Paper No. _____
Filed: April 24, 2015

Filed on behalf of: VirnetX Inc.
By:

Joseph E. Palys
Paul Hastings LLP
875 15th Street NW
Washington, DC 20005
Telephone: (202) 551-1996
Facsimile: (202) 551-0496
E-mail: josephpalys@paulhastings.com

Naveen Modi
Paul Hastings LLP
875 15th Street NW
Washington, DC 20005
Telephone: (202) 551-1990
Facsimile: (202) 551-0490
E-mail: naveenmodi@paulhastings.com

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

APPLE INC.
Petitioner

v.

VIRNETX INC.
Patent Owner

Case IPR2014-00404
Patent 7,987,274[1]

Patent Owner's Demonstrative Exhibits

[1] Case IPR2014-00484 has been joined with this case.

Inter Partes Review of U.S. Patent No. 7,987,274 Case No. IPR2014-00403 Case No. IPR2014-00404

Oral Hearing: April 28, 2015

Instituted Grounds

- **IPR2014-00403**
  - Claims 1, 7, 8, 10, 12, 13, 15, and 17 are anticipated by Provino
  - Claims 2-5 are obvious over Provino in view of Kosiur
  - Claim 18 is obvious over Provino in view of Xu

- **IPR2014-00404**
  - Claims 1-4, 7, 8, 10, 12, 15, and 17 are anticipated by Kiuchi
  - Claims 1-4, 7, 8, 10, 12, 15, and 17 are obvious over Kiuchi and Bhatti
  - Claim 5 is obvious over Kiuchi, Lindblad, and Bhatti

Independent Claim 1

1. A method of accessing a secure network address, comprising:

sending a query message from a first network device to a secure domain service, the query message requesting from the secure domain service a secure network address for a second network device;

receiving at the first network device a response message from the secure domain name service containing the secure network address for the second network device; and

sending an access request message from the first network device to the secure network address using a virtual private network communication link.

Instituted Grounds (IPR2014-00403)

Instituted Grounds: IPR2014-00403

- 35 U.S.C. § 102
  - Claims 1, 7, 8, 10, 12, 13, 15, and 17 are anticipated by Provino
- 35 U.S.C. § 103
  - Claims 2-5 are obvious over Provino in view of Kosiur
  - Claim 18 is obvious over Provino in view of Xu

Summary

- Deficiency A: Provino fails to teach the claimed "sending a query message" to a "secure domain service"
- Deficiency B: Provino fails to teach the claimed "sending an access request message"
- Deficiency C: Provino fails to teach the claimed "tunneling" or "tunnel packeting"
- Deficiency D: Provino fails to teach the claimed "registered" limitations
- Deficiency E: Provino in combination with cited references fail to support the asserted obviousness grounds

IPR2014-00403
Provino
Deficiency A

Deficiency A

- Provino does not disclose:

sending a query message from a first network device to a secure domain service, the query message requesting from the secure domain service a secure network address for a second network device;

  - **Part 1:** The '274 Patent disclaims conventional domain name servers like that disclosed by Provino
    - '274 Patent disclosure
    - Prosecution file history
    - District court
  - **Part 2:** Provino does not disclose a "secure domain service" under Petitioner's proposed construction of the term

Ex. 1001, '274 Patent, Claim 1

Deficiency A: Provino

- Decision points to nameserver 32

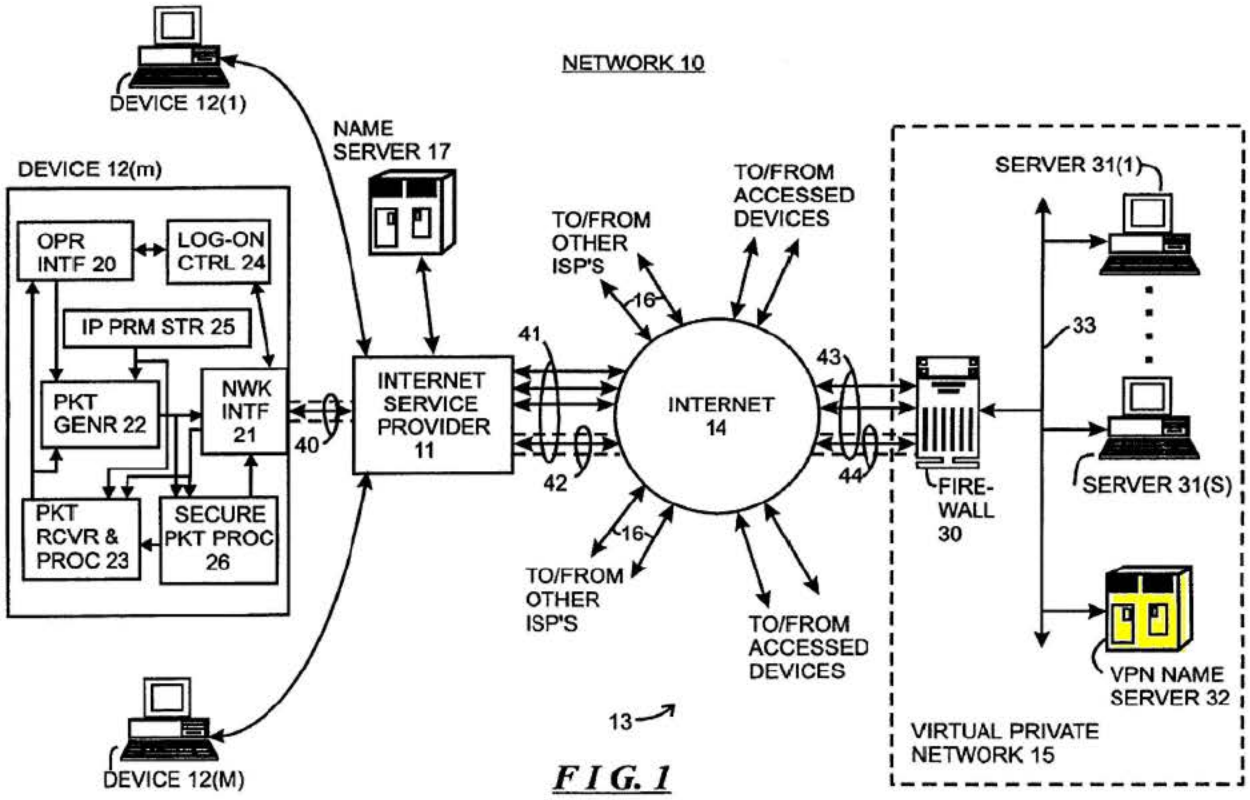


FIG. 1

Ex. 1003, Fig. 1; Decision at 15; Petition at 29

Deficiency A: "Secure Domain (Name) Service"

Patent Owner's Proposed Construction	Apple's Proposed Construction	Board's Preliminary Construction
A lookup service that recognizes that a query message is requesting a secure computer address, and returns a secure computer network address for a requested secure domain name	A service that can resolve secure computer network addresses for a secure domain name for which a conventional domain name service cannot resolve addresses	No construction

A Secure DNS is Not a Conventional DNS: Specification

- The '274 patent specification explains that the claimed "secure domain service" performs *more than* conventional DNS functions

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

Ex. 1001, 38:54-60; Patent Owner Response at 29

A Secure DNS is Not a Conventional DNS: Specification

One conventional scheme that provides secure virtual private networks over the Internet provides the DNS server with the public keys of the machines that the DNS server has the addresses for. This allows hosts to retrieve automatically the public keys of a host that the host is to communicate with so that the host can set up a VPN without having the user enter the public key of the destination host. One implementation of this standard is presently being developed as part of the FreeS/WAN project (RFC 2535).

Ex. 1001, 39:14-22; Patent Owner Response at 29

A Secure DNS is Not a Conventional DNS: Specification

According to certain aspects of the invention, a specialized DNS server traps DNS requests and, if the request is from a special type of user (e.g., one for which secure communication services are defined), the server does not return the true IP address of the target node, but instead automatically sets up a virtual private network between the target node and the user.

Ex. 1001, 39:26-31; Patent Owner Response at 30

A Secure DNS is Not a Conventional DNS: Specification

Moreover, an entity can register several secure domain names, with each respective secure domain name representing a different priority level of access in a hierarchy of access levels to a secure website. For example, a securities trading website can provide users secure access so that a denial of service attack on the website will be ineffectual with respect to users subscribing to the secure website service. Different levels of subscription can be arranged based on, for example, an escalating fee, so that a user can select a desired level of guarantee for connecting to the secure securities trading website. When a user queries SDNS **3313** for the secure computer network address for the securities trading website, SDNS **3313** determines the particular secure computer network address based on the user's identity and the user's subscription level.

