

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

CISCO SYSTEM, INC.,
Petitioner,

v.

UMBRA TECHNOLOGIES LTD.,
Patent Owner.

IPR2024-00498
Patent 10,574,482 B2

Before ST. JOHN COURTENAY III, MICHAEL R. ZECHER, and
GREGG I. ANDERSON, *Administrative Patent Judges*.

ZECHER, *Administrative Patent Judge*.

DECISION
Denying Institution of *Inter Partes* Review
35 U.S.C. § 314

I. INTRODUCTION

Petitioner, Cisco Systems, Inc. (“Cisco”), filed a Petition requesting an *inter partes* review (“IPR”) of claims 1–26 of U.S. Patent No. 10,574,482 B2 (Ex. 1001, “the ’482 patent”). Paper 1 (“Pet.”). Patent Owner, UMBRA Technologies Ltd. (“UMBRA”), filed a Preliminary Response. Paper 6 (“Prelim. Resp.”). With our authorization, Cisco filed a Preliminary Reply (Paper 10 (“Prelim. Reply”)), and UMBRA filed a Preliminary Sur-reply (Paper 11 (“Prelim. Sur-reply”)). See Paper 9. Cisco’s Preliminary Reply and UMBRA’s Preliminary Sur-reply each were tailored narrowly to address the following two issues: (1) the scope and meaning of the claim term “access point server”; and (2) UMBRA’s arguments presented in the Preliminary Response that implicate the claim terms “first perimeter firewall” and “second perimeter firewall.” *Id.* at 3.

Based on the authority delegated to us by the Director under 37 C.F.R. § 42.4(a), we may not institute an IPR unless the information presented in the Petition and any response thereto shows “there is a reasonable likelihood that the petitioner would prevail with respect to at least 1 of the claims challenged in the petition.” 35 U.S.C. § 314(a) (2024). Taking into account UMBRA’s Preliminary Response, Cisco’s Preliminary Reply, and UMBRA’s Preliminary Sur-reply, we conclude that the information presented in the Petition does not establish that there is a reasonable likelihood that Cisco would prevail in challenging any one of claims 1–26 of the ’482 patent as unpatentable. We, therefore, *deny* Cisco’s Petition.

A. Real Party in Interest (“RPI”)

Cisco identifies itself as the only RPI. Pet. 64. UMBRA identifies itself as the only RPI. Paper 4 (UMBRA’s Mandatory Notice Information Under 37 C.F.R. § 42.8(a)(2)), 2.

B. Related Matters

The parties indicate that the ’482 patent is involved in the following two district court cases: (1) *UMBRA Technologies Ltd. (UK) v. Cisco Systems, Inc.*, No. 1:23-cv-00903-DII (W.D. Tex.); (2) *UMBRA Technologies Ltd. (UK) v. VMware, Inc.*, No. 1:23-cv-00904-DII (W.D. Tex.). Pet. 65; Paper 4, 2. UMBRA indicates that the ’482 patent is currently the subject of U.S. Reexamination Control No. 90/019,363. Paper 4, 2.

The parties also identify the following patent and patent applications as related to the ’482 patent: (1) U.S. Patent No. 11,271,778 B2; (2) U.S. Patent Application No. 17/686,870; (3) PCT/IB2016/000528; (4) PCT/IB2016/000528. Paper 4, 2; Ex. 1013.

C. The ’482 Patent

The ’482 patent, titled “Multi-Perimeter Firewall in the Cloud,” issued from U.S. Patent Application No. 15/563,261, filed on April 7, 2016. Ex. 1001, codes (54), (45), (21), (22). The ’482 patent claims the benefit of the following two provisional applications: (1) U.S. Provisional Patent Application 62/151,174, filed on April 22, 2015; and (2) U.S. Provisional Patent Application No. 62/144,293, filed on April 7, 2015. *Id.* at code (60).

The ’482 patent generally relates to network security in “a global virtual network or similar network by the strategic positioning of distributed firewall (FW) devices placed at multiple perimeters in the cloud.” Ex. 1001,

1:15–19. The ’482 patent states that “[h]igh latency combined with high packet loss” in online systems such as thin-client to cloud-based servers, customer relationship management, enterprise resource planning, or other systems “can make a connection unusable.” *Id.* at 1:25–30. “Even if data gets through,” slow speeds result in poor user experience, which, in turn, can result in “refusal by users to accept those conditions in effect rendering poorly delivered services as useless.” *Id.* at 1:30–34. Although “last mile connectivity” has vastly improved, problems persist with “long distance connectivity and throughput due to issues related to distance, protocol limitations, peering, interference and other problems,” thereby necessitating a solution for “secure network optimization services running over the top of standard internet connections.” *Id.* at 2:26–32.

