

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

APPLE INC.,
Petitioner,

v.

VIRNETX INC.,
Patent Owner.

Case IPR2016-00332
Patent 8,504,696 B2

Before MICHAEL P. TIERNEY, *Vice Chief Administrative Patent Judge*,
KARL D. EASTHOM and STEPHEN C. SIU, *Administrative Patent Judges*.

EASTHOM, *Administrative Patent Judge*.

FINAL WRITTEN DECISION
35 U.S.C. § 318(a) and 37 C.F.R. § 42.73

I. INTRODUCTION

A. Background

Petitioner, Apple Inc., filed a Petition (Paper 1, “Pet.”) seeking an *inter partes* review of claims 1–11, 14–25, 28, and 30 (the “challenged claims”) of U.S. Patent No. 8,504,696 B2 (Ex. 1001, “the ’696 patent”), pursuant to 35 U.S.C. §§ 311–319. Pet. 6. After Patent Owner, VirnetX Inc., filed a Preliminary Response (Paper 6, “Prelim. Resp.”), we instituted an *inter partes* review of the challenged claims (Paper 8, “Institution Decision” or “Inst. Dec.”).

Subsequent to institution, Patent Owner filed a Patent Owner Response (Paper 14, “PO Resp.”), Petitioner filed a Reply (Paper 17, “Pet. Reply”), and Patent Owner filed a Sur-Reply (Paper 18, “PO Sur-Reply”). The Board filed a transcription of the Oral Hearing held on March 27, 2017. (Paper 28, “Tr.”). This Final Written Decision issues concurrently with the final written decision involving the ’696 patent in *Apple Inc. v. VirnetX Inc.*, IPR2016-00331 (PTAB June 22, 2017).

The Board has jurisdiction under 35 U.S.C. § 6(c). This Final Written Decision issues pursuant to 35 U.S.C. § 318(a) and 37 C.F.R. § 42.73. For the reasons that follow, we determine that Petitioner has shown by a preponderance of the evidence that claims 1–11, 14–25, 28, and 30 of the ’696 patent are unpatentable.

B. Related Matters

Petitioner indicates that the ’696 patent “has not been asserted in litigation or the subject of other IPR proceedings.” Pet. 2. Petitioner concurrently filed a petition challenging the same claims and claim 29 in the ’696 patent in IPR2016-00331. *Id.* at 5. Petitioner and Patent Owner

provide listings of district court actions, other *inter partes* review, and *inter partes* reexamination proceedings challenging related patents. *See id.* at 2–5, Paper 5, 3–15; *see also VirnetX, Inc. v. Cisco Systems, Inc.*, 767 F.3d 1308, 1317–19 (Fed. Cir. 2014) (addressing ancestor *VirnetX* patents);¹ *VirnetX Inc. v. Apple Inc.*, 665 F. App’x 880 (Fed. Cir. 2016) (affirming *Apple Inc. v. VirnetX Inc.*, Cases IPR2014-00237, IPR2014-00238 (PTAB May 11, 2015) (final written decisions “’237 FWD,” “’238 FWD,” or generally, “’237 IPR,” ’238 IPR”) (appealed by *VirnetX*));² *VirnetX Inc. v. Apple Inc.*, 671 F. App’x 786 (Fed. Cir. 2016) (affirming *Apple Inc. v. VirnetX Inc.*, Cases IPR2014-00403, IPR2014-00404, IPR2014-00481, IPR2014-00482 (PTAB July 29, 2015) (final written decisions, “’403 FWD,” “’404 FWD,” “’481 FWD,” “’482 FWD,” or generally, “’403 IPR,” ’404 IPR,” etc.) (appealed by *VirnetX*));³ *Apple Inc. v. VirnetX Inc.*, Case IPR2015-00811 (PTAB Sept. 8, 2016) (appealed by *VirnetX*); *Apple Inc. v. VirnetX Inc.*, Case IPR2015-00812 (PTAB Aug. 30, 2016) (appealed by

¹ The ’696 patent is a continuation of an application, which is a continuation of U.S. Patent No. 7,921,211, which is a continuation of U.S. Patent No. 7,418,504 (“’504 patent”), which is a continuation-in-part of U.S. Patent No. 6,502,135 (“’135 patent”)—three of the four patents at issue in *Cisco*. *See Cisco*, 767 F.3d at 1313. (The fourth patent at issue in *Cisco*, is U.S. Patent No. 7,490,151 (“’151 patent”), a division of the ’135 patent.)

² The court affirmed the ’237 FWD and the ’238 FWD without reaching the merits of the ’237 FWD. *See* 665 F. App’x at 889 (*In re Gleave*, 560 F.3d 1331, 1338 (Fed. Cir. 2009) (“declining to address alternative grounds of invalidity when the court upholds one such ground”).

³ The court affirmed the four final written decisions without reaching the merits of the ’404 FWD and ’482 FWD. *See* 671 F. App’x at 787 (finding “no error in the Patent Trial and Appeal Board’s (‘the Board’) claim constructions or findings in the 403 and 481 proceedings).

IPR2016-00332
Patent 8,504,696 B2

VirnetX); *Apple Inc. v. VirnetX Inc.*, IPR2015-00870 (PTAB Sept. 28, 2016) (appealed by VirnetX); *Apple Inc. v. VirnetX Inc.*, IPR2015-00871 (PTAB Sept. 28, 2016) (“’871 FWD” or generally “’871 IPR”) (appealed by VirnetX). Some of these related cases involve overlapping claim construction and prior art issues with the instant case and are discussed further below as necessary.

C. References and Declarations

Petitioner relies on the following references.

Reference	Description	Publication or Issue Date	Exhibit No.
Aventail	Aventail (see note 4)	1996–1999	Ex. 1009–1011 ⁴
RFC 2401	S. Kent & R. Atkinson, RFC 2401, <i>Security Architecture for the Internet Protocol</i> , Network Working Group, Request for Comments	Nov. 1998	Ex. 1008
RFC 2543	Handley et al., <i>SIP: Session Initiation Protocol</i> , Network Working Group, Request for Comments	Mar. 1999	Ex. 1013

⁴ Exhibits 1009–1011 relate to an Aventail Connect software application and are collectively referred to as “Aventail” unless otherwise noted. See *Aventail Connect v3.01/v2.51 Administrator’s Guide* (“Aventail Administrator Guide,” Ex. 1009), *Aventail Connect v3.01/v2.51 User’s Guide* (1996–1999) (“Aventail User Guide,” Exhibit 1010), and *Aventail ExtraNet Center v3.0 Administrator’s Guide (NT and UNIX)* (“Aventail ExtraNet,” Exhibit 1011).

Reference	Description	Publication or Issue Date	Exhibit No.
Yeager	N. YEAGER & R.E. MCGRAW, WEB SERVER TECHNOLOGY, THE ADVANCED GUIDE FOR WORLD WIDE WEB INFORMATION PROVIDERS (Michael B. Morgan et al. eds., 1996)	1996	Ex. 1066

Pet. 6, Attachment B.

Petitioner also relies on, *inter alia*, the Declaration of Roberto Tamassia (Ex. 1005, “Tamassia Declaration”), the Declaration of the RFC Publisher for the Internet Engineering Task Force, an Organized Activity of the Internet Society, signed by Sandy Ginoza (Ex. 1060, “Ginoza Declaration”), the Declaration of Christopher Hopen (Ex. 1023, “Hopen Declaration”), the Declaration of Michael Fratto (Ex. 1043, “Fratto Declaration”), and the Declaration of James Chester (Ex. 1022 “Chester Declaration”). The latter three declarations were submitted in a related inter partes reexamination proceeding. *See* Pet. 18–19 (listing reexamination 95/001,682).

Patent Owner relies on two declarations, Declaration of Fabian Monroe, Ph.D., submitted originally in two related cases, *Apple Inc. v. VirnetX, Inc.*, Cases IPR2015-00811, IPR2015-00812 (PTAB Dec. 11, 2015) (Ex. 2016 “Monroe Declaration”; Ex. 2018, “Monroe Declaration”).

D. Asserted Grounds of Unpatentability

Petitioner challenges claims of the ’696 patent as unpatentable on the following 35 U.S.C. § 103(a) grounds.

References	Claims Challenged
Aventail, RFC 2401	1, 4, 5, 9–11, 14–16, 19, 20, 24,

	25, 28, and 30
Aventail, RFC 2401, and RFC 2543	2, 3, 6–8, 17, 18, and 21–23
Aventail, RFC 2401, and Yeager	15 and 30

Pet. 6.

E. The '696 Patent

The '696 patent describes secure methods for communicating over the Internet. Ex. 1001, Abstract, 10:3–8. Specifically, the '696 patent describes “the automatic creation of a virtual private network (VPN) in response to a domain-name server look-up function.” *Id.* at 39:23–25. This automatic creation employs a modified Domain Name Server, which may include a conventional Domain Name Server (DNS) and a DNS proxy (*id.* at 40:20–40:22):

Conventional Domain Name Servers (DNSs) provide a look-up function that returns the IP address of a requested computer or host. For example, when a computer user types in the web name “Yahoo.com,” the user’s web browser transmits a request to a DNS, which converts the name into a four-part IP address that is returned to the user’s browser and then used by the browser to contact the destination web site.

Id. at 39:26–32.

The DNS proxy of the modified DNS server intercepts DNS lookup requests, determines whether the user has requested access to a secure site (using for example, a domain name extension or an internal table of secure sites), and if so, whether the user has sufficient security privileges to access the requested site. *Id.* at 40:26–35. If the user has requested access to a secure site to which it has insufficient security privileges, the DNS proxy returns a “‘host unknown’” error to the user. *Id.* at 40:49–52. If the user has requested access to a secure site to which it has sufficient security privileges, the DNS proxy requests a

gatekeeper to create a VPN between the user's computer and the secure target site. *Id.* at 40:32–35. The DNS proxy then returns to the user the resolved address passed to it by the gatekeeper, which need not be the actual address of the destination computer. *Id.* at 40:39–44.

The VPN is “preferably implemented using the IP address ‘hopping’ features,” (i.e., changing IP addresses based upon an agreed upon algorithm) described elsewhere in the ’696 patent, “such that the true identity of the two nodes cannot be determined even if packets during the communication are intercepted.” *Id.* at 3:4–8. The system may hide the identities (i.e., anonymity, a form of security) by encrypting parts of packets, including the true final destination. *See id.* at 1:50–56, 10:3–10:67.

“Tunneled Agile Routing Protocol (TARP)” (*id.* at 3:16–18) routers 122–127, described as “special servers or routers” (*id.* at 10:4–5) along the hopping path, “are similar to regular IP routers 128–132” (*id.* at 10:5–6). *See id.* Fig. 2. TARP routers determine the “next-hop in a series of TARP router hops” (*id.* at 10:15–16) in the path and the final destination, by authenticating or decrypting transmitted encrypted parts of packets to find the next-hop TARP router address. *Id.* at 3:36–63, 10:23–67. “Once the outer layer of encryption is removed, the TARP router determines the final destination. Each TARP packet 140 undergoes a minimum number of hops to help foil traffic analysis.” *Id.* at 3:47–50 “[T]he hops may be chosen at random. . . .” *Id.* at 3:50–51. “The fact that different packets take different routes provides distinct advantages by making it difficult for an interloper to obtain all the packets forming an entire multi-packet message.” *Id.* at 3:56–59. Data messages in the packets also may be encrypted. *See id.* at 1:50–56, 4:7–12.

F. Illustrative Challenged Claim 1

Independent claims 1 and 16 recite the same limitations respectively in system and method format. *Compare* Ex. 1001, 56:8–23, *with id.* at 57:1–14. All other challenged claims depend from claims 1 or 16. Claim 1, illustrative of the challenged claims, follows:

1. A system for connecting a first network device and a second network device, the system including one or more servers configured to:
 - intercept, from the first network device, a request to look up an internet protocol (IP) address of the second network device based on a domain name associated with the second network device;
 - determine, in response to the request, whether the second network device is available for a secure communications service; and
 - initiate a virtual private network communication link between the first network device and the second network device based on a determination that the second network device is available for the secure communications service, wherein the secure communications service uses the virtual private network communication link.

Ex. 1001, 56:7–23.

II. ANALYSIS

A. Claim Construction

In an *inter partes* review, the Board construes claims by applying the broadest reasonable interpretation in light of the specification. 37 C.F.R. § 42.100(b); *Cuozzo Speed Techs., LLC v. Lee*, 136 S. Ct. 2131, 2144–46 (2016) (upholding the use of the broadest reasonable interpretation standard under 37 C.F.R. § 42.100(b)). Under this standard, absent any special definitions, claim terms or phrases are given their ordinary and customary meaning, as would be understood by one of ordinary skill in the art, in the

context of the entire disclosure. *In re Translogic Tech., Inc.*, 504 F.3d 1249, 1257 (Fed. Cir. 2007).

For the purposes of this Decision, only the claim clause below needs express construction. *See Vivid Techs., Inc. v. Am. Sci. & Eng'g, Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999) (only those terms which are in controversy need to be construed and only to the extent necessary to resolve the controversy); Pet. Reply 5–6 (“Patent Owner advances no patentability arguments based on its proposed constructions for ‘server,’ ‘domain name,’ ‘secure communication service,’ ‘modulation,’ and ‘intercept[ing] . . . [a/the] request,’ so they need not be construed.”) (citing *Vivid Techs.*, 200 F.3d at 803).

Virtual Private Network Link (“VPN Link”)

Claims 1 and 16 recite a “virtual private network link” (“VPN link”). Citing, *inter alia*, the Board’s claim construction in the ’237 IPR and ’481 IPR, Petitioner proposes that the terms “VPN link” means “a transmission path that includes portions of a public network and restricts access to data, addresses, or other information on the path, generally using obfuscation methods to hide information on the path, including, but not limited to, one or more of authentication, encryption, or address hopping.” *See* Pet. 15–16 (citing ’237 FWD 10; Ex. 1005 ¶ 75); Pet. Reply 3–5 (citing ’481 FWD 10, arguing that prosecution history and the ’696 patent do not show that a secure communication and VPN link requires a “direct” communication).

Patent Owner states “[a] ‘virtual private network communication link’ in view of the specification is ‘a communication path between two devices in a virtual private network,’ where a virtual private network is a network of computers which privately and directly communicate with each other by

encrypting traffic on insecure paths between the devices where the communication is both secure and anonymous.” PO Resp. 3 (citing Ex. 2018 ¶¶ 21–30). This latter part of Patent Owner’s construction that pertains to a virtual private network does not address the issue clearly of the recited VPN link. Patent Owner does not urge anonymity clearly or specifically as required for the recited VPN link under a broadest reasonable construction. Citing *Cisco*, Patent Owner also contends “[a]s the Court noted, ‘encryption of traffic’ is required on these ‘insecure paths.’” *Id.* at 14 (quoting *Cisco*, 767 F.3d at 1322). In another section of its Response, Patent Owner argues that a VPN link requires a direct link and encryption (i.e., without mentioning anonymity). *Id.* at 27. (“[I]n the context of the ’696 patent claims, the virtual private network communication link between a first network device and a second network device is a *direct* communication link between the first network device and the second network device that is encrypted.”).

In addition to arguing a VPN link only requires a direct encrypted link (*see id.*), Patent Owner also does not argue that Aventail does not disclose or suggest anonymity on its VPN link. *See id.* at 27–30. Accordingly, on this record, it is not necessary to determine if a VPN link requires anonymity on all parts of the link under a broadest reasonable construction of a VPN link.

On one hand, because we determine below that the combination of Aventail and RFC 2401 teaches or suggests the argued features of a VPN link under at least one of Patent Owner’s proposed constructions, we need not resolve each of the various claim construction arguments. On the other hand, as an alternative, because Patent Owner contends the combination of Aventail and RFC 2401 does not teach or suggest a direct encrypted VPN

link, with a VPN link as part of a VPN network, we reach these disputed portions of the claim construction.

Petitioner contends that collateral estoppel prevents Patent Owner from making these particular claim construction arguments, because prior related Board final written decisions affirmed by the Federal Circuit previously addressed the construction of the term. Pet. Reply 3–4 (citing the ’481 FWD and generally the *VirnetX-Apple* decisions recently affirmed, *supra* nn. 2 & 3). In additional briefing requested by Patent Owner and granted, Patent Owner contends that the “Federal Circuit expressly did not reach” the merits of any Board decision where construction of the term “was essential to a final judgment.” See P.O. Sur-Reply 1–2. This argument has merit. Petitioner does not meet its burden of showing collateral estoppel applies here, because Petitioner does not direct specific attention to a Board or Federal Circuit final judgment in which resolving the construction regarding the direct requirement was necessary to the judgment.

Regarding the alleged “network of computers” requirement of a VPN asserted by Patent Owner, Petitioner quotes the ’696 Specification: “The secure communication link is a virtual private network communication link over the computer network.” Pet. 16 (quoting Ex. 1001, 6:63–65). This cited sentence does not require a VPN link to be in a VPN network of other computers that communicate privately with the first and second network devices. Furthermore, claim 1 only recites two devices: “a virtual private network communication link between the first network device and the second network device.”

Petitioner also notes the ’696 Specification states “software module 3309 accesses secure server 3320 through VPN communication link 3321.”