Ex. 1001, 47:23-37; Patent Owner Response at 17

A Secure DNS is Not a Conventional DNS: Specification

The grandparent of the '274 patent, the '180 patent, similarly includes embodiments that perform more than the conventional DNS functions. For example,

"DNS proxy 2610 transmits a message to gatekeeper 2603 requesting that a virtual private network be created between user computer 2601 and secure target site 2604," with an IP address only being returned after the secure communication link is set up. (Ex. 1025, 40:53-65; Ex. 2041 at ¶ 37, Monrose Decl.)

"[t]he gatekeeper would establish a VPN between the client and the requested target" before any IP address is returned. (Ex. 1025, 41:65-42:7; Ex. 2041 at ¶ 37, Monrose Decl.) Likewise, in another embodiment, the SDNS only returns a secure URL after it has already coordinated with the VPN gatekeeper to establish a VPN. (Ex. 1025, 52:27-40; Ex. 2041 at ¶ 3738, Monrose Decl.)

Patent Owner Response at 31-32

A Secure DNS is Not a Conventional DNS: File History

- Patent Owner disclaimed domain services that do not recognize that a query message is requesting a secure computer network address

During the now-completed *inter partes* reexamination of USPN 7,188,180 ("the '180 patent"), the grandparent of the '274 patent, VirnetX unambiguously stated:

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

(Ex. 2040 at 7, Response to Office Action in Control No. 95/001,270 (Apr. 19, 2010); *see also id.* at 8, "the secure domain name service . . . is different from a conventional domain name service." 11; Ex. 1001 at 47:15-51.)

Patent Owner Response at 16-17; Ex. 2040 at 7 (Control No. 95/001,270)

A Secure DNS is Not a Conventional DNS: District Court

> VirnetX repeatedly distinguishes a secure domain name service from a *conventional* domain name service, implying that the secure domain name service is not conventional. Further, the '180 Patent distinguishes between a secure domain name service and a standard domain name service. *See* '180 Patent col. 51:29–45 (distinguishing between a "secure domain name service (SDNS)" and a "standard domain name service (STD DNS)").

> The Court construes "secure domain name service" as "a non-standard lookup service that recognizes that a query message is requesting a secure computer address, and returns a secure computer network address for a requested secure domain name."

Ex. 1018 at 18-19; Patent Owner Response at 17

Deficiency A- Part 1

– *In re Abbott Diabetes Care Inc.*, 696 F.3d 1142 (Fed. Cir. 2004)

The specification may "disavow [a prior art] embodiment," even if it "would otherwise be covered by the plain language of the claims," by criticizing such an embodiment in the specification or repeatedly illustrating the novel features that are different from that prior art embodiment. *In re Abbott Diabetes Care Inc.*, 696 F.3d 1142, 1149-50 (Fed. Cir. 2004)

Deficiency A- Part 1

– *In re Abbott Diabetes Care Inc.*, 696 F.3d 1142, 1149-50 (Fed. Cir. 2004)

Further, an amendment to the claims to remove any alleged ambiguity is not required when the specification provides the required disclaimer of claim scope. *Abbott*, 696 F.3d at 1149 (rejecting the Office's argument that patentee had "'the opportunity and responsibility to remove any ambiguity in claim term meaning by amending' the claims during reexamination, yet failed to do so" (quoting *In re Bigio*, 381 F.3d 1320, 1324 (Fed. Cir. 2004))).

A Secure DNS is Not a Conventional DNS: Provino

Provino's nameserver 32 operates in precisely the same way as the conventional domain name service described and disparaged in the '274 patent. When nameserver 32 receives a human-readable address, it simply checks "whether it has an integer Internet address associated with the human-readable Internet address provided in the request message packet," and, if so, "generate[s] a response message packet including the integer Internet address for transmission to the firewall." (Ex. 1003, 14:39-46; Ex. 2041 at ¶ 38, Monrose Decl.)

Patent Owner Response at 32

A Secure DNS is Not a Conventional DNS: Provino

Prosecution history disclaimer confirms the view that *Provino*'s nameserver 32 is a conventional DNS that does not read on the claimed "secure domain service" of the '274 patent. During reexamination of U.S. Patent No. 8,051,181, from which the '274 patent claims priority, VirnetX explicitly and unambiguously stated—consistent with the distinctions discussed above in the '274 patent specification—that *Provino*'s "nameserver 32 is a conventional DNS server that does not resolve secure names." (*See, e.g.*, Ex. 2037 at 12, Rebuttal Brief in *inter partes* reexamination control no. 95/001,949 (Aug. 15, 2014); Ex. 2038 at 41, Appeal Brief in *inter partes* reexamination control no. 95/001,949 (Mar. 14, 2014); Ex. 2039 at 30, Patent Owner's Response filed March 18, 2013 in *inter partes* reexamination control no. 95/001,949.)

Patent Owner Response at 33

Deficiency A- Part 2

– Provino does not disclose a "secure domain service" under Petitioner's proposed construction of the term

Patent Owner's Proposed Construction	Apple's Proposed Construction	Board's Preliminary Construction
A lookup service that recognizes that a query message is requesting a secure computer address, and returns a secure computer network address for a requested secure domain name	A service that can resolve secure computer network addresses for a secure domain name for which a conventional domain name service cannot resolve addresses	No construction

Nameserver 32 is a Conventional DNS Under Apple's Construction

– That a DNS can resolve a domain name that another DNS cannot does not make it a "secure domain service"

Moreover, nameserver 32 behaves just like nameserver 17, which Petitioners concede is a conventional DNS. (*See* Pet. at 27.) When nameserver 17 receives a human-readable address, it simply checks whether it "has an integer Internet address associated with the human-readable Internet address [and, if so,] provide[s] the integer Internet address." (Ex. 1003, 13:43-46; Ex. 2041 at ¶ 40, Monrose Decl.) Likewise, when nameserver 32 receives a human-readable address, it simply checks "whether it has an integer Internet address associated with the human-readable Internet address provided in the request message packet," and, if so, "generate[s] a response message packet including the integer Internet address for transmission to the firewall." (Ex. 1003, 14:39-46; Ex. 2041 at ¶ 40, Monrose Decl.)

Patent Owner Response at 35-36

Nameserver 32 is a Conventional DNS Under Apple's Construction

Nameserver 17 and nameserver 32 also operate in the same manner when they do not have an integer Internet address associated with a human-readable Internet address provided in a request. If "nameserver 17 does not have a integer Internet address associated with the human-readable Internet address, it (that is, the nameserver 17) will provide a response message packet so indicating to device 12(m)." (Ex. 1003, 13:54-58; Ex. 2041 at ¶ 41, Monrose Decl.) Likewise, "if the nameserver 32 does not have an integer Internet address associated with the human-readable Internet address provided by the device 12(m) in the request message packet, it (that is, nameserver 32) can so indicate in the response message packet generated thereby." (Ex. 1003, 15:31-35; Ex. 2041 at ¶ 41, Monrose Decl.)

IPR2014-00403
Provino
Deficiency B

Deficiency B

- Provino does not disclose:

sending an access request message from the first network device to the secure network address using a virtual private network communication link.

Deficiency B ("Access Request Message")

Patent Owner's Proposed Construction	Apple's Proposed Construction	Board's Preliminary Construction
No construction necessary; plain and ordinary meaning	No construction proposed	A signal in a packet or other message format that signifies that the first network device seeks communication, information, or services, with a second network device associated with the secure network address

Deficiency B ("Access Request Message")

- Institution Decision points to Provino's request to set-up tunnel

> On this record, according to the foregoing claim construction discussion and discussion of Provino, an "access request message," as claim 1 recites, reads on Provino's message packets that either essentially request the set-up for an encrypted secure tunnel to server/computer 31(s), or thereafter, request encrypted information or processes from server/computer 31(s) (or other similar devices 12(m') or 13).

Deficiency B ("Access Request Message")

- Claim 1 requires "sending an access request message from the first network device to the secure network address"

The Board, unlike Petitioners, alternatively relies on *Provino*'s alleged disclosure of "message packets that . . . essentially request the set-up for an encrypted secure tunnel to server/computer 31(s)" for the "access request message" feature of claim 1. (Decision at 17.) However, what *Provino* discloses is that "device 12(m) . . . generates a message packet for transfer through the ISP 11 and Internet 14 to the firewall 30 requesting establishment of a secure tunnel between the device 12(m) and firewall 30." (Ex. 1003 at 9:46-52; Ex. 2041 at ¶ 43, Monrose Decl.)

