

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

FORESCOUT TECHNOLOGIES, INC.,
Petitioner,

v.

FORTINET, INC.,
Patent Owner.

IPR2021-01329
Patent 9,894,034 B2

Before MICHAEL R. ZECHER, THOMAS L. GIANNETTI, and
CHRISTOPHER L. OGDEN, *Administrative Patent Judges*.

GIANNETTI, *Administrative Patent Judge*.

JUDGMENT
Final Written Decision
Determining Some Challenged Claims Unpatentable
35 U.S.C. § 318(a)

I. INTRODUCTION

A. Background

Forescout Technologies, Inc. (“Petitioner”) filed a Petition requesting *inter partes* review (“IPR”) of claims 1–4, 9, 13–18, 23, 27, and 28 (the “challenged claims”) of U.S. Patent No. 9,894,034 B2 (Ex. 1001, “the ’034 patent”). Paper 2 (“Pet.”). Fortinet, Inc. (“Patent Owner”) filed a Preliminary Response. Paper 7 (“Prelim. Resp.”). Pursuant to 35 U.S.C. § 314, we instituted this *inter partes* review as to all challenged claims and all grounds raised in the Petition. Paper 13 (“Institution Dec.”).

Following institution, Patent Owner filed a Response. Paper 19 (“PO Resp.”). Subsequently, Petitioner filed a Reply (Paper 20, “Pet. Reply”), and Patent Owner filed a Sur-reply (Paper 22, “PO Sur-reply”).

On October 27, 2022, we held an oral hearing. A transcript of the hearing is included in the record. Paper 33 (“Hearing Tr.”).

We have jurisdiction under 35 U.S.C. § 6. This decision is a Final Written Decision issued pursuant to 35 U.S.C. § 318(a). For the reasons we discuss below, we determine that Petitioner has proven by a preponderance of the evidence that claims 1, 2, 15, and 16 of the ’034 patent are unpatentable. Petitioner, however, has not proven by a preponderance of the evidence that claims 3, 4, 9, 13, 14, 17, 18, 23, 27, and 28 are unpatentable.

B. Related Proceedings

The parties identify the following district court proceeding concerning the ’034 patent: *Fortinet, Inc. v. Forescout Technologies, Inc.*, No. 3:20-cv-03343-EMC (N.D. Cal., filed May 15, 2020). Pet. 69; Paper 5, 2.

C. Real Party-in-Interest

The Petition identifies Forescout Technologies, Inc., as the real party-in-interest. Pet. 69. Patent Owner identifies Fortinet, Inc., as the real party-in-interest. Paper 5, 2.

D. The '034 Patent

The '034 patent is titled “Automated Configuration of Endpoint Security Management.” Ex. 1001, (54). The patent “relate[s] to providing various endpoint security management features based on information regarding the network environment of [a] client device.” *Id.* at 1:19–21.

Figure 1 of the '034 patent, reproduced below, illustrates an exemplary network architecture. *Id.* at 2:11–12.

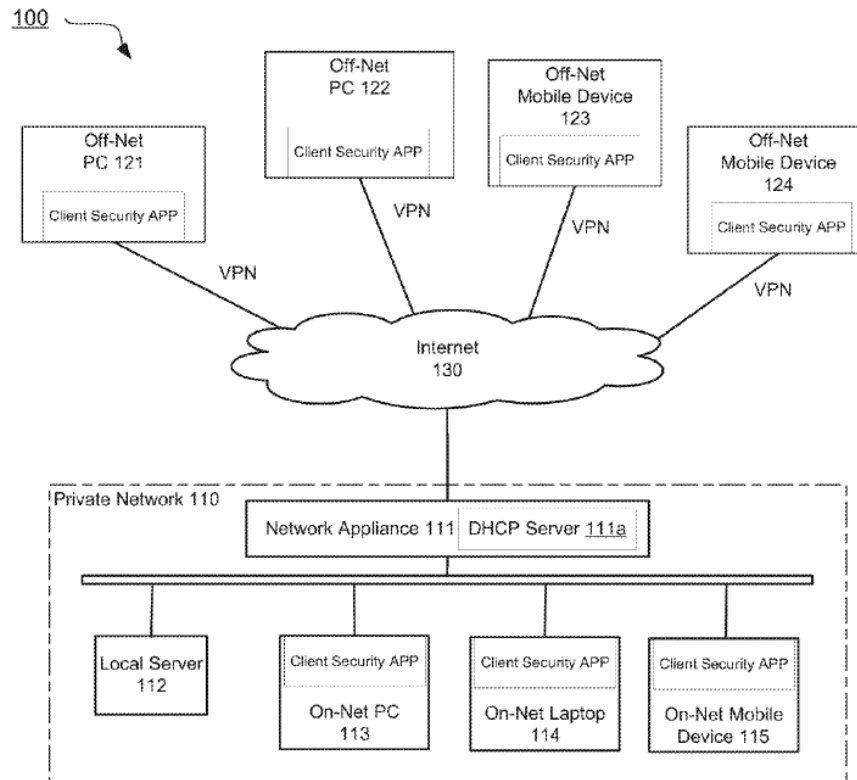


FIG. 1

Figure 1 of the '034 patent illustrates network architecture 100. *Id.* at 2:11–12, 4:65–67. Network architecture 100 includes: (i) private network 110 which is connected to Internet 130; (ii) multiple network appliances on private network 110, including local server 112, on-net personal computer (“PC”) 113, on-net laptop 114, and on-net mobile phone 115, operatively coupled to each other through a Local Area Network (“LAN”); and (iii) network appliances not on the private network 110, such as off-net PC 121, off-net PC 122, off-net mobile device 123, and off-net mobile device 124, which may connect to private network 110 from outside through Internet 130. *Id.* at 5:1–30.

The '034 patent describes a client security application installed on each of the on-net and off-net client devices. *Id.* at 5:56–57. “The client security application may include multiple engines that provide security functions.” *Id.* at 5:56–63. The '034 patent further explains, “[t]hese security functions may be launched optionally when the client security application is started depending upon the network environment.” *Id.* at 5:63–66.

The '034 patent explains also that “it is more convenient for the user if an appropriate configuration of the client security application is selected automatically based on the network environment and corresponding functions or engines associated with the selected configuration are launched when the client security application is started.” *Id.* at 6:10–15. “[T]o do this, the client security application determines whether the client device is on-net or off-net [(i.e., determines whether the client device is in a first network environment state, e.g., on-net, or in a second network environment state, e.g., off-net)].” *Id.* at 6:16–20.

After determining the network connection state and after selecting the appropriate configuration based on the network connection state, the client security application launches one or more functions of the client security application that are designated by the selected configuration. *Id.* at 1:64–67, 8:55–59.

E. Illustrative Claim

The '034 patent has 28 claims, of which claims 1–4, 9, 13–18, 23, 27, and 28 are challenged in the Petition. Claims 1 and 15 are independent.

Claim 1 is representative of the challenged claims. Claim 1 recites:¹

1. [preamble] A method comprising:

[1a.i] during initialization of a client security application running on a client device:

[1a.ii] determining, by the client security application, a network connection state of the client device with respect to a private network;

[1a.iii] selecting, by the client security application, a configuration for the client security application based on the determined network connection state; and

[1a.iv] launching, by the client security application, one or more functions of the client security application that are designated by the selected configuration to be performed by the client security application, wherein the one or more functions include one or more of web content filtering, anti-virus scanning and network access logging.

Ex. 1001, 11:35–50.

F. References and Other Evidence

The Petition (Pet. 10–11) relies on the following references:

U.S. Patent App. Pub. No. 2003/0097590 A1 (Ex. 1005, “Syvanne”);

¹ Paragraph numbering provided by Petitioner has been added.

