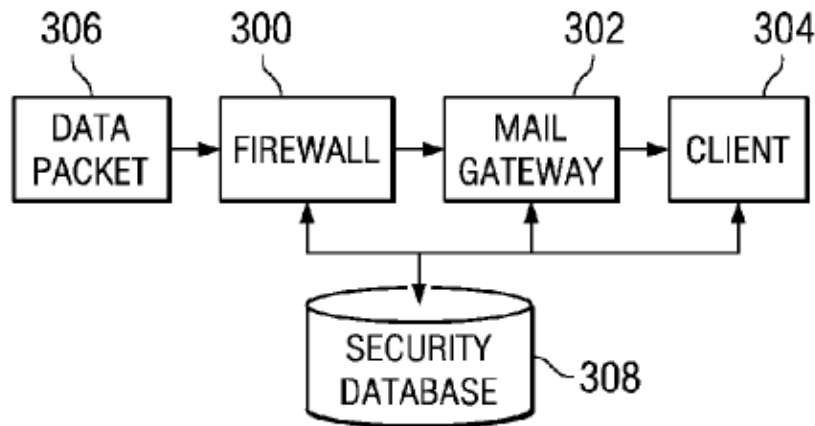


FIG. 3

Figure 3 depicts firewall 300, mail gateway 302, and client 304 that perform multiple levels of cooperative network security on data packets. Ex. 1008 ¶ 33. Firewall 300 determines whether a data packet 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 that the data packet is from a trusted source and no viruses were found. Client 304 may scan data packets for spyware but will not perform other security actions that mail gateway 302 has performed on packets to avoid redundancy. *Id.* ¶ 37.

2. *Claim 1*

a. *1[pre]*

(1) *Petitioner's contentions*

Petitioner asserts that Keohane discloses a method for screening data packets. Pet. 69 (citing Ex. 1008, Abstr.).

(2) *Patent Owner's arguments*

Patent Owner does not contest Petitioner's assertions that Keohane discloses element 1[pre]. *See generally* PO Resp.; Sur-reply.

(3) *Conclusion*

Based on the parties' contentions and evidence, we agree with and adopt Petitioner's assertions that Keohane discloses element 1[pre], and we determine Petitioner has established by a preponderance of evidence that Keohane discloses element 1[pre] to the extent the preamble is limiting.

b. *1[a]*

(1) *Petitioner's contentions*

Petitioner contends that Keohane's mail gateway 302 is a 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 in a CSF. Pet. 69–71 (citing Ex. 1008 ¶¶ 22–24, 32, 36, Figs. 1, 3; Ex. 1009; Ex. 1002 ¶¶ 160, 161). Petitioner contends that Keohane's gateway and other participating appliances insert a signature into a data packet to indicate that the data packet is from a trusted source and to identify the security actions taken based on a code included in the signature so redundant actions can be avoided and data processing time can be saved. *Id.* at 71–74 (citing Ex. 1008 ¶¶ 11, 35, 37, 38, 53, Fig. 7; Ex. 1001, 5:45–47; Ex. 1002 ¶¶ 163, 164, 167).

(2) *Patent Owner's arguments*

Patent Owner argues that Keohane does not disclose a cooperative security fabric whose plain meaning is “a topology of network security appliances that cooperate to inspect incoming and outgoing traffic along multiple interconnected paths.” PO Resp. 47–48. Patent Owner asserts that Keohane discloses a single path that only processes in one direction. *Id.* at 48–49. Patent Owner argues that “[c]ooperation among network security appliances to inspect traffic along a single path in a single direction is not a ‘cooperative security fabric’ under its plain meaning [because] Keohane only describes a single, unidirectional path.” *Id.* at 50.

