NO:

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

_____

BEFORE THE PATENT TRIAL AND APPEAL BOARD

_____

THE MANGROVE PARTNERS MASTER FUND, LTD.
Petitioner,

v.

VIRNETX INC.,
Patent Owner.

_____

Case IPR2015-_____
Patent U.S. 6,502,135

_____

PETITION FOR INTER PARTES REVIEW OF UNITED STATES PATENT NO. 6,502,135 PURSUANT TO 35 U.S.C. §§ 311-319, 37 C.F.R. § 42

Mail Stop Patent Board
Patent Trial and Appeal Board
U.S. Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450

TABLE OF CONTENTS

EXHIBITS

Ex. 1001	U.S. Patent No. 6,502,135 to Munger et al. (the "'135 Patent")
Ex. 1002	Takahiro Kiuchi and Shigekoto Kaihara, "C-HTTP - The Development of a Secure, Closed HTTP-based Network on the Internet," published by IEEE in the Proceedings of SNDSS 1996 ("Kiuchi")
Ex. 1003	Declaration of Dr. Roch Guerin
Ex. 1004	(Reserved)
Ex. 1005	Mockapetris, P., RFC 1034, "Domain Names–Concepts and Facilities," Nov. 1997
Ex. 1006	(Reserved)
Ex. 1007	Patent Owner's Preliminary Response, Paper 7, in IPR2014-00610
Ex. 1008	Excerpts from Webster's Third New International Dictionary (1971)
Ex. 1009	VirnetX's Reply Claim Construction Brief in *VirnetX Inc. v. Cisco Systems, Inc. et al*., 6:10-cv-417 (Dec. 19, 2011) (E.D. Tex.)
Ex. 1010	Bradner, S., RFC 2026, "The Internet Standards Process – Revision 3," Oct. 1996
Ex. 1011	Decision to Institute *Inter Partes* Review, Paper 9, in IPR2014-00610 (Oct. 15, 2014)
Ex. 1012	(Reserved)
Ex. 1013	(Reserved)
Ex. 1014	Berners-Lee et al., RFC 1945, "Hypertext Transfer Protocol -- HTTP/1.0," May 1996
Ex. 1015	Patent Owner's Preliminary Response, Paper 10, in IPR2013-00348
Ex. 1016	Eastlake, D., RFC 2535, "Domain Name System Security Extensions," Mar. 1999
Ex. 1017	Patent Owner's Comments in Response to Examiner's Determination in *Inter Partes* Reexamination 95/001,792 (March, 11, 2015)
Ex. 1018	VirnetX's Opening Claim Construction Brief in *VirnetX Inc. v. Cisco Systems, Inc. et al*., 6:10-cv-417 (Dec. 19, 2011) (E.D. Tex.)
Ex. 1019	Memorandum Opinion and Order in *VirnetX Inc. v. Cisco Systems, Inc. et al*., 6:10-cv-417 (April 25, 2012) (E.D. Tex.)
Ex. 1020	Petition for *Inter Partes* Review in IPR2013-00349
Ex. 1021	Patent Owner's Preliminary Response, Paper 11, in IPR2014-00558

Ex. 1022	Decision to Institute *Inter Partes* Review, Paper 15, in IPR2014-00237
Ex. 1023	"Glossary for the Linux FreeS/WAN project," (Feb. 21, 2002)
Ex. 1024	(Reserved)
Ex. 1025	Declaration of Dr. Roch Guerin in IPR2014-00401

The Mangrove Partners Master Fund, Ltd. ("Petitioner" or "Mangrove") petitions for Inter Partes Review ("IPR") under 35 U.S.C. §§ 311–319 and 37 C.F.R. § 42 of claims 1, 3, 4, 7, 8, 10, and 12 ("the Challenged Claims") of U.S. Patent No. 6,502,135 ("the '135 Patent"). As explained in this petition, there exists a reasonable likelihood that Mangrove will prevail with respect to at least one of the Challenged Claims.

The Challenged Claims are unpatentable based on teachings set forth in at least the references presented in this petition. Mangrove respectfully submits that an IPR should be instituted, and that the Challenged Claims should be canceled as unpatentable.

I. MANDATORY NOTICES UNDER 37 C.F.R § 42.8(A)(1)

A. REAL PARTY-IN-INTEREST UNDER 37 C.F.R. § 42.8(B)(1)

Petitioner, The Mangrove Partners Master Fund, Ltd., is the real party-in-interest.

B. RELATED MATTERS UNDER 37 C.F.R. § 42.8(B)(2)

The '135 Patent is the subject of a number of civil actions including: (i) Civ. Act. No. 6:13-cv-00211-LED (E.D. Tex.), filed February 26, 2013; (ii) Civ. Act. No. 6:12-cv-00855-LED (E.D. Tex.), filed November 6, 2012; and (iii) Civ. Act. No. 6:10-cv-00417-LED (E.D. Tex.), filed August 11, 2010.

The '135 Patent was the subject of petitions for *inter partes* review filed by RPX Corporation (IPR2014-00171 and IPR2014-00172), Apple, Inc. (IPR2013-

00348 and IPR2013-00349), and a petition filed by Microsoft (IPR2014-00558), which were each found untimely by the PTAB and not instituted. Additionally, the '135 Patent was the subject of a petition for *inter partes* review filed by New Bay Capital, LLC (IPR2013-00375), which was abandoned by petitioner prior to a decision to institute. The '135 Patent is also the subject of *inter partes* reexamination nos. 95/001,679 and 95/001,682. In the formerly merged proceedings, the Office issued a Non-Final Action rejecting all 18 claims of the '135 Patent, including rejections based on, *inter alia*, Kiuchi (Ex. 1002), which is one of the prior art references presented herein.[1] The '135 Patent also was subject to reexamination no. 95/001,269, which concluded on June 7, 2011 – after the petitioner in that proceeding (Microsoft) ceased participating -- with an *inter partes* reexamination certificate confirming all of the claims subject to the reexamination and adding new claim 18.

C. LEAD AND BACK-UP COUNSEL UNDER 37 C.F.R. § 42.8(B)(3)

Mangrove provides the following designation of counsel.

.LEAD COUNSEL	BACKUP COUNSEL
Abraham Kasdan, Reg. No. 32,997	James T. Bailey, Reg. No. 44,518

[1] In subsequent Office Actions in the severed proceedings relating to 95/001,679 , the re-examination of claims 10-12 was terminated based on pre-AIA 35 U.S.C. 317(b), with the remaining rejections of claims 1-9 and 13-18 maintained.

Wiggin and Dana LLP 450 Lexington Avenue New York, NY 10017 T: 212-551-2841 Email: akasdan@wiggin.com	504 W. 136th St. #1B New York, NY 10031 T: 917-626-1356 Email: jtb@jtbaileylaw.com

D. Service Information

Please address all correspondence and service to counsel at the address provided in Section I(C). Mangrove also consents to electronic service by email at IP@wiggin.com.

II. PAYMENT OF FEES – 37 C.F.R. § 42.103

Mangrove authorizes the Patent and Trademark Office to charge Deposit Account No. 23-1665 for the fee set in 37 C.F.R. § 42.15(a) for this Petition and further authorizes payment for any additional fees to be charged to this Deposit Account.

III. REQUIREMENTS FOR IPR UNDER 37 C.F.R. § 42.104

A. GROUNDS FOR STANDING UNDER 37 C.F.R. § 42.104(A)

Mangrove certifies that the '135 Patent is eligible for IPR. Mangrove is not barred or estopped from requesting this review challenging the Challenged Claims on the below-identified grounds.