Pet. 16 (quoting Ex. 1050, 52:19–20; Fig. 33). Petitioner explains that with respect to Figure 33, “communication link 3321 is shown *as only the portion of the path between computer 3301 and server 3320 that is over network 3302.*” *Id.* (citing Ex. 1001; 52:19–20, Fig. 33; Ex. 1005 ¶ 74) (emphasis added). Figure 33 and relevant descriptions thereof reveal a mere communications link 3321 that connects between ISP 3303 and server 3320, without requiring a network of other devices, as Petitioner contends. *See* Ex. 1050, 52:19–20, Fig. 33. Therefore, the Specification supports Petitioner. Contrary to Patent Owner’s arguments, the claim language and Specification do not support a requirement for a VPN link that includes a VPN that requires additional network computers to be connected via the recited VPN link, in order to communicate separately and privately with each other or the first and second network computers.

Regarding the “direct” requirement, Petitioner contends the inclusion of “direct” adds an additional limitation that the Board previously rejected in the related ’481 FWD. *See* Pet. Reply 3 (citing ’481 FWD, 7–11). Patent Owner contends that the Specification “*describes a virtual private network link as ‘direct’ between a client and target device.*” PO Resp. 28 (emphasis added). Contrary to Patent Owner’s arguments, even if the Specification describes embodiments that skilled artisans would have recognized may have a direct connection, without more, such a mere description is not enough to support a lexicographic definition, claim disavowal, or importation of an embodiment’s features into the claim term.

Moreover, none of the citations provided by Patent Owner, relating to the TARP routers or otherwise, use the term “direct” or otherwise indicate what the term embraces. *See* PO Resp. 8 (citing Ex. 1001, 10:3–12, Fig. 2;

34:3–8, 40:32–35, 41:25–28), 42:32–36, 43:25–29 (allegedly “describing a variation of the TARP embodiments as including a direct communication link”), 38:29–32, 49:13–15, 49:21–36. The cited TARP embodiment at least includes an edge router 2903 or an ISP 2901 within an Internet path. *See* Ex. 1001, 43:25–29, Fig. 29.

Patent Owner and Petitioner agree that any direct embodiments include various intervening devices (including routers): “In each of these embodiments, the ’696 patent specification discloses that the link traverses a network (or networks) through which it is simply passed or routed via various network devices such as Internet Service Providers, firewalls, and routers.” PO Resp. 9 (citing Ex. 1001, Figs. 2, 24, 28, 29, 33; Ex. 2018 at ¶¶ 16, 17, 27)). Similarly, Petitioner states that the ’696 patent Specification “describes secure communication links that traverse firewalls, edge routers, and proxies between end devices in a connection.” Pet. Reply 5 (citing Ex. 1001, 33:60–34:30, 49:39–43, 53:38–54:32, 55:55–67).

The disclosed TARP routers do not require the claims to have a direct element. Each TARP router processes packets to determine the “next-hop in a series of TARP router hops” (Ex. 1001 at 10:15–16) in the path and the final destination, by authenticating or decrypting transmitted encrypted parts of packets to find the next-hop TARP router address, which may be “random.” *Id.* at 3:36–63, 10:23–67. “[T]he TARP router receiving the TARP packet 140 may forward the TARP packet 140 to a TARP router 122–127 that the current TARP terminal chooses at random.” *Id.* at 10:62–64. And each TARP router decides “whether it should forward the TARP packet 140 to another TARP router 122–127 or to the destination TARP terminal 110.” *Id.* at 10:55–57.

In other words, these TARP routers create a multitude of random paths by decrypting and processing packets. Moreover, after “the outer layer of decryption is completed by a TARP router 122–127, *the TARP router determines the final destination.*” Ex. 1001, 10:47–49 (emphasis added). In addition to including various TARP routers and other intervening devices that do not impede a direct path, the path also may include “Internet, through an ISP 3303,” an “edge router,” and a “load balancer that distributes packets across different transmission paths.” See Ex. 1001, 6:11–12, 49:40–43; Fig. 33. Patent Owner does not argue that a “direct” path (or the claims) precludes a TARP router or a load balancer. See, e.g., PO Resp. 8 (citing 42:32–36, 43:25–29 as “describing a load balancing example in which a virtual private network is direct between a first host and a second host”).

The '696 Specification portions cited by Patent Owner do not even mention a direct path, let alone shed light on what it means. Patent Owner also does not provide a definition or clarify in its briefing what “direct” means. For example, Patent Owner contends that “some anonymity techniques involve ‘an intermediate server interposed between a client and destination server’ and thus are not direct.” PO Resp. 6–7 (quoting Ex. 1001, 1:65–2:8, 2:44–48, Fig. 1). Patent Owner’s oblique argument “that some anonymity techniques” do not create a direct communication link does not support its disavowal or disclaimer arguments. *Id.* at 7. The Specification does not describe the prior art “intermediate server” as an indirect link, and the cited passage does not mention anything about the link as being direct or indirect. See *id.* at 6–7 (citing Ex. 1001, 1:65–2:8). Furthermore, the cited embodiment employs a proxy server with the intermediate server, and Patent Owner obliquely implies without any

explanation or evidence that the Specification somehow describes one server (the intermediate server), but not the other server (the proxy server), as impeding a direct link. *See id.*; Ex. 1001, 1:65–2:9; Fig. 1.

Another passage cited by Patent Owner employs “crowd proxies . . . interposed between originating and target terminals. . . . Each intermediate proxy can send the message either to another randomly chosen proxy in the ‘crowd’ or to the destination.” *See* Ex. 1001 2:47–52 (cited at PO Resp. 6–7). Patent Owner does not explain how these crowd proxies impede a direct link, and nothing in the passage mentions direct or indirect links. The crowd proxies appear to operate much like the TARP routers of the disclosed invention, as described above and further below, which create random router hops and decide to send the message packet either to another randomly chosen router or the destination. *Compare* Ex. 1001, 2:47–52 (crowd proxies), *with id.* at 3:36–63 and 10:23–67 (TARP routers).

Accordingly, the Specification does not show clearly how different edge routers, intervening routers, load balancers, TARP routers, proxy servers, or any other devices, some of which may or may not decrypt and/or encrypt packets along the way and provide random hop blocks, require a “direct” connection or show what the unclaimed term “direct” means. In the absence of a clear special definition or other consideration, even if Patent Owner points to a direct connection in an embodiment, “limitations are not to be read into the claims from the specification.” *In re Van Geuns*, 988 F.2d 1181, 1184 (Fed. Cir. 1993).

Patent Owner also alleges that it disclaimed the term “VPN” during prosecution of a completed reexamination of the related ’135 patent (*see supra* note 1) so as to require a “direct” VPN link. *See* PO Resp. 8–10

(citing 2002, 5; Ex. 2006, 6–9; Ex. 2011, 7), 28 (citing Ex. 2012, 8); Ex. 3001 (part of the ’135 patent’s prosecution history). These arguments are not persuasive. The ’135 patent reexamination Examiner first found that Aventail *anticipates* claims directed to a VPN, Patent Owner made arguments attempting to overcome Aventail, and then, the Examiner determined that the requestor had not shown Aventail to be prior art (based on Patent Owner’s additional arguments directed to the publication date of Aventail). See Ex. 3001 (Examiner’s responses during the ’135 patent reexamination);⁵ Ex. 2011, 2–3 (Patent Owner arguing “the Office Action has failed to establish that Aventail is prior art” during the ’135 patent reexamination). As discussed further below, Patent Owner’s Aventail-based VPN prosecution history arguments, which effectively became moot according to the reexamination record, do not amount to a clear disclaimer that binds the public. See Ex. 3001; *supra* note 5.

Where a “patent has been brought back to the agency for a second review,” the Board should consult the patent’s prosecution history. *Microsoft Corp. v. Proxyconn, Inc.*, 789 F.3d 1292, 1298 (Fed. Cir. 2015); *Straight Path IP Grp., Inc. v. Sipnet EU S.R.O.*, 806 F.3d 1356, 1362 (Fed. Cir. 2015) (prosecution history “is to be consulted even in determining a claim’s broadest reasonable interpretation”). After consulting the prosecution history, in cases like this one, *Tempo Lighting, Inc. v. Tivoli*,

⁵ See Ex. 3001, 20–21 (Reexam. Cont. No. 95/001,269, Action Closing Prosecution (June 16, 2010)), 12 (Right of Appeal Notice, 4 (Oct. 29, 2010)), 4–5 (NIRC)) (all confirming claims directed to a VPN over Aventail because Aventail was not shown to be prior art), 29–34 (Non-final Office Action (Jan. 15, 2010) (finding anticipation by Aventail of claims ’135 patent claims 1, 3, 4, 6–10, and 12)).

LLC, 742 F.3d 973 (Fed. Cir. 2014) “observes that the PTO is under no obligation to accept a claim construction proffered as a prosecution history disclaimer.”

Assuming the equitable doctrine of prosecution estoppel (disclaimer) applies to this ongoing proceeding, the party seeking to invoke the doctrine bears the burden of proving the existence of a “clear and unmistakable” disclaimer that would have been evident to one skilled in the art. *See Elbex Video, Ltd. v. Sensormatic Elecs. Corp.*, 508 F.3d 1366, 1371 (Fed. Cir. 2007) (“Claim terms are entitled to a ‘heavy presumption’ that they carry their ordinary and customary meaning to those skilled in the art in light of the claim term’s usage in the patent specification,” and the “doctrine [of prosecution disclaimer] does not apply ‘where the alleged disavowal is ambiguous;’ the disavowal must ‘be both clear and unmistakable’ to one of ordinary skill in the art.”) (citations omitted); *Rambus Inc. v. Infineon Techs. AG*, 318 F.3d 1081, 1089–91 (Fed.Cir.2003) (finding no clear disclaimer because the statement made was “facially inaccurate” in light of the remainder of the prosecution history); *Biotec Biologische Naturverpackungen GmbH & Co. KG v. Biocorp, Inc.*, 249 F.3d 1341, 1348 (Fed.Cir.2001) (finding no clear disclaimer because “a person of reasonable intelligence would not be misled into relying on the erroneous statement, for it is contrary not only to the plain language of the claims and the specification, but also to other statements in the same prosecution document”); *cf. Desper Prods., Inc. v. QSound Labs., Inc.*, 157 F.3d 1325, 1334–36 (Fed.Cir.1998) (concluding prosecution statements were clear and unmistakable disclaimer because they were entirely consistent with written description and knowledge of those skilled in the art).

Patent Owner argues that during the District Court phase of the *Cisco* litigation, Petitioner (as a defendant) argued that Patent Owner narrowed the claims by arguing the prior art did not include a “direct” VPN during the ’135 reexamination proceeding, and our reviewing court (at the Federal Circuit) agreed with Petitioner by affirming (in part) the District Court. *See* PO Resp. 9–10 (citing *Cisco*, 767 F.3d at 1317 n.1; Ex. 2002, 5; Ex. 2004, 6–8). Patent Owner also contends that the Federal Circuit “noted that a virtual private network link requires direct communication.” *See id.* at 10 (citing *Cisco*, 767 F.3d at 1317 n.1). Specifically, Patent Owner points out that *Cisco* “stat[ed] that the district court’s construction of VPN is ‘a network of computers which privately and directly communicate with each other by encrypting traffic on insecure paths between the computers where the communication is both secure and anonymous.’” *Id.* at 10 (quoting *Cisco*, 767 F.3d at 1317 n.1).

Nevertheless, although the *Cisco* District Court relied on the alleged ’135 patent reexamination VPN disclaimer arguments, it is not clear if the parties informed the court to consider that the ’135 patent reexamination Examiner found that Aventail anticipates the argued claims of the related ’135 patent and allowed the claims only because the requestor failed to meet the burden of showing Aventail is prior art to the related ’135 patent. *See* Ex. 2003, 6–8 (District Court addressing “directly”; *VirnetX Inc. v. Apple Inc.* 925 F. Supp. 816, 830 (E.D. Tex. 2013) (similar). Also, in its briefing in the instant proceeding, as discussed above and further below, Patent Owner does not clarify what the term “direct” means.

Under these circumstances and others discussed below, not requiring the challenged claims to include a “direct” VPN does not contradict the

construction the *Cisco* reviewing court adopted from the District Court. That particular claim construction was not at issue during the *Cisco* appeal. In other words, in the *Cisco* appeal, the parties did not dispute the “direct” requirement, and our reviewing appellate court simply adopted the requirement. *See, e.g., Cisco*, 767 F.3d at 1317–19 & n.1 (no discussion of a controversy about the “direct” requirement).

Also, our reviewing court employs a different standard when reviewing a district court’s construction. *See In re Rambus, Inc.*, 694 F.3d 42, 46 (Fed. Cir. 2012) (contrasting the Board’s review of expired patents, which is “similar to that of a district court’s review,” with the Board’s review of unexpired patents, which involves the broadest reasonable interpretation standard); *Cuozzo*, 136 S. Ct. at 2142. As indicated above, the ’696 patent Specification does not require a direct link and Patent Owner does not explain clearly how to interpret “direct” on this record. *See* PO Resp. 8–12 (arguing a VPN link must be direct based on prosecution history without specifying what “direct” means). Accordingly, and as discussed further below, Patent Owner’s alleged disavowal was not made “with reasonable *clarity*, *deliberateness*, and *precision*,” because the scope of a “direct” VPN link is unclear on this record. *See In re Paulsen*, 30 F.3d 1475, 1480 (Fed. Cir. 1994) (emphases added).

Furthermore, *even Patent Owner’s* arguments during the *Cisco* District Court litigation *agree* with our finding above that any “direct” requirement lacks requisite clarity. That is, referring to the reexamination of the ’135 patent, Patent Owner contended the opposite of what it contends now: It informed the *Cisco* District Court that its reexamination prosecution arguments *did not amount to clear disclaimer*. *See* Ex. 2004, 6 (District

Court noting “VirnetX argues that its statements during reexamination [of the ’135 patent] *are not a clear disavowal* of claim scope”) (emphasis added).⁶

During the reexamination of the ’135 patent, Patent Owner (then Patentee) made several arguments regarding a VPN in an attempt to distinguish over Aventail. In one argument during the ’135 patent reexamination, Patentee argued that “Aventail Connect’s falsification of [i.e., a false DNS response] the network information would prevent the correct transfer of data,” and “[t]hus, Aventail has not been shown to disclose a VPN.” Ex. 2011, 7. In another argument, Patentee described a scenario in which a VPN requires two public computers X, Y to be able to communicate with two private computers A, B “without establishing a separate SOCKS connection,” implying that a VPN requires all four “to be a part of the same VPN.” *See id.* at 6. Patentee also argued that Aventail did not disclose a VPN “because computers connected according to Aventail do not communicate directly with each other.” *Id.* at 7. Patentee also argued that “Aventail does not disclose a VPN, where data can be addressed to one or more different computers across the network, regardless of the location of the computer.” *Id.* at 6. Patentee also argued “Aventail has not been shown to demonstrate that computers connected via the Aventail system are able to

⁶ We similarly noted in ’871 FWD (*see supra* Section I.D) that notwithstanding the Cisco District Court’s findings of a disclaimer, Patent Owner argued that *it did not* make a clear disclaimer at the PTO disavowing the scope of a VPN regarding the direct requirement. *See* Ex. 2002, 5–6; ’871 FWD, 25–26 n. 12.

communicate with each other as though they were on the same network.”
Id. at 5.

It is not clear how any single one of these arguments (e.g., the direct argument, the false network information argument, or the several computers on the same network argument) amounts to a clear disclaimer that should bind the public *in this proceeding*—especially when the Examiner adopted a totally different reason (i.e., Aventail was not prior art), and Patent Owner argued during the *Cisco* litigation its prosecution arguments lacked the requisite clarity to rise to a disclaimer.⁷ Even though a defendant may pick from one of several clear arguments made during prosecution to bind a patent owner during infringement litigation, such a disclaimer “generally only binds the patent owner” under the equitable doctrine of disclaimer. *See Tempo Lighting*, 742 F.3d at 978. Otherwise, a Patent Owner generally may be able to cherry pick any one of several arguments it made during a prior prosecution and assert it as an allegedly clear disclaimer against the public at a subsequent stage at the PTO.

Tellingly, in this case, during the jury trial in the *Cisco* litigation, the parties ultimately disagreed over what “direct” means or covers. *See VirnetX Inc. v. Apple Inc.* 925 F. Supp. 816, 830 (E.D. Tex. 2013). That is, addressing the jury’s decision, the District Court determined “[b]oth parties agree that ‘secure communication’ requires a direct communication, *however the parties dispute whether a network address translator (NAT)*

⁷ The defendants and the court in the District Court litigation noted that Patentee (VirnetX) contended it made several non-binding prosecution arguments. *See* Ex. 2002, 6–7 & nn. 5–6; *see also* Ex. 2004, 6 (similar determination by District Court).

allows for direct communication” and determined “there was substantial evidence to support a finding that NATs allow direct communication.” *Id.* at 830, 831(emphasis added). This disagreement coalesces with Patent Owner’s argument to the *Cisco* District Court that it did not make a clear disagreement. *See supra* notes 6 & 7; Ex. 2004, 6.⁸

Although generally an examiner need not agree to prosecution arguments in order for a district court subsequently to bind a patent owner to a those arguments (as clear disclaimer arguments), the lack of any agreement here signifies the lack of a meaningful understanding that otherwise would serve the public notice function of a disclaimer. *See Phillips v. AWH Corp.*, 415 F.3d 1303, 1317 (Fed. Cir. 2005 (en banc)) (“Like the specification, *the prosecution history provides evidence of how the PTO and the inventor understood the patent.* . . . Yet because the prosecution history represents an ongoing negotiation between the PTO and the applicant, rather than the final product of that negotiation, it often lacks the clarity of the specification and thus is less useful for claim construction purposes.” (Emphasis added)).

