Paper No. _____
Filed: June 15, 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 Preliminary Response to Petition for *Inter Partes* Review of U.S. Patent No. 8,850,009

Table of Contents

TABLE OF AUTHORITIES

Page(s)

Cases

Federal Statutes

Federal Rules

I. Introduction

Patent Owner VirnetX Inc. respectfully submits this Preliminary Response in accordance with 35 U.S.C. § 313 and 37 C.F.R. § 42.107, responding to the Petition for *Inter Partes* Review (the "Petition") filed by Apple Inc. against Patent Owner's U.S. Patent No. 8,850,009 ("the '009 patent"). Patent Owner requests that the Board not institute *inter partes* review for several reasons.

First, Petitioner relies on material that it has not shown is a "patent[] or printed publication[]" under 35 U.S.C. § 311(b). Second, Petitioner proposes redundant grounds without identifying how any one ground improves on any other, contravening Board precedent requiring petitioners to identify differences in proposed rejections. Next, Petitioner has not met its burden of demonstrating a reasonable likelihood of prevailing in proving unpatentability of any challenged '009 patent claim. The Petition also fails to identify where and what in the prior art discloses each claimed feature, violating the particularity requirements of 35 U.S.C. § 312(a)(3) and 37 C.F.R. § 42.104(b). And finally, Petitioner proposes a number of incorrect claim constructions upon which it bases its unpatentability grounds. Each of these reasons requires denial of institution.

II. The Petition Fails to Meet the Requirements for Instituting an *Inter Partes* Review

The grounds that may be raised in a petition for *inter partes* review (IPR) are limited to those "that could be raised under section 102 or 103 and only on the

basis of prior art consisting of patents or printed publications." 35 U.S.C. § 311(b). In addition, the Board will not consider redundant grounds and to the extent they are proposed, Petitioner carries the burden of "articulat[ing] a meaningful distinction in terms of relative strengths and weaknesses with respect to application of the prior art disclosures to one or more claim limitations." *ScentAir Techs., Inc. v. Prolitic, Inc.*, IPR2013-00180, Paper No. 18 at 3 (Aug. 26, 2013); *see also Idle Free Sys., Inc. v. Bergstrom, Inc.*, IPR2012-00027, Paper No. 26 at 3 (June 11, 2013) ("[A]t [the] time of institution the Board analyzes the petition on a claim-by-claim, ground-by-ground basis, to eliminate redundant grounds.") To be instituted, a petition must also "show[] that there is a reasonable likelihood that the petitioner would prevail with respect to at least 1 of the claims challenged in the petition." 35 U.S.C. § 314(a). This showing requires that the petition "identif[y], in writing and with particularity, each claim challenged, the grounds on which the challenge to each claim is based, and the evidence that supports the grounds for the challenge to each claim." 35 U.S.C. § 312(a)(3). Petitioner fails to meet each of these requirements.

A. The Petition Improperly Relies on Material That It Fails to Establish Is Statutory Prior Art

Prior art relied on in a petition for *inter partes* review may only consist of "patents or printed publications." 35 U.S.C. § 311(b). As such, the burden is on Petitioner to establish that RFC 2401, which is not a patent, was "sufficiently

accessible to the public interested in the art." *In re Klopfenstein*, 380 F.3d 1345, 1348 (Fed. Cir. 2004); *see also Actavis, Inc. v. Research Corp. Techs., Inc.*, IPR2014-01126, Paper No. 22 at 9-13 (Jan. 9, 2015) (finding that "Petitioner has not satisfied its burden to prove that [a] thesis is a printed publication under § 102(b)"); *L-3 Comm. Holdings, Inc. v. Power Survey, LLC*, IPR2014-00832, Paper No. 9 at 12 (Nov. 14, 2014) ("The party seeking to introduce the reference 'should produce sufficient proof of its dissemination or that it has otherwise been available and accessible to persons concerned with the art to which the document relates and thus most likely to avail themselves of its contents.'"); *A.R.M., Inc. v. Cottingham Agencies Ltd.*, IPR2014-00671, Paper No. 10 at 7 (Oct. 3, 2014).

Petitioner merely alleges that "RFC 2401 (Ex. 1008) was published in November 1998." (Pet. at 26 (citing Ex. 1008 at 1).) However, Petitioner does not provide evidence to establish that RFC 2401 would have been sufficiently accessible to the public interested in the art on that date. While RFC 2401 nominally recites "November 1998" on its first page, nowhere in the document is there any indication as to what the date means. (*See* Ex. 1008 at 1.)

RFC 2026, provided by the same "Network Working Group" as RFC 2401 (*compare* Ex. 1036 at 1, *with* Ex. 1008 at 1), purports to "document[] the process used by the Internet community for the standardization of protocols and procedures" and to "define[] the stages in the standardization process, the

requirements for moving a document between stages and the types of documents used during this process." (*See* Ex. 1036 at 1.)[1] Petitioner's expert, Dr. Tamassia, refers to RFC 2026 in his discussion of how RFCs are "typically" released. (Ex. 1005 at ¶ 152.) Neither Dr. Tamassia nor the Petition establish or even allege that Dr. Tamassia has personal knowledge that RFC 2401 was actually released in November 1998 in the way he says RFCs are typically released. However, even if RFC 2401 was released in this manner (and Patent Owner submits that Petitioner has not provided any evidence to establish that it was), Petitioner has still not established that RFC 2401 qualifies as a printed publication within the meaning of Section 311(b).

