

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

Netskope, Inc.,
Petitioner,

v.

Fortinet, Inc.,
Patent Owner

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

**DECLARATION OF DR. JOHN BLACK JR.
IN SUPPORT OF PATENT OWNER'S PRELIMINARY RESPONSE**

1. I have been retained on behalf of Fortinet, Inc. (“Patent Owner”) in connection with the above-captioned *inter partes* review (IPR). I have been retained to provide my opinions in support of Fortinet’s Patent Owner Preliminary Response. I am being compensated for my time at the rate of \$625 per hour. I have no interest in the outcome of this proceeding.

2. In preparing this declaration, I have reviewed and am familiar with the Petition for IPR2023-00459, U.S. Patent No. 10,084,825 (“the ’825 patent”) and its file history, and all other materials cited and discussed in the Petition (including the declaration of Petitioner’s expert Michael Franz, Ph.D.), and cited and discussed in this Declaration.

3. The statements made herein are based upon my own knowledge and opinion. This Declaration represents only the opinions I have formed to date. I may consider additional documents as they become available or other documents that are necessary to form my opinions. I reserve the right to revise, supplement, or amend my opinions based on new information and on my continuing analysis.

I. QUALIFICATIONS

4. My qualifications can be found in my Curriculum Vitae (*see* Ex. 2002), which includes my detailed employment background, professional experience, and list of technical publications and patents.

5. I am an Associate Professor of Computer Science at the University of Colorado, Boulder. I received a B.S. in Mathematics and Computer Science from the California State University at Hayward (now "California State University, East Bay") in 1988. I received an M.S. in Computer Science in 1997, and a Ph.D. in Computer Science in 2000, both from the University of California at Davis.

6. I have taught more than 60 classes in computer science, on subjects including data structures, algorithms, networking, operating systems, software engineering, security, cryptography, discrete mathematics, and quantum computing. I have authored or coauthored more than 20 publications, primarily on issues relating to computer security. I have been involved with computers for over 40 years in both commercial and academic capacities.

7. My earliest interest was in networks and security. My first memories in this regard were around 1975 when a group of friends and I learned about the telephone network and its security. A few years later, personal computers became available and I spent most of my free time studying, programming, and modifying them. I worked extensively with various networking products throughout the 1980s, and developed an interest in cryptography soon thereafter. Although my undergraduate institution had no courses in cryptography or security in the 1980s, I decided to pursue self-study at the time, and opted to double major in Computer

Science and Mathematics because cryptography is a blend of these two subject areas.

8. After earning my B.S. degree in 1988, I worked for six years at Ingres Corp as a software developer, writing and reviewing code written in C. My work primarily was directed at transaction logging, data type support, and security.

9. In 1995, I began my Ph.D. at UC Davis under cryptographer Phillip Rogaway. My area of focus was cryptography and security and my research involved encryption, authentication, hash functions, and network security.

10. After graduation I took a position as an Assistant Professor at the University of Nevada at Reno. In the Fall of 2001, I taught the networking class there, which included coverage of Ethernet, interior gateway protocols, exterior gateway protocols, ARP, DHCP/BOOTP, IP, UDP, TCP, HTTP, SMTP and other protocols. In 2001, a graduate student and I looked at the security of ARP and invented a new protocol "AuthARP" to add security to the protocol.

11. In 2002, I moved to the University of Colorado at Boulder where I am currently employed. In the Fall of 2002, I co-designed and co-taught a new course called "Foundations of Computer and Network Security," which included descriptions of security issues around both wired and wireless security challenges, mostly for public-facing network services including the world-wide web. I have

taught this class seven more times since then, including modern topics such as wireless networking, the Internet of Things, and so forth.

12. In my career at the University of Colorado, I have published several more papers in the area of cryptography and network security. I have taught more than 30 courses in network security and cryptography, and have graduated several PhD students in these areas.

13. I also have worked for a consulting company at times, writing software on contract basis. Although most projects are covered by NDAs, many involved networks and/or aspects of computer security.

