

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 RESPONSE

TABLE OF CONTENTS

	<u>Page</u>
I. Introduction	1
II. Level of Ordinary Skill in the Art	3
III. Overview of the '825 patent.....	3
IV. OVERVIEW OF CERTAIN CITED ART	6
A. Chandra (Ex. 1004).....	6
B. Keohane (Ex. 1008)	8
V. Claim Construction.....	10
A. Intrinsic Evidence	13
1. Specification of the '825 patent.....	13
2. Provisional Application No. 62/503,252	20
B. Extrinsic Evidence	22
1. Fortinet Documentation	22
2. Other Extrinsic Evidence	26
C. Petitioner's Interpretation is Unreasonable.....	31
VI. Ground 1: Chandra Does Not Render Obvious Claims 1-5, 12, 15-16, 21-22, and 27	34
A. Independent Claims 1, 15, 21, 27: Chandra does not disclose a "cooperative security fabric"	35
B. Dependent Claims 2, 4, 15: Chandra does not disclose "local network policies"	38
C. Dependent Claim 12: Chandra does not disclose or render obvious that flags are carried in "a first packet of a session".....	41

VII.	Ground 2: Chandra in Combination with Buruganahalli Does Not Render Obvious 6-7, 17-18, 23-24, 28-29	42
VIII.	Ground 3 and 4: Petitioner Fails to Establish that Chandra in Combination with Other References Render Obvious Claims 10-11, 13-14, 19-20, 25-26, and 30-31	47
IX.	Ground 5: Keohane Does Not Render Obvious Claims 1-5, 12, 15-16, 21-22, 27	47
A.	Independent Claims 1, 15, 21, 27: Keohane does not disclose a “cooperative security fabric”	47
B.	Dependent Claim 4: Keohane does not disclose or render obvious a first network security appliance that receives traffic “not transmitted from the second network security appliance”	50
C.	Dependent Claim 12: Keohane does not disclose or render obvious that flags are carried in “a first packet of a session”	53
X.	Ground 6: Keohane in Combination With Buruganahalli Does Not Render Obvious Claims 6-7, 17-18, 23-24, 28-29	53
A.	Dependent Claims 6-7, 17-18, 23-24, 28-29: Keohane in view of Buruganahalli does not render obvious a “next network appliance”	54
B.	Dependent Claims 6, 17, 23, 28: A POSITA would not be motivated to use Buruganahalli’s updating of tags with Keohane’s signatures	56
C.	Dependent Claims 7, 18, 24, 29: A POSITA would not be motivated to remove Keohane’s signatures	59
XI.	Grounds 7 and 8: Keohane in Combination with Other References Does Not Render Obvious Claims 10, 13-14, 19-20, 25-26, and 30-31	61
XII.	Conclusion	61

EXHIBIT LIST

No.	Exhibit
2001	Declaration of John Black, Jr., Ph.D.
2002	<i>Curriculum vitae</i> of John Black, Jr., Ph.D.
2003	“fabric,” Newton’s Telecom Dictionary, 30 th 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

I. INTRODUCTION

Patent Owner is one of the largest commercial suppliers of network security appliances in the world and an innovator in the field. Many of Patent Owner's commercial products that predate the challenged patent, such as its FortiGate products, employ a technology known as a "cooperative security fabric," or a "CSF"—a term that Patent Owner introduced to the industry to describe its technology. A CSF is a specific type of fabric topology and is the focus of the challenged claims. Petitioner ignores the well-established meaning of this industry term (identified in both intrinsic and extrinsic evidence) and has taken the position that a "CSF" embodies *any* communications connection, including, remarkably, a simple, unidirectional point-to-point connection between two devices.

This position does not withstand scrutiny. As evidenced by both the intrinsic and extrinsic record, including dictionaries, textbooks, and industry publications, a "cooperative security fabric" is a topology of network security appliances that cooperate to inspect incoming and outgoing traffic along multiple interconnected paths. The '825's *primary focus* is the inspection of incoming and outgoing traffic between network appliances within the claimed CSF.

The Petition’s primary references are **not** directed to a CSF.

Chandra’s system only coordinates inspection of traffic ***within the same network*** rather than incoming and outgoing traffic. Chandra expressly states that, for securing incoming traffic, its system does **not** involve any cooperation between network appliances—it therefore does not disclose a CSF.

The Petition also argues that Keohane’s firewall, mail gateway, and client comprise a CSF. But there is no dispute that this connection is a point-to-point, unidirectional path. Petitioner’s own expert has admitted that a “fabric” is analogous to a piece of clothing with multiple (*i.e.*, paths). Keohane’s single thread (a single point-to-point connection) is thus not a fabric.

The Petition fails for additional reasons. For example, Chandra does not render obvious performing operations based on local policies—instead, Chandra performs operations based on a global policy. Chandra, being limited to communications between two appliances, also does not render obvious a third network security appliance. Likewise, since Keohane is limited to a single, unidirectional path or tread, it does not render obvious performing operations on traffic **not** received from CSF nodes. And neither

reference discloses or renders obvious the transmission of flags within a *first* packet of a session.

II. LEVEL OF ORDINARY SKILL IN THE ART

A person of ordinary skill in the art (“POSITA”) relevant to the ’825 patent at the time of the invention 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. Ex. 2004, ¶18. Petitioner’s expert, Dr. Black, was a POSITA at the time of the priority date of the ’825 patent. Ex. 2004, ¶20.

Patent Owner’s description of the level of ordinary skill in the art is almost the same as that of the Petitioner. See Pet. 19; Ex. 2004, ¶19. The positions set forth in this response would be the same under either parties’ proposal.

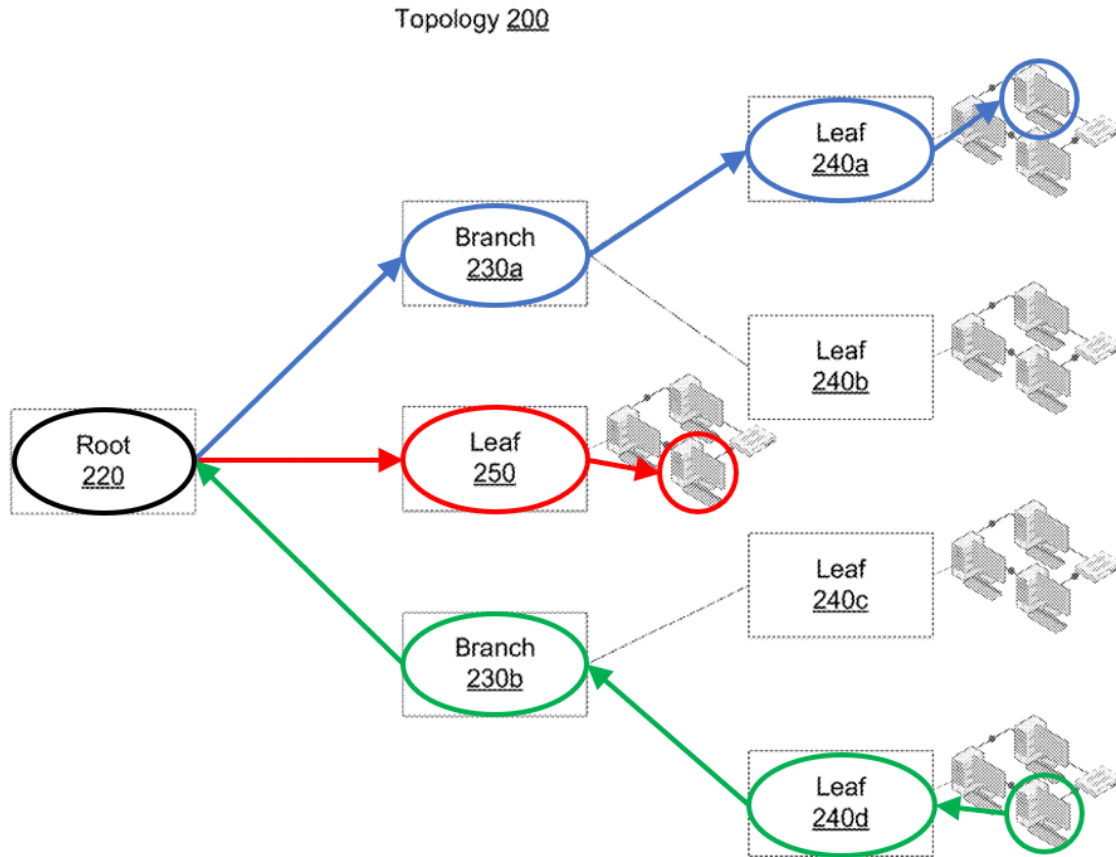
III. OVERVIEW OF THE ’825 PATENT

The ’825 patent explains that “[i]n a large network” with “many network security appliances,” each appliance may “work independently and execute operations” on “network traffic transmitted to/from the network” that may be redundant. Ex. 1001, 1:33-37, 1:45-52; Ex. 2004, ¶30. The ’825

patent solves this redundancy issue by using a “cooperative security fabric (CSF).” A “CSF” is a term Patent Owner introduced to the industry prior to the ‘825 patent to refer to the topology and the mechanisms in which its network appliances, such as the FortiGate, operated. Ex. 2004, ¶31. The ‘825 patent explains that within this topology, interconnected network security appliances “coordinat[e] security operations” using flags carried by incoming/outgoing network traffic to indicate which operations have already been executed by an appliance, and further indicate whether the packets were transmitted by participating appliances in the CSF. Ex. 1001, 2:1-16.

Figure 2 of the ‘825 patent is an example topology of a CSF. Ex. 2004, ¶32. The “root node ... is the outermost network security appliance of the cooperative security fabric [and] acts as a WAN role in topology 200 that connects a private network to other networks or the Internet.” Ex. 1001, 5:52-56. The topology also includes branch nodes that constitute a middle layer and leaf nodes that connect endpoint devices to the network. *Id.*, 5:60-6:5. As is evident, there are several different paths that network traffic could take, thereby requiring different coordination depending on the path. Ex. 2004, ¶32. The ‘825 patent explains that a topology may have multiple root nodes, multiple layers of branch nodes, and paths that do not involve branch nodes

(such as the red path below in the modified version of Figure 2). Ex. 1001, 6:14-24; Ex. 2004, ¶32.



Thus, when coordinating operations, the network security appliances operate on “downstream network traffic that is transmitted *from the Internet 110 to a subnet*” or “upstream network traffic that is transmitted *from [a] subnet ... to the Internet 110.*” *Id.*, 5:33-38. The network appliances will inspect network packets for flags that, if present, indicate that the flag “was added to the original network packet by a previous member node along the transmission path ... to indicate that the network packet is transmitted from a

member node” as well as “information about the distribution of security operations among member nodes of a CSF.” *Id.*, 6:53-7:4. However, if the flag is **not** present, “it means that the member node is the first member of the CSF to receive the incoming packet” which “happen[s] to root nodes for downstream network traffic and leaf nodes for upstream network traffic.” *Id.*, 7:26-30; Ex. 2004, ¶33.

IV. OVERVIEW OF CERTAIN CITED ART

Petitioner’s Grounds rely on two primary references: Chandra (Grounds 1-4) and Keohane (Grounds 5-8). Petitioner relies exclusively on these references to show the claimed “cooperative security fabric” and determining that network traffic was “transmitted from a ... network security appliance that is participating in the CSF” also required by the claims. But Chandra and Keohane fail to disclose either limitation. Ex. 2004, ¶34.

