Paper No. ___
Filed: June 6, 2016

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 IPR2015-00812
Patent No. 8,850,009

PATENT OWNER'S DEMONSTRATIVE EXHIBITS

Inter Partes Review of
U.S. Patent No. 8,868,705
U.S. Patent No. 8,850,009

Case Nos. IPR2015-00810, IPR2015-00811, and IPR2015-00812

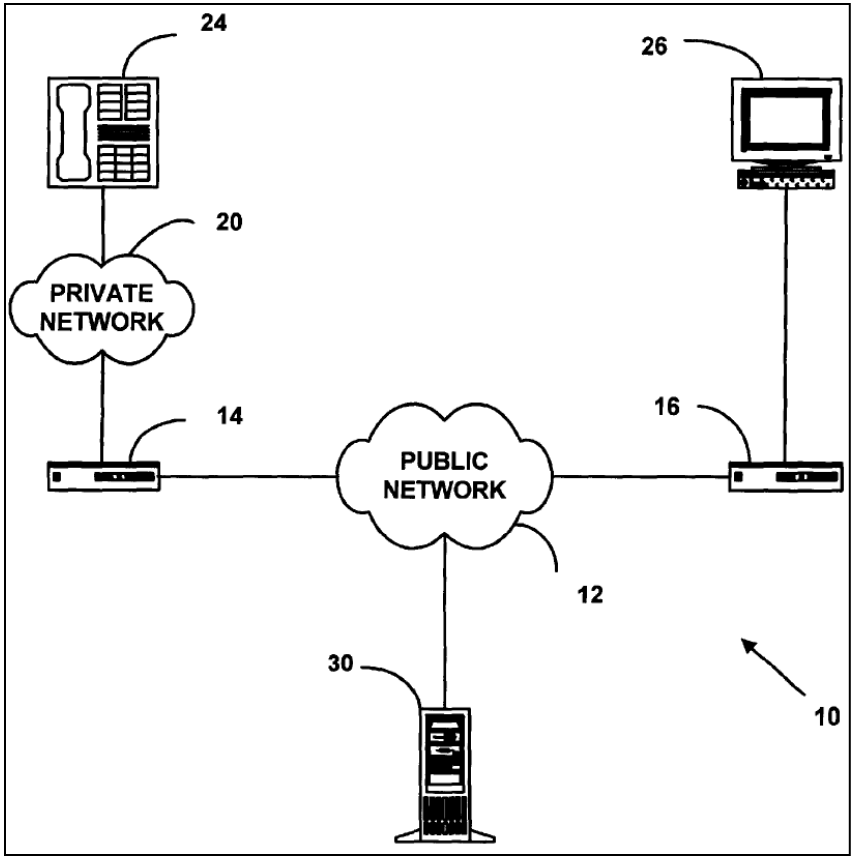
Oral Hearing: June 8, 2016

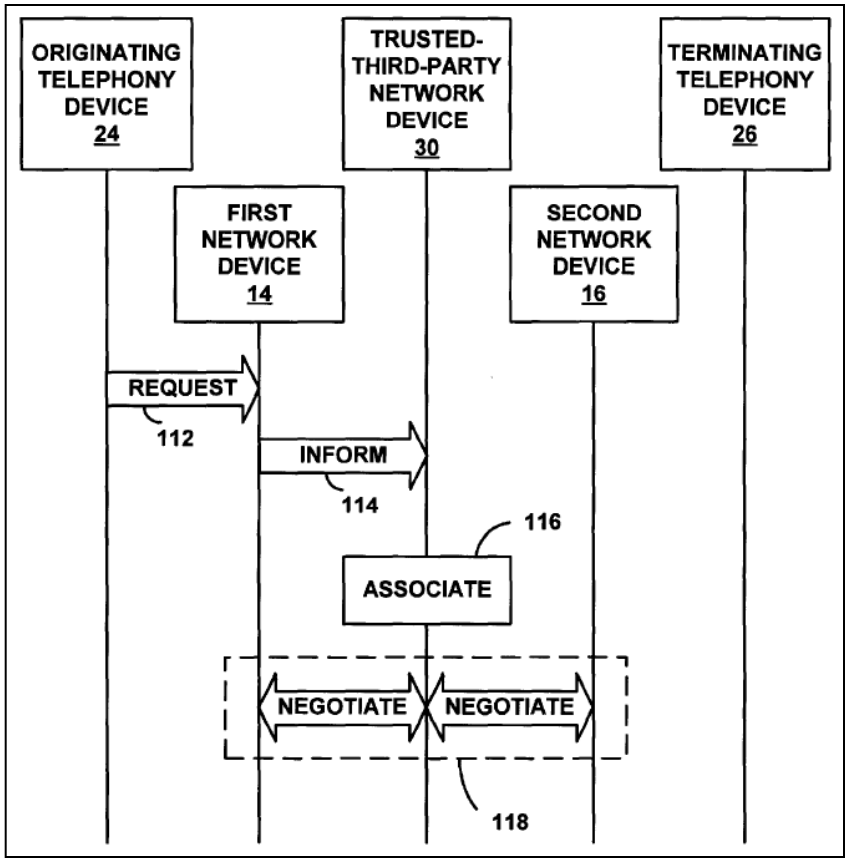
Instituted Grounds

- **IPR2015-00810 (U.S. Patent No. 8,868,705)**
  - Claims 1-4, 6-10, 12-26, and 28-34 as obvious over Beser and RFC 2401
  - Claims 5, 11, and 27 as obvious over Beser, RFC 2401, and Brand
- **IPR2015-00811 (U.S. Patent No. 8,868,705)**
  - Claims 1-3, 6, 14, 16-25, 28, 31, 33, and 34 as obvious over Aventail Connect and RFC 2401
  - Claims 8-10, 12, 15, 30, and 32 as obvious over Aventail Connect, RFC 2401, and RFC 2543
  - Claims 4, 5, 7, 26, 27, and 29 as obvious over Aventail Connect, RFC 2401, and Brand
  - Claims 11 and 13 as obvious over Aventail Connect, RFC 2401, RFC 2543, and Brand
- **IPR2015-00812 (U.S. Patent No. 8,850,009)**
  - Claims 1-8, 10-20, and 22-25 as obvious over Beser and RFC 2401

IPR2015-00810
U.S. Patent No. 8,868,705

Beser's Tunneling Method





Beser's Tunneling Method

Apple's expert:

Q. Okay. What is the purpose of the tunneling method disclosed by Beser?

MR. DILLON: Objection, form.

A. So the general purpose is the one of initiating a tunneling type of communication between two devices, referred to as originating device and terminating device. The method describes the involvement of what are called first network device, second network device, and the trusted third-party device.

