

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

F5 NETWORKS, INC.,
Petitioner,

v.

PROVEN NETWORKS, LLC,
Patent Owner.

IPR2021-00701
Patent 7,877,786 B2

Before TREVOR M. JEFFERSON, PATRICK M. BOUCHER, and
JOHN A. HUDALLA, *Administrative Patent Judges*.

BOUCHER, *Administrative Patent Judge*.

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

F5 Networks, Inc. (“Petitioner”) filed a Petition pursuant to 35 U.S.C. §§ 311–319 to institute an *inter partes* review of claims 1, 3, 4, 6, and 10–18 of U.S. Patent No. 7,877,786 B2 (Ex. 1001, “the ’786 patent”). Paper 2

(“Pet.”). Proven Networks, LLC (“Patent Owner”) filed a Preliminary Response. Paper 6 (“Prelim. Resp.”).

Applying the standard set forth in 35 U.S.C. § 314(a), which requires demonstration of a reasonable likelihood that Petitioner would prevail with respect to at least one challenged claim, we grant the Petition and institute an *inter partes* review. The Board has not made a final determination regarding the patentability of any claim.

I. BACKGROUND

A. The '786 Patent

The '786 patent “relates to the field of data networks and, more specifically, to methods of protecting network systems from viruses and other malicious applications by enforcing security policies using an isolated sub-network.” Ex. 1001, 1:8–11. Figure 1 of the '786 patent is reproduced below.

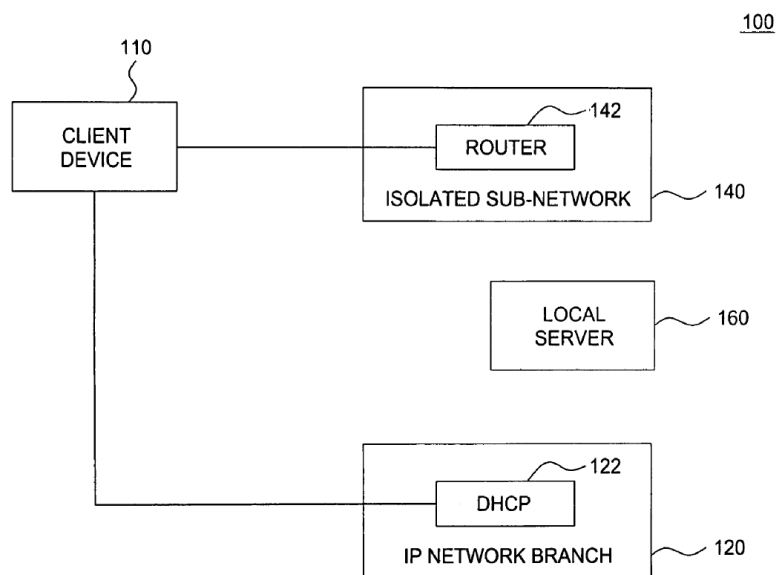


FIG. 1

Figure 1 is a block diagram of a portion of an IP network having an isolated sub-network. *Id.* at 3:1–3. As shown, IP network 100 includes client device 110, IP network branch 120, and isolated sub-network 140 (also referred to in the '786 patent as a “quarantine sub-network”). *Id.* at 3:3–6. In the illustration, sub-network 140 comprises captive portal 142 (shown as a router), and IP network branch 120 comprises a “typical IP network comprising typical IP network components,” such as IP address server 122 (shown as a dynamic host configuration protocol (“DHCP”) server). *Id.* at 3:6–11.

When client 110 establishes a connection with IP network branch 120, IP address server 122 examines the connection for a “special mark or token” sent by client 110. *Id.* at 3:61–65. Such a mark may “indicate[] conformance to the latest security policy,” such as may be determined by calculation and comparison of a hash value over a security-policy file. *Id.* at 4:2–8. Although the '786 patent notes that security policies “may be expressed in substantially any format,” a distinction is drawn between “passive formats,” such as “documents in a memory of a client, and “active formats,” such as “script.” *Id.* at 4:9–14. For example, security policies may be expressed in a scripting language like JavaScript or VBScript that is executed on client 110. *Id.* at 4:14–17. “Using a scripting language, reference may be made to the state of the local machine, for example the Windows registry, a version of the operating system installed, installed patches and software, versions of applications installed, services running, network ports open for receiving packets, general configuration and settings, and users logged into the system, to determine if a client is in conformance with the latest security policies.” *Id.* at 4:17–24.

If IP address server 122 receives a mark indicating conformance with the latest security policy, IP address server 122 issues an IP address to client 110 for communication with IP network branch 120 “as in conventional IP networks.” *Id.* at 4:2–8. Conversely, if no mark is received or if an invalid or outdated mark is received, IP address server 122 directs client 110 to sub-network 140 by assigning an IP address from a predetermined sub-network range that is part of a free private address space and not routable across the Internet. *Id.* at 4:25–35. Isolation is completed by ensuring that packets with a source address within this range are also not forwarded by internal routers and are filtered out at each server to be protected. *Id.* at 4:36–41.

The ’786 patent notes certain alternatives to this quarantine procedure that use multiple virtual local area networks (“VLANs”), in particular by using an extensible authentication protocol (“EAP”). *Id.* at 6:32–67. In such embodiments, “a client is required to do authentication before being granted network access,” and “a RADIUS [i.e., Remote Authentication Dial-In User Service] server may distinguish compliant clients from non-compliant clients and return an appropriate VLAN ID (regular or quarantined, respectively) and/or specific IP address to issue to a client.” *Id.* at 6:39–41, 6:52–56.

