Paper No. _____
Filed: December 11, 2015

Filed on behalf of: VirnetX Inc.
By:

Joseph E. Palys
Paul Hastings LLP
875 15th Street NW
Washington, DC 20005
Telephone: (202) 551-1996
Facsimile: (202) 551-0496
E-mail: josephpalys@paulhastings.com

Naveen Modi
Paul Hastings LLP
875 15th Street NW
Washington, DC 20005
Telephone: (202) 551-1990
Facsimile: (202) 551-0490
E-mail: naveenmodi@paulhastings.com

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

APPLE INC.
Petitioner

v.

VIRNETX INC.
Patent Owner

Case IPR2015-00812
Patent 8,850,009

Patent Owner's Response

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Cases

Statutes

Other Authorities

I. Introduction

Patent Owner VirnetX Inc. respectfully submits this Response to the Board's decision to institute *inter partes* review (Paper No. 8, the "Decision") and to the petition for *inter partes* review (the "Petition" or "Pet.") filed by Petitioner Apple Inc. The Board instituted review of claims 1-8, 10-20, and 22-25 of U.S. Patent No. 8,850,009 ("the '009 patent") as obvious over *Beser* and RFC 2401. Apple has not carried its "burden of proving . . . unpatentability by a preponderance of the evidence" (35 U.S.C. § 316(e)) because the asserted references fail to disclose each of the claimed features. In addition, Apple has failed to show that RFC 2401 is a prior art printed publication. Apple's submitted expert testimony should also be given little to no weight because it fails to describe how any of the claim features are taught or suggested in the asserted references. Accordingly, the Board should enter judgment against Apple and terminate this proceeding.

II. Claim Construction

The Petition identified nine terms for construction. In its Preliminary Response, Patent Owner addressed Petitioner's constructions. The Decision did not provide a construction for any of the terms, finding that "no claim term needs express interpretation." (Decision at 6.) Patent Owner respectfully disagrees and addresses the terms below under the broadest reasonable interpretation (BRI) standard.

In *inter partes* review, claims are to be given their "broadest reasonable construction in light of the specification." 37 C.F.R. § 42.100(b). Although VirnetX's constructions represent the BRI of the claims in light of the specification and prosecution history, the Board should apply the claim construction standard applied by the courts, especially given the litigations and prosecution histories of the patents in the same family as the '705 patent. The BRI standard "is solely an examination expedient, not a rule of claim construction." *In re Skvorecz*, 580 F.3d 1262, 1267-68 (Fed. Cir. 2009). It is certainly justified during the examination process because applicant has the opportunity to amend the claims during prosecution. *In re Yamamoto*, 740 F.2d 1569, 1571 (Fed. Cir. 1984). But, as the Board has noted, *inter partes* review is not an examination and is "more adjudicatory than examinational, in nature." *Idle Free Sys., Inc. v. Bergstrom, Inc.*, IPR2012-00027, Paper No. 26 at 6 (June 11, 2013).

The ability to amend claims during *inter partes* review is so severely restricted that the rationale underpinning the BRI—the ability to freely amend claims—does not apply especially given the litigations and prosecution histories of patents in the same family as the '009 patent. As a result, to the extent the Board would have adopted a narrower construction under the courts' claim construction standard than it has adopted here, it should adopt the narrower construction because the BRI standard should not apply to this proceeding.

The Court of Appeals for the Federal Circuit refused to reconsider *en banc* the application of the BRI standard in Board proceedings. *In re Cuozzo*, 793 F.3d 1297 (Fed. Cir. 2015). VirnetX nevertheless respectfully submits that, given "the adjudicative nature and the limited amendment process of IPRs," claims in IPR proceedings should be given their "actual meaning." *Id.* at 1299, 1301-02 (Prost, C.J., dissenting from denial of *en banc* rehearing). VirnetX preserves this argument in the event the Supreme Court grants review of the Federal Circuit's decision in *Cuozzo* and instructs that a different standard should be applied. *See* Pet'n for a Writ of Certiorari, *Cuozzo Speed Techs., LLC v. Lee*, No. 15-446, 2015 WL 5895939 (Oct. 6, 2015).

A. "Domain Name Service (DNS) Request" (Claims 1, 12-14, 24 and 25)[1]

Patent Owner's Proposed Construction	Petitioner's Proposed Construction	Decision's Construction
A request for a resource corresponding to a domain name	A request for a resource corresponding to a domain name	No construction proposed

As noted, in Patent Owner's preliminary response, the parties' proposed constructions are the same. (*See* Prelim. Resp. at 24; *see also* Ex. 2016 at ¶ 31.)

[1] Patent Owner identifies only the challenged claims that expressly recite the terms at issue. Claims that depend from the identified claims may also implicitly contain the terms.

B. "Interception of the DNS Request" (Claims 1, 12-14, 24, and 25)

Patent Owner's Proposed Construction	Petitioner's Proposed Construction	Decision's Construction
No construction necessary; alternatively, 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 an encrypted communication link	Receiving a DNS request pertaining to a first entity at another entity	No construction proposed

Though the Board declined to preliminarily construe this term, if the Board later deems construction necessary, it should adopt Patent Owner's construction because Petitioner's proposed construction does not reflect the appropriate construction in view of the specification. Petitioner's proposed construction for the "intercept[ing]" phrase (Pet. at 11) is similar to a construction that the Board adopted in a related proceeding. *Apple Inc. v. VirnetX Inc.*, IPR2014-00237, Paper No. 15 at 12-13 (May 14, 2014).

As explained in Patent Owner's Preliminary Response, Patent Owner's alternative construction appropriately captures the notion of performing an additional evaluation on a request to look up an IP address related to establishing an encrypted communications channel, beyond conventionally resolving it and returning the address. (Prelim. Resp. at 25-28; *see also* Ex. 2016 at ¶ 31.) The

independent claims support this construction, for example, by reciting that a determination is made that the request to look up the network address corresponds to a device that is available for the secure communications service, and that "following" this determination, provisioning information required to initiate the encrypted communication link is provided. (Ex. 1003, claims 1 and 14.) Additionally, dependent claims 12 and 24 expressly specify the evaluation, reciting that the "interception" involves "receiving the DNS request to determine that the second network device is available for the secure communications service." (Ex. 1003, claims 12 and 24.)

C. "Encrypted Communication Link" Phrases (Claims 1, 2, 8, 11, 14, 15, and 23)

Patent Owner's Proposed Construction	Petitioner's Proposed Construction	Decision's Construction
A direct communication link that is encrypted	A transmission path that restricts access to data, addresses, or other information on the path at least by using encryption	No construction proposed

Independent claims 1 and 14 of the '009 patent recite an "encrypted communication link" and more specifically recite that the network device "connect[s] to the second network device over the encrypted communication link." (Ex. 1003, claims 1 and 14.) Thus, in the context of the '009 patent claims, the encrypted communication link is a direct communication link that is encrypted. Petitioner attempts to construe "encrypted communication link" in isolation.

However, "encrypted communication link" can only be understood with its surrounding claim language.

The '009 patent describes encrypted communications that are direct between a first and second device. For instance, in one embodiment, the '009 patent describes the link between an originating TARP terminal and a destination TARP terminal as direct. (*See, e.g.,* Ex. 1003, 10:16-25, Fig. 2; *see also id.* at 34:13-20 (describing a variation of the TARP embodiments as including a direct communication link); 38:42-45 (describing the embodiment of Figure 24 in which a first computer and second computer are connected directly).) The '009 patent similarly describes direct encrypted communications in later embodiments as well. (*See, e.g., id.* at 40:45-48, 41:39-42 (describing a virtual private network as being direct between a user's computer and target), 42:49-53, 43:42-46 (describing a load balancing example in which a virtual private network is direct between a first host and a second host), 49:44-46, 49:55-67 (describing a secure communication link that is direct between a first computer and a second computer), Figs. 24, 26, 28, 29, 33 Ex. 2016 at ¶¶ 15-16.)

In each of these embodiments, the '009 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. (*See, e.g.,* Ex. 1003 at Figs. 2, 24, 28, 29, 33; Ex. 2016 at ¶ 17.) In

litigation, Petitioner and its co-defendants recognized that this type of network traversal is a "direct" communication. (*See* Ex. 2003 at 42:16-21, 44:17-45:12, Markman Hearing Transcript in the '417 litigation (E.D. Tex. Jan. 5, 2012); *see also id.* at 44:13-45:12, Markman Hearing Transcript in the '417 litigation (E.D. Tex. Jan. 5, 2012) (Petitioner explaining that the claims should be limited to "direct" communication because the specification teaches direct communication between the client and target).)

In view of Petitioner's arguments and the patent specification, both a district court, (Ex. 2004 at 8, 13, Memorandum Opinion and Order in the '417 litigation), and the Federal Circuit construed the related terms "secure communication link" and "virtual private network" to include "direct" communication. *VirnetX Inc. v. Cisco Sys. Inc.*, 767 F.3d, 1317 n.1, 1319 (Fed. Cir. 2014). Accordingly, under the applicable BRI standard, and in light of the language of the '009 patent claims, the Board should construe the "encrypted communication link" as a "direct communication link that is encrypted."