In addition to Patentee’s above-noted arguments during the ’135 patent reexamination proceeding, Patentee also argued that Aventail’s SOCKS (ExtraNet) server merely “relays” data “to a target computer on a private network,” and “[t]he client cannot open a connection with the target itself. . . . Instead the client computer and target computer are deliberately

⁸ As noted above, VirnetX initially argued during claim construction that it did not disclaim the scope of a VPN to require a direct communication. *See* Ex. 2004, 6 (District Court Memorandum Opinion and Order construing claims and noting “VirnetX argues that its statements during reexamination are not a clear disavowal of claim scope”).

separated by the intermediate SOCKS server.” Ex. 2011, 7 (emphasis added). But as explained above, the parties agree that the disclosed routers, load balancers, proxy servers, and firewalls in the ’696 patent also may “separate” targets and clients without impeding a direct path, and the disclosed TARP routers (like the Aventail SOCKS server) relay packet information (and decrypt packet information). In addition, as described above, like the SOCKS server, the ’696 patent requires the proxy server to “open a connection.” See, e.g., Ex. 1001, 40:26–28 (“DNS proxy 2610 intercepts all DNS look up functions from client 2605”). And in *Cisco*, the court affirmed a finding of infringement even though the infringing product included intermediate “VPN servers, VPN authentication servers, proxy servers, and firewalls.” *Cisco*, 767 F.3d at 1322.

In the instant proceeding, Patent Owner argues that “*the path* between the client device and the remote host is *relayed* through the SOCKS server and is not a direct link connection.” PO Resp. 28. Patent Owner also argues “[t]he link between the client device and the remote host is not a direct link because the connection is terminated at the SOCKS server, causing a new connection to be created to the remote host.” *Id.* at 29. Patent Owner makes these arguments in an attempt to distinguish over Aventail, but the arguments do not appear in Patent Owner’s claim construction section that relies on a prosecution history disclaimer. Compare PO Resp. 8–12 (arguing a VPN requires a “direct” connection without explaining what “direct” means), with PO Resp. 28–29 (making “relayed” and “terminated” arguments to distinguish over Aventail). Even if these arguments implicitly (somehow) tie into Patent Owner’s alleged disclaimer arguments made during prosecution, the arguments ambiguously suggest a “path” can be

“relayed,” and also that a server (or router) relay constitutes a termination that impedes a direct link somehow. In other words, these unclear prior art arguments by Patent Owner fail to clarify how to interpret the alleged “direct” requirement of a VPN.

During the oral hearing of the trial in the related ’871 IPR (*see supra* Section I.B), the panel asked Patent Owner “for a simple definition of ‘direct’” and Patent Owner stated that it “can’t come up with exact words,” but “the crux of direct is direct addressability.” ’871 IPR Tr. 42:21–43:2 (Paper 38 (record of the ’871 IPR oral hearing)). But when asked “[s]o, that’s the definition of direct is that you have to have the destination in the packet? . . . You have to have the destination address in the packet header, is that what ‘direct’ means?,” Patent Owner replied, “[n]o Your Honor, I mean, *I think there are many ways.*” *Id.* at 42:14–19 (emphasis added). According to this colloquy, Patent Owner appears to have answered “no” to both questions of the compound question—i.e., indicating neither a packet nor its header must contain the final destination address to support a “direct” requirement. In a preceding explanation, Patent Owner stated that the disclosed packets “are routed to each immediate routers, for instance, but they’re addressed directly to [the] final destination.” *Id.* at 42:11–13. None of this represents a clear depiction of what “direct” means.

Recall, for example, that Patent Owner’s Response arguments cited above attempt to distinguish crowd proxies in the prior art as impeding a direct link, but there, the proxies appear somehow to process packets to obtain the final destination, just like the TARP routers of the disclosed invention. *See* PO Resp. 6–7 (citing Ex. 1001, 2:50–52 (prior art crowd proxies using anonymity technique)). Of course, Patent Owner cannot

create a disclaimer *during this trial* in order to narrow the challenged claims *for this trial*, but Patent Owner's belated explanations here fail to clarify its alleged prior prosecution history disclaimers allegedly made during the '135 patent reexamination. As noted, even until recently, Patent Owner "cannot come up with exact words" to describe its alleged disclaimer that occurred via arguments made during the '135 patent reexamination. See '871 IPR, Tr. 42:21–43:2

During the Oral Hearing in this case, the panel asked questions similar to those asked during the '871 IPR oral hearing in an effort to determine what the term "direct" means in the context of Aventail's SOCKS servers and the disclosed TARP routers:

Judge Easthom: Okay. I guess one of the questions I have, there was language in [the record] that said that you are not precluding firewalls, you're not precluding servers, you're not precluding routers. And we have a server here in Aventail, so I'm trying to -- I can't figure out how do we know which type of server this is in Aventail, the SOCKS server? Why is that one sort of the one that's precluded [as impeding a direct path], as it would be if it was a Kiuchi-type server [as determined in *Cisco*], versus the kind of router you have disclosed in your patent?

For example, in your [disclosed TARP] routers, you take a packet and I think you strip off the encryption off the outer layer of the packet before you send the packet on to the next router. So there is a bit of processing going on. And that's what I am kind of struggling with with [respect to] Aventail, if you could help us out. Your ['696 patent] allow[s] for some processing in the server evidently, because your routers, your TARP routers, do allow for processing.

Mr. Zeilberger: Well, your Honor, again . . . our primary argument for the construction for "direct" requirement is prosecution history disclaimer. *Our specification is consistent with that in that*, in the example you pointed to you are *directly*

addressing the target in that, by virtue of having the IP address, that has enough information to send -- to get the packet that you are sending to arrive at the target. Whereas in Aventail, the SOCKS server breaks down the connection, and actually you need all the extra information that is at the SOCKS server to arrive at the end destination.

Tr. 30:15–31:11 (emphasis added).

Patent Owner’s explanation that the “directly addressing” requirement “is consistent” (*see id.*) with the prosecution history disclaimer implies Patent Owner did not make the argument in a sufficiently clear fashion, if at all, during the relied-upon prosecution. *See* Ex. 2011, 5–8 (making three main arguments without mentioning direct addressability). Also, the argument made *after prosecution during the Oral Hearing in this case*, that direct addressability implies “having the IP address,” and having “*enough information to send*” the packet to its destination, does not specify clearly on one hand, if direct addressability requires *the packets* to have the actual final destination’s IP address, or on the other hand, if direct addressability requires the packet to have enough information, so that the TARP routers can determine the final destination via processing along (the random) path to the final destination. *See id.* (emphasis added).

Also, the arguments at both oral hearings (here and in the ’871 IPR) appear to attempt to create a distinction between addressing the packets to an intermediate device (the SOCKs server) (or routers) and “routing,” a distinction that Patent Owner does not clarify and that does not exist. *See* ’871 IPR Tr. 42:11–12 (alleging the packets in the disclosed invention “are routed to each immediate router[], for instance, but they’re addressed

directly to final destination”), 42:6–7 (alleging “the packets [in Aventail] are actually addressed to the SOCKS server, not to the final destination”).⁹

Materially similar to the Aventail system (with a SOCKS server), as discussed above, the ’696 patent’s disclosed packets may contain *some information* regarding the final destination address (but not necessarily the “real IP address”), the disclosed system addresses packets to TARP routers along the way, and the disclosed TARP routers process the packets to obtain the final destination. *See* Ex. 1001, 11:28 (discussing “agile routing” features and stating “[i]n reality, whenever a TARP router looks up the address of a destination in the encrypted header, *it must convert a TARP address to a real IP address using its LUT*”) (emphasis added). In similar fashion, as Patent Owner’s counsel argued during the instant Oral Hearing as quoted above and as discussed further before (in addressing the challenged claims), Aventail’s system initially proxies (addresses) packets to the SOCKS server, but the packets ultimately contain sufficient information for the SOCKS server to process the packets and determine the final terminal destination requested by a user during a VPN communication. *See also infra* Sections II.C.1 & II.C.4 (discussing Aventail’s disclosure and the challenged claims).

The oral hearing arguments also do not comport with the Specification for other reasons. For example, similar to not including the “real IP address” in packets, the ’696 patent states that “[t]he address that is returned need

⁹ As noted above, Patent Owner did not indicate clearly, during the ’871 oral hearing, if the packets or the packet headers must contain the destination address in order to satisfy the alleged “direct” requirement. *See* ’871 IPR Tr. 42:14–19 (“No, Your Honor, I think there are many ways.”).

*not be the actual address of the destination computer.” See Ex. 1001, 40:43–44. This latter disclosure comports generally with some descriptions of TARP router examples discussed above, in which routers decide where to send the packets using processing and decryption (sending packets either to another randomly selected TARP router or the final destination TARP terminal using agile routing). See Ex. 1001, 3:36–4:40, 10:23–11:29 (discussed above), Fig. 2. So although the Specification states at one place that “[e]ach TARP packet’s true destination is concealed behind a layer of encryption generated using a link key,” as just noted, it also states the TARP packets *do not contain “the real IP address”* of the final destination (TARP terminal 110) or intervening TARP routers. *Id.* at 3:36–36, 11:27–30; Fig. 2. Moreover, a “TARP router[] and terminal[]” (i.e., the final destination) “may change its IP address” at any time, using a look up table (LUT) for translation, and the “TARP address[] *is known only to TARP routers and terminals.*” See Ex. 1001, 11:14–28 (emphasis added), Fig. 2. Hence, in summary of the disclosed TARP process touted in the ’696 patent as agile routing, packets do not necessarily include the actual IP address of the final destination, but via processing (including decryption of the outer layer) of packet information and using LUTs along the way, *the TARP routers determine the final IP address.**

In other words, the Specification shows that contrary to Patent Owner’s related attempted distinction during the Oral Hearing of the instant case, like the Aventail SOCKS server system, “you need all the extra information that is at the [TARP router] to arrive at the end destination” (see Tr. 30:15–31:11), because without it (i.e. without information to decrypt the packet and send it to the next random hop and without the LUT processing,

etc.), the TARP router certainly could not send the packet to the next router or final destination. *See* Ex. 1001, 3:36–4:40, 10:23–63 (discussed above). In a similar vein, none of Patent Owner’s explanations or citations to the Specification describe how packets would arrive at a typical firewall or load balancer if they were not addressed to the particular destination, and the parties agree neither type of device (or others) impede the direct requirement.

Consequently, the record leaves vague and open the types of a VPN Patent Owner allegedly disclaimed during the reexamination prosecution of the related ’135 patent. Even though the *Cisco* District Court determined Patent Owner disclaimed indirect VPNs for purposes of that litigation, for the reasons explained above, the interpretation of “direct” on this record includes layers of ambiguity. For example, does “direct” require “direct addressability” as Patent Owner contended during at least two IPR oral hearings, but does not contend in any briefing here and did not contend clearly in any cited prosecution of this or related patents? If so, what does “direct addressability” mean? Does “direct” preclude any intervening device that does more than “relay” the data as the prosecution history arguments may or may not imply? If so, how does “direct” preclude an intervening device that provides more than a little processing (i.e., load balancing, decryption, and/or subsequent re-encryption of outer layers in a TARP device) prior to relaying or forwarding packets to their final destination? In other words, how much processing does “direct” allow before the packet is deemed to “stop” at the device so as to impede the alleged “direct” requirement? Does “direct” require all of the stated attributes? For

example, does “direct” require “direct addressability,” and does that require the real IP address of the target itself to be in the packet somewhere?

As explained above, the disclosed TARP embodiments relay packets, and the packets necessarily “stop and start” at each router (at least temporarily) so that the routers can decrypt the packets to determine the next hop in the series, including the final destination. At the *Cisco* jury trial, the court determined Apple’s FaceTime “relay server” does not impede direct traffic. *See* 925 F. Supp.2d at 830. But in that case, VirnetX agreed that Apple’s FaceTime “relay server” did not infringe its related claims, and the record here is devoid of a clear explanation as to why the disclosed TARP routers and Apple’s “relay server” do not impede direct addressability, but somehow, Aventail’s SOCKs server does. *See id.* Similar remarks apply to typical firewalls, other servers, and load balancers, which do not impede the direct requirement according to Patent Owner.

In District Court, multiple prosecution history arguments are not fatal to a disclaimer, as the District Court determined in the *Cisco* litigation (*see* Ex. 2004, 6–8), but on this record, layers of ambiguity remain, as explained above. In sum, Patent Owner originally contended in cited District Court litigation that the construction of VPN does not require a direct link and contended it did not make a clear disclaimer during prosecution. Patent Owner argues the exact opposite now. Stated differently, Patent Owner attempts to turn prosecution history arguments that Aventail does not disclose any type of VPN into an argument that it disclaimed VPNs without direct links, contradicting itself. *Compare* Ex. 2011, 5 (“Aventail has not been shown to disclose the VPN claimed in Claim 1 of the ’135 Patent for at least three reasons”), *with* Ex. 2004, “VirnetX argues that its statements

during prosecution are not a clear disavowal”). Also, during the cited reexamination of the ’135 patent, the examiner initially found that Aventail anticipates similar claims in the ’135 patent, and the parties simply appeared to have agreed on a direct requirement during litigation in *Cisco*.

In the Institution Decision, we specifically noted that the direct requirement begged for a clear explanation, and Patent Owner does not provide one in its briefing (or otherwise). See Inst. Dec. 21 (“If a direct connection requirement becomes a dispositive issue with respect to Aventail, Patent Owner will have an opportunity to clarify the record in its Patent Owner Response and point out how the Specification limits a VPN link to a direct link (and also what the term “direct” means)”). The “doctrine [of prosecution history (file wrapper) estoppel] is an equitable tool for determining the scope of patent claims.” *Builders Concrete, Inc. v. Bremerton Concrete Prods. Co.*, 757 F.2d 255, 258 (Fed. Cir.1985). On this record and in this proceeding, faced with shifting and unclear arguments by Patent Owner, the *public* should not be bound, via a doctrine grounded in *equity*, to a construction of unknown breadth under a broadest reasonable construction, which may or may not include “direct addressability.” See *Tempo Lighting*, 742 F.3d at 978 (“the PTO is under no obligation to accept a claim construction proffered as a prosecution history disclaimer, which generally only binds the patent owner.”). That the District Court bound Patent Owner to one of its reexamination arguments that became an issue during litigation in that case should not bind the public on a different record here, especially where the experts testified in *Cisco* about what “direct” means, and the parties agreed to be bound by “direct” at least during the latter stages of the litigation. See *Cisco*, 767 F.3d at 1319–20 (noting jury

had substantial evidence via experts to support infringement by Apple's FaceTime because NAT routers "do not impede direct communication," "VirnetX presented evidence that NATs operate like routers or firewalls," and Apple's expert "admitted that the connection does not stop at the NAT routers"))).

Here, the parties do not provide similar sufficient evidence as to what direct means, and if anything, Patent Owner clouds the record, especially in the context of Aventail, and in other contexts, such as Patent Owner's citations indicating that some prior art crowd proxies and intermediate servers (but not proxy servers) may impede a direct connection somehow (without explaining how). See PO Resp. 6–7 (quoting Ex. 1001, 1:65–2:8, citing 2:44–48, Fig. 1). The *Cisco* litigation, prosecution history, briefing, oral arguments, and record as a whole, fail to clarify what "direct" or "direct addressability" means, in the context of the '696 patent's disclosed TARP routers, which do not appear to be disclaimed embodiments. After considering the prosecution history in light of the arguments presented, the Specification, and other record evidence, Patent Owner fails to support its alleged disavowal or disclaimer in a fashion that presents a "clear," "exacting," "unmistakable," and precise, see *id.*, line of demarcation between what it allegedly disclaimed (during prosecution) and its preferred embodiments that include TARP routers, load balancers, and other intervening devices or servers. See *GE Lighting Sols., LLC v. AgiLight, Inc.*, 750 F.3d 1304, 1309 (Fed. Cir. 2014) ("The standards for finding lexicography and disavowal are exacting."); *Omega Eng'g, Inc. v. Raytek Corp.*, 334 F.3d 1314, 1325–26 (Fed. Cir. 2003) ("[F]or prosecution disclaimer to attach, our precedent requires that the alleged disavowing

actions or statements made during prosecution be both clear and unmistakable.”); *Paulsen*, 30 F.3d at 1480.¹⁰

Turning to another VPN link issue, encryption, *Cisco* is instructive, and the patents at issue in *Cisco* have common descriptions to the ’696 patent. *See Cisco*, 767 F.3d at 1313. In *Cisco*, the court found that “[b]oth the claims and the specification of the ’151 patent make clear that encryption is a narrower, more specific requirement than security.” *Id.* at 1323 (citing a passage in the ’151 patent at 1:49–50 (“Data security is usually tackled using some form of data encryption.”)). This passage, relied upon by the Federal Circuit in its construction, also appears in the ’696 patent. Ex. 1001, 1:57–58; *see supra* note 1 (the ’696 patent and ’151 patent are related).

