Paper No. _____
Filed: February 5, 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 IPR2014-00238
Patent 8,504,697

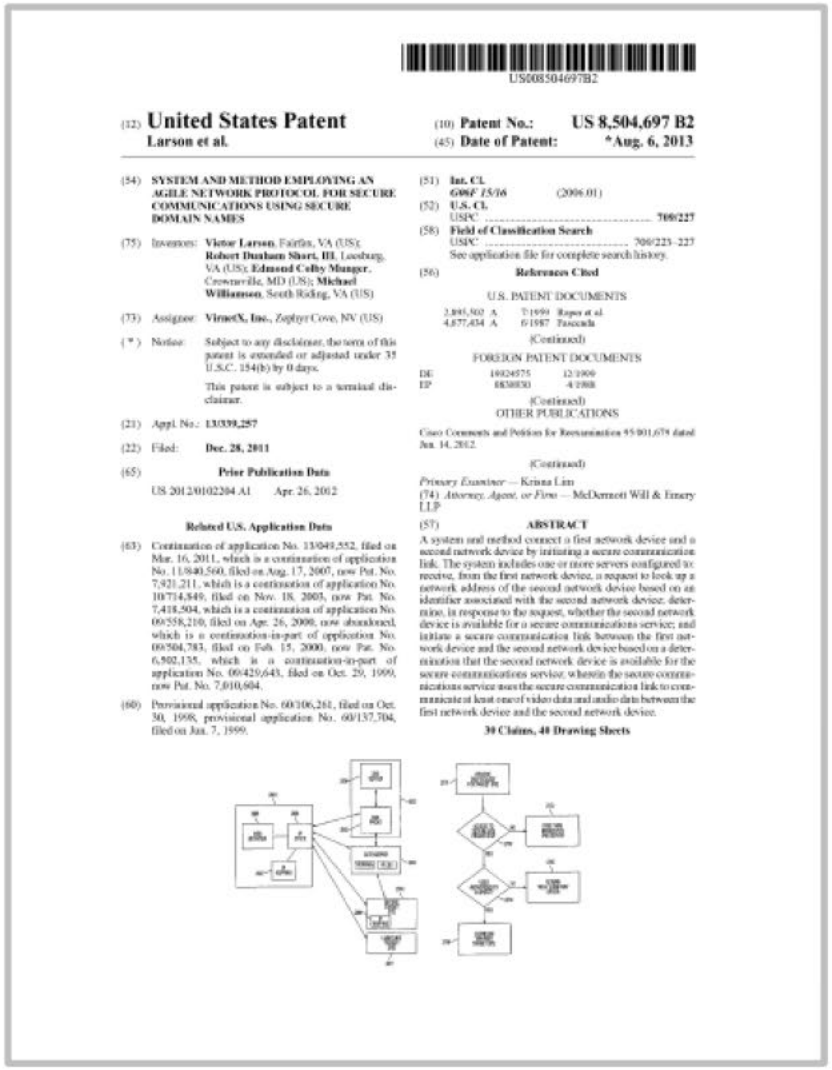
Patent Owner's Demonstrative Exhibits

Inter Partes Review of U.S. Patent No. 8,504,697 Case No. IPR2014-00237 Case No. IPR2014-00238

Oral Hearing: February 9, 2015

Background

The ’697 Patent



US008504697B2

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

(10) **Patent No.: US 8,504,697 B2**
(45) **Date of Patent: *Aug. 6, 2013**

(54) **SYSTEM AND METHOD EMPLOYING AN AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES**

(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: **VirnetX, Inc.**, Zephyr Cove, NV (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

This patent is subject to a terminal disclaimer.

(21) Appl. No.: **13/339,257**

(22) Filed: **Dec. 28, 2011**

(65) **Prior Publication Data**

US 2012/0102204 A1 Apr. 26, 2012

Related U.S. Application Data

(63) Continuation of application No. 13/048,552, filed on Mar. 16, 2011, which is a continuation of application No. 11/840,560, filed on Aug. 17, 2007, now Pat. No. 7,921,211, which is a continuation of application No. 10/714,849, filed on Nov. 18, 2003, now Pat. No. 7,418,504, which is a continuation of application No. 09/558,210, 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 15/16 (2006.01)

(52) **U.S. Cl.**
USPC **709/227**

(58) **Field of Classification Search**
USPC 709/223–227
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

2,895,502 A 7/1959 Rapee et al.
4,877,434 A 6/1987 Tascarella

(Continued)

FOREIGN PATENT DOCUMENTS

DE 19824575 12/1999
EP 0838930 4/1998

(Continued)

OTHER PUBLICATIONS

Cisco Comments and Petition for Reexamination 95/001,679 dated Jun. 14, 2012.

(Continued)

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

(57) **ABSTRACT**

A system and method connect a first network device and a second network device by initiating a secure communication link. The system includes one or more servers configured to: receive, from the first network device, a request to look up a network address of the second network device based on an identifier associated with the second network device; determine, in response to the request, whether the second network device is available for a secure communications service; and initiate a secure communication link between the first network device and the second network device based on a determination that the second network device is available for the secure communications service, wherein the secure communications service uses the secure communication link to communicate at least one of video data and audio data between the first network device and the second network device.

30 Claims, 40 Drawing Sheets

Ex. 1001, ’697 Patent

The ’697 Patent

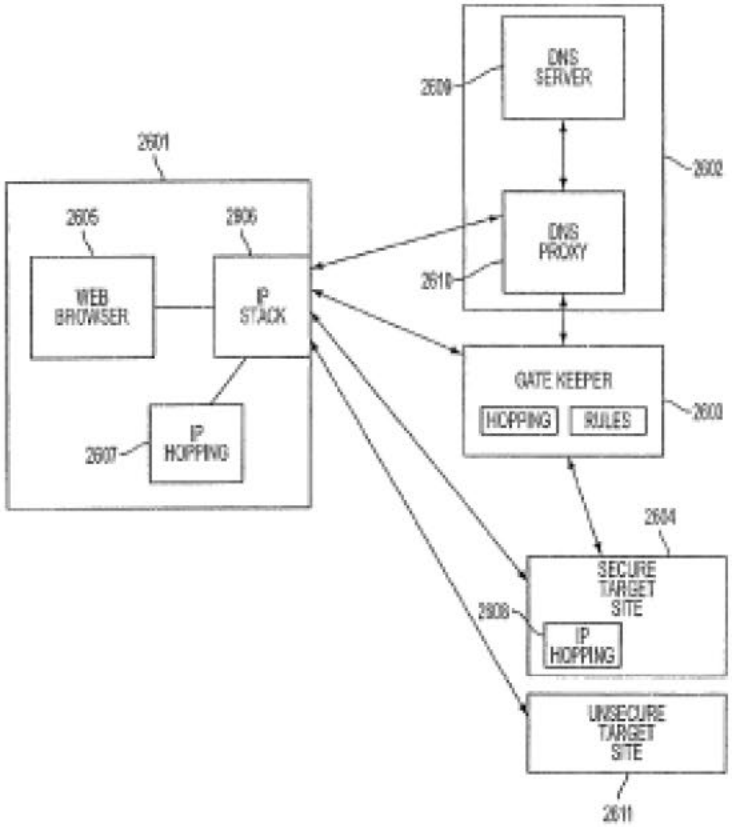


FIG. 26

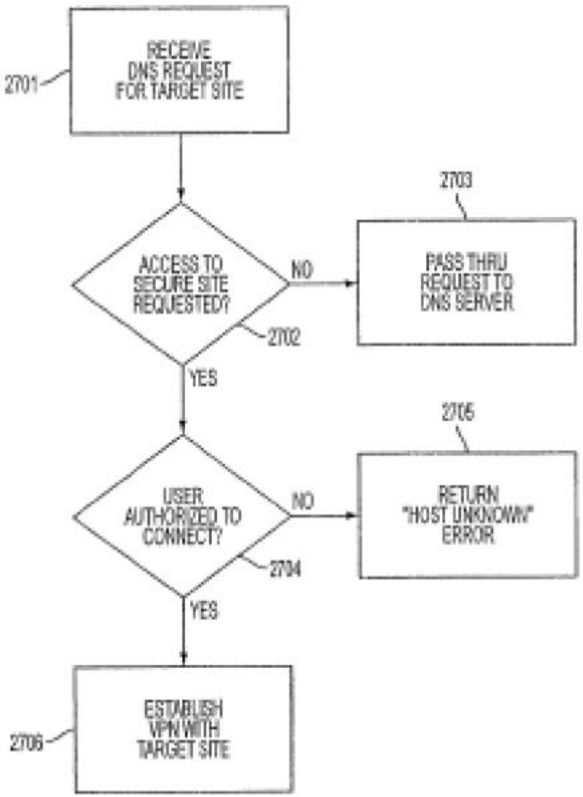


FIG. 27

Ex. 1001, ’697 Patent

The ’697 Patent: Independent Claim 1

1. A method of connecting a first network device and a second network device, the method comprising:

intercepting, from the first network device, a request to look up an internet protocol (IP) address of the second network device based on a domain name associated with the second network device;

determining, in response to the request, whether the second network device is available for a secure communications service; and

initiating a secure communication link between the first network device and the second network device based on a determination that the second network device is available for the secure communications service;

wherein the secure communications service uses the secure communication link to communicate at least one of video data and audio data between the first network device and the second network device.

Ex. 1001, ’697 Patent, Claim 1

The ’697 Patent: Independent Claim 16

16. A system for connecting a first network device and a second network device, the system including one or more servers configured to:

intercept, from the first network device, a request to look up an internet protocol (IP) address of the second network device based on a domain name associated with the second network device;

determine, in response to the request, whether the second network device is available for a secure communications service; and

initiate a secure communication link between the first network device and the second network device based on a determination that the second network device is available for the secure communications service,

wherein the secure communications service uses the secure communication link to communicate at least one of video data and audio data between the first network device and the second network device.

Ex. 1001, ’697 Patent, Claim 16

Instituted Grounds

- IPR2014-00237
  - Claims 1-11, 14-25, and 28-30 are anticipated by Beser
  - Claims 1-11, 14-25, and 28-30 are obvious over Beser in view of RFC 2401
- IPR2014-00238
  - Claims 1-3, 8-11, 14-17, 22-25, and 28-30 are anticipated by Wesinger
  - Claims 4-7 and 18-21 are obvious over Wesinger in view of RFC 2543

Claim Construction

"secure communication link"

Patent Owner's Proposed Construction	Apple's Proposed Construction	Board's Preliminary Construction
A direct communication link that provides data security through encryption	A communication link in which computers privately and directly communicate with each other on insecure paths between the computers where the communication is both secure and anonymous, and where the data transferred may or may not be encrypted	A transmission path 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 10

"Authentication" and "Address Hopping"

- Decision

> Based on the foregoing, using a plain and ordinary construction in light of the '697 Patent, the broadest reasonable construction of the term "secure communication link" is a transmission path 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.

