Paper No. _____
Filed: May 19, 2014

Filed on behalf of: VirnetX Inc.
By: Joseph E. Palys
Naveen Modi
Finnegan, Henderson, Farabow,
Garrett & Dunner, L.L.P.
11955 Freedom Drive
Reston, VA 20190-5675
Telephone: 571-203-2700
Facsimile: 202-408-4400
E-mail: joseph.palys@finnegan.com
naveen.modi@finnegan.com

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

MICROSOFT CORPORATION
Petitioner

v.

VIRNETX INC.
Patent Owner

Case IPR2014-00404
Patent 7,987,274

Patent Owner's Preliminary Response to Petition for *Inter Partes* Review of U.S. Patent No. 7,987,274

Table of Contents

TABLE OF AUTHORITIES

Page(s)

Federal Cases

Federal Statutes

Regulations

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 Revised Petition for *Inter Partes* Review (the "Petition") filed by Microsoft Corporation against VirnetX's U.S. Patent No. 7,987,274 ("the '274 patent). VirnetX requests that the Board not institute *inter partes* review for several reasons.

First, the Petition fails to identify where 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). Next, the Petition proposes redundant grounds without identifying how any one ground improves on any other, violating Board precedent requiring petitioners to identify differences in the proposed rejections. Finally, Microsoft proposes a series of incorrect claim constructions. Because its unpatentability challenges are premised on incorrect claim constructions, Microsoft has not met its burden of demonstrating a reasonable likelihood of prevailing in proving unpatentability of any '274 patent claim.

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

A. The Petition Fails to Comply with 35 U.S.C. § 312(a)(3) and 37 C.F.R. § 42.104(b)

Independent claim 1 recites, among other things, "sending an access request message to the secure computer network address using a virtual private network

communication link." Nowhere does the Petition explain where a purported "access request message" is disclosed in *Kiuchi*. Nor does the accompanying declaration provide the missing explanation. Consequently, the Petition fails to satisfy the substantive requirements for institution set forth in 35 U.S.C. § 312(a)(3) and 37 C.F.R. §§ 42.104(b)(4), 42.104(b)(5), and should be denied.

Petitions must identify "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). They must also "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)) and identify "specific portions of the evidence that support the challenge" (37 C.F.R. § 42.104(b)(5)). Failure to comply with these substantive requirements for petitions warrants denial of a petition. *Apple Inc. v. Evolutionary Intelligence, LLC*, IPR2014-00079, Paper No. 8 at 17-19 (Apr. 25, 2014); *Wowza Media Sys., LLC et al. v. Adobe Sys., Inc.*, IPR2013-00054, Paper No. 16 at 3, 6 (July 13, 2013); *Tasco, Inc. v. Pagnani*, IPR2013-00103, Paper No. 6 at 18-22 (May 23, 2013); *Atrium Med. Corp. v. Davol Inc.*, IPR2013-00186, Paper No. 34 at 3 (Oct. 23, 2013); *Synopsys, Inc. v. Mentor Graphics Corp.*, IPR2012-00041, Paper No. 16 at 14-15 (Feb. 22, 2013). As the Board has explained, it will not "search the record and piece together any evidence or arguments that may support Petitioner's

ultimate conclusion." *CaptionCall, LLC v. Ultratec, Inc.*, IPR2013-00549, Paper No. 20 at 5 (Apr. 28, 2014).

The Petition contends that a "REQUEST" message mentioned in *Kiuchi* corresponds to "sending an access request message to the secure computer network address using a virtual private network communication link," as recited in independent claim 1.[1] Specifically, the Petition cites "step 6" of section 2.3 of *Kiuchi*. (Pet. at 30 (citing Ex. 1004, p. 66, § 2.3, step 6).) This portion of *Kiuchi* simply states:

> 6) Sending C-HTTP requests to the server-side proxy (Fig. 2g)
>
> Once the connection is established, a client-side proxy forwards HTTP/1.0 requests from the user agent in encrypted form using C-HTTP format.

According to the Petition, the example *Kiuchi* provides with reference to Figs. (a), (b), and (c) involves the end-user's request for "the resource 'sample.html' from the server-side proxy corresponding to the hostname 'server.in.current.connection,'" which the "client-side proxy will forward" using the C-HTTP connection. (*Id*. at 31.)

[1] The Board recently entered a new ground of rejection in pending reexamination control no. 95/001,792 of the '180 patent, which relies in part on mapping *Kiuchi*'s request in "step (6)" to the recited "access request message."

Next, the Petition contends that each "REQUEST" message "include[s] the IP address of the server-side proxy, which the client-side proxy received from the C-HTTP name server." (*Id*. at 30 (citing Ex. 1004, p. 70-71, Appendix 1, § 1; Ex. 1011 ¶ 40).) The Petition further cites Appendix 3 of *Kiuchi*, which the Petition contends illustrates an "example of the structure of these REQUEST messages." (*Id*. at 32-33 (citing Ex. 1011 ¶ 41).) In addition, the Petition generally cites the Abstract of *Kiuchi* for the general proposition that "Kiuchi further describes that the client-side proxy and server-side proxy exchange encrypted requests and responses via the Internet." (*Id*. at 32 (citing Ex. 1004, p. 64, abstract).)