D. "Provisioning Information" (Claims 1 and 14)

Patent Owner's Proposed Construction	Apple's Proposed Construction	Decision's Construction
Information that is used to establish an encrypted communication link	Information that enables communication in a virtual private network, where the virtual private network uses encryption	No construction proposed

In a related proceeding involving a related patent, IPR2015-00811 ("the '811 proceeding"), the Board preliminarily construed "provisioning information" to be "information that is provided to enable or aid in establishing a secure communications channel." *Apple Inc. v. VirnetX Inc.*, IPR2015-00811, Paper No. 8 at 9 (Sept. 11, 2015). In doing so, it recognized that "[t]he claims do not recite or implicate in any way explicitly a VPN," contrary to Petitioner's proposed construction. *Id.* Here too, there is nothing in the claims, specification, or prosecution history that indicates that "encrypted communication link" has a special, narrower meaning or associated disclaimer that requires a virtual private network. (*See* Prelim. Resp. at 28-31.)

The Board's substitution of "*secure* communications channel" for the recited "*encrypted* communications channel" in that proceeding also cannot stand, however. Indeed, the claims here repeatedly refer to an "*encrypted* communication link."[2] (Ex. 1003, claims 1 and 14 (reciting "provisioning information for an encrypted communication link").)

The Board's construction in the '811 proceeding is also overly broad in that it encompasses any information that "enables or aid[s] in" communication using a

[2] This is distinction is significant given the Board's previous findings in related proceedings that security does not require encryption. *See, e.g., Apple Inc. v. VirnetX Inc.*, IPR2014-00237, Paper No. 41 at 5-8 (May 11, 2015).

secure communications channel, even if that information has nothing to do with provisioning. For example, it would encompass source and destination information for individual packets of data that are traveling over a pre-existing channel. While this type of information may "enable or aid in" communication using an encrypted communication link, it has no relationship to the traditional notions of provisioning or the portions of the '009 patent. (Ex. 2016 at ¶¶ 18-19.)

As discussed in the Preliminary Response, Patent Owner's construction is more consistent with the general notion that provisioning refers to setting up or establishing a connection or service. As the Board noted, one dictionary explains that provisioning is "[s]etting up a telecommunications service for a particular customer," and that "[c]ommon carriers provision circuits by programming their computers to switch customer lines into the appropriate networks." *Apple*, IPR2015-00811, Paper No. 8 at 9 (citing Ex. 2007 at 6, *McGraw-Hill Computer Desktop Encyclopedia* (9th ed. 2001).). Applying these principles to provisioning in the context of the '009 patent, encrypted communication link provisioning refers to setting up or establishing an encrypted communication link—not merely the sending of any and all information that may "enable or aid in" communication. Indeed, one of ordinary skill in the art[3] would not have understood a link to be

[3] 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 and approximately

provisioned every time a data packet is sent across it, but the Decision's construction in the '811 proceeding inaccurately encompasses this scenario. (Ex. 2016 at ¶ 20); *see Microsoft*, 789 F.3d at 1298 (explaining that a construction is "unreasonably broad" where it is not "consistent with the one that those skilled in the art would reach") (citation omitted).

Accordingly, the BRI of "provisioning information" means "information that is used to establish an encrypted communications channel."

E. "Secure Communications Service" (Claims 1-3, 10, 12, 14-16, 22, and 24)

Patent Owner's Proposed Construction	Petitioner's Proposed Construction	Decision's Construction
The functional configuration of a network device that enables it to participate in a secure communications link with another network device	The functional configuration of a network device that enables it to participate in a secure communications link with another computer or device	No construction proposed

As discussed in Patent Owner's Preliminary Response, the parties generally agree on the construction of "secure communications service," though Petitioner's proposed use of "computer" should instead be replaced with "network device." (*See* Prelim. Resp. at 34; *see also* Ex. 2016 ¶ 31.)

---

two years of experience in computer networking and computer security. (Ex. 2016 at ¶ 13; *see also id.* at ¶¶ 4-12.)

F. "Indication" (Claims 1, 10, 14, and 22)

Patent Owner's Proposed Construction	Petitioner's Proposed Construction	Decision's Construction
No construction necessary	Something that shows the probable presence or existence or nature of	No construction proposed

As noted in Patent Owner's Preliminary Response, Patent Owner agrees that the Board need not construe this term. (*See* Prelim. Resp. at 35-36; *see also* Ex. 2016 at ¶ 31.) In any event, Petitioner's construction is inconsistent with the express language of the claims and introduces ambiguity. (Pet. at 15-16.) The claims require that the "indication" is that the "the second network device is available for the secure communications service." Something that does nothing more than show the "probable presence" or mere "existence" of the second network device is not an indication that the device "is available **for the secure communications service**." Petitioner's construction reads this feature out of the claims and should be rejected. Moreover, Petitioner's construction introduces ambiguities where none exist with the term. For instance, Petitioner does not explain what would entail a "probable presence" of something, and does not show how such a conditional feature is found in the claims or specification of the '009 patent.

G. "Virtual Private Network Communication Link" (Claim 8)

Patent Owner's Proposed Construction	Petitioner's Proposed Construction	Decision's Construction
A communication path between two devices in a virtual private network	A transmission path between two devices 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 authentication, encryption, or address hopping	No construction proposed

As discussed in the preliminary response, the plain meaning of a "virtual private network communication link" (or "VPN communication link") in view of the specification is "a communication path between two computers 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. (Prelim. Resp. at 36-46; *see also* Ex. 2016 at ¶ 21.) Petitioner's proposed construction contradicts the plain language of the claims, is internally inconsistent, and is inconsistent with the '009 specification and prosecution history.

1. A "VPN Communication Link" Does Not Exist Outside of a Virtual Private Network

Petitioner's proposed construction does not require that the virtual private network communication link be between devices in a virtual private network. However, the '009 patent discloses that a VPN communication link is a communication path between computers in a virtual private network. (Ex. 2016 at ¶ 22.)

As explained in the '009 patent, a VPN communication link does not exist outside of a virtual private network. For example, when a secure domain name service (SDNS) receives a query for a secure network address, it "accesses VPN gatekeeper 3314 for establishing a VPN communication link between software module 3309 [at the querying computer 3301] and secure server 3320." (Ex. 1003 at 52:7-9.) Then, "VPN gatekeeper 3314 provisions computer 3301 and secure web server computer 3320 . . . thereby creating the VPN" between the devices. (Ex. 1003 at 52:10-13, emphasis added.) Notably, secure server 3320 "can only be accessed through a VPN communication link." (Ex. 1003 at 52:9-10.) And "[f]urther communication between computers 3301 and 3320 occurs via the VPN" through the VPN communication link. (Ex. 1003 at 52:40-42; Ex. 2016 at ¶ 22.)

Patent Owner's adversaries and their experts agree that a VPN communication link refers to a link in a virtual private network. Specifically, Petitioner itself has understood and construed a VPN communication link to be

"any communication link between two end points in a virtual private network." (*See, e.g.*, IPR2014-00481, Paper No. 1 at 6 (Mar. 7, 2014).) In district court, Microsoft proposed a similar construction requiring the link to be in a virtual private network. (Ex. 2001 at 25, Memorandum Opinion in *VirnetX Inc. v. Microsoft Corp.*, Case No. 6:07-CV-80 (E.D. Tex. Jul. 30, 2009), a "communication link in a virtual private network.") There, the court relied on its construction of VPN, finding it unnecessary to separately construe VPN communication link, suggesting that a VPN communication link is not separate from a VPN. (*Id.* at 25-26.)

Thus, parties and courts have universally understood that a VPN communication link exists in a VPN. This is the BRI, and Petitioner's proposed construction incorrectly deviates from this understanding.

2. "Authentication" and "Address Hopping" Alone Do Not Result in a "Virtual Private Network Communication Link"

Petitioner's proposed construction is also internally inconsistent and technically flawed. Of the obfuscation methods in the proposed construction—authentication, encryption, and address hopping—only encryption restricts access to "data, addresses, or other information on the path," as required by the first portion of the construction. (Ex. 2016 at ¶ 23.) The other techniques alone do not "hide information on the path," as Petitioner's construction requires. (Ex. 2016 at ¶ 23.)

Authentication merely "[e]nsur[es] that a message originated from the expected sender and has not been altered on route." (Ex. 2008 at 3, Glossary for the Linux FreeS/WAN Project.) It does not prevent an eavesdropper from accessing data transmitted over an unsecure communication link. (Ex. 2016 at ¶ 24.) The specification supports this fact by describing at least one scenario where an authenticated transmission occurs "in the clear"—i.e., over an unsecured communication link:

> SDNS [secure domain name service] 3313 can be accessed through secure portal 3310 "in the clear", that is, without using an administrative VPN communication link. In this situation, secure portal 3310 preferably authenticates the query using any well-known technique, such as a cryptographic technique, before allowing the query to proceed to SDNS [3313].

(Ex. 1003 at 52:21-26.)

