UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

APPLE INC.,
Petitioner

v.

VIRNETX INC.,
Patent Owner

Case IPR2016-00331
Patent No. 8,504,696

PATENT OWNER VIRNETX INC.'S NOTICE OF APPEAL

Director of the United States Patent and Trademark Office
c/o Office of the General Counsel
Madison Building East, 10B20
600 Dulany Street
Alexandria, VA 22314-5793

Notice is hereby given, pursuant to 37 C.F.R. § 90.2(a), that Patent Owner VirnetX Inc. ("VirnetX") appeals to the United States Court of Appeals for the Federal Circuit from the Final Written Decision entered on June 22, 2017, (Paper 29) (the "Final Written Decision") by the United States Patent and Trademark Office, Patent Trial and Appeal Board (the "Board"), and from all underlying orders, decisions, rulings, and opinions. A copy of the Final Written Decision is attached.

In accordance with 37 C.F.R. § 90.2(a)(3)(ii), VirnetX indicates that the issues on appeal include, but are not limited to, the Board's authority to invalidate a granted patent through *inter partes* review proceedings, the Board's determination of unpatentability of claims 1-11, 14-25, and 28-30 of U.S. Patent No. 8,504,696 under 35 U.S.C. § 103, and any findings or determinations supporting or related to those rulings including, without limitation, the Board's construction and application of the claim language, the Board's interpretation of the references, and the Board's interpretation of expert evidence.

Simultaneous with this submission, a copy of this Notice of Appeal is being filed with the Board. In addition, the Notice of Appeal and the required fee are being filed electronically with the Clerk of Court for the United States Court of Appeals for the Federal Circuit.

Respectfully submitted this 23rd day of August, 2017.

By: /Naveen Modi/

Naveen Modi
Registration No. 46,224
Paul Hastings LLP
875 15th Street, N.W.
Washington, DC 20005
(202) 551-1700
naveenmodi@paulhastings.com

Counsel for VirnetX Inc.

CERTIFICATE OF SERVICE

The undersigned certifies that, in addition to being filed electronically through Patent Trial and Appeal Board End to End (PTAB E2E), the original version of this Notice of Appeal was filed by hand on August 23, 2017 with the Director of the United States Patent and Trademark Office, at the following address:

Director of the United States Patent and Trademark Office
c/o Office of the General Counsel
Madison Building East, 10B20
600 Dulany Street
Alexandria, VA 22314-5793

The undersigned also certifies that a true and correct copy of this Notice of Appeal and the required fee were filed electronically via CM/ECF on August 23, 2017, with the Clerk of Court for the United States Court of Appeals for the Federal Circuit.

The undersigned also certifies that a true and correct copy of this Notice of Appeal was served on August 23, 2017 on counsel of record for Petitioner Apple Inc. by electronic mail (by agreement of the parties) at the following address:

Jeffrey P. Kushan
Scott Border
Thomas A. Broughan III
iprnotices@sidley.com
Sidley Austin LLP
1501 K Street NW
Washington, DC 20005

Date: August 23, 2017 By: /Naveen Modi/

Naveen Modi
Registration No. 46,224
Paul Hastings LLP
875 15th Street, N.W.
Washington, DC 20005
(202) 551-1700
naveenmodi@paulhastings.com

Counsel for VirnetX Inc.

Trials@uspto.gov
Tel: 571-272-7822

Paper 29
Entered: June 22, 2017

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

APPLE INC.,
Petitioner,

v.

VIRNETX INC.,
Patent Owner.

Case IPR2016-00331
Patent 8,504,696 B2

Before *Vice Chief Administrative Patent Judge* MICHAEL P. TIERNEY, 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.") requesting an *inter partes* review of claims 1–11, 14–25, and 28–30 (the "challenged claims") of U.S. Patent No. 8,504,696 B2 (Ex. 1001, "the '696 patent"). Patent Owner, VirnetX Inc., filed a Preliminary Response. Paper 6 ("Prelim. Resp.").

Subsequent to institution (Paper 9, "Inst. Dec."), Patent Owner filed a Patent Owner Response (Paper 14, "PO Resp."), and Petitioner filed a Reply (Paper 17, "Pet. Reply"). Patent Owner also filed a Motion to Exclude evidence (Paper 20), Petitioner filed an Opposition (Paper 23), and Patent Owner filed a Reply to the Opposition (Paper 24).

The record includes a transcription of the Oral Hearing held on March 27, 2017. Paper 28. This Final Written Decision issues concurrently with the final written decision involving the '696 patent in *Apple Inc. v. VirnetX Inc.*, IPR2016-00332 (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, and 28–30 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 in the '696 patent in IPR2016-00332. *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* Pet. 2–5, Paper 5, 2–15; *see also VirnetX, Inc. v. Cisco Systems, Inc*., 767 F.3d 1308, 1317–19 (Fed. Cir. 2014) (addressing ancestor *VirnetX* patents); *VirnetX Inc. v. Apple Inc.*, 665 F. App'x 880 (Fed. Cir. 2016) (affirming *Apple Inc. v. VirnetX Inc.*, Cases IPR2014-00237, IPR2014-00238 (final written decisions "'237 FWD," "'238 FWD," or generally, "'237 IPR," "'238 IPR") (PTAB May 11, 2015) (appealed by VirnetX))[1]; *VirnetX Inc. v. Apple Inc.*, 671 F. App'x. 786 (Fed. Cir. 2016) (affirming *Apple Inc. v. VirnetX Inc.*, Cases IPR2014-00403, IPR2014-00404, (PTAB July 29, 2015) (appealed by VirnetX)); *Apple Inc. v. VirnetX Inc.*, Cases IPR2014-00481, IPR2014-00482 (PTAB August 24, 2015) (appealed by VirnetX))[2]; *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 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) (appealed by VirnetX). Some of these related cases involve overlapping claim construction and prior art issues with the instant case as discussed further below.

[1] 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").

[2] The court affirmed the four final written decisions without reaching the merits of the '404 and '482 proceedings. *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).

C. Instituted Grounds of Unpatentability

We instituted under 35 U.S.C. § 103 on the ground that combination of Beser[3] and RFC 2401[4] would have rendered obvious claims 1–11, 14–25, and 28–30 of the '696 patent. Petitioner relies on, *inter alia*, the "Declaration of Roberto Tamassia Regarding U.S. Patent Nos. 8,540,696." Ex. 1005 (the "Tamassia Declaration"). Patent Owner relies on, *inter alia*, the "Declaration of Fabian Monrose, Ph.D." Ex. 2018 (the "Monrose Declaration"), originally filed in a related case, *Apple Inc. v. VirnetX Inc.*, IPR2015-00866 (PTAB Jan. 25, 2016) (Ex. 2018).

D. 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.

---

[3] U.S. Patent No. 6,496,867 B1 (Ex. 1007).
[4] S. Kent and R. Atkinson, *Security Architecture for the Internet Protocol*, Request for Comments: 2401, BBN Corp., November 1998 (Ex. 1008).

The DNS proxy of the modified DNS server intercepts all 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 40:49–53. 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 40:31–42. 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 40:4–8. 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. The system also may encrypt data in the packets. *See id*. at 1:50–56, 4:7–12.

E. 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, 56:8–23.

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 terms or clauses below need express construction. *See Vivid Techs., Inc. v. Am. Sci. & Eng'g, Inc*., 200 F.3d 795, 803 (Fed. Cir. 1999) (only those terms in controversy need to be construed and only to the extent necessary to resolve the controversy).

"*intercept . . . a request*"

Relying partly on the '237 FWD, Petitioner proposes that we construe the claim 1 phrase "intercept . . . a request" as "receiving a request pertaining to a first entity at another entity." Pet. 12 (citing '237 FWD, 10–12).[5] Claim 16 recites a similar "intercepting a request" phrase. Patent

[5] Claim 1 of U.S. Patent No. 8,504,697 ("'697 patent") at issue in the'237 FWD (*see supra* notes 1 and *infra* note 6) recites a similar clause: "intercepting, 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." '237 FWD 4. The '697 and '696 patents each have common ancestor patents at issue in *Cisco*, 767 F.3d

Owner states that "[n]o construction [is] necessary; alternatively," Patent Owner proposes that the phrase means "receiving a request to look up an internet protocol address and, apart from resolving it into an address, performing an evaluation on it related to establishing a virtual private network communication link." Prelim. Resp. 40. Patent Owner contends that its "construction appropriately captures the notion of performing an additional evaluation on a request related to establishing a virtual private network communication link, beyond conventionally resolving it and returning the address." *Id*. at 43.

Patent Owner's contentions are not persuasive. Patent Owner fails to explain sufficiently why the notion of "performing an additional evaluation" constitutes an implicit part of the claimed intercept clause. Addressing similar arguments by Patent Owner, a Board panel made a similar determination in the '237 FWD relied upon by Petitioner. '237 FWD 11 ("the record show[s] that the additional functionality urged by Patent Owner should not be imported into the intercepting phrase").

To support its construction, Patent Owner states "a request to look up an address of a secure target site 2604 or unsecure target site 2611 (a first entity) is received at a DNS server 2602 (a second entity)." PO Resp. 18

---

at 1308: The '696 patent is a continuation of an application, which like the '697 patent, 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* 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.)

