

Presentation of Petitioner Apple Inc.

IPR2014-00237

IPR2014-00238

U.S. Patent No. 8,504,697

Grounds in -00237

- Whether Claims 1-11, 14-25, and 28-30 of the '697 patent are anticipated by U.S. Patent No. 6,496,867 to Beser (Ex. 1009)
- Whether Claims 1-11, 14-25, and 28-30 of the '697 patent are obvious over Beser in view of RFC 2401 (Ex. 1010)

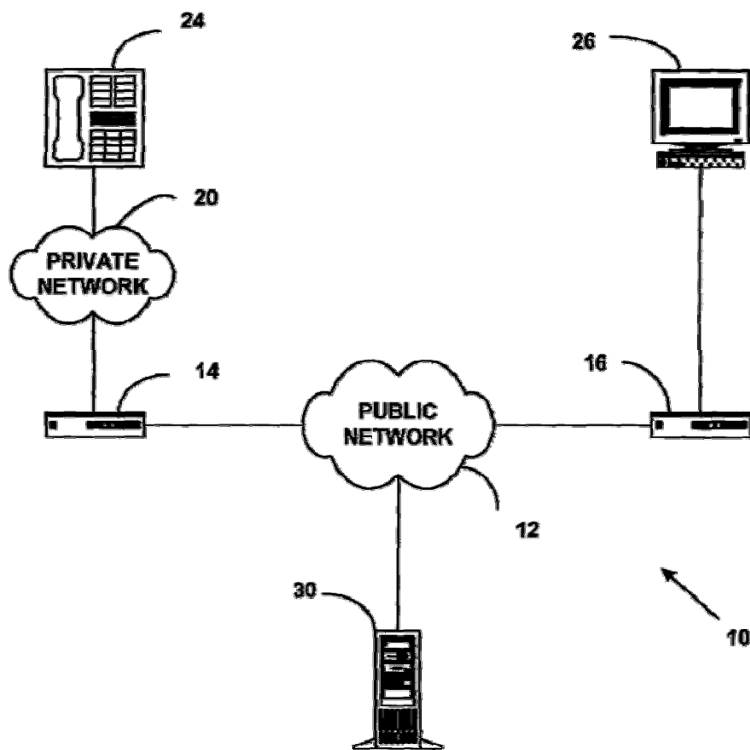
IPR2014-00237: Anticipation by Beser

(12) United States Patent
Beser et al.



US006496867B1
(10) Patent No.: US 6,496,867 B1
(45) Date of Patent: Dec. 17, 2002

FIG. 1




Ex. 1009 at Fig. 1
Decision at 17; Pet. at 16-127; Ex. 1003 at ¶ 260

One aspect of the invention includes a method for initiating a tunneling association between an originating end of the tunneling association and a terminating end of the tunneling association. The method includes receiving a request to initiate the tunneling association on a first network device. The first network device is associated with the originating end of the tunneling association, and the request includes a unique identifier for the terminating end of the tunneling association. A trusted-third-party network device is informed of the request on a public network. A public network address for a second network device is associated with the unique identifier for the terminating end of the tunneling association on the trusted-third-party network device. The second network device is associated with the terminating end of the tunneling association. A first private network address on the first network device and a second private network address on the second network device are negotiated through the public network. The first private network address is assigned to the originating end of the tunneling association and the second private network address is assigned to the terminating end of the tunneling association.

Ex. 1009 at 2:46-67
Pet. at 16-18; Ex. 1003 at ¶ 257

The '697 Patent, Claim 1


 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); Edmond Colby Mlunger, 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. 13/049,552, 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 709/223-227
(58) Field of Classification Search USPC 709/223-227
 See application file for complete search history.

(56) References Cited

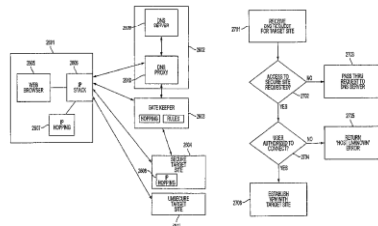
U.S. PATENT DOCUMENTS
 2,895,502 A 7/19/50 Roper et al.
 4,677,434 A 6/1987 Fawcenda
 (Continued)

FOREIGN PATENT DOCUMENTS
 DE 19924575 12/1999
 EP 0838930 4/1988
 (Continued)

OTHER PUBLICATIONS
 Cisco Comments and Petition for Reexamination 95/001,679 dated Jun. 14, 2012.
 (Continued)

(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



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.

'697 Patent (Ex. 1001) at Claim 1

The '697 Patent, Claim 16

(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); Edmond Colby Mlunger, 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. 13/049,552, 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 709/223

(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 7/19/50 Roper et al.
4,677,434 A 6/19/87 Fawcenda
(Continued)

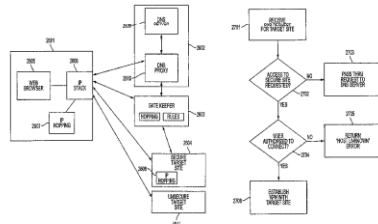
FOREIGN PATENT DOCUMENTS
DE 19924575 12/1999
EP 0838930 4/1988
(Continued)

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

(Continued)
Primary Examiner — Krisna 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



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.

'697 Patent (Ex. 1001) at Claim 16

The '697 Patent, Claim 1

“intercepting . . .”

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



US008504697B2

(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); **Edmond Colby Mungler**, 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

(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 7/19/50 Roper et al.
4,677,434 A 6/1987 Fossenda
(Continued)
FOREIGN PATENT DOCUMENTS

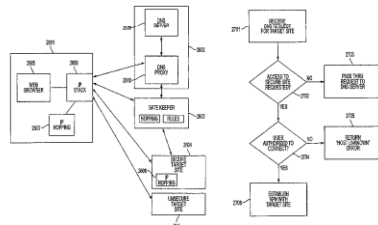
1. A method of connecting a first network device and a second network device, the method comprising:
intercepting, from the first network device, a request to look up an internet protocol (IP) address of the second network device based on a domain name associated with the second network device;
determining, in response to the request, whether the second network device is available for a secure communications service; and

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;

the first network device is available for a secure communications service of the second network device.

'697 Patent (Ex. 1001) at Claim 1

30, 1998, provisional application No. 60/137,704, filed on Jun. 7, 1999. 30 Claims, 40 Drawing Sheets



Institution Decision

Construction of “*intercepting* . . .”

Trials@uspto.gov
571-272-7822

Paper 15
Date: May 14, 2014

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

Based on the foregoing discussion, the term “intercepting” means

“receiving a request pertaining to a first entity at another entity.”