B. Illustrative Claim

Independent claim 1 is illustrative of the challenged claims and is reproduced below.

1. A computer program product embodied in a non-transitory computer readable storage medium, the computer program product comprising computer instructions which, when

executed by a processor, cause the processor to perform a method for enforcing security policies of a network, the method comprising:

determining if a client desiring a connection to the network is in conformance with a current version of said security policies, wherein said security policies are expressed in an active format adapted to execute on a client and conformance is determined by examining a token sent by the client; and

if a client is not in conformance with the current version of said security policies, restricting client access to said network of a plurality of virtual local area networks (VLANs), by using an extensible authentication protocol (EAP) to authenticate the client as a valid user of only a subset of available virtual local area networks (VLANs) within the network.

Ex. 1001, 7:7–25.

C. Evidence

Petitioner relies on the following references:

Herrmann	US 2004/0107360 A1	June 3, 2004	Ex. 1005
Krantz	US 2004 /0111520 A1	June 10, 2004	Ex. 1006
Freund	US 2003/0055962 A1	March 20, 2003	Ex. 1019
Yip	US 6,914,905 B1	July 5, 2005	Ex. 1020

In addition, Petitioner relies on a Declaration by David M. Goldschlag, Ph.D. Ex. 1003.

D. Asserted Grounds of Unpatentability

Petitioner challenges claims 1, 3, 4, 6, and 10–18 on the following grounds. Pet. 3.

Claim(s) Challenged	35 U.S.C. §	References
1, 3, 6, 10, 11, 13, 14, 16–18	103 ¹	Herrmann, Krantz
4, 15	103	Herrmann, Krantz, Yip
12	103	Herrmann, Krantz, Freund

E. Real Parties in Interest

The parties identify only themselves as real parties in interest.

Pet. 72; Paper 9, 1.

F. Related Matters

Both parties identify *Proven Networks, LLC v. F5 Networks, Inc.*, No. 3:20-05571 (N.D. Cal.), which has been transferred to the Western District of Texas for inclusion in Multi-District Litigation 2959, Case 20-MC-02959, as involving the '786 patent. Pet. 72; Paper 9, 2.

Petitioner additionally notes that the '786 patent was involved in *Proven Networks, LLC v. F5 Networks, Inc.*, No. 5:20-cv-02521 (N.D. Cal.) and *Proven Networks, LLC v. Extreme Networks, Inc.*, No. 5:20-cv-2067 (N.D. Cal.), both of which were dismissed. Pet. 72–73. Patent Owner additionally notes *Proven Networks, LLC v. Barracuda Networks, Inc.*, No. 5:21-02185 (N.D. Cal.) as a further related matter. Paper 9, 2.

¹ The Leahy-Smith America Invents Act, Pub. L. No. 112-29, 125 Stat. 284 (2011) (“AIA”), included revisions to 35 U.S.C. § 103 that became effective after the filing of the application that led to the challenged patent. Therefore, we apply the pre-AIA version of 35 U.S.C. § 103.

II. ANALYSIS²

A. Legal Principles

A claim is unpatentable for obviousness under 35 U.S.C. § 103 if the differences between the claimed subject matter and the prior art are “such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains.” *KSR Int’l Co. v. Teleflex Inc.*, 550 U.S. 398, 406 (2007). The question of obviousness is resolved on the basis of underlying factual determinations, including: (1) the scope and content of the prior art; (2) any differences between the claimed subject matter and the prior art; (3) the level of skill in the art; and (4) when in evidence, objective indicia of nonobviousness, i.e., secondary considerations.³ *Graham v. John Deere Co.*, 383 U.S. 1, 17–18 (1966).

Additionally, the obviousness inquiry typically requires an analysis of “whether there was an apparent reason to combine the known elements in the fashion claimed by the patent at issue.” *KSR*, 550 U.S. at 418 (citing *In re Kahn*, 441 F.3d 977, 988 (Fed. Cir. 2006) (requiring “articulated reasoning with some rational underpinning to support the legal conclusion of obviousness”)); see *In re Warsaw Orthopedic, Inc.*, 832 F.3d 1327, 1333 (Fed. Cir. 2016) (citing *DyStar Textilfarben GmbH & Co. Deutschland KG v. C.H. Patrick Co.*, 464 F.3d 1356, 1360 (Fed. Cir. 2006)).

² Patent Owner does not advance any arguments for exercising discretion under § 325(d) based on art or arguments previously presented to the Office. We decline to address this issue any further. See Pet. 70–72.

³ At this time, the parties do not address objective indicia of nonobviousness, which accordingly do not form part of our analysis.

B. Level of Ordinary Skill in the Art

In determining whether an invention would have been obvious at the time it was made, we consider the level of ordinary skill in the pertinent art at the time of the invention. *Graham*, 383 U.S. at 17. “The importance of resolving the level of ordinary skill in the art lies in the necessity of maintaining objectivity in the obviousness inquiry.” *Ryko Mfg. Co. v. Nu-Star, Inc.*, 950 F.2d 714, 718 (Fed. Cir. 1991). The “person of ordinary skill in the art” is a hypothetical construct, from whose vantage point obviousness is assessed. *In re Rouffet*, 149 F.3d 1350, 1357 (Fed. Cir. 1998). “This legal construct is akin to the ‘reasonable person’ used as a reference in negligence determinations” and “also presumes that all prior art references in the field of the invention are available to this hypothetical skilled artisan.” *Id.* (citing *In re Carlson*, 983 F.2d 1032, 1038 (Fed. Cir. 1993)).