Decision at 10

- Patent Owner's Response

> The Decision's construction is also technically flawed. Of the obfuscation methods in the construction—authentication, encryption, and address hopping—only encryption restricts access to "data, addresses, or other information on the path," as required by the first portion of the construction. (Ex. 2025 at 11, ¶ 15, Monrose Decl.) The other techniques alone do not provide the claimed security.

Patent Owner Response at 11

Disclaimer

- Prosecution History: Patent Owner's Response to Office Action of Dec. 29, 2011

> One of ordinary skill in the art would have understood a secure communication link to require encryption. (*Id.*)

Ex. 1056 at 25, Patent Owner's Response to Office Action of Dec. 29, 2011

- Apple's Petition

> [2] In the grandparent of the present patent (*i.e.*, the '504 patent), Patent Owner unequivocally disclaimed secure communication links that did not employ encryption. *See* Ex. 1056 at 25.

Petition at 10 n.2 in IPR2014-00237

District Court

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

VIRNETX INC.,

Plaintiff,

vs.

CISCO SYSTEMS, INC. et al.,

Defendants.

Before the Court is Defend

term "Secure Communication Link

In light of VirnetX's

Reconsideration (Docket No. 424),

(Docket No. 366). The term "s

communication link that provides data security through encryption."

So ORDERED and SIGNED this 4th day of October, 2012.

LEONARD DAVIS
UNITED STATES DISTRICT JUDGE

VIRNETX EXHIBIT 2003
Apple v. VirnetX
Trial IPR2014-00237

In light of VirnetX's Notice of Non-Opposition to Defendant's Motion for Reconsideration (Docket No. 424), the Court GRANTS Defendants' Motion for Reconsideration (Docket No. 366). The term "secure communication link" is construed to mean "a direct communication link that provides data security through encryption."

Ex. 2003

"intercepting . . . a request to look up an internet protocol (IP) address"

Patent Owner's Proposed Construction	Apple's Proposed Construction	Board's Preliminary Construction
No construction necessary; alternatively, receiving a request to look up an internet protocol address and, apart from resolving it into an address, performing an evaluation on it related to establishing a secure communication link	A proxy computer or device receiving and acting on a request sent by a first computer that was intended for another computer	Receiving a request pertaining to a first entity at another entity

Patent Owner Response at 23

Patent Owner's Construction: "performing an evaluation . . ."

- Patent Owner's Response

> However, the '697 patent goes on to explain that the claimed embodiments differ from conventional DNS, in part, because they apply an additional layer of functionality to a request to look up a network address beyond merely resolving it and returning the network address. (Ex. 2025 at 17, ¶ 24, Monrose Decl.) For

Patent Owner Response at 25

"determining, in response to the request, whether the second network device is available for a secure communications service"

Patent Owner's Proposed Construction	Apple's Proposed Construction	Board's Preliminary Construction
No construction proposed	No construction proposed	Includes determining one or more of 1) whether the device is listed with a public internet address, and if so, allocating a private address for the second network device, or 2) some indication of the relative permission level or security privileges of the requester

Patent Owner Response at 27

"determining, in response to the request, whether the second network device is available for a secure communications service"

- Decision

> Based on the record, "determining, in response to the request, whether the second network device is available for a secure communications," includes determining, one or more of 1) whether the device is listed with a public internet address, and if so, allocating a private address for the second network device, or 2) some indication of the relative permission level or security privileges of the requester.

Decision at 15

"determining, in response to the request, whether the second network device is available for a secure communications service"

- '697 Patent

> According to one embodiment, DNS proxy **2610** intercepts all DNS lookup functions from client **2605** and determines whether access to a secure site has been requested. If access to a secure site has been requested (as determined, for example, by a domain name extension, or by reference to an internal table of such sites), DNS proxy **2610** determines whether the user has sufficient security privileges to access the site.

Ex. 1001 at 40:31-37, '697 Patent

"determining, in response to the request, whether the second network device is available for a secure communications service"

- Decision

> Based on the record, "determining, in response to the request, whether the second network device is available for a secure communications," includes determining, one or more of 1) whether the device is listed with a public internet address, and if so, allocating a private address for the second network device, or 2) some indication of the relative permission level or security privileges of the requester.

Decision at 15

"determining, in response to the request, whether the second network device is available for a secure communications service"

- Patent Owner's Response

> The claimed determination, however, expressly focuses on the second network device (Ex. 1001, claims 1 and 16, "whether the second network device is available for a secure communications service," emphasis added), so the "determining" phrase need not be limited to the Decision's determining "permission level or security privileges of the requester."

Patent Owner Response at 29-30

"virtual private network"

Patent Owner's Proposed Construction	Apple's Proposed Construction	Board's Preliminary Construction
No construction proposed	No construction proposed	A secure communication link with the additional requirement that the link includes a portion of a public network

Patent Owner Response at 19

"modulation"

Patent Owner's Proposed Construction	Apple's Proposed Construction	Board's Preliminary Construction
No construction necessary; alternatively, the process of encoding data for transmission over a medium by varying a carrier signal	The process of encoding data for transmission over a physical or electromagnetic medium by varying a carrier signal	The process of encoding data for transmission

Preliminary Response at 28
Decision at 14

"secure communications service"

Patent Owner's Proposed Construction	Apple's Proposed Construction	Board's Preliminary Construction
The functional configuration of a network device that enables it to participate in a secure communications link with another network device	The functional configuration of a computer that enables it to participate in a secure communications link with another computer	The functional configuration of a network device that enables it to participate in a secure communications link with another network device

Preliminary Response at 28
Decision at 14

Instituted Grounds (IPR2014-00237)

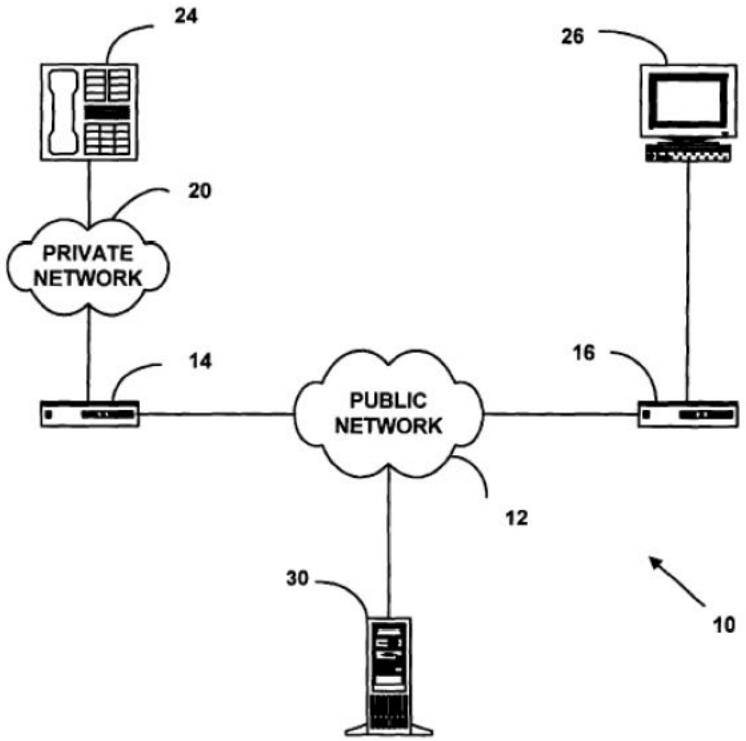
Instituted Grounds: IPR2014-00237

- 35 U.S.C. § 102
  - Claims 1-11, 14-25, and 28-30 are anticipated by Beser
- 35 U.S.C. § 103
  - Claims 1-11, 14-25, and 28-30 are obvious over Beser in view of RFC 2401

