

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

NETSKOPE, INC.,
Petitioner,

v.

FORTINET, INC.,
Patent Owner.

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

PATENT OWNER'S PRELIMINARY RESPONSE

TABLE OF CONTENTS

	<u>Page</u>
I. INTRODUCTION	1
II. OVERVIEW OF THE '825 PATENT	3
III. OVERVIEW OF CERTAIN CITED ART	5
A. Chandra (Ex. 1004)	5
B. Keohane (Ex. 1008)	6
IV. LEVEL OF ORDINARY SKILL IN THE ART	8
V. CLAIM CONSTRUCTION	8
A. The plain meaning of “fabric” requires processing of bidirectional communications	9
VI. GROUND 1: PETITIONER FAILS TO ESTABLISH THAT Chandra Renders Obvious Claims 1-5, 12, 15-16, 21-22, and 27	16
A. Chandra does not disclose a “fabric”	16
B. Chandra does not disclose “determining ... whether the network traffic has been transmitted from a second network security appliance that is participating in the CSF based on a flag”	18
VII. GROUNDS 2, 3, and 4: Petitioner Fails to Establish that Chandra in Combination with Other References Render Obvious Claims 6-7, 10-11, 13-14, 17-20, 23-26, and 28-31 ..	20
VIII. GROUND 5: PETITIONER FAILS TO ESTABLISH THAT Keohane Renders Obvious Claims 1-5, 12, 15-16, 21-22, 27..	20
A. Keohane does not disclose a “fabric”	21
B. Keohane does not disclose “determining ... whether the network traffic has been transmitted from a second	

	network appliance that is participating in the CSF based on a flag”	23
IX.	GROUND 6, 7, and 8: Petitioner Fails to Establish that Chandra in Combination with Other References Render Obvious Claims 6-7, 10, 13-14, 17-20, 23-26, and 28-31	25
X.	CONCLUSION	26

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)

I. INTRODUCTION

The petition fails to meet its burden to establish unpatentability for at least two reasons. **First**, neither of the primary references—Chandra and Keohane—disclose a “fabric.” The plain meaning of a “fabric” is a network of devices for processing **bidirectional** communication. There is no dispute that the relied-upon art only processes **unidirectional** communication. Nor is there any dispute that the term “fabric” should be given its ordinary meaning—Petitioner argues as much. But despite arguing that “fabric” has an ordinary meaning, Petitioner fails to provide any such meaning. Instead, Petitioner commits one of the cardinal sins of claim construction and cherry-picks a single, isolated statement from the specification and imports it into the claims. Petitioner does so without explanation—it does not, for example, argue that its lone statement reflects the ordinary meaning of “fabric.” Nor does it argue that this statement is definitional, through lexicography, disavowal, or otherwise. Moreover, this lone statement ignores the vast majority of the specification that expressly describes a fabric as bidirectional. Even more egregious, Petitioner admits that the statement on which it relies is functional—the statement does not explain what a fabric **is**, merely “**what it achieves**.” Petitioner thus urges the Board to adopt a functional definition for the term fabric. But functional claim terms are

prohibited, and such a definition could lead to the claim being invalid. If Petitioner truly believed “fabric” to be a functional term, an IPR is not the place for it to bring this dispute, as the Board is prohibited from determining invalidity based on anything other than printed publications.

In stark contrast, Patent Owner has provided the ordinary meaning for the term “fabric,” supported by detailed expert testimony. Patent Owner’s definition is also consistent with the intrinsic evidence—it embraces not only the lone statement the Petition hangs on, but also all of the disclosure in the ‘825 patent describing a fabric. And last, Patent Owner’s definition is consistent with extrinsic evidence, including attached dictionary definitions. In short, Patent Owner’s proposed definition encompasses not only the specification’s description of what a fabric **does**, but also the description of what it **is**, and avoids Petitioner’s self-inflicted pitfall of construing the term functionally.

Second, neither Chandra or Keohane disclose a feature that allows one node to determine that network traffic was transmitted from another node participating in the CSF as required by the claims. Chandra and Keohane merely include flags that identify prior operations performed on the data packets. But this does not provide information that the packet originated from another node participating in the CSF.

II. 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 that may be redundant. Ex. 1001, 1:33-37, 1:45-52. The '825 patent solves this issue by introducing a “cooperative security fabric (CSF)” with interwoven member nodes that can “coordinat[e] security operations” using flags carried by network traffic to indicate which operations have already been executed, and further indicate whether the packets were transmitted by participating nodes in the CSF. Ex. 1001, 2:1-16; Ex. 2001, ¶¶29-30.