Petitioner proposes that a person of ordinary skill in the art would [have] possess[ed] at least a bachelor’s degree in computer science or electrical engineering and 3-5 years of professional experience in computer networks, or a master’s or doctorate and 1-2 years of professional experience in computer networks. Additional education could substitute for professional experience, and vice versa. Such a person would have been familiar with computer networks and would have been aware of design trends relating to authentication, authorization, and accounting (AAA).

Pet. 15–16 (citing Ex. 1003 ¶ 13). At this stage, Patent Owner neither challenges Petitioner’s proposal nor proposes its own specific articulation of a level of ordinary skill in the art. Because we find Petitioner’s proposal reasonable, consistent with the level of skill reflected by the prior art, and

supported by the testimony of Dr. Goldschlag, we adopt it for purposes of this Decision. *See Okajima v. Bourdeau*, 261 F.3d 1350, 1355 (Fed. Cir. 2001) (the prior art may reflect an appropriate level of skill in the art).

C. Claim Construction

The Board uses “the same claim construction standard that would be used to construe the claim in a civil action under 35 U.S.C. 282(b), including construing the claim in accordance with the ordinary and customary meaning of such claim 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) (2019); *see Phillips v. AWH Corp.*, 415 F.3d 1303, 1312–13 (Fed. Cir. 2005) (en banc). Although Petitioner notes certain constructions that it has proposed in district court, both parties agree that no term requires construction to decide whether to institute an *inter partes* review in this proceeding. *See* Pet. 14 (Petitioner asserting that “[n]o term needs construction in this proceeding”); Prelim. Resp. 3 (“Patent Owner does not contend that any term requires construction for purposes of this Preliminary Response”).

Because we also discern no term that requires construction to resolve the issues before us, we do not expressly construe any term for purposes of this Decision. *See 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))).

D. Overview of the Prior Art

1. Herrmann

Herrmann “relates generally to information processing and, more particularly, to systems and methods for policy enforcement on computer systems connected to one or more networks, such as Local Area Networks (LANs) and Wide Area Networks (WANs), including the Internet.”

Ex. 1005 ¶ 3. Figure 4 of Herrmann is reproduced below.

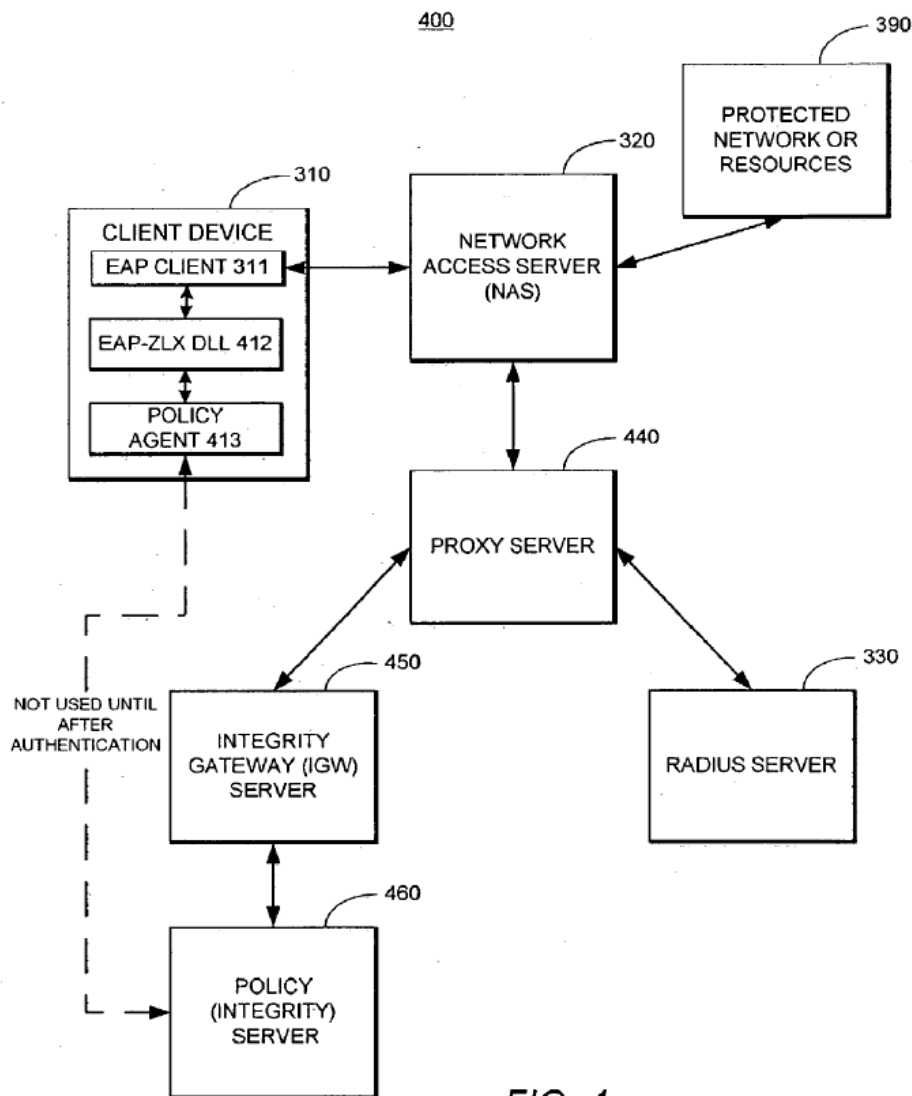


FIG. 4

Figure 4 is a block diagram that illustrates an environment within which Herrmann's methods may operate. *Id.* ¶ 62. As illustrated, environment 100 includes at least one client device 310, network access server ("NAS") 320, RADIUS server 330, protected network or resources 390, proxy server 440, integrity gateway server ("IGW") 450, and policy or integrity server 460. *Id.*