Deficiency B ("Access Request Message")

- Institution Decision points to message packets between device 12(m) and device 13

> Device 12(m) also must have "the required permissions to request [services from or access to] . . . device 13," *id.* at 6:67–7:2, which Provino explains either is a VPN or is a computer device similar to device 12(m) or 12(m') within a VPN. *Id.* at 5:47–6:63, 8:58–62.
>
> On this record, according to the foregoing claim construction discussion and discussion of Provino, an "access request message," as claim 1 recites, reads on Provino's message packets that either essentially request the set-up for an encrypted secure tunnel to server/computer 31(s), or thereafter, request encrypted information or processes from server/computer 31(s) (or other similar devices 12(m') or 13).

Institution Decision at 16-17

Deficiency B ("Access Request Message")

Likewise, Petitioner's expert—whose substantive findings were never challenged during his deposition—similarly understood that "requests sent to server 31(s) by device 12(m) may be *requests for information* stored at the server 31(s)." Ex. 1011 ¶ 40; *see* Ex. 1090 at 42:12-43:10 (discussing Ex. 1003 at 6:19-28).

In particular, Provino describes that the server 31(s) may be a "storage server" that provides information that is requested by a client. *See* Ex. 1003, 6:19-50. As a consequence, the requests sent to server 31(s) by device 12(m) may be requests for information stored at the server 31(s).

Petitioner's Reply at 11; Ex. 1011, ¶ 40

IPR2014-00403
Provino
Deficiency C

Deficiency C: Claims 12 and 13

12. The method according to claim 1, further including using tunneling over the virtual private network communication link.

13. The method according to claim 1, further including using tunnel packeting over the virtual private network communication link.

"Tunnel Packeting"

Patent Owner's Proposed Construction	Apple's Proposed Construction	Board's Preliminary Construction
Forming a packet to be transmitted that contains data structured in one protocol format within the format of another protocol	Encapsulating a first packet of a first protocol in a second packet of a second protocol	Placing data or information in one protocol format (or packet portion), into another protocol format (or portion) of a packet

Deficiency C: "Tunnel Packeting" – Decision

Based on the claim construction discussion of "tunnel packeting," Provino's placement of a device Internet address inside the data or other portion of a packet that is not the normal address portion (e.g. header) for that packet, reasonably constitutes tunnel packeting. On this record, Petitioner sufficiently establishes that Provino's system reads on claims 12 and 13. *See* Pet. 41–42 (citations omitted).

Deficiency C: "Tunnel Packeting" – Provino

However, the Decision has not alleged that the integer Internet address is ever actually placed from "one protocol format (or packet portion)" into "another protocol portion (or portion) of a packet," as required by the Board's construction. Nor does *Provino* disclose whether an address is placed from "one protocol format (or packet portion)" into "another protocol portion (or portion) of a packet." (Ex. 2041 at ¶ 47, Monrose Decl.) Simply placing the integer Internet address inside the data portion of a packet does not necessitate a change in protocol format from "one protocol" to "another protocol." (Ex. 2041 at ¶ 47, Monrose Decl.)

IPR2014-00403
Provino
Deficiency D

Deficiency D: Claim 17

17. The method according to claim 1, wherein the secure network address is registered with the secure domain service prior to the step of sending a query message to a secure domain service.

Deficiency D: Claim 17

The Decision contends that *Provino*'s integer Internet address is registered before what it claims is *Provino*'s "access request message." (Decision at 17.) But what claim 17 requires is that the secure network address be registered before the step of sending a query message, not the step of sending an access request message. Even assuming the Decision's allegations are true, claim 17 is not met.

Deficiency D: Provino

According to the Decision, "nameserver 32 in *Provino* provides the integer Internet address by associating it with a human-readable Internet address," and "*Provino*'s query message for secure information or services . . . occurs after the implied association was created in the nameserver" (Decision at 19.)

Deficiency D: Provino

The Decision's treatment of claim 17 is also incorrect because it relies on an allegedly "implied" teaching by *Provino* that is not necessarily, or even likely, present. This is an inherency argument that is unsupported by the evidence. The Decision has not demonstrated that the nameserver 32 would operate in the manner it describes. *See Robertson*, 169 F.3d at 745. For example, nameserver 32 could request that a network address of server 31(s) be registered after receiving a request for the network address from device 12(m). (Ex. 2041 at ¶ 48, Monrose Decl.)

IPR2014-00403
Provino
Deficiency E

Instituted Grounds: IPR2014-00403

- 35 U.S.C. § 102
  - Claims 1, 7, 8, 10, 12, 13, 15, and 17 are anticipated by Provino
- 35 U.S.C. § 103
  - Claims 2-5 are obvious over Provino in view of Kosiur
  - Claim 18 is obvious over Provino in view of Xu

The ’274 Patent: Claims 2-5

2. The method according to claim 1, further including supporting a plurality of services over the virtual private network communication link.

3. The method according to claim 2, wherein the plurality of services comprises a plurality of communication protocols, a plurality of application programs, multiple sessions, or any combination thereof.

4. The method according to claim 3, wherein the plurality of application programs comprises video conferencing, e-mail, a word processing program, telephony or any combination thereof.

5. The method according to claim 2, wherein the plurality of services comprises audio, video, or any combination thereof.

Claims 2-5 – Kosiur

Kosiur discusses videconferencing in its "Looking Ahead" section when explaining that, "in the future," "[n]etwork performance over VPNs will also improve, enabling VPN links to be used for . . . videoconferencing." (Ex. 1006 at 256; Ex. 2041 at ¶ 51, Monrose Decl.) *Kosiur* does not explain how such improvements of network performance over VPNs would be achieved to enable videoconferencing. (Ex. 2041 at ¶ 51, Monrose Decl.) Indeed, while *Kosiur* explains that "[s]ecure videoconferencing is another application of interest," *Kosiur* admits that "this application may require even more constraints on bandwidth and quality of service," and does not describe how such constraints could be addressed. (Ex. 1006 at 264; Ex. 2041 at ¶ 51, Monrose Decl.)

Patent Owner Response at 45-46

Instituted Grounds (IPR2014-00404)

Instituted Grounds: IPR2014-00404

- 35 U.S.C. § 102
  - Claims 1-4, 7, 8, 10, 12, 15, and 17 are anticipated by Kiuchi
- 35 U.S.C. § 103
  - Claims 1-4, 7, 8, 10, 12, 15, and 17 are obvious over Kiuchi in view of Bhatti
  - Claim 5 is obvious over Kiuchi in view of Bhatti and Lindblad

Summary

- Deficiency A: Kiuchi fails to teach the claimed "secure network address" and "second device" features
- Deficiency B: Kiuchi fails to teach the claimed "sending an access request message"
- Deficiency C: Kiuchi fails to teach the claimed "client computer"
- Deficiency D: Kiuchi and Bhatti do not disclose the claimed "secure network address" and "second device" features
- Deficiency E: Kiuchi and Bhatti do not disclose the claimed "sending an access request message"

