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

VIRNETX INC.,	§	
	§	
Plaintiff,	§	
	§	
vs.	§	**CASE NO. 6:10-CV-417**
	§	
CISCO SYSTEMS, INC., et al.,	§	
	§	
Defendants.	§	
	§	

MEMORANDUM OPINION AND ORDER

This Memorandum Opinion construes the disputed claim terms in U.S. Patent Nos. 6,502,135 ("the '135 Patent"), 6,839,759 ("the '759 Patent"), 7,188,180 ("the '180 Patent"), 7,418,504 ("the '504 Patent"), 7,490,151 ("the '151 Patent"), and 7,921,211 ("the '211 Patent").

Further, as stated at the *Markman* hearing and agreed by the parties, the Court **ORDERS** that VirnetX Inc.'s Motion to Compel from Apple a Complete Response to VirnetX's Eighth Common Interrogatory (Docket No. 179) is **DENIED AS MOOT**.

BACKGROUND

VirnetX Inc. ("VirnetX") asserts all six patents-in-suit against Aastra Technologies Ltd.; Aastra USA, Inc.; Apple Inc.; Cisco Systems, Inc.; NEC Corporation; and NEC Corporation of America (collectively "Defendants"). The '135 Patent discloses a method of transparently creating a virtual private network ("VPN") between a client computer and a target computer. The '759 Patent discloses a method for establishing a VPN without a user entering user identification information. The '180 Patent discloses a method of establishing a secure communication link between two computers. The '504 and '211 Patents disclose a secure domain name service. The

‘151 Patent discloses a domain name service capable of handling both standard and non-standard domain name service queries.

The patents-in-suit are all related; Application No. 09/504,783 (“the ‘783 Application”) is an ancestor application for every patent-in-suit. The ‘135 Patent issued on December 31, 2002, from the ‘783 Application. The ‘151 Patent issued from a division of the ‘783 Application. The ‘180 Patent issued from a division of a continuation-in-part of the ‘783 Application. Both the ‘759 and ‘504 Patents issued from a continuation of a continuation-in-part of the ‘783 Application. Finally, the ‘211 Patent is a continuation of the application that resulted in the ‘504 patent.

The Court has already construed many of the terms at issue in a previous case that involved the ‘135, ‘759, and ‘180 Patents. *See VirnetX, Inc. v. Microsoft Corp.*, 2009 U.S. Dist. LEXIS 65667, No. 6:07cv80 (E.D. Tex. July 30, 2009) (“*Microsoft*”).

APPLICABLE LAW

“It is a ‘bedrock principle’ of patent law that ‘the claims of a patent define the invention to which the patentee is entitled the right to exclude.’” *Phillips v. AWH Corp.*, 415 F.3d 1303, 1312 (Fed. Cir. 2005) (en banc) (quoting *Innova/Pure Water Inc. v. Safari Water Filtration Sys., Inc.*, 381 F.3d 1111, 1115 (Fed. Cir. 2004)). In claim construction, courts examine the patent’s intrinsic evidence to define the patented invention’s scope. *See id.*; *C.R. Bard, Inc. v. U.S. Surgical Corp.*, 388 F.3d 858, 861 (Fed. Cir. 2004); *Bell Atl. Network Servs., Inc. v. Covad Commc’ns Group, Inc.*, 262 F.3d 1258, 1267 (Fed. Cir. 2001). This intrinsic evidence includes the claims themselves, the specification, and the prosecution history. *See Phillips*, 415 F.3d at 1314; *C.R. Bard, Inc.*, 388 F.3d at 861. Courts give claim terms their ordinary and accustomed meaning as understood by one of ordinary skill in the art at the time of the invention in the

context of the entire patent. *Phillips*, 415 F.3d at 1312–13; *Alloc, Inc. v. Int'l Trade Comm'n*, 342 F.3d 1361, 1368 (Fed. Cir. 2003).

The claims themselves provide substantial guidance in determining the meaning of particular claim terms. *Phillips*, 415 F.3d at 1314. First, a term's context in the asserted claim can be very instructive. *Id.* Other asserted or unasserted claims can also aid in determining the claim's meaning because claim terms are typically used consistently throughout the patent. *Id.* Differences among the claim terms can also assist in understanding a term's meaning. *Id.* For example, when a dependent claim adds a limitation to an independent claim, it is presumed that the independent claim does not include the limitation. *Id.* at 1314–15.

"[C]laims 'must be read in view of the specification, of which they are a part.'" *Id.* (quoting *Markman v. Westview Instruments, Inc.*, 52 F.3d 967, 979 (Fed. Cir. 1995) (en banc)). "[T]he specification 'is always highly relevant to the claim construction analysis. Usually, it is dispositive; it is the single best guide to the meaning of a disputed term.'" *Id.* (quoting *Vitronics Corp. v. Conceptronic, Inc.*, 90 F.3d 1576, 1582 (Fed. Cir. 1996)); *see also Teleflex, Inc. v. Ficosa N. Am. Corp.*, 299 F.3d 1313, 1325 (Fed. Cir. 2002). This is true because a patentee may define his own terms, give a claim term a different meaning than the term would otherwise possess, or disclaim or disavow the claim scope. *Phillips*, 415 F.3d at 1316. In these situations, the inventor's lexicography governs. *Id.* Also, the specification may resolve ambiguous claim terms "where the ordinary and accustomed meaning of the words used in the claims lack sufficient clarity to permit the scope of the claim to be ascertained from the words alone." *Teleflex, Inc.*, 299 F.3d at 1325. But, "'[a]lthough the specification may aid the court in interpreting the meaning of disputed claim language, particular embodiments and examples appearing in the specification will not generally be read into the claims.'" *Comark Commc'ns,*

Inc. v. Harris Corp., 156 F.3d 1182, 1187 (Fed. Cir. 1998) (quoting *Constant v. Advanced Micro-Devices, Inc.*, 848 F.2d 1560, 1571 (Fed. Cir. 1988)); *see also Phillips*, 415 F.3d at 1323. The prosecution history is another tool to supply the proper context for claim construction because a patent applicant may also define a term in prosecuting the patent. *Home Diagnostics, Inc., v. Lifescan, Inc.*, 381 F.3d 1352, 1356 (Fed. Cir. 2004) ("As in the case of the specification, a patent applicant may define a term in prosecuting a patent.").