B. IDENTIFICATION OF CLAIMS BEING CHALLENGED (37 C.F.R. § 42.104(B))

Petitioner requests an IPR of the Challenged Claims on the grounds set forth in the table shown below, and requests that each of the Challenged Claims be

found unpatentable. An explanation of how these claims are unpatentable under the statutory grounds identified below is provided in the form of a detailed description that indicates where each element can be found in the cited prior art, and the relevance of that prior art. Additional explanation and support for each ground of rejection is set forth in Exhibit 1003, the Declaration of Dr. Roch Guerin ("Guerin Declaration"), referenced throughout this Petition.

Claims 1, 3, 4, 7, 8, 10, and 12 of the '135 Patent are unpatentable as being anticipated under 35 U.S.C. § 102 (b), and/or for being obvious over the prior art under 35 U.S.C. § 103. Specifically:

Ground	'135 Patent Claims	Basis for Rejection
Ground 1	1, 3, 4,7, 8, 10, and 12	Anticipated under § 102(b) by Takahiro Kiuchi and Shigekoto Kaihara, "C-HTTP - The Development of a Secure, Closed HTTP-based Network on the Internet," the Proceedings of SNDSS 1996 ("Kiuchi") (Ex. 1002)
Ground 2	8	Obvious under § 103 based upon Kiuchi (Ex. 1002) in view of RFC 1034 (Ex. 1005)

Kiuchi qualifies as prior art under 35 U.S.C § 102(b). Specifically, Kiuchi (Ex. 1002) is a printed publication that was presented at the 1996 Symposium on Network and Distributed Systems Security (SNDSS) on February 22 & 23, 1996, and published by IEEE in the Proceedings of SNDSS 1996.

RFC 1034 likewise qualifies as prior art under 35 U.S.C § 102(b). Specifically, RFC 1034 (Ex. 1005) was published in November 1987 by the Internet Engineering Task Force (IETF). RFC 1034 was publically distributed no later than November 1987. Ex. 1005.

Petitioner's proposed construction of the contested claims, the evidence relied upon, and the precise reasons why the claims are unpatentable are provided in §§ IV and V, below.

IV. SUMMARY OF THE '135 PATENT

A. BRIEF DESCRIPTION

The '135 Patent generally addresses secure communications over the Internet. As acknowledged in the '135 Patent, "[a] tremendous variety of methods have been proposed and implemented to provide security and anonymity for communications over the Internet." Ex. 1001 at 1:16-18. The majority of the '135 specification is dedicated to describing one particular way of providing secure and anonymous communications using an allegedly inventive protocol called the "Tunneled Agile Routing Protocol (TARP)." *See, e.g.*, *id*. at 2:65-5:64. The challenged claims of the '135 Patent, however, are not limited to TARP and instead all address one of five alleged "improvements" added by CIP application serial number 09/504,783 filed on February 15, 2000. *See id*. at 5:65-6:10.

The claims of the '135 Patent are directed to a system and method for

securely communicating over the Internet. *See* Ex. 1001 at 2:66. More specifically, the claims all address "a DNS proxy server that transparently creates a virtual private network in response to a domain name inquiry." *Id*. at 6:1-3.

Claim 1 of the '135 Patent is reproduced below:

> 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 that requests an IP address corresponding to a domain name associated with the target computer;
>
> (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 the target computer.

B. '135 PATENT CLAIM CONSTRUCTION UNDER 37 C.F.R. §§ 42.104(B)(3)

A claim subject to IPR is given its "broadest reasonable construction in light of the specification of the patent in which it appears." 37 C.F.R. § 42.100(b); *see also Patent Trial Practice Guide,* 77 Fed. Reg. 48,756, 48,766 (Aug. 14, 2012). Under the broadest reasonable standard, claim terms are given their ordinary and customary meaning as would be understood by one of ordinary skill in the art in the context of the entire disclosure. *In re Translogic Tech., Inc.*, 504 F.3d 1249,

1257 (Fed. Cir. 2007). Any special definition for a claim term must be set forth in the specification with reasonable clarity, deliberateness, and precision. *In re Paulsen*, 30 F.3d 1475, 1480 (Fed. Cir. 1994). In this regard, however, care must be taken not to read a particular embodiment appearing in the written description into the claim if the claim language is broader than the embodiment. *In re Van Geuns*, 988 F.2d 1181, 1184 (Fed. Cir. 1993).

Petitioner submits constructions for the following terms. All remaining terms should be given their plain meaning.

1. VIRTUAL PRIVATE NETWORK (VPN) (CLAIMS 1 AND 10)

Petitioner submits that the broadest reasonable interpretation of "virtual private network" or "VPN" should be broad enough to encompass "a secure network that includes portions of a public network."

Petitioner's proposed interpretation was previously adopted by the PTAB in IPR2014-00237 regarding related U.S. Patent No. 8,504,697. Ex. 1022, pp. 11-12 (Decision to Institute *Inter Partes* Review, Paper No. 15). This interpretation is consistent with both the specification and the common meaning of "VPN" for the reasons addressed therein. *Id*.

In prior IPR proceedings regarding the '135 Patent, Patent Owner has proposed an interpretation of "VPN" that differs in two main respects; namely, that it requires (i) encryption, and (ii) computers in the VPN to *directly* communicate

with each other. Ex.1015, p. 22. Both positions are inconsistent with the broadest reasonable interpretation of "VPN."

A VPN does not require encryption:

The '135 Patent does not explicitly define the term "VPN." *See* Ex. 1003, ¶ 17. However, the '135 Patent explains that one can provide data security using "IP hopping" schemes, rather than solely by using encryption. As it states, "Data security is *usually* tackled using some form of data encryption." Ex. 1001 at 1:38-39 (emphasis added). The '135 Patent also illustrates use of a quasi-random IP hopping scheme to implement a VPN. *See, e.g.*, *id.* at 23:10-14 ("In a second mode referred to as 'promiscuous per VPN' mode, a small set of fixed hardware addresses are used, with a fixed source/destination hardware address used for all nodes communicating over *a virtual private network*." (Emphasis added)).

Moreover, claims 6 and 11, which depend on independent claims 1 and 10 respectively, rely on this particular embodiment. For example, claim 6 specifies that step 3 of claim 1 "comprises the step of *establishing the VPN by creating an IP address hopping scheme* between the client computer and the target computer." *Id.* at 47:53-55 (emphasis added). Similarly, claim 11 requires that "the gateway computer *creates the VPN by establishing an IP address hopping regime* that is used to pseudorandomly change IP address in packets transmitted between the client computer and the secure target computer." *Id*. at 48:20-24 (emphasis

added); *see also id.* at 2:25-36 (explaining use of anonymity techniques). Accordingly, the specification envisions VPNs that do not require encryption.

To support its contention that a VPN requires encryption, Patent Owner has in prior proceedings pointed to the term "FreeS/WAN" in one passage of the '135 Patent. Ex. 1015, p. 23 (citing Ex. 1001 at 37:50-62). That passage, however, does not define *what* a VPN is, but simply explains that RFC 2535 (the "FreeS/WAN" protocol) can be used to implement *one type of a VPN*. *See id.* Notably, Patent Owner does not cite to any passage of RFC 2535 (Ex. 1016) – the publication actually cited in the '135 Patent – to support its assertions. This is because RFC 2535 does not even mention the terms "encryption" or "VPN," much less state that a VPN *must* use encryption.

