

: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 SUR-REPLY

TABLE OF CONTENTS

	<u>Page</u>
I. Introduction	1
II. Claim Construction	2
A. CSF is Properly Defined By Fortinet Patents and Documentation.....	2
B. The Intrinsic and Extrinsic Record Supports Fortinet’s Definition of a CSF.....	4
C. Petitioner’s Unsupported Construction Completely Excises a CSF from the Patent	8
III. Neither Chandra or Keohane teach a “CSF” as properly construed	12
A. Chandra does not teach a “CSF”	12
B. Keohane does not teach a “CSF”	13
IV. Chandra and Keohane Do Not Teach Several Dependent Claims	16
A. Chandra Does Not Teach “Local Network Policies” (claims 2, 4, 15)	16
B. Chandra and Keohane Do Not Render Obvious Flags Carried In “a First Packet of a Session” (Claim 12)	18
C. Chandra Does Not Render Obvious a “Next Network Appliance” (claims 6-7, 17-18, 23-24, 28-29).....	19
D. Keohane Does Not Render Obvious a “Next Network Appliance” (claims 6-7, 17-18, 23-24, 28-29).....	22
E. A POSITA Would Not Be Motivated to Update Keohane’s Signatures (Claims 6, 17, 23, 28).....	24
F. A POSITA Would Not Be Motivated to Remove Keohane’s Signatures (Claims 7, 18, 24, 29).....	25

V.	Conclusion.....	26
----	-----------------	----

EXHIBIT LIST

No.	Exhibit
2001	Declaration of John Black Jr., Ph.D.
2002	Curriculum vitae of John Black Jr., Ph.D.
2003	“fabric,” Newton’s Telecom Dictionary, 30th Updated, Expanded, Anniversary Edition (2016)
2004	Supplemental Declaration of John Black, Jr., Ph.D.
2005	Transcript of the Testimony of Michael Franz (December 28, 2023)
2006	Excerpts from NIIT, “Special Edition Using Storage Area Networks,” published by Que, 2002 (full publication available upon request)
2007	“IBM and Cisco: Together for a World Class Data Center,” IBM Redbooks, July 2013
2008	Intentionally Left Blank
2009	Transcript of the Testimony of Wenke Lee (July 26, 2023) in IPR2023-00030
2010	Declaration of Wenke Lee, Ph.D. in support of Petition for <i>Inter Partes</i> Review of U.S. Patent No. 9,197,601 (Exhibit 1002 from IPR2023-00175)
2011	U.S. Patent No. 8,000,329 (“Fendick”)
2012	“Cooperative Security Fabric,” June 8, 2016, archived July 28, 2016 at https://web.archive.org/web/20160728170025/http://cookbook.fortinet.com/cooperative-security-fabric-54
2013	“Installing internal FortiGates and enabling a security fabric,” June 8, 2016, archived August 28, 2016 at https://web.archive.org/web/20160828235831/http://cookbook.fortinet.com/installing-isfw-fortigate-enabling-csf-54/

2014	“Fortinet Security Fabric Named 2016 CRN Network Security Product of the Year,” December 5, 2016, available at https://www.fortinet.com/corporate/about-us/newsroom/press-releases/2016/fortinet-security-fabric-named-2016-crn-network-security-product
2015	“Fortinet Security Fabric Earns 100% Detection Scores Across Several Attack Vectors in NSS Labs’ Latest Breach Detection Group Test,” August 2, 2016, available at https://www.fortinet.com/de/corporate/about-us/newsroom/press-releases/2016/security-fabric-earns-100-percent-breach-detection-scores-nss-labs
2016	Provisional Application No. 62/503,252
2017	Transcript of the Testimony of Michael Franz (June 10, 2024)

I. INTRODUCTION

Patent Owner Fortinet introduced the claimed term “cooperative security fabric” or “CSF” into the industry, and, through Patent Owner’s efforts successfully commercializing its products, “CSF” became an industry term known to ordinary artisans. As a result, the “ordinary and customary meaning” of “CSF” has been defined by Fortinet’s product documentation and patents. And this intrinsic and extrinsic evidence consistently describes a CSF as inspecting incoming and outgoing traffic along multiple interconnected paths.

Petitioner attempts to ignore this indisputable evidence about the term’s customary meaning and to unreasonably broaden the term CSF to cover technologies and network topologies that existed *decades* before the term was ever used, including that it covers a single path between two nodes—a mere *thread* not a *fabric*. As a result, Petitioner’s proposed construction renders the term superfluous and ignores Fortinet’s efforts to standardize this industry term.

Neither Chandra or Keohane disclose a CSF as properly construed. Petitioner does not dispute that Chandra’s inspection of incoming traffic lacks cooperation. And Keohane’s appliances do not operate on outgoing traffic or form a fabric.

Moreover, Chandra and Keohane fail to disclose or render obvious additional limitations of the dependent claims, including that the appliances operate on “local network policies,” that the “first packet in a session” carries the flags, and that the packet can be sent to a “next network appliance.”