Although extrinsic evidence can be useful, it is "'less significant than the intrinsic record in determining the legally operative meaning of claim language.'" *Phillips*, 415 F.3d at 1317 (quoting *C.R. Bard, Inc.*, 388 F.3d at 862). Technical dictionaries and treatises may help a court understand the underlying technology and the manner in which one skilled in the art might use claim terms, but technical dictionaries and treatises may provide definitions that are too broad or may not be indicative of how the term is used in the patent. *Id.* at 1318. Similarly, expert testimony may aid a court in understanding the underlying technology and determining the particular meaning of a term in the pertinent field, but an expert's conclusory, unsupported assertions as to a term's definition is entirely unhelpful to a court. *Id.* Generally, extrinsic evidence is "less reliable than the patent and its prosecution history in determining how to read claim terms." *Id.*

Defendants also contend that some claims at issue are invalid for indefiniteness. A claim is invalid under 35 U.S.C. § 112 ¶ 2 if it fails to particularly point out and distinctly claim the subject matter that the applicant regards as the invention. The party seeking to invalidate a claim under 35 U.S.C. § 112 ¶ 2 as indefinite must show by clear and convincing evidence that one skilled in the art would not understand the scope of the claim when read in light of the

specification. *Intellectual Prop. Dev., Inc. v. UA-Columbia Cablevision of Westchester, Inc.*, 336 F.3d 1308, 1319 (Fed. Cir. 2003).

LEVEL OF ORDINARY SKILL IN THE ART

The parties agree that a person of ordinary skill in the art would have a master's degree in computer science or computer engineering and approximately two years of experience in computer networking and computer network security.

CLAIM TERMS

virtual private network

VirnetX proposes "a network of computers which privately communicate with each other by encrypting traffic on insecure communication paths between the computers." Defendants propose the following emphasized additions: "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***."

secure and anonymous

VirnetX proposes the same construction adopted by this Court in *Microsoft*. *See Microsoft*, 2009 U.S. Dist. LEXIS 65667, at *8. Defendants seek to explicitly include the "secure and anonymous" language that was implicitly included in the Court's *Microsoft* construction. *See id.* at *16 ("[T]he Court construes 'virtual private network' as requiring both data security and anonymity."). Just as in *Microsoft*, the parties here dispute whether a virtual private network requires anonymity, and the Court hereby incorporates by reference its reasoning in *Microsoft*. *See id.* at *14–17. For the same reasons stated in *Microsoft*, the Court finds that a virtual private network requires both data security and anonymity. For clarity, this language is now explicitly included in the Court's construction of "virtual private network."

directly

Defendants propose that communication within a virtual private network is "direct" based on arguments that VirnetX made to the United States Patent and Trademark Office ("PTO") to overcome rejections based on the Aventail reference during reexamination of the '135 Patent.[1] VirnetX provided three reasons that Aventail did not disclose a virtual private network:

> First, Aventail has not been shown to demonstrate that computers connected via the Aventail system are able to communicate with each other as though they were on the same network. . . .
> . . .
> Second, according to Aventail, Aventail Connect's fundamental operation is incompatible with users transmitting data that is sensitive to network information. . . .
> Third, Aventail has not been shown to disclose a VPN because computers connected according to Aventail do not communicate directly with each other.

Docket No. 182 Attach. 16, at 5–7. Defendants argue that VirnetX's third distinction warrants a finding that communication over a virtual private network must be direct.

VirnetX argues that its statements during reexamination are not a clear disavowal of claim scope. Rather, VirnetX contends that it "overcame Aventail on the ground that Aventail did not teach a VPN at all." Docket No. 173, at 8. However, the statements made by VirnetX—particularly points one and three—reveal that the *reason* Aventail did not disclose a VPN was because it did not permit direct communication between the source and target computers.

VirnetX further argues that it did not clearly disavow claim scope regarding any one of the three distinctions between Aventail and a VPN. For support, VirnetX relies on *Momentus Golf, Inc. v. Swingrite Golf Corp.*, 187 Fed. App'x 981 (Fed. Cir. 2006), which involved a patent directed to a golf club swing aide. During prosecution of the *Momentus Golf* patent, the applicants stated: "A hollow device having 10–25% club head weight cannot meet the

[1] The Aventail reference involved a means of secure communication between two clients via an intermediary SOCKS server.

requirement in applicant's claims that the center of gravity of the trainer be substantially at the center of a solid round stock." *Momentus Golf*, 187 Fed. App'x at 984 (quoting prosecution history). The district court held that this statement presented a clear disavowal of golf trainers with 10–25% club head weight because they would not meet the center of gravity requirement. *Id.* at 982. The Federal Circuit agreed that the district court's interpretation was a fathomable one. *Id.* at 983–84. However, it reversed the district court because another interpretation was also reasonable and still supported the applicant's distinguishing arguments—that the statement only clearly disavowed *hollow clubs* with 10–25% club head weight. *Id.* at 984 (emphasis added). The Federal Circuit held that the statement could reasonably be interpreted to disavow (1) clubs with 10–25% club head weight or (2) hollow clubs with 10–25% club head weight. In light of the competing interpretations, the Federal Circuit determined that there was only a disclaimer of the more narrow interpretation.