(citing Ex. 1001, Fig. 26). Patent Owner explains "the claimed embodiments differ from [a] conventional DNS, in part, because they apply an additional layer of functionality to a request to look up a network address beyond merely resolving it and returning the network address." *Id.*

As one example, Patent Owner contends that DNS proxy 2610 (part of DNS server 2602) "may intercept the request and 'determine whether access to a secure side has been requested.'" *Id*. (quoting Ex. 1001, 40:26–35). Patent Owner provides two additional "example" DNS functions, but fails to describe which examples are necessary to the construction of the intercept clause. *See id*. (listing examples: 1) determining if a user has sufficient security privileges to access the site; 2) transmitting a message to a gate keeper to request a VPN creation; and 3) resolving an address and returning it to the DNS). These additional disclosed functions of a DNS fail to show that the "intercept" clause at issue requires the unclaimed additional functionality. The intercept clause does not recite a DNS.

Furthermore, the disclosed embodiment cited by Patent Owner supports Petitioner's proposed claim construction, as DNS server 2602 performs the intercept by "receiving a request pertaining to a first entity [2604 or 2611] at another entity [2602]." *See* Ex. 1001, Fig. 26. As the '696 patent discloses, in one embodiment, a "single server" having "the functions of DNS proxy 2610 and DNS server 2609" (Ex. 1001, 40:63–65, Fig. 26) "intercepts all DNS lookup functions" (*id*. at 40:26–27). In other words, pursuant to requests for a connection to a secure or unsecure device (first entity), intercepting DNS server 2602 (second entity) returns the IP address of the first entity after looking up the domain name. *See id*. at 40:26–34.

Based on the foregoing discussion, we adopt Petitioner's proposed construction that the phrase "intercept . . . a request" means "receiving a request pertaining to a first entity at another entity."[6]

B. Prior Art Printed Publication Status of RFC 2401

Patent Owner asserts that Petitioner fails to show that RFC 2401 was publicly accessible as of November 1998 (the date recited on each of its pages). PO Resp. 42 (citing Ex. 1008). On this basis, according to Patent Owner, Petitioner cannot rely upon RFC 2401 as prior art to meet its burden of showing obviousness of the challenged claims over the combination of Beser and RFC 2401. *See id.*

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). On its face, RFC 2401 is a dated "Request for Comments" from the "Network Working Group," discussing a particular standardized security protocol for the Internet. Ex. 1008, 1. Moreover, RFC 2401 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." *Id.* These

[6] *See* '237 FWD 12 (reaching the same construction). As also noted in the '237 FWD (a final judgment affirmed by our reviewing court, *supra* note 1), "Patent Owner concedes that "[t]he *Decision's construction* [of intercepting a request] *addresses* a common aspect of *a conventional DNS and the disclosed embodiments*, namely that a request to look up an address of one entity may be received at another entity." '237 FWD 24 (quoting '237 patent owner response 26) (emphases added).

indicia suggest that the document was made available to the public (over the Internet), in order to obtain feedback prior to implementation of the standard it describes.

To bolster its showing, Petitioner provides evidence suggesting that RFC 2401 would have been accessible to the interested public. For example, Petitioner relies on testimony by Dr. Tamassia, and an article dated March 15, 1999, referencing RFC 2401 availability on a website. Pet. 25–26 (citing Ex. 1005 ¶¶ 115–21; Ex. 1065, 3). Petitioner also explains that RFC 2401 describes the IPsec protocol promulgated by the Internet Engineering Task Force (IETF). *Id*. Petitioner provides a declaration by Sandy Ginoza, who, acting as a designated representative of the IETF, previously testified that RFC 2401 was published on the RFC Editor's website and was publicly available in November 1998. *Id*. at 25–26 (citing Ex. 1060 ¶¶ 105–07; Ex. 1063, 39:14–24). 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 October 1996 RFC 2026 publication (Ex. 1036, 5–6 (explaining that any interested person can obtain RFC documents from a number of Internet hosts using anonymous FTP, gopher, WWW, and other document-retrieval systems)). *Id*. at 25–26 (citing Ex. 1064, 9; Ex.1036, 5–6).

Patent Owner characterizes Petitioner's showing as insufficient. PO Resp. 43–51. Patent Owner contends that Sandy Ginoza and Dr. Tamassia lack personal knowledge about the publication of RFC 2401, and challenges other evidence as too general and lacking a sufficient foundation. *See* PO Resp. 44–47 (discussing Pet. 25–26, Ex. 1036, 4–6; Ex. 1060–65)). Patent

Owner does not contest Petitioner's characterization of the two magazine articles, Exhibits 1064 and 1065, other than to refer to them as follows: "Exhibit 1064 is allegedly an article from InfoWorld magazine (dated August 16, 1999) and Exhibit 1065 is allegedly an article from NetworkWorld magazine (dated March 15, 1999)." PO Resp. 45.

RFC 2026 states it reflects "generally accepted practices" for RFC documents and states "any interested person can obtain RFCs from a number of Internet hosts." *See* PO Resp. 47 n.9 (citing Ex. 1036, 4, discussing Inst. Dec. 13). Patent Owner contends that Petitioner has not shown that this evidence of "generally accepted practices" "is accurate." *Id*. Patent Owner notes that the document represents "flexible" standards, so that "there is no assurance that the procedures of RFC 2026 that were quoted by Petitioner were actually applied." *Id*. at 47.

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.[7] 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, but does not point us to any discussion of this issue. Moreover, RFC 2401's contents are consistent with the publication process described by RFC 2026 and Dr. Tamassia, including the inclusion of a date "November 1998" on the top right corner of the first page of the document. Ex. 1008, 1. In addition, this document—a request for suggestions and improvements for an Internet standards protocol,

[7] As addressed below, Patent Owner objects and moves to dismiss a number of Exhibits based on hearsay and relevancy. *See* Paper 20 (Motion to Exclude).

having no indication of being a mere draft or internal paper—is precisely the type of document whose very purpose is public disclosure, including on the Internet. 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. We do not rely on the testimony of Sandy Ginoza, Exhibits 1060 and 1063, which Patent Owner seeks to exclude as discussed further below.

Petitioner also points out that at least one District Court characterized RFCs as having "been written and circulated": "[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, 6 n.3. (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, 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)). We find that Petitioner has established, by a preponderance of the evidence, that RFC 2401 (dated November 1998) was disseminated and made available to persons of ordinary skill interested in computer networking and security to be deemed "publicly accessible" at the relevant time. Therefore, on this record, we determine RFC 2401 qualifies as a prior art printed publication under 35 U.S.C. § 102(b).

C. Tamassia Declaration (Ex. 1005)

Patent Owner argues that the entirety of the Tamassia Declaration should be given little or no weight because Dr. Tamassia "failed to consider, let alone opine on, how any of the claim features are disclosed in asserted references." PO Resp. 51. Petitioner responds that Dr. Tamassia has "offered probative testimony on many of the factual inquiries underpinning an obvious analysis" that "can certainly 'assist the tier of fact to understand the evidence or determine a fact in issue.'" Pet. Reply 22–23 (quoting Fed. R. Evid. 702). Petitioner also contends "no rule requires an expert to opine on the ultimate question of obviousness or on every potentially relevant fact at issue for his opinion to be admissible or entitled to weight." *Id.* at 23.

Patent Owner does not articulate a persuasive reason for giving Dr. Tamassia's declaration, as a whole, little or no weight in our analysis. We agree with Petitioner that experts are not required to opine on every relevant factual and legal issue in order to be accorded substantial weight. The cases upon which Patent Owner relies do not show otherwise. For example, Patent Owner cites *Schumer v. Laboratory Computer Systems, Inc.*, 308 F.3d 1304, 1315 (Fed. Cir. 2002), for the proposition that "[expert] testimony . . . 'must identify each claim element, state the witnesses' interpretation of the claim element, and explain in detail how each claim element is disclosed in the prior art reference.'" PO Resp. 52–53. Patent Owner's quotation, however, mischaracterizes *Schumer* by omitting introductory words necessary to the meaning of the quoted sentence. In its entirety, the quoted portion of *Schumer* states the following:

> *Typically, testimony concerning anticipation* must be testimony from one skilled in the art and must identify each claim element, state the witnesses' interpretation of the claim element,

> and explain in detail how each claim element is disclosed in the prior art reference. The testimony is insufficient if it is merely conclusory.

Schumer, 308 F.3d at 1315–16. The Federal Circuit then adds that it is not the task of the courts to "attempt to interpret confusing or general testimony to determine whether a case of invalidity has been made out" and "if the testimony relates to prior invention and is from an interested party, as here, it must be corroborated." *Id.* at 1316. So, instead of laying out a specific, required format for the content of all testimony regarding invalidity, as asserted by Patent Owner, this portion of *Schumer* confirms the unremarkable proposition that conclusory, overly general, confusing, and self-interested testimony should not be relied upon. *Id.*; *see also Koito Mfg. Co., Ltd. v. Turn-Key-Tech, LLC*, 381 F.3d 1142, 1152 (Fed. Cir. 2004) ("General and conclusory testimony, such as that provided by Dr. Kazmer in this case, does not suffice as substantial evidence of invalidity."). Patent Owner does not show that the whole of Dr. Tamassia's testimony suffers from any of these failings.