II. CLAIM CONSTRUCTION

A. CSF is Properly Defined By Fortinet Patents and Documentation

CSF is a term that Fortinet introduced in 2016. It has since become a customary, industry term by way of its use in connection with Fortinet’s network appliance products. POR 22-25; Ex. 2004, ¶¶66-73. The term CSF does not appear in any academic papers or books, and a search for the term on the Internet results in only patents and documentation about Fortinet products (or discussions thereof). *Id.*, ¶¶67-69; Exs. 2012-2014. Petitioner does not dispute any of this, and its expert Dr. Franz confirmed that he did not attempt to search for the term CSF in any book, paper, library, patent, or on the Internet generally. Ex. 2017, 115:5-116:20.

The term CSF thus has an “ordinary and customary meaning” defined by Fortinet’s product documentation and patents. *Phillips v. AWH Corp.*, 415 F.3d 1303, 1312 (Fed. Cir. 2005). Before Fortinet first introduced the term CSF in 2016 as a term for its products, a POSITA would not have attributed *any* customary meaning to it because the term had never been previously

used.¹ Ex. 2004, ¶¶66-69. Following its introduction, ordinary artisans became familiar with the term through Fortinet’s products and documentation because of Fortinet’s successful commercialization of its products—making it an industry term having an ordinary and customary meaning, *as defined by Fortinet*. Ex. 2004, ¶66. This was the backdrop of the industry when Fortinet filed the provisional application to the ’825 patent on May 8, 2017 in order to patent the very thing it introduced—a CSF. Petitioner does not dispute this.

Petitioner ignores the roots of this term, and instead attempts to define “cooperative security fabric” by dissecting its constituent parts. Reply 4. Yet Petitioner provides no evidence beyond its expert’s say-so to support its position. This is an untenable position in view of the undisputed evidence that CSF was an industry term invented by Fortinet in 2016. Ex. 2004, ¶¶67-69. Dr. Franz’s testimony is also undermined by the fact that he did not attempt

¹ This is a similar principle to a “coined term” which “has no ordinary and customary meaning” (*Iridescent Networks Inc. v. AT&T Mobility, LLC*, 993 F.3d 1345, 1353 (Fed. Cir. 2019))—though to be clear, CSF is not a term that was coined by the ’825 patent but was instead introduced by Fortinet a year earlier and made a customary, industry term through its efforts. Ex. 2004, ¶¶66-73.

to determine the term's customary meaning as used in the industry by actual ordinary artisans. Ex. 2017, 115:5-116:20. Petitioner's argument is also not consistent with the fact that the claims combined the terms into a single phrase and abbreviation: "CSF," indicating that it should *not* be considered by its constituent parts.

B. The Intrinsic and Extrinsic Record Supports Fortinet's Definition of a CSF

The intrinsic and extensive extrinsic record all consistently support Patent Owner's construction of CSF as "a topology of network security appliances that cooperate to inspect incoming and outgoing traffic along multiple interconnected paths." POR 13-34.

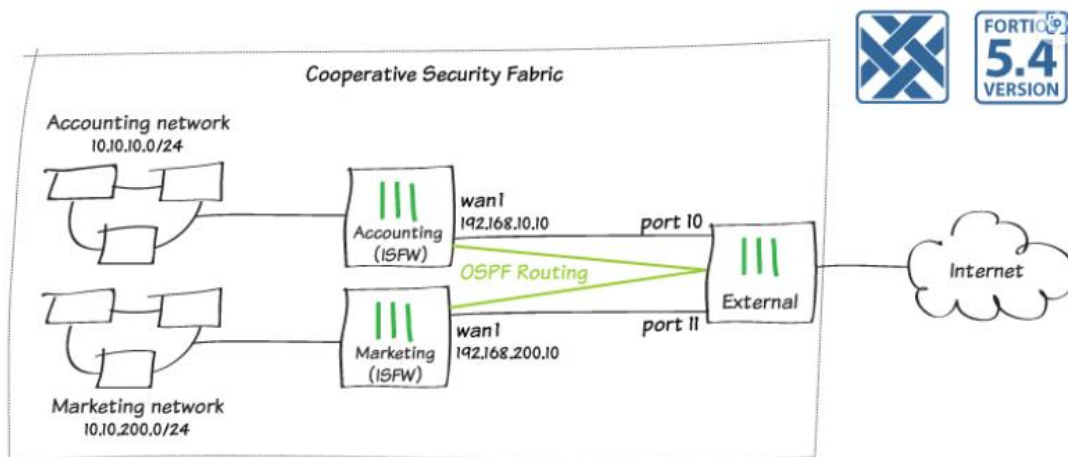
The undisputed evidence establishes that a CSF *must* inspect traffic that goes *through* the CSF, *i.e.*, incoming and outgoing traffic. For example, the '825 patent states that a CSF "coordinate[s] operations performed on network traffic" that is "transmitted **to/from** the network." Ex. 1001, 1:34-36, 1:64-67.² The specification consistently describes the CSF as monitoring "downstream network traffic that is transmitted from the Internet" or "upstream network traffic that is transmitted ... to the Internet." *Id.*, 5:32-38. Petitioner's expert Dr. Franz **agreed** that "the CSF has the ... **objective** of

