

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

NETSKOPE, INC.,
Petitioner,
v.
FORTINET, INC.,
Patent Owner.

PTAB Case No. IPR2023-00459

Patent No. 10,084,825

**PETITIONER NETSKOPE, INC.'S REPLY TO PATENT OWNER'S
RESPONSE TO PETITION FOR *INTER PARTES* REVIEW
OF U.S. PATENT NO. 10,084,825**

Table of Contents

UPDATED EXHIBIT LIST	III
I. INTRODUCTION	1
II. CORRECTLY CONSTRUING “FABRIC,” THE BOARD FOUND CHANDRA AND KEOHANE TEACH A “COOPERATIVE SECURITY <i>FABRIC</i> ”	1
A. The Board Correctly Construed “Fabric” In “Cooperative Security <i>Fabric</i> .”	2
1. As the Board correctly found, a “fabric” is simply “a network topology.”	2
2. “Cooperative security <i>fabric</i> ” requires devices that form a network topology and work together to coordinate security operations among them.	3
B. Chandra and Keohane Taught a “CSF” Under Its Correct Meaning.	5
1. Chandra	6
2. Keohane	7
III. PO IMPROPERLY TRIES TO IMPORT TWO NEW LIMITATIONS.....	9
A. PO’s Construction Is Riddled with Hidden Limitations.	10
B. PO’s Construction Has No Record Support.....	10
1. Intrinsic Evidence	10
C. Chandra and Keohane Taught “CSF” Even Under PO’s Incorrect Construction.	19
1. Chandra	19
2. Keohane	20
A. Chandra Taught or Rendered Obvious “Local Network Policies” (Claims 2, 4, 15).	23
B. Chandra and Keohane Rendered Obvious Flags That Were Carried In “a First Packet of a Session” (Claim 12).	24
C. Chandra and Keohane Taught or Rendered Obvious “Next Network	

Appliance” (Claims 6, 17, 23, 28) and “Next Network Appliance Participating in a CSF” (Claims 7, 18, 24, 29).	25
1. Chandra	25
2. Keohane	27
D. Keohane Taught or Rendered Obvious a First Network Security Appliance that Received Traffic “Not Transmitted from the Second Network Security Appliance” (Claim 4).....	29
E. A POSITA Would Be Motivated to Use Buruganahalli’s Updating of Tags with Keohane’s Signatures (Claims 6, 17, 23, 28).	30
F. A POSITA Would Be Motivated to Remove Keohane’s Signatures (Claims 7, 18, 24, 29).....	31
V. CONCLUSION.....	32

UPDATED EXHIBIT LIST

Exhibit	Description
Ex. 1001	U.S. Patent No. 10,084,825 to Xu (“the ’825 patent”)
Ex. 1002	Supporting Declaration of Dr. Michael Franz (“Franz”)
Ex. 1003	File History of U.S. Patent No. 10,084,825
Ex. 1004	U.S. Patent Application Publication 2007/0204018 A1 (“Chandra”)
Ex. 1005	U.S. Patent Application Publication 2014/0282843 A1 (“Buruganahalli”)
Ex. 1006	U.S. Patent Application Publication 2009/0144818 A1 (“Kumar”)
Ex. 1007	U.S. Patent Application Publication 2017/0093917 A1 (“Chandra-2”)
Ex. 1008	U.S. Patent Application Publication 2008/0134332 A1 (“Keohane”)
Ex. 1009	Microsoft Computer Dictionary Fifth Edition (2002)
Ex. 1010	U.S. Patent Publication 2006/0156401 A1 (“Newstadt”)
Ex. 1011	U.S. Patent Publication 2007/0237147 A1 (“Quinn”)
Ex. 1012	Declaration of Andrew N. Klein in Support of <i>Pro Hac Vice</i> Admission
Ex. 1013	Wayback Machine Archive of Merriam-Webster on November 26, 2016 (“Ex. 1013”)
Ex. 1014	Wayback Machine Archive of Merriam-Webster on November 17, 2016 (“Ex. 1014”)
Ex. 1015	L. Wang, Cooperative Security in D2D Communications, first online on September 1, 2017 at https://link.springer.com/chapter/10.1007/978-3-319-61863-0_5 (“Ex. 1015”)
Ex. 1016	U.S. Patent No. 10,334,442 (“Ex. 1016”)
Ex. 1017	FotiOS 6.4.0 Administration Guide (2021) (“Ex. 1017”)

Exhibit	Description
Ex. 1018	Deposition Transcript of Dr. John Richard Black (“Black Depo. Tr.”)
Ex. 1019	Rebuttal Declaration of Dr. Michael Franz (“Franz. Reb.”)
Ex. 1020	Dictionary of Computer and Internet Terms, Tenth Edition (2009) (“Ex. 1020”)

I. INTRODUCTION

While the POR suffers from many flaws, the most fatal is PO's attempt to read limitations into the claims to avoid prior art. Before institution, PO argued "fabric" required bidirectional communications. The Board rejected that argument, interpreting that term and finding it satisfied by prior art. Unhappy with the Board's construction, PO makes another attempt at reading limitations into the claims, this time requiring that a "cooperative security *fabric* (CSF)" must inspect "incoming and outgoing traffic" (to avoid Chandra) and have "multiple interconnected paths" (to avoid Keohane). None of these backup limitations find support in the record. Consequently, as explained below, the Board should affirm its preliminary finding that the challenged claims are unpatentable.

II. CORRECTLY CONSTRUING "FABRIC," THE BOARD FOUND CHANDRA AND KEOHANE TEACH A "COOPERATIVE SECURITY *FABRIC*"

In its ID, the Board rejected PO's argument that "fabric" required bidirectional communication, instead finding that the plain meaning only required "a network topology such as the physical structure of a switch or network." (ID, 9.) As detailed below, the Board's interpretation of "fabric" within "cooperative security *fabric*" comport with straightforward, plain meaning of "CSF"—devices that form a network topology and work together to coordinate security operations among them. This interpretation is supported by the words themselves and the intrinsic and

extrinsic evidence. Under that interpretation, both Chandra and Keohane disclosed a “CSF,” as the Board preliminarily found.

A. The Board Correctly Construed “Fabric” In “Cooperative Security *Fabric*.”

1. As the Board correctly found, a “fabric” is simply “a network topology.”

In the ID, the Board construed “fabric” as “a network topology such as the physical structure of a switch or network.” (ID, 9; *see also id.*, 28 (“‘fabric’ of a CSF [is] a network topology that connects network devices to perform security actions”).) While the Board’s decision is supported by extensive evidence, Petitioner highlights the below.

First, the Board relied on a definition of “fabric” as “[a] descriptive term referring to the physical structure of a switch or network.” (*Id.*, 9.) That definition comports with the Dictionary of Computer and Internet Terms (10th Edition)’s definition of “fabric” as simply “network interconnections.” (Ex. 1020, 185; Franz Reb., ¶11.)

Second, PO’s own expert supports the Board’s interpretation. For example, Dr. Black opines that, as enterprises grew, “a fabric of network devices (such as switches or access points for each subnetwork) was developed to manage network traffic between subnetworks, and to and from the Internet.” (ID, 9 (citing POPR,

10).) Dr. Black agrees that “fabric” can refer to the “physical structure of a [network] topology.” (Black Dep., 77:6-8.)

Finally, Petitioner’s expert, Dr. Franz¹, agrees that the Board’s construction comports with the term’s customary use. (Franz Reb., ¶11; Franz Dep. Tr., 7:8-23, 26:16-17.)