Decision (00237) at 13

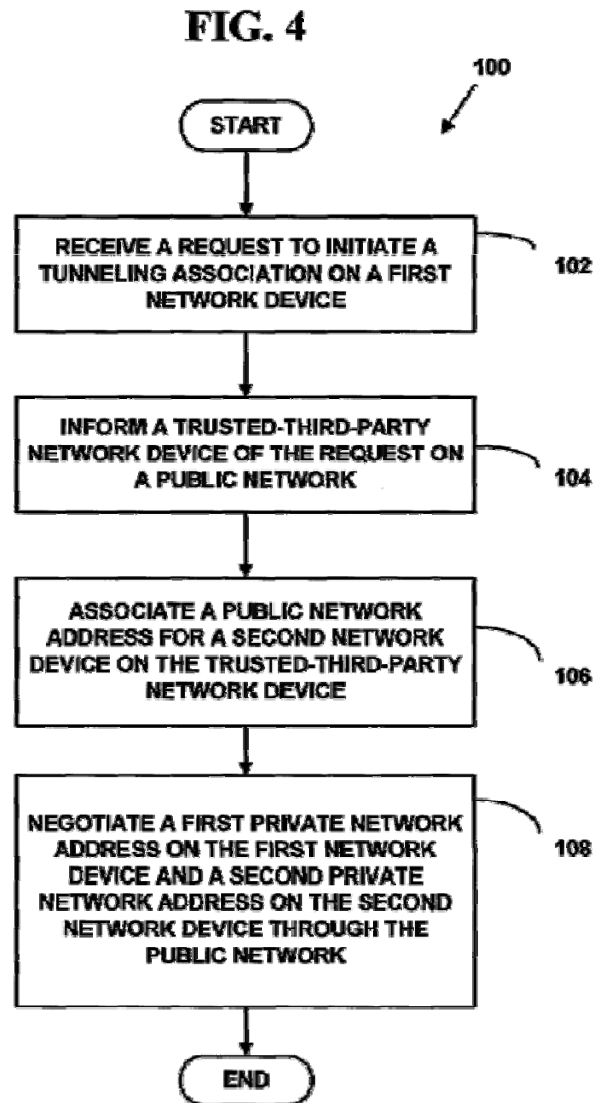
Before MICHAEL P. TIERNEY, KARL D. EASTHOM, and STEPHEN C. SIU,
Administrative Patent Judges.

EASTHOM, *Administrative Patent Judge.*

DECISION
Institution of *Inter Partes* Review
37 C.F.R. § 42.108

Anticipation by Beser

“*intercepting . . .*” by the first network device



Ex. 1009 at Fig. 4

Decision at 18, 21; Pet. at 18-19; Ex. 1003 at ¶¶ 294-300

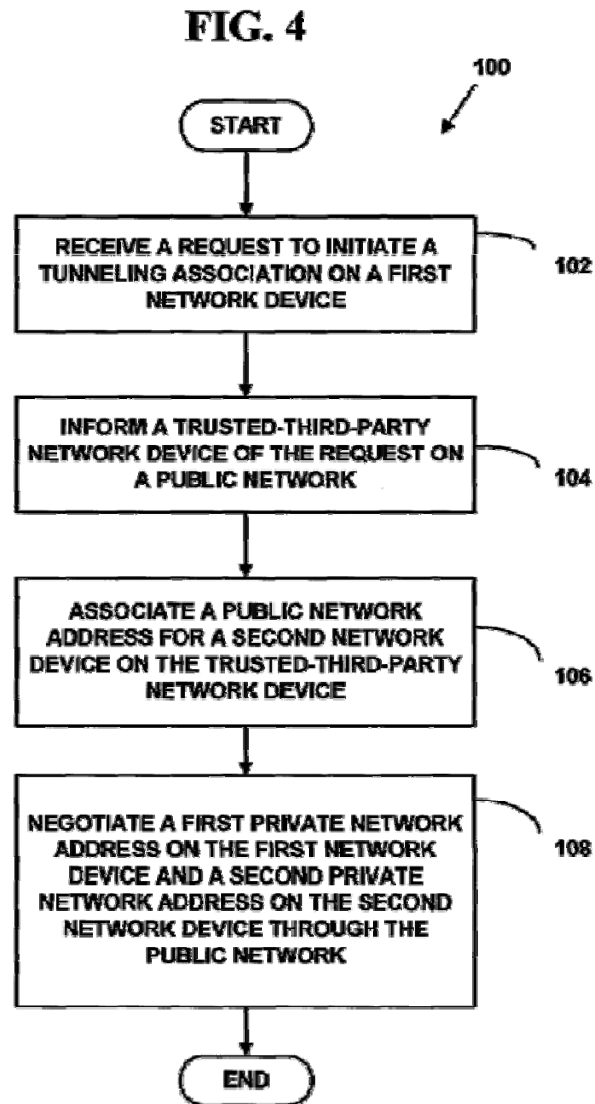
At Step 102 of Method 100, the first network device receives a request to initiate the tunneling connection. In one embodiment of the present invention, the request is received in a higher layer of a protocol stack for the first network device. For example, with reference to FIG. 2, the request may be received in the transport layer or the application layer of the protocol stack 50. In another exemplary preferred embodiment, the higher layer of the protocol stack that receives the request is the application layer. As discussed below, the application layer may have an interface to the originating end of the tunneling association and the request takes the form of an event on the interface. Alternatively, the request may take the form of a datagram that is passed up from the transport layer. In yet another exemplary preferred embodiment, the request includes an indicator that the request datagram is associated with this 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 than the transport or application layers, the protocol stack may be other than the OSI model of FIG. 2, and it should be understood that the present invention is not limited to these embodiments.

Ex. 1009 at 8:21-47

Decision at 18-21; Pet. at 18-23; Ex. 1003 at ¶¶ 286, 294

Anticipation by Beser

“*intercepting . . .*” by the TTP network device



Ex. 1009 at Fig. 4

Decision at 18, 21; Pet. at 18-19; Ex. 1003 at ¶¶ 294-300

At Step 104 of Method 100, the **trusted-third-party network device** is informed of the request. In one exemplary preferred embodiment, the trusted-third-party network device is informed in a higher layer of a protocol stack for the trusted-third-party network device. For example, with reference to FIG. 2, the information may be received in the transport layer of the protocol stack 50 of the trusted-third-party network device. In another exemplary preferred embodiment, the higher layer of the protocol stack that receives the information is the application layer. An informing message may take the form of a datagram that is passed up from the transport layer. **In yet another exemplary preferred embodiment, the informing message includes an indicator that the information datagram is associated with this 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 data-link, 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 informing message for its content and not ignore the datagram.** However, the higher layer may be other than the transport or application layers, the protocol stack may be other than the OSI model of FIG. 2, and it should be understood that the present invention is not limited to these embodiments.