The ’482 patent purports to address these issues by providing “[s]ystems and methods for providing multi-perimeter firewalls via a virtual global network.” Ex. 1001, 2:36–37. Figure 12 of the ’482 patent, reproduced below, illustrates one embodiment for a multi-perimeter firewall in the cloud enabled by a global virtual network. *Id.* at 3:33–34.

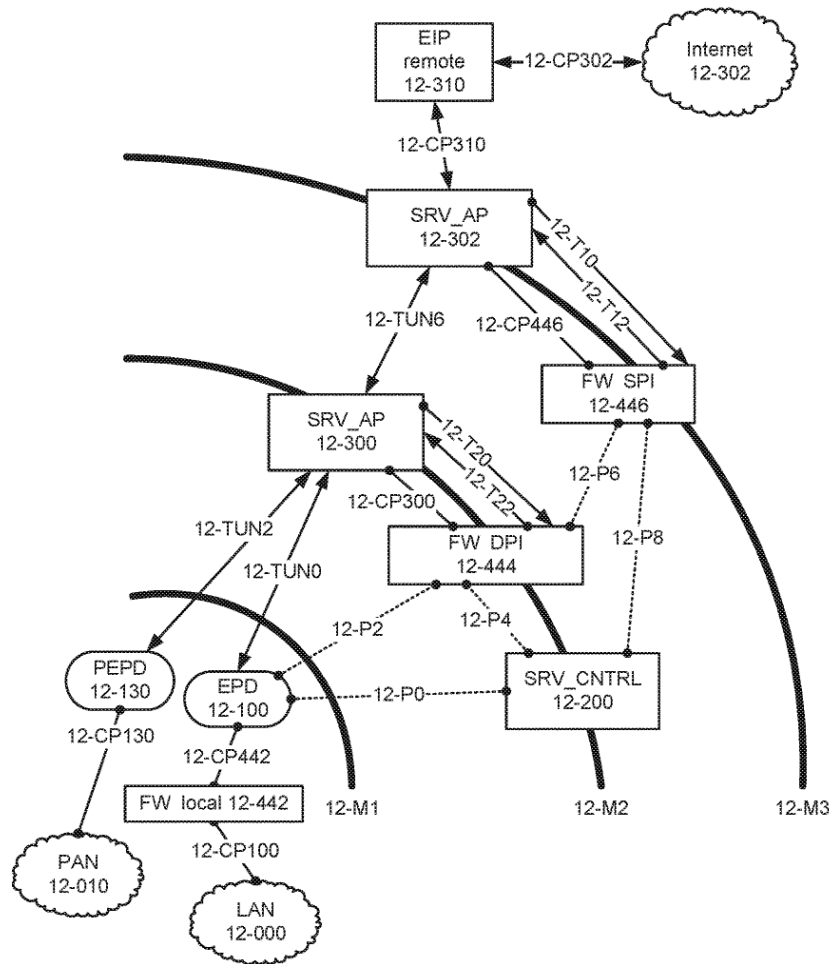


Figure 12, reproduced above, illustrates three perimeters 12-M1, 12-M2, and 12-M3 with access point server 12-302 located at a perimeter 12-M3 and access point server 12-300 located at the perimeter 12-M2. Ex. 1001, 13:64–14:4. Local firewall 12-442, which is an example of a firewall that a client may use to protect their local area network (“LAN”) from internet-based threats, is located between the endpoint device 12-100 and LAN 12-000. *Id.* at 14:17–24. The other types of firewalls illustrated in Figure 12 are firewall stateful packet inspection (“FW SPI”) 12-446 located at perimeter 12-M3, which provides stateful packet inspection (“SPI”), and firewall deep packet inspection (“FW DPI”) 12-444 located at perimeter 12-M2, which provides deep packet inspection (“DPI”). *Id.* at 14:24–27.

The '482 patent describes SPI as inspection that “examines the headers of packets to look for malformed information, or for patterns, or to match IP [Internet Protocol] address or port or other information from its list of known threats against the current flow of packets.” Ex. 1001, 14:30–34. The '482 patent describes DPI as inspection that “takes a deeper look at the whole packet and in the case of a multi-part, multi-packet transmission, will look at the compilation of a series of a packets to gain insight into the data being transferred.” *Id.* at 14:33–37. Turning back to Figure 12 of the '482 patent, traffic flows from the egress ingress point remote 12-310 to access point server 12-302, and then to FW SPI 12-446 located at perimeter 12-M3. *Id.* at 14:49–54. At the next perimeter 12-M2, all traffic flows through FW DPI 12-444 or, alternatively, FW DPI 12-444 just receives a cloned copy of traffic from access point server 12-300. *Id.* at 14:60–63.