In the ’237 FWD, the Board noted the Federal Circuit’s construction of “secure communications link” in *Cisco* and construed the term as meaning “a transmission path that restricts access to data, addresses, or other information on the path, generally using obfuscation methods to hide information on the path, including, but not limited to, one or more of anonymity, authentication, or encryption.” ’237 FWD 8. The Board also interpreted “virtual private network communication link” to mean “a secure communication link that includes a portion of a public network.” *Id.* at 10;

¹⁰ Our reviewing court in the *Cisco* case indicates that “direct addressability” does not preclude “routers, firewalls, and similar servers.” *See Cisco* 767 F.3d. 1320 (citing 925 F. Supp.2d at 831). This finding supports our findings, but unfortunately does not address the question here of why Aventail’s SOCK’s server allegedly impedes alleged “direct” (or “direct addressability”) requirement(s), but somehow the ’696 patent’s disclosed TARP router, load balancer, and other embodiments do not.

Pet. 16 (citing '237 FWD 10; Ex. 1001, 6:63–65, 52:19–20, Fig. 33; Ex. 1005 ¶ 74).

In making the determination in the '237 FWD, the Board noted that *Cisco* determined “encryption is a narrower, more specific requirement than security,” based on the same disclosure here as the patent at issue in *Cisco* that “[d]ata security is usually tackled using some form of data encryption.” See '237 FWD 6 (quoting *Cisco*, 767 F.3d at 1323 and patents under challenge). Therefore, under a broadest reasonable interpretation, as the Board determined in that related case (and others), “secure communications link” may include, *inter alia*, encryption and/or other forms of security, including anonymity.¹¹

Notwithstanding its claim construction position, however, Petitioner contends using encryption would have been obvious, and Patent Owner contends anonymity is not enough to make a link secure. See Pet. 33 (“Although Petitioner maintains, and the Board has confirmed, that the broadest reasonable interpretation of ‘virtual private network communication link’ does not require encryption, to limit the impact from any potential disputes or related legal proceedings over the construction of this term in the context of the '696 patent, this petition demonstrates that Aventail renders obvious an encrypted “virtual private network communication link.”); PO

¹¹ In the *Cisco* litigation, Patent Owner argued a secure link does not require anonymity. *Cisco*, 767 F.3d at 1318. (“VirnetX also argues that the specification teaches that different users have “different needs” such that some users need data security while, in other cases, “it may be desired” to also have anonymity.”). Applying the district court claim construction standard, the *Cisco* disagreed. See *id.* at 1317–19 (determining anonymity is required).

Resp. (“anonymity alone does not result in a VPN communication link”). Accordingly, for purposes of this proceeding, where Petitioner implies that encryption as a claim construction requirement is not outcome determinative in this case, and Patent Owner’s claim construction requires encryption only on insecure paths (PO Resp. 3), “secure communication link” includes encryption along insecure paths, but does not require encryption on secure paths (such as on physically secure paths as set forth in *Cisco* and as Patent Owner contends as noted above).

Based on the foregoing, for purposes of this proceeding and based on the respective positions of the parties in light of the Specification and other record evidence, a VPN link means “a secure communication link that includes a portion of a public network, with encryption employed on insecure portions of the network.” This construction, which requires encryption, is slightly narrower than, but consistent with, the Board’s construction applied in the ’237 FWD (discussed above as part of Petitioner’s showing (*see* Pet. 15–16)), and we adopt the reasons and analysis set forth therein to the extent required to support the broadest reasonable construction of the phrase. *See* ’237 FWD 5–10 (listing anonymity, encryption, and other obfuscation methods).

B. Level of Ordinary Skill in the Art

The parties do not appear to disagree materially over the level of ordinary skill in the art. For example, Petitioner’s expert, Dr. Tamassia, states that a person of ordinary skill in the art would have “a good working knowledge of networking protocols, including those employing security techniques, as well as cryptographic methods and computer systems that support these protocols and techniques.” Ex. 1005 ¶ 81; *see* Pet. 10. Such a

person would have gained this knowledge “either through several years of practical working experience or through education and training” or some combination of both. Ex. 1005 ¶ 81. Dr. Monroe states that “a person of ordinary skill in the art [at the relevant time] would have had a master’s degree in computer science or computer engineering, as well as two years of experience in computer networking with some accompanying exposure to network security.” Ex. 2016 ¶ 13.

Dr. Monroe’s definition requires a particular educational background, but appears to result in the same level of expertise as Petitioner’s definition. *See id.* Based on the testimony of the parties’ experts as well as a review of the ’705 patent and the prior art involved in this proceeding, a person of ordinary skill in the art would have a master’s degree in computer science or computer engineering and approximately two years of experience in computer networking and computer security—or the equivalent, obtained through practical work experience and training.

*C. Prior Art Printed Publication Status of
Aventail, RFC 2401, and RFC 2543*

Petitioner persuasively shows “the effective filing date of the ’696 patent claims is no earlier than February 15, 2000,” which Patent Owner does not challenge. *See* Pet. 10; PO Resp. 36, 43. Patent Owner asserts that Petitioner fails to provide evidence to establish that Aventail Administrator Guide (Ex. 1009), RFC 2401 (Ex. 1008), and RFC 2543 (Ex. 1013) would have been sufficiently accessible to the public interested in the art, on January 31, 1999, in November 1998, and in March 1999, the dates associated with, or recited on, pages of the respective references. *See* PO Resp. 36, 43. According to Patent Owner, Petitioner fails to show that

Aventail, RFC 2401, and RFC 2543 constitute prior art printed publications; therefore, they cannot be used to show obviousness according. *See id.* at 35–36 (citing 35 U.S.C. § 311(b)). The determination of whether a given reference qualifies as a prior art “printed publication” involves a case-by-case inquiry into the facts and circumstances surrounding the reference’s disclosure to members of the public. *In re Klopfenstein*, 380 F.3d 1345, 1350 (Fed. Cir. 2004).

1. Aventail

The Aventail manuals include Aventail Connect v3.01/v2.51 Administrator’s Guide (Ex. 1009); Aventail Connect v3.01/v2.51 User’s Guide (1996–1999) (Exhibit 1010); and Aventail ExtraNet Center v3.0 Administrator’s Guide (Exhibit 1011). Patent Owner challenges the public availability of “Aventail v3.01 (the version of Aventail Connect corresponding to Ex. 1009).” PO Resp. 39; *see also id.* at 37 (the AEC v3.0 product was distributed along with a copy of Aventail Connect v3.01/2.51 Administrator’s Guide, which is *Aventail*.” In general, “Aventail” or the “Aventail manuals” herein refers to all three manuals (even though the parties sometimes refer to “Aventail” as one manual (Exhibit 1009). *See, e.g.*, PO Resp. 37; Pet. 18–19.

Petitioner asserts the Aventail manuals are prior art under 35 U.S.C. § 102(b). *See* Pet. 18–19 (“a printed publication . . . distributed to the public without restriction no later than January 31, 1999”). The Petition cites the declarations of James Chester (“Chester Declaration,” Ex. 1022), Christopher Hopen (“Hopen Declaration(s),” Exs. 1023 and 1058), and Michael Fratto (“Fratto Declaration,” Ex. 1043), to support its allegation that Aventail “was distributed to the public without restriction no later than

January 31, 1999.” Pet. 17–19. It also cites deposition testimony. *See id.* (citing Ex. 1057 Ex. 1057, 79:25–80:9, 100:2-104:7 (“Mr. Hopen testifying at trial that the Aventail documents were publicly available”); Ex. 1059, 20–32 (jury trial transcript including excerpts from Mr. Hopen’s deposition)).

The Aventail Administrator Guide is a colored brochure listing products and bearing a 1996–1999 copyright notice by Aventail Corporation, a website <http://www.aventail.com>, and the statement “[p]rinted in the United States of America.” Ex. 1009, i. The Aventail Administrator Guide bears other indicia showing it is a product manual to be distributed with a commercial product. For example, it seeks customer feedback: “*please e-mail comments to **support@aventail.com**. Your input is appreciated.*” Ex. 1009, 6. It provides contact information for “Aventail Technical Support.” *Id.* at 5. It lists Aventail protected trademarks and copyrights, the Aventail mailing and email addresses, and bears color indicia of the front of the brochure, all further evidencing that the Aventail Administrator Guide is the kind of document expected to be widely disseminated. *Id.* at Cover, i. In addition, Petitioner asserts that the effective filing date for the ’696 patent is no earlier than February 15, 2000. Pet. 10. Furthermore, the Aventail documents cross-reference the products or brochures of each other as system components, further evidencing an intent to distribute, such that an interested artisan of ordinary skill would have been led to brochures about the system products. *See, e.g.*, Ex. 1010, 5 (referring user’s to the “Administrator’s Guide” (Ex. 1009)); Ex. 1005 ¶ 116 (discussing interrelationship).

Petitioner contends the Aventail Administrator Guide was shipped to customers with software products between “December 1998 and January of

1999.” Pet. 19 (citing Ex. 1022; Ex. 1023; Ex. 1058 ¶¶ 13–16; Ex. 1059 at 20–32).¹² Mr. Hopen, testifies that as a former Aventail employee, he was involved in the design, development, and distribution of Aventail products, and that an estimated “thousands of copies” of the software products and manuals were distributed during the first six months of 1999. Ex. 1058 ¶¶ 4, 14–16. Mr. Chester, formerly of IBM, testifies that he received the relevant Aventail products and brochures no later than the end of December 1998, and subsequently distributed the documents with the relevant products (“AEC v3.0”) to customers and IBM employees in mid-January of 1999. See Pet. 19 (citing Ex. 1022).

Patent Owner argues the Hopen, Chester, and Fratto Declarations do not prove Aventail was a printed publication publicly available as of January 31, 1999. PO Resp. 47–51. Patent Owner contends that Mr. Hopen, Mr. Chester, and Mr. Fratto provide uncorroborated testimony. *Id.* at 48 (citing *Typeright Keyboard Corp. v. Microsoft Corp.*, 374 F.3d 1151, 1158–60 (Fed. Cir. 2004); *Finnigan Corp. v. ITC*, 180 F.3d 1354, 366 (Fed. Cir. 1999)). Patent Owner also contends Mr. Fratto is biased against Patent Owner. See PO Resp. 40–41.

Patent Owner acknowledges that Mr. Hopen states in the Hopen Declaration that the AEC v3.0 product was distributed along with a copy of Aventail Connect v3.01/2.51 Administrator’s Guide (Ex. 1009) “no later than January of 1999.” See PO Resp. 37–38 (quoting Ex. 1023 ¶ 14, citing ¶¶ 13–15). Although Patent Owner also acknowledges the Hopen

¹² The two Hopen Declarations (Ex. 1023 and 1058) originally were filed in separate reexamination proceedings challenging related VirnetX patents. The two declarations appear to be materially the same.

Declaration testimony that “‘thousands of copies of’ Aventail Connect v3.01 were distributed during the first six months of 1999,” Patent Owner contends “Mr. Hopen provides no evidence of how many copies were distributed in January of 1999—the date alleged by Petitioner as the latest publication date of Aventail.” *Id.* at 38 (citing Pet. 18; Ex. 1023 ¶¶ 9, 16). Patent Owner also argues the Fratto and Chester Declarations do not corroborate Mr. Hopen’s testimony that “‘thousands of’ copies of Aventail were distributed.” *Id.* at 50. Patent Owner contends that the Declarations fail to show how much of the distribution occurred in January of 1999, the date alleged by Petitioner as the publication date of Aventail. *See id.* at 39.

Patent Owner’s arguments do not rebut Petitioner’s showing. Mr. Hopen testifies he was involved in the “design, development and distribution of all of Aventail’s network security products.” Ex. 1023 ¶ 4. Mr. Hopen also generally testifies that “Aventail included printed manuals with the software packages that it distributed.” *Id.* ¶ 8. Mr. Hopen testifies to an initial release of the “AEC” product as version 3.0, or AEC v3.0, which included version 3.01/2.51 of Aventail Connect and version 3.0 of the Aventail Extranet Server. *Id.* ¶ 13. He testifies that the AEC v3.0 product included three software components. *Id.* ¶ 11. He testifies that Aventail announced a release of AEC in an October 12, 1998 press release. *Id.* ¶ 10 (attaching Ex. D to Ex. 1023). In addition, the testimony shows Aventail Connect v3.01/2.51 (i.e., Ex. 1009, Ex. E of Ex. 1023) and Aventail Extranet Center v3.01 Administrator’s Guide (i.e., Ex. 1011, Ex. F of Ex. 1023) were distributed with the software, and the software product was “publicly distributed . . . no later than January of 1999” (*see id.* ¶¶ 8, 14–16), with

thousands of copies distributed “during the first six months of 1999” (*id.* ¶ 16).

We find that the testimony of Mr. Hopen shows that at least some copies of Exhibits 1009 and 1011 were distributed in January of 1999 through February 15, 1999. We also find that the October 8, 1998 press release (Ex. H of Ex. 1023) coupled with the testimony regarding actual distribution during January of 1999, shows that persons interested in the AEC software product including AEC v3.0, would have had access to its associated manuals (i.e., at least Exhibits 1009 and 1011) such that they were publically available prior to February 15, 1999.

Mr. Fratto testifies as “presently an Editor of the Network Computing magazine and website.” Ex. 1043 ¶ 2. Mr. Fratto testifies that between 1997 and 1999 he reviewed and published articles “on a number of VPN products distributed by Aventail, Inc.” *Id.* ¶ 6. He describes “Aventail Extranet Center (‘AEC’), which included client software called ‘Aventail Connect’ and server software called ‘Aventail Extranet Server.’” *See id.* ¶¶ 6–14 (citing articles attached to his declaration). Mr. Fratto also testifies that he received a copy of the “Aventail Connect v.3.01/2.51 Administrator’s Guide,” attached as Exhibit G to his declaration, which “was distributed with the AEC v3.0 product” in October of 1998. *Id.* ¶¶ 12, 14. A published article in October of 1998 corroborates his testimony about an announcement and release by Aventail Corp. of the Aventail Extranet Center 3.0 product. *Id.* ¶ 13 (citing Exhibit I to his declaration, a “Network World” article—*see* “Briefs”).

Patent Owner contends that Mr. Fratto is biased against patents generally and Patent Owner specifically. PO Resp. 40–41 (citing Exs.

2023–35). Some of the cited Exhibits confirm that Mr. Fratto commented unfavorably about certain perceived patent types and his role as a witness. Nevertheless, Mr. Fratto’s statements in the cited Exhibits do not extend to all patents, all cases, and the patent system in general. Any bias Mr. Fratto may have against what he characterized as “stupid, obvious” patents, or similar characterizations that Patent Owner relies upon, in social media or otherwise, does not relate to his testimony at issue here, which pertains to the public dissemination issue. *See* PO Resp. 51 (citing Ex. 2034; Ex. 2036, 86:1–87:21).

Further, the record corroborates Mr. Fratto’s testimony. *See, e.g.*, Ex. 1043 ¶ 13 (citing Exhibit I attached to Exhibit 1043, “Intranet Applications: Briefs,” *Network World*, 55 (October 19, 1998)). Mr. Hopen’s testimony corroborates it further, because the testimony by each shows that the relevant software products were shipped with at least one of the manuals at issue here (i.e., Ex. 1009) before the end of January 1999. *See* Ex. 1023 ¶¶ 8, 14–16; Ex. 1043 ¶¶ 13–14 (Mr. Fratto received Exhibit G with the AEC v3.0 product). They also each testify about, and provide attached evidence of, published press release announcements of the AEC product in October of 1998. Ex. 1023 ¶ 10 (Ex. D, Oct. 12, 1998 press release announcing “Aventail ExtraNet Center” software product); Ex. 1043 ¶ 13 (Ex. I, Oct. 19, 1998 *Network World* Brief announcing “the Aventail Extranet Center 3.0” software product release).

Mr. Chester’s testimony, discussed further below, similarly corroborates Mr. Fratto. For example, Mr. Chester similarly “recall[s] that Aventail announced its AEC v3.0 product in the fall of 1998, and began

distributing this product no later than mid-January 1999,” which IBM being the largest “user of Aventail products.” Ex. 1022 ¶ 15.

Mr. Chester also testifies as “a present[] CEO of . . . Assured Products Group,” a software development and consulting firm. Ex. 1022 ¶ 4. Mr. Chester worked for IBM between March 1992 and August 2002 evaluating network security products. *Id.* ¶ 5. Mr. Chester evaluated Aventail VPN products between 1996 and 2000. *Id.* ¶ 9. As just noted, Mr. Chester “recall[s] that Aventail announced its AEC v3.0 product in the fall of 1998, and began distributing this product no later than mid-January 1999.” *Id.* ¶ 15. Mr. Chester testifies that the AECv3.0 product included version 3.01/2.51 of the Aventail Connect software and version 3.0 of the Aventail Extranet Server. *Id.* ¶ 16. He testifies that he received “Exhibit C with the AEC v3.0 product” “no later than July 1998” and “Exhibit C is a copy of the Administrator’s Guide for Aventail Connect v.3,01/2.51”—i.e., Exhibit 1009. Ex. 1022 ¶¶ 16–17, pp. 97–98 (Exhibit C to the Chester Declaration, which corresponds to Exhibit 1009).