RFC 2026 generally states that "RFCs can be obtained from a number of Internet hosts using anonymous FTP, gopher, World Wide Web, and other Internet document-retrieval systems." (*Id.* at 6.) RFC 2026 does not explain how the

[1] The Petition does not cite to RFC 2026 or to any testimony citing to the document. Therefore, it cannot properly be relied upon to establish RFC 2401 as a printed publication. However, Patent Owner addresses the document to the extent the Board considers statements by Petitioner's expert regarding RFC 2026 not cited in the Petition. As explained, these statements, and RFC 2026 itself, still fail to establish that RFC 2401 qualifies as a printed publication within the meaning of Section 311(b).

public interested in the art would become aware of the location of such Internet document-retrieval systems. Indeed, Dr. Tamassia suggests that the intended audience of RFC 2401 would have been limited to the "Network Working Group," stating the nominal date that RFC documents are "published" merely "starts a period for others to provide comments on the document" (in particular, what RFC 2026 refers to as "community review"). (*See* Ex. 1005 at ¶ 152; Ex. 1036 at 20.) RFC 2026 also acknowledges that "[m]any standards groups other than the IETF create and publish standards documents." (*See id.* at 24.)

In the past, the Board has found that references similar to RFC 2401 are not statutory prior art. For example, in *Samsung Elecs. Co. v. Rembrandt Wireless Techs., LP*, IPR2014-00514, Paper No. 18 at 5, 7 (Sep. 9, 2014), the petitioner relied on a "Draft Standard" of the Institute of Electrical and Electronics Engineers ("IEEE"). The Board found that the petitioner had failed to establish the Draft 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. *See id.* at 7-8. Similarly, in *Elec. Frontier Found. v. Pers. Audio, LLC*, IPR2014-00070, Paper No. 21 at 22-24 (Apr. 18, 2014), the Board found 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." In both cases, the Board denied institution based on these findings. *See Samsung Elecs.*, IPR2014-00514, Paper No. 18 at 10 ("Because Petitioner has not met its burden in establishing that Draft Standard is a 'printed publication' and, thus, prior art, Petitioner has not shown a reasonable likelihood of prevailing on the grounds asserted."); *Elec. Frontier Found.*, IPR2014-00070, Paper No. 21 at 26.

Petitioner has similarly failed to meet its burden to establish that RFC 2401 is a printed publication. For example, Petitioner has not provided any evidence as to (1) whether RFC 2401 was made available to persons outside of the "Network Working Group"; (2) how members of the public outside of the "Network Working Group" would have known about RFC 2401; (3) who is in "Network Working Group"; or (4) the size of the Network Working Group. Therefore, because the Petition does not establish that RFC 2401 was a printed publication to qualify as prior art, and because all of Petitioner's proposed rejections rely on RFC 2401, the Board should deny institution of the Petition.

B. The Petition's Obviousness Ground Is Redundant and Should Be Denied

Concurrent with this Petition, in which Petitioner challenges claims 1-8, 10-20, and 22-25 of the '009 patent as obvious over *Beser* in view of RFC 2401, Petitioner also filed a petition for *inter partes* review in IPR2015-00813 ("the '813

Petition"). The '813 Petition challenges the same patent and the same claims, asserting two grounds of rejection. The '813 Petition's first ground of rejection simply substitutes *Beser* with *Aventail*, alleging that claims 1-8, 10-20, and 22-25 are obvious over *Aventail* in view of RFC 2401. Its second ground of rejection alleges that claims 2-5 and 15-18 are obvious over *Aventail* in view of RFC 2401 and further in view of RFC 2543. The Petition fails to assert or explain why the proposed grounds in the Petition are not redundant of the grounds in the '813 Petition. Instead, the Petition contends, without explanation, that each Petition presents "non-redundant grounds." (Pet. at 2.) Given the Board's jurisprudence regarding redundancy, Petitioner's redundant grounds should be rejected.

Redundant grounds place a significant burden on the Board and the patent owner, and cause unnecessary delay that jeopardizes meeting the statutory deadline for final written decisions. *Liberty Mut. Ins. Co. v. Progressive Cas. Ins. Co.*, CBM2012-00003, Paper No. 7 at 2 (Oct. 25, 2012). The consideration of redundant grounds frustrates Congress's intent that the Board "secure the just, speedy, and inexpensive resolution of every proceeding," in violation of 37 C.F.R. § 42.1(b).