Decision at 33

Beser

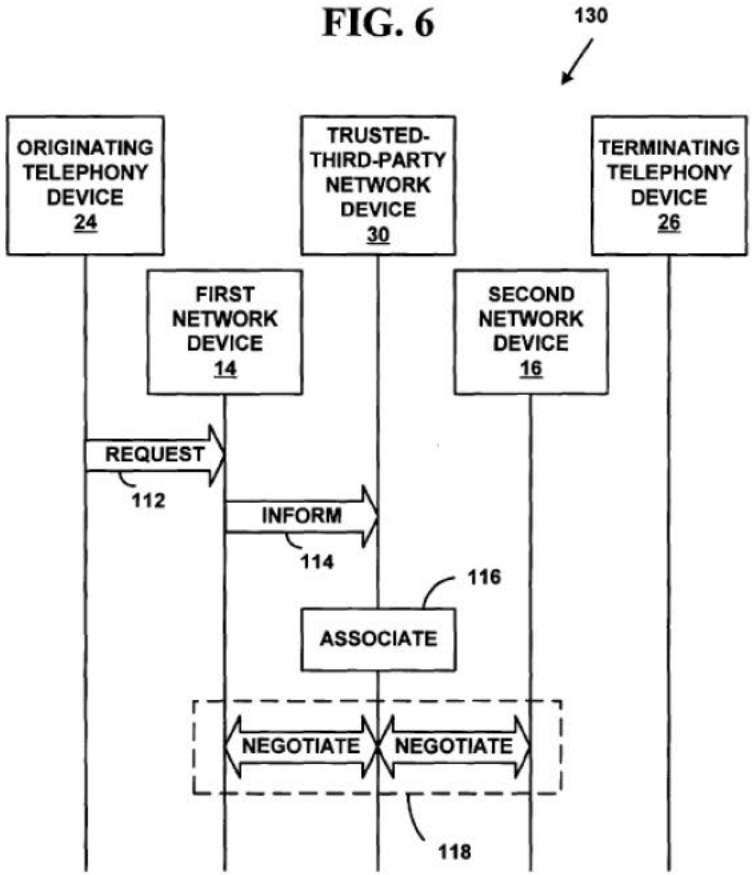
FIG. 1



Ex. 1009, Fig. 1

Beser

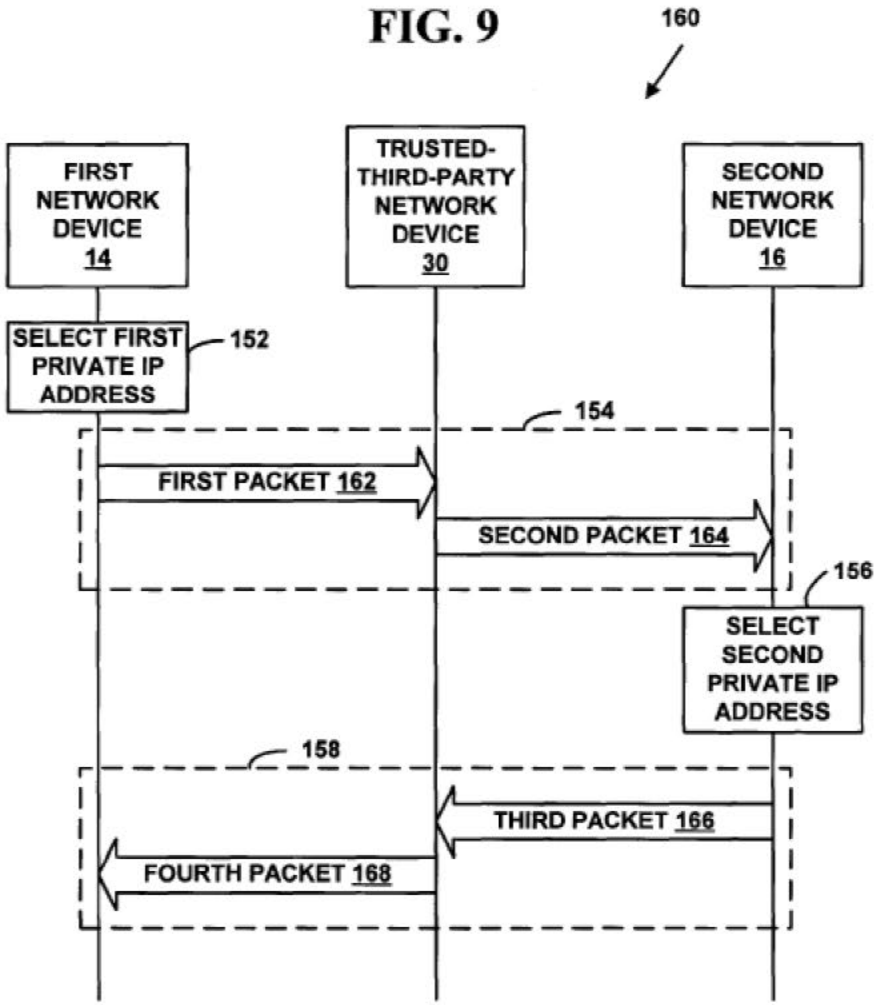
FIG. 6



Ex. 1009, Fig. 6

Beser

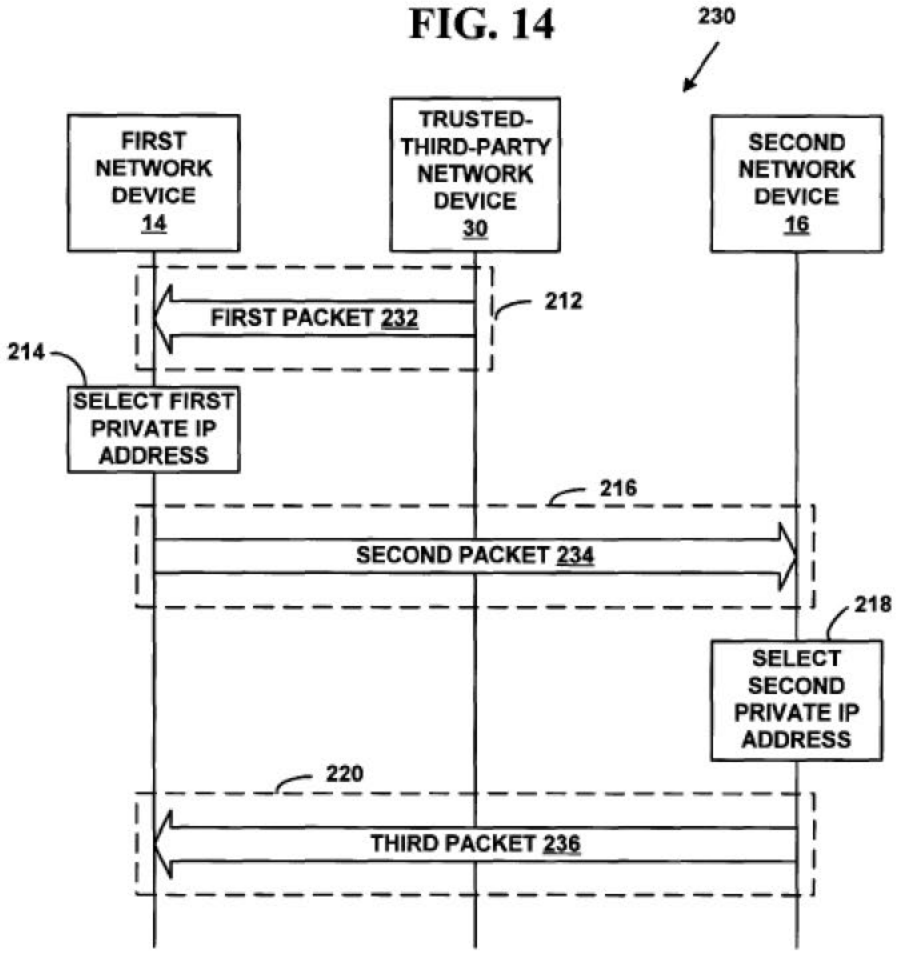
FIG. 9



Ex. 1009, Fig. 9

Beser

FIG. 14



Ex. 1009, Fig. 14

Instituted Grounds: IPR2014-00237

- 35 U.S.C. § 102
  - Claims 1-11, 14-25, and 28-30 are anticipated by Beser
- 35 U.S.C. § 103
  - Claims 1-11, 14-25, and 28-30 are obvious over Beser in view of RFC 2401

Decision at 33

Beser

1. A method of connecting a first network device and a second network device, the method comprising:

intercepting, from the first network device, a request to look up an internet protocol (IP) address of the second network device based on a domain name associated with the second network device;

determining, in response to the request, whether the second network device is available for a secure communications service; and

initiating a secure communication link between the first network device and the second network device based on a determination that the second network device is available for the secure communications service;

wherein the secure communications service uses the secure communication link to communicate at least one of video data and audio data between the first network device and the second network device.

Ex. 1001, '697 Patent, Claim 1

"intercepting . . . a request to look up an internet protocol (IP) address"

Patent Owner's Proposed Construction	Apple's Proposed Construction	Board's Preliminary Construction
No construction necessary; alternatively, receiving a request to look up an internet protocol address and, apart from resolving it into an address, performing an evaluation on it related to establishing a secure communication link	A proxy computer or device receiving and acting on a request sent by a first computer that was intended for another computer	Receiving a request pertaining to a first entity at another entity

Patent Owner Response at 23

"intercepting . . . a request to look up an internet protocol (IP) address"

- Decision

> domain name associated with the second network device." According to Mr. Fratto, device 14, a router, intercepts requests from other originating or first network devices. *See* Ex. 1003 ¶ 355. According further to Mr. Fratto, a router evaluates all traffic flowing through it, and if a packet contains a request for initiating an IP tunnel, it will send the request to trusted-third-party network device 30.

Decision at 20-21

A Request to Initiate Tunneling Is Not an IP Address Lookup Request

- Patent Owner's Response

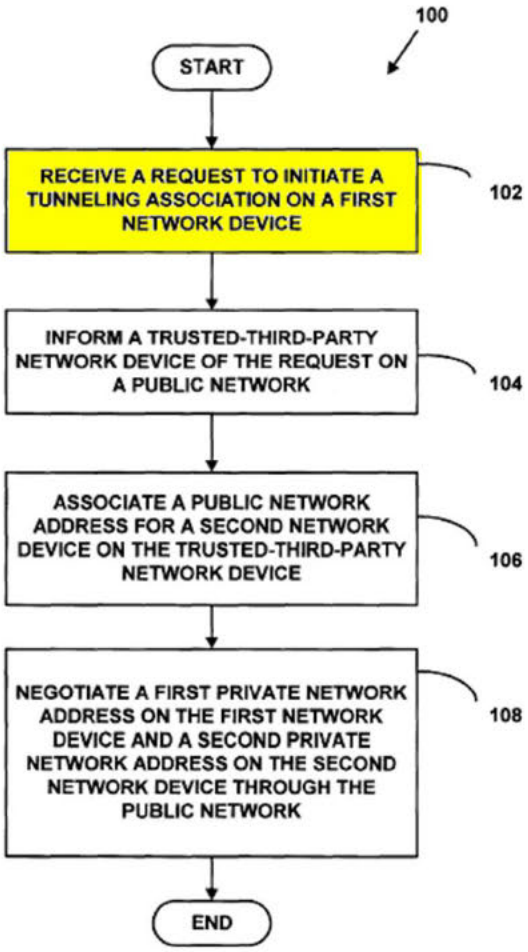
> connection.") A request to initiate a tunneling connection, even if it happens to include a domain name in some embodiments, does not convert the tunneling request into the claimed "request to look up an internet protocol (IP) address of the second network device," as recited in claim 1. (Ex. 2025 at 25, ¶ 40, Monrose Decl.) Whether the request includes a domain name or some other type of

Patent Owner Response at 37

A Request to Initiate Tunneling Is Not an IP Address Lookup Request

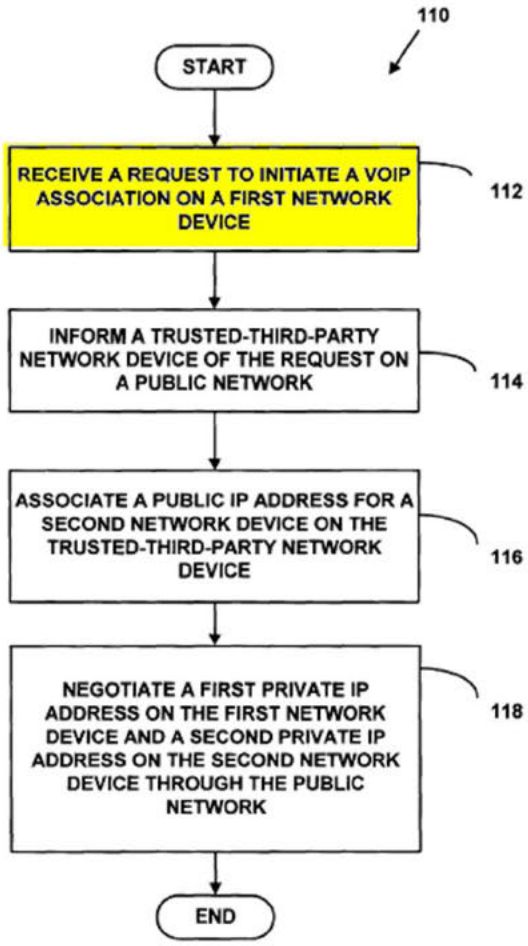
- Beser

FIG. 4



Ex. 1009 at Fig. 4

FIG. 5



Ex. 1009 at Fig. 5

"intercepting . . . a request to look up an internet protocol (IP) address"

- Decision

> Mr. Fratto and Petitioner alternatively reason that trusted-third-party device 30, a domain name server, intercepts the request from the recited first network device, originating device 24, because the request includes a unique identifier, including a domain name, that identifies the terminating end 26, or second network device, of the tunneling association, instead of the trusted-third-party. *See* Pet. 18–19; Ex. 1003 ¶¶ 305–306, 357–358. Pursuant to the request, trusted-third-party device 30 negotiates a private internet address, in part by looking up a public internet address based on the domain name associated with "second network device" 26, as claim 1 requires.