14. In 2011, I began technical consulting for a local company called Cardinal Peak, which focuses primarily on video encoding and delivery systems. My work for Cardinal Peak has largely been directed to video encoding, transcoding, compression, encryption, and DRM, but also has included networking projects and embedded device work. For example, I designed the security system for the Pro1 smart thermostat, implemented the DRM for the Yonder Music App, worked on 802.1X code for smart dog collars, and helped design the cryptography used in Fitbit devices for wireless transfer of a Fitbit watch to a phone or laptop.

15. In 2016, I took a two-and-a-half year leave of absence from the University of Colorado to start a company named "SecureSet" in Denver, Colorado. The objective of SecureSet is to take reasonably proficient technical

people and turn them into computer and network security specialists via five months of intensive training. SecureSet was sold to WeWork in 2019 and continues to offer computer security classes today. In 2018 I returned to my position at the University where I remain employed to the present day.

II. LEGAL UNDERSTANDING

A. The Person of Ordinary Skill in the Art

16. I understand that a person of ordinary skill in the relevant art at the time of the invention (also referred to herein as “ordinary artisan”) is presumed to be aware of all pertinent art, thinks along conventional wisdom in the art, and is a person of ordinary creativity—not an automaton.

17. I have been asked to consider the level of ordinary skill in the field that someone would have had at the time the claimed invention was made. In deciding the level of ordinary skill, I considered the following:

- the levels of education and experience of persons working in the field;
- the types of problems encountered in the field; and
- the sophistication of the technology.

18. A person of ordinary skill in the art relevant to the '825 patent at the time of the invention would have 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.

19. I have reviewed the declaration of Dr. Franz, including his opinions regarding the Person of Ordinary Skill in the Art. My description of the level of ordinary skill in the art is essentially the same as that of the Dr. Franz. The opinions set forth in this Declaration would be the same under either my or Dr. Franz's proposal.

20. I am well-qualified to determine the level of ordinary skill in the art and am personally familiar with the technology of the '825 patent. I was a person of at least ordinary skill in the art at the time of the priority date of the '825 patent. Regardless if I do not explicitly state that my statements below are based on this timeframe, all of my statements are to be understood as a ordinary artisan would have understood something as of the priority date of the '825 patent.

B. Legal Principles

21. I am not a lawyer and will not provide any legal opinions. Though I am not a lawyer, I have been advised that certain legal standards are to be applied by technical experts in forming opinions regarding the meaning and validity of patent claims.

1. Obviousness

22. I understand that to obtain a patent, a claimed invention must have, as of the priority date, been nonobvious in view of prior art in the field. I understand that an invention is obvious when the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art.

23. I understand that to prove that prior art, or a combination of prior art, renders a patent obvious, it is necessary to: (1) identify the particular references that singly, or in combination, make the patent obvious; (2) specifically identify which elements of the patent claim appear in each of the asserted references; and (3) explain how the prior art references could have been combined to create the inventions claimed in the asserted claim.

24. I understand that a patent composed of several elements is not proved obvious merely by demonstrating that each of its elements was, independently, known in the prior art, and that obviousness cannot be based on the hindsight combination of components selectively culled from the prior art to fit the parameters of the patented invention.

25. I also understand that a reference may be said to teach away when a person of ordinary skill, upon reading the reference, would be discouraged from following the path set out in the reference, or would be led in a direction divergent

from the path that was taken by the applicant. Even if a reference is not found to teach away, I understand its statements regarding preferences are relevant to a finding regarding whether a skilled artisan would be motivated to combine that reference with another reference.

2. *My Understanding of Claim Construction Law*

26. I have been informed that patent claims are construed from the viewpoint of a person of a ordinary artisan and that patent claims generally should be understood consistent with their ordinary and customary meaning at the time of the invention. A review of the patent claim language, the patent specification, and its prosecution history are also necessary to determine the proper meaning and scope of the term at issue.

27. I have further been informed that in the specification and prosecution history the patentee may define a claim term in a way that differs from the ordinary and customary meaning. I understand that during prosecution of the patent before the U.S. Patent and Trademark Office, the Applicant may make representations or provide definitions of terms that may affect the scope of the patent claims. In particular, the Applicant may, during the course of prosecution, limit the scope of the claims to overcome prior art and/or disavow claim coverage by making clear and unambiguous statements to that effect.