² All emphases are added unless noted otherwise.

coordinating security operations on the network traffic ***passing through them***”—which describes incoming and outgoing traffic. Ex. 2005, 26:4-7; *see also id.*, 19:10-16 (agreeing with the Board’s description that the ’825 patent “describes methods of performing security operations on network traffic ***passing through*** a cooperative security fabric (CSF)”; Paper 10 at 3. Consistent with this understanding, the ’825 patent does not provide any embodiments where security operations are performed on traffic between subnets of the same network. *See* Ex. 2005, 35:7-17.

In addition, a CSF requires “multiple interconnected paths” and not just a single path through two network appliances. As the ’825 patent explains, in a simple network with a single path, no coordination is necessary because network traffic always goes through the same appliances in the same order. Ex. 2004, ¶51; Ex. 1001, 1:46, 1:54-56. However, as networks became larger with “many network security appliances ... deployed at different locations within the network,” coordination became necessary to “avoid or reduce redundant operations among members of the CSF.” Ex. 1001, 1:33-37, 1:64-67. Thus, Figure 2 of the ’825 patent, which depicts a cooperative security fabric, shows multiple paths that incoming or outgoing network traffic can take through the CSF.

The extrinsic evidence also consistently defines a CSF as handling incoming/outgoing traffic on multiple paths. Ex. 2004, ¶¶64-84; see Exs. 2012, 2013, 2015. For example, Ex. 2012 describes steps for “configur[ing] a Cooperative Security Fabric (CSF)” where the very first step is to install “the *internet-facing, or upstream*, FortiGate in the security fabric,” and the subsequent steps are to install two more FortiGates where “a security fabric is set up between them and the external FortiGate.” Ex. 2012, 1-2. Ex. 2013 provides a depiction of a “Cooperative Security Fabric” that clearly coordinates incoming/outgoing traffic on multiple paths. Ex. 2013, 1.



Finally, the extrinsic evidence for the term “fabric” establishes that a fabric of network security appliances has multiple interconnected paths. Ex. 2004, ¶¶74-83; Ex. 2003, 2006, 2007; Ex. 2005, 7:25-8:8 (acknowledging that the term “fabric” was inspired by clothing fabric). Petitioner provides no

extrinsic evidence to the contrary. The underlying, undisputed fact is that two-node networks have been known and in-use for over 50 years, and yet the term “fabric” was not used until the early 2000’s as enterprise networks became larger and more complex. Ex. 2004, ¶88; Ex. 2017, 97:13-98:4 (“[W]e have more diversity on the networks. We have more devices. We have different networking technologies that coexist.”). The term “fabric” is analogous to “a piece of cloth” which constitutes multiple “threads”—it therefore belies all reasoning to contend that a single “thread” somehow constitutes a “fabric.” Ex. 2003; Ex. 2004, ¶¶75-76; Ex. 2005, 7:25-8:8.

Petitioner asserts Patent Owner’s construction has “hidden limitations” not supported by the evidence. POPR 10. Not true. Patent Owner’s construction requires that cooperative inspection of incoming and outgoing traffic, as established by the intrinsic and extrinsic evidence—whether or not it *also* inspects internal traffic is simply not within the scope of the claims. See POR 19 (“Petitioner is incorrect” that “a CSF need only process purely internal network traffic (such as VPN traffic or subnetwork-to-network traffic).”). Dr. Black’s testimony was about the scope of the term, not about whether a CSF could perform other tasks. Ex. 1018, 70:5-13. Dr. Black’s testimony also did not limit CSF to inspecting Internet-only traffic. *Id.*, 32:1-

9 (“I just want to be clear that when I say ‘incoming’ ... I’m talking about traffic ***external from the network*** arriving to the network.”).

As for the other so-called “hidden limitations”—that a CSF requires three appliances, paths that do not share a starting/ending point, and more than a single thread—these are simply a reflection of the fact that a CSF requires “multiple interconnected paths,” as reflected in Patent Owner’s proposed construction and supported by the intrinsic and extrinsic evidence. POPR 10. A path through two appliances (a single thread) is not a “cooperative security ***fabric.***”

C. Petitioner’s Unsupported Construction Completely Excises a CSF from the Patent

Petitioner argues that the plain meaning of CSF is “devices that form a network topology and work together to coordinate security operations among them,” where such a network topology need only include “two network security appliances” in a single path. Reply 3, 5. As just discussed, Petitioner’s approach to construing the term by its constituent parts is completely at odds with how “CSF” is customarily defined by ordinary artisans. In addition, Petitioner’s construction is not consistent with the claims, the specification, or the extrinsic evidence.