Despite its general citation to a "REQUEST" message and an exchange of requests, the Petition fails to explain why these messages constitute an "access request message" as recited in the challenged claims. The Petition offers no construction for "sending an access request message," and it is unclear from the Petition why Microsoft believes that *Kiuchi*'s "REQUEST" satisfies the claim language. The cited portions of the accompanying declaration also fail to provide the missing explanation. (*See* Ex. 1011 ¶ 40 (also referring to the "example of a request for the resource 'sample.html' using an existing C-HTTP connection"); *id*. at ¶ 43 (stating that "the access request sent using the C-HTTP connection" is shown in red in an annotated figure of *Kiuchi*).)

The Petition's claim chart contains the same defects. The claim chart cites portions of *Kiuchi* discussing "a client-side proxy forward[ing] HTTP/1.0 requests from the user agent in encrypted form using C-HTTP format." (*Id*. at 36 (citing Ex. 1004, p. 66, § 6).) The claim chart also refers to the structure of a C-HTTP request as including the IP address of the server-side proxy. (*Id*. at 36 (citing Ex. 1004, p. 71, Appendix 1, § 1).) But beyond indicating that a request message is sent from the client-side proxy to the server-side proxy, the Petition fails to explain why the request message is an "access request message," as recited in independent claim 1.

Because the Petition fails to explain how *Kiuchi* discloses "sending an access request message to the secure computer network address using a virtual private network communication link," as recited in independent claim 1, the Petition does not demonstrate how *Kiuchi* anticipates each and every limitation of the challenged claims. The Petition lacks the "particularity" required by 35 U.S.C. § 312(a)(3), and fails to "specify where each element of the claim is found in the prior art patents or printed publications relied upon" and identify "specific portions of the evidence that support the challenge," as required by 37 C.F.R. §§ 42.104(b)(4) and 42.104(b)(5)). *See Apple Inc. v. Evolutionary Intelligence, LLC*, IPR2014-00079, Paper No. 8 at 17-19 (Apr. 25, 2014) (relying on 37 C.F.R. §§ 42.104(b)(4), (b)(5) and rejecting a petition because its discussion of the prior

art "refers generally" to features of the prior art and is "vague" for certain limitations). The Petition should be denied based on these substantive defects.

B. The Board Should Not Institute Based on the Petition's Redundant Grounds

The Petition includes a section titled "Redundancy," which does not assert or explain why the proposed grounds of rejection in the Petition are not redundant in view of those in the Microsoft's Petition for *Inter Partes* Review in IPR2014-00403 ("the'403 Petition"). Instead, the Petition alleges that Microsoft's two petitions against the '274 patent present a "limited number" of grounds and then alleges some teachings of the primary references. (Pet. at 50.) Giving no justification based on the Board's jurisprudence regarding redundancy, Microsoft's redundant grounds should be rejected.

The Board does not consider redundant grounds of rejection because it must issue a final written decision within one year of institution (or 18 months for good cause). *Liberty Mut. Ins. Co. v. Progressive Cas. Ins. Co.*, CBM2012-00003, Paper No. 7 (Oct. 25, 2012). 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. *Id*.

Because "[t]he Board seeks to streamline and converge issues at all phases of the proceeding . . . at [the] time of institution the Board analyzes the petition on a claim-by-claim, ground-by-ground basis, to eliminate redundant grounds." *Idle*

Free Sys., Inc. v. Bergstrom, Inc., IPR2012-00027, Paper No. 26 at 3 (June 11, 2013). 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). Instead, the Board considers "whether the petitioner articulated 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. The petitioner carries the burden of articulating that "meaningful distinction." *ScentAir Techs., Inc. v. Prolitec, Inc.*, IPR2013-00180, Paper No. 18 at 3 (Aug. 26, 2013).

In *Liberty Mutual*, the Board identified two types of redundant rejections: (1) "horizontally" redundant rejections and (2) "vertically" redundant rejections. *Liberty Mutual*, 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, Microsoft's Petition is horizontally redundant in view of the '403 Petition. In this Petition, Microsoft alleges that *Kiuchi* anticipates claims 1-4, 7, 8, 10, 12, 15, and 17. Yet in the '403 Petition, Microsoft alleges that *Provino* anticipates an overlapping group of claims, namely claims 1, 7, 8, 10, 12, 13, 15, and 17. Further, the present Petition contends that *Kiuchi* in view of two other references renders obvious claims 1-5, 7, 8, 10, 12, 15, and 17. And in the '403 Petition, Microsoft contends that *Provino* in view of two other references renders obvious claims 2-5 and 18. Microsoft's *Kiuchi*-based grounds of rejection are horizontally redundant in view of its *Provino*-based grounds of rejection. Furthermore, the present Petition's anticipation ground for claims 1, 4, 10, 12-15, 17, 20, 26, 28-31, 33, and 35 based on *Kiuchi* is vertically redundant in view of its proposed obviousness ground for the same claims with *Kiuchi* asserted as the lead reference. In addition, Microsoft's Petition is horizontally redundant in view of Apple's two petitions challenging common claims of the '274 patent—IPR2014-00483 and IPR2014-00484.

Microsoft does not explain why its two petitions' respective grounds of rejection are not redundant. Microsoft expresses its belief that *Provino* discloses a "virtual private network" and "communication link," and that *Kiuchi* discloses a "C-HTTP name server send[ing] the IP address and public key of the server-side proxy and both request and response Nonce values used in communication." (Pet.

at 50 (emphasis in original).) But Microsoft 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." *EMC Corp. v. Personal Web Techs., LLC*, IPR2013-00087, Paper No. 25 at 3-4 (June 5, 2013) (emphases added). Microsoft has essentially admitted that it proposes redundant grounds but has not explained why any of its grounds are not redundant. Consequently, the Board should deny Microsoft's redundant grounds. *ScentAir Techs., Inc. v. Prolitec, Inc.*, IPR2013-00180, Paper No. 18 at 3 (Aug. 26, 2013).

