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

VIRNETX, INC.,	§	
	§	
Plaintiff,	§	
	§	
vs.	§	**Civil Action No. 6:10-cv-417**
	§	
CISCO SYSTEMS, INC., et al.	§	
	§	**JURY TRIAL DEMANDED**
Defendants.	§	
	§	

VIRNETX'S REPLY CLAIM CONSTRUCTION BRIEF

I. ARGUMENT IN REPLY

1. *"virtual private network"*

"Anonymous." With respect to the Defendants' proposed "anonymity" construction, the issue is whether the Court was correct in requiring all claims to achieve both data security and anonymity based on the discussion in the Background of the Invention. Even though VirnetX squarely raised this issue in its Opening Brief, the Defendants avoided the issue. There is no reason—and the Defendants have offered none—that all claims must achieve anonymity. *Cf. PSN Ill., LLC v. Ivoclar Vivadent, Inc.*, 525 F.3d 1159, 1166 (Fed. Cir. 2008) ("[C]ourts must recognize that disclosed embodiments may be within the scope of other allowed but unasserted claims."). Moreover, VirnetX explained in its Opening Brief how it is just the unasserted "IP address hopping" dependent claims—as opposed to all claims—that achieve the anonymity discussed in the Background of the Invention.[1]

"Directly." VirnetX did not overcome Aventail by disclaiming the type of VPN taught by Aventail; rather, VirnetX demonstrated that Aventail did not teach a VPN at all. The Defendants assert that "[t]his is a difference without a distinction." They are wrong in this assertion. The very inquiry of prosecution disclaimer is whether the ordinary scope of a term was disclaimed. *See Omega Eng'g, Inc. v. Raytek Corp.*, 334 F.3d 1314, 1324 (Fed. Cir. 2003) ("[W]here the patentee has unequivocally disavowed a certain meaning to obtain his patent, the doctrine of prosecution disclaimer attaches and narrows the ordinary meaning of the claim congruent with the scope of the surrender.") (emphasis added). And the Defendants have failed to establish that VirnetX's three arguments over Aventail departed from the ordinary meaning of VPN.

[1] Instead of addressing why the Background of the Invention discussion should limit all claims, the Defendants attempt to justify their construction by pointing out that VirnetX proved Microsoft's infringement under the Court's Markman Order in that case, which required anonymity. This argument completely misses the point. VirnetX preserved error for this construction, and VirnetX is specifically seeking reconsideration of this issue in this case.

Moreover, the Defendants failed to establish a "clear and unmistakable" disclaimer.[2] The Defendants assert—without any justification, analysis, or argument—that the three arguments that VirnetX made over the Aventail reference are "independent" of each other and therefore disclaim scope of the claim term. *See* Res. at 6-7. The Defendants are demonstrably wrong in this assertion. In re-examination, VirnetX explained the meaning of its third argument:

> Third, Aventail has not been shown to disclose a VPN because computers connected according to Aventail do not communicate directly with each other. Aventail discloses a system where a client on a public network transmits data to a SOCKS server via a singular, point-to-point SOCKS connection at the socket layer of the network architecture. The SOCKS server then relays that data to a target computer on a private network on which the SOCKS server also resides. All communications between the client and target stop and start at the intermediate SOCKS server. The client cannot open a connection with the target itself. Therefore, one skilled in the art would not have considered the client and target to be virtually on the same private network.

See Ex. B. at 14 (internal citations removed). In other words, because Aventail does not virtualize the physically direct communications of a private network,[3] one skilled in the art would not have considered computers in the Aventail system to be virtually on the same private

[2] Contrary to the Defendants' straw man attack, VirnetX never suggested that there cannot be unambiguous waiver anytime a patentee makes multiple distinctions over prior art. In its Opening Brief, VirnetX correctly cited the "clear and unmistakable" test for finding prosecution history estoppel and discussed the Federal Circuit's opinion in *Momentus Golf* to illustrate how, in cases involving multiple distinctions in the prosecution history, courts must be careful in determining whether a particular, isolated distinction rises to the level of clear and unmistakable disclaimer. *See* Opening Brief at 7-8.