D. Challenged Claims

Of the challenged claims, claims 1 and 13 are independent claims. Independent claims 1 and 13 are each directed to “[a] multi-perimeter firewall system located in a cloud and forming part of a global virtual network.” Ex. 1001, 25:63–64, 27:1–2. Claims 2–12 directly or indirectly depend from independent claim 1; and claims 14–26 directly or indirectly depend from independent claim 13. *Id.* 26:23–67, 27:29–28:38. Independent claim 1 is illustrative of the challenged claims and is reproduced below:

1. A multi-perimeter firewall system located in a cloud and forming part of a global virtual network, comprising:
 - an egress ingress point device;
 - a first access point server in communication with the egress ingress point device;

a second access point server in communication with the first access point sever;

an endpoint device in communication with the second access point server;

a first perimeter firewall in communication with the first access point server, wherein the first perimeter firewall performs stateful packet inspection to prevent at least some traffic from passing from the first access point server to the second access point server; and

a second perimeter firewall in communication with the second access point server, wherein the second perimeter firewall performs deep packet inspection to prevent at least some traffic from passing from the second access point server to the end point device,

wherein at least one of the egress ingress point device, the first access point server, the second access point server, the endpoint device, the first perimeter firewall, or the second perimeter firewall comprises hardware,

wherein the deep packet inspection is performed on a cloned copy of traffic that flows through the second perimeter firewall.

Ex. 1001, 25:62–26:22.

E. Asserted Prior Art References

Cisco relies on the prior art references set forth in the table below.

Name¹	Reference	Dates	Exhibit No.
Shieh	US 8,955,093 B2	issued Feb. 10, 2015; filed Apr. 10, 2013	1004
Potti	US 2007/0156919 A1	published July 5, 2007; filed June 21, 2006	1005

¹ For clarity and ease of reference, we only list the first named inventor.

F. Asserted Grounds of Unpatentability

Cisco challenges claims 1–26 of the ’482 patent based on the asserted ground of unpatentability set forth in the table below. Pet. 19–58.

Claims Challenged	35 U.S.C. §	Reference(s)/Basis
1–26	103 ²	Shieh, Potti

II. ANALYSIS

A. Claim Construction

In this IPR, claim terms are construed using the same claim construction standard as in a civil action under 35 U.S.C. § 282(b). *See* 37 C.F.R. § 42.100(b) (2024). That is, claim terms generally are construed in accordance with their ordinary and customary meaning, as would have been understood by a person of ordinary skill in the art, in view of the specification and the prosecution history pertaining to the patent at issue. *See id.* The ordinary and customary meaning of a claim term “is its meaning to the ordinary artisan after reading the entire patent,” and “as of the effective filing date of the patent application.” *Phillips v. AWH Corp.*, 415 F.3d 1303, 1313, 1321 (Fed. Cir. 2005) (en banc).

In its Petition, Cisco proposes that “each claim term in the Challenged Claims be given its plain and ordinary meaning,” and contends that “no specific construction of any claim term is required because the prior art

² The Leahy-Smith America Invents Act (“AIA”), Pub. L. No. 112-29, 125 Stat. 284, 287–88 (2011), amended 35 U.S.C. § 103, effective March 16, 2013. Because the ’482 patent claims the benefit of two provisional patent applications that were filed after this date, the post-AIA version of § 103 applies. Ex. 1001, code (60).

relied on in [the] Petition meets each of the claim terms under any reasonable construction.” Pet. 13. In its Preliminary Response, UMBRA proposes a construction for the claim term “access point server.” Prelim. Resp. 3–9.

In its Preliminary Reply, Cisco argues that “Shieh discloses *access point servers* even under [UMBRA’s] restrictive definition,” but Cisco does not propose its own construction for the claim term “access point server.” Prelim. Reply 1–3. In its Preliminary Sur-Reply, UMBRA maintains that its proposed construction of the claim term “access point server” found in its Preliminary Response is correct. Prelim Sur-reply 1–3.

We need not construe the claim term “access point server” identified by UMBRA and opposed by Cisco because, as we explain below, the Petition includes the following two deficiencies: (1) inconsistent claim mapping; and (2) insufficient rationale to combine the teachings of Shieh with those of Potti.

*B. Obviousness Over the Combined Teachings of
Shieh and Potti*

Cisco contends that claims 1–26 of the ’482 patent are unpatentable under § 103 as obvious over the combined teachings of Shieh and Potti. Pet. 20–58. Cisco contends that the combined teachings of Shieh and Potti account for the subject matter of each challenged claim, but does not provide sufficient reasoning as to why a person of ordinary skill in the art would have been prompted to combine the teachings of these references. *Id.* Cisco also relies on the testimony of Dr. A.L. Narasimha Reddy to support its positions. *See* Ex. 1003.