Independent Claim 1 of the ’705 Patent

1. A method of transparently creating an encrypted communications channel between a client device and a target device, each device being configured to allow secure data communications between the client device and the target device over the encrypted communications channel once the encrypted communications channel is created, the method comprising:

(1) **intercepting** from the client device a request to look up an Internet Protocol (IP) address corresponding to a domain name associated with the target device;

(2) determining whether the request to look up the IP address [[transmitted]] intercepted in step (1) corresponds to a device that accepts an encrypted channel connection with the client device; and

(3) in response to determining, in step (2), that the request to look up the IP address in step (2) corresponds to a device that accepts an encrypted communications channel connection with the client device, providing provisioning information required to initiate the creation of the encrypted communications channel between the client device and the target device such that the encrypted communications channel supports secure data communications transmitted between the two devices, the client device being a device at which a user accesses the encrypted communications channel.

The "Intercepting" Feature

Apple's Petition:

Accordingly, the broadest reasonable interpretation of the term "intercepting . . . a request" includes "***receiving a request pertaining to a first entity at another entity***." Ex. 1005 at ¶ 69.

The "Intercepting" Feature

Apple's expert:

MR. DILLON: Objection, form.

A. I picked a slightly different word, "pertaining," instead of "intended for." And under the broadest reasonable interpretation, what I have been doing is to consider this case of intended for and also a situation where there may be no explicit intention, the request is ordinarily processed by another entity or received by another entity, will say more specifically, ordinarily received by another entity, and instead, it is received at the first entity.

The "Intercepting" Feature

Apple's Reply:

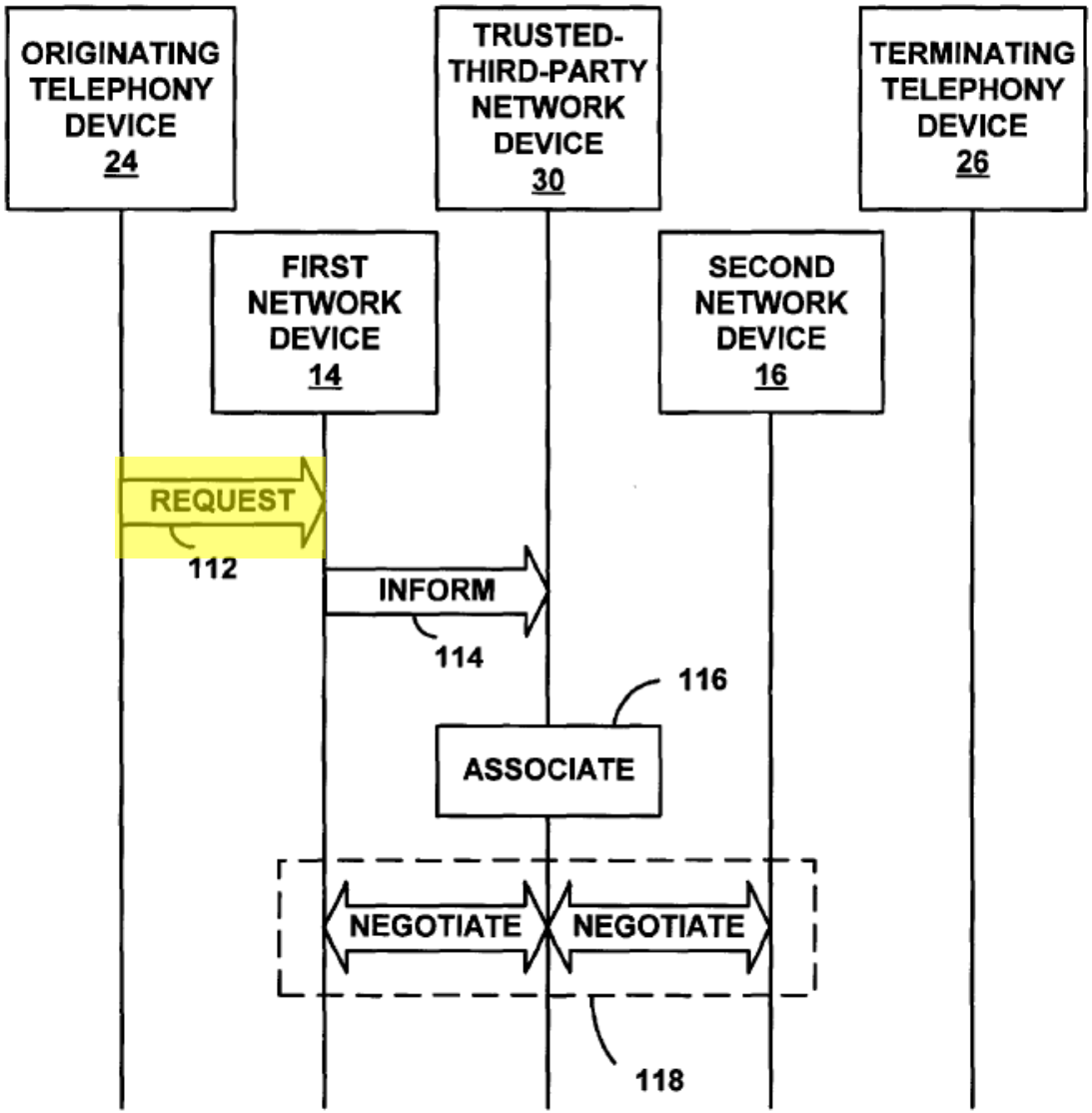
Patent Owner asserts Dr. Tamassia "clarified" his construction of "interception" to mean "receiving a request ~~pertaining to~~ intended for or ordinarily received by a first entity at another entity." Resp. at 24; Ex. 1005 at ¶69. But it mischaracterizes Dr. Tamassia's testimony, who was discussing the rationale underpinning his construction, and was neither proposing nor applying a different construction. Ex. 2015 at 79:9-80:13, 85:9-12; *see* Ex. 1005 at ¶68.