Address hopping alone also does not provide the claimed security, as there is nothing inherent in moving from address to address that hides information on the path or precludes an eavesdropper from reading the details of a communication. (Ex. 2016 at ¶ 25.) This is why the '009 patent discloses embodiments that use encryption in conjunction with address hopping to protect, for example, the next address in a routing scheme from being viewed by eavesdroppers. (*See, e.g.*, Ex. 1003 at 3:40-54, stating in part that "[e]ach TARP packet's true destination is

concealed behind a layer of encryption generated using a link key.") It is the encryption that hides information on the path while moving from address to address. (*See, e.g.*, Ex. 1003 at 3:20-4:44; Ex. 2016 at ¶ 25.)

While authentication and address hopping may be used in conjunction with encryption as an "obfuscation method," this fact does not make them sufficient by themselves to "hide information on the path," as Petitioner's construction requires. (Ex. 2016 at ¶ 26.) Because Petitioner's construction presents them as alternatives, allowing each to be sufficient, Petitioner's construction must be rejected.

3. A "Virtual Private Network Communication Link" Must Be Direct

Petitioner's construction incorrectly encompasses links that are not direct. As discussed above with respect to the claimed "encrypted communication link," the '009 patent "repeatedly and consistently" describes its secure links as "direct" between a client and target device. *See supra* Section II.C; (Ex. 2016 at ¶ 27). The prosecution history of related VirnetX patents supports this understanding.

During both the original prosecution and the now-completed reexamination of related VirnetX patents, VirnetX clearly and unambiguously disclaimed any virtual private networks and virtual private network communication links that are not direct. (*See, e.g.*, Ex. 2006 at 6-9, Office Action Response filed January 10, 2011, in application no. 11/839,987; Ex. 2011, Office Action Response filed April 15, 2010, in control no. 95/001,269 at 7.) Referring to *Aventail*, a reference now

asserted in Petitioner's co-pending petition in IPR2014-00813, Patent Owner explained that the reference did not disclose a VPN because, among other things, "computers connected according to *Aventail* do not communicate directly with each other." (*See* Ex. 2006 at 8, Office Action Response filed January 10, 2011, in application no. 11/839,987; Ex. 2011, Office Action Response filed April 15, 2010, in control no. 95/001,269 at 7.)

In district court, Petitioner and other defendants agreed that Patent Owner's disclaimer is clear, describing Patent Owner's statements as a "clear mandate to the Patent Office that computers in a 'virtual private network' communicate directly with each other, and that absent direct communication between the computers, there is no virtual private network." (Ex. 2002 at 5, Defendants' Responsive Claim Construction Brief in the '417 litigation.) A disclaiming statement is unambiguous when "a competitor would reasonably believe that the applicant had surrendered the relevant subject matter." *Cyber Corp. v. FAS Techs., Inc.*, 138 F.3d 1448, 1457 (Fed. Cir. 1998). Here, VirnetX's disclaimer "show[s] reasonable clarity and deliberateness." *Biogen Idec, Inc. v. GlaxoSmithKline LLC*, 713 F.3d 1090, 1096 (Fed. Cir. 2013) (citation omitted). Given Patent Owner's statements, the district court found disclaimer and required the claimed VPN to include direct communication. (Ex. 2004 at 6-8, Memorandum Opinion and Order in the '417 litigation (E.D. Tex. Apr. 25, 2012).)

There is no reason the Board should find any differently here. Indeed, the Board has relied on prosecution history statements in construing claims in numerous other *inter partes* reviews. *See, e.g., Garmin Int'l inc. v. Cuozzo Speed Tech, LLC*, IPR2012-00001, Paper No. 15 at 8 (Jan. 9, 2013); *Motorola Solutions, Inc. v. Mobile Scanning Techs., LLC*, IPR2013-00093, Paper No. 28 at 10 (Apr. 29, 2013); *ZTE Corp. & ZTE (USA) Inc. v. ContentGuard Holdings Inc.*, IPR2013-00134, Paper No. 12 at 16 (June 19, 2013); *Xilinx, Inc. v. Intellectual Ventures I LLC*, IPR2013-00112, Paper No. 14 at 6 (June 27, 2013).

Furthermore, the Federal Circuit noted that virtual private network and secure communication links require direct communication. It stated 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." *VirnetX, Inc.*, 767 F.3d at 1317 n.1. Based on that construction, the Federal Circuit held that a secure communication link similarly requires "a direct communication link . . . ." *Id*. at 1319.

In related IPR proceedings, the Board has relied on *Tempo Lighting, Inc. v. Tivoli, LLC*, 742 F.3d 973 (Fed. Cir. 2014), to dismiss Patent Owner's prosecution history arguments. Specifically, the Board has highlighted the Federal Circuit's dicta in *Tempo Lighting* that the PTO is not automatically required "to accept a

claim construction proffered as a prosecution history disclaimer," since the disclaimer "generally only binds the patent owner." 742 F.3d at 978. But while a patent examiner is not bound by a patent owner's disclaimer when construing claim terms, an unambiguous disclaimer is nevertheless informative with respect to the patent's scope and should be given effect in subsequent IPR proceedings. 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.*, No. 2015-1212, 2015 WL 7567492, at *6 (Fed. Cir. Nov. 25, 2015) (prosecution history "is to be consulted even in determining a claim's broadest reasonable interpretation").

Despite its statement in *Tempo Lighting*, the Federal Circuit there applied prosecution history disclaimer where an examiner requested the patent applicant to rewrite its claims to clarify a specific claim term, resulting in an applicant's disclaiming remarks. 742 F.3d at 977-78. Here too, in the related reexamination proceeding, the examiner construed "virtual private network communication link" more broadly than the specification, and VirnetX disclaimed embodiments that did not involve direct communication in response to the examiner's broadening of the claim. (Ex. 2006 at 8; Ex. 2011 at 7.) Just as in *Tempo Lighting*, this disclaimer was a "clarification" of the meaning of the term "virtual private network

communication link." 742 F.3d at 978. The Board should consider and apply Patent Owner's prosecution history disclaimer here.

Petitioner's construction of "virtual private network communication link," which does not require direct communication, should be rejected.

4. A "Virtual Private Network Communication Link" Requires a Network

Petitioner's construction incorrectly neglects to include that the virtual private network communication link must be in a network of computers, which eliminates the "network" from the virtual private network communication link.

Consistent with the plain meaning of a VPN communication link, the link must exist in a VPN (*see supra* Section II.G.1) and therefore must be between computers in a network. (Ex. 2016 at ¶ 28.) In describing a VPN, the '009 patent refers to the "FreeS/WAN" project, which has a glossary of terms. (Ex. 1003 at 40:7 and bibliographic data showing references cited.) The FreeS/WAN glossary defines a VPN as "a network which can safely be used as if it were private, even though some of its communication uses insecure connections. All traffic on those connections is encrypted." (Ex. 2008 at 24, Glossary for the Linux FreeS/WAN Project.) According to this glossary, a VPN includes at least the requirement of a "network of computers." (Ex. 2016 at ¶ 28.)

The specification further describes a VPN as including multiple "nodes." (*See, e.g.,* Ex. 1003 at 17:36-40, referring to "each node in the network" and

"vastly increasing the number of distinctly addressable nodes," 22:11, "nodes on the network"; *see also id.* 19:61-63, 19:24:59.) More specifically, the network allows "[e]ach node . . . to communicate with other nodes in the network." (Ex. 1003 at 17:40-42.) So a device within a VPN is able to communicate with the other devices within that same VPN. (Ex. 2016 at ¶ 29.) In addition, the specification distinguishes point-to-point queries from those carried on a VPN communication link, stating that they occur "without using an administrative VPN communication link." (*See, e.g.,* Ex. 1003 at 52:21-23, 52:26-29; Ex. 2016 at ¶ 29.)

Accordingly, Petitioner's proposed construction should be rejected.

5. A "Virtual Private Network Communication Link" Requires Encryption

Because claim 8 expressly recites that "the encrypted communication link is part of a virtual private network communication link," a "virtual private network communication link" requires encryption. (Ex. 1003, claim 8.) Nevertheless, Petitioner's proposed construction neglects to require encryption at least over insecure communication paths between the devices. (Pet. at 16-17.)

The specification "repeatedly and consistently" explains that a virtual private network requires encryption. *See Eon–Net LP v. Flagstar Bancorp.*, 653 F.3d 1314, 1321–23 (Fed. Cir. 2011). For instance, the '009 patent specification's "TARP" embodiments describe a "unique two-layer encryption format" where

"[e]ach TARP packet's true destination address is concealed behind a layer of encryption" (first layer) and "[t]he message payload is hidden behind an inner layer of encryption" (second layer). (Ex. 1003 at 3:21-23.) In addition, as described above, the FreeS/WAN glossary of terms in the '009 patent's prosecution history explains that a VPN is "a network which can safely be used as if it were private, even though some of its communication uses insecure connections. All traffic on those connections is encrypted." (Ex. 2008 at 24, Glossary for the Linux FreeS/WAN Project.) A contemporaneous computing dictionary agrees that "VPNs enjoy the security of a private network via access control and encryption . . . ." (Ex. 2007 at 8, *McGraw-Hill Computer Desktop Encyclopedia* (9th ed. 2001); Ex. 2016 at ¶ 30.) Moreover, Petitioner has repeatedly agreed that a virtual private network requires encryption. (*See, e.g.*, IPR2014-00481, Paper No. 1 at 6 (Mar. 7, 2014); Ex. 2002 at 2, Defendant's Responsive Claim Construction Brief in the '417 litigation (E.D. Tex. Dec. 7, 2011).)