First, looking at the language of the claims, Petitioner’s construction would render the limitation “participating in a cooperative security fabric (CSF)” superfluous and is therefore “highly disfavored.” *Wasica Fin. GmbH v. Cont’l Automotive Systems, Inc.*, 853 F.3d 1272, 1288 n.10 (Fed. Cir. 2017) (“It is highly disfavored to construe terms in a way that renders them void, meaningless, or superfluous.”). The claims already recite two determining steps with two network security appliances, the first of which determines whether the second has already performed network security operations, and, if so, declining to repeat that operation. As admitted by Dr. Franz, these two steps already disclose two “devices that form a network topology and work together to coordinate security operations among them,” thus rendering the limitation that the devices “participat[e] in a cooperative security fabric” a nullity. Ex. 2017, 113:20-114:1 (confirming that cooperation occurs when the first network appliance decides “what network security operations to perform based on the knowledge it gained by the communication from the second security appliance”).

Second, looking at the specification, Dr. Franz admitted that it does not include any examples of inspecting internal network traffic or traffic over a single path. Ex. 2005, 35:7-17. Patent Owner’s construction does not limit “CSF” to exemplary embodiments—for example, the embodiments in the

'825 patent have at least three interconnected paths (*see* Fig. 2), whereas Patent Owner's construction requires only two. By contrast, Petitioner's construction is completely detached from the specification as well as the undisputed evidence that Fortinet defined the customary meaning of the term within the industry as understood by a POSITA.

Petitioner's example of a VPN does not establish that cooperatively processing internal traffic is within the scope of the CSF. Reply 12-13. While Figure 1 depicts a VPN, the '825 patent never states nor suggests that its cooperative security functions is performed on VPN traffic. Reply 19. And Petitioner's contrived example of a network with two nodes (*see* Reply 14-15) is not supported by the '825 patent—the patent instead makes clear that the two-node path is simply **one path** of many within the CSF. Ex. 1001, 18-20 (“Topology 200 may have **paths** with no branch nodes, **such as** the network path in which a leaf node 250 is connected to root node 220 directly.”).

Third, Petitioner argues the provisional application supports its construction (Reply 15-16), which is not true. Although the application states that a single network security device “may **initially** represent a CSF containing only one member,” it makes clear that other NSDs are to “join the CSF to which its parent belongs” which “**stabilizes**” the CSF and gives the first NSD “**full information** regarding CSF 100.” Ex. 2016, ¶26. This

describes the first step of **setting up** a CSF, and the presence of a single node is only temporary—similar to the process described in Fortinet’s documentation. See Ex. 2012. Petitioner also cannot credibly argue that a single node constitutes a CSF. Ex. 2017, 117:12-14 (“[C]ooperation require[s] more than one” device, it “requires at least two to cooperate.”).

In addition, the disclosures in paragraph 41 describe possible tunneling paths within the multi-path CSF (or even between multiple CSFs) described throughout the application, including in the preceding paragraph 40. See, e.g., Ex. 2016, ¶40 (“[A] CSF based on the **hierarchical connections** among the[NSDs] by determining its relative position as a root, intermediate or leaf node.”). Similarly, Petitioner’s reliance on claim 1 ignores that it requires a CSF with “hierarchical interconnections among the plurality of network security devices,” which Dr. Black testified cannot be accomplished by two or three nodes in a single path—testimony that Petitioner does not dispute. *Id.*, cl. 1; POR 21; Ex. 2004, ¶¶61-63.

Fourth, the extrinsic evidence does not support Petitioner’s construction as they argue. Reply 18-19. Petitioner relies on Exhibit 2013’s disclosure of “OSPF” as indicating that the CSF handles internal traffic. *Id.* at 18. But Exhibit 2013 makes clear that OSPF is enabled **before** the CSF is enabled. Ex. 2013, 7-18. Thus, the security appliances in Exhibit 2013 are

able to handle internal traffic, too, but that capability is independent of and does not define the CSF functionality within the Fortigate products.

Petitioner also relies on an unauthenticated exhibit published in **2021**, four years after the patent's effective filing date, that does not even mention a "Cooperative Security Fabric," much less disclose one with only two nodes. Ex. 1017, 117. Moreover, even according to this page, the "Security Fabric" has more than two nodes, with the image relied on by Petitioner depicting just one of three groups of devices ("Security Fabric: Group_3"). *Id.*

III. NEITHER CHANDRA OR KEOHANE TEACH A "CSF" AS PROPERLY CONSTRUED

As explained in the POR, neither Chandra or Keohane teach a CSF when it is given its proper construction of "a topology of network security appliances that cooperate to inspect incoming and outgoing traffic along multiple interconnected paths." POR 35-38; POR 47-50.

A. Chandra does not teach a "CSF"

Petitioner does not dispute that, in Chandra, its inspection of incoming Internet traffic is only performed by a single node. Reply 19-20. Instead, Petitioner now argues that this still meets the proper construction of "CSF" because "two security appliances are still in the same 'CSF' even when only one appliance inspects traffic." POR 20. However, Petitioner fails to explain how inspection by a single node involves "network security appliances that

cooperate to inspect incoming and outgoing traffic.” As Dr. Franz admitted, “cooperation require[s] more than one” device, it “requires at least two to cooperate.” Ex. 2017, 117:12-14. Thus, Chandra’s devices **never** cooperate to inspect **incoming and outgoing traffic**—the cooperation only occurs for internal-only traffic, which is outside the scope of the claims.