The instant case does not present such an ambiguous statement. VirnetX stated that "Aventail has not been shown to disclose the VPN . . . for at least three reasons." Docket No. 182 Attach. 16, at 5. VirnetX then proceeded to independently present and discuss each of the three distinct reasons that Aventail did not disclose the claimed VPN. *See* Docket No. 182 Attach. 16, at 5–6 (discussing the first reason); *id.* at 6–7 (discussing the second reason); *id.* at 7 (discussing the third reason). In *Momentus Golf*, the applicant combined two potential distinctions in a single sentence, creating ambiguity as to whether the distinctions were independent or intertwined. Here, VirnetX expressly stated that there were three bases for distinction. Each of these reasons, alone, served to distinguish the claimed VPN from the Aventail reference. *See Andersen Corp. v. Fiber Composites, LLC*, 474 F.3d 1361, 1374 (Fed. Cir. 2007) ("An applicant's invocation of multiple grounds for distinguishing a prior art reference does not immunize each of them from

being used to construe the claim language."). Accordingly, the Court finds that the claimed "virtual private network" requires direct communication between member computers.[2]

The Court construes "virtual private network" as "a network of computers which privately and directly communicate with each other by encrypting traffic on insecure paths between the computers where the communication is both secure and anonymous."

virtual private link

VirnetX proposes "a communication link that permits computers to privately communicate with each other by encrypting traffic on insecure communication paths between the computers." Defendants, except the two Aastra entities, propose "a link in a virtual private network." The Aastra entities propose "a link in a virtual private network that accomplishes data security and anonymity through the use of hop tables."

VirnetX's proposed construction closely tracks its proposal for "virtual private network," replacing "a network of computers which" with "a communication link that permits computers to." "Network of computers" implies that the computers are linked together; likewise a "communication link that permits computers [to communicate]" implies a computer network.

Defendants also note the similarity between VirnetX's proposed construction of "virtual private network" and "virtual private link." Defendants contend that VirnetX's proposal is essentially "a communication link that permits computers to VPN." Tr. of *Markman* Hr'g 55, Jan. 5, 2012. As a simplification, Defendants propose "a link in a virtual private network."

The Aastra entities argue that a virtual private link should be limited to virtual private network links that use hop tables to achieve data security and anonymity. An embodiment of

[2] Defendants stipulated at the *Markman* hearing that they were not arguing "directly" requires a direct electromechanical connection. *See* Tr. of *Markman* Hr'g 49–50, Jan. 5, 2012. Rather, Defendants maintained that directly requires direct addressability. Thus, routers, firewalls, and similar servers that participate in typical network communication do not impede "direct" communication between a client and target computer.

claim 13 of the '135 Patent, which contains the term "virtual private link," is depicted in Figure 31. A detailed description of this embodiment is also provided in the specification. *See* '135 Patent cols. 44:14–45:35. This description discusses the use of hopping tables; thus, Aastra argues that this limitation should be imported into the claims.

The Court rejects Aastra's attempt to incorporate limitations of a preferred embodiment into the claims. *See Falana v. Kent State Univ.*, 669 F.3d 1349, 1355 (Fed. Cir. 2012) (cautioning against importing limitations from a preferred embodiment into the claims). The specification notes that the use of hopping is one *option* for accomplishing the data security and anonymity features. *See* '135 Patent col. 45:10–13 ("Next, signaling server 3101 issues a request to transport server 3102 to allocate a hopping table (or hopping algorithm *or other regime*) for the purpose of creating a VPN with client 3103" (emphasis added)). Thus, the applicants envisioned alternate methods of implementing data security and anonymity beyond hopping tables, and importing the hopping limitation into the claims is inappropriate.

The patent specification, in the detailed description of Figure 31, uses the term virtual private network and virtual private link interchangeably. *Compare id.* col. 44:37–40 ("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 . . . ."), *with id.* col. 45:10–13 (noting that the signaling server requests the transport server to create a hopping table for the purpose of "creating a VPN with client 3103."), *and id.* col. 45:32–35 ("After a VPN has become inactive for a certain time period (e.g., one hour), the VPN can be automatically torn down by transport server 3102 or signaling server 3101."); *see Nystrom v. Trex Co., Inc.*, 424 F.3d 1136, 1143 (Fed. Cir. 2005) ("Different terms or phrases in separate claims may be construed to cover the same subject matter where the written description and prosecution history indicate that such a reading of the

terms or phrases is proper."). Finally, VirnetX's and Defendants' proposed constructions of virtual private link are very similar to their proposed constructions for virtual private network. Accordingly, the Court construes "virtual private link" as "a virtual private network as previously defined."

secure communication link

VirnetX proposes "an encrypted communication link." Defendants propose "virtual private network communication link." The parties in *Microsoft* agreed that this term, as used in the '759 Patent, did not require construction because the claims themselves provide a definition of the term. *Microsoft*, 2009 U.S. Dist. LEXIS 65667, at *43. For instance, claim 1 states: "the secure communication link being a virtual private network communication link over the computer network." '759 Patent col. 57:20–22. Here, the parties also agree that, as to the '759 Patent, the term means "virtual private network communication link." However, the claims of the '504 and '211 Patents use this term without further defining it. Thus, the parties dispute the construction of the term as used in the '504 and '211 Patents.

VirnetX contends that "secure" means the link uses some form of data encryption, highlighting the following passage from the '504 Patent specification: "Data security is usually tackled using some form of data encryption." '504 Patent col. 1:55–56. VirnetX argues that the inventors would have used the term "virtual private network communication link" had it desired to limit "secure communication link" to that interpretation. VirnetX further argues Defendants' proposal improperly imports a limitation from the preferred embodiment, which discloses a secure communication link that is also a virtual private network communication link. VirnetX states that "Defendants fail to explain why a secure communication link *must always* be a virtual private network communication link for *all* possible embodiments of the claims." Docket No.

192, at 4. Finally, VirnetX argues that it did not narrow the interpretation of "secure communication link" during the prosecution of the '504 and '211 Patents.

Defendants argue that secure communication link is defined in the Summary of the Invention: "The secure communication link is a virtual private network communication link over the computer network." '504 Patent col. 6:61–62. Defendants further argue that the detailed description of the invention also uses the terms "secure communication link" and "virtual private network communication link" synonymously. Defendants also highlight VirnetX's arguments regarding "secure communication link" while prosecuting U.S. Patent No. 8,051,181 ("the '181 patent"), a related patent that is not at issue in the instant case.