Under 35 U.S.C. § 316(e), the preponderance of the evidence standard governs in determining whether Petitioner establishes unpatentability. We exercise discretion to determine the appropriate weight to accord the evidence presented, including expert opinions, based on the underlying facts supporting the opinion. We accord relevant portions of Dr. Tamassia's testimony the appropriate weight based on that particular testimony and supporting evidence.

D. Obviousness Over Beser and RFC 2401

1) Overview of Beser

Beser describes a system that establishes an IP (internet protocol) tunneling association on a public network between two end devices. *See* Ex. 1007, Abs.

Figure 1 of Beser follows:

FIG. 1

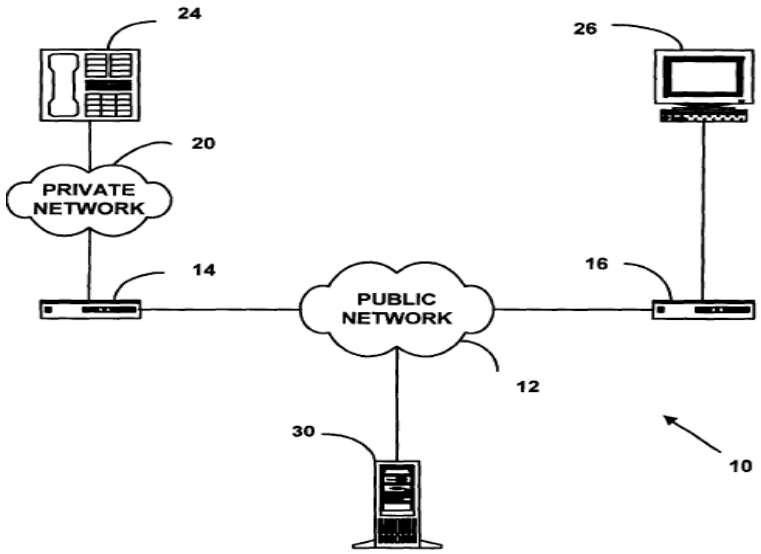

Figure 1 of Beser illustrates a network system, including public network 12, network devices 24 and 26, private network 20, trusted third-party network device 30, and modified routers or gateways 14 and 16. Ex. 1007, 3:60–4:19. Beser describes network devices 24 and 26 as telephony devices, multimedia devices, VoIP devices, or personal computers. *Id.* at 4:43–52.

Beser's system "increases the security of communication on the data network" by providing and hiding, in packets, "private addresses" for originating device 24 and terminating device 26 on the network. *See id.* at Abs., Fig. 1, Fig. 6. To begin a secure transaction, requesting device 24

sends a request to initiate a tunneling connection to network device 14. *Id.* at 8:21–47. This request includes a unique identifier for the terminating end of the tunneling association—terminating device 26. *Id.*at 7:64–8:3. The packets used to transfer this unique identifier across the public network "may require encryption or authentication to ensure that the unique identifier cannot be read on the public network." *Id.* at 11:22–25. Beser discloses, as background prior art, known forms of encryption for the information inside these packets, including IP Security ("IPsec"). *Id.* at 1:54–56. Once network device 14 receives the request, it passes the request to trusted-third-party network device 30. *Id.* at 8:3–4, 8:48–9:5.

Trusted-third-party network device 30 contains a directory of users, such as a DNS, which retains a list of public IP addresses associated at least with second network device 16 and terminating devices 26. *See id.* at 11:32–58. DNS 30 associates terminating network device 26, based on its unique identifier in the request, with a public IP address for router device 16. *See id.* at 11:26–36. Trusted-third-party network device 30 then assigns, by negotiation, private IP addresses to requesting network device 24 and terminating device 26. *Id.* at 9:29–35, 12:17–19. The negotiated private IP addresses are "isolated from a public network such as the Internet," and "are not globally routable." *Id.* at 11:62–65.

2) Overview of RFC 2401

RFC 2401 describes security services using IPsec protocols on the Internet (Ex. 1008, 3) including "access control, connectionless integrity, data origin authentication, [and] . . . confidentiality (encryption)" (*id.* at 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) Claims 1 and 16

i) Petitioner's Contentions

Petitioner asserts that Beser's streaming audio/video examples, in light of the encryption teachings based on the combination of Beser and RFC 2401, would have rendered obvious claims 1 and 16. *See* Pet. 29–30. According to Petitioner, Beser teaches or suggests most of the limitations of claims 1 and 16, with Beser and RFC 2401 at least suggesting encryption of data. *See* Pet. 28–34. "[T]o limit the impact from any potential disputes or related legal proceedings over the construction" of a VPN communications link, Petitioner contends that even if a VPN communications link requires data encryption, the combination of Beser and RFC 2401 would have rendered such a VPN link obvious. *See id*. at 29.[8]

[8] According to *Cisco*, "the [related '151] 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." *Cisco*, 767 F.3d at 1323. *Cisco* refers to "physical security" on private networks that do not necessarily have encryption, notes that the VirnetX patents (at issue in that litigation) describe encryption as one possible way to tackle data security, and notes that the district court's claim construction for security only requires encryption *on insecure paths* (for example, on the Internet—as opposed to physically secure private networks). *See id*. at 1321–22.

Addressing the preambles claims 1 and 16, Petitioner contends that the claimed first network device reads on Beser's originating end device 24, and that the claimed second network device reads on Beser's terminating end device 26. *See id*. at 35–36 (citing Ex. 1007, 8:15–20, 21:52–62, 22:2–22; Ex. 1005 ¶¶ 127, 195–96); Ex. 1007, Fig. 1. Petitioner points out that Beser discloses various end devices including WebTV devices and VoIP devices that communicate over a private tunneling association established by trusted-third party network device 30 "with the help of first and second network devices" 14 and 12. *See* Pet. 35 (citing Ex. 1007, 4:43–54, 7:64–66, 8:15–20, 14:51–67, 10:22–36, 10:55–66, 14:51–67; Ex. 1005 ¶¶ 131, 169, 173, 177, 188–93, 198).

Regarding the "intercept" clause of claim 1, Petitioner explains that Beser's trusted-third-party network device 30 (which includes a DNS), first network device 14, and second network device 16, work together such that devices 30 and 14 singly or together intercept the request, and then look up (also using device 16 in some embodiments) private and public IP addresses based on a request from originating VoIP device 24 that includes a unique domain name for the claimed target device—terminating end device 26. *See id*. at 36–39 (citing Ex. 1007 4:9–11, 8:21–47, 10:37–42, 10:55–11:5, 11:26–36, 11:45–58, 13:49–65, 14:2–14, 16:1–37; Ex. 1005 ¶¶ 66, 152–53, 170–72, 175–78, 192–92; '237 FWD 24, 26 n.6, 27). According to Petitioner, Beser's first network device 14 and trusted-third-party device 30 constitute "another entity" that intercepts the request according to the claim construction of "intercept" as set forth above. *Id*. at 38–39.

Regarding the "determine" clause of claim 1, Petitioner contends "Beser teaches that the trusted-third-party network device [30] determines

whether the unique identifier in a request specifies a destination that can establish a secure tunnel by checking its internal database of registered users or devices." *Id*. at 39 (citing Ex. 1007, 11:30–36, 11:45–58; Ex. 1005 ¶¶ 163, 176, 178, 180). According to Petitioner, "[t]his is done '*in response to the request*' and is the same type of 'determining' disclosed in the '696 patent." Pet. 39 (citing Ex. 1001, 40:28–35; '237 FWD 28–36).

Petitioner also contends that Beser's system implies integrating normal DNS functionality with requests for tunneling, as implied by the use of unique domain name (or other identifier) functioning as part of a request for secure tunneling, and the disclosure of a conventional DNS. *See* Pet. 21–22 (citing Ex. 1007, 4:7–42; 8:21–52, 9:6–11, 11:26–58: Ex. 1005 ¶¶ 152–53, 160–63, 170, 175). In other words, according to Petitioner, a skilled artisan would have understood that Beser's DNS would have been a modified conventional DNS equipped to handle requests to communicate using Beser's IP tunnel and to handle typical DNS requests. *See* Pet. 19–22, 39–41; Ex. 1007, 4:7–42, 8:21–51, 9:26–30, 11:8–12:19; Figs. 1, 6, 9; Ex. 1005 ¶¶ 156–164, 170–71, 176–83.

Regarding the "initiate a [VPN] communication link" clause recited in claim 1, Petitioner argues that the combination of Beser and RFC 2401 would have rendered obvious encryption of at least low-resolution audio and video packet information on Beser's tunnel. Pet. 41–44. Petitioner also contends that based on the combination of Beser and RFC2401, a skilled artisan would have recognized that any problems associated with encryption of high-volume multimedia traffic may be overcome by providing more computing power, and that the combination would have rendered obvious end-to-end encryption in Beser's system. *See id*. at 42–46 (citing '237 FWD

40, 43; Ex. 1007, 2:13–17). Petitioner also contends that initiating the VPN connection would be based on a determination that Beser's terminating end device is available for the secure communications service, because, for example, if the device is not listed in Beser's DNS as associated with a private IP for tunneling, it would not be available for tunneling, and no secure connection will be made. *See* Pet. 40–43; Ex. 1005 ¶¶ 176–83 (testifying, *inter alia*, that it would have been obvious to configure Beser's DNS to return an IP address if the unique domain name was not registered for secure use).