[3] This also highlights the reason that VirnetX opposes the Defendants' construction. If the Court adopts this construction, then the Defendants will undoubtedly argue that "directly" requires computers in a VPN to be physically directly connected. But this is not what VirnetX argued in re-examination. Rather, VirnetX used the word "directly" to explain how a VPN virtualizes a direct connection between computers on a physical network. *See* Ex. B. at 14 ("Third, Aventail has not been shown to disclose a VPN because computers connected according to Aventail do not communicate directly with each other. . . . **Therefore, one skilled in the art would not have considered the client and target to be virtually on the same private network**.") (emphasis added). (Note that, in this brief, references to exhibits and Dr. Jones's declaration refer to the exhibits and declarations attached to VirnetX's Opening Brief.)

network. In this way, VirnetX's third argument over Aventail in re-examination is a corollary of its first argument over Aventail—that "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**." *See* Ex. B. at 12 (emphasis added). And because VirnetX's third argument over Aventail is a corollary of its first, it would be improper to impose the third argument onto the claims with no regard to the first.[4] For these reasons, the Defendants' proposed construction should be rejected.

2. *"virtual private link"*

The parties' respective constructions are very similar, but the Defendants' proposed construction requires the link to be a link in a network whereas VirnetX's proposed construction simply requires a link. The Defendants have cited no evidence that this is the ordinary meaning of "link," and there is no limiting language in the claims, written description, or prosecution history that would require the link to be in a network. Consequently, the Defendants' proposed construction includes an extraneous limitation and should be rejected. *See Phillips v. AWH Corp.*, 415 F.3d 1303, 1316–17 (Fed. Cir. 2005).

3. *"secure communication link"*

The Detailed Description of the Invention teaches a "One-click Secure" preferred embodiment. This preferred embodiment, which spans over four columns, teaches how a secure communication link can be augmented to create a virtual private network communication link. *See* '504::49:1-53:9. VirnetX discussed this preferred embodiment at length in its Opening Brief

[4] Moreover, VirnetX's proposed construction for this term would require computers in a VPN to be able to communicate as if they were on the same private network. *See* Opening Brief at 5-6 (explaining how "privately" in the Court's construction should refer to the ability of computers to communicate as though they were on the same private network and should not refer to anonymity). Under this construction, it would be redundant to exclude from the scope of VPN communications that do not virtualize the physically direct communications of a private network.

to demonstrate that a secure communication link is not always a virtual private network communication link. *See* Opening Brief at 11-12. In their response, the Defendants quote a few lines that describe how the secure communication link in this particular embodiment is also a virtual private network communication link, but the 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. This violates one of the most fundamental principles of claim construction. "[A]lthough the specification often describes very specific embodiments of the invention, [the Federal Circuit has] repeatedly warned against confining the claims to those embodiments." *Phillips*, 415 F.3d at 1323.

As VirnetX discussed in its Opening Brief, this preferred embodiment teaches how software module 3309 augments the secure communication link to create a virtual private network communication link. *See* '504::50:25-27 ("At step 3407, a secure VPN communications mode of operation has been enabled and **software module 3309 begins to establish a VPN communication link.**") (emphasis added); *see also* '504::50:40-52 (describing how the software module 3309 enables computer 3301 to communicate in the private network 3311 as though it were physically in that network). The Court should not follow the Defendants' misunderstanding of the preferred embodiment and should not restrict this term to the special case presented in the preferred embodiment.[5] For the foregoing reasons, the Court should reject the Defendants' proposed construction and adopt VirnetX's proposed construction.

[5] The Defendants also argue that VirnetX "conceded" that a secure communication link is a virtual private network communication link in the *Microsoft* litigation. Not so. The only patent in that case that contained the term "secure communication link" was the '759 patent. And as the Court recognized in its *Markman* order, the claims of '759 patent defined and limited the secure communication link to a virtual private network communication link. *See* Ex. A at 25.