As set forth in the accompanying declaration of Dr. Black, a “fabric” is a term of art whose ordinary meaning requires a network of devices that processes bidirectional communication. Ex. 2001, ¶¶31-32. The '825 patent uses this term according to its ordinary meaning, and proposes no special meaning or engage in lexicography, and Petitioner does not allege otherwise. Ex. 2001, ¶32. Specifically, the '825 patent describes the fabric handles both “downstream network traffic” and “upstream network traffic” and that member nodes of the CSF process data packets from any other member node. *See, e.g.*, Ex. 1001, 7:28-30, 6:65-67. An example of a “fabric” is shown in connection with Fig. 2:

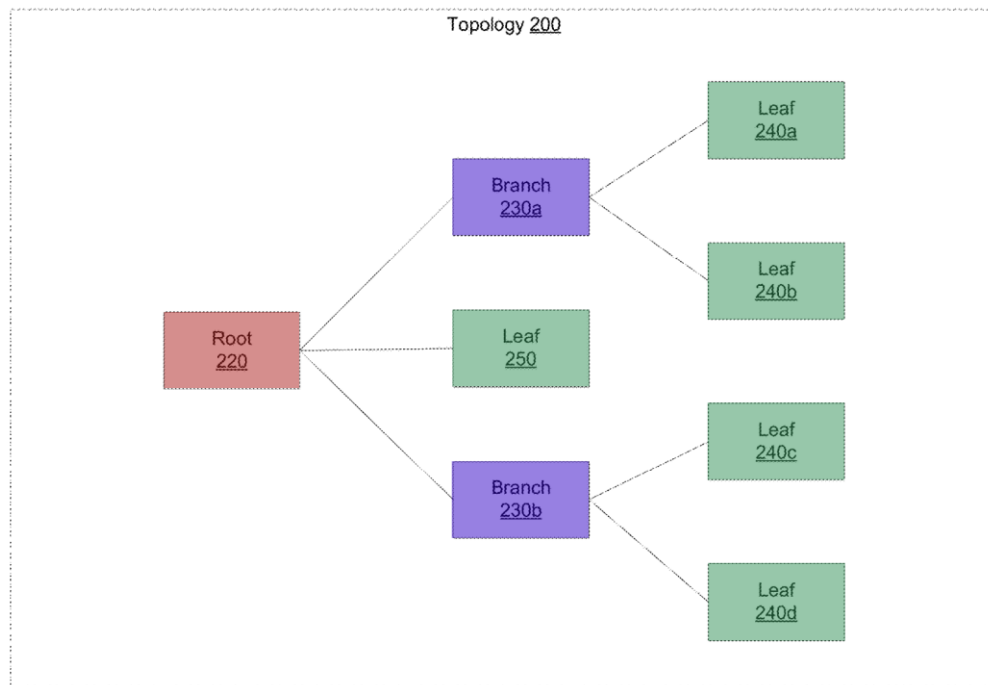


FIG. 2

Ex. 1001, Fig. 2.

In order to improve coordination, the '825 patent also describes that its member nodes can determine from a data packet whether it was transmitted from another member node participating in the CSF. Ex. 2001, ¶33. When a member node of the CSF receives a data packet, it “checks whether the incoming packet [was transmitted] from another member node of the CSF based on the flag carried by the incoming packet.” *Id.*, 6:65-67. The '825 patent explains that “a signature of the member node may be included in or accompany the flag” which allows “[o]ther member nodes [to] extract the

signature from the packet to authenticate that the flag carried by the network packet was actually transmitted from the member node.” *Id.*, 7:17-22.

Thus, any given node can potentially receive network traffic from any other member node, and will coordinate operations for the transmission of data in any direction between the nodes of the CSF. Ex. 2001, ¶34.

III. 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. 2001, ¶35.

A. Chandra (Ex. 1004)

Chandra is directed to managing *unidirectional* network traffic between two nodes. Ex. 1004, Abstract, ¶17; Ex. 2001, ¶36. The system disclosed by Chandra is depicted in the annotated Figure 2 below. Ex. 2001, ¶36.