Client device 310 connects to NAS 320 to access protected network resources 390 in two phases. *Id.* ¶ 63. "In the first phase of this process, the NAS 320 works in conjunction with an EAP client 311 on the client device 310 and the RADIUS server 330 to authenticate the session," with identity and authentication information typically obtained from client device 310 using the EAP. *Id.* ¶¶ 56, 63. In response to one or more challenges issued when client device 310 connects to NAS 320, EAP client 311 attempts to collect "appropriate authentication information" and forwards EAP packets containing the information to NAS 320. *Id.* ¶ 56. RADIUS server 330 decides whether to permit access after checking the authentication information and returns either an "Access Reject" or "Access-Accept" message based on the result of that check. *Id.*

The second phase of the process, which is more relevant to Petitioner's challenges, extends the EAP protocol to support "policy-based authentication" in which both client-side and server-side components are used to support "endpoint security negotiation." *Id.* ¶ 63. The client-side components include EAP-ZLX extension dynamic link library ("DLL") 412, which communicates with policy agent 413 to retrieve "information about the current security policy in operation on the client device 310." *Id.* ¶ 64. Such information is packaged by EAP client 311 and sent to NAS 320 for

handling by the server-side components, including proxy server 440, IGW 450, and policy or integrity server 460, which determines whether client device 310 is “in compliance with applicable security policies” and approves or denies the request accordingly. *Id.* ¶¶ 60, 64–65. If client device 310 is not in compliance, “access for the session may be permitted only to a limited group of IP addresses (i.e., a designated ‘sandbox’ area).” *Id.* ¶ 97.

2. *Krantz*

Krantz relates to “automatically providing a computer system with appropriate information such that the computer system can be provisioned to communicate on a network.” Ex. 1006 ¶ 2. Figure 2 of Krantz is reproduced below.