Based on the current record, we determine that Cisco has not shown that there is a reasonable likelihood that it would prevail in challenging any one of claims 1–26 of the ’482 patent as unpatentable. We begin our analysis with the principles of law that generally apply to a ground based on obviousness, an assessment of the level of skill in the art, followed by brief overviews of Shieh and Potti, and then we focus on two deficiencies in the Petition.

1. Principles of Law

A claim is unpatentable under § 103 if the differences between the claimed subject matter 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 to which said subject matter pertains. *KSR Int’l Co. v. Teleflex Inc.*, 550 U.S. 398, 406 (2007). The question of obviousness is resolved on the basis of underlying factual determinations, including (1) the scope and content of the prior art; (2) any differences between the claimed subject matter and the prior art; (3) the level of skill in the art; and (4) when in evidence, objective indicia of non-obviousness (i.e., secondary considerations, such as commercial success, long-felt but unresolved needs, failure of others, etc.).³ *Graham v. John Deere Co.*, 383 U.S. 1, 17–18 (1966).

An invention “composed of several elements is not proved obvious merely by demonstrating that each of its elements was, independently, known in the prior art.” *KSR*, 550 U.S. at 418. The obviousness evaluation

³ In its Preliminary Response, UMBRA does not present arguments or evidence of secondary considerations. *See* Prelim. Resp.

“should be made explicit,” and “it can be important to identify a reason that would have prompted a person of ordinary skill in the relevant field to combine the elements in the way the claimed new invention does.” *Id.* Furthermore, “[t]o satisfy its burden of proving obviousness, a petitioner cannot employ mere conclusory statements. The petitioner must instead articulate specific reasoning, based on evidence of record, to support the legal conclusion of obviousness.” *In re Magnum Oil Tools Int’l, Ltd.*, 829 F.3d 1364, 1380 (Fed. Cir. 2016). We analyze the asserted grounds based on obviousness with the principles identified above in mind.

2. *Level of Skill in the Art*

At this stage in the proceeding, there is sufficient evidence in the current record that enables us to determine the knowledge level of a person of ordinary skill in the art. Relying on the testimony of Dr. Reddy, Cisco argues the following:

a [person of ordinary skill in the art] in April 2015 timeframe would have been familiar with communication networks having a distribute firewall system in the cloud. A [person of ordinary skill in the art] would have a working knowledge of the function performed by firewalls including stateful inspection and deep packet inspection.

A [person of ordinary skill in the art] would have gained knowledge of these concepts through a mixture of training and work experience, such as by having a Bachelor’s degree in computer science and two years of experience; or by obtaining a Master’s degree in computer science, but having only one year of experience; or by having no formal education but experience in computer network security of at least four years.

Pet. 14 (citing Ex. 1003 ¶ 40). UMBRA does not address the level of skill in the art in its Preliminary Response. *See* Prelim. Resp. 1–16.

To the extent necessary, and for purposes of this Decision, we adopt Cisco’s assessment of the level of skill in the art because it is supported by the testimony of Dr. Reddy and it is consistent with the ’482 patent and the asserted prior art.

3. Overview of Shieh

Shieh generally relates to “network security” and, more specifically, “to enabling network security with network equipment.” Ex. 1004, 1:12–15. Figure 1 of Shieh, reproduced below, illustrates one embodiment of a network configuration. *Id.* at 1:35–37.

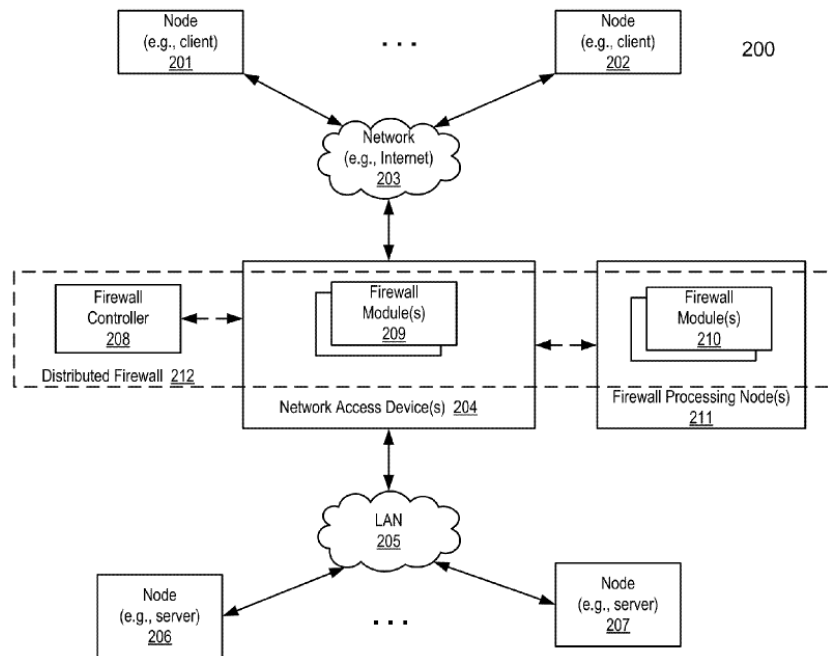


FIG. 1

Figure 1 illustrates an example of network configuration including network access device(s) 204, which may be a router, gateway, switch or an access point, that provides an interface between network 203 and LAN 205. Ex. 1004, 2:60–65. Network access device(s) 204 are associated with distributed firewall 212 that further includes various firewall processing