C. Microsoft's Arguments About the Priority Date of Claim 18 Are Incorrect and Moot

Microsoft contends that claim 18 of the '274 patent should "be accorded a priority date no earlier than the date on which the '274 patent was filed: August 16, 2007." (Pet. at 21.) Microsoft is incorrect. When claim 18 was added during prosecution of the '274 patent application, the Examiner did not find any problems regarding written description support. Instead, the Examiner noted that "claims 2-18 [were] newly added for examination," and proceeded to reject the claims on other grounds. (Ex. 1002 at 296.) The Examiner was correct in not finding a lack of written description support. The '274 patent specification provides adequate written description support for claim 18. (*See, e.g.*, Ex. 1001 at 21:20-22, 34:36-42, 45:8-49:13, 52:15-18; Figs. 12A, 33, 34, 35.)

In any event, Microsoft's argument about priority dates is entirely academic. The Petition does not challenge claim 18 at all, so Microsoft's arguments regarding the priority date of claim 18 have no bearing on the Petition and should be disregarded.

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

Microsoft proposes several defective claim constructions that do not represent the broadest reasonable interpretation ("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 '274 patent.

A. Overview of the '274 Patent

The '274 patent discloses several embodiments relating to accessing secure network addresses using virtual private network communication links. In one embodiment, as shown in FIG. 33 reproduced below, a client computer 3301 may send a query message to a specialized, secure DNS server 3313 requesting a secure network address for a second network device. (Ex. 1001 at 46:44-47, 60-62.) The client computer 3301 may receive a response message from the secure DNS server 3313 containing the secure network address, and then send an access request message to the secure computer network address. (*Id.* at 47:15-37.) The access request message is sent over a virtual private network communication link, i.e., a communication link over a virtual private network. (*Id.* at 47:37-51.)

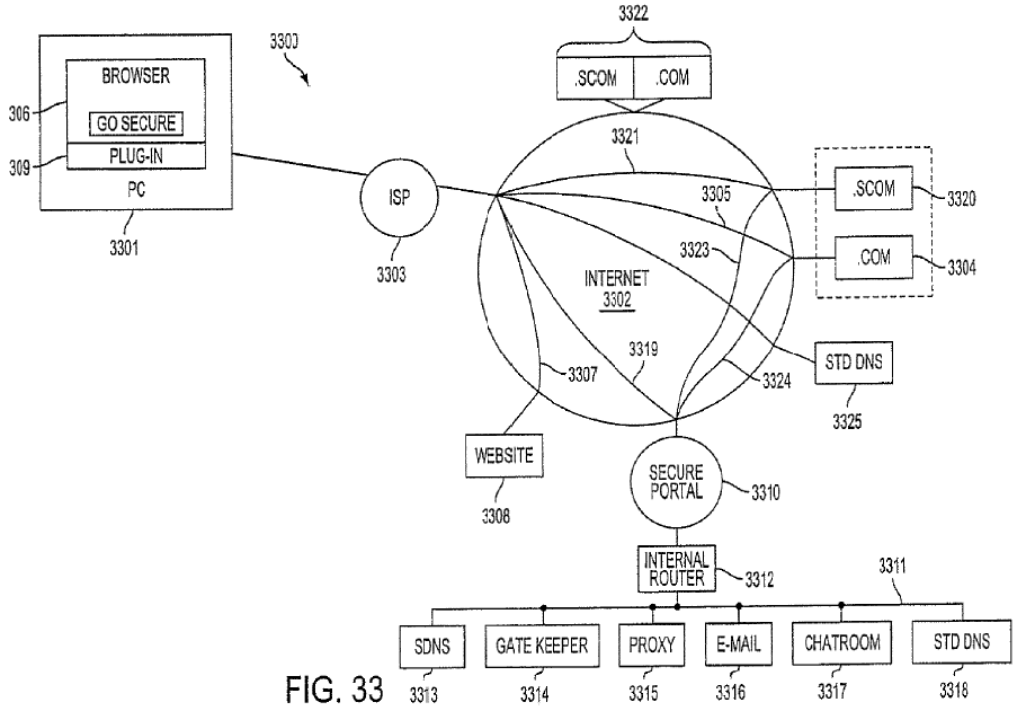

FIG. 33

(Ex. 1001, FIG. 33.)

The claims of the '274 patent are directed to some of these embodiments. Claim 1 is the only independent claim, and claims 2-18 depend directly or indirectly from claim 1.

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. In litigation related to VirnetX's patents, this level of skill was adopted by a host of companies, including Apple, Inc.; Cisco Systems, Inc.; NEC Corporation; NEC Corporation of America; Aastra USA, Inc.; Aastra Technologies Ltd.; Mitel

Networks Corp.; Mitel Networks, Inc.; Siemens Enterprise Communications GmbH & Co. KG; Siemens Enterprise Communications, Inc.; and Avaya Inc. (Ex. 2023 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. 1018 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).)