In the same IPR proceedings, Patent Owner also relied upon a "glossary" related to "FreeS/WAN" that was purportedly cited in the prosecution history of the '135 patent. Ex. 1015, p. 23. That glossary, which is internally dated February 21, 2002 (two years after the filing of the CIP application that matured as the '135 patent), states that a VPN is "a network that can safely be used as if it were private, even though some of its communication uses insecure connections. All traffic on those connections is encrypted." Ex. 1023, p. 24. This later-created document further describing what is called out in the specification as "[o]ne implementation" of "[o]ne conventional scheme" for creating a VPN, Ex. 1001 at 37:50-62, falls far

short of a definition of VPN and should not be read into the claims. Notably, however, the glossary's definition by its use of "those connections" only envisions the use of encryption over "insecure connections." Ex. 1023, p. 24. In other words, encrypting while on the public network. *Id*. As described in further detail in §V.A below, this is exactly what Kiuchi does – uses encryption on the public network connecting the client-side and server-side proxies with the rest of the communication paths made secure by the use of firewalls.

Patent Owner has also pointed to the constructions adopted by certain District Courts that a VPN requires encryption. Ex. 1015, pp. 23-24. These constructions, however, are not the broadest reasonable interpretation, but reflect the meaning of the term as used in district court litigation; it is not controlling in this proceeding. *In re Trans Texas Holdings Corp.*, 498 F.3d 1290, 1298-99 (Fed. Cir. 2007);

Finally, the Patent Owner has contended that Petitioner's expert, Dr. Roch Guerin, has in other IPRs regarding related patents "supported" interpretations of VPN requiring encryption and has "identif[ied] passages [in the specification] that support defining a VPN to require encryption." Ex. 1021, p. 32. However, Dr. Guerin did not provide an opinion regarding the broadest reasonable interpretation of VPN. Instead, he offered an opinion that the broadest reasonable interpretation of VPN would be "broad enough" to cover a proposed interpretation that included

"encrypting traffic on insecure communication paths" because that interpretation was "not inconsistent" with the specification of the related patent at issue. Ex. 1025, ¶ 19. Dr. Guerin also noted that the '180 patent at issue in that proceeding described a VPN as including "a secure communication link" and that "some of the VPNs" described in that patent "rely upon encryption" to achieve that security. *Id*. at ¶¶ 19-20. Dr. Guerin's prior opinions do not support reading a requirement of encryption into the term VPN.

The broadest reasonable construction of "VPN" thus does not require encryption, but can establish a "private network" using either encryption or other methods, such as IP hopping, or both.

A VPN does not require computers to directly communicate with each other:

Patent Owner has also contended in prior proceedings that a "VPN" requires computers in a VPN to "*directly communicate* with each other." *See e.g.*, Ex. 1009, pp. 1-3 (emphasis added). But in the August 2010 litigation, the Court found that Patent Owner had *disclaimed* VPNs that do not involve "direct communications" between the involved computers. Ex. 1019, pp. 6-9. The Court relied on Patent Owner's statements to the Office during the '269 reexamination proceeding involving the '135 Patent to make this determination; specifically, that the claims of the '135 Patent were not anticipated by the prior art "Aventail" because "computers connected according to Aventail *do not communicate directly with*

each other." *Id* (Emphasis added). The Court also observed that "…routers, firewalls, and similar servers that participate in typical network communication do not impede 'direct' communication between a client and target computer." Ex. 1019, p. 8, n. 2. The Court's finding that Patent Owner disclaimed a *portion of the literal scope of the '135 Patent claims* (*i.e.*, that covering VPNs in which computers do not "directly" communicate) means that the '135 claims in *their broadest reasonable construction* must still encompass this subject matter. Patent Owner's prosecution disclaimer is effective in a district court proceeding but not here. *E.g.*, M.P.E.P. § 2111; *id*. at § 2111.01(I) ("Although claims of issued patents are interpreted in light of the specification, prosecution history, prior art and other claims, *this is not the mode of claim interpretation to be applied during examination*.").

Finally, in the context of IPR proceedings IPR 2014-00237 and -00238 concerning related U.S. Patent No. 8,504,697, the Board has in the past construed the term "virtual private network" to mean "a 'secure communication link' with the additional requirement that the link includes a portion of a public network." Again, there is no requirement that a VPN include encryption or direct communication.

For all these reasons, the broadest reasonable construction of "VPN" therefore encompasses "a secure network that includes portions of a public

network."

2. DOMAIN NAME (CLAIM 10)

The Patent Owner has asserted to the PTAB in proceedings regarding U.S. Patent No. 7,490,151, a divisional of the '135 Patent having a common specification, that a "domain name" means "a name corresponding to a network address." Ex. 1007, p. 21.

In view of the Patent Owner's own assertions, it is reasonable, for purposes of this proceeding in which the broadest reasonable interpretation standard applies, to consider the term "domain name" as encompassing "a name corresponding to a network address." This is consistent with its plain and ordinary meaning and usage in the '135 Patent. Ex. 1001 at 37:22-39.

In the earlier proceedings, Patent Owner has urged that no interpretation of this term is needed, because it did not appear alone in the claims of that patent, but rather only as part of a larger phrase. Ex. 1007, p. 21. That is not the case here. In the '135 Patent, "domain name" is used as a free-standing term in the claims. Ex. 1001 at 48:7. In addition, the term "domain name" informs the meaning of other claim terms such as "Domain Name Service (DNS) request" (claim 1) and "DNS proxy server" (claim 8 and 10).

Accordingly the term "domain name" should be interpreted and it should be interpreted to encompass "a name corresponding to a network address."

3. DNS REQUEST (CLAIM 1)

The Patent Owner has asserted to the PTAB in proceedings regarding U.S. Patent No. 7,490,151, a divisional of the '135 Patent having a common specification, that a "DNS request" means "a request for a resource corresponding to a domain name." Ex. 1007, p. 22. In IPR2014-00610 the PTAB agreed with and adopted this interpretation. Ex. 1011, p. 6.

Petitioner generally agrees with this interpretation, but believes that the agreed understanding of "domain name" should be incorporated into the interpretation of "DNS request," which should then be interpreted to mean "a request for a resource corresponding to a network address."

4. DNS PROXY SERVER (CLAIMS 10, 8)

Patent Owner has in prior proceedings regarding the '135 Patent asserted that a "DNS proxy server" is "a computer or program that responds to a domain name inquiry in place of a DNS." *See* Ex. 1018, pp. 16-17 (Plaintiff's Opening Claim Construction Brief in case no. 6:10-cv-417 (E.D. Tex.)); Ex. 1015, pp. 32-33 (IPR2013-00348, Paper No. 10).

This is consistent with the embodiments disclosed in the specification of the '135 Patent. *See* Ex. 1001 at 38:23-47. Accordingly, for the purposes of this Petition, Mangrove adopts this construction.

Petitioner notes that Patent Owner has admitted that – and the above construction allows for the fact that –the claimed DNS proxy server can be

distributed among different computers or processes, under the broadest reasonable interpretation. *See* Ex. 1015, pp. 32-33.

5. CLIENT COMPUTER (CLAIMS 1 AND 10)

In a prior IPR proceeding (IPR2014-00558) involving the '135 Patent, Patent Owner argued that the term "client computer" should be interpreted to mean "user's computer." Ex. 1021, pp. 37-39 (IPR2014-00558, Paper 11). Patent Owner's proposed interpretation does not reflect the broadest reasonable interpretation of the term and should be rejected.