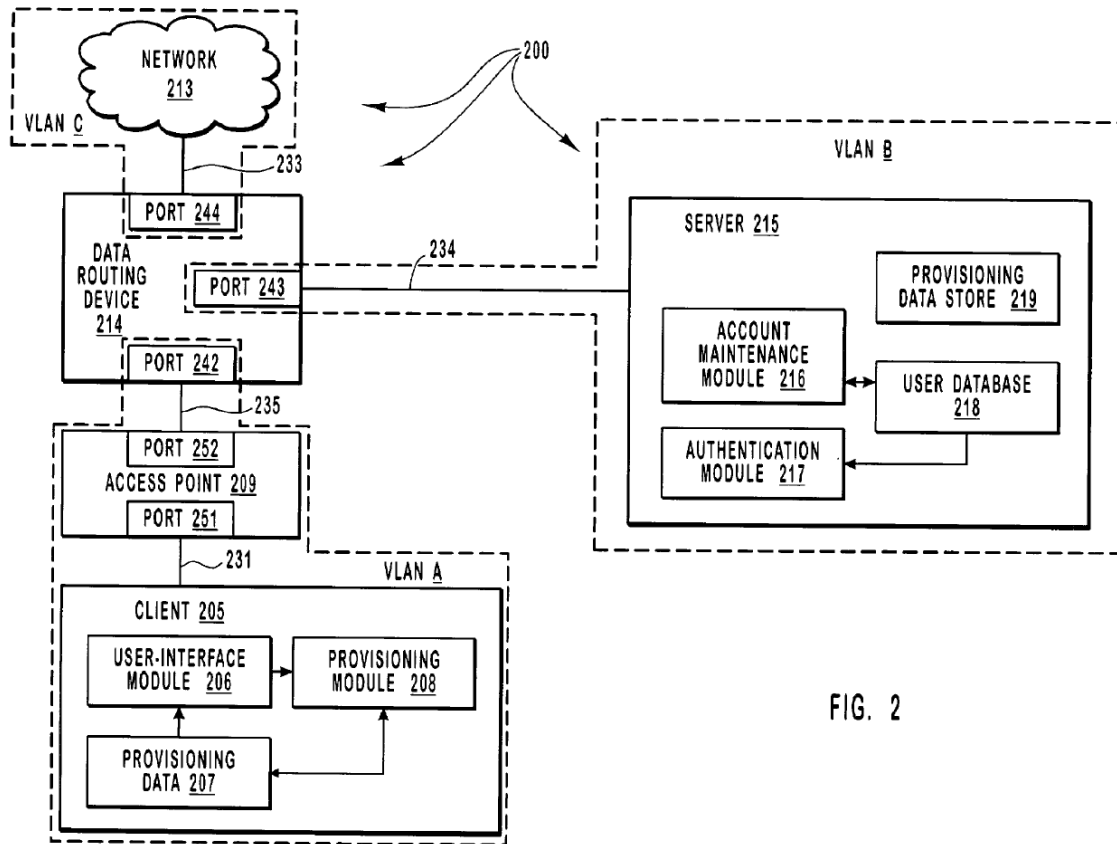


FIG. 2

Figure 2 “illustrates an example of network architecture 200 that can facilitate increasing the level of automation when provisioning a client.” *Id.* ¶ 57. Of particular note, data routing device 214 “has been configured to separate network architecture 200 into VLANs A, B, and C.” *Id.* ¶ 60. Krantz notes that, with this configuration, a client “may be denied access to resources located on VLAN C when a user cannot be authenticated, a user has sent guest credentials, or an authenticated user is not authorized to access resources located on VLAN C.” *Id.* ¶ 77. And, if a client is denied access to resources located on VLAN C, server 215 can authorize the client “for limited resources located on VLAN B.” *Id.*

3. *Yip*

Yip “relates to the field of virtual local area network (VLAN) topologies and internetwork communications technologies.” Ex. 1020, 1:8–10. Yip explains that, “[a]s the number of networks requiring access to the Internet has grown, a third level was introduced into Internet routing protocols to augment the original two-level addressing structure,” with this third level defining “subnetworks” or “subnets.” *Id.* at 2:22–26. According to Yip, subnets can be defined based on IP addresses, such as by assigning some of the host bits to define the subnet. *Id.* at 2:14–44; 3:63–4:3.

4. *Freund*

Freund describes “system[s] and methods for regulating access and maintaining security of individual computer systems and Local Area Networks (LANs) connected to larger open networks (Wide Area Networks or WANs), including the Internet.” Ex. 1019 ¶ 4. In Freund’s system, “[r]equests to connect to the Internet from non-compliant computers are redirected to [a] sandbox server.” *Id.* ¶ 40. “The sandbox server operates by looking for communications on certain port addresses and using the port address as a response code” so that “different port addresses can, in effect, indicate a certain problem or condition.” *Id.* ¶ 95. “Based on the port which the packet is received, the sandbox server displays an appropriate error page corresponding to the compliance problem that is detected.” *Id.* ¶ 115. In some instances, redirection of non-compliant computers includes replacing a destination IP address “with the IP address of the sandbox server.” *Id.* ¶ 149.

E. Obviousness over Herrmann and Krantz

Petitioner challenges claims 1, 3, 6, 10, 11, 13, 14, 16–18 as unpatentable under 35 U.S.C. § 103 over Herrmann and Krantz. Pet. 25–60.

1. Independent Claims 1 and 13

Petitioner treats independent claims 1 and 13 collectively because they “share identical limitations” except that “the preamble of claim 1 recites a computer program product and the preamble of claim 13 recites an apparatus.” Pet. 25.

a. Preambles

For the preambles, Petitioner notes that, because Herrmann describes a “system and methodology for policy enforcement during authentication of a client device for access to a network,” Herrmann thereby discloses techniques “for enforcing security policies of a network,” as recited in each of independent claims 1 and 13. Pet. 25–26 (citing Ex. 1005, Abstr.; Ex. 1003 ¶ 65). In addition, Herrmann discloses that client device 310 requests access to protected network 390 such that, according to Petitioner, Herrmann discloses enforcing its security policies “upon a client requesting a connection to [a] network,” as additionally recited in the preamble of independent claim 13. *Id.* at 26 (citing Ex. 1005 ¶¶ 53, 63).

Patent Owner does not contest Petitioner’s analysis of the preambles at this stage. We determine that Petitioner makes a sufficient showing at this stage of the proceeding that the respective preambles are disclosed by Herrmann. We also find sufficient Petitioner’s further identification of Herrmann’s disclosure of implementation on a general-purpose computer to

meet the “computer program product” and “apparatus comprising a memory” as respectively recited in independent claims 1 and 13. *Id.* (citing Ex. 1005 ¶¶ 41–44, 86). We therefore need not determine whether the preambles are limiting.

b. “determining” step

The “determining” step of both independent claims 1 and 13 includes three aspects: (1) “determining if a client desiring a connection to the network is in conformance with a current version of said security policy,” (2) requiring that “said security policies are expressed in an active format adapted to execute on a client,” and (3) requiring that “conformance is determined by examining a token sent by the client.” Ex. 1001, 7:13–18, 8:11–16. For each of these three aspects, Petitioner relies on Herrmann alone. *See* Pet. 28–37.

Petitioner addresses the first of these aspects by noting Herrmann’s express disclosure that its policy server 460 (shown in Figure 4 of Herrmann, reproduced above) interacts with NAS 320 and IGW 450 to “determine whether or not the client device 310 is in compliance with applicable security policies.” *Id.* at 30 (quoting Ex. 1005 ¶ 66). Specifically, Herrmann’s “policy server 460 evaluates the information that is received to determine whether or not the client is in compliance with applicable rules and requirements,” including whether it has “the correct security policy in place.” *Id.* at 31 (quoting Ex. 1005 ¶¶ 78, 79). For the second aspect, Petitioner identifies Herrmann’s security policy as expressed “at least through the EAP-ZLX DLL 412 and policy agent 413.” *Id.* at 32 (citing Ex. 1005 ¶ 70; Ex. 1013 ¶ 76). Because “[a] DLL and an agent such

as Herrmann’s policy agent are both well-understood to be executable software,” Petitioner contends that Herrmann teaches expressing security policies in an active format. *Id.* at 33 (citing Ex. 1003 ¶ 77). For the third aspect, Petitioner notes that Herrmann discloses that client device 310 may return “the policy MD5 of the policy located on the client device,” which Herrmann characterizes as a “fingerprint” or “message digest.” *Id.* at 34; Ex. 1005 ¶¶ 31, 77. Petitioner supports each of these identifications with testimony by Dr. Goldschlag. Ex. 1003 ¶¶ 69–86.