The "Intercepting" Feature

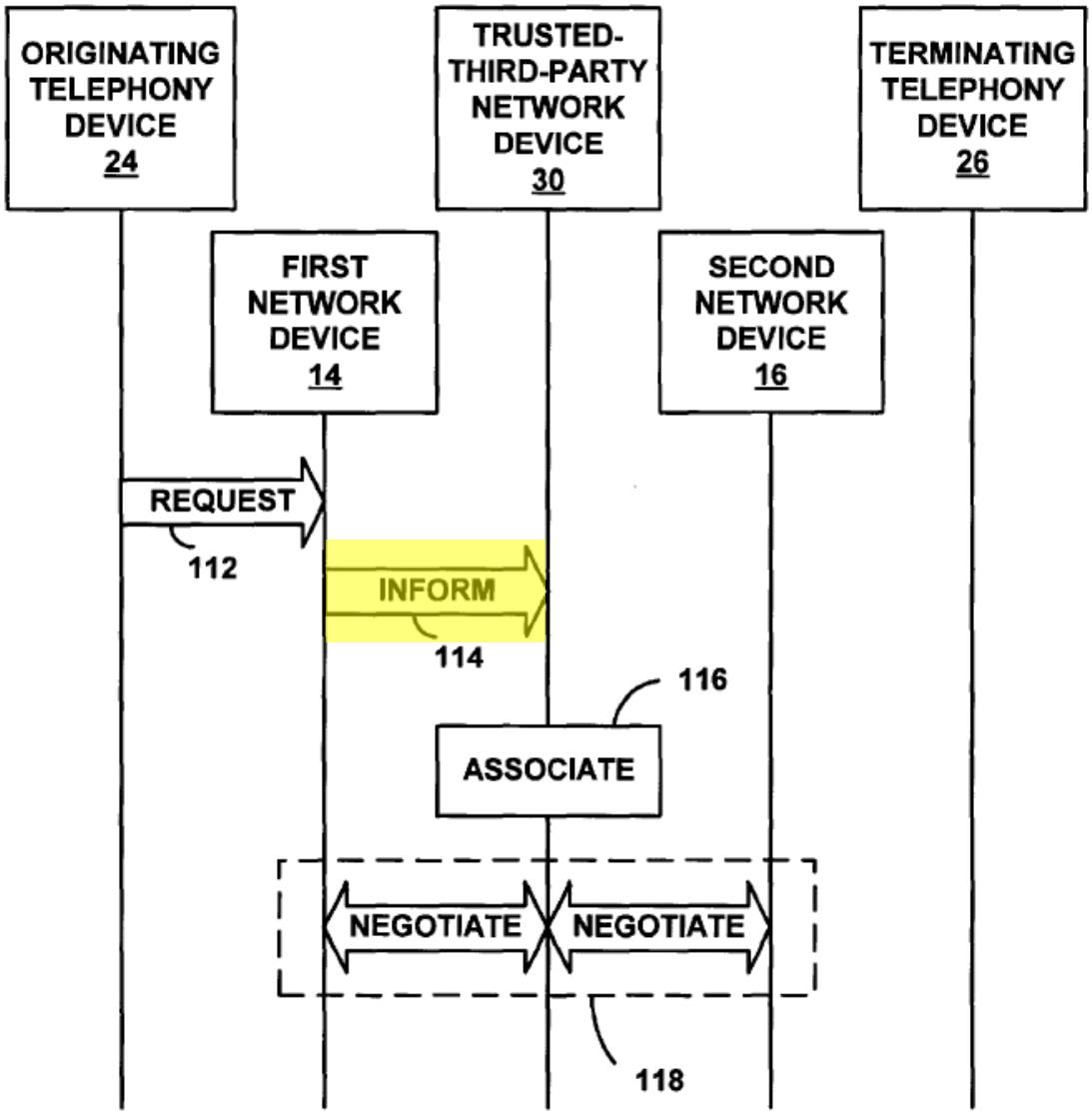
Apple's Petition:

Beser thus shows that, even though the request contains a unique identifier associated with the terminating end device, the request is actually "intercepted" by each of the first network device and the trusted-third-party network device because they each receive "a request pertaining to a first entity at another entity." Ex. 1007 at 8:21-47; Ex. 1005 at ¶ 69. Accordingly, Beser shows "interception" of a request as specified in **claims 1 and 14**.

The Alleged Request in Beser Is Not "Intercept[ed]"



The Alleged Request in Beser Is Not "Intercept[ed]"



The Alleged Request in Beser Is Not "Intercept[ed]"

At Step **114**, a trusted-third-party network device **30** is informed of the request on the public network **12**. The informing step may include one or multiple transfer of IP **58** packets across the public network **12**. The public network **12** may include the Internet. For each transfer of a packet from the first network device **14** to the trusted-third-party network device **30**, the first network device **14** constructs an IP **58** packet. The header **82** of the IP **58** packet includes the public network **12** address of the trusted-third-party network device **30** in the destination address field **90** and the public network **12** address of the first network device **14** in the source address field **88**. At least one of the IP **58** packets includes the unique identifier for the terminating telephony device **26** that had been included in the request message. The IP **58** packets may require encryption or authentication to ensure that the unique identifier cannot be read on the public network **12**.

IPR2015-00810, Ex. 1007 at 11:15-20, Fig. 6; P.O. Resp. at 26-27

Claims 14 and 31 of the ’705 Patent

Claims 14 and 31:

14. The method of claim 1, wherein the target device is a server.

31. The system according to claim 21, wherein the target device is a server.

Apple’s Petition:

> A person of ordinary skill in the art would understand that a Web-TV device or a multimedia application would be used by connecting to and downloading content from a server. Ex. 1005 at ¶ 289.

Claims 14 and 31 of the ’705 Patent

Apple’s expert:

289. As examples of multimedia devices, Beser identifies “Web-TV sets and decoders, interactive video-game players, or personal computers running multimedia applications.” Ex. 1007 (Beser) at 4:47-49. Again, a person of ordinary skill would have understood a “personal computer” to include both desktop and portable laptop computers. That person also would have understood “multimedia applications” to include web browsers, audio and video players, photo browsers, and audio- and video-conferencing software. Web-TV devices and multimedia applications could be used to connect to and downloading from a server.

Claims 14 and 31 of the ’705 Patent

Apple’s Petition:

Indeed, Beser explains that the unique identifier associated with a terminating end device can be a domain name (Ex. 1007 at 10:39-41, 10:55-11:5), which would suggest to a person of ordinary skill in the art that the terminating end device could be a server. *See* Ex. 1005 at ¶¶ 122-128. Accordingly, Beser in view of RFC 2401 would have rendered obvious **claims 14 and 31**.

Claims 14 and 31 of the ’705 Patent

Apple’s expert:

126. The Domain Name System (DNS) translates hostnames (e.g., www.apple.com) into IP address (e.g., 17.172.224.47) necessary to route communications to a destination. DNS is a distributed database that allows for address resolution via a client-server model. The servers in this model are programs called “name servers” that make information from the database available to client programs called “resolvers,” which are responsible for creating queries and submitting them to a name server.

IPR2015-00812
U.S. Patent No. 8,850,009

Independent Claim 1 of the ’009 Patent

1. A network device, comprising: a storage device storing an application program for a secure communications service; and

at least one processor configured to execute the application program for the secure communications service so as to enable the network device to:

send a **domain name service (DNS) request** to look up a network address of a second network device based on an identifier associated with the second network device;

receive, following interception of the DNS request and a determination that the second network device is available for the secure communications service: (1) an indication that the second network device is available for the secure communications service, (2) the requested network address of the second network device, and (3) provisioning information for an encrypted communication link;

connect to the second network device over the encrypted communication link, using the received network address of the second network device and the provisioning information for the encrypted communication link; and

communicate data with the second network device using the secure communications service via the encrypted communication link,

the network device being a device at which a user uses the secure communications service to access the encrypted communication link.

The "Domain Name Service (DNS) Request" Feature

Apple's expert:

Q. And what I'd like to know is what's the significance of the addition of a DNS or domain name service to the phrase -- to the request that's in '009 patent as opposed to the request that's in the '705 patent, as I just pointed out?

MR. DILLON: Objection, form.

A. My understanding is that in the '009 patent, in these lines that we are talking about on -- about Claim 1 of '009, the request in question is a request that follows the DNS protocol for such requests. That is my understanding of the meaning of a domain name service request.