H. "Domain Name" (Claims 7 and 20)

Patent Owner's Proposed Construction	Apple's Proposed Construction	Decision's Construction
A name corresponding to a network address	A name corresponding to an IP address	No construction proposed

As discussed in Patent Owner's Preliminary Response, the BRI of "domain name" is "a name corresponding to a network address." (*See* Prelim. Resp. at 46-

47; *see also* Ex. 2016 at ¶ 31.) Patent Owner's proposed construction is consistent with Petitioner's but recognizes that a name may correspond to types of network addresses other than an "IP" address. (Pet. at 17-18.)

I. "Modulation" (Claims 4, 5, 17, and 18)

Patent Owner's Proposed Construction	Petitioner's Proposed Construction	Decision's Construction
No construction necessary, alternatively, the process of encoding data for transmission over a medium by varying a carrier signal.	The process of encoding data for transmission over a medium by varying a carrier signal	No construction proposed

Though the Board declined to preliminarily construe this term, if the Board later deems construction necessary, however, the parties agree that the broadest reasonable interpretation of the claimed "modulation" is "the process of encoding data for transmission over a medium by varying a carrier signal." (*See* Pet. at 18-19; *see also* Ex. 2016 at ¶ 31.) As the Petitioner notes, the Board has previously agreed with this construction. (*Id.*, citing IPR2014-00237, Paper No. 15 at 14 (May 14, 2014).)

III. *Beser* and RFC 2401 Do Not Render Obvious Claims 1-8, 10-20, and 22-25

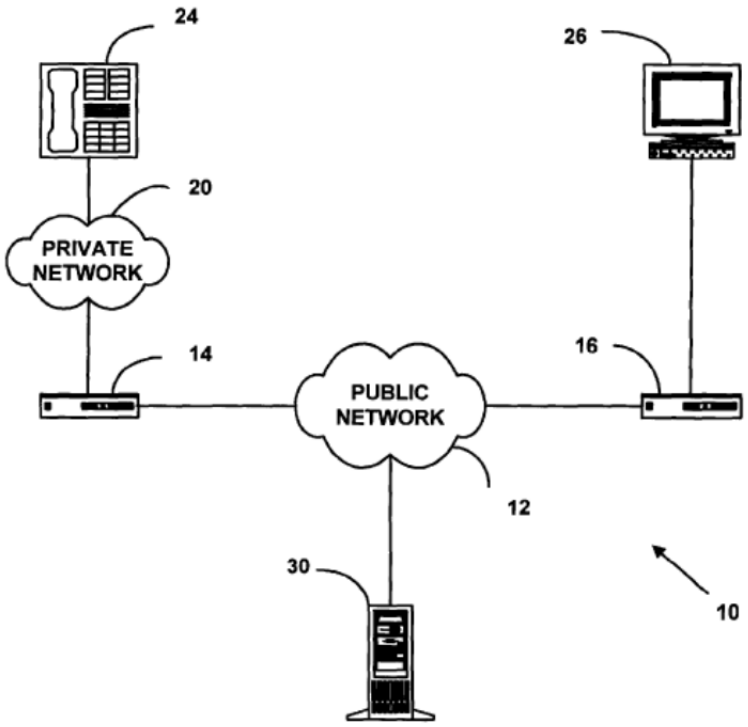
A. *Beser*'s Disclosure

Beser "relates to communications in data networks," (Ex. 1007 at 1:8-9), and the fact that "the Internet is not a very secure network," (*id.* at 1:26-27). Prior art

methods attempted to secure communications by "encrypt[ing] the information inside the IP packets before transmission." (*Id.* at 1:54-56; Ex. 2016 at ¶ 32.) *Beser* teaches that this method is not secure because a determined hacker could accumulate enough packets from a source to decrypt the message. (Ex. 1007 at 1:56-58; Ex. 2016 at ¶ 32.) Nor, as *Beser* teaches, is this method practicable, especially in the context of voice and audio data, because encryption at the source and decryption at the destination are computationally intensive. (Ex. 1007 at 1:58-67, 2:8-17; Ex. 2016 at ¶ 32.) *Beser* therefore identifies a need for a more secure system that prevents a hacker from intercepting media flow without the computational burden associated with encryption. (Ex. 1007 at 2:36-40; Ex. 2016 at ¶ 32.)

Instead of using encryption, *Beser* teaches a "tunneling association" that hides the originating and terminating ends of the tunnel during communications on a public network. (Ex. 1007 at 3:1-9; Ex. 2016 at ¶ 33.) Because the source is hidden, hackers are prevented from intercepting communications, resulting in "increase[d] [] security of communication *without an increased computational burden*." (Ex. 1007 at 2:36-40, 3:4-9 (emphasis added); Ex. 2016 at ¶ 33.) One of ordinary skill in the art would have understood that *Beser* teaches away from encryption and that its proposed solution avoids encryption. (Ex. 2016 at ¶ 33.)

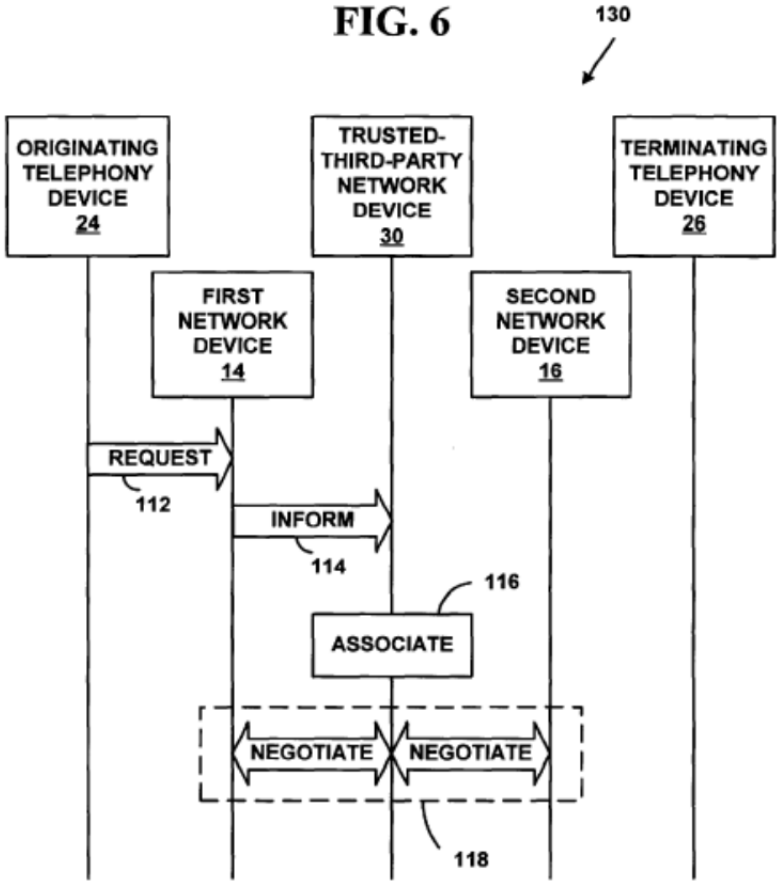
Beser's solution involves "initiating a tunnelling association between an originating end [24] and a terminating end [26]" facilitated by an intermediary, trusted-third-party network device 30. (Ex. 1007 at 1:45-67, 7:62-64; Ex. 2016 at ¶ 34.) Figure 1 of *Beser* illustrates this solution:



(Ex. 1007 at Fig. 1.)

When an originating end device 24 in *Beser* wants to communicate with a terminating end device 26, it sends a tunnel initiation request 112 to first network device 14. (*Id.* at 7:65-67; Ex. 2016 at ¶ 35.) This request "includes a unique identifier for the terminating end of the tunnelling association." (Ex. 1007 at 8:1-3; Ex. 2016 at ¶ 35.) One of ordinary skill in the art would not understand this

request (even containing a "unique identifier") to be a "request to look up an internet protocol (IP) address of the second network device." (Ex. 2016 at ¶ 35.)



(Ex. 1007 at Fig. 6.)

The first network device 14 then sends an inform message 114 with tunnel initiation request 112 to trusted-third-party network device 30 by constructing one or more IP packets 58. (*Id.* at 8:3-4, 11:9-25; Ex. 2016 at ¶ 36.) The trusted-third-party network device 30 associates a public IP address of a second network device 16 with the unique identifier of terminating telephony device 26. (Ex. 1007 at 8:4-7, 11:26-32; Ex. 2016 at ¶ 36.) The first and second network devices 14 and 16

then "negotiate" private IP addresses through the public network 12. (Ex. 1007 at 8:9-15, 11:58, Fig. 6 (step 118); Ex. 2016 at ¶ 36.) This "negotiation" assigns a first private network address to the originating device 24 and a second private network address to the terminating device 26. (Ex. 1007 at 12:2-4.)

