

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*.

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

I. INTRODUCTION

A. Background

Forescout Technologies, Inc. (“Petitioner”) filed a Petition requesting *inter partes* review 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.”).

The Board has authority to determine whether to institute an *inter partes* review. *See* 35 U.S.C. § 314; 37 C.F.R. § 42.4(a). Under 35 U.S.C. § 314(a), we may not authorize an *inter partes* review unless the information in the petition and the preliminary response “shows that there is a reasonable likelihood that the petitioner would prevail with respect to at least 1 of the claims challenged in the petition.”

For the reasons stated below, we determine that Petitioner has established a reasonable likelihood that it would prevail with respect to at least one challenged claim. We therefore institute *inter partes* review as to all challenged claims of the ’034 patent.

B. Related Proceeding

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 only real party-in-interest. Pet. 69. Patent Owner in its Preliminary Response does not contest this identification. Patent Owner identifies Fortinet, Inc., as the only real party-in-interest. Paper 5, 2.

D. The '034 Patent

The '034 patent is titled “Automated Configuration of Endpoint Security Management.” Ex. 1011, (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.

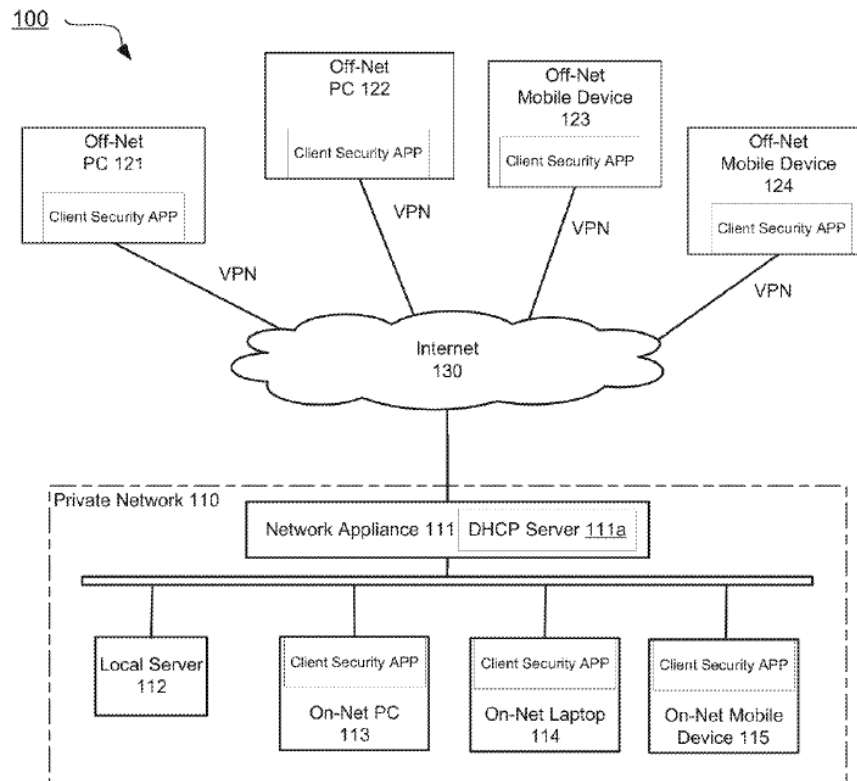


FIG. 1

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 the 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 also explains 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., determine 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 said 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 claims. Claim 1 recites:¹

1. [1pre] 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 relies on the following references:

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

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 Eric Cole, Ph.D. (Ex. 1003, “Cole Decl.”).

¹ Paragraph numbering provided by Petitioner has been added.

G. Asserted Grounds of Unpatentability

Petitioner asserts that the challenged claims would have been 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 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 experience, could also be considered a [person of ordinary skill in the art].” Pet. 7 (citing Cole Decl. ¶¶ 26–28).

Patent Owner states, “[t]o narrow the issues for purposes of this Preliminary Response only, Patent Owner does not dispute Petitioner’s definition of a [person of ordinary skill in the art].” Prelim. Resp. 6.

² Because the application from which the ’034 patent issued was filed after March 16, 2013, the post-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).

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.

B. Claim Construction

In an *inter partes* review, the claims of a patent shall be 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 such 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 be 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).

We construe claim terms only as relevant to the parties' contentions and only to the extent necessary to resolve the issues in dispute. *See Vivid Techs., Inc. v. Am. Sci. & Eng'g, Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999); *Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co. Matal*, 868 F.3d 1013, 1017 (Fed. Cir. 2017).