The "Domain Name Service (DNS) Request" Feature

Apple's Reply:

> A person of ordinary skill would have understood that when a request to resolve a domain name is sent to a DNS server, that request follows the DNS protocol. *Id.* at ¶306; *see* Ex. 1007 at 1:50-53.

Apple's expert:

> **306.** The functionality of a DNS server was extremely well-known by February 2000. The primary function of a DNS server was correlate IP addresses with domain names, and to respond to look-up requests by returning the appropriate address information for a requested name. *See* ¶126 above; *see also* Ex. 1001 ('705 patent) at 39:1-3 ("Conventional Domain Name Servers (DNSs) provide a look-up function that returns the IP of a requested computer or host."). If the IP address is unknown, a DNS server would not resolve the address and instead return an error message.

IPR2015-00812, Reply at 10; Ex. 1005 at ¶ 306

IPR2015-00811
U.S. Patent No. 8,868,705

Basic Configuration for Aventail

- Application->Aventail Connect->SOCKS server ->Remote Host

- Aventail Connect
  - Checks redirection rule for the hostname of a remote (step 1)
  - Checks *a connection request* by application (step 2a)

- SOCKS server
  - Negotiates authentication method with Aventail Connect (step 2b)
  - If encryption option selected by SOCKS server, data is encrypted to the SOCKS server (step 3)

Basic Configuration for Aventail

1. The application does a DNS lookup to convert the hostname to an IP address. If the application already knows the IP address, this entire step is skipped. Otherwise, Aventail Connect does the following:

   - If the hostname matches a local domain string or does not match a redirection rule, Aventail Connect passes the name resolution query through to the TCP/IP stack on the local workstation. The TCP/IP stack performs the lookup as if Aventail Connect were not running.
   - If the destination hostname matches a redirection rule domain name (i.e., the host is part of a domain we are proxying traffic to) then Aventail Connect creates a false DNS entry (HOSTENT) that it can recognize during the connection request. Aventail Connect will forward the hostname to the extranet (SOCKS) server in step 2 and the SOCKS server performs the hostname resolution.
   - If the DNS proxy option is enabled and the domain cannot be looked up directly, Aventail Connect creates a fake DNS entry that it can recognize later, and returns this to the calling application. The false entry tells Aventail Connect that the DNS lookup must be proxied, and that it must send the fully qualified hostname to the SOCKS server with the SOCKS connection request.

Basic Configuration for Aventail

2. The application requests a connection to the remote host. This causes the underlying stack to begin the TCP handshake. When the handshake is complete, the application is notified that the connection is established and that data may now be transmitted and received. Aventail Connect does the following:

   a. Aventail Connect checks the connection request.

      - If the request contains a false DNS entry (from step 1), it will be proxied.
      - If the request contains a routable IP address, and the rules in the configuration file say it must be proxied, Aventail Connect will call WinSock to begin the TCP handshake with the server designated in the configuration file.
      - If the request contains a real IP address and the configuration file rule says that it does not need to be proxied, the request will be passed to WinSock and processing jumps to step 3 as if Aventail Connect were not running.

   b. When the connection is completed, Aventail Connect begins the SOCKS negotiation.

      - It sends the list of authentication methods enabled in the configuration file.
      - Once the server selects an authentication method, Aventail Connect executes the specified authentication processing.
      - It then sends the proxy request to the extranet (SOCKS) server. This includes either the IP address provided by the application or the DNS entry (hostname) provided in step 1.

   c. When the SOCKS negotiation is completed, Aventail Connect notifies the application. From the application's point of view, the entire SOCKS negotiation, including the authentication negotiation, is merely the TCP handshaking.

Basic Configuration for Aventail

3 The application transmits and receives data.

If an encryption module is enabled and selected by the SOCKS server, Aventail Connect encrypts the data on its way to the server on behalf of the application. If data is being returned, Aventail Connect decrypts it so that the application sees cleartext data.

Independent Claim 1 of the ’705 Patent

1. A method of transparently creating an encrypted communications channel between a client device and a target device, each device being configured to allow secure data communications between the client device and the target device over the encrypted communications channel once the encrypted communications channel is created, the method comprising:

(1) intercepting from the client device a request to look up an Internet Protocol (IP) address corresponding to a domain name associated with the target device;

(2) determining whether the request to look up the IP address [[transmitted]] intercepted in step (1) corresponds to a device that accepts an encrypted channel connection with the client device; and

(3) in response to determining, in step (2), that the request to look up the IP address in step (2) corresponds to a device that accepts an encrypted communications channel connection with the client device, providing provisioning information required to initiate the creation of the encrypted communications channel between the client device and the target device such that the encrypted communications channel supports secure data communications transmitted between the two devices, the client device being a device at which a user accesses the encrypted communications channel.

Aventail Does Not Disclose the "Determining" Feature

Apple's Petition:

For example, Aventail explains that if the domain name in a connection request matches a domain name in Aventail Connect's table of redirection rules, Aventail Connect flags the request to be proxied to the Aventail Extranet server for handling, including establishing an encrypted connection when Aventail Connect is configured to encrypt all communications (*see, e.g.*, Ex. 1009 at 73). Ex. 1009 at 11-12; *see also id.* at 72-73; Ex. 1003 ¶¶ 229-237. Inclusion of the remote host in the redirection rule table therefore enables the Aventail Connect client to determine if the remote host will accept an encrypted connection ("*corresponds to a device that accepts an encrypted channel connection with the client device*") by checking to see if the remote host is listed in the redirection rule table. Ex. 1009 at 8-9, 11-12, 40; *see also* Ex. 1003 ¶ 237. Aventail's disclosure of using a lookup

Aventail Does Not Disclose the "Determining" Feature

Patent Owner's Response:

Petitioner's first proposition is incorrect because a domain name is never specified **in the connection request**. (Ex. 2016 at ¶¶ 29, 30.) Instead, the connection request includes an IP address, which is either the fake IP address that was previously returned by Aventail Connect (in step 1), a routable IP address, or a real IP address. (*See supra* section III.A.1; Ex. 1009 at 12; Ex. 2013 (steps 2, 2a(1), 2a(2), 2a(3), 2a(4)); Ex. 2016 at ¶ 30.) Dr. Tamassia concedes this point.

Aventail Does Not Disclose the "Determining" Feature

Patent Owner's Response:

In its institution decision, the Board also stated that for *Aventail* to disclose the "determining" step, "[a]ll that is required is that the target device accepts an encrypted communication." (Decision at 19.) These positions are misplaced for two reasons. First, *Aventail* does not have any disclosure of a remote host accepting an encrypted connection. (Ex. 2016 at ¶ 34.) Indeed, as Petitioner acknowledges, *Aventail* does not disclose an encrypted connection *to the remote host* or target device. (Pet. at 39-43, "Aventail, thus, does not explicitly show that the entire path between the client device and the target device (**including the portion of path between the Extranet server and remote host**) remains encrypted" (emphasis added).) If an encrypted connection to the remote host is not even disclosed, then there would no point in determining whether the remote host accepts the encrypted connection. (Ex. 2016 at ¶ 34.)