U.S. Patent App. Pub. No. 2008/0148402 A1 (Ex. 1006, “Bogineni”);
U.S. Patent No. 9,973,534 B2 (Ex. 1007, “Mahaffey”).

In addition, Petitioner submits the Declaration of Dr. Eric Cole (Ex. 1003, “Cole Decl.”) and a reply declaration by Dr. Cole (Ex. 1015, “Cole Reply Decl.”). Patent Owner did not submit an expert declaration, nor did Patent Owner cross-examine Petitioner’s expert, Dr. Cole.

G. Asserted Grounds of Unpatentability

Petitioner asserts that the challenged claims are unpatentable based on the following grounds:

Claims Challenged	35 U.S.C. §²	Reference(s)
1–3, 14–17, 28	103	Syvanne
4, 9, 13, 18, 23, 27	103	Syvanne, Bogineni
1, 2, 15, 16	103	Mahaffey

Pet. 10.

II. PRELIMINARY MATTERS

A. Level of Ordinary Skill

Petitioner contends that a person of ordinary skill in the art “[a]s of May 21, 2014 . . . would typically be a person with a bachelor’s degree in computer science, computer engineering, or electrical engineering and at least three years of experience in networking operating systems and cyber security, or a person with a master’s degree in one of the foregoing and at least two years of experience in the aforementioned fields,” while “[s]omeone with less or different technical education but more relevant practical experience, or more relevant education but less practical

² Because the application from which the ’034 patent issued was filed after March 16, 2013, the AIA (“America Invents Act”) version of § 103 applies. Leahy-Smith America Invents Act (“AIA”), Pub. L. No. 112-29, 125 Stat. 284, 285–88 (2011).

experience, could also be considered a [person of ordinary skill in the art].” Pet. 7 (citing Cole Decl. ¶¶ 26–28).

Patent Owner states, “[f]or the purpose of this proceeding only, Patent Owner does not object to the definition of a [person of ordinary skill in the art] set forth in the Petition.” PO Resp. 8.

We find that Petitioner’s definition is consistent with the prior art and patent specification before us and is supported by credible expert testimony. *See Okajima v. Bourdeau*, 261 F.3d 1350, 1355 (Fed. Cir. 2001) (prior art itself may reflect an appropriate level of skill). For the purpose of our decision, we adopt Petitioner’s proposal on the level of ordinary skill.

B. Claim Construction

1. Background

In an *inter partes* review, the claims of a patent are construed using the same claim construction standard that would be used to construe the claims in a civil action under 35 U.S.C. § 282(b), including construing the claims in accordance with the ordinary and customary meaning of the claims as understood by one of ordinary skill in the art and the prosecution history pertaining to the patent. 37 C.F.R. § 42.100(b) (2020); *see also Phillips v. AWH Corp.*, 415 F.3d 1303, 1312–14 (Fed. Cir. 2005). Under that standard, and absent any special definitions, we give claim terms their ordinary and customary meaning, as would have been understood by one of ordinary skill in the art at the time of the invention. *See In re Translogic Tech., Inc.*, 504 F.3d 1249, 1257 (Fed. Cir. 2007). Any special definitions for claim terms must be set forth with reasonable clarity, deliberateness, and precision. *See In re Paulsen*, 30 F.3d 1475, 1480 (Fed. Cir. 1994).

2. Discussion

The Petition in this case failed to address a key issue, namely, the construction of “web content filtering.” *See* Pet. 7–9. Petitioner initially asserted that the parties disagreed over the meaning of only one term: “configuration [for/of] the [client/endpoint] security application.” *Id.* at 8. But Petitioner also contended “there are no claim construction issues that would affect the outcome of any trial on this petition.” *Id.* at 9. This statement turned out to be incorrect.

Patent Owner observed that, “[a]lthough Petitioner did not expressly propose any claim construction for ‘web content filtering,’ Grounds 1 and 2³ [of Petitioner’s challenge] are based on an implicit interpretation of the limitation ‘web content filtering’ by Petitioner that is not the plain and ordinary meaning, and thus is not reasonable.” Prelim. Resp. 7. Patent Owner submitted that “the plain and ordinary construction of web content filtering” is “blocking access to a webpage based on the content of the information on the webpage.” *Id.* This construction “would not include filtering based on specific IP addresses using an access control list (referred to as an ‘ACL’).” *Id.* at 7–9.

3. Web Content Filtering

In our Institution Decision, we determined that we needed to expressly construe “web content filtering” to resolve the parties’ dispute. Institution Dec. 9. We considered the construction of this term in the context of our analysis of the Syvanne prior art. *Id.* at 20–21. We concluded that Petitioner’s contention that Syvanne’s personal firewall

³ These grounds are both based, in whole or in part, on Syvanne. *See* Pet. 10.

performs “web content filtering” because, “[b]ased on the rule base selected, the personal firewall [of Syvanne] may control what access to web content is permitted by allowing or not allowing certain connections of protocols, e.g., HTTP connections” was incorrect. *Id.* at 20. Instead, we agreed with Patent Owner that Petitioner’s reliance on the argument that Syvanne teaches web content filtering by disclosing blocking HTTP connections but allowing HTTPS connections was “misplaced.” *Id.* We concluded that “[s]imply allowing or blocking a connection is not web content filtering.” *Id.* Instead, for our Institution Decision, we adopted Patent Owner’s construction of “web content filtering” as “blocking access to a webpage based on the content of the information on the webpage.” *Id.* at 21.

Petitioner has avoided providing a proposed construction for “web content filtering.” *See* Hearing Tr. 6:17–20. Instead, Petitioner responds that Patent Owner’s construction adopted by the Board for the Institution Decision is “too narrow for at least three reasons.” Pet. Reply 3. Petitioner argues first that “Patent Owner’s construction narrowly limits the claims to a ‘webpage’ even though the specification does not require such a limitation.” *Id.* Petitioner argues next that the construction is “inconsistent with the specification.” *Id.* at 4 (citing Ex. 1001, 8:65–67). We disagree with both of these arguments for the reasons that follow.

The specification of the ’034 patent does not support Petitioner’s arguments. Petitioner’s claim construction argument is based on equating “web content filtering” with the more inclusive term “web filtering.” *See* Hearing Tr. 20:1–6; PO Sur-reply 2–5. Petitioner asserts that “the specification does not limit ‘filtering’ to analyzing content of a webpage (as urged by Patent Owner). Instead, the specification makes clear that ‘filtering’ encompasses checking any ‘content’ transmitted to/from the

device.” Pet. Reply 4. Patent Owner responds that “[t]he heart of Petitioner’s argument is that *web content filtering* should include filtering based on any characteristic of a transmission, not just limited to filtering based on the content of a webpage.” PO Sur-reply 2 (internal quotation marks omitted). Patent Owner continues, “under Petitioner’s construction, any filtering would constitute ‘web content filtering’ so long as it ‘encompasses checking any “content” transmitted to/from the device.’” *Id.*

We do not agree with Petitioner that “web content filtering” and “web filtering” are the same. “Web content filtering” appears in the specification once, as a single item in a list of functions provided by network appliances.⁴ *See* Ex. 1001, 4:30–37; Hearing Tr. 17:12–18:10 (discussion of specification with Petitioner’s counsel). This listing also includes “content filtering” (without reference to web content) as a separate item (*see* Ex. 1001, 4:32–33). The appearance of “Web content filtering” and “content filtering” as separate items contradicts Petitioner’s argument that “every single reference to ‘filtering’ by the client device—i.e., the filtering recited in the claim—is described only as ‘web filtering’” (Pet. Reply 5). and strongly suggests that the terms “web filtering” and “web content filtering” have different meanings. The use of different terms in different places in a patent indicates that they are not the same. *Chicago Bd. Options Exchange, Inc. v. Int’l Securities Exchange*, 677 F.3d 1361, 1369 (Fed. Cir. 2012).