Given this unanimity, the Board correctly construed “fabric.”

2. “Cooperative security *fabric*” requires devices that form a network topology and work together to coordinate security operations among them.

The plain meaning of “cooperative security fabric” flows from “fabric”: devices that form a network topology and work together to coordinate security operations among them. This is supported by the words themselves, the specification, and extrinsic evidence.

a. Claims

Claim construction begins and ends with the claims. *Interactive Gift Exp., Inc. v. Compuserve Inc.*, 256 F.3d 1323, 1331 (Fed. Cir. 2001). A claim term’s ordinary meaning “may be readily apparent even to lay judges, and claim construction in such cases involves little more than the application of the widely accepted meaning of

¹ PO questions Dr. Franz’s experience with the ’825 patent’s technology, but Dr. Franz qualifies as a POSITA. (Franz Reb., ¶5-10.)

commonly understood words.” *Phillips v. AWH Corp.*, 415 F.3d 1303, 1314 (Fed. Cir. 2005); *see also Malvern Panalytical Inc. v. TA Instruments-Waters LLC*, 85 F.4th 1365, 1372 (Fed. Cir. 2023) (finding it appropriate to construe a phrase by looking to its constituent words).

Here, “CSF” is easily understood by the ordinary usage of its individual words. In addition to “fabric” which refers to “a network topology,” Merriam-Webster defines “cooperative” as “marked by a willingness and ability to work with others (Ex. 1013),” and “security” as “measures taken to guard against espionage or sabotage, crime, attack, or escape (Ex. 1014).” Therefore, “cooperative” refers to the network appliances working together and “security” refers to security measures/operations against attacks. Combining these well-understood terms, a POSITA would have understood the plain meaning of “CSF” as devices that form a network topology and work together to coordinate security operations among them. (Franz Reb., ¶12-13; *see also* Franz Dep., 7:13-15.)

This plain meaning is consistent with the independent claims, which describe a first network security appliance in a CSF receiving network traffic, determines whether the traffic is from a second network security appliance in the CSF, determines the security operations executed on the traffic by the second network security appliance, and executes security operations based on the security actions already executed. (*See* ’825 patent, cls. 1, 15, 21, 27.) Thus, the claims require two

network security appliances in a CSF working together to coordinate security operations performed on received network traffic. (Franz Reb., ¶14.)

b. Specification

The specification also supports this plain meaning. According to the '825 patent, multiple network security appliances historically could perform redundant security actions on network traffic. ('825 patent, 1:52-56, 64-67.) The patent believed “there is a need for a cooperative security fabric (CSF) that may coordinate operations performed on network traffic to avoid or reduce redundant operations among members of the CSF.” (*Id.*) To accomplish that, a first network security appliance in a CSF receives network traffic, determines whether the traffic is from a second network security appliance in the CSF, determines the security operations executed on the traffic by the second network security appliance, and determines local security operations. (*Id.*, 2:5-14.) In other words, two network security appliances in a CSF work together to coordinate security operations performed on received network traffic. (Franz Reb., ¶15.)

B. Chandra and Keohane Taught a “CSF” Under Its Correct Meaning.

Both Chandra and Keohane taught devices that form a network topology and work together to coordinate security operations among them. (Petition, 26-27, 71-72.)

1. Chandra

Chandra taught a setup “consist[ing] of a transmitting end (202) and a receiving end (204), each of which included a network device (206, 212), a Customer Edge (CE) (208, 214), and a Provider Edge (PE) (210, 216).” (Petition, 20.) Network link (218) connected transmitting end (202) and receiving end (204).

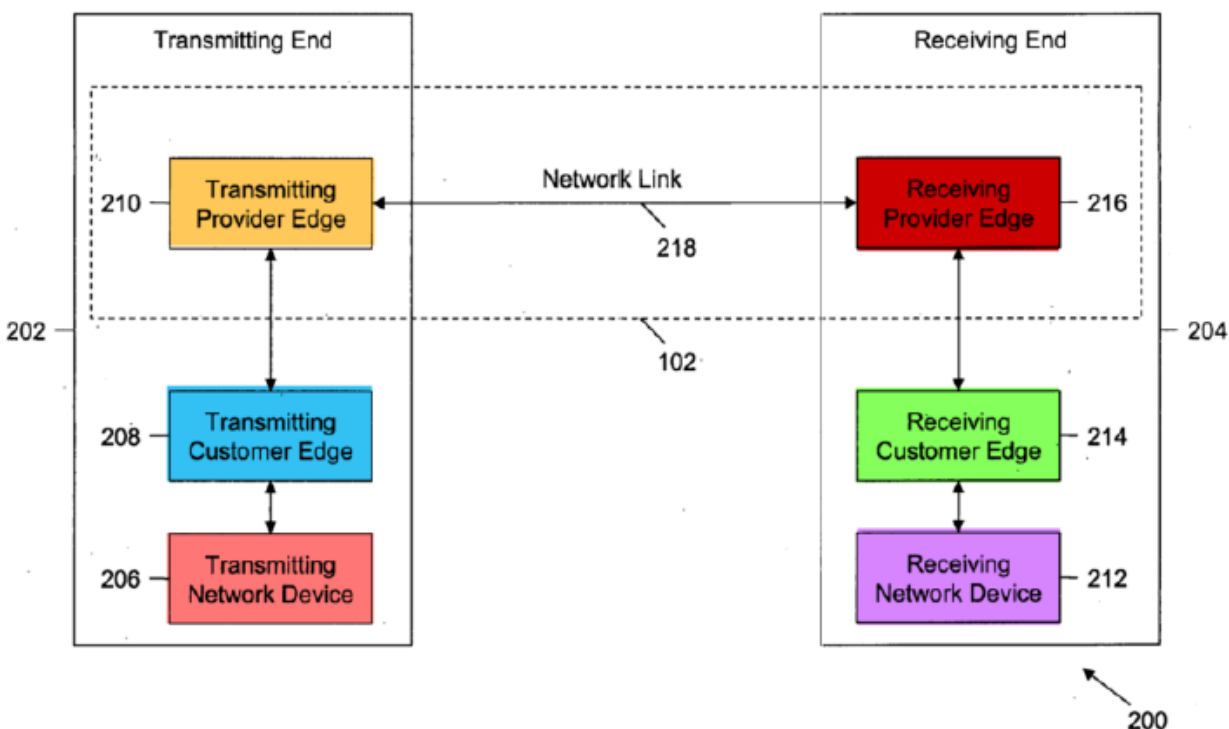


FIG. 2 (Annotated)

This teaches a “fabric,” as it illustrated the network topology containing the two ends, laying out the physical structure including the network devices, customer edges, provider edges, and network link. As shown by the double-ended arrow, network traffic traveled in both directions between transmitting end 202 and receiving end 204 through network link 218. “[T]ransmitting end 202 and receiving end 204 can be any identifiable part or region of network 102,” and any network device of

network 102 “can act both as transmitting network device 206 and receiving network device 212.” (Chandra, ¶29, 56; Franz Reb., ¶16-17.)