The parties' claim construction positions are complex. Petitioner contends that the parties disagree over the meaning of only one term: "configuration [for/of] the [client/endpoint] security application." Pet. 8.

Petitioner proposes that the meaning of this term is “a particular hardware and/or software arrangement for the [client/endpoint] security application.” *Id.* (citing Ex. 1009, 23).³

Referring to the parties’ joint claim construction statement in district court, Petitioner asserts that “Patent Owner advances that this term means ‘data defining the functions of the [client/endpoint] security application.’” *Id.* (citing Ex. 1009, 23). Petitioner further submits that, “[r]egardless of which party’s construction is adopted for this term, the prior art teaches this claim element under both parties’ constructions.” *Id.*

Petitioner submits further that Patent Owner advances constructions of several other terms in the parallel district court litigation, and provides a table showing Patent Owner’s proposed constructions. Pet. 9 (citing Ex. 1009, 19–22). Petitioner asserts that for these terms it “has not proposed a construction or has proposed that the claim is indefinite.” *Id.* at 8. But Petitioner contends those terms do not need to be construed, because “the prior art invalidates [the claims] under Patent Owner’s construction.” *Id.* at 9. In sum, Petitioner contends “there are no claim construction issues that would affect the outcome of any trial on this petition.” *Id.*

Patent Owner takes a different approach to claim construction. Prelim. Resp. 6–9. Patent Owner asserts the claim constructions from the district court litigation “are not relevant for the purposes of this Preliminary Response.” *Id.* at 7. Patent Owner responds that to “narrow the issues for purposes of this Preliminary Response only, Patent Owner asserts that the claim terms be given their plain and ordinary meaning.” *Id.* at 6. But Patent

³ Unless otherwise specified, citations to exhibits refer to the page numbers assigned by the parties.

Owner “maintains that the claims are patentable under any reasonable interpretation of the claims.” *Id.* at 7.

Notwithstanding its position that construction is not necessary, Patent Owner observes that, “[a]lthough Petitioner did not expressly propose any claim construction for ‘web content filtering,’ Grounds 1 and 2^[4] [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.” *Id.* at 7. Patent Owner submits instead 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 [Internet Protocol] addresses using an access control list (referred to as an ‘ACL’).” *Id.* at 7–9.

We disagree that no constructions are necessary. But we determine that we need to expressly construe only the term “web content filtering” to resolve the parties’ disputes on the current record. *See Nidec Motor Corp.*, 868 F.3d at 1017 (“[W]e need only construe terms ‘that are in controversy, and only to the extent necessary to resolve the controversy.’” (quoting *Vivid Techs., Inc.*, 200 F.3d at 803)). We discuss our construction of this term in the context of our analysis of Syvanne as applied by Petitioner, *infra*.

We determine that we need not explicitly construe any other claim terms at this stage of the proceeding.

⁴ These two grounds are both based on Syvanne. *See* Pet. 10.

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.

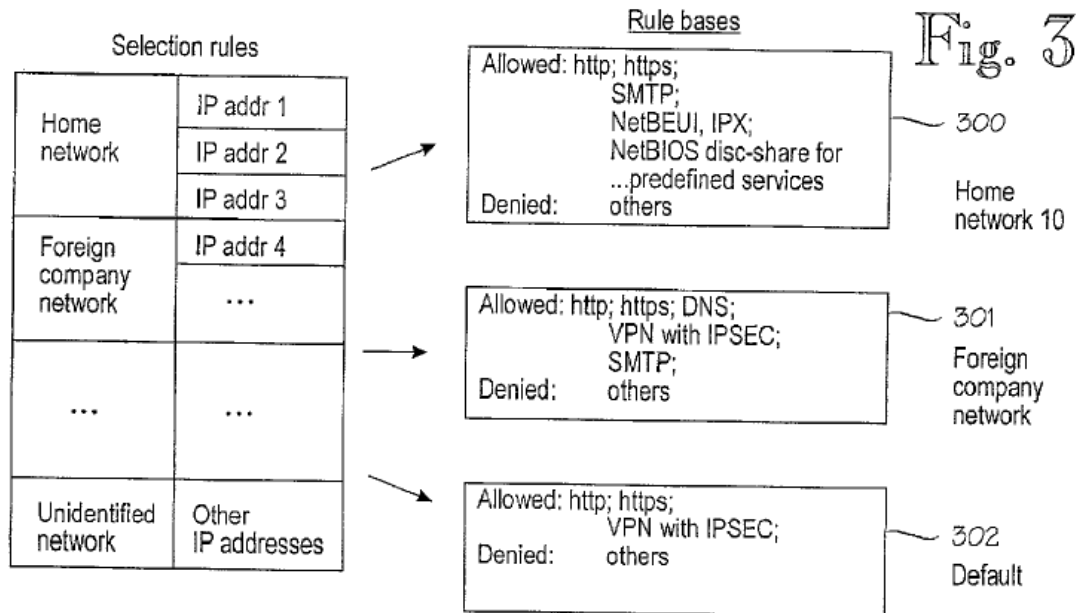
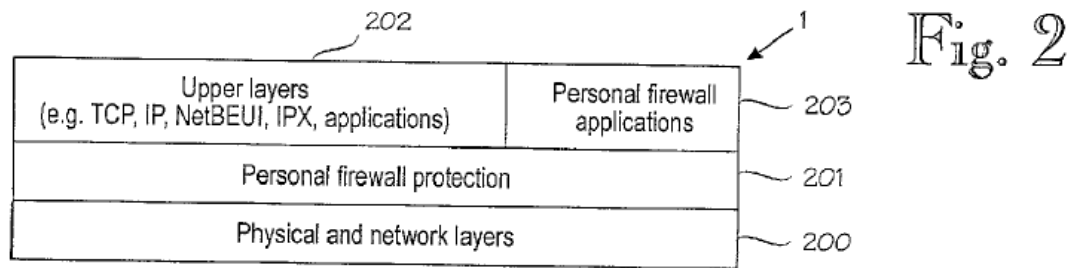


