Paper No. _____

UNITED STATES PATENT AND TRADEMARK OFFICE

_____

BEFORE THE PATENT TRIAL AND APPEAL BOARD

_____

Apple Inc.
Petitioner,

v.

VirnetX, Inc. and Science Application International Corporation,
Patent Owner

Patent No. 6,502,135
Issued: Dec. 31, 2002
Filed: Feb. 15, 2000
Inventors: Edmund C. Munger, *et al*
Title: Agile Network Protocol For Secure Communications With Assured System Availability

_____

Inter Partes Review No. 2013-00348

PETITION FOR INTER PARTES REVIEW

TABLE OF CONTENTS

I. COMPLIANCE WITH REQUIREMENTS FOR A PETITION FOR INTER PARTES REVIEW

A. Certification the '135 Patent May Be Contested by Petitioner

Petitioner certifies it is not barred or estopped from requesting *inter partes* review of U.S. Patent No. 6,502,135 (the '135 patent) (Ex. 1001). Neither Petitioner, nor any party in privity with Petitioner, has filed a civil action challenging the validity of any claim of the '135 patent. The '135 patent has not been the subject of a prior *inter partes* review by Petitioner or a privy of Petitioner.

Petitioner also certifies this petition for *inter partes* review is filed within one year of the date of service of a complaint alleging infringement of a patent. Petitioner was served with a complaint alleging infringement of the '135 patent on **December 31, 2012**, which led to Civil Action No. 6:12-cv-00855-LED in the Eastern District of Texas. Ex. 1050. Because the date of this petition is less than one year from December 31, 2012, this petition complies with 35 U.S.C. § 315(b).

Petitioner notes it was previously served with a complaint asserting infringement of the '135 patent in August of 2010, which led to Civil Action No: 6:10-cv-417. During that action, the District Court established an additional civil action, Civil Action No. 6:13-cv-00211-LED, on February 26, 2013 (also pending in the Eastern District of Texas). The August 2010 complaint does not foreclose the present petition, as Patent Owner served a **new complaint** on Petitioner asserting infringement of the '135 patent in **December of 2012**.

Petitioner submits this conclusion is compelled by the plain language of § 315(b). Notably, § 315(b) does not specify a one-year deadline that runs from the date of the **first** complaint served on a petitioner. Rather, it states "[a]n inter partes review may not be instituted if the petition requesting the proceeding is filed more than 1 year after the date on which the petitioner, real party in interest, or privy of the petitioner is served with **a complaint** alleging infringement of the patent." Thus, a petition filed within 1 year of the date **any** complaint alleging infringement of the patent is served on a petitioner is timely under the plain statutory language of § 315(b). This is also the only reading of § 315(b) consistent with the statutory design. Congress designed the IPR authority to be option to contest validity of a patent **concurrently** with district court proceedings involving the same patent. A timely filed IPR proceeding in **any** action a patent owner elects to commence is perfectly consistent with this statutory design.

Reading § 315(b) in this manner also is the only way to effectively foreclose gaming of the system by a Patent Owner. Indeed, if § 315(b) were read to foreclose IPR proceedings in a second, independent action for infringement a patent owner elected to commence, it would unfairly foreclose use of the IPR system. For example, a patent owner could assert irrelevant claims in a first action, wait a year, and then assert different claims in a new action that do present risks to a third party. In this scenario, the patent owner would foreclose legitimate use of

an IPR to contest validity of the patent claims asserted in the second action based on the third party's reasonable business decision to not dispute validity of irrelevant claims in the first action. Rather than attempting to decipher which scenarios would be improper, the Board should follow the plain meaning of § 315(b), and find a petition timely if it is filed within 1 year of the date **any** complaint alleging infringement of the patent is served on a Petitioner.

Finally, reading §315(b) to foreclose this petition based on the August 2010 complaint would be particularly unjust in this case. The 1-year period following service of the August 2010 complaint expired before it was possible to submit an IPR petition – petitions could only be filed on or after September 16, 2012.

B. Fee for Inter Partes Review (§ 42.15(a))

The Director is authorized to charge the fee specified by 37 CFR § 42.15(a) to Deposit Account No. 18-1260.

C. Mandatory Notices (37 CFR § 42.8(b))

1. Real Party in Interest (§ 42.8(b)(1))

The real party of interest of this petition pursuant to § 42.8(b)(1) is Apple Inc. ("Apple") located at One Infinite Loop, Cupertino, CA 95014.

2. Other Proceedings (§ 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; (iii) Civ. Act. No.

6:10-cv-00417-LED (E.D. Tex.), filed August 11, 2010 (the "2010 litigation"); (iv) Civ. Act. No. 6:11-cv-00018-LED (E.D. Tex), (iv) Civ. Act. No. 6:13-cv-00351-LED (E.D. Tex), filed April 22, 2013; (v) Civ. Act. No. 6:10-cv-00094 (E.D. Tex); and (vi) Civ. Act. No. 6:07-cv-00080 (E.D. Tex). Actions (i) to (iii) name Petitioner as a defendant.

The '135 patent is also the subject of merged *inter partes* reexamination nos. 95/001,679 and 95/001,682. Petitioner is the real party of interest in the '682 proceeding. In the merged proceedings, the Office recently issued a Non-Final Action rejecting all 18 claims of the '135 patent, including rejections based on Ex. 1007 (Aventail), Ex. 1008 (BinGO), and Ex. 1009 (Beser), as well as on other prior art references. Petitioner recognizes it may be appropriate for the Panel to merge, join or take other steps to manage these concurrent proceedings. The '135 patent also was the subject of reexamination no. 95/001,269, which is concluded.

Finally the '135 patent is the subject of IPR petition No. 2013-00349, being filed concurrently with the present Petition.

3. Designation of Lead and Backup Counsel

Lead Counsel	Backup Lead Counsel
Jeffrey P. Kushan Reg. No. 43,401 **jkushan@sidley.com** (202) 736-8914	Joseph A. Micallef Reg. No. 39,772 **jmicallef@sidley.com** (202) 736-8492

4. Service Information (§42.8(b)(4))

Service on Petitioner may be made by mail or hand delivery to: Sidley Austin LLP, 1501 K Street, N.W., Washington, D.C. 20005. The fax number for lead and backup counsel is (202) 736-8711.

D. Proof of Service (§§ 42.6(e) and 42.105(a))

Proof of service of this petition is provided in **Attachment A**.

II. Identification of Claims Being Challenged (§ 42.104(b))

Claims **1-10, 12-15, and 18** of the '135 patent are unpatentable as being anticipated under 35 U.S.C. § 102(a) & (e), and/or for being obvious over the prior art under 35 U.S.C. § 103. Specifically:

(i) Claims 1-10, 12-15, and 18 are anticipated under § 102(e) by U.S. Patent No. 6,496,867 to Beser et al. (Beser) (Ex. 1009);

(ii) Claims 1-10, 12-15, and 18 are obvious under § 103 based on Beser (Ex. 1009) in view of RFC 2401 (Ex. 1010);

(iii) Claims 3, 5, 8, 10, 12, and 18 are obvious under § 103 based on Beser (Ex. 1009) in view of Blum (Ex. 1011);

(iv) Claims 3, 5, 8, 10, and 18 are obvious under § 103 based on Beser (Ex. 1009) in view of RFC 2401 (Ex. 1010) and Blum (Ex. 1011);

(v) Claims 18 and 5 are obvious under § 103 based on Beser (Ex. 1009) in view of RFC 2401 (Ex. 1010) and Aventail (Ex. 1007);

(vi) Claims 1-10, 12-15, and 18 are obvious under § 103 based on Beser (Ex. 1009) in view of Hoke (Ex. 1012);

(vii) Claims 3, 5, 8, 10, 12, and 18 are obvious under § 103 based on Beser (Ex. 1009) in view of Hoke (Ex. 1012) and Blum (Ex. 1011);

(viii) Claims 9, 12, and 13 are obvious under § 103 based on Beser (Ex. 1009) in view of RFC 2401 (Ex. 1010) and Hoke (Ex. 1012);

(ix) Claims 5 and 18 are obvious under § 103 based on Beser (Ex. 1009) in view of Hoke (Ex. 1012) and Aventail (Ex. 1007);

(x) Claims 1-10, 12-15, and 18 are obvious under § 103 based on Beser (Ex. 1009) in view of RFC 2401 (Ex. 1010), Hoke (Ex. 1012), Blum (Ex. 1011), and Aventail (Ex. 1007);

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**, below. The evidence relied upon in this petition is listed in **Attachment B**.

III. Relevant Information Concerning the Contested Patent

A. Effective Filing Date and Prosecution History of the '135 patent

The '135 patent issued from U.S. Application No. 09/504,783, filed February 15, 2000. The '783 application is a continuation-in-part of U.S. Application No. 09/429,653, filed on October 29, 1999. The '783 and '653 applications each claim priority to Provisional Application Nos. 60/106,261, filed October 30, 1998 and 60/137,704, filed June 7, 1998.

Claims 1, 10, 13 and 18 are the independent claims. Claims 1, 10 and 18 rely on information first presented in the '783 CIP application. For example, claim 1 specifies "generating from the client computer a **Domain Name Service (DNS) request** …" and subsequent steps involving that DNS request, while claim 10 specifies "[a] system … comprising … a **DNS proxy server**…" No application filed prior to the '783 application even uses the term "domain name service" much

less describes methods or systems that use DNS requests or DNS proxy servers to establish virtual private networks. Ex. 1003 at ¶¶54-61. Claim 13 likewise relies on information first presented in the disclosure of the '783 application. For example, it specifies "…receiving from one of the plurality of client computers **a request** to establish a connection…" and "…authenticating, with reference to one of the plurality of authentication tables, that **the request** received in step (1) is from an authorized client." Neither step is described in any application filed before the '783 application. Ex. 1003 at ¶¶54-61. Accordingly, the effective filing date of claims 1-10, 12-15 and 18 is no earlier than **February 15, 2000**. Ex. 1003 at ¶61. In the *inter partes* reexamination proceedings involving the '135 patent, Patent Owner did not dispute that the effective filing date of the '135 patent was no earlier than February 15, 2000.