Aventail Does Not Disclose the "Determining" Feature

- Aventail's redirection rule:

Proxy Redirection	Specify how to redirect traffic.	
	Redirect via	Redirect all traffic through the extranet server selected from the list.
	Do not redirect	Route traffic directly to the specified destination without being redirected through SOCKS.
	Deny service	Deny access to the specified destination. The network connection is blocked locally instead of at the server level.

Apple's Reply

Patent Owner argues Aventail *alone* does not disclose a remote host that "accepts[] an encrypted connection," Resp. at 20, but that argument may be disregarded for several reasons. Initially, nothing in the claim language restricts the "a device that accepts an encrypted channel connection" to the "target device"—it expressly need not be. Patent Owner agrees that Aventail's "system [] determines whether to encrypt traffic to the SOCK server," thus conceding Aventail shows determining whether "a device" accepts an encrypted connection. Resp. at 21.

Apple's Reply

Patent Owner's argument must also be disregarded as it is premised on an unclaimed requirement of end-to-end encryption. The Board correctly accepted the evidence advanced by Dr. Tamassia that "Aventail Connect will evaluate the redirection rule to determine *if the target host is one for which proxy redirection (and an encrypted communication)* through the Aventail Extranet Server is required." Dec. at 19 (citing Ex. 1005 ¶ 237) (emphasis in original); *see also* Ex. 1009 at 8-11. Thus, the evidence described in the Petition, Pet. at 33-35, and by Dr. Tamassia, Ex. 1005 ¶¶ 229-237, establishes that Aventail, even if considered alone, satisfies this step under the broadest reasonable interpretation.

Apple's Reply

Finally, the Board instituted on obviousness grounds based on Aventail with RFC 2401, in which the Aventail system is modified to include "end-to-end encryption," *i.e.*, "data encrypted on the client remains encrypted as it passes through firewall or proxy computers *until it arrives at the specified host computer*." Dec. at 17-21, Pet. at 27-28. A determination by the modified Aventail system that the domain name requires a proxied connection is a determination that the domain name corresponds to a device that accepts an encrypted channel connection, even under Patent Owner's improperly narrow view of the claims.

Apple's Reply

Patent Owner also asserts that "determining whether a domain name . . . matches a redirection rule for a destination is not the same as determining whether the remote host will accept an encrypted connection." Resp. at 21. Patent Owner appears to rely on the *capacity* of the Aventail system to be configured to work differently than the challenged claims specify to incorrectly argue Aventail *must only* be configured in such a way. But Patent Owner ignores the configuration described in Aventail and relied on by Petitioner and the Board—a configuration *where a match of a redirection rule necessarily results in an encrypted connection*. *See* Dec. at 19, Pet. at 34-35. In that configuration, connections to internal private networks "*require all users* to use Aventail Connect to authenticate and encrypt their sessions *before any connection to the internal private*

Independent Claim 1 of the ’705 Patent

1. A method of transparently creating an encrypted communications channel between a client device and a target device, each device being configured to allow secure data communications between the client device and the target device over the encrypted communications channel once the encrypted communications channel is created, the method comprising:

(1) intercepting from the client device a request to look up an Internet Protocol (IP) address corresponding to a domain name associated with the target device;

(2) determining whether the request to look up the IP address [[transmitted]] intercepted in step (1) corresponds to a device that accepts an encrypted channel connection with the client device; and

(3) **in response to determining, in step (2), that the request to look up the IP address in step (2) corresponds to a device that accepts an encrypted communications channel connection with the client device, providing provisioning information required to initiate the creation of the encrypted communications channel between the client device and the target device** such that the encrypted communications channel supports secure data communications transmitted between the two devices, the client device being a device at which a user accesses the encrypted communications channel.

"Provisioning Information" Feature

Patent Owner's Response:

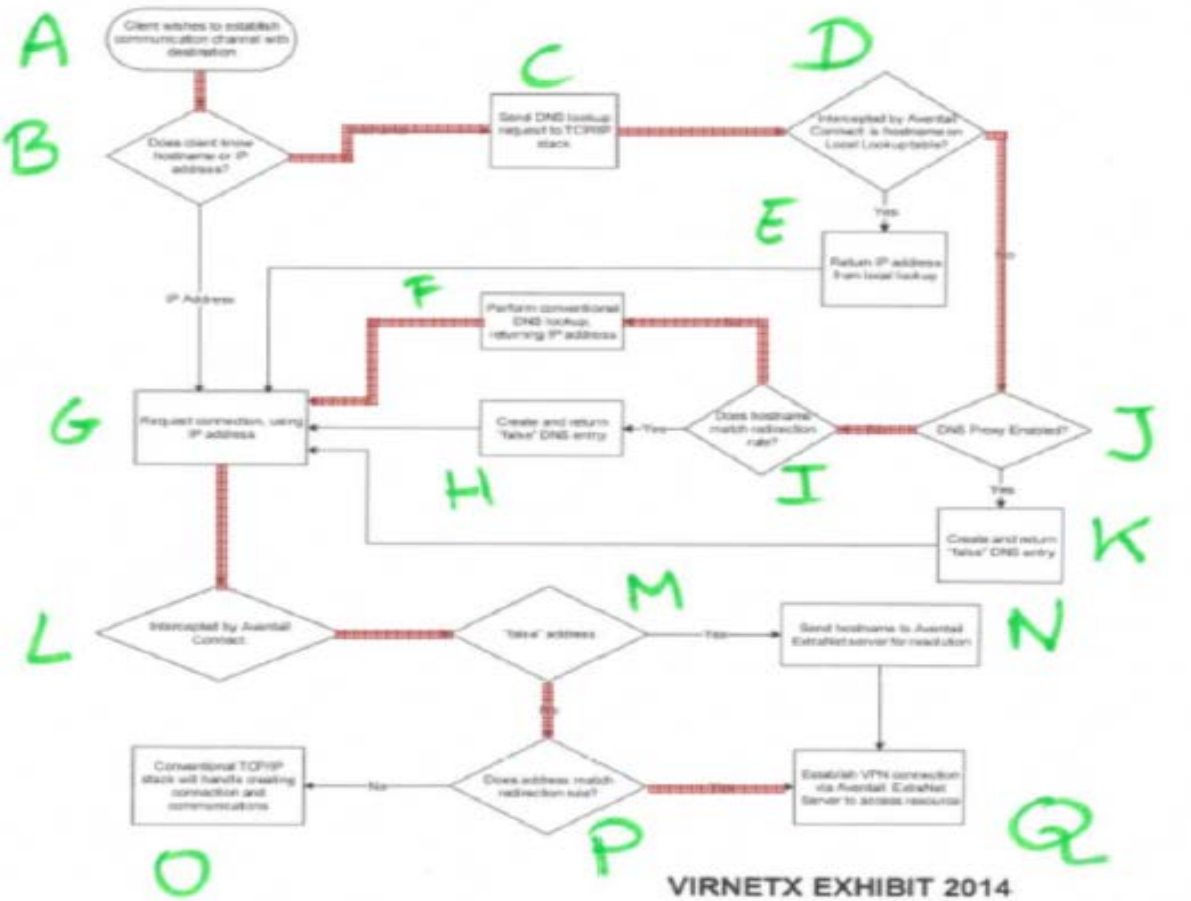
> Accordingly, the "provisioning information" recited in claims 1 and 21 must be (1) *required to initiate the creation of the encrypted communications channel* between the client device and the target device, and (2) provided in response to determining, in step (2), that the request to look up the IP address in step (2) corresponds to a device that accepts an encrypted communications channel connection with the client device. (Ex. 2016 at ¶ 41.)