modules, where “each firewall [processing] module is responsible for performing one or more firewall functions, but does not include all of the firewall functions of a firewall.” *Id.* at 3:5–11. “Examples of the firewall functions include . . . network address translation (NAT), virtual private network (VPN), deep packet inspection (DPI), and anti-virus.” *Id.* at 3:11–14.

Figure 3 of Shieh, reproduced below, illustrates one embodiment of a distributed firewall. Ex. 1004, 1:44–46.

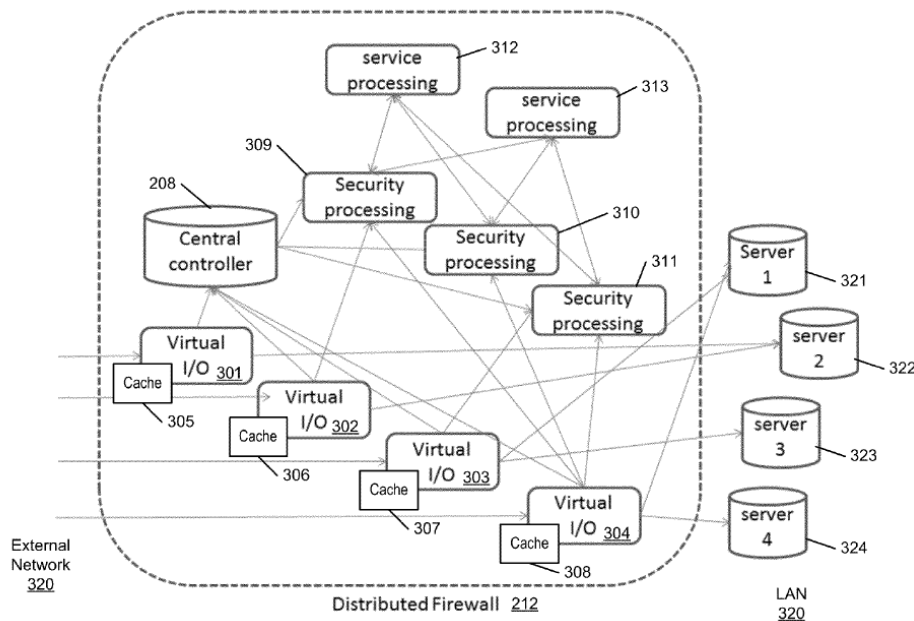


FIG. 3

Figure 3 illustrates that distributed firewall 212 includes four different types of modules, including virtual input/output (“I/O”) modules 301–304, security processing modules 309–311, service processing modules 312 and 313, and central controller 208. *Id.* at 7:14–18. According to Shieh, all of these modules “can run on the same virtual machine, or on different virtual machines, or on same or different physical hosts.” *Id.* at 7:18–20. “Each of

virtual I/O modules 301-304 receives packets from any of servers 321-324,” and “sends packets to external network 315 outside of the firewall.” *Id.* at 7:32–35. Security processing modules 309–311 are capable of “receiv[ing] packets and run[ning] the packets through one or more various security functions in the module for security processing.” *Id.* at 7:55–58. Shieh also discloses that “[t]here could be several security modules and each handles the same or different security functions.” *Id.* at 7:58–60. Furthermore, Shieh contemplates dividing a firewall into different modules, which “allows putting virtual I/O and security processing functions at the best locations to protect the network entrance, while keeping the central control and monitoring functionality at the central controller.” *Id.* at 8:33–37.

4. Overview of Potti

Potti generally relates to “network elements in computer networks” and, more specifically, “to enforcing network service level agreements.” Ex. 1005 ¶ 3. Figure 26A, reproduced below, illustrates a flow diagram of a process of enforcing network service level agreements in a network element according to one embodiment. *Id.* ¶ 45.