Patent Owner responds that “Petitioner mischaracterizes Mr. Chester’s testimony,” because “Mr. Chester says nothing about what he distributed ‘in mid-January of 1999.’” PO Resp. 39 (citing Pet. 19; Ex. 1022 ¶¶ 16–20.) This argument is not persuasive. As noted, Mr. Chester testifies he received the relevant product with the Administrator Guide (i.e. Ex. 1009) “no later than July 1998.” Ex. 1022 ¶¶ 16–17. He also testifies IBM “deployed VPN solutions based on this product to more than 20,000 IBM domestically by March 1998 and more that 65,000 IBM employees worldwide by July 1998.” *Id.* ¶ 19). “Like earlier Aventail products, we distributed copies of the AutoSOCKS Administrator’s Guide along [with] the other printed

materials that came with the [software] to IBM clients to whom we deployed VPN solutions, and to IBM employees using the Aventail Connect v.3.01/v2.51 client.” *Id.* ¶ 18. The thrust of the testimony shows at the least that artisans of ordinary skill readily would have had access to the relevant Aventail manuals and would have been interested in obtaining them for the purpose of running the software. Accordingly, as indicated above, Mr. Chester corroborates Mr. Fratto, and we do not discount Mr. Fratto’s testimony. *See* Pet. Reply 19 n.3 (alleging the “attacks against Mr. Fratto are irrelevant and unfounded”).

Furthermore, neither Mr. Hopen, Mr. Fratto, nor Mr. Chester have been shown to have any relationship or interest in the outcome of this proceeding. There is no evidence or even argument that Aventail Corporation, for whom Mr. Hopen worked, is a competitor to Patent Owner. Although both Mr. Fratto and Mr. Chester received compensation for their testimony, expert witnesses typically receive compensation, and nothing in the record indicates bias based on compensation. *See, e.g.*, Ex. 1022 ¶ 2; Ex. 1043 ¶ 5.

Although the testimony of the three witnesses is sufficient to establish the Aventail documentation is prior art, Petitioner offers additional evidence of corroboration submitted with the declarations, which Petitioner argues Patent Owner ignores. *See* Pet. Reply 19 (citing Ex. 1023, 7 (announcement), 10 (article), 94 (announcement), 293 (announcement), 295 (press release), 424 (article)). The cited exhibits do not relate directly to the Aventail client software or Aventail manuals, but constitute evidence that the Aventail Corporation was developing VPN security products in mid-1997 and late 1998. *See* Ex. 1023, 9 (“For secure remote-access needs,

Aventail Corporation’s Mobile VPN 2.0 and AutoSocks 2.1 comprise a virtual private network (VPN) software solution . . .”). This evidence ties into the timeline of Aventail Corporation’s VPN products introduced between 1996 and 2000, as Mr. Chester describes. *See* Ex. 1022 ¶¶ 9–13. Petitioner cites additional evidence, also related to Aventail Corporation products. *See* Pet. Reply 17 (citing Ex. 1057, 79:25–80:9, 83:10–84:16, 91:20–92:2, 100:2–104:7; Ex. 1059, 20–32); Pet 19 (similar citations and reliance).

The testimony at pages 100–104 of Mr. Hopen’s deposition (Exhibit 1057) describes Exhibit 9 of his deposition, Aventail Connect version 3.01/2.51 Administrator’s Guide (Ex. 1009 here), and correlates it with a discussion about an October 1998 date of a press release for the Extranet Center 3.0 product. *See* Ex. 1057, 100:2–104:4. The Hopen deposition testimony was taken in the district court litigation and was subject to cross-examination by Patent Owner. *See* Ex. 1057, 148:1–227:4 (examination by Patent Owner’s attorney Mr. Curry). The cross-examination, and the fact that the testimony is consistent with Mr. Hopen’s declaration, adds to the credibility of Mr. Hopen’s testimony.

Even if corroboration is required to show public availability, corroboration “does not require that every detail of the testimony be independently and conclusively supported by explicit disclosures in the pre-critical date documents or physical exhibits.” *Ohio Willow Wood Co. v. Alps S., LLC*, 735 F.3d 1333, 1348 (Fed. Cir. 2013). *Willow Wood* stated a “rule of reason” test in which “the totality of the evidence . . . including circumstantial evidence” is assessed “in order to ascertain whether the testimonial assertions are credible.” *Id.* “A given reference is ‘publicly

accessible’ upon a satisfactory showing that such document has been disseminated or otherwise made available to the extent that persons interested and ordinarily skilled in the subject matter or art exercising reasonable diligence, can locate it.” *SRI Int’l, Inc. v. Internet Sec. Sys., Inc.*, 511 F.3d 1186, 1194 (Fed. Cir. 2008) (quoting *Bruckelmyer v. Ground Heaters, Inc.*, 445 F.3d 1374, 1378 (Fed. Cir. 2006)).

The evidence as outlined above supports a finding that persons interested and ordinarily skilled in the subject matter of the manuals could have located them. The evidence shows that Aventail Corp. announced release of the products and they were disseminated with the manuals. In addition, two declarants had actual access to the Aventail Extranet Center v3.0 product, and its manuals, by January 1999. In the case of Mr. Fratto, as indicated above, between 1997 and 1999, he reviewed and published articles for his Network Computing magazine and website relating to “Aventail Connect” and “Aventail Extranet Center.” Ex. 1043 ¶¶ 2, 6. As also noted above, Mr. Fratto testified that the Aventail Extranet Center 3.0 product was distributed in the fall of 1998 and identified “Intranet Applications: Briefs,” Network World, 55 (October 19, 1998) (Exhibit I to Ex. 1043) as support. *Id.* ¶ 13. Mr. Fratto identified Exhibit G as a non-confidential copy of Aventail Extranet Center v3.01 (Ex. 1009) he received in April, 1999. *Id.* ¶ 14. Mr. Chester testifies generally that, while at IBM, “the Aventail products were distributed with installation disks and printed manuals.” Ex. 1022 ¶ 12. He specifically testifies about a press announcement about Aventail Corp. releasing the AEC v3.0 product, testifies about receiving the Administrator’s Guide for Aventail Connect v3.0/2.51 (Exhibit C to the declaration, Ex. 1009 here), “no later than July 1998,” and testifies that

Aventail Corp. “began distributing this product no later than mid-January of 1999,” which he knew about because “he was personally involved” at IBM with Aventail. *Id.* ¶¶ 15–17.

After listing Exhibits 1009–11, Dr. Tamassia states that the Aventail “documents cross-reference each other, which is logical as they are describing two components of a single system that are designed to work together (i.e., the Aventail Connect client running on the client computer, and the Aventail Extranet Server running on a server computer).” See Ex. 1005 ¶ 115 (listing documents), ¶ 116 (citing Ex. 1009, 3, 5, 6, 11, 14, 19, 36–40, 44, 46, 48, 50, 52, 55–57, 61–71, 76, 77, 79–83, 92–94, 96, 99, and 107–109); Pet. 20. As one cited example, Aventail (Ex. 1009, 14) refers to a CD that “contains the Administrator’s Guide and the User’s Guide” for help in executing Aventail Connect —i.e., the latter reasonably pointing to the availability of Exhibit 1010 (“Aventail Connect v3.01/v2.51 User’s Guide (1996–1999)”). Exhibit 1009 also states that “[f]or additional information on how to configure the Aventail ExtraNet Server product, consult the Aventail ExtraNet Server Administrator’s Guide [i.e., Ex. 1011].” Ex. 1009, 73.

Therefore, the record supports the unchallenged evidence of cross-referencing as to the inter-related products (Aventail Connect and the SOCKS server, ExtraNet, etc.) and the three manuals at issue, thereby supporting the finding that because at least Exhibits 1009 and 1011 were accessible and disseminated as discussed above, Exhibit 1010 also would have been accessible to persons interested in the subject matter of the Aventail v3.0 product. Furthermore, skilled artisans seeking Aventail v3.0 products would have sought out relevant and existing documentation for

using and/or acquiring the product. The record evidence shows that the testimony of Mr. Hopen, Mr. Fratto, and Mr. Chester is credible, and supports Petitioner's showing by a preponderance of the evidence that Exhibits 1009–11 of Aventail not only were publically available, but Exhibits 1009 and 1011 also were disseminated to persons of ordinary skill interested in computer networking and security as of January 1999.

Viewing the evidence as a whole, Petitioner has shown persuasively that Aventail was publicly available before February 15, 1999. Accordingly, we find that Petitioner has established, by a preponderance of the evidence, that the Aventail manuals, including Exhibits 1009–11 qualify as prior art printed publications under 35 U.S.C. § 102(b).

2. RFC 2401 and 2543

Petitioner asserts RFC 2401 and 2543 were available publically as prior art under 35 U.S.C. § 102(b). Pet. 27–28, 30–31(citing Ex. 1005 ¶ 126; Ex. 1008, 1). Patent Owner contends Petitioner's showing is not sufficient. PO Resp. 43–52. In our Decision to Institute, in addition to citing the Tamassia Declaration, we found that RFC 2401 and RFC 2543 each independently include indicia suggesting a reasonable likelihood that the documents were publically available. *See* Inst. Dec. 11–13.

RFC 2401 and RFC 2543 each include dates on each page, and the cover sheets bear the designations “Request for Comments” from the “Network Working Group,” discussing particular standardized security protocols for the Internet. Ex. 1008, 1; Ex. 1013, 1. Each document describes itself as a “document [that] specifies an Internet standards track protocol for the Internet community, and requests discussion and suggestions for improvements Distribution of this memo is unlimited.”

See Ex. 1008, 1; Ex. 1013, 1; Ex. 1005 ¶¶ 117–128 (discussing Request for Comment (“RFC”) publications)).

In support of Petitioner’s position, Dr. Tamassia testifies that RFCs are “prepared and distributed under a formalized publication process overseen by one of several Internet standards or governing bodies,” such as the IETF. Ex. 1005 ¶ 117. Dr. Tamassia also relies on an RFC publication that discusses the RFC development and publication process itself—RFC 2026, dated October 1996. *Id.* ¶¶ 118–124 (citing Ex. 1036, 21). Dr. Tamassia states that “[t]he publication date of each RFC is contained in the RFC, typically in the top right corner of the first page of the document” and “[t]his is the date it was released for public distribution on the Internet.” *Id.* ¶ 121 (citing Ex. 1036, 20). Dr. Tamassia quotes RFC 2026, which explains that anyone can obtain RFCs from “a number of Internet hosts,” making the “working document readily available to a wide audience, facilitating the process of review and revision.” Ex. 1005 ¶ 120 (quoting Ex. 1036, 8). Each RFC “is published as part of the ‘Request for Comments’ (RFC) document series. . . . RFCs can be obtained from a number of Internet hosts using . . . World Wide Web, and other Internet document retrieval systems.” *Id.* ¶ 118 (quoting Ex. 1036, 6, and testifying the RFC documents “are widely disseminated on the Internet”).

Patent Owner argues that Petitioner cannot rely on evidence it has proffered to support this finding. Patent Owner argues Dr. Tamassia’s testimony “does not constitute sufficient evidence” and “should not be accorded any weight” because Dr. Tamassia has not been established to have personal knowledge that RFC 2401 actually was released to the public in November 1998 nor has Dr. Tamassia “been established as someone familiar

with, let alone an expert in, the workings of the internet Engineering Task Force (IETF)—the body responsible for the RFCs.” PO Resp. 44–45.¹³ Patent Owner also contends that nothing shows that interested persons could have located the documents. See PO Resp. 50–51.

We find Dr. Tamassia’s testimony as to public accessibility of RFCs in general to be credible, especially given the independent support of RFC 2026 (Ex. 1036), the contents of which Patent Owner does not challenge. The contents of RFC 2401 and 2543 are consistent with the publication process described by RFC 2026 and Dr. Tamassia, including the requests for discussion and suggestions for improvements in each document, and the dates “November 1998” and “March 1999” respectively on the top right corner of the first page of each document. See Ex. 1008, 1; Ex. 1013, 1. The title itself on each document, “Request for Comments,” coupled with evidence in RFC 2026 that each RFC document was made widely available “from a number of Internet hosts,” constitutes sufficient evidence that RFC 2401 and 2543 each was intended for publication and would have been accessible to interested artisans seeking documents related to “Internet standards.” Ex. 1036, 6, 8, Ex. 1008, 1; Ex. 1013, 1; Ex. 1005 ¶¶ 187–89. In other words, these documents—each a request for suggestions and improvements for Internet standards and having no indication of being a mere draft or internal paper—are precisely the type of documents whose

¹³ Patent Owner also argues we should give Dr. Tamassia’s testimony on this issue no weight because the Petition does not cite to these paragraphs. PO Resp. 44 n.10. Patent Owner, itself, however, directed the Board’s attention to this testimony in its Preliminary Response (Paper 6, 27 n.6), and, thus, clearly has had adequate notice of its contents such that it may respond with no resulting prejudice.

main purpose is for public disclosure. The Tamassia Declaration specifically references RFC 2401 and RFC 2543, including their publication dates. *See, e.g.*, Ex. 1005 ¶¶ 118–124.

Petitioner provides additional documentary evidence, in the form of an August 16, 1999 magazine article (Ex. 1064, 9 (discussing RFC 2401 and IPsec protocols and stating “[a]ll of these documents are available on the IETF website”)), and an article from Network World magazine (dated March 15, 1999) (Ex. 1065), which sets forth an imperative statement: “See the IETF documents RFC 2401 . . . at www.ietf.org/rfc/rfc/rfc2411.text.” Ex. 1065, 3. Pet. 28 (citing Ex. 1064, 9; Ex. 1036, 5–6). Both of the magazine articles, Exhibits 1064 and 1065, further corroborate the indicia of availability on the face of RFC 2401, although they are not necessary to our finding of public accessibility.

Petitioner also points out that RFCs have been characterized as “written and circulated” by at least one District Court: “[M]uch of the development and technical management of the Internet has been by the consensus of Internet users. This is evidenced . . . by IETF and the more than 2000 RFC’s which have been written and circulated.” Paper 23, 13 n.5. (quoting *PGMedia, Inc. v. Network Sols., Inc.*, 51 F. Supp. 2d 389, 406 (S.D.N.Y. 1999)).

“A given reference is ‘publicly accessible’ upon a satisfactory showing that such document has been disseminated or otherwise made available to the extent that persons interested and ordinarily skilled in the subject matter or art exercising reasonable diligence, can locate it.” *SRI Int’l*, 511 F.3d at 1194 (quoting *Bruckelmyer*, 445 F.3d at 1378). Faced with record evidence as set forth in the Institution Decision, as part of routine

discovery, *see* 37 C.F.R. § 42.51(b)(1)(ii), Patent Owner had the opportunity to cross-examine Dr. Tamassia about the RFC documents and process of publication, but does not point us to any discussion of the issue.

We find that Petitioner has established, by a preponderance of the evidence, that RFC 2401(dated November 1998) and RFC 2543 (dated March 1999) were made available to persons of ordinary skill interested in computer networking and security sufficiently to be deemed “publicly accessible” at the relevant time. *See SRI Int’l*, 511 F.3d at 1194. Therefore, we determine RFC 2401 and RFC 2543 qualify as prior art printed publications respectively under 35 U.S.C. § 102(b) and 35 U.S.C. § 102(a).

*C. Analysis of Obviousness Grounds
Based on Aventail, RFC 2401, and RFC 2543*

1. Aventail

Aventail describes an Aventail Connect Client and Aventail ExtraNet Server application that allows work stations to connect securely with a private network through the Aventail ExtraNet Server. Ex. 1009, 1, 7, 9, 10, 72; Ex. 1011, 5, 9. Aventail describes its “Aventail ExtraNet Server” as a “VPN server.” *Id.* at 72 (Figure). “[B]ased on the security policy, the Aventail ExtraNet Server will proxy mobile user traffic into the private network but only to those resources allowed.” Ex. 1009, 73.

Aventail Connect resides between a WinSock application and an underlying TCP/IP stack. *Id.* at 9. WinSock, a Windows component, connects a Windows PC to the Internet using TCP/IP protocols. *Id.* at 7. Aventail Connect automatically routes traffic from WinSock to the Aventail ExtraNet Server, which Aventail refers to an extranet (SOCKS) server, such that workstations employ the SOCKS v5 protocol— an Internet Engineering

Task Force approved security protocol for securely traversing corporate firewalls. *Id.* at 6–7.¹⁴ In other words, Aventail Connect can be used in a network as a simple proxy client for managed outbound access and secure inbound access. *Id.* at 7. In addition, “Aventail Connect can establish an encrypted tunnel automatically.” *Id.* Aventail Connect also can compress or encrypt data before routing to the network. *Id.*

In operation, when a calling application, for example, an e-mail application or a browser, requests to communicate with an external network destination, Aventail Connect receives or intercepts it. *See* Ex. 1009, 8, 11. If the destination matches a redirection rule domain name or a proxy option is enabled, Aventail Connect creates a false DNS that later will be recognized during a connection request as one to be proxied to the Aventail ExtraNet Server. *See id.* at 10–12. “When the Aventail Connect . . . receives a connection request, it determines whether or not the connection needs to be redirected (to an Aventail ExtraNet Server) and/or encrypted” *Id.* at 10.