Chandra’s fabric was a “CSF” because members (e.g., receiving CE (214) and transmitting CE (208)) worked together to coordinate security operations. (Petition, 26-27.) As the Board found, “Chandra discloses that transmitting and receiving CEs” “participat[ed] in a CSF” “to coordinate actions.” (ID, 16.) The Board reasoned that “transmitting and receiving CEs...authentica[ed] themselves to one another as participants in a CSF, so receiving CE 214 can determine that network traffic was transmitted by transmitting CE 208 participating in the same CSF.” (*Id.*) “[CE] labels indicated to the receiving CE 214 that the network traffic was transmitted by transmitting CE 208 in the same CSF for distributed enforcement of rules to coordinate actions and reduce redundancy.” (*Id.*) Thus, as the Board preliminarily found, Chandra disclosed a “CSF.” (Franz Reb., ¶18.)

2. Keohane

Keohane taught a “multi-level security system...includ[ing] a data packet (306), firewall (300), mail gateway (302), client (304), and a security database (308).” (Petition, 65-66.)

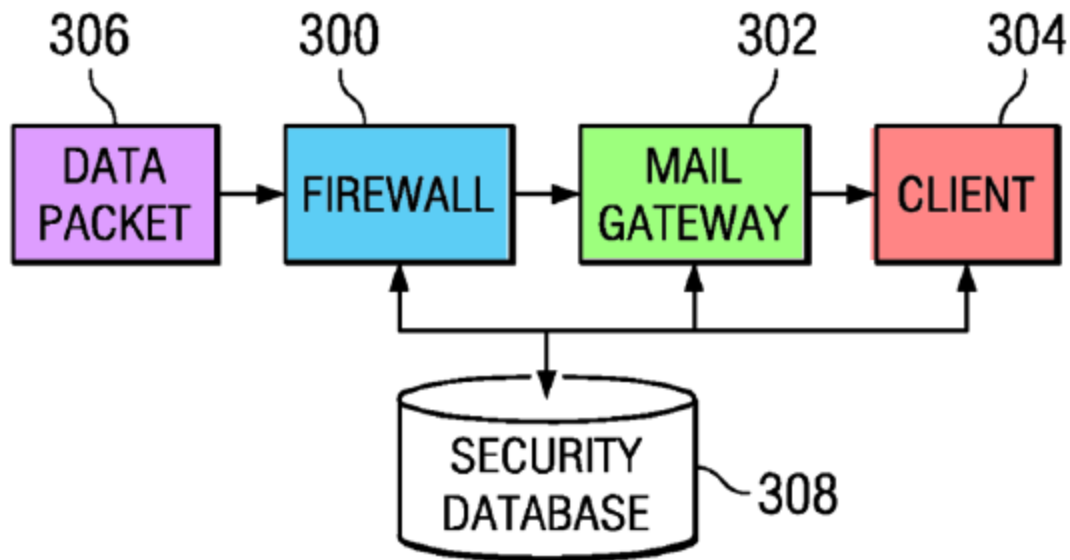


FIG. 3
(Annotated)

This was a “fabric,” as it illustrated the network topology, laying out the physical structure including the security appliances, client, security database, and the connectivity therebetween. (Franz Reb., ¶19-20.)

Keohane’s fabric was a “CSF” because members (e.g., firewall 300, mail gateway 302, client 304) worked together to coordinate security actions among them. (Petition, 71-72.) As the Board preliminarily found, “Keohane’s multilevel security system of...firewall 300, mail gateway 302, and client 304 is configured to perform security actions as a CSF.” (ID, 30.) “Signatures are added to data packet 306 to indicate the packet is sent by a trusted [member] of the CSF [and] the action performed” so the CSF members could coordinate security actions among them. (*Id.*, 31.) For example, “[w]hen client device 304 receives a data packet 306 with

signatures from firewall 300 and mail gateway 302, it recognizes, based on the signatures, that the packet is from trusted devices in the CSF [and] only performs” security actions that were not performed by the upstream devices. (*Id.*) Thus, as the Board preliminarily found, Keohane disclosed a “CSF.” (Franz Reb., ¶21.)

III. PO IMPROPERLY TRIES TO IMPORT TWO NEW LIMITATIONS

Because the Board rejected PO’s construction of “fabric,” PO now tries again to evade prior art by reading not one *but two* limitations into “CSF”. Specifically, PO contends “CSF” must inspect incoming and outgoing traffic (to avoid Chandra) and have multiple interconnected paths (to avoid Keohane). As explained below, PO’s unduly narrow construction—which contradicts the Board’s construction of “fabric”²—is unsupported by the record. And, even if the Board adopted PO’s improper construction, both Chandra and Keohane still disclosed “CSF.”

² For example, requiring “incoming and outgoing traffic” contradicts the Board’s decision that “fabric” does not require bidirectionality. (ID, 30). The Board’s construction is also not limited to PO’s “complex topology” of “multiple interconnected paths.” PO’s argument that “fabric” is a specific type of topology (POR, 14) contradicts the Board’s finding that “fabric” refers to “a network topology” generally.

A. PO's Construction Is Riddled with Hidden Limitations.

Before addressing the lack of support for PO's construction, Petitioner wishes to note that PO's construction contains several hidden limitations:

1. "CSF" *cannot* inspect internal network traffic, i.e., traffic from one part of the network to another. (POR, 20; Black Depo. Tr., 33:11-15.)
2. "CSF" only processes traffic transmitted *from the Internet* into the network and from the network *to the Internet*. (POR, 20; Black Depo. Tr., 70:10-13.)
3. "CSF" requires *three or more* interconnected security appliances. (Black Depo. Tr., 19:2-7.)
4. "Fabric" requires multiple data paths that cannot all share a starting point and endpoint. (Black Depo. Tr., 15: 5-21; 21:16-22.)
5. "CSF" cannot be "a single thread." (POR, 12.)
(Franz Reb., ¶22-26.)

B. PO's Construction Has No Record Support.

1. Intrinsic Evidence

a. Claims

While PO started its claim construction analysis in the wrong place (the specification), Petitioner properly begins its analysis with the claims.

As Dr. Black admits, the claims nowhere require "CSF" to inspect only

“incoming and outgoing traffic” or have “multiple interconnected paths.” (Black Depo. Tr., 35:11-14, 37:5-11.) Rather, the claims only require two appliances and traffic to go from one appliance to the other. None of PO’s additional limitations finds support in the claims. (Franz Reb., ¶27.)

b. Specification

The specification does not require “CSF” to “inspect incoming and outgoing traffic along multiple interconnected paths.” Indeed, PO’s analysis of the “specification” consists of Dr. Black’s extrinsic opinions or citations to the background and exemplary embodiments.