The '181 Patent is related to the patents-in-suit; it is a division of a continuation-in-part of the '783 Application that serves as an ancestor application for all of the patents-in-suit. The Federal Circuit has held that arguments to the PTO regarding one patent application are applicable to related patent applications. *See Microsoft Corp. v. Multi-Tech Sys., Inc.*, 357 F.3d 1340, 1349 (Fed. Cir. 2004) ("[T]he prosecution history of one patent is relevant to an understanding of the scope of a common term in a second patent stemming from the same parent application."). The Federal Circuit has also held that arguments regarding a later filed application may be applicable to a previously filed application. *See Verizon Servs. Corp. v. Vonage Holdings Corp.*, 503 F.3d 1295, 1307 (Fed. Cir. 2007) (rejecting the argument that a disclaimer should not apply because it occurred after the patent under consideration had issued). Here, the '181 Patent issued after all of the patents-in-suit. Its application was filed later than the applications for the patents-in-suit except for the '211 Patent, which was filed approximately six months earlier.

When prosecuting the '181 Patent, VirnetX distinguished the Aventail reference from the "secure communication link" limitation using arguments nearly identical to those discussed

earlier regarding Aventail and the "virtual private network" term. VirnetX argued that Aventail failed to disclose a "secure communication link" for the same three reasons asserted in the '135 reexamination. *Compare* Docket No. 182 Attach. 16, at 5–7 (arguments regarding "virtual private network" and Aventail), *with* Docket No. 202 Attach. 1, at 6–8 (arguments regarding "secure communication link" and Aventail). Therefore, for the same reasons stated earlier regarding "virtual private network," a "secure communication link" also requires direct communication between its nodes.

"Secure communication link" was originally used in the claims of the '759 Patent, which was also at issue in *Microsoft*. There, the parties agreed that it did not require construction because the claim language itself defined the term as "being a virtual private network communication link." '759 Patent col. 57:20–22. However, the later-filed applications that issued as the '504 and '211 Patents removed this defining language from the claims. Accordingly the term is not so limited in the '504 and '211 Patents as in the '759 Patent.

Defendants argue that the Summary of the Invention defined a secure communication link as a virtual private network communication link. However, this discussion in the Summary of the Invention relates to a particular preferred embodiment and opens as follows:

> According to one aspect of the present invention, a user can conveniently establish a VPN using a "one-click" . . . technique without being required to enter [information] for establishing a VPN. The advantages of the present invention are provided by a method for establishing a secure communication link . . . .

'504 Patent col. 6:36–42. Thus, the advantage of being able to seamlessly establish a one-click VPN is provided by "a method for establishing a secure communication link." The description continues by describing the details of an embodiment that realizes this advantage. *See id.* cols. 6:43–7:10 (describing the one-click embodiment). It is within this description of the preferred embodiment that the specification acknowledges that the "secure communication link is a virtual

private network communication link." *Id.* col. 6:61–63. The patentee is not acting as his own lexicographer here; rather, he is describing a preferred embodiment. The claims and specification of the '504 and '211 Patents reveal that the patentee made a conscious decision to remove the virtual private network limitation originally present in the '759 Patent claims. Thus, secure communication link shall be interpreted without this limitation in the '504 and '211 Patents.

VirnetX proposes that a secure communication link is an encrypted link. However, claim 28 of the '504 Patent[3] covers "[t]he system of claim 1, wherein the secure communication link uses encryption." '504 Patent col. 57:17–18. VirnetX's proposal seeks to import a limitation from dependent claim 28 into independent claim 1, and this violates the doctrine of claim differentiation. *See Curtiss-Wright Flow Control Corp. v. Velan, Inc.*, 438 F.3d 1374, 1380 (Fed. Cir. 2006) ("'[C]laim differentiation' refers to the presumption that an independent claim should not be construed as requiring a limitation added by a dependent claim."). The specification notes that "[d]ata security is *usually* tackled using some form of data encryption." '504 Patent col. 1:55–56 (emphasis added). Therefore, encryption is not the only means of addressing data security. Accordingly, a secure communication link is one that provides data security, which includes encryption.

The Court construes "secure communication link" as "a direct communication link that provides data security."[4]

[3] Claim 28 of the '211 Patent is similar.

[4] As the Court discussed earlier, the '759 Patent claims further limit the secure communication link recited therein. This construction does not contradict these provisions of the '759 claims, which limit the secure communication link there to a virtual private network communication link. Thus, as a practical matter, the "secure communication link" recited in the '759 Patent claims is a "virtual private network communication link."

domain name service

VirnetX proposes "a lookup service that returns an IP address for a requested domain name," adopting the Court's previous construction of this term in *Microsoft*. Defendants propose to append "to the requester" to VirnetX's proposed construction.

VirnetX argues that Defendants' proposal incorporates an extraneous limitation. Further, VirnetX provides an expert declaration stating that one of skill in the art, after reading the specification, would understand that a domain name service does not necessarily return the requested IP address to the requester. *See* Docket No. 173 Attach. 17 ¶¶ 7–8 (stating that in the context of a DNS proxy, the IP address may be returned to the original requesting client, the proxy, or both). VirnetX also argues that the specification envisions a domain name service that does not always return an address to the requester. For instance, the specification states:

> According to certain aspects of the invention, a specialized DNS server traps DNS requests and, if the request is from a special type of user . . . , the server does not return the true IP address of the target node, but instead automatically sets up a virtual private network between the target node and the user.

'135 Patent cols. 37:63–38:2. Defendants argue that VirnetX ignores the implicit meaning of the Court's *Microsoft* construction by arguing that a domain name service does not necessarily return the requested IP address to the requester.

VirnetX's expert explains that "in one mode, the domain name request can be received by a DNS proxy (or DNS proxy module), which, in turn, may forward the request to a DNS function that can return an IP address." Docket No. 173 Attach. 17 ¶ 8. Thus, VirnetX argues, a domain name request may cause an IP address to be returned "to the client, or to a DNS proxy . . . , or both." *Id.* VirnetX's expert is effectively describing a scenario detailed in the '135 Patent and cited above by VirnetX. This scenario is further described in detail in the specification and depicted in Figure 26. *See* '135 Patent col. 38:13–42 (describing the operation of the system

depicted in Figure 26). VirnetX asserts that Defendants' proposed construction precludes this preferred embodiment.