(3) *Analysis*

As discussed in Section II.B.1. *supra*, we interpret a “cooperative security fabric” as “a network topology of devices that coordinate their efforts to inspect network traffic.” Patent Owner does not dispute that Keohane discloses devices that coordinate their security operations. Claim 1 does not require bidirectional travel of data packets or multiple threads. Keohane discloses a multiple level security system in which firewall 300, mail gateway 302, and client 304 each perform different levels of network security and security actions. Ex. 1008 ¶¶ 33–40. Firewall 300 determines whether a data pack originates from a trusted source and adds a signature to data packets to indicate source verification was done. *Id.* ¶¶ 32–34. Mail gateway 302 performs a virus scan, and adds a signature to data packet 306 to indicate a virus scan was performed. *Id.* ¶¶ 34–36. Client 304 performs additional security actions by scanning for spyware. *Id.* ¶ 37. This distributed, cooperative security fabric performs security operations that Patent Owner ascribes to a CSF. *See* PO Resp. 10–12, 24–25.

(4) *Conclusion*

Based on the parties' contentions and evidence, we agree with and adopt Petitioner's analysis that Keohane discloses or suggests element 1[a], and we determine Petitioner has shown by a preponderance of evidence that Keohane discloses or suggests element 1[a].

c. 1[b], 1[c], 1[d][i], 1[d][ii], 1[e]

(1) *Petitioner's contentions*

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 by a network security appliance in the CSF. Keohane's gateway 302 also looks for a flag (e.g., a code "01" or "02") to indicate the actions taken by a transmitting entity as recited in element 1[b]. 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).

Petitioner asserts that Keohane's mail gateway 302 uses a signature in data packet 306 received from firewall 300 to determine if firewall 300 of the CSF performed a security action before it transmitted data packet 306 to mail gateway 302 as recited in element 1[c], mail gateway 302 identifies the security action performed and determines a security action not performed (e.g., a virus scan) as recited in element 1[d][i], and mail gateway 302 determines a security action to be performed based on signatures in the data packet as recited in element 1[d][ii]. Pet. 76–79 (citing Ex. 1008 ¶¶ 12, 32–38, 40, 54, 55, 58, Figs. 3, 7; Ex. 1002 ¶¶ 171, 173, 174). Petitioner asserts that Keohane's security elements execute local operations on network traffic based on security actions performed by other devices in the CSF as recited in element 1[e]. *Id.* at 79 (citing Ex. 1008 ¶¶ 11, 36, 37; Ex. 1002 ¶ 180).

(2) *Patent Owner's arguments*

Patent Owner does not contest that Keohane discloses elements 1[b], 1[c], 1[d][i], 1[d][ii], and 1[e]. *See generally* PO Resp.; Sur-reply.

(3) *Conclusion*

Based on the parties' contentions and evidence, we agree with and adopt Petitioner's analysis that Keohane discloses or suggests elements 1[b], 1[c], 1[d][i], 1[d][ii], and 1[e], and we determine Petitioner has shown by a preponderance of evidence Keohane discloses or suggests these elements.

d. *Conclusion*

We determine that Petitioner has established by a preponderance of evidence that claim 1 is unpatentable over Keohane.

3. *Independent Claims 15, 21, and 27*

a. *Petitioner's contentions*

Petitioner asserts that Keohane discloses elements of claim 15 based on its contentions for elements 1[pre]–1[d][i], 1[e], and 2[b]. Pet. 88–89. Petitioner contends that Keohane discloses elements of claim 21 based on its contentions for elements 1[pre]–1[d][i], 1[e], and 3[b]. *Id.* at 89. Petitioner asserts that Keohane discloses elements of claim 27 based on its contentions for elements 1[pre]–1[b], 1[d], 1[d][i], 1[e], and claim 5. *Id.* at 89–90.

b. *Patent Owner's arguments*

Patent Owner does not contest these assertions that claims 15, 21, and 27 are unpatentable over Keohane. *See generally* PO Resp.; Sur-reply.

c. *Conclusion*

We agree with and adopt Petitioner's contentions and determine that Petitioner has established by a preponderance of evidence that claims 15, 21, and 27 are unpatentable over Keohane.