Microsoft largely agrees with VirnetX's proposed level of skill, contending through its expert that "one of ordinary skill . . . would have a Master's degree in computer science or computer engineering, or in a related field such as electrical engineering, as well as about two years of experience in computer networking and in some aspect of security with respect to computer networks." (Ex. 1011 at 3, ¶ 7.) Because so many companies have agreed that VirnetX's proposed level of skill is correct and because Microsoft's proposed level of skill is similar in most respects, the Board should adopt VirnetX's proposed level of skill.

C. "Virtual Private Network" (Construe as Part of "Virtual Private Network Communication Link")

VirnetX's Proposed Construction	Microsoft's Proposed Construction
Not a separate claim term, construe as part of "virtual private network communication link"; alternatively, a network of computers which privately and directly communicate with each other by encrypting traffic over insecure communication paths between the computers	A network of computers that privately communicate with each other by encrypting traffic on insecure communication paths between the computers

The term "virtual private network" does not require construction here because the term is not separately recited in the '274 patent claims. (*See* Ex. 1001 at 51:53-52:57.) Instead, it forms part of "virtual private network communication link," which is construed separately elsewhere. (*See infra* Section III.D.)

Should the Board deem construction necessary, VirnetX and Microsoft largely agree on the construction of "virtual private network" (or "VPN"). The main point of dispute is whether the computers in the network must be able to directly communicate. Microsoft relies on a district court's interpretation of the term in the 2007 Microsoft Litigation (Pet. at 8-9), but it does not mention that the district court later revised its construction to require the ability to directly communicate. (Ex. 1018 at 6-8.) The district court reviewed the reexamination record of related U.S. Patent No. 6,502,135 ("the '135 patent"), where VirnetX distinguished a reference referred to as *Aventail* on the ground that it did not disclose a VPN because, among other things, "computers connected according to

Aventail do not communicate directly with each other." (*See* Ex. 2024 at 7, Office Action Response filed April 15, 2010, in control no. 95/001,269.) The district court relied on this statement to construe "virtual private network" to require the ability to directly communicate.[2] (*See* Ex. 1018 at 6-8.)

VirnetX also made a virtually identical statement during reexamination of parent U.S. Patent 7,188,180 ("the '180 patent), which recites a "virtual private network" in its claims. VirnetX said that "Aventail has not been shown to disclose a VPN, as recited in claim 1, 17, and 33, because computers connected according to Aventail do not communicate directly with each other." (Ex. 1023 at 166.) Given the identical term for construction and nearly verbatim reexamination statements regarding the '135 and '180 patents, the district court's reasoning should apply with equal force here. The ability to directly communicate should be part of the construction.

The portions of the construction on which VirnetX and Microsoft agree are supported by the patent specification. For example, the specification discloses

[2] VirnetX did not disclaim claim scope regarding "virtual private network" in the sense that only certain types of VPNs fall within the scope of the claims. VirnetX merely explained that *Aventail* did not create a VPN in the ordinary sense of the term. The court treated VirnetX's explanation of an ordinary VPN as a disclaimer by adopting it as part of its claim construction.

techniques for implementing a VPN using encryption. (*See, e.g.*, Ex. 1001 at 3:13-4:13 (describing "the Tunneled Agile Routing Protocol (TARP) [that] uses a unique two-layer encryption format").) The specification also discloses that its later-discussed embodiments can use the earlier-discussed principles of encryption, identifying "different embodiments or modes that can be employed using the aforementioned principles." (*Id.* at 24:34-35; *see also id.* at 33:65-66 ("The following describes various improvements and features that can be applied to the embodiments described above.").)

The specification also refers to the "FreeS/WAN" project as a conventional scheme of creating a "VPN." (Ex. 1001 at 39:14-22.) The FreeS/WAN glossary of terms in the '274 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. 2025 at 24, Glossary for the Linux FreeS/WAN Project.) A contemporaneous dictionary similarly explains that "VPNs enjoy the security of a private network via access control and *encryption* . . . ." (Ex. 2026 at 8, *McGraw-Hill Computer Desktop Encyclopedia* (9th ed. 2001) (emphasis added).) Thus, both intrinsic and extrinsic evidence demonstrate that VPNs require encryption.

VirnetX's construction is also consistent with the constructions presented and adopted in three district court litigations involving patents in the same family

as the ’274 patent that similarly recited a “virtual private network” in their claims. In those cases, VirnetX and the defendants proposed several different claim constructions, all of which included encryption. (*See, e.g.*, Ex. 2027 at 9-14, Microsoft’s Responsive Claim Construction Brief in *VirnetX, Inc. v. Microsoft Corp.*, Case No. 6:07-CV-80 (E.D. Tex. Jan. 20, 2009); Ex. 2028 at 2-3, Defendants’ Responsive Claim Construction Brief in *VirnetX Inc. v. Cisco Systems, Inc. et al.*, Case No. 6:10-CV-417 (E.D. Tex. Dec. 7, 2011); Ex. 2029 at 8, Defendants’ Responsive Claim Construction Brief in *VirnetX Inc. v. Mitel Networks Corp. et al.*, Case No. 6:11-CV-18; Ex. 2030 at 9-13, VirnetX’s Opening Claim Construction Brief in *VirnetX Inc. v. Microsoft Corp.*, Case No. 6:07-cv-00080.) In all three instances, the court construed “VPN” to require encryption. (*See* Ex. 1016 at 4-10; Ex. 2023 at 4-6; Ex. 1018 at 5-8.) While the Office construes the claims under a different standard than the district court, this consistent understanding by all parties and the district court is additional evidence that the BRI of VPN requires encryption.