Ex. 1009 at 8:48-9:5

Decision at 18; Reply at 9; See Pet. at 17; Ex. 1003 at ¶ 298

Patent Owner Assertion

Construction of “intercepting . . .”

VimnetX's Proposed 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

Opposition at 23

The Decision preliminarily construed “intercepting” to mean “receiving a request pertaining to a first entity at another entity.” (Decision at 12-13.) VimnetX respectfully disagrees with this construction, but it does not appear that the construction of “intercepting” will bear on the outcome of the issues in this *inter partes* review. Thus, the Board need not adopt a formal construction in the final written decision. If the Board decides to provide a construction, it should modify its current construction because it does not reflect how one of ordinary skill in the art reading the '697 patent would have understood “intercepting.”

Opposition at 23

v.

VIRNETX INC.
Patent Owner

Case IPR2014-00237
Patent 8,504,697

Patent Owner's Response

Patent Owner's Expert Construction of “*intercepting . . .*”

Filed on behalf of: Vime
By:
Joseph E. Palys
Paul Hastings LLP
875 15th Street NW
Washington, DC 20005
Telephone: (202) 551-
Facsimile: (202) 551-0
E-mail: josephpalys@p

UNITED STA

BEFORE TH

24. 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. For example, the DNS proxy 2610 may intercept the request and “determine[] whether access to a secure site has been requested,” “determine[] whether the user has sufficient security privileges to access the site,” and/or “transmit[] a message to gatekeeper 2603 requesting that a virtual private network be created between 40 user computer 2601 and secure target site 2604.” (*Id.* at 40:31-40.) Additionally, the DNS resolves an address and returns it to the first network device. (*Id.* at 44-48.)

Ex. 2025 at ¶ 24

Patent Owner's Expert Construction of "intercepting . . ."

A Normally we're saying the same thing. So in the context of '697, this interception here, the DNS request, is providing this additional evaluation, of which some of them are to determine whether the access to a secure site has been requested.

Ex. 1083 at 140:5-9; Reply at 5

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

APPLE INC.
Petitioner

v.

VIRNETX INC.
Patent Owner

Case IPR2014-00237
Patent 8,504,697

Patent Owner's Response

Q All right. Now, if you look at the second clause, it says "Determining in response to the request whether the second network is available for secure communication service," those examples that you have listed in 24 seem to be the determining -- examples of determining steps that are in the second step of clause 2 of the claim 1, right?

A So there are three examples supported here in my declaration. One is determining whether access to a secure site has been requested, in the context of '697 that's like, you know, example dot S com, determine whether user has sufficient security privileges to access the site.

Ex. 1083 at 135:7-19; Reply at 5; Ex. 1025 at ¶¶ 24, 30

The '697 Patent, Claim 1

“intercepting . . .”

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



US008504697B2

(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); **Edmond 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

(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 7/19/50 Roper et al.
4,677,434 A 6/1987 Fossenda
(Continued)
FOREIGN PATENT DOCUMENTS

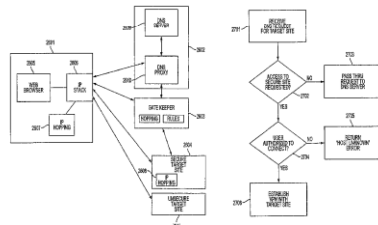
1. A method of connecting a first network device and a second network device, the method comprising:
intercepting, from the first network device, a request to look up an internet protocol (IP) address of the second network device based on a domain name associated with the second network device;
determining, in response to the request, whether the second network device is available for a secure communications service; and

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;

the first network device is available for a secure communications service of the second network device.

'697 Patent (Ex. 1001) at Claim 1

30, 1998, provisional application No. 60/137,704, filed on Jun. 7, 1999. 30 Claims, 40 Drawing Sheets



Patent Owner Assertion (Beser)

“intercepting . . .”

Filed on behalf of: VirmetX 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.c

UNITED STATES PATENT

BEFORE THE PATENT

AP
P

VIRMETX
Patent Owner

Case IPR2014-00237
Patent 8,504,697

Patent Owner's Response

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.

Opposition at 37

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.

Opposition at 37

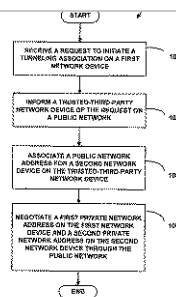
Anticipation by Beser

“request to look up [an IP] address”

306. As I explained, in one example, the trusted-third-party network device can function as a DNS server. See ¶ 262, above. If the identifier specified a non-secure destination, the trusted-third-party network device would resolve the domain name and return the IP address – this is simply what DNS servers do. See, e.g., Ex. 1001 ('697 patent) at 39:29-34 (“Conventional Domain Name Servers (DNSs) provide a look-up function that returns the IP address of a requested computer or host.”); see also ¶¶ 80-81, above.

307. If the unique identifier in the request specifies a secure destination (e.g., the unique identifier corresponds to a second network device), the trusted-third-party network device will automatically establish a tunneling association by negotiating with the first and second network devices. See, e.g., Ex. 1009 (Beser) at Figure 4; *id.* at 11:9-44; *id.* at 11:58-12:19.

Ex. 1003 at ¶ 306-07; Pet. at 19, 21



Petitioner Apple Inc. - Exhibit 1009, p. 1

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 preferred embodiment, the trusted-third-party network device 30 is a back-end service, a domain name server, or the owner/manager of database or directory services and may be distributed over several physical locations. In another exemplary preferred embodiment, the second network device 16 is any of a CM or CMTS in a data-over-cable network. The CM or CMTS is assigned a globally addressable public IP 58 address which appears in an IP 58 packet header field 82 sent to/from the CM or CMTS. In yet another exemplary preferred embodiment, the second network device 16 is a set-top box adapted to connect to the terminating telephony device 26.

Ex. 1009 at 11:26-44
Decision at 18; Pet. at 17; Ex. 1003 at ¶ 298


Anticipation by Beser

“[an IP] address of the second network device”

The network addresses are stored in network address tables respectively associated with the first 14 and second 16 network devices. The assignment of private network addresses to the ends of the tunneling association on the network devices, referred to above, includes the recording of the private network addresses in the network address tables. These network address tables allow for the translation from the private network addresses to the public network addresses. For example, the transmission of a packet from the originating network device 24 to the terminating network device 26, without revealing the identity of either end on the public network 12, requires that the packet is received on the first network device 14. The first network device 14 recognizes that the packet has come from the originating network device 24 and is destined for the terminating network device 26 by determining that the packet includes a private network address for the terminating network device 26. **The first network device 14 examines the entry in its network address table that contains the private network address for the terminating network device 26 and determines that this private network address is associated with the public network address for the second network device 16.** In this manner, the first network device 14 knows where to route the packet on the public network 12 by translating the private network address for the terminating network device 26 to the public network address for the second network device 16.