Contrary to VirnetX's argument, Defendants' proposed limitation does not preclude a preferred embodiment. The "specialized" or "modified" DNS server referenced in the specification is shown as 2602 in Figure 26. This modified DNS server contains a DNS proxy function and a standard DNS server function. Requests for non-secure sites are passed through to the DNS server, and an IP address is returned to the requesting client. In this case, two separate domain name requests are effectively being made: (1) between the client computer 2601 and the modified DNS server 2602; and (2) between the DNS Proxy 2610 and the DNS Server 2609. If the original client request is for a secure site, then the DNS Proxy 2610 establishes a VPN connection between the client and the secure site. The specification explains the final stages of this process:

> Thereafter, DNS proxy 2610 returns to user computer 2601 the resolved address passed to it by the gatekeeper (this address could be different from the actual target computer) 2604, preferably using a secure administrative VPN. The address that is returned need not be the actual address of the destination computer.

Id. col. 38:36–42. The DNS Proxy 2610, operating as an internal component of the modified DNS server 2602, returns an address to the requestor, the client computer 2601. Thus, viewing the modified DNS server 2602 as a black box, it returned an address to the requesting client computer.

For these reasons, the Court finds that a domain name service inherently returns the IP address for a requested domain name to the requesting party. The Court construes "domain name service" as "a lookup service that returns an IP address for a requested domain name to the requester."

domain name

VirnetX proposes the same construction adopted by the Court in *Microsoft*: "a name corresponding to an IP address." Defendants propose "a hierarchical sequence of words in decreasing order of specificity that corresponds to a numerical IP address." In *Microsoft*, the Court addressed Defendants' argument that a domain name is necessarily hierarchical in nature; that analysis is incorporated herein. *See Microsoft*, 2009 U.S. Dist. LEXIS 65667, at *24–25. For the same reasons stated in *Microsoft*, the Court construes "domain name" as "a name corresponding to an IP address."

DNS proxy server

VirnetX proposes "a computer or program that responds to a domain name inquiry in place of a DNS." Defendants propose "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." VirnetX's proposal and the first portion of Defendants' proposal reflect the construction adopted by this Court in *Microsoft*. *Id.* at *39. Here, the dispute is whether a DNS proxy server "prevents destination servers from determining the identity of the entity sending the domain name inquiry."

Defendants derive support for their proposed limitation directly from the Background of the Invention: "Proxy servers prevent destination servers from determining the identities of originating clients." '135 Patent col. 1:49–50. VirnetX argues that this statement should be read in the context of the sentence that precedes it: "To hide traffic from a local administrator or ISP, a user can employ a local proxy server in communicating over an encrypted channel with an outside proxy such that the local administrator or ISP only sees the encrypted traffic." *Id.* col. 1:46–49. VirnetX contends that these statements are not regarding all proxy servers, but merely detail how proxy servers may be configured to achieve anonymity.

VirnetX also argues that adopting Defendants' construction would read out a preferred embodiment disclosed in Figure 26 of the '135 Patent. In Figure 26, user computer 2601, after interfacing with DNS Proxy 2610, communicates directly with Secure Target Website 2604 or Unsecure Target Site 2611. In this configuration, the DNS Proxy does not prevent the destination servers (secure and unsecure target websites) from learning the identity of the originating client (user computer). Rather, the DNS Proxy enables direct communication between the originating client and destination servers. Accordingly, Defendants' proposed additional limitation should be rejected. *See Globetrotter Software, Inc. v. Elan Computer Grp., Inc.*, 362 F.3d 1367, 1381 (Fed. Cir. 2004) ("A claim interpretation that excludes a preferred embodiment from the scope of the claim 'is rarely, if ever, correct.'" (quoting *Vitronics Corp. v. Conceptronic*, 90 F.3d 1576, 1583 (Fed. Cir. 1996))).

For these reasons and those stated in *Microsoft*, *see* 2009 U.S. Dist. LEXIS 65667, at *39–42, the Court construes "DNS proxy server" as "a computer or program that responds to a domain name inquiry in place of a DNS."

secure domain name service

VirnetX proposes "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." Defendants propose "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." Both parties propose a different construction from that adopted by this Court in *Microsoft* because of arguments made during reexamination of the '180 Patent. The following statements by VirnetX during the reexamination of the '180 Patent provide the basis for both parties' proposals:

> 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 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.

Docket No. 173 Attach. 13, at 24 (internal citations omitted). The parties dispute whether "non-standard" should characterize the secure domain name service and whether the "perform its services accordingly" language should be included in the construction.

Defendants contend that VirnetX's reexamination arguments require that a secure domain name service be qualified as a "non-standard" service. During reexamination, VirnetX argued that the PTO's "position that a secure domain name service is nothing more than a *conventional* DNS server that happens to resolve domain names of secure computers" was faulty. *Id.* (emphasis added). VirnetX clarified that a "secure domain name service is unlike a *conventional* domain name service . . . ." *Id.* (emphasis added). VirnetX further explained 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." *Id.* (emphasis added). VirnetX repeatedly distinguishes a secure domain name service from a *conventional* domain name service, implying that the secure domain name service is not conventional. Further, the '180 Patent distinguishes between a secure domain name service and a standard domain name service. *See* '180 Patent col. 51:29–45 (distinguishing between a "secure domain name service (SDNS)" and a "standard domain name service (STD DNS)").

VirnetX argues that the "non-standard" limitation is not supported by the specification or prosecution history. However, the '180 Patent specification and VirnetX's statements during the '180 reexamination support Defendants' proposed distinction between a standard domain name service and a secure (non-standard) domain name service. Accordingly, the "non-standard" characterization proposed by Defendants should be retained.