VirnetX’s construction is supported by intrinsic and extrinsic evidence, so “virtual private network” should be construed to mean “a network of computers

which privately and directly communicate with each other by encrypting traffic over insecure communication paths between the computers."[3]

D. "Virtual Private Network Communication Link" (Claims 1, 2, and 11-13)[4]

VirnetX's Proposed Construction	Microsoft's Proposed Construction
A communication path between computers in a virtual private network	Any communication link between two end points in a virtual private network

A "virtual private network communication link" (or "VPN communication link") is "a communication path between computers in a virtual private network." The plain meaning of the claim language and the patent specification support this construction. (*See, e.g.*, Ex. 1001 at 47:66-48:6.)

---

[3] In IPR2014-00237 and -00238, the Board preliminarily construed "virtual private network" in the context of related U.S. Patent No. 8,504,697 to mean "a 'secure communication link' with the additional requirement that the link includes a portion of a public network." (*See, e.g.*, IPR2014-00237, Paper No. 15 at 12 (May 14, 2014).) VirnetX respectfully disagrees with the Board's construction and will present additional evidence and argument supporting its construction in those proceedings.

[4] VirnetX 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.

VirnetX's proposed construction is similar to Microsoft's and Apple's, which are identical. (*Compare* Pet. at 6-9 *with* Ex. 2031 at 6, Pet. in IPR2014-00481.) A primary difference between the parties' constructions is the use of "end points" in Microsoft's and Apple's constructions. "End points" might inaccurately suggest that no additional computers in the VPN may be "behind" the computers communicating over the VPN communication link. A "network" includes numerous interconnected communication paths and, thus, may be configured in a way that has no "beginning" or "end," such as in a ring network topology. To the extent Microsoft's and Apple's construction implies that topologies of this type are not networks, the construction is incorrect and should be rejected. VirnetX proposes using "computers" instead of "end points" to avoid this issue.

Although Microsoft contends that "VirnetX has not proposed a specific definition for . . . a virtual private network communication link" in the co-pending reexamination of the parent '180 patent (Pet. at 7), VirnetX did provide a construction and supported it with expert testimony and specification citations. (*See, e.g.*, Ex. 1024 at 315-316, Dec. 19, 2012 Response at 6; *id.* at 334, Dec. 19, 2012 Keromytis Declaration at ¶ 24, defining it as "a communication path between computers in a virtual private network.") It is the same construction VirnetX

proposes here, and the evidence cited in the reexamination and submitted here supports VirnetX's construction.[5]

E. "Secure Network Address" (Claims 1, 6-8, 10, and 17)

VirnetX's Proposed Construction	Microsoft's Proposed Construction
A network address that requires authorization for access and is associated with a computer capable of virtual private network communications	A network address that requires authorization for access and is associated with a computer configured to be accessed through a virtual private network

The broadest reasonable interpretation of "secure network address" is "a network address that requires authorization for access and is associated with a computer capable of virtual private network communications." Microsoft's proposed construction is close to VirnetX's proposed construction, with Microsoft contending the term means "a network address that requires authorization for access and is associated with a computer configured to support virtual private

[5] In reexamination control no. 95/001,792, the Board adopted a construction of VPN communication link that is broader than the constructions proposed in the IPRs. VirnetX is seeking to reopen prosecution, and will be presenting evidence and explanation as to why the Board's construction is incorrect. For the IPRs, the Board may adopt a construction consistent with the parties' proposals, as that construction is all that is necessary to resolve the dispute between the parties.

network communications." (Pet. at 10.)[6] These constructions are consistent with the surrounding claim language, the specification, statements in a prior reexamination of the parent '180 patent, the construction adopted by a district court, and the construction agreed to by VirnetX's litigation adversaries.

The parties agree that a "secure network address" requires, among other things, "authorization for access." In adopting this requirement, a district court explained that, because the parent '180 patent claims recite "sending an access request message to the secure computer network address," "there must be a request made to the 'secure computer network address' in order to access the 'secure computer network address." (Ex. 1016 at 28-29.) At Microsoft's urging, the court concluded that authorization was required. (*Id.*) That the network address "requires authorization for access" is also evident from VirnetX's statements

[6] In IPR2014-00403 and -00404, Microsoft simultaneously proposed two different constructions for "secure network address." (*Compare* Pet. at 5, *with id.* at 10.) However, both constructions agree that the network address requires authorization for access and is associated with a computer configured to have a relationship to a virtual private network. Microsoft phrases the relationship between the computer and the virtual private network differently in each construction, but does not explain the difference or its significance. (*See id.* at 6, 10-11.)

during reexamination of the parent '180 patent, which distinguished several references for failing to disclose a network address that requires authorization. (*See* Ex. 1023 at 159, 168-70, 180, 184, 187 (Office Action Response filed April 19, 2010, in control no. 95/001,270).) Since the same language "sending an access request message . . . to the secure network address" is found in the '274 patent, the same reasoning applies here as well.

The parties also agree that the "secure network address" is "associated with a computer" having a relationship to a virtual private network. This association with a computer is evident from the claim language, which recites that the "secure network address" is "for the second network device" that may be a computer. It is also supported by the specification, which describes a computer (e.g., a secure server) being at a secure network address. (Ex. 1001 at 47:38-51.)