28. I have been informed that a ordinary artisan may, among other things, consider dictionaries, publications, other patents, and treatises (*i.e.*, “extrinsic evidence”). I understand that extrinsic evidence may generally not be relied on if it contradicts the meaning of claim language provided by the intrinsic evidence, such as express definitions given for terms in the specification.

III. OVERVIEW OF THE '825 PATENT

A. The '825 Patent Specification

29. The '825 patent, entitled “Reducing Redundant Operations Performed by Members of a Cooperative Security Fabric” was filed June 27, 2017 and claims priority to a provisional application filed on May 8, 2017. Ex. 1001.

30. 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.

31. A “fabric” is a term of art that was known at the time of the '825 patent. It is a network of interconnected network appliances that handles

bidirectional traffic coming in to and going out of the network. As I discuss below in the Claim Construction section, network fabrics were developed to handle increasingly large enterprise networks.

32. The '825 patent uses the term “fabric” (specifically a “cooperative security fabric”) according to its ordinary meaning, and the patent does not propose any special meaning. Specifically, the '825 patent describes that the fabric handles both “downstream network traffic” and “upstream network traffic” and also CSF member nodes send to and process data packets potentially 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:

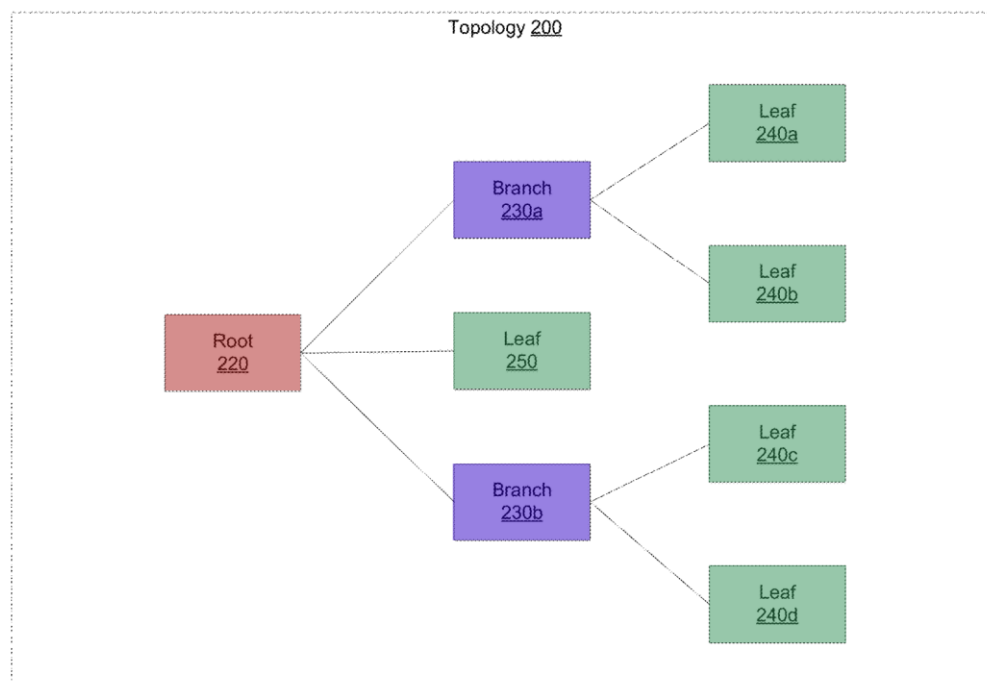


FIG. 2

33. In order to improve coordination, the '825 patent also describes that CSF member nodes determine which node the data packet came from, and whether that node is a CSF member node. 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.

34. Thus, the '825 patent describes that any given CSF member 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.

IV. OVERVIEW OF CERTAIN ART

35. Although the petition cites to a number of references, the main references it relies on for its challenge against the independent claims are Chandra (for Grounds 1-4) and Keohane (for Grounds 5-8). The petition's first ground of challenge asserts Chandra alone renders obvious the independent claims (as well as some of the dependent claims). The petition's fifth ground of challenge asserts that

Keohane alone renders obvious the independent claims (as well as some of the dependent claims). Below, I summarize Chandra and Keohane.