Petitioner also contends that the combination of Beser and RFC 2401 teaches or suggests the remaining elements of claims 1 and 16, including the preamble of "including one or more servers configured to" perform the functions recited in claim 1. *See* Pet. 44 (citing Ex. 1007, 4:9–11, 4:18–5:2, 5:15–47, 10:37–42, 10:55–11:5; Ex. 1005 ¶¶ 130, 146, 156).

Regarding reasons to combine, Petitioner contends that "a person of ordinary skill would have considered the teachings of Beser in conjunction with those in RFC 2401 because Beser expressly refers to the IPsec protocol (which is defined in RFC 2401) as being the conventional way that the IP tunnels described in Beser are established." Pet. 31 (citing Ex. 1007, 1:54–56; Ex. 1005 ¶¶ 218–20, 230). Petitioner adds that Beser also indicates that "its IP tunneling schemes are compliant with standards-based processes and techniques (*e.g.*, IPsec), and can be implemented using pre-existing equipment and systems," and that "IP tunnels are and should ordinarily be encrypted, even for the data streaming examples." *Id.* at 31–32 (citing Ex. 1007, 1:54–56, 4:55–5:2, 11:22–25, 18:2–5; Ex. 1005 ¶¶ 135–36, 138, 220, 221, 223–25, 229, 230, 233–38). Petitioner also contends that Beser

discloses encryption employed to hide addresses in its tunneling scheme, criticizes prior art systems that do not use encryption, discusses challenges to data encryption, and implies a trade-off between power and data quality for audio and video streaming. *See* Pet. 32–35; Ex. 1007, 1:54–2:40, 11:22–25, 18:2–5, 20:11–14.

Petitioner contends further that a person of ordinary skill would have recognized that IPsec, which Beser and RFC2401 each discloses, readily could have been integrated into Beser's systems, for example, to provide end-to-end enhanced security of Beser's tunneling (which provides anonymity by hiding addresses using encryption and private addresses) and using encryption to provide secure data security. *See id*. 32–33 (citing Ex. 1005 ¶¶ 224–25, 228–29, 233–35). Petitioner explains that basic configurations, including edge routers, of the two disclosed systems as disclosed in Beser and RFC 2401, are similar. *Id*. at 33 (citing Ex. 1005 ¶¶ 231–32, 234; Ex. 1007, 4:7–8, 18–29, Fig. 1; Ex. 1008, 25); *see* Ex. 1005 ¶¶ 221–32 (comparing RFC2401 and Beser, discussing tunnels and encryption, testifying that skilled artisans readily would have been motivated to use data encryption to enhance security in VPNs by adding computing power if necessary).

ii) Patent Owner's Arguments

a. Intercept 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

With respect to the "intercept" clause of claims 1 and 16 referenced in the section heading, Patent Owner contends that Beser's trusted-third-party device does not negotiate, and even if it does, "negotiation does not involve

looking up any IP address, but rather involves *assignment* of a first private network address to the originating device and a second private network address to the terminating device." PO Resp. 23 (citing Ex. 1007, 12:2–4; Ex. 2018 ¶ 43). Patent Owner explains "*Beser* never suggests that this [domain name] data structure is looked up," and "only teaches that when a trusted-third-party network device 30 is informed of a request to initiate a tunnel, it *associates* a public IP address of a second network device 16 with the unique identifier of terminating telephony device 26." *Id*. at 24 (citing Ex. 1007, 11:26–32; Ex. 2018 ¶ 44) (emphasis added). Patent Owner also contends that Beser discloses a bifurcated system that does not provide look up functionality. *See* PO Resp. 24 (arguing "there is simply no evidence suggesting that the alleged typical look up functionality of a DNS would apply to the alleged additional functionality of trusted third party network device 30"). Patent Owner contends that "[n]one of the processes in *Beser* transform the request to initiate a tunneling connection into a request to look up an IP address. Indeed, one of the novel aspects of the challenged claims (discussed in detail in Section III.C below) is that, while a request to look up an IP address is transmitted, the request is intercepted allowing it *not* to be processed in the conventional manner." *Id.* at 26 (citing Ex. 1001, 39:62–40:25; Ex. 2018 at ¶ 45).

These arguments appear to attempt to draw a distinction between "look up" and "associates" (or "assigns") that does not exist in light of the '696 patent Specification. Beser's tunneling system must "look up" an IP address based on a domain name (or other unique identifier) in order to associate an IP address or other addresses with the requested terminating telephony device 26. *See* Ex. 1007, 10:37–11:58, Figs. 5–7. Like Patent

Owner, Dr. Monrose does not explain the basis for any distinction. *See* Ex. 2018 ¶ 44.

As Petitioner contends, "Beser's trusted device 30 performs the negotiation with the first and second network devices." Pet Reply 14 (citing Ex. 1007, 9:29–30, 12:16–19, 14:19–27, Figs. 6 and 9; *see* Pet., 22–24, 40–41. Beser's "trusted-third-party 30 may be . . . a domain name server" or other typical database structure. Ex. 1007, 4:9–11; *accord* Ex. 1007, 10:41–57, 11:33–34. The "request includes a unique identifier for the terminating telephony device 26" that may be "a dial-up number, and electronic mail address, *or a domain name*." Ex. 1007, 10:4–6, 10:38–41.

Given Beser's teachings, a skilled artisan would have understood that Beser's trusted-third-party device 30 discloses or at least suggests DNS functionality working with the tunneling application to associate one or more (private and public) IP addresses for the requested device. *See* Pet. 19–22, 39–41; Ex. 1007, 4:7–42, 8:21–51, 9:26–30, 11:8–12:19; Figs. 1, 6, 9; Ex. 1005 ¶¶ 156–164, 170–71, 176–83.[9] As Petitioner contends, Beser's system employs the tunneling application to instigate negotiation, whereby trusted-third-party device 30 responds to that request and "associates" the domain name or other unique identifier of terminating device 26 with device

[9] Beser's trusted-third-party device 30, a "domain name server" (Ex. 1007, 11:34), may include a "*database entry* . . . includ[ing] a public IP 58 address[] for the terminating telephony device 26. Many data structures that are known to those skilled in the art are possible *for the association of the unique identifiers and IP 58 addresses for the second network devices 16*" (*id*. at 11:50–55 (*emphases added*)). Therefore, Beser's DNS 30 implicitly looks up the public IP 58 addresses of devices 16 and 26 based on a domain name (unique identifier) of terminating device 26—in order to associate the two devices.

16 and a public IP address for device 16 and/or device 26. Ex. 1007, 11:26–32; Pet. 21–22; Pet. Reply 11–15; Ex. 1007, 11:51–55 (disclosing a "public IP addresses 58 for the terminating . . . device 26. *Many data structures that are known to those skilled in the art are possible for the association of the unique identifiers and IP 58 addresses for the second network devices 16*") (emphasis added); *supra* note 9 (discussing the passage), *infra* note 10 (admitting conventional DNS functions provide a look up function).

The '696 patent and the record support Petitioner's showing that DNS look up functions or other similar look up functions were conventional and well-known.[10] Notwithstanding Patent Owner's arguments, based on the record, Beser discloses (or at least suggests) the recited look up function, because a DNS and similar known database structures disclosed by Beser typically must look up stored data base information in order to associate the IP address with a unique identifier. *See* Ex. 1007, 11:9–62, *supra* notes 9, 10.

Quoting Beser, as Petitioner summarizes persuasively, in addition to the public address look up of terminating device 26 that Beser teaches as described above (*see* Pet. 22, note 9)[11], Beser discloses two other look ups

[10] According to the '696 patent, "[c]onventional Domain Name Servers (DNSs) provide a look-up function that returns the IP address of a requested computer or host." Ex. 1001, 39:26–28. In this conventional scheme, "[w]hen the user enters the name of a destination host, a request DNS REQ is made . . . to look up the IP address associated with the name." *Id*. at 39:36–38.

[11] "As Beser explains, the database contains the list of authorized devices, and each entry in the database includes the unique identifier, the 'IP 58 address of a particular second network device 16,' and the 'public IP 58

associated with terminating device 26 that each also satisfy the disputed intercept of a request for a look up clause:

> The tunneling request sent by originating device 24 is a "request to lookup an [IP] address" because in response to receiving the request, the Beser trusted device 30 looks up two IP addresses. Pet., 37–38. First, it consults an internal database of registered devices to look up the IP address of second device 16 that is associated with the unique identifier. *Id*, 21–22, 37–38; Ex. 1007, 11:45–58. Second, it looks up a private IP address for terminating device 26 by sending a message to device 16 requesting the address. Pet., 22–23, 37–38; Ex. 1007, 9:29–30, 12:16–19, 14:14–27, Figs. 6 & 9. As a result of this process, originating device 24 receives an IP address for terminating device 26. Pet., 22; Ex. 1007, 21:48–52; *see* Ex. 1077, 103:22–104:3.