The parties diverge on the particular relationship between the associated computer and the virtual private network. VirnetX proposes that the computer is "capable of virtual private network communications," while Microsoft proposes that the computer is "configured to be accessed through a virtual private network" (Pet. at 5) or is "configured to support virtual private network communications" (*id.* at 9-10). VirnetX's construction is supported by the claim language, which recites "sending an access request message . . . to the secure network address using a virtual private network communication link." (*See, e.g.*, Ex. 1001 at 52:5-7.) For

the sending to occur as claimed, the computer must be capable of virtual private network communications. VirnetX's construction is also supported by the patent specification, which discloses that a secure server at a secure computer network address has the capability to communicate in a virtual private network. (Ex. 1001 at 48:36-49.)

VirnetX's construction has been agreed to by its litigation adversaries and has been adopted by a district court. (Ex. 1016 at 28-29; Ex. 1017 at 19.) While the Office construes claims under a different standard than courts, this consistent understanding of the phrase "secure network address" demonstrates that VirnetX's construction is correct.

Microsoft's constructions, on the other hand, are proposed here for the first time and Microsoft provides no support for either of them. Instead, Microsoft argues that "the broadest reasonable interpretation of the term 'secure network address' should be considered in light of the features referenced by VirnetX" during reexamination and in its 2007 litigation against Microsoft. (Pet. at 9.) But in the 2007 litigation, VirnetX proposed that the computer be "capable of virtual private network communications," just as VirnetX proposes here. (Ex. 1016 at 28.) It is unclear why Microsoft advocates for adopting VirnetX's prior statements but then proposes constructions that do not accurately reflect those prior statements. To the extent Microsoft's proposed constructions deviate from

VirnetX's prior statements and constructions, they should be rejected, as Microsoft has not explained why the deviation is necessary or is otherwise supported. (*See* Pet. at 9-10.)

F. "Secure Domain Name" (Construe as Part of "Secure Domain (Name) Service")

VirnetX's Proposed Construction	Microsoft's Proposed Construction
Not a separate claim term, construe as part of "secure domain name service"; alternatively, a non-standard domain name that corresponds to a secure computer network address and cannot be resolved by a conventional domain name service (DNS)	A non-standard domain name that corresponds to a secure computer network address and cannot be resolved by a conventional domain name service (DNS)

The term "secure domain name" does not require construction here because the term is not separately recited in the '274 patent claims. (*See* Ex. 1001 at 51:53-52:57.) Instead, it forms part of "secure domain name service," which is construed separately elsewhere. (*See infra* Section III.G.)

If the Board deems construction necessary, the parties agree that "secure domain name" means "a non-standard domain name that corresponds to a secure computer network address and cannot be resolved by a conventional domain name service (DNS)." (Pet. at 5, 10-11.) This same construction was agreed to by the parties in a litigation involving VirnetX and Cisco Systems, Inc. (Ex. 1017 at 19-20.) In addition to this confirmation from multiple parties that the proposed

construction here is correct, the specification and claim language support the construction.

The specification teaches that a "secure domain name" may be "a non-standard domain name." (Ex. 1001 at 7:26-28; 46:31-40.) Examples of "a non-standard domain name" are provided in the specification : .scom, .snet, .sorg, .sedu, .smil, and .sgov. (*Id.* at 7:36-39.)

The specification also explains that "secure domain name" "corresponds to a secure computer network address." For example, the specification explains that "SDNS 3313 contains a cross-reference database of secure domain names and corresponding secure network addresses." (*Id.* at 47:15-19.) Because a "secure domain name" is "a non-standard domain name," the specification explains that "a query to a standard domain name service (DNS) will return a message indicating that the universal resource locator (URL) is unknown." (*Id.* at 46:41-44; Figs. 33, 34.) To obtain the URL for a "secure domain name," "a secure domain name service (SDNS)" must be queried. (*Id.* at 46:44-47; Figs. 33, 34.) The claims acknowledge this fact by reciting that the query message is sent to "a secure domain name service" as opposed to a conventional DNS.

Because each aspect of the parties' construction of "secure domain name" is supported by intrinsic and extrinsic evidence, the Board should adopt the parties' construction that "secure domain name" means "a non-standard domain name that

corresponds to a secure computer network address and cannot be resolved by a conventional domain name service (DNS)."

G. "Secure Domain (Name) Service" (Claim 1)

VirnetX's Proposed Construction	Microsoft's Proposed Construction
A lookup service that recognizes that a query message is requesting a secure computer address, and returns a secure computer network address for a requested secure domain name	A service that can resolve secure computer network addresses for a secure domain name for which a conventional domain name service cannot resolve addresses

"Secure domain (name) service"[7] ("SDNS") refers to "a lookup service that recognizes that a query message is requesting a secure computer address, and returns a secure computer network address for a requested secure domain name." The intrinsic record supports this view. For example, the '274 patent specification explains that "[a]n entity can register a secure domain name in SDNS 3313 so that a user who desires a secure communication link to the website of the entity can automatically obtain the secure computer network address for the secure website." (Ex. 1001 at 47:19-22.) Upon registration, the SDNS recognizes whether a received DNS query is requesting a secure computer network address. (*E.g.*, *id.* at 47:33-37, "[w]hen a user queries SDNS 3313 for the secure computer network

[7] "Name" is in parentheses because the '274 patent claims recite "secure domain service" and "secure domain name service." The parties agree that both terms should receive the same construction for purposes of the '274 patent.

address for the [registered secure domain name], SDNS 3313 determines the particular secure computer network address based on the user's identity and the user's subscription level.') If so, the SDNS returns a secure computer network address for a requested secure domain name. (*E.g.*, *id.* at 47:48-51, "in step 3410, SDNS 3313 returns a secure URL to software module 3309 for the .scom server address for a secure server 3320 corresponding to server 3304.")