B. Person of Ordinary Skill in the Art

A person of ordinary skill in the art in the field of the '135 patent would have been someone with a good working knowledge of networking protocols, including those employing security techniques, as well as computer systems that support these protocols and techniques. The person also would be very familiar with Internet standards related to communications and security, and with a variety of client-server systems and technologies. The person would have gained this

knowledge either through education and training, several years of practical working experience, or through a combination of these. Ex. 1003 at ¶68.

C. Construction of Terms Used in the Claims

In this proceeding, claims must be given their broadest reasonable construction in light of the specification. 37 CFR 42.100(b). The broadest reasonable construction should encompass subject matter Patent Owner contends infringes the claims, and constructions Patent Owner has advanced in litigation. Also, if Patent Owner contends terms in the claims should be read to have a special meaning in this proceeding, those contentions should be disregarded unless Patent Owner presents amendments to the claims compliant with 35 U.S.C. § 112 that conform the claim language to such contentions. *See* 77 Fed .Reg. 48764 at II.B.6 (August 14, 2012). *Cf.*, *In re Youman*, 679 F.3d 1335, 1343 (Fed. Cir. 2012). Petitioner consequently has identified subject matter that falls within the scope of the claims read in their broadest reasonable construction, which Petitioner submits is sufficient for the purposes of this proceeding.

1. Virtual Private Network (VPN) (Claims 1, 10, 13, 18)

The ’135 patent does not define the term “**virtual private network**” or “**VPN.**” Ex. 1003 at ¶194. Two issues are raised by Patent Owner’s contentions in litigation involving the ’135 patent regarding this term.

First, Patent Owner has contended a VPN requires the network traffic sent over the VPN to be encrypted. *See* Ex. 1046 at 3-8 (a VPN is "a network of computers which privately communicate with each other **by encrypting traffic** on insecure communication paths between the computers."); Ex. 1003 at ¶193. The District Court in the 2010 litigation held a VPN is "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." Ex. 1043 at 8. The broadest reasonable construction of VPN, however, would not require the network traffic to be encrypted. For example, the '135 patent states "Data security is **usually** tackled using some form of data encryption" (Ex. 1001 at 1:38-39) and refers to a technique that does not use encryption to protect the anonymity of the VPN. Ex. 1001 at 2:25-36; *see also* Ex. 1003 at ¶¶193-198. The '135 patent also shows a particular type of VPN – one using "TARP" routers – that does use encryption (Ex. 1001 at 2:66-3:29) but indicates this scheme is not mandatory in the DNS-based VPN schemes it claims. *See, e.g.*, Ex. 1001 at 38:2-5 ("The VPN is **preferably** implemented using the IP address "hopping" features of the basic invention described above…"). The '135 disclosure also does not show any explicit encryption steps for DNS-related VPN schemes. *See* Ex. 1001 at 37:17-40:13. In February of 2000, it was understood a VPN could be established without encryption; namely, by using "obfuscation" or

hiding techniques to ensure the security and anonymity of the network traffic over the public network. *See* Ex. 1003 at ¶¶193-198.

Second, Patent Owner disputed in concurrent litigation that the claims require computers in a VPN to "**directly communicate** with each other." *See, e.g.*, Ex. 1046 at 1-3. In the August 2010 litigation, the Court found that Patent Owner had **disclaimed** from the literal scope of the '135 claims VPNs that do not involve "direct communications" between the involved computers. Ex. 1043 at 6; *see also* Ex. 1046 at 6-9; Ex. 1048 at 5-7. The Court specifically relied on Patent Owner's representations to the Office during the '269 reexamination proceeding involving the '135 patent to make this determination – it found that Patent Owner had asserted the '135 claims were not anticipated by the Aventail systems because "computers connected according to Aventail **do not communicate directly with each other**." 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. 1043 at 8 (FN2).

The Court thus determined that a **portion of the literal scope** of the '135 patent claims **has been disclaimed** (*i.e.*, that portion covering VPNs in which computers do not "directly" communicate). The logical consequence of that determination is that the claims in **their broadest reasonable construction** still encompass this disclaimed subject matter. Patent Owner's prosecution disclaimer

– which is plainly effective in a district court proceeding to limit the claims because the claims cannot be amended in that proceeding – should not be given weight in this proceeding under the broadest reasonable construction standard. *See, 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**. During examination, the claims must be interpreted as broadly as their terms reasonably allow"). Instead, in this proceeding, Patent Owner must amend the claims to exclude subject matter it has disclaimed. The broadest reasonable construction of "VPN" thus encompasses "a network of computers which privately communicate – directly or otherwise – with each other on insecure paths between the computers where the communication is both secure and anonymous, where the data transferred may or may not be encrypted."

This also demonstrates that the literal scope of the claims (disregarding Patent Owner's disclaimer) encompass what the Office found to be described in Aventail (Ex. 1007). Aventail also describes VPNs in which computers communicate "directly" pursuant to the Court's construction. *See* § IV.A.1, *below*.

2. Virtual Private Link (Claim 13)

The '135 patent does not define the term "**virtual private link.**" Patent Owner has asserted a "virtual private link" is "a communication link that permits computers to privately communicate with each other by encrypting traffic on insecure communication paths between the computers." Ex. 1043 at 8. The Court, however, found this term means the same thing as a VPN. Ex. 1043 at 8-9 ("the Court construes 'virtual private link' as 'a virtual private network as previously defined.'"). Consequently, Petitioner submits the same construction should be used for "virtual private link" as is used for "virtual private network."

3. Domain Name (Claims 1, 10, 13, 18)

The '135 patent does not define the term "**domain name.**" Patent Owner has asserted a "domain name" means "a name corresponding to an IP address." Ex. 1046 at 14-15. The broadest reasonable construction of this "domain name" should include Patent Owner's proposed definition.

4. Domain Name Service (Claims 1, 10, 13, 18)

The '135 patent does not define the term "**domain name service.**" Patent Owner has asserted a "domain name service" is "a lookup service that returns an IP address for a requested domain name." Ex. 1046 at 13-14. A domain name service performs domain name resolution according to Internet standards, namely, RFC 1034 (Ex. 1016) and RFC 1035 (Ex. 1017). Ex. 1003 at ¶¶116-117. Under these standards, an IP address will not always be returned – an **error** also may be

returned. Ex. 1003 at ¶¶116-125. The broadest reasonable construction of "domain name service" thus includes "a lookup service that will return an IP address or an error code in response to a domain name resolution request."

5. DNS Server (Claims 18, 2 and 8)

The '135 patent does not define the term "**DNS Server.**" The '135 patent indicates that when this term is used, it is being used generally as a "server" that returns an IP address in response to a request containing a domain name. *See* Ex. 1003 at ¶210-216. As noted in § 4, a domain name service also may return an error. The broadest reasonable construction of "DNS server" thus includes "a computer or computer-based process that will return an IP address or an error code in response to a domain name resolution request."

6. DNS Proxy Server (Claims 10, 8)

The '135 patent does not define the term "**DNS proxy server.**" It does discuss features of a "DNS Proxy Server." For example, it explains a DNS proxy server may distribute its functions across multiple computers and processes. *See* Ex. 1003 at ¶219 (citing to Ex. 1001 at 38:23-53). Patent Owner also has asserted a "DNS proxy server" is "a computer or program that responds to a domain name inquiry in place of a DNS." Ex. 1046 at 16-17. The broadest reasonable construction of a "DNS Proxy Server" thus includes "one or more computers or

processes that individually or collectively respond to a domain name inquiry in place of a DNS server."

7. Web Site (Claims 1, 10, 18)

The '135 patent does not define the term "**web site.**" Patent Owner asserted a "web site" means "a computer associated with a domain name and that can communicate in a network." Ex. 1046 at 21-22. The broadest reasonable construction of "web site" should include Patent Owner's construction.

8. Secure Web Site/Target Web Site (Claims 1, 8, 10, 18)

The '135 patent does not define the terms "**secure web site**" or "**secure target web site.**" Patent Owner has asserted a "secure web site" means "a computer associated with a domain name and that can communicate in a virtual private network." Ex. 1046 at 21-22. Patent Owner proposed a similar definition for a "secure target web site"; namely, "a target computer associated with a domain name and that can communicate in a virtual private network." Ex. 1046 at 21-22. The broadest reasonable construction of these terms should include Patent Owner's proposed constructions for each term.

9. Secure Web Computer (Claim 10)

The '135 patent does not define the term "**secure web computer.**" Patent Owner has asserted that a "secure web computer" means "a computer that requires authorization for access and that can communicate in a virtual private network."

Ex. 1046 at 22-24. The broadest reasonable construction of "secure web computer**"** should include the Patent Owner's proposed construction.

10. Target Computer (Claims 1, 10, 18)

The '135 patent does not define the term "**target computer.**" Patent Owner has asserted this term can mean "a computer with which the client computer seeks to communicate." Ex. 1046 at 24-25. The broadest reasonable construction of this term should include Patent Owner's proposed construction.

