IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXAS
TYLER DIVISION

VirnetX Inc.,

Plaintiff,

v.

Cisco Systems, Inc., Apple Inc., Aastra USA, Inc., Aastra Technologies Ltd., NEC Corporation, and NEC Corporation of America,

Defendants.

Civil Action No. 6:10-cv-00417-LED

JURY TRIAL DEMANDED

DEFENDANTS' RESPONSIVE CLAIM CONSTRUCTION BRIEF

VIRNETX EXHIBIT 2002
Apple v. VirnetX
Trial IPR2015-00812

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

I. INTRODUCTION

To prevail at trial in its litigation against Microsoft, VirnetX relied on this Court's constructions of key language from the patents-in-suit—such as "virtual private network" and "secure domain name." VirnetX then turned around and told the Patent Office that this Court's constructions were ***wrong***. Specifically, in distinguishing prior art in subsequent reexamination proceedings, VirnetX argued that the terms "virtual private network" and "secure domain name" contain limitations found nowhere in this Court's constructions.

Now VirnetX seeks to reverse course once again. While conceding that its reexamination arguments require narrowing of this Court's prior definition of "secure domain name," VirnetX asks this Court not only to disregard its reexamination arguments concerning "virtual private network," but also to revisit and ***broaden*** the construction of that language from the *Microsoft* case. VirnetX should not be permitted to expand and contract the scope of the asserted claims to suit whatever validity or infringement dispute it currently confronts. Defendants' proposed claim constructions avoid that result by applying settled claim construction principles to interpret the asserted claims consistent with VirnetX's statements to the Patent Office, both in the original applications and during subsequent reexamination proceedings.

II. LEGAL STANDARDS

This Court is familiar with the pertinent claim construction principles. For convenience, Defendants cite to relevant authority in the body of the brief.

III. PATENTS-IN-SUIT

The six Patents-in-Suit are closely related. The specifications of the '135 and '151 Patents are substantively identical, as are the specifications of the '180, '759, '504, and '211

Patents.[1] The latter patents are based on a continuation-in-part to the '135 Patent, adding new material to the specification, most notably a section titled "One-Click Secure On-Line Communications and Secure Domain Name Service" and related Figures 34 and 35.

Several of the Patents-in-Suit have been subject to reexamination. The Patent Office granted Microsoft's request for *inter partes* reexamination of the '135 and '180 Patents, but confirmed the claims after Microsoft settled with VirnetX and withdrew from the reexaminations. Since that time, the Patent Office has initiated new reexaminations of the '135, '151, '180, and '759 Patents.

IV. DISPUTED CLAIM CONSTRUCTIONS[2]

A. Disputes Concerning Virtual Private Networks

1. Virtual Private Network

Term	VirnetX's Proposed Construction	Defendants' Proposed Construction
Virtual Private Network	a network of computers which privately communicate with each other by encrypting traffic on insecure communication paths between the computers	a network of computers which privately and directly communicate with each other by encrypting traffic on insecure communication paths between the computers where the communication is both secure and anonymous

Proceedings that occurred after this Court's Claim Construction Order in the *Microsoft* litigation warrant modification of the Court's pervious construction of "virtual private network" (1) to expressly reflect this Court's prior ruling that communications in a "virtual private network" are both secure and anonymous, and (2) to specify that the claimed network of computers directly communicate with each other, as VirnetX represented to the Patent Office in subsequent reexamination proceedings.

[1] Not all of the patents or claims from those patents are asserted against all of defendants. Each Defendant joins in this brief to the extent the disputed term appears in the patent claims asserted against that Defendant.

[2] The parties agree that a person of ordinary skill in the art would have a Master's degree in computer science or computer engineering, or in a related field, as well as about two years of experience in computer networking and in some aspect of security with respect to computer networks. The parties also agree that such person would have actual experience with networking protocols as well as the security of those protocols.

a) Secure And Anonymous

This Court already decided that a virtual private network requires "both data security and anonymity" (*Microsoft* case, D.I. 246 (attached as Ex. A) at 8-9) and expressly recognized that the disclosed virtual private networks were designed to prevent eavesdroppers on insecure networks from intercepting data and determining which computers were communicating, and therefore must accomplish both data security and anonymity. Nevertheless, the Court's prior Order did not explicitly incorporate those requirements into the text of its construction.[3] Defendants' construction expresses these requirements so as to avoid jury confusion.

In the *Microsoft* case, Microsoft largely hinged its noninfringement case on the argument that its accused products did not achieve anonymity. *See e.g. Microsoft* case, D.I. 393 (attached as Ex. D) at 62:20-65:15; *Microsoft* case, D.I. 396 (attached as Ex. F) at 19:4-32:6. Accordingly, both parties repeatedly referred to an element required by the prior Claim Construction Order but absent from the express definition of "virtual private network." While no party disputed that a "virtual private network" must achieve data security and anonymity[4], the parties had to rely on cross examination to convey those requirements to the jury, thereby complicating the trial and increasing the risk of jury confusion. Express incorporation of all of the requirements of a virtual private network into the construction will remove ambiguity and ensure that claim construction issues are not left to the jury. *See Every Penny Counts, Inc. v. Am. Express Co.*, 563

[3] After the Court's claim construction order, Microsoft moved to have the "data security and anonymity" language incorporated in the Court's construction of virtual private network. *Microsoft* case, D.I. 247. Neither party disputed that a virtual private network requires anonymity when the Court considered the issue at the pretrial conference. *Microsoft* case, D.I. 339 (attached as Ex. O) at 6:16-14:16. VirnetX went so far as to promise that its expert would not contradict that "private" requires both anonymity and security." *Id.* at 12:20-13:2. Microsoft eventually agreed to rely on cross examination of VirnetX's expert witnesses, instead of express incorporation into the construction, to convey that requirement to the jury. *Id.* at 14:2-4.

[4] *See Microsoft* case, D.I. 391 (attached as Ex. B) at 88:18-89:17, 155:8-15; *Microsoft* case, D.I. 392 (attached as Ex. C) at 64:1-71:12, 85:19-89:1, 93:10-15; *Microsoft* case, D.I. 393 (Ex. D) at 42:1-43:11, 62:20-65:15; *Microsoft* case, D.I. 395 (attached as Ex. E) at 100:12-101:25, 105:1-9; *Microsoft* case, D.I. 396 (Ex. F) at 19:5-32:6, 70:2-88:12, 98:22-109:19, 118:12-121:19, 126:8-18; *Microsoft* case, D.I. 397 (attached as Ex. G) at 56:3-59:8; *Microsoft* case, D.I. 398 (attached as Ex. H) at 136:12-137:16.

F.3d 1378, 1383 (Fed. Cir. 2009).

In its opening brief, VirnetX now argues—contrary to this Court's ruling in the *Microsoft* case—that a virtual private network does ***not*** require anonymity. But the intrinsic evidence shows otherwise. The Background of the Invention frames the patent as addressing "two security issues . . . called ***data security and anonymity***." '135 Patent (attached as Ex. 1) at 1:35-36 (emphasis added). It also explains that anonymity involves "prevent[ing] an eavesdropper from discovering that terminal 100 is in communication with terminal 110." *Id.* at 1:26-27. And the specification consistently equates the word "private" in "virtual private network" with "anonymity," explaining that "[a]nonymity would thus be an issue, for example, for companies that want to keep their market research interests ***private***." *Id.* at 1:32-33 (emphasis added). The rest of the specification describes ways to solve the twin security issues of data security and anonymity. *Id.* at 2:66-3:17, 19:66-20:3, 23:11-36, 37:40-49, 37:63-38:6, 39:29-33. As the Court previously recognized, because the Detailed Description of the Invention section refers back to the anonymity features disclosed earlier in the specification, the term VPN requires anonymity wherever it appears. Ex. A at 8-9.