We find that the specification, therefore, supports Patent Owner’s argument that the term “web content filtering” differs from “web filtering”

⁴ “Network appliances” in Figure 1 of the ’034 patent include on-net PC 113, on-net laptop 114, on-net mobile phone 115, off-net PC 121, off-net PC 122, off-net mobile device 123, and off-net mobile device 124. Ex. 1001, 5:1–30; *see* Section I.D, *supra*.

and refers to a specific type of filtering that is based on web content, and does not include blocking certain IP addresses or connection protocols. *See* PO Sur-reply 3.

We find also that the prosecution history of the '034 patent supports Patent Owner. Petitioner asserts that the original application claims recited “web filtering” but not “content filtering.” Pet. Reply 5. According to Petitioner, a person of ordinary skill “would understand the intrinsic evidence to equate ‘web filtering’ and ‘web content filtering.’” *Id.* We disagree. Instead, we find that the prosecution history, specifically the deletion of “web filtering” from certain claims during prosecution of the '034 patent and the addition of “web content filtering” to independent claims 1 and 15 to distinguish over the prior art, signifies a distinction between the terms “web filtering” and “web content filtering” that is inconsistent with Petitioner’s argument that they are the same. *See* PO Sur-reply 3–4 (citing Ex. 1002, 160, 161, 163, 169–172). That the applicant may have cited the same specification support for the amendment, as asserted by Petitioner, does not signify that the terms have the same meaning. *Cf.* Hearing Tr. 20:20–21:15, 73:17–74:5.

We do not find credible Petitioner’s argument that “[t]here’s not an explanation” for why the attorney prosecuting the application for the '034 patent would have made such an amendment.” *Id.* at 21:20–22:16. There would have been no need for such an amendment if the terms “web filtering” and “web content filtering” had the same meaning.

Patent Owner also relies on a technical dictionary definition of “web content filtering” (Ex. 2001) and a document describing Cisco Router Firewall Security (Ex. 2002). The Cisco document describes using a “content filtering server” as an alternative to an access control list (ACL) of

IP addresses “to prevent users from accessing pornography, gambling, and peer-to-peer file-sharing sites.” PO Resp. 10–11 (citing Ex. 2002, 4).⁵

Petitioner’s third argument is that “Patent Owner’s construction [of web content filtering] is inconsistent with the extrinsic evidence,” specifically, the dictionary definition of “web content filtering” (Ex. 2001) and the Cisco document (Ex. 2002) cited by Patent Owner. Pet. Reply 6. Petitioner contends that the dictionary definition shows that “web content filtering is not limited to examining content on a website but can also be based solely on “characteristics’ of the resource,” which can include the communications protocol by which the client receives the page. *Id.* Petitioner contends that the Cisco document “does not exclude ACLs from the definition of filtering but simply contrasts the frequency of use of one type of filtering (a content-filtering server) with another (ACLs).” *Id.* at 7.

We do not find either of these arguments to be persuasive. Patent Owner argues that Petitioner’s assertion that the communications protocol (e.g., HTTP, HTTPS) is a “characteristic” of a web page “is without factual support.” PO Sur-reply 4. We agree. As Patent Owner points out, “many different protocols can be used to deliver the identical webpage.” *Id.* Likewise, we do not find persuasive Petitioner’s argument that the Cisco document was “randomly selected,” or that its recommendation for using content filtering and ACL together contradicts Patent Owner’s point that web content filtering does not include filtering based on IP addresses. *See* Pet. Reply 6–7.

⁵ Unless otherwise specified, citations to exhibits use the page numbers assigned by the parties and not the original page numbers.

“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 IPR petitions to identify “with particularity . . . the evidence that supports the grounds for the challenge to each claim”)) (emphasis added). This burden does not shift to Patent Owner, except in limited circumstances not present here. *See Dynamic Drinkware, LLC v. Nat’l Graphics, Inc.*, 800 F.3d 1375, 1378 (Fed. Cir. 2015) (citing *Tech. Licensing Corp. v. Videotek, Inc.*, 545 F.3d 1316, 1326–27 (Fed. Cir. 2008)) (discussing the burden of proof in an IPR).

By not providing a claim construction for a key term, “web content filtering,” Petitioner failed to live up to its obligation to provide an understandable explanation of the element-by-element specifics of the unpatentability challenges, including the particular portions of prior art supporting those challenges. *See* 37 C.F.R. §§ 42.22(a)(2), 42.104(b)(3)–(4); *Harmonic Inc.*, 815 F.3d at 1363–64; *Ariosa Diagnostics v. Verinata Health, Inc.*, 805 F.3d 1359, 1367 (Fed. Cir. 2015). “It is of the utmost importance that petitioners in the IPR proceedings adhere to the requirement that the initial petition identify ‘with particularity’ the ‘evidence that supports the grounds for the challenge to each claim.’” *Intel. Bio-Systems, Inc. v. Illumina Cambridge Ltd.*, 821 F.3d 1359, 1369 (Fed. Cir. 2016) (quoting 35 U.S.C. § 312(a)(3)); *see also MModal LLC v. Nuance Communications, Inc.*, 846 Fed. Appx. 900, 906 (Fed. Cir. 2021) (non-precedential).

For the reasons given by Patent Owner and summarized above, we find Petitioner’s arguments attempting to discredit the claim construction favored by Patent Owner and adopted by us to be unavailing. For the

reasons given above and in Patent Owner’s Response and Sur-reply, and in our Institution Decision, we maintain our construction of “web content filtering” as “blocking access to a webpage based on the content of the information on the webpage.” For the same reasons, we find that our construction would not include filtering based on specific IP addresses.

We determine that we need not explicitly construe any other claim terms for this proceeding. *Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co.*, 868 F.3d 1013, 1017 (Fed. Cir. 2017) (“[W]e need only construe terms ‘that are in controversy, and only to the extent necessary to resolve the controversy.’” (quoting *Vivid Techs., Inc. v. Am. Sci. & Eng’g, Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999))).

C. Description of the Prior Art References

1. Syvanne (Ex. 1005)

Syvanne describes a computer device provided with a local security mechanism (which Syvanne calls “a personal firewall”) for protecting the device from attacks from a foreign network, in addition to (or instead of) a firewall in the internal network which protects the computer when connected to a home network. Ex. 1005, (57), ¶ 10. The personal firewall is provided with different sets of security rules for the home network and foreign networks. *Id.* at (57).

The personal firewall is arranged to detect a current location, i.e., determine to which network it is connected to at each particular moment. *Id.* Then the personal firewall activates one of the security rules according to the detected current location of the computer device. *Id.* More particularly, “the personal firewall automatically uses the security rules predefined for the network to which the computer device is connected at each particular moment.” *Id.* Further, “[u]pon detecting a change in the location, the

personal firewall immediately adapts to use security rules predefined for the new location.” *Id.*

Figures 2 and 3 of Syvanne are reproduced below.