11. IP Address Hopping Scheme (Claim 6)

The '135 patent does not define the term "IP address hopping scheme." It does refer to a variety of schemes that route traffic through intermediary network devices according to a pre-defined scheme as "IP hopping schemes." *See, e.g.*, Ex. 1001 at 5:30-64, 14:59-16:15. These schemes use a wide variety of routing concepts and strategies. The broadest reasonable construction of "IP address hopping scheme" thus encompasses any type of scheme that routes IP traffic from a client to the destination through intermediary devices.

IV. Precise Reasons for Relief Requested

A. Claims 1-10, 12-15 and 18 Are Anticipated By U.S. Patent No. 6,496,867 to Beser et al. (Beser).

Beser has an effective filing date of August 27, 1999, and is prior art under at least under §102(e). A concise summary of the systems and processes described in Beser is provided at ¶¶299-613 of Ex. 1003.

1. Beser Anticipates Claim 1

Beser describes processes that automatically and transparently establish an IP tunneling association between two end devices with the aid of a first and second network device and a trusted-third-party network device on a public network. Ex. 1003 at ¶¶299-304. In the Beser schemes, an originating end device is on a local network that is connected to the public network via a first network device. Ex. 1003 at ¶¶304-305, 314-320. Similarly, the terminating end device is on a different local network that is connected to the public network by a second network device. *Id.* Beser shows that the trusted-third-party network device may be a DNS server. Ex. 1003 at ¶¶306, 320-324. Beser also teaches that IP traffic sent over the public network in an IP tunneling association ordinarily is encrypted. *See* Ex. 1003 at ¶¶311-313, 358-365. Beser therefore shows "*[a] method for transparently creating a virtual private network (VPN) between a client computer and a target computer*." Ex. 1003 at ¶¶425-430; *see generally* Ex. 1003 at ¶¶170-185.

In the Beser schemes, an originating device sends a request containing a domain name associated with a terminating device to the first network device. Ex. 1003 at ¶¶330-334. The first network device then forwards the request to the trusted-third-party network device. Ex. 1003 at ¶¶330, 335. Beser thus describes a process that includes a step of "*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." Ex. 1003 at ¶¶431-433.

Beser shows that after receiving a request, the trusted-third-party network device compares the unique identifier in a request (*e.g.*, a domain name) to an internal database of users or end devices. Ex. 1003 at ¶¶334-337. If there is a match, the trusted-third-party network device initiates a tunneling association. Ex. 1003 at ¶¶337, 340-342. Beser thus describes a process including a step of "*determining whether the DNS request transmitted in step (1) is requesting access to a secure web site*." Ex. 1003 at ¶¶434-439.

To establish an IP tunnel, the trusted-third-party network device will negotiate private IP addresses for the first and second network devices to use when transmitting data between the end devices across the public network. Ex. 1003 at ¶¶342-345. This process occurs without any interactions or further action from the user or end device that originally made the request. Ex. 1003 at ¶¶299-304, 340. Beser teaches that IP traffic sent over the public network in an IP tunneling association ordinarily is encrypted. Ex. 1003 at ¶¶311-313, 358-365. Beser thus describes a process which includes a step of "*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*." Beser

thus describes a process having all the steps specified in claim 1. Ex. 1003 at ¶¶440-442.

2. Beser Anticipates Claim 10

As explained in § 1 above, Beser describes systems and processes that automatically and transparently establish a tunneling association between two end devices with the aid of a first and second network device and a trusted-third-party network device on a public network. *See* Ex. 1003 at ¶¶299-304. Beser teaches that IP traffic sent over the public network in an IP tunneling association ordinarily is encrypted. *See* Ex. 1003 at ¶¶311-313, 358-365. Beser thus discloses a "*system that transparently creates a virtual private network (VPN) between a client computer and a secure target computer*." Ex. 1003 at ¶¶505-510; *see generally* Ex. 1003 at ¶¶170-185.

In the Beser schemes, an originating device sends a request containing a unique identifier (*e.g.*, a domain name) to the first network device. Ex. 1003 at ¶¶330-334. The first network device then forwards the request to the trusted-third-party network device. Ex. 1003 at ¶¶330, 335. If the unique identifier (*e.g.*, domain name) is not one that will cause negotiation of a tunneling association, the trusted-third-party network device inherently will return the corresponding IP address. Ex. 1003 at ¶¶320-322, 334, 338-339; *see* Ex. 1003 at ¶¶102-114.

Beser shows that the trusted-third-party network device may comprise a DNS server, and further explains the functions of the device can be distributed over multiple devices. Ex. 1003 at ¶¶306, 323; *see* Ex. 1003 at ¶¶82-107. In the Beser schemes, a request from an end device specifying a remote destination (*e.g.*, a VOIP device on a different private network) will be received by a first network device (*e.g.*, a gateway device, such as an edge router) and automatically forwarded to a trusted-third-party network device as appropriate for evaluation and handling. Ex. 1003 at ¶¶316-319; *see* Ex. 1003 at ¶¶77-80. The first network device, thus, acts as a proxy for the request, and is a "DNS proxy server" within the meaning of claim 10. *See* § III.C.6. It also was well-known that such configurations would include a recursive DNS server or a DNS resolver. Ex. 1003 at ¶¶106-114, 320-325. A DNS resolver is a proxy server that contacts DNS name servers to resolve a domain name for a client. Ex. 1003 at ¶¶106-114, 321-324. Thus, a person of ordinary skill would have recognized that the trusted-third-party device system in Beser includes a DNS proxy server and that server would be able to resolve standard DNS requests. Ex. 1003 at ¶¶106-114, 320-325. Beser shows that if a request includes a domain name that specifies a secure destination, the trusted-third-party network device will securely negotiate a tunneling association for the first and second network devices to use when transmitting data between the end devices across the public network. Ex. 1003 at ¶¶340-345. Beser thus shows

"*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 name if it is determined that access to a non-secure web site 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*." Ex. 1003 at ¶¶511-521.

In negotiating the tunneling association, the trusted-third-party network device allocates private IP addresses and necessarily allocates resources between the first and second network devices. Ex. 1003 at ¶¶341-344. Similarly, the first and second network devices are "gateway" computers that allocate resources by receiving and evaluating requests from end devices and by routing traffic to destinations on the private network. Ex. 1003 at ¶¶316-319, 325, 347; *see* Ex. 1003 at ¶¶77-80. Beser thus describes a system having a "*gateway 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*." Beser thus describes systems having all the elements specified in claim 10. Ex. 1003 at ¶¶522-525.

3. Beser Anticipates Claim 13

Beser explains that its systems ordinarily should be configured to require a user to authenticate before initiating a tunneling association such as a VOIP connection. Ex. 1003 at ¶¶336, 348-353. For example, it was common for authentication to automatically be handled, such as by caching the user's credentials or through use of a certificate. Ex. 1003 at ¶¶349-350; *see* Ex. 1003 at ¶¶137-147. Beser also explains that the trusted-third-party network device will determine whether to initiate a tunneling association by comparing the unique identifier in a request (*e.g.*, a domain name) against an internal database. Ex. 1003 at ¶¶335-337. Beser shows that the trusted-third-party network device can initiate connections between multiple end devices. Ex. 1003 at ¶308. Beser thus shows "*A method of establishing communication between one of a plurality of client computers and a central computer that maintains a plurality of authentication tables each corresponding to one of the client computers*…" Ex. 1003 at ¶¶540-545.

Beser shows that the end devices would generate requests to make a connection to either Internet destinations or other end device destinations (*e.g.*, other VOIP devices). Ex. 1003 at ¶¶331-335, 339-340. These requests would be sent to and received by the trusted-third-party networking device. *Id.* Beser thus shows a process including the step of "*in the central computer, receiving from one*

of the plurality of client computers a request to establish a connection." Ex. 1003 at ¶¶546-549.

Beser shows that a user can be required to authenticate itself to present a connection request to the trusted-third-party networking device. Ex. 1003 at ¶¶336, 348-353; *see* Ex. 1003 at ¶¶137-147. A trusted-third-party network device inherently will use locally stored values to perform authentication of the user. Ex. 1003 at ¶138. Beser thus shows a method including the step of "*authenticating, with reference to one of the plurality of authentication tables, that the request received in step (1) is from an authorized client*." Ex. 1003 at ¶¶550-552.

Beser describes systems and processes that automatically and transparently establish a tunneling association between two network devices with the aid of a trusted-third-party network device on a public network. Ex. 1003 at ¶¶299-304. Beser teaches that IP traffic sent over the public network in an IP tunneling association ordinarily is encrypted. Ex. 1003 at ¶¶311-313, 358-365. In negotiating the tunneling association, the trusted-third-party network device allocates private IP addresses and necessarily allocates resources between the first and second network devices. Ex. 1003 at ¶¶341-344. Also, the first and second network devices are "gateway" computers that allocate resources by receiving and evaluating requests from end devices and by routing traffic to destinations on the private network. Ex. 1003 at ¶¶316-319, 325, 347; *see* Ex. 1003 at ¶¶77-80. Beser

thus shows a process including the step of "*responsive to a determination that the request is from an authorized client, allocating resources to establish a virtual private link between the client and a second computer*." Ex. 1003 at ¶¶553-559; *see generally* Ex. 1003 at ¶¶170-185.

Beser shows that secure communications will flow between the end devices (*e.g.*, a VOIP call) after the client has successfully established the tunneling association. *See* ¶346. Beser thus shows a method with the step of "*communicating between the authorized client and the second computer using the virtual private link.*" Beser thus show a process meeting every element of claim 13. Ex. 1003 at ¶¶560-561.