Patent Owner's proposed construction transparently attempts to rewrite the claim term to substitute "user's" for "client." This approach to claim construction, in which limitations from preferred embodiments that are not present in the claims are "read in" to the claims, has been rejected multiple times by the Patent Office under the broadest reasonable interpretation standard. For example, in IPR2014-00610 regarding a divisional of the '135 Patent (U.S. Patent No. 7,490,151) the PTAB rejected Patent Owner's attempt to give the term "client" the identical interpretation Patent Owner has offered in the '135 Patent for "client computer." Ex. 1011, pp. 7-8. Instead, the PTAB found that the broadest reasonable interpretation of the term "client" in light of the same specification was "a device, computer, system, or program from which a data request to a server is generated." Petitioner agrees with this interpretation and proposes that the same reasoning

should be applied here. As such, the term "client computer" should be interpreted to mean "a computer from which a data request to a server is generated."

As used in ordinary technical usage and in the '135 Patent, a "client computer" refers to the computer from which a data request to a server is originated. *See* Ex. 1001('135 Patent at 1:49-55 ("Proxy servers prevent destination servers from determining the identities of the originating clients. This system employs an intermediate server interposed between client and destination server. The destination server sees only the Internet Protocol (IP) address of the proxy server and not the originating client."). There is no requirement anywhere in the intrinsic record that a client computer be a "user computer," as Patent Owner asserts.

Finally, Petitioner's proposed interpretation is also consistent with the Office's interpretation of the term "client computer" in another patent in the '135 family. As the Patent Owner previously admitted, "[i]n reexamination control no. 95/001,792, which pertains to related U.S. Patent No. 7,188,180, the Board found that the term 'client computer' may read on a proxy computer where no user resides." Ex. 1021, p. 40, n. 10.[2]

[2] While the Patent Owner has stated its intent to reopen prosecution in that reexamination, *see* Ex. 1021 at 40, n. 10, the examiner has to date maintained the rejections based on the above interpretation of "client computer." *See* Ex. 1017, p.

6. AUTOMATICALLY (CLAIM 1)

The Patent Owner has previously asserted to the PTAB that "automatically initiating/creating an encrypted/ secure channel" means "initiating/creating the encrypted/secure channel without involvement of a user." Ex. 1007, pp. 24-25. However, as the PTAB has previously pointed out, "the term 'automatic' has a plain and ordinary meaning of 'marked by action that . . . arises as a really or apparently necessary reaction to or consequence of a given set of circumstances' or 'having a self-acting or self-regulating mechanism.'" Ex. 1011, p. 7, *quoting* WEBSTER'S THIRD NEW INTERNATIONAL DICTIONARY 148 (1971) (Ex. 1008). As the PTAB previously found, neither the plain meaning of "automatically" nor the '151 specification support the Patent Owner's proposed added limitation that "automatically" means "without user involvement." Ex. 1011, pp. 6-7. Accordingly, the word "automatically" should be interpreted under its ordinary meaning as "marked by action that arises as a really or apparently necessary reaction to or consequence of a given set of circumstances" or "having a self-acting or self-regulating mechanism."

---

4 (Patent Owner's Comments in Response to Examiner's Determination (Mar. 11, 2015)).

V. MANNER OF APPLYING CITED PRIOR ART TO EVERY CLAIM FOR WHICH AN IPR IS REQUESTED, THUS ESTABLISHING A REASONABLE LIKELIHOOD THAT AT LEAST ONE CLAIM OF THE '135 PATENT IS UNPATENTABLE

A. [GROUND 1] – CLAIMS 1-4, 7, 8, 10, AND 12 ARE ANTICIPATED BY KIUCHI (EX. 1002)

Kiuchi is a printed publication that was presented at the 1996 Symposium on Network and Distributed Systems Security (SNDSS) on February 22 & 23, 1996, and published by IEEE in the Proceedings of SNDSS 1996. Kiuchi was distributed publicly without restriction no later than February 1996. *See* Ex. 1002. Kiuchi is prior art to the '135 Patent at least under § 102(b).

Overview of Kiuchi

Kiuchi describes a system and a protocol called "C-HTTP" that "provides secure HTTP communication mechanisms within a closed group of institutions on the Internet, where each member is protected by its own firewall." Ex. 1002, p. 64, Abstract. Kiuchi describes that C-HTTP can be used to create "a closed HTTP-based virtual network . . . for closed groups; for example, the headquarters and branches of a given corporation." Ex. 1002, p. 69, § 5. The following Diagram 1 illustrates relevant parts within the C-HTTP system described by Kiuchi, and will be used to describe the C-HTTP system. *See* Ex. 1003, ¶ 18.

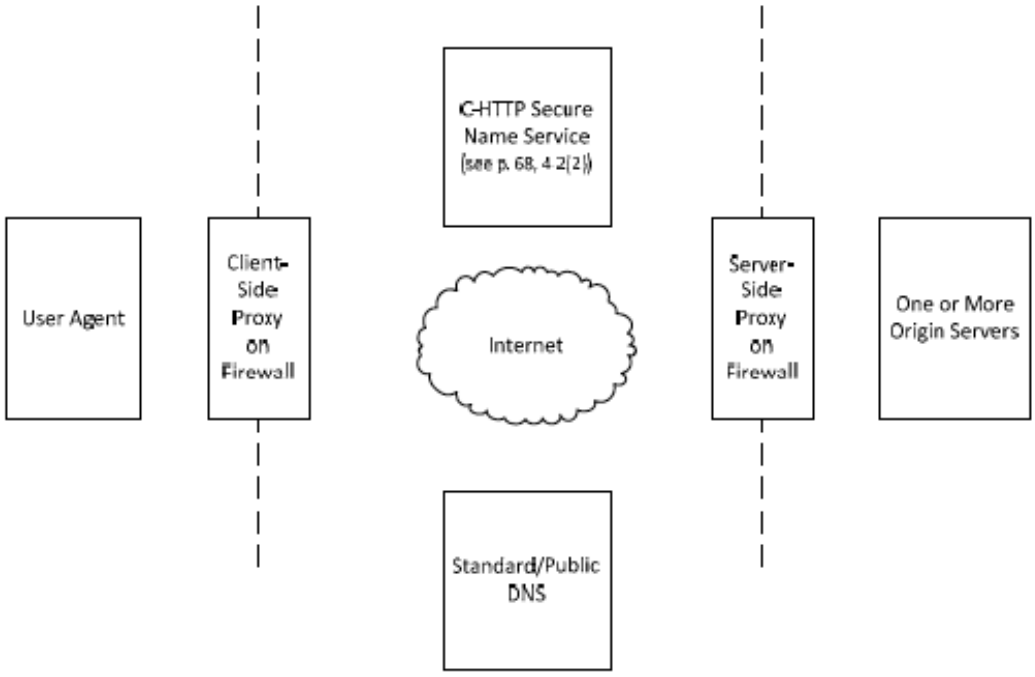

Diagram 1

Leveraging these parts, Kiuchi describes a process by which a client-side proxy establishes a secure connection with a server-side proxy using the C-HTTP protocol over the Internet (i.e., a C-HTTP connection), thus establishing a closed virtual network including a user agent and an origin server. *See* Ex. 1002, p. 64, § 2.1; p. 69, § 5; *see also* Ex. 1003, ¶ 19. Through the C-HTTP connection, a user agent associated with the client-side proxy may request information stored on an origin server associated with the server-side proxy. *See id*. In order to establish a C-HTTP connection, Kiuchi teaches discrete steps that will be described using the following block diagram. *See* Ex. 1002, pp. 65-66, § 2.3; *see also*, Diagram 2, where each step is numbered to indicate a temporal sequence of the steps taught by Kiuchi (Ex. 1003, ¶ 20).