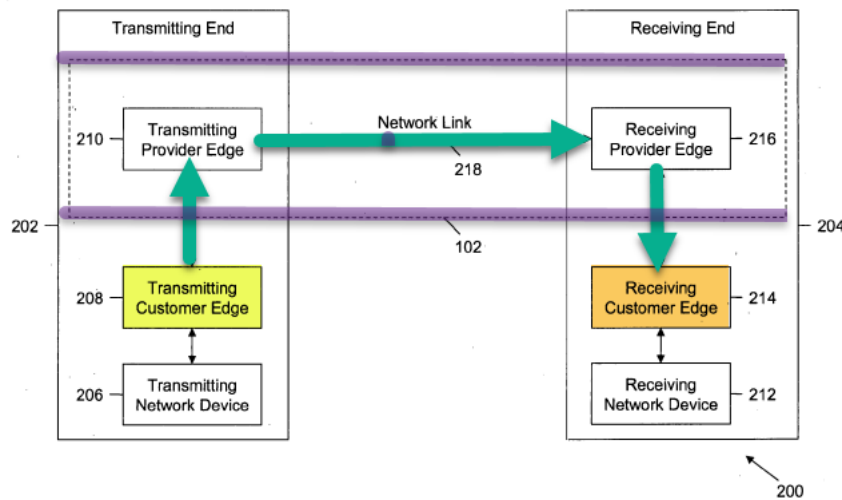


FIG. 2

As shown in the above figure, Chandra does not disclose a “fabric.” Ex. 2001, ¶37. Instead, Chandra discloses a one-way tunnel between two nodes comprising a transmitting end and a receiving end, between which data packets are transferred “with a [tagged] label indicating a first set of actions performed on the data packet at [the] transmitting end.” Ex. 1004, ¶18; Ex. 2001, ¶37. According to Chandra, “[t]he tagged label helps to determine a second set of actions that has to be performed on the data packet at a receiving end.” *Id.*

B. Keohane (Ex. 1008)

Like Chandra, Keohane also fails to disclose a “fabric.” Instead, it relates to a method for performing iterative security operations on incoming network traffic in a single direction. Ex. 1008, ¶¶33-37; Ex. 2001, ¶38.

Keohane’s method is depicted in Figure 3 below.

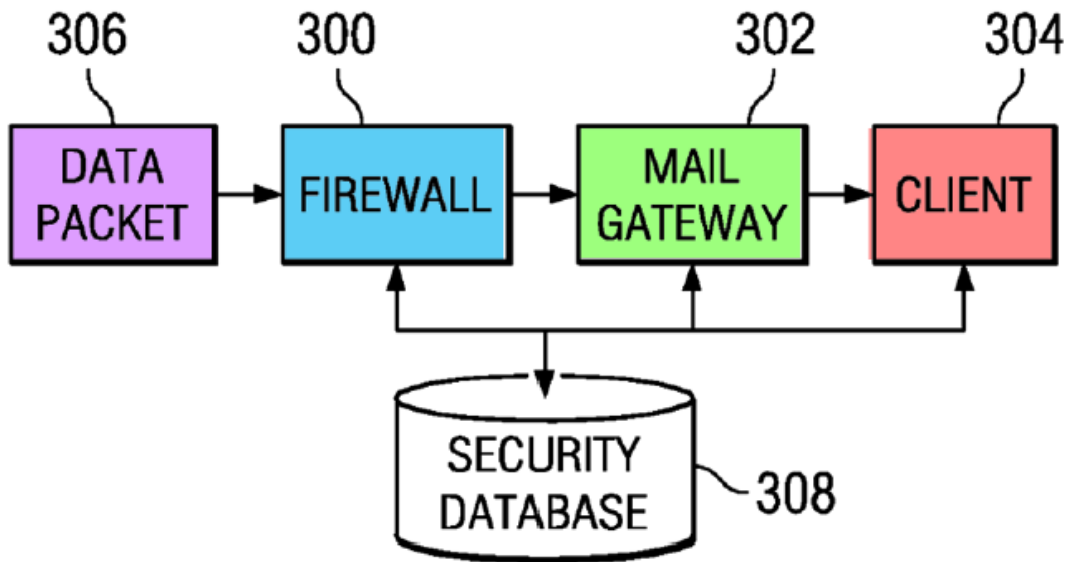


FIG. 3
(Annotated)

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 packet. Ex. 2001, ¶39. Keohane’s unidirectional tunnel is just like the scheme disclosed in Chandra. *Id.*

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 determine whether a previous security action has been performed by the upstream network element. Ex. 1008, ¶11; Ex. 2001, ¶40. Thus, as depicted in Figure 3, 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 inserts a “signature ... indicat[ing] that a previous security action has been performed on the data packet.” Ex. 1008, ¶¶32-37; Ex. 2001, ¶40.

IV. 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. 2001, ¶18. Petitioner’s expert, Dr. Black, was a POSITA at the time of the priority date of the ’825 patent. Ex. 2001, ¶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. 2001, ¶19. The positions set forth in this preliminary response would be the same under either parties’ proposal.