The system then performs a SOCKS TCP/IP handshake negotiation using the Aventail ExtraNet Server, and Aventail Connect notifies the calling application. *Id.* at 11–12. Ultimately, the calling application transmits and receives data using SOCKS. *Id.* The server may select an encryption module. *Id.* Aventail Connect decrypts any returned data. *Id.*

“Only traffic destined for the internal network [behind the Aventail ExtraNet Server in the VPN] is authenticated and encrypted; all other traffic

¹⁴ The parties, like Aventail, refer to the terms “SOCKS server” and “Aventail Extranet Server” interchangeably. *See id.* Prelim. Resp. n.2; Pet. 19.)).

passes through Aventail Connect unchanged.” *Id.* at 73. “[N]o direct network connections between the public LAN and the private LAN can be created *without being securely proxied through the Aventail ExtraNet Server.*” *Id.* at 72 (emphases added). “User authentication and encryption on the Aventail ExtraNet Server *require all users* to use Aventail Connect to authenticate and encrypt their sessions before any connection to the internal private network(s). For this example, the Aventail ExtraNet Server encrypts all sessions with SSL.” *Id.* at 73 (emphasis added).

Client work stations must have Aventail Connect to connect to the extranet:

Due to the routing restrictions described above, these clients will have no network access beyond the Aventail ExtraNet Server unless they are running Aventail Connect. Depending on the security policy and the Aventail ExtraNet Server configuration, Aventail Connect will automatically proxy their allowed application traffic into the private network. In this situation, Aventail Connect will forward traffic destined for the private internal network to the Aventail ExtraNet Server. Then, based on the security policy, the Aventail ExtraNet Server will proxy mobile user traffic into the private network but only to those resources allowed.

Id. at 72–73.

2. RFC 2401

RFC 2401 describes security services offered by IPsec protocols, including “access control, connectionless integrity, data origin authentication, [and] . . . confidentiality (encryption).” Ex. 1008, 3–4. According to RFC 2401, one of the IPsec goals is to provide “confidentiality (encryption).” *Id.* at 4. Using IPsec protocols

allows the user (or system administrator) to control the granularity at which a security service is offered. For example,

one can create a single encrypted tunnel to carry all the traffic between two security gateways or a separate encrypted tunnel can be created for each TCP connection between each pair of hosts communicating across these gateways.

Id. at 7.

3. RFC 2543

RFC 2543 describes a network-based secure video telephony architecture that supports both audio and video (i.e., multimedia). Ex. 1013, 1, 137. These multimedia telephony sessions may use end-to-end encryption. Ex. 1013, 54.

4. Claims 1 and 16—*Intercept a Request and Determine*

The preamble, “intercept,” and “determine” clauses of claim 1 follows:

1. A system for connecting a first network device and a second network device, the system including one or more servers configured to:

intercept, from the first network device, a request to look up an internet protocol (IP) address of the second network device based on a domain name associated with the second network device; [and]

determine, in response to the request, whether the second network device is available for a secure communications service; and

initiate a virtual private network [VPN] communication link

Ex. 1001, 56:7–18.

Claim 16 recites similar limitations. Petitioner initially persuasively characterizes Aventail as describing “highly analogous” systems and methods to those disclosed and claimed in the ’696 patent:

Both describe techniques whereby connection requests made by a client computer are intercepted and evaluated, and where, if a secure destination has been specified in the connection request, a VPN communication link is transparently established between the client computer and the host specified in the request, with network traffic between the client computer and secure network host being automatically encrypted/decrypted.

Pet. 32.

Petitioner contends the claimed server may be software and/or hardware according to the Specification and other persuasive evidence. *See* Pet. 12. Addressing the preamble and “one or more servers” of the claimed system, Petitioner contends Aventail discloses a scheme for creating secure connections between first (client) and second (host) network devices, using one or more servers, such as Aventail Connect and/or the Aventail Extranet Server. *Id.* at 34–36 (citing Ex. 1009, 5, 12, 77, 91–92).

Addressing the intercept clause of claim 1, Petitioner contends that Aventail employs an Aventail Connect software server running on a client device that looks up an IP address and intercepts the request from the client device. *See id.* at 35–36.¹⁵ Petitioner alternatively contends that an Aventail Extranet Server (also a SOCKs server) performs a name resolution of a connection request when it specifies a host name for a target device, thereby intercepting the request from the client device. *See* Pet. 37.

With respect to the latter alternative, according further to Petitioner:

¹⁵ Claim 15 depends from claim 1 and implies that a server need not be separate from the first network device of claim 1 (or client machine of Aventail). Claim 15 follows: “The system of claim 1, wherein the one or more servers configured to intercept the request are separate from the first network device.” Ex. 1001, 56:65–67. Claim 30 depends from claim 16 and recites a similar limitation in method format. *See id.* at 58:28–30.

Aventail . . . explains that the Aventail Connect client can be configured to route all connection requests to the Aventail Extranet server (“*one or more servers*”) for handling and resolution. Ex. 1009 at 61; *see also id.* at 12. The server in this configuration will receive the connection request containing either the IP address or the domain name of the destination computer from the client computer running Aventail Connect, and resolve these connection requests. Ex. 1009 at 12; *see also* Ex. 1009 at 61; Ex. 1005 at ¶¶ 196–199.

Id.

Aventail Connect consults a table of redirection results to determine whether the request corresponds to a target private device available via an Aventail ExtraNet Server. *See* Ex. 1009, 8–12. Aventail Connect also employs a proxy enabled option and proxies DNS requests to the ExtraNet Server, which resolves the target host name by returning an IP address. *See* Ex. 1009, 12, 61; Ex. 1005 ¶¶ 197–198 (testifying that enabling DNS Proxy functionality causes Aventail Connect to route all DNS requests that do not match a local domain string to the Aventail Extranet Server “for interception and resolution”); *see also* Ex. 1005 ¶ 189 (purported flow chart for Aventail’s system); Ex. 1009, 12 (“The false entry tells Aventail Connect that the DNS lookup must be proxied, and that it must send the fully qualified hostname to the SOCKS [Aventail ExtraNet] server with the SOCKS connection request.”).

As part of the determination step of claim 1, Dr. Tamassia testifies the Aventail Extranet Server “would be responsible for resolving the DNS request and returning an IP address to the client running Aventail Connect.” Ex. 1005 ¶ 199 (citing Ex. 1009, 11–12, 61–64). Petitioner explains that using either the proxy enable feature or redirection rules, the ExtraNet server

includes an option for encrypting all sessions or providing encryption for selected connections, and as part of a request, the DNS query results in the server returning the network address of the host to the client computer running Aventail Connect. *See* Pet. 23 (citing Ex. 1005 ¶¶ 209–210; Ex. 1009, 12). Dr. Tamassia supports Petitioner’s position. For example, he testifies “the Aventail Extranet Server will indicate to the Aventail Connect client whether an encrypted communication channel is supported (and required) for communication with the target device for which the Aventail Extranet Server will act as a proxy.” Ex. 1005 ¶ 217.

Further addressing the determination clause, Dr. Tamassia states

[a] person of ordinary skill would thus have understood this SOCKS-negotiation disclosure in Aventail to be explaining the Extranet server would determine whether the client device is allowed (or denied) access to the target device to which the client device has requested a connection. Ex. 1009 at 5, 12. This determination by the Extranet server is further described by the Aventail Extranet Center Administrator’s Guide which explains how the Extranet Server “determine[s] which people and groups can access what machines and services based on where they came from, the time of day, how they authenticated, and encryption strength, etc.” Ex. 1011 at 19.

Ex. 1005 ¶ 214 (citing and quoting Aventail manuals Exs. 1009, 1011).

Also, “[w]hen the SOCKS negotiation is completed, Aventail Connect notifies the application.” Ex. 1005 ¶ 224 (quoting Ex. 1009, 12, Step 2.c).

Dr. Tamassia additionally provides an example that shows “Aventail Connect communicates ‘directly’ with the Extranet Server” through another proxy gateway server, thereby showing all the ExtraNet servers can employ direct connections. *See* Ex. 1005 ¶ 236. He also testifies that the “Extranet Neighborhood” feature allows “a remote user who had successfully

established a VPN to a private network using Aventail Connect would be able to see and access all of the network resources that user was authorized to access, just as if the remote user had a local connection to the network.” *Id.* ¶¶ 238, 236–240 (citing Ex. 1009, 90–101).

Relying on one of the Monroe Declarations from a prior related proceeding, Patent Owner contends that Aventail does not disclose the claimed “determine” function of claim 1. *See* PO Resp. 21–27 (citing Ex. 2016). According to Patent Owner, Aventail Connect only encrypts traffic through to the SOCKS server and hence, at best *Aventail*’s disclosed system only determines whether to encrypt traffic to the SOCKS server but not to the remote host. PO Resp. 23 (citing Ex. 1009, 12, step 3; Ex. 2016 ¶ 35). Patent Owner also argues “[t]he redirection rules do not . . . imply that the remote host will require an encrypted connection because, as even Petitioner admits, *Aventail* does not teach an encrypted connection to the remote host.” *Id.* at 23 (citing Pet. 42; Ex. 2016 ¶ 36).

Patent Owner advances the same argument in its Preliminary Response and contends that the Petition did not address it. Prelim. Resp. 10; PO Resp. 24–25. According to Patent Owner, “the Institution Decision introduces positions not proffered by [Petitioner] and that are not supported by any evidence introduced in this proceeding.” PO Resp. 25. Patent Owner makes a similar argument regarding Petitioner’s showing with respect to “end-to-end” encryption as it relates to the determining step:

Indeed, the Petition’s reliance on RFC 2401 regarding claim 1 is limited to an alleged modification to “implement the Aventail system by providing end-to-end encryption” from a client computer to a remote host computer. (*See, e.g.*, Pet. at 42–46). Nowhere does the Petition present any position or rely on any

evidence that demonstrates the alleged combination of *Aventail* and RFC 2401 discloses, suggests, or renders obvious the “determining” limitations of claim 1 of the ’696 patent. (Ex. 1001 at 56:15-17; *see also* Pet. at 38–39.) Moreover, if all target devices would be secure under the position stated in the Decision, there would be no need to make a “determination” whether any target device requires encryption. Therefore, even under the Decision’s revised analysis, *Aventail* or *Aventail* in combination with RFC 2401 does not disclose the “determining” feature.

See id. at 25–26.

Patent Owner’s arguments are not persuasive. The arguments conflate whether a device uses encryption with the determine clause. Challenged claim 1 requires the server to be configured to “determine . . . whether the second network device is available for a *secure* communications service.” (Emphasis added). The ’696 patent is consistent with claim 1 and describes determining whether a device is available for a *secure* communication—not necessarily whether the determination involves making a specific decision about a device’s capability (in a private network) to include encryption. *See* Ex. 1001, 40:1–15; *accord* *VirnetX, Inc.*, 767 F.3d at 1323 (“But the patent consistently differentiates between ‘security’ and ‘encryption.’ Both the claims and the specification of the ’151 patent make clear that encryption is a narrower, more specific requirement than security.”).

Claim 1 does not necessarily require end-to-end encryption. Patent Owner’s proffered claim construction of a VPN link only requires encryption on insecure paths. *See supra* Section II.A; PO Resp. 3. Devices on secure paths behind a firewall on internal company networks are secure without using encryption. *See* *Cisco*, 767 F.3d at 1322 (finding that with respect to related *VirnetX* patent claims, “paths beyond the VPN server may

be rendered secure and anonymous by means of ‘physical security’ present in the private corporate networks connected to by VPN on Demand,” and that the district court’s claim construction of VPN “does not require that traffic on a secure path be encrypted. Rather, the construction only requires encryption of traffic ‘on insecure paths.’”).

In any event, assuming claim 1 may require end-to-end encryption, Petitioner contends that it would have been obvious in view of RFC 2401 to require all devices behind a firewall, such as the Aventail ExtraNet Server, to include encryption (i.e., end-to-end encryption) in order to further ensure data security and to allow the end device to decrypt the data. See Pet. 38–39, 42–46; Ex. 1005 ¶ 268 (“so as to keep information within user organizations secure”). In Aventail’s system, at least all originating users connected via proxy can be required to have encryption. “When the Aventail Connect . . . receives a connection request, it determines whether or not the connection needs to be redirected (to an Aventail ExtraNet Server) and/or encrypted” Ex. 1009, 10. “User authentication and encryption on the Aventail ExtraNet Server *require all users* to use Aventail Connect to authenticate and encrypt their sessions before any connection to the internal private network(s). For this example, the Aventail ExtraNet Server encrypts all sessions with SSL.” *Id.* at 73 (emphasis added).

Determining whether the connection request needs to be redirected and/or encrypted and returning a host address discloses or suggests determining if the host device is available for a secure connection, because otherwise the request and traffic would not need to be redirected. Ex. 1009, 10, 73; Pet. 38–39 (citing Ex. 1005 ¶¶ 200–218; Ex. 1009, 8–12, 73). In other words, requiring all users to authenticate and encrypt and/or

redirecting requests for encrypted connections teaches that employing the redirect rule or proxy enabled option to connect to a *private* network device (i.e., behind a firewall) constitutes a determination that the device listed within a private network is available for a secure connection. *See* Ex. 1009, 10, 73; Ex. 1005 ¶¶ 200–218, ¶¶ 267–80 (discussing combining IPsec via RFC 2401 with SOCKs servers, to provide end-to-end encryption to ensure security).

In a related argument, Patent Owner asserts that “determining whether a domain name matches a redirection rule for a destination is not the same as determining whether the remote host is available for an encrypted connection” because “the mere fact that a remote host accepts a *proxied connection* does not disclose or suggest that the remote host is one that is available for an *encrypted connection*.” PO Resp. 23–24. Again, the claims do not require determining if a device is available for an encrypted connection, and Aventail at least suggests that satisfying the proxy connection request or redirect rules constitutes a determination that the device listed within a private network is available for a secure connection. *See* Pet. 38–39.

As Petitioner similarly responds, Aventail’s system tracks the ’696 patent disclosure:

[C]onnections to internal private networks “**require all users** to use Aventail Connect to authenticate and encrypt their sessions **before any connection to the internal private network(s)**. For this example, the Aventail ExtraNet Server **encrypts all sessions with SSL**.” Ex. 1009, 73 (emphasis added); Dec. 20; Ex. 1005, ¶¶ 267–75. As explained in the Petition, this “*determin[ation]*” in Aventail thus occurs in virtually the same way described in the ’696 patent. Pet. 39 (citing Ex. 1001, 40:26–32, 41:9–16.).

Pet. Reply 9.

Determining if a connection to a target will be proxied via the Aventail ExtraNet Server using a redirection rule or the proxy configuration based on the target's domain name discloses, or at least suggests, determining that the target device also employs encryption, because, for example, all secure devices (i.e. satisfying proxy determination) would be encrypted under this modified option as suggested by RFC 2401. *See* Pet. 34, 38–39, 42–46. RFC 2401 suggests encrypting traffic end-to-end, including on relatively more secure or private parts of Aventail's network, with Aventail teaching the determination based on that encryption modification to its system (i.e., end-to-end encryption). *See* Pet. Reply 7–8 (“A determination by the modified Aventail system that the domain name requires a proxied connection *is* a determination whether the second network device is available for an encrypted connection, because a proxied connection would be encrypted end-to-end. Thus, Aventail in view of RFC 2401 teaches the claimed “*determination*” even under Patent Owner's view of the scope of its claims.”).

The Institution Decision does not go beyond Petitioner's mapping of the claims, as Petitioner argues. *See* Pet. Reply 10. The Institution Decision briefly describes some of Patent Owner's arguments and Petitioner's showing regarding end-to-end encryption. *See* Pet. Reply 10 (“Nowhere does the Board's Institution Decision go beyond this mapping—it simply rebuts, point by point, Patent Owner's arguments to the contrary. *See* Dec. 18–20. Nor is there any requirement, as Patent Owner seems to suggest, under 35 U.S.C. § 312(a)(3) or 37 C.F.R. § 42.104(b)(4) that the Petition must preemptively rebut every erroneous or irrelevant counterargument.”).

The Petition asserts that even if the claims require end-to-end encryption, determining if a device is listed in Aventail's table constitutes the claimed determining, with RFC 2401 providing a suggestion for end-to-end encryption:

Inclusion of the remote host in the redirection rule table therefore enables Aventail Connect to determine if the remote host will require an encrypted connection ("*is available for the secure communication[s] service*"). Ex. 1009 at 8–9, 11–12, 40; *see also* Ex. 1005 at ¶ 208. Aventail's disclosure of using a lookup table to check whether a host is one requiring communications to be proxied is very similar to the technique disclosed in the '696 patent for determining availability of a host for a secure communications service.

Pet. 39 (*citing* Ex. 1001 at 40:26–32, 41:9–16).

Contrary to Patent Owner's arguments, the Institution Decision does not rely on using RFC 2401 to make a determination—RFC 2401 suggests adding end-to-end encryption, as the Petition alleges. Furthermore, the Petition fairly indicates the materially same or similar determination process would be employed even without end-to-end encryption, because determining if a device is listed in an Aventail table or otherwise satisfies an Aventail security policy constitutes determining whether a host device would be available for security by virtue of its status as being listed in the table (or included as part of the proxy enablement feature) as a secure device (i.e., behind the SOCKS server, a firewall). *See* Pet. 38 ("Aventail discloses this determination being made using redirection rules based on the identity of the remote host specified in the connection request."); 43 ("This [alleged end-to-end] distinction, *even if established for the present claims*, would not have been a patentable distinction over Aventail." (Emphasis added)).