The Board explains that where multiple grounds of rejection are presented, the "[d]ifferences between the claimed invention and the prior art are a critically important underlying factual inquiry . . . ." *Liberty Mut. Ins. Co.*, CBM2012-

00003, Paper No. 7 at 2-3. The redundancy inquiry does not focus on "whether the applied prior art disclosures have differences, for it is rarely the case that the disclosures of different prior art references, will be literally identical. *EMC Corp. v. Personal Web Techs., LLC*, IPR2013-00087, Paper No. 25 at 3 (June 5, 2013). Rather, the Board considers "whether the petitioner articulated a meaningful distinction in terms of relatives strengths and weaknesses with respect to application of the prior art disclosures to one or more claim limitations." *Id.* at 3-4. The Petitioner carries the burden of articulating that "meaningful distinction." *ScentAir Techs.*, IPR2013-00180, Paper No. 18 at 3. Put simply, "[t]o avoid a holding of redundancy, the Petition has to explain why one reference is better in one respect but worse in another respect." *Toyota Motor Corp. v. Am. Vehicular Sciences LLC*, IPR2013-00421, Paper No. 15 at 29 (Jan. 13, 2014).

Petitioner's burden of articulating a distinction between its redundant grounds is not lessened or removed simply because those grounds may appear in more than one petition. In fact, the policy considerations behind denying redundant grounds are even more compelling when those grounds are presented across multiple petitions. Multiple petitions necessitate multiple written decisions and an analysis of a corresponding number of briefs, as well as the potential for differing panels of judges, multiple scheduling conferences, and multiple oral arguments—all of which tax the Board's resources and diminish its ability to

ensure the speedy resolution of each proceeding. Moreover the Board has previously recognized grounds as being redundant across petitions and dismissed the redundant grounds. *See Apple Inc. v. VirnetX Inc.*, IPR2014-00483, Paper No. 11 at 6 (Sept. 15, 2014).

In *Liberty Mutual*, the Board identified two types of redundant rejections: (1) "horizontally" redundant rejections and (2) "vertically" redundant rejections. *Liberty Mut. Ins. Co.*, CBM2012-00003, Paper No. 7 at 3. The Board explained that horizontally redundant rejections apply "a plurality of prior art references . . . not in combination to complement each other but as distinct and separate alternatives." *Id.* Vertical redundancy "exists when there is assertion of an additional prior art reference to support another ground of unpatentability when a base ground already has been asserted against the same claim without the additional reference and the Petitioner has not explained what are the relative strength and weakness of each ground." *Id.* at 12.

Here, the Petition is horizontally redundant in view of the '813 Petition. In both petitions, Petitioner alleges that claims 1-8, 10-20, and 22-25 are rendered obvious by either *Beser* or *Aventail* in view of RFC 2401. These grounds are horizontally redundant and Petitioner fails to provide any explanation to the contrary.

In the instant Petition, Petitioner claims that *Beser* discloses each of the claimed limitations, including a "communication link," but relies on RFC 2401 for the claimed "encrypted communication link." (Pet. at 34-50.) According to the Petition, one skilled in the art would have encrypted the tunneling associations taught in *Beser* in light of RFC 2401. (*Id.* at 30-34.) Similarly, in the '813 Petition, Petitioner claims that *Aventail* discloses each of the claimed limitations, including a communication link, but again relies on RFC 2401 for the claimed "encrypted communication link." Attempting to address redundancy, Petitioner claims its grounds are "non-redundant" because each petition "present[s] unique correlations of the challenged '009 claims to the prior art." (Pet. at 2.) But, as the Board has explained, a redundancy analysis does not focus on whether the prior art references are identical. *EMC Corp.*, IPR2013-00087, Paper No. 25 at 3. And Petitioner does not attempt to "articulate[] a meaningful distinction in terms of relative strengths and weaknesses with respect to application of the prior art disclosures to one or more claim limitations." *Id.* at 3-4 (emphasis added). Consequently, the Board should deny Petitioner's redundant grounds.

C. The Petition Fails to Show a Reasonable Likelihood Petitioner Will Prevail With Respect to Obviousness

Petitioner proposes that claims 1-8, 10-20, and 22-25 would be rendered obvious under 35 U.S.C. § 103 based on *Beser* in view of RFC 2401. Obviousness is a question of law based on underlying factual findings, including: (1) the scope

and content of the prior art; (2) the differences between the claims and the prior art; (3) the level of ordinary skill in the art; and (4) objective indicia of nonobviousness. *Graham v. John Deere Co. of Kansas City*, 383 U.S. 1, 17-18 (1966). Each of these factors should be considered in an obviousness analysis. *In re Cyclobenzaprine Hydrochloride Extended-Release Capsule Patent Litig.*, 676 F.3d 1063, 1075, 1077, 1080 (Fed. Cir. 2012). In particular, "[i]t is not sufficient to demonstrate that each of the components in a challenged claim is known in the prior art." *Petroleum Geo-Services Inc., v. WesternGeco LLC*, IPR2014-01476, Paper No. 18 at 18 (Mar. 17, 2015) (citing *KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398 (2007).) "Petitioner also must explain how a person of ordinary skill in the art would combine the elements disclosed in the [claims], and why such a person would be motivated to do so." *Id.* (emphasis added, citing *In re Chaganti*, 554 F. App'x 917, 922 (Fed. Cir. 2014)).