Defendants next argue that "perform its services accordingly" should be included in the construction because this is part of the language that VirnetX used to distinguish a secure domain name service from a conventional domain name service during reexamination. VirnetX responds that this language is superfluous because both parties agree on the task performed by the secure domain name service, namely, returning a secure network address for a requested secure domain name. The Court agrees that "perform its services accordingly" adds little to the understanding of secure domain name service and should not be included in the construction.

The Court construes "secure domain name service" as "a non-standard 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."

domain name service system

VirnetX proposes that no construction is necessary, but alternatively proposes "a computer system that includes a domain name service (DNS)." Defendants propose "a DNS that is capable of differentiating between, and responding to, both standard and secure top-level domain names."

Both parties cite claim 1 of the '504 Patent to support their proposed constructions, which states:

> A system for providing a domain name service for establishing a secure communication link, the system comprising:
>
> a *domain name service system* configured to be connected to a communication network, to store a plurality of domain names and corresponding network addresses, to receive a query for a network address, and to comprise an indication that the *domain name service system* supports establishing a secure communication link.

'504 Patent col. 55:49–56 (emphases added). VirnetX argues that the claim language itself describes the required properties of a domain name service system. Defendants argue that the addition of the word "system" to domain name service means it must be something more than a

lookup service. Defendants also cite the preferred embodiment disclosed in Figures 33 and 34 of the specification to further support their construction. There, the client computer 3301 is potentially able to communicate with the non-secure server 3304 and the secure server 3320. Accordingly, Defendants argue, the domain name service system, which correlates to the preferred embodiment described in Figures 33 and 34, necessarily includes the ability to handle both secure and standard domain names.

The claims do not require that that domain name service system be able to handle both secure and non-secure domain names. Rather, it must "comprise an indication that [it] supports establishing a secure communication link." *Id.* col. 55:54–56. Defendants seek to improperly import limitations from a preferred embodiment into the claim language. The claim language itself provides a description of the domain name service system. Thus, the Court finds that "domain name service system" does not require construction.

web site

VirnetX proposes "a computer associated with a domain name and that can communicate in a network ." Defendants propose "one or more related web pages at a location on the World Wide Web." These two proposals mirror the proposals made in *Microsoft*. *See Microsoft*, 2009 U.S. Dist. LEXIS 65667, at *26. There, the Court adopted Defendants' proposal.

The parties' arguments mirror those made in *Microsoft*; in fact, VirnetX has incorporated its *Microsoft* arguments by reference. VirnetX notes that the examiner failed to mention web pages or the World Wide Web in determining that the Aventail reference met the "secure web site" limitation of certain claims of the '135 Patent. VirnetX argues that this supports its broader construction of website, showing that a person of ordinary skill in the art would not read web site so narrowly as to implicate the World Wide Web. As both parties have recognized, however, this

Court is not bound by the examiner's evaluation of prior art. The Court hereby incorporates its previous analysis of the arguments regarding the term "web site." *See id.* at *26–31.

For the same reasons stated in *Microsoft*, the Court construes "web site" as "one or more related web pages at a location on the World Wide Web."

secure web site

VirnetX proposes "a computer associated with a domain name and that can communicate in a virtual private network." Defendants propose "a web site that requires authorization for access and that can communicate in a VPN." Again, the proposals and arguments regarding this term mirror those in *Microsoft*, and the Court incorporates by reference its previous analysis. *See id.* at *31–33. The Court construes "secure web site" as "a web site that requires authorization for access and that can communicate in a VPN."

secure target web site

VirnetX proposes "a target computer associated with a domain name and that can communicate in a virtual private network." Defendants propose "a secure web site on the target computer."

Claim 1 of the '135 Patent, in relevant part, states:

> A method of transparently creating a virtual private network (VPN) between a client computer and a *target computer*, comprising the steps of:
> (1) generating from the client computer a Domain Name Service (DNS) request . . . ;
> (2) determining whether the DNS request transmitted in step (1) is requesting access to a *secure web site*; and
> (3) 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 *target computer*.

'135 Patent col. 47:20–33 (emphases added). The method can be stated differently as: if there is a DNS request for a secure web site, create a VPN between the client computer and target computer. This VPN is presumably for accessing the secure web site, and the target computer is

hosting the secure web site. The claim language itself supports this interpretation because step 3 refers to "secure target web site," thus linking the earlier referenced secure web site to the earlier referenced target computer. Accordingly, the Court construes "secure target web site" as "a secure web site on the target computer."

secure web computer

VirnetX proposes "a computer that requires authorization for access and that can communicate in a virtual private network." Defendants propose that the term is indefinite or, alternatively propose "the target computer that hosts the secure web site."

Defendants initially argue that "secure web site" is indefinite for lack of a proper antecedent basis. Claim 10 of the '135 Patent is representative and states:

> A system that transparently creates a virtual private network (VPN) between a client computer and *a secure target computer*, comprising:
>
> [1] a DNS proxy server that receives a request from the client computer to look up an IP address for a domain name, . . . wherein the DNS proxy server generates a request to create the VPN between the client computer and *the secure target computer* if it is determined that access to *a secure web site* has been requested; and
>
> [2] a gatekeeper computer that allocates resources for the VPN between the client computer and *the secure web computer* in response to the request by the DNS proxy server.

'135 Patent col. 48:3–19 (emphases added). The preamble states that a VPN is created "between a client computer and a secure target computer." *Id.* col. 48:3–5. Element 1 of the system, the DNS proxy server, requests to create a VPN "between the client computer and the secure target computer [when] access to a secure web site has been requested." *Id.* col. 48:11–14. Element 2 of the system, the gatekeeper computer, "allocates resources for the VPN between the client computer and the secure web computer." *Id.* col. 48:16–18. Element 2 contains the only reference to "secure web computer."

VirnetX argues that the terms "secure target computer" and "secure web computer" are used interchangeably; thus, "secure target computer" provides the antecedent basis for "secure web computer." Defendants alternatively argue that the term must derive its antecedent basis from "secure target computer" if the term is not found indefinite. The Court finds that the term is not indefinite and derives its antecedent basis from "secure target computer." Reading the claim as a whole, it is clear that "secure web computer" refers to the "secure target computer" discussed earlier in the claim.