Figure 2 illustrates a protocol stack of a computer device containing a personal firewall. Figure 3 illustrates selection rules and associations between them. *Id.* ¶¶ 18–19.

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 in 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.* 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.* 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 discloses 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.

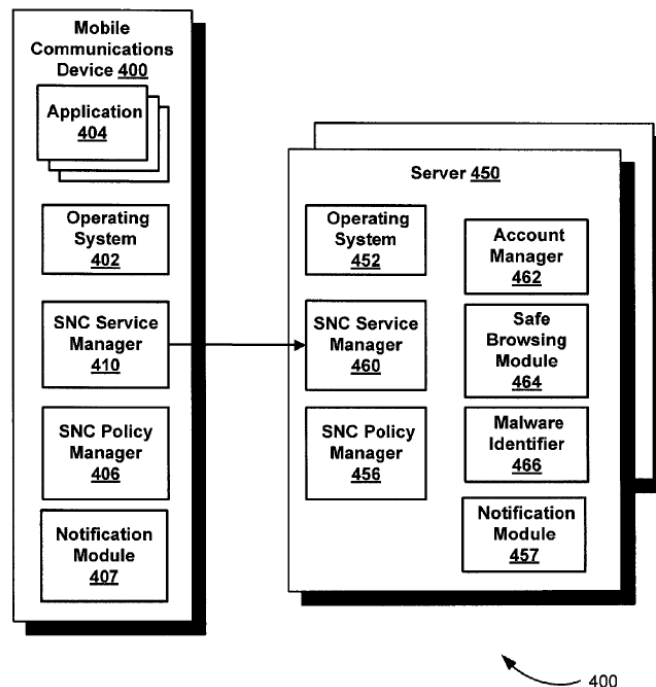


Figure 4A

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. The 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. The 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/revoca- tion 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 to be used. *Id.* at 52:45–50. In an alternative embodiment, policy rules define an explicit security level, and associated information that 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 the Petition nor the Preliminary Response 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. 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.*, Prelim. Resp. 9–19. We initially focus our analysis on claim 1.

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 the flow diagram in Syvanne’s Figure 4 discloses this limitation “[t]o the extent the preamble is limiting.”⁵ Pet. 17; Cole Decl. ¶¶ 84–86. Patent Owner does not dispute this contention at this stage. We determine that for the reasons given, Petitioner demonstrates sufficiently that Syvanne teaches 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 at this stage. We determine that for the reasons given, Petitioner demonstrates sufficiently 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 at this stage. We determine that for the reasons given, Petitioner demonstrates sufficiently that Syvanne discloses element 1a.ii of claim 1.

⁵ 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 at this stage. We determine that for the reasons given, Petitioner demonstrates sufficiently 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.

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 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.

Petitioner maintains that “Syvanne satisfies this [launching] limitation under Patent Owner’s proposed construction of ‘launching.’” *Id.* at 26. Petitioner explains that “the personal firewall [of Syvanne] automatically selects and activates the proper rule base according to the current location of the laptop, which means the security functions of the client security application that are designated by the selected configuration, i.e., the proper rule base according to the current location of the laptop, are initiated by the client security application, i.e., activated by the personal firewall.” *Id.* (citing Cole Decl. ¶¶ 114–115).