Decision at 21

Device 30 Does Not Translate Domain Names to IP Addresses

- Patent Owner's Response

> Moreover, the trusted-third-party network device 30 does not perform any translation into an IP address of the domain name of the terminating device 26. (Ex. 2025 at 25-26, ¶ 41, Monrose Decl.) After being informed of the request, trusted-third-party network device 30 associates an identifier (e.g., a domain name) of terminating device 26 with a public IP address of a second network device 16.

Patent Owner Response at 37

- Beser

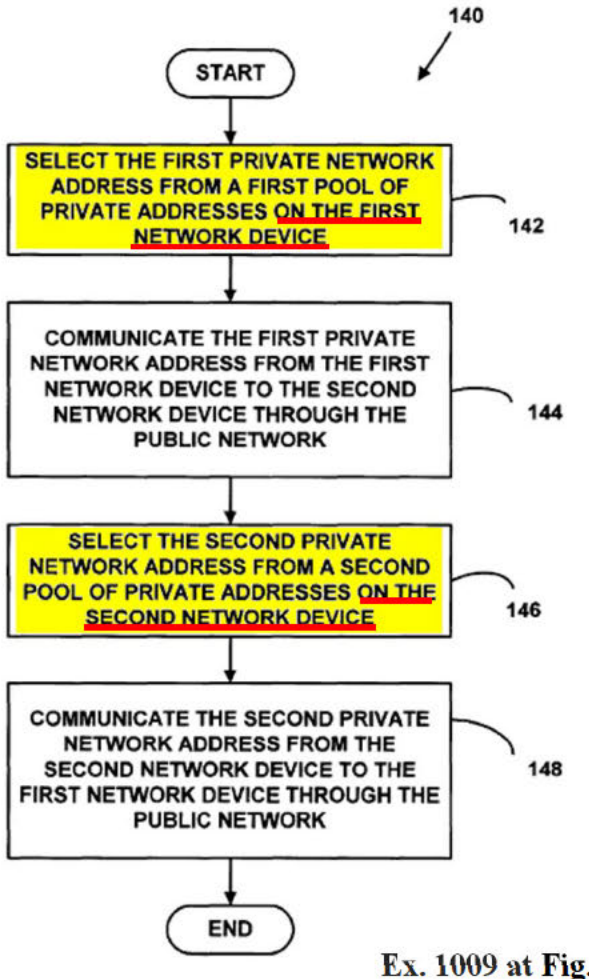
> A public IP **58** address for a second network device **16** is associated with the unique identifier for the terminating telephony device **26** at Step **116**. The second network device **16** is associated with the terminating telephony device **26**. This association of the public IP **58** address for the second network device **16** with the unique identifier is made on the trusted-third-party network device **30**. In one exemplary

Ex. 1009 at 11:26-32

Devices 14 and 16 Negotiate Private Addresses Themselves

- Beser

FIG. 7



Ex. 1009 at Fig. 7

Beser

1. A method of connecting a first network device and a second network device, the method comprising:

intercepting, from the first network device, a request to look up an internet protocol (IP) address of the second network device based on a domain name associated with the second network device;

determining, in response to the request, whether the second network device is available for a secure communications service; and

initiating a secure communication link between the first network device and the second network device based on a determination that the second network device is available for the secure communications service;

wherein the secure communications service uses the secure communication link to communicate at least one of video data and audio data between the first network device and the second network device.

Ex. 1001, '697 Patent, Claim 1

"determining, in response to the request, whether the second network device is available for a secure communications service"

Patent Owner's Proposed Construction	Apple's Proposed Construction	Board's Preliminary Construction
No construction proposed	No construction proposed	Includes determining one or more of 1) whether the device is listed with a public internet address, and if so, allocating a private address for the second network device, or 2) some indication of the relative permission level or security privileges of the requester

Patent Owner Response at 27

"determining, in response to the request, whether the second network device is available for a secure communications service"

- Apple's Petition

> Consequently, when methods shown in Beser are performed, they will necessarily determine if a second network device is available for secure communications.

Petition at 21

- Decision

> On this record, Beser's system satisfies the determining step, because as outlined above in the claim construction section, determining the availability of second network device 26 for secure communication service reasonably includes determining that the device has a private internet address assigned to it, and that the originating device, device 24, has authorization to communicate, or a private network address assigned to it, or both. *See* Pet. 19–21; Ex. 1003 ¶¶ 363–371.

Decision at 23

"determining, in response to the request, whether the second network device is available for a secure communications service"

- Apple's Petition

> Consequently, when methods shown in Beser are performed, they will necessarily determine if a second network device is available for secure communications.

Petition at 21

Beser Does Not Teach Apple's Hypothetical System

- Patent Owner's Response

> *Beser* does not disclose what would happen in Apple's undisclosed hypothetical system in which "a domain name in a request is recognized by the trusted-third-party network device but does not map to a device requiring negotiation of an IP tunnel." (Ex. 2025 at 28, ¶ 45, Monrose Decl.) The DNS server in *Beser* could operate in a number of ways contrary to the way Apple suggests.

Patent Owner Response at 42

"determining, in response to the request, whether the second network device is available for a secure communications service"

- Decision

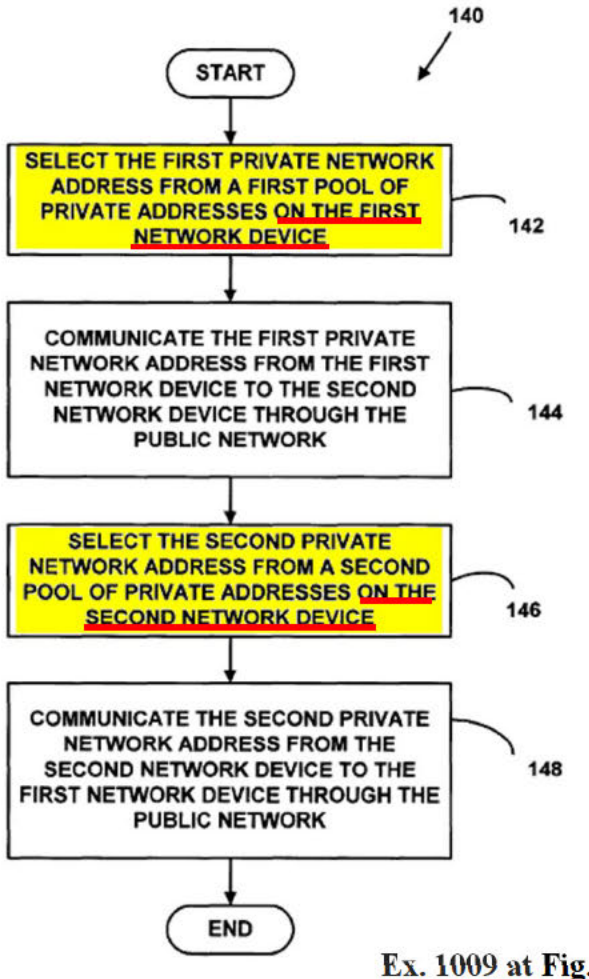
> On this record, Beser's system satisfies the determining step, because as outlined above in the claim construction section, determining the availability of second network device 26 for secure communication service reasonably includes determining that the device has a private internet address assigned to it, and that the originating device, device 24, has authorization to communicate, or a private network address assigned to it, or both. *See* Pet. 19–21; Ex. 1003 ¶¶ 363–371.

Decision at 23

Devices 14 and 16 Negotiate Private Addresses Themselves

- Beser

FIG. 7



Ex. 1009 at Fig. 7

Beser's Tunnel Establishment Is Not In Response to a DNS Request

- Patent Owner's Response

> In particular, *Beser*'s tunnel-establishment process occurs in response to *Beser*'s request to initiate a tunnel, but that request is not a "DNS" request that might result in a domain name server performing Mr. Fratto's "known DNS operations." (Ex. 2025 at 31-32, ¶ 50, Monrose Decl.) *Beser* provides no teaching on this issue. Also, a "DNS" request has no role in *Beser*'s tunnel-establishment process, so *Beser*'s system would not perform the tunnel-establishment process in response to a "DNS" request. (*Id.*)

Patent Owner Response at 46-47

A Conventional DNS Would Not Implement Beser's Tunnel Establishment

- Patent Owner's Response

> Similarly, if *Beser*'s trusted-third-party network device included a conventional domain name server, the domain name server would only be capable of performing "known DNS operations" in response to a "DNS" request. (*Id.*) It would be unable to recognize or process *Beser*'s request to initiate a tunnel, much less be capable of carrying out *Beser*'s tunnel-establishment process. (*Id.*)

Patent Owner Response at 47,
Citing Ex. 2025 at ¶ 50, Monrose Decl.

"determining, in response to the request, whether the second network device is available for a secure communications service"

- Decision

> On this record, Beser's system satisfies the determining step, because as outlined above in the claim construction section, determining the availability of second network device 26 for secure communication service reasonably includes determining that the device has a private internet address assigned to it, and that the originating device, device 24, has authorization to communicate, or a private network address assigned to it, or both. *See* Pet. 19–21; Ex. 1003 ¶¶ 363–371.

Decision at 23

The Unique Identifier Does Not Indicate Authorization of Device 24

- Patent Owner's Response

> *Beser* discloses two items sent from first network device 24, but neither pertains to authorization. (Ex. 2025 at 32-33, ¶ 52, Monrose Decl.) The first is a unique identifier associated with device 26 (i.e., the identifier indicating the end device with which the requesting device wishes to communicate), but the unique identifier associated with device 26 provides no indication of the authorization of device 24. (*See, e.g.*, Ex. 1009 at 10:4-6; Ex. 2025 at 32-33, ¶ 52, Monrose Decl.)

Patent Owner Response at 48

- Beser

> Step **112**. The first network device **14** is associated with the originating telephony device **24**, and the request includes a unique identifier for the terminating telephony device **26**. In

Ex. 1009 at 10:4-6

The Bit Sequence Does Not Indicate Authorization of Device 24

- Patent Owner's Response

> The second is a bit sequence from device 24 that "indicates to the tunnelling application that it should examine the informing message for its content and not ignore the datagram." (Ex. 1009 at 8:35-9:1; Ex. 2025 at 32-33, ¶ 52, Monrose Decl.) It says nothing about device 24's authorization.

Patent Owner Response at 48

- Beser

> higher layer. For example, the indicator may be a distinctive sequence of bits at the beginning of a datagram that has been passed up from the network and transport layers. By methods known to those skilled in the art, the distinctive sequence of bits indicates to the tunneling application that it should examine the request message for its content and not ignore the datagram. However, the higher layer may be other

Ex. 1009 at 8:37-43

Beser Does Not Disclose "initiating a secure communication link . . . ."