Once assigned, the private network address of originating device 24 and the public IP address of first network device 14 are communicated to the second network device 14. (*Id.* at 13:33-48.) Similarly, the private network address of the terminating device 26 and the public IP address of the second network device 16 are communicated to the first network device 14. (*Id.* at 14:19-33; Ex. 2016 at ¶ 37.)

B. *Beser* and RFC 2401 Do Not Disclose "Send[ing] a Domain Name Service (DNS) Request To Look Up a Network Address of a Second Network Device Based On an Identifier Associated With the Second Network Device"

Independent claim 1 recites, *inter alia*, to "send a domain name service (DNS) request to look up a network address of a second network device based on an identifier associated with the second network device." Independent claim 14 similarly recites "sending a domain name service (DNS) request to look up a network address of a second network device based on an identifier associated with the second network device." In addressing these limitations, Petitioner points to *Beser*'s "request to initiate a tunneling association with a terminating end device." (Pet. at 36 (citing Ex. 1007 at 7:64-8:1, 9:64-10:41).) *Beser*'s request, however, is

not a "domain name service (DNS) request to look up a network address." (*See* Ex. 2016 at ¶ 38.)

Beser's request to initiate a tunneling connection is just that—a request to initiate a tunnel. (Ex. 2016 at ¶ 39.) This understanding is consistent with the purpose of *Beser*'s tunneling method; as explained by Petitioner's own expert, "the general purpose is the one of initiating a tunneling type of communication between two devices." (Ex. 2015 at 110:9-11.) Simply put, a tunneling request is issued and is processed in a pre-established way to initiate a tunnel between two devices. (Ex. 2016 at ¶ 39.)

During cross-examination, Petitioner's expert explained that he understood the "domain name service (DNS) request to look up a network address" recited in claim 1 to be a "request that follows the DNS protocol for such requests." (Ex. 2015 at 102:9-13.) But neither Petitioner nor its expert ever established that *Beser*'s tunneling requests follow the DNS protocol. Indeed, while tunneling requests may be received by a domain name server (*see* Ex. 1007 at 4:9-11), *Beser* is silent as to whether tunneling requests "follow the DNS protocol." (Ex. 2016 at ¶ 40.) This reason alone is sufficient to reject Petitioner's analysis of the claimed "domain name service (DNS) request to look up a network address."

The Petition also resorts to demonstrably incorrect statements about *Beser* in attempting to address these limitations. For example, the Petition alleges that the

trusted-third-party network device in *Beser* will "negotiate[] private IP addresses for the originating and terminating end devices." (Pet. at 36.) This is incorrect. The first and second network devices, not the trusted-third-party network device, "negotiate" private IP addresses, including the private IP address for the originating and terminating device. (Ex. 1007 at 8:9-15, 11:58, Fig. 6 (step 118); Ex. 2016 at ¶ 41.) Moreover, the 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. (Ex. 1007 at 12:2-4; Ex. 2016 at ¶ 41.)

The Petition also alleges that the trusted-third-party network device in *Beser* will "look[] up the public IP address associated with the unique identifier." (Pet. at 36.) But *Beser* simply states that the database entry in the trusted-third-party network device 30 may include a public IP 58 address for the terminating telephony device 26. (Ex. 1007 at 11:50-55.) *Beser* never suggests that this data structure is looked up when the tunnel request is received by device 30, let alone that the public address of telephony device 26 is specifically looked up. (Ex. 2016 at ¶ 42.) *Beser* 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. (Ex. 1007 at 11:26-32; Ex. 2016 at ¶ 42.)

In short, none 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 claims 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. (*See, e.g.*, Ex. 1001 at 40:1-29; Ex. 2016 at ¶ 43.) Therefore, *Beser* does not disclose to "send a domain name service (DNS) request to look up a network address of a second network device based on an identifier associated with the second network device," as recited in claim 1, or similarly recited in claim 14. Petitioner's reliance (albeit inaccurate) on operations in *Beser* that always occur foretells the fact that *Beser* also does not disclose the claimed "intercepting."

C. *Beser* and RFC 2401 Do Not Disclose "Interception of the DNS Request"

Independent claims 1 and 14 recite, *inter alia*, "interception of the DNS request." Petitioner alleges that the tunneling request in *Beser* is "'intercepted' by each of the first network device and the trusted-third-party network device." (Pet. at 38.) Petitioner alleges that this is so because "the request contains a unique identifier associated with the terminating end device." (*Id.*) In other words, under Petitioner's theory, because the tunneling request includes a unique identifier associated with the terminating end device, it "pertains to" the terminating end

device, but is received (as intended by *Beser*'s system) by the first network device and the trusted-third-party network device. (*See* Ex. 2016 at ¶ 44.)

Petitioner's own expert, however, admitted during cross-examination that this understanding of "intercepting" was incorrect, and instead explained that when he referred to the term "pertaining," what he meant was that it could include either a scenario in which a request is "intended for" receipt at a destination other than the destination at which the request is intercepted, or a scenario in which a request is "ordinarily received by another entity, and instead, it is received at the first entity." (Ex. 2015 at 80:3-13.)[4] At the outset, Petitioner has not analyzed the claims under this understanding of "intercepting," and so the Petition never properly addressed the claims. In fact, Petitioner could not have done so. Neither

[4] Even Petitioner nebulously explains that "The Board . . . explained that 'intercepting' a request involves 'receiving and acting on' a request, the request being 'intended for' receipt at a destination other than the destination at which the request is intercepted." (Pet. at 10.) Likewise, the Board has explained in a related proceeding involving a related patent that "one of ordinary skill in the art would have understood that 'intercepting' a request would require 'receiving and acting on' a request, the request being 'intended for' receipt at a destination other than the destination at which the request is intercepted." *Apple Inc. v. VirnetX Inc.*, IPR2014-00237, Paper No. 15 at 12 (May 14, 2014).

the first network device nor the trusted-third-party network device performs "intercepting" when analyzed in a manner consistent with how Petitioner's expert understands the term. (Ex. 2016 at ¶ 44.)

In *Beser*, when an originating end device wants to communicate with a terminating end device, it sends a tunnel initiation request to the first network device. (Ex. 1007 at 7:65-67; Ex. 2016 at ¶ 45.) Tunneling requests in *Beser* always go to, and are always intended to go to, the first network device. (Ex. 2016 at ¶ 45.) *Beser* does not disclose a single scenario in which a tunneling request is ordinarily received by another entity, but is *instead* received by the first network device. (*Id.*) Nor does *Beser* disclose any scenario in which a tunneling request is intended for receipt at another entity, but is *instead* received by the first network device. (*Id.*) Therefore, the first network device in *Beser* cannot perform "intercepting" under Petitioner's expert's understanding of the term, Petitioner's proposed construction, or the Board's construction of the term in related proceedings.

Petitioner's reliance on the trusted-third-party network device is no better. For instance, *Beser* explains that when first network device 14 informs trusted-third-party network device 30 of a request, it "constructs an IP 58 packet," where the "header 82 of the IP 58 packet includes the public network 12 address of the trusted-third-party network device 30 in the destination address field 90 and the

public network 12 address of the first network device 14 in the source address field 88." (Ex. 1007 at 11:15-20.) Thus, the packet received by trusted-third-party network 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. Just as with the first network device, *Beser* does not disclose a single scenario in which a tunneling request is ordinarily received by another entity, but is *instead* received by the trusted-third-party network device. (Ex. 2016 at ¶ 46.) Nor does *Beser* disclose any scenario in which a tunneling request is intended for receipt at another entity, but is *instead* received by the trusted-third-party network device. (*Id.*) Therefore, the trusted-third-party network device in *Beser* also cannot perform "intercepting" under any of the Petitioner's expert's understanding of the term, Petitioner's proposed construction, or the Board's construction of the term in a related proceeding.

Therefore, *Beser* does not disclose "interception of the DNS request," as recited in claims 1 and 14.

D. *Beser* and RFC 2401 Would Not Have Been Combined as the Petition Suggests

Petitioner concedes that *Beser*, by itself, does not disclose the challenged claims. Thus, Petitioner turns to RFC 2401 for the teaching that data sent between two devices in a tunnel should be encrypted. Relying on a discussion of prior art systems in *Beser*, Petitioner contends that one of skill in the art would have

combined *Beser* with RFC 2401 to achieve encrypted IP traffic. (Pet. at 30-34.) But, Petitioner misconstrues *Beser* and its contentions contradict the express teaching and purpose of *Beser's* method. (Ex. 2016 at ¶ 47.)