4. Beser Anticipates Claim 18

As explained in § 1 with respect to claim 1, Beser describes processes that automatically and transparently establish a tunneling association between two end devices with the aid of a first and second network device and a trusted-third-party network device on a public network. Ex. 1003 at ¶¶299-304. Beser teaches that IP traffic sent over the public network in an IP tunneling association ordinarily is encrypted. Ex. 1003 at ¶¶311-313, 358-365. Beser therefore shows "*A method of transparently creating a virtual private network (VPN) between a client computer and a target computer*." Ex. 1003 at ¶¶578-583; *see generally* Ex. 1003 at ¶¶170-185.

In Beser's schemes, an originating device sends a request containing a domain name associated with a terminating device to the first network device. Ex. 1003 at ¶¶330-334. The first network device then forwards the request to the trusted-third-party network device. Ex. 1003 at ¶¶330, 335. Beser thus describes a process that includes a step of "*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*." Ex. 1003 at ¶¶584-586.

After receiving a request, the trusted-third-party network device compares the domain name to an internal database of users or end devices. Ex. 1003 at ¶¶334-337. If there is a match, the trusted-third-party network device initiates a tunneling association. Ex. 1003 at ¶¶337, 340-342. Beser thus describes a process including a step of "of "*determining whether the DNS request transmitted in step (1) is requesting access to a secure web site*." Ex. 1003 at ¶¶587-592.

If the domain name matched an entry in the database, the trusted-third-party network device automatically initiates a tunneling association by negotiating private IP addresses. Ex. 1003 at ¶¶337, 340-345. The tunneling association shown in Beser securely transmits network traffic between the first and second network devices. Ex. 1003 at ¶¶307-313, 344-345. Beser thus shows a process including the step of "*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." Ex. 1003 at ¶¶593-595.

Beser explains the trusted-third-party network device is located at a different network location relative to the other network devices. Ex. 1003 at ¶¶304-306. Beser thus shows a process where "*steps (2) and (3) are performed at a DNS server separate from the client computer.*" Ex. 1003 at ¶¶596-598.

Beser explains its systems may be configured to require a user to authenticate before initiating a tunneling association. Ex. 1003 at ¶¶336, 348-352. It was common in February 2000 to configure authentication processes to automatically cache the user's credentials or to use a certificate. Ex. 1003 at ¶¶349-350; *see* Ex. 1003 at ¶¶137-147. The trusted-third-party network device will determine whether to initiate a tunneling association by comparing the domain name against an internal database. Ex. 1003 at ¶¶335-337. The trusted-third-party network device also can initiate connections between many different end devices. Ex. 1003 at ¶308.

As explained in § 1 above Beser shows that the trusted-third-party network device may be a DNS server. Ex. 1003 at ¶306, 320-324. If the trusted-third-party network device cannot resolve a domain name because the name is not recognized or the user is not authenticated, it inherently will return an error message to the user. Ex. 1003 at ¶¶320-322, 352; *see* Ex. 1003 at ¶¶116-125. Beser thus shows a

process where "*prior to automatically initiating the VPN between the client computer and the target computer, determining whether the client computer is authorized to resolve addresses of non secure target computers and, if not so authorized, returning an error from the DNS request*." Ex. 1003 at ¶¶599-603. Beser thus shows a process meeting every element of claim 18.

5. Beser Anticipates Claim 2

Beser explains the trusted-third-party network device is located on a public network at a different network location relative to the other network devices. Ex. 1003 at ¶¶304-306. Beser thus shows a process where "*steps (2) and (3) are performed at a DNS server separate from the client computer*." Ex. 1003 at ¶¶449-451.

6. Beser Anticipates Claim 3

In the Beser schemes, an originating device sends a request containing a domain name to the trusted-third-party network device. Ex. 1003 at ¶¶331-335. If the domain name is not one that will cause negotiation of a tunneling association, the trusted-third-party network device inherently will return the corresponding IP address. Ex. 1003 at ¶¶320-322, 338-339; *see* Ex. 1003 at ¶¶82-125. Beser thus shows a process including the step of "*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." Ex. 1003 at ¶¶452-456.

7. Beser Anticipates Claims 4 and 12

Beser explains that the trusted-third-party network device may be configured to require a user to be authenticated before it will evaluate a request from that user containing a domain name. Ex. 1003 at ¶¶336, 348-352. It was common for authentication to automatically be handled, such as by caching the user's credentials or through use of a certificate. Ex. 1003 at ¶¶349-350; *see* Ex. 1003 at ¶¶137-147. Beser also shows that if it is determined the client has not successfully authenticated with the trusted third network device, a domain name will not be resolved and a tunneling association will not be initiated. Ex. 1003 at ¶352. If a domain name cannot be resolved, an error message will be returned. Ex. 1003 at ¶¶320-322, 352; *see* Ex. 1003 at ¶¶116-125.

Beser thus shows a process in which "*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*" pursuant to claim 4. Ex. 1003 at ¶¶461-464.

Beser also discloses processes that include "*the system of claim 10, wherein the gatekeeper 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" which anticipates claim 12. Ex. 1003 at ¶¶533-537.

8. Beser Anticipates Claim 5

As explained above (§ 4), Beser shows that a trusted-third-party network device may be configured to require a user to authenticate before processing a request from that user containing a domain name. Ex. 1003 at ¶336. Beser also explains that a domain name will not be resolved if it is determined that the client has not successfully authenticated with the trusted third network device. Ex. 1003 at ¶¶348-352. If a domain name cannot be resolved, an error message will be returned. Ex. 1003 at ¶352; *see* Ex. 1003 at ¶¶116-125. Beser thus discloses processes where "*step (3) comprises 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 resolve addresses of non secure target computers and, if not so authorized, returning an error from the DNS request*," as specified in claim 5. Ex. 1003 at ¶¶466-470.

9. Beser Anticipates Claims 6 and 14

Beser shows a process where the source and destination IP addresses are modified and changed for transmission over the public network to obfuscate the identities of the end devices. Ex. 1003 at ¶¶307-310, 344-347. Beser thus shows

processes that include "*[t]he method of claim 1, wherein step (3) comprises the step of establishing the VPN by creating an IP address hopping scheme between the client computer and the target computer,*" as specified in claim 6. Ex. 1003 at ¶¶307-310, 344-347, 479-480.

Because this process changes at least one field in the IP packet, Beser also shows a process that includes the step of "*communicating according to a scheme by which at least one field in a series of data packets is periodically changed according to a known sequence,*" as specified in claim 14. Ex. 1003 at ¶¶307-310, 344-347, 568-569.

10. Beser Anticipates Claim 7

Beser describes a process in which a trusted-third-party network device is used to negotiate the establishment of an IP tunnel. Ex. 1003 at ¶¶299-304. In this process, the trusted-third-party network device allocates private IP addresses and necessarily allocates resources between the first network device and the second network device. Ex. 1003 at ¶342. The first and second network devices shown in Beser may be edge routers ("gateway computers"). Ex. 1003 at ¶318; *see* Ex. 1003 at ¶¶77-80. Edge routers inherently allocate resources because they evaluate requests from end devices and route traffic to destinations on the private network. Ex. 1003 at ¶¶316-319, 325, 347. Beser therefore describes processes that include the step of *"using a gatekeeper computer that allocates VPN resources for*

communicating between the client computer and the target computer," as specified in claim 7. Ex. 1003 at ¶¶486-489.

11. Beser Anticipates Claim 8

Beser shows that the trusted-third-party network device may be a DNS server, and further explains the functions of the device can be distributed over multiple devices. Ex. 1003 at ¶¶306-323. As explained in respect to claim 10 (§ 2), it was well-known that such configurations would include a recursive DNS server and a DNS resolver. The DNS resolver acts a proxy server, and resolves domain names by iteratively passing the request to DNS name servers on behalf of a client. Ex. 1003 at ¶¶106-114, 321-324. Thus, a person of ordinary skill would have recognized that the trusted-third-party device system in Beser include a DNS proxy server and that server would be able to resolve standard DNS requests by passing them on to DNS name servers. Ex. 1003 at ¶¶106-114, 321-324. Beser thus discloses processes that include "*[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*," as specified in claim 8. Ex. 1003 at ¶¶490-495.

12. Beser Anticipates Claim 9

As explained above (§ 4), Beser shows that a trusted-third-party network device may be configured to require a user to authenticate before processing a

request from that user containing a domain name. Ex. 1003 at ¶¶336, 348-352. Inherent in that process is sending a message to the client to request credentials. Ex. 1003 at ¶¶350, 501; *see* Ex. 1003 at ¶¶137-147. Beser thus discloses processes that render obvious "*the step of transmitting a message to the client computer to determine whether the client computer is authorized to establish the VPN target computer*," as specified in claim 9. Ex. 1003 at ¶¶500-502.

13. Beser Anticipates Claim 15

In the Beser scheme, the first and second network devices establish an IP tunnel by modifying the source and destination IP addresses in each packet that gets routed through them. Ex. 1003 at ¶¶345, 347. Beser shows that an incoming IP address in a header of a data packet is compared to a table of valid IP addresses maintained in a second computer (*i.e.*, the second network device). Ex. 1003 at ¶347. Thus, Beser discloses processes that include the step of "*comparing an Internet Protocol (IP) address in a header of each data packet to a table of valid IP addresses maintained in a table in the second computer*," as specified in claim 15. Ex. 1003 at ¶¶575-577.