PO imports limitations from the background that do not describe the invention. For example, while PO asserts that “in a network fabric, where there are many different paths of network appliances for traffic to [sic] ‘[n]etwork traffic transmitted to/from the network may go through multiple network security appliances along a path within the network (POR, 15 (quoting ’825 patent, 1:33-37)),” the background does not mention a “network fabric” with “many different paths.” Instead, the background undermines PO’s argument by describing “multiple network security appliances along *a* path.”³ Similarly, while the background generally describes “a large network” with “network traffic transmitted to/from the network,” (’825 patent,

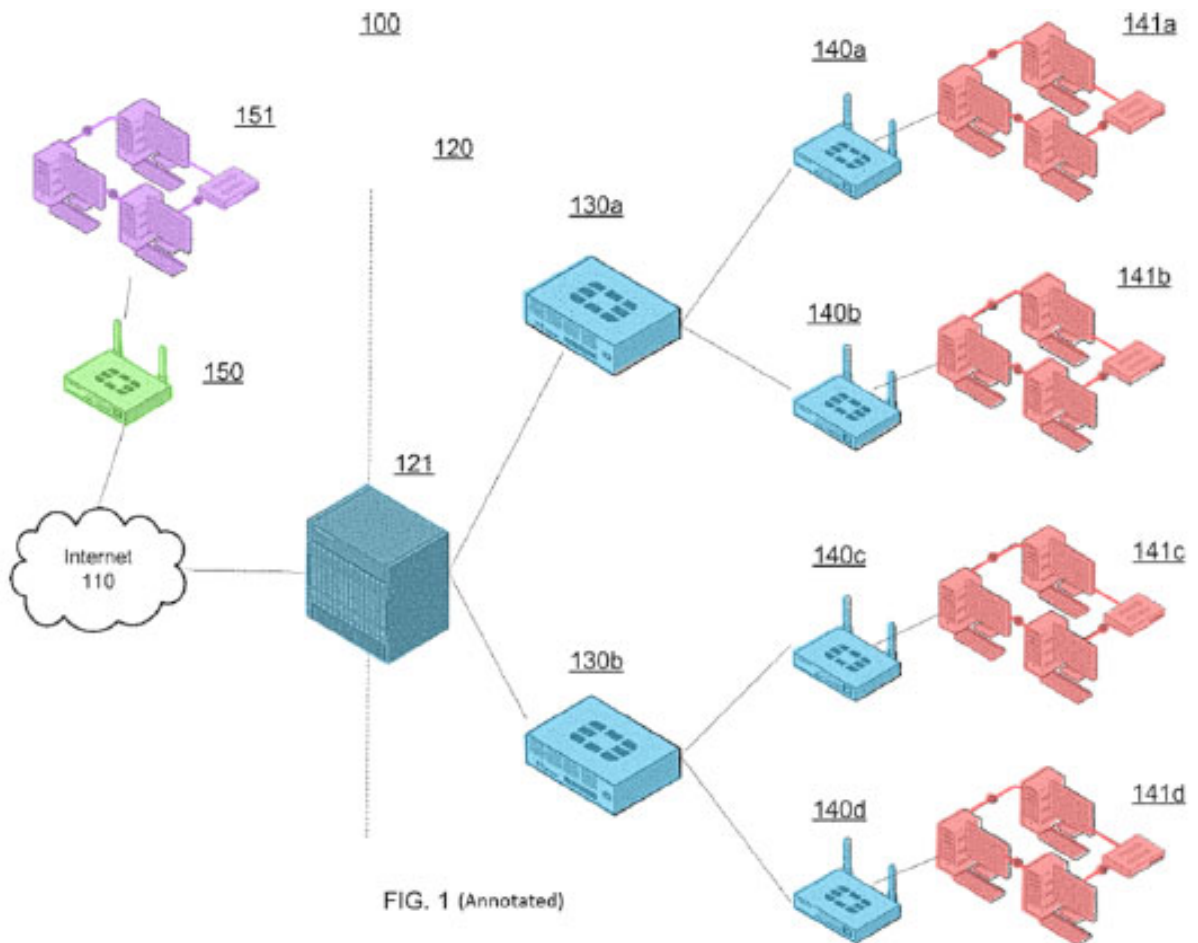
³ Emphases added by Petitioner unless otherwise specified.

1:33-35), PO unjustifiably reads processing “network traffic transmitted to/from the network” as part of the claimed “CSF.” (POR, 15-16; Franz Reb., ¶28.)

PO also tries to limit “CSF” to exemplary embodiments even though doing so flouts settled caselaw, *Woods v. DeAngelo Marine Exhaust, Inc.*, 692 F.3d 1272, 1284 (Fed. Cir. 2012) (ruling against reading a limitation into claim term “merely because it is disclosed in some embodiments”), and the specification, ’825 patent, 10:49-51 (“it will be clear that the invention is not limited to these embodiments only”). (Franz Reb., ¶29.)

The specification does not limit “CSF” to inspecting Internet traffic or exclude inspection of internal traffic. Nor does it limit “CSF” to a specific type of topology with multiple paths. Instead, it teaches that a CSF “may coordinate operations performed on *network traffic* (’825 patent, 1:65-66)” without any modifier before “network traffic,” and that a CSF can be flexibly composed. (Franz Reb., ¶30.)

One embodiment, illustrated below and described in the Petition (Petition 11-13), shows “CSF” can process internal network traffic.



As PO agrees, subnet 151 connects to private network 120 via VPN over Internet 110, making it part of private network 120. So, communication from subnet 151 to the CSF is internal network traffic. (POR 19-20.) The patent does not preclude “CSF” from processing VPN traffic, or traffic from one subnet (e.g., 141a) to another (e.g., 141d). In fact, so limiting the “CSF” makes no sense. A POSITA would find it obvious that various situations require the inspection of internal network traffic to prevent malware. (Franz Reb., ¶31.)

Other embodiments indicate “CSF” can be flexibly composed. Figure 2 illustrates an exemplary CSF topology. The specification explains that “topology 200 may consist of other combinations of root, branch and leaf nodes.” (’825 patent, 6:14-16.) A member network security appliance of the CSF can be “a branch node and a leaf node in the same time.” (*Id.*, 6:26-27.) For example, “[t]opology 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.” (*Id.*, 18-20.) Petitioner annotated Figure 2 to illustrate such direct connection of leaf node 250 to root node 220. (Franz Reb., ¶32.)