As *Beser* explains, prior art systems typically addressed Internet security in one of two ways. (Ex. 1007 at 1:54-2:35.) The first involved encrypting information inside IP packets before transmission. (*Id.* at 1:53-56.) The second involved network address translation whereby an IP packet's address information was modified to re-map one address space into another. (*Id.* at 2:18-22.) According to *Beser*, however, each of these prior art systems suffered from certain disadvantages. (Ex. 2016 at ¶ 48.)

For example, encryption still allowed a determined hacker to accumulate all packets from a particular source address, ultimately providing the hacker with sufficient information to decrypt the message. (*Id.* at 1:41-48, 1:56-58.) Encryption could also be infeasible for certain data formats where the speed and accuracy of message transmission are important. (*Id.* at 1:58-67.) *Beser* explains that streaming data flows, such as multimedia and Voice-over-Internet-Protocol ("VoIP") "require a great deal of computing power to encrypt or decrypt the IP packets on the fly." (*Id.* at 1:62-63.) The strain of such computations "may result in jitter, delay, or the loss of some packets." (*Id.* at 1:64-65; Ex. 2016 at ¶ 49.)

The Institution Decision asserts that *Beser* "recognizes that the use of encryption may cause challenges, [but] also suggests that such problems may be overcome by providing more computer power." (Institution Decision at 12 (citing Ex. 1007 at 1:60-63).) This position reflects a misunderstanding of *Beser*. If adding computing power to every computational problem was a solution, there would have been no need for Beser's tunneling solution. (Ex. 2016 at ¶ 50.) Indeed, in the passage cited by the Board, *Beser* notes the *problems* with allocating more computing power to encryption, such as "jitter, delay, or the loss of some packets." (Ex. 1007 at 1:60-65.) *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. (Ex. 1007 at 1:65-67; Ex. 2016 at ¶ 50.)

Beser further discloses that network address translation was similarly "computationally expensive." (Ex. 1007 at 2:22-23.) And like encryption, this type of security "may be inappropriate for the transmission of multimedia or VoIP packets." (*Id.* at 2:34-35.) "What is more, network address translation interferes with the end-to-end routing principal of the Internet that recommends that packets flow end-to-end between network devices without changing the contents of any packet along a transmission route." (*Id.* at 2:27-31; Ex. 2016 at ¶ 51.)

To address the problems of the prior art security methods—in particular, their inability to protect the identity of source and destination users and their disproportionately high use of computing power—*Beser* proposes a method of hiding the addresses of originating and terminating devices. (*See* Ex. 2016 at ¶ 52.) Its method establishes a tunneling association to hide addresses within the payload of tunneled messages. (*See* Ex. 1007 at 2:36-40, 9:49-51.) By hiding the identities of the network devices in this manner, *Beser* touts that its method is able to increase communication security without increasing computational burden. (*Id.* at 2:43-3:14.) Thus, one of ordinary skill in the art would understand that *Beser* is directed to providing a method for securing communications *other than* encryption. (*See* Ex. 2016 at ¶ 52.)

Indeed, each of *Beser's* disclosed embodiments is directed at providing increased communication security by hiding the addresses of the originating and terminating devices. (*See generally* Ex. 1007.) And while Petitioner claims that *Beser* "teaches that IP tunnels are and should ordinarily be encrypted," its citations to *Beser* fail to support this point. (Pet. at 31.) In particular, Petitioner cites repeatedly to the statement that "the sender may encrypt the information inside the IP packets before transmission," which, tellingly, is found in *Beser's* "Background of the Invention" section and is part of a description of the prior art systems over which *Beser's* method is distinguished. (*Id.* at 26, 28, 30, 31, 47.) Petitioner

further claims that because *Beser* refers to the IPSec protocol, one of skill would have combined *Beser's* tunnel with RFC 2401. (*Id.* at 30-31.) But again, the IPSec protocol is mentioned in the "Background of the Invention" and in connection with the problems in the prior art that *Beser* is attempting to overcome. (Ex. 1007 at 1:54-67; Ex. 2016 at ¶ 53.)

Petitioner next points to *Beser's* teaching that "[t]he first IP 58 packet 232 may require encryption or authentication to ensure that the public IP 58 address of the second network device 16 cannot be read on the public network 12" (*id.* at 18:2-5) to contend that "IP tunnels are and should ordinarily be encrypted." (Pet. at 31; *see also id.* at 26, 28, 33.) Petitioner's statement incorrectly characterizes *Beser*. As even Petitioner concedes, this statement in *Beser* describes only the establishment of a tunnel, what Petitioner contends is the claimed encrypted communication link. (*Id.* at 31.) Specifically, *Beser* explains that during the set-up of a tunneling association, encryption may be used to hide the identity of network device 16 (e.g., the router). (*See* Ex. 1007 at 18:2-5.) However, *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. Moreover, because the purpose of the encryption 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. (*See* Ex. 2016 at ¶ 54.) Thus, *Beser* does not use encryption in transmitting data over the established tunnel and, in fact, teaches away from doing so.

According to the Institution Decision, because *Beser* "characterizes some prior art systems as creating 'security problems by preventing certain types of encryption from being used,'" *Beser* does not teach away from adding encryption to its system. (Institution Decision at 12 (citing Ex. 1007 at 2:23-24).) The opposite is true. *Beser* acknowledges that in certain systems, certain types of *encryption cannot be used*. *Beser* manages to obtain its desired security without adding encryption to its system. (*See* Ex. 2016 at ¶ 55.)

Given the teachings of *Beser*, a person of ordinary skill in the art "would be discouraged from following the path set out in the reference, or would be led in a direction divergent from the path [in RFC 2401]." *In re Gurley*, 27 F.3d 551, 553 (Fed. Cir. 1994); (*see, e.g.*, Ex. 2016 at ¶¶ 47-55). *Beser* does not merely disclose two alternatives, one of which is the claimed alternative. Rather, *Beser's* disclosure "criticize[s], discredit[s], or otherwise discourage[s]" the use of encryption for communication over the Internet. *In re Fulton*, 391 F.3d 1195, 1201 (Fed. Cir. 2004). In fact, the entirety of the *Beser* disclosure is directed to

overcoming the problems of and providing a solution to the prior art use of encryption to secure communications over the Internet.

Petitioner cites *Medichem, SA v. Rolabo, SL*, 437 F.3d 1157 (Fed. Cir. 2006), for the proposition that despite a teaching away, a motivation to combine may still exist. (Pet. at 32-33.) *Medichem* cautions, however, that "[w]here the prior art contains 'apparently conflicting' teachings . . . each reference must be considered 'for its power to suggest solutions to an artisan of ordinary skill . . . . [and for] the degree to which one reference might accurately discredit another.'" *Medichem*, 437 F.3d at 1165 (citing *In re Young*, 927 F.2d 588, 591 (Fed. Cir. 1991)). Unlike the facts in *Medichem*, where the prior art provided clear guidance that a particular reaction could be optimized by the addition of low levels of a tertiary amine (*id.* at 1167), *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. (Ex. 1007 at 1:40-67, 2:43-3:9.)

Because *Beser* teaches away from using encryption by providing an alternate solution to cure the problems posed by encryption, Petitioner has not shown that one of ordinary skill in the art would combined the teachings of *Beser* with the encrypted tunnel of RFC 2401. Thus, for this additional reason, Petitioner's

challenge to claims 1-8, 10-20, and 22-25 should be rejected and the claims confirmed.

E. The Petition's Mapping of *Beser* and RFC 2401 Does Not Show the Features as Arranged in the Claims

The Board should also reject Petitioner's improper attempt to rely on an overlapping set of elements in *Beser* for two separate claimed features. Independent claims 1 and 14 of the '009 patent recite the return of three separate claim elements upon sending a DNS request to look up a network address. Specifically, claims 1 and 14 recite that a first network device receives "(1) an indication that the second network device is available for the secure communications service, (2) the requested network address of the second network device, and (3) provisioning information for an encrypted communication link." (Ex. 1003 at claims 1 and 14.)

In addressing the claimed "(1) indication that the second network device is available for the secure communications service," Petitioner argues that "[b]y receiving both its own private IP address and the *private address of the terminating end device*, the originating end device ('first network device') receives an 'indication.'" (Pet. at 41 (emphasis added).) Petitioner relies on an overlapping disclosure of *Beser* to address the claimed "(2) the requested network address of the second network device," arguing that "[t]he *private IP address of the terminating end device* is 'the requested network address of the second network

device.'" (Pet at 42 (emphasis added).) In other words, Petitioner relies on receipt of "the private IP address of the terminating end device" to address both claim elements. Settled case law reveals the error in Petitioner's analysis.