A. Chandra (Ex. 1008)

36. Chandra is clearly directed to managing **unidirectional** network traffic between two nodes. Ex. 1004, Abstract, ¶17. The below Figure 2 is annotated to show how traffic travels from the Transmitting CE to the Receiving CE, *i.e.* in only one direction.

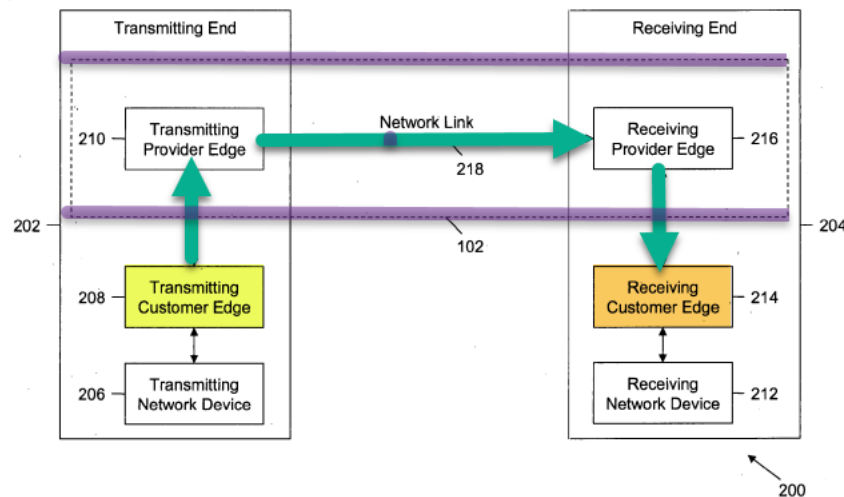


FIG. 2

37. In my opinion, Chandra does not disclose a “fabric” according to how that term was ordinarily understood by a POSITA at the time of the patent. This is because, among other things, Chandra discloses that it handles traffic in only one direction. What Chandra describes is a one-way tunnel between a **transmitting** end and a **receiving** end. Specifically, in Chandra, the transmitting CE is always the node that sets a “label indicating a first set of actions performed on the data packet”

and it is always the receiving CE that receives the data packet and uses the label “to determine a second set of actions that has to be performed on the data packet at a receiving end.” Ex. 1004, ¶18.

B. Keohane (Ex. 1008)

38. Like Chandra, in my opinion Keohane also fails to disclose a “fabric.” Keohane instead relates to a method for performing iterative security operations on incoming network traffic in a single direction. Ex. 1008, ¶¶33-37. Keohane’s method is depicted in Figure 3 below, as annotated by Petitioner:

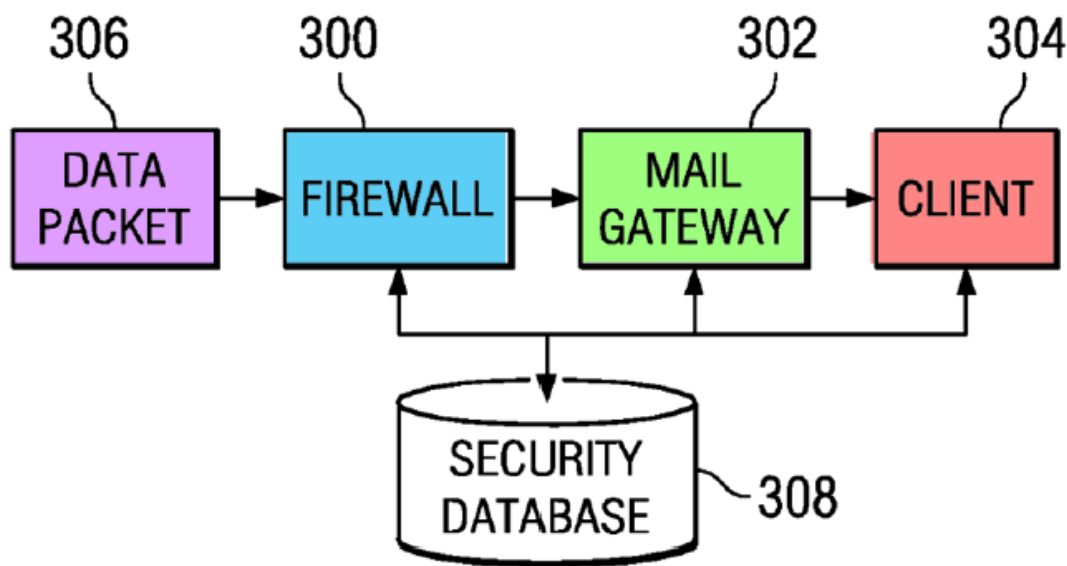


FIG. 3
(Annotated)

39. 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. Keohane's unidirectional tunnel is just like the one-way link disclosed in Chandra.

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 determine whether a previous security action has been performed by the upstream network element. *Id.*, ¶11. 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." *Id.*, ¶¶32-37.

V. CLAIM CONSTRUCTION

41. In my opinion, all claim terms should be given their ordinary meaning. I understand that Petitioner and Dr. Franz also agree that all the terms should be given their ordinary meaning. Pet. 19; Ex. 1003, ¶53.

42. However, as discussed herein, Petitioner applies "fabric" in a way that is not consistent with its ordinary meaning. In particular, Dr. Franz states in his declaration that he has "afforded [all claim terms] their ordinary and customary meaning in light of the intrinsic evidence" but then adopts a construction of "fabric" that does not accord with either the normal meaning or the meaning of the term as used in the '825 specification.

A. “fabric”

43. The plain and ordinary meaning of “fabric” as understood by a POSITA in view of the patent in 2017 requires, at a minimum, network nodes that process bidirectional communications.

44. By 2017, a network fabric was a term of art. As enterprise networks became larger and larger, a complex, interconnected topology known as a “fabric” was developed to handle the management of such networks. In particular, enterprise networks needed to support increasingly numerous subnetworks as a result of, for example, increases in the enterprise’s number of office locations, departments, enterprise functions, etc. Thus, 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. Naturally, 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. Without this ability to handle bidirectional traffic, a “fabric” would not be able to serve its purpose of managing all of the traffic of these large enterprise networks.

45. This plain understanding of a “fabric” is consistent with how the ’825 patent uses the term. The ’825 patent describes a fabric that is required to process ***bidirectional*** communication between its nodes. 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.”).

46. The ’825 patent also describes that member nodes of the fabric (specifically the cooperative security fabric) potentially handle traffic coming from any other member node, and therefore handles traffic from any direction. 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.

47. The plain meaning of a “fabric” is also supported by extrinsic evidence. 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.* These descriptions indicate that a fabric requires bidirectional communication, and is therefore consistent with the term’s plain meaning. Nodes that only handled network traffic in one direction would not be considered a “fabric” as Petitioner suggests by its definition.

48. Dr. Franz does not apply “fabric” according to its ordinary meaning. Dr. Franz instead describes “fabric” in terms of its functionality, claiming that “[t]he ’825 patent describes the CSF primarily by what it achieves—it ‘coordinates operations among members and avoids redundant operations.’” Ex. 1002, ¶70 (quoting Ex. 1001, 5:45-47). There are multiple issues with his description.

49. First, this description of the function of a CSF is merely one sentence in the specification and fails to account for specification’s numerous other descriptions. Also, while it is certainly true that a CSF “coordinates operations among members and avoids redundant operations,” this fails to assign any meaning to the word “fabric,” much less its plain meaning. Certainly a fabric that has “cooperative security” includes coordinating operations to avoid redundant

operations, but that says nothing about what a “fabric” *is*. For example, a “cooperative security network” could just as well “coordinate[] operations among members and avoid[] redundant operations,” and yet such a description says nothing about what a network is. And of course, a POSITA would not consider a “network” to be the same as a “fabric.”

50. Second, it is clear that Petitioner applies the term “fabric” in an unreasonably broad way. As discussed above, Chandra and Keohane are alleged to be fabrics, and yet neither handle bidirectional network communications. Petitioner thus ignores that the patent specifically requires that a “fabric” be able to handle bidirectional communications, which is how a POSITA would have understood the term in 2017.