4. *"domain name service"*

The Defendants seem to have a truncated view of the role of "ordinary meaning" in claim construction. The standard for determining the legally operative scope of a claim term is not simply looking to a term's "ordinary meaning" irrespective of the patent. Rather, "the 'ordinary meaning' of a claim term is its meaning to the ordinary artisan ***after reading the entire patent***." *Phillips*, 415 F.3d at 1321 (emphasis added). As such, the Defendants' argument as to how a "conventional" DNS operates misses the point. The patents explicitly teach "a specialized DNS server" that "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" if secure communications are requested. *See* '135::37:63-38:2. As such, the Defendants' proposed construction should be rejected.

5. *"domain name"*

The Defendants' argument completely misses the point. For claim construction purposes, it is irrelevant that the most typical syntax of domain names is the hierarchical syntax of domain names on the Internet. Nor does it matter that the specification gives examples of hierarchical domain names. *See* Ex. A (the Court's Claim Construction Opinion from the *Microsoft* litigation) at 14. ("The specification's disclosure or omission of examples does not create limitations on claims.") Rather, "the 'ordinary meaning' of a claim term is its meaning to the ordinary artisan after reading the entire patent." *Phillips*, 415 F.3d at 1321. As Dr. Jones explained in his declaration, a skilled artisan would not have imported the hierarchical syntax of the typical domain name after reading the patents. Specifically, Dr. Jones explained that one skilled in the art would understand that the reason that domain names on the Internet have a hierarchical syntax is because that syntax enables a distributed approach to managing the naming of a huge number of computers around the world. *See* Jones Decl. at ¶ 10. But as far as the patents are

concerned, formatting domain names in this way would be unnecessary. Specifically, because the DNS proxy server taught in the patents is not expected to provide answers for every domain name on the Internet, a skilled artisan would understand that it is not necessary for domain names to have a hierarchical syntax to practice the patents. *See id*. As such, the Court should reject the Defendants' proposed construction.

6. *"DNS proxy server"*

In their Response, the Defendants do not present any argument for this term that VirnetX did not already preemptively address in its Opening Brief. As explained in VirnetX's Opening Brief and in Dr. Jones's declaration, the discussion of DNS proxy servers in the Background of the Invention of the patents refers to a specific use of proxy servers to attempt to achieve anonymity. *See* Opening Brief at 16-17; Jones Decl. at ¶¶ 13-16. The Defendants respond by asserting: "The statement is ***not*** so limited—it describes what a 'proxy server' is, regardless of the system in which it is used." *See* Res. at 18 (emphasis in original). The Defendants support this assertion with only their *ipse dixit*—the Defendants offered no counterargument and their own expert was conspicuously silent on this point. As such, the Court should reject the Defendants' proposed construction for the reasons given in VirnetX's Opening Brief.

7. *"secure domain name service"*

"Non-Standard." The Defendants misinterpret the prosecution history in their brief. A secure domain name service can resolve addresses for a secure domain name because: (i) it can recognize that a query message is requesting a secure computer address and (ii) it can return a secure computer network address for a requested secure domain name—not because the lookup service is "non-standard." The Court should not follow the Defendants' misreading of the prosecution history and should reject their proposed construction.

"Performs Its Services Accordingly." VirnetX opposes this aspect of the Defendants' construction because "returning a secure network address for a requested secure domain name" is the service that is performed. As such, this language is superfluous at best, ambiguous at worst, and should be rejected.

8. *"domain name service system"*

The Defendants assume, without any intrinsic support, that the word "system" must connote an "extra something." *See* Res. at 16-17. But as detailed below, the Defendants present no cognizable legal basis for the unnecessary limitations added into their proposed construction.

"Differentiating." The Defendants discuss how the specification teaches—in a preferred embodiment—a DNS that is capable of differentiating between standard and secure top-level domain names. But because the Defendants can point to no "words or expressions of manifest exclusion or restriction" that limit the invention to this embodiment, this discussion is meaningless. *See E-Pass Techs.*, 343 F.3d at 1369.