Even when elements may be known in the art, "there [must be] an apparent reason to combine the known elements in the fashion claimed by the patent at issue," and "this analysis should be made explicit." *KSR*, 550 U.S. at 418. "[R]ejections on obviousness grounds cannot be sustained by mere conclusory statements; instead, there must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness." *In re Kahn*, 441 F.3d 977, 988 (Fed. Cir. 2006).

1. *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. (*See* Ex. 2009, *Apple Inc. v. VirnetX, Inc.*, IPR2014-00237, Declaration of Fabian Monrose, Ph.D. (Aug. 28, 2014) at 34-35, ¶¶55-56.)

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.

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.)

Beser further discloses that network address translation was similarly "computationally expensive." (*Id.* 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.)

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. 2009, IPR2014-00237, Declaration of Fabian Monrose, Ph.D. (Aug. 28, 2014) at 34-35, ¶ 56.) 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. 2009, IPR2014-00237, Declaration of Fabian Monrose, Ph.D. (Aug. 28, 2014) at 34-35, ¶ 56.)

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.)

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. Thus, *Beser* does not use encryption in transmitting data over the established tunnel and, in fact, teaches away from doing so.

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). *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. Accordingly, there is not a reasonable likelihood that Petitioner will prevail over any of the '009 patent claims and the Petition does not meet the requirements for institution.

2. 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 two elements for three 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.) Although the claims plainly enumerate the three features that must be received at the first network device, Petitioner improperly identifies just two elements in *Beser* that satisfy these features. *In re Robertson*, 169 F.3d 743, 745 (Fed. Cir. 1999) (finding that three

separate claim features are not taught by a prior art reference containing only two features).

Petitioner contends that the three claimed features are satisfied by receipt at the originating end device of its own private IP address and the private IP address of the terminating end device. (Pet. at 40-46.) In explaining how the first device "connect[s] to the second network device over the encrypted communication link, using the received network address of the second network device and the provisioning information for the encrypted communication link," Petitioner explains:

> [T]he originating end device receives (1) its own private IP address (*i.e.*, "*provisioning information for the encrypted communication link*") and (2) the private IP address assigned to the terminating end device (*i.e.*, "*the requested network address of the second network device*").

(*Id.* at 46.) However, Petitioner relies on these same addresses to also satisfy the claimed "indication" feature. (*Id.* at 41, "By 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".) Settled case law reveals the error in Petitioner's analysis.

In *Robertson*, the Federal Circuit held that where a claim recites separate elements that 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.

169 F.3d at 745; *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 just two addresses for these three distinct elements.

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 three separate claim features with two features that perform multiple functions or add an additional element to *Beser* to be received by the originating device. (*See* Pet. at 40-46.) Because Petitioner has

failed to explain "[h]ow the construed claim is unpatentable," and "specify where each element of the claim is found in the prior art patents or printed publications relied upon" (37 C.F.R. § 42.104(b)(4)), there is not a reasonable likelihood that the proposed ground will prevail over any of the '009 patent claims and the petition should be rejected as not meeting the requirements for institution. *See, e.g.*, *Google Inc. et al. v. EveryMD.com LLC*, IPR2014-00347, Paper No. 9 at 18-20 (May 22, 2014) (rejecting petition for insufficient explanation); *Apple Inc. v. Evolutionary Intelligence, LLC*, IPR2014-00079, Paper No. 8 at 17-19 (Apr. 25, 2014) (rejecting petition for including "vague" explanation of the prior art); *Tempur Sealy Int'l, Inc. v. Select Comfort Corp.*, IPR2014-01419, Paper No. 9 (Mar. 27, 2015) (rejecting petition for not identifying specific portions of the evidence that support the challenge and not specifying where each element of the claim is found in those references).

III. The Petition's Claim Constructions Are Flawed and Should Be Rejected

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). In applying the "broadest reasonable construction" or interpretation ("BRI") standard, the words of the claim must be given their plain meaning unless the plain meaning is inconsistent with the specification. *In re Zletz*, 893 F.2d 319, 321 (Fed. Cir. 1989). The ordinary meaning of a term may be evidenced by a variety of sources,

including "the words of the claims themselves, the remainder of the specification, the prosecution history, and extrinsic evidence concerning relevant scientific principles, the meaning of technical terms, and the state of the art." *Phillips v. AWH Corp.*, 415 F.3d 1303, 1314 (Fed. Cir. 2005) (en banc) (citation omitted).

Additionally, the prosecution history is part of the intrinsic record and should be considered when construing the claims. *Id.* at 1317. In *inter partes* review proceedings, the Board considers the prosecution history when construing the claims. *See, e.g.*, *Garmin Int'l, Inc. v. Cuozzo Speed Techs. 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).

As explained below, Petitioner proposes defective claim constructions that do not represent the BRI of the claims. Because it is based on incorrect claim constructions, the Petition cannot demonstrate a reasonable likelihood of prevailing for any claim of the '009 patent.

A. Overview of the '009 Patent

The '009 patent discloses embodiments relating to creating an encrypted communication link for communication between a first network device and a second network device. (*See, e.g.*, Ex. 1003, Figs. 26 (items 2601 and 2604), 27, 33 (items 3301 and 3320), 34.)