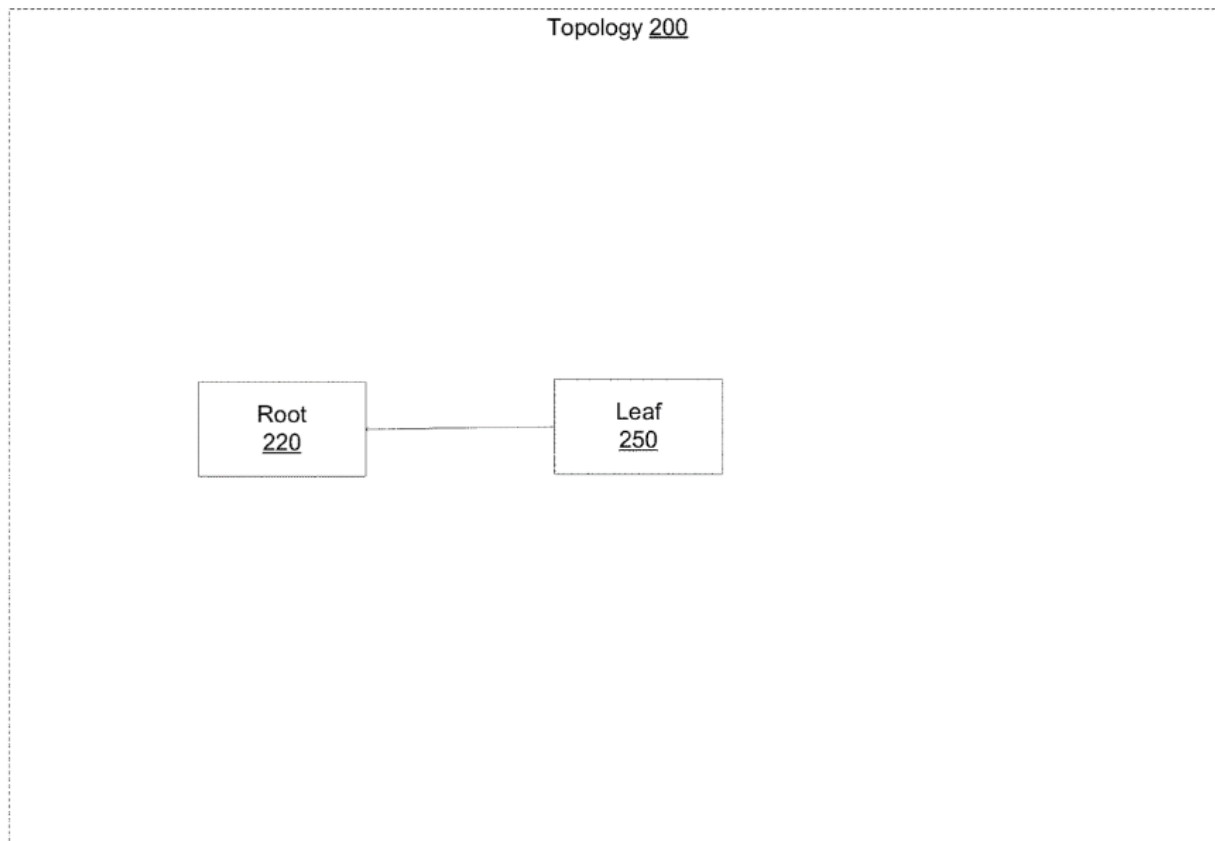


FIG. 2 (Edited)

Thus, the specification undermines PO's construction.

c. Provisional Application

Finally, PO's construction contradicts the provisional application—incorporated by reference ('825 patent, 1:5-10)—for at least two reasons.

First, the provisional expressly states that "CSF" can have a *single* device. The provisional describes that a network security device (NSD) "may initially represent *a CSF containing only one member.*" (Ex. 2016, ¶26.) Thus, the provisional contradicts PO's requirement of three or more appliances (Black Depo.

Tr., 19:2-7) and “multiple interconnected paths.” (Franz Reb., ¶33-34.)

Second, the provisional expressly recites that a CSF of *two* or three devices can be arranged in a line.

The provisional application teaches a CSF where “[t]unnel based communication module [] establishes tunnels between NSD [] and its parent, *if any*, and each of its children, *if any*.” (Ex. 2016, ¶41.) “In general, when an upstream NSD queries a downstream NSD, the query is passed from...the upstream NSD...to...an intermediate NSD, *if any*, ...and ultimately to the destination NSD.” (*Id.*, ¶31.) Therefore, “CSF” can have two NSDs with tunnel-based communication between them and no intermediate NSD. Such CSF does not require three or more security appliances or “multiple interconnected paths.” (Franz Reb., ¶35-36.)

The provisional also recites a CSF “in a form of a tree, having a plurality of nodes, including *a* root node, *one or more* intermediate nodes and *one or more* leaf nodes.” (Ex. 2016, cl. 1; *see also, id.*, ¶18 (“each node of the CSF, except a root node of the CSF and leaf nodes of the CSF, has *one* parent node and *one or more* child nodes”).) Therefore, in a CSF with one each of root node, intermediate node, and leaf node, tunnel-based communication connects the root and intermediate nodes, and the intermediate and leaf nodes. This undermines PO’s argument that “CSF” cannot be one single thread (POR, 12). (Franz Reb., ¶37.)

d. Extrinsic Evidence

Extrinsic evidence also undermines PO's construction. None of PO's citations limit the scope of "CSF" and other extrinsic evidence contradicts PO's construction.

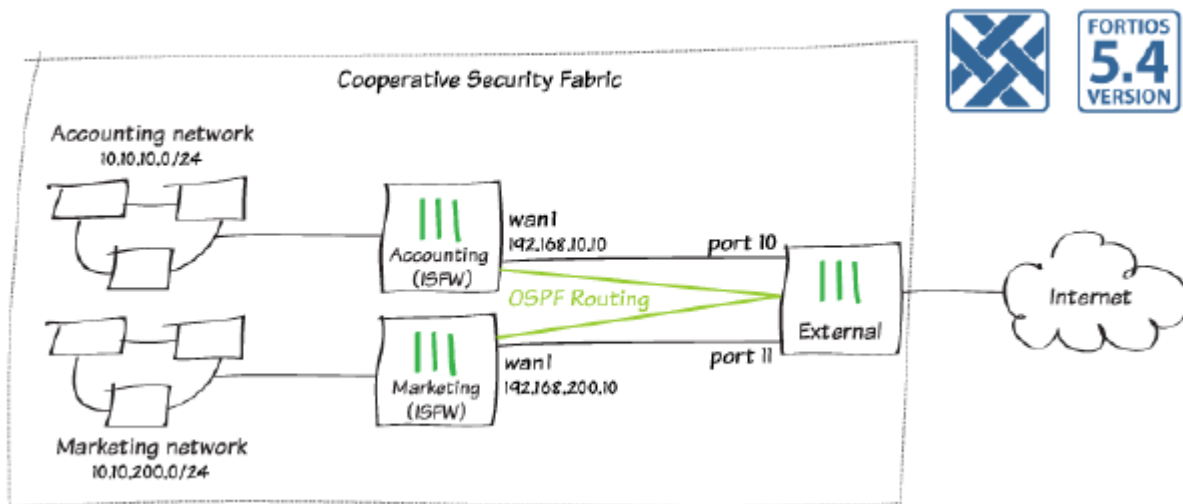
PO attempts to import limitations from its alleged product literature about "CSF." Setting aside whether those limitations exist in the literature (they do not), none of them are disclosed in the intrinsic record. Notably, while the specification identifies various Fortinet "network appliances" ('825 patent, 4:16-42), it never mentions Fortinet's "cooperative security fabric" product. There is simply no indication that the plain and ordinary meaning of "CSF" as used in the '825 patent is dictated by Fortinet's extrinsic documentation. (Franz Reb., ¶38.)

Unrelated to Fortinet products, the term "cooperative security" was well-known in the art around the '825 patent's priority date. It described cooperative behavior between network nodes for security risk avoidance in device-to-device communication⁴ and cooperative behavior between wireless nodes to detect

⁴ See Ex. 1015 (L. Wang, *Cooperative Security in D2D Communications*, first online on September 1, 2017 at https://link.springer.com/chapter/10.1007/978-3-319-61863-0_5).

unsecure nodes⁵. Thus, PO's product literature is far from the best guide to understand the term. (Franz Reb., ¶39.)

But even PO's literature undermines its construction. For example, Ex. 2013 shows the possibility of inspecting internal network traffic as it disclosed "OSPF routing" between the FortiGate of the accounting network and the marketing network. This shows the possibility for the CSF to handle *internal* traffic from the accounting network to the marketing network, and vice versa. (Franz Reb., ¶40.)

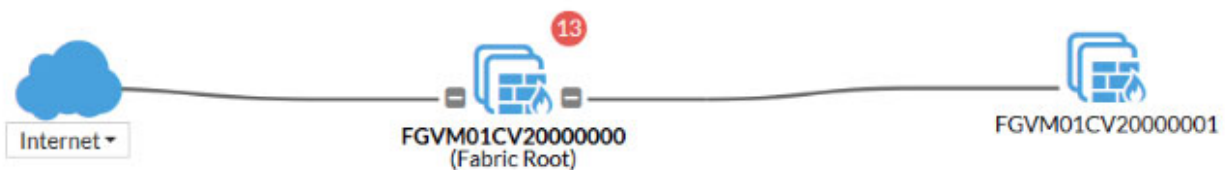


(Ex. 2013, 1.)