Patent Owner disputes Petitioner’s showing by noting that Petitioner “unambiguously relies *only* on Herrmann’s DLL and policy agent as allegedly disclosing ‘security policies’ that are ‘expressed in an active format adapted to execute on a client’ or ‘expressed in an active language.’” Prelim. Resp. 7. Because the “determining” limitation requires “conformance with a current version of said security policies,” Patent Owner reasons that “the Petition’s [unpatentability] theory can thus only succeed if the prior art discloses ‘determining . . . conformance with a current version of’ Herrmann’s DLL or policy agent.” *Id.* at 9 (second alteration in original). Patent Owner accordingly faults Petitioner’s analysis for making insufficient connection between the “applicable security policies” Petitioner discusses in addressing the first aspect of the “determining” limitation with the “DLL or policy agent” Petitioner identifies in addressing the second aspect. *Id.* at 10 (“But the Petition provides no allegation that these ‘applicable security policies’ refer to a current version of Herrmann’s DLL or policy agent.”).

The record would benefit from further development of this issue at trial. Although Patent Owner appears to be correct that Petitioner’s theory

requires that the “current version of said security policies” recited in the first aspect of the limitation must correspond to the “security policies” expressed in an “active format” according to the second aspect, it is not apparent at this stage that Petitioner’s theory is ultimately flawed. Petitioner identifies disclosure by Herrmann that its policy server 460 determines whether client device 310 is in compliance with “applicable security policies.” And Petitioner identifies a specific embodiment in which Herrmann’s security policy is expressed through Herrmann’s DLL 412 and policy agent 413. Dr. Goldschlag supports these identifications in Petitioner’s analysis. *See* Ex. 1003 ¶¶ 69–79. Notably, Patent Owner does not dispute that the required correspondence exists in Herrmann, but rather argues that Petitioner has not made such a showing in a particular manner. Mindful of the reasonable-likelihood standard that we apply at this stage, and mindful that Petitioner’s theory is supported by testimonial evidence while Patent Owner relies only on attorney argument, we find Petitioner’s showing sufficient.

c. “restricting” step

The “restricting” step of independent claims 1 and 13 is implicated “if a client is not in conformance with the current version of said security policies.” Ex. 1001, 7:19–20, 8:17–18. In such a case, the claims require that client access be restricted “to said network of a plurality of virtual local area networks (VLANs), by using an extensible authentication protocol (EAP) to authenticate the client as a valid user of only a subset of available virtual local area networks (VLANs) within the network.” *Id.* at 7:20–25, 8:19–23.

In addressing the “restricting” step, Petitioner notes that “Herrmann restricts access to its network for clients that do not conform with the required security policy.” Pet. 37. Specifically, upon determining nonconformance, Herrmann’s policy server 460 “may restrict a session to limited access (e.g., a set of IP addresses) rather than deny access completely.” *Id.* (citing Ex. 1005 ¶ 78). In addition, Herrmann also teaches the use of EAP during both authentication and authorization, including an express extension “to support policy-based authentication systems.” *Id.* at 40 (citing Ex. 1005 ¶¶ 56, 58; Ex. 1003 ¶¶ 92–93). Although Herrmann does not expressly describe implementing restricted access in the context of a network of VLANs, Petitioner reasons that such would have been obvious in light of Krantz’s teaching of VLANs, particularly because Krantz specifically assigns a subset of VLANs as an isolated “sandbox” area. *Id.* at 37–38.

Specifically, Petitioner reasons that a person of ordinary skill in the art “would have been motivated to segregate Herrmann’s sandbox area using at least one separate VLAN to improve network security,” and supports that reasoning with testimony by Dr. Goldschlag. *Id.* at 22 (citing Ex. 1003 ¶ 53). Petitioner also provides evidence that VLANs would have been recognized at the time of invention as a well-known technique for segregating network portions having different security needs. *Id.* at 23 (citing Ex. 1003 ¶ 54 (testimony of Dr. Goldschlag); Ex. 1031, Abstr. (IEEE 802.1Q standard)). In addition, Dr. Goldschlag testifies that a person of ordinary skill in the art would have been motivated to implement Herrmann’s network using VLANs “for improved scalability and network management.” Ex. 1003 ¶ 55. Furthermore, Petitioner identifies language

in Krantz to support its contention that Krantz itself motivates the combination by teaching that VLANs were a known alternative to IP filtering for restricting network access. Pet. 24 (citing Ex. 1006 ¶ 32; Ex. 1003 ¶ 56).

Patent Owner does not dispute Petitioner’s reasons for combining Herrmann and Krantz, and, on the record before us, we find that reasoning supported by a rational underpinning. We accordingly find that Petitioner makes a sufficient showing at this stage with respect to the “restricting” limitation of independent claims 1 and 13.

d. Summary

In light of these considerations, we conclude that Petitioner demonstrates a reasonable likelihood of prevailing on its challenge of independent claims 1 and 13 as unpatentable under 35 U.S.C. § 103 over Herrmann and Krantz.