The independent claims also recite that the secure computer network address is received from the SDNS in response to the SDNS query message. (*See, e.g.*, *id.* at 51:53-52:7.) So the SDNS must not only be able to recognize the nature of the query message, but also to return the secure computer network address as proposed in VirnetX's construction. Dependent claim 17 also supports the SDNS's "recognition" capability by reciting that "the secure network address is registered with the secure domain service prior to the step of sending a query message to a secure domain service." (*Id.* at 52:50-53.)

A district court has adopted the construction VirnetX proposes here, except it added "non-standard" before "lookup service." (Ex. 1018 at 17-19.) Microsoft's construction contains a similar non-"conventional" requirement. (Pet. at 6.) The broadest reasonable construction, however, does not require this limitation.

Although VirnetX's and Microsoft's constructions share some common aspects, Microsoft's proposed construction is technically inaccurate to the extent it

suggests that the SDNS resolves secure computer network addresses. A domain name service "resolves" domain names into addresses, but it does not "resolve" the addresses themselves.[8] While one of ordinary skill in the art could refer to the returned address as a "resolved" address, the skilled artisan would understand that the resolution occurs on the name, not the address.

H. "[X], [Y], [Z], or Any Combination Thereof" (Claims 3-5)

VirnetX's Proposed Construction	Microsoft's Proposed Construction
No construction necessary	Any one of the elements [x], [y], or [z] or any combination of the elements [x], [y], or [z]

Claims 3-5 each include a phrase listing elements in the form "[X], [Y], [Z], or any combination thereof." These phrases require no construction, as each phrase uses plain and ordinary language that is readily apparent to a person of ordinary skill in the art, and the specification and prosecution history does not identify alternate meanings.

[8] In some systems, something that appears to be an address may be used as a name. In that instance, the address-used-as-a-name would be resolved into an address that would be used as an address. Thus, even in this example, the system is resolving the name into an address, not resolving an address, as Microsoft's construction requires.

Microsoft's construction does not add any clarity to the meaning of these phrases. Indeed, Microsoft does not dispute that these phrases are clear from the specification and claim language. Nor does Microsoft dispute that the plain and ordinary meaning of these phrases encompasses its construction. Therefore, no construction is necessary and the terms should be given their plain and ordinary meaning.

I. "Tunneling" (Claim 12)

VirnetX's Proposed Construction	Microsoft's Proposed Construction
Transmitting data structured in one protocol format within the format of another protocol	Encapsulating a payload of a first protocol in a second protocol

The broadest reasonable interpretation of "tunneling" is "transmitting data structured in one protocol format within the format of another protocol." The specification of the '274 patent supports this construction by describing, among other things, a "client-side proxy application program" that "tunnels [] unencrypted, unprotected communication packets through a new protocol, thereby protecting the communications from a denial of service at the server side." (Ex. 1001, 49:28-36.) It then provides an example in which a second protocol's packet

may be formed for a tunnel by modifying the payload[9] portion of second protocol's packets to include the first protocol's unencrypted, unprotected communication packets. (Ex. 1001 at 50:44-52.) In this example, data structured in a first protocol format is placed into the payload of a packet in a second protocol format.

Consistent with the specification's use of the term, a contemporaneous computer dictionary defines "tunneling" to mean "transmitting data structured in one protocol format within the format of another protocol." (Ex. 2026 at 7.) This "[t]unneling allows other types of transmission streams to be carried within the prevailing protocol." (*Id.*) Thus, both intrinsic and extrinsic evidence support VirnetX's construction.

In its Petition, Microsoft discusses "tunneling" in similar terminology as above but reverses the order of key terms, resulting in a construction that does not accurately reflect the technology or the embodiments of the specification. Under Microsoft's construction, the payload of a first protocol is stripped out and is

[9] Packets generally contain a header portion and a payload portion. The header portion contains information like the source and destination of the packet, while the payload generally contains the data to be transmitted. (*See* Ex. 2026 at 4, defining "payload" as "the data-carrying capacity of some structure. It typically refers to a part of a packet or frame in a communications system that holds the message data in contrast to the headers, which are considered overhead.")

encapsulated in a second protocol. The patent, however, teaches that a first protocol's entire packet (not just its payload) can become the payload of a second protocol's packet. Microsoft's construction is inaccurate and not supported by the patent specification, so it should be rejected.

"Tunneling," therefore, is "transmitting data structured in one protocol format within the format of another protocol."

J. "Tunnel Packeting" (Claim 13)

VirnetX's Proposed Construction	Microsoft's Proposed Construction
Forming a packet to be transmitted that contains data structured in one protocol format within the format of another protocol	Encapsulating a first packet of a first protocol in a second packet of a second protocol

Consistent with the construction of "tunneling" in the previous section, the broadest reasonable interpretation of "tunnel packeting" is "forming a packet to be transmitted that contains data structured in one protocol format within the format of another protocol." Contrary to Microsoft's allegation that the term "appears to lack the necessary support under 35 U.S.C. § 112" (Pet. at 14), "tunnel packeting" is supported by, and described in, the '274 patent specification.