Ultimately, VirnetX's claim construction brief simply rehashes a settled dispute from the *Microsoft* case about the "purpose" of encapsulation. D.I. 173 at 5. That discussion is beside the point. For one thing, the aforementioned teachings of the patents-in-suit, which define a virtual private network as requiring "anonymity," do not hinge on their use of encapsulation. Ex. 1 at 7:49-58 (describing how anonymity is accomplished by having the destination field of the IP header point to an intermediary router instead of the ultimate destination). Indeed, this Court's Claim Construction Order expressly acknowledges that techniques other than tunneling exist to achieve anonymity. Ex. A at 9-10. Furthermore, to the extent that "encapsulation" plays a role

in anonymity, the virtual private network described and claimed by the patents-in-suit ensures anonymity regardless of whether that result is the "purpose." In any case, encapsulation can serve several purposes depending on its implementation, including data security and anonymity. Kelly Decl. at ¶ 5. VirnetX's reiteration of its arguments from the *Microsoft* litigation should again be rejected.

b) Directly

In reexamination proceedings following this Court's Claim Construction Order in the *Microsoft* case, VirnetX responded to office actions rejecting several claims of the '135 and '180 Patents in light of the "Aventail" reference. In particular, VirnetX argued that Aventail does not "disclose a VPN because ***computers connected according to Aventail do not communicate directly with each other.***" '135 reexam (attached as Ex. I) at 5-7 (emphasis added); *see also* '180 reexam (attached as Ex. K) at 11-13. Defendants' construction incorporates VirnetX's 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.

VirnetX confirmed that a "virtual private network" requires direct communication between computers by further distinguishing the Aventail reference from the claimed invention:

> The [Aventail] client cannot open a connection with the target itself. . . . ***Instead, the client computer and target computer are deliberately separated by the intermediate SOCKS server.***

Ex. I at 7 (emphasis added); *see also* Ex. K at 13. VirnetX summarized Aventail by explaining that, unlike the claimed virtual private network, in Aventail, "[r]egardless of the number of servers or proxies between the client and target, at least one is required . . . ." *Id.* (referring to a network diagram from the Aventail reference). Finally, VirnetX relied on expert testimony that "Aventail has not been shown to disclose a VPN because computers connected according to

Aventail do not communicate ***directly*** with each other." '135 reexam, Nieh declaration (attached as Ex. J) at ¶ 26 (emphasis added); '180 reexam, Nieh declaration (attached as Ex. L) at ¶ 29. VirnetX therefore repeatedly and clearly confirmed that "virtual private network" communications must be direct.

Confronted with its own unambiguous statements to the Patent Office, VirnetX protests that it "was not forced to overcome a reference by disclaiming a certain scope of VPN taught by Aventail [but rather] overcame Aventail on the ground that Aventail did not teach a VPN at all." D.I. 173 at 7-8. This is a difference without a distinction. In arguing that Aventail does not disclose a VPN, VirnetX clearly defines "virtual private networks" as requiring direct communications between communicating computers.

Nor can VirnetX escape the consequences of its statements to the Patent Office by portraying them as a case of ambiguous disclaimer. The disclaimer case VirnetX cites, *Momentus Golf, Inc. v. Swingrite Golf Corp.*, 187 F. App'x. 981 (Fed. Cir. 2006), concerned an ambiguity not present here. There, the patentee argued to the Patent Office that "[a] hollow device having 10-25% club head weight cannot meet the requirement in applicant's claims that the center of gravity of the trainer be substantially at the center of a solid round stock." *Id.* at 983. The Federal Circuit found that statement to be ambiguous because it was unclear whether the patent owner was disclaiming (1) devices that were both hollow ***and*** had 10-25% head weight, or (2) devices that either were hollow ***or*** that had 10-25% head weight. *Id.* at 983-84.

Here, in contrast, VirnetX unequivocally argued that Aventail does not disclose a VPN because it does not teach direct communication between computers. VirnetX also attempted to distinguish Aventail on the same grounds in the reexamination of the '180 Patent. Ex K at 11-

13. VirnetX suggests that because it distinguished Aventail on additional independent grounds,[5] there cannot be a clear disclaimer. But the case law makes it clear that "an applicant's argument that a prior art reference is distinguishable on a particular ground can serve as a disclaimer of claim scope even if the applicant distinguishes the reference on other grounds as well." *Am. Piledriving Equip. v. Geoquip, Inc.*, 637 F.3d 1324, 1336 (Fed. Cir. 2011). Furthermore, "[A]n applicant's argument made during prosecution may lead to a disavowal of claim scope even if the Examiner did not rely on the argument." *Seachange Int'l, Inc. v. C-COR Inc.*, 413 F.3d 1361, 1374 (Fed. Cir. 2005). As such, the Court should construe virtual private network to require direct communications.[6]

2. Virtual Private Link

Term	VirnetX's Proposed Construction	Defendants' Proposed Construction
Virtual Private Link	a communication link that permits computers to privately communicate with each other by encrypting traffic on insecure communication paths between the computers	a link in a virtual private network

a) Defendants' Construction of Virtual Private Link

Defendants agree that a "virtual private link," as referenced in claim 13 of the '135 Patent, is a link in a virtual private network.

b) Aastra's Construction of Virtual Private Link

Defendant Aastra submits that a virtual private link ("VPL") is "a link in a virtual private

[5] During reexamination, VirnetX also argued that two additional reasons existed why Aventail did not disclose VPN. In particular, VirnetX argued that computers connected via the Aventail system are not able to communicate with each other as though they were on the same network, and that Aventail's operation is incompatible with users transmitting data that is sensitive to network information. Ex. I at 5-7; *see also* Ex. K at 11-13. Defendants do not believe that these additional VPN requirements are relevant to the disputed issues in the current case and therefore have not included them in their proposed construction. *See Vivid Techs., Inc. v. Am. Science & Eng'g, Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999) ("[O]nly those terms need be construed that are in controversy, and only to the extent necessary to resolve the controversy."). However, should a dispute arise, Defendants reserve the right to seek further clarification from the Court or other appropriate remedies.

[6] VirnetX admits that it likewise narrowed the definition of "secure domain name service" during reexamination and that the Court's prior construction of that term should be narrowed accordingly. *See* D.I. 173 at 17-18.

network that accomplishes data security and anonymity through the use of hop tables."[7] In addition to requiring a VPL to have all the characteristics of a virtual private network, the specification further dictates that hop tables must be used to create a VPL.

> When a packet is received from a known user, the signaling server activates a virtual private link (VPL) between the user and the transport server, where hopping tables are allocated and maintained. When the user logs onto the signaling server, the user's computer is provided with hop tables for communicating with the transport server, thus activating the VPL.

Ex. 1 at 44:37-43 (emphasis added). The specification also explains how anonymity and security are accomplished through the use of hopping technology. *See id.* at 3:10-17 and 3:39-42. Accordingly, Aastra submits that a virtual private link is a link in a VPN that requires the use of hop tables.