Fig. 26A

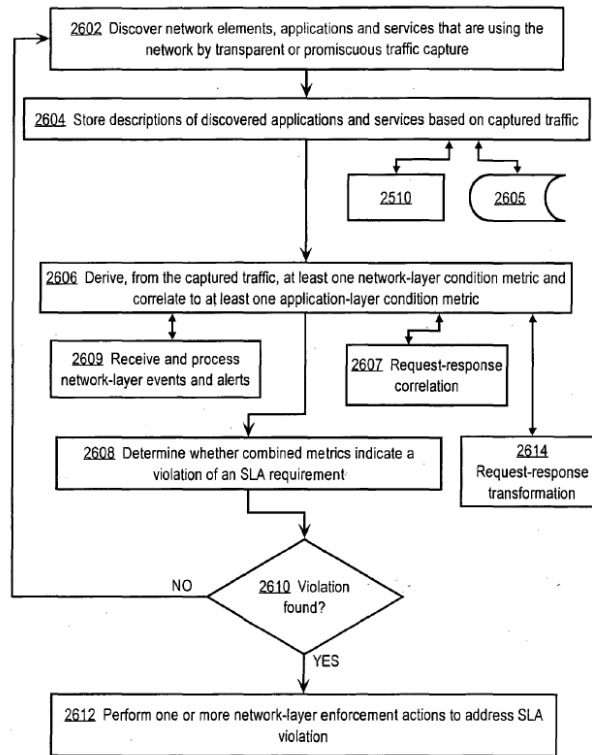


Figure 26A illustrates that, at step 2602, “the process discovers one or more network elements, applications and services that are using the network, by transparent or promiscuous traffic capture.” *Id.* ¶ 345. In one embodiment of the invention, step 2602 “comprises receiving packets in the network element, forwarding the packets to a next hop, and concurrently copying the packets without modification and without interrupting the flow of traffic through the network element.” *Id.* The copied packets are then subject to “deep packet inspection in which values of the IP header, [transmission control protocol] header and application-layer payload are examined.” *Id.*

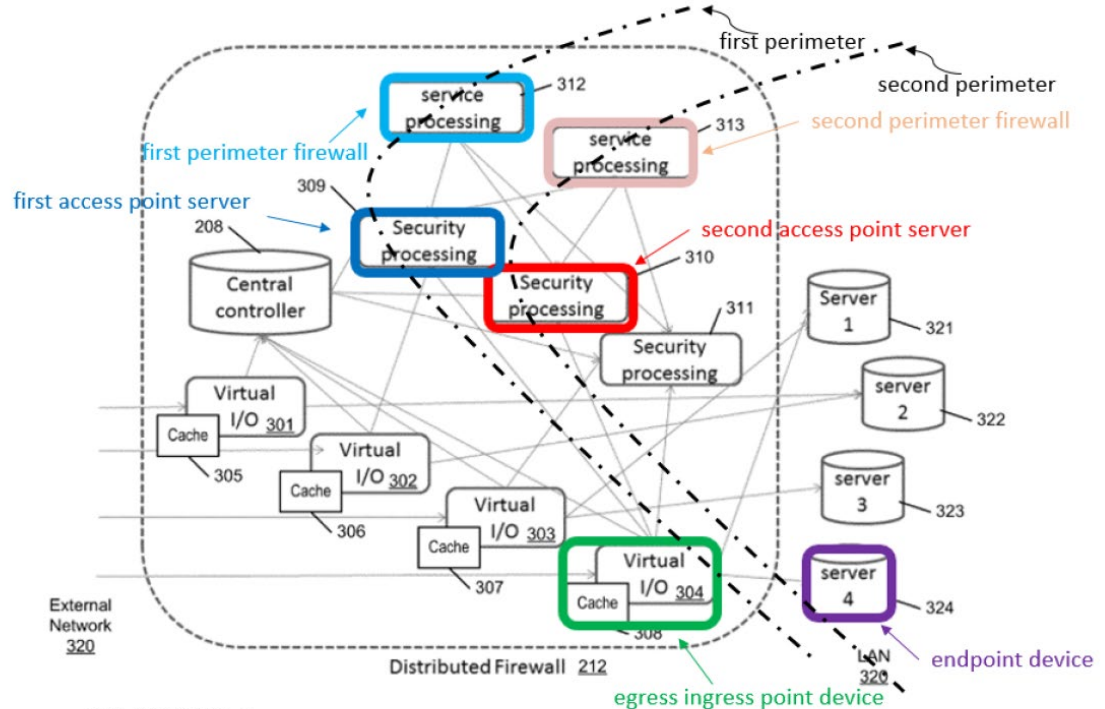
5. Claims 1 and 13

“In an IPR, the petitioner has the burden from the onset to show with particularity why the patent it challenges is unpatentable.” *Harmonic Inc. v.*

Avid Tech., Inc., 815 F.3d 1356, 1363 (Fed. Cir. 2016) (citing 35 U.S.C. § 312(a)(3) (requiring an IPR petition to identify “with particularity . . . the evidence that supports the grounds for the challenge to each claim”)). This burden of persuasion does not shift to the patent owner. *See Dynamic Drinkware, LLC v. Nat’l Graphics, Inc.*, 800 F.3d 1375, 1378 (Fed. Cir. 2015) (discussing the burden of proof in an IPR). Keeping in mind that Cisco has the burden of persuasion, we address the following two deficiencies in the Petition: (1) inconsistent claim mapping; and (2) insufficient rationale to combine the teachings of Shieh with those of Potti.

a. Inconsistent Claim Mapping

Cisco contends that Shieh discloses a distributed firewall system located in a cloud using virtual machines located at several perimeters. Pet. 29. Cisco’s presents an annotated, color-coded version of Figure 3 of Shieh, reproduced below, that illustrates how Shieh’s distributed firewall teaches most of the limitations of independent claims 1 and 13. *Id.* at 32.