Pet. Reply 11.

In other words, Petitioner contends persuasively, by way of a specific example, that Beser's trusted-third-party device "looks up" a private IP address for terminating device 26 in part by asking device 16 for it. *See also* Pet. Reply 15 (discussing packet 162 containing public IP 58 address for device 16 and return packet 166 containing a private address for device 26) (citing Ex. 1007, Fig. 9 (packets 164 & 166), 13:34–64, 13:66–14:18; 38).

Focusing on the claim language "associated," Petitioner also shows that the system looks up the public IP address of device 16, and associates it with the unique identifier for terminating device 26, which satisfies the disputed phrase, because "the '696 specification provides that the IP address looked up 'need not be the actual address of the destination computer,' (*id.* at 40:43–44)." Pet. Reply 14. In other words, trusted-third-party device 30

---

addresses for the terminating telephony device 26.'" Pet. 22 (quoting Ex. 1007, 11:48–52).

intercepts the request for a look up even if part of a look up occurs at device 16 based on the request and negotiation by device 30.

Patent Owner contends for other reasons that Beser fails to disclose "intercept[ing] . . . a request," as set forth in the claim 1 and 16. *See* PO Resp. 26–30. According to Patent Owner, "tunneling requests in Beser always go to, and are always intended to go to, the first network device [14]." *Id*. at 28 (citing Ex. 2018 ¶ 48). Patent Owner also explains that first network device 14 constructs a packet intended for trusted-third-party network device 30, so that "the packet received by trusted-third-party device 30 is 'intended for' and 'ordinarily received by' trusted-third-party network device 30 since the destination address of the packet contains the address of the trusted-third-party network device 30." *Id*. at 28–29 (citing Ex. 2018 ¶ 49).

These arguments turn on claim construction and are not persuasive. Patent Owner's proposed claim construction of the "intercept" clause does not include any "intent" requirement. In the Institution Decision, we initially observed "it also is not clear why that would create a distinction over the prior art, even if somehow, it is required." Inst. Dec. 21 (citing Prelim. Resp. 40–41). We also observed "[f]or example, Patent Owner does not dispute that tunneling requests in Beser are intended as requests for a tunneling connection with terminating end device 26." *See id*.; Ex. 2018 ¶ 49. The record supports these observations.

Nevertheless, Patent Owner contends these observations "miss[ ] the point that such tunneling requests are not intercepted in accordance *with Petitioner's expert's understanding of the construction of 'intercepting'* set forth by Petitioner and in the Institution Decision." PO Resp. 29 (emphasis

added). To the contrary, the Petition and Institution Decision rely upon the claim construction set forth above, which, in light of the Specification and plain meaning, does not require an intent or other related elements that Patent Owner contends Beser does not disclose. *See* Pet. Reply 16 ("Patent Owner's arguments are irrelevant to what the claims require."), 17 (citing Ex. 2019, 79:9–80:13, 85:9–12; *see* Ex. 1005 ¶¶65–66). As noted, Patent Owner does not even advance an intent element or "ordinarily received" element in its proposed claim construction. *See supra* Section II.A; *compare* PO Resp. 17–19 (proposed claim construction), *with* PO Resp. 30 (arguments based on elements not in proposed claim construction, citing Ex. 2019, 80:3–13; 74:2–17, 79). Moreover, Patent Owner's cited deposition colloquy obfuscates the issue of what "intercept" means in the challenged claims, where, for example, Dr. Tamassia states that "'intended to' in a general context is different from 'intercepting.'" Ex. 2019, 85:9–12.

Beser's system satisfies the claim construction of "intercept," which means "receiv[e] a request pertaining to a first entity at another entity." *Supra* Section A.II. (Claim Construction). First network device 14 and trusted-third-party device 30 work together and receive (intercept) a request pertaining to terminating device 26. *See* Ex. 1001, Figs. 6–7 (depicting and describing tunneling negotiation and association). As discussed above, Beser discloses or at least suggests a look up function or table, wherein DNS 30 also works with second network device 16 to match a unique domain name for target device 26 and associate it with one or more of three IP addresses as found above: a public address for second device 16 (which is associated with target device 26), a private address for target device 26, and a public address for target device 26. *See id*. at 9:35–37, 11:48–58; note 9.

Beser's scheme, as described by Patent Owner, is consistent with the scheme disclosed in the '696 patent, wherein either a "single server" or distributed server (i.e., servers "can be combined") having "the functions of DNS proxy 2610 and DNS server 2609" intercepts all requests for connection to either a secure or unsecure device. *See* Ex. 1001, 40:63–65; Ex. 2018 ¶¶ 48–49; *compare* Prelim Resp. 13–14 (describing Beser), *with* 42–44 (describing disclosed embodiments in the '696 patent) and PO Resp. 18 ("DNS proxy 2610 may intercept the request"). In these disclosed embodiments of the '696 patent, packet requests travel to server 2609 and DNS proxy 2610, which have "functions . . . [that] can be combined into a single server" (Ex. 1001, 40:63–64), and which "intercepts *all DNS lookup functions* from client 2605" (*id.* at 40:26–27 (emphasis added)). *See* Ex. 1001 39:65–40:67.

In addition, as we initially determined in the Institution Decision, "[a]lthough Patent Owner contends that Beser's system uses a packet addressed to server 30 as an alleged distinction with respect to claims 1 and 16, Patent Owner fails to explain how its disclosed server 'intercepts' any packet that does not have a packet addressed to that server." Inst. 22; (citing Ex. 2018 ¶¶ 48–49; Prelim Resp. 13–14, 42–44). Of course, Patent Owner *does not have the burden* to come forward with any explanation, but Patent Owner does not support its argued distinction over Beser's DNS 30, which operates similarly to the '696 patent's DNS proxy 2610. *See* PO Resp. 28–29 (arguing a packet source address for trusted-third-party network device 30 shows the request "is 'intended for' and 'ordinarily received'" by device 30); *supra* note 6 (noting our reviewing court affirmed the '237 FWD employing the same or similar claim construction).

b. Virtual Private Communication Link

Patent Owner contends "*Beser* expressly differentiates its tunnel between devices 24 and 26 from a VPN and any related VPN communication link." PO Resp. 30 (citing Ex. 2018 ¶ 51). According to Patent Owner,

> *Beser* states that "[o]ne method of thwarting [a] hacker is to establish a Private Network ('VPN') by initiating a tunneling connection between edge routers on the public network." (Ex. 1007 at 2:6–8; Ex. 2018 at ¶ 51.) *Beser* goes on to criticize a VPN as "[a] form of tunneling [that] may be inappropriate for the transmission of multimedia or VoIP packets" (Ex. 1007 at 2:6–17), immediately before introducing *Beser*'s tunnel as a solution to the problems posed by VPNs for VoIP (*id.* at 2:43–66). So *Beser* is not just silent on whether its tunnel is a VPN communication link, *Beser* expressly teaches that its tunnel is not a VPN communication link. (Ex. 2018 at ¶ 51.)

PO Resp. 30–31 (quoting Beser, citing Dr. Monrose).

Patent Owner fails to explain clearly why it contends Beser does not disclose the claimed VPN communication link. Patent Owner appears to be arguing that Beser does not disclose a VPN communication link because Beser's tunnel does not encrypt data: "Thus, one of ordinary skill in the art would have understood that *Beser* is directed to providing a method for securing communications *other than* encryption and teaches away from encryption." *See* PO Resp. 34; Pet. Reply ("Beser and RFC 2401 disclose this limitation under any reasonable interpretation of this phrase.").[12]

[12] Patent Owner argues in its claim construction section "a VPN communication link is a communication path between devices in a virtual private network." *See* PO Resp. 4–6. Nevertheless, apart from its encryption arguments, Patent Owner does not argue that the combination of Beser and RFC 2401 does not teach such a communication path in a VPN.

Patent Owner's arguments are not persuasive. Beser explicitly states "[o]ne method of thwarting the hacker is *to establish a Virtual Private Network ('VPN') by initiating a tunneling connection between edge routers on the public network.*" Ex. 1007, 2:6–8 (emphasis added). This not only shows a tunnel connection between edge routers over a public network is a VPN, Beser's "method . . . initiat[es] a tunneling association in a data network" that extends between "edge router[s]" over a public network. Ex. 1007, Abstract, Fig. 1, 4:19–21. Contrary to teaching away from a VPN, Beser explains "[t]he tunneled IP packets, however, *may need to be encrypted before the encapsulation in order to hide the source IP address*. Once again, *due to computer power limitations*, this form of tunneling may be inappropriate for the transmission of multimedia or VoIP packets." *Id*. at 2:12–17. This shows that Beser's tunnel scheme, a VPN, also "may" require encryption. Patent Owner acknowledges that Beser provides "a solution to some of the problems posed by VPNs." PO Resp. 31. Patent Owner also acknowledges that Beser's "method establishes a tunneling association to hide addresses within the payload of tunneled messages." PO Resp. 34 (citing Ex. 1007, 2:36–40, 9:49–51). Dr. Monrose provides no reasoned

---

No reason exists to resolve this "network" claim construction contention here Patent Owner fails to argue it is material as it relates to the prior art. In any event, Beser discloses a VPN link that includes a number of network devices (for example, 14, 16, 30, 24, 26) and a portion of a public network, so that the combination of Beser and RFC 2401 discloses or suggests a VPN link in a VPN. *See* Ex. 1007, Fig. 1. To the extent it matters, we adopt the same construction as that in the '237 FWD: "the broadest reasonable construction of a 'virtual private network communication link' is 'a secure communication link that includes a portion of a public network.'" '237 FWD 10.

explanation as to why Beser's tunnel is not a VPN, beyond asserting that Beser criticizes a VPN as "[a] form of tunneling [that] may be inappropriate for the transmission of multimedia or VoIP packets." *See* Ex. 2018 ¶ 51 (quoting Ex. 1007, 2:6–17).