Another Fortinet document (FortiOS Administration Guide) shows a typical Fortinet "Security Fabric," which disclosed a CSF with only two nodes (two FGVMs)

⁵ See Ex. 1016 (U.S. Patent No. 10,334,442, "Cooperative Security in Wireless Sensor Networks").

connected via a single path:



(Ex. 1017, 117.) As the Board can see, there were no “multiple interconnected paths” in this CSF. (Franz Reb., ¶41.)

PO’s other extrinsic evidence does not support its construction, either. If we adopted Ex. 2003’s definition of “fabric” as “consist[ing] of *multiple, interwoven* communications paths/channels...much like [] clothing (POR 26-27) (emphasis in original)”, ’825 patent Fig. 2’s tree-shaped “CSF” would not fit this definition. Conversely, Exhibits 2006, 2007 and 2010 all referred to “fabric” in fields that were not directly related to the ’825 patent’s subject matter and did not lend insight into “CSF” as claimed. (Franz Reb., ¶42-47.)

C. Chandra and Keohane Taught “CSF” Even Under PO’s Incorrect Construction.

1. Chandra

PO contends Chandra’s CSF lacked only “inspection of incoming and outgoing traffic (POR, 35),” which PO interprets to mean inspection of Internet traffic, as explained in III.A.

PO acknowledges that Chandra disclosed receiving and inspecting Internet traffic. As the POR points out, “when receiving CE 214 receives a data packet from

the Internet, it performs actions corresponding to rules regarding such data packets.” “[R]eceiving end can identify a data packet from the Internet as insecure, and perform rigorous actions on it.” (POR 36-37 (quoting Chandra ¶53, 77); *see also* Petition, 41.)

While PO contends this disclosure does not meet its construction (*id.*, 37), the claims say otherwise. Claim 1 recites a first network security appliance and a second network security appliance in the same CSF coordinating security operations between them. (’825 patent, cl. 1.) Dependent claim 4 then recites a situation in which the first network security appliance receives network traffic not from the second network security appliance and proceeds to execute security operations on the traffic. (*Id.*, cl. 4.) In that situation, the two security appliances are still in the same “CSF” even when only one appliance inspects traffic. Chandra disclosed this exact configuration. (Franz Reb., ¶48-49.)

Accordingly, Chandra taught a “CSF” under PO’s construction.

2. Keohane

PO contends Keohane’s CSF lacked “a series of interconnected paths.” (POR, 50.) Dr. Black admitted his interpretation of “interconnected paths” means that “CSF” can have three appliances in a line if there are multiple paths for data to travel. For example, if appliances A, B, and C are arranged linearly, such topology has “multiple interconnected paths” if network traffic can be received by either A or B

before being passed down. (Black. Depo. Tr., 66:4-12.)

This is exactly what Keohane disclosed. Below, for example, Keohane disclosed three network security appliances (firewall 300, mail gateway 302, client 304) arranged linearly.

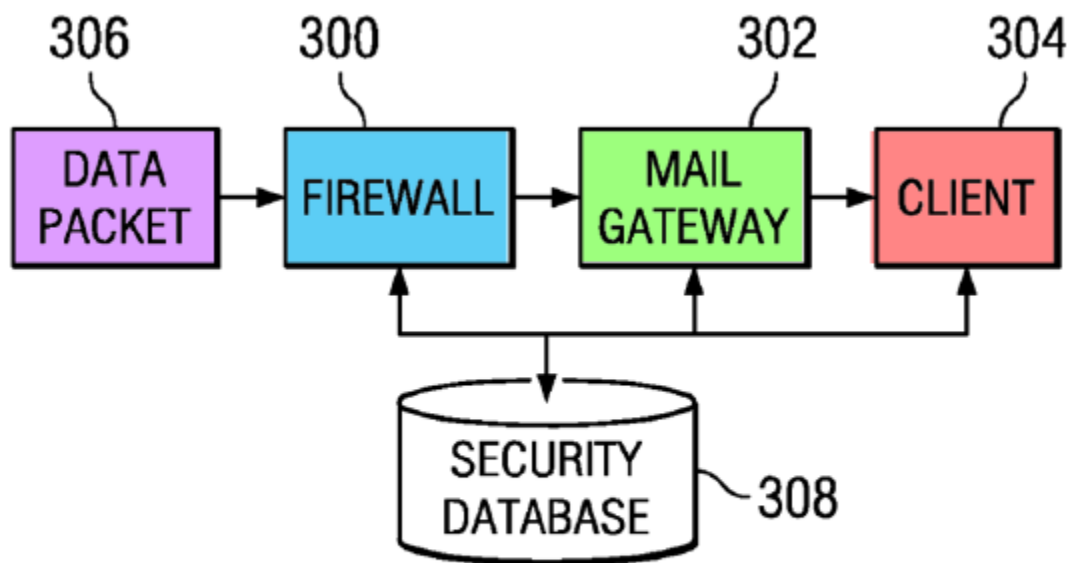


FIG. 3
(Annotated)

Firewall 300 could receive network traffic and transmit it down a data path. Separately, mail gateway 302 could do the same. Mail gateway 302 examined the data packet “to determine whether a signature from a trusted security element is present” in the data packet. (Keohane ¶35.) “[A] trusted security element is a network element, such as a firewall, mail gateway, router, or some other security intermediary that performs a security action on a data packet.” (*Id.*) This indicated that traffic to mail gateway 302 could come from sources other than firewall 300. (Petition, 85.) Therefore, traffic could enter at either firewall 300 or mail gateway

302 and travel down a data path. According to Dr. Black, Keohane's system had "multiple interconnected paths." (Franz Reb., ¶50-51.)

While acknowledging that Keohane disclosed "inspecting incoming network traffic," PO contends Keohane did not disclose inspecting "outgoing network traffic." (POR, 50.) PO's position that "CSF" requires inspection of *both* incoming and outgoing traffic is not required by the claims and contradicts the Board's construction, the POR, and Dr. Black's Declaration. The Board was clear that "a 'fabric' does not require bidirectional communications." (ID, 30.) The POR and Dr. Black's Declaration also state that "CSF" requires "inspect[ing] incoming *and/or* outgoing network traffic." (POR 38; Black Decl. ¶96-97.) (Franz Reb., ¶52.)

Despite PO's erroneous construction, Keohane disclosed inspecting "outgoing network traffic." Keohane disclosed that *both* "clients and servers may include software and/or hardware used to perform security actions...[on] *data packets received by them.*" (Keohane ¶23.) Therefore, clients could receive data packets originating from servers and vice-versa. (Franz Reb., ¶53.)

Therefore, Keohane disclosed a "CSF" under PO's construction.

IV. THE ASSERTED ART TAUGHT ALL DEPENDENT CLAIMS

PO argues that the asserted art failed to disclose certain limitations in dependent claims 2, 4, 6-7, 12, 15, 17-18, 23-24, 28-29. However, as explained below, the asserted art addressed all these limitations.

A. Chandra Taught or Rendered Obvious “Local Network Policies” (Claims 2, 4, 15).

PO argues that “Chandra does not disclose that network actions are performed according to policies that are local to the endpoint” because “Chandra never states that the second set of actions is determined according to a policy that is local to the receiving CE.” (POR, 39.) That argument ignores the fact that, after the CE labels (reproduced below) were exchanged and registered at the transmitting and receiving ends, the two ends executed security actions independently, autonomously, and “locally” according to rules associated with their respective CE labels. (*See* Petition, 37-38.)