1. A method of connecting a first network device and a second network device, the method comprising:

intercepting, from the first network device, a request to look up an internet protocol (IP) address of the second network device based on a domain name associated with the second network device;

determining, in response to the request, whether the second network device is available for a secure communications service; and

initiating a secure communication link between the first network device and the second network device based on a determination that the second network device is available for the secure communications service;

wherein the secure communications service uses the secure communication link to communicate at least one of video data and audio data between the first network device and the second network device.

Ex. 1001, '697 Patent, Claim 1

"secure communication link"

Patent Owner's Proposed Construction	Apple's Proposed Construction	Board's Preliminary Construction
A direct communication link that provides data security through encryption	A communication link in which computers privately and directly communicate with each other on insecure paths between the computers where the communication is both secure and anonymous, and where the data transferred may or may not be encrypted	A transmission path 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 10

"secure communication link"

- Apple's Petition

> tunnel based on the results of that evaluation. Ex. 1003 at ¶¶ 302-309. Beser explains that IP traffic within an IP tunnel ordinarily will be encrypted utilizing the techniques described in RFC 2401 (*i.e.*, under the IPsec protocol), and that encryption of the tunneling connection occurs automatically. Ex. 1003 at ¶¶ 268-

Petition at 22

- Decision

> Based on the this determination of availability that involves negotiating between first and second network devices 24 and 26, Beser's system initiates a communication between the two devices, which includes audio or video data, or both, satisfying the last two clauses of claim 1 and similar clauses in claim 16.

Decision at 23

"secure communication link"

- Apple's Petition

> tunnel based on the results of that evaluation. Ex. 1003 at ¶¶ 302-309. Beser explains that IP traffic within an IP tunnel ordinarily will be encrypted utilizing the techniques described in RFC 2401 (*i.e.*, under the IPsec protocol), and that encryption of the tunneling connection occurs automatically. Ex. 1003 at ¶¶ 268-

Petition at 22

Beser Does Not Teach Encryption of Traffic on the Tunnel

- Apple's Previous Admission Regarding Beser

> A person of ordinary skill in the art would have relied on Kent to modify the design of Beser to incorporate IPsec to encrypt all traffic being sent in IP tunnels between a first and second network device in the IP tunneling procedures being described in Beser, rather than to encrypt only the traffic used to establish the IP tunnel. Accordingly, Beser in view of Kent would have rendered obvious claim 1 under 35 U.S.C. § 103.

Ex. 2029 at 2, Apple's Request for *Inter Partes* Reexamination in Control No. 95/001,682
***See also* PO Response at 51**

Beser Teaches Away from Using Encryption

- Dr. Monrose's Declaration

> Given *Beser*'s extensive teaching away from encryption and its associated computational burdens, *Beser* never discloses using encryption or other similarly burdensome techniques for transmitting data through its tunnels.

Ex. 2025 at ¶ 56, Monrose Decl.

- Beser

BACKGROUND OF THE INVENTION

> packet that is transmitted on the public network. The tunneled IP packets, however, may need to be encrypted before the encapsulation in order to hide the source IP address. Once again, due to computer power limitations, this form of tunneling may be inappropriate for the transmission of multimedia or VoIP packets.

Ex. 1009 at 2:12-17

"secure communication link"

- Decision

> Based on the this determination of availability that involves negotiating between first and second network devices 24 and 26, Beser's system initiates a communication between the two devices, which includes audio or video data, or both, satisfying the last two clauses of claim 1 and similar clauses in claim 16.

Decision at 23

Beser Does Not Teach Encryption of Audio/Video on the Tunnel

- Patent Owner's Response

> In the first cited passage, *Beser* discloses that some packets "may require encryption or authentication to ensure that the unique identifier cannot be read on the public network." (Ex. 1009 at 11:22-25.) These packets, however, are not communicated between device 24 and device 26 (i.e., over the tunnel). (Ex. 2025 at 35-36, ¶ 58, Monrose Decl.) Rather, the surrounding passages make clear that these packets are transmitted from the network device 14 to the trusted-third-party network device 30 during *Beser*'s "inform" step as part of setting up the tunnel—not over the tunnel after it is established. (*See* Ex. 1009 at 11:9-25; FIG. 6, 114 "INFORM"; Ex. 2025 at 35-36, ¶ 58, Monrose Decl.) *Beser* also does not state that these packets contain any video or audio data, and they do not.

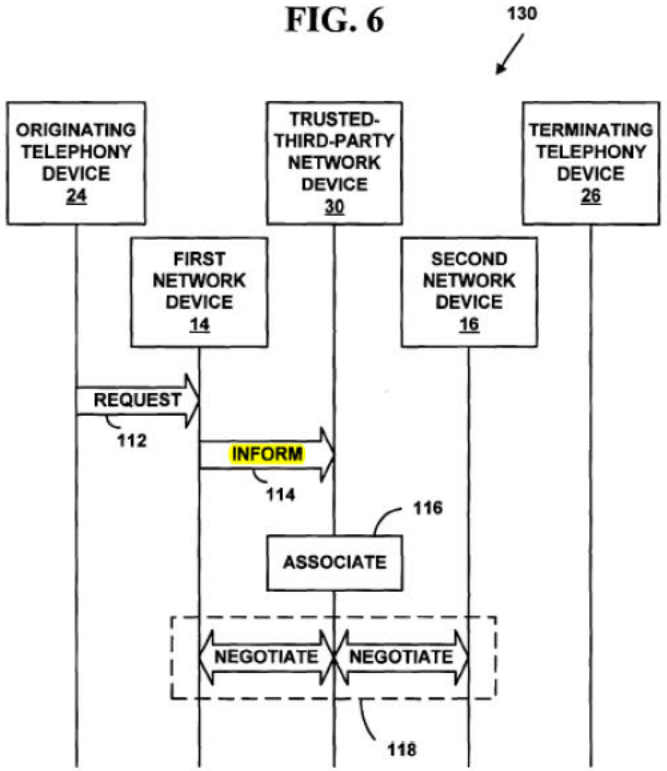
Patent Owner Response at 52-53

Beser Does Not Teach Encryption of Audio/Video on the Tunnel

- Beser

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**.

Ex. 1009 at 11:9-25



Ex. 1009, Fig. 6

Beser Does Not Incorporate IPsec by Reference

- Beser

BACKGROUND OF THE INVENTION

Of course, the sender may encrypt the information inside the IP packets before transmission, e.g. with IP Security ("IPSec"). However, accumulating all the packets from one source address may provide the hacker with sufficient information to decrypt the message. Moreover, encryption at the source and decryption at the destination may be infeasible for certain data formats. For example, streaming data flows, such as multimedia or Voice-over-Internet-Protocol ("VoIP"), may require a great deal of computing power to encrypt or decrypt the IP packets on the fly. The increased strain on computer power may result in jitter, delay, or the loss of some packets. The expense of added computer power might also dampen the customer's desire to invest in VoIP equipment.

Ex. 1009 at 1:40-67

Beser Does Not Incorporate IPsec by Reference

- Patent Owner's Response

> First, even if *Beser* had incorporated IPsec by reference, the teaching away from using its encryption techniques would lead one of ordinary skill to understand that none of *Beser*'s embodiments employ IPsec. This explains why *Beser* never mentions using IPsec or encryption for any data on its tunnels.
>
> Second, *Beser*'s brief mention of IPsec is not a legal incorporation by reference of that protocol. "To incorporate matter by reference, a host document must contain language 'clearly identifying the subject matter which is incorporated and where it is to be found'; a '*mere reference* to another application, or patent, or publication is not an *incorporation* of anything therein.'" *Callaway Golf Co. v. Acushnet Co.*, 576 F.3d 1331, 1346 (Fed. Cir. 2009) (*emphasis original*).

Patent Owner Response at 54

Beser: Claims 2 and 24

2. The method of claim **1**, wherein at least one of the video data and the audio data is encrypted over the secure communication link.

Ex. 1001, '697 Patent, Claim 2

24. The system of claim **16**, wherein at least one of the video data and the audio data is encrypted over the secure communication link.

Ex. 1001, '697 Patent, Claim 24

Beser Does Not Teach Encryption of Traffic on the Tunnel

- Apple's Previous Admission Regarding Beser

> A person of ordinary skill in the art would have relied on Kent to modify the design of Beser to incorporate IPsec to encrypt all traffic being sent in IP tunnels between a first and second network device in the IP tunneling procedures being described in Beser, rather than to encrypt only the traffic used to establish the IP tunnel. Accordingly, Beser in view of Kent would have rendered obvious claim 1 under 35 U.S.C. § 103.

Ex. 2029 at 2, Apple's Request for *Inter Partes* Reexamination in Control No. 95/001,682.
***See also* PO Response at 51**

Beser Teaches Away from Using Encryption

- Dr. Monrose's Declaration

> Given *Beser*'s extensive teaching away from encryption and its associated computational burdens, *Beser* never discloses using encryption or other similarly burdensome techniques for transmitting data through its tunnels.

Ex. 2025 at ¶ 56, Monrose Decl.

- Beser

BACKGROUND OF THE INVENTION

packet that is transmitted on the public network. The tunneled IP packets, however, may need to be encrypted before the encapsulation in order to hide the source IP address. Once again, due to computer power limitations, this form of tunneling may be inappropriate for the transmission of multimedia or VoIP packets.

Ex. 1009 at 2:12-17

Beser Does Not Teach Encryption of Audio/Video on the Tunnel

- Patent Owner's Response

> In the first cited passage, *Beser* discloses that some packets "may require encryption or authentication to ensure that the unique identifier cannot be read on the public network." (Ex. 1009 at 11:22-25.) These packets, however, are not communicated between device 24 and device 26 (i.e., over the tunnel). (Ex. 2025 at 35-36, ¶ 58, Monrose Decl.) Rather, the surrounding passages make clear that these packets are transmitted from the network device 14 to the trusted-third-party network device 30 during *Beser*'s "inform" step as part of setting up the tunnel—not over the tunnel after it is established. (*See* Ex. 1009 at 11:9-25; FIG. 6, 114 "INFORM"; Ex. 2025 at 35-36, ¶ 58, Monrose Decl.) *Beser* also does not state that these packets contain any video or audio data, and they do not.