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. 19. For purposes of this preliminary response, Patent Owner agrees that all claims should be given their plain and ordinary meaning. Ex. 2001, ¶¶41-42.

With respect to the term “fabric,” its ordinary meaning requires processing of bidirectional communications. Ex. 2001, ¶¶43-51. As discussed below, Petitioner applies the wrong meaning of these terms and cherry-picks from the spec. If the Board gives “fabric” its plain meaning, Petitioner’s references indisputably fail to disclose a fabric, for they lack processing of bidirectional communications. However, regardless of how the Board resolves this dispute, Petitioner’s references also fail to disclose “determining ... whether the network traffic has been transmitted from a second network security appliance that is participating in the CSF based on a flag.”

A. The plain meaning of “fabric” requires processing of bidirectional communications

It is fundamental that the “starting point” for claim construction begins with a term’s ordinary meaning. *Phillips*, 415 F.3d at 1313. Notably, Petitioner argues that no claim construction is necessary for the term “fabric”

(Pet. 19). Thus, there is no dispute that this term should be given its plain meaning.

The plain meaning of a “fabric” as understood by a POSITA in view of the patent requires network nodes that process bidirectional communications. Ex. 2001, ¶43. This ordinary meaning is supported by Dr. Black, the intrinsic record and extrinsic evidence. *Id.*, ¶¶43-51.

As set forth in the accompanying Dr. Black declaration, a “fabric” in the context of computer networks is a well-understood term. Ex. 2001, ¶44. As he explains, “[a]s enterprise networks became larger and larger, a complex, interconnected topology known as a ‘fabric’ was developed to handle the management of such networks.” *Id.* As the number of enterprise subnetworks increased (“as a result of, for example, increases in the enterprise’s number of office locations, departments, enterprise functions, etc.”), 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.* Thus, “network fabrics were required to handle network traffic within the network traveling in any direction, *e.g.* both traffic that was upstream and downstream of the subnetworks..” *Id.* Without the ability to handle bidirectional traffic, a “fabric” could not manage the traffic to and from the enterprise subnetworks as enterprises required. *Id.*

Dr. Black’s opinions are entirely consistent with the intrinsic evidence. Ex. 2001, ¶45. Starting with the specification, it describes a fabric that is required to process **bidirectional** communication between its nodes. *Id.* In particular, the ’825 patent describes that the fabric handles both “downstream network traffic” and “upstream network traffic.” Ex. 1001, 7:28-30; *see also* 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.”).

Moreover, the ’825 patent describes that “[i]n order to cooperate among members of a cooperative security fabric, **a 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. Thus, because **any member node** of the fabric can potentially transmit packets and coordinate operations with **any other member node**, the ’825 patent’s “fabric” supports handling of bidirectional communications between its member nodes, consistent with the term’s ordinary meaning. Ex. 2001, ¶46.

In addition to the foregoing intrinsic evidence, the plain meaning of “fabric” is also supported by extrinsic evidence. Ex. 2001, ¶47. 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) are *interwoven from port-to-port* (end-to-end).” Ex. 2003. In such a network, “data works its way through a complex, and even unpredictable, interwoven *network of networks* comprising transmission facilities, packet switches and multiple carriers.” *Id.* A POSITA would understand that these definitions require bidirectional communication, and is therefore consistent with the term’s plain meaning. Ex. 2001, ¶47. Nodes that only handled network traffic in one direction would not be considered a “fabric” as Petitioner suggests by its definition. *Id.*

By contrast, Petitioner argues in its claim construction section that the term “fabric” should be construed “in accordance with the ordinary and customary meaning ... as understood by one of ordinary skill in the art” yet it fails to even identify that “ordinary meaning,” and its expert likewise fails to provide his understanding of the term. Pet. 19; Ex. 1002, ¶54 (“For all terms of the challenged claims of the ’825 patent, I have afforded them their ordinary

and customary meaning in light of the intrinsic evidence at the time of the invention in May 2017.”); Ex. 2001, ¶48.