3. Secure Server

Term	VirnetX's Proposed Construction	Defendants' Proposed Construction
Secure Server	a server that requires authorization for access and that can communicate in a secure communication link	a server that requires authorization for access and communicates in a VPN

Defendants' proposed construction recognizes that the word "secure" in the context of the patent refers to a server that communicates in a virtual private network. The specification plainly dictates that for a server to be "secure," it must achieve both the data security and anonymity requirements of a VPN:

> "It is desired for the communications [over the internet] to be ***secure***, that is, ***immune to eavesdropping***. For example, terminal 100 may transmit secret information to terminal 110 over the Internet 107. Also, it may be desired to ***prevent an eavesdropper from discovering that terminal 100 is in communication with terminal 110***. . . . These two ***security*** issues may be called ***data security*** and ***anonymity***."

'151 Patent (attached as Ex. 2) at 1:34-48 (emphasis added); *see also* 19:43-48. Moreover, the specification indicates that the secure server claimed in the '151 Patent communicates in a virtual

[7] Only Defendant Aastra advances this construction and argument.

private network:

> "[A] specialized DNS server traps DNS requests and, if the request is from a special type of user (*e.g.*, one for which secure communication services are defined), ***the server . . . automatically sets up a virtual private network*** . . . . ."

Id. at 37:33-49 (emphasis added). Indeed, this Court previously cited the same portion of the '135 Patent's specification in concluding that a "secure web site" communicates in a virtual private network. Ex. A at 18 (citing '135 Patent at 37:63-38:13). Just as a "secure ***web site***" communicates in a "virtual private network," so too does a "secure ***server***" communicate in a "virtual private network."

While the only mention of the precise phrase "secure server" in the '151 Patent occurs in the claims, the other related Patents-in-Suit dictate that a "secure server" is a server that communicates in a virtual private network. The specifications of the '504, '211, '180, and '759 Patents all state that "software module 3309 accesses ***secure server*** 3320 ***through VPN communication link 3321***," '180 Patent (attached as Ex. 3) at 52:55-56 (emphasis added), and that "[s]erver 3320 can ***only*** be accessed through a VPN communication link." *Id.* at 52:29-30 (emphasis added). The Patents distinguish "secure servers" from "non-secure servers" based on whether the server communicates in a VPN:

> computer 3301 can establish a VPN communication link 3323 with secure server computer 3320 through proxy computer 3315. Alternatively, computer 3301 can establish a non-VPN communication link 3324 to a non-secure website, such as non-secure server computer 3304.

Id. at 53:20-25. Together, these passages explain that a secure server is a server dedicated to VPNs.

Defendants' proposed construction also comports with this Court's constructions of other claim terms that use the word "secure." The Court previously decided (and the parties agree) that "secure computer network address" means "a network address that requires authorization for

access and is associated with a computer capable of virtual private network communications." Ex. A at 28. The parties also agree that the construction for "secure domain name," by virtue of incorporating the term "secure computer network address," also communicates in a VPN. D.I. 175 Ex. A. Finally, although the parties disagree about the construction of the term "secure web site," both Defendants' and VirnetX's proposed definitions specify that it "can communicate in a virtual private network." D.I. 175 Ex. B. Because the word "secure" in the context of servers should be given the same meaning as in the context of related claim terms, Defendants' proposal should be adopted. *Omega Eng'g., Inc. v. Raytek Corp.*, 334 F.3d 1314, 1334 (Fed. Cir. 2003) ("[W]e presume, unless otherwise compelled, that the same claim term in the same patent or related patents carries the same construed meaning.").

4. Secure Communication Link

Term	VirnetX's Proposed Construction	Defendants' Proposed Construction
Secure Communication Link	an encrypted communication link	virtual private network communication link

Defendants' proposed construction is taken verbatim from the definition provided in the Summary of the Invention, which states that "***[t]he secure communication link is a virtual private network communication link*** over the computer network." '504 Patent (attached as Ex. 5) at 6:61-63 (emphasis added). The rest of the specification consistently defines secure communication link in the same way. Thus, the Detailed Description of the Invention explains when secure communication links are specified, ***all*** communication links will be VPN communication links:

> [w]hen software module 3309 is being installed or when the user is off-line, the user can optionally specify that all communication links established over computer network 3302 are ***secure communication links. Thus, anytime that a communication link is established, the link is a VPN link.***"

Id. at 52:15-19 (emphasis added). Similarly, selecting a secure communication link enables a

computer to establish a VPN communication link: "[a]dditionally, a user at computer 3301 can optionally select a secure communication link through proxy computer 3315. ***Accordingly, computer 3301 can establish a VPN communication link*** 3323 with secure server computer 3320 through proxy computer 3315." *Id.* at 52:25-29 (emphasis added).[8]

In the *Microsoft* case, VirnetX actually conceded that a secure communication link is a VPN communication link. *See Microsoft* case D.I. 194 (attached as Ex. M) at 31-32. VirnetX now reverses course by engaging in a tortured reading of the specification. But even the passage VirnetX cites explains that a secure communication link ***is*** a VPN because it can securely access a private network. D.I. 173 at 11-12 (citing '504 Patent at 50:21-53). VirnetX's only purported support for its construction of secure communication link is the specification's discussion of "***data*** security." *See* D.I. 173 at 10 (citing '504 at 1:55-56). The specification clearly distinguishes "secure," which encompasses data security and anonymity from "data security." Ex. 5 at 1:33-54. Therefore, VirnetX's discussion of "data security"—a phrase that does not appear in the disputed claim language—is not relevant to the construction of "secure communication link."[9]

B. Disputes Relating to Domain Names

1. Domain Name

Term	VirnetX's Proposed Construction	Defendants' Proposed Construction
Domain Name	a name corresponding to an IP address	a hierarchical sequence of words in decreasing order of specificity that corresponds to a numerical IP address

VirnetX's proposed construction reads out the meaning of "domain." *Compare* '181

[8] These descriptions are also consistent with the specification's use of the word "secure." *See* Section IV.A.3., *supra*. As this Court previous recognized, in the context of the patent, "'secure' relates to registered users who have the ability to set up a virtual private network with a target node." Ex. A at 18.

[9] In the *Microsoft* case, this Court declined to construe the term "secure communication link" because the claims of the '759 Patent explain "the secure communication link being a virtual private network." Ex. A at 25. Here, the claim language of the '504 and '211 Patents does not itself explain that the secure communication link is a virtual private network communication link.

Patent at claim 2 (attached as Ex. 7) (claiming a "secure name"), *with* '180 Patent at claim 1 (Ex. 3) (claiming a "secure domain name"). Moreover, VirnetX's rejection of Defendants' proposed construction turns on an incorrect application of the law. Where no explanations or limitations are present, one of ordinary skill in the art's understanding of the claim language controls, not the broadest possible reading of the specification. *See Phillips v. AWH Corp.*, 415 F.3d 1303, 1312 (Fed. Cir. 2005) ("[T]he claims of a patent define the invention to which the patentee is entitled the right to exclude.").

VirnetX acknowledges that domain names are ***hierarchical*** sequences in relation to the Internet because that allows for a distributed approach to managing the naming of a huge number of computers around the world. D.I. 173 at 14. Yet VirnetX argues that such a meaning cannot hold here because the described DNS proxy server would have different requirements than the Internet generally. But VirnetX does not provide any reason that one of skill in the art would understand the term differently than its admitted ordinary meaning. *Id.* at 14-15.