"Secure Top-Level." The Defendants argue that the description of the invention in the Summary of the Invention limits all claims of the patent. This summary, however, refers to certain dependent claims and should not be applied against all claims. *Cf. PSN Ill.*, 525 F.3d at 1166 ("[C]ourts must recognize that disclosed embodiments may be within the scope of other allowed but unasserted claims."). Because the Defendants have offered no legitimate support for their construction,[6] it should be rejected.

9. *"web site" / "secure web site" / "secure target web site"*

During the re-examination of the '135 patent, the examiner made a record of his application of these claims terms to the alleged prior art. In doing so, the examiner made no

[6] The Defendants also argued that certain passages from the prosecution history somehow support their proposed construction. For the sake of completeness, VirnetX notes that these cited passages do not even mention "differentiating" or "secure top-level domain names."

mention of the "web page" and "World Wide Web" requirements in the Court's prior constructions. The Defendants attempt to dismiss this evidence by citing a case that stands for the position that the Court is not bound by an examiner's evaluation of prior art. *See* Res. at 26, n.17. The argument misses the point. VirnetX is not arguing that the Court should be bound by the examiner's conclusions regarding patentability; rather, VirnetX is asking the Court to recognize that the examiner's application of these claims is objective evidence of how one of ordinary skill reads, interprets, and applies these claims in light of the specification.

10. *"secure web computer"*

The Defendants argue that one of ordinary skill would parse this term into "secure web" and "computer" and then concatenate "secure web" with "site." The Defendants, however, offer no evidence that would support this assertion—not even from their own expert. In any event, the correct inquiry is how a skilled artisan would understand the ordinary meaning of a claim term—not how a skilled artisan would rewrite it. As such, the Court should reject the Defendants' proposed construction for this term.

11. *"secure server"*

This claim term appears only in the '151 patent, which concerns encrypted channels as opposed to VPNs. The Defendants have offered no cognizable legal basis for overriding the language of the claims and forcing the claimed encrypted channels to further be VPNs. Moreover, the Defendants ignore that the meaning of "secure" depends on its context. As this Court has recognized, when "secure" modifies computers and servers, it refers to "authorization for access" of those computers/servers. *See* Ex. A. at 18. Conversely, when "secure" modifies a type of communication, it refers to encryption. *See, e.g.*, '135::1:38-39 ("Data security is usually

tackled using some form of data encryption.").[7] Because the Defendants have conflated these meanings, the Court should reject the Defendants' proposed construction.

12. *"target computer"*

There is nothing in the claim language that precludes a communication from going beyond a target computer. In fact, when a client computer forms a VPN with a target computer, the client computer might communicate with multiple computers on the private network virtually as if it were in that private network. *See* Jones Decl. at ¶ 19. Further, the preferred embodiments that the Defendants discuss do not support their construction. Indeed, the lynchpin of the Defendants' argument ("But only the ultimate destination with which the client computer seeks to communicate is the target computer." Res. at 24) lacks citation to any evidence and is nothing more than attorney argument. Moreover, even if the Defendants' characterizations of the preferred embodiments were accurate (which they are not), the Defendants would still need to show "words or expressions of manifest exclusion or restriction" to support their narrowing construction (which they have not). *See E-Pass Techs.*, 343 F.3d at 1369.

13. *"an indication 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"*

The Defendants argue that "visible" should be imported from the preferred embodiments because all of preferred embodiments allegedly have this characteristic. *See* Response at 19 ("***All*** of these examples have one thing in common – they are user-visible.") (emphasis in original). But as this Court has recognized, "The specification's disclosure or omission of examples does not create limitations on claims." *See* Ex. A at 14.

[7] The Defendants also argue that "secure" also requires anonymity, but that is beside the point, which is that the Defendants have conflated "secure" as used in a computer/server context and "secure" as used in a communication context.