Instead, Petitioner ignores the ordinary meaning, and turns directly to the specification, arguing that “fabric” should be defined **functionally**, because “[t]he ‘825 describes the [cooperative security fabric] primarily **by what it achieves**—it ‘coordinates operations among members and avoids redundant operations.’” Pet. 27 (quoting Ex. 1001, 5:45-47). Petitioner’s end-run around the ordinary meaning of the term “fabric” has multiple issues. Ex. 2001, ¶¶48-51. First, and primarily, Petitioner commits one of the cardinal sins of claim construction—it imports a portion of the specification into the claims, without any explanation as to **why**. Ex. 2001, ¶49. It is well-settled that statements in the specification are not definitional unless the patent “clearly express[s] an intent to redefine the terms.” *Kyocera Senco Industrial Tools v. ITC*, 22 F.4th 1369, 1378 (Fed. Cir. 2022) *Merck & Co., Inc. v. Teva Pharmaceuticals USA, Inc.*, 395 F.3d 1364, 1370 (Fed. Cir. 2005). But while it is true that a CSF performs this **function**, that says nothing about the plain meaning of a “fabric.” Petitioner’s failure to identify the plain meaning of this term is fatal to its petition. 37 C.F.R. §42.104(b)(3); *Kingston Technology Co., Inc. v. Imation Corp.*, IPR2015-00066, Paper 19 at 31-32 (Mar. 24, 2016) (rejecting Petitioner’s arguments for failing to construe term in its petition).

Petitioner’s argument also fails because it is based solely on a truncated excerpt from an exemplary embodiment in the specification, that a CSF “coordinates operations among members and avoids redundant operations.” Pet. 27 (quoting Ex. 1001, 5:45-47); Ex. 2001, ¶49. This is yet another reason to reject Petitioner’s construction. Petitioner is attempting to broadly define a “fabric” by its function, ignoring its plain meaning, including how the rest of the specification defines a “fabric.” Ex. 2001, ¶49. Indeed, Petitioner’s application of its improper construction to Chandra and Keohane is inconsistent with the portions of the specification—cited above and explained by Dr. Black—that expressly describe a “fabric” as handling bidirectional communications. Ex. 2001, ¶50.

Moreover, Petitioner’s definition of a fabric based on its function also renders the limitation superfluous. Ex. 2001, ¶51. Specifically, in addition to reciting a “cooperative security fabric,” the independent claims of the ’825 patent *separately* recite “coordinat[ing] operations among members and avoid[ing] redundant operations” through the use of flags. Ex. 1001, 5:45-47. Petitioner’s construction collapses “cooperative security fabric” with these distinct limitations, thus rendering a “cooperative security fabric” superfluous. Ex. 2001, ¶51. This is yet another reason to reject Petitioner’s construction. *See Stumbo v. Eastman Outdoors, Inc.*, 508 F.3d 1358, 1362

(Fed. Cir. 2007) (“Therefore [the district court’s construction] would render [one of the claim terms] superfluous, a methodology of claim construction that this court has denounced.”).

Last, Petitioner’s interpretation should be rejected because it attempts to define a “fabric” functionally. A claim term is “functional” if it recites a feature “by what it **does** rather than by what it **is**.” MPEP §173.05(g). It is axiomatic that pure functional claiming is impermissible, and claims that are written in this manner are potentially invalid. *Aristocrat Techs. Austl. Pty. Ltd. v. Int’l Game Tech.*, 521 F.3d 1328, 1333 (Fed.Cir.2008) (“The point of the requirement that the patentee disclose particular structure in the specification and that the scope of the patent claims be limited to that structure and its equivalents is to avoid pure functional claiming.”). Petitioner’s interpretation asks the Board to construe “fabric” purely functionally, presumably so that it could then argue that the term is invalid. But if that is the case, Petitioner has chosen the incorrect forum—the Board can only consider invalidity in the context of printed publications. 35 U.S.C. §311(b). If Petitioner’s functional interpretation of the claim is correct, then the petition must nevertheless be denied, as the proper forum to decide the issue is in the district court.

VI. GROUND 1: PETITIONER FAILS TO ESTABLISH THAT CHANDRA RENDERS 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 for at least the following reasons: (1) the ordinary meaning of term “fabric” requires processing of bidirectional communications, which Chandra indisputably does not disclose, and (2) Chandra’s receiving CE cannot use the “CE label” (*i.e.* the alleged “flag”) to determine whether the transmitting CE is “a second network security appliance that is participating in the CSF.” Ex. 2001, ¶52.

A. Chandra does not disclose a “fabric”

Ground 1 relies on Chandra alone as rendering the claims obvious. But Ground 1 fails to establish that Chandra discloses a “fabric,” whose ordinary meaning requires a topology that processes ***bidirectional*** communications. Instead, it is undisputed that Chandra discloses a two-node tunnel that only processes ***unidirectional*** communication. Ex. 2001, ¶¶53-60.