"Provisioning Information" Feature

Patent Owner's Response:

For instance, the Petition contends that Aventail Connect provides a "HOSTENT" value to the client application, which also allegedly corresponds to the claimed "provisioning information." (Pet. at 36.) The Petition also contends that TCP sequence numbers exchanged during a TCP handshake are "provisioning information." (*Id*. at 36.) The Petition contends that *Aventail* discloses the sending of a digital certificate and selection of an encryption method, which allegedly corresponds to the claimed "provisioning information." (*Id* at 35-36.) Finally, the Petitioner contends that the SOCKS parameters exchanged during the SOCKS negotiation are "provisioning information." (*Id*. at 37.)

HOSTENT



VIRNETX EXHIBIT 2014
Apple v. VirnetX
Trial IPR2015-00810, -00811, -00812

TCP Sequence Numbers

Patent Owner's Response:

> First, there is no relationship between encryption as required by an "encrypted connection" and the TCP sequence numbers. (Ex. 2016 at ¶ 49.)

> Second, the TCP sequence numbers are simply necessary to establish a TCP connection with the SOCKS server and not a remote host. (Ex. 1009 at 12, explaining the TCP handshake with the SOCKS server; Ex. 2016 at __.) As such, the TCP sequence numbers are not required to "initiate the creation of the encrypted communications channel *between the client device and the target device*" (emphasis added). (Ex. 2016 at ¶ 50.)

"Selection of Encryption Method"

Patent Owner's Response:

This is incorrect because both the certificate exchange and the selection of the encryption method relate, at best, to an encrypted connection to the SOCKS server, not the remote host (alleged "target device"). As such, they do not "initiate the creation of the encrypted communications channel *between the client device and the target device*." (Ex. 2016 at ¶ 53.) Indeed, no encrypted connection exists to the remote host in *Aventail* (Pet. at 39-43) and hence, they cannot be required to "initiate the creation of the encrypted communications channel *between the client device and the target device*" (emphasis added). (Ex. 2016 at ¶ 53.)

"SOCKS Exchanges"

Patent Owner's Response:

First, the SOCKS negotiations result in a connection between the client device and the SOCKS server, not a remote host (alleged "target device"). (Ex. 1009 at 12; Ex. 2016 at ¶¶ 54, 55.) As such the SOCKS negotiations do not "initiate the creation of the encrypted communications channel *between the client device and the target device*." (Ex. 2016 at ¶ 55.) Indeed, as acknowledged by Petitioner, no encrypted connection exists to a remote host in *Aventail* (Pet. at 39-43) and hence, the SOCKS negotiations cannot be information required to "initiate the creation of the encrypted communications channel *between the client device and the target device*" (emphasis added). (Ex. 2016 at ¶ 55.)

Claims 2, 16, and 33 of the ’705 Patent

Claim 2:

2. The method of claim 1, wherein providing the provisioning information required to initiate the encrypted communications channel is based on **a determination that the target device is a device with which an encrypted communications channel can be established** when the IP address request corresponds to a target device identified in an network address lookup.

Apple’s Petition:

> Aventail explains that the SSL parameters, HOSTENT, SOCKS parameters, and TCP sequence numbers are provided only if it is determined that the domain name lookup corresponds to a remote host for which an encrypted connection is required. *See, e.g.*, Ex. 1009 at 11-12; Ex. 1018 at 5-6; *see also* § IV.B.1.d), above.

Claims 3 and 25 of the ’705 Patent

Claims 3 and 25:

3. The method of claim 1, wherein the domain name is a secure domain name.

25. The system according to claim 21, wherein the domain name is a secure domain name.

Claims 3 and 25 of the ’705 Patent

Apple’s Petition:

> Domain names that can be resolved only with access to the private domain name server or local domain resolution are not part of the conventional domain name system. *See* 1009 at 72-74. Computers that have not created an authenticated and encrypted connection to the private network (via Aventail) will therefore not be able to resolve the domain names handled by the private domain name server of Aventail. *See* 1009 at 72-74; Ex. 1005 at ¶ 243.
>
> Aventail also shows that the domain names intercepted by Aventail Connect correspond to secure computer network addresses. Aventail discloses that the computers that correspond to these network addresses are not accessible to external users except by way of an authenticated and encrypted connection created by Aventail Connect. *See* 1009 at 72-74.

Claims 3 and 25 of the ’705 Patent

Patent Owner’s Response:

However, while Petitioner contends that *Aventail* discloses a private DNS, Petitioner makes no showing of where *Aventail* discloses that the hostname relied upon by Petitioner as a domain name for claim 1 (Pet. at 31-33), is resolved by this private DNS. And Petitioner cannot make such a showing because *Aventail* only discloses resolution of the hostname from step 1 by either the SOCKS server or a conventional DNS—not by a private DNS. (Ex. 1009 at 11-12; Ex. 2016 at ¶ 62.)

Patent Owner’s Response:

But *Aventail* does not disclose and Petitioner also does not contend that the hostname in step 1 of *Aventail* is a “non-standard domain name.” (Ex. 2016 at ¶ 63.)

Claims 3 and 25 of the ’705 Patent

Apple’s Reply:

Dependent claims 3 and 25 recite that “the domain name is a secure domain name.” Aventail in view of RFC 2401 renders this feature obvious for two reasons. *First*, Aventail relies on a private DNS server that would resolve domain names unable to be resolved by a public DNS. Pet. at 44-45; Ex. 1005 at ¶¶ 224, 243. Patent Owner argues that Aventail does not disclose that the domain name submitted to the SOCKS server for resolution is resolved by the private DNS, Resp. at 36-37, but Aventail explains that when DNS requests are being proxied, “the SOCKS server performs the hostname resolution,” Ex. 1009 at 12, and shows a private DNS server to allow for hostname resolution on the private network, *id.* at 72. Dr. Tamassia testified that the domain names of servers on the private network would be resolved via the private DNS server, Ex. 1005 at ¶ 273, and Dr. Monrose and Patent Owner fail to point to any other resolution mechanism for how the SOCKS server “performs the hostname resolution,” *see* Ex. 2016 at ¶ 62.

Claims 17 and 34 of the ’705 Patent

1. A method of transparently creating an encrypted communications channel between a client device and a target device . . . :

(1) intercepting from the client device a request to look up an Internet Protocol (IP) address corresponding to a domain name associated with the target device;

(2) determining whether the request to look up the IP address [[transmitted]] intercepted in step (1) corresponds to a device that accepts an encrypted channel connection with the client device; and

. . . .