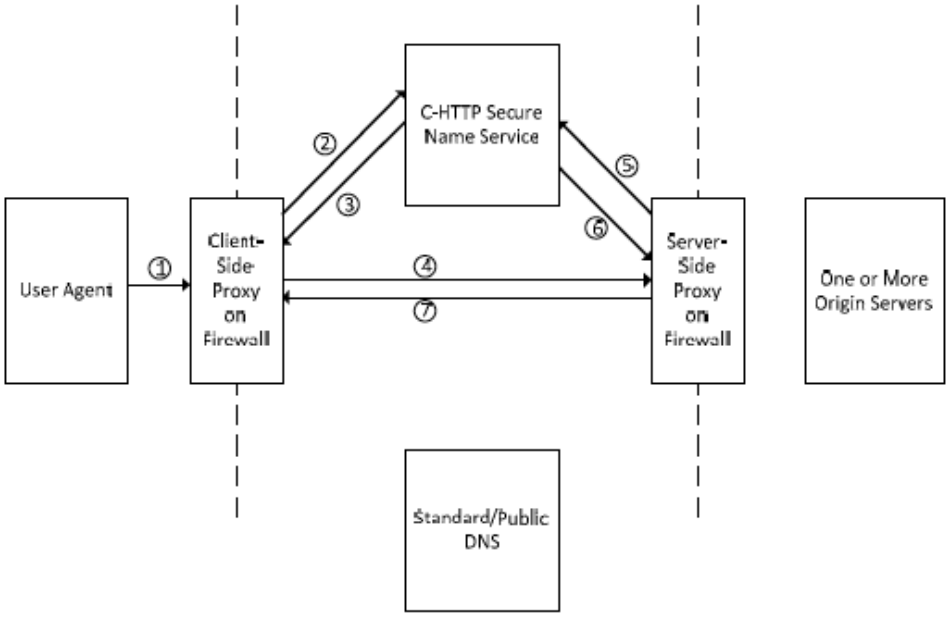

Diagram 2

To enable initiation of this set of steps, the user agent displays HTML documents to an end-user. *See* Ex. 1002, p. 65, § 2.3. Through interaction with the user agent, the end user selects a hyperlink URL included within an HTML document. *See id*. Kiuchi provides an example of the selected URL: "http://server.in.current.connection/sample.html=@=6zdDfldfcZLj8V!i", where "server.in.current.connection" is the hostname, "sample.html" is the name of the resource being requested, and "6zdDfldfcZLj8V!i" is a connection ID. *See* Ex. 1002, p. 65, § 2.3; Ex. 1003, ¶ 21.

Thereafter, as illustrated by Diagram 3, initial steps are performed by Kiuchi's system in response to user selection of the hyperlink. These steps include: (1) a request being sent from the user agent to the client-side proxy for the selected URL; (2) a request being sent from the client-side proxy to the C-HTTP name

server for an IP address corresponding to the hostname included in the selected URL; and (3) a response being returned from the C-HTTP name server that either includes the IP address associated with the server-side proxy or an error message. Ex. 1003, ¶ 25. If the C-HTTP name server returns an error message (i.e., if the hostname does not correspond to a secure server in the closed network, or the connection is not permitted), then the client-side proxy performs a DNS lookup using the standard/public DNS, as illustrated by the dashed line. *See* Ex. 1002, p. 65, § 2.3; *see also* Ex. 1003, ¶ 25.

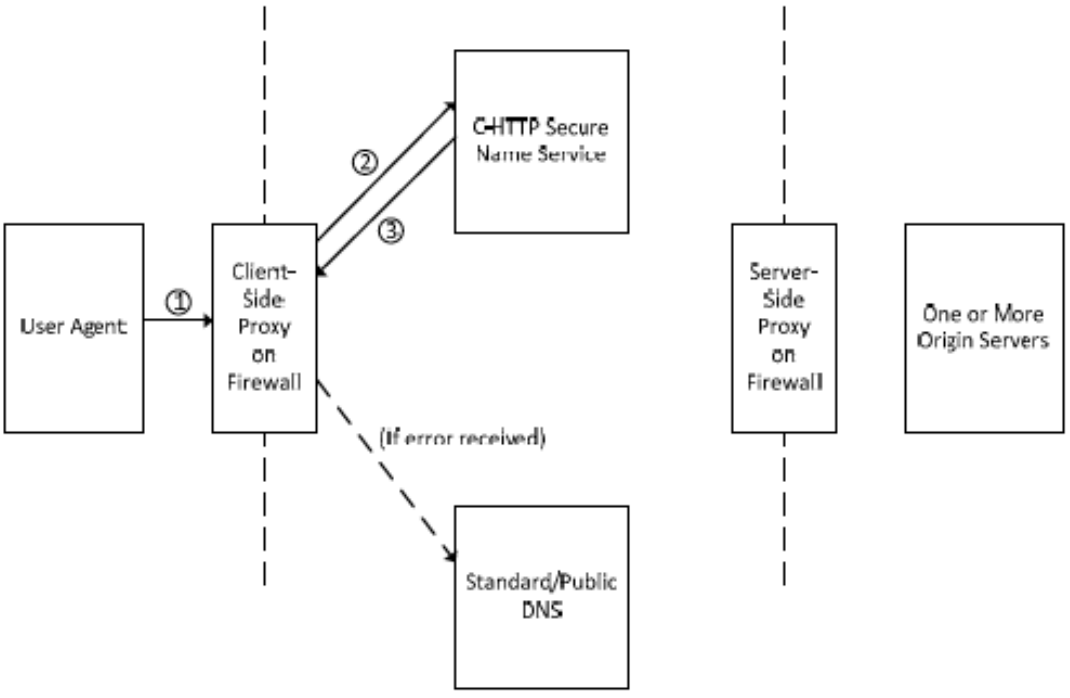

Diagram 3

Analyzing these steps in further detail, when the end user selects the hyperlink in the displayed HTML document, the user agent sends a request for the URL to the client-side proxy, as illustrated by (1) in Diagram 3. *See* Ex. 1002, p.

65, § 2.3. When the client-side proxy receives the URL (including the hostname) from the user agent, it determines whether the connection ID included in the URL matches the IDs of any current connections being maintained by the client-side proxy. *See id*. If the connection ID is not found in the current connection table in the client-side proxy, the client-side proxy attempts to establish a new connection with the host corresponding to the hostname included in the URL. *See id*.

To establish a new connection with the corresponding host, as illustrated by (2) in Diagram 3, the client-side proxy sends a request to ask the C-HTTP name server whether the client-side proxy can communicate with the host associated with the hostname and, if so, to resolve the hostname included in the URL such that the corresponding IP address is returned by the C-HTTP name server to the client-side proxy. *See* Ex. 1002, p. 65, § 2.3(2). In some instances, the hostname corresponds to an origin server associated with a server-side proxy and is associated with an IP address for the server-side proxy. *See* Ex. 1002, p. 65, § 2.3; *see also* Ex. 1003, ¶¶ 21-23. In other instances, the hostname corresponds to a server on the Internet outside the C-HTTP network. Ex. 1002, p. 65, § 2.3; Ex. 1003, ¶ 23.