Ex. 1009 at 21:63-22:22

Pet. at 19; Ex. 1003 at ¶¶ 305, 313-15; Decision at 21; Reply at 8



US006496867B1

(12) **United States Patent** (10) Patent No.: **US 6,496,867 B1**
 Beser et al. (45) Date of Patent: **Dec. 17, 2002**

(54) **SYSTEM AND METHOD TO NEGOTIATE PRIVATE NETWORK ADDRESSES FOR INITIATING TUNNELING ASSOCIATIONS THROUGH PRIVATE AND/OR PUBLIC NETWORKS** 6,381,646 B2 * 4/2002 Zhang et al. 709/227
 6,400,722 B1 * 6/2002 Chuah et al. 370/401

(75) Inventors: **Nicetto B. Beser**, Evanston, IL (US),
Michael Borella, Naperville, IL (US)

(73) Assignee: **3Com Corporation**, Santa Clara, CA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. (54b) by 0 days.

(21) Appl. No.: **09/284,120**

(22) Filed: **Aug. 27, 1999**

(51) Int. Cl. **G06F 15/16; G06F 15/173**

(52) U.S. Cl. **709/245; 709/227; 709/225**

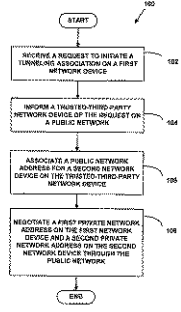
(58) Field of Search **709/225, 226, 227, 228, 229, 245, 218, 217, 370/401, 349; 713/201**

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,159,592 A	10/1992	Perkins
5,227,778 A	7/1993	Vacou et al.
5,550,984 A	8/1996	Gelb
5,639,216 A	6/1997	Fox et al.
5,708,655 A	11/1998	Tob et al.
5,793,763 A	8/1998	Maves et al.
5,812,019 A	8/1999	Rodwin et al.
5,867,660 A	2/1999	Schmidt et al.
5,872,847 A	2/1999	Boyle et al.
6,018,767 A	1/2000	Pjosek et al. 709/218
6,236,652 B1 *	5/2001	Pesson et al. 370/349
6,253,327 B1 *	6/2001	Zhang et al. 713/201
6,377,982 B1 *	4/2002	Rat et al. 709/217

41 Claims, 17 Drawing Sheets



Petitioner Apple Inc. - Exhibit 1009, p. 1

IPR2014-00237: Anticipation by Beser

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

(10) **Patent No.:** US 6,496,867 B1
(45) **Date of Patent:** Dec. 17, 2002



(54) **SYSTEM AND METHOD TO NEGOTIATE PRIVATE NETWORK ADDRESSES FOR INITIATING TUNNELING ASSOCIATIONS THROUGH PRIVATE AND/OR PUBLIC NETWORKS**

(75) Inventors: **Nicetto B. Beser**, Evansou, H. (US),
Michael Borella, Naperville, IL (US)

(73) Assignee: **3Com Corporation**, Santa Clara, CA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. (54b) by 0 days.

(21) Appl. No.: 09/284,120
(22) Filed: Aug. 27, 1999

(51) Int. Cl. G06F 15/16; G06F 15/173
(52) U.S. Cl. 709/245; 709/227; 709/225
(58) Field of Search 709/225, 226, 227, 228, 229, 245, 218, 217, 370/401, 349; 713/201

(56) **References Cited**
U.S. PATENT DOCUMENTS

5,159,592 A	10/1992	Perkins
5,227,778 A	7/1993	Vacou et al.
5,530,984 A	8/1996	Gelb
5,639,216 A	6/1997	Fox et al.
5,708,655 A	11/1998	Toth et al.
5,793,763 A	8/1998	Maves et al.
5,812,019 A	9/1999	Rodwin et al.
5,867,660 A	2/1999	Schmidt et al.
5,872,847 A	2/1999	Boyle et al.
6,018,767 A	1/2000	Fijolek et al.
6,236,652 B1	5/2001	Presson et al.
6,253,327 B1	6/2001	Zhang et al.
6,377,982 B1	4/2002	Rat et al.
709/218		
370/349		
713/201		
709/217		

6,381,646 B2 * 4/2002 Zhang et al. 709/227
6,400,722 B1 * 6/2002 Chuah et al. 370/401

OTHER PUBLICATIONS

Lee et al., "The Next Generation of the Internet: Aspects of the Internet Protocol Version 6", IEEE Network, Jan.-Feb. 1988, pp. 28-33.
"Internet Engineering Task Force", Request for Comments 791, Internet Protocol, Sep. 1981, pp. 1 to 45.
"Internet Engineering Task Force", Request for Comments 1853, IP in IP Tunneling, Oct. 1995, pp. 1 to 8.
"Internet Engineering Task Force", Request for Comments 1701, Generic Routing Encapsulation (GRE), Oct. 1994, pp. 1 to 8.
"Internet Engineering Task Force", Request for Comments 1241, A Scheme for an Internet Encapsulation Protocol, Jul. 1991, pp. 1 to 17.

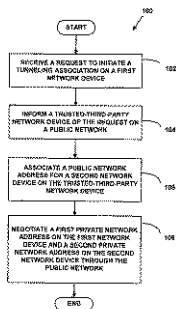
(List continued on next page.)

Primary Examiner—Le Hien Lau
(74) *Attorney, Agent, or Firm*—McDonnell, Boehnen, Hulbert & Berghoff

ABSTRACT

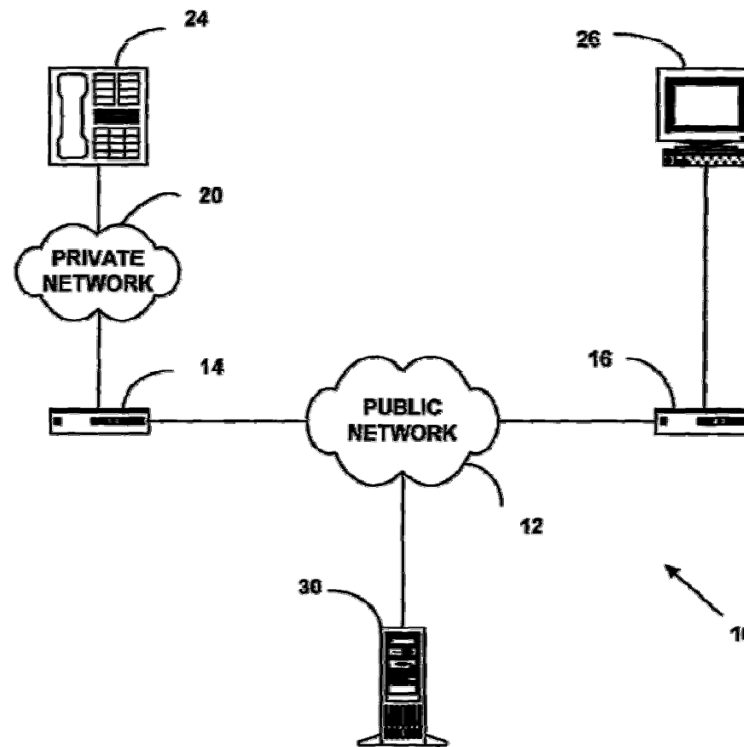
A method for initiating a tunneling association in a data network. The method includes negotiating private addresses, such as private Internet Protocol addresses, for the ends of the tunneling association. The negotiation is performed on a public network, such as the Internet, through a trusted-third-party without revealing the private addresses. The method provides for hiding the identity of the originating and terminating ends of the tunneling association from the other users of the public network. Hiding the identities may prevent interception of media flow between the ends of the tunneling association or eavesdropping on Voice-over-Internet-Protocol calls. The method increases the security of communication on the data network without imposing a computational burden on the devices in the data network.