The ordinary meaning of “fabric” to a POSITA in view of the specification requires a topology of network nodes that process bidirectional communications. See Section V.A; Ex. 2001, ¶54.

Petitioner argues that Chandra’s receiving CE (214) and transmitting CE (208) are network security appliances participating in a “cooperative

security fabric. Pet. 26-27. But Chandra discloses that its receiving CE (214) and transmitting CE (208) are two nodes that can only process traffic in one direction. Ex. 2001, ¶¶55-56.

Transmitting end 202 includes a transmitting network device 206, a transmitting Customer Edge (CE) 208, and a transmitting Provider Edge (PIE) 210. Transmitting network device 206 is a network devices...which is capable of transmitting data.

Similarly, receiving end 204 includes a receiving network device 212, a receiving CE 214, and a receiving PI 216. Receiving device 212 is a network devices...which is capable of receiving data.

Ex. 1004, ¶¶25-26. This is shown, for example, in Figure 2 of Chandra, as annotated by Patent Owner below:

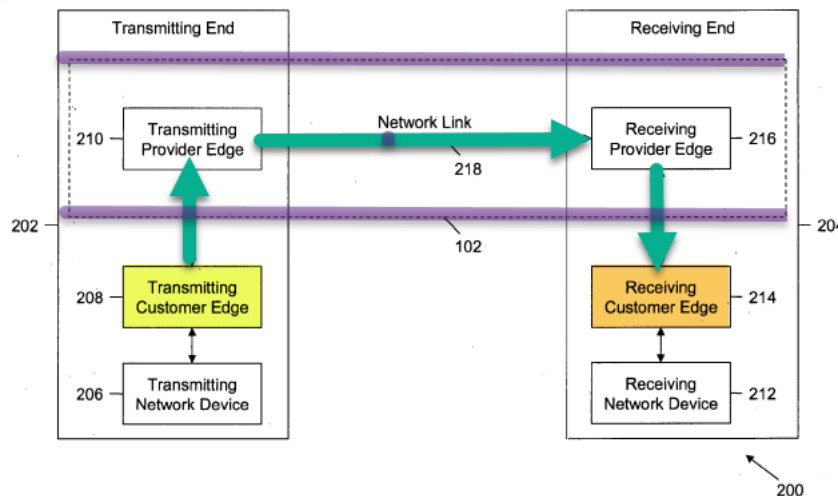


FIG. 2

Ex. 1004, Fig. 2 (annotated); Ex. 2001, ¶57. As shown in the figure, transmitting CE (208) (yellow) acts as a dedicated data transmitter, which

transmits data through a network tunnel (218) (purple) to a dedicated receiver, receiving CE (214). Ex. 2001, ¶58.

This is not a “fabric” under its plain meaning. Ex. 2001, ¶59. There is no processing of bidirectional communications, processing only occurs using a unidirectional tunnel connecting a dedicated transmitter CE (208) and receiver CE (214). *Id.*

Accordingly, Petitioner’s Ground 1 should be rejected because Chandra fails to disclose a “fabric” under its plain meaning. Ex. 2001, ¶60.

B. Chandra does not disclose “determining ... whether the network traffic has been transmitted from a second network security appliance that is participating in the CSF based on a flag”

A second independent reason to deny institution is that Petitioner also fails to establish that Chandra discloses that the receiving CE can “determin[e] ... whether the network traffic has been transmitted from a second network security appliance that is participating in the CSF based on a flag” because Chandra’s “CE label” provides no information about whether the transmitting CE participates in the same CSF as the receiving CE. Ex. 2001, ¶61.

Petitioner argues that the receiving CE (214) is the claimed “first network security appliance” and the transmitting CE (208) is the claimed “second network security appliance.” Pet. 23, 30. Petitioner argues that

Chandra discloses that the transmitting CE (208) adds a “CE label” (*i.e.* the alleged “flag”) to data packets before transmitting them to the receiving CE (214). Pet. 28-32. Petitioner further argues that “a POSITA would find it obvious that when receiving CE (214) checks the data packet for a label (flag), the presence of a registered CE label in the data packet indicated that the data packet had been transmitted from transmitting CE (208).” Pet. 31.