EX-1004 FIG. 3

FIG. 3

In Cisco’s annotated, color-coded version of Figure 3 of Shieh, Cisco contends that Shieh’s virtual I/O 304 and corresponding cache (green) teaches the claimed “egress ingress point device,” security processing module 309 (dark blue) teaches the claimed “first access point server,” security processing module 310 (red) teaches the claimed “second access point server,” server 4 324 (purple) teaches the claimed “endpoint device,” service processing module 312 (light blue) teaches the claimed “first perimeter firewall,” and service processing module 313 (pink) teaches the claimed “second perimeter firewall.” *Id.* at 29–43 (addressing the limitations of independent claim 1), 51–54 (relying on the same arguments and evidence presented for independent claim 1 to address the limitations of independent claim 13). Cisco, however, is inconsistent with its proposed claim mapping.

As one example, when addressing limitation [1.2], which recites “a first access point server in communication with the egress ingress point device,” Cisco relies on Shieh’s security processing module 309 (blue) to teach the claimed “*first access point server*.” Pet. 33–34 (citing Ex. 1004, 9:9–12, Fig. 6). When addressing limitation [1.5], which recites, in relevant part, “a first perimeter firewall in communication with the first access point server,” Cisco departs from its initial claim mapping by relying on security processing module 310 (red) to teach the claimed “*first access point server*.” *Id.* 36 (citing Ex. 1004 8:1–13). Cisco then appears to revert back to its initial claim mapping two pages later, stating that “[a]fter processing by servicing processing module 312 (*first perimeter firewall*), the packets then are sent back to the same security processing module 309 (*first access point server*) for the next security function processing.” *Id.* at 38 (citing Ex. 1004 8:1–13). In our view, this example of inconsistent claim mapping is not dispositive, but it is exemplary of the weaknesses in the Petition that are further amplified by Cisco’s insufficient rationale to combine the teachings of Shieh with those of Potti, which we discuss below.

b. Insufficient Rationale to Combine

Cisco also contends that Shieh teaches all limitations of independent claims 1 and 13, except Shieh does not teach limitations [1.8] and [13.8], each of which require performing “deep packet inspection . . . on a cloned copy of traffic that flows through the second perimeter firewall.” Pet. 41–43 (addressing limitation [1.8]), 54 (relying on the same arguments and evidence presented for limitation [1.8] to address limitation [13.8]). Cisco relies on Potti’s disclosure of performing DPI on a cloned copy of traffic, together with the general background knowledge of a person of

ordinary skill in the art, to teach or suggest these limitations. *Id.* at 42–43 (citing Ex. 1004, 4:38–44; Ex. 1005 ¶ 345; Ex. 1003 ¶¶ 130, 131, 134, 136), 54.

Turning to the rationale to combine, Cisco contends that, “[t]o the extent that [UMBRA] asserts that a [person of ordinary skill in the art] would not understand Shieh to disclose performing DPI on a cloned copy of traffic, it would be obvious for a [person of ordinary skill in the art] to modify the teachings of Shieh to include DPI on a cloned copy of traffic.” Pet. 42 (citing Ex. 1003 ¶ 131). To support this argument, Cisco refers back to its “State of the Art” section, and asserts that “performing deep packet inspection on a cloned copy of traffic was well-known and provided several benefits.” *Id.* Cisco then argues that Potti discloses performing DPI on a cloned copy of traffic “because deep packet inspection can be time consuming and interrupt traffic flow, allowing packets to be forwarded to their destination while cloned copies are inspected allows traffic to flow without interrupting the flow of traffic through the network element.” *Id.* (citing Ex. 1005 ¶ 345).

Notably absent from the “State of the Art” section is a specific reason why a person of ordinary skill would take Potti’s disclosure of performing DPI on a cloned copy of traffic and apply it to Shieh’s service processing module 313, which Cisco relies on to teach the claimed “second perimeter firewall.” *See* Pet. 15–19; *see also id.* at 40 (arguing that Shieh’s service processing module 313 (pink) teaches the claimed “second perimeter firewall”). Instead, Cisco generally discusses the evolution of firewall technology and its move to the

cloud as of April 2015, but does not identify the benefits that result from modifying Shieh in this way.