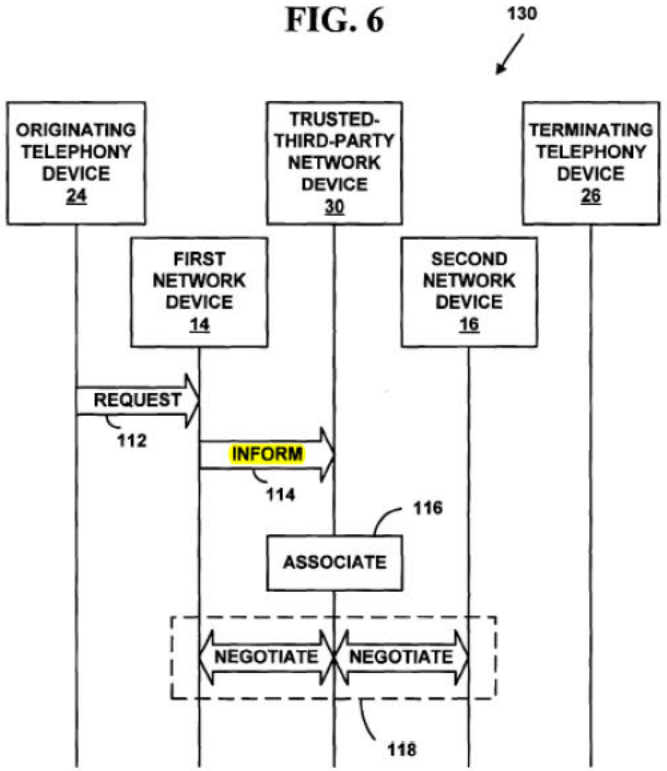
Patent Owner Response at 52-53

Beser Does Not Teach Encryption of Audio/Video on the Tunnel

- Beser

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**.

Ex. 1009 at 11:9-25



Ex. 1009, Fig. 6

Beser Does Not Incorporate IPsec by Reference

- Beser

BACKGROUND OF THE INVENTION

Of course, the sender may encrypt the information inside the IP packets before transmission, e.g. with IP Security ("IPSec"). However, accumulating all the packets from one source address may provide the hacker with sufficient information to decrypt the message. Moreover, encryption at the source and decryption at the destination may be infeasible for certain data formats. For example, streaming data flows, such as multimedia or Voice-over-Internet-Protocol ("VoIP"), may require a great deal of computing power to encrypt or decrypt the IP packets on the fly. The increased strain on computer power may result in jitter, delay, or the loss of some packets. The expense of added computer power might also dampen the customer's desire to invest in VoIP equipment.

Ex. 1009 at 1:40-67

Beser Does Not Incorporate IPsec by Reference

- Patent Owner's Response

> First, even if *Beser* had incorporated IPsec by reference, the teaching away from using its encryption techniques would lead one of ordinary skill to understand that none of *Beser*'s embodiments employ IPsec. This explains why *Beser* never mentions using IPsec or encryption for any data on its tunnels.
>
> Second, *Beser*'s brief mention of IPsec is not a legal incorporation by reference of that protocol. "To incorporate matter by reference, a host document must contain language 'clearly identifying the subject matter which is incorporated and where it is to be found'; a '*mere reference* to another application, or patent, or publication is not an *incorporation* of anything therein.'" *Callaway Golf Co. v. Acushnet Co.*, 576 F.3d 1331, 1346 (Fed. Cir. 2009) (*emphasis original*).

Patent Owner Response at 54

Beser: Claim 3

3. The method of claim **1**, wherein the secure communication link is a virtual private network communication link.

Ex. 1001, '697 Patent, Claim 3

Beser Criticizes VPNs

- Beser

BACKGROUND OF THE INVENTION

One method of thwarting the hacker is to establish a Virtual Private Network ("VPN") by initiating a tunneling connection between edge routers on the public network. For example, tunneling packets between two end-points over a public network is accomplished by encapsulating the IP packet to be tunneled within the payload field for another packet that is transmitted on the public network. The tunneled IP packets, however, may need to be encrypted before the encapsulation in order to hide the source IP address. Once again, due to computer power limitations, this form of tunneling may be inappropriate for the transmission of multimedia or VoIP packets.

Ex. 1009 at 2:6-16

Instituted Grounds: IPR2014-00237

- 35 U.S.C. § 102
  - Claims 1-11, 14-25, and 28-30 are anticipated by Beser
- 35 U.S.C. § 103
  - Claims 1-11, 14-25, and 28-30 are obvious over Beser in view of RFC 2401

Decision at 33

Beser Teaches Away from Using Encryption and IPsec

- Dr. Monrose's Declaration

> RFC 2401, however, is the Network Working Group document outlining the standards for the IPsec protocol, which is the very feature *Beser* suggests not to use. *Beser* acknowledges the existence of the IPsec protocol, but then recognizes its problems for video or audio data. Thus, in my opinion, *Beser* would lead one of ordinary skill in the art away from RFC 2401 and the proposed combination of *Beser* and RFC 2401.

Ex. 2025 at ¶ 61, Monrose Decl.

Beser Teaches Away from Using Encryption and IPsec

- Beser

> Of course, the sender may encrypt the information inside the IP packets before transmission, e.g. with IP Security ("IPSec"). However, accumulating all the packets from one source address may provide the hacker with sufficient information to decrypt the message. Moreover, encryption at the source and decryption at the destination may be infeasible for certain data formats. For example, streaming data flows, such as multimedia or Voice-over-Internet-Protocol ("VoIP"), may require a great deal of computing power to encrypt or decrypt the IP packets on the fly. The increased strain on computer power may result in jitter, delay, or the loss of some packets. The expense of added computer power might also dampen the customer's desire to invest in VoIP equipment.

Ex. 1009 at 1:54-67

Instituted Grounds (IPR2014-00238)

Instituted Grounds: IPR2014-00238

- 35 U.S.C. § 102
  - Claims 1-3, 8-11, 14-17, 22-25, and 28-30 are anticipated by Wesinger
- 35 U.S.C. § 103
  - Claims 4-7 and 18-21 are obvious over Wesinger in view of RFC 2543

Decision at 22

Wesinger

The configuration of FIG. **4**, however, further allows the physical firewall machines **407** and **408** to share the aggregate processing load of current connections. Load sharing may be achieved in the following manner. Each of the DNS modules of all of the machines receive all DNS queries, because the machines are connected in parallel. Presumably, the DNS module of the machine that is least busy will be the first to respond to a query. An ensuing connection request is then mapped to a virtual host on the responding least-busy machine.

Ex. 1008 at 13:6-15

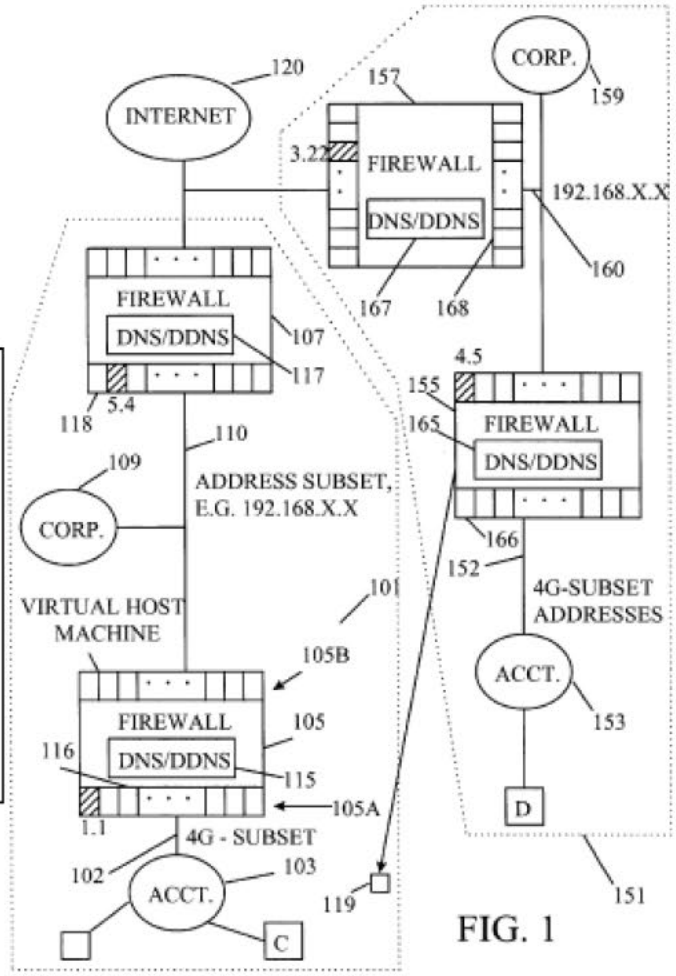


FIG. 1

Ex. 1008, Fig. 1

Wesinger

The configuration of FIG. **4**, however, further allows the physical firewall machines **407** and **408** to share the aggregate processing load of current connections. Load sharing may be achieved in the following manner. Each of the DNS modules of all of the machines receive all DNS queries, because the machines are connected in parallel. Presumably, the DNS module of the machine that is least busy will be the first to respond to a query. An ensuing connection request is then mapped to a virtual host on the responding least-busy machine.

Ex. 1008 at 13:6-15

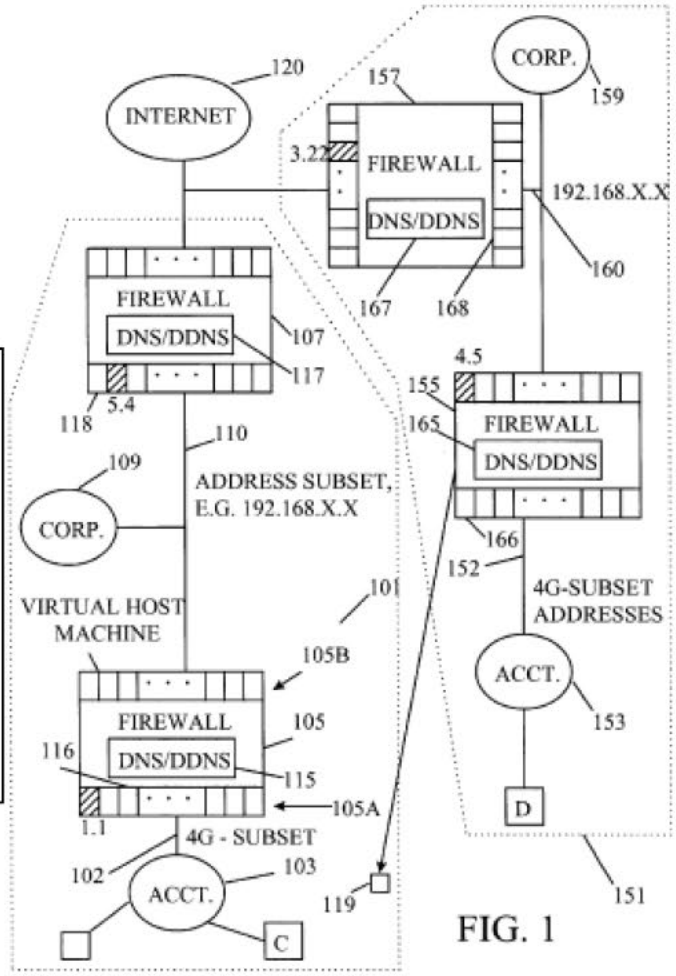


FIG. 1

Ex. 1008, Fig. 1

Wesinger

The configuration of FIG. **4**, however, further allows the physical firewall machines **407** and **408** to share the aggregate processing load of current connections. Load sharing may be achieved in the following manner. Each of the DNS modules of all of the machines receive all DNS queries, because the machines are connected in parallel. Presumably, the DNS module of the machine that is least busy will be the first to respond to a query. An ensuing connection request is then mapped to a virtual host on the responding least-busy machine.