Upon receipt of the request, the C-HTTP name server first authenticates the client-side proxy (and, by association, the user agent) to determine if the request is legitimate. *See* Ex. 1002, p. 65, § 2.3; *see also* Ex. 1003, ¶ 23. When the request is

legitimate, the C-HTTP name server determines whether a "server-side proxy [associated with the hostname] is registered in the closed network." *See id*. As illustrated by (3) in Diagram 3, if a server-side proxy associated with the hostname is not registered in the closed network, or the connection is not permitted, then the C-HTTP name server returns an error message, in response to which the client-side proxy performs a look-up with a standard/public DNS server, behaving like an ordinary HTTP proxy. *See id*. The standard/public DNS server then returns an IP address of the host corresponding to the hostname, which the client-side proxy uses to connect to the host on behalf of the user agent. *See id*.

On the other hand, if the server-side proxy is registered in the closed network and is permitted to accept a connection from the client-side proxy, then the C-HTTP name server sends a response to the client-side proxy's request that includes "the IP address and public key of the server-side proxy and both request and response Nonce values," as illustrated by (3) in Diagram 3. *See* Ex. 1002, p. 65, § 2.3; *see also* Ex. 1003, ¶ 23. Notably, the C-HTTP name server never provides the IP address of the origin server to the client-side proxy. *See* Ex. 1002, p. 65, § 2.2; *see also* Ex. 1003, ¶ 28. Rather, when the C-HTTP name server returns the IP address of the server-side proxy along with the server-side proxy's public key and the nonce values, the client-side proxy attempts to establish a C-HTTP connection with the server-side proxy using the IP address received from

the C-HTTP name server. *See* Ex. 1002, p. 65, § 2.3; *see also* Ex. 1003, ¶ 26. The steps for doing so are illustrated in Diagram 4. *See* Ex. 1003, ¶ 27.

In particular, Kiuchi describes that the client-side proxy, in response to receiving the IP address of the server-side proxy and other information from the C-HTTP name server, sends a "[r]equest for connection to the server-side proxy" (4), the server-side proxy performs a "[l]ookup of client-side proxy information" with the C-HTTP name server (5 and 6), and the server-side proxy sends confirmation of the connection to the client-side proxy (7), if the server-side proxy is able to properly authenticate the client-side proxy. *See* Ex. 1002, pp. 65-66, § 2.3, steps 3-5; *see also* Ex. 1003, ¶ 29-30.

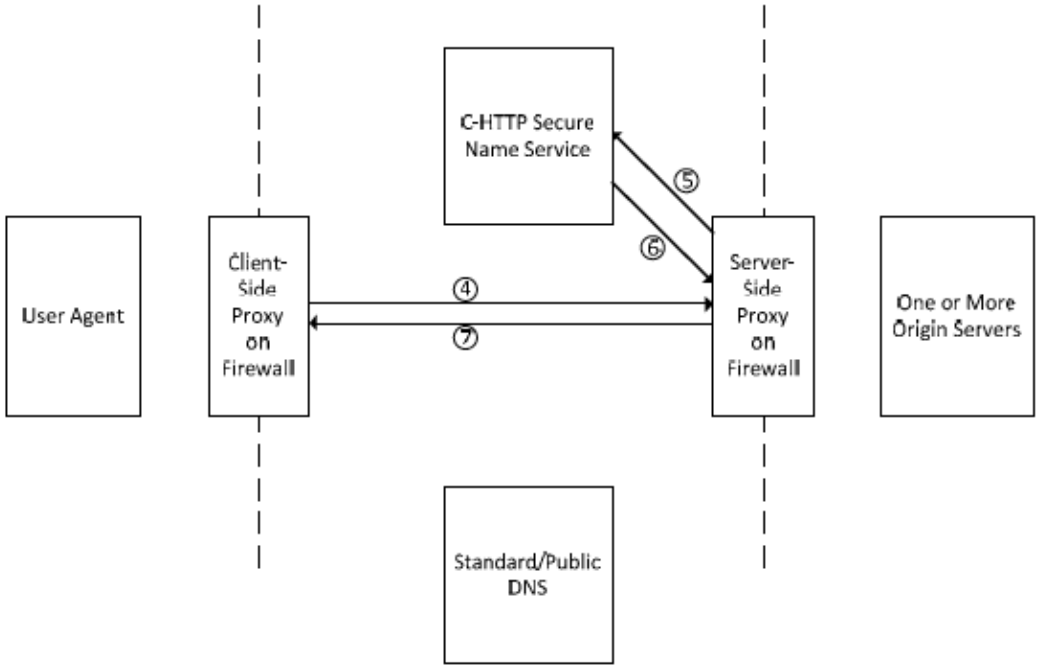

Diagram 4

Considering these steps in further detail, the client-side proxy, in response to

receiving the IP address and associated information from the C-HTTP server, sends a request for connection to the server-side proxy, as illustrated by (4) in Diagram 4. *See* Ex. 1002, p. 65, § 2.3; *see also* Ex. 1003, ¶ 29. The client-side proxy encrypts the request for connection using the server-side proxy's public key and includes in the request "the client-side proxy's IP address, hostname, request Nonce value and symmetric data exchange key for request encryption." *See* Ex. 1002, p. 65, § 2.3; *see also* Ex. 1003, ¶ 30. After receiving the request, the server-side proxy "asks the C-HTTP name server whether the client-side proxy is an appropriate member of the closed network," as illustrated by (5) in Diagram 4, and, in response, the C-HTTP name server "examines whether the client-side proxy is permitted to access the server-side proxy." Ex. 1002, pp. 65-66, § 2.3; *see also* Ex. 1003, ¶ 27. If the C-HTTP name server determines that "access is permitted, the C-HTTP name server sends [to the serverside proxy] the IP address and public key of the client-side proxy and both request and response Nonce values," as illustrated by (6) in Diagram 4. Ex. 1002, p. 66, § 2.3; *see also* Ex. 1003, ¶ 67.

After "the C-HTTP name server provides both client-side and server-side proxies with each peer's public key," the proxies establish a C-HTTP connection. Ex. 1002 p. 66, § 2.3; *see also* Ex. 1003, ¶ 30. The C-HTTP connection "provides [a] secure HTTP communication mechanisms" in which communications over the C-HTTP connection are encrypted. Ex. 1002, pp. 64-66, abstract; *see also* Ex.

1003, ¶ 30.

1. KIUCHI ANTICIPATES INDEPENDENT CLAIM 1

Preamble

Kiuchi shows "*[a] method for transparently creating a virtual private network (VPN) between a client computer and a target computer*." *See* Ex. 1003, ¶ 31. Kiuchi describes a method (termed "C-HTTP") for constructing a closed network over the Internet that allows a user agent (*e.g.*, a web browser) running on a computer in one private network to access private web pages (e.g., HTML pages) stored on an origin server in a different private network. *See* Ex. 1002, pp. 64, 69. The closed network is created over the Internet using a client-side proxy and a server-side proxy that transparently perform specialized proxy functions for the user agent and origin server. *Id.* at 64-65. The proxies are installed in firewalls between the user agent and the origin server, which are unaware of the proxies. *Id.* The user agent, origin server, and proxies are HTTP/1.0 compatible devices. *Id.* The proxies work in conjunction with a C-HTTP name server on the Internet. *Id.*

Kiuchi describes systems and processes in which a secure connection between a client-side proxy and a server-side proxy (and by extension between the user agent and origin server, which are secured behind the firewalls containing the proxies) automatically is established by the proxy servers and a C-HTTP name server in response to a request specifying a destination in the closed network. *See*

Ex. 1003, ¶¶ 18-20, 31. The proxy servers automatically initiate the secure connection to encrypt any traffic sent over the Internet between the user agent and the origin server. *Id.*

Step (1)

Kiuchi also discloses a process that includes "*generating from the client computer a Domain Name Service (DNS) request that requests an IP address corresponding to a domain name associated with the target computer*." *See* Ex. 1002, p. 65, § 2.3; *see also* Ex. 1003, ¶¶ 20-22. Kiuchi shows that a user agent makes an HTTP request to connect to a host that is specified within a URL. *See id.* The client-side proxy receives the request and sends a request to a C-HTTP name server asking to resolve the hostname in the request into an IP address. *See id.*

If the hostname in the URL corresponds to a secure destination and the C-HTTP name server determines the client-side proxy is authorized to make a connection with the server-side proxy, the C-HTTP name server will return an IP address corresponding to the hostname to the client-side proxy. *See* Ex. 1002, p. 65, § 2.3; *see also* Ex. 1003, ¶¶ 23-24.