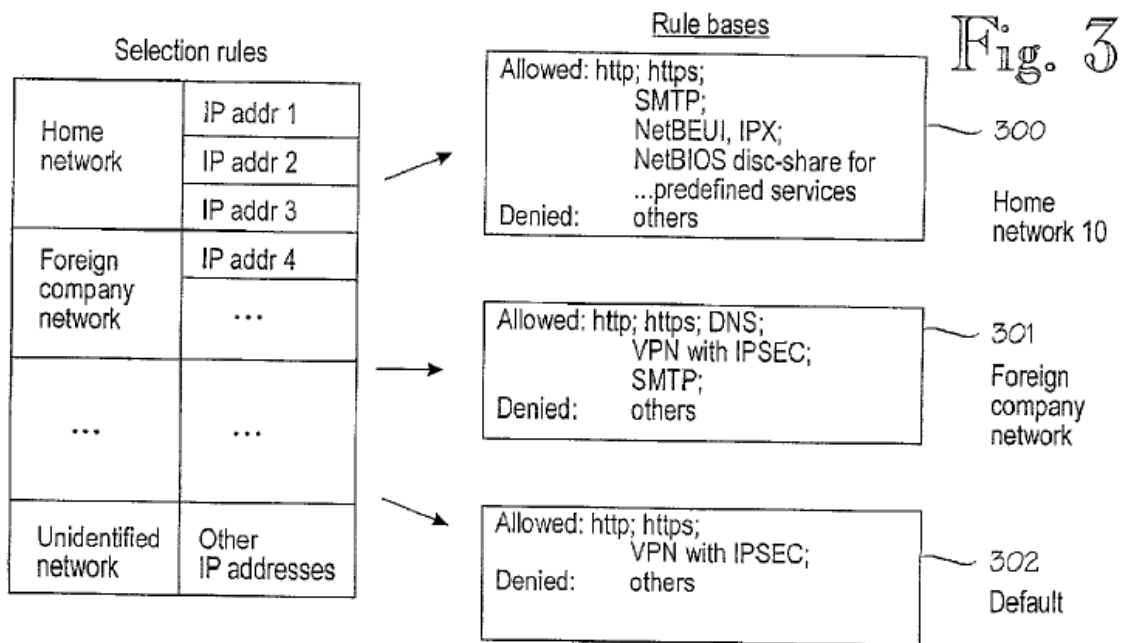
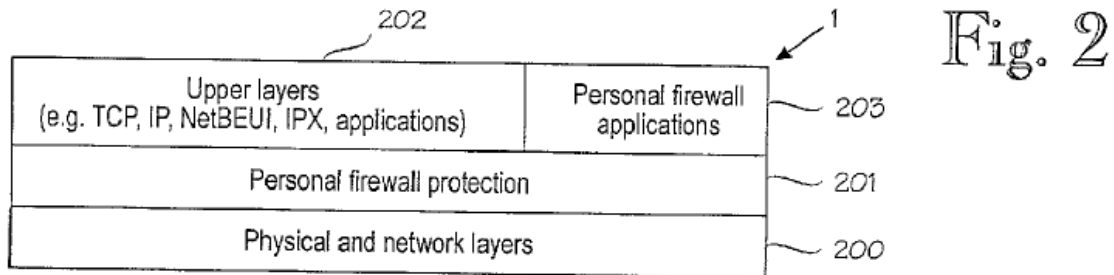


Figure 2 illustrates a protocol stack of a computer device containing a personal firewall. Figure 3 illustrates selection rules and associations between them. *Id.* ¶¶ 18–19. Syvanne’s personal firewall protects the computer device (e.g., a laptop) on which the firewall is installed. *Id.* ¶ 29.

As shown in Figure 2, personal firewall protection layer 201—implemented or controlled by personal firewall application 203 run on the laptop—operates in a manner analogous to a firewall between networks, i.e., as a connector and a separator between the underlying layers and the upper

layer, keeping track of traffic that passes through, and restricting connections and packets that are defined as unwanted according to the security rules. *Id.* ¶ 30.

Syvanne's personal firewall has different rules for a home network (such as a private company network) and for a foreign network (such as the public Internet, or a foreign private network). *Id.* ¶ 31. Figure 3 illustrates examples of security rules of the personal firewall. *Id.* ¶ 31. The rules illustrated in Figure 3 include rule base 301 for a foreign company network; rule base 302 for a default network, such as the public Internet; and rule base 300 for a home network. *Id.* ¶ 31. Syvanne explains that "[t]he different rule bases could be activated manually by a user" but "according to the basic principle of [Syvanne's] invention, the personal firewall automatically selects and activates the proper rule base according to the current location of the laptop." *Id.* ¶ 32.

2. *Bogineni (Ex. 1006)*

Bogineni "relates to improved security across layers and paths of a native packet communication network, based on network management of security functions of [an] access terminal device, such as might be used in a next generation network deployment for wireless communication services." Ex. 1006, (54), ¶ 2. Bogineni explains that access terminal devices intended for operation via a network are expected to have security agent functionality, e.g., in the form of security agent software loaded into or otherwise enabled on the access terminal devices. *Id.* ¶ 5. Bogineni provides techniques that "relate to operations of an access terminal device and/or a node of the communications network to check the access terminal device with respect to the security agent functionality, before permitting network registration of the

device and thus before the network provides communication service to the access terminal device.” *Id.*

3. *Mahaffey (Ex. 1007)*

Mahaffey “relates to the field of mobile technology and more particularly, to systems and techniques that relate to network connections.” Ex. 1007, (54), 1:6–8. Mahaffey’s technique collects context information associated with a mobile communications device and a network connection for the mobile communications device and applies a security policy to determine whether the security offered by the network connection is appropriate for the context. *Id.* at (57). If the security offered by the network connection is not appropriate for the context, the network connection may be made more secure, less secure, or a different network connection having an appropriate level of security may be used for the data associated with the context. *Id.*

Figure 4A of Mahaffey is reproduced below.