As with "web site" and "secure web site," VirnetX's proposal ignores the presence of "web" in the term and its link to the World Wide Web. Claim 10 details a system that may create a VPN between two computers in response to a request for access to a web site. If the request is for a non-secure website, the "DNS proxy server returns the IP address for the requested domain name." *Id.* col. 48:6–11. If the request is for a secure website, the "DNS proxy server generates a request to create the VPN between the client computer and the secure target computer." *Id.* col. 48:12–15. Further, in the event that a VPN is created, the claimed system includes "a gatekeeper computer that allocates resources for the VPN between the client computer and the secure web computer." *Id.* col. 48:16–19. Thus, the claims establish that the secure web computer is a target computer for the VPN connection and is able to respond to a request for access to a secure web site. Accordingly, the Court construes "secure web computer" as "the target computer that hosts the secure web site."

secure server

VirnetX proposes "a server that requires authorization for access and that can communicate in an encrypted channel." Defendants propose "a server that requires authorization for access and communicates in a VPN." The dispute concerns whether the secure server can communicate in an encrypted channel or communicates in a VPN.

Defendants argue that, in the context of the patents-in-suit, the modifier "secure" means that the modified term (i.e., sever or website) operates or communicates on a VPN. VirnetX contends that "secure" must be read in context and that the claim language itself provides the appropriate context for the term "secure server." Only claims of the '151 Patent contain the term. Claim 1 covers "[a] data processing device, comprising memory storing a domain name server (DNS) proxy module that intercepts DNS requests sent by a client and . . . when the intercepted DNS request corresponds to a secure server, *automatically initiating an encrypted channel between the client and the secure server*." '151 Patent col. 46:55–67 (emphasis added). Claim 2, which depends from claim 1, also recites the following method step: "when the client is authorized to access the secure server, sending a request to the secure server *to establish an encrypted channel between the secure server and the client*." *Id.* col. 47:5–8 (emphasis added). Both claims envision creating an encrypted channel between the secure server and requesting client.

Defendants' proposal that a secure server "communicates in a VPN" is too limiting for two reasons. First, the claims only require the creation of an encrypted channel, not a VPN. Second, requiring that a secure server actively "communicates" is not supported by the claim language. On the other hand, VirnetX's proposal recognizes the *possibility* of communication over an encrypted channel, which is supported by the language of the claims. Accordingly, the Court construes "secure server" as "a server that requires authorization for access and that can communicate in an encrypted channel."

target computer

VirnetX argues that no construction is necessary, but alternatively proposes "a computer with which the client computer seeks to communicate." Defendants propose "the ultimate destination with which the client computer seeks to communicate." The parties essentially agree

that a target computer is one "with which the client computer seeks to communicate." The dispute pertains to whether target computer needs further limitation.

In general, the claims cover communications among various entities in determining whether a VPN or link should be established. If it is determined that a VPN or link should be established, the claims cover methods of initiating such VPN or link. The term "target computer" is used within this general context. Claim 1 of the '135 Patent captures the essence of this term: "A method of transparently creating a virtual private network (VPN) between a client computer and a target computer, comprising . . . ." '135 Patent col. 47:20–22. Claim 2, which depends from claim 1, covers the use of a DNS server separate from the client computer. *See id.* col. 47:33–35. Claim 8 envisions the use of a DNS proxy server to pass through requests made for non-secure websites. *See id.* col. 47:60–64. Claim 7, which depends from claim 1, adds the "step of using a gatekeeper computer that allocates VPN resources for communicating between the client computer and the target computer." *Id.* col. 47:56–59.

Defendants argue that "target computer" should be limited to the "ultimate destination" of the client computer's intended communication. Defendants contend that omitting this clarification would permit a claim interpretation where the DNS proxy server or gateway computer (referenced in claims 7 and 8) were target computers. VirnetX argues that "nothing in the claim language precludes a communication from going beyond a target computer." Docket No. 192, at 9. VirnetX further argues that establishing a VPN between a client computer and a target computer on a private network would possibly allow the client to communicate with multiple computers on that private network.

One of skill in the art, reading the claims as a whole, would not confuse target computer with the DNS proxy server or gatekeeper computer, as Defendants suggest. Claim 1 clearly

indicates that it covers a method for establishing a VPN between a client computer and target computer. The claims and specification discuss the DNS proxy server and gatekeeper server as facilitating that process. Further, the claims do not limit the client computer's communication once a VPN has been established. Thus, Defendants' proposed "ultimate destination" limitation is inappropriate. The Court finds that "target computer" does not require construction.

between [A] and [B]

VirnetX argues that no construction is necessary, and Defendants propose "extending from [A] to [B]." The term "between [A] and [B]" is used in various claims of the patents-in-suit, where A and B refer to computers or locations. The parties do not dispute that all of the "between" phrases should be construed in the same manner. Claim 1 of the '135 Patent provides a representative example of the phrase's use: "A method of transparently creating a virtual private network (VPN) between [A] a client computer and [B] a target computer, comprising . . . ." '135 Patent col. 47:20–22. The following arguments and analysis are presented in light of this representative claim.

Defendants argue that the between phrase requires the VPN to extend from the client computer to the target computer. VirnetX contends that the VPN must only extend along public communication paths because private communication paths are inherently secure. The specification does not reveal or suggest the embodiment hypothesized by VirnetX. One of ordinary skill in the art, in light of the specification and claims, would understand creating a VPN between a client computer and target computer as creating a VPN that extends from the client computer to the target computer. Accordingly, the Court construes "between [A] and [B]" as "extending from [A] to [B]."

generating from the client computer a Domain Name Service (DNS) request

VirnetX contends that no construction is necessary. Defendants propose "creating and transmitting from the client computer a DNS request." At the *Markman* hearing, the parties agreed to the following construction for this term: "generating and transmitting from the client computer a DNS request."

an indication that the domain name service system supports establishing a secure communication link

VirnetX argues that this term does not require construction. Defendants propose "a visible message or signal that informs the user that the domain name service system supports establishing a secure communication link."