Ex. 1008 at 13:6-15

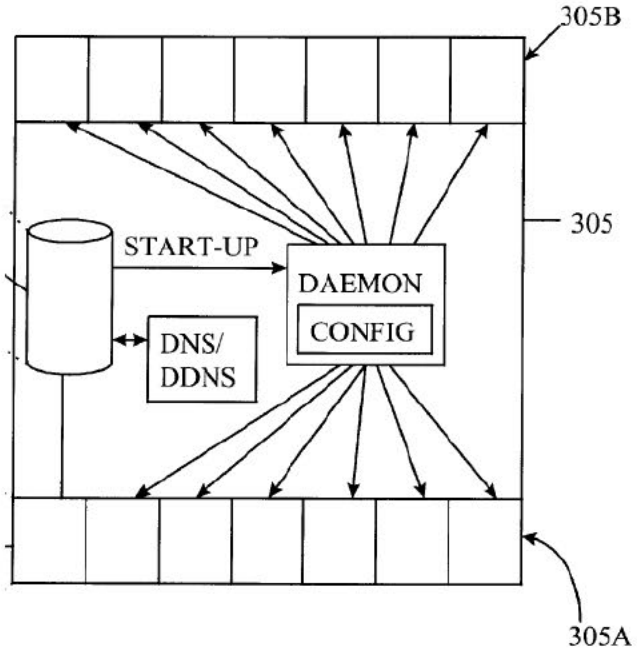


FIG. 3

Ex. 1008, Fig. 3

Instituted Grounds: IPR2014-00238

- 35 U.S.C. § 102
  - Claims 1-3, 8-11, 14-17, 22-25, and 28-30 are anticipated by Wesinger
- 35 U.S.C. § 103
  - Claims 4-7 and 18-21 are obvious over Wesinger in view of RFC 2543

Decision at 22

Wesinger

1. A method of connecting a first network device and a second network device, the method comprising:

intercepting, from the first network device, a request to look up an internet protocol (IP) address of the second network device based on a domain name associated with the second network device;

determining, in response to the request, whether the second network device is available for a secure communications service; and

initiating a secure communication link between the first network device and the second network device based on a determination that the second network device is available for the secure communications service;

wherein the secure communications service uses the secure communication link to communicate at least one of video data and audio data between the first network device and the second network device.

Ex. 1001, '697 Patent, Claim 1

"determining, in response to the request, whether the second network device is available for a secure communications service"

Patent Owner's Proposed Construction	Apple's Proposed Construction	Board's Preliminary Construction
No construction proposed	No construction proposed	Includes determining one or more of 1) whether the device is listed with a public internet address, and if so, allocating a private address for the second network device, or 2) some indication of the relative permission level or security privileges of the requester

Patent Owner Response at 27

"determining, in response to the request, whether the second network device is available for a secure communications service"

- Apple's Petition

> The firewall also forwards the host name in the request to the DNS/DDNS module, which will attempt to resolve the destination's name into an IP address. Ex. 1003 ¶¶ 282-285. If the destination cannot be found, the DNS/DDNS will, by virtue of being a DNS server, return an error message. Ex. 1003 ¶ 281. If the destination is found, the DNS/DDNS returns an IP address. Ex. 1003 ¶¶ 275-279, 290-291. If the destination is available and the configuration file specifies that traffic should be encrypted, the firewall determines that the remote host is available for a secure communications service. Ex. 1003 ¶¶ 282-285, 299-303, 305-308. Wesinger thus shows "*determining, in response to the request, whether the second network device is available for a secure communications service*" as specified by **claim 1**. Ex. 1003 ¶¶ 339-343.

Petition at 19

"determining, in response to the request, whether the second network device is available for a secure communications service"

- Apple's Reply

> Read accurately, there is thus no "second" or "ensuing" connection request in the Wesinger scheme – the "connection request" is ***the same request*** from the client device that contains the domain name of the remote host requiring name resolution (*i.e.*, it is a request, *inter alia*, to look up an IP address of a remote host).

Reply at 7

Firewall Allow/Disallow Decision Is Not In Response to DNS Request

- Patent Owner's Response

> First, *Wesinger* contrasts the "usual" DNS operation that occurs in response to a DNS query with the later-described firewall allow/disallow decision that occurs "when a connection request is received." (*Compare* Ex. 1008 at 9:16-18 *with id.* at 16:22-28; Ex. 2025 at 27, ¶ 40, Monrose Decl.) *Wesinger*'s discussion of the DNS process responsive to the DNS query does not invoke the firewall allow/disallow decision. (Ex. 2025 at 27, ¶ 40, Monrose Decl.) Likewise, *Wesinger*'s discussion of the firewall allow/disallow decision does not invoke the DNS resolution process. (*Id.*)

Patent Owner Response at 38

Firewall Rules Checking Is Not Performed on a DNS Query Packet

- Patent Owner's Response

> Second, *Wesinger* states that the firewall's "[r]ules checking is performed on a first data packet to be sent from the first computer to the second computer." (Ex. 1008 at 14:6-7.) This excludes a DNS query for at least two reasons. One is that the "first computer" and the "second computer" refer respectively to *Wesinger*'s client C and host D (*see, e.g., id.* at 17:18-24, "a connection between a first computer to the second computer through a first intermediate system"), but a DNS query is sent from the client C to a DNS module on a firewall, not to the host D (*see, e.g., id.* at 13:8-10). (Ex. 2025 at 27, ¶ 40, Monrose Decl.) The other reason is that, at the time client C sends a DNS query, it does not yet have the address to which it might send any "data packets." (*Id.*) Thus, the "data packet" that rules-checking is performed on cannot be part of a DNS query. (*Id.*)

Patent Owner Response at 39

Firewall Rules Checking Is Not Performed on a DNS Query Packet

- Wesinger

> tionless traffic using envoys. Rules checking is performed on a first data packet to be sent from the first computer to the second computer. If the result of this rules checking is to allow the first packet to be sent, a time-out limit associated with communications between the first computer and the second computer via UDP is established, and the first packet is sent from one of the virtual hosts to the second computer on behalf of the first computer. Thereafter, for so long as the time-out limit has not expired, subsequent packets between the first computer and the second computer are checked and sent. A long-lived session is therefore created for UDP traffic. After the time-out limit has expired, the virtual host may be remapped to a different network address to handle a different connection.

Ex. 1008 at 14:6-18

A DNS Query Is Not a Connection Request

- Apple's Reply

> Read accurately, there is thus no "second" or "ensuing" connection request in the Wesinger scheme – the "connection request" is ***the same request*** from the client device that contains the domain name of the remote host requiring name resolution (*i.e.*, it is a request, *inter alia*, to look up an IP address of a remote host).

Reply at 7

A DNS Query Is Not a Connection Request

- Wesinger

> The configuration of FIG. **4**, however, further allows the physical firewall machines **407** and **408** to share the aggregate processing load of current connections. Load sharing may be achieved in the following manner. Each of the DNS modules of all of the machines receive all DNS queries, because the machines are connected in parallel. Presumably, the DNS module of the machine that is least busy will be the first to respond to a query. An ensuing connection request is then mapped to a virtual host on the responding least-busy machine.

Ex. 1008 at 13:6-15

A DNS Query Is Not a Connection Request

- Wesinger

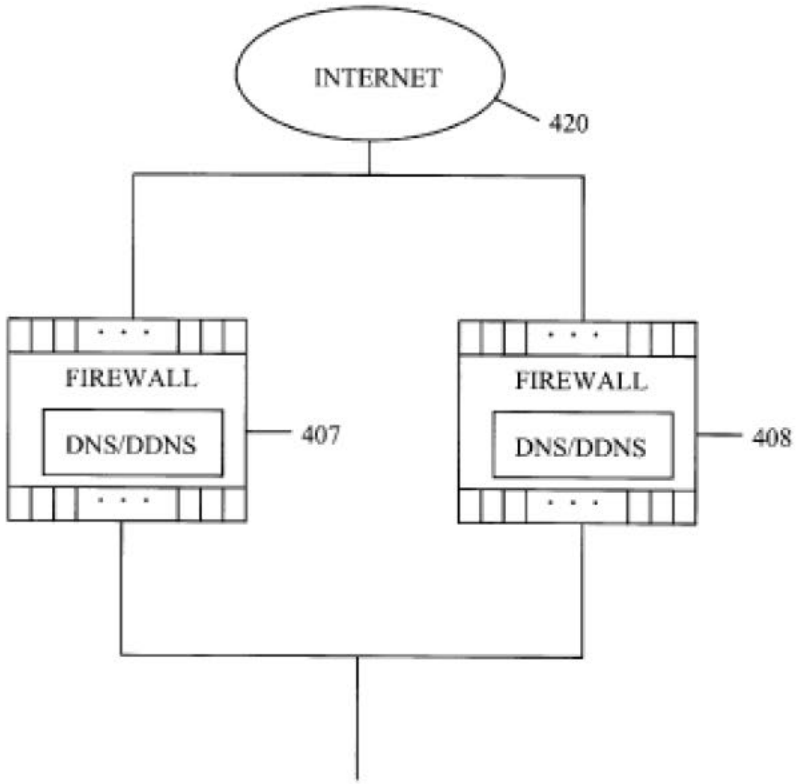


FIG. 4

Ex. 1008 at Fig. 4

A DNS Query Is Not a Connection Request

- Wesinger

> When a connection request is received, the daemon spawns a process to handle the connection request. This process then uses a piece of code referred to herein as an INET Wrapper **810** to check on the local side of the connection and the remote side of the connection to determine, in accordance with the appropriate Allow and Deny databases, whether the connection is to be allowed.

Ex. 1008 at 16:22-28

Wesinger

1. A method of connecting a first network device and a second network device, the method comprising:

intercepting, from the first network device, a request to look up an internet protocol (IP) address of the second network device based on a domain name associated with the second network device;

determining, in response to the request, whether the second network device is available for a secure communications service; and

initiating a secure communication link between the first network device and the second network device based on a determination that the second network device is available for the secure communications service;

wherein the secure communications service uses the secure communication link to communicate at least one of video data and audio data between the first network device and the second network device.

Ex. 1001, '697 Patent, Claim 1

"intercepting . . . a request to look up an internet protocol (IP) address"

Patent Owner's Proposed Construction	Apple's Proposed Construction	Board's Preliminary Construction
No construction necessary; alternatively, receiving a request to look up an internet protocol address and, apart from resolving it into an address, performing an evaluation on it related to establishing a secure communication link	A proxy computer or device receiving and acting on a request sent by a first computer that was intended for another computer	Receiving a request pertaining to a first entity at another entity

Patent Owner Response at 23

"intercepting . . . a request to look up an internet protocol (IP) address"

- Apple's Petition

283. The first step of the connection request is for the client to obtain an IP address associated with the destination. The client will initiate the connection by requesting to obtain an IP address associated with the domain name of the destination. Ex. 1008 (Wesinger) at 9:15-19 ("When client C tries to **initiate a connection to host D using the name of D**, DNS operates in the usual manner to propagate a name request to successive levels of the network until D is found.").