B. Beser Considered with RFC 2401 Renders Obvious Claims 1-10, 12-15, and 18

Patent Owner may contend that Beser does not anticipate claims 1-10, 12-15, and 18 of the '135 patent for certain reasons, noted below. Even if those contentions were accepted, a person of ordinary skill in the art would have

considered the processes and systems defined by claims 1-10, 12-15 and 18 to have been obvious in February of 2000 based on the guidance in RFC 2401, alone or in conjunction with Hoke, Blum or Aventail, for the reasons set forth below. Ex. 1003 at ¶¶366-372.

Initially, Beser would have been considered in conjunction with the guidance in RFC 2401. For example, Beser explains its IP tunneling schemes are compliant with standards-based processes and techniques, and are to be implemented using pre-existing (legacy) equipment and systems. Ex. 1003 at ¶¶307, 320-322, 371. Beser also specifically refers to the IPSec protocol, described in RFC 2401, as being the typical way that IP tunneling schemes are established. Ex. 1003 at ¶¶312-313, 360. The common topics and this specific reference in Beser to RFC 2401 would have led the person of ordinary skill to consider the two references in conjunction. Ex. 1003 at ¶¶312-313, 360, 443-446. Consequently, a person of ordinary skill would have looked to combine elements of those references to improve the functionality of systems shown in each. Ex. 1003 at ¶371.

RFC 2401 explains the IPSec protocol is used to provide automatic encryption and encapsulation of VPN traffic as it is sent through security gateways over a public network. Ex. 1003 at ¶¶373-383. RFC 2401 explains that IP traffic is evaluated and the necessary encryption is added to the appropriate packets. Ex.

1003 at ¶¶377-379. RFC 2401 also explains that, for each tunneling security association, an IPSec header is added to each IP packet (*i.e.*, the packet is placed inside of another packet with an IPSec IP header). Ex. 1003 at ¶¶158, 376-378, 384. RFC 2401 also shows use of nested VPN connections that are sent through multiple gateways. Ex. 1003 at ¶¶384-388. As IP packets are passed through each gateway in a nested connection, the outer IP header is added or stripped off before forwarding the packets to the next gateway. Ex. 1003 at ¶¶380, 388. As a result, the source and destination IP addresses change in packets constituting the VPN traffic as that traffic passes through each gateway. Ex. 1003 at ¶388.

A person of ordinary skill also would have recognized that IPSec could be readily integrated into the Beser systems. Ex. 1003 at ¶¶312, 366-372, 381, 383, 443-446. For example, Beser describes systems that use edge routers and gateways as intermediaries in transmitting traffic over tunneling associations, which is one of the precise network designs described in RFC 2401. Ex. 1003 at ¶¶380, 381, 383; *see* Ex. 1003 at ¶¶77-80. A person of ordinary skill also would have recognized that the nested VPN system described in RFC 2401 would improve the security of the Beser systems by further obfuscating the identity of the communicating devices. Ex. 1003 at ¶¶384-388.

1. Claims 1, 10, 13 and 18 Would Have Been Obvious

Patent Owner may contend that Beser does not describe the automatic encryption of all IP packets sent through an IP tunnel, and thus, does not show creation of a VPN or a virtual private link. As explained above in § A.1, above, Beser expressly describes use of encryption in its IP tunneling solutions. First, it shows use of encryption to shield the traffic between the trusted-third-party network device and the first and second networks during establishment of the secure IP tunnel. Ex. 1003 at ¶¶348, 365. Second, it explains that encryption is ordinarily used in IP tunnels other than in two specific situations involving high volume data transfers and equipment that cannot handle encryption of the traffic. Ex. 1003 at ¶¶358-365.

This purported distinction, even if established, would been considered an obvious design variation of the Beser schemes. First, the obvious and common sense solution to the capacity problem identified by Beser associated with sending high volumes of IP traffic (*e.g.*, VOIP or multimedia data) over a VPN would be to either use more powerful edge routers or gateway computers that could handle the added computational demands of encrypting that volume of data, or to reduce the quality of the voice call or multimedia data, which would decrease the amount of data that would have to be encrypted. Ex. 1003 at ¶¶446-447. Each of those

would resolve the practical "problem" Beser identifies with sending high volumes of encrypted IP traffic through a VPN. *Id.*

Second, it would have been obvious to automatically encrypt all network traffic being sent over the Beser IP tunnels based on the combined teachings of Beser and RFC 2401. Ex. 1003 at ¶¶369, 381-383, 443-447. Beser explains IPSec is typically used to encrypt traffic sent through an IP tunnel. Ex. 1003 at ¶¶312-313. The IPSec protocol (RFC 2401) shows use of automatic encryption of all traffic sent over secure IP tunnels in precisely the same network configuration described in Beser (*i.e.*, network devices on private networks communicating through a tunnel established between edge routers over the Internet). Ex. 1003 at ¶¶380-383; *see also id.* at ¶¶374-380. RFC 2401 also explains its schemes are granular and modular, and can be adjusted based on the needs presented by any particular implementation. Ex. 1003 at ¶¶313, 382-383. Thus, a person of ordinary skill would have considered it obvious to modify the Beser scheme to provide for encryption of all IP traffic in the Beser IP tunneling schemes. Ex. 1003 at ¶¶443-447. To the extent claims 1, 10, 13 or 18 are found not anticipated by Beser based on this purported distinction, a person of ordinary skill in the art would have considered each of claims 1, 10, 13 and 18 to have been obvious based on Beser in view of RFC 2401. Ex. 1003 at ¶¶443-447, 526, 562, 606; *see also* §§ A.1-A.4, respectively, above.

2. Dependent Claims 2-9, 12, 14 and 15

Beser describes systems or processes meeting the requirements of each of dependent claims 2-9, 12, 14 and 15, as explained above at §§ A.5-A.13, above. The combined teachings of Beser and RFC 2401 would have rendered obvious the encryption of all IP traffic sent in an IP tunnel as described in Beser, for the reasons set forth in § B.1, above. Because Beser itself describes systems and processes meeting the requirements of each of claims 2-9, 12, 14 and 15, each of those claims would have been considered obvious in February of 2000 by a person of ordinary skill based on the combined teachings of Beser and RFC 2401 for the same reasons presented in §§ A.5-A.13, above.

3. Dependent Claims 6 and 14

As explained above in § A.9, Beser anticipates claims 6 and 14, and would have been considered obvious based on Beser in view of RFC 2401 in February of 2000 for the reasons set forth above in § B.2. Patent Owner may contend Beser does not describe "IP hopping" schemes specified in claim 6 or schemes wherein "at least one field in a series of data packets is periodically changed according to a known sequence" pursuant to claim 14. Any such distinction between claims 6 and 14 and the Beser schemes, if established, would not have rendered either of these claims patentable to a person of ordinary skill in February of 2000.

As explained above, Beser teaches that IPSec is typically used to encrypt IP tunnels, of which its scheme is one. Ex. 1003 at ¶¶311-313, 360, 362. Beser also specifically references the IPSec protocol that is the subject of RFC 2401. Ex. 1003 at ¶¶312, 362. RFC 2401 shows used of a variety of secure networking designs, including one (*e.g.*, Case 3) that is identical to that described in Beser. Ex. 1003 at ¶¶374, 380-383. RFC 2401 also explains that the IPSec protocol is designed allow multiple and varied combinations of security associations, which can be used create "iterated" or "nested" security associations between pairs of points in an overall path of network traffic. Ex. 1003 at ¶¶384-388. In this iterated hopping design, each successive gateway through which VPN traffic is routed will add or strip off an outer IP header before forwarding the packet to the next gateway, whose destination is known. Ex. 1003 at ¶¶387-388. These nested tunnel schemes necessarily use a predefined path, at least with regard to successive hops in the path. Ex. 1003 at ¶¶388-389, 481, 570.

RFC 2401 would have suggested modifying the Beser IP tunneling scheme to incorporate nested or iterated tunneling designs to increase security of the tunneling traffic. *Id.* Beser considered in view of RFC 2401, thus, would have made obvious the use of a nested IP tunnels, which are an "*IP hopping scheme*" according to claim 6. Ex. 1003 at ¶¶481-485; *see* § III.C.11. Beser in view of RFC 2401, thus, would have rendered obvious claim 6.

In addition, the nesting schemes specifically suggested by the combination of Beser in view of RFC 2401 would also yield designs in which "*at least one field in a series of data packets is periodically changed according to a known sequence*" as specified in claim 14. Ex. 1003 at ¶¶570-574. For example, the nested VPN schemes will change a least one field in a series of data packets (*i.e.*, the source and destination IP addresses) periodically according to a known sequence. Ex. 1003 at ¶¶387-389, 570-574. Beser in view of RFC 2401, thus, would have rendered obvious claim 14.

C. Beser in View of Blum Renders Obvious Claims 3, 5, 8, 10, 12, and 18

Claims 3, 5, 8, 10, 12, and 18 are anticipated by Beser for the reasons set forth in §§A.1 to A.13, above. Patent Owner may contend that the schemes described in Beser do not satisfy certain of the provisions in independent claims 10 and 18, and dependent claims 3, 5 and 8 (depending from claim 1). These provisions generally relate to steps where a determination is made that a request is specifying a "non-secure" website. If it is determined that claims 3, 4, 8, 10 or 18 are not anticipated by Beser due to these provisions, the distinction between each claim relative to Beser would not have been considered patentable to a person of ordinary skill in the art in February of 2000 based on the guidance in Blum (Ex. 1011) for the reasons set forth below.