In one embodiment, a first network device executes a method that enables it to communicate with a second network device. The method includes sending a DNS request to look up a network address of a second network device. (*See, e.g., id.* at 40:29-38, 51:29-31.) It further includes intercepting the DNS request and determining that the second network device is available for the secure communications service. (*See, e.g., id.* at 40:39-56, 51:51-52:6.) Following the interception and determination steps, the 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. (*See, e.g., id* at 40:48-56, 41:65-67, 52:10-13, 52:17-20, 52:35-40.) It then includes connecting to the second network device over the encrypted communication link, using the received network address of the second network device and the provisioning information for the encrypted communication link. Data is communicated from the first network device to the second network device using the secure communications service via the encrypted communication link. (*See, e.g., id* at 40:11-22, 40:39-56, 41:39-46, 41:58-67, 52:10-13, 52:32-42, Figs. 27, 34.) The first network device is a device at which a user uses the secure communications service to access the encrypted communication link. (*See, e.g., id.* at 40:29-38, 49:55-61, 50:54-57.)

B. Level of Ordinary Skill in the Art

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 two years of experience in computer networking and computer security. Petitioner proposes a lower level of skill (Pet. at 8-9), but Patent Owner's proposed level is the same level of skill that Petitioner and nearly a dozen other parties have consistently advocated in related litigation involving patents in the same family as the '705 patent. (Ex. 2005 at 4, Memorandum Opinion and Order in *VirnetX Inc. v. Mitel Networks Corp. et al.*, Case No. 6:11-CV-18 (E.D. Tex. Aug. 1, 2012); Ex. 2004 at 5, Memorandum Opinion and Order in *VirnetX Inc. v. Cisco Systems, Inc. et al.*, Case No. 6:10-CV-417 (E.D. Tex. April 25, 2012) (hereinafter, "the '417 litigation").)

Patent Owner's proposed level of skill is essentially the same level of skill that both Petitioner and Microsoft advocated in *inter partes* reviews and reexamination proceedings of Patent Owner's patents in the same family as the '009 patent. (*See, e.g.*, Declaration of Mr. Fratto at 1, ¶ 5, filed Aug. 6, 2012 in Apple's *inter partes* reexamination control no. 95/001,789; Declaration of Mr. Fratto at 1, ¶ 5, filed June 25, 2012 in Apple's *inter partes* reexamination control no. 95/001,788.)

In other proceedings, Patent Owner's expert, Dr. Fabian Monrose, also agreed that a person of ordinary skill in art for Patent Owner's patents would have had a master's degree in computer science or computer engineering, as well as two years of experience in computer networking with some accompanying exposure to network security. (*See, e.g.*, Ex. 2009, IPR2014-00237, Declaration of Fabian Monrose, Ph.D. (Aug. 28, 2014) at 10, ¶ 12.) Because there is nearly universal agreement that this is the level of skill that applies to Patent Owner's patents in this family, the Board should apply it here.

C. "Domain Name Service (DNS) Request" (Claims 1, 12-14, 24 and 25) [2]

Patent Owner's Proposed Construction	Petitioner's Proposed Construction
A request for a resource corresponding to a domain name	A request for a resource corresponding to a domain name

The parties agree that the broadest reasonable interpretation of the claimed "DNS request" is "a request for a resource corresponding to a domain name." (*See* Pet. at 10.) As the Petitioner notes, the Board has previously agreed with this construction. (*Id.*, citing IPR2014-00610, Paper No. 9 at 6 (Oct. 15, 2014).) The Board should thus adopt the construction proposed by the parties.

[2] 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.

D. "Interception of the DNS Request" (Claims 1 and 14)

Patent Owner's Proposed Construction	Petitioner's Proposed 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

Petitioner adopts a construction for "interception of the DNS request" (Pet. at 11) that 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). If the Board decides to provide a construction, it should adopt Patent Owner's construction because Petitioner's proposed construction does not reflect how one of ordinary skill in the art reading the '009 patent would have understood the "interception" phrase.

As explained in the '009 patent, in conventional DNS, a DNS request seeking an address of a target web site 2503 (a first entity) is received at a DNS server 2502 (a second entity), which returns the address. (Ex. 1003 at Fig. 25, reproduced below; *id.* at 9:47-48, 39:46-55; *see* Ex. 2009, IPR2014-00237, Declaration of Fabian Monrose, Ph.D. (Aug. 28, 2014) at 15-16, ¶ 23.)

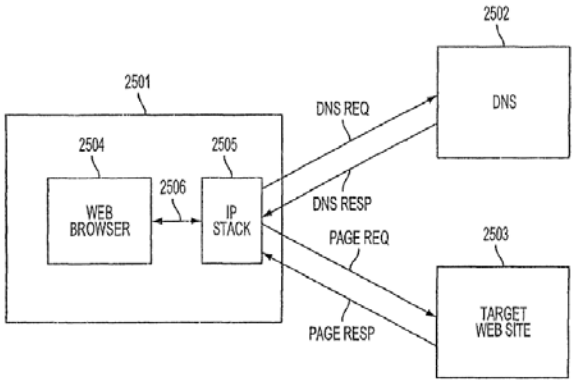

FIG. 25
(PRIOR ART)

The same is true of the '009 patent's embodiment in which a DNS request to look up a network 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). (Ex. 1003 at FIG. 26, reproduced below; *see also id.* at 40:39-48; Ex. 2009, IPR2014-00237, Declaration of Fabian Monrose, Ph.D. (Aug. 28, 2014) at 15-16, ¶ 23.)