Similar to the disclosed invention, at other passages cited in the Petition, Aventail teaches using a security policy to determine which terminals in a private network are allowed (i.e., available for a secure connection):

*Depending on the security policy and the Aventail ExtraNet Server configuration, Aventail Connect will automatically proxy their *allowed* application traffic [from the public Internet] into the private network. In this situation Aventail connect will forward traffic destined for the *private internal network* to the Aventail ExtraNet Server. Then, *based on the security policy*, the Aventail ExtraNet Server will proxy mobile user traffic into the private network but only to those resources allowed.*

Ex. 1009, 72–73 (emphases added); Pet. 20–21 (citing Ex. Ex. 1009, 72–73), 38 (citing Ex. 1009, 73). As noted above in the claim construction of a VPN link, Patent Owner does not argue Aventail does not disclose anonymity or argue that a VPN link requires it. Nevertheless, to the extent required, Aventail’s security policy includes encrypting “traffic” to make it “*private and secure*,” thereby implying or suggesting anonymity (by encrypting whole packets of the “traffic”). See Ex. 1009, 7 (emphasis added) (“Encryption ensures that network traffic is private and secure.”); Ex. 1005 ¶ 168 (quoting passage).

With further respect to end-to-end encryption, at the source end, Aventail Connect encrypts and decrypts data after selecting an “encryption module” at the “SOCKS server.” See Ex. 1009, 12 (“Aventail Connect encrypts the data on its way to the server If data is being returned, Aventail Connect decrypts it so that the application sees cleartext data.”). This suggests that target devices behind the SOCKs (Aventail ExtraNet Server) in a corporate network, which also may use Aventail Connect, would

be able to perform similar encryption and decryption functions, rendering “end-to-end” encryption obvious. *See id.* at 73 (“Installing and using Aventail Connect for remote access purposes differs a bit from its installation and use within a corporate network.”). Otherwise, if the target devices do not perform encryption and decryption, the Aventail Extranet Server would be required to perform it for all target devices connected behind the firewall, necessarily causing an increased computational burden at the Aventail Extranet Server as the number of connected target devices increase. As just quoted, Aventail discloses different security options, i.e., depending on the selected “security policy,” thereby disclosing, or at least suggesting, keeping track of the policy options by requiring all users to have the necessary security. *See Ex. 1009, 73.*

Finally, faced with its concession that an accused VPN On Demand product did not literally infringe similar claims because the accused product did not perform “end-to-end” encryption, Patent Owner (VirnetX) informed the *Cisco* court that “the difference between secure communication via encryption and secure communication *in general is insubstantial.*” *Cisco*, 767 F.3d at 1322 (emphasis added).

5. Claims 1 and 16— Initiate a VPN Communication Link

Petitioner shows that Aventail, as combined with RFC 2401, renders obvious initiating a VPN link based on the determination discussed above, as set forth in claims 1 and 16. Pet. 39–41. Petitioner relies on basing the determination upon matching a domain name in the redirection rules table, which Aventail Connect flags to be proxied, and then setting up the “VPN,” pursuant to that and pursuant to authorization for an encrypted connection to

target hosts, for example, within the Extranet Explorer feature. *See* Pet. 39–40 (citing Ex. 1009, 11–12, 73, 94–105; Ex. 1005 ¶¶ 2008, 237–243).

Patent Owner argues that the Aventail ExtraNet Server “terminate[s]” the connection and, therefore, does not constitute a “direct” connection according to Patent Owner’s construction of the claimed VPN link recited in claims 1 and 16. *See* PO Resp. 29. Relying on the testimony of Dr. Monroe, Patent Owner contends that Aventail “distinguishes the SOCKS server from a regular firewall stating that ‘SOCKS is more than a standard security firewall.’” PO Resp. 29 (quoting Ex. 1009, 7; citing Ex. 2016 ¶ 39). Patent Owner also contends that “the traffic is addressed to the SOCKS server and ‘[t]he SOCKS server *then* sends the traffic to the Internet or the external network’ depending on the rules defined by an administrator for that incoming or outgoing traffic.” *Id.* at 29 (quoting Ex. 1009, 7).

Patent Owner’s arguments are not persuasive. Aventail describes its “Aventail ExtraNet Server” as a “VPN server,” as Petitioner contends. Ex. 1009, 72 (Figure); Pet. 39–40. Based on the claim construction above, a VPN link does not require a direct link. In addition, even if it does, Aventail also states that “no *direct* network connections between the public LAN and the private LAN can be created *without* being securely proxied through the Aventail ExtraNet Server.” Ex. 1009, 72 (emphases added). In other words, the Aventail system provides a direct secure connection via a secure VPN link, to target hosts in a private LAN behind the forwarding/proxy Aventail ExtraNet Server. This type of server operates much like the “VPN On Demand” server that Patent Owner argued infringed similar claims in *Cisco*. In *Cisco*, the court affirmed a finding of infringement even though the infringing product included intermediate “VPN servers, VPN authentication

servers, proxy servers, and firewalls *which regulate access to private resources* and prevent unauthorized users from breaching.” *Cisco*, 767 F.3d at 1320 (direct connection does not preclude “routers, firewalls, and similar servers”), 1321 (“VPN On Demand is intended to connect employ security measures including VPN serves, VPN authentication servers, proxy servers, and firewalls which regulate access to private resources and prevent unauthorized users from breaching”).¹⁶

The Aventail ExtraNet Server operates similarly to the “VPN server” in the VPN On Demand system at issue in *Cisco*, in other words, similar to a router, firewall, or gateway to a private corporate network, and thereby provides a direct connection under reasoning in *Cisco*. See 767 F.3d 1320–22; Ex. 1009, 72. Dr. Monroe does not address the cited teaching in Aventail that implies a direct connection to the private LAN “securely proxied through the Aventail ExtraNet Server.” See Ex. 1009, 72; Ex. 2016 ¶ 39. Dr. Monroe does not even address squarely whether a VPN link requires a direct connection. See Ex. 2016 ¶¶ 39–40 (addressing a different claim term from a related patent—i.e., the “claimed ‘encrypted communications channel between the client device and the target device,’ as recited in claim 1, or similarly recited in claim 21”).

Dr. Monroe does not define what “direct” means, though he ambiguously states that “the connection is terminated at the SOCKS server,

¹⁶ As noted above in the discussion of public availability, other witnesses independently describe Aventail as disclosing “VPN solutions.” For example, Mr. Chester testifies IMB “deployed VPN solutions based on this product to more than 20,000 IBM domestically by March 1998 and more that 65,000 IBM employees worldwide by July 1998.” Ex. 1022 ¶ 19.

which may create a new connection to the remote host.” Id. ¶ 39 (emphasis added). Dr. Monroe does not describe how the connection is “terminated,” and what that means, or under what conditions the server in Aventail “may create a new connection.” The testimony is conclusory and fails to provide a sufficient foundation to ascertain what is meant. As described above in the claim construction and background sections, the ’696 patent discloses TARP routers that relay packets only by processing (decrypting, encrypting, using a LUT, etc.) the packets, and then, based on such processing, the routers decide whether to send the packets to another router or the final destination. *Supra* Sections II.A, I.E. This shows that the disclosed TARP routers at least temporarily stop packets while “relaying” them, with each router otherwise including some type of algorithm to determine the address of the next router hop and/or the address of the final destination. *See id.* And *Cisco* states that mere address translation, or addressing communications to “a NAT, rather than to the receiving device,” does not impede a direct communication and allows “end-to-end communication between the two devices.” *Cisco*, 767 F.3d at 1319–20. The court added that this type of addressing does not defeat a finding of “direct addressability,” because “routers, firewalls, and similar servers . . . do not impeded ‘direct’ communication.” *Id.* at 20.

The court also noted that “Virnetx distinguished such proxy activities from the operation of NAT routers which—unlike proxy servers in the prior art—do not terminate the connection.” *Cisco*, 767 F.3d at 1324. On this record, the Aventail SOCKS server is similar to a “proxy server[] in the prior art.” *See id.* Patent Owner’s related argument that Aventail announces “SOCKS is more than a standard security firewall” relies on what amounts

to Aventail’s sales puffery or added aspects of SOCKS that do not impede a direct connection, and it does not explain what “more” the server does in a sufficient manner to rebut Petitioner’s showing that Aventail discloses a VPN or direct VPN.¹⁷ See PO Resp. 29 (quoting Ex. 1009, 6). As described above, the SOCKs server provides “more” in terms of performing proxy and other functions that do not preclude a direct connection.

Cisco describes servers that do not meet the direct requirement as follows: “The jury heard expert testimony that Kiuchi’s client-side and server-side proxies terminate the connection, process information, and *create a new connection*—actions that are not ‘direct’ within the meaning of the asserted claims.” *Id.* (emphasis added). In contrast, the evidence of record shows that Aventail itself indicates the connections are direct, acting like “a prior art proxy server” or corporate firewall. See *Cisco*, 767 F.3d at 1324; Ex. 1009, 72 (“no *direct* network connections between the public LAN and the private LAN can be created without being securely proxied through the Aventail ExtraNet Server” (emphasis added)); Pet. 26–27 (citing Ex. 1005 ¶¶ 228–233 and similar evidence about intermediate proxy servers being able to route a client through each server to the final destination), 50 (citing Ex. 1009 11, 12, 72–73); Pet. Reply 9–10 (summarizing evidence); Inst. Dec. 15 (quoting Ex. 1009, 72), 20–21 (quoting Ex. 1009, 72—i.e., discussing the “direct” passage in Aventail in light of *Cisco*).

¹⁷ Petitioner has the burden to show that Aventail discloses, or suggests, all of the claim limitations. But as discussed above in the claim construction section, Petitioner does not have a burden to show what “direct” means, because it is Patent Owner in this proceeding who asserts a disclaimer or disavowal of the plain meaning of a VPN link. See *supra* Section II.A (citing cases).

Dr. Monroe’s ambiguous and conclusory testimony stating “the connection is terminated at the SOCKs server, which *may* create a new connection,” fails to rebut this evidence. *See* Ex. 2016 ¶ 39. Dr. Monroe also testifies that the SOCKs server “path . . . is relayed through the SOCKs server, and is not a direct connection,” but relay of a “path” does not make much sense. *See id.* In any case, if anything, relaying packets constitutes a similar operation as routing. *See* Ex. 1005 ¶ 230 (describing SOCKs servers as “routing . . . communications”). “Aventail MultiProxy . . . allows Aventail Connect to travers multiple firewalls by making connections through successive proxy servers.” *Id.* (quoting Ex. 1009, 59); ¶¶ 231, 231–233 (reproducing figure from Ex. 1009, 60, which illustrates a direct connection through three proxy servers to a “final destination”). In addition, Dr. Monroe’s testimony assumes that the SOCKs server encrypts all the communications (*see* Ex. 2016 ¶ 39), but as discussed above, Petitioner’s showing includes showing the obviousness of providing encryption using end-to-end encryption performed at each end terminal (not an intermediate SOCKs terminal).

In the Institution Decision, citing *Cisco* several times (Inst. Dec. 2, 21–22), we informed the parties that “[i]f a direct connection requirement becomes a dispositive issue with respect to Aventail, Patent Owner will have an opportunity to clarify the record in its Patent Owner Response and point out how the Specification limits a VPN link to a direct link (and also what the term “direct” means).” Inst. Dec. 22. As discussed above, Patent Owner urges a prosecution disclaimer based on VPNs that are not “direct,” but does not clarify what “direct” means with sufficient precision. *See* Pet. Reply 10–11 (“neither Patent Owner nor its expert have attempted to explain what

is required by ‘direct[ness],’ . . . despite the Board’s repeated requests for a simple definition”). Pet. Reply 11 (citing IPR2015-00871, Paper 39, 27; PO Resp. 8–12, 27–28); *supra* Section II.A Claim Construction.

Petitioner also points out persuasively that even if a VPN link must be direct,

Patent Owner also ignores that Aventail discloses configurations in which client computers proxy their communications into a private network but communicate directly with target computers as though they were on the same private network. *See* Pet. 26–27, 40–41; Ex. 1009, 11–12, 94–105; Ex. 1005 ¶¶ 237–243. For example, Aventail shows remote client computers accessing private network resources via the “Secure Extranet Explorer” feature. Pet. 40. Using that functionality, users can access computers on the remote network by browsing a dynamic list of available resources “just as [the user] would” using the Windows network neighborhood locally. Ex. 1009, 91–92. Patent Owner, however, ignores this disclosure too.
Pet. Reply 11–12.

The record supports Petitioner, including the citations above discussing MultiProxy features. Ex. 1005 ¶¶ 231–234.

In summary, Petitioner persuasively shows the obviousness of claims 1 and 16, including using the VPN link and initiating a connection based on the determination. *See* Pet. 38–40. These limitations in large part build upon the showing of the interrelated determining clause, discussed above. Patent Owner does not present arguments specifically directed to these clauses, other than in relation to overlapping features contained in the determining clause or as discussed in related connections above. Based on the foregoing discussion, Petitioner shows by a preponderance of evidence that claims 1 and 16 would have been obvious.

7. *Claims 14 and 28*

Claim 14 depends from claim 1 and further recites “wherein the determination that the second network device is available for the secure communications service is a function of the result of a domain name lookup.” Claim 28 depends from claim 16 and recites a similar phrase in method format. Petitioner sets forth detailed showings and rationale to support its challenge that the combination of Aventail, RFC 2401, and 2543 would have rendered claims 14 and 16 obvious. *See* Pet. 50–51. The analysis of these claims track the showing above with respect to claims 1 and 14.

For example, Petitioner contends

Aventail shows that the domain name in a request is evaluated to see if it matches a redirection rule, which, if there is a match, will establish that the host specified in the connection request can establish a VPN with the client computer. Ex. 1009 at 11, 12. As part of the same process, the client computer will then be authenticated and a VPN will be established involving the client computer and the specified host computer (e.g., on the corporate network).

Pet. 50 (citing Ex. 1009 11, 12, 72–73).

In response, Patent Owner contends “determining whether a domain name in a DNS lookup request in Aventail’s step 1 matches a redirection rule for a destination (e.g., a remote host) is not the same as determining whether the remote host is available for an encrypted connection (allegedly the claimed secure communications service).” PO Resp. 31 (citing Ex. 2016 ¶¶ 36, 37). Patent Owner explains that “[t]he redirection rule only specifies the particular protocol for the traffic (i.e., TCP and/or UDP) that will be allowed to be routed to that destination.” *See id.* (citing Ex. 1009, 38–40;

Ex. 2016 ¶ 36). Patent Owner concludes that “the function of the result of the alleged domain name lookup in *Aventail* is a specification of the particular protocol for traffic,” and “not a determination that the second network device is available for an encrypted connection.” *Id.*

These arguments are similar to the arguments pertaining to claims 1 and 16, which are not persuasive, as noted above. Patent Owner essentially argues that having two or more results of the domain name look up function (e.g., specifying the type of protocol and determining if the request must be proxied) precludes the natural result of determining that a device to be proxied (or matching a redirection rule) necessarily means, or at least suggests, when combined with end-to-end encryption per RFC 2401’s teachings, determining the device is available for a secure connection. Similar to *Cisco*’s explanation with respect to the related ’135 patent (*supra* note 1), “the proxy identifies a request for ‘access to a secure site . . . by reference to an internal table of such sites.’ That is precisely how the VPN On Demand feature operates.” *Cisco*, 767 F.3d 1320 (quoting the ’135 patent). Like the VPN On Demand system accused in *Cisco*, similar to the explanation in connection with claim 1, *Aventail*’s system provides access to physically secure corporate networks by ensuring the connection satisfies its security policies, which at least suggests, in combination with RFC 2401, end-to-end encryption, via keeping track of the security policies employed, and thereby teaches the claimed determination step as a result of a domain name look up. *See* Pet. 50–51.

Based on the foregoing discussion, Petitioner shows by a preponderance of evidence that claims 14 and 28 would have been obvious.

8. Claims 11, 15 and 30— Based on Aventail and RFC 2401, or and Aventail, RFC 2401, and Yeager

Claim 11 depends from claim 1 and further specifies “the one or more servers are configured to intercept the request by receiving the request to determine whether the second network device is available for the secure communications service.” Apart from the server language, claim 11 tracks the language of claim 14 addressed above. And as discussed above, claim 1 already recites one or more servers.

Claim 15 also depends from claim 1 and further specifies “wherein the one or more servers configured to intercept the request are separate from the first network device.” Claim 30 depends from claim 16 and similarly further specifies “wherein intercepting the request occurs within another network device that is separate from the first network device.”

Similar to its showing with respect to claims 14 and 28, Petitioner sets forth detailed showings and rationale to support its challenge that the combination of Aventail and RFC 2401, or Aventail, RFC 2401, and Yeager would have rendered claims 11, 15, and 30 obvious. *See* Pet. 51–52, 56–59. For example, addressing claims 15 and 30 and relying on teachings in Aventail and partially its showing with respect to claim 1, Petitioner contends

Aventail explains that an Aventail Extranet server intercepts the domain lookup requests originating from a computer running Aventail Connect. *See* § IV.B.1.b) above. Aventail also shows that the Aventail Extranet server can reside on a different device separate from the computer running Aventail Connect (“*another device that is separate from the network device*”).
Pet. 51–52 (citing Ex. 1009, 72–73; Ex. 1005 ¶¶ 196–199).