1. Claim 10, and Claims 3 and 8 Would Have Been Obvious

Independent claim 10, and dependent claims 3 and 8 (from claim 1) each specify that if the process or system determine if the domain name in a request is not specifying a "secure" destination, then the domain name will either be directly resolved into an IP address, or will be "passed through" for name resolution by a DNS server. Specifically:

- Claim 10 specifies that, in response to receipt of "*a request to look up an IP address for a domain name*," the "*the DNS proxy server returns the IP address for the requested domain name if it is determined that access to a non-secure web site has been requested*";
- Claim 3 specifies the process of Claim 1 includes the step of "*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*"; and
- Claim 8 specifies "*step (2)* [of Claim 1] *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.*"

Each of these claims, thus, envisions a process where, if a determination is made that the destination of a request containing a domain name is not a secure

destination requiring a VPN, the request is "passed through" or handled like a normal domain name resolution request.

Blum describes use of a DNS proxy scheme that automatically and transparently intercepts connection requests from a client application, evaluates the domain name in the request, and takes actions dependent on the value of the domain name. Ex. 1003 at ¶¶325-326, 405-408. More specifically, Blum describes a DNS proxy server that determines if a domain name in a connection request requires proxying to a remote server for handling, and if not, can either locally resolve the domain name or send it to a public DNS server for resolution. Ex. 1003 at ¶¶407-410. Blum also explains the DNS proxy server can be configured (*e.g.*, using "protocol filters") to establish a connection to a remote server based on the value of the domain, and to apply various security and monitoring services based on the content of a request. Ex. 1003 at ¶¶409-411. Blum teaches that if the proxy cannot resolve a domain name, an error message is returned to the client. Ex. 1003 at ¶410.

In February of 2000, a person of ordinary skill would have considered the guidance in Beser and Blum together. For example, the Beser schemes use a trusted-third-party network device that, in one embodiment, can be a "DNS proxy server." Ex. 1003 at ¶¶306, 320-324; *see* Ex. 1003 at ¶¶77-80. This device is a server to which traffic is redirected, it functions to resolve domain names, and

routes connections based on the domain specified in a request. The Blum reference similarly describes capabilities and the design of DNS proxy servers, particularly ones that are designed to route connection requests based on the domain name value specified in the request. Ex. 1003 at ¶¶320-326, 408, 412. The schemes described in Beser and Blum are thus closely analogous. Ex. 1003 at ¶¶372, 412.

To the extent that Beser is found to not expressly teach that destinations requesting non-secure names are resolved by the trusted-third-party network device using standard DNS resolution protocols (*e.g.*, as specified in RFC 1035 (Ex. 1017)), providing for this capability would have been expressly suggested by Blum. Ex. 1003 at ¶¶370, 457-460, 457-460, 471-474, 529-532. In particular, a person of ordinary skill would have recognized that Blum specifically shows a DNS proxy being configured to route connection requests containing "non-secure" domain names to a local or public DNS server for conventional name resolution. Ex. 1003 at ¶407. The combination of Beser with Blum, thus, would have specifically suggested configuring the trusted-third-party network device to directly resolve a "non-secure" domain name, or to pass through a request containing a non-secure domain name for ordinary name resolution by a public DNS server. Ex. 1003 at ¶¶460, 474, 532. The combination also would have specifically suggested configuring the first network device to forward a "non-

secure" domain name to a local DNS server or a public DNS server for ordinary name resolution. Ex. 1003 at ¶¶412, 474. Consequently, claims 10, 3 and 8 would been considered obvious for the reasons set forth in §§A.2, A.6 and A.11, respectively, in view of the observations set forth above based on the guidance in Blum. Ex. 1003 at ¶¶457-460, 471-474, 529-532.

2. Claim 18 and Claim 5 Would Have Been Obvious

Claim 18 and dependent claim 5 (from claim 1) each specify that "*step (3)* [of claim 18 or claim 1] *comprises 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 resolve addresses of non secure target computers and, if not so authorized, returning an error from the DNS request.*" The processes in claims 1 and 18 thus specify performing a determination whether the client computer is authorized to resolve "non-secure" web sites before performing the step where a VPN would be established (if the domain name were a "secure" domain name).

Including this step in the processes defined by claims 1 and 18 would have been obvious to a person of ordinary skill in the art based on the guidance in Blum (Ex. 1011). The Beser systems describe schemes where a third-party-trusted device functions as a DNS proxy server, and where that device determines whether a domain name in a request sent to it requires establishing a secure IP tunnel. Ex.

1003 at ¶¶306, 323-325. Beser points out that IP packets sent by the first network device to the trusted-third-party network device may require authentication by the trusted-third-party network device, which indicates the device can be configured to require authentication before receiving and acting upon the incoming request. Ex. 1003 at ¶¶348-352, 599; *see* Ex. 1003 at ¶¶137-147.

As noted above in § C.1, Blum describes transparent DNS proxy server schemes that intercept and evaluate connection requests containing domain names. Blum also shows these DNS proxy servers also will perform different actions based on the domain name (*e.g.*, routing names requiring establishing connections to remote servers or directly resolving or sending for resolution by a public DNS server non-secure domain names). Ex. 1003 at ¶¶325-326, 407-411. Blum also shows an example where the DNS proxy server can be configured to return an error if there is a violation of a "protocol filter" used by the DNS proxy server. Ex. 1003 at ¶¶409-410. An obvious example of a protocol filter would be one that checks credentials of an incoming request to determine if it is authorized. Ex. 1003 at ¶¶409, 475, 611; *see* Ex. 1003 at ¶¶140-147.

A person of ordinary skill evaluating Beser in view of Blum would have thus found it obvious to (i) require authentication from a requesting network device at the trusted-third-party network device before receiving or evaluating a domain name in a request, and (ii) to return an error to the requesting device if there were a

"protocol" violation (*e.g.*, a failure to successfully authenticate). Ex. 1003 at ¶¶475, 611; *see id.* at ¶¶140-147.

Patent Owner also may contend that claims 18 and 5 should be read as requiring the DNS proxy server to only require authentication for requests containing "non-secure" domain names. Petitioner observes there is no description of such a scheme in '135 specification. Such an embodiment also would have been considered obvious in February of 2000 based on the combined teachings of Beser and Blum for the same reasons that a scheme requiring authentication before resolution of any domain name request (secure or insecure) would have been considered obvious in view of these two references, for the reasons noted above.

3. Dependent Claim 12

Beser describes systems or processes meeting the requirements of dependent claim 12, as explained above at § A.7. The combined teachings of Beser and Blum would have rendered obvious the inclusion of a DNS proxy server into the Beser scheme, for the reasons set forth in § C.1, above. Because Beser itself describes systems and processes meeting the requirements claim 12, that claim would have been considered obvious in February of 2000 by a person of ordinary skill based on the combined teachings of Beser and Blum for the same reasons presented in § A.7, above.

D. Beser in View of RFC 2401, and Further in View of Blum Renders Claims 3, 5, 8, 10, and 18 Obvious

As noted above, Patent Owner may contend Beser does not anticipate claims 1, 10, 13 or 18 based on its belief that these claims require all IP traffic sent over a VPN to be encrypted, and its belief that this is not described by Beser. Such contentions should be disregarded for the reasons set forth in § C.1, above. Moreover, even if the claims and Beser were construed as Patent Owner may contend, those claims would have been obvious based on Beser considered in view of RFC 2401 for the reasons set forth in § B, above.

The additional potential distinctions Patent Owner may contend exist regarding independent claims 10 and 18 and dependent claim 3, 5 and 8 relative to the systems and processes shown in Beser also would not have been considered sufficient to render these claims patentable, as such claims, even with those distinctions, would have been considered obvious for the reasons set forth in §§ C.1 and C.2, above.

E. Beser in view of Aventail Renders Claims 18 and 5 Obvious

As explained above, Beser describes systems that anticipate claims 1 and 18. Claims 18 and 5 specify that the processes include a "*step of, prior to automatically initiating the VPN between the client computer and the target computer, determining whether the client computer is authorized to resolve addresses of non secure target computers and, if not so authorized, returning an*

error from the DNS request." If this element is found to not be described in Beser, this distinction would not render claims 18 and 5 patentable.

Aventail describes systems for automatically and transparently establishing VPNs based on the domain name in a connection request. Ex. 1003 at ¶¶413-423. The Aventail schemes are analogous to the Beser schemes in that both systems transparently evaluate DNS requests and use the domain name in a request to determine whether to automatically establish VPNs between a client computer and a secure destination. Ex. 1003 at ¶¶370-372, 471-478, 606-613. A person of ordinary skill thus would have considered the teachings in Beser with those in Aventail. *Id.*

Aventail explains that its automatic DNS-based VPN systems can be configured to proxy all connection requests (including those requiring domain name resolution) from a client computer to a DNS proxy server for evaluation and handling. Ex. 1003 at ¶¶415-418. For example, Aventail shows a scheme where, when a "DNS Proxy" option is enabled in the Aventail Connect software on a client computer, all connection requests (including those containing secure or non-secure domain names) not matching a local domain rule will be sent to the DNS proxy server (the Aventail Extranet Server). *Id.* Aventail also explains that the DNS proxy server will require successful authentication before receiving or evaluating the incoming proxied domain name request. Ex. 1003 at ¶¶420-421.

Both Beser and Aventail use DNS and other Internet communication protocols that are based on standards. Ex. 1003 at ¶¶307, 371, 414-417. When these protocols are followed, an error will be returned to a requesting application if a domain name request cannot be resolved (*e.g.*, because a client has not successfully authenticated itself with a proxy server). Ex. 1003 at ¶¶321-322, 421.