4. *Dependent claims 2, 3, 5, 10, 11, 16, and 22*

a. *Petitioner's contentions*

Petitioner provides detailed contentions that claims 2, 3, 5, 10, 11, 16, and 22 are unpatentable over Keohane. Pet. 79–89 (citing Ex. 1008 ¶¶ 12, 32, 34–38, 40, 53, 54; Ex. 1002 ¶¶ 185–187, 191, 192, 197, 200 and previous contentions for element 1[d][i], element 2[a], and claim 5).

b. *Patent Owner's arguments*

Patent Owner does not contest that claims 2, 3, 5, 10, 11, 16, and 22 are unpatentable over Keohane. *See generally* PO Resp.; Sur-reply.

c. *Conclusion*

We agree with and adopt Petitioner's undisputed analysis that Keohane discloses or suggests claims 2, 3, 5, 10, 11, 16, and 22, and we determine Petitioner has established by a preponderance of evidence that claims 2, 3, 5, 10, 11, 16, and 22 are unpatentable over Keohane.

5. *Claim 4*

a. *Petitioner's contentions*

Petitioner asserts that Keohane's network security appliance performs local network security operations on network traffic when it determines the traffic was not transmitted by a second network security appliance as recited in claim 4, e.g., because it lacks a signature header. Pet. 83 (citing Ex. 1008 ¶¶ 53, 56, Fig. 7 (steps 706, 722); Ex. 1002 ¶ 196). Petitioner asserts that a skilled artisan would have found it obvious that a packet without a signature was not transmitted by an upstream second network security appliance participating in the CSF because each device that participated in the CSF added a signature to a packet so a packet without a signature could not have come from upstream in the CSF. *Id.* at 85 (citing Ex. 1008 ¶ 32).

b. Patent Owner's arguments

Patent Owner argues that Keohane's network security appliances do not determine that traffic is from another network security appliance as recited in claim 4. PO Resp. 50–51. Patent Owner argues that Keohane's mail gateway 302 always receives data from a firewall and never determines that traffic did not come from another network security appliance. *Id.* at 51–52. Patent Owner argues that client 304 only receives traffic from the mail gateway and never determines that traffic did not come from another network security appliance as claimed. *Id.* at 52.

c. Analysis

Patent Owner's arguments are contradicted by Keohane's teachings that mail gateway 302 receives packets from a variety of network elements. Keohane discloses that “mail gateway 302 examines data packet 306 to determine whether a signature from a trusted security element is present in data packet 306 [and] a trusted security element is a network element, such as a firewall, mail gateway, router, or some other security intermediary that performs a security action on a data packet.” Ex. 1008 ¶ 35. Because mail gateway 302 may receive data packets from many network security devices, it checks packets to determine if a signature header is present to indicate the other device is participating in the CSF and actions it performed. *Id.* ¶¶ 53–56, Fig. 7. If a signature header is not present, it determines that the packet was not sent by firewall 300, and another security action is performed. *Id.*

d. Conclusion

We agree with and adopt Petitioner's contentions that Keohane discloses or suggests claim 4, and we determine Petitioner has established by a preponderance of evidence that claim 4 is unpatentable over Keohane.

6. *Claim 12*

a. *Petitioner's contentions*

Petitioner contends that Keohane did not disclose expressly that the packets carrying the flag were the first packet of a session, but a skilled artisan would have found this limitation obvious because TCP/IP sessions with only one route between endpoints would only need a flag in the first packet. Pet. 87–88 (citing Ex. 1002 ¶¶ 203, 204).

b. *Patent Owner's arguments*

Patent Owner relies on its arguments that Chandra does not disclose this feature. PO Resp. 53 (citing contentions in PO Resp. Section VI.C. for claim 12's unpatentability over Chandra).

c. *Analysis*

As discussed in Section II.D.6. *supra*, we agree with Petitioner that a receiving security appliance must receive a flag before it performs security operations on session packets so it would have been obvious to transmit a flag in a first session packet before any data packets are sent. Reply 24. A skilled artisan would have understood that the sooner a receiving CE obtains a flag listing security operations that were performed, the sooner it can process the data packets for network security actions that avoid redundant operations. A skilled artisan would have been motivated to send a flag in the first packet. *DyStar*, 464 F.3d at 1368 (an implicit motivation exists when an “improvement” makes a process faster or more efficient); Ex. 1019 ¶ 56.

d. *Conclusion*

We agree with and adopt Petitioner's analysis that Keohane discloses or suggests claim 12, and we determine Petitioner has established by a preponderance of evidence that claim 12 is unpatentable over Keohane.