IPR2014-00404
Kiuchi
Deficiency A

Deficiency A: Secure Network Address / Second Network Device

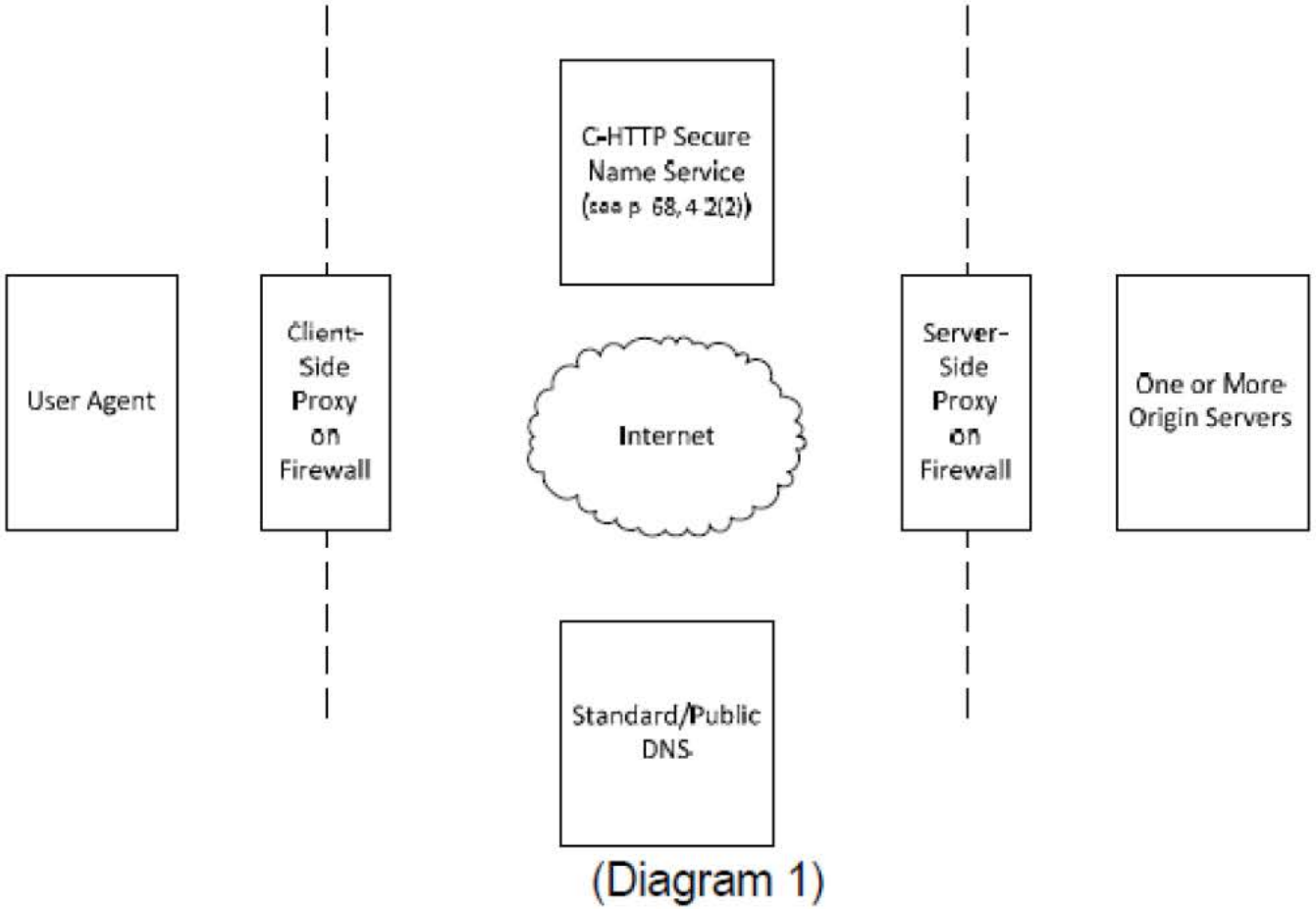
1. A method of accessing a secure network address, comprising:

sending a query message from a first network device to a secure domain service, the query message requesting from the secure domain service a secure network address for a second network device;

receiving at the first network device a response message from the secure domain name service containing the secure network address for the second network device; and

sending an access request message from the first network device to the secure network address using a virtual private network communication link.

Kiuchi



(Diagram 1)

The Decision's Mapping: Secure Network Address and Second Network Device

Claim Element	Secure Network Address	Second Network Device
the query message requesting from the secure domain service a secure network address for a second network device	Server-side proxy's IP address (Decision at 12)	Server-side proxy (Decision at 12)
a response message . . . containing the secure network address for the second network device	Host's IP address (Decision at 13)	Host (Decision at 13)
sending an access request message from the first network device to the secure network address using a virtual private network communication link	Host's IP address (Decision at 13) OR Server-side proxy's IP address (Decision at 14)	Server-side proxy (Decision at 13, 14)

Patent Owner Response at 31-32

The Host Server is the Origin Server: Kiuchi

1) Connection of a client to a client-side proxy

When one of these resource names with a connection ID, for example, "http://server.in.current.connection/sample.html=@=6zd DfldfcZLj8V!i" in Figure (b), is selected and requested by an end-user, the client-side proxy takes off the connection ID and forwards the stripped, the original resource name to the server in its request as described in Figure (c).

2) Lookup of server-side proxy information (Appendix 3. a,b)

A client-side proxy asks the C-HTTP name server whether it can communicate with the host specified in a given URL. If the name server confirms that the query is

Ex. 1004 at 65, § 2.3(1)-(2), Kiuchi

The Host Server is the Origin Server: Petitioner

Petitioners acknowledge that the origin server is the host and that the server-side proxy and host are different devices. For instance, petitioners state that each origin server has a hostname that is registered with the C-HTTP name server (Pet. at 26) and that the origin server's hostname may be different than the origin server's DNS name (Pet. at 24-25). Citing to *Kiuchi's* teaching that "the host [is] specified in a given URL," petitioners explain that the "[t]he hostname 'server.in.current.connection' included in the URL" is the origin server's hostname. (*Id.* at 24-25.) Thus, the host is the origin server, which petitioners depict and describe as being different from the server-side proxy. (*See* Pet. at 22-31, Diagrams 1-7 depicting the "Server-Side Proxy on Firewall" as different and separate from the "One or More Origin Servers," 22, stating "one or more origin servers [are] associated with the server-side proxy"; Ex. 1011 at ¶ 28.)

IPR2014-00404
Kiuchi
Deficiency B

Deficiency B

- Kiuchi does not disclose:

sending an access request message from the first network device to the secure network address using a virtual private network communication link.

  - **Part 1:** Kiuchi's HTTP/1.0 Message is not sent to the alleged secure computer address
  - **Part 2:** Kiuchi's HTTP/1.0 Message is not an "access request message"
  - **Part 3:** Kiuchi's HTTP/1.0 Message is not sent using a virtual private network communication link
  - **Part 4:** Kiuchi's step (3) request for connection is not sent using a virtual private network communication link

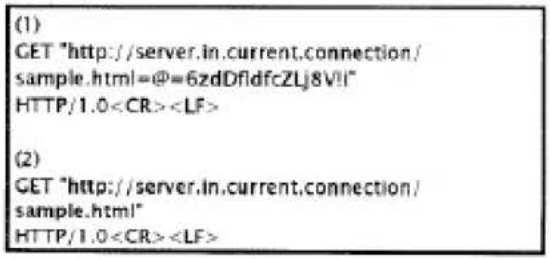
Deficiency B: Part 1 - Decision

Hence, Kiuchi discloses sending an "access request message" (i.e., an "HTTP/1.0 request") from the first network device (i.e., the "client-side proxy") to the secure network address (i.e., the IP address corresponding to the host) using a virtual private network communication link, i.e., the HTTP/1.0 request signifies that the client-side proxy (i.e., "first network device") seeks communication with the "server-side proxy" (i.e., a second network device associated with the secure network address).

Deficiency B: Part 1 - HTTP/1.0 Message Is Not Sent From a First Network Device to a Secure Network Address

As shown in *Kiuchi*'s Fig. (c)(1) and (c)(2), reproduced below, the HTTP/1.0 request is a "GET" request that is sent "from the user agent" to the client-side proxy.

c. HTTP/1.0 request from the user agent (1) and HTTP/1.0 request encrypted and wrapped in C-HTTP request dispatched by the client-side proxy (2)



(Ex. 1004 at 66, Fig. (c), § 2.3(6).) In Fig. (c)(2), the client-side proxy receives the HTTP/1.0 request and initiates and dispatches a new C-HTTP request. (*See id.* at Fig. (c).) Thus, what is sent from the client-side proxy is not an HTTP/1.0 request, but a C-HTTP request. The HTTP/1.0 request is neither sent by the alleged first network device (the client-side proxy), nor is it received at the alleged secure network address (host server's IP address or the server-side proxy's IP address).

Deficiency B: Part 2
HTTP/1.0 Message Is Not an Access Request Message

Because the HTTP/1.0 message seeks an HTML resource from the origin/host server, it is not seeking any "communication, information, or services" from the server-side proxy. (Ex. 1004 at 65-66, § 2.3(1), Fig. (c); Ex. 2041 at ¶ 45, Monrose Decl.) Unlike the earlier messages sent between the client-side and server-side proxies to establish the C-HTTP connection, the user agent sending the HTTP/1.0 request is not seeking communication with the server-side proxy, but with the origin server to which the HTTP/1.0 message is addressed. (Ex. 2041 at ¶ 45, Monrose Decl.)

Deficiency B: Part 3 - HTTP/1.0 Message Is Not Sent Using a Virtual Private Network Communication Link

Properly construed, a virtual private network communication link requires a VPN. And a VPN necessarily requires a "network" and "direct communication." (*See supra* Sections II.A.2-3.) The sending of *Kiuchi's* HTTP/1.0 message meets neither of these requirements.