The specification, where using this term, conforms to and supports Defendants' construction. *See* Ex. 3 at 39:45-52 ("Yahoo.com"), 39:63-40:5 ("Target.com"), 53:26-40 ("website.scom" and "website.com"). Kelly Decl. at ¶ 6. Indeed, VirnetX's evidence supports the same construction. D.I. 175 Ex. C at 27-28 ("domain name . . . *n*. An address of a network connection that identifies the owner of that address in ***a hierarchical format***: *server.organization.type*. For example, www.whitehouse.gov identifies the Web serve[r] at the White House, which is part of the U.S. government." (quoting Microsoft Press, Computer Dictionary (3rd ed. 1997), p. 158.) (emphasis added)). Accordingly, this Court should adopt the

Defendants' proposed ordinary meaning construction.[10]

2. Domain Name Service

Term	VirnetX's Proposed Construction	Defendants' Proposed Construction
Domain Name Service	a lookup service that returns an IP address for a requested domain name	a lookup service that returns an IP address for a requested domain name to the requester

The parties dispute whether a Domain Name Service (DNS) returns the IP address to the device "requester" that requested the IP address. This Court construed "Domain Name Service" in the *Microsoft* case as "a lookup service that returns an IP address for a requested domain name." Ex. A at 11-12. VirnetX seeks to exploit the fact that the Court's construction does not explicitly indicate ***to whom*** the request is returned, even though the context of the Court's prior Claim Construction Order makes clear that the Domain Name Service returns the IP address to the device that is seeking the IP address from the DNS.

In the *Microsoft* action, this Court arrived at its construction noting that the "specification's description of DNS is consistent with construing DNS as 'a lookup service that returns an IP address for a requested domain name.'" *Id.* at 11. Specifically, the Court correctly cited to the following relevant passage from the specification:

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

Id. at 11-12 (emphasis added). The specification describes that the client computer needs the IP address so it can communicate with the target device: "The DNS returns the IP address . . . to client application 2504, which is then able to use the IP address ***to communicate with the host***

[10] VirnetX contends that Defendants' proposed construction excludes proper domain names. (D.I. 173 at 15.) But Defendants do not intend "words" to exclude alphanumeric strings. If Defendants' proposed construction excludes "words," it is not clear how Plaintiff's proposed construction ("a name…") is not similarly limiting.

2503 . . . ." Ex. 1 at 37:36-39. Accordingly, the IP address must be returned to the requester.

To dispute the intrinsic evidence, VirnetX relies on a declaration from its expert, Dr. Jones. D.I. 173 at 13. Dr. Jones refers to "modes" of operation that pertain to the DNS proxy, not DNS. In particular, Dr. Jones argues that the specification describes a "mode" in which the DNS returns the IP address to the DNS proxy instead of the client. But a DNS proxy "responds to a domain name inquiry ***in place of a DNS***." *See* Ex. A at 22-23. Insofar as a domain name inquiry is concerned, the DNS proxy acts like the DNS and returns the IP address ***to the client*** (*e.g.*, the requester). *See, e.g.*, Ex. 1 at 38:37-38 ("DNS proxy 2610 returns to user computer 2601 the resolved address passed to it by the gatekeeper . . . ."). Kelly Decl. at ¶ 7.

3. Secure Domain Name Service

Term	VirnetX's Proposed Construction	Defendants' Proposed Construction
Secure Domain Name Service	a lookup service that recognizes that a query message is requesting a secure computer address, and returns a secure network address for a requested secure domain name	a non-standard lookup service that recognizes that a query message is requesting a secure computer address and performs its services accordingly by returning a secure network address for a requested secure domain name[11]

VirnetX's modification to this Court's prior construction of secure domain name service selectively incorporates statements made by VirnetX during reexamination while ignoring others. Defendants' construction takes into account ***all*** of VirnetX's statements and properly reflects that a secure domain name service is a ***non-standard*** lookup service that recognizes that a query message is requesting a secure computer address and ***performs its services accordingly***.

a) Non-Standard

During the *Microsoft* case, this Court construed secure domain name service as "a lookup service that returns a secure network address for a requested secure domain name." During subsequent reexamination proceedings, VirnetX challenged this Court's construction by arguing

[11] In response to VirnetX's Opening Claim Construction brief, Defendants have removed the phrase "that requires authorization for access" to narrow the dispute between the parties.

that "the Request and Office Action rely on the faulty position that a secure domain name service is nothing more than a conventional DNS server that happens to resolve domain names of secure computers." Ex. K at 7. VirnetX argued that "a secure domain name service can resolve addresses for a secure domain name; whereas, ***a conventional domain name service cannot resolve addresses for a secure domain name***" and cited a portion of the specification referencing a "standard domain name service." *Id.* (citing '180 Patent at 51:18-45) (emphasis added). Because a conventional/standard domain name service cannot resolve addresses for a secure domain name, a secure domain name service must be non-conventional/non-standard. In the above passage, VirnetX uses the terms "conventional" and "standard" interchangeably. Defendants therefore propose the phrase "non-standard" to remain consistent with the parties' agreed upon definition of secure domain name, which also uses the phrase "non-standard."

b) Performs Its Services Accordingly

To support incorporating the phrase "recognizes that a query message is requesting a secure computer network address" into the term "secure domain name service," VirnetX relies on reexamination proceedings where it argued:

> A secure domain name service is not a domain name service that resolves a domain name query that, unbeknownst to the secure domain name service, happens to be associated with a secure domain name. . . . A secure domain name service of the '180 Patent, instead, ***recognizes that a query message is requesting a secure computer network address*** and performs its services accordingly.

Id. at 7 (emphasis added). But, VirnetX's proposed construction omits the final part of its explanation—"***and performs its services accordingly.***" This omission introduces ambiguity into the claim term because it does not address what it means for a secure domain name system to "recognize" properties of a query message. VirnetX's statements during reexamination explain that this recognition triggers the secure domain name system to perform its services and return a secure network address for a requested secure domain name. *Id.* at 7-8. Defendants' proposed

construction simply incorporates VirnetX's own explanation of what it means to "recognize[] that a query message is requesting a secure computer network address."

4. Domain Name Service System

Term	VirnetX's Proposed Construction	Defendants' Proposed Construction
Domain Name Service System	a computer system that includes a domain name service (DNS)	a DNS that is capable of differentiating between, and responding to, both standard and secure top-level domain names

This phrase, found only in the claims of the '504 and '211 Patents, adds the modifier "system" to the phrase "domain name service" (DNS) discussed *supra*, and thus must be ***something*** more than the "lookup service" that forms the basis of the parties' definition of DNS. Looking to the intrinsic record, this extra ***something*** must include at least the ability to differentiate between, and respond to, both standard and secure top-level domain names.

Indeed, claim 1 of the '504 Patent[12] confirms that the DNS System is much more than just a DNS — it is the heart of the invention. It must at least provide: (1) the required DNS functionality (*i.e.*, "to store a plurality of domain names and corresponding network addresses…;" ***and*** (2) a visual message or signal to a user that a secure link is available (*i.e.*, "to comprise an indication …").