A. Chandra (Ex. 1004)

Chandra is directed to a network where “data is transferred between network devices,” *i.e.* network traffic only **within** a network. Ex. 1004, ¶4. Chandra notes that, with respect to a network involving multiple VPN sites, the VPN firewall policies may “be uniform among all the VPN sites.” *Id.*, ¶6. However, “[t]his can result in the same action being performed by more than one VPN site.” *Id.*; Ex. 2004, ¶35.

To resolve this specific issue of redundant actions performed on internal network traffic, Chandra describes a system involving coordination between “a transmitting Customer Edge (CE)” and a “receiving CE,” where the transmitting CE and receiving CE can be “for example, Intrusion Detection Systems (IDSs), firewalls, etc.” Ex. 1004, ¶30; Ex. 2004, ¶36. In other words, the transmitting CE may be a firewall for the VPN site that receives traffic from the transmitting endpoint, and the receiving CE may be a firewall for another VPN site that sends traffic to the receiving endpoint. See Fig. 2; Ex. 2004, ¶36.

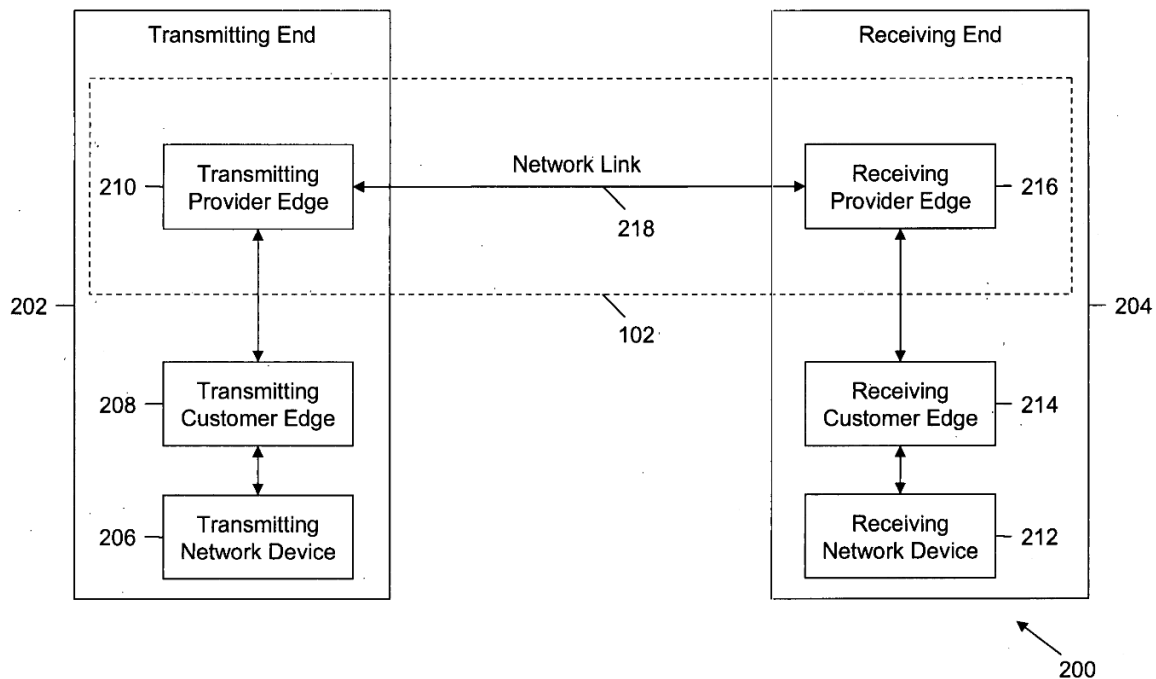


FIG. 2

Transmitting CE and receiving CE coordinate which actions to perform on the network traffic by using labels that are used to tag the data packets. Ex.

1004, ¶¶31-32. Prior to that, the transmitting CE and receiving CE will first “authenticate each other” and exchange the “CE labels that can be used for tagging the data packets.” *Id.*, ¶33; Ex. 2004, ¶37.

Notably, Chandra only discloses coordination for traffic between **two** nodes ***within the same network***, not traffic coming into or going out of the network. Ex. 1004, ¶21. For incoming traffic that originates from outside the network, such as the Internet, only the “receiving CE” receives such traffic and thus only the receiving CE performs actions on such traffic—which involves no cooperation with other appliances. *Id.*, ¶53; *see also* ¶77 (“[R]eceiving end can identify a data packet from the Internet as insecure, and perform rigorous actions on it.”); Ex. 2004, ¶38.

B. Keohane (Ex. 1008)

Keohane is directed to a method for performing iterative security operations on incoming network traffic in a single direction. Ex. 1008, ¶¶33-37; Ex. 2004, ¶39. Keohane’s method is depicted in Figure 3 below.

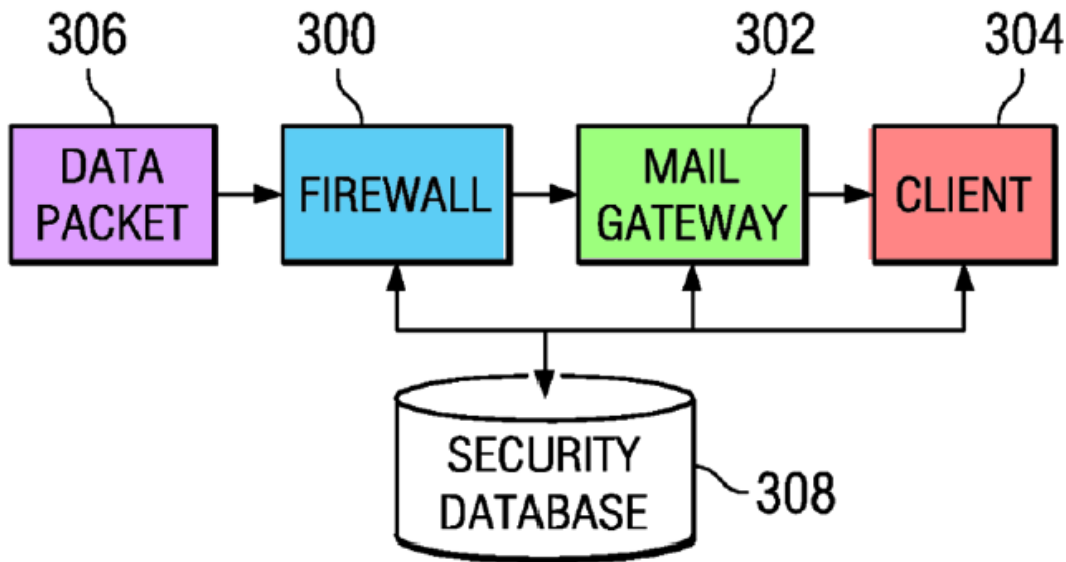


FIG. 3
(Annotated)

As shown in the figure, Keohane screens incoming data through a Firewall (300) and a Mail Gateway (302) before ultimately allowing the data to be transmitted to the client. Ex. 2004, ¶40.

Keohane's data screen methods involve the attachment of a signature located in the header of a data packet by an upstream network element in order for a downstream network element to be able to confirm the traffic was received from the upstream network element. Ex. 1008, ¶11; Ex. 2004, ¶41. Thus, as depicted in Figure 3, Keohane discloses that its system operates *unidirectionally* along a *single* path: a data packet travels in one direction from network element "firewall 300," to "mail gateway 302," and to "client 304," with each network element performing a security action on the data and

inserting a “signature ... indicat[ing] that a previous security action has been performed on the data packet.” Ex. 1008, ¶¶32-37; Ex. 2004, ¶41.

V. CLAIM CONSTRUCTION

In an *inter partes* review, claim terms receive their plain and ordinary meaning in light of the specification of the patent in which it appears, the same standard as used in district court. 37 C.F.R. § 42.100(b); *see Phillips v. AWH Corp.*, 415 F.3d 1303 (Fed. Cir. 2005). Petitioner states that all “challenged claims should be construed in accordance with the ordinary customary meaning of such claim.” Pet. 14; Ex. 2004, ¶42.

Patent Owner argued in its preliminary response that the plain meaning of the term “fabric” “requires network nodes that process bidirectional communications.” Paper 6 at 10-15. While the Board credited Patent Owner’s evidence, it construed “fabric” as “a network topology such as the physical structure of a switch or network.” Paper 10 at 9. Respectfully, this definition is overly broad. Indeed, its breadth is demonstrated by Dr. Franz’s testimony elicited during cross-examination, where he testified that in his opinion, a “network fabric” would include “just ... two boxes with the cable.” Ex. 2005, 14:18-24; Ex. 2004, ¶43. He further testified that a “fabric,” in the context of the distributed computing (the field the ‘825 patent is directed to) is simply “the physical infrastructure that something is built out of.” Ex. 2005,

16:8-14. Building on this interpretation of “fabric,” Petitioner then contends that even the larger phrase (“cooperative security fabric”) can be met by just two devices connected directly to each other. Pet. 27 (arguing that “as few as two [appliances] are needed” to “form a CSF”).

Dr. Franz’s overly-broad interpretation of this claim term is unsurprising, given his admitted lack of experience with a critical technology of the ‘825 patent—distributed computing.¹ Ex. 2004, ¶43. The Board found that the ‘825 patent describes methods for “coordinat[ing] ... security operations” among multiple network security appliances, which Dr. Franz agreed with. Ex. 2005, 19:1-16. Coordinating operations among multiple network security appliances falls squarely in the field of distributed computing. Ex. 2004, ¶43. Nonetheless, Dr. Franz admitted that he understood distributed computing only “a little bit.” Ex. 2005, 15:4-6 (“Q: Do you have an understanding of a field called distributed computing? A: A *little bit*.”). When pressed, he refused to respond to the question “under oath”:

¹ See, e.g., Ex. 1001, 7:2-4 (“[T]he flag may include more information about the *distribution* of security operations among member nodes of a CSF.”); 8:50-52 (“CSF manager 402 is used for managing *distribution* of security operations among members of the CSF”).

Q. Well, I'm asking: Do you have an understanding of the term "fabric" in the context of distributed computing?

A. I would not want to answer that under oath without doing some additional research, you know, to make sure that my understanding is totally consistent with – yeah.

Id., 16:1-7.

Petitioner's interpretation cannot be correct and runs contrary to even just the word "fabric." The term comes from an analogy to clothing: just like fabric in clothing consists of interleaved threads, a fabric in networking consists of interconnected paths. Ex. 2004, ¶44. Even Petitioner's own expert testified "that's probably where the analogy comes from" and that "the term in computer science and networking ... may be inspired by the idea that you have cables weaving ... through buildings." Ex. 2005, 7:25-8:8. Yet according to Petitioner, just two computers connected via cable—a single "thread" in the clothing analogy—would qualify as a "fabric." Petitioner's position runs against common sense: a single thread is not a fabric. Ex. 2004, ¶44.

Even more egregiously, Petitioner's overly broad interpretation of the claim language ignores the entirety of the phrase "**cooperative security fabric**," or a "CSF." A CSF is a term that Patent Owner introduced to the industry. Ex. 2004, ¶¶66-73; Section V.B.1. It is a specific type of fabric

topology Patent Owner's products employ to address challenges in coordinating security operations performed by network security appliances on incoming and outgoing network traffic in "a larger network" with "many network security appliances." Ex. 1001, 1:33-37, 5:38-40. It is in such a network that there is "a need for" not just any fabric, but "a cooperative security fabric (CSF) that may coordinate operations performed on network traffic to avoid or reduce redundant operations among members of the CSF." *Id.*, 1:64-67.