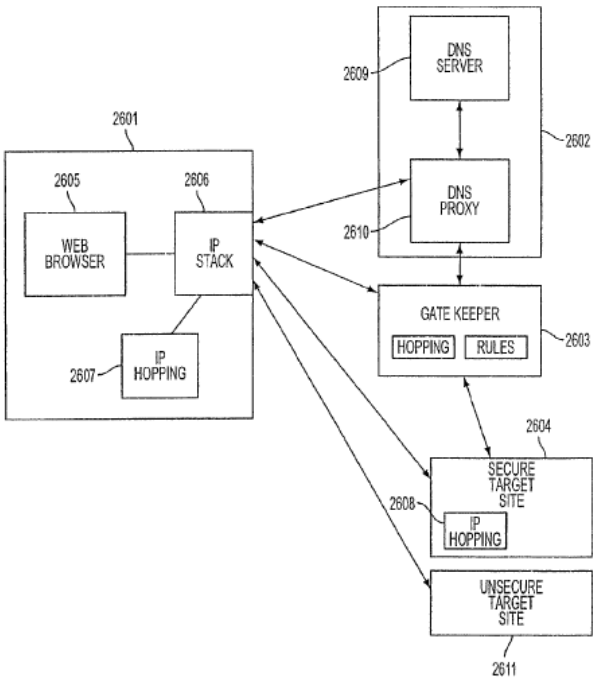

FIG. 26

However, the ’009 patent goes on to explain that the claimed embodiments differ from 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. (Ex. 2009, IPR2014-00237, Declaration of Fabian Monrose, Ph.D. (Aug. 28, 2014) at 17, ¶ 24.) For example, the DNS proxy 2610 may intercept the request and “determine[ ] whether access to a secure side has been requested,” “determine[ ] whether the user has sufficient security privileges to access the site,” and/or “transmit[ ] a message to gatekeeper 2603 requesting that a virtual private network be created between 40 user computer 2601 and secure target site 2604.” (Ex. 1003 at 40:39-48; Ex. 2009, IPR2014-00237, Declaration of Fabian Monrose, Ph.D. (Aug. 28, 2014) at 17, ¶ 24.) Additionally, the DNS resolves an address and returns it to the first network device. (Ex. 1003 at 40:52-56; Ex. 2009, IPR2014-00237, Declaration of Fabian Monrose, Ph.D. (Aug. 28, 2014) at 17, ¶ 24.) Petitioner’s construction overlooks the aspects distinguishing the “intercepting” phrase from conventional DNS. (*See* Ex. 2009, IPR2014-00237, Declaration of Fabian Monrose, Ph.D. (Aug. 28, 2014) at 17, ¶ 24.)

If the Board deems an express construction necessary, Patent Owner’s alternative construction appropriately captures the notion of performing an

additional evaluation on a DNS request related to establishing an encrypted communication link, beyond conventionally resolving it and returning the address. 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.)

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

Patent Owner's Proposed Construction	Petitioner's Proposed 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

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 secure communications which may be 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 secure communication in later embodiments that may be direct 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.)

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., id.* at Figs. 2, 24, 28, 29, 33.) 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.*, 767 F.3d at 1317 n.1, 1319. Nevertheless, Petitioner's construction neglects to include this "direct" aspect—despite the claims' express language that the "network device . . . connect[s] to the second network device over an encrypted communication link." (*See* Ex. 1003, claim 1.) Petitioner's construction simply introduces more terms requiring construction and/or explanation by requiring a "transmission path that restricts access to data, addresses, or other information on the path at least by using encryption." Accordingly, Petitioner's construction should be rejected. Under the applicable broadest reasonable interpretation

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."

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

Patent Owner's Proposed Construction	Petitioner's Proposed 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

In the context of the '009 patent claims, "provisioning information" means "information that is used to establish an encrypted communication link." The claims support this construction by reciting that network devices connect "over the encrypted communication link, using . . . the provisioning information for the encrypted communication link." (Ex. 1003, claims 1 and 14.) The '009 specification likewise explains that provisioning information is used to establish the link. (*See, e.g.,* Ex. 1003 at 52:10-13.)

Patent Owner's construction is also consistent with the more general notion that provisioning refers to setting up or establishing a connection or service at the time of the invention for the '009 patent. 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." (Ex. 2007 at 6, *McGraw-Hill Computer Desktop Encyclopedia* (9th ed. 2001).) Applying these principles to

provisioning in the context of the ’009 patent, the recited “provisioning information for an encrypted communication link” refers to setting up or establishing an encrypted communication link. Thus, the “provisioning information” is “information that is used to establish an encrypted communication link.”