The specification, Ex. 5 at 49:1-52:31 and FIGS. 33-34, discloses that the required DNS functionality includes a method whereby a client computer 3301 connects to server 3304 with "a standard top-level domain name such as .com" (*Id.* at 49:29-37), and "secure server 3320 corresponding to server 3304" with a non-standard top-level domain name, such as ".scom." *Id.* at 50:25-36, 51:44-47, to create a secure connection. As both connections are necessary, the DNS System must be ***able*** to handle both standard and secure top-level domain names – otherwise the invention would not function.

[12] Claim 1 of the '504 Patent is representative of the independent claims of the '504 and '211 Patents.

The Summary of the Invention confirms that "[t]he present invention provides a domain name service that provides secure computer network addresses for secure, non-standard top-level domain names." *Id.* at 7:27-29. By disclosing the ability to handle secure top-level domain names in the Summary of the Invention section, the patentee described the entire invention and not just a preferred embodiment. *Ciena Corp. v. Nortel Networks Inc.*, No. 2:05-CV-14, 2006 U.S. Dist. LEXIS 97450, at *32 (E.D. Tex. Apr. 25, 2006) (citing *Microsoft Corp. v. Multi-Tech. Sys.,* 357 F.3d 1340, 1348 (Fed. Cir. 2003)).

Moreover, the prosecution history dictates that the DNS System must be able to handle both standard and secure top-level domain names. The originally-filed claims of the '504 and '211 Patents were directed to "a system for providing a secure domain name service over a computer network." The Examiner rejected this claim, and stated that it "is unclear how the system is providing a secure domain name service." '504 File History, July 11, 2007 Office Action (attached as Ex. N), p. 11. Applicants replaced this claim language with "domain name service system," and argued that this change, along with other claim language "should address the … issue raised by the Examiner." *Id.* Thus, Applicants explicitly told the Examiner that the clarifying amendments (i.e., the addition of "domain name service system") addressed how the system is providing a "secure domain name service." Claim 1, as issued, must therefore be able to provide that functionality.

5. DNS Proxy Server[13]

Term	VirnetX's Proposed Construction	Defendants' Proposed Construction
DNS Proxy Server	a computer or program that responds to a domain name inquiry in place of a DNS	a computer or program that responds to a domain name inquiry in place of a DNS, and prevents destination servers from determining the identity of the entity sending the domain name inquiry

[13] A dispute between Microsoft and VirnetX as to whether the meaning of "DNS Proxy Server" included an interception and analysis requirement was resolved in the previous litigation. *See* Ex. A at 22. The current dispute is different, and was not raised in the *Microsoft* litigation.

Defendants' definition of DNS proxy server comes directly from the specification, which states the well understood concept that "[p]roxy servers prevent destination servers from determining the identities of the originating clients." Ex. 1 at 1:49-51. Such a definition is consistent with extrinsic evidence regarding the functionality of proxy servers. See *Webster's New World Dictionary of Computer Terms* (8th ed. 2000) (Proxy Server) (attached as Ex. P).

VirnetX argues that this express definition is irrelevant because the "Background of the Invention" is not a general statement, but rather "refers to proxy servers employed in a specific way known in the prior art to attempt to achieve anonymity." D.I. 173 at 16. The statement is ***not*** so limited—it describes what a "proxy server" is, regardless of the system in which it is used.[14] Moreover, Courts regularly look to the Background section to understand the scope of the claim term in dispute. *See, e.g.*, *Eon-Net LP v. Flagstar Bancorp*, 653 F.3d 1314, 1321 (Fed. Cir. 2011); and *Golden Hour Data Sys. v. emsCharts, Inc.*, 614 F.3d 1367, 1369 (Fed. Cir. 2010). Indeed, this Court referred to the "Background of the Invention" in construing these patents in the *Microsoft* case. *See, e.g.*, Ex. A at 8.

VirnetX also argues that Defendants' construction "would read out a preferred embodiment" because, in FIG. 26, "computer 2601 communicates directly with computers 2604 and 2611 . . . [and] [g]iven that authentication and authorization are likely to be required, it is implausible that computers 2604 and 2611 would not know the identity of 2601." D.I. 173 at 16. Yet VirnetX fails to explain why authentication and authorization would be required by computers 2604 and 2611. Even if authentication and authorization were required, the

[14] Moreover, the description is not limited to one specific embodiment. The "Background" discusses uses of a proxy server: (i) in a local/outside proxy system, Ex. 5 at 1:45-48; (ii) interposed between client and destination servers, *id.* at 1:51-53; (iii) in a Chaum's mix, *id.* at 1:65-67; and (iv) in a "crowd," *id.* at 2:25-28. The definition is general and applies to each example — and to the specification as a whole. Nowhere is there a statement that limits the definition of "proxy server" to a particular prior art implementation.

specification teaches that these steps can be performed by the DNS proxy server itself:

> DNS proxy 2610 intercepts all DNS lookup functions from client 2605 and determines whether access to a secure site has been requested. If access to a secure site has been requested (as determined, for example, by a domain name extension, or by reference to an internal table of such sites), DNS proxy 2610 determines whether the user has sufficient security privileges to access the site. If so, DNS proxy 2610 transmits a message to gatekeeper 2603 requesting that a virtual private network be created between user computer 2601 and secure target site 2604 . . . .

Ex. 1 at 38:23-33*; see also id.* at FIG. 27, 39:7-10.

C. Disputes Concerning Indicating, Indications, and Indicate

1. An Indication That The Domain Name Service System Supports Establishing A Secure Communication Link

Term	VirnetX's Proposed Construction	Defendants' Proposed Construction
An Indication That The Domain Name Service System Supports Establishing A Secure Communication Link	[no construction necessary]	a visible message or signal that informs the user that the domain name service system supports establishing a secure communication link
Indicate/Indicating . . . Whether The Domain Name Service System Supports Establishing A Secure Communication Link	[no construction necessary]	display/displaying a visible message or signal that informs the user whether the domain name service system supports establishing a secure communication link

The claims of the '504 and '211 Patents are based on a section of the specification entitled "One-click Secure On-line Communications and Secure Domain Name Service." Ex. 5 at 49:1-53:8; '211 Patent (attached as Ex. 6) at 48:55-52:67. Related FIGS. 33 and 34 are both explicitly directed to "one-click" systems. Thus, the section must deal with an interactive system that involves a user "clicking" on ***something*** to create a secure connection. That ***something*** is the recited "indication." The specification provides examples of such an "indication" such as a "go secure" hyperlink and an icon representing a hyperlink. Ex. 5 at 49:35-45, 57-58.[15] ***All*** of these examples have one thing in common – they are user-visible.

[15] The citations are to the '504 Patent, although corresponding citations can also be found in the '211 Patent.

The detailed description of FIGS. 33 and 34 demonstrate that the purpose of the indication is to provide information to a user. In FIG. 33, client computer 3301 connects with server 3304, and displays a web page related to server 3304 in its web browser 3306. *Id.* at 49:12-25. On the web page is a "hyperlink, or an icon representing a hyperlink, for selecting a virtual private network (VPN) communication link ('go secure' hyperlink) through computer network 3302 between terminal 3301 and server 3304." *Id.* at 49:38-42. "By ***displaying*** the 'go secure' hyperlink, ***a user at computer 3301 is informed*** that the current communication link between computer 3301 and server computer 3304 is a non-secure, non-VPN communication link." *Id*. at 49:46-49. If a user wants to initiate a secure connection with server 3304 (*e.g.*, to secure server 3320), the user selects the "go secure" hyperlink, or can otherwise enter a command to "go secure," *Id*. at 49:49-58, 50:14-17, and the system "begins to establish a VPN communication link." *Id*. at 50:26-27. Thus, the disclosed embodiments are focused on the interactions of a user with the system to create a secure connection, such as by the user "clicking" on a hyperlink.