Step (2)

Kiuchi describes processes that include the step of "*determining whether the DNS request transmitted in step (1) is requesting access to a secure web site*." *See* Ex. 1002, p. 65, § 2.3; *see also* Ex. 1003, ¶¶ 22-26. As described above, when the

client-side proxy receives the request from the user agent, it sends a request to a C-HTTP name server. *See id.* The C-HTTP name server evaluates the request to determine if the hostname specifies a destination that is part of the closed network and whether the connection between the user agent and the origin server is permitted. *See id.* If the C-HTTP server determines the destination is not part of the closed network, it returns an error code. *See id.* In response to the error code, the client-side proxy concludes that the request specifies a non-secure destination and performs a look-up to a conventional DNS server. *See id.*

If the C-HTTP name server determines the hostname specifies a secure destination and the connection is permitted, it will return an IP address associated with the secure hostname along with other information. *See id.* The client-side proxy uses the returned IP address to send a request to the server-side proxy to make a connection. *See id.* Thus, the C-HTTP name server and client-side proxy each determine whether the user agent is requesting to connect to a secure destination. *See* Ex. 1003, ¶¶ 23-24.

Step (3)

Kiuchi also shows a process that includes "*in response to a determination that the DNS request is requesting access to a secure target web site, automatically initiating the VPN between the client computer and the target computer*." *See* Ex. 1002, pp. 65-66, § 2.3; *see also* Ex. 1003, ¶¶ 24, 29-31. Kiuchi discloses that if a

connection is permitted, the C-HTTP name server initiates the connection by returning an IP address and public key associate with the hostname. *See* Ex. 1002, pp. 65-66, § 2.3; *see also* Ex. 1003, ¶¶ 23-24, 27. The client-side proxy sends an encrypted connection request to the server-side proxy. *See id.* This is consistent with the '135 Patent, which shows an example of automatically initiating a VPN by sending a message requesting to create a VPN. *See* Ex. 1001 at 38:30-33.

If the server-side proxy accepts the connection, it sends to the client-side proxy a message containing a data exchange key. *See* Ex. 1002, pp. 65-66, § 2.3; *see also* Ex. 1003, ¶¶ 27-30. After the client-side proxy receives the message, a connection is established. *See id.* Data is securely transmitted between the user agent and origin server because the proxy servers automatically encrypt any traffic sent between them. *See* Ex. 1002, p. 65, § 1; *see also* Ex. 1003, ¶ 26. The connect message the client-side proxy sends to the server-side proxy and the response message the server-side proxy sends to the client- side proxy (both of which are sent without intervention from the user agent) act to initiate the connection. *See* Ex. 1002, pp. 65-66, § 2.3; *see also* Ex. 1003, ¶¶ 27-30.

2. KIUCHI ANTICIPATES CLAIM 3

Claim 3 depends from claim 1 and further requires the step of "*(4) in response to determining that the DNS request in step (2) is not requesting access to a secure target web site, resolving the IP address for the domain name and*

returning the IP address to the client computer."

Kiuchi shows a process that includes this step. *See* Ex. 1002 p. 65, § 2.3; *see also* Ex. 1003, ¶¶ 22-25.

Specifically, Kiuchi shows that when the client-side proxy receives an HTTP request, it sends a request to a C-HTTP name server. *See id.* If the destination is not part of the closed network, the C-HTTP name server returns an error code. *See id.* If the client-side proxy receives an error code, it determines the URL specifies a non-secure destination and it sends the hostname in the URL to a conventional DNS server. *See id.* The DNS server will return an IP address, which the client-side proxy uses to establish an ordinary HTTP connection. *See id.*

3. KIUCHI ANTICIPATES CLAIM 4

Claim 4 depends from claim 1 and further requires the step of "*prior to automatically initiating the VPN between the client computer and the target computer, determining whether the client computer is authorized to establish a VPN with the target computer and, if not so authorized, returning an error from the DNS request*." *See* Ex. 1002, p. 65, § 2.3; *see also* Ex. 1003, ¶¶ 22-25. Kiuchi likewise discloses this step.

Specifically, Kiuchi shows that when the client-side proxy receives an HTTP request from a user agent, it sends a request to a C-HTTP name server. *See id.* The C-HTTP name server authenticates the request and then evaluates it to determine if

the connection is permitted. *See* Ex. 1003, ¶¶ 22-25; Ex. 1002, pp. 64-65 ("the name server . . . examines whether the client-side proxy is permitted to access to the server-side proxy."). If the C-HTTP name server determines the connection is not permitted, it returns an error code. *See* Ex. 1003, ¶¶ 22-25.

4. KIUCHI ANTICIPATES CLAIM 7

Claim 7 depends from claim 1 and further requires that "*wherein step (3) comprises the step of using a gatekeeper computer that allocates VPN resources for communicating between the client computer and the target computer*." *See* Ex. 1003, ¶ 30.

Kiuchi discloses this step. Specifically, Kiuchi shows that the server-side proxy acts as a gatekeeper computer that allocates resources. *See* Ex. 1003, ¶ 30. When the client-side proxy receives the request from the user agent, it sends a request to a C-HTTP name server. *See* Ex. 1002, p. 65, § 2.3; *see also* Ex. 1003, ¶ 23. If the C-HTTP name server determines the connection is permitted, it will return an IP address and public key corresponding to the hostname; otherwise it will return an error code. *See id.* If an IP address and key are returned, the client-side proxy sends an encrypted request to the server-side proxy containing a data exchange key; if an error message is returned the client-side proxy performs a standard DNS lookup. *See* Ex. 1002, p. 65, § 2.3; *see also* Ex. 1003, ¶¶ 27-30

After the server-side proxy receives the request from the client-side proxy, it

sends a message to the C-HTTP name server to verify the client-side proxy is part of the closed network. *See id.* If the server-side proxy determines it should accept the connection, it sends a message to the client-side proxy containing a connection identifier and a second data exchange key. *See id.* After the client-side proxy receives the message from the server-side proxy, the connection is established. *See id.* The server-side proxy acts as a gatekeeper by providing the client-side proxy with the connection identifier and the second data exchange key. *See* Ex. 1003, ¶ 30. This is consistent with the '135 Patent specification, which shows the gatekeeper may receive a request from the DNS proxy requesting that a VPN be created. *See* Ex.1001 at 38:30-33.

5. KIUCHI ANTICIPATES CLAIM 8

Claim 8 depends from claim 1 and requires "*[t]he method of claim 1, wherein step (2) is performed in a DNS proxy server that passes through the request to a DNS server if it is determined in step (3) that access is not being requested to a secure target web site*." *See* Ex. 1002, pp. 65, § 2.3; *see also* Ex. 1003, ¶¶ 23-27. This additional step is also disclosed in Kiuchi.