In any event, even if Beser's tunnel is not a VPN or VPN communication link, allegedly because the tunnel does not explicitly include encryption, Beser at most mildly criticizes (tempered by an implied solution) a specific type of tunneling (between edge routers) that employs encapsulation and encryption of multimedia or VoIP packets—i.e., "due to computer power limitations, this form of tunneling may be inappropriate for the transmission of multimedia or VoIP packets." Ex. 1007, 2:15–17. In other words, Beser at least suggests that with adequate power or using typical data transmission rates (as opposed to higher data rates involved in some VoIP or multimedia), a tunnel (a VPN according to Beser) and encryption would be appropriate for providing security.

Therefore, and as explained further below, Petitioner shows by a preponderance of evidence that Beser and RFC 2401 suggest encryption in Beser's tunnel in order to provide data security and/or to enhance anonymity. Stated differently, Petitioner shows that Beser's system, in view of RFC 2401, at least suggests communicating encrypted data packets over the Internet on a tunnel between end devices on private networks, in order to protect the data on the Internet and in private networks for enhanced security. *See* Ex. 1007, Fig. 1 (depicting private network 20 on the requesting end); 11:62–64 ("Private IP 58 addresses are addresses that are reserved for use in private networks that are isolated from a public network

such as the Internet."); note 8 *supra* (discussing *Cisco* and physical security on private networks).

c. Reason to Combine and Encryption

Patent Owner argues that Beser and RFC 2401 would not have been combined as asserted by Petitioner to arrive at a VPN communication link—i.e., apparently a tunnel that includes encryption. *See* PO Resp. 31, 31–38 ("Petitioner turns to RFC 2401 for the teaching that data sent between two devices in a tunnel should be encrypted.") According to Patent Owner, Beser teaches away from using the IPsec protocol of RFC 2401 for audio or video data packets by explaining that streaming data flow packets, such as multimedia and VoIP, "require a great deal of computing power to encrypt or decrypt the IP packets on the fly" and the "strain of such computations 'may result in jitter, delay, or the loss of some packets.'" *Id.* at 32 (quoting Ex. 1007, 1:62–65; citing Ex. 2018 ¶ 54). Patent Owner also contends that Beser's method "hide[s] addresses [of sources and targets] within the payloads of tunneled messages . . . . to increase communication security without increasing computational burden." *Id*. at 34 (citing Ex. 1007, 2:36–40, 2:43–3:14, 9:49–51; Ex. 2015 ¶ 57).

According further to Patent Owner, "[i]f adding computing power to every computational problem was a solution, there would have been no need for Beser's tunneling solution." *Id*. at 33 (citing Ex. 2018 ¶ 55). Patent Owner also contends that "*Beser* dismisses the idea of encryption entirely, noting that the 'expense of added computer power might also dampen the customer's desire to invest in VoIP equipment' at all." *Id.* at 33 (quoting Ex. 1007, 1:65–67; citing Ex. 2018 at ¶ 55). Patent Owner also contends "*Beser*

notes the *problems* with allocating more computing power to encryption, such as 'jitter, delay, or the loss of some packets.'" *Id.* (quoting Ex. 1007, 1:60–65). Patent Owner adds further that because Beser "also teaches that encryption does not deter a determined hacker from deducing source and identity information, and so, once the tunnel is established, *Beser* eschews encryption in favor of hiding the identities within the tunnel." *Id*. at 35.

Patent Owner also contends "Beser plainly discredits the use of encryption for transmitting data over its established tunnel. Its solution, according to *Beser*, rectifies the security issues and computational burden inherent to encryption." *Id.* at 37 (citing Ex. 1007, 1:40–67, 2:43–3:9). Patent Owner concludes "one of ordinary skill in the art would have understood that Beser is directed to providing a method for securing communications *other than* encryption." *Id.* at 34 (citing Ex. 2018 ¶ 57).

Patent Owner's arguments are not supported by the record, and they unpersuasively attempt to cabin Beser's teachings to isolated passages. Beser does provide a low power solution for hiding *addresses* without encryption as Patent Owner contends, but Beser, in light of RFC 2401, also suggests using the solution of hiding addresses with high power encryption in order to protect the packet *data*. *See* Reply Br. 8 (arguing and citing supporting evidence that increasing power solves any encryption problems), 10 ("Beser never states its technique is intended to replace encryption.); Ex. 1005 ¶¶ 224–25 (persons of ordinary skill would have recognized that adding more computing power or using a lower resolution media stream solves data encryption issues addressed in Beser). Contrary to Patent Owner's arguments, an "increased *strain on computer power* [i.e., as

opposed to *increased computer power*] may result in jitter, delay, or the loss of some packets." *Id*. at 1:63–64.

In other words, Beser teaches the opposite of what Patent Owner states. Increasing power *solves*, rather than *creates*, the problems of jitter, delay, or the loss of packets. *See id.*; Ex. 1005 ¶¶ 223–226. The fact that Beser notes that adding power increases cost supports this finding and does not support Patent Owner's allegation that "Beser dismisses the idea of encryption entirely." *See* PO Resp. 33. "That a given combination would not be made by businessmen for economic reasons does not mean that persons skilled in the art would not make the combination because of some technological incompatibility. Only the latter fact would be relevant." *In re Farrenkopf*, 713 F.2d 714, 718 (Fed. Cir. 1983) (citing *Orthopedic Equip. Co. v. United States*, 702 F.2d 1005, 1013 (Fed. Cir. 1983)); *see also Muniauction, Inc. v. Thomson Corp.*, 532 F.3d 1318, 1328 (Fed. Cir. 2008) ("market-force skepticism also lacks the requisite nexus to the claimed invention" and therefore does not show non-obviousness).

Patent Owner correctly contends that Beser discusses two prior art security issues, anonymity ("address translation" or otherwise hiding addresses in packets) and data security (solved for example by encryption). *See* PO Resp. 31. Nevertheless, Patent Owner argues "*Beser* plainly discredits the use of encryption for transmitting *data* over its established tunnel. Its solution, according to *Beser*, rectifies the security issues and computational burden inherent to encryption." *Id.* at 37 (emphasis added). The latter argument contradicts Patent Owner's correct argument that "*Beser* proposes a method of *hiding the addresses* of originating and terminating devices." *Id.* at 34 (emphasis added). Beser's method of hiding *addresses*

simply does not deal with the other security issue of *data* security (by encryption), so contrary to Patent Owner's arguments, Beser's "solution" does not "rectif[y] the security issues and computational burden" of "encryption for transmitting *data* over its established tunnel." *See id.* at 37 (emphasis added); *supra* note 8 (discussing *Cisco* and the two security issues); Reply Br. 8–10.

In other words, Beser teaches a method to hide addresses that can be used with systems that either protect data using encryption or do not protect data using encryption. *See* Ex. 1007, 2:36–41. Beser does not teach an alternative to encryption for *data* security, rather, Beser teaches a method for providing *address* anonymity. *See id.* at Abs.; Reply Br. 8–10. And even if Beser does teach an alternative to *data* encryption (it does not), "[a] reference that 'merely expresses a general preference for an alternative invention but does not criticize, discredit, or otherwise discourage investigation into' the claimed invention does not teach away." *Meiresonne v. Google, Inc.*, 849 F.3d 1379, 1383 (Fed. Cir. 2017) (quoting *Galderma Labs., L.P. v. Tolmar, Inc.*, 737 F.3d 731, 738 (Fed. Cir. 2013) ("Finseth does not say or imply that text descriptions are 'unreliable,' 'misleading,' 'wrong, or 'inaccurate,' which might lead one of ordinary skill in the art to discard text descriptions completely."). The "mere disclosure of alternative designs does not teach away." *In re Fulton*, 391 F.3d 1195, 1201 (Fed. Cir. 2004).

Although Beser recognizes that the use of data encryption may cause (power) challenges, as noted above, Beser also suggests that these challenges may be overcome by providing more computer power and/or less quality (fewer packets per a normal data stream). *See* Ex. 1007, 1:60–67;

Pet. 29–32; Pet Reply 7–8 (citing Ex. 1007, 1:54–56, 2:1–8, 2:22–24, 2:43–45, 11:22–25; Ex. 1005 ¶¶ 224–228). As Petitioner notes, Dr. Monrose admitted as much. *See* Pet. Reply 8 (citing Ex. 1077, 79:3–1180:20–81:8, 82:7–17; Ex. 1055, 206:20–208:6, 211:16–212:2). Petitioner also relies on Dr. Tamassia's persuasive testimony. Pet. Reply 8 (citing Ex. 1005 ¶¶ 224–225 and summarizing Dr. Tamassia's testimony as follows: "adding more computing power or using a lower resolution media stream could solve any issues").