Accordingly, consistent with the purpose of the '825 patent and the other intrinsic and extrinsic evidence, a POSITA would have understood that a CSF is "a topology of network security appliances that cooperate to inspect incoming and outgoing traffic along multiple interconnected paths." Ex. 2004, ¶45. By contrast, Petitioner's overly broad interpretation of CSF—such that it may consist of just two devices connected via a cable—removes any meaning from the claim term, defeats the very purpose of the '825 patent's innovative cooperative processing, and thus cannot be correct. *Id.*

A. Intrinsic Evidence

1. Specification of the '825 patent

Construing the plain meaning of a term begins with the patent's intrinsic evidence, especially its specification. *Phillips v. AWH Corp.*, 415

F.3d 1303, 1315 (Fed. Cir. 2005) (“[T]he specification ... is the single best guide to the meaning of a disputed term.”). Here, the specification supports Patent Owner’s proposed interpretation for a CSF. Ex. 2004, ¶¶46-60.

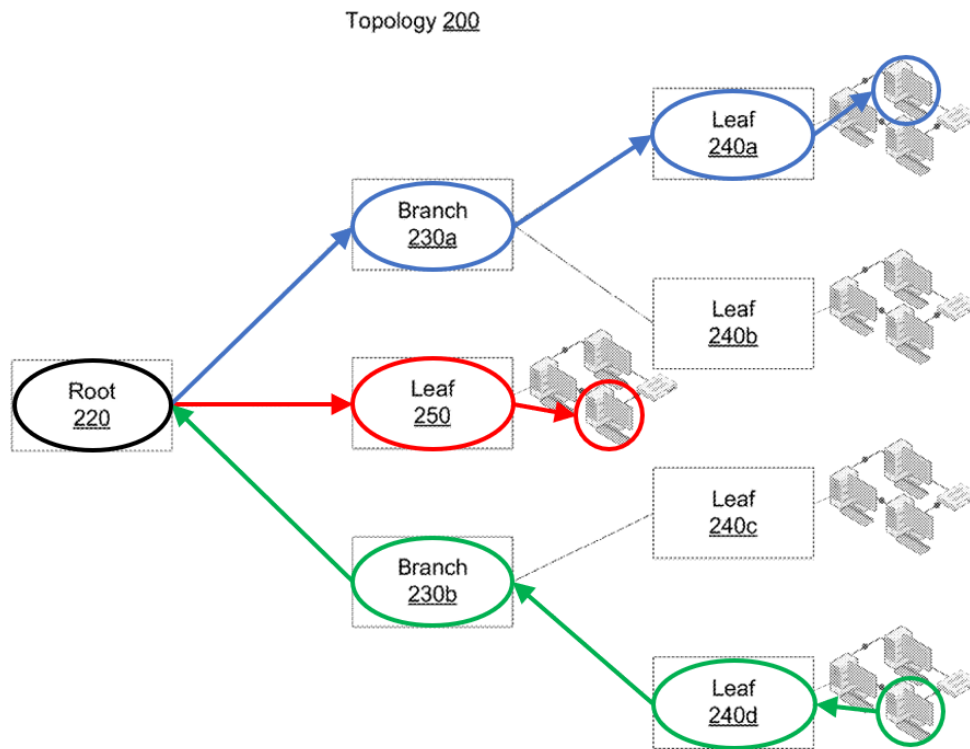
The ’825 patent is directed to cooperative security within a “large network” with “many network security appliances ... deployed at different locations within the network.” Ex. 1001, 1:33-37. In its earlier days, computer networks were straightforward. Ex. 2004, ¶¶48-49. For example, two computers could be connected directly to each other (called a point-to-point topology), multiple computers could have access to the same communication medium (called a bus topology), or they could be connected to each other in a ring (called a ring topology). *Id.* These topologies employed clearly defined paths between individual computers. *Id.* Over time, however, networks grew more complex as enterprises increased the number of offices, locations, departments, functions, etc., that needed to be connected to each other via a network. *Id.* Thus, as enterprise networks became larger, a complex, interconnected topology known as a “fabric” was developed to handle the management of such networks. *Id.* In contrast to more traditional network topologies, such as point-to-point, bus, and ring topologies, a “fabric” topology consists of multiple paths to and from endpoints. *Id.* The resultant

cabling, as Dr. Franz admits, resembles interwoven threads in a piece of cloth—i.e., a “fabric.” Ex. 2005, 7:25-8:8.

The ’825 patent sought to improve such fabrics, by using a specific type of fabric called a “cooperative security fabric.” Ex. 2004, ¶50. In a simple network where all network traffic traverses the same path of network appliances, no coordination is necessary, even if that path traverses multiple network security appliances. Ex. 2004, ¶51. In such a simplistic topology, each network security appliance could be configured to always perform the same subset of security operations, thereby eliminating redundancy even without cooperation. *Id.*, ¶51. But in a network fabric, where there are many different paths of network appliances for traffic to “[n]etwork traffic transmitted to/from the network may go through multiple network security appliances along a path within the network.” Ex. 1001, 1:33-37.; Ex. 2004, ¶¶50, 52. In the prior art, the network security appliances “work[] independently,” which possibly leads to an appliance performing a “redundant” operation that have “already been done by a previous network security appliance at a previous hop.” *Id.*, 1:46, 1:54-56. The ’825 patent therefore notes a “need for a cooperative security fabric (CSF) that may coordinate operations performed on network traffic,” i.e. traffic “transmitted

to/from the network,” “to avoid or reduce redundant operations among members of the CSF.” *Id.*, 1:64-67.

Figure 2 of the '825 patent depicts such a cooperative security fabric. In the below modified version of Figure 2, each leaf is further connected to one or more endpoints, such as the endpoints shown in Figure 1,² and annotated to show three different paths through the network. Ex. 2004, ¶52.



² Ex. 1001, 6:1-3 (“Leaf nodes 250 a-250 d are the network security appliances that are used for connecting endpoint devices of the private network.”).

In this example, all three transmission paths traverse Root node 220, but diverge thereafter. Ex. 2004, ¶53. In the blue and green transmission path, traffic goes through the same Root node 220 but then through different Branch nodes 230a and 230b, and different Leaf nodes 240a and 240d. *Id.* In addition, the blue transmission path is shown as being “downstream,” *i.e.*, from the Internet to an endpoint, whereas the green transmission path is shown as being “upstream,” *i.e.*, from an endpoint to the Internet. See Ex. 1001, 5:32-38 (“[D]ownstream network traffic that is transmitted from the Internet 110 to a subnet 141 goes through three network security appliances, *i.e.* a root, a middle and a subnet network security appliance, while upstream network traffic that is transmitted from subnet 141 to the Internet 110 goes through a subnet, a middle and a root network security appliance.”). The red transmission path also differs from the blue transmission path as it has “no branch nodes.” *Id.*, 6:18-20; Ex. 2004, ¶54. Finally, while not pictured, “Topology 200 may have multiple layers of branch nodes, *i.e.*, multiple branch nodes exist between a root node and a leaf node” and nodes that act “as multiple roles in the topology 200,” such as “a network security appliance [that is] connect[ed] to another network security appliance as well as endpoint devices,” thereby acting as “a branch node and a leaf node in the same time.” Ex. 1001, 6:21-27.

It is this complexity and existence of multiple possible paths through a network “fabric” that creates “a need for ... coordinat[ing] operations performed on network traffic to avoid or reduce redundant operations” as traffic traverses any one of multiple potential paths through the network fabric. Ex. 2004, ¶55; Ex. 1001, 1:64-67. For example, in the annotated version of Figure 2 above, traffic arriving at a leaf node may have traversed zero network security appliances (green upstream path), one network security appliance (red downstream path), or two network security appliances (blue downstream path). Ex. 2004, ¶55. In this scenario, a mechanism is needed to dynamically determine what security operations have already been performed and what additional security operations still need to be performed. *Id.* Thus, the ’825 patent describes that each “**member node** of the cooperative security fabric may add one or more flags ... to a network packet,” which is then “transmitted **to another member node** at the next hop.” Ex. 1001, 6:28-34. The member node that receives the packet “can be **any node** of the CSF.” *Id.*, 6:50-51.

This accords with the Institution Decision’s description of the ’825 patent: the ’825 patent “describes methods of performing security operations on network traffic **passing through** a cooperative security fabric (CSF) of network security appliances that coordinate their security operations to avoid

redundant security operations.” Paper 10 at 3; Ex. 2004, ¶¶56-57. Petitioner’s expert Dr. Franz testified that he agrees with this description. Ex. 2005, 19:10-16; *see also* 26:4-7 (“[T]he CSF has the ... objective of coordinating security operations on the network traffic passing through them.”). Traffic that “pass[es] through” a network is understood as traffic transmitted into or out of the network. Ex. 2004, ¶57. Indeed, Dr. Franz further confirmed that the ’825 patent does not provide any examples of “performing security operations on traffic between two subnets” of the same network. Ex. 2005, 35:7-17.

To the extent Petitioner argues that a CSF need only process purely internal network traffic (such as VPN traffic or subnetwork-to-subnetwork traffic), Petitioner is incorrect. Ex. 2004, ¶58. The ’825 patent never describes an embodiment that only inspects internal traffic. Dr. Franz did testify that the ’825 patent describes a VPN security appliance “connected to private network 120 through the Internet 110” (Ex. 1001, 4:66-67), which he described as “subnetworks being able to communicate with each other.” Ex. 2005, 74:14-23. But the ’825 patent does not describe that such VPN traffic to other endpoints within the network is inspected by the CSF.

Moreover, a POSITA would understand that a VPN is virtually part of the same network, and thus communications with a VPN site are still

considered to be within the same network regardless of the physical path taken. *Id.*; Ex. 1001, 4:65-5:2 (“[A] subnet 151 and a subnet security appliance 150 [that] are connected to private network 120 through the Internet 110 via VPN ... may be seen as a ***part of private network 110.***”); Ex. 2005, 42:12-43:5 (“[O]ne of the purposes of VPN technology is that from the perspective of the two endpoints ... they appear to be connected to the same virtual private network.”); Ex. 2004, ¶159. Again, the ’825 patent does not describe that its CSF inspects internal network traffic—instead, the ’825 patent is concerned with and directed to “downstream network traffic that is transmitted from the Internet 110 to a subnet,” or “upstream network traffic that is transmitted from [a] subnet ... to the Internet.” Ex. 1001, 5:32-36. And such traffic does not include VPN traffic, which is considered to be internal traffic. Ex. 2004, ¶160.

Accordingly, the intrinsic evidence consistently shows that the claimed “cooperative security network” is “a topology of network security appliances that cooperate to inspect incoming and outgoing traffic along multiple interconnected paths,” as proposed by Patent Owner.

2. Provisional Application No. 62/503,252

The ’825 patent claims priority to Provisional Application No. 62/503,252 (“’252 Provisional”). Ex. 1001. Exhibit 2016 is a copy of the

'252 Provisional. A provisional application incorporated by reference (as is the case here) is also intrinsic evidence for the purposes of claim construction when addressing common subject matter. *E.I. Du Pont de Nemours & Co. v. Unifrax I LLC*, 921 F.3d 1060, 1070 (Fed. Cir. 2019).

The '252 Provisional provides additional intrinsic evidence that supports the plain meaning of a CSF as “a topology of network security appliances that cooperate to inspect incoming and outgoing traffic along multiple interconnected paths.” Ex. 2004, ¶¶61-63. For example, the '252 Provisional describes the “dynamic formation of a CSF among multiple network security devices within a private network ***based on hierarchical interconnections among the network security devices.***” Ex. 2016, ¶13. The “hierarchical interconnections” involve different levels of network security devices, and in one embodiment, it teaches that there are multiple nodes at the same hierarchical level within a CSF, and that a node has downstream and upstream nodes.” *Id.*, ¶18; Ex. 2004, ¶62. Thus, this description describes a CSF where multiple network security nodes belong to each hierarchical level and have their own downstream nodes, indicating multiple interconnected paths. Ex. 2004, ¶63.