41 Claims, 17 Drawing Sheets



Petitioner Apple Inc. - Exhibit 1009, p. 1

FIG. 1



Ex. 1009 at Fig. 1
Decision at 17; Pet. at 16-27; Ex. 1003 at ¶ 260

Patent Owner's Expert (Beser)

“[an IP] address of the second network device”

It says "Internet protocol IP address," so is it required in the claim that the domain name resolve into an IP address, or some other kind of -- an Internet address, or can it resolve into like a private Internet address?

MR. PALYS: Objection to form.

A It's a request to look up an IP address.

BY MR. KUSHAN:

Q So that would be a public IP address?

A Of the second network device.

Ex. 1083 at 228:3-12; Reply at 8

VIRNETX INC.
Patent Owner

Case IPR2014-00237
Patent 8,504,697

Patent Owner's Response


So this is stating pretty clearly that there are in the Beser scheme scenarios, two scenarios, one where the trusted third-party network device is participating in conducting that negotiation to get the IP addresses of the terminating device, and the other example is where it's not participating in that, right?

A Sure.

Ex. 1083 at 192:9-16 (discussing Ex. 1009 at 9:26); Reply at 8

The '697 Patent, Claim 1

“determining . . .”

	
US008504697B2	
<p>(12) United States Patent Larson et al.</p>	<p>(10) Patent No.: US 8,504,697 B2 (45) Date of Patent: *Aug. 6, 2013</p>
<p>(54) SYSTEM AND METHOD EMPLOYING AN AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES</p>	<p>(51) Int. Cl. <i>G06F 15/16</i> (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.</p>
<p>(75) Inventors: Victor Larson, Fairfax, VA (US); Robert Dunham Short, III, Leesburg, VA (US); Edmund Colby Mungler, Crownsville, MD (US); Michael Williamson, South Riding, VA (US)</p>	<p>(56) References Cited U.S. PATENT DOCUMENTS 2,895,502 A 7/19/50 Roper et al. 4,677,434 A 6/19/87 Fawcetta (Continued) FOREIGN PATENT DOCUMENTS DE 19924575 12/1999 EP 0838930 4/1988 (Continued) OTHER PUBLICATIONS Cisco Comments and Petition for Reexamination 95/001,679 dated Jun. 14, 2012. (Continued)</p>
<p>(73) Assignee: VirnetX, Inc., Zephyr Cove, NV (US)</p>	<p>(74) Primary Examiner — Krisna Lim (74) Attorney, Agent, or Firm — McDermott Will & Emery LLP</p>
<p>(*) 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.</p>	<p>(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.</p>
<p>(21) Appl. No.: 13/339,257</p>	<p>30 Claims, 40 Drawing Sheets</p>
<p>(22) Filed: Dec. 28, 2011</p>	
<p>(65) Prior Publication Data US 2012/0102204 A1 Apr. 26, 2012</p>	
<p>Related U.S. Application Data</p>	
<p>(63) Continuation of application No. 13/049,552, 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.</p>	
<p>(60) Provisional application No. 60/106,261, filed on Oct. 30, 1998, provisional application No. 60/137,704, filed on Jun. 7, 1999.</p>	

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.

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

'697 Patent (Ex. 1001) at Claim 1

Institution Decision

Construction of “*determining . . .*”

Trials@uspto.gov
571-272-7822

Paper 15
Date: May 14, 2014

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

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 \(00237\) at 15](#)

DECISION
Institution of *Inter Partes* Review
37 C.F.R. § 42.108

Anticipation by Beser “determining . . .”

For example, the trusted-third-party network device **30** may be a directory service, owned and operated by a telephone company, that retains a list of E.164 numbers of its subscribers. Associated with a E.164 number in the directory database is the IP **58** address of a particular second network device **16**. The database entry may also include a public IP **58** addresses for the terminating telephony device **26**. Many data structures that are known to those skilled in the art are possible for the association of the unique identifiers and IP **58** addresses for the second network devices **16**. However, it should be understood that the present invention is not restricted to E.164 telephone numbers and directory services and many more unique identifiers and trusted-third-party network devices are possible.

Ex. 1009 at 11:45-58; Ex. 1003 at ¶ 263; Pet. at 20; Reply at 10; Decision at 21, 22

(12) United States Patent Beser et al.

(10) Patent No.: US 6,496,867 B1
(45) Date of Patent: Dec. 17, 2002

(54) SYSTEM AND METHOD TO NEGOTIATE PRIVATE NETWORK ADDRESSES FOR INITIATING TUNNELING ASSOCIATIONS THROUGH PRIVATE AND/OR PUBLIC NETWORKS

6,381,646 B2 * 4/2002 Zhang et al. 709/227
6,400,722 B1 * 6/2002 Chuah et al. 370/401

OTHER PUBLICATIONS

Lee et al., "The Next Generation of the Internet: Aspects of the Internet Protocol Version 6", IEEE Network, Jan.-Feb. 1988, pp. 28-33.
"Internet Engineering Task Force", Request for Comments 791, Internet Protocol, Sep. 1981, pp. 1 to 45.
"Internet Engineering Task Force", Request for Comments 1853, IP in IP Tunneling, Oct. 1995, pp. 1 to 8.
"Internet Engineering Task Force", Request for Comments 1701, Generic Routing Encapsulation (GRE), Oct. 1994, pp. 1 to 8.
"Internet Engineering Task Force", Request for Comments 1241, A Scheme for an Internet Encapsulation Protocol, Jul. 1991, pp. 1 to 17.

(75) Inventors: **Nicetto B. Beser**, Evanston, IL (US),
Michael Borella, Naperville, IL (US)

(73) Assignee: **3Com Corporation**, Santa Clara, CA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. (54b) by 0 days.