Indeed, each time the term "indicate" is used in the section of the specification supporting the claims of the '504 Patent, it is used to describe a message ***visible to a user***:

- "the 'go secure' hyperlink is displayed as part of the web page downloaded from server computer 3304, thereby ***indicating*** that the entity providing server 3304 also provides VPN capability"
- "Because the secure top-level domain name is a non-standard domain name, a query to a standard domain name service (DNS) will return a message ***indicating*** that the universal resource locator (URL) is unknown"
- "At step 3412, web browser 3306 displays a secure icon ***indicating*** that the current communication link to server 3320 is a secure VPN communication link"

Id. at 49:42-45, 50:37-40, 51:64-66 (emphasis added). Moreover, the "Summary of the Invention" dictates a user-viewable indication:

- "[t]he present invention also provides a computer system having a communication link to a computer network, and a display showing a hyperlink for establishing a virtual private network through the computer network. When the hyperlink for establishing the virtual private network is selected, a virtual private network is established over the computer network."

Id. at 7:17-23. As this statement is found in the "Summary of the Invention," and is directed to "the present invention" (rather than a preferred embodiment), it is particularly strong evidence of the inventor's intent as to what must be provided with the invention. *Ciena*, 2006 U.S. Dist. LEXIS 97450, at *32.

D. Disputes Concerning the Scope of Virtual Private Networks

1. "Between [A] and [B]"

Term	VirnetX's Proposed Construction	Defendants' Proposed Construction
Between [A] and [B]	[no construction necessary]	extending from [A] to [B]

The disputed phrase "between [A] and [B]" appears in various forms in the patents-in-suit, where A and B are computers or locations.[16] For example, claim 1 of the '135 Patent (Ex. 1 at 47:32-33) recites "automatically initiating the VPN ***between the client computer and the target computer.***" The parties' dispute centers on whether the phrase "between device A and device B" requires the VPN (in the context of claim 1 of the '135 Patent) to extend from client computer to target computer, as required by the claims. VirnetX apparently contends that the VPN need not extend from the client to the secure server but rather that the claims simply require the encrypted channel to lie somewhere intermediate the two communicating devices (*e.g.*, the client computer and target computer).

[16] The "between" phrase appears in various claims in the patents-in-suit, each reciting the phrase, "between [A] and [B]," where A and B are computers or locations. For example, claim 1 of the '135 Patent (Ex. 1 at 47:32-33) uses the phrase "***between the client computer and the target computer***;" while claim 16 of the '504 Patent (Ex. 5 at 56:42-43) uses the phrase "***between the first location and the second location***." Though the above list is not inclusive of all uses of the term in all claims, the parties do not dispute that the meaning of each should be the same. For ease of discussion, the "between" phrase is addressed in the context of claim 1 of the '151 Patent (Ex. 2 at 46:66-67) ("automatically initiating an encrypted channel ***between the client and secure server***").

The plain language supports Defendants' position that the VPN extends along the entire path from client to target. For example, claim 1 of the '135 Patent recites "[a] method of transparently creating a virtual private network (VPN) ***between a client computer and a target computer***" and automatically initiating the VPN ***between the client computer and the target computer***."

The specification likewise describes providing security and anonymity for information as it travels all the way from an originating terminal to a destination terminal:

> A basic heuristic framework to aid in discussing these different security techniques is illustrated in FIG. 1. Two terminals, an originating terminal 100 and a destination terminal 110 are in communication over the Internet. It is desired for the communications to be secure, that is, ***immune to eavesdropping***. For example, terminal 100 may transmit secret information to terminal 110 over the Internet 107. Also, it may be desired to prevent an eavesdropper from discovering that terminal 100 is in communication with terminal 110. For example, if terminal 100 is a user and terminal 110 hosts a web site, terminal 100's user may not want ***anyone in the intervening networks*** to know what web sites he is "visiting."

Ex. 1 at 1:20-31. To ensure that the communication from terminal 100 to terminal 110 is "immune to eavesdropping" from "anyone in the intervening networks," the security must extend from terminal 100 to terminal 110. If this were not the case, the entire security objective of the patents would be undermined because there would be unprotected gaps along the way.

Finally, VirnetX's expert witness, Dr. Jones, previously supported Defendants' definition in his declaration in support of VirnetX's claim construction brief in the *Microsoft* litigation, stating that "a VPN communication link is the entire path between the laptop computer and the server." Ex. M., Jones Declaration at ¶ 33.

2. Target Computer

Term	VirnetX's Proposed Construction	Defendants' Proposed Construction
Target Computer	a computer with which the client computer seeks to communicate	the ultimate destination with which the client computer seeks to communicate

Claim 1 of the '135 Patent recites "a method of . . . creating a virtual private network (VPN) between a client computer and a target computer." The claim language and specification of the '135 Patent make clear that the VPN is created between the client computer and the ultimate destination with which the client computer seeks to communicate.

The specification of the '135 Patent describes the creation of a VPN between the client computer and the target computer exclusively in the context of two "scenarios." In the first scenario, the client computer seeks ultimately to communicate with—and has permission to access—the target computer. Ex. 1 at 39:40-60. As the specification describes, the client computer communicates a DNS request to the DNS proxy server 2610 to access the "requested target." *Id*. at 39:42-48. The DNS proxy server 2610 forwards the DNS request to gatekeeper 2603. *Id*. at 39:42-46. Once the gatekeeper 2603 determines that the client computer has permission to access the target computer, the gatekeeper establishes a VPN between the client and the requested target. *Id*. at 39:46-48. The client computer and target computer can then communicate in the VPN. *Id*.

In the second scenario, the client seeks ultimately to communicate with—but lacks permission to access—the target computer. *Id*. at 39:53-54. The client once again generates a DNS request and communicates the request to the DNS proxy server to access the target computer. *Id*. at 39:54-55. The DNS proxy server forwards the request to gatekeeper 2603. *Id*. at 55-56. However, in this scenario, the gatekeeper rejects the DNS request, informing DNS proxy server 2610 that it was unable to find the target computer. *Id*. at 39:56-58. A "host unknown" error message is therefore communicated from the DNS proxy 2610 to the client, and no VPN is established between the client computer and the target computer. *Id*. at 39:58-60. Therefore, while the client computer still seeks to communicate the DNS request to the DNS

proxy server and gatekeeper, the client computer is unable to communicate with the requested target computer. *Id*.

In both scenarios, the client computer first seeks to communicate with the DNS proxy server 2610, which in turn forwards the request to a gatekeeper computer. Both the DNS proxy server and gatekeeper computer are computers with which the client computer seeks to communicate. *See, e.g.,* Ex. A at 23 (finding that the "DNS proxy server" is a "computer or program"). But only the ultimate destination with which the client computer seeks to communicate is the ***target*** computer. One of ordinary skill in the art would therefore understand that a target computer in the context of the '135 Patent refers to the ultimate destination with which the client computer seeks to communicate. Kelly Decl. at ¶ 8.