B. Extrinsic Evidence

1. Fortinet Documentation

The extrinsic evidence also supports that the industry has accepted Patent Owner’s definition as the plain meaning of CSF. Ex. 2004, ¶¶64-84. The concept of a CSF was first introduced by Patent Owner Fortinet in 2016. Ex. 2004, ¶66; Exs. 2012, 2013. Thus, the extrinsic evidence of the plain meaning of CSF can be found in Patent Owner’s marketing and technical literature. Ex. 2004, ¶67. A POSITA would have been familiar with such products and documentation, because Patent Owner was and is a leading company and innovator in the field of network and data security. Ex. 2004, ¶66.

A POSITA would have also understood that Fortinet documents would be the best source for the meaning of the term CSF. Ex. 2004, ¶67. The term does not appear in any academic papers or books. *Id.*, ¶68. A search for patents (both foreign and domestic) only results in Fortinet-owned patents or applications. *Id.* Searching for the term on Google likewise only results in Fortinet documentation or discussions about Fortinet products. *Id.*, ¶69.

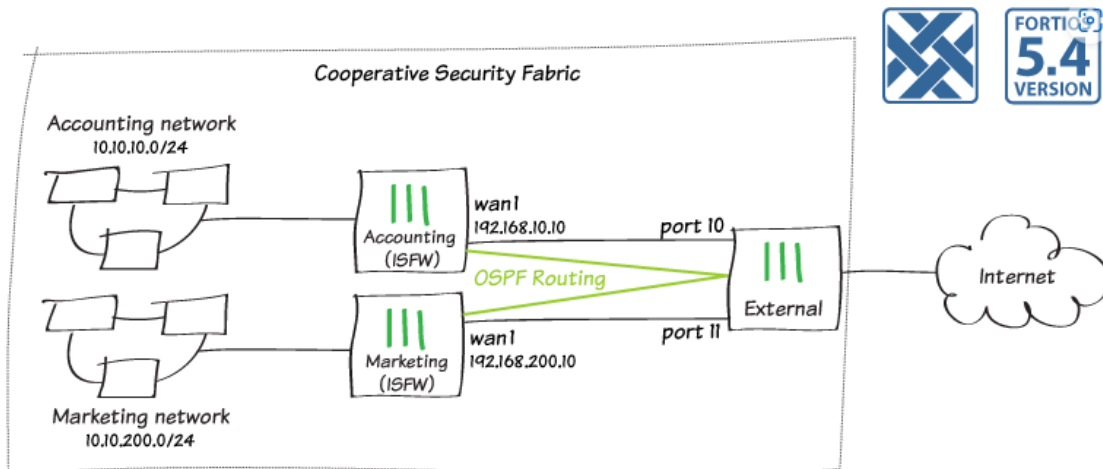
Even before the filing date of the ’825 patent, the networking industry was well-aware of Fortinet’s “security fabric” and associated “cooperative security fabric.” Indeed, Fortinet’s “Security Fabric” won the 2016 Network

Security Product of the Year Award. Ex. 2014. One aspect of the Fortinet “security fabric” is its ability to detect breaches in network security, which by definition entails protecting networks from outside threats. Ex. 2015 (“These results further demonstrate the effectiveness of the Fortinet Security Fabric, combining global and local security to protect enterprises and mid-sized organizations against the most advanced cyber threats.”).

In that same time frame, Fortinet published extensive documentation online regarding the nature of its “cooperative security fabric.” One document, published June 8, 2016 and entitled “Cooperative Security Fabric” describes the steps for “configur[ing] a Cooperative Security Fabric (CSF) ... throughout your network, using a range of Fortinet products.” Ex. 2012, 1.³ It instructs that the first step is to “install the initial FortiGate which will later be used as the **Internet-facing, or upstream**, FortiGate in the security fabric.” *Id.*, 2. The next step is to “[i]nstall[] internal FortiGates and enabl[e] a security fabric,” where in the example provided in the documentation, “two additional FortiGates are added to the network” and once installed, “a security fabric is set up between them **and the external FortiGate.**” *Id.*

3

This second step includes a link to another document which provides additional detail for setting up the internal FortiGates. Ex. 2013. This document provides a diagram of a simple CSF that depicts the two internal FortiGates (Accounting and Marketing) being routed through the Internet-facing External Fortigate, thus indicating that network traffic travels through multiple interconnected paths. *Id.*, 1.



The document describes how to install the internal FortiGates and enable them as a CSF. Once the internal FortiGates are installed, the CSF can be configured to “allow you to distribute security functions to different FortiGates in the security fabric,” such as “implement[ing] virus scanning on the External FortiGate but add[ing] application control and web filtering to the ISFW [internal] FortiGates.” Ex. 2013, 9. This “results in distributed processing between the FortiGates in the CSF; reducing the load on each one.”

Id. In other words, the CSF described in these documents uses FortiGates that cooperate to inspect incoming and outgoing network traffic along multiple interconnected paths, as reflected in Patent Owner’s proposed construction for “cooperative security fabric.”

Exhibits 2012 and 2013 are true and correct copies of Patent Owner’s website as archived by the Internet Archive in 2016. Ex. 2004, ¶73. As Dr. Black attests, the Internet Archive operates a service known as the Wayback Machine, which a website that has for many years stored archived copies of webpages. *Id.* The Internet Archive uses crawlers to surf the Internet and make copies of web pages to be preserved. *Id.* On every archived copy of a web page, the Wayback Machine provides the date and time it made the archived copy—for Exhibit 2012, it was archived July 28, 2016, and for Exhibit 2013, it was archived August 28, 2016. *Id.* Thus, these exhibits are authentic copies of those web pages as they existed in 2016. *Id.*; MPEP 2128.E (“[Documents] obtained via the Wayback Machine® sets forth a prima facie case that the [document] was publicly accessible at the date and time provided in the time stamp.”); *Valve Corp. v. Ironburg Inventions, Ltd.*, 8 F.4th 1364, 13674 (Fed. Cir. 2021) (“[C]ontents of webpages available through the Wayback Machine [are] sources whose accuracy cannot reasonably be questioned.”).

2. Other Extrinsic Evidence

Other extrinsic evidence that supports Patent Owner’s proposed construction for “cooperative security fabric” includes extrinsic evidence regarding the term “fabric” which establishes that a fabric, and therefore a CSF, includes network security appliances with multiple interconnected paths. Ex. 2004, ¶¶74-83.

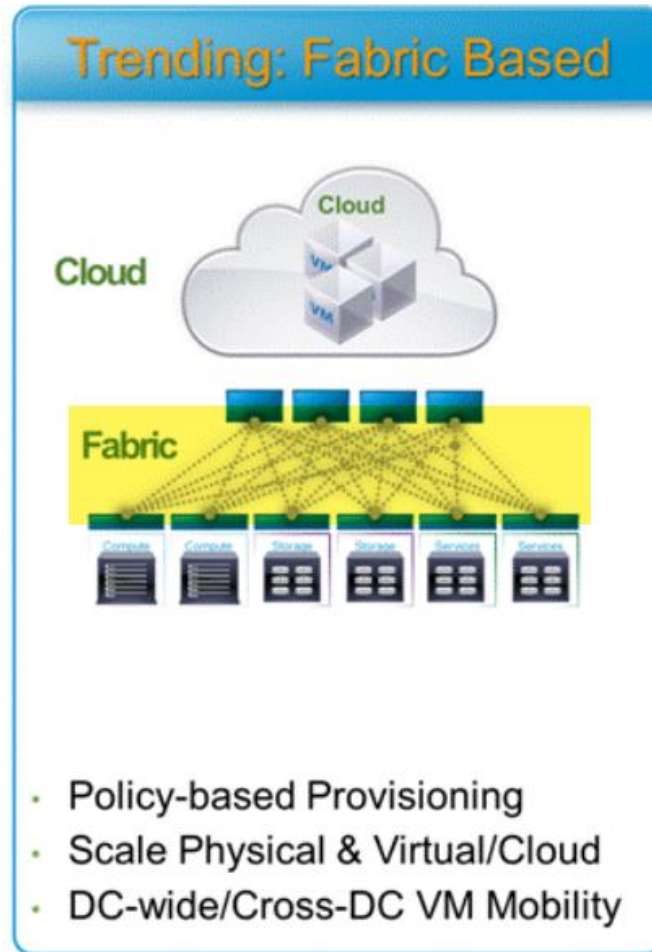
For example, the 30th Edition of Newton’s Telecom Dictionary (2016) defines “fabric” as “[a] descriptive term referring to the physical structure of a switch or network,” where “[*m*]uch like a piece of cloth, physical/logical communications *channels (threads) [plural] are interwoven* from port-to-port (end-to-end).” Ex. 2003.⁴ In other words, a “fabric” consists of *multiple*,

⁴ The Board’s institution decision focused on the first sentence of this definition (“A descriptive term referring to the physical structure of a switch or network.”) while not incorporating the second sentence (“Much like a piece of cloth, physical/logical communications channels (threads) are interwoven from port-to-port (end-to-end).”). Respectfully, the first sentence merely states that a “fabric” describes a type of network topology, and it is the second sentence that defines what type of network topology qualifies as a “fabric.” Ex. 2004, ¶77.

interwoven communications paths/channels (which are analogous to individual threads within a piece of cloth) that define the network paths from one end to another—much like with clothing, a single thread does not constitute a fabric. Ex. 2004, ¶75. Petitioner’s expert, Dr. Franz, agreed that this dictionary definition “reflects the ordinary and customary meaning of fabric” (Ex. 2005, 29:13-16) and that the term “fabric” was inspired by clothing fabric (Ex. 2005, 7:25-8:8 (“[T]hat’s probably where the analogy comes from.”)). Ex. 2004, ¶76.

In addition, a 2002 book titled “Using Storage Area Networks” identifies three kinds of “Topologies”: point-to-point, loop, and switched fabric. Ex. 2006, 145; Ex. 2004, ¶78. Whereas a “point-to-point” topology is “a simple and easily applied topology for connecting two nodes” which is “best used on a small scale,” a “switched fabric topology is appropriate for **large-scale or enterprise networks** in which **a number of users are interconnected.**” *Id.*, 146. The “fabric is used to connect networks across large distances” and “works in a similar fashion to a switched telephone network in that it can provide a dedicated connection between multiple pairs of nodes.” *Id.*

Similarly, a 2013 networking book depicts a “Fabric Based” network as a collection of multiple interconnections between endpoints and the edge nodes of the network. Ex. 2007, 167; Ex. 2004, ¶79.



The same book also depicts a “Traditional three-tier Network **Fabric** Architecture,” with “access switches” (i.e. subnetwork switches) that “are connected via Ethernet to aggregation switches,” and then “aggregation switches [that] are connected into a set of core switches or routers that forward traffic flows from servers to an intranet and internet.” Ex. 2007, 169. This

fabric is depicted below and shows multiple paths to and from Access-layer switches. Ex. 2004, ¶80.