Petitioner’s discussion of dependent claim 4 is irrelevant. While this claim specifies that “the first network security appliance” can **also** process traffic “not transmitted from the second network security appliance,” this additional capability does not address the nature of the claimed CSF.

B. Keohane does not teach a “CSF”

Petitioner argues that Keohane discloses “a series of interconnected paths” even though its “three appliances [are] in a line” because both firewall 300 and mail gateway 302 “could receive network traffic and transmit it down a data path.” Reply 20-21. This argument is based on a misreading of Keohane. As Dr. Black explained, in order to have multiple paths even though all appliances are in a single line, as is the case in Keohane, traffic would have to be able to enter **the network** via multiple nodes. Ex. 1018, 23:15-22 (“It could be if traffic can enter, let’s say, the middle one in that line and then go left and out, but it could also enter the middle and then go right. As long as there are separate paths that the traffic can follow, then yes. But if the traffic

can only enter on the left side and go to the second node and the third node and exit and that's it, then I wouldn't say that's a fabric."), 65:21-66:2 (“[A]s long as packets can take multiple paths, *arrive at A, exit B, let's say, or arrive at B and exit C*, then we have a fabric.”).

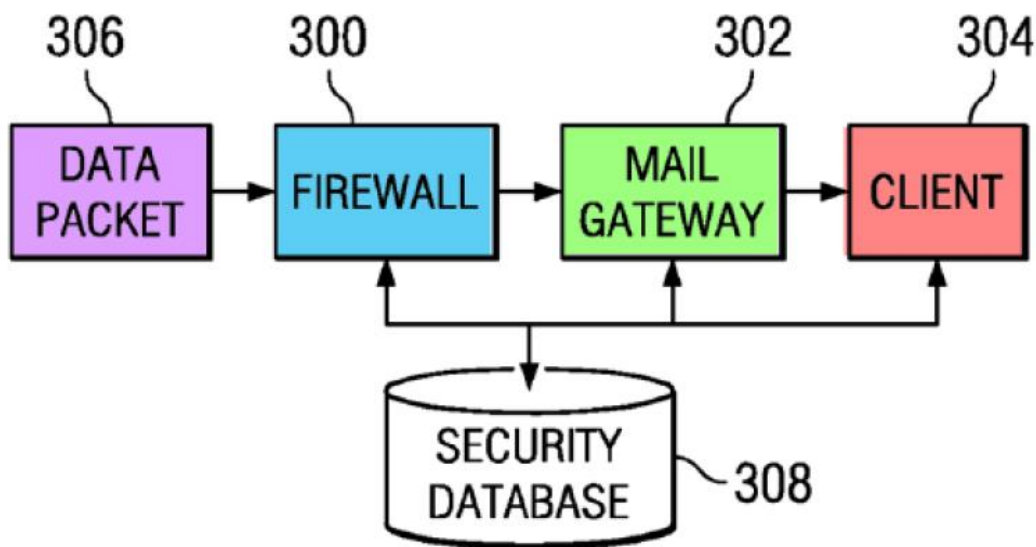


FIG. 3
(Annotated)

While obviously Keohane's mail gateway can receive network traffic, *i.e.*, from firewall 300, Keohane never discloses that mail gateway 302 can receive **incoming** network traffic, *i.e.*, Keohane never discloses that traffic can enter the network via mail gateway 302. In Figure 3 and its corresponding description, the data packet enters the network via firewall 300, and mail gateway 302 only receives traffic from firewall 300. Petitioner points to Keohane's "signature[s]" but those signatures only "indicate[]" that a previous

security action has been performed on the data packet.” Ex. 1008 at Abstract. Thus, lack of a signature indicates that the traffic originated internally or that the firewall 300 did not perform any security actions, not that incoming traffic somehow entered the network via mail gateway 302. Indeed, Dr. Franz confirmed that Keohane does not disclose “what else is happening in this network” besides this unidirectional flow along a single path. Ex. 2005, 59:3-12. Petitioner’s contention that “traffic could enter at either firewall 300 or mail gateway 302” is not supported by Keohane. Reply 21.

In addition, Keohane does not disclose inspecting traffic going out of the network as required by a CSF when properly construed. Petitioner argues that “Keohane disclosed that **both** ‘clients and servers may include software and/or hardware used to perform security actions...[on] **data packets received by them.**’” Reply 22 (quoting Ex. 1008, ¶23). This, however, does not suggest at all that outgoing traffic is inspected. In Keohane’s embodiment in Figure 3, it explains for an incoming data packet traveling in a single direction, “Firewall 300 performs a security action that includes determining whether a data packet originates from a trusted source” and, later, “Client 304 scans data packet 306 for spyware.” Ex. 1008, ¶¶33, 37. In other words, both clients and servers can perform security actions on data packets they received **upstream**, which does not suggest that they inspect outgoing traffic.