284. The request is intercepted by the local firewall, which will spawn a virtual host to process the request. Ex. 1008 (Wesinger) at 15:9-12 ("When a connection request is received, the firewall spawns a process, or execution thread, to create a virtual host VHn to handle that connection request."); *id.* at 16:19-24 ("When a connection request is received, the daemon spawns a process to handle the connection request.").

Ex. 1003 at 81-82

The DNS Query Is Not Evaluated Beyond Being Resolved

- Patent Owner's Response

> 25; Ex. 2025 at 37-38, ¶ 59, Monrose Decl.) *Wesinger* does not evaluate a DNS query beyond resolving it into an address, so *Wesinger*'s DNS query is not "intercepted" under VirnetX's construction. (Ex. 2025 at 37-38, ¶ 59, Monrose Decl.)

Patent Owner Response at 52

"intercepting . . . a request to look up an internet protocol (IP) address"

- Decision

> a user "will first enter the name of a firewall that the user wishes to connect through" and that the "firewall will then prompt the user for the name of the remote host the user wishes to connect to." Ex. 1008, 3:10-13. In other words, the firewall of Wesinger receives from the user a request pertaining to a first entity (i.e., pertaining to "the remote host the user wishes to connect to") at another entity (i.e., the firewall). Therefore, Wesinger discloses "intercepting a request."

Decision at 16

The Firewall Prompts Are Not a Request to Look Up an IP Address

- Patent Owner's Response

> In addition, the prompts cited in the Decision also are not the claimed "request to look up an internet protocol (IP) address." *Wesinger* provides little detail about these prompts for the name of the firewall and the remote host, and it does not disclose that they function as or result in a request to look up an IP address as claimed. (Ex. 2025 at 36, ¶ 57, Monrose Decl.) Instead, the cited passage forms part of *Wesinger*'s background describing a prior "custom" firewall approach in which "users must perform extra manual configuration to direct the software to contact the proxy on the intermediate system." (Ex. 1008 at 3:5-7.) In

Patent Owner Response at 49

The Firewall Prompts Are Not a Request to Look Up an IP Address

- Wesinger

> that users prefer. Furthermore, using custom client software, users must perform extra manual configuration to direct the software to contact the proxy on the intermediate system. With the custom procedure approach, the user tells the client to connect to the proxy and then tells the proxy which host to connect to. Typically, the user will first enter the name of a firewall that the user wishes to connect through. The firewall will then prompt the user for the name of the remote host the user wishes to connect to. Although this procedure is relatively simple in the case of a connection that traverses

Ex. 1008 at 3:5-13

Wesinger: Claims 8 and 9

8. The method of claim **1**, wherein at least one of the first network device and the second network device is a mobile device.

9. The method of claim **8**, wherein the mobile device is a notebook computer.

Ex. 1001, '697 Patent, Claims 8, 9

Wesinger: Claims 8 and 9

- Apple's Petition

> Claims 8 and 22 depend from claims 1 and 16, respectively, and specify the method (claim 8) or the system (claim 22) "*wherein at least one of the first network device and the second network device is a mobile device.*" Wesinger shows the first network device can be a personal computer. *See* Ex. 1008 (Wesinger) at Figure 1. Wesinger also shows that the first network device can be any device that supports IP communications. Ex. 1003 ¶¶ 270, 388. Such devices include laptop computers, PDAs, and WAP-enabled mobile phones. Ex. 1003 ¶¶ 270, 388. Wesinger thus shows a method and system that anticipate claims 8 and 22. Ex. 1003 ¶¶ 388-390.

Petition at 25

Wesinger: Claims 8 and 9

- Apple's Petition

> Claims 9 and 23 depend from claims 1 and 16, respectively, and specify the method (claim 9) or the system (claim 23) "*wherein the mobile device is a notebook computer*." Wesinger shows that a first network device can be any device that supports IP communications. Ex. 1003 ¶¶ 270, 388. Such devices include laptop computers, PDAs, and WAP-enabled mobile phones. Ex. 1003 ¶¶ 270, 391. Wesinger thus describes a method and system that anticipates claims 9 and 23. Ex. 1003 ¶¶ 391-393.

Petition at 25

Wesinger: Claims 8 and 9

- Mr. Fratto

> 270. Wesinger explains that its firewall is transparent to the computers making the connections. Ex. 1008 (Wesinger) at 8:16-20, 50-54. Wesinger shows that the end devices can be any IP enabled device that is connected to a network based on Internet standards. *See* Ex. 1008 (Wesinger) at 6:59-63 ("One of the two networks may be the Internet, or both of the two networks may be intranets-the nature and identity of the two networks is immaterial."); *id.* at 1:32-35 ("In addition, a network may use the same underlying technologies as the Internet. Such a network is referred to herein as an "Intranet," an internal network based on Internet standards."). I note that it would have been understood that such IP enabled devices included, personal computers, laptop computers, PDAs, WAP-enabled mobile phones, and other devices.

Ex. 1003 at 76-77

Wesinger Does Not Disclose any Mobile Devices

- Patent Owner's Response

> *Wesinger*, however, which does not mention any "laptop computers, PDAs, and WAP-enabled mobile phones." *Wesinger* does not identify any specific embodiments for the client C or the host D—it just calls them "computers" in a few instances. (*See, e.g.*, Ex. 1008 at 14:6-8.) The client C and the host D might be embodied as a desktop computer or other type of non-mobile computer, and need not be a mobile device, such as the claimed notebook computer. (Ex. 2025 at 38, ¶ 61, Monrose Decl.)

Patent Owner Response at 53

Instituted Grounds: IPR2014-00238

- 35 U.S.C. § 102
  - Claims 1-3, 8-11, 14-17, 22-25, and 28-30 are anticipated by Wesinger
- 35 U.S.C. § 103
  - Claims 4-7 and 18-21 are obvious over Wesinger in view of RFC 2543

Decision at 22

Apple's Argument

- Apple's Petition

> A person of ordinary skill in the art in February 2000 would have found it obvious to use the Wesinger system to provide video conferencing services based on the guidance in RFC 2543 (Ex. 1012).

Petition at 29

> A person of ordinary skill also would have recognized that it was a common and desirable practice to use a single communications architecture to support a variety of services, including both a VOIP server and a firewall. Ex. 1003 ¶¶ 309-

Petition at 30

Wesinger Teaches Away

- Wesinger

> this controlled access point. To avoid possible security compromises, the firewall should ideally run on a dedicated computer, i.e. one which does not have any other user-accessible programs running on it that could provide a path via which communications could circumvent the firewall.

Ex. 1008 at 7:1-5

Appendix

The '697 Patent

1. A method of connecting a first network device and a second network device, the method comprising:

intercepting, from the first network device, a request to look up an internet protocol (IP) address of the second network device based on a domain name associated with the second network device;

determining, in response to the request, whether the second network device is available for a secure communications service; and

initiating a secure communication link between the first network device and the second network device based on a determination that the second network device is available for the secure communications service;

wherein the secure communications service uses the secure communication link to communicate at least one of video data and audio data between the first network device and the second network device.

Ex. 1001, '697 Patent, Claim 1

The ’697 Patent

2. The method of claim **1**, wherein at least one of the video data and the audio data is encrypted over the secure communication link.

3. The method of claim **1**, wherein the secure communication link is a virtual private network communication link.

4. The method of claim **1**, wherein the secure communications service includes a video conferencing service.

5. The method of claim **1**, wherein the secure communications service includes a telephony service.

6. The method of claim **5**, wherein the telephony service uses modulation.

Ex. 1001, ’697 Patent, Claims 2-6

The ’697 Patent

7. The method of claim **6**, wherein the modulation is based on one of frequency-division multiplexing (FDM), time-division multiplexing (TDM), or code division multiple access (CDMA).

8. The method of claim **1**, wherein at least one of the first network device and the second network device is a mobile device.

9. The method of claim **8**, wherein the mobile device is a notebook computer.

Ex. 1001, ’697 Patent, Claims 7-9

The ’697 Patent

10. The method of claim **1**, wherein intercepting the request consists of receiving the request to determine whether the second network device is available for the secure communications service.

11. The method of claim **1**, wherein the secure communication link supports data packets.

Ex. 1001, ’697 Patent, Claims 10-11

The ’697 Patent

14. The method of claim **1**, wherein determining that the second network device is available for a secure communications service is a function of a domain name lookup.

15. The method of claim **1**, wherein intercepting the request occurs within another network device that is separate from the first network device.

Ex. 1001, ’697 Patent, Claims 14-15

The '697 Patent

16. A system for connecting a first network device and a second network device, the system including one or more servers configured to:

intercept, from the first network device, a request to look up an internet protocol (IP) address of the second network device based on a domain name associated with the second network device;

determine, in response to the request, whether the second network device is available for a secure communications service; and

initiate a secure communication link between the first network device and the second network device based on a determination that the second network device is available for the secure communications service,

wherein the secure communications service uses the secure communication link to communicate at least one of video data and audio data between the first network device and the second network device.

Ex. 1001, '697 Patent, Claim 16

The '697 Patent

17. The system of claim **16**, wherein the secure communication link is a virtual private network communication link.

18. The system of claim **16**, wherein the secure communications service includes a video conferencing service.

19. The system of claim **16**, wherein the secure communications service includes a telephony service.

20. The system of claim **16**, wherein the telephony service uses modulation.

21. The system of claim **20**, wherein the modulation is based on one of frequency-division multiplexing (FDM), time-division multiplexing (TDM), or code division multiple access (CDMA).

Ex. 1001, '697 Patent, Claims 17-21

The ’697 Patent

22. The system of claim **16**, wherein at least one of the first network device and the second network device is a mobile device.

23. The system of claim **22**, wherein the mobile device is a notebook computer.

24. The system of claim **16**, wherein at least one of the video data and the audio data is encrypted over the secure communication link.

25. The system of claim **16**, wherein the secure communication link supports data packets.

Ex. 1001, ’697 Patent, Claims 22-25

The '697 Patent

28. The system of claim **16**, wherein the determination that the second network device is available for the secure communications service is a function of the result of a domain name lookup.

29. The system of claim **16**, wherein the one or more servers are configured to intercept the request by receiving the request to determine whether the second network device is available for the secure communications service.

30. The system of claim **16**, wherein the one or more servers configured to intercept the request are separate from the first network device.

Ex. 1001, '697 Patent, Claims 28-30

CERTIFICATE OF SERVICE

I hereby certify that on this 5th day of February 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: February 5, 2015

Respectfully submitted,

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