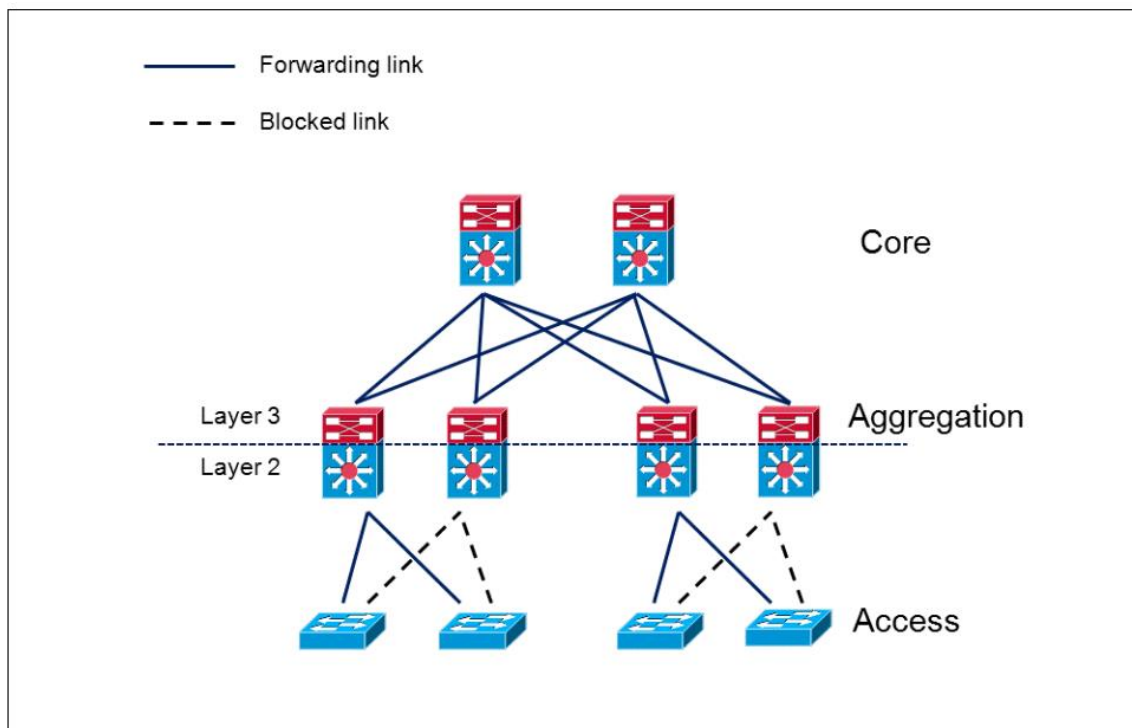


Figure 3-9 Traditional three-tier Network Fabric Architecture

Petitioner’s expert in related cases also agrees that the plain meaning of “fabric” requires multiple paths to and from endpoints. Ex. 2004, ¶81. For example, in IPR2023-00030, Petitioner’s expert Dr. Wenke Lee testified at his deposition that a fabric is “**multiple** security elements and controls that one would use or one would want to have,” with firewalls (which controls traffic into and out of a network) being “part of the fabric.” Ex. 2009, 109:4-6. And in IPR2023-00175, in describing U.S. Patent No. 8,000,329 (“Fendick”) (which was filed June, 29, 2007), Dr. Lee testified that a “fabric” is “basically,

a communications hub” “for connecting the platform components,” and provided the below annotated figure depicting how a fabric provides interconnected paths between multiple components, including the components that provide ingress/egress. Ex. 2010, ¶160.

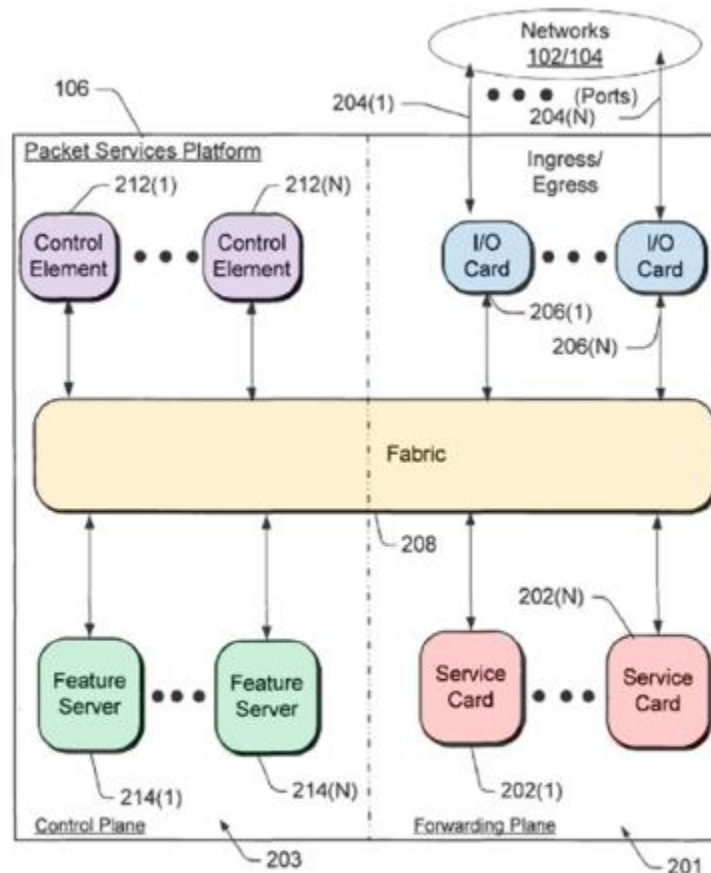


Fig. 2
(Annotated)

Indeed, the Fendick reference explains that a “fabric” “facilitates *multiple parallel communication sessions* of traffic, as well as, permits multiple entities, such as control elements 212 and service cards 202, to

communicate with each other in a simultaneous fashion.” Ex. 2011, 7:42-45; Ex. 2004, ¶82.

Thus, the extrinsic evidence for “fabric” establishes that the plain meaning of “cooperative security fabric” includes network security appliances with multiple interconnected paths. Ex. 2004, ¶83.

C. Petitioner’s Interpretation is Unreasonable

Although Petitioner did not provide a definition of “cooperative security fabric” in its Petition, Petitioner’s expert Dr. Franz has testified that he believes (1) a “fabric” is merely “the physical structure of a network,” and “is how ... you physically realize the topology” (Ex. 2005, 7:18-19, 11:3-4), which is an overly broad interpretation that would include “just ... two boxes with [a] cable” (*id.*, 14:18-24), and (2) the term CSF is simply a “compound ... term” whose plain meaning is merely defined by the plain meaning of its constituent parts, that is, it “coordinate[s] security operations on the network traffic passing through” its network appliances (*id.*, 7:6-15, 25:25-26:7). Ex. 2004, ¶84. Combining these interpretations allowed Petitioner to take the overly broad position that “as few as two [appliances] are needed” to “form a CSF.” Pet. at 27. That cannot be correct. Ex. 2004, ¶85.

First, Petitioner has no intrinsic support for its theory that “as few as two [network appliances] are needed” to form a fabric or CSF. Pet. 27; Ex.

2004, ¶86. Petitioner cites '825 patent at col. 6:18-20 in support of this assertion, which states that one of *multiple “paths” (plural)* in topology 200 may pass through just two nodes. Ex. 1001, 6:18-20. Thus, the '825 patent teaches that a CSF topology consists of multiple paths to and from endpoints, and if anything emphasizes that one of the challenges with a “fabric” is that different paths may have a different number of nodes along the way—the very type of complexity of a fabric compared to a point-to-point connection that motivated the innovation of the '825 patent. Ex. 2004, ¶86. Thus, the cited disclosure of the '825 patent is consistent with the rest of the specification in describing a network “fabric” as being applicable to “a large network” with “many network security appliances.” Ex. 1001, 1:33.

Second, Petitioner’s definition of “fabric” and CSF renders the terms superfluous within the claims of the '825 patent. Ex. 2004, ¶87. For example, Claim 1 recites a second network security appliance that transmits network traffic to a first network security appliance. According to Dr. Franz, such a transmission is sufficient to meet the “fabric” claim limitation, even without the additional claim language that requires both appliances to be part of the same “fabric.” Ex. 2005, 14:18-24. Claim 1 also recites coordination between the first and second network security appliances for performing network security operations on traffic. Thus, under Dr. Franz’s definitions, the

limitation “cooperative security fabric” would have no effect on claim scope, rendering the term superfluous. Ex. 2004, ¶87. Petitioner’s definition of a CSF (including its definition of fabric) is thus “highly disfavored.” See *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.”).

Third, Petitioner’s definition is not consistent with the history of networks and the term “fabric.” Ex. 2004, ¶88. As explained in Dr. Black’s testimony, the first computer networks were developed in the 1950s, when AT&T released the first commercial modem that allowed two or more computers to communicate with one another. *Id.* Yet, as Dr. Black further explained, network fabrics were not developed until many decades later when enterprise networks became significantly larger and administratively complex—the term does not appear in the literature until the 2000s. *Id.* As a result, a POSITA would consider a “fabric” to be a complex network topology with many paths to and from endpoints. *Id.* Petitioner’s position that even the earliest computer networks would qualify as a “fabric” is thus inconsistent with the terms emergence only in the context of larger, more complex networks. *Id.* Dr. Franz admitted that he is “not [a] historian of computer

science terms” and thus is in no position to rebut Dr. Black’s testimony. Ex. 2005, 8:2-3.

Fourth, the term “cooperative security fabric” is not merely defined by its constituent parts with no reference to the intrinsic or extrinsic evidence. Ex. 2004, ¶89. As discussed above, the term was introduced by Patent Owner, first found in Patent Owner’s products, and only appears in Patent Owner’s documentation and patents. *Id.* As a result, a POSITA would have known that the plain meaning of a CSF is found in Fortinet’s patents, documents, and products. *Id.* Moreover, the ’825 patent clearly describes the claimed “cooperative security fabric” and the concerns it addresses. Petitioner’s interpretation, based on the individual constituent words considered in a vacuum, fails to account for this evidence.

For all these reasons, Petitioner’s definition of CSF should be rejected and the Board should find that the plain meaning of CSF is “a topology of network security appliances that cooperate to inspect incoming and outgoing traffic along multiple interconnected paths.” Ex. 2004, ¶90.

VI. GROUND 1: CHANDRA DOES NOT RENDER OBVIOUS CLAIMS 1-5, 12, 15-16, 21-22, AND 27

Petitioner fails to establish that Chandra renders claims 1-5, 12, 15-16, 21-22, and 27 obvious because Chandra does not disclose a “cooperative

security fabric,” as claimed. For claims 2, 4, and 15, Chandra also does not disclose or render obvious that actions are taken based on “local network policies.” Finally, for claim 12, Petitioner provides no rationale to include flags in a “first packet of a session.” Ex. 2004, ¶91.

A. Independent Claims 1, 15, 21, 27: Chandra does not disclose a “cooperative security fabric”

Ground 1 relies on Chandra alone as rendering the claims obvious. But 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.” See Section V; Ex. 2004, ¶92.

Petitioner’s mapping of the ’825 patent claims to Chandra fails. Ex. 2004, ¶93. As properly construed, the claimed CSF requires inspection of incoming and outgoing traffic. But in Chandra, both the transmitting and receiving device are *within the same network*. Ex. 2004, ¶93; Ex. 2005, 41:13-16 (“[B]oth the transmitting end and the receiving end are connected to the same network 102”). Thus, “network devices 104 [are] connected to network 102,” which “function[s] as a single larger network.” Ex. 1004, ¶21. Chandra describes that, when coordinating network actions, there is a “transmitting end” and “receiving end,” which Dr. Franz described as

“endpoints.” *Id.*, ¶24; Ex. 2005, 42:24-43:5. Both the transmitting end and the receiving end have a corresponding “network device” which is one of the network devices within network 102, and which are connected via a “network link 218.” *Id.*, ¶¶26-27; *see also* ¶29 (“transmitting end 202 and receiving end 204 can be any identifiable part or region of network 102”). Each data packet in Chandra originates from “transmitting network device,” then a “transmitting customer edge” or “CE” performs a “first set of actions,” the packet is then transmitted over network 102 to a “receiving customer edge that performs a “second set of actions,” and finally arrives at the receiving network device. But in this context, 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.” Ex. 2004, ¶93.