51. Third, in my opinion, Petitioner’s description of a fabric would render the entire term “cooperative security fabric” superfluous. In particular, the independent claims, separate of a cooperative security fabric, already disclose “coordinat[ing] operations among members and avoid[ing] redundant operations.” Ex. 1001, 5:45-47. The independent claims disclose that a first network security appliance uses a flag to “determine[] whether the network traffic has been transmitted from a second network security appliance that is participating in the CSF,” “determin[e] one or more network security operations that are executed by the second network security appliance,” and “skip[] [the] operations that are

executed by the second network security appliance.” These limitations already satisfy “coordinat[ing] operations among members and avoid[ing] redundant operations.” Petitioner’s construction of fabric gives the term no meaning in the context of the claims.

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

52. In my opinion, Petitioner has not shown that Chandra renders claims 1-5, 12, 15-16, 21-22, and 27 obvious for two independent reasons. These reasons are that (1) Chandra does not disclose a “fabric” using its ordinary meaning, which requires processing of bidirectional communications, and (2) Chandra’s receiving CE does not use the “CE label” to determine whether the transmitting CE is “a second network security appliance that is participating in the CSF.”

A. Chandra does not disclose a “fabric”

53. In my opinion, Petitioner has not shown that Chandra discloses a “fabric,” much less a “cooperative security fabric.” Chandra does not, in fact, disclose a “fabric” as that term is ordinarily understood by a POSITA.

54. The ordinary meaning of “fabric” requires a topology of network devices that handle bidirectional communications. Chandra does not disclose a “fabric.”

55. Instead, Chandra only discloses two nodes: a receiving CE (214) and a transmitting CE (208), which Petitioner has asserted are the network security

appliances participating in a CSF. Pet. at 26-27. Chandra is clear that these two nodes only process network traffic in one direction, which is apparent from their names: the transmitting CE sends data in one direction to the receiving CE.

56. Specifically, Chandra says: “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 at ¶¶25-26.

57. Figure 2, as annotated by Patent Owner, depicts how network traffic travels through these two nodes:

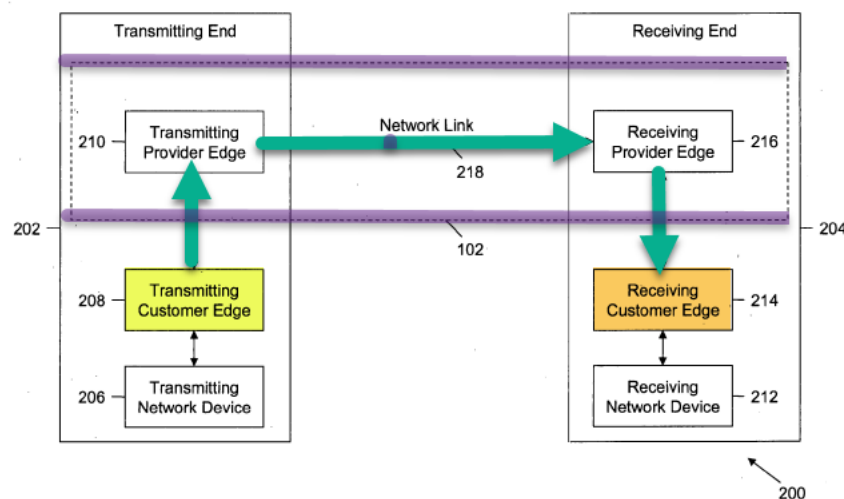


FIG. 2

58. 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).

59. In my opinion, it is clear this two-node unidirectional tunnel is not a “fabric” under its plain meaning. Processing of traffic only ever occurs in one direction, never in both directions. This makes such a system unsuitable for handling traffic for large, enterprise networks that were the impetus for creating network fabrics.

60. Thus, it is my opinion that Chandra does not disclose a “fabric” under its plain meaning and that this ground of challenge should be rejected.