Specifically, in Kiuchi the function of the DNS proxy is distributed among the client-side proxy and the C-HTTP name server . *See* Ex. 1003, ¶ 19-26, 34. When the client-side proxy receives a request from a user agent, it determines whether the requested hostname in the URL specifies a secure server by sending to

a C-HTTP name server a request to resolve the hostname. *See* Ex. 1002, pp. 65, § 2.3; *see also* Ex. 1003, ¶¶ 23-26. If the C-HTTP name server returns an error code, the client-side proxy determines the URL specifies a non-secure destination. *See id.* The client-side proxy then sends the hostname to a conventional DNS server for resolution. *See id.* This is the same as the '135 Patent, where a conventional DNS lookup is performed when access is not being requested to a secure target web site. Ex. 1001 at 38:43-47, and is covered by the broadest reasonable interpretation.

6. KIUCHI ANTICIPATES INDEPENDENT CLAIM 10

Kiuchi shows a "*system that transparently creates a virtual private network (VPN) between a client computer and a secure target computer*." *See* Ex. 1003, ¶ 31. Kiuchi describes systems in which a VPN between a user agent and origin server is automatically and transparently established by proxy servers and a C-HTTP name server. *See* § V.A.1, *supra*. Kiuchi shows that the C-HTTP name server and proxy servers are part of a system of computers. *See* Ex. 1003, ¶¶ 18-19.

Kiuchi shows a system including "*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 returns the IP address for the requested domain if it is determined that the access to a non-secure website has been requested, and 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." *See* Ex. 1003, ¶¶ 19, 21-25, 27. When the client-side proxy receives from the user agent a request to retrieve a resource on an origin server, it sends a request to a C-HTTP name server to resolve a corresponding domain name. *See* Ex. 1002, p. 65, § 2.3; *see also* Ex. 1003, ¶¶ 20-22. If the C-HTTP name server determines the destination is not part of the closed network, it returns an error code. *See id.* If the client-side proxy receives an error code, it concludes the hostname in the URL specifies a non-secure destination and sends the hostname to a conventional DNS server. *See id.* If the C-HTTP name server determines the hostname specifies a secure destination, it returns an IP address and other information. *See id.*

Thus, where a user agent requests to connect to a destination in the closed network, the C-HTTP name server and client-side proxy act as proxy servers, acting in place of a conventional DNS server. *See id.* But where the user agent requests to connect to a non-secure server, the hostname in the connection request will be resolved by a conventional DNS server. *See id.*

Kiuchi shows 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*" as specified in claim 10. As explained with respect to claim 7 (see § V.A.4, *supra*), Kiuchi shows that the server-side proxy acts as a gatekeeper that allocates VPN resources.

7. KIUCHI ANTICIPATES CLAIM 12

Claim 12 depends from claim 10 and further requires "*wherein the gakekeeper computer determines whether the client computer has sufficient security privileges to create the VPN, and, if the client computer lacks sufficient security privileges, rejecting the request to create the VPN*." Kiuchi discloses this process. *See* Ex. 1003, ¶ 30. Specifically, as explained above with respect to claim 7 (*see* § 4, *supra*), Kiuchi shows the server-side proxy acts as a gatekeeper that allocates VPN resources. If the server-side proxy determines a requested connection is not permitted, it does not accept the client-side proxy's connection request. *See* Ex. 1003, ¶¶ 27-28.

B. [GROUND 2] – KIUCHI IN VIEW OF RFC 1034 RENDERS CLAIM 8 OBVIOUS

As explained above, claim 8 depends from claim 1 and further requires that *step (2) is performed in a DNS proxy server that passes through the request to a DNS server if it is determined in step (3) that access is not being requested to a secure target web site*." *See* Ex. 1002, pp. 65, § 2.3; *see also* Ex. 1003, ¶¶ 23-26. "Step 2" refers to the step of claim 1 of "determining whether the DNS request transmitted in step (1) is requesting access to a secure web site."

As explained above in §§ V.A.1 and V.A.5, *supra*, Kiuchi anticipates claim 8. However, Patent Owner may contend Kiuchi does not show that step (2) of "determining whether the DNS request transmitted in step (1) is requesting access

to a secure web site" is not "performed in a DNS proxy server . . ." as required by claim 8, because the function of the DNS proxy is distributed among the client-side proxy and the C-HTTP name server. As explained above, Petitioner submits that under the proper claim construction of DNS proxy server, DNS proxy server can be distributed among different computers or processes.

However, even if a narrower claim construction were adopted, this would not render claim 8 patentable. As described below, it would have been an obvious modification of the Kiuchi C-HTTP system to configure the C-HTTP name server to resolve non-secure addresses as well.

Kiuchi explains that its systems enable users to securely access resources in various private networks by establishing a closed network over the Internet. *See* Ex. 1002, p. 64, § 21; *See also* Ex. 1003, ¶¶ 18-19. Kiuchi defines three specialized parts for the system: the client-side proxy, server-side proxy, and C-HTTP name server. *See id.* While Kiuchi describes that the client-side proxy makes a conventional DNS lookup request, a person of ordinary skill would have recognized that the DNS lookup step could be integrated into the C-HTTP name server based on the guidance in RFC 1034 (Ex. 1005), which describes the functional requirements of DNS name servers. *See* Ex. 1003, ¶¶ 34-35. Such a change would have been an obvious design choice. *Id.*

Notably, the C-HTTP name server already determines whether a DNS

request is requesting to access a secure web site. *See* Ex. 1002, 65, § 2.3(2); *see also* Ex. 1003, ¶35. Rather than returning an error code to the client-side proxy when the DNS request does not specify a secure web site, it would have been an obvious design choice for the C-HTTP name server to pass the domain name to a conventional DNS server for resolution, since the C-HTTP server already includes name service functionality. *See* Ex. 1003, ¶ 35. Such a configuration, which places a DNS proxy server function in a modified C-HTTP name server (similar to the placement of the DNS proxy server of the '135 Patent in the DNS server – *see* Ex.1001 at FIG. 26), is merely a rearrangement of existing functions within the C-HTTP system. *See* Ex. 1003, ¶¶ 35-37. For example, a C-HTTP name service response containing an IP address without a public key and nonce values (*e.g.*, using values of zero or other convention for those fields, or modifying the protocol to use a flag in the response to indicate those values are not provided) could indicate that the response specifies a conventional web site and hence that no VPN is needed. *See* Ex. 1003, ¶¶ 37-38. The motivation for modifying Kiuchi in this way would have been to streamline the system's operation, *e.g.*, instead of the C-HTTP name server sending an error code to the client-proxy which would then initiate a DNS inquiry, the change simplifies the process by having the C-HTTP name server initiate the request to the conventional DNS server. *See* Ex. 1003, ¶¶ 39-40.

VI. CONCLUSION

The cited prior art references identified in this Petition contain pertinent technological teachings, either explicitly or inherently disclosed, which were not previously considered in the manner presented herein, or relied upon on the record during original examination of the '135 Patent.

In sum, these references provide new, non-cumulative technological teachings which indicate a reasonable likelihood of success as to Petitioner's assertion that the Challenged Claims of the '135 Patent are not patentable pursuant to the grounds presented in this Petition.

Accordingly, Petitioner respectfully requests institution of an IPR for those claims of the '135 Patent for each of the grounds presented herein.