(21) Appl. No.: 09/284,120

(22) Filed: Aug. 27, 1999

(51) Int. Cl. G06F 15/16; G06F 15/173

(52) U.S. Cl. 709/245; 709/227; 709/225

(58) Field of Search 709/225, 226, 227, 228, 229, 245, 218, 217, 370/401, 349; 713/201

(56) References Cited

U.S. PATENT DOCUMENTS

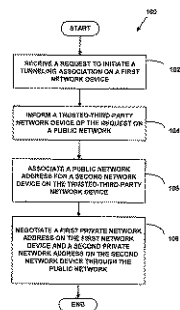
5,159,592 A 10/1992 Perkins
5,227,778 A 7/1993 Vacou et al.
5,550,984 A 8/1996 Gelb
5,639,216 A 6/1997 Fox et al.
5,708,655 A 1/1998 Toth et al.
5,793,763 A 8/1998 Mayes et al.
5,812,919 A 8/1999 Rodwin et al.
5,867,660 A 2/1999 Schmidt et al.
5,872,847 A 2/1999 Boyle et al.
6,018,767 A 1/2000 Fijolek et al. 709/218
6,236,652 B1 * 5/2001 Presson et al. 370/349
6,253,327 B1 * 6/2001 Zhang et al. 713/201
6,377,982 B1 * 4/2002 Kit et al. 709/217

(List continued on next page.)
Primary Examiner—Le Hien Lau
(74) *Attorney, Agent, or Firm*—McDonnell, Boehnen, Hulbert & Berghoff

(57) ABSTRACT

A method for initiating a tunneling association in a data network. The method includes negotiating private addresses, such as private Internet Protocol addresses, for the ends of the tunneling association. The negotiation is performed on a public network, such as the Internet, through a trusted-third-party without revealing the private addresses. The method provides for hiding the identity of the originating and terminating ends of the tunneling association from the other users of the public network. Hiding the identities may prevent interception of media flow between the ends of the tunneling association or eavesdropping on Voice-over-Internet-Protocol calls. The method increases the security of communication on the data network without imposing a computational burden on the devices in the data network.

41 Claims, 17 Drawing Sheets



Petitioner Apple Inc. - Exhibit 1009, p. 1

Anticipation by Beser “determining . . .”

IP tunnel between those network devices. Ex. 1003 at ¶¶ 259-260, 302-309. If the domain name sent to the trusted-third-party network device specifies a destination that is unavailable or unknown to the trusted-third-party network device, under the inherent operation of the Beser system, the request will not be routed further. Ex. 1003 at ¶¶ 282-289, 306-308; *see also id.* at ¶¶ 95-118. Beser is able to perform these functions because the trusted-third-party network device stores domain names and associated IP addresses, and may also contain a database of users or end devices. Ex. 1003 at ¶¶ 262-264, 286-290, 302-308.

Pet. at 20

Patent Owners

Patent No. 8,504,697

Issued: August 6, 2013

Filed: December 28, 2011

Inventors: Victor Larson, *et al.*

Title: SYSTEM AND METHOD EMPLOYING AN AGILE NETWORK
PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN
NAMES

Inter Partes Review No. IPR2014-00237

Declaration of Michael Fratto Regarding

U.S. Patent No. 8,504,697

Petitioner Apple Inc. - Exhibit 1003, p. 1

306. As I explained, in one example, the trusted-third-party network device can function as a DNS server. *See* ¶ 262, above. If the identifier specified a non-secure destination, the trusted-third-party network device would resolve the domain name and return the IP address – this is simply what DNS servers do. *See, e.g.,* Ex. 1001 (‘697 patent) at 39:29-34 (“Conventional Domain Name Servers (DNSs) provide a look-up function that returns the IP address of a requested computer or host.”); *see also* ¶¶ 80-81, above.

307. If the unique identifier in the request specifies a secure destination (*e.g.,* the unique identifier corresponds to a second network device), the trusted-third-party network device will automatically establish a tunneling association by negotiating with the first and second network devices. *See, e.g.,* Ex. 1009 (Beser) at Figure 4; *id.* at 11:9-44; *id.* at 11:58-12:19.

**Ex. 1003 at ¶¶ 306-07
Decision at 22; Pet. at 29**

367. Under the inherent operation of this process, a domain name sent to the trusted-third-party network device that specifies a destination that is unavailable or unknown to the trusted-third-party network device will not be routed further. *See* ¶¶ 282-289, 306-308, above; *see also* ¶¶ 95-118, above.

Ex. 1003 at ¶ 367; Pet. at 29

Anticipation by Beser “determining . . .”

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
Decision at 17; Opposition at 49; Ex. 1003 at ¶¶ 316-17

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

(10) Patent No.: US 6,496,867 B1
(45) Date of Patent: Dec. 17, 2002



(54) **SYSTEM AND METHOD TO NEGOTIATE PRIVATE NETWORK ADDRESSES FOR INITIATING TUNNELING ASSOCIATIONS THROUGH PRIVATE AND/OR PUBLIC NETWORKS**

6,381,646 B2 * 4/2002 Zhang et al. 709/227
6,400,722 B1 * 6/2002 Chuah et al. 370/401

OTHER PUBLICATIONS

Lee et al., "The Next Generation of the Internet: Aspects of the Internet Protocol Version 6", IEEE Network, Jan.-Feb. 1988, pp. 28-33.
"Internet Engineering Task Force", Request for Comments 791, Internet Protocol, Sep. 1981, pp. 1 to 45.
"Internet Engineering Task Force", Request for Comments 1853, IP in IP Tunneling, Oct. 1995, pp. 1 to 8.
"Internet Engineering Task Force", Request for Comments 1701, Generic Routing Encapsulation (GRE), Oct. 1994, pp. 1 to 8.
"Internet Engineering Task Force", Request for Comments 1241, A Scheme for an Internet Encapsulation Protocol, Jul. 1991, pp. 1 to 17.

(List continued on next page.)

(75) Inventors: **Nicetto B. Beser**, Evanston, IL (US),
Michael Borella, Naperville, IL (US)

(73) Assignee: **3Com Corporation**, Santa Clara, CA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. (54b) by 0 days.