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

A POSITA would understand that the specific operations executed by each end were determined by their respective local policies. Specifically, the “local network policies” were the respective executing algorithms in conjunction with the local

tables storing CE labels and rules. Therefore, Chandra taught or rendered obvious performing security operations based on “local network policies.” (Franz Reb., ¶54-55.)

B. Chandra and Keohane Rendered Obvious Flags That Were Carried In “a First Packet of a Session” (Claim 12).

While acknowledging that “[i]ncluding flags in the first packet [of a session] may be sufficient,” PO argues “that does not explain why a POSITA would do so in the first place.” (POR, 41.) The reason cannot be simpler, as the Petition explained—the flags determined whether the packets of the session came from the trusted transmitting security appliance (Petition 29-31, 74-76) and what operations were already performed (*e.g.*, Petition, 36, 76-77). Hence, the receiving security appliance needed the flags before it could perform security operations on the packets in the session. So, the flag would naturally be transmitted in the first packet of the session before any traffic data. (Franz Reb., ¶56.)

PO further argues that Chandra’s CE labels were not in the first packet of a session because “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.” (POR, 42.) PO misinterprets Chandra. The authentication and exchange of “CE labels *to be* used for tagging the data packets (Chandra, ¶34)” were performed *before* any session containing data packets to be inspected *began*. (Petition, 20; Franz Reb., ¶57.)

Therefore, Chandra and Keohane rendered obvious that flags were carried in “a first packet of a session.”

C. Chandra and Keohane Taught or Rendered Obvious “Next Network Appliance” (Claims 6, 17, 23, 28) and “Next Network Appliance Participating in a CSF” (Claims 7, 18, 24, 29).

While POR Section VII and X.A discuss several dependent claims together, some of those dependent claims require “a next network appliance participating in the CSF (’825 patent, cl. 6, 17, 23, 28)” while the others require “a next network appliance (*id.*, cl. 7, 18, 24, 29).” Chandra and Keohane taught or rendered obvious both.

1. Chandra

PO does not dispute that receiving CE 214 transmitted processed network traffic to receiving network device 212 (Chandra, ¶30), which was at least a “next network appliance.” (Petition 54; Franz Reb., ¶58-59.)

Petitioner explained, and PO acknowledges, that Chandra disclosed that “a plurality of [] CEs [could] be associated with a single PE.” (POR, 43 (quoting Petition, 54).) It would be obvious to arrange some of these CEs in series so that traffic passed through multiple receiving CEs before reaching receiving PE. A POSITA would find it obvious to implement a version of Chandra where traffic received by the receiving end was inspected by multiple network security appliances (CEs) capable of different functions participating in the CSF. In such a case, the

network traffic was transmitted to “a next network appliance participating in the CSF.” (Franz Reb., ¶60.)

Petitioner also explained that a POSITA would find it obvious to implement a version of Chandra where the CSF was extended by combining Chandra’s Figures 2 and 8, as illustrated below. In such an example, “receiving CE could transmit the data packet...to a device in an extended VPN network.” (Petition 54-56.) The next device in the extended VPN network was “a next network appliance participating in the CSF.” (Franz Reb., ¶61.)

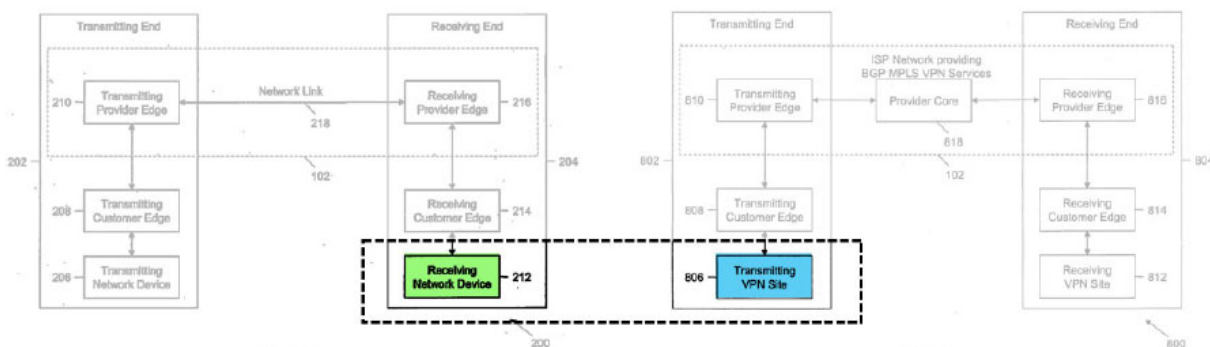


FIG. 2

FIG. 8

(Redrawn and Annotated)

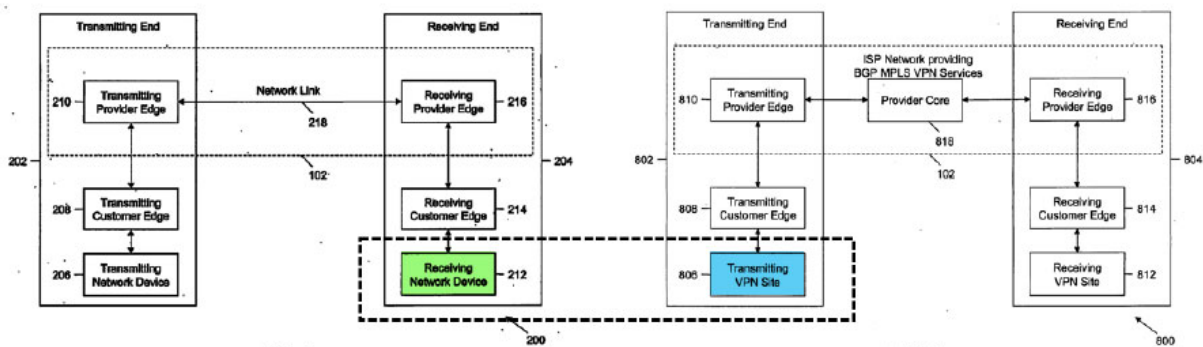


FIG. 2

FIG. 8

(Redrawn and Annotated)

Contrary to PO’s assertion that “Petitioner...provides no rationale for why a POSITA would modify Chandra...or explain why a POSITA would reasonably

expect it to succeed (POR, 45),” Petitioner provides ample reasons why (Petition 54-56). Dr. Franz provided an example of a widely circulated official publication by the National Security Agency containing a reference architecture that recommended cascading multiple VPN solutions. (Franz. Decl. ¶¶127-130; Franz Reb., ¶¶62.)

PO argues that combining Chandra’s Figures 2 and 8 would be difficult because “[a]dding additional CE’s would require an exponential increase in the exchange of [label] data.” (POR, 46.) However, the labels needed to be exchanged only once when the CSF was being configured. Even in a large corporate network with many security appliances, the amount of traffic generated by this label exchange would be insignificant relative to the network traffic to be inspected. (Franz Reb., ¶¶63.)

Thus, Chandra taught or rendered obvious “next network appliance” and “next network appliance participating in a CSF.”

2. Keohane

PO argues that Keohane’s client 304, a personal or network computer, was neither a “network appliance” nor a “network appliance participating in the CSF” because it was a destination endpoint. (POR, 56.)