2. Independent Claim 18

Petitioner challenges independent claim 18 as unpatentable under 35 U.S.C. § 103(a) over Herrmann and Krantz. Pet. 43–53. The preamble of claim 18 recites a “network architecture for enforcing security policies of a network upon a client requesting a connection to said network.” Ex. 1001, 8:37–39. Petitioner contends that “Herrmann’s client, servers, protected resources, and sandbox area, and their various relationships and connections, constitute a ‘*network architecture*’ because together they describe the underlying structure of Herrmann’s network.” Pet. 43. We agree with this contention, which is supported by Dr. Goldschlag’s testimony. See Ex. 1003

¶¶ 117, 119. We further agree with Petitioner’s contention that such an architecture is “for enforcing security policies of a network upon a client requesting a connection to said network” for the reasons we discuss above in connection with claims 1 and 13. *See* Pet. 44. We accordingly determine that Petitioner makes a sufficient showing with respect to claim 18’s preamble, and we need not determine whether the preamble is limiting.

The body of claim 18 recites that the network architecture comprises “at least one client” and “an isolated sub-network.” Ex. 1001, 8:40–46. The “at least one client” is “adapted to execute, among other applications, security policies that are expressed in an active language.” *Id.* at 8:40–42. For this limitation, Petitioner identifies Herrmann’s client device 310, which includes EAP-ZLX DLL 412 and policy agent 413, as providing expression of security policies in an active language. Pet. 45–47. For the reasons we discuss in connection with independent claims 1 and 13, we determine that Petitioner makes a sufficient showing with respect to this limitation.

The “isolated sub-network” is “for making accessible to non-conforming clients a current version of said security policies and isolating said non-conforming clients for network resources.” Ex. 1001, 8:43–46. For this limitation, Petitioner identifies Herrmann’s sandbox area, and Dr. Goldschlag supports that identification through his testimony that a person of ordinary skill in the art “would have understood the sandbox area to constitute an ‘*isolated sub-network*’ because users cannot access other resources from this sandbox area.” Pet. 48; Ex. 1003 ¶ 130 (citing Ex. 1005 ¶ 79). We agree with Petitioner’s analysis, which is not contested by Patent Owner at this time.

In addition to these limitations, independent claim 18 requires that the “network” itself includes an “address server for controlling the access of said at least one client to said network” and is adapted to perform steps that largely parallel the “determining” and “restricting” steps of independent claims 1 and 13. Ex. 1001, 8:47–62. Petitioner contends that “Herrmann motivates the use of an ‘*address server*’ because to gain access to Herrmann’s network, the client requires a network address.” Pet. 50. Dr. Goldschlag’s testimony supports this contention, and Dr. Goldschlag also testifies that “[a]n obvious way to issue such IP addresses would be for the apparatus to include an address server such as a DHCP server, as disclosed by Krantz.” Ex. 1003 ¶¶ 99–100, 114, 135. Dr. Goldschlag further testifies that, in the combined system, the address server is “for controlling the access of said at least one client to said network” because both Herrmann and Krantz include an NAS that controls access of clients to the network. *Id.* ¶ 136 (citing Ex. 1005 ¶ 63; Ex. 1006 ¶ 58). Patent Owner does not dispute this reasoning at this time, and on the current record we find it sufficient.

Rather, Patent Owner disputes Petitioner’s showing with respect to the “determining” and “restricting” steps required for the address server—for which Petitioner relies on the same reasoning presented for independent claims 1 and 13. Prelim. Resp. 6; *see* Pet. 52–53 (Petitioner noting similarity of limitations and referring to its earlier analysis). Specifically, Patent Owner contends that “[c]laim 18’s recitation of ‘said security policies’ in the ‘determining’ step . . . refers back to the ‘security policies’ of [the ‘at least one client’ limitation,] which limitation . . . requires to be ‘expressed in an active language.’” Prelim. Resp. 6. Nevertheless, as

discussed above in the context of independent claims 1 and 13, we do not agree on the current record that Patent Owner's contentions undermine the adequacy of Petitioner's showing. In particular, Petitioner both identifies disclosure in Herrmann that its policy server 460 determines whether client device 310 is in compliance with "applicable security policies" and identifies a specific embodiment in which Herrmann's security policy is expressed through Herrmann's DLL 412 and policy agent 413. *See supra* § II.E.1.b. For the same reasons mentioned above, this analysis, along with Dr. Goldschlag's supporting testimony, is sufficient for institution. Notwithstanding, the record would benefit from further development of this issue at trial.

For these reasons, we conclude that Petitioner demonstrates a reasonable likelihood of prevailing on its challenge of independent claim 18 as unpatentable under 35 U.S.C. § 103(a) over Herrmann and Krantz.

3. Dependent Claims 3, 6, 10, 11, 14, 16, and 17

Petitioner challenges claims 3, 6, 10, 11, 14, 16, and 17, which depend from either independent claim 1 or independent claim 13, as unpatentable under 35 U.S.C. § 103(a) over Herrmann and Krantz. Pet. 53–60.

Petitioner's analysis is supported by Dr. Goldschlag's testimony, and is not contested at this time by Patent Owner outside of Patent Owner's arguments directed at the independent claims. *See* Ex. 1003 ¶¶ 97–115.