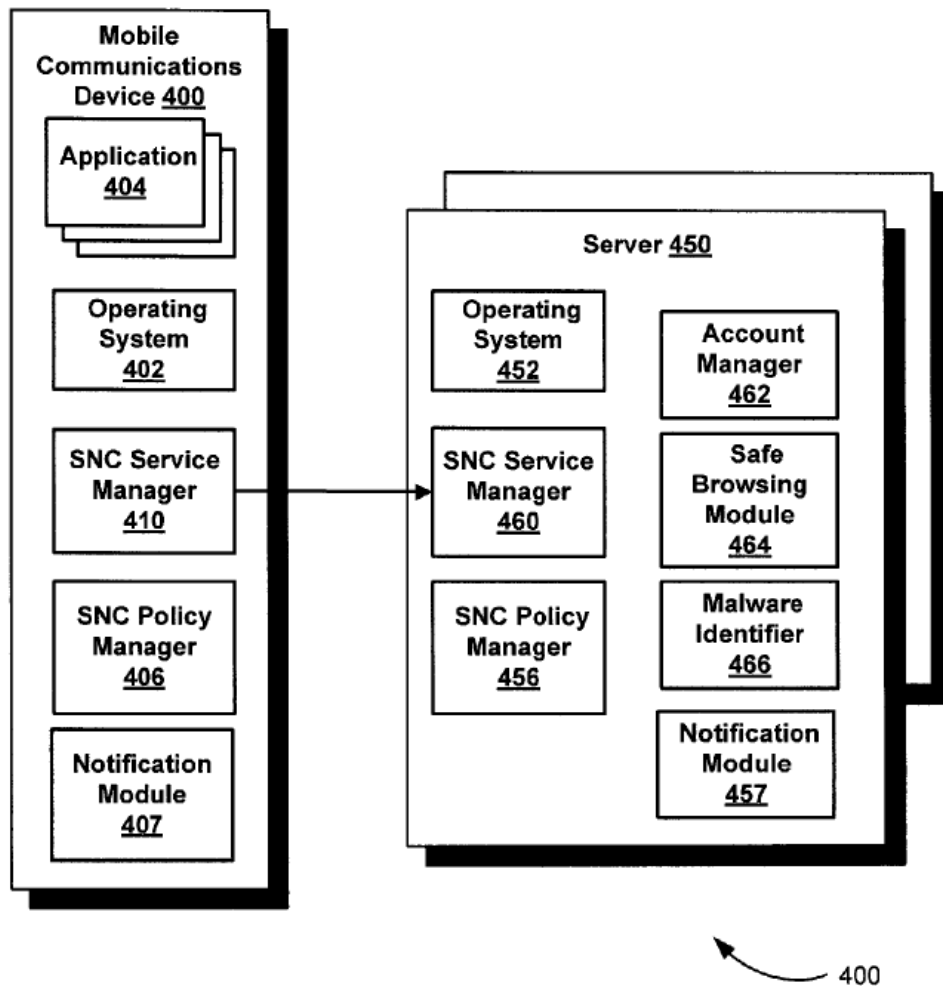


Figure 4A

Figure 4A illustrates mobile communications device 400 and server 450 with which the device communicates. *Id.* at 13:60–61, 14:15–16. Mobile communications device 400 includes operating system 402, which manages hardware resources on mobile communications device 400 and provides services to one or more programs or applications 404 installed on mobile communications device 400. *Id.* at 14:5–14.

Mobile communications device 400 further includes secure network connections (“SNC”) service manager 410, which may be a process or

application implemented on mobile communications device 400. *Id.* at 18:54–60. SNC service manager 410 may be configured to provide SNC services, such as establishing and terminating an endpoint of a SNC tunnel, and applying one or more policies to a SNC connection. *Id.* at 18:61–64. “[T]he operations of SNC service manager 410 may be controlled or configured by one or more rules or policies stored in SNC policy manager 406.” *Id.* at 18:64–67. “For example, a policy stored in SNC policy manager 406 may configure SNC service manager 410 to establish a SNC connection in a first geographical location, but not in a second geographical location.” *Id.* at 19:4–8.

Mobile communications device 400 may connect to remote destinations via a network in various contexts. *Id.* at 14:21–23. Such contexts may be location-based, such as contexts pertaining to a user’s home, the user’s workplace, an airport, a school, a library, a train, etc. *Id.* at 14:30–15:5, 17:53–58.

Table C of Mahaffey is reproduced below.

TABLE C

POLICY SECURITY LEVEL	NETWORK CONNECTION TYPE
0	Unsecured Wi-Fi connection
1	Wi-Fi connection with WEP
2	Cell connection, small cell
3	Wi-Fi connection with EAP (original)
4	Wi-Fi connection with WPA or WPA2 or TKIP
5	Wi-Fi connection with EAP (extended, e.g., EAP-MD5, EAP-TLS, etc.)
6	Cell connection, macro cell
7	SSL or TLS connection to a specific destination
8	OVERLAY NETWORK (e.g., VPN, IPSEC tunnel, SSL/TLS proxy, etc.)
9	OVERLAY NETWORK using pinned certificates or secure alternate channel certificate verification/revocation check

Table C shows an example of a list of different network connection types and corresponding policy security levels. *Id.* at 53:40–60. As shown in Table C, the security of a network connection may be determined or ranked, with policy rules indicating what type of network connection needs are to be used. *Id.* at 52:45–50. In an alternative embodiment, policy rules define an explicit security level, and associated information lists which types of network connection can be used to achieve a given security level. *Id.* at 52:50–54.

III. ANALYSIS OF THE CHALLENGED CLAIMS

The Petitioner challenges claims 1–4, 9, 13–18, 23, 27, and 28 of the '034 patent. Petitioner asserts unpatentability of the claims based on obviousness.

A. Obviousness

A claim is unpatentable if the differences between the claimed subject matter and the prior art are such that the claimed invention, as a whole, would have been obvious before the effective filing date of the claimed invention to a person having ordinary skill in the art to which the claimed invention pertains. 35 U.S.C. § 103.

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) so-called “secondary considerations,” including commercial success, long-felt but unsolved needs, failure of others, and unexpected results. *Graham v. John Deere Co.*, 383 U.S. 1, 17–18 (1966) (“the *Graham* factors”). Neither party presents evidence on the fourth *Graham* factor. We therefore do not consider that factor in this decision.

B. Syvanne Challenges

In its first ground, Petitioner contends that claims 1–3, 14–17, and 28 would have been obvious over Syvanne. Pet. 10, 12–35. Of these claims, claims 1 and 15 (reciting similar limitations) are the independent claims. *See supra*. Patent Owner addresses claims 1 and 15 together. *See, e.g.*, PO Resp. 17. We initially focus our analysis on claim 1, but our analysis equally applies to claim 15.

1. Claim 1

Petitioner contends each limitation of claim 1 is taught or suggested by Syvanne, and provides an element-by-element analysis. Pet. 17–26. Petitioner provides supporting testimony from Dr. Cole. Cole Decl.

¶¶ 83–116.

a. Element 1 preamble (“A method comprising . . .”)

Petitioner contends that the flow diagram in Syvanne’s Figure 4 discloses the preamble “to the extent [it] is limiting.”⁶ Pet. 17. Patent Owner does not dispute this contention. We find that for the reasons given, Petitioner demonstrates that Syvanne discloses the preamble of claim 1.

b. Element 1a.i (“during initialization of a client security application running on a client device”)

Petitioner contends that Syvanne’s personal firewall running on a computer device, such as a laptop, is a client security device meeting this limitation. Pet. 18. “Furthermore, the personal firewall performs its functions during initialization of the personal firewall application running on the laptop.” *Id.* (citing Cole Decl. ¶ 89).

Patent Owner does not dispute this contention. We find that for the reasons given, Petitioner demonstrates that Syvanne discloses element 1a.i of claim 1.

c. Element 1a.ii (“determining, by the client security application, a network connection state of the client device with respect to a private network”)

Petitioner contends Syvanne discloses this limitation: “Syvanne discloses that the personal firewall determines what network the laptop is connected to at each particular moment.” Pet. 20 (citing Cole Decl. ¶ 96).

Patent Owner does not dispute this contention. We determine that for the reasons given, Petitioner demonstrates that Syvanne discloses element 1a.ii of claim 1.

⁶ We do not express a view on whether the preambles of the challenged claims are limiting.

d. Element 1a.iii (“selecting, by the client security application, a configuration for the client security application based on the determined network connection state”)

Petitioner contends that Syvanne meets this limitation by disclosing “a flow diagram illustrating the selection of a rule base by the personal firewall based on the current location, i.e., the network to which the laptop is connected at each particular moment.” Pet. 22 (citing Cole Decl. ¶ 103; Ex. 1005, Fig. 4). Referring to Syvanne’s Figure 4, Petitioner further explains, “after determining whether the laptop has changed locations, step 405 ‘[s]elect[s] a rule base linked to the IP address.’” *Id.* (alterations in original).