17. The method according to claim 1, wherein the intercepting the request occurs within another device that is separate from the client device.

Claims 17 and 34 of the ’705 Patent

Apple’s Petition:

Aventail discloses that the Aventail Extranet server intercepts the domain lookup requests originating from a computer running Aventail Connect. *See* § IV.B.1.b). The Aventail Extranet server is a different device that is separate from the computer running Aventail Connect. Ex. 1009 at 72; *see also* Ex. 1005 at ¶ 182.

Aventail Not Shown As a Printed Publication

Apple's Petition:

The Aventail Connect v3.01/v2.51 Administrator's Guide (Ex. 1009, "Aventail"), Aventail Connect v3.01/v2.51 User's Guide (Ex. 1010, "Aventail User's Guide"), and Aventail ExtraNet Center v3.0 Administrator's Guide (Ex. 1011, "Aventail Extranet Guide") are documentation for software (version 3.0 of a product called Aventail Extranet Center) that were distributed together. Aventail is a printed publication that was distributed to the public without restriction no later than January 31, 1999. Enclosed with this request are declarations under 37 CFR § 1.32 from three individuals having personal knowledge that Aventail was publicly distributed no later than January 31, 1999. The declarations were previously filed in *inter partes* reexamination 95/001682.

Hopen Declaration

- The version of Aventail Extranet Center relevant here is AEC v3.0, which allegedly included Aventail Connect v3.01/2.51. It was allegedly announced in Fall of 1998.

13. The initial release version of the AEC product was version 3.0. The AEC v3.0 product included version 3.01/2.51 of Aventail Connect and version 3.0 of the Aventail Extranet Server.

14. The AEC v3.0 product with its client and server components was publicly distributed during no later than January of 1999.

15. Exhibit E is a copy of the Aventail Connect v3.01/2.51 Administrator's Guide that was distributed with the Aventail Connect v3.01/2.51 software. Exhibit F is a copy of the Aventail Extranet Server v3.0 Administrator's Guide that was distributed with the Aventail Extranet Server software. Both of these documents were distributed without any confidentiality restrictions.

10. In the fall of 1998, Aventail announced a product called the Aventail Extranet Center ("AEC"). Exhibit D is a copy of an October 12, 1998 Aventail press release announcing the Aventail Extranet Center product.

Hopen Declaration

14. The AEC v3.0 product with its client and server components was publicly distributed during no later than January of 1999.

16. I estimate that Aventail distributed thousands of copies of the AEC v3.0 product (including the Administrator Guides for Aventail Connect and Extranet Center) during the first six months of 1999.

Chester Declaration

Apple's Petition:

In Exhibit 1022, James Chester, formerly of IBM, testifies that he received Aventail no later than the end of December of 1998, and subsequently distributed this document to customers and IBM employees in connection with deployment of VPN solutions to these entities and individuals in mid-January of 1999.

Chester Declaration

14. A second VPN solution Aventail distributed between 1996 and 2000 was called the Aventail Extranet Center (AEC). This product included client software called Aventail Connect and server software called Aventail Extranet Server.

15. I recall that Aventail announced its AEC v3.0 product in the fall of 1998, and began distributing this product no later than mid-January of 1999. Because IBM was the largest user of Aventail VPN products, we would be one of the first companies to receive new versions of the Aventail products; both evaluation and production products. I was personally involved in Aventail's strategic planning and direction from March 1998.

16. The AEC v3.0 product included version 3.01/2.51 of the Aventail Connect software, and version 3.0 of the Aventail Extranet Server.

17. Exhibit C is a copy of the Administrator's Guide for Aventail Connect v3.01/2.51. I recall receiving Exhibit C with the AEC v3.0 product no later than July 1998.

19. The AEC product was a very versatile and stable VPN solution. It received very good reviews from the technical press. We deployed VPN solutions based on this product to more than 20,000 IBM employees domestically by March 1998 and more than 65,000 IBM employees worldwide by July 1998.

Appendix

Claim 1 of the ’705 Patent

1. A method of transparently creating an encrypted communications channel between a client device and a target device, each device being configured to allow secure data communications between the client device and the target device over the encrypted communications channel once the encrypted communications channel is created, the method comprising:(1) intercepting from the client device a request to look up an Internet Protocol (IP) address corresponding to a domain name associated with the target device;

(2) determining whether the request to look up the IP address [[transmitted]] intercepted in step (1) corresponds to a device that accepts an encrypted channel connection with the client device; and

(3) in response to determining, in step (2), that the request to look up the IP address in step (2) corresponds to a device that accepts an encrypted communications channel connection with the client device, providing provisioning information required to initiate the creation of the encrypted communications channel between the client device and the target device such that the encrypted communications channel supports secure data communications transmitted between the two devices, the client device being a device at which a user accesses the encrypted communications channel.

Claims 2-6 of the ’705 Patent

2. The method of claim 1, wherein providing the provisioning information required to initiate the encrypted communications channel is based on a determination that the target device is a device with which an encrypted communications channel can be established when the IP address request corresponds to a target device identified in an network address lookup.

3. The method of claim 1, wherein the domain name is a secure domain name.

4. The method of claim 1, wherein the encrypted communications channel is a broadband connection.

5. The method of claim 1, wherein the encrypted communications channel is an unmodulated transmission link.

6. The method of claim 1, wherein the encrypted communications channel is a modulated transmission link.

Claims 7-11 of the ’705 Patent

7. The method of claim 1, wherein the encrypted communications channel supports at least one of the following: FDM, TDM and CDMA.

8. The method of claim 1, wherein the client device is a phone.

9. The method of claim 8, wherein providing the provisioning information required to initiate the encrypted communications channel is based on a determination that the target device is a device with which an encrypted communications channel can be established when the IP address request corresponds to a target device identified in an network address lookup.

10. The method of claim 8, wherein the domain name is a secure domain name.

11. The method of claim 8, wherein the encrypted communications channel is an unmodulated transmission link.

Claims 12-17 of the ’705 Patent

12. The method of claim 8, wherein the encrypted communications channel is a modulated transmission link.

13. The method of claim 8, wherein the encrypted communications channel supports at least one of the following: FDM, TDM and CDMA.

14. The method of claim 1, wherein the target device is a server.

15. The method of claim 1, wherein the target device is a phone.

16. The method according to claim 1, wherein intercepting the request consists of receiving the request to determine whether the target device accepts an encrypted channel connection with the client device.

17. The method according to claim 1, wherein the intercepting the request occurs within another device that is separate from the client device.

Claims 18-20 of the ’705 Patent

18. The method according to claim 1, wherein the encrypted communications channel supports a plurality of services.

19. The method according to claim 18, wherein the plurality of services comprises a plurality of communication protocols, a plurality of application programs, multiple sessions, or a combination thereof.

20. The method according to claim 19, wherein the plurality of other application programs comprises at least one of the following: e-mail, a word processing program, and telephony.