VirnetX's proposed construction, on the other hand, reads out the meaning of "target." VirnetX cites to *i4i* to support its argument that "target" is not limiting. D.I. 173 at 25. But *i4i* supports Defendants' construction here. "Target" expressly limits the "computer" with which the client computer seeks to communicate. *See i4i Ltd. P'ship v. Microsoft Corp.*, 598 F.3d 831, 843 (Fed. Cir. 2010); *see also Merck & Co., Inc. v. Teva Pharms. USA, Inc*., 395 F.3d 1364, 1372 (Fed. Cir. 2005) ("A claim construction that gives meaning to all of the terms of the claim is preferred over one that does not do so.") VirnetX's construction would encompass all computers with which the client computer seeks to communicate—including, for example, the DNS proxy server and gatekeeper computers described in the specification's two "scenarios." Defendants' construction, on the other hand, is consistent with the description of the "target computer" as explained the '135 specification and clarifies that the client computer ultimately seeks to communicate with the target computer.

E. Disputes Relating to Websites

1. Web Site

Term	VirnetX's Proposed Construction	Defendants' Proposed Construction
Web Site	a computer associated with a domain name and that can communicate in a network	one or more related web pages at a location on the World Wide Web
Secure Web Site	a computer associated with a domain name and that can communicate in a virtual private network	a web site that requires authorization for access and that can communicate in a VPN
Secure Target Web Site	a target computer associated with a domain name and that can communicate in a virtual private network	a secure web site on the target computer

The disputed phrases "web site," "secure web site," and "secure target web site" appear in the claims of the '135 Patent. Of these three disputed phrases, the only phrase that the Court has not previously construed is "secure target web site." As with the *Microsoft* case, the parties dispute whether the phrase "web site" can be impermissibly broadened to include "computers" or "hosts." Regarding the phrases "web site" and "secure web site," Defendants' proposed constructions for these phrases mirror the ones previously determined by the Court. Likewise, Defendants' proposed construction of the phrase "secure target web site" incorporates the Court's previous construction of "secure web site" by including the phrase in their proposed construction. Defendants' proposed construction for this phrase further recognizes that the secure web site is located on the target computer.

As the Court recognized in the *Microsoft* case, VirnetX's construction for these disputed phrases attempts to "broaden the meaning of 'web site' beyond how this term is used in the patent." Ex. A at 17. The Court noted that the "patentee chose to use 'web site' in the claims instead of using a more encompassing term like 'host,' 'target computer,' or 'Internet resource.'" *Id.* Accordingly, Defendants respectfully request that the Court adopt its previous construction for the phrases "web site" and "secure web site."

Regarding the phrase "secure target web site," VirnetX once again attempts to "broaden the meaning of 'web site' beyond how this term is used in the patent." *Id.* Specifically, VirnetX's proposed construction defines the "target web site" as a "target computer." As discussed above, the Court has rejected this argument.[17]

VirnetX also argues that the "target web site" need not be on the target computer. But the claim language itself is directed to "transparently creating a virtual private network (VPN) between a client computer and a target computer." *See e.g.*, '135 Patent at Claim 1 (Ex. 1). This occurs by "determining whether the DNS request transmitted in step (1) is requesting access to a secure web site," and "in response to determining that the DNS request in step (2) is requesting access to a secure target web site, automatically initiating the VPN between the client computer and the target computer." *Id.* One of ordinary skill in the art would understand that the DNS request to access the "secure target web site" located on the target computer triggers establishing a VPN between the two devices. This Court reached the same conclusion in its *Microsoft* claim construction opinion when it stated "[b]ecause a VPN may be established between the client computer and target computer, the 'secure target web site' can communicate in the VPN so that the client computer can access the 'secure target web site' ***at the target computer***." Ex. A at 19 (emphasis added) (citing '135 Patent at 47:29-32, 48:16-19).

[17] VirnetX provides only one new argument to support its doomed construction. That is, VirnetX argues that the examiner in the reexamination used the terms in a "manner consistent with" VirnetX's proposed construction when comparing a prior art reference. Notwithstanding, the proper focus is not on speculating how the examiner may have or may not have used the term, but instead on how one of ordinary skill in the art would interpret the claim language. Here, the Court has carefully made that determination, and Plaintiff's "addendum" does not change or alter the Court's prior analysis. *Lindemann Maschinenfabrik GMBH v. Am. Hoist & Derrick Co.*, 730 F.2d 1452, 1460 n.5 (Fed. Cir. 1984) ("Though the courts will give due respect to the examiner's evaluation of prior art, they are not of course bound thereby.") Accordingly, the Court should once again reject VirnetX's overly broad construction.

2. Secure Web Computer

Term	VirnetX's Proposed Construction	Defendants' Proposed Construction
Secure Web Computer	a server that requires authorization for access and that can communicate in a secure communication link	[indefinite or "the target computer that hosts the secure web site"]

Like the term "secure target website," the parties dispute whether the "secure web site" must be located on the "secure web computer" as required by claim 10 of the '135 Patent. The term first appears as "***the*** secure web computer" and not, *e.g.*, "***a*** secure web computer." Because the term first appears without proper antecedent basis, the term is either indefinite or must derive its antecedent basis from the "secure target computer" that is recited earlier in the claim. The modifier "secure web" preceding "computer" informs one of ordinary skill in the art that the "secure web site" is located on the "secure target computer" because the "secure target computer" is also described as the "secure web computer." Indeed, just as the language of claim 1 confirms that "secure target web site" is at the "target computer," *see supra* IV.E.1., the language of claim 10 confirms that the "secure website" is at the secure web computer (that is, the secure target computer with the secure website).

For reasons set forth above, Defendants' construction of "web computer" is correct. VirnetX's construction is improper because it reads out the term "web" from its construction.[18]

[18] As discussed above, the phrase "secure web computer" lacks antecedent basis in claim 10 of the '135 Patent. VirnetX attempts to resolve this invalidity problem by arguing that the phrase "secure target computer" provides the antecedent basis for the phrase "secure web computer." Regardless, to avoid rendering the claim insolubly ambiguous, the phrase "secure web computer" and the phrase "secure target computer" must be referring to the same computer. In fact, when considered in the context of the entire claim, the modifier "secure web" preceding "computer" further informs one of ordinary skill in the art that the "secure web site" is located on the "secure web computer," which is the same computer as the "secure target computer."

F. Disputes pertaining to the '759 Patent

1. Cryptographic Information

Term	VirnetX's Proposed Construction	Cisco's Proposed Construction[19]
Cryptographic Information	information that is used to encode data or information that is used to decode data	information that is required in order to encode/decode or encrypt to ensure secrecy

Both parties agree that the construction of this term from the *Microsoft* case could benefit from clarification to more closely comport with the specification. Cisco submits, however, that contrary to VirnetX's proposal, the Court's previous construction need not be rewritten entirely, and requires only a minor clarification. Cisco's proposed construction therefore closely tracks the Court's prior order and the meaning accorded to the term by the specification.

According to the specification, cryptographic information is not information that is ***itself*** encrypted, but rather is used to set up an encrypted virtual private network communication link. The '759 specification refers to cryptographic information in the context of ***establishing*** a virtual private network link. The specification notes that "[t]he user does not need to enter any user identification information, passwords or encryption keys for establishing a secure communication link." '759 Patent (attached as Ex. 4) at 51:39-41. Such "cryptographic information" is not necessarily encoded/decoded itself, but rather is required to encode/decode information passing through the virtual private network. With the exception of this small modification, Cisco's proposed construction is virtually identical to the Court's construction from the *Microsoft* case.