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”

61. In my opinion, an independent reason for rejecting Ground 1 is that Petitioner has also not shown that Chandra discloses a first network security appliance “determining ... whether the network traffic has been transmitted from a second network security appliance that is participating in the CSF based on a flag.” In fact, Chandra does not disclose this limitation, because Chandra’s “CE label” does not provide information about whether the transmitting CE participates in the same CSF as the receiving CE.

62. Under Petitioner’s theory, the transmitting CE (208) (*i.e.* the alleged second network security appliance) performs an operation on a data packet and adds a “CE label” (*i.e.* the alleged flag), before transmitting it to the receiving CE (214) (*i.e.* the alleged first network security appliance). The receiving CE checks for the presence of a “CE label,” and Petitioner 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. at 31.

63. However, in my opinion, even under Petitioner’s theory, the receiving CE cannot use the CE flag to determine whether the network traffic was transmitted from “a second network security appliance that is participating in the CSF.” This is because the CE label only indicates that certain security operations were performed by the transmitting CE. There is no indication that the transmitting CE is participating in the same CSF as the receiving CE.

64. By contrast, the ’825 patent teaches how CSF member nodes can determine whether traffic comes from other member nodes that are participating in the CSF. In particular, a CSF member node 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 at 6:65-7:4.

65. 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. 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.

66. For these reasons, it is my opinion that Chandra does not disclose this limitation.

VII. GROUNDS 2, 3, AND 4 FAIL FOR THE SAME REASONS AS GROUND 1

67. Grounds 2, 3, and 4 of the petition challenge claims that are dependent on the independent claims challenged in Ground 1. Thus, they rely on the analysis of Ground 1. In my opinion, Grounds 2, 3, and 4 fail for the same reasons I discussed above with respect to Ground 1.

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

68. In my opinion, Petitioner has not shown that Keohane renders claims 1-5, 12, 15-16, 21-22, and 27 obvious for two independent reasons. These are similar reasons as explained for Chandra in Ground 1, *i.e.* because (1) Keohane does not disclose a “fabric” using its ordinary meaning, which requires processing of bidirectional communications, and (2) Keohane’s mail gateway does not use the “signature” to determine whether the firewall is “a second network security appliance that is participating in the CSF.”

A. Keohane does not disclose a “fabric”

69. In my opinion, Petitioner has not shown that Keohane discloses a “fabric,” much less a “cooperative security fabric.” Keohane does not, in fact, disclose a “fabric” as that term is ordinarily understood by a POSITA.

70. The ordinary meaning of “fabric” requires a topology of network devices that handle bidirectional communications. Keohane does not disclose such a “fabric,” because, like Chandra, it only discloses processing of ***unidirectional communications***.

71. Keohane discloses a system comprising firewall (300), mail gateway (302, and client (304) that can only process traffic in one direction: “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. In fact, Petitioner also describes Keohane in this way, stating that

“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). Petitioner admits there are dedicated downstream devices, *i.e.* devices that are always downstream of other devices.

72. Indeed, it is clear that Keohane only describes processing of unidirectional communication because every embodiment in Keohane describes that the first appliance “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. A network security appliance (such as a firewall) that protects a subnetwork checks if data coming from an external network into the subnetwork is from a trustworthy source, but does not (usually) need to check if data traveling from the subnetwork to an outside network comes from a trustworthy source.