Patent Owner disputes this assertion. Prelim. Resp. 10–19. Patent Owner argues that Petitioner has failed to meet its burden with respect to this challenge to claim 1 because Syvanne does not disclose the launching limitation. *Id.* at 9.

The launching limitation requires that the client security application launch “one or more” of three specified functions that are designated by the selected configuration. Ex. 1001, 11:44–47. Those enumerated functions are “web content filtering, anti-virus scanning and network access logging.” *Id.* at 11:47–50.

Patent Owner argues that “the combinations [including Syvanne] that Petitioner relies on . . . do not disclose the launching limitation, and more specifically, do not disclose one or more designated functions of web content filtering, anti-virus scanning, and network access logging.” Prelim. Resp. 9 (emphasis omitted). For the reasons that follow, we agree.

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 in the art] 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 responds that Syvanne does not disclose “web content filtering” as claimed. Prelim. Resp. 15–17. We agree. As Patent Owner points out, Petitioner’s reliance on the argument that Syvanne teaches web content filtering by disclosing blocking HTTP connections but allowing HTTPS connections is misplaced. *Id.* at 16. Petitioner relies on Figure 3 of Syvanne as illustrating web content filtering. Pet. 25. But as Patent Owner points out, Figure 3 of Syvanne describes allowing both HTTP and HTTPS connections, even when communication is with a “potentially hostile” unidentified network. Prelim. Resp. 16 (citing Ex. 1005 ¶ 35). Thus, there is no “filtering” based on those protocols.

More fundamentally, however, we agree with Patent Owner that “[s]imply allowing or blocking a connection is not *web content filtering*.” *Id.* In that regard, we find Patent Owner’s proposed construction of “web content filtering” as “blocking access to a webpage based on the content of the information on the webpage” to be pertinent to our analysis. Prelim. Resp. 7. We note that Petitioner has not provided an explicit construction

for “web content filtering,” nor do we find any definition of the term in the ’034 patent specification.

We find Patent Owner’s construction to be consistent with the plain meaning of the term, and therefore we adopt it for the purpose of this decision. It 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. Prelim. Resp. 16–17. Applying this construction, we determine that Petitioner does not demonstrate that Syvanne teaches “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. *Id.* Accordingly, Petitioner does not demonstrate that Syvanne discloses “web content filtering.”

ii. Network Access Logging

Petitioner contends that Syvanne discloses creating a log file that meets this claim limitation. Pet. 26 (“[T]he personal firewall creates a log file each time the laptop is involved with a communication transaction, such as an Internet session” (citation omitted)). But Patent Owner responds that the personal firewall in Syvanne “creates a log file *before* the current location of the computer device is determined.” Prelim. Resp. 18. Thus, the logging is not “designated by the selected configuration,” as claimed. *Id.* (emphasis omitted).

We agree with Patent Owner that the claimed step of “selecting . . . a configuration for the client security application’ in Syvanne takes place after a log file has been created.” *Id.* (emphasis omitted). As a result, the log file creation in Syvanne does not satisfy the launching limitation, which requires that network access logging to be “designated by the selected configuration.”

We determine that Petitioner has not demonstrated that Syvanne discloses this limitation.

iii. Antivirus Scanning

Petitioner does not assert that Syvanne's personal firewall performs anti-virus scanning, nor does Syvanne disclose this. Prelim. Resp. 19.

f. Conclusion – Claim 1

On the current record, Petitioner has not made a sufficient showing that Syvanne teaches or suggests the “launching” limitation of independent claim 1. Therefore, Petitioner has not demonstrated a reasonable likelihood of prevailing on this challenge to claim 1 as obvious over Syvanne.

2. Claim 15

Petitioner contends independent claim 15 would have been obvious in view of Syvanne. Pet. 30–33. Independent claim 15 includes limitations similar to the limitations recited in independent claim 1, including the launching limitation. *See* Ex. 1001, 13:4–10. At this stage of the proceeding, Patent Owner does not raise arguments for claim 15 that are separate from those discussed above with respect to claim 1. *See* Prelim. Resp. 910–19.

Based on the current record, we determine that for the reasons given for claim 1, Petitioner has not demonstrated a reasonable likelihood of prevailing on this challenge to claim 15 as obvious over 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.

At this stage of the proceeding, Patent Owner does not raise arguments for dependent claims 2, 3, 14, 16, 17, and 28 that are separate

from those discussed above with respect to claims 1 and 15, from which they depend. *See* Prelim. Resp. 10–19.