Petitioner construes “provisioning information” to mean “information that enables communication in a virtual private network, where the virtual private network uses encryption.” (Pet. at 13-14.) This construction should be rejected because it is overly broad in one aspect and overly narrow in another. It is overly broad in that it encompasses any information that “enables” communication using an encrypted communication link, 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 encrypted communication link. While this type of information may enable communication using an encrypted communication link, it has no relationship to the traditional notions of provisioning or provisioning as it is discussed in the ’009 patent. One of ordinary skill in the art would not have understood an encrypted communication link to be provisioned every time a data packet is sent across it, but Petitioner’s construction inaccurately encompasses this scenario.

Petitioner's construction is also incorrect because it substitutes the broader term "encrypted communication link," recited in the claims, with the narrower term "virtual private network." (*See generally*, *infra* Section III.I.) While an encrypted communication link over a virtual private network requires encryption, an encrypted communication link does not require a virtual private network. Contrary to Petitioner's assertion that every encrypted communication link requires a virtual private network (Pet. at 14), an encrypted communication link can exist with or without a virtual private network. For instance, unlike the encrypted communication link recited in claims 1 and 14, dependent claims 8 and 21 expressly recite a narrower link in which "the encrypted communication link **is part of a virtual private network** communication link." (Ex. 1003, claims 8 and 21.)[3] (*See also* Section III.I, *infra*.) Moreover, nothing in the specification or prosecution history indicates that "encrypted communication link" has a special, narrower meaning or associated disclaimer that requires a virtual private network. The term should be given its plain meaning discussed above and not replaced with the narrower "virtual private network," as suggested by Petitioner. *See Phillips*, 415 F.3d at 1313-1314, 1316, 1319 (citations omitted).

Accordingly, "provisioning information" means "information that is used to establish an encrypted communication link."

[3] All emphasis is added except where otherwise noted.

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

Patent Owner's Proposed Construction	Petitioner's Proposed 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

Patent Owner generally agrees with Petitioner's proposed construction of "secure communications service." However, Petitioner's proposed construction involves terms not recited in the claims. (Pet. at 14-15.) Because the claims recite an encrypted communication link between a "network device" or "first network device" and a "second network device," any proposed construction of "secure communications service" should use those terms instead of "computer," as proposed by Petitioner.

Petitioner's use of "computer" for the claimed "network devices" is incorrect. The specification provides a variety of examples that do not involve traditional computers and may instead involve telephones or other devices. For example, it discloses "video conferencing, e-mail, word processing programs, telephony, and the like." (Ex. 1003 at 21:62-64.) And dependent claims 3-5 and 16-18 are directed to a telephony secure communications service.

Accordingly, "secure communications service" should be construed to mean "the functional configuration of a network device that enables it to participate in a secure communications link with another network device."

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

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

Claims 1 and 14 of the '009 patent recite the phrase "an indication that the second network device is available for the secure communications service." (Ex. 1003, claims 1 and 14.) As recognized by a district court in a litigation involving related patents, the plain meaning of the term "indication" is readily understandable, so it does not require further construction. (*See* Ex. 2004 at 27-28, 31, Memorandum Opinion and Order in the '417 litigation (E.D. Tex. Apr. 25, 2012); Ex. 2005 at 10, Memorandum Opinion and Order in *VirnetX Inc. v. Mitel Networks Corp. et al.*, Case No. 6:11-CV-18 (E.D. Tex. Aug. 1, 2012).)

Furthermore, 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." Applying Petitioner's construction, 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.

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

Patent Owner's Proposed Construction	Petitioner's Proposed 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

The plain meaning of a "virtual private network communication link" (or "VPN communication link") 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. 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.

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; *see* Ex. 2010, *Apple Inc. v. VirnetX, Inc.*, IPR2014-00481, Declaration of Fabian Monrose, Ph.D. (Jan. 5, 2015) at ¶ 15) 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; *see* Ex. 2010, *Apple Inc. v. VirnetX, Inc.*, IPR2014-00481, Declaration of Fabian Monrose, Ph.D. (Jan. 5, 2015) at ¶ 15.) Notably, secure server 3320 "can only be accessed through a VPN communication link." (Ex. 1003 at 52:9-10; *see* Ex. 2010, *Apple Inc. v. VirnetX, Inc.*, IPR2014-00481, Declaration of Fabian Monrose, Ph.D. (Jan. 5, 2015) at ¶ 15.) And "[f]urther communication between computers 3301 and 3320 occurs via the VPN" through the VPN communication link. (Ex. 1003 at 52:40-42; *see* Ex. 2010, *Apple Inc. v. VirnetX, Inc.*, IPR2014-00481, Declaration of Fabian Monrose, Ph.D. (Jan. 5, 2015) at ¶ 16.)