Indeed, all of Keohane’s disclosed “security actions” indicate that they are only performed on incoming, not outgoing, traffic—whether it is “an action taken on a data packet in an effort to prevent *the introduction* [into the network] of malware” or “determination of whether the data packet is from a trusted source.” Ex. 1008, ¶33. According to Keohane, there is no need to perform such actions on outgoing traffic that originates from within the network because, “the participants *trust each other*.” Ex. 1019, ¶72.

IV. CHANDRA AND KEOHANE DO NOT TEACH SEVERAL DEPENDENT CLAIMS

A. Chandra Does Not Teach “Local Network Policies” (claims 2, 4, 15)

Patent Owner argued in the POR that Chandra does not teach “local network policies” because all of the CE labels that are exchanged between the CE’s are the same and thus global policies. POR 39-40; Ex. 1004, ¶6 (“policies [are] uniform among all the VPN sites within a VPN”); ¶¶51, 53 (showing that the CE labels and rules are identical).

Petitioner does not dispute that each CE in Chandra receives the same copy of the labels. Instead, Petitioner abandons its argument in the Petition and argues that “the two ends executed security actions ... ‘locally’” and that the “local network policies” are the “*executing algorithms* in conjunction with the local tables storing CE labels and rules.” Pet. 23-24. Petitioner

appears to be arguing that because different CEs may execute different operations despite having the same exact set of policies, they are different local network policies. This is a different argument than the one presented in the Petition, which instead argues that local policies are “stored at and **executed by** the respective CE.” Pet. 38. The Petition argues that local policies are executed, whereas the Reply argues that the local policies are the executing algorithms—the Board should not consider it.

Regardless, it is nonsensical to argue that the executing algorithms are the local policies. Claim 4 of the ’825 patent clearly states that the “local policies” “specif[y]” the “local network security operations” that will be performed. Thus, the policies must specify which operations are performed under which circumstances—which in Chandra are the CE labels and which are **not** local as they are identical across all CEs. POR 39-40.

In addition, the “executing algorithms” are also global, not local, because they are the same algorithms for all CEs. Each CE performs the same algorithm: “refer[] to the receiving CE table, and determine[] that actions corresponding to rules ... have been performed on the data packet” because the data packet was tagged with a certain label. Ex. 1004, ¶53. For example, a data packet with a label 1256 is considered to have executed actions for “Rules A and B” by every CE—because every CE has the same, global

policies. *Id.* Every CE will then perform the same algorithm, look at the same table, and come to the same conclusion: that “actions corresponding to rules A and B have been performed on the data packet.” *Id.* Thus, neither the CE Labels or the executing algorithms are “**local** network policies.”

B. Chandra and Keohane Do Not Render Obvious Flags Carried In “a First Packet of a Session” (Claim 12)

The POR argued that the Petition did not provide a sufficient rationale to modify Chandra or Keohane to have its flags transmitted in the “first packet of a session.” POR 41. The Reply does not cure this deficiency. The Reply instead argues that because the “receiving security appliance needed the flags before it could perform security operations on the packets in the session,” the flags would “naturally be transmitted in the first packet.” Reply 24.

This does not provide any rationale to include the flags in the **first** packet of the session. In Chandra, the “a data packet” can actually be “a group of packets, a message, a file, etc,” thereby indicating that **multiple** packets are transmitted before any security operations need to be performed on those packets. Ex. 1004, ¶24. Moreover, a session could involve multiple packets between the CEs, such as handshakes. As the POR explained, one such handshake involved the exchange of labels between the CEs. POR 41. Petitioner argues that such labels were exchanged “**before** any session

containing data packets to be inspected ***began.***” Reply 24 (emphasis in original). However, Petitioner provides no citations to Chandra or any evidence beyond its expert say-so—there is no notion that the exchange of labels much happen in a different session than the session where data packets are transmitted. Indeed, following exchange of labels, it would make no sense to disconnect and reconnect the session to begin transmitting data packets—it would be more efficient and straightforward to continue to use the same session.

C. Chandra Does Not Render Obvious a “Next Network Appliance” (claims 6-7, 17-18, 23-24, 28-29)

It is undisputed that Chandra does not disclose a “next network appliance” because Chandra only ever discloses cooperation between a transmitting and a receiving CE (and only for internal traffic)—two network appliances at most. The POR provides several different reasons why Chandra does not render obvious a “next network device.” POR 42-47.

As an initial matter, Petitioner has abandoned their argument that a POSITA would be motivated to add a “next network appliance” to Chandra in view of Buruganahalli. Pet. 53-54. The POR pointed out that Buruganahalli’s devices are not part of a fabric or a CSF, and that Petitioner

provided no motivation for this combination. POR 43. Petitioner did not respond to this argument in the Reply.