At best, Cisco asserts that “[t]he prior art references, and the discussions of what was known to a [person of ordinary skill in the art], provide the factual support for the general description of the state of the art at the time of the invention, and provide additional motivation to modify or combine the references.” Pet. 15. In our view, merely providing a general description of the state of the art and asserting that it provides a motivation to combine, without providing the necessary factual underpinnings to support the purported benefits that result for combining the relevant teachings of Shieh and Potti, is akin to stating in a conclusory fashion that this proposed combination “would have been obvious.” *See In re Van Os*, 844 F.3d 1359, 1362 (Fed. Cir. 2017) (explaining that “a finding that a combination of prior art would have been ... ‘intuitive’ is no different than merely stating the combination ‘would have been obvious’ ”).

Cisco also contends that a person of ordinary skill in the art would have understood that the speed and low latency requirements presented in Shieh “*could be* fulfilled by performing DPI on cloned copies.” Pet. 42–43 (emphasis added) (citing Ex. 1003 ¶ 134). Cisco further argues that “a [person of ordinary skill in the art] understood that implementing a security processing function in Shieh that performed deep packet inspection of clone traffic that required low latency as taught by Potti *could be* implemented successfully using well-known techniques. *Id.* at 43 (emphasis added) (citing Ex. 1003 ¶ 136).

In our view, Cisco does not explain the purported “well-known techniques” that a person of ordinary skill would have used to combine Shieh’s service processing module 313 with Potti’s disclosure of performing DPI on a cloned copy of traffic. Cisco merely indicates that a skilled artisan *could have* made such modifications to arrive at the claimed invention, but that, by itself, does not establish that a person of ordinary skill *would have* made such modifications. *See Belden v. Berk-Tek LLC*, 805 F.3d 1064, 1073 (Fed. Cir. 2015) (stating that “obviousness concerns whether a skilled artisan not only *could have made* but *would have been motivated to make* the combinations or modifications of prior art to arrive at the claimed invention”) (citing *InTouch Technologies, Inc. v. VGO Communications, Inc.*, 751 F.3d 1327, 1352 (Fed. Cir. 2014)).

A review of Cisco’s testimony from its declarant, Dr. Reddy, reveals no additional explanation as to why a person of ordinary skill would have been motivated to combine the teachings of Potti with those of Shieh. *See* Ex. 1003 ¶¶ 130–137. These portions of Dr. Reddy’s testimony merely parrot the arguments presented by Cisco in the Petition. That is, he relies on a general description of the state of the art, without providing any additional explanation beyond the bare assertion in the Petition that a person of ordinary skill would have used purported “well-known techniques” to combine Shieh’s service processing module 313 with Potti’s disclosure of performing DPI on a cloned copy of traffic.

For all the reasons we identify above, we are not persuaded that Cisco presents a sufficient rationale to combine the teachings of Shieh with those of Potti in the manner required to account for all the limitations of independent claim 1 and 13.

c. Summary

Accordingly, Cisco has not shown a reasonable likelihood that it would prevail on its assertions that the subject matter of independent claims 1 and 13 would have been obvious over the combined teachings of Shieh and Potti.

6. Claims 2–12 and 14–26

By virtue of their dependency, claims 2–12 and 14–26 include the same limitations as either independent claim 1 or 13. Cisco does not present arguments or evidence with respect to these dependent claims that remedy the deficiencies in its analysis of the combined teachings of Shieh and Potti that we identify above. *See* Pet. 43–51, 54–58. Accordingly, for the same reasons we discuss above with respect to independent claims 1 and 13, Cisco has not shown a reasonable likelihood that it would prevail on its assertions that the subject matter of dependent claims 2–12 and 14–26 would have been obvious over the combined teachings of Shieh and Potti.

III. CONCLUSION

Taking into account UMBRA’s Preliminary Response, Cisco’s Preliminary Reply, and UMBRA’s Preliminary Sur-reply, we conclude that the information presented in the Petition does not demonstrate that there is a reasonable likelihood that Cisco would prevail in challenging any one of claims 1–26 of the ’482 patent as unpatentable.

IV. ORDER

In consideration of the foregoing, it is ORDERED that the Petition is *denied* and no trial is instituted.

IPR2024-00498
Patent 10,574,482 B2

FOR PETITIONER:

Patrick D. McPherson
Patrick Muldoon
Joseph Powers
DUANE MORRIS LLP
pdmcpherson@duanemorris.com
pcmuldoon@duanemorris.com
japowers@duanemorris.com

FOR PATENT OWNER:

Greg H. Gardella
James E. Harris
Michael A. Dorfman
GARDELLA GRACE P.A.
ggardella@gardellagrace.com
jharris@gardellagrace.com
mdorfman@gardellagrace.com