Patent Owner's Proposed Construction	Apple's Proposed Construction	Board's Preliminary Construction
A communication path between computers in a virtual private network	Any communication link between two end points in a virtual private network	A transmission path between two devices that restricts access to data, addresses, or other information on the path, generally using obfuscation methods to hide information on the path, including, but not limited to, one or more of authentication, encryption, or address hopping

Patent Owner Response at 39, 4

Deficiency B: Part 3 - A VPN Communication Link Exists Only in a VPN: Specification

As explained in the '274 patent, a VPN communication link does not exist outside of a virtual private network. When a secure domain name service (SDNS) receives a query for a secure network address, it "accesses VPN gatekeeper 3314 for establishing a VPN communication link between software module 3309 [at the querying computer 3301] and secure server 3320." (Ex. 1001 at 47:38-40; Ex. 2041 at ¶ 15, Monrose Decl.) Then, "VPN gatekeeper 3314 provisions computer 3301 and secure web server computer 3320 . . . *thereby creating the VPN*" between the devices. (Ex. 1001 at 47:41-44; Ex. 2041 at ¶ 15, Monrose Decl.)[6] Notably, secure server 3320 "can only be accessed through a VPN communication link." (Ex. 1001 at 47:40-41; Ex. 2041 at ¶ 15, Monrose Decl.)

The VPN communication link is initiated to send an access request message between the querying computer 3301 and secure server 3320. (*See* Ex. 1001 at 47:66-48:1, Ex. 2041 at ¶ 16, Monrose Decl.) "Further communication between computers 3301 and 3320 occurs via the VPN" through the VPN communication link. (Ex. 1001 at 48:4-6; Ex. 2041 at ¶ 16, Monrose Decl.)

Deficiency B: Part 3 - A VPN Communication Link Exists Only in a VPN: Claims 1 and 11

11. The method according to claim 1, further including automatically initiating the virtual private network communication link after the access request message is received at the second network device.

Claims 1 and 11 are consistent with the '274 patent's description. Claim 1 recites that the access request message is sent "using a virtual private network communication link." (Ex. 2041 at ¶ 18, Monrose Decl.)

Claim 11 refers to instances in which the virtual private network communication link may need to be automatically re-initiated following the last step in claim 1. (Ex. 2041 at ¶ 19, Monrose Decl.)

Ex. 1001, Claim 11; Patent Owner Response at 7-8

Deficiency B: Part 3 - A VPN
Communication Link Exists Only in a VPN: Petitioner

Claim Term	Definition Encompassed by Broadest Reasonable Interpretation
"virtual private network"	a network of computers that privately communicate with each other by encrypting traffic on insecure communication paths between the computers
"virtual private network communication link"	any communication link between two end points in a virtual private network

Petition at 5

Deficiency B: Part 3 - A VPN Communication Link Requires a "Network": Specification

The specification further describes a VPN as including multiple "nodes." (*See, e.g.*, Ex. 1001 at 16:59-63, referring to "each node in the network" and "vastly increasing the number of distinctly addressable nodes," 21:36, "nodes on the network"; *see also id.* 19:17-19, 24:27.) More specifically, the network allows "[e]ach node . . . to communicate with other nodes in the network." (Ex. 1001 at 16:63-65; Ex. 2041 at ¶ 22, Monrose Decl.) So a device within a VPN is able to communicate with the other devices within that same VPN. (Ex. 2041 at ¶ 22, Monrose Decl.) In addition, the specification distinguishes point-to-point queries from those carried on a VPN communication link, stating that they occur "without using an administrative VPN communication link." (*See, e.g.*, Ex. 1011 at 47:53-54, 47:57-60; Ex. 2041 at ¶ 22, Monrose Decl.)

Deficiency B: Part 3 - A VPN Communication Link Requires "Direct Communication": Disclaimer

VirnetX explained that during reexamination of the '135 patent, VirnetX distinguished its claims over a prior art reference by describing ordinary VPNs as requiring direct communication.

Among other things, VirnetX stated that the reference Aventail does not "disclose a VPN because computers connected according to Aventail do not communicate directly with each other." (Ex. 2036 at 7, Response to Office Action in Control No. 95/001,269 (Apr. 15, 2010); *see also* Ex. 1067 at 5, Defendants' Responsive Claim Construction Brief in the '417 litigation.)

Patent Owner Response at 9, 12

Deficiency B: Part 3 - A VPN Communication Link Requires "Direct Communication": Petitioner

In district court, Apple and other defendants described VirnetX's statements as a "clear mandate to the Patent Office that computers in a 'virtual private network' communicate directly with each other, and that absent direct communication between the computers, there is no virtual private network." (Ex. 1067 at 5, Defendants' Responsive Claim Construction Brief in *VirnetX Inc. v. Cisco Systems, Inc. et al.*, Case No. 6:10-CV-417 (E.D. Tex. Dec. 7, 2011), ("the '417 litigation").)

Apple and other parties have all agreed that VirnetX's statements are clear, unambiguous, and result in disclaimer. (*Id.* at 5-7, "VirnetX unequivocally argued that Aventail does not disclose a VPN because it does not teach direct communication between computers.")

Patent Owner Response at 9-10, 12

Deficiency B: Part 3 - A VPN Communication Link Requires "Direct Communication": Courts

Furthermore, the Federal Circuit noted that virtual private network and secure communication links require direct communication.[7] It stated that the district court's construction of 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." *VirnetX, Inc. v. Cisco Sys., Inc.*, 767 F.3d 1308, 1317 n.1 (Fed. Cir. 2014). Based on that construction, the Federal Circuit held that a secure communication link similarly requires "a direct communication link . . . ." *Id.* at 1319.

Kiuchi: HTTP/1.0 Message Is Not Sent in a "Network"

Kiuchi's C-HTTP system lacks the "network" aspect of a VPN. (Ex. 2041 at ¶ 49, Monrose Decl.) Rather than using interconnected computers that can directly communicate with one another, *Kiuchi* provides for a specialized, point-to-point connection existing only between two proxies at a time. (Ex. 2041 at ¶ 49, Monrose Decl.) If one proxy in a C-HTTP connection needs to connect to a different proxy than the one it is currently connected to, it must first dismantle the existing C-HTTP connection: "[t]he [C-HTTP] session is finished when the client accesses another C-HTTP server," meaning that "the current connection is disconnected." (Ex. 1004 at 65, § 2.3(1); Ex. 2041 at ¶ 49, Monrose Decl.) When accessing another C-HTTP server, *Kiuchi* requires that "a new connection [be] established." (Ex. 1004 at 65, § 2.3(1); *see also id.* at 66, Figs. (b), (c), §§ 2.3(5), 2.3(8).) Each connection requires a separate connection ID. (*Id.* at 65, § 2.3(1); *see also id.* at 66, § 2.3(9); Ex. 2041 at ¶ 49, Monrose Decl.)

Kiuchi: HTTP/1.0 Message Is Not Sent Using "Direct Communication"

Again assuming, but not admitting, that the HTTP/1.0 request continues all the way to the origin server in *Kiuchi's* C-HTTP system, the request must pass through both the client-side and server-side proxies to reach the origin server. (Ex. 2041 at ¶ 51, Monrose Decl.) These proxy servers operate to preclude the user and the host server from directly communicating with each other. (Ex. 2041 at ¶ 51, Monrose Decl.) The proxies stop the communications, wrap/unwrap the messages with C-HTTP formatting, encrypt/decrypt their contents, reformat them, and ultimately resend the messages onwards to their destination. (Ex. 1004 at 65, § 2.3(1), "[i]n the client-side proxy, the HTML document is rewritten"; *id.* at 66, §§ 2.3(6)-(8), explaining that a client-side proxy encrypts and reformats HTTP/1.0 requests to C-HTTP format, and decrypts and reformats C-HTTP responses to HTTP/1.0 format; *see also id.* at 67, §3(2); Ex. 2041 at ¶ 51, Monrose Decl.)

HTTP/1.0 Message Is Not Sent Using "Direct Communication": Courts

The Federal Circuit confirmed that the proxy servers in *Kiuchi* impede direct communication. *See VirnetX*, 767 F.3d at 1324. In particular, the Federal Circuit noted that substantial evidence existed to find that "Kiuchi's proxy servers at least do not teach 'direct communication' between a client and target computer" because "Kiuchi's client-side and server-side proxies terminate the connection, process information, and create a new connection . . . ." *Id.*

Deficiency B: Part 4 - Step (3) Request for Connection Is Not Sent Using a Virtual Private Network Communication Link

While the step (3) request for connection is outside the proper scope of this proceeding because Petitioners did not propose it, *Kiuchi* nevertheless fails to disclose the features of an "access request message" with its step (3) request for connection.