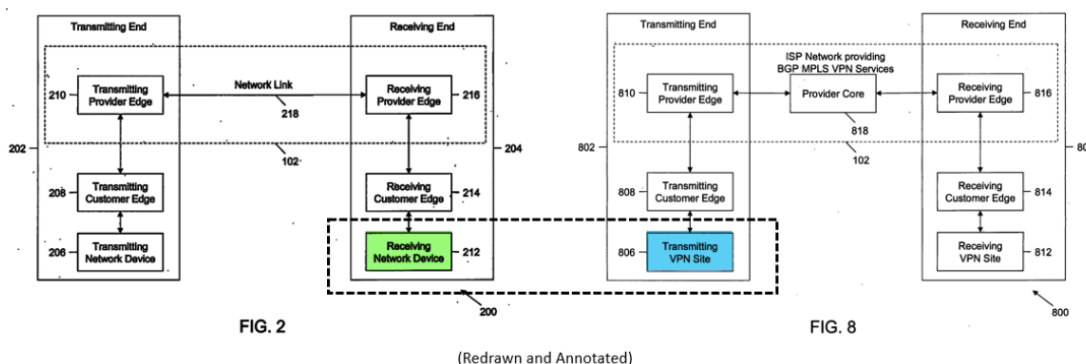
Petitioner has also abandoned their argument that the “receiving network device (212)” is the next network appliance. Pet. 54; see Reply 25-27. As the POR explained, the “receiving network device (212)” is an endpoint device and therefore not a “network appliance.” POR 44; Ex. 2004, ¶108. Petitioner did not respond to this argument in the Reply.

Finally, Petitioner has abandoned their argument that Chandra discloses a “next network appliance” merely because it discloses “a plurality of such CEs [could] be associated with a single PE”—*i.e.* a provider edge which is essentially a network of CEs (which are subnetworks). Pet. 54. After the POR pointed out that Chandra does not disclose that these CEs communicate with each other *in seriatim* (POR 43; Ex. 2004, ¶107), Petitioner did not challenge that explanation.

Rather, Petitioner now raises a brand new obviousness argument, arguing for the first time that “[i]t would be obvious to arrange some of these CEs in series so that traffic passed through multiple receiving CEs before reaching receiving PE.” Reply 25. However, Petitioner does not provide any motivation or rationale for making such an arbitrary change. *Id.* Chandra discloses that transmissions between CEs only involve two nodes: the

transmitting CE and receiving CE. There is no reason to complicate this simple setup and route traffic through other CEs instead of directly to the receiving CE. Doing so would complicate the network topology and increase network latency.

Finally, Petitioner doubles-down on its completely arbitrary, contrived and hindsight-driven combination of Figure 2 and Figure 8 as depicted below. Pet. 56; Reply 26.



But again, Chandra describes that a transmitting CE can directly transmit to a receiving CE, including the Receiving CE 814 in Figure 8—there is no rational reason to go through so many additional devices. Ex. 1004, ¶¶33-34; Ex. 2004, ¶111. Moreover, Petitioner’s combination is nonsensical. In its combination, the “receiving network device (212) could be coupled with transmitting VPN site (806).” Pet. 56. Yet both of these are network endpoints within different networks, *i.e.* network devices such as “personal

computers, servers, mobile phones, etc.” Ex. 1004, ¶¶21, 30. There is no mechanism in Chandra that allows receiving network device 212 to transmit information directly to transmitting VPN site, especially when the network on the right is a VPN network that *must* be routed through “a security device, such as a firewall, to control access.” *Id.*, ¶5. Different networks are understood to be separated by devices like firewalls in order to secure traffic going into or out of the network, and thus it would not make sense to have two network devices directly connected to one another, bypassing the security measures of their respective CEs/firewalls.

D. Keohane Does Not Render Obvious a “Next Network Appliance” (claims 6-7, 17-18, 23-24, 28-29)

Petitioner’s argument that Keohane discloses a “next network appliance” requires that the term “network appliance” include client devices, such as Keohane’s client 304. Reply 27-28. This is essentially a claim construction argument first brought in the Reply and for which Patent Owner cannot bring any testimony from its own expert to rebut.

In any case, Petitioner does not cite to any evidence beyond its expert’s say-so that a “network appliance” includes a “client device.” Indeed, according to Petitioner’s expert, Dr. Franz, network appliances and client devices are *not* the same. Specifically, Dr. Franz explained that a “network

appliance” has “a *small operating system* ... that are *managed*” and performs “a small set of *specific tasks*, mostly without requiring interaction.” Ex. 1017, 101:24-102:9. This description does not comport at all with Keohane’s client device, which is a “personal computer[] or network computer[.]” Ex. 1008, ¶23.