Consequently, a person of ordinary skill would have found the idea of requiring authentication at a DNS proxy server before allowing name resolution of an incoming connection request, and returning an error if the user is not authorized to access the proxy server, to have been obvious based on the use of this feature within the Aventail systems and in view of how standardized DNS systems function. Ex. 1003 at ¶¶321-322, 370-372, 471-478, 606-613. Consequently, claims 18 and 5 (dependent from 1), to the extent they are found not anticipated by Beser due to this common feature of claims 18 and 5, would have been considered obvious based on Beser in view of Aventail. Ex. 1003 at ¶¶471-478, 606-613.

F. Beser in view of Hoke Renders Claims 1-10, 12-15, and 18 Obvious

1. Claims 1, 10, 13, and 18 Would Have Been Obvious

As explained above in §§ A.1-A.4, Beser anticipates claims 1, 10, 13, and 18. Patent Owner may contend that Beser does not expressly show the automatic encryption of all IP packets sent over an IP tunnel, and thus, does not show

creation of a VPN or a virtual private link. These distinctions, if established, would not render the claims patentable.

As explained above, Beser indicates that IP packets sent through IP tunnels are ordinarily encrypted. *See* § A.1, above; *see also* § B.1, above. Beser also explains its systems are based on established Internet networking standards. Ex. 1003 at ¶¶307, 321-322, 371. Hoke shows that systems which encrypt all traffic sent through a VPN were well known in February of 2000. Ex. 1003 at ¶¶171-185, 390-404. In particular, Hoke describes systems which automatically and transparently establish VPNs, and which encrypt all VPN traffic being sent between two computers in the VPN over a public network. Ex. 1003 at ¶¶174-178, 390-392; *see* Ex. 1003 at ¶¶77-80.

Consequently, to the extent the encryption of all VPN traffic is not described in Beser, a person of ordinary skill would have considered that modification to have been obvious in February of 2000 based on the combined guidance of Beser and Hoke. Ex. 1003 at ¶¶366-372, 390-392, 402-404, 448. That combination, in turn, would have rendered obvious each of claims 1, 10, 13 and 18, to the extent those claims are found not anticipated by Beser. Ex. 1003 at ¶¶448, 528, 564, 606.

2. Claims 9 and 12 Would Have Been Obvious

As explained above in §§ A.12 and A.7 respectively, Beser anticipates claims 9 and 12. Patent Owner may contend that Beser does not expressly describe

a process that transmits a message to the client computer to determine if it is authorized to establish a VPN (claim 9) or includes a gatekeeper computer that determines whether a client computer is authorized to create a VPN (claim 12). These distinctions, if established, would not render these claims patentable.

As explained above, Hoke describes systems that automatically establish VPNs. Ex. 1003 at ¶¶390-392. In those systems, Hoke shows that authentication of a client computer is required before initiation of a VPN. Ex. 1003 at ¶¶356-357, 392-393, 396-397; *see* Ex. 1003 at ¶¶77-80. Hoke discloses that as a part of a standard authentication process, the VPN unit will issue a challenge (a "message") to an unknown remote client, requiring the remote client to authenticate itself. Ex. 1003 at ¶397; *see* Ex. 1003 at ¶¶137-147. Consequently, a person of ordinary skill would have considered the step of "*transmitting a message to the client computer to determine whether it is authorized to establish the VPN*" as specified in claim 9 to have been obvious based on Beser in view of Hoke in February of 2000. Ex. 1003 at ¶503.

Hoke also teaches that if authentication is successful, a device will be permitted to send traffic through the VPN. Ex. 1003 at ¶¶390-392, 397-398. Logically, if authentication fails, a VPN connection will not be initiated. *Id.* Consequently, a person of ordinary skill would have considered the step of "*determining 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 a VPN" as specified in claim 12 to have been obvious based on Beser in view of Hoke in February of 2000. Ex. 1003 at ¶¶538-539.

3. Claim 13 Would Have Been Obvious

As explained in § A.3, above, Beser anticipates claim 13. Beser in view of Hoke also renders obvious claim 13 if it were not found to anticipate on the basis of encrypting all IP traffic in the VPN. *See* § F.1, above. Patent Owner may additionally contend that Beser does not expressly describe a method that uses "*a central computer that maintains a plurality of authentication tables each corresponding to one of the client computers*." If this distinction were determined to exist between the schemes shown in Beser and claim 13, it would have been considered obvious by a person of ordinary skill in the art based on the combined teachings in Beser and Hoke.

Initially, Beser explains that its trusted-third-party network device may require a client computer to be authenticated. Ex. 1003 at ¶¶336, 348. Authentication of incoming IP packets carrying authentication credentials necessarily will require comparison by the trusted-third-party network device to a pre-existing table of authorized values. Ex. 1003 at ¶¶350, 353. Indeed, using

tables to store data used during authentication processes was a well-known feature of authentication techniques in February of 2000. Ex. 1003 at ¶138.

Hoke describes VPN systems in which VPN routers use lookup tables to determine if a destination is a secure destination and to determine if a client is authorized to access a destination. Ex. 1003 at ¶¶396-398.

To the extent this is not explicitly described in Beser, it would have been obvious to configure the first or second network devices, and/or the trusted-third-party network devices in the Beser schemes to use authentication tables stored on the device to verify that a user was authorized to make a VPN connection to a particular destination, based on the guidance in Hoke showing use of this technique in an analogous system. Ex. 1003 at ¶¶394, 564. For example, such a person would have used tables of values stored at the first or second network device or at the trusted-third-party device to improve the identification and routing of traffic intended for a tunneling association. Ex. 1003 at ¶564. Consequently, a person of ordinary skill would have considered the step of "*authenticating, with reference to one of the plurality of authentication tables, that the request received in step (1) is from an authorized client*" as specified in claim 13 to have been obvious an obvious variation of the Beser schemes based on the guidance in Hoke in February of 2000. Ex. 1003 at ¶564.

4. Dependent Claims 2-8, and 14-15

Beser describes systems or processes meeting the requirements of each of dependent claims 2-8 and 14-15, as explained above at §§ A.5-A.13. The combined teachings of Beser and Hoke would have rendered obvious the encryption of all IP traffic sent in an IP tunnel as described in Beser, for the reasons set forth in § F.1, above. Because Beser itself describes systems and processes meeting the requirements of each of claims 2-8 and 14-15, each of those claims would have been considered obvious in February of 2000 by a person of ordinary skill based on the combined teachings of Beser and Hoke for the same reasons presented in §§ A.5-A.13, above.

G. Beser in view of Hoke and Blum Renders Claims 10, 18, 3, 5, 8, and 12 Obvious

As noted above, Patent Owner may contend Beser does not anticipate claims 1, 10, 13 or 18, or the dependent claims, based on its belief that these claims require all IP traffic sent over a VPN to be encrypted, and its belief that this is not described by Beser. Such contentions should be disregarded for the reasons set forth in § III.C.1, above. Moreover, even if the claims and Beser were construed as Patent Owner may contend, those claims would have been obvious based on Beser considered in view of Hoke for the reasons set forth in § F, above.

The additional potential distinctions Patent Owner may contend exist regarding independent claims 10 and 18 and dependent claims 3, 5, 8, and 12, also would have been considered obvious for the reasons set forth in § C, above.

H. Beser in view of RFC 2401 and Hoke Renders Claims 13, 9, and 12 Obvious

As noted above, Patent Owner may contend Beser does not anticipate claims 1, 10, 13 or 18, or the dependent claims, based on its belief that these claims require all IP traffic sent over a VPN to be encrypted, and its belief that this is not described by Beser. Such contentions should be disregarded for the reasons set forth in § III.C.1, above. Moreover, even if the claims and Beser were construed as Patent Owner may contend, those claims would have been obvious based on Beser considered in view of RFC 2401 for the reasons set forth in § B, above.

The additional potential distinctions Patent Owner may contend exist regarding independent claim 13 and dependent claims 9 and 12, also would have been considered obvious for the reasons set forth in §§ F.2 and F.3, above.

I. Beser in view of RFC 2401 and Aventail Renders Claims 18 and 5 Obvious

As noted above, Patent Owner may contend Beser does not anticipate claims 1, 10, 13 or 18, or the dependent claims, based on its belief that these claims require all IP traffic sent over a VPN to be encrypted, and its belief that this is not described by Beser. Such contentions should be disregarded for the reasons set

forth in § III.C.1, above. Moreover, even if the claims and Beser were construed as Patent Owner may contend, those claims would have been obvious based on Beser considered in view of RFC 2401 for the reasons set forth in § B, above.

The additional potential distinctions Patent Owner may contend exist regarding independent claim 18 and dependent claim 5, also would have been considered obvious for the reasons set forth in § E, above.

J. Beser in view of Hoke and Aventail Renders Claims 18 and 5 Obvious

As noted above, Patent Owner may contend Beser does not anticipate claims 1, 10, 13 or 18, or the dependent claims, based on its belief that these claims require all IP traffic sent over a VPN to be encrypted, and its belief that this is not described by Beser. Such contentions should be disregarded for the reasons set forth in § III.C.1, above. Moreover, even if the claims and Beser were construed as Patent Owner may contend, those claims would have been obvious based on Beser considered in view of Hoke for the reasons set forth in § F, above.

The additional potential distinctions Patent Owner may contend exist regarding independent claim 18 and dependent claim 5, also would have been considered obvious for the reasons set forth in § E, above.

K. Beser in view of RFC 2401, Hoke, Blum, and Aventail Renders Claims 1-10, 12-15, and 18 Obvious

As noted above, Patent Owner may contend Beser does not anticipate claims 1, 10, 13 or 18, or the dependent claims, based on its belief that these certain claim elements are not described by Beser. Those claims would have been obvious based on Beser considered in view of RFC 2401, Hoke, Blum, and Aventail for the reasons set forth in §§ B. to J., above.