I. Ground 6: Obviousness over Keohane and Buruganahalli

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

1. Claims 6, 17, 23, and 28

a. Petitioner's contentions

Petitioner contends that Buruganahalli discloses a network security appliance that updates a metadata tag (flag) to indicate operations that were performed by the network device and transmits the network traffic with the updated flag to the next network security appliance participating in the CSF as recited in claims 6, 17, 23, and 28. Pet. 91–93. Petitioner contends that network device 52 received data 58 from network device 54 and performed actions on metadata tag 64 contained in data 58 by adding or updating fields 76 to metadata tag 64 to indicate analysis performed on the network data by the receiving device. *Id.* (citing Ex. 1005 ¶¶ 32, 38, 40, Fig. 3). Petitioner contends that network device 52 sent network data 50 to network device 50 with metadata tag 64 so that they could coordinate their security actions to reduce redundancies. *Id.* at 93–94 (citing Ex. 1005 ¶¶ 27, 44, 46, 48).

Petitioner asserts that it would have been obvious to add this feature to the metadata tag of Keohane so each network device did not have to add its own signature to a data packet to indicate actions that it performed thereby reducing the time needed to read the metadata by the next security device and reducing the size requirement to store all of the signatures that would be needed by Keohane's network security devices to coordinate their security actions along a path. Pet. 93–94 (citing Ex. 1002 ¶¶ 222, 223, 226).

b. Patent Owner's arguments

Patent Owner argues that the “next network appliance” in Keohane is client 304, which is not a network security appliance participating in a CSF because it is an endpoint device. PO Resp. 54–55. Patent Owner argues that the rationale is flawed because “Buruganahalli does not teach how to modify digital signatures and making Keohane’s digital signatures modifiable would defeat their purpose” to authenticate a sender and prevent tampering. *Id.* at 57. Patent Owner argues that the signature cannot be modified. *Id.* at 58.

c. Analysis

Patent Owner’s argument that Keohane’s client 304 is not a network security appliance is contradicted by Keohane’s disclosure that client 304, firewall 300, and mail gateway 302 form different levels of network security in the network. Ex. 1008 ¶ 33. When client 304 receives a data packet from mail gateway 302, client 304 examines the data packet to identify signatures indicating the data packet is from a trusted security element, and client 304 “performs an additional security action based on the security actions already performed [and] scans data packet 306 for spyware.” *Id.* ¶ 37.

We determine that a skilled artisan would have been motivated to update the digital signature (flag) in Keohane based on Buruganahalli’s teachings because the signature before updating would indicate that the previous network security appliance was a trusted source that performed the specified actions, and the updated signature would authenticate the next network security appliance and identify security actions that it performed. Reply 30–31 (citing Ex. 1008 ¶ 38). We also agree that it would have been obvious for security devices participating in the same CSF to share the same key that they use to create digital signatures. *See DyStar*, 464 F.3d at 1368.

d. Conclusion

We agree with and adopt Petitioner’s analysis that Buruganahalli discloses or suggests claims 6, 17, 23, and 28, and we determine Petitioner has established by a preponderance of evidence that claims 6, 17, 23, and 28 are unpatentable over the combination of Keohane and Buruganahalli.