Beser plainly corroborates what both experts agree upon: IP packets "may need to be encrypted," but "[o]nce again, due to computer power limitations, this form of tunneling may be inappropriate for the transmission of multimedia or VoIP packets." Ex. 1007, 2:12–17. That encrypting high data rate packets "may be inappropriate" "due to computer power limitations" simply informs skilled artisans that encryption would have been advantageous for protecting lower data rate packets with less power and higher data rate packets with more power. *See* Ex. 1005 ¶¶ 224–225 (citing and discussing Beser as suggesting "simply using more powerful equipment" to handle multimedia or simply using "lower resolution video" without adding any power).

In addressing arguments by Patent Owner related to potential hacking addressed in Beser, we observed preliminarily in the Institution Decision that "it is not clear how a hacker could defeat Beser's system, whether it employs data encryption or not." Inst. Dec. 24. We further observed (preliminarily) that "[o]btaining, by decryption, a private address otherwise hidden in encrypted packets according to Beser's scheme, would not

necessarily reveal a true network address to a routine hacker, but encrypting adds a layer of data and/or address protection." *Id.*

> Responding to these preliminary observations, Patent Owner contends
>
> this only reinforces the fact that one skilled in the art would not have been motivated to add encryption to *Beser*'s system, since, if true, *there would be no reason to add encryption*. Moreover, because the purpose of the encryption in *Beser* is simply to hide address information on the public network prior to *Beser*'s tunnel establishment, once the tunnel is created, the originating and terminating device information is hidden and *encryption would not only be redundant, it would contravene Beser's express objective of increasing security without increasing computational burden*.

PO Resp. 35–36 (citing Ex. 2018 ¶ 60) (emphases added).

Again, this response by Patent Owner conflates the two security issues (anonymity and data security) that the '696 patent and *Cisco* show clearly consist of two distinct (and well-known) aspects of communications security. *See* Ex. 1001, 1:35–36 ("A tremendous variety of methods have been proposed and implemented to provide security and anonymity for communications over the Internet."); *Cisco*, 767 F.3d at 1317–18 ("Security in this context refers to protection of data itself, to preserve the secrecy of its contents, while anonymity refers to preventing an eavesdropper from discovering the identity of a participating terminal.") (discussing background art as disclosed in a related VirnetX patent); *supra* note 8 (discussing *Cisco*). As Patent Owner notes, Beser provides a solution to hiding addresses and in one embodiment uses encryption to hide public addresses during the tunnel set up process. PO Resp. 35. But contrary to Patent Owner's arguments, the reason to add encryption to protect *data* in the tunnel still exists even in the tunnel process for hiding *addresses*, and encryption of data was notoriously

well known at the time of the invention, as RFC 2401, Beser, and the '696 patent all make clear. *See* Ex. 1001, 1:57–58 ("Data security is usually tackled using some form of data encryption. . . . Many encryption methods are known."); Ex. 1008, 7 ("one can create a single encrypted tunnel to carry all the traffic between two security gateways"); Ex. 1007, 2:23–24 (discussed next).

Beser makes a desire for encryption clear by specifically characterizing some prior art systems as creating "*security problems by preventing certain types of encryption from being used*." Ex. 1007, 2:23–24 (emphasis added). In other words, Beser does not discourage encrypting data to make it secure; rather, Beser provides a solution for providing anonymity by using a tunnel technique with or without encryption of data. *See* Ex. 1007, 2:36–41 (describing "hiding the identities" in tunnels as an object of the invention). Patent Owner's argument that Beser's address hiding method avoids computationally expensive prior art network address translation methods similarly has nothing to do with providing data security, as Petitioner argues. *See* PO Resp. 33–34; Pet. Reply 9–10 ("Because of its low computational burden, Beser's method is flexible and can be combined with other security techniques.") As Petitioner persuasively adds, Beser's address hiding tunnel method, combined with known IPsec flexible encryption methods (as taught by Beser and RFC 2401), obviously would have aided in preventing packet accumulation that Beser explains hackers need to decrypt the data. *See* Pet. Reply 9–10 (citing Ex. 1005 ¶¶228–34; Ex. 1007, 2:3–40, 3:4–9, 4:55–5:2).

Petitioner also contends "as explained in the petition and by Dr. Tamassia, a person of ordinary skill in the art would have found it obvious to

combine Beser and RFC 2401 to provide end-to-end encryption in an IP tunnel between Beser's originating and terminating end devices. Pet. Reply 6 (citing Pet. 31–35; Ex. 1005 ¶¶228–34). Patent Owner does not argue the point—i.e., does not argue the challenged claims require end-to-end encryption. Under the rationale of *Cisco* (*supra* note 8), these challenged claims do not require end-to-end encryption, and Beser's private networks at least suggest that the private networks provide physical security as part of the VPN tunnel. *See Cisco*, 767 F.3d at 1322 ("Virnetx provided substantial evidence for the jury to conclude that paths beyond the VPN server may be rendered secure and anonymous by means of 'physical security' present in the private corporate networks connected to the by VPN On Demand."); Ex. 1007, Fig. 1 (depicting private network 20 on the origination end); 11:62–64 ("*Private IP 58 addresses are addresses that are reserved for use in private networks that are isolated* from a public network such as the Internet." (Emphasis added)); Ex. 1005 ¶¶228–34.

Even if the claims require end-to-end encryption (i.e., encryption of data on the public portion of Beser's tunnel and also within Beser's private networks 20), Petitioner shows such an extra layer of security would have been obvious in order to ensure data security. *See* Pet. 31–35; Ex. 1005 ¶ 230 (providing credible testimony that encryption would have been obvious "between a first and second network device or between the two end devices"), ¶¶ 228–34 (providing a foundation that the combination suggests either tunnel or end-to-end encryption to enhance security over the whole path); Reply Br. 6–7. Petitioner's point is persuasive, because in the event a hacker or other nefarious listener breaches Beser's private networks 20, an extra layer of security via encryption would protect the data. *See* Ex. 1005

¶ 231 (testifying that RFC 2401 discloses end-to-end and tunnel encryption) (citing Ex. 1008, 25), ¶ 238 (discussing how the combination would be configured for end-to-end encryption).

In summary, Petitioner presents persuasive reasons supporting its showing that a person of ordinary skill would have found it obvious to combine the teachings of RFC 2401 with Beser to encrypt data in order to enhance security in a tunnel and beyond the tunnel, based on a determination that a requested target device would have been available for secure communications. Petitioner also sets forth a sufficient rationale showing that Beser's combined system includes or suggests using a typical DNS functionality or similar look up techniques to help determine that a requested end device is available for secure communications by, among other things, associating that end device with a private and/or public IP address. Based on the foregoing discussion and a review of the record, we determine that Petitioner demonstrates by a preponderance of evidence that the combination of Beser and RFC 2401 would have rendered claims 1 and 16 obvious.

4) Claims 2, 3, 17, and 18

Claims 3 and 18 depend respectively from 2 and 17, which depend respectively from claims 1 and 16. Claims 3 and 18 (including the limitations of 2 and 17), further require encryption of data on an audio-video service (i.e., of at least one of video and audio data). Petitioner and Patent Owner essentially rely on their positions regarding the alleged obviousness of providing video or audio data encryption in Beser's system as suggested further by RFC2401, wherein Beser's system provides multimedia devices such as Web-TV and VoIP services. *See* Ex. 1007, 4:47–49; Pet. 45–46; PO Resp. 38–39; Pet. Reply 18–19 (citing Ex. 1005 ¶¶ 224–225). In other

words, these challenged claims require encryption of "audio data" within an "audio-video conferencing service" without any specified audio data rate. In any event, as Dr. Tamassia's credible testimony shows, "[a] person of ordinary skill in the art would recognize that the concerns expressed in Beser in connection with encryption of high volumes of network traffic [i.e., multimedia] can be easily resolved by simply using more powerful equipment." *See* Ex. 1005 ¶ 225.

In addition,

> [a] person of ordinary skill in the art reading Beser in February 2000 would also have understood that encryption should ordinarily be used even in high data volume applications, if possible. Beser only warns that it *may* not be possible to encrypt every packet and maintain transmission quality due to computer power limitations (*e.g.*, during times of high network traffic). Ex. 1007 at 1:62–67, 2:15–17. Beser refers to the use of encryption in IP tunneling schemes as a conventional technique that is ordinarily used. *See* Ex. 1007 at 1:54–56, 2:12–14.

Id. ¶ 224.

As indicated above, the resolution of these claims tracks that of claims 1 and 16. Based further on the discussion of claims 1 and 16 above, which applies here, and the respective positions of the parties, we determine that Petitioner shows by a preponderance of evidence that claims 2, 3, 17, and 18 would have been obvious based on the combination of Beser and RFC 2401.

5) Claims 4, 5, 19, and 20

Claims 4 and 19 depend respectively from claims 1 and 16 and recite "wherein the secure communications service includes a messaging service." Claims 5 and 20 respectively depend from claims 4 and 19, and further recite that "wherein the messaging service includes an e-mail service."