(21) Appl. No.: 09/284,120

(22) Filed: Aug. 27, 1999

(51) Int. Cl. G06F 15/16; G06F 15/173

(52) U.S. Cl. 709/245; 709/227; 709/225

(58) Field of Search 709/220, 222, 709/225, 226, 227, 228, 229, 245, 218, 217, 370/401, 349; 713/201

(56) **References Cited**

U.S. PATENT DOCUMENTS

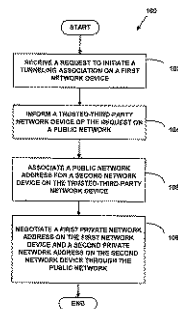
5,159,592 A 10/1992 Perkins
5,227,778 A 7/1993 Vacou et al.
5,550,984 A 8/1996 Gelb
5,639,216 A 6/1997 Fox et al.
5,708,655 A 11/1998 Toth et al.
5,793,763 A 8/1998 Mayes et al.
5,812,019 A 8/1999 Rodwin et al.
5,867,660 A 2/1999 Schmidt et al.
5,872,847 A 2/1999 Boske et al.
6,018,767 A 1/2000 Fijolek et al. 709/218
6,236,652 B1 * 5/2001 Presson et al. 370/349
6,253,327 B1 * 6/2001 Zhang et al. 713/201
6,377,982 B1 * 4/2002 Kit et al. 709/217

Primary Examiner—Le Hien Lau
(74) *Attorney, Agent, or Firm*—McDonnell, Boehnen, Hulbert & Berghoff

(57) **ABSTRACT**

A method for initiating a tunneling association in a data network. The method includes negotiating private addresses, such as private Internet Protocol addresses, for the ends of the tunneling association. The negotiation is performed on a public network, such as the Internet, through a trusted-third-party without revealing the private addresses. The method provides for hiding the identity of the originating and terminating ends of the tunneling association from the other users of the public network. Hiding the identities may prevent interception of media flow between the ends of the tunneling association or eavesdropping on Voice-over-Internet-Protocol calls. The method increases the security of communication on the data network without imposing a computational burden on the devices in the data network.

41 Claims, 17 Drawing Sheets



Petitioner Apple Inc. - Exhibit 1009, p. 1

Patent Owner Assertion

Construction of “determining . . .”

Paper No. _____
Filed: August 29, 2014

Filed on behalf of: VirmetX 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

It will be appreciated that different levels of security can also be provided for different categories of hosts. For example, some sites may be designated as having a certain security level, and the security level of the user requesting access must match that security level. The user’s security level can also be determined by transmitting a request message back to the user’s computer requiring that it prove that it has sufficient privileges.

Ex. 1001 at 41:20-27; Reply at 5-6

The Decision also does not explain why the secure communications service availability determination should require “some indication of the relative permission level or security privileges of the requester.” In fact, the specification provides examples of determinations focusing on the second network device to which access is requested, as well as examples of separate determinations focusing on the first network device desiring the access. (*Compare*, for example, Ex. 1001 at 40:32-33, “determin[ing] whether access to a secure site has been requested” with *id.* at 40:36-37, “determines whether the user has sufficient security privileges to access the site.”) **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.”

Opposition at 23

Patent Owner Assertion (Beser)

“*determining . . .*”

Paper No. 1001
Filed: August 1, 2014

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 IPR2014-00237
Patent 8,504,697

Patent Owner's Response

permission level or security privileges of the requester.” In fact, the specification provides examples of determinations focusing on the second network device to which access is requested, as well as examples of separate determinations focusing on the first network device desiring the access. (*Compare*, for example, Ex. 1001 at 40:32-33, “determin[ing] whether access to a secure site has been requested” *with id.* at 40:36-37, “determines whether the user has sufficient security privileges to access the site.”) The claimed determination, however, expressly focuses on the

[Opposition at 29](#)

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. If so,

[Ex. 1001 at 40:31-37; Opposition at 29](#)

Patent Owner Assertion (Beser)

“*determining . . .*”

Paper No. _____
Filed: August 29, 2014

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 IPR2014-00237
Patent 8,504,697

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, Monroe Decl.) The DNS server in *Beser* could operate in a number of ways contrary to the way Apple suggests. For example, the DNS server in *Beser* could return an error message, could discard the request, could do nothing, or could wait until the domain name does map to a device requiring negotiation of an IP tunnel. (*Id.*) Even if Apple's proposed manner of operating the DNS server in *Beser* could actually be implemented, it would be one of several possibilities and is not necessarily present in *Beser's* system. (*Id.*)

Opposition at 42

Anticipation by Beser “determining . . .”

UNITED

BEFOR

VIRNETX, IN


Before MICHAEL P
Administrative Paten

message” or “discard[] the request.” Resp. at 41-43. Initially, Patent Owner ignores that a standard DNS lookup returns an associated IP address of a domain name. Ex. 1003 at ¶¶ 77-81, 109-12, 287-89. But more importantly, Patent Owner’s argument actually supports the Board’s finding – the counterexamples show that *no tunnel is created* if the domain name is *not listed* in the trusted-third-party network device’s table. Dec. 21-23; Ex. 1003 at ¶ 367. Thus, the determination affects whether the secure communication link is established.

Reply at 11; see also Ex. 1003 at ¶ 367

The '697 Patent, Claim 1

“initiating a secure communication link . . .”

 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	(51) Int. Cl. <i>G06F 15/16</i> (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.
(75) Inventors: Victor Larson , Fairfax, VA (US); Robert Dunham Short, III , Leesburg, VA (US); Edmond Colby Mungler , Crownsville, MD (US); Michael Williamson , South Riding, VA (US)	(56) References Cited U.S. PATENT DOCUMENTS 2,895,502 A 7/19/50 Roper et al. 4,677,434 A 6/1987 Fawcenda (Continued)
(73) Assignee: VirnetX, Inc. , Zephyr Cove, NV (US)	FOREIGN PATENT DOCUMENTS DE 19924575 12/1999 EP 0838930 4/1988 (Continued)
(*) 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.	OTHER PUBLICATIONS Cisco Comments and Petition for Reexamination 95/001,679 dated Jun. 14, 2012. (Continued)
(21) Appl. No.: 13/339,257	Primary Examiner — Krisna Lim (74) Attorney, Agent, or Firm — McDermott Will & Emery LLP
(22) Filed: Dec. 28, 2011	(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 com-
(65) Prior Publication Data US 2012/0102204 A1 Apr. 26, 2012	(60) Provis 30, 1 filed e
(63) Related U.S. Application Data Continuation of application No. 13/049,552, 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.	

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

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;

'697 Patent (Ex. 1001) at Claim 1

Institution Decision

Construction of “*secure communication link*”

Trials@uspto.gov
571-272-7822

Paper 15
Date: May 14, 2014

UNITED STATES PATENT AND TRADEMARK OFFICE

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 \(00237\) 10](#)

DECISION
Institution of *Inter Partes* Review
37 C.F.R. § 42.108

Anticipation by Beser “secure communication link”

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

(10) Patent No.: US 6,496,867 B1
(45) Date of Patent: Dec. 17, 2002



(54) **SYSTEM AND METHOD TO NEGOTIATE PRIVATE NETWORK ADDRESSES FOR INITIATING TUNNELING ASSOCIATIONS THROUGH PRIVATE AND/OR PUBLIC NETWORKS**

(75) Inventors: **Nicetto B. Beser**, Evanston, IL (US),
Michael Borella, Naperville, IL (US)

(73) Assignee: **3Com Corporation**, Santa Clara, CA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. (54b) by 0 days.