V. CONCLUSION

Because the information presented in this petition shows that there is a reasonable likelihood that the petitioner would prevail with respect to at least 1 of the claims challenged in the petition, the Petitioner respectfully requests that a Trial be instituted and that claims 1-10, 12-15, and 18 be canceled as unpatentable.

Dated: June 12, 2013 Respectfully Submitted,

/Jeffrey P. Kushan/
Jeffrey P. Kushan
Registration No. 43,401
Sidley Austin LLP
1501 K Street NW
Washington, DC 20005

PETITION FOR INTER PARTES REVIEW

OF U.S. PATENT NO. 6,173,135

Attachment A:

Proof of Service of the Petition

CERTIFICATE OF SERVICE

I hereby certify that on this 12th day of June 2013, a copy of this Petition, including all attachments, appendices and exhibits, has been served in its entirety by Federal Express on the following counsel of record for patent owner:

FINNEGAN, HENDERSON, FARABOW, GARRETT & DUNNER
901 NEW YORK AVENUE, NW
WASHINGTON DC 20001-4413

Dated: June 12, 2013

Respectfully submitted,

/Jeffrey P. Kushan/
Jeffrey P. Kushan
Reg. No. 43,401
Attorney for Petitioner

PETITION FOR INTER PARTES REVIEW

OF U.S. PATENT NO. 6,173,135

Attachment B:

List of Evidence and Exhibits Relied Upon in Petition

Exhibit #	Reference Name
1001	U.S. Patent No. 6,502,135 to Munger
1002	File History of U.S. Patent No. 6,502,135
1003	Declaration of Michael Allyn Fratto re ’135
1004	Curriculum Vitae of Michael Fratto
1005	Declaration of Chris A. Hopen re ’135
1006	Declaration of James Chester re ’135
1007	Aventail Connect v3.01/2.51 Administrator’s Guide and Aventail ExtraNet Server v3.0 Administrator’s Guide (UNIX and Windows NT) (1996-1999)
1008	BinGO! User’s Guide / Extended Feature Reference, Version 1.2 (1999)
1009	U.S. Patent No. 6,496,867 to Beser
1010	Kent, S., *et al.*, RFC 2401, “Security Architecture for the Internet Protocol,” November 1998
1011	U.S. Patent No. 6,182,141 to Blum
1012	U.S. Patent No. 6,701,437 to Hoke
1013	Leech, M., *et al.*, RFC 1928, “Socks Protocol Version 5,” March 1996
1014	Reed, M., *et al.*, “Anonymous Connections and Onion Routing,” IEEE Journal on Selected Areas in Communications, Vol. 16, No. 4, 482-494 (May 1998)
1015	Reed, M., *et al.*, “Proxies for Anonymous Routing,” 12th Annual Computer Security Applications Conference, San Diego, CA (December 9-13, 1996)
1016	Mockapetris, P., RFC 1034, “Domain Names – Concepts and Facilities,” November 1987

Exhibit #	Reference Name
1017	Mockapetris, P., RFC 1035, "Domain Names – Implementation and Specification," November 1987
1018	Srisuresh, P., *et al*., RFC 2663, "IP Network Address Translator (NAT) Terminology and Considerations," August 1999
1019	Tittel, E., *et al*., Windows NT Server 4 for Dummies, Ch. 12, pp. 191-210 (1999)
1020	Microsoft Press, "Microsoft Windows 98 Resource Kit, The Professional's Companion to Windows 98," Ch. 9, pp. 355-396 and Ch. 19, pp. 849-918 (1998)
1021	Aventail AutoSOCKS v2.1 Administration and User's Guide, 1996-1997
1022	Aventail Connect v3.1/v2.6 Administrator's Guide, 1996-1999
1023	U.S. Patent No. 4,405,829 to Rivest et al.
1024	Ferguson, P. and Huston, G., What Is a VPN? – Part II," The Internet Protocol Journal, Vol. 1, No. 2 (September, 1998)
1025	Braden, R., RFC 1123, "Requirements for Internet Hosts – Application and Support," October 1989
1026	Fielding, R., *et al*., RFC 2068, "Hypertext Transfer Protocol – HTTP/1.1," January 1997
1027	Socolofsky, T., *et al.*, RFC 1180, "A TCP/IP Tutorial," January 1991
1028	RFC 791, "Internet Protocol – DARPA Internet Program Protocol Specification," September 1981
1029	Rescorla, E., *et al.*, RFC 2660, "The Secure HyperText Transfer Protocol," August 1999
1030	Lloyd, B., *et al.*, RFC 1334, "PPP Authentication Protocols," October 1992

Exhibit #	Reference Name
1031	Simpson, W., RFC 1994, "PPP Challenge Handshake Authentication Protocol (CHAP)," August 1996
1032	Dierks, T., *et al.*, RFC 2246, "The TLS Protocol – Version 1.0," January 1999
1033	Simpson, W., RFC 1661, "The Point-to-Point Protocol (PPP)," July 1994
1034	Meyer, G., RFC 1968, "The PPP Encryption Control Protocol (ECP)," June 1996
1035	Kummert, H., RFC 2420, "The PPP Triple-DES Encryption Protocol (3DESE)," September 1998
1036	Pall, G., RFC 2118, "Microsoft Point-To-Point Compression (MPPC) Protocol," March 1997
1037	Gross, G., *et al.*, RFC 2364, "PPP Over AAL5," July 1998
1038	Townsley, W.M., *et al.*, RFC 2661, "Layer Two Tunneling Protocol 'L2TP'," August 1999
1039	Heinanen, J., RFC 1483, "Multiprotocol Encapsulation over ATM Adaptation Layer 5," July 1993
1040	Adams, C., *et al.*, RFC 2510, "Internet X.509 Public Key Infrastructure Certificate Management Protocols," March 1999
1041	Bradner, S., RFC 2026, "The Internet Standards Process – Revision 3," October 1996
1042	Record of publication of Reed et al. (Ex. 1015) on IEEE Xplore (available at http://ieeexplore.ieee.org/xpl/articleDetails.jsp?tp=&arnumber=569678&queryText%3Dgoldschlag+reed+syverson).
1043	Record of publication of Reed et al. (Ex. 1015) on ACM Digital Library (available at http://dl.acm.org/citation.cfm?id=784588.784596&coll=DL&dl=GUIDE&CFID=334755788&CFTOKEN=79391000).

Exhibit #	Reference Name
1044	Record of publication of Reed, et al. (Ex.1015) on ACSAC 12th Annual Conference (available at http://www.acsac.org/pastconf/1996/wed.html)
1045	Memorandum Opinion in *VirnetX, Inc. v. Microsoft Corporation*, 6:07-CV-80 (7/30/09) (EDTX)
1046	VirnetX's Opening Claim Construction Brief in *VirnetX Inc. v. Cisco Systems, Inc., et al.*, 6:10-CV-417 (11/4/11) (EDTX)
1047	Defendants' Responsive Claim Construction Brief in *VirnetX Inc. v. Cisco Systems, Inc., et al.*, 6:10-CV-417 (12/7/11) (EDTX)
1048	VirnetX's Reply Claim Construction Brief in *VirnetX Inc. v. Cisco Systems, Inc., et al.* , 6:10-CV-417 (12/19/11) (EDTX)
1049	Memorandum Opinion and Order in *VirnetX Inc. v. Cisco Systems, Inc., et al.*, 6:10-CV-417 (4/25/12) (EDTX)
1050	VirnetX Inc.'s and Science Applications International Corporation's Original Complaint in *VirnetX Inc., et al. v. Apple Inc.*, 6:12-CV-855 (11/6/2012) (EDTX)
1051	Declaration of Jason Nieh, Ph.D., *Inter Partes* Reexamination Proceeding, Control No. 95/001,269 (April 15, 2010) (USPTO)
1052	Declaration of Angelos D. Keromytis, Ph.D., *Inter Partes* Reexamination Proceeding, Control No. 95/001,682 (May 15, 2012) (USPTO)
1053	Declaration of Robert Dunham Short III, *Inter Partes* Reexamination Proceeding, Control No. 95/001,679 and 95/001,682 (May 14, 2012) (USPTO)
1054	Goldschlag, D., *et al.*, "Hiding Routing Information," Workshop on Information Hiding, Cambridge, UK, May 1996
1055	Office Action in *Inter Partes* Reexamination - Non-Final Office Action, Control No. 95/001,269, January 15, 2010 (USPTO)

Exhibit #	Reference Name
1056	Office Action in *Inter Partes* Reexamination – Non-Final Office Action, Control No. 95/001,679 and 95/001,682, March 11, 2013 (USPTO)
1057	Curriculum Vitae of Chris Hopen
1058	"Aventail Ships the First Standards-Based Virtual Private Network Software Solution," PR Newswire, PR Newswire Association LLC, May 2, 1997
1059	Szeto, L., "Aventail delivers highly secure, flexible VPN solution," InfoWorld Media Group, June 23, 1997
1060	"Aventail Introduces the First Extranet-Ready Platform; Aventail Previews its Latest Solution, Aventail ExtraNet Center, at Networld+Interop in Atlanta," PR Newswire, PR Newswire Association LLC, October 12, 1998
1061	"Intranet Applications: Briefs," Network World, October 19, 1998
1062	Curriculum Vitae of James Chester
1063	Malkin, G., RFC 2453, "RIP Version 2," November 1998
1064	Moy, J., RFC 2328, "OSPF Version 2," April 1998
1065	Comments by Third Party Requester Pursuant to 37 C.F.R. § 1.947, *Inter Partes* Reeexam, Control No. 95/001,682 (USPTO)