2. Claims 7, 18, 24, and 29

a. Petitioner’s contentions

Petitioner contends that Buruganahalli discloses that the last network device to receive the network data prior to sending the data outside the group of network device may remove the metadata tag before transmitting the data to an “undesired network device.” Pet. 94 (citing Ex. 1005 ¶¶ 29, 47). Petitioner contends that it would have been obvious to perform this step in Keohane to maintain the privacy of the network’s labeling scheme and prevent malicious devices from intercepting a data packet and exploiting the labeling mechanism and prevent compatibility issues with proprietary tags. *Id.* at 95 (citing Ex. 1005 ¶¶ 29, 47; Ex. 1008 ¶¶ 46–48; Ex. 1002 ¶ 231).

b. Patent Owner’s arguments

Patent Owner argues that Petitioner does not explain how a malicious device could exploit labeling that uses digital signatures to perform essential functions that a skilled artisan would not want to remove, and Keohane does not describe incompatibility issues for proprietary tags. PO Resp. 59–61.

c. Analysis

Buruganahalli states, “the last network device to receive the network data prior to sending the data outside of the group of network devices may remove the metadata tag.” Ex. 1005 ¶ 29. Tag module 72 may remove a metadata tag 64 if the next device is not a CSF destination/node. *Id.* ¶ 47.

Petitioner reasonably asserts that this technique would have improved Keohane by preventing a device outside of the CSF from receiving a data packet with a signature and discovering a labeling scheme to circumvent it. Pet. 95; *see KSR*, 550 U.S. at 417 (using a known technique that improved one device to improve similar devices in the same way is obvious unless its application is beyond the level of ordinary skill in the art). A next security device outside the CSF would not need to know what security actions were performed by security devices in the CSF. We agree with Petitioner that there is no reason to forward a digital signature with security details to a device outside the CSF that may be hostile to the CSF. Pet. 95.

Dr. Franz testifies it would have been obvious to do so to prevent the data packet and signature from being received by undesired network devices as Buruganahalli discloses. Ex. 1002 ¶ 230 (citing Ex. 1005 ¶¶ 29, 47); *see DyStar*, 464 F.3d at 1368 (implicit motivation exists when an improvement makes a process more efficient or strong (i.e., more secure)). Dr. Franz also testifies persuasively that tags based on proprietary technology would be removed to prevent compatibility issues in subsequent devices that lacked those capabilities. Ex. 1002 ¶ 231.

d. Conclusion

We agree with and adopt Petitioner's analysis that Buruganahalli discloses or suggests claims 7, 18, 24, and 29, and we determine Petitioner has established by a preponderance of evidence that claims 7, 18, 24, and 29 are unpatentable over the combination of Keohane and Buruganahalli.

J. Ground 7: Obviousness over Keohane and Kumar

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

1. Motivation to combine

a. Petitioner's contentions

Petitioner asserts that a skilled artisan would have used Kumar's digital signature to create a security tag to insert into a packet with Keohane to authenticate data packets sent by a trusted security element and improve source authentication. Pet. 96–97 (citing Ex. 1002 ¶¶ 233, 236, 237).

b. Patent Owner's arguments

Patent Owner does not contest Petitioner's reasons for combining the teachings of Keohane and Kumar. *See generally* PO Resp.; Sur-reply.

c. Conclusion

We determine that Petitioner has established by a preponderance of evidence it would have been obvious to combine the teachings of Keohane and Kumar in the manner asserted by Petitioner with predictable results.

2. Claim 10

a. Petitioner's contentions

Petitioner contends that Kumar discloses the use of a digital signature to authenticate devices as recited in claim 10. Pet. 96–97 (citing Ex. 1006 ¶¶ 36, 45, 46, 49, 50; Ex. 1008 ¶ 54; Ex. 1002 ¶¶ 236, 237).

b. Patent Owner's arguments

Patent Owner does not contest Petitioner's assertions for claim 10 apart from its arguments against Keohane for claim 1. *See* PO Resp. 61.

c. Conclusion

We agree with and adopt Petitioner's analysis that Kumar discloses or suggests claim 10, and we determine that Petitioner has established by a preponderance of evidence that claim 10 is unpatentable over the combination of Keohane and Kumar.

K. Ground 8: 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 the combination of Keohane and Chandra-2. Pet. 4, 97–99.