Deficiency B: Part 4 - Step (3) Request For Connection Is Not Sent in a VPN

In *Kiuchi*, the step (3) request for connection is sent prior to the establishment of a C-HTTP connection. (Ex. 1004 at 65-66, §§ 2.3(3)-(5); Ex. 2041 at ¶ 52, Monrose Decl.) The claimed "access request message," however, must be sent "using a virtual private network communication link."

Deficiency B: Part 4 - Step (3)
Request For Connection Is Not Sent in a "Network"

Just as point-to-point C-HTTP requests during established C-HTTP connections lack the "network" aspect of a VPN communication link, (*see supra* Section III.B.3.c.1), the point-to-point requests sent prior to C-HTTP establishment also lack this feature. When a step (3) request for connection is sent, there is no existing connection between the client-side proxy and the server-side proxy, let alone a "network." (Ex. 1004 at 65, § 2.3(3); Ex. 2041 at ¶ 53, Monrose Decl.) To the contrary, *Kiuchi* explains that no connection exists at all until step (5) at which time the server-side proxy communicates with the C-HTTP name server and forwards information to the client-side proxy. (Ex. 1004 at 66, § 2.3(5), "When the client-side proxy accepts and checks them, the connection is established.") To the extent a connection did exist, *Kiuchi* discloses that any preexisting connection is disconnected when negotiating a new C-HTTP connection. (*Id.* at 65, § 2.3(1); Ex. 2041 at ¶ 53, Monrose Decl.)

IPR2014-00404
Kiuchi
Deficiency C

Deficiency C: Claim 15 – "Client Computer"

15. The method according to claim 1, further including performing the method of claim 1 with a client computer connected to a communication network.

"Client Computer"

Patent Owner's Proposed Construction	Apple's Proposed Construction	Board's Preliminary Construction
User's computer	No construction proposed	No construction

The "Client Computer" is the "User's Computer": Specification

But, in the context of the '274 and '180 patents, the client is repeatedly and consistently discussed in connection with the user. Accordingly, the broadest reasonable interpretation of "client computer" is a "user's computer."

The specification explains that the VPN communication link is initiated between the user's computer 2601 and the target:

> If [the DNS request from the user's computer 2601 is requesting access to a secure site and the user is authorized], DNS proxy 2610 transmits a message to gatekeeper 2603 requesting that a virtual private network be created between user computer 2601 and secure target site 2604.

(*See, e.g.*, Ex. 1025 at 40:53-56; Ex. 2041 at ¶ 27, Monrose Decl.)

The "Client Computer" is the "User's Computer": Specification

The specification further explains that a software module 3309 for accessing the secure computer network address using the VPN is installed on a computer 3301, (*see* Ex. 1001 at 47:66-48:1), and elsewhere describes that the computer 3301 is manned by a user and equipped with a web browser 3306 and user input devices such as a keyboard, display, and/or mouse (*see id.* at 45:16-29, 45:50-62, 46:11-28; FIG. 34). In another embodiment, the specification explains that a "user's computer 2501" includes this "client application." (*See id.* at 38:61-62; *see also* Ex. 1025 at 40:36-38.) Thus, the '274 patent equates the user's computer 2601 with the "client computer" in claim 15.

Patent Owner Response at 21-22

The "Client Computer" is the "User's Computer": Petitioner

This construction is further confirmed by a dictionary that Apple cited in its petitions against other VirnetX patents. It defines "client machine" as "[a] user's workstation that is attached to a network." (Ex. 2026 at 3.)

The "Client Computer" is the "User's Computer": Dictionaries

Term	Dictionary Definition
Client	A workstation or personal computer in a client/server environment
Client application	An application running in a workstation or personal computer on a network
Client based	Refers to hardware or software that runs in the user's machine (client)
Client program	Software that runs in the user's PC or workstation
Client/server	An architecture in which the user's PC (the client) is the requesting machine and the server is the supplying machine[.]

(*Id.*) According to the same dictionary, "workstation" "is just a generic term for a user's computer." (*Id.* at 9.)

Kiuchi: The Client-Side Proxy Is Not a "User's Computer"

In *Kiuchi*'s system, the client-side proxy is software installed on an institution's firewall where there is no "user" present. (Ex. 1004 at 65, § 2.2, "When a given institution wants to participate in a closed network, it must 1) install a client-side and/or server-side proxy on its firewall . . . ."; Ex. 2041 at ¶ 57, Monrose Decl.) The firewall/client-side proxy then serves as a proxy *for* the users' computers in conducting transactions for HTML resources. (Ex. 1004 at 65, § 2.3(1), "A client-side proxy . . . should be specified as a proxy server for external (outside the firewall) access in each user agent within the firewall"; Ex. 2041 at ¶ 57, Monrose Decl.)

Kiuchi: The Client-Side Proxy Is Not a "User's Computer"

Kiuchi further distinguishes between a client-side proxy and a user computer by explaining that "C-HTTP-based communication is performed only between two types of C-HTTP proxies . . . . They do not communicate directly with various types of user agents and servers using C-HTTP." (Ex. 1004 at 68, § 4.2(2); *see also id.* at 67-68, § 4.2, "Other secure HTTP protocols are designed to be implemented in origin servers and user agents in order to assure 'end-to-end' security protection. Our approach is aimed at assuring proxy-proxy security and is fundamentally different from theirs."; Ex. 2041 at ¶ 58, Monrose Decl.) Thus, when an end-user selects a URL at a user agent, *Kiuchi* step (1) begins the "[c]onnection of a client [i.e., the user agent] to a client-side proxy." (Ex. 1004 at 65, § 2.3(1); Ex. 2041 at ¶ 58, Monrose Decl.) Because *Kiuchi* discloses that the client-side proxy is not a user's computer, the client-side proxy does not anticipate claim 15.

Patent Owner Response at 45-46

The '274 Patent: Distinguishes Between Proxy Servers and Client Computers

Like *Kiuchi*, the '274 patent also distinguishes between proxy servers and client computers. For example, the '274 patent explains that "[p]roxy servers prevent destination servers from determining the identities of the originating clients." (Ex. 1001 at 1:65-67; Ex. 2041 at ¶ 59, Monrose Decl.) In addition, similar to *Kiuchi's* description of a user agent, the '274 patent describes that client functions and applications such as a "web browser" are included within a "user's computer." (*See, e.g.*, Ex. 1001 at 38:61-63, Fig. 26, item 2601; *see also* Ex. 1025 at 40:37-40; Ex. 2041 at ¶ 59, Monrose Decl.) The '274 patent further distinguishes a firewall, such as the one on which *Kiuchi*'s client-side proxy is installed, from a client computer. It explains that message packets "pass through firewall 3603" and "are directed to client computer 3604." (*See* Ex. 1001 at 51:34-37.)

The Client-Side Proxy Is Not a "User's Computer": Courts

Additionally, the Federal Circuit found that the client-side proxy of *Kiuchi* does not satisfy the claimed "client":

> Apple argued that the "client-side proxy" of Kiuchi meets the "client" limitation, but there was evidence that the "client" of Kiuchi is actually a web browser, a component that is distinguishable from the client-side proxy.
>
> *VirnetX*, 767 F.3d at 1324.

Patent Owner Response at 46-47

IPR2014-00404
Kiuchi
Deficiency D

Deficiency D: The Decision's Mapping of Secure Network Address and Second Network Device

Furthermore, the Petitioners' and the Decision's mapping of *Kiuchi* with *Bhatti* to claim 1 of the '274 patent is defective at least because it relies on two different addresses and devices for the "secure network address" and "second network device."

Deficiency D: The Decision's Mapping of Secure Network Address and Second Network Device

Claim Element	Secure Network Address	Second Network Device
the query message requesting from the secure domain service a secure network address for a second network device	Server-side proxy's IP address (Decision at 12)	Server-side proxy (Decision at 12)
sending an access request message from the first network device to the secure network address using a virtual private network communication link	Content Server's IP address (Decision at 16)	Content Server (Decision at 16)

In *Kiuchi*, the content server is referred to as the host or origin server. (Ex. 2041 at ¶ 60, Monrose Decl.)

Patent Owner Response at 47-48

Deficiency D: The Petitioner's and Decision's Combination

Petitioners suggest that *Kiuchi* and *Bhatti* may be combined by simply plugging *Bhatti's* request into *Kiuchi*'s C-HTTP framework such that "requests made by the user agent and responses provided by the origin server are structured the same as they would be in . . . Bhatti." (Pet. at 45.) Following Petitioners' suggestion, however, would necessarily require an altogether different read of claim 1. In the system envisioned by Petitioners, the sending of an access request message from a first network device to the secure network address of a second network device would occur between *Kiuchi's* user agent and origin server. However, Petitioners make clear that the first and second network devices correspond to *Kiuchi's* client-side and server-side proxies—not the user agent and origin server. (Pet. at 47, 34-36.) Thus, even if *Kiuchi* and *Bhatti* could be combined as proposed, the combination still does not disclose or suggest every feature as recited in independent claim 1.