PO points to nothing in the ’825 patent that excludes destination endpoints from the definition of “network appliances.” PO argues that the specification distinguishes between “network security appliances” and “endpoint devices.” (*Id.*,

55.) Even assuming there was a distinction, “network appliances” are broader than “network security appliances.” *Promptu Systems Corporation v. Comcast Corporation*, 92 F.4th 1372 (Fed. Cir. 2024) (“The absence of the ‘centralized’ modifier in the claims, in turn, means that the claimed ‘wireline node’ must be broader in some way than the ‘centralized wireline node’ defined in the specification.”) The ’825 patent does not exclude clients from “network appliances.” To the contrary, it says “some network appliances are implemented as general-purpose computers with appropriate software configured for the particular functions to be provided by the network appliance.” (’825 patent 4:3-6.) Therefore, Keohane’s client 304, which was a personal or network computer capable of performing security operations (Keohane ¶23; *see also* Petition, 65), was “a next network appliance.” (Franz Reb., ¶67-69.)

Client 304 was also “a next network appliance in the CSF.” Client 304 was distinguishable from the “endpoint devices” described in the ’825 patent because client 304 was a network security element capable of cooperating security operations with its upstream security elements. (*E.g.*, Petition, 71-72, 78.) In other words, while it was an endpoint device, it also functioned as a CSF member appliance performing its security functions. (Franz Reb., ¶70.)

For the reasons above, Keohane taught or rendered obvious both “a next network appliance” and “a next network appliance participating in a CSF.”

D. Keohane Taught or Rendered Obvious a First Network Security Appliance that Received Traffic “Not Transmitted from the Second Network Security Appliance” (Claim 4).

Keohane disclosed that the downstream security element (first network security appliance) sometimes received network traffic “not transmitted from” the upstream security element (second network security appliance). This could happen when the downstream security element received network traffic that did not include a signature of the upstream security element, meaning that this signature-less traffic could be from sources other than the upstream security element. (Petition, 85.; Franz Reb., ¶64.)

Using PO’s own words, “the very purpose of a signature is to authenticate that a message truly came from a certain sender.” (POR, 57.) Therefore, a message without a signature from the sender might not be from the sender. If Keohane’s “mail gateway always receives data from the firewall (POR, 51)” and “client...only receives traffic from the mail gateway (*id.*, 52),” the signature would lose its “very purpose...to authenticate...a message (POR at 58).” Thus, because the downstream security element sometimes received data packets without a signature of the upstream security element, the downstream security element (first network security appliance) sometimes received network traffic “not transmitted from” the upstream security element (second network security appliance). (Franz Reb., ¶65.)

PO’s only contention is that the “lack of a signature *could* simply mean that

the upstream device did not perform any security action.” (POR, 53.) But what the prior art discloses *in addition to* the practice of the claimed invention is irrelevant. While the lack of signature *could* indicate the lack of action by the upstream device, it could also indicate that the traffic did not come from the upstream device. Keohane’s security system included a variety of appliances such as “routers, gateways, and firewalls,” “or some other security intermediary.” (Petition, 65, 72-73 (quoting Keohane ¶¶23, 35).) It would be obvious for the downstream device to receive traffic from a variety of appliances. (Franz Reb., ¶66.)

E. A POSITA Would Be Motivated to Use Buruganahalli’s Updating of Tags with Keohane’s Signatures (Claims 6, 17, 23, 28).

PO argues that “making Keohane’s digital signatures modifiable would defeat their purpose” because “a purpose of a digital signature is to prevent tampering” to ensure that the source of the signature is authenticated. (POR, 57.) But updating the signature as Petitioner proposed would still ensure that the signature indicated a secure source as long as all the security appliances along the data paths were previously authenticated with each other. The whole point of a CSF is that it is collaborative and the participants trust each other. It would be obvious that the CSF participants could use a common, pre-shared cryptographic key to prevent non-members from tampering with the signature while each of the CSF members would be able to decrypt, update, and then re-encrypt the signature. As the Petition explains, Keohane’s signatures contained codes indicating what security actions were

performed and whether the source of the data packet was a secure source. (Keohane ¶38, Petition, 81.) The signature could easily be updated to modify the codes or add more codes in the same signature. (Franz Reb., ¶71-72.)

Therefore, a POSITA would be motivated to update Keohane's signature.

F. A POSITA Would Be Motivated to Remove Keohane's Signatures (Claims 7, 18, 24, 29).

PO argued that Keohane's signatures could not be removed from the data packet before it was transmitted to the client because the "signature is essential" as it "indicate[d] that the packet came from 'trusted security elements'" and "which security actions have already been performed on the network packet." (POR, 60.) However, as Petitioner explained, sometimes "the next destination," such as the client, "was not one of the network devices that could read and utilize the [flag] to cooperate network operations." (Petition, 95.) A POSITA would find it obvious to implement a version of Keohane where the client only received data packet from an upstream network security appliance participating in the CSF and performed no security actions of its own. This would be the obvious configuration in an enterprise network in which clients were connected to the enterprise's networking infrastructure. In this situation, it would be obvious to remove the signature for reasons provided in the Petition (Petition, 94-96) because the signature lost its purpose of authenticating the source and record previous security actions. (Franz Reb., ¶73.)

Therefore, a POSITA would be motivated to remove Keohane's signature.

V. CONCLUSION

Petitioner requests the Board find '825 patent's claims 1-7 and 10-31 unpatentable as obvious over prior art.

Dated: April 10, 2024

Respectfully submitted,

/Babak Tehranchi/

Lead Counsel

Thomas N. Millikan, Reg. No. 72,316

PERKINS COIE LLP

11452 El Camino Real, Suite 300

San Diego, California 92130-2080

858.720.5700 (phone)

858.720.5799 (fax)

Back-up Counsel

Babak Tehranchi (Reg. No. 55,937)

Andrew N. Klein (*pro hac vice*)

Attorneys for Petitioner

CERTIFICATE OF WORD COUNT UNDER 37 CFR §42.24(d)

Under 37 C.F.R. §42.24(d), the undersigned certifies that the word count for this **Petitioner's Reply To Patent Owner's Response** totals 5,592, excluding the parts exempted by 37 C.F.R. § 42.24(a). Accordingly, this paper is under the word count limit of 5,600 words.

The word count was made using the built-in word count function in the Microsoft® Word 365 software used to prepare this document.

Dated: April 10, 2024

PERKINS COIE LLP
11452 El Camino Real, Suite 300
San Diego, California 92130-2080
858.720.5700 (phone)
858.720.5799 (fax)

Respectfully submitted,

/Babak Tehrani/

Lead Counsel

Thomas N. Millikan, Reg. No. 72,316

Back-up Counsel

Babak Tehrani (Reg. No. 55,937)

Andrew N. Klein (*pro hac vice*)

Attorneys for Petitioner

CERTIFICATE OF SERVICE

I hereby certify that on April 10, 2024, I caused a true and correct copy of the foregoing **Petitioner's Reply To Patent Owner's Response** and supporting materials to be served electronic mail on the following attorneys of record for Patent Owner:

James M. Glass - jimglass@quinnemanuel.com
John T. McKee - johnmckee@quinnemanuel.com
Quincy Lu - quincylu@quinnemanuel.com
Andrew M. Holmes - drewholmes@quinnemanuel.com
Quinn Emanuel Urquhart & Sullivan LLP
51 Madison Ave, 22nd Floor
New York, New York 10010

Dated: April 10, 2024

Respectfully submitted,

PERKINS COIE LLP
1201 Third Avenue, Suite 4900
Seattle, Washington 98101

/Anita Chou/
Anita Chou
Patent Paralegal