As discussed in the previous section, the '274 patent describes a "client-side proxy application program" that "tunnels [] unencrypted, unprotected communication packets through a new protocol, thereby protecting the communications from a denial of service at the server side." (Ex. 1001 at 49:28-

36.) It also provides an example in which a second protocol's packet may be formed for a tunnel by modifying the payload portion of second protocol's packets to include the first protocol's unencrypted, unprotected communication packets. (*Id.* at 50:44-52.) In the context of the '274 patent, therefore, one of ordinary skill in the art would have understood "tunnel packeting" to refer to forming a packet to be transmitted via tunneling. Taken together with the construction of tunneling, the construction of "tunnel packeting" is "forming a packet to be transmitted that contains data structured in one protocol format within the format of another protocol."

K. "Client Computer" (Claim 15)

VirnetX's Proposed Construction	Microsoft's Proposed Construction
User's computer	No construction offered

In the context of the '274 patent claims, the broadest reasonable interpretation of "client computer" is a "user's computer." The claims and specification support this construction.

For example, one of the steps in independent claim 1 is sending an access request message using the VPN communication link, and dependent claim 15 requires that step to be performed with a client computer. (Ex. 1001 at 52:45-47.) So claim 15 requires the client computer to communicate over the VPN communication link, and the specification describes a user's computer as the computer communicating over the VPN communication link. For example, the

specification explains that a software module 3309 for using the VPN is installed on a computer 3301, (*id.* at 47:66-48:1), and elsewhere describes that the computer 3301 is manned by a user and equipped with a web browser 3306 and user input devices such as a keyboard, display, and/or mouse, (*id.* at 45:16-29, 45:50-62, 46:11-28; FIG. 34.) In another embodiment, the specification explains that a "user's computer 2501" includes this "client application." (*Id.* at 38:61-62.) Thus, the '274 patent equates the user's computer with the "client computer" in the claims.

The ordinary meaning is further confirmed by a dictionary that an IPR petitioner cited in its petitions against other VirnetX patents. It defines "client machine" as "[a] user's workstation that is attached to a network." (Ex. 2026 at 3.) The relevant definitions for the other client-related terms also unanimously require a user, either expressly or implicitly, by identifying a "client" as a "workstation," "personal computer," "user's machine," or "user's PC" in those definitions:

Term	**Dictionary Definition**
Client	A workstation or personal computer in a client/server environment
Client application	An application running in a workstation or personal computer on a network
Client based	Refers to hardware or software that runs in the user's machine (client)

Term	Dictionary Definition
Client program	Software that runs in the user's PC or workstation
Client/server	An architecture in which the user's PC (the client) is the requesting machine and the server is the supplying machine[.]

(*Id.*) According to the same dictionary, "workstation" "is just a generic term for a user's computer." (*Id.* at 9.) Likewise, "personal computer" or "PC" is "a computer that serves one user in the office or home." (*Id.* at 5.) Accordingly, each of the client-related definitions incorporates the view that a client computer is a user's computer.[10]

IV. If Trial Is Instituted, VirnetX Requests an 18-Month Schedule

For the reasons discussed, Microsoft's Petition cannot be instituted. If trial is instituted in this matter, however, it would be very difficult to complete the proceeding within one year. For the '274 patent alone, there are four *inter partes*

[10] In reexamination control no. 95/001,792, the Board found that the term "client computer" may read on a proxy computer where no user resides. VirnetX is seeking to reopen prosecution in the reexamination based in part on this issue, and will be presenting additional evidence and explanation in the reexamination to support its position.

review petitions that have been filed by two parties. There are also numerous other pending *inter partes* review petitions and reexaminations involving related patents. *See* Updated Patent Owner's Mandatory Notices Pursuant to 37 C.F.R. § 42.8, Paper No. 8 at 2-7 (identifying copending matters). The sheer number of issues, the overlapping issues (e.g., claim construction), the need for consistency, and other interplay between the numerous proceedings renders their administration complex for the Board and the parties. Thus, if instituted, there is good cause for the Board to set an 18-month schedule for this proceeding pursuant to 35 U.S.C. § 316(a)(1) and 37 C.F.R. § 42.100(c).

V. Conclusion

For these reasons, VirnetX respectfully requests that the Board deny the petition for *inter partes* review.[11]

Respectfully submitted,

Dated: May 19, 2014

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

Counsel for VirnetX Inc.

[11] If trial is instituted, VirnetX reserves its rights to raise additional arguments as to why Microsoft has failed to carry its burden and why the claims should be confirmed.

CERTIFICATE OF SERVICE

Pursuant to 37 C.F.R. § 42.6(e), I certify that I caused to be served on the counsel for Petitioner a true and correct copy of the foregoing Patent Owner's Preliminary Response to Petition for *Inter Partes* Review of U.S. Patent No. 7,987,274 and associated exhibits by electronic means on May 19, 2014 as follows:

Counsel for Microsoft Corporation:

W. Karl Renner, Reg. No. 41,265
3200 RBC Plaza
60 South Sixth Street
Minneapolis, MN 55402
T: 202-783-5070
F: 202-783-2331

Kevin E. Greene, Reg. No. 46,031
3200 RBC Plaza
60 South Sixth Street
Minneapolis, MN 55402
T: 202-626-6376
F: 202-783-2331

IPR38868-0004IP1@fr.com

Dated: May 19, 2014

By: /Joseph E. Palys/
Joseph E. Palys
Reg. No. 46,508
Finnegan, Henderson, Farabow, Garrett & Dunner, LLP
11955 Freedom Drive
Reston, VA 20190-5675
(571) 203-2700

Counsel for Patent Owner