In *In re Robertson*, 169 F.3d 743 (Fed. Cir. 1999), the Federal Circuit held that where a claim recites separate elements the perform different functions, a single disclosed element in a prior art reference is insufficient to teach each and every element as set forth in the claims. *In re Robertson*, 169 F.3d 743, 745 (Fed. Cir. 1999); *see also Becton, Dickenson & Co. v. Tyco Healthcare Group, LP*, 616 F.3d 1249, 1254 (Fed. Cir. 2010) ("Where a claim lists elements separately, 'the clear implication of the claim language' is that those elements are 'distinct compontent[s]' of the patented invention."); *Lantech Inc. v. Keip Machine Co.*, 32 F.3d 542, 547 (Fed. Cir. 1994). Likewise, in *Ex Parte Weideman*, the Board held that "[c]onsistent with the principle that all limitations in a claim must be considered meaningful, it is improper to rely on the same structure in the [prior art] reference as being responsive to two different [claimed] elements." Appeal No. 2008-3454, Decision on Appeal at 7 (BPAI Jan. 27, 2009). Here, Petitioner attempts to do just that. Claims 1 and 14 require that the first network device receive three separate elements—an "indication that the second network device is available," a "network address of the second network device," and "provisioning information for the encrypted communication link," with each element having a

separate function, but Petitioner relies on the same receipt of "the private IP address of the terminating end device" to address both the claimed "indication" and the claimed "network address."

While *Robertson* and *Weideman* discuss an anticipation analysis, their findings apply here as well. Petitioner has not argued that one of skill would have found it obvious to either replace the two separate claim features with one feature that perform multiple functions or add an additional element to *Beser* to be received by the originating device. (*See* Pet. at 40-46.) As such, Petitioner has not properly addressed the features of claims 1 and 14, and its analysis should be rejected.

F. Dependent Claims 2-8, 10-13, 15-20, and 22-25

Beser and RFC 2401 do not render obvious claims 2-8, 10-13, 15-20, and 22-25 for at least the reasons discussed above for independent claims 1 and 14, from which they depend.

IV. Petitioner Has Not Shown that RFC 2401 Is a Prior Art Printed Publication

In its Petition, Petitioner contends that "RFC 2401 (Ex. 1008) was published in November 1998" without any supporting evidence. (Pet. at 26 (citing Ex. 1008 at 1).) After trial was instituted, Petitioner submitted additional evidence (Exs. 1060-1065) as supplemental information in support of its contention. (*See generally* Paper No. 17.) However, as discussed below, the totality of admissible

evidence offered by Petitioner is insufficient for Petitioner to establish by a preponderance of the evidence that RFC 2401 qualifies as a printed publication as of its alleged publication date.

A. The Evidence Presented with the Petition Cannot Establish by a Preponderance of the Evidence that RFC 2401 Was Publicly Accessible

The Petition did nothing more than make a naked assertion that "RFC 2401 (Ex. 1008) was published in November 1998." (Pet. at 26.) The Petition provided no explanation regarding how RFC 2401 was publicly accessible as of its alleged publication date. (*Id*.) The Board has routinely found such naked assertions to be insufficient to establish that a reference qualifies as a printed publication.

For instance, in *Apple Inc. v. DSS Technology Management, Inc*., IPR2015-00369, Paper No. 9 (June 25, 2015), where Apple was also the Petitioner, Apple asserted, without more, that a cited reference (Barber, an archived MIT Thesis) "was published at least as early as April 11, 1996." *Apple Inc. v. DSS Technology Management, Inc*., IPR2015-00369, Paper No. 9 at 12 (June 25, 2015) (hereinafter *DSS Technology Management Institution*). There, the Board denied institution because the Petition lacked any explanation or citation to evidence tending to show that Barber became publicly accessible as of April 11, 1996—the date stamped on the cover of Barber. *Id*. The Board explained that Apple's naked assertion of a publication date without more did not meet the threshold for institution. *Id*. The

Board's decision in *DSS Technology Management* is not without precedent. *See, e.g.*, *Square Inc. v. Unwired Planet, LLC*, CBM2014-00156, Paper No. 22 at 6-7 (Feb. 26, 2015); *Google Inc. v. Art+Com Innovationpool GMBH*, IPR2015-00788, Paper No. 7 at 6-11 (September 2, 2015); *Symantec Corp. v. Trustees of Columbia Univ. in the City of N.Y.*, IPR2015-00371, Paper No. 13 at 5-9 (July 17, 2015). If such naked assertions cannot establish that a reference qualifies as a printed publication under the reasonable likelihood standard, they cannot establish the same under the preponderance of the evidence standard.

Moreover, Dr. Tamassia's testimony does not constitute sufficient evidence to show that RFC 2401 was publicly accessible as of November 1998.[5] This is because neither Dr. Tamassia nor the Petition establish or even allege that Dr. Tamassia has personal knowledge that RFC 2401 was actually released to the public in November 1998. Neither 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 such that he can opine on when

[5] The Petition never cites to Dr. Tamassia's testimony regarding the publication of RFCs. (Pet. at 26.) Accordingly, the Board should not give any weight to this testimony. 37 C.F.R. § 42.104(b)(5); *see also Google*, Paper No. 7 at 10 (declining to give any weight to expert testimony regarding public accessibility because it was neither cited nor discussed in the Petition).

and how RFC 2401 was made available to the public. Accordingly, Dr. Tamassia's testimony regarding RFC 2401's public accessibility should not be accorded any weight. *Dish Network L.L.C. v. Dragon Intellectual Property, LLC*, IPR2015-00499, Paper No. 7 at 11 (July 17, 2015). Therefore, Dr. Tamassia's testimony is also insufficient to show that RFC 2401 was publicly accessible as of November 1998.

B. The Board's Findings Are Insufficient to Establish by a Preponderance of the Evidence that RFC 2401 Was Publicly Accessible

The Board found that RFC 2401 includes "indicia suggest[ing] that there is a reasonable likelihood the document was made available to the public . . . ." (Decision at 7.) The Board's rationale for this conclusion is that "[o]n its face . . . RFC 2401 is a dated 'Request for Comments' from the 'Network Working Group,' discussing a particular standardized security protocol for the Internet." (*Id*.) Furthermore, "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*.) The Board's case law, however, demonstrates that these "indicia" are insufficient to constitute even a preliminary showing, let alone a showing under the preponderance of the evidence standard, that RFC 2401 would have been sufficiently accessible to the public interested in the art as of November 1998.

For example, in *Symantec*, the Petitioner submitted as prior art a thesis whose cover page contained a date "March 1999," with the further notation "[a]pproved for public release; distribution unlimited." IPR2015-00371, Paper No. 13 at 6-7. The Board acknowledged these notations, but denied institution because Petitioner had "not provided evidence . . . tending to show when the thesis *actually* may have been released or distributed to the public." *Id*. at 8-9 (emphasis added). The Board explained that "[t]he Petition points to no evidence, however, that the thesis was entered into an electronic database prior to the critical date, much less into a publicly accessible database prior to the critical date." *Id*. Similarly, in *Google*, the Board held that the notation "Approved for Public Release; Distribution Unlimited," on a cited reference was not a sufficient indicia of public accessibility because "[i]t is not enough that a reference is accessible, we must 'consider whether *anyone* would have been able to learn of its existence and potential relevance.'" IPR2015-00788, Paper No. 7 at 9-10 (emphasis added), citing *In re Lister*, 583 F.3d 1307, 1314 (Fed. Cir. 2009).

As in *Symantec*, RFC 2401's notation that "Distribution of this memo is unlimited" does not indicate that RFC 2401 was "*actually* . . . released or distributed to the public" to meet the requirement of public accessibility. IPR2015-00371, Paper No. 13 at 8-9 (emphasis added); (*see also* Prelim. Resp. at 4). Indeed, there are insufficient indicia of public accessibility because there is simply

no evidence in RFC 2401 or in the Petition tending to show that any researcher interested in RFC 2401 could "locate and examine the reference." *In re Lister*, 583 F.3d at 1311.

While RFC 2401 is purportedly from a "Network Working Group" and is a "protocol for the Internet community, [requesting] discussion and suggestions for improvements," these vague statements provide no indication as to who is in the "Network Working Group" or the "Internet community," what the size of these groups was as of November 1998, or whether anyone outside these groups could locate and examine RFC 2401 as of November 1998. *Id*.; *see also Samsung Elecs. Co. v. Rembrandt Wireless Techs., LP*, IPR2014-00514, Paper No. 18 at 5-8 (Sep. 9, 2014) (finding that the petitioner had failed to establish that a Draft IEEE Standard qualified as a printed publication because the petitioner did not provide evidence as to whether the Draft Standard was made available to persons outside of the IEEE "Working Group" responsible for the Draft Standard and how members of the public would have known about the Draft Standard); *Elec. Frontier Found. v. Pers. Audio, LLC*, IPR2014-00070, Paper No. 21 at 22-24 (Apr. 18, 2014) (finding that a reference was not a printed publication where a "Petitioner fail[ed] to provide any information regarding [a reference] posting, the group [to which the reference was posted], who is in the group, or the size of the group.").)

Furthermore, like in *Symantec*, the Petition presents no evidence that the version of RFC 2401 with the November 1998 date on it was placed in a database or similar location that would have allowed anyone interested in RFC 2401 to retrieve and examine it. IPR2015-00371, Paper No. 13 at 8-9. Accordingly, the "indicia" in RFC 2401 are not sufficient to constitute a showing under the preponderance of the evidence standard that RFC 2401 would have been sufficiently accessible to the public interested in the art as of November 1998.