VirnetX argues that Cisco's proposed construction is "ambiguous at points" since it "seems to require the inclusion of all conceivable information that is required to encrypt and decrypt information in order for it to be 'cryptographic information.'" D.I. 173 at 28. The Court has already rejected a similar argument directed toward "encoding or decoding" in the *Microsoft*

[19] The '759 Patent is only asserted against Defendant Cisco.

case, noting that this concern "is addressed by the Court's construction language 'to ensure secrecy,' which modifies both 'encoded/decoded' and 'encrypted.'" Ex. A at 27. Here, too, the language "to ensure secrecy" should resolve any concerns of ambiguity, and Cisco proposes slightly modifying the Court's previous construction to emphasize that cryptographic information is required to "encode/decode or encrypt to ensure secrecy," rather than being encrypted or encoded itself.

2. Enabling A Secure Communication Mode Of Communication

Term	VirnetX's Proposed Construction	Cisco's Proposed Construction
Enabling A Secure Communication Model of Communication	[no construction necessary]	using an input device to select a secure communication mode of communication

While the Court's claim construction ruling in *Microsoft* states that this term requires no construction, Cisco respectfully submits that a fair reading of the specification explains exactly what it means to enable a secure communication mode of communication, and that the term should be construed accordingly. Specifically, according to the specification, enabling a secure communication mode requires using an input device to select the mode. Thus, for example:

- "***By clicking on the 'go secure' hyperlink***, a user at computer 3301 has enabled a secure communication mode of communication between computer 3301 and server computer 3304."
- In one embodiment, a secure communication mode is enabled at a first computer without a user entering any cryptographic information for establishing the secure communication mode of communication, ***preferably by merely selecting an icon displayed on the first computer***. Alternatively, the secure communication mode of communication can be enabled ***by entering a command into the first computer***.

Ex. 4 at 51:34-37; 6:44-51 (emphasis added). These passages make clear that the act of enabling a secure communication mode of communication involves a user's use of an input device, such as a mouse or keyboard to perform a selection.

VirnetX does not challenge the substance of Cisco's proposed construction, but instead

argues that the disputed term is "really [an] entire paragraph[]" and therefore does not lend itself to construction. D.I. 173 at 27. But the purpose of the claim construction exercise is to elucidate the meaning of the claim language, and no rule exists mandating that the analysis be performed on a word-by-word basis. *On Demand Mach. Corp. v. Ingram Indus.*, 442 F.3d 1331, 1344 (Fed. Cir. 2006) ("Care must be taken lest word-by-word definition, removed from the context of the invention, leads to an overall result that departs significantly from the patented invention.").

G. Dispute Regarding The "Generating" Limitation

Term	VirnetX's Proposed Construction	Defendants' Proposed Construction
Generating From The Client Computer a DNS Request	[no construction necessary]	creating and transmitting from the client computer a DNS request

The dispute between the parties is whether the "generating from" phrase requires the DNS request to be transmitted from the client computer. The plain language of Claim 1 of the '135 Patent requires that it does, otherwise the claim would be invalid for indefiniteness. Step (1) of Claim 1 requires "generating from the client computer" a DNS request. Ex. 1, claim 1, at 47:23-28. The next step requires "determining whether the DNS request ***transmitted in step (1)*** is requesting access to a secure web site". *Id.* (emphasis added). However, there is no previous reference to "transmitted" in step (1). Reading steps (1) and (2) together makes it clear that "generating ***from*** the client computer" means the DNS request is transmitted from the client computer; hence the step (2) reference to "the DNS request transmitted in step (1)." The patent specification describes that the DNS request is transmitted from the client computer 2601 to the modified DNS server 2602.[20] *See id.* at Fig. 26, 38:13-22.

[20] This issue was not addressed in the earlier *Microsoft* litigation. In *Microsoft*, the issue was whether the client computer could perform the determining step or whether, because the client computer transmits the DNS request, the determining step must, therefore, be performed on another computer. Here, the dispute is whether the DNS request must be transmitted from the client computer in the first place. As shown above, the plain language requires that it must.

Dated: December 7, 2011

Respectfully submitted,

By: */s/ Dmitriy Kheyfits*

John M. Desmarais (*pro hac vice*)
jdesmarais@desmaraisllp.com
Michael P. Stadnick (*pro hac vice*)
mstadnick@desmaraisllp.com
Dmitriy Kheyfits (*pro hac vice*)
dkheyfits@desmaraisllp.com
DESMARAIS LLP
230 Park Avenue
New York, NY 10169
Telephone: (212) 351-3400
Facsimile: (212) 351-3401

LEAD COUNSEL FOR DEFENDANT CISCO SYSTEMS, INC.

Michael E. Jones
State Bar No. 10929400
mikejones@potterminton.com
POTTER MINTON, P.C.
110 N. College Ave., Suite 500
Tyler, Texas 75702
(903) 597-8311
(903) 593-0846 (Facsimile)

LOCAL COUNSEL FOR DEFENDANT CISCO SYSTEMS, INC.

/s/ Danny L. Williams
Danny L. Williams - LEAD ATTORNEY
State Bar No. 21518050
E-mail: danny@wmalaw.com
Ruben S. Bains
Texas Bar No. 24001678
E-mail: rbains@wmalaw.com
Drew Kim
Texas Bar No. 24007482
E-mail: dkim@wmalaw.com
Williams, Morgan &Amerson, P.C.
10333 Richmond, Suite 1100
Houston, Texas 77042
Telephone: (713) 934-7000
Facsimile: (713) 934-7011

ATTORNEYS FOR DEFENDANT APPLE INC.

By: */s/ Jon B. Hyland*
Jon B. Hyland
Lead Attorney
jhyland@pattonroberts.com
State Bar No. 24046131
Robert D. Katz
rkatz@pattonroberts.com
State Bar No. 24057936
PATTON ROBERTS, PLLC
901 Main St., Suite 3300
Dallas, Texas 75202
Telephone: 214-580-3826
Facsimile: 903-334-7007

ATTORNEYS FOR DEFENDANTS AASTRA USA, INC. AND AASTRA TECHNOLOGIES LTD.

By:*/s/ Douglas R. McSwane, Jr.*
Douglas R. McSwane, Jr.
Texas State Bar No. 13861300
dougmcswane@potterminton.com
500 Plaza Tower
110 N. College Ave. (75702)
P.O. Box 359
Tyler, Texas 75710
Telephone: 903-597-8311
Facsimile: 903-593-0846

Robert M. Masters
robmasters@paulhastings.com
Timothy P. Cremen
timothycremen@paulhastings.com
PAUL, HASTINGS, JANOFSKY &WALKER LLP
875 15th Street, N.W.,
Washington, D.C. 20005
Telephone: 202-551-1700
Facsimile: 202-551-0238

ATTORNEYS FOR DEFENDANTS NEC CORPORATION AND NEC CORPORATION OF AMERICA

CERTIFICATE OF SERVICE

The undersigned hereby certifies that counsel of record who are deemed to have consented to electronic service are being served with a copy of this **DEFENDANTS'RESPONSIVE CLAIM CONSTRUCTION BRIEF**, *via* the Court's CM/ECF system per Local Rule CV-5(a)(3) on this the 7th Day of December, 2011.

/s/ Dmitriy Kheyfits
Dmitriy Kheyfits