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

packet from the Internet as insecure, and perform rigorous actions on it.”). As Dr. Franz explains it, “[i]f the data packet did not have a recognized label (e.g., ***the traffic originated from the Internet***), the receiving CE identified the packet as non-secure and performed a third set of actions on the packet.” Ex. 1002, ¶96. This is because such a packet “was not transmitted from the transmitting CE.” *Id.* Accordingly, for incoming traffic to and from the Internet, *i.e.*, incoming or outgoing traffic that is the focus of the ’825 patent, there is no “cooperative security fabric” consisting of multiple “network security appliances that cooperate to inspect” such traffic. Ex. 2004, ¶94.

Chandra also discloses in connection with Figure 8 that the transmitting CE and receiving CE can be connected via a VPN connection, but that scenario also fails to disclose the claimed “cooperative security fabric.” Ex. 2004, ¶95. As addressed above in connection with Patent Owner’s construction of “cooperative security fabric,” VPN sites are considered to be part of the same network. *Id.* Thus, any traffic between VPN sites is purely internal network traffic and fails to meet the requirement that a CSF inspects incoming or outgoing traffic.

The same reasoning applies here. Chandra considers transmitting and receiving CEs connected via VPN to be part of the same network 102. Ex. 2005, 42:11-43:5; Ex. 2004, ¶96. Under that view, even though the

transmitting and receiving CEs are physically remote from each other, they are *virtually* in the same network and only cooperate to process traffic within the same network 102. Thus, they do not cooperate to “inspect *incoming and/or outgoing network traffic*,” as required of a “cooperative network security fabric.” Ex. 2004, ¶96.

Even if traffic received over a VPN connection is considered “incoming and/or outgoing network traffic,” then that traffic is inspected on each end by just a single transmitting or receiving CE, and thus does not constitute multiple cooperating network security appliances. Ex. 2004, ¶97. Accordingly, regardless of how Chandra’s disclosure is viewed, Chandra lacks a “cooperative security fabric” as defined by the ’825 patent. Ex. 2004, ¶97.

B. Dependent Claims 2, 4, 15: Chandra does not disclose “local network policies”

Dependent claims 2 and 4 and independent claim 15 recite that network security operations are executed “based on local network policies.” But nowhere in Chandra does it disclose that network actions are taken based on local policies, and Petitioner provides no support for its contention that “[a] POSITA would find it obvious that Chandra contained two sets of local

policies: one local to receiving CE and another local to transmitting CE.” Pet. 38; Ex. 2004, ¶¶98-101.

Chandra does not disclose that network actions are performed according to policies that are local to the endpoint. Ex. 2004, ¶99. Chandra discloses that when a receiving CE receives a labeled data packet, it will forego performing a “first set of actions” that were already performed by a transmitting CE. *See, e.g.*, 1004, ¶32. The receiving CE will instead “determine[] a second set of actions” and perform those actions. *Id.* However, Chandra never states that the second set of actions is determined according to a policy that is local to the receiving CE. Ex. 2004, ¶99.

Instead, Chandra discloses that actions are performed according to a **global** policy, or at least, a policy that is shared by endpoints. Ex. 2004, ¶100. Chandra discloses that its system is operating within a network where “policies [are] uniform among all the VPN sites within a VPN.” Ex. 1004, ¶6. Moreover, in the examples provided by Chandra, transmitting CE and receiving CE have the same set of labels and rules. *Id.*, ¶¶51, 53. Chandra, in fact, consistently describes the “second set of actions” performed by receiving CE as a set of actions “that **has to be** performed on the data packet.” *Id.*, ¶¶18, 32, 46, 67. A POSITA would understand this to mean that there is

a global policy that defines which actions must be performed on the data packet. Ex. 2004, ¶100.

Although Petitioner argues that it would be “obvious that Chandra” has policies local to receiving CE and transmitting CE, Petitioner does not cite to anything in Chandra that indicates as such. Ex. 2004, ¶101. Nor does Petitioner assert or provide any rationale for why a POSITA would modify Chandra to use local policies. *Id.* Petitioner states only that “[a] POSITA would find it obvious that Chandra contained two sets of local policies: one local to receiving CE and another local to transmitting CE.” Pet. 38. This is insufficient—this statement provides no explanation as to **why** a POSITA would modify Chandra to use local policies. Petitioner’s conclusory statements are not enough to sustain an obviousness argument in view of Chandra’s lack of disclosure of local policies. *KSR Intern. Co. v. Teleflex Inc.*, 550 U.S. 398, 418 (2007) (“Rejections on obviousness grounds cannot be sustained by mere conclusory statements; instead, there must be **some articulated reasoning with some rational underpinning** to support the legal conclusion of obviousness.”); *Harmonic, Inc. v. Avid Technology, Inc.*, 815 F.3d 1356, 1363 (Fed. Cir. 2016) (“Harmonic’s expert testimony in support of this theory is equally unavailing, adding nothing beyond the conclusory statements in Harmonic’s petition.”).

C. **Dependent Claim 12: Chandra does not disclose or render obvious that flags are carried in “a first packet of a session”**

Claim 12 recites “one or more packets in which the flag is carried comprises a first packet of a session.” Petitioner acknowledges that Chandra does not disclose that Chandra’s labels are carried in a “first packet of a session.” Pet. 43. Petitioner argues that using the first packet is obvious because “including the flag(s) in the first packet would be sufficient.” *Id.* Petitioner then goes on to explain how in a network with only one route between endpoints, “flags in a given session would be redundant after the initial packet [that contains the flags].” *Id.*

Petitioner’s argument fails because Petitioner provides no rationale for including Chandra’s labels in a “first packet of a session” (as opposed to any other packet). Ex. 2004, ¶¶102-103. Including flags in the first packet may be sufficient, but that does not explain *why* a POSITA would do so in the first place. *Id.* An obviousness argument cannot be sustained without “some articulated reasoning with some rational underpinning,” which is sorely lacking in the Petition. *KSR Intern. Co. v. Teleflex Inc.*, 550 U.S. 398, 418 (2007); *Harmonic, Inc. v. Avid Technology, Inc.*, 815 F.3d 1356, 1363 (Fed. Cir. 2016) (“Harmonic’s expert testimony in support of this theory is equally

unavailing, adding nothing beyond the conclusory statements in Harmonic’s petition.”).

Moreover, Chandra is clear that before a data packet containing a label is received, the labels must first be exchanged between transmitting CE and receiving CE, and they must also first authenticate each other. Ex. 1004, ¶34. Thus, the asserted “flag” (*i.e.* Chandra’s labels) is not received by the receiving CE until several other transmissions between transmitting CE and receiving CE are first performed. Ex. 2004, ¶103.

VII. GROUND 2: CHANDRA IN COMBINATION WITH BURUGANAHALLI DOES NOT RENDER OBVIOUS 6-7, 17-18, 23-24, 28-29

The dependent claims challenged in Ground 2 require that the receiving network security appliance either update or remove flags before sending them to a “next network appliance” in the CSF. Chandra, however, only describes coordination between two nodes, and therefore does not describe a “next network appliance.” Ex. 1004, ¶¶31-32; Ex. 2004, ¶104. Indeed, Dr. Franz acknowledged that Chandra’s receiving CE is an “endpoint.” Ex. 2005, 42:24-43:5.

Petitioner provides several arguments that Chandra in view of Buruganahalli renders obvious a “next network appliance participating in the CSF,” each of which are unavailing. Ex. 2004, ¶¶105-13. *First*, Petitioner

cites Buruganahalli's disclosure of processing packets by a sequence of three or more network devices. Pet. 53-54. But Buruganahalli only teaches processing packets along a single sequence of network device 54, followed by network device 52, followed by network device 50. Ex. 2004, ¶106. There are no multiple paths for packets to traverse Buruganahalli's network devices, and those devices are thus not part of a "fabric." This also means that, adding Buruganahalli's network devices to Chandra fails to add "a next network appliance *participating in the* [cooperative security *fabric*]," as claimed. Ex. 2004, ¶106. Petitioner also provides no reason for adding Buruganahalli's additional network devices to Chandra. *Id.*

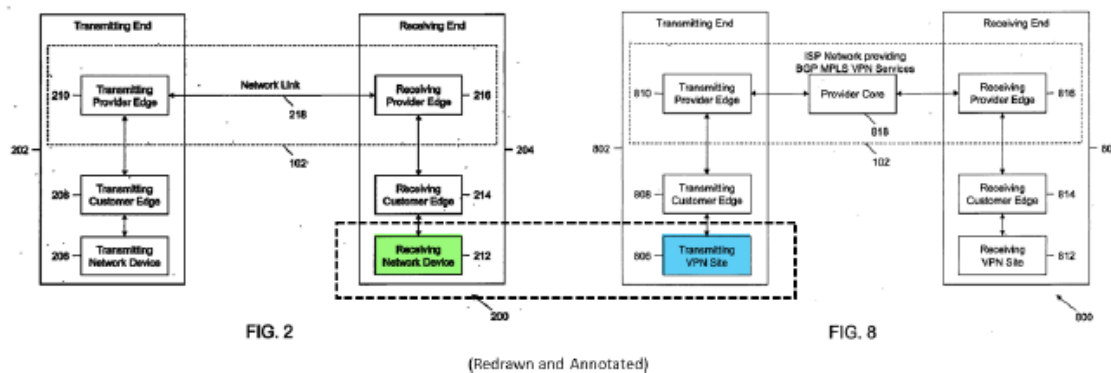
Second, Petitioner relies on Chandra's disclosure that "a plurality of such CEs [could] be associated with a single PE." Pet. 54 (quoting Ex. 1004, ¶28). Chandra, however, does not disclose that the plurality of CEs ever communicate with each other *in seriatim*. Ex. 2004, ¶107. Chandra is clear that a transmitting CE sends a packet to a receiving CE, after which the chain ends. *Id.*; Ex. 2005, 69:15-16 ("Chandra **only** talks about packages going from **one** source to **one** destination."). That multiple CEs may use the same PE to communicate with other CEs does not change the fact that Chandra's communications are only between two CEs. Ex. 2004, ¶107.

Third, Petitioner argues that “receiving CE (214) could transmit the data packet with updated label to receiving network device (212).” Pet. 54. However, “receiving network device (212)” is not a “network appliance participating in the CSF.” Ex. 2004, ¶108. The receiving network device is the destination endpoint for the transmission of data—by contrast, as discussed above, the nodes of a CSF are the components that make up the communication paths **between** endpoints, such as switches, routers, etc. *Id.* In accordance with this plain meaning, the ’825 patent makes a distinction between “network appliances” of a CSF and “endpoint devices.” For example, the ’825 patent teaches that “Leaf nodes 250 a-250 d are the network security appliances that are used for connecting endpoint devices of the private network” and that “LAN ports of leaf node are connected to endpoint devices, such as personal computers, servers, laptops, tablet computers, smart phones, printers and etc.” Ex. 1001, 6:1-9.