For the reasons discussed above with respect to claims 1 and 15, Petitioner has not demonstrated a reasonable likelihood of prevailing on this challenge to claims 2, 3, 14, 16, 17, and 28 as obvious over 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.

At this stage of the proceeding, 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* Prelim. Resp. 9, 20.

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. 42 (“Bogineni teaches the additional limitation of claim 4.”)

Thus, for the reasons discussed with respect to claims 1 and 15, we determine that Petitioner has not demonstrated a reasonable likelihood of prevailing in challenge to claims 4, 9, 13, 18, 23, and 27 as 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

We initially focus our analysis on 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 each claim element is disclosed by Mahaffey. For example, Petitioner identifies Mahaffey’s SNC service manager 410 as the “a client security application running on a client device” recited in claim element 1a.1. Pet. 55.

Claim element 1a.ii recites that the method 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 1.a 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.” Pet. 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 this contention that Mahaffey discloses the “determining” step. Prelim. Resp. 23–25. According to Patent Owner, “Mahaffey describes subsequently passing that context information to a separate network device, which makes the actual assessment of the current network connection (i.e., the alleged step of determining a network connection state),” referring to server 450 in Mahaffey’s Figure 4, *supra.* *Id.* at 24 (emphases omitted).

We do not agree with Patent Owner that Mahaffey’s disclosure is so limited. In fact, Mahaffey discloses that 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). The operation of SNC service manager 410 on the mobile device is discussed by Petitioner. Pet. 59–63. We determine

that at this stage, Petitioner has presented sufficient evidence that would support a finding that Mahaffey's SNC service manager 410 provides control over network connections and therefore discloses the "determining" limitation.

The additional limitations of claim 1 are not in dispute at this stage. Thus, Petitioner demonstrates sufficiently that the "selecting" step (claim element 1a.iii) is met by Mahaffey's SNC service manager 410 and policy manager 406. *Id.* at 59. Petitioner explains, "The policies that configure or manage the actions performed by the SNC manager [410] 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 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 62 (citing Cole Decl. ¶¶ 218–219).

Moreover, Petitioner demonstrates that Mahaffey's 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.

At this stage, Patent Owner does not dispute these contentions regarding the "selecting" or "launching" steps.

In summary, on the current record, Petitioner has made a sufficient showing that Mahaffey teaches or suggests the "determining" limitation of independent claim 1 challenged by Patent Owner and all other limitations of

the claim. Therefore, Petitioner has demonstrated a reasonable likelihood of prevailing on this challenge to claim 1 as obvious over Mahaffey.

2. Claim 15

Petitioner contends independent claim 15 would have been obvious over Mahaffey. Pet. 65–68.

At this stage of the proceeding, Patent Owner does not raise arguments for claim 15 that are separate from those discussed above with respect to claim 1. *See* Prelim. Resp. 20–25.

Based on the current record, we determine that for the reasons given for claim 1, Petitioner has established a reasonable likelihood of proving that claim 15 would have been obvious over Mahaffey.

3. Claims 2 and 16

These claims depend from claim 1 or from claim 15. Petitioner relies on Mahaffey to meet the limitations added by these claims. Pet. 63–65, 68–69.

At this stage of the proceeding, 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* Prelim. Resp. 26.

For the reasons given by Petitioner, we are persuaded that Petitioner has demonstrated a reasonable likelihood of prevailing on this challenge to dependent claims 2 and 16 as obvious over Mahaffey.

IV. CONCLUSION

For the foregoing reasons, we have determined that there is a reasonable likelihood that the Petitioner would prevail with respect to at

least one of the claims challenged in the Petition. We therefore institute trial as to all challenged claims on all grounds stated in the Petition.⁶

V. ORDER

Upon consideration of the record before us, it is:

ORDERED that *inter partes* review of claims 1–4, 9, 13–18, 23, 27, and 28 of the '034 patent is instituted on all grounds in the Petition;

FURTHER ORDERED that pursuant to 35 U.S.C. § 314(c) and 37 C.F.R. § 42.4, notice is hereby given of the institution of a trial; the trial will commence on the entry date of this decision.

⁶ We do not address the Petition's discussion of *Fintiv* and other grounds for discretionary denial as Patent Owner has not requested discretionary denial. See Pet. 71–73 (citing, e.g., *Apple Inc. v. Fintiv, Inc.*, IPR2020-00019, Paper 11 at 5–6 (PTAB Mar. 20, 2020) (precedential)).

IPR2021-01329
Patent 9,894,034 B2

FOR PETITIONER:

Katherine A. Vidal
Louis L. Campbell
WINSTON & STRAWN LLP
kvidal@winston.com
llcampbell@winston.com

FOR PATENT OWNER:

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