Patent Owner does not dispute this contention. We determine that for the reasons given, Petitioner demonstrates that Syvanne discloses element 1a.iii of claim 1.

e. Element 1a.iv (the “launching” limitation)

Claim element 1a.iv recites “launching, by the client security application, one or more functions of the client security application that are designated by the selected configuration to be performed by the client security application, wherein the one or more functions include one or more of *web content filtering*, anti-virus scanning and network access logging.” Ex. 1001, 11:44–50 (emphasis added). Petitioner contends that Syvanne discloses only the first of these three limitations (“web content filtering”).⁷

Petitioner contends Syvanne teaches the “launching” limitation because “Syvanne discloses the personal firewall launches, i.e., activates, the proper rule base that is selected based on the determined location of the

⁷ Initially, Petitioner asserted that Syvanne’s personal firewall also performs network access logging (Pet. 25–26) but apparently abandoned that contention by the oral hearing. Hearing Tr. 9:19–10:8; PO Sur-reply 9–10.

laptop.” Pet. 24 (citing Cole Decl. ¶¶ 110–111). Petitioner contends this is illustrated in Syvanne’s Figure 3, reproduced *supra*, where “the different rule bases have different functions that are launched by the personal firewall if that rule base is selected, i.e., the selected configuration.” *Id.* at 25.

i. Web Content Filtering

Petitioner contends that Syvanne’s personal firewall performs “web content filtering” because, “[b]ased on the rule base selected, the personal firewall [of Syvanne] may control what access to web content is permitted by allowing or not allowing certain connections of protocols, e.g., HTTP connections.” Pet. 25. Petitioner explains further that “[a person of ordinary skill] would have understood that by blocking HTTP connections but, for example, allowing HTTPS connections, the personal firewall is performing web content filtering by only allowing access to secure websites.” *Id.* at 26.

Patent Owner disputes the assertion that Syvanne discloses web content filtering. PO Resp. 17–20. We agree with Patent Owner and find that Syvanne does not disclose web content filtering as claimed.

As Patent Owner points out, Petitioner relies on the argument that Syvanne teaches web content filtering by disclosing blocking HTTP connections but allowing HTTPS connections. *Id.* at 18–19. Petitioner relies on Figure 3 of Syvanne as an illustration. Pet. 25. But as Patent Owner points out, Figure 3 of Syvanne describes *allowing* both HTTP and HTTPS connections, even when the computer device needs a “maximum protection” in unidentified network. *Id.* at 19; PO Sur-reply 7. Petitioner does not deny this, responding that Figure 3 of Syvanne “is merely an example, as expressly stated in Syvanne.” Pet. Reply 11 (citing Ex. 1005 ¶ 31).

More fundamentally, however, we agree with Patent Owner that “[s]imply allowing or blocking a connection is not *web content filtering*.” PO Resp. 19. *See* discussion in Sections II.B.2 & II.B.3 *supra*. In our claim construction analysis, we found that Petitioner failed to adequately articulate its position as to the meaning of “web content filtering,” but that, based on the evidence of record, the term is not simply “content filtering” or “web filtering.” *See supra*, Section II.B.3. As we stated in our Institution Decision, “[i]t is self-evident that ‘web content filtering’ of a webpage should be based on the content of the page, rather than the communications protocol by which the client receives the page.” Institution Dec. 21. Petitioner does not persuade us that our preliminary findings in this regard are not correct, and we see no need to change course based on the arguments presented and developed during trial.

Applying this construction, we determine that Petitioner does not demonstrate that Syvanne teaches or suggests web content filtering. Filtering the protocol of a web page URL does not block access based on the content and, therefore, does not filter the content of the web page. *See* PO Resp. 19–20. This is because Syvanne only discloses the type of connections that are allowed, and any connection not specifically allowed is denied. *Id.* Accordingly, we find that Petitioner does not demonstrate that Syvanne discloses or suggests web content filtering.

Petitioner challenges this conclusion by asserting in its Reply a number of new arguments that were not presented and developed in the Petition. Pet. Reply 10–12. We are not persuaded by those arguments. For example, Petitioner contends that “[t]he protocol used for a transmission is certainly a ‘characteristic’ of that transmission and thus would constitute ‘web content filtering’ under the plain meaning.” *Id.* at 11. This argument

is unavailing. A protocol dictates how the page is received by the client, and does not dictate its content. PO Sur-reply 4. As Patent Owner points out, “[m]any different protocols can be used to deliver the identical webpage.” *Id.*

Petitioner also argues that, “even under Patent Owner’s proposed construction,” Syvanne discloses web content filtering. Pet. Reply 13–16. According to Petitioner, “firewalls in general and Syvanne’s personal firewall are both designed to block undesired traffic.” *Id.* at 13. Petitioner contends that Syvanne’s personal firewall allows it to block unwanted traffic “based on specific information, such as blocking a webpage’s traffic based on the content of the information on the webpage . . . because the personal firewall has to look at the content of the transmitted packet (which is part of the content of the webpage) to determine whether the packet is HTTP traffic that should be blocked.” *Id.* at 14–15 (citing Cole Reply Decl. ¶¶ 36, 37).

We are not persuaded by these belated arguments, as they are based entirely on testimony by Dr. Cole as to what a person of ordinary skill “would understand” that is unsupported by any citations to Syvanne or other evidence of record. Such unsupported opinions are not entitled to any weight. 37 C.F.R. § 42.65(a) (“Expert testimony that does not disclose the underlying facts or data on which the opinion is based is entitled to little or no weight.”); *see also* Consolidated Trial Practice Guide 35 (November 2019)⁸ (“The Board has broad discretion to assign weight to be accorded expert testimony. . . . However, the testimony must be based on sufficient facts and data.”); Fed. R. Evid. 702(b). “[E]xpert testimony cannot take the place of disclosure from patents or printed publications. In other words,

⁸ Available at <https://www.uspto.gov/TrialPracticeGuideConsolidated>.

expert testimony may explain ‘patents and printed publications,’ but is not a substitute for disclosure in a prior art reference itself.” Consolidated Practice Guide at 36.

Moreover, as Patent Owner points out, Petitioner’s reliance on packet-level filtering and ACLs as web content filtering is, in fact, a variation on Petitioner’s claim construction argument that web content filtering is not limited to examining webpage content. PO Sur-reply 4–9. As Patent Owner explains, “Petitioner’s expert admits that this extrinsic evidence is directed to generic filtering, rather than *web content filtering*.” *Id.* at 5 (citing Pet. Reply 8). For these additional reasons, we find these arguments by Petitioner unavailing.

We find that for the reasons given, under the construction we have adopted, Petitioner has not demonstrated that Syvanne teaches or suggests “web content filtering.”

f. Conclusion – Claim 1

Petitioner has not demonstrated that Syvanne teaches or suggests the “launching” limitation of independent claim 1. Therefore, Petitioner has not demonstrated by a preponderance of the evidence that claim 1 would have been obvious in view of Syvanne.

2. Claim 15

Petitioner contends that independent claim 15 would have been obvious in view of Syvanne. Pet. 30–33. Claim 15 includes limitations similar to the limitations recited in independent claim 1. *See* PO Resp. 5–7 (comparing claims 1 and 15). Petitioner does not raise arguments for the “launching” limitation in claim 15 that are separate from those discussed above with respect to claim 1. *See* Pet. 32–33.

We determine that for the same reasons given for claim 1, Petitioner has not demonstrated by a preponderance of the evidence that claim 15 would have been obvious in view of Syvanne.

3. Claims 2, 3, 14, 16, 17, and 28

Claims 2, 3, and 14 depend from claim 1, and claims 16, 17, and 28 depend from claim 15. Petitioner does not raise arguments for dependent claims 2, 3, 14, 16, 17, and 28 that are separate from those discussed above with respect to the “launching” limitation in claims 1 and 15, from which they depend. *See, e.g.*, Pet. 27–28 (addressing only the “additional limitation of claim 2”).

For the same reasons discussed above with respect to claims 1 and 15, we determine that Petitioner has not demonstrated by preponderance of the evidence that claims 2, 3, 14, 16, 17, and 28 would have been obvious in view of Syvanne.