We have reviewed Petitioner's analysis of these claims and find it sufficient at this stage of the proceeding.

4. *Dependent Claims 4 and 15*

Claim 4 depends from independent claim 1 and recites that “a non-conforming client is directed to said network of a plurality of virtual local area networks by being issued a predetermined address adapted to direct said client to said network of a plurality of virtual local area networks.”

Ex. 1001, 7:32–36. Claim 15 depends from independent claim 13 and recites a substantially similar limitation. *Id.* at 8:26–30. Petitioner acknowledges that “neither Herrmann nor Krantz explicitly discloses that a non-conforming client is directed to the VLANs by being issued a predetermined address,” and thus relies on Yip’s disclosure of defining subnets based on IP addresses to meet this feature. Pet. 61–65.

Supported by Dr. Goldschlag’s testimony, Petitioner reasons that a person of ordinary skill in the art “would have been motivated to define the plurality of VLANs disclosed in Krantz by subnet IP addresses as disclosed in Yip,” particularly in light of Yip’s disclosure that layer-3 VLANs “allow[] hosts to move to a different physical port on the switch in the same VLAN without having to reconfigure the host IP addresses.” *Id.* at 62–63 (quoting Ex. 1020, 1:55–58) (citing Ex. 1003 ¶ 145). Patent Owner does not, at this time, challenge Petitioner’s analysis of claims 4 and 15 outside of its arguments directed at the underlying independent claims, and we find Petitioner’s analysis sufficient at this stage.

We conclude that Petitioner demonstrates a reasonable likelihood of prevailing on its challenge of dependent claims 4 and 15 as unpatentable under 35 U.S.C. § 103(a) over Herrmann, Krantz, and Yip.

5. *Dependent Claim 12*

Claim 12 depends from independent claim 1 and recites that “said isolated sub-network directs a non-conforming client to a web server which directs said non-conforming client to a predetermined web-site for accessing a current version of said security policies.” Ex. 1001, 8:1–5. Although Petitioner contends that Herrmann discloses “an isolated sub-network directs a non-conforming client to a web server . . . for accessing a current version of said security policies,” Petitioner acknowledges that “Herrmann does not explicitly disclose that the web server directs the client to a ‘*predetermined web-site*.’” Pet. 66 (citing Ex. 1003 ¶ 151).

For this aspect of claim 12’s limitation, Petitioner relies on Freund’s redirection of a non-compliant computer to a sandbox by replacing a destination IP address with the IP address of the sandbox server. *Id.* at 69. Based on Freund’s teaching of directing a client request to the sandbox server to a specific port in accordance with the reason for non-compliance, Petitioner reasons that “[t]he webpage corresponding to a given port is a ‘*predetermined web-site*’ because it is predetermined based on the reason for the client’s non-compliance.” *Id.* (citing Ex. 1003 ¶ 154; Ex. 1034, 479). Because Herrmann expressly incorporates Freund by reference, specifically for “[f]urther description of a ‘sandbox’ web server for assisting users in remedying non-compliance,” Ex. 1005 ¶ 79, Petitioner reasons that a person of ordinary skill in the art would have been motivated to combine Freund’s sandbox teachings with the systems and methods described in Herrmann. Pet. 69–70. Patent Owner does not at this time challenge Petitioner’s analysis of claim 12 outside of its arguments directed at underlying

independent claim 1, and we find Petitioner’s analysis sufficient at this stage.

We accordingly conclude that Petitioner demonstrates a reasonable likelihood of prevailing on its challenge of claim 12 as unpatentable under 35 U.S.C. § 103(a) over Herrmann, Krantz, and Freund.

III. CONCLUSION

For the foregoing reasons, we conclude that the information presented in the Petition establishes a reasonable likelihood that Petitioner would prevail in showing that at least one of claims 1, 3, 4, 6, and 10–18 of the ’786 patent is unpatentable. Accordingly, we institute an *inter partes* review, which will include all challenged claims and grounds asserted in the Petition. See *SAS Inst., Inc. v. Iancu*, 138 S. Ct. 1348, 1359–60 (2018); *AC Techs. S.A. v. Amazon.com, Inc.*, 912 F.3d 1358, 1364 (Fed. Cir. 2019) (“[I]f the Board institutes an IPR, it must . . . address all grounds of unpatentability raised by the petitioner.”); U.S. Patent and Trademark Office, *Guidance on the impact of SAS on AIA trial proceedings* (Apr. 26, 2018), <https://www.uspto.gov/patents-application-process/patent-trial-and-appeal-board/trials/guidance-impact-sas-aia-trial> (“SAS Guidance”).

IV. ORDER

In consideration of the foregoing, it is

ORDERED that, pursuant to 35 U.S.C. § 314(a), *inter partes* review is hereby instituted as to claims 1, 3, 4, 6, and 10–18 of the ’786 patent on all grounds set forth in the Petition; and

IPR2021-00701
Patent 7,877,786 B2

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, commencing on the entry date of this Decision.

IPR2021-00701
Patent 7,877,786 B2

PETITIONER:

Lori Gordon
Steven Peters
David Brun
KING & SPALDING LLP
lgordon@kslaw.com
speters@kslaw.com
sbrun@kslaw.com

PATENT OWNER:

Reza Mirzaie
C. Jay Chung
RUSS AUGUST & KABAT
rmirzaie@raklaw.com
jchung@raklaw.com