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. (*See* Ex. 2009, IPR2014-00237, Declaration of Fabian Monrose, Ph.D. (Aug. 28, 2014) at 11, ¶ 15.) The other techniques alone do not "hide information on the path," as Petitioner's construction requires. (*Id.*)

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; *see* Ex. 2009, IPR2014-00237, Declaration of Fabian Monrose, Ph.D. (Aug. 28, 2014) at 12, ¶ 16.) It does not prevent an eavesdropper from accessing data transmitted over an unsecure communication link. (*See* Ex. 2009, IPR2014-00237, Declaration of Fabian Monrose, Ph.D. (Aug. 28, 2014) at 12, ¶ 16.) 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; *see* Ex. 2009, IPR2014-00237, Declaration of Fabian Monrose, Ph.D. (Aug. 28, 2014) at 12, ¶ 16.)

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. (*See* Ex. 2009, IPR2014-00237, Declaration of Fabian Monrose, Ph.D. (Aug. 28, 2014) at 12-13, ¶ 17.) 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"; *see* Ex. 2009, IPR2014-00237, Declaration of Fabian Monrose, Ph.D. (Aug. 28, 2014) at 12-13, ¶ 17.) 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; *see also* Ex. 2009, IPR2014-00237, Declaration of Fabian Monrose, Ph.D. (Aug. 28, 2014) at 12-13, ¶ 17.)

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. (*See, e.g.*, Ex. 2009, IPR2014-00237, Declaration of Fabian Monrose, Ph.D. (Aug. 28, 2014) at 14, ¶ 20.) 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 III.E. 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.) 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.

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 III.I.1) and therefore must be between computers in a network. (*See* Ex. 2010, *Apple Inc. v. VirnetX, Inc.*, IPR2014-00481, Declaration of Fabian Monrose, Ph.D. (Jan. 5, 2015) at ¶ 19.) 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." (*See* Ex. 2010, *Apple Inc. v.*

VirnetX, Inc., IPR2014-00481, Declaration of Fabian Monrose, Ph.D. (Jan. 5, 2015) at ¶ 19.)

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, 24:59.) More specifically, the network allows "[e]ach node . . . to communicate with other nodes in the network." (Ex. 1003 at 17:40-42; Ex. 2010, *Apple Inc. v. VirnetX, Inc.*, IPR2014-00481, Declaration of Fabian Monrose, Ph.D. (Jan. 5, 2015) at ¶ 20.) So a device within a VPN is able to communicate with the other devices within that same VPN. (Ex. 2010, *Apple Inc. v. VirnetX, Inc.*, IPR2014-00481, Declaration of Fabian Monrose, Ph.D. (Jan. 5, 2015) at ¶ 20.) 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, 26-29; Ex. 2010, *Apple Inc. v. VirnetX, Inc.*, IPR2014-00481, Declaration of Fabian Monrose, Ph.D. (Jan. 5, 2015) at ¶ 20, Monrose Decl.)

Accordingly, Petitioner's proposed construction should be rejected.

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

While the issue of whether a "virtual private network communication link" requires encryption does not appear to be relevant to the parties' disputes given

claim 8's recitation that "the encrypted communication link is part of a virtual private network communication link," Petitioner's proposed construction incorrectly neglects to require encryption at least over insecure communication paths between the devices.

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).) 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).)

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

Patent Owner's Proposed Construction	Petitioner's Proposed Construction
A name corresponding to a network address	A name corresponding to an IP address

The BRI of "domain name" is "a name corresponding to a network address." 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.) The '009 patent claims support this construction by reciting that the DNS request is "to look up a **network address** of a second network device" based on a domain name. (*See, e.g.,* Ex. 1003, claims 1 and 7.)

Patent Owner's construction is also consistent with the specification, which explains that Internet Protocol or "IP" is but one type of network. (*See, e.g.,* Ex. 1003 at 4:23, 5:17-18, 11:60-62.) The specification also contemplates "'boutique' embodiments . . . for use in smaller networks, such as small virtual private networks" instead of large networks like the Internet, where IP addresses are commonplace. (Ex. 1003 at 17:2-6.) Nothing requires these smaller networks to use IP addresses. The specification similarly contemplates applications including "video-conferencing, e-mail, word processing programs, telephony, and the like," which do not necessarily use IP addresses. (Ex. 1003 at 21:62-64.)

Accordingly, under the applicable BRI standard, a "domain name" is "a name corresponding to a network address."

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

Patent Owner's Proposed Construction	Petitioner's Proposed 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

The meaning of "modulation" is apparent to one skilled in the art without construction. Should the Board deem further 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.) As the Petitioner notes, the Board has previously agreed with this construction. (*Id.*, citing IPR2014-00237, Paper No. 15 at 14 (May 14, 2014).)

IV. Conclusion

For these reasons, Patent Owner respectfully requests that the Board deny the petition for *inter partes* review.[4]

[4] If trial is instituted, Patent Owner reserves its rights to raise additional arguments as to why Petitioner has failed to carry its burden and why the claims should be confirmed.

Respectfully submitted,

Dated: June 15, 2015

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

Counsel for VirnetX Inc.

Certificate of Service

I certify that I caused to be served on the counsel identified below a true and correct copy of the foregoing Patent Owner's Preliminary Response by electronic means on June 15, 2015:

Counsel for Apple Inc.:

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

Dated: June 15, 2015

Respectfully submitted,

/Joseph E. Palys/
Joseph E. Palys
Reg. No. 46,508
Counsel for VirnetX Inc.