C. Syvanne and Bogineni Challenge

Petitioner’s second ground asserts that dependent claims 4, 9, 13, 18, 23, and 27 would have been obvious over Syvanne and Bogineni. Pet. 10, 35–50. Patent Owner does not raise arguments for this challenge to claims 4, 9, 13, 18, 23, and 27 that are separate from those discussed above with respect to claims 1 and 15. *See* PO Resp. 23.

Each of claims 4, 9, 13, 18, 23, and 27 depends from one of independent claims 1 and 15, and therefore includes all the limitations required by those respective claims, including the “launching” limitation discussed *supra*. In this challenge, Petitioner relies on Syvanne to meet the “launching” limitation. Petitioner relies on Bogineni to meet the additional limitations of these dependent claims. *See, e.g.*, Pet. 4 (“Bogineni teaches the additional limitation of claim 4.”).

Thus, for the same reasons discussed with respect to claims 1 and 15, we determine that Petitioner has not demonstrated by preponderance of the evidence that claims 4, 9, 13, 18, 23, and 27 would have been obvious over the combination of Syvanne and Bogineni.

D. Mahaffey Challenge

Petitioner asserts that claims 1, 2, 15, and 16 would have been obvious over Mahaffey. Pet. 10, 50–69.

1. Claim 1

Petitioner contends each limitation of claim 1 is met by Mahaffey, and provides an element-by-element analysis. Pet. 55–63; Cole Decl. ¶¶ 189–224. Petitioner asserts that Mahaffey discloses each claim element. For example, Petitioner identifies Mahaffey’s SNC service manager 410 as the “client security application running on a client device” recited in claim element 1a.i. Pet. 55.

Claim element 1a.ii recites that the method claimed includes “determining, by the client security application, a network connection state of the client device with respect to a private network.” Petitioner contends Mahaffey discloses the “determining” step of claim element 1a ii. *Id.* at 57–59. Petitioner contends that in Mahaffey, “the SNC service manager determines the context and current network connection of the mobile device, i.e., the network connection state of the client device.” *Id.* at 57. Petitioner points to Mahaffey’s Table C (reproduced *supra*, Section II.C.3). *Id.* at 57–58. Petitioner explains that “Table C of Mahaffey . . . illustrates an example of different policy security levels associated with different network connection types.” *Id.* at 57–58 (citing Cole Decl. ¶ 203).

Petitioner explains that “Mahaffey satisfies Patent Owner’s construction of ‘determining, by the client security application, a network

connection state of the client device with respect to a private network’ because the SNC service manager applies different policies based on determining the mobile communications device’s network connection type, which requires the SNC service manager to determine ‘whether the client device is connected to a private network, and the means by which the client device is connected to said private network.’” *Id.* at 59 (citing Cole Decl. ¶¶ 205–206).

Patent Owner challenges Petitioner’s contention that the “determining” step is met by Mahaffey. PO Resp. 33–40. Patent Owner contends Petitioner’s argument that the SNC service manager in Mahaffey meets the “determining” limitation “is defective for two reasons.” *Id.* at 33. Patent Owner contends the disclosure in Mahaffey relied on by Petitioner describes a network device separate from the SNC that assesses the current network connection to determine the network connection state. *Id.* at 34. Petitioner further contends that Petitioner relies on a passage that describes the Figure 4C “embodiment” of Mahaffey illustrating mobile device 480 that “differs” from mobile communications device 400 in Figure 4A that includes the SNC. *Id.* at 34–35. Patent Owner contends further that, “even if the embodiment of FIG. 4C disclosed that mobile device 480 performed the recited *determining a network connection state* limitation (which it does not), the Petition does not provide any explanation for why a [person of ordinary skill] would be motivated to combine the embodiment of Fig. 4C with the embodiment of FIG 4A.” *Id.* at 35. Thus, according to Patent Owner, Mahaffey describes subsequently passing context information to a separate network device, not the SNC, that makes the actual assessment of the current network connection (i.e., the alleged step of determining a network connection state). *Id.* at 33.

We disagree with Patent Owner because these arguments are based on an interpretation of Mahaffey that is too limited. As Petitioner asserts, the context information detected by the SNC service manager in Mahaffey “may include the security level of the first network connection.” Pet. Reply 18 (quoting Ex. 1007, 2:59–61). We do not agree with Patent Owner that Mahaffey’s disclosure is so limited. Mahaffey discloses that Mahaffey’s SNC service manager 410 selectively provides security services on the mobile device that are controlled by SNC policy manager 406, also on the mobile device:

Thus, SNC service manager 410 may be configured to provide SNC services, such as establishing and terminating an endpoint of a SNC tunnel, and applying one or more policies to a SNC connection. In various implementations, *the operations of SNC service manager 410 are controlled or configured by one or more rules or policies stored in SNC policy manager 406.*

Ex. 1007, 18:61–67 (emphasis added). Moreover, SNC policy manager 406 on the mobile device provides policies that configure the SNC service manager 410 based on location:

Thus, SNC policy manager 406 may include or be coupled to one or more data stores that store policies that configure or manage one or more actions or operations performed by SNC service manager 410. *For example, a policy stored in SNC policy manager 406 may configure SNC service manager 410 to establish a SNC connection in a first geographical location, but not in a second geographical location.*

Id. at 19:1–8 (emphasis added).⁹

Petitioner provides further evidence that Mahaffey meets the “determining step.” Pet. Reply 18. Petitioner quotes Mahaffey’s disclosure

⁹ This operation of SNC service manager 410 on the mobile device is discussed by Petitioner in connection with the both the “determining step” and the “launching” steps. Pet. 59–63.

that “[s]ystem 400 implements SNC service managers and SNC policy managers to determine when an SNC connection should be established, and to automatically establish the SNC connection in response to making such as [sic] determination.” *Id.* (quoting Ex. 1007, 13:55–59) (emphasis omitted) (alterations in original); Cole Decl. ¶¶ 201–207.

Patent Owner’s argument that Figures 4A, 4B, and 4C are three different embodiments fails also. *See* PO Resp. 25–28; PO Sur-reply 12–13. As Petitioner explains, “a simple look at Mahaffey’s description of Figures 4A-4C debunks those allegations.” Pet. Reply 19. The fact that these three block diagrams were assigned the same figure number 4 is strong evidence, in itself, that the figures are to be considered together, and not separately. Add to that the descriptions of the figures cited by Petitioner, and we find that Figures 4B and 4C show particular contexts or applications for the system of Figure 4A, and not separate embodiments. Pet. Reply 19–21. Thus, Figure 4A “illustrates an example of a block diagram of a system for automatically providing a secure network connection to a mobile communications device, implemented in accordance with some implementations.” Ex. 1007, 5:41–44. Figure 4B is described by Mahaffey as “an example of contexts in which a mobile communications device might be used.” Ex. 1007, 5:45–46. Similarly, Figure 4C is described as showing “a more detailed block diagram of a particular context.” *Id.* at 5:47–48.

We find that for the reasons given, Petitioner has demonstrated that Mahaffey’s SNC service manager 410 provides control over network connections and meets the “determining” limitation of claim 1.

The additional limitations of claim 1 are not in dispute. Petitioner demonstrates that the “selecting” step (claim element 1a.iii) is met by Mahaffey’s SNC service manager 410 and policy manager 406. Pet. 59.

Petitioner explains, “The policies that configure or manage the actions performed by the SNC manager are based on the determined network connection state of the mobile communications device.” *Id.* at 59–60 (citing Cole Decl. ¶ 209). Similarly, the “launching” step (claim element 1a.iv) is met because “the SNC service manager [410] applies one or more policies, i.e., launches, of the SNC services configured to be provided by the SNC service manager, i.e., the one or more functions that are designated by the selected configuration to be performed by the client security application.” *Id.* at 61 (citing Cole Decl. ¶¶ 218–219).