73. The one-way tunnel of Keohane is depicted in Figure 3, which is annotated by Petitioner below:

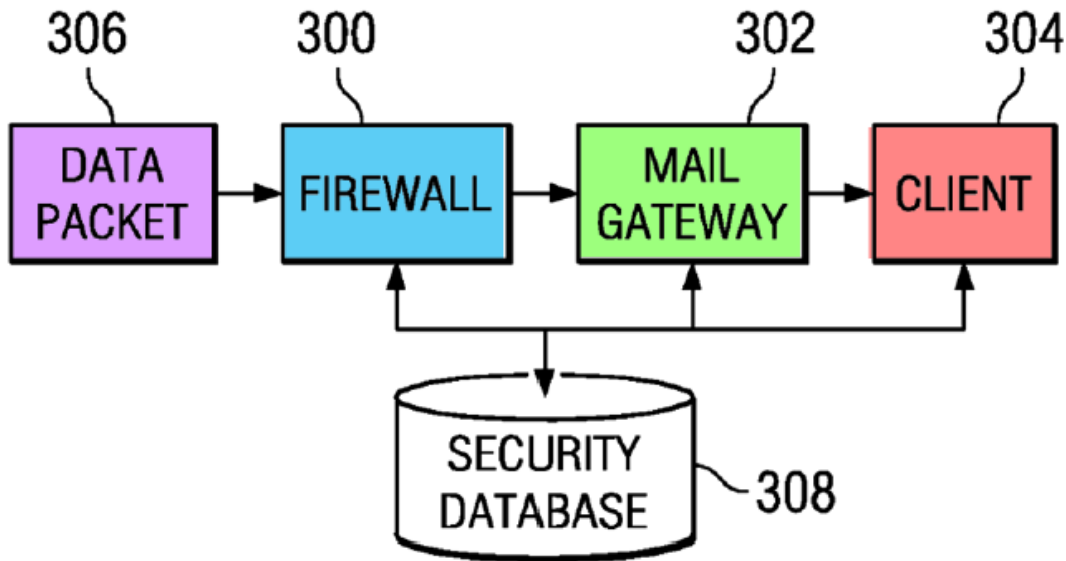


FIG. 3
(Annotated)

74. 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.

75. In my opinion, it is clear this unidirectional tunnel is not a “fabric” under its plain meaning. Processing of traffic only ever occurs in one direction, never in both directions. This makes such a system unsuitable for handling traffic for large, enterprise networks that were the impetus for creating network fabrics.

76. Thus, it is my opinion that Keohane does not disclose a “fabric” under its plain meaning and that this ground of challenge should be rejected.

B. Keohane 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”

77. In my opinion, an independent reason for rejecting Ground 5 is that Petitioner has also not shown that Keohane discloses a first network security appliance “determining ... whether the network traffic has been transmitted from a second network security appliance that is participating in the CSF based on a flag.” In fact, Keohane does not disclose this limitation, because Keohane’s “signature” only indicates which operations have already been performed on the data packet and otherwise provides no information about which node transmitted the data packet, or whether that node is participating in a CSF, or whether that node is participating in the same CSF as the recipient of the data packet.

78. Under Petitioner’s theory, the firewall (300) (*i.e.* the alleged second network security appliance) performs an operation on a data packet and adds a “signature” (*i.e.* the alleged flag), before transmitting it to the mail gateway (302) (*i.e.* the alleged first network security appliance). 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.

79. However, in my opinion, even under Petitioner’s theory, the mail gateway (302) cannot use the “signature” to determine whether the network traffic was transmitted from “a second network security appliance that is participating in the CSF.” This is because Keohane is clear that the signature merely “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.

80. By contrast, and as I already noted above in Ground 1, the ’825 patent teaches how CSF member nodes can determine whether traffic comes from other member nodes that are participating in the CSF. In particular, a CSF member node 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 at 6:65-7:4.

81. 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. 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—Keohane’s “signature” is only described as merely “indicat[ing] that a security action has been performed on data packet 306.” Ex. 1008 at ¶34.

82. For these reasons, it is my opinion that Keohane does not disclose this limitation.

IX. GROUNDS 6, 7, AND 8 FAIL FOR THE SAME REASONS AS GROUND 5

83. Grounds 6, 7, and 8 of the petition challenge claims that are dependent on the independent claims challenged in Ground 5. Thus, they rely on the analysis of Ground 5. In my opinion, Grounds 6, 7, and 8 fail for the same reasons I discussed above with respect to Ground 1.

X. CONCLUSION

84. In signing this declaration, I recognize that the declaration will be filed as evidence in a contested case before the Patent Trial and Appeal Board of the United States Patent and Trademark Office. I also recognize that I may be subject to

cross-examination in the case and that cross-examination will take place within the United States. If cross-examination is required of me, I will appear for cross-examination within the United States during the time allotted for cross-examination.

85. I hereby declare that all statements made herein of my own knowledge are true and that all statements made on the information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code.

Executed: June 20, 2023

A handwritten signature in black ink, appearing to read 'J. Black Jr.', written over a horizontal line.

John Black Jr., Ph.D.