In addition, the ’825 patent, Keohane, and Chandra all distinguish appliances like routers or firewalls from client devices. Ex. 2004, ¶135. The ’825 patent distinguishes “network appliances” which “connect[] endpoint devices” from “endpoint devices” which are “personal computers, servers, laptops, tablet computers, smart phones, printers and etc.” Ex. 1001, 6:1-9. Similarly, Keohane makes a distinction between “routers, gateways, and firewalls” and “clients” like “personal computers or network computers.” Ex. 1008, ¶23. And in Chandra, there is a distinction between “Intrusion Detection Systems (IDSs), firewalls, etc.” that perform network actions on network data, and “network devices,” which are “personal computers, servers, mobile phones, etc.” Ex. 1004, ¶¶21, 30; Ex. 2004, ¶109. Thus, all three references recognize the difference between network appliances and the client devices which are served by the appliances. As a result, Keohane’s “client device” is not a “next network appliance.”

E. A POSITA Would Not Be Motivated to Update Keohane's Signatures (Claims 6, 17, 23, 28)

After the POR pointed out that there was no motivation to alter Keohane's signatures in view of Buruganahalli given that the "purpose of a digital signature is to prevent tampering" (POR 57; Ex. 2004, ¶138), the Reply presents a new obviousness theory that "[i]t would be obvious that the CSF participants could use a common, pre-shared cryptographic key to prevent non-members from tampering with the signature." Reply 30. Patent Owner is prejudiced by this new argument because it cannot provide expert testimony to rebut it.

If given the opportunity, Patent Owner would have provided testimony that sharing cryptographic keys among multiple nodes presents a significant security risk. As Petitioner's expert Dr. Wenke Lee explained in a different case, exchanging keys are subject to "man in the middle" attacks that involve the exchanged key being stolen. IPR2023-00458, Ex. 2004, 80:23-81:21. In addition, Petitioner's complicated and processing-intensive proposal that each node "decrypt, update, and then re-encrypt the signature" (Reply 30) is completely unnecessary when Keohane discloses that each node already adds its own signature after it performs operations. Ex. 1008, ¶36 ("mail gateway 302 adds a signature to data packet 306").

F. A POSITA Would Not Be Motivated to Remove Keohane's Signatures (Claims 7, 18, 24, 29)

Petitioner argues that a POSITA would be motivated to remove Keohane's signatures "where the client ... performed no security actions of its own," such as "when clients were connected to the enterprise's networking infrastructure." Reply 31. Yet Keohane does not disclose any embodiment where a client cannot perform its own security actions—indeed, Keohane states precisely the opposite, that the client device "scans data packet 306 for spyware" because the signatures indicated that the upstream devices "did not include scanning data packet 306 for this type of malware." Ex. 1008, ¶37. But had an upstream device "performed both virus and anti-spyware scans on data packet 306, client 304 would taken [sic] no action." *Id.*

Thus, Keohane makes clear that the signatures in the data packet must be intact when it reaches the client devices in order for the client device to determine what security actions it should itself perform. POR 60; Ex. 2004, ¶46. Petitioner provides no evidence that it would be desirable to remove such functionality from client devices, and doing so would increase security risks especially given that Keohane contemplates situations where not all necessary security actions are performed by upstream devices. Ex. 1008, ¶37.

V. CONCLUSION

For the foregoing reasons, Patent Owner requests that the Board find that Petitioner has not established that the '825 patent's claims 1-7 and 10-31 are unpatentable.

Date: May 22, 2024

By: /s/ James Glass
James M. Glass (Reg. No. 46,729)
QUINN EMANUEL URQUHART &
SULLIVAN LLP
51 Madison Avenue, 22nd Floor
New York, NY 10010
Email: jimglass@quinnemanuel.com
Phone: 212-849-7142
Fax: 212-849-7100

Counsel for Patent Owner
Fortinet, Inc.

CERTIFICATE OF LENGTH (37 C.F.R. §§ 42.24)

The undersigned hereby certifies that, according to the word-processing system used to prepare the foregoing document, this document has 5,198 words and thus complies with the applicable word limit.

Date: May 22, 2024

By: /s/ James Glass

James M. Glass (Reg. No. 46,729)

QUINN EMANUEL URQUHART &
SULLIVAN LLP

51 Madison Avenue, 22nd Floor

New York, NY 10010

Email: jimglass@quinnemanuel.com

Phone: 212-849-7142

Fax: 212-849-7100

Counsel for Patent Owner

Fortinet, Inc.

CERTIFICATE OF SERVICE (37 C.F.R. §§ 42.6(E), 42.105(A))

The undersigned hereby certifies that the foregoing document was served in its entirety on May 22, 2024 upon the following parties via Electronic Mail:

Thomas N. Millikan (millikan-ptab@perkinscoie.com)

Babak Tehrani (tehranchi-ptab@perkinscoie.com)

Andrew N. Klein (klein-ptab@perkinscoie.com)

Bingjie (Kay) Li

Netskope-FortinetIPRTeam@perkinscoie.com

Date: May 22, 2024

By: /s/ James Glass

James M. Glass (Reg. No. 46,729)

QUINN EMANUEL URQUHART &
SULLIVAN LLP

51 Madison Avenue, 22nd Floor

New York, NY 10010

Email: jimglass@quinnemanuel.com

Phone: 212-849-7142

Fax: 212-849-7100

*Counsel for Patent Owner
Fortinet, Inc.*