Patent Owner Response at 48-49

IPR2014-00404
Kiuchi
Deficiency E

Deficiency E

- Kiuchi and Bhatti do not disclose:

sending an access request message from the first network device to the secure network address using a virtual private network communication link.

  - **Part 1:** Bhatti's request is not an "access request message"
  - **Part 2:** Bhatti's request to a content server is not sent using a VPN communication link

Deficiency E: Part 1- Bhatti's Request to a Content Server Is Not an "Access Request Message"

Assuming the first and second network devices are the client-side and server-side proxies, as the Petitioners and the Decision contend, (Pet. at 34; Decision at 12), *Bhatti's* request does not signify that the client-side proxy is seeking communication, information, or services with the server-side proxy. (Ex. 2041 at ¶ 60, Monrose Decl.) What *Bhatti* discloses is that "[w]hen a user at a user terminal desires to access a content file stored in a content server . . . at least one request is generated and sent to the content server." (Ex. 1010 at 4:7-10; Ex. 2041 at ¶ 60, Monrose Decl.)

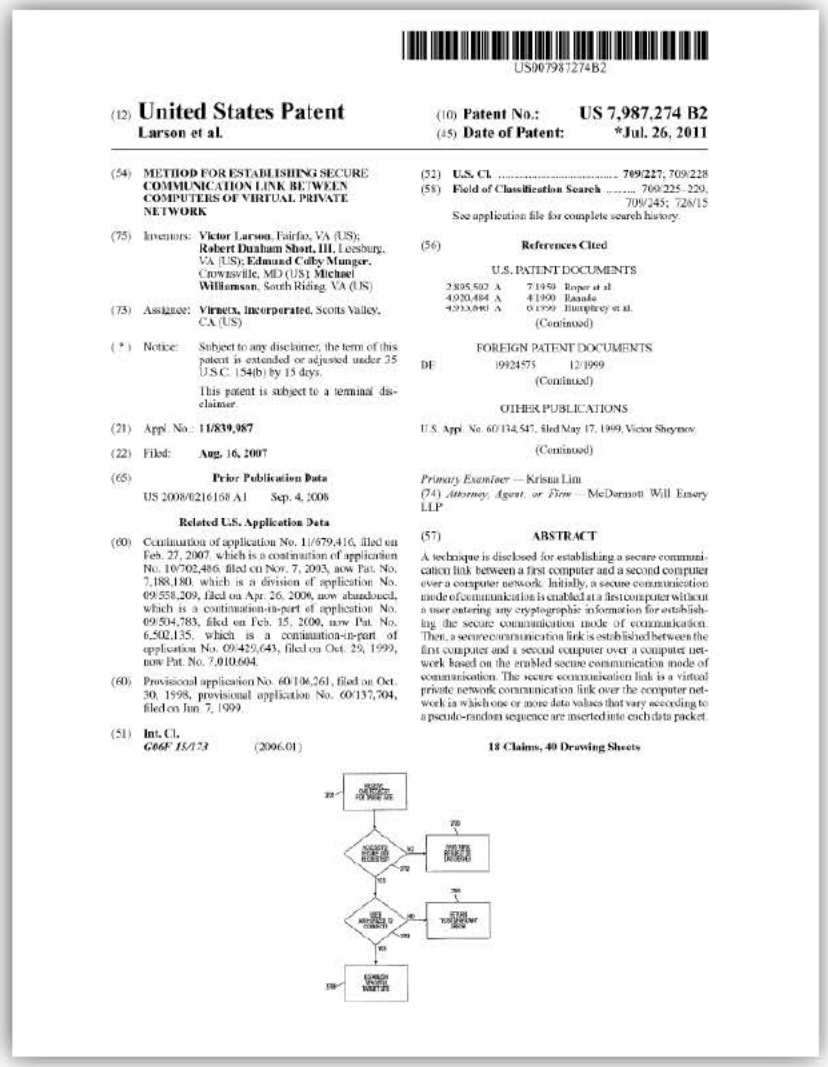
Deficiency E: Part 2- Bhatti's Request to a Content Server Is Not Sent Using a "VPN Communication Link"

Any request in *Bhatti* also fails to cure the deficiencies of *Kiuchi* because it is not sent "using a virtual private network communication link." Neither Petitioners nor the Decision rely on *Bhatti* as disclosing the link. Instead, they rely exclusively on *Kiuchi*'s C-HTTP communication. (Decision at 16-17; Pet. at 46, "These access requests would be handled within the structure of the C-HTTP protocol.") As discussed above, *Kiuchi* does not disclose the claimed virtual private network communication link. (*See supra* Sections III.B.3.c-d.) And the proposed combination with *Bhatti* does not disclose or suggest modifying *Kiuchi's* C-HTTP communication system to remedy this deficiency.

Appendix

Background

The ’274 Patent



US007987274B2

(12) **United States Patent**
Larson et al.

(10) **Patent No.: US 7,987,274 B2**
(45) **Date of Patent: *Jul. 26, 2011**

(54) **METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK**

(75) Inventors: **Victor Larson**, Fairfax, VA (US); **Robert Dunham Short, III**, Leesburg, VA (US); **Edmund Colby Munger**, Crownsville, MD (US); **Michael Williamson**, South Riding, VA (US)

(73) Assignee: **Virtnetx, Incorporated**, Scotts Valley, CA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 15 days.

This patent is subject to a terminal disclaimer.

(21) Appl. No.: **11/839,987**

(22) Filed: **Aug. 16, 2007**

(65) **Prior Publication Data**

US 2008/0216168 A1 Sep. 4, 2008

Related U.S. Application Data

(60) Continuation of application No. 11/679,416, filed on Feb. 27, 2007, which is a continuation of application No. 10/702,486, filed on Nov. 7, 2003, now Pat. No. 7,188,180, which is a division of application No. 09/558,209, filed on Apr. 26, 2000, now abandoned, which is a continuation-in-part of application No. 09/504,783, filed on Feb. 15, 2000, now Pat. No. 6,502,135, which is a continuation-in-part of application No. 09/429,643, filed on Oct. 29, 1999, now Pat. No. 7,010,604.

(60) Provisional application No. 60/106,261, filed on Oct. 30, 1998, provisional application No. 60/137,704, filed on Jun. 7, 1999.

(51) **Int. Cl.**
G06F 15/173 (2006.01)

(52) **U.S. Cl.** **709/227**; 709/228

(58) **Field of Classification Search** 709/225–229, 709/245; 726/15

See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

2,895,502 A 7/1959 Roper et al.
4,920,484 A 4/1990 Ranade
4,933,840 A 6/1990 Humphrey et al.
(Continued)

FOREIGN PATENT DOCUMENTS

DE 19924575 12/1999
(Continued)

OTHER PUBLICATIONS

U.S. Appl. No. 60/134,547, filed May 17, 1999, Victor Sheymov.
(Continued)

Primary Examiner — Krista Lim
(74) *Attorney, Agent, or Firm* — McDermott Will Emery LLP

(57) **ABSTRACT**

A technique is disclosed for establishing a secure communication link between a first computer and a second computer over a computer network. Initially, a secure communication mode of communication is enabled at a first computer without a user entering any cryptographic information for establishing the secure communication mode of communication. Then, a secure communication link is established between the first computer and a second computer over a computer network based on the enabled secure communication mode of communication. The secure communication link is a virtual private network communication link over the computer network in which one or more data values that vary according to a pseudo-random sequence are inserted into each data packet.