But even if Petitioner’s description of Chandra is accepted, this fails to disclose the claim limitation. Ex. 2001, ¶¶62-63. At best, the CE “flag” merely indicates which security operations were performed by the transmitting CE. Ex. 2001, ¶63. It does **not** include any indication that the transmitting CE (208) is participating in the same CSF as the receiving CE (214). *Id.*

This is in stark contrast to the ’825 patent which expressly discloses that member nodes of a CSF can “check[] whether the incoming packet is from another member node of the CSF based on the flag carried by the incoming packet,” because “the ***flag is set to indicate that the network packet is transmitted from a member node*** [of a CSF].” Ex. 1001, 6:65-7:4. Thus, the ’825 patent does not determine participation merely by a flag describing operations already performed on a data packet as in Chandra—rather it discloses a flag that signals the packet came from another member node

participating in the CSF. Ex. 2001, ¶¶64-65. For example, the '825 patent explains that “a signature of the member node may be included in or accompany the flag” which allows “[o]ther member nodes [to] extract the signature from the packet to authenticate that the flag carried by the network packet was *actually transmitted from the member node.*” *Id.*, 7:17-22. This check allows “the local member node [to] determine that the network packet was transmitted from another *member node of the CSF.*” *Id.*, 7:22-25. Chandra’s CE label discloses no such flag. Ex. 2001, ¶65. Thus, Petitioner has failed to show that Chandra discloses this limitation. *Id.*, ¶66.

VII. GROUNDS 2, 3, AND 4: PETITIONER FAILS TO ESTABLISH THAT CHANDRA IN COMBINATION WITH OTHER REFERENCES RENDER OBVIOUS CLAIMS 6-7, 10-11, 13-14, 17-20, 23-26, AND 28-31

Grounds 2, 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. 2001, ¶67.

VIII. GROUND 5: PETITIONER FAILS TO ESTABLISH THAT KEOHANE RENDERS 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 for at least the following reasons: (1) the ordinary meaning of term “fabric” requires processing of bidirectional

communications, which Keohane indisputably does not disclose, and (2) Keohane's mail gateway the "signature" (*i.e.* the alleged "flag") to determine whether the firewall 300 is "a second network security appliance that is participating in the CSF." Ex. 2001, ¶68.

A. Keohane does not disclose a "fabric"

Ground 5 relies on Keohane alone as rendering the claims obvious. But Ground 5 fails to establish that Keohane discloses a "fabric," whose ordinary meaning requires a topology that processes ***bidirectional*** communications. Instead, it is undisputed that Keohane, like Chandra, discloses a tunnel that only processes ***unidirectional*** communication. Ex. 2001, ¶¶69-76.

The ordinary meaning of "fabric" to a POSITA in view of the specification requires a topology of network nodes that process bidirectional communications. *See* Section V.A; Ex. 2001, ¶70.

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), mail gateway (302), and client (304) are nodes that can only process traffic in one direction. Ex. 2001, ¶71.

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. Indeed, every embodiment in Keohane describes that the first action is to “determin[e] whether a data packet originates from a trusted source,” which a POSITA would understand indicates that it only handles traffic that originates from outside the network. Ex. 1008, ¶33; Ex. 2001, ¶72. This is shown, for example, in Figure 3 of Keohane, as annotated by Petitioner below:

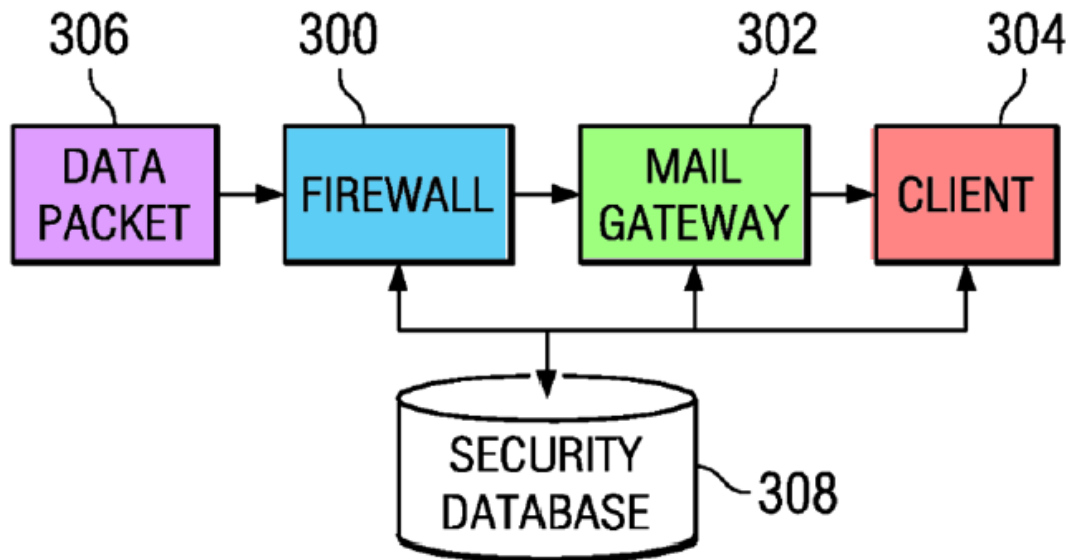


FIG. 3
(Annotated)

Ex. 1008, Fig. 3 (annotated); Ex. 2001, ¶73. As shown in the figure, the data packet 306 only flows in **one direction**, with firewall 300 acting as a dedicated

data transmitter to mail gateway 302, which acts as a dedicated data transmitter to client 304. Ex. 2001, ¶74.