14. *"between [A] and [B]"*

The Defendants argue that their proposed construction is necessary because, if a secure communication did not extend from one endpoint to the other, "the entire security objective of the patents would be undermined because there would be unprotected gaps along the way." *See* Response at 22. But if this reasoning were truly airtight, then the Defendants would not need their construction. Indeed, the Defendants are wrong in their reasoning. Security—i.e., encryption—is only necessary for public communication paths for the security objective of the patents to be met because security can be inherently present on private portions of the path.[8]

15. *"enabling a secure communication mode of communication"*

The Defendants offer only non-limiting examples to support their construction. But as this Court has recognized, "The specification's disclosure or omission of examples does not create limitations on claims." *See* Ex. A at 14.

16. *"generating from the client computer a Domain Name Service (DNS) request"*

The Defendants employ faulty logic to support their construction. Namely, the Defendants argue that, since the DNS request must be transmitted, it follows that: (i) generating means creating and transmitting; and (ii) the creating and transmitting must occur at the client computer. But logic does not dictate this result. Method claims can have unclaimed steps. "Use of the open-ended transition 'which comprises' indicates that there may be additional unclaimed steps in the method." *Wasinger v. Levi Strauss & Co.*, 106 Fed. Appx. 34, 36 (Fed. Cir. 2004).

17. *"cryptographic information"*

The Defendants did not meaningfully address VirnetX's concerns of ambiguity.

[8] The Defendants assert that Dr. Jones claim construction declaration in the *Microsoft* case supports their construction. Not so. In that declaration, the example Dr. Jones gave was just that—an example. Further, Dr. Jones stated that the VPN "is the entire path between the laptop computer and the server." *See* Dkt. No. 182-20 at ¶ 33. Dr. Jones did not argue that the VPN extended beyond the server, which is what the Defendants' construction would require, as that communication path is private and therefore physically secure. *See* id.

DATED: December 19, 2011

Respectfully submitted,

McKOOL SMITH, P.C.
/s/ *Douglas A. Cawley*
Douglas A. Cawley, *Lead Attorney*
Texas State Bar No. 04035500
E-mail: dcawley@mckoolsmith.com
Bradley W. Caldwell
Texas State Bar No. 24040630
E-mail: bcaldwell@mckoolsmith.com
Luke F. McLeroy
Texas State Bar No. 24041455
E-mail: lmcleroy@mckoolsmith.com
Jason D. Cassady
Texas State Bar No. 24045625
E-mail: jcassady@mckoolsmith.com
John Austin Curry
Texas State Bar No. 24059636
E-mail: acurry@mckoolsmith.com
Daniel R. Pearson
Texas State Bar No. 24070398
E-mail: dpearson@mckoolsmith.com
Stacie Lynn Greskowiak
Texas State Bar No. 24074311
E-mail: sgreskowiak@mckoolsmith.com
McKool Smith P.C.
300 Crescent Court, Suite 1500
Dallas, Texas 75201
Telephone: (214) 978-4000
Telecopier: (214) 978-4044

Sam F. Baxter
Texas State Bar No. 01938000
E-mail: sbaxter@mckoolsmith.com
McKOOL SMITH P.C.
104 East Houston, Suite 300
Marshall, Texas 75670
Telephone: (903) 923-9000
Telecopier: (903) 923-9099

Robert M. Parker
Texas State Bar No. 15498000
E-mail: rmparker@pbatyler.com
Robert Christopher Bunt
Texas State Bar No. 00787165
E-mail: rcbunt@pbatyler.com
PARKER, BUNT & AINSWORTH, P.C.
100 East Ferguson, Suite 1114
Tyler, Texas 75702
Telephone: (903) 531-3535
Telecopier: (903) 533-9687

ATTORNEYS FOR PLAINTIFF VIRNETX, INC.

CERTIFICATE OF SERVICE

The undersigned certifies that, on December 19, 2011, the foregoing document was served via the Court's ECF system on all counsel who has filed notices of appearance in this case.

/s/ Austin Curry
John Austin Curry

McKool 405485v1