Petitioner demonstrates that SNC service manager 410 performs web content filtering “because the SNC service manager detects the context on the mobile device and assesses the current network connection to decide what level of security is necessary for the context and taking the appropriate security actions on the network connection.” *Id.* at 62–63.

Patent Owner does not dispute these contentions regarding the “selecting” or “launching” steps.

In summary, we find for the reasons given that Petitioner has demonstrated that Mahaffey teaches or suggests the “determining” limitation of independent claim 1 challenged by Patent Owner and all other limitations of the claim. Therefore, we determine that for the reasons given, Petitioner has demonstrated by preponderance of the evidence that claim 1 would have been obvious in view of Mahaffey.

2. Claim 15

Independent claim 15 includes limitations similar to the limitations recited in independent claim 1, including the launching limitation. *Compare* Ex. 1001, 13:4–10, *with id.* at 11:44–50. Petitioner contends independent claim 15 would have been obvious over Mahaffey for essentially the same

reasons discussed above with respect to claim 1. Pet. 65–68. Patent Owner does not raise arguments for claim 15 that are separate from those discussed above with respect to claim 1. *See* PO Resp. 33. We have reviewed and agree with Petitioner’s contentions and disagree with Patent Owner’s arguments for the same reasons given for claim 1. We therefore determine that Petitioner has demonstrated by preponderance of the evidence that claim 15 would have been obvious in view of Mahaffey.

3. Claims 2 and 16

These claims depend from claim 1 or from claim 15, respectively. Petitioner relies on Mahaffey to meet the limitations added by these claims. Pet. 63–65, 68–69. Patent Owner does not raise arguments for this challenge to claims 2 and 16 that are separate from those discussed above with respect to claims 1 and 15. *See* PO Resp. 43. We, therefore, determine that for the same reasons given for claim 1 as well as those given in the Petition for the additional limitations of claims 2 and 16, Petitioner has demonstrated by preponderance of the evidence that claims 2 and 16 would have been obvious in view of Mahaffey.

IV. OTHER MATTERS

Each party has filed objections to the other party’s demonstrative exhibits. Papers 31 (Petitioner’s Objections), 32 (Patent Owner’s Objections).

A. Petitioner’s Objections

Petitioner objects to Patent Owner’s demonstrative slide 27. Paper 31, 3. Slide 27 quotes Petitioner’s Reply regarding Syvanne’s firewall and Patent Owner’s Sur-reply argument based on Exhibit 2003, an excerpt from a textbook authored by Petitioner’s expert, Dr. Cole, concerning network

security. Paper 29, 27.¹⁰ According to Petitioner, slide 27 “contain[s] improper new argument raised for the first time in Patent Owner’s Sur-Reply.” Paper 31, 1. This subject was addressed by Petitioner’s counsel at the Oral Hearing. Hearing Tr. 34:14–35:16.

The objection is overruled. Petitioner’s Reply argues that in blocking specific traffic, Syvanne’s personal fire wall examines the content of the HTTP traffic, and therefore Syvanne discloses “web content filtering” under Patent Owner’s proposed construction of the term. Pet. Reply 15–16. Citing Dr. Cole’s textbook, Patent Owner responds that Syvanne’s firewall filtering is based on the HTTP packet’s header, not the “payload” of the packet that contains the web content. PO Sur-reply 8–9. Patent Owner’s argument based on Dr. Cole’s textbook is a fair response to Petitioner’s argument.

Petitioner objects also to Patent Owner’s demonstrative slide 26, which quotes a Sur-reply argument based on the prosecution history of the ’034 patent. Petitioner raises the issue of the prosecution history in its Reply by referring to the claims originally filed in the application for the ’034 patent. *See* Pet. Reply 5 (“The claims submitted with the original application similarly recited only ‘web filtering’ but not ‘content filtering.’”). In response, Patent Owner’s Sur-reply asserts that certain claims were subsequently amended to include “web content filtering” and others were amended to delete “web filtering.” PO Sur-reply 3. This argument by Patent Owner is reflected slide 26 and is a fair response to the argument made by Petitioner concerning the original claims. Petitioner objects also to Patent Owner’s slide 12, which refers to this argument. Petitioner’s objections to slides 12 and 26 are overruled.

¹⁰Patent Owner’s slide 25 also cites Exhibit 2003.

B. Patent Owner's Objections

Patent Owner objects to Petitioner's demonstrative slides 24, 25, 42, and 43 (Paper 30). Patent Owner asserts that these slides include new argument or citations to evidence that were not previously made in the Petition or Petitioner's Reply. Paper 32, 2–4.

Petitioner's slides 24 and 25 address alleged “new support” for Patent Owner's arguments appearing in the Sur-reply and show excerpts from the prosecution history and specification that Petitioner contends demonstrate that the amendment relied on by Patent Owner does not show that “web content filtering” is narrower than “web filtering.” *See* Hearing Tr. 73:10–74:2. We do not rely on these arguments by Petitioner and therefore dismiss these objections by Patent Owner as moot.

Slides 42 and 43 address alleged “new evidence” from Patent Owner citing Exhibit 2003, introduced with Patent Owner's Sur-reply. *See supra*. Petitioner did not refer to these slides during its oral argument. We therefore dismiss Patent Owner's objections as moot.

V. CONCLUSION

For the foregoing reasons, we determine that Petitioner has demonstrated by a preponderance of the evidence that claims 1, 12, 15, and 16 of the '034 patent would have been obvious and are, therefore, unpatentable.¹¹

¹¹ Should Patent Owner wish to pursue amendment of the challenged claims in a reissue or reexamination proceeding subsequent to the issuance of this decision, we draw Patent Owner's attention to the April 2019 *Notice Regarding Options for Amendments by Patent Owner Through Reissue or Reexamination During a Pending AIA Trial Proceeding*. *See* 84 Fed. Reg. 16,654 (Apr. 22, 2019). If Patent Owner chooses to file a reissue application or a request for reexamination of the challenged patent, we remind Patent

Our conclusions are summarized in the following table.

Claims	35 U.S.C. §	Reference(s)/Basis	Claims Shown Unpatentable	Claims Not Shown Unpatentable
1–3, 14– 17, 28	103	Syvanne		1–3, 14–17, 28
4, 9, 13, 18, 23, 27	103	Syvanne, Bogineni		4, 9, 13, 18, 23, 27
1, 2, 15, 16	103	Mahaffey	1, 2, 15, 16	
Overall Outcome			1, 2, 15, 16	3, 4, 9, 13, 14, 17, 18, 23, 27, 28

VI. ORDER

Upon consideration of the record before us, it is:

ORDERED that claims 1, 2, 15, and 16 of the '034 patent are unpatentable; and

FURTHER ORDERED that, because this is a Final Written Decision, parties to the proceeding seeking judicial review of the decision must comply with the notice and service requirements of 37 C.F.R. § 90.2.

Owner of its continuing obligation to notify the Board of any such related matters in updated mandatory notices. *See* 37 C.F.R. § 42.8(a)(3), (b)(2).

For PETITIONER:

Lois Campbell
Mathew McCullough
Kimball Anderson
WINSTON & STRAWN LLP
llcampbell@winston.com
mrmccullough@winston.com
kanderso@winston.com

For PATENT OWNER:

Patrick McPherson
Christopher Tyson
D. Joseph English
Patrick Muldoon
Tairan Wang
Paul Belnap
DUANE MORRIS LLP
pdmcpherson@duanemorris.com
cjtyson@duanemorris.com
djenglish@duanemorris.com
pcmuldoon@duanemorris.com
twang@duanemorris.com
phbelnap@duanemorris.com