Claim 21 of the ’705 Patent

21. A system for transparently creating an encrypted communications channel between a client device and a target device, each device being configured to allow secure data communications therebetween over an encrypted communications channel once the encrypted communications channel is created, the system including a memory storing instructions, and a server configuration arranged to:(1) intercept from the client device a request to look up an Internet Protcol (IP) address corresponding to a domain name associated with the target device;

(2) determine whether the request to look up the IP address [[transmitted]] intercepted in step (1) corresponds to a device that accepts an encrypted channel connection with the client device; and

(3) in response to determining, in step (2), that the request to look up the IP address corresponds to a device that accepts an encrypted communications channel connection with the client device, provide provisioning information required to initiate the creation of the encrypted communications channel between the client device and the target device such that the encrypted communications channel supports secure data communications transmitted between the two devices, the client device being a device at which a user accesses the encrypted communications channel.

Claims 22-26 of the ’705 Patent

22. A system according to claim 21, wherein the encrypted communications channel supports a plurality of services.

23. The system according to claim 21, wherein the plurality of services comprises a plurality of communication protocols, a plurality of application programs, multiple sessions, or a combination thereof.

24. The system according to claim 23, wherein the plurality of other application programs comprises at least one of the following: e-mail, a word processing program, and telephony.

25. The system according to claim 21, wherein the domain name is a secure domain name.

26. The system according to claim 21, wherein the encrypted communications channel is a broadband connection.

Claims 27-32 of the ’705 Patent

27. The system according to claim 21, wherein the encrypted communications channel is an unmodulated transmission link.

28. The system according to claim 21, wherein the encrypted communications channel is a modulated transmission link.

29. The system according to claim 21, wherein the encrypted communications channel supports at least one of the following: FDM, TDM and CDMA.

30. The system according to claim 21, wherein the client device is a phone.

31. The system according to claim 21, wherein the target device is a server.

32. The system according to claim 21, wherein the target device is a phone.

Claims 33-34 of the ’705 Patent

33. The system according to claim 21, wherein intercepting the request consists of the system receiving the request to determine whether the target device accepts an encrypted channel connection with the client device.

34. The system according to claim 21, wherein intercepting the request occurs within another device that is separate from the client device.

Claim 1 of the ’009 Patent

1. A network device, comprising: a storage device storing an application program for a secure communications service; and
at least one processor configured to execute the application program for the secure communications service so as to enable the network device to:
send a domain name service (DNS) request to look up a network address of a second network device based on an identifier associated with the second network device;
receive, following interception of the DNS request and a determination that the second network device is available for the secure communications service: (1) an indication that the second network device is available for the secure communications service, (2) the requested network address of the second network device, and (3) provisioning information for an encrypted communication link;
connect to the second network device over the encrypted communication link, using the received network address of the second network device and the provisioning information for the encrypted communication link; and
communicate data with the second network device using the secure communications service via the encrypted communication link,
the network device being a device at which a user uses the secure communications service to access the encrypted communication link.

Claims 2-6 of the ’009 Patent

2. The network device of claim 1, wherein the secure communications service includes an audio-video conferencing service, and the at least one processor is configured to execute the application program to communicate at least one of encrypted video data and audio data with the second network device via the encrypted communication link using the secure communications service.

3. The network device of claim 1, wherein the secure communications service includes a telephony service.

4. The system of claim 3, wherein the telephony service uses modulation.

5. The network device of claim 4, wherein the modulation is based on one of frequency-division multiplexing (FDM), time-division multiplexing (TDM), or code division multiple access (CDMA).

6. The network device of claim 1, wherein the network device is a mobile device.

Claims 7-10 of the ’009 Patent

7. The network device of claim 1, wherein the identifier associated with the second network device is a domain name.

8. The network device of claim 1, wherein the encrypted communication link is part of a virtual private network communication link.

9. The network device of claim 1, wherein the virtual private network communication link is based on inserting into each data packet communicated over the virtual private network communication link one or more data values that vary according to a pseudo-random sequence.

10. The network device of claim 1, wherein the indication that the second network device is available for the secure communications service is a function of the result of a domain name lookup.

Claims 11-13 of the ’009 Patent

11. The network device of claim 1, wherein the encrypted communication link is an end-to-end link extending from the network device to the second network device.

12. The network device of claim 1, wherein the interception of the DNS request consists of receiving the DNS request to determine that the second network device is available for the secure communications service.

13. The network device of claim 1, wherein the interception of the DNS request occurs at another network device that is separate from the network device.

Claim 14 of the ’009 Patent

14. A method executed by a first network device for communicating with a second network device, the method comprising:sending a domain name service (DNS) request to look up a network address of a second network device based on an identifier associated with the second network device;

receiving, following interception of the DNS request and a determination that the second network device is available for a secure communications service: (1) an indication that the second network device is available for the secure communications service, (2) the requested network address of the second network device, and (3) provisioning information for an encrypted communication link;

connecting to the second network device over the encrypted communication link, using the received network address of the second network device and the provisioning information for the encrypted communication link; and

communicating data with the second network device using the secure communications service via the encrypted communication link,

the first network device being a device at which a user uses the secure communications service to access the encrypted communication link.

Claims 15-19 of the ’009 Patent

15. The method of claim 14, wherein the secure communications service includes a video conferencing service, and communicating includes communicating at least one of encrypted video data and audio data with the second network device via the encrypted communication link using the secure communications service.

16. The method of claim 14, wherein the secure communications service includes a telephony service.

17. The method of claim 14, wherein the telephony service uses modulation.

18. The method of claim 17, wherein the modulation is based on one of frequency-division multiplexing (FDM), time-division multiplexing (TDM), or code division multiple access (CDMA).

19. The method of claim 14, wherein the network device is a mobile device.

Claims 20-23 of the ’009 Patent

20. The method of claim 14, wherein the identifier associated with the second network device is a domain name.

21. The method of claim 14, wherein the encrypted communication link is part of a virtual private network communication link, and communicating with the second network device using the secure communications service includes inserting into data packets communicated over the virtual private network communication link one or more data values that vary according to a pseudo-random sequence.

22. The method of claim 14, wherein the indication that the second network device is available for a secure communications service is a function of a domain name lookup.

23. The method of claim 14, wherein the encrypted communication link is an end-to-end link extending from the first network device to the second network device.

Claims 24-25 of the ’009 Patent

24. The method of claim 14, wherein the intercepting the DNS request consists of receiving the DNS request to determine that the second network device is available for the secure communications service.

25. The method of claim 14, wherein the intercepting the DNS request occurs at another network device that is separate from the first network device.

CERTIFICATE OF SERVICE

I hereby certify that on this 6th day of June 2016, a copy of the foregoing Patent Owner's Demonstrative Exhibits was served electronically, pursuant to agreement, upon the following:

Counsel for Apple Inc.:

iprnotices@sidley.com
Sidley Austin LLP
1501 K Street NW
Washington, DC 20005

Respectfully submitted,

Dated: June 6, 2016

By:/Joseph E. Palys/
Joseph E. Palys
Reg. No. 46,508
Counsel for VirnetX Inc.