18 Claims, 40 Drawing Sheets

Ex. 1001, ’274 Patent

Figure 33 of the ’274 Patent

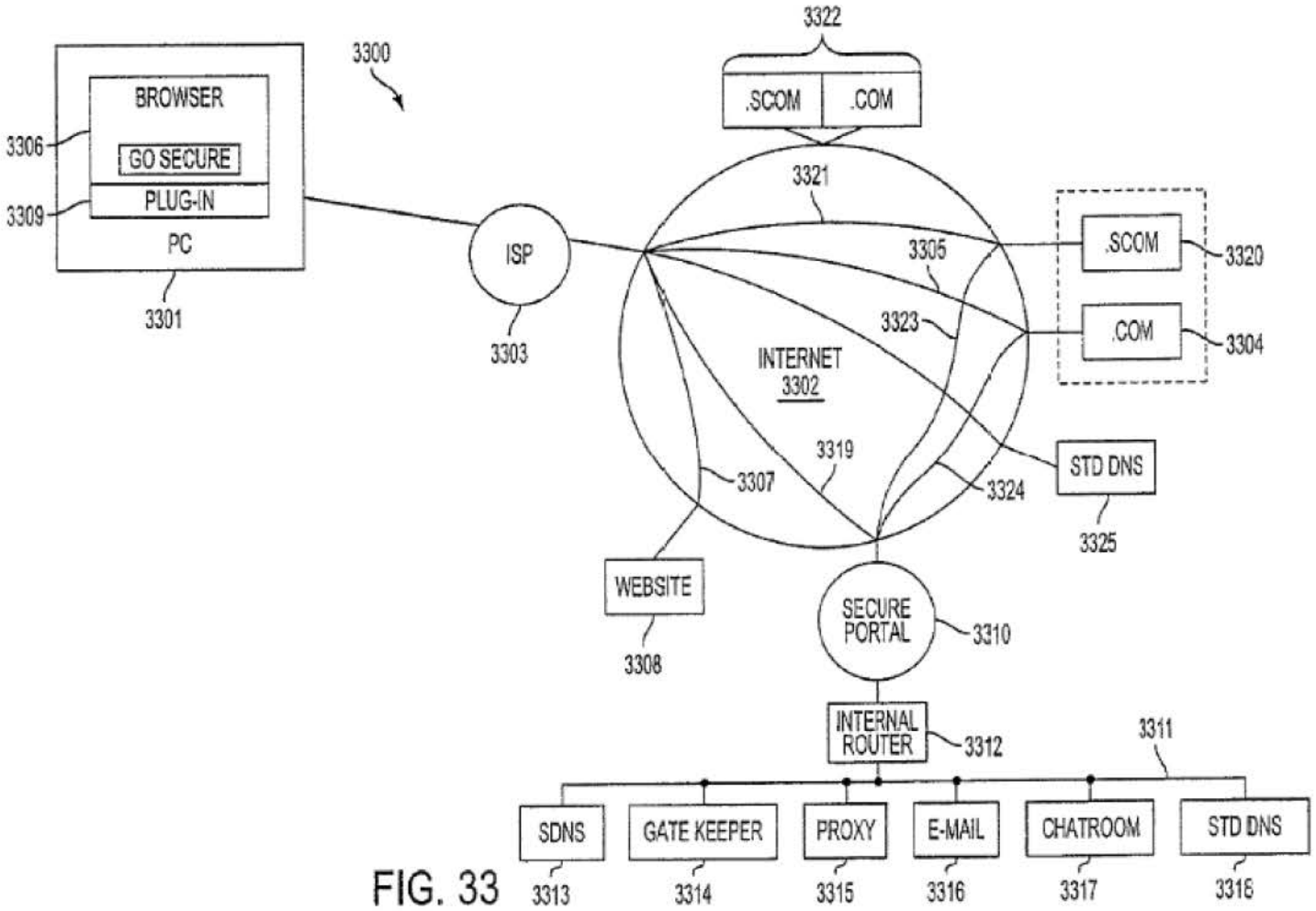


FIG. 33

Figure 26 of the ’274 Patent

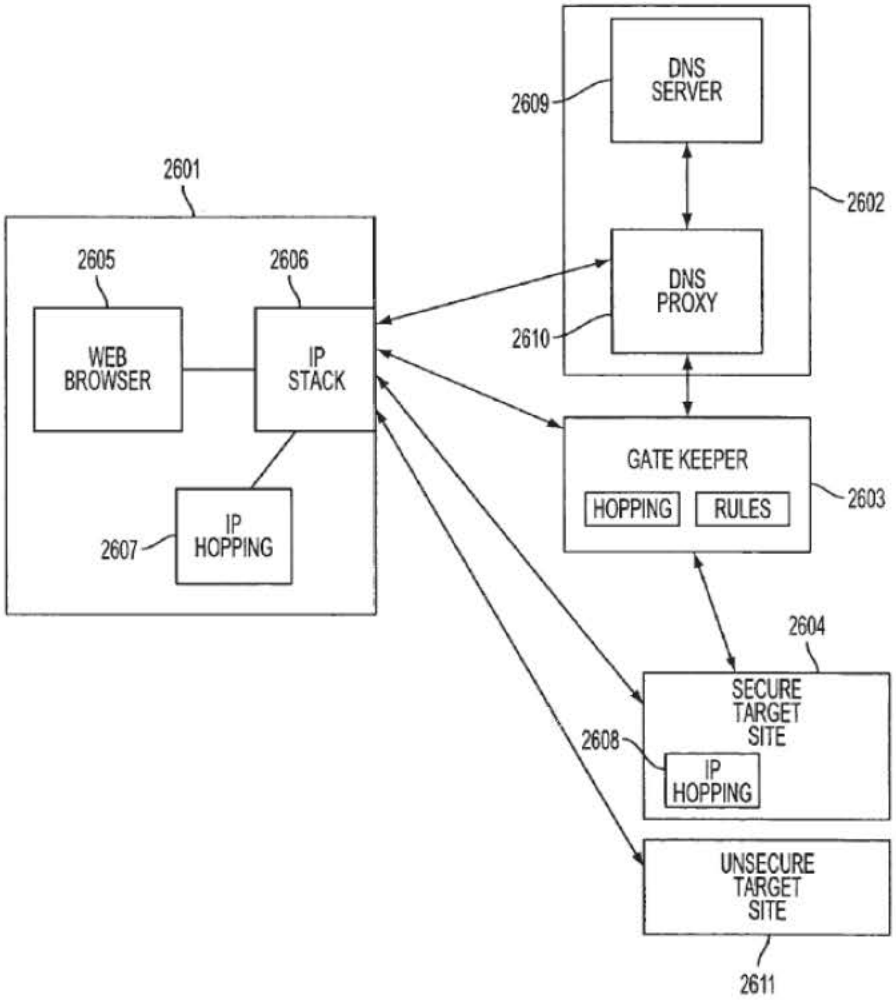


FIG. 26

Claim Construction

"VPN Communication Link"

Patent Owner's Proposed Construction	Apple's Proposed Construction	Board's Preliminary Construction
A communication path between computers in a virtual private network	Any communication link between two end points in a virtual private network	A transmission path between two devices that restricts access to data, addresses, or other information on the path, generally using obfuscation methods to hide information on the path, including, but not limited to, one or more of authentication, encryption, or address hopping

"Secure Domain (Name) Service"

Patent Owner's Proposed Construction	Apple's Proposed Construction	Board's Preliminary Construction
A lookup service that recognizes that a query message is requesting a secure computer address, and returns a secure computer network address for a requested secure domain name	A service that can resolve secure computer network addresses for a secure domain name for which a conventional domain name service cannot resolve addresses	No construction

"Tunnel Packeting"

Patent Owner's Proposed Construction	Apple's Proposed Construction	Board's Preliminary Construction
Forming a packet to be transmitted that contains data structured in one protocol format within the format of another protocol	Encapsulating a first packet of a first protocol in a second packet of a second protocol	Placing data or information in one protocol format (or packet portion), into another protocol format (or portion) of a packet

"Client Computer"

Patent Owner's Proposed Construction	Apple's Proposed Construction	Board's Preliminary Construction
User's computer	No construction proposed	No construction

"Access Request Message"

Patent Owner's Proposed Construction	Apple's Proposed Construction	Board's Preliminary Construction
No construction necessary; plain and ordinary meaning	No construction proposed	A signal in a packet or other message format that signifies that the first network device seeks communication, information, or services, with a second network device associated with the secure network address

Patent Owner Response at 23

"Secure Network Address"

Patent Owner's Proposed Construction	Apple's Proposed Construction	Board's Preliminary Construction
A network address that requires authorization for access and is associated with a computer capable of virtual private network communications	A network address that requires authorization for access and is associated with a computer configured to be accessed through a virtual private network	An address that requires authorization for access

CERTIFICATE OF SERVICE

I hereby certify that on this 24th day of April 2015, a copy of the foregoing Patent Owner's Demonstrative Exhibits was served by electronic mail upon the following:

Jeffrey P. Kushan (jkushan@sidley.com)
Joseph A. Micallef (jmicallef@sidley.com)
Sidley Austin LLP
1501 K Street NW
Washington, DC 20005

Counsel for Petitioner Apple Inc.

Dated: April 24, 2015

Respectfully submitted,

/Joseph E. Palys/
Joseph E. Palys
Counsel for VirnetX Inc.