Similarly, throughout Chandra, there is a distinction between CE’s (which can be “Intrusion Detection Systems (IDSs), firewalls, etc.”) that perform network actions on network data, and “network devices”, which are “personal computers, servers, mobile phones, etc.,” and which send and receive data. Ex. 1004, ¶¶21, 30; Ex. 2004, ¶109. Thus, Chandra never discloses that “network devices” perform any network actions on network

data. Indeed, Chandra discloses that the receiving CE performs all remaining actions “that ha[ve] to be performed on the data packet.” Ex. 1004, ¶32. The “receiving network device” therefore does not perform any actions on the data packet and is not an appliance that is part of the CSF, or cooperating with other appliances. Ex. 2004, ¶109.

Fourth, Petitioner argues that “a POSITA would have found it obvious that Figure 8’s VPN could be attached as an extension of Figure 2’s private network,” and provides the below modified Figures. Ex. 2004, ¶110.



Petitioner, however, 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. Ex. 2004, ¶111. Chandra clearly describes that in its system, there is a transmitting CE and a receiving CE without any indication that it would be beneficial to involve additional CE’s and network devices as Petitioner proposes. *Id.* Moreover, in Chandra’s

system, the CE's have to authenticate and exchange labels before data is transmitted between them. Ex. 1004, ¶¶33-34. Adding additional CE's would require an exponential increase in the exchange of such data—in Petitioner's proposed combination, Figure 2's transmitting CE would need to exchange labels not only with Figure 2's receiving CE, but also both Figure 8's transmitting and receiving CE; Figure 2's receiving CE would need to exchange labels with Figure 8's transmitting and receiving CE's, *etc.* Ex. 2004, ¶111. Instead of one exchange as described in Chandra, Petitioner's proposal would involve *six* exchanges of labels, which is far less efficient. *Id.*

The more reasonable conclusion to be drawn from Chandra is that transmitting provider edge 810 already acts as a gateway to the transmitting network device. Ex. 2004, ¶112. In other words, if transmitting network device 206 were to transmit data to receiving VPN site 812, it would be able to do so directly through transmitting provider edge 810, rather than first going through transmitting provider edge 210 and receiving provider edge 216. *Id.* Since Chandra already configures a single transmitting CE and a single receiving CE to perform all necessary actions, there is no need in Chandra for the same traffic to traverse an additional two CEs as proposed by Petitioner (receiving CE 214 and transmitting CE 808). *Id.* Doing so, as proposed in Petitioner's combination, only leads to inefficiencies. *Id.*

For these reasons, Chandra does not disclose or render obvious a “next network appliance participating in the CSF.” Ex. 2004, ¶113.

VIII. GROUND 3 AND 4: PETITIONER FAILS TO ESTABLISH THAT CHANDRA IN COMBINATION WITH OTHER REFERENCES RENDER OBVIOUS CLAIMS 10-11, 13-14, 19-20, 25-26, AND 30-31

Grounds 3 and 4 of the petition rely on Chandra for the same limitations discussed in Section VI. Accordingly, these Grounds should be rejected for the same reasons. Ex. 2004, ¶114.

IX. GROUND 5: KEOHANE DOES NOT RENDER OBVIOUS CLAIMS 1-5, 12, 15-16, 21-22, 27

Petitioner fails to establish that Keohane renders claims 1-5, 12, 15-16, 21-22, and 27 obvious because Keohane does not disclose a “cooperative security fabric,” whose plain meaning requires “network security appliances that cooperate to inspect incoming and outgoing traffic along multiple interconnected paths.” Keohane instead discloses a single communication path (i.e., a single thread rather than a fabric) that only handles traffic coming into a network. Ex. 2004, ¶115.

A. Independent Claims 1, 15, 21, 27: Keohane does not disclose a “cooperative security fabric”

Ground 5 relies solely on Keohane to establish obviousness. But Ground 5 fails to establish that Keohane 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.” Instead, it is undisputed that Keohane discloses a single path that only processes communications coming into the network. Ex. 2001, ¶¶69-76; Ex. 2004, ¶116.

Petitioner argues that in Keohane, “each participating appliance inserted a signature into a packet to indicate the security operations performed,” and that “[d]ownstream devices ... determined the security operations performed by prior devices., and thus are a “cooperative security fabric.” Pet. 71-72 (citing Ex. 1008, ¶11). But Keohane discloses that firewall (300) and mail gateway (302) are nodes that can only process traffic in one direction. Ex. 2004, ¶117.

Data packet 306 is received by firewall 300. ... [F]irewall 300 allows data packet 306 to be passed to mail gateway 302. ... Then, data packet 306 is passed to client 304.

Ex. 1008, ¶¶33-37. This is shown, for example, in Figure 3 of Keohane, as annotated by Petitioner below:

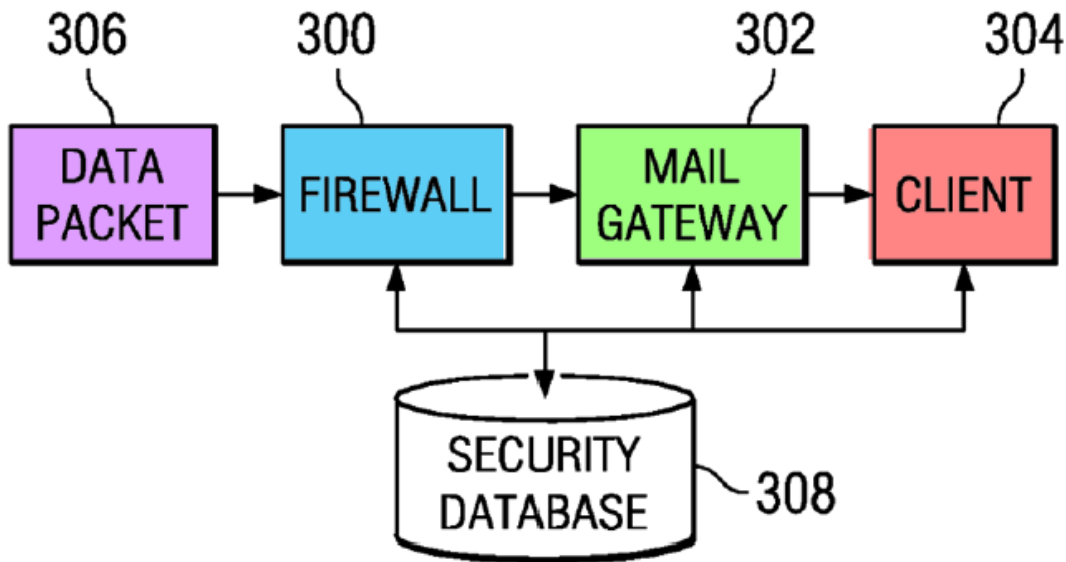


FIG. 3
(Annotated)

Ex. 1008, Fig. 3 (annotated); Ex. 2004, ¶73. As shown in the figure, the data packet 306 only flows in one direction along a single path, with firewall 300 acting as a dedicated data transmitter to mail gateway 302, which acts as a dedicated data transmitter to client 304. Ex. 2004, ¶119. The coordination between these nodes only occurs for data that originates outside of the firewall and only along one path. *Id.*

Dr. Franz confirmed that in Keohane, a packet is “first received by firewall 300” and then forwarded to “mail gateway 302,” and that this flow is “illustrative to the specific method that is described in [Keohane].” Ex. 2005, 59:3-12. Dr. Franz also confirmed that Keohane does not disclose “what else

is happening in this network” besides this unidirectional flow along a single path. *Id.*; Ex. 2004, ¶120.

Cooperation 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. Rather than a series of interconnected paths, the very thing that necessitated the use of a CSF, Keohane only describes a single, unidirectional path. Ex. 2004, ¶121. Keohane also only describes inspecting incoming network traffic—there is no disclosure that Keohane’s Mail Gateway and Firewall cooperate to inspect outgoing network traffic. *Id.*

Accordingly, Petitioner’s Ground 5 should be rejected because Keohane fails to disclose a “cooperative security fabric” under its plain meaning. Ex. 2004, ¶122.

B. Dependent Claim 4: Keohane does not disclose or render obvious a first network security appliance that receives traffic “not transmitted from the second network security appliance”

Claim 1 recites a “first network security appliance” that receives network traffic, and can determine that the network traffic was transmitted by a “second network security appliance.” Claim 4 further requires that the first network security appliance can determine that the network traffic is “not

transmitted from the second network security appliance,” and if it is not, executing security operations specified by a local policy. Ex. 2004, ¶123.

Keohane does not disclose or render obvious this limitation because none of its alleged network security appliances can both determine that traffic is from another network security appliance and determine that traffic is not from another appliance. Ex. 2004, ¶124.

Petitioner alleges for claim 1 that Keohane’s “mail gateway (302)” is a “first network security appliance.” Pet. 69. However, Keohane discloses that the mail gateway always receives data from the firewall, which Petitioner alleges to be the “second network security appliance.” Ex. 1008, ¶34, Fig. 3; Pet. 74. Thus, Keohane’s mail gateway will never determine that the traffic did **not** come from another network security appliance and therefore does not disclose claim 4. Ex. 2004, ¶125.

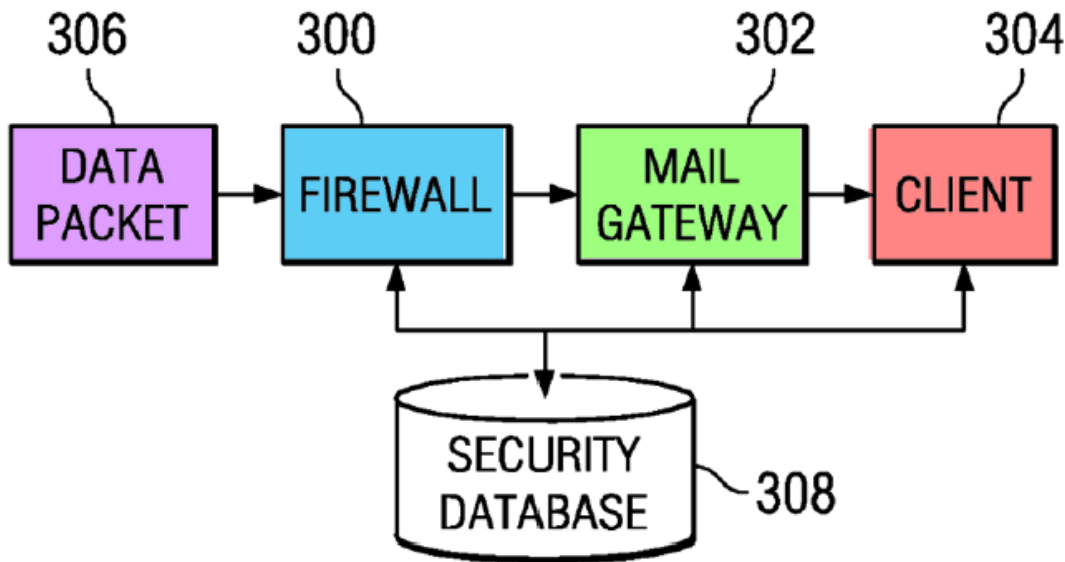


FIG. 3
(Annotated)

Petitioner also alleges that “the first network security appliance could also be any network appliance in the appliance chain (e.g., client (304)) that received network traffic.” Pet. 71. However, client 304 has the same issue—it only receives traffic from the mail gateway, an alleged network security appliance. Ex. 2004, ¶126. Client 304 can never determine that traffic did not come from another network security appliance. *Id.*

If firewall 300 is the alleged first network security appliance, then the opposite problem occurs. Ex. 2004, ¶127. Firewall 300 never receives traffic from an alleged network security appliance. *Id.* As a result, it cannot perform claim 1’s determination that the network traffic came from a second network security appliance, nor perform the steps that follow such a determination. *Id.*

Although Petitioner relies on step 706 of Figure 7, which determines the presence of a signature header, such a determination does not determine if the traffic was or was not “transmitted by an upstream device” as Petitioner claims. Pet. 85. This is because the signature only indicates “that a previous security action has been performed on the data packet.” Ex. 1008, ¶32; Ex. 2004, ¶128. The lack of a signature could simply mean that the upstream device did not perform any security action—not that it did not come from an upstream device. Ex. 2004, ¶128.