Petitioner contends that using e-mail in Beser's system would have been obvious "because it already transmits other types of communication data such as audio and video." Pet. 47. Petitioner points out that "Beser explains that the unique identifier included in a request can be an email address." Pet. 47 (citing Ex. 1007, 10:55–11:5; Ex. 1005 ¶ 129). Petitioner also contends that "Beser . . . explains that a variety of originating and terminating end devices are compatible with its methods, including telephony and multimedia devices, and that 'the ends of the data flow may be other types of network devices.'" Pet. 47 (citing Ex. 1007, 4:43–54; Ex. 1005 at ¶¶ 139–43). Petitioner cites another prior art document as evidence to show that "[t]ransmitting email over a secure communication link or VPN was well-known at the time of the invention." *Id*. (citing Ex. 1052, Figs. 5A, 5B, 12:11–23).

Patent Owner contends that Petitioner's showing is insufficient as it merely relies on "'an obvious design choice' without any analysis or evidence as to how a 'messaging service' or 'e-mail service' would be included in *Beser*'s tunneling scheme or what the results of such a modification would be." PO Resp. 40. Patent Owner also contends "[a] 'simple substitution' obviousness rationale requires, *inter alia*, a showing that the results of the substitution would have been predictable." *Id.* (citing *KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 416 (2007)). Patent Owner also contends that *Beser* suggests using an e-mail address for things *other than* an e-mail." *Id.* at 40–41.

Although Patent Owner cites to *KSR*, Patent Owner does not contend that sending e-mail on an encrypted tunnel would have been unpredictable. *See id.* Contrary to Patent Owner's arguments, Petitioner presents, as

summarized above, a persuasive rationale of a simple substitution of sending one type of data for another in a known application for the purpose of making the similar application data secure. As Petitioner contends, Beser and RFC 2401 suggests encrypting multimedia, telephony, audio, video, and all types of data, so that transmitting encrypted e-mail data would have been predictable and easily within the grasp of an ordinary artisan for the simple purpose of providing another type of secure data communication, as the references fairly suggest in disclosing IPsec. *See* Ex. 1005 ¶ 165 ("Email is a type of data like audio and video, and transmitting it via Beser's secure IP tunnel would protect it in the same way."); Pet. 47; Ex. 1008, 4–8 (IPsec encryption); *supra* Section II.D.1, 2 (discussing IPsec teachings in each of Beser and RFC 2401)

Petitioner also establishes persuasively that Beser further discloses or suggests using e-mail services by disclosing "that the unique identifier is an electronic mail address." Ex. 1007, 10:55–11:5; Pet. 47 (also citing Ex. 1052, Fig. 5A–B (stating the reference "show[s] a messaging server being accessed via VPN and IPsec"), 12:11–23 (stating it "describ[es] messaging servers providing email applications")). As Petitioner contends, Exhibit 1052 constitutes further evidence of ordinary skill in the art concerning the known use of an e-mail application and/or data on a VPN. *See* Pet. 47–48 (citing Ex. 1005 ¶¶ 139–143, 165; Ex. 1052).

Based on the foregoing discussion, Petitioner demonstrates by a preponderance of evidence that claims 4, 5, 19, and 20 would have been obvious based on the combination of Beser and RFC 2401.

6) Claims 6–11, 14, 15, 21–25, and 28–30

Relying partially on the Tamassia Declaration, Petitioner presents an articulated rationale and a detailed mapping of claim elements, in its showing that the combination of Beser and RFC 2401 would have rendered obvious claims 6–11, 14, 15, 21–25, and 28–30. *See* Pet. 48–58. As Petitioner shows, by way of summary, these claims simply add known subject matter elements involving communication services, such as for example, a "telephony service," a "mobile device," a "notebook computer," known modulation types (FDM or TDM), or other similar subject matter. *See* 48–51 (addressing the limitations persuasively). Claims 11 and 29 recite "receiving the request to determine whether the second network device is available for the secure communication service." Similar to its showing with respect to claims 1 and 16, Petitioner persuasively relies on Beser's unique identifier as a part of a request that the trusted-third-party network device uses to determine if terminating device 26 is available for the secure service. *See* Pet. 51–52. In similar vein, claims 14, 15, and 28–30 track limitations that are materially similar to recited elements in claims 1 and 16. Petitioner's showing related to claims 1 and 16 overlaps its showing with respect to these claims, and Petitioner also shows separately and persuasively that Beser and RFC 2401 would have rendered the subject matter of these claims obvious. *See* Pet. 53–55 (addressing limitations related to a domain look up, a separate intercepting server, and receiving the request to make the recited determination).

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. In response, Patent Owner relies on its arguments presented with respect to claims 1 and 16. *See* PO Resp. 42. We informed Patent Owner "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 that claims 6–11, 14, 15, 21–25, and 28–30 would have been obvious based on the combination of Beser and RFC 2401.

E. COLLATERAL ESTOPPEL

Petitioner contends Patent Owner is estopped from re-litigating identical issues involved in the '237 FWD (and other cases affirmed by our reviewing court). *See supra* notes 1, 2; Pet. Reply 2 ("Patent Owner is precluded from taking positions in this proceeding that are inconsistent with the final judgment in those proceedings."). Patent Owner responds that 37 C.F.R. § 42.73(d)(3) does not act as a prohibition against arguments to defend a patent in an IPR proceeding and the conditions for common law estoppel are not met. *See* Paper 18, 1–3.

Given our holding herein and in companion Case IPR2016-00332, no need exists to address collateral estoppel, as we have determined that the challenged claims are unpatentable.

III. PATENT OWNER'S MOTION TO EXCLUDE

Patent Owner seeks to exclude Exhibits 1010–12, 1014–18, 1020–31, 1037, 1043, 1054, 1060, and 1063–65 and portions of Exhibit 1005. Paper 20, 1 ("Motion"). 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 is *dismissed* as *moot* in part and *denied* in part.

1. Exhibits 1060 and 1063–65

Patent Owner moves to exclude Exhibits 1060 and 1063–65 as inadmissible hearsay. Paper 20, 2. Exhibit 1060 is a declaration originally submitted in litigation before the International Trade Commission. Ex. 1060. It contains testimony from Sandy Ginoza, a representative of IETF, in support of Petitioner's contention that RFC 2401 qualifies as a printed publication as of November 1998. *Id.* Exhibit 1063 is a "transcript of Ms. Ginoza's February 8, 2013 deposition that was taken as part of the ITC action." Paper 20, 2 (citing Pet. 25–27). Exhibits 1064 and 1065 are both magazine articles dated 1999 that relate to the same issue. *See* Paper 17, 7–8. Because we do not rely Exhibits 1060 and 1063 to decide the issue of whether RFC 2401 qualifies as a printed publication, we dismiss the motion as to these Exhibits as moot.

Patent Owner does not explain why Exhibits 1064 and 1065 are hearsay or what part of them constitute hearsay. *See* Paper 20, 5. Exhibit 1064 states "all of these documents [including RFC 2401] are available on the ETF Web site: www.left.org/rfc.html." Ex. 1064, 7; *see* Pet. 26 (relying on the statement and a 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/rfc/rfc2411.text." Ex. 1065, 3. Petitioner contends these statements are not employed for the truth that the documents actually are available on the website:

> 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, 2 n. 1 (citing Reply Br. 21; 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"); *accord* Reply Br. 21 n. 6 ("These articles show that the skilled person would have known that RFCs such as RFC 2401 could be downloaded from the IEFT's website.").

Petitioner's argument is persuasive. Patent Owner has not met its burden of explaining why Exhibits 1064 and 1065 must be excluded as hearsay. Petitioner offers the articles to show that skilled artisans believed the RFC 2401 document was available at the time of its publication. Patent Owner does not challenge the publication dates of the magazines of the articles as hearsay. As noted, Patent Owner does not state what aspects of the documents are hearsay. *See* Paper 20; Paper 24 n.1 (Patent Owner "disagrees" with Petitioner). 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). 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.

2. Exhibits 1010–12, 1014–18, 1020–31, 1037, 1043, and 1054

Patent Owner seeks to exclude the above-listed Exhibits as lacking relevance. Paper 30, 1, 5–6. Because we do not rely on any of the Exhibits

listed above, Patent Owner's Motion to Exclude 1010–12, 1014–18, 1020–31, 1037, 1043, and 1054, is dismissed as moot.

III. CONCLUSION

For the foregoing reasons, Petitioner establishes by a preponderance of evidence that claims 1–11, 14–25, and 28–30 of the '696 patent are unpatentable for obviousness.

IV. ORDER

In consideration of the foregoing, it is hereby

ORDERED that claims 1–11, 14–25, and 28–30 of U.S. Patent No. 8,504,696 B2 are unpatentable;

FURTHER ORDERED that Patent Owner's Motion to Exclude is *dismissed as moot* with respect to Exhibits 1010–1012, 1014–1018, 1020–1031, 1037, 1043, 1054, 1060, and 1063 and is *denied* with respect to Exhibits 1064 and 1065;

FURTHER ORDERED that, because this Final Written Decision is final, a party 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