To the extent Aventail and RFC 2401 do not satisfy claims 15 and 30, Petitioner relies on Yeager, providing several sufficient reasons “to move the secure connection functionality to an intermediate proxy,” including in order “to reduce[] the ‘huge administrative task’ involved with configuring each client computer.” Pet. 57 (citing Ex. 1066, 309–310; Ex. 1005 ¶¶ 287–89) (internal quotations omitted). Dr. Tamassia explains that Yeager teaches that using a separate proxy alleviates portability problems otherwise associated with “installing or re-installing software on possibly thousands of computers.” Ex. 1005 ¶ 287 (citing Ex. 1066, 307).

Addressing claim 11, Petitioner contends

Aventail explains that, depending on its configuration, both the Aventail Connect and the Aventail Extranet server can intercept requests to look up IP addresses to determine whether the request corresponds to a remote host (“second network device”) for which a link needs to be created to allow communications. See, e.g., Ex. 1009 at 11–12, 72–73; see also IV.B.1.b). Aventail in view of RFC 2401 thus would have rendered obvious claim 11.

Pet. 50.

In response with respect to claims 15 and 30, Patent Owner relies on its arguments with respect to claim 1. PO Resp. 35. With respect to claim 11, Patent Owner submits Petitioner’s showing is insufficient because

Petitioner fails to address the language of claim 11, which requires that “the one or more servers are configured to intercept the request by receiving the request to *determine whether the second network device is available for the secure communications service.*” (Ex. 1001 at 56:47-50 (emphasis added).) That is, even assuming *arguendo* that Aventail discloses to intercept a request “to determine whether the request corresponds to a remote host . . . for which a link needs to be created to allow communications,” as alleged by Petitioner (Pet. at 50), this does not even nominally address interception of a

request “to determine whether the second network device is available for the secure communications service,” as claimed (Ex. 1001 at 56:47–50).
PO Resp. 33–34.

Patent Owner’s arguments are not persuasive for reasons largely explained above in connection with claim 1. The arguments essentially repeat the claim language without explaining what is missing from Petitioner’s showing. Claim 11 recites “configured to intercept the request by receiving the request to determine whether the second network device is available for the secure communication service”—a recitation which rearranges the intercept clause of independent claim 1 and specifically requires the intercepting server to receive what it intercepts. The Aventail SOCKs server satisfies the subject matter of claim 11, for the reasons tracking those as set forth above in the discussion of claim 1. Petitioner similarly covers this analysis as summarized above, tracking the analysis of claim 1. See Pet. 49–50; Pet. Reply 13 (“Given that ‘*intercept[ing]* ... *a request*’ includes ‘*receiving*’ the request even under Patent Owner’s construction . . . , the only apparent additional requirement of claim 11 is that the request is intercepted ‘*to*’ perform the determination.”).

In other words, summarizing the explanation above, Aventail discloses or teaches the determine clause by using at least one server and setting up connections only to secure devices and keeping track of relative security policies via use of look up requests using the redirect rules table or proxy configuration, i.e., “*determine whether the second network device is available for the secure communications service.*” In addition, Petitioner persuasively shows that the claim construction of a server includes “hardware and/or software elements,” and Patent Owner does not dispute the

construction. *See* Pet. 12 (citations omitted). Software in Aventail, including Aventail Connect and/or the Aventail Extranet Server, performs the intercept and determination in a similar manner that the disclosed DNS proxy 2610 and/or DNS server 2609 performs it. *See* Pet. 32–34, 38–41 and discussion of claim 1 *supra* (addressing similar limitations in claim 1); 12 (citing Ex. 1001, 40:63–65; 50:5; Ex. 1005 ¶¶ 61–62); *Cisco*, 767 F.3d 1320 (“the proxy identifies a request for ‘access to a secure site . . . by reference to an internal table of such sites’”) (quoting the related ’135 patent, *see also supra* note 1).

Patent Owner’s related argument that Petitioner relies on the combination of Aventail and RFC 2401 without explaining how it employs RFC 2401 ignores that claim 11 depends from claim 1 and Petitioner relies on RFC 2401 to reach claim 1. *See id.* at 34.

Based on the foregoing discussion, Petitioner’s shows by a preponderance of evidence that claims 11, 15, and 30 would have been obvious.

8. Challenged Dependent Claims 2–10 and 17–25

Relying partially on the Tamassia Declaration, Petitioner sets forth detailed showings and rationale to support the following challenges: 1) the combination of Aventail and RFC 2401 would have rendered obvious dependent claims 4, 5, 9–10, 19, 20, 24, 25 (Pet. 46–50); and 2) the combination of Aventail, RFC 2401, and RFC 2543 would have rendered obvious dependent claims 2, 3, 6–8, 17, 18, and 21–23. *See* Pet. 52–56.

As Petitioner shows, these claims simply add known subject matter elements involving communication services, and specific data types, such as for example, one of video and audio data (claims 2, 3, 17, and 18), a

messaging service (claim 4, 19), an e-mail service (claim 5, 20), a telephony service (claim 6, 21), modulation (claim 7, 22), specific modulation types such as FDM, TDM, or CDMA (claim 8, 23), a mobile device (claim 9, 24), and a notebook computer (claim 10, 25). *See* Pet. 46–50 and 52–56 (addressing the limitations persuasively).

Rather than attempting to repeat explicitly Petitioner’s persuasive showing, we incorporate and adopt that showing, including supporting citations to the record, as our own and refer to it generally in summary as noted above. *See* Pet. 46–50 and 52–56. In summary, Petitioner shows that these added limitations amount to adding predictable types of data, data services, modulation schemes, and device types, all known features to artisans of ordinary skill as reflected by the record, and contemplated or suggested for known transmission purposes using Aventail’s system, in order to provide desired data types and transmissions modulated using known schemes and delivered using known devices in order to provide the predictable result of reliable communication services. *See id.*; *KSR Int’l Co. v. Teleflex Inc.*, 550 U.S. 398, 418 (2007) (citing *In re Kahn*, 441 F.3d 977, 988 (Fed. Cir. 2006)).

In response, Patent Owner relies on its arguments presented with respect to claims 1 and 16. *See* PO Resp. 33–35. At the start of trial, Patent Owner was informed “that any arguments for patentability not raised in the response will be deemed waived.” Paper 10, 3.

Based on the record as summarized above, Petitioner shows by a preponderance of evidence the following: 1) the combination of Aventail and RFC 2401 would have rendered obvious dependent claims 4, 5, 9–10, 19, 20, 24, 25 (Pet. 46–50); and 2) the combination of Aventail, RFC 2401,

and RFC 2543 would have rendered obvious dependent claims 2, 3, 6–8, 17, 18, and 21–23. *See* Pet. 52–56.

III. MOTION TO EXCLUDE

Patent Owner filed a Motion to Exclude Exhibits 1007, 1012, 1017, 1022, 1023, 1026–29, 1038–40, 1043, 1048, 1052, 1054, 1055, 1058, 1060, and 1063–65. Paper 20, 1–2. Petitioner filed an Opposition to the Motion to Exclude (Paper 23), and Patent Owner filed a Reply in Support of the Motion to Exclude. Paper 24. As movant, Patent Owner has the burden of proof to establish that it is entitled to the requested relief. *See* 37 C.F.R. § 42.20(c). For the reasons stated below, Patent Owner’s Motion to Exclude is denied or dismissed as moot.

A. Exhibits 1022, 1023, 1043, and 1058

Patent Owner seeks to exclude Exhibits 1022, 1023, 1043, and 1058 (collectively, the “Aventail declaration testimony”) as inadmissible hearsay. Paper 20, 2. As detailed above, Exhibit 1022 is the Chester Declaration, Exhibits 1023 and 1058 are Hopen Declarations, and Exhibit 1043 is the Fratto Declaration. The Petition relies on these Exhibits (and others) to establish that Aventail is prior art. *See* Pet. 18–20.

Although the Aventail declaration testimony originally was filed in other proceedings and not created specifically for this proceeding, the main distinction between it and the expert declaration testimony of Dr. Tamassia is the caption. That difference is artificial because all of the declarations were filed in this proceeding, as if they were prepared for this matter. Patent Owner chose not to seek the opportunity to cross examine the declaration testimony because, according to Patent Owner, “cross-examination . . . was not provided as routine discovery.” Paper 24, 2–3; *see* 37 C.F.R.

§ 42.51(b)(ii). This contention is not persuasive, because Patent Owner could have sought to cross-examine these declarants, and had Petitioner not provided them, then could have sought to exclude their testimony.

Even if considered hearsay, Federal Rule of Evidence 807 provides a “residual exception” to the hearsay rule, which may apply even if no specific exception of Federal Rule of Evidence 803 applies. We determine that the exception applies here. To fall under this exception, the statement must satisfy the following requirements: 1) have equivalent circumstantial guarantees of trustworthiness; 2) be offered as evidence of a material fact; 3) be more probative on the point for which it is offered than any other evidence that the proponent can obtain through reasonable efforts; and 4) be in the interests of justice to admit. Fed. R. Evid. 807. The residual exception to the hearsay rule is to be reserved for “exceptional cases,” and is not “a broad license on trial judges to admit hearsay statements that do not fall within one of the other exceptions.” *Conoco Inc. v. Dep’t of Energy*, 99 F.3d 387, 392 (Fed. Cir. 1996), as amended on rehearing in part (Jan. 2, 1997) (internal quotations omitted). Trial courts are accorded wide discretion in applying the residual hearsay exception. *Doe v. United States*, 976 F.2d 1071, 1076–77 (7th Cir. 1992), *cert. denied* 510 U.S. 812 (1993); *United States v. North*, 910 F.2d 843, 909 (D.C. Cir. 1990), *cert. denied* 500 U.S. 941 (1991).

Petitioner responded to the objections by relying on Federal Rule of Evidence 807. Paper 23, 1–9. Petitioner analyzes each factor in detail. *Id.* We agree with and adopt Petitioner’s analysis. For example, we agree with Petitioner that the Aventail sworn declaration testimony has the same circumstantial guarantees of trustworthiness as those declarations actually

created for this proceeding. *See* Paper 23, 3–7. The vast majority of testimony in *inter partes* reviews is admitted in paper form, as a declaration, instead of as live witness testimony. Thus, whether or not testimony is specifically created for a specific IPR or is created for another proceeding, if the declaration is sworn testimony and the witness is available for cross-examination, the testimony bears the same guarantees of trustworthiness. *See also* Fed. R. Evid. 804(b)(1) (exception against the rule against hearsay for former testimony that “was given as a witness at a trial, hearing, or lawful deposition” and “is now offered against a party who an opportunity and similar motive to develop it by direct, cross-, or redirect examination”).

In addition, Exhibit 1057 is the deposition transcript of Mr. Hopen from a district court proceeding. Exhibit 1059 is a portion of deposition testimony read into evidence in the above-mentioned district court trial. As Petitioner argues, Exhibits 1057 and 1059 corroborate the thrust of Mr. Hopen’s testimony in Exhibits 1023 and 1058, and Patent Owner deposed Mr. Hopen about the veracity of Exhibits 1023 and 1058, as also indicated above the discussion of the public availability of Aventail. *See* Paper 23, 4–6.

Patent Owner argues the exception should be used sparingly in exceptional cases. Paper 20, 3–4. Patent Owner also criticizes the testimony of each witness. *Id.* at 4–6. Patent Owner argues the events occurred long after the testimony, citing as an example, the Hopen Declaration as being prepared 10 years after the event in question, the January 1999 distribution of Aventail. *See id.* at 4–5. We found, above, in the discussion of public availability, that the testimony includes self-corroboration between the declarations and other documentation which corroborates each of the

witnesses' memory of the sequence of events. We are not persuaded by Patent Owner's remaining arguments.¹⁸

Petitioner's showing is persuasive. *See* Opp.1–9. We adopt the showing by Petitioner, and for those reasons, we deny Patent Owner's Motion to Exclude Exhibits 1022, 1023, 1043, and 1058.

B. Exhibits 1060 and 1063–65

Patent Owner moves to exclude Exhibits 1060 and 1063–65 as inadmissible hearsay. Paper 20, 7–10. Because we do not rely Exhibits 1060 and 1063, we dismiss the motion as to Exhibits 1060 and 1063 as moot.

Exhibits 1064 and 1065 each constitute magazine articles dated 1999 that relate to the issue of public availability of RFC 2401 and 2543. *See* Paper 20, 10. Patent Owner does not explain why Exhibits 1064 and 1065 are hearsay or what part of them constitutes hearsay. *See* Paper 20, 7–10. As indicated above, Petitioner relies on the documents to support its contention that RFC 2401 and RFC 2543 qualify as a printed publication as of November 1998. Pet. Reply 21 (citing Ex. 1064, 9; 1065, 3). Referring to several listed RFC documents, including RFC 2401, Exhibit 1064 states “all of these documents are available on the ETF Web site: www.left.org/rfc.html.” 1064, 9; *see* Pet. 26 (relying on the statement and a

¹⁸ For example, Patent Owner argues “the rules recognize that former statements carry credibility risks that must be guarded against. It follows that when an otherwise available declarant's former statements are presented, the former statements are hearsay with no exception.” Paper 20, 6. But if Patent Owner is correct, then Patent Owner's Monroe Declarations (Ex. 2016, Ex. 2018), not having been prepared for this trial, would equally “carry credibility risks.”

similar statement at Exhibit 1065). Exhibit 1065 sets forth an imperative statement: “See the IETF documents RFC 2401 . . . and RFC 2411. . . at www.ietf.org/rfc/rfc2411.text.” Ex. 1065, 3.

Petitioner contends “Exhibits 1064–1065 are also relied upon to show that an interested ordinary artisan, exercising reasonable diligence, would have known how to locate RFC 2401 and RFC 2543. They are not hearsay when offered for that purpose.” Paper 23, 9 n.2 (citing Reply at 21–23; Fed. R. Evid. 801(c)(2) (a hearsay statement is one “a party offers in evidence to prove the truth of the matter asserted in the statement”))).

Petitioner’s argument is persuasive. Patent Owner has not met its burden of explaining why Exhibits 1064 and 1065 must be excluded as hearsay. The statements are offered to show that skilled artisans believed the RFC 2401 document and other RFC documents were available at the time of publication. Patent Owner does not challenge the publication dates of the magazines as hearsay. As noted above, Patent Owner does not state what aspects of the documents are hearsay. *See* Paper 20, 7–10; Paper 24, 4 n.1 (Patent Owner “disagrees” with Petitioner about the documents status as hearsay).

In any event, Petitioner shows that the documents also satisfy the residual hearsay exception. They have circumstantial guarantees of trustworthiness as written prior to litigation by disinterested parties in periodical trade magazines that almost qualify as ancient documents. Both magazine articles bear specific volumes and issue numbers along with the publication dates. *See* Ex. 1064 (Aug. 16, 1999, vol. 21, iss. 33); Ex. 1065 (March 15, 1999, vol. 16, no. 11); Paper 23, 3–8; Fed. Rule Evid. 803 (16) (ancient authentic documents of 20 years old are not hearsay). In addition,

as Petitioner argues, other documents and testimony corroborate the statements:

Dr. Tamassia explained that RFCs are the official publication channel for Internet standards, with the publication process described in RFC 2026 (Ex. 1036), Ex. 1005 at ¶¶117–24, which explains that anyone can obtain RFCs from a number of Internet hosts, Ex. 1036 at 6–8, and that each RFC “is made available for review via world-wide on-line directories,” *id.* at 4; *see* Ex. 1005 at ¶118.

Paper 23, 11. In addition, Petitioner points out that RFCs have been characterized as “written and circulated” by at least one District Court, further corroborating the statements: “[M]uch of the development and technical management of the Internet has been by the consensus of Internet users. This is evidenced . . . by IETF and the more than 2000 RFC’s which have been written and circulated.” Paper 23, 13 n.5. (quoting *PGMedia, Inc. v. Network Sols., Inc.*, 51 F. Supp. 2d 389, 406 (S.D.N.Y. 1999)).

Based on the foregoing, Patent Owner’s Motion to Exclude Exhibits 1064 and 1065 is denied and Patent Owner’s Motion to Exclude Exhibits 1063 and 1060 is dismissed as moot.

C. Exhibits 1007, 1012, 1017, 1026–29, 1038–40, 1048, 1052, 1054, and 1055

Patent Owner seeks to exclude the above listed Exhibits as lacking relevance. Paper 20, 1–2, 9–10. Because we do not rely on the above listed Exhibits, we dismiss this request as moot.

IV. ORDER

For the reasons given, it is

ORDERED that claims 1–11, 14–25, 28, and 30 of the ’696 patent are unpatentable;

IPR2016-00332
Patent 8,504,696 B2

FURTHER ORDERED that Patent Owner's Motion to Exclude is *dismissed as moot* with respect to Exhibits 1007, 1012, 1017, 1026–29, 1038–40, 1048, 1052, 1054, 1055, 1060, and 1063, and is *denied* with respect to Exhibits 1022, 1023, 1043, 1058, 1064 and 1065; 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.

PETITIONER:

Jeffrey P. Kushan
Scott M. Border
Thomas A. Broughan, III
SIDLEY AUSTIN LLP
jkushan@sidley.com
sborder@sidley.com
tbroughan@sidley.com
iprnotices@sidley.com

PATENT OWNER:

Joseph E. Palys
Naveen Modi
PAUL HASTINGS LLP
josephpalys@paulhastings.com
naveenmodi@paulhastings.com
PH-VirnetX-IPR@paulhastings.com