This is not a “fabric” under its plain meaning. There is no processing of bidirectional communications, processing only occurs using a unidirectional tunnel connecting a firewall (300), mail gateway (302), and client (304). Ex. 2001, ¶75.

Accordingly, Petitioner’s Ground 5 should be rejected because Keohane fails to disclose a “fabric” under its plain meaning. Ex. 2001, ¶76.

B. Keohane does not disclose “determining ... whether the network traffic has been transmitted from a second network appliance that is participating in the CSF based on a flag”

A second independent reason to deny institution is that Petitioner also fails to establish that Keohane discloses that the mail gateway (302) can “determin[e] ... whether the network traffic has been transmitted from a second network appliance that is participating in the CSF based on a flag” because Keohane’s “signature” provides no information about the transmitting node, such as which node it was, whether the node participates in a CSF, or whether the node participates in the same CSF as the mail gateway (302). Ex. 2001, ¶77.

Petitioner argues that mail gateway (302) is the claimed “first network security appliance” and that firewall (300) is the claimed “second network security appliance.” Pet. 74. Petitioner argues that Keohane discloses that the firewall (300) adds a “signature” (*i.e.* an alleged flag) to data packets before transmitting them to mail gateway (302). Pet. 75-76. Petitioner argues that if the mail gateway (302) recognizes the “flag” inserted into the data packet by the firewall (300), then mail gateway (302) would know the data packet “had been transmitted from another device in the system.” Pet. 75. Thus, Petitioner concludes that mail gateway (302) (*i.e.* the alleged “second network security appliance”) uses the flag to determine that network traffic had been transmitted “from a trusted security element participating in the CSF.” Pet. 76.

But even if Petitioner’s description of Keohane is accepted, this fails to disclose the claim limitation. Ex. 2001, ¶¶78-79. Keohane makes clear that the “signature” only “indicates that a security action has been performed on data packet 306”—there is no disclosure in Keohane that the signature includes any indication that the network packet was transmitted from firewall (300), or that firewall (300) is participating in the same CSF as mail gateway (302). Ex. 1008, ¶34; Ex. 2001, ¶79.

By contrast, as noted with respect to Ground 1, the ’825 patent expressly describes that member nodes of a CSF can “check[] whether the

incoming packet is from another member node of the CSF based on the flag carried by the incoming packet,” because “the *flag is set to indicate that the network packet is transmitted from a member node.*” Ex. 1001, 6:65-7:4; Ex. 2001, ¶80. Thus, the ’825 patent does not determine participation merely by a flag describing operations already performed on a data packet as in Keohane—rather it discloses a flag that signals the packet came from another member node participating in the CSF. Ex. 2001, ¶81. As an example, the ’825 patent explains that “a signature of the member node may be included in or accompany the flag” which allows “[o]ther member nodes [to] extract the signature from the packet to authenticate that the flag carried by the network packet was *actually transmitted from the member node.*” *Id.*, 7:17-22. This check allows “the local member node [to] determine that the network packet was transmitted from another *member node of the CSF.*” *Id.*, 7:22-25. Keohane discloses no such flag. Ex. 2001, ¶81. Thus, Petitioner has failed to show that Keohane discloses this limitation. Ex. 2001, ¶82.

IX. GROUND 6, 7, AND 8: PETITIONER FAILS TO ESTABLISH THAT CHANDRA IN COMBINATION WITH OTHER

REFERENCES RENDER OBVIOUS CLAIMS 6-7, 10, 13-14, 17-20, 23-26, AND 28-31

Grounds 6, 7, and 8 of the petition rely on Keohane for the same limitations discussed in Section VIII. Accordingly, these Grounds should be rejected for the same reasons. Ex. 2001, ¶83.

X. CONCLUSION

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

Date: June 20, 2023

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 4,882 words and thus complies with the applicable word limit.

Date: June 20, 2023

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 June 20, 2023 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: June 20, 2023

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.*