C. The Supplemental Information Is Also Insufficient to Establish by a Preponderance of the Evidence that RFC 2401 Was Publicly Accessible

After trial was instituted, Petitioner submitted additional evidence (Exs. 1060-1065) as supplemental information in support of its contention that RFC 2401 was publicly accessible as of November 1998. (Paper No. 17 at 5-7.) Exhibit 1060 is a declaration from Sandy Ginoza, a representative of the IETF, submitted in litigation before the International Trade Commission (337-TA-858) and Exhibit 1063 is a "transcript of Ms. Ginoza's February 8, 2013 deposition that was taken as part of the ITC action." (*Id*. at 5-6.) 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)." (*Id*. at 6-7.)

To the extent the testimony in Exhibits 1060-1065 is admitted and ultimately considered by the Board, the evidence in the record is still insufficient to establish that RFC 2401 qualifies as a printed publication for purposes of this proceeding. For instance, Petitioner relies upon Ms. Ginoza's following statement in its motion to submit supplemental information:

> Based on a search of RFC Editor records, I have determined that the RFC Editor maintained a copy of RFC 2401 in the ordinary course of its regularly conducted activities. RFC 2401 has been publicly available through the RFC Editor's web site or through other means since its publication in November 1998.

(Paper No. 17 at 5, citing Ex. 1060 at ¶ 107.) But this statement from Ms. Ginoza is insufficient evidence to establish that RFC 2401 qualifies as a printed publication for purposes of this proceeding. As an initial matter, Ms. Ginoza does not have any personal knowledge that RFC 2401 became publicly available in November 1998 because she was not even involved with the RFC editor's publication process until June of 1999. (Ex. 1031 at 14 (page 50, lines 17-25).) Ms. Ginoza's only testimony is a blanket assertion that "RFC 2401 has been publicly available through the RFC editor's web site or through other means since its publication in November 1998." But Ms. Ginoza does not provide the

"underlying facts or data" on which her opinion is based as a result of which her testimony is entitled to little or no weight. 37 C.F.R. § 42.65(a).

While Ms. Ginoza states that she did a "search of RFC Editor records," this statement is in the context of providing a true copy of RFC 2401 as maintained by the RFC Editor, and not in the context of her testimony that RFC 2401 was publicly available. (Ex. 1060 at ¶ 107; Ex. 1063 at 11 (p. 40, ll. 2-5).) But even if the RFC Editor records form the basis for Ms. Ginoza's statement regarding the publication date of RFC 2401, Ms. Ginoza fails to produce those RFC Editor records or even explain what existed in those records that allowed her to form her stated opinion with respect to RFC 2401. As a result, no weight should be accorded to her testimony regarding the publication date of RFC 2401. 37 C.F.R. § 42.65(a); *see also Kinetic Technologies, Inc. v. Skyworks Solutions, Inc.*, IPR2014-00690, Paper No. 43 at 19-20 (Oct. 19, 2015) (explaining that the database that formed the basis of a declarant's assertion of a reference being available should have been produced because it is important corroborating evidence); *Typeright Keyboard Corp. v. Microsoft Corp.*, 374 F.3d 1151, 1158-60 (Fed. Cir. 2004) (corroboration requirement for testimonial evidence); *Finnigan Corp. v. ITC*, 180 F.3d 1354, 1366 (Fed. Cir. 1999) (same).

V. Petitioner's Expert Testimony Should be Accorded Little, If Any Weight

Petitioner's expert, Dr. Tamassia, submitted a lengthy declaration in this proceeding totaling nearly 200 pages. (Ex. 1005.) Nevertheless, he failed to consider, let alone opine on, how any of the claim features are disclosed in asserted references. Given this glaring deficiency, Dr. Tamassia's testimony should be given little, if any, weight. Petitioner's arguments, unsupported by expert testimony, fail to meet its burden of showing unpatentability by a preponderance of the evidence.

Where the involved "subject matter is sufficiently complex to fall beyond the grasp of an ordinary layperson," expert testimony is required to establish invalidity. *Proveris Scientific Corp. v. Innovasystems, Inc.*, 536 F.3d 1256, 1267 (Fed. Cir. 2008); *see also Centricut, LLC v. Esab Group, Inc.*, 390 F.3d 1361 (Fed. Cir. 2004) (finding a failure of proof in the absence of relevant expert testimony where the patent involved "complex technology"); *Aspex Eyewear, Inc. v. Concepts In Optics, Inc.*, 111 F. App'x 582, 588 (Fed. Cir. 2004) (summary judgment of invalidity "could not have been granted without expert testimony clearly explaining how each claim element is disclosed"). This requirement for expert testimony applies to contested proceedings before an expert administrative agency like the PTAB. *See, e.g., Brand v. Miller*, 487 F.3d 862, 868-871 (Fed. Cir. 2007).

Moreover, the 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." *Schumer v. Lab. Computer Sys., Inc.*, 308 F.3d 1304, 1315 (Fed. Cir. 2002); *see also Koito Mfg. Co. v. Turn-Key-Tech LLC*, 381 F.3d 1142 (Fed. Cir. 2004) (finding insufficient general assertions by an expert regarding invalidity based on prior art references without specifying the claim limitations and explaining how the claim limitations are disclosed or rendered obvious by the references). The Federal Circuit has explained that it is insufficient for an expert to simply describe (1) his understanding of a prior art reference and (2) what he considered known to one of skill prior to the challenged invention, without also clearly describing how each claim element is disclosed by the reference. *See Schumer*, 308 F.3d at 1316.

Here, Dr. Tamassia's testimony falls short of the standard for expert testimony prescribed by the Federal Circuit. In particular, he never explains in any detail how each claim element is disclosed, taught, or suggested by the references. (*See* Ex. 2015 at 48:6-13 ("My declaration does not indicate explicitly specific correspondences between claim components, phrases, elements, and the previous work at combinations I have identified."); 51:2-12 ("I have not done what can be considered correspondence or mapping where one would create, let's say, a table, what is on the left and on the right. I have not put any such correspondence in my

declaration . . . ."); 51:16-22 ("I believe that throughout the descriptions of prior work in combinations I have not cited claim numbers. What I believe is the work I've done may be helpful to others in making the case for correspondences specific, as you said, mappings."); *see also id.* at 44:6-20; 45:4-46:7; 51:24-53:2, 55:22-25.) Nor does he even appear to have considered how each claim element is taught or suggested in the prior art reference. Such expert testimony is insufficient to establish a *prima facie* case of obviousness, as Petitioner attempts to do here. *Schumer*, 308 F.3d at 1315.

Apple's lack of supporting expert testimony cannot simply be excused. Here, the technology involved is undisputedly complex. Apple has repeatedly agreed with Patent Owner that a person of ordinary skill in the art would have had a master's degree in computer science or computer engineering and two years of experience in computer networking and network security, which indicates the complexity of the technology involved in these proceedings. (*See, e.g.*, Ex. 2004 at 5; Declaration of Mr. Fratto at 1, ¶ 5, filed Aug. 6, 2012 in Apple's *inter partes* reexamination control no. 95/001,789; Prelim. Resp. at 23.) Indeed, the transparent creation of an encrypted communications channel between a client device and a target device wherein a request to look up an IP address is intercepted, a determination is made whether the request corresponds to a device that accepts an encrypted channel connection, and in response to the determination,

provisioning information required to initiate the creation of the encrypted communications channel is provided, requires testimony and analysis from one of ordinary skill in the art. *See Proveris Scientific*, 536 F.3d at 1267; *Aspex Eyewear*, 111 F. App'x at 588 (finding it to be a "rare case[] where the invention is so simple that expert testimony is not required").

The cited references are similarly complex, and require explanatory expert testimony. Apple can hardly disagree that the technology and references at issue are complex given that its expert provided an almost 200-page expert declaration (*see, e.g.*, Ex. 1005). *Alexsam, Inc. v. IDT Corp.*, 715 F.3d 1336, 1348 (Fed. Cir. 2013) (finding that any "claim that the technology is simple is belied by the fact that both sides believed it necessary to introduce extensive expert testimony regarding the content of the prior art"). Because expert testimony is required to support Apple's arguments, and because the expert testimony relied upon by the Petitioner is insufficient to support Apple's unpatentability analysis, the Board should enter judgment against Apple.

VI. Conclusion

For these reasons, Apple has failed to prove that claims 1-8, 10-20, and 22-25 are unpatentable. The Board should enter judgment against Apple and terminate this proceeding.

Respectfully submitted,

Dated: December 11, 2015

By: /Joseph E. Palys/
Joseph E. Palys
Registration No. 46,508

Counsel for VirnetX Inc.

CERTIFICATE OF SERVICE

I hereby certify that on this 11th day of December 2015, a copy of Patent Owner's Response was served by electronic mail, as agreed by the parties, upon the following:

Counsel for Apple Inc.:

iprnotices@sidley.com
Sidley Austin LLP
1501 K Street NW
Washington, DC 20005

Dated: December 11, 2015

Respectfully submitted,

/Joseph E. Palys/
Joseph E. Palys
Counsel for VirnetX Inc.