1. Motivation to combine

a. Petitioner's contentions

Petitioner asserts it would have been obvious to use Chandra-2's well-known security operations as in claims 13, 14, 19, 20, 25, 26, 30, and 31 to expand Keohane's security operations with predictable results. Pet. 97–98.

b. Patent Owner's arguments

Patent Owner does not contest Petitioner's assertions that it would have been obvious to combine the teachings of Keohane and Chandra-2 in the manner asserted by Petitioner. See PO Resp. 61.

c. Conclusion

We determine that Petitioner has established by a preponderance of evidence it would have been obvious to combine the teachings of Keohane and Chandra-2 in the manner asserted by Petitioner with predictable results.

2. Claims 13, 14, 19, 20, 25, 26, 30, and 31

a. Petitioner's contentions

Petitioner asserts that Chandra-2's network security device provides logging as recited in claims 13, 19, 15, and 30 and the security operations recited in claims 14, 20, 26, and 31. Pet. 98–99 (citing Ex. 1007 ¶¶ 23, 24; Ex. 1001, 9:23–26; Ex. 1002 ¶¶ 241, 243).

b. Patent Owner's arguments

Patent Owner does not contest Petitioner's assertions apart from relying on its arguments against Keohane for claim 1. See PO Resp. 61.

c. Conclusion

We agree with and adopt Petitioner's assertions that Chandra-2 discloses or suggests claims 13, 14, 19, 20, 25, 26, 30, and 31, and we determine that Petitioner has established by a preponderance of evidence that claims 13, 14, 19, 20, 25, 26, 30, and 31 are unpatentable over the combination of Keohane and Kumar.

III. CONCLUSION

Petitioner has demonstrated by a preponderance of evidence that claims 1–7 and 10–31 of the '825 patent are unpatentable.

Claim(s)	35 U.S.C. §	References	Claims Shown Unpatentable	Claims Not Shown Unpatentable
1–5, 12, 15, 16, 21, 22, 27	103	Chandra	1–5, 12, 15, 16, 21, 22, 27	
10, 11	103	Chandra, Buruganahalli	10, 11	
13, 14, 19, 20, 25, 26, 30, 31	103	Chandra, Chandra-2	13, 14, 19, 20, 25, 26, 30, 31	
1–5, 10–12, 15, 16, 21, 22, 27	103	Keohane	1–5, 10–12, 15, 16, 21, 22, 27	
6, 7, 17, 18, 23, 24, 28, 29	103	Keohane, Buruganahalli	6, 7, 17, 18, 23, 24, 28, 29	
10	103	Keohane, Kumar	10	
13, 14, 19, 20, 25, 26, 30, 31	103	Keohane, Chandra-2	13, 14, 19, 20, 25, 26, 30, 31	
Overall Outcome			1–7, 10–31	

IV. ORDER

In consideration of the foregoing, it is hereby:

ORDERED that claims 1–7 and 10–31 of the '825 patent have been shown to be unpatentable; and

FURTHER ORDERED that because this is a Final Written Decision, parties to this proceeding seeking judicial review of this Decision must comply with the notice and service requirements of 37 C.F.R. § 90.2.⁸

⁸ Should Patent Owner wish to amend the challenged claims in a reissue or reexamination proceeding, we draw Patent Owner's attention to the *Notice Regarding Options for Amendments by Patent Owner Through Reissue or Reexamination During a Pending AIA Trial Proceeding*. See 84 Fed. Reg. 16654 (Apr. 22, 2019). If Patent Owner files a reissue application or request for reexamination of the challenged patent, we remind Patent Owner of its continuing obligation to notify the Board of such related matters in updated mandatory notices. See 37 C.F.R. § 42.8(a)(3), (b)(2).

IPR2023-00459
Patent 10,084,825 B1

PETITIONER:

Thomas Millikan
Babak Tehrani
PERKINS COIE LLP
Millikan-ptab@perkinscoie.com
Tehrani-ptab@perkinscoie.com

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