C. Dependent Claim 12: Keohane does not disclose or render obvious that flags are carried in “a first packet of a session”

Petitioner acknowledges that Keohane does not expressly disclose claim 12. However, Petitioner argues that claim 12 is obvious for the same reasons discussed in Ground 1 with respect to Chandra. Petitioner’s arguments therefore fail for the same reasons discussed above in Section VI.C. Ex. 2004, ¶130.

X. GROUND 6: KEOHANE IN COMBINATION WITH BURUGANAHALLI DOES NOT RENDER OBVIOUS CLAIMS 6-7, 17-18, 23-24, 28-29

The claims challenged in Ground 6 require that the receiving network security appliance either update or remove flags before sending them to the next network appliance in the CSF. Keohane does not render these claims

obvious because (1) for claims 6, 17, 23, and 28, a POSITA would not be motivated to use Buruganahalli's updating of tags in Keohane, (2) for claims 7, 18, 24, and 29, a POSITA would not be motivated to remove Keohane's signatures, and (3) Keohane does not disclose a "next network appliance participating in the CSF" and Petitioner provides no explanation for incorporating Buruganahalli's "next network appliance." Ex. 2004, ¶131.

A. Dependent Claims 6-7, 17-18, 23-24, 28-29: Keohane in view of Buruganahalli does not render obvious a "next network appliance"

These claims recite that the receiving network security appliance sends the network packet to a next network appliance that participates in the CSF. Ex. 2004, ¶132. Petitioner argues that "[i]n the Keohane-Buruganahalli combination, a POSITA would incorporate Buruganahalli's disclosure of updating a tag into Keohane's security element updating the signature and transmitting the updated signature to the next security element along the data path." Pet. 94.

However, Keohane's "next security element" is not a "next network appliance." Ex. 2004, ¶133. Under Petitioner's invalidity theory, Keohane's mail gateway in Figure 3 is the claimed "first network security appliance." Pet 74. As depicted in Figure 3, reproduced below, the downstream element

from the mail gateway is “client 304.” However, “client 304” is not a network appliance participating in the CSF. Ex. 2004, ¶133.

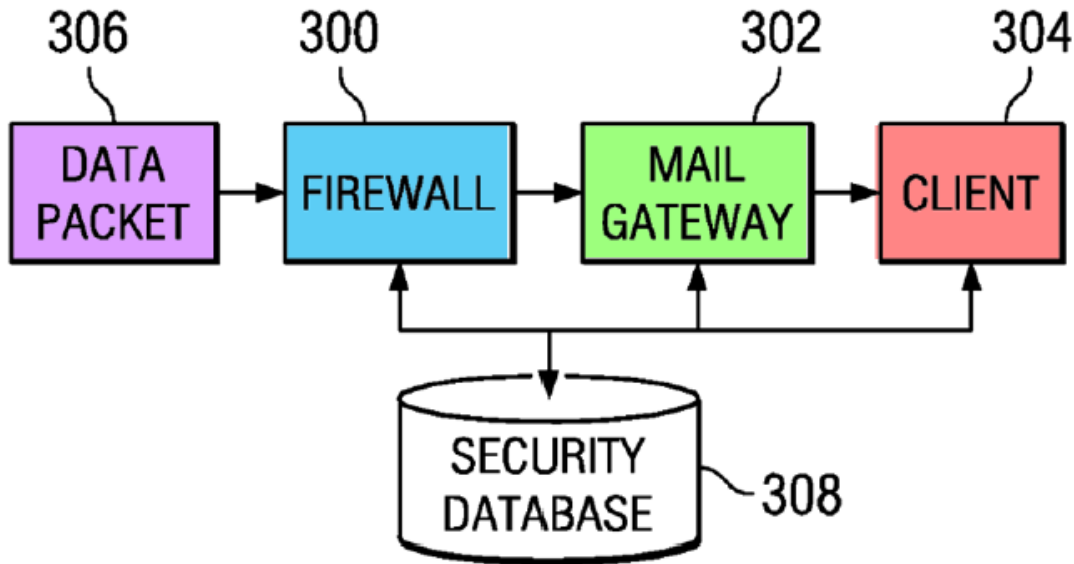


FIG. 3
(Annotated)

Client 304 is the destination endpoint for the transmission of data—by contrast, “network security appliances” are the components that make up the communication paths *between* endpoints, such as switches, routers, etc. Ex. 2004, ¶134. In accordance with this plain meaning, the ’825 patent makes a distinction between “network appliances” of a CSF and “endpoint devices.” For example, the ’825 patent teaches that “Leaf nodes 250 a-250 d are the network security appliances that are used for connecting endpoint devices of the private network” and that “LAN ports of leaf node are connected to

endpoint devices, such as 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,” “servers,” and “clients,” the latter of which are “personal computers or network computers.” Ex. 1008, ¶23. As a result, Keohane’s clients are not network appliances nor are they part of a fabric under its plain meaning. Ex. 2004, ¶135. For these reasons, Keohane does not disclose a “next network appliance.”

In addition, Buruganahalli, like Keohane, only discloses forwarding traffic along a single, unidirectional path of network devices. Ex. 2004, ¶136. Such a single, unidirectional path is not a “fabric,” and thus Buruganahalli also cannot supply the missing “a next network appliance participating in the [cooperative security *fabric*],” as claimed. *Id.*

B. Dependent Claims 6, 17, 23, 28: A POSITA would not be motivated to use Buruganahalli’s updating of tags with Keohane’s signatures

Recognizing that Keohane does not disclose updating signatures from packets, Petitioner argues that “[a] POSITA would have been motivated to add Buruganahalli’s feature of updating the metadata tag to Keohane,” and specifically combining them so that Keohane’s security elements “updated the signature before passing the data packet to the next element instead of adding

a new signature.” Pet. 93. In other words, Petitioner’s proposal is to use Buruganahalli’s teachings to somehow modify the digital signatures embedded by Keohane’s security elements into a data packet. Petitioner’s proposal is flawed because Burganahalli does not teach how to modify digital signatures and making Keohane’s digital signatures modifiable would defeat their purpose. Ex. 2004, ¶137.

Keohane discloses that a “signature from a trusted security element” “is a digital signature.” Ex. 1008, ¶¶34-35. However, a POSITA would have understood that a purpose of a digital signature is to prevent tampering. Ex. 2004, ¶138. This is because the very purpose of a signature is to authenticate that a message truly came from a certain sender—in Keohane’s case, the signature also authenticates which security actions were performed by the sender. *Id.*; Ex. 1008, ¶34. If a signature could be easily altered, then the message could not be authenticated as coming from the sender. Ex. 2004, ¶138.

For example, a well-known, conventional method for signing a message involves using a private-public key pair. Ex. 2004, ¶139. The sender of the message will, for example, derive a hash of the message (*i.e.* using a one-way function that converts any message into an ideally-unique number), and then encrypt the message hash with the sender’s **private key** (a key known

only to the sender). *Id.* The recipient can authenticate the sender and message by decrypting the hash using the sender's **public key** (a key known to the public) and comparing it to the hash of the message calculated by the recipient. *Id.* The recipient knows that the sender truly sent the message because the sender's public key was able to decrypt the hash.

A POSITA would understand that the sender's signature could not be modified. Ex. 2004, ¶140. This is because in order for the signature to indicate that it is the sender's signature, the sender's private key must be used. *Id.* But the sender's private key is not known to anyone but the sender.

If the recipient were to instead sign the message using the recipient's private key, downstream elements would be unable to confirm that the packet came from the original sender, which in Keohane must be a "trusted security element," such as an upstream firewall. Ex. 1008, ¶¶35-36; Ex. 2004, ¶141. Downstream elements would be unable to verify that the packet was first received by a firewall, or to verify that the firewall performed the security actions, such as ensuring that "the data packet 306 has originated from a trusted source." Ex. 1008, ¶34.

Buruganahalli provides no teachings about modifying a digital signature and Petitioner does not explain how such a modification would be performed, or why a POSITA would expect it to succeed. Ex. 2004, ¶142.

Indeed, somehow modifying Keohane to render its digital signatures modifiable, as proposed by Petitioner, would defeat the very purpose of those signatures. *Id.*

For these reasons, a POSITA would not be motivated to look to Buruganahalli to modify Keohane's signatures. Ex. 2004, ¶143.

C. Dependent Claims 7, 18, 24, 29: A POSITA would not be motivated to remove Keohane's signatures

Keohane does not disclose removing signatures from packets. Petitioner argues a POSITA would be motivated to incorporate Buruganahalli's removal of a tag for two reasons, both of which fail. Ex. 2004, ¶144.

First, Petitioner argues that “removing the tag before passing the data packet would keep the network's labeling mechanism private, preventing malicious devices from intercepting the data packet and exploiting the labeling mechanism.” Pet. 95. But Petitioner provides no explanation for how a “malicious device[]” could “exploit[] the labeling mechanism.” Indeed, because Keohane's labeling mechanism uses digital signatures, such exploitation is difficult—the signature ensures that the label was added by a trusted device. Ex. 2004, ¶145.

Moreover, in Keohane, the signatures provide an essential function which a POSITA would not be motivated to remove. Ex. 2004, ¶146. For example, the signatures first indicate that the packet came from “trusted security elements.” Ex. 1008, ¶37. Second, the signatures indicate which security actions have already been performed on the network packet. *Id.* Thus, a firewall’s signature verifies to the client that “the data packet is from a trusted source,” and the mail gateway’s signature verifies that “no viruses were found in the data packet.” *Id.* Not only do these signatures mean the client does not need “to perform a virus scan,” it also allows the client to trust the data packet—a security action that the client cannot itself perform. *Id.* Thus, without the signatures, the client cannot ensure that data packets are trustworthy. Ex. 2004, ¶146.

Second, Petitioner argues that “removing the tag would prevent compatibility issues in subsequent devices that might not be compatible with the proprietary tags.” Pet. 95. Keohane does not disclose that any downstream devices are incompatible with the “proprietary tags.” Ex. 2004, ¶147. Moreover, a POSITA would understand that a downstream device can simply ignore the signatures. *Id.* However, as explained above, Keohane is clear that the signature is essential for a downstream device to verify that the

sender is trusted and that certain security actions were performed. *Id.* Thus, a POSITA would not be motivated to remove the signature.

XI. GROUNDS 7 AND 8: KEOHANE IN COMBINATION WITH OTHER REFERENCES DOES NOT RENDER OBVIOUS CLAIMS 10, 13-14, 19-20, 25-26, AND 30-31

Grounds 7 and 8 of the petition rely on Keohane for the same limitations discussed in Section IX. Accordingly, these Grounds should be rejected for the same reasons. Ex. 2004, ¶148.

XII. CONCLUSION

For the foregoing reasons, Patent Owner respectfully requests that the Petition be denied.

Date: January 11, 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 11,402 words and thus complies with the applicable word limit.

Date: January 11, 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 January 11, 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)
Wei Yuan (yuan-ptab@perkinscoie.com)
Netskope-FortinetIPRTeam@perkinscoie.com

Date: January 11, 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.*