Defendants argue that the "indication" must be visible to the user, noting that the preferred embodiments disclose user-visible indications. *See, e.g.*, '504 Patent Figs. 33 & 34 (containing a "Go Secure" hyperlink). VirnetX argues that limitations present in the preferred embodiments should not be imported into the claims.

The specification of the '504 Patent states:

> Preferably, a user enables a secure communication link using a single click of a mouse, or a corresponding minimal input from another input device such as a keystroke entered on a keyboard or a click entered through a trackball. Alternatively, the secure link is automatically established as a default setting at boot-up of the computer (i.e., no click).

Id. col. 49:6–12. Thus, the specification envisions alternative methods of activating a secure communication link other than clicking a hyperlink, which is necessarily visible. An audible message could be provided to the user indicating that the system supports establishing a secure communication link, and a simple key press may be used to activate such a secure communication link. Neither the specification nor the claim language provides a basis for

limiting "indicating" to a visual indicator. The Court finds that this term is readily understandable and does not require construction.

indicate/indicating . . . whether the domain name service system supports establishing a secure communication link

VirnetX argues that this term does not require construction. Defendants propose "display/displaying a visible message or signal that informs the user whether the domain name service system supports establishing a secure communication link." The issue and arguments regarding this term are identical to those raised for the previous term. For the same reasons stated regarding the previous term, the Court finds that this term does not require construction.

enabling a/the secure communication mode of communication

VirnetX argues that this term does not require construction. Defendants propose "using an input device to select a secure communication mode of communication."

Defendants argue that the specification teaches that a secure communication mode of communication is enabled by using an input device such as a mouse or keyboard. *See* '759 Patent col. 6:44–51 (noting that a secure communication mode of communication is preferably enabled by selecting an icon or entering a command). However, the specification also envisions establishing a secure link "as a default setting at boot-up of the computer (i.e., no click)." *Id.* col. 50:28–29. Thus, Defendants' proposal is overly limiting because it requires a user to activate the secure mode of communication. Further, as noted in *Microsoft*, the Court finds that this term is readily understandable to a jury. *See Microsoft*, 2009 U.S. Dist. LEXIS 65667, at *45. Accordingly, the Court finds that this term does not require construction.

cryptographic information

VirnetX proposes "information that is used to encrypt data or information that is used to decrypt data." Defendants propose "information that is required in order to encode/decode or

encrypt to ensure secrecy." Both parties agree that cryptographic information concerns information used to perform encryption or decryption as opposed to the underlying data that is encrypted or decrypted.

VirnetX argues that Defendants' proposal is ambiguous for the following two reasons. First, it seems to require the inclusion of all information necessary for encryption, opening a debate about what information is necessary. Second, the phrase "to ensure secrecy" invites an additional dispute about the strength of the encryption enabled by the cryptographic information. Defendants respond that their construction closely tracks that issued by this Court in *Microsoft*.[5] Defendants assert that the phrase "to ensure secrecy" was used in *Microsoft* to clarify the type of encryption at issue (security as opposed to compression) and should likewise be used here for the same reasons.

Claim 1 of the '759 Patent includes the following step: "enabling a secure communication mode of communication at the first computer without a user entering any cryptographic information *for establishing the secure communication mode of communication*." '759 Patent col. 57:10–16 (emphasis added). The claim language itself establishes the purpose of the cryptographic information; thus, the "to ensure secrecy" clarification is not necessary. Also, the claim covers a method that does not require the user to enter any cryptographic information. Further, the parties acknowledge that there are different types of cryptographic information (i.e., username, password, encryption key, etc.). Whether some or all of that information is required for encryption or decryption is application specific. What is important to the claims of the '759 Patent is whether any such information is required by the user "for establishing the secure

[5] In *Microsoft*, the Court construed the term as "information that is encoded/decoded or encrypted to ensure secrecy." *Microsoft*, 2009 U.S. Dist. LEXIS 65667, at *46.

communication mode of communication." Thus, the arguments about how much cryptographic information must be used are irrelevant.

The Court construes "cryptographic information" as "information that is used to encrypt data or information that is used to decrypt data."

CONCLUSION

For the foregoing reasons, the Court interprets the claim language in this case in the manner set forth above. Further, VirnetX Inc.'s Motion to Compel from Apple a Complete Response to VirnetX's Eighth Common Interrogatory (Docket No. 179) is **DENIED AS MOOT**. For ease of reference, the Court's claim interpretations are set forth in a table in Appendix A.

So ORDERED and SIGNED this 25th day of April, 2012.

LEONARD DAVIS
UNITED STATES DISTRICT JUDGE

APPENDIX A

Claim Term	Court's Construction
virtual private network	a network of computers which privately and directly communicate with each other by encrypting traffic on insecure paths between the computers where the communication is both secure and anonymous
virtual private link	a virtual private network as previously defined
secure communication link	a direct communication link that provides data security
domain name service	a lookup service that returns an IP address for a requested domain name to the requester
domain name	a name corresponding to an IP address
DNS proxy server	a computer or program that responds to a domain name inquiry in place of a DNS
secure domain name service	a non-standard 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
domain name service system	No construction necessary
web site	one or more related web pages at a location on the World Wide Web
secure web site	a web site that requires authorization for access and that can communicate in a VPN
secure target web site	a secure web site on the target computer
secure web computer	the target computer that hosts the secure web site
secure server	a server that requires authorization for access and that can communicate in an encrypted channel
target computer	No construction necessary
between [A] and [B]	extending from [A] to [B]
generating from the client computer a Domain Name Service (DNS) request	generating and transmitting from the client computer a DNS request
an indication that the domain name service system supports establishing a secure communication link	No construction necessary
indicate/indicating . . . whether the domain name service system supports establishing a secure communication link	No construction necessary
enabling a/the secure communication mode of communication	No construction necessary
cryptographic information	information that is used to encrypt data or information that is used to decrypt data