(21) Appl. No.: 09/284,120
(22) Filed: Aug. 27, 1999

(51) Int. Cl. G06F 15/16; G06F 15/173
(52) U.S. Cl. 709/245; 709/227; 709/225
(58) Field of Search 709/225, 226, 227, 228, 229, 245, 218, 217, 370/401, 349; 713/201

(56) **References Cited**
U.S. PATENT DOCUMENTS

5,159,592 A	10/1992	Perkins
5,227,778 A	7/1993	Vacou et al.
5,550,984 A	8/1996	Gelb
5,639,216 A	6/1997	Fox et al.
5,708,655 A	11/1998	Tob et al.
5,793,763 A	8/1998	Maves et al.
5,812,019 A	8/1999	Rodwin et al.
5,867,660 A	2/1999	Schmidt et al.
5,872,847 A	2/1999	Boyle et al.
6,018,767 A	1/2000	Fjosek et al.
6,236,652 B1	5/2001	Prieston et al.
6,253,327 B1	6/2001	Zhang et al.
6,377,982 B1	4/2002	Rat et al.

6,381,646 B2 * 4/2002 Zhang et al. 709/227
6,400,722 B1 * 6/2002 Chuah et al. 370/401

OTHER PUBLICATIONS

Lee et al., "The Next Generation of the Internet: Aspects of the Internet Protocol Version 6", IEEE Network, Jan.-Feb. 1988, pp. 28-33.
"Internet Engineering Task Force", Request for Comments 791, Internet Protocol, Sep. 1981, pp. 1 to 45.
"Internet Engineering Task Force", Request for Comments 1853, IP in IP Tunneling, Oct. 1995, pp. 1 to 8.
"Internet Engineering Task Force", Request for Comments 1701, Generic Routing Encapsulation (GRE), Oct. 1994, pp. 1 to 8.
"Internet Engineering Task Force", Request for Comments 1241, A Scheme for an Internet Encapsulation Protocol, Jul. 1991, pp. 1 to 17.

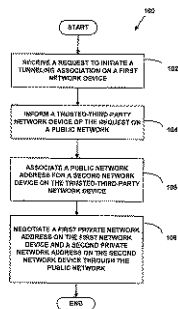
(List continued on next page.)

Primary Examiner—Le Hien Lau
(74) **Attorneys, Agents, or Firm**—McDonnell, Boehnen, Hulbert & Berghoff

(57) **ABSTRACT**

A method for initiating a tunneling association in a data network. The method includes negotiating private addresses, such as private Internet Protocol addresses, for the ends of the tunneling association. The negotiation is performed on a public network, such as the Internet, through a trusted-third-party without revealing the private addresses. The method provides for hiding the identity of the originating and terminating ends of the tunneling association from the other users of the public network. Hiding the identities may prevent interception of media flow between the ends of the tunneling association or eavesdropping on Voice-over-Internet-Protocol calls. The method increases the security of communication on the data network without imposing a computational burden on the devices in the data network.

41 Claims, 17 Drawing Sheets



Petitioner Apple Inc. - Exhibit 1009, p. 1

At Step 118, a first private IP 58 address on the first network device 14 and a second private IP 58 address on the second network device are negotiated through the public network 12. Private IP 58 addresses are addresses that are reserved for use in private networks that are isolated from a public network such as the Internet. Private IP 58 addresses are not globally routable. As is known in the art, private IP 58 addresses typically include IP 58 addresses beginning with 10.0.0.0, 172.16.0.0, and 192.168.0.0. These private IP 58 addresses are assigned to the telephony devices (24, 26), viz., the first private IP 58 address is assigned to the originating telephony device 24 and the second private IP 58 address is assigned to the terminating telephony device 26. The assignment of private IP 58 addresses is discussed below. The negotiation ensures that neither the private nor any public IP 58 addresses for the ends of the VoIP association appear in the source 88 or destination 90 address fields of the IP 58 packets that comprise the negotiation. The IP 58 packets of the negotiation step 118 will only have source 88 or destination 90 address fields containing the IP 58 addresses of the first 14, second 16, or trusted-third-party 30 network device. In this manner the identities of the originating 24 and terminating 26 telephony devices are inside the payload fields 84 of the IP 58 packets and may be hidden from hackers on the public network 12. The negotiation may occur through the trusted-third-party network device 30 to further ensure the anonymity of the telephony devices (24, 26).

Ex. 1009 at 11:59-12:19
Decision at 19; Ex. 1003 at ¶¶ 307-309, 312; Pet. at 21; Reply at 13

Patent Owner Assertion

Construction of “secure communication link”

VirnetX’s Proposed Construction

A direct communication link that provides data security through encryption

Opposition at 10

Naveen Modi
Paul Hastings LLP
875 15th Street
Washington, DC
Telephone: (202) 462-1000
Facsimile: (202) 462-1001
E-mail: naveen@phillips.com

ATTORNEY AND TRADEMARK AGENT

FOR PETITIONER AND APPELLANT

APPLE INC.
Petitioner

v.

VIRNETX INC.
Patent Owner

Case IPR2014-00237
Patent 8,504,697

Patent Owner’s Response

As explained in the Preliminary Response, the Decision’s construction is contrary to the plain meaning of “secure communication link” and the teachings of the ’697 patent because it permits, but does not require, encryption.

Opposition at 11

The ’697 patent explains that “secure communication links” require encryption for the reasons discussed above. However, to the extent the Decision indicates that the term would ordinarily encompass links without encryption, VirnetX’s undisputed disclaimer should override the broader meaning.

Opposition at 15

Patent Owner's Expert

Construction of "secure communication link"

And there's no passage in the '697 patent that gave "secure communication link" an explicit definition, right?

A I believe -- if my memory serves me correctly, there are opposing views on what that means.

Ex. 1083 at 66:12-17; Reply at 4

APPLE INC.
Petitioner

v.

VIRNETX INC.
Patent Owner

Q But you can enhance data security using authentication techniques, right?

A You can.

Ex. 1083 at 74:12-14; Reply at 4

Q So address hopping would provide protection against disclosure of the addresses of the parties to a communication, right?

MR. PALYS: Objection, form.

A Address hopping may hide who is talking to whom.

BY MR. KUSHAN:

Q And so that's enhancing the security of the communication between those two parties, because you cannot determine who is speaking to whom, right?

MR. PALYS: Objection, form.

A You may not be able to determine in isolation who is speaking to whom.

BY MR. KUSHAN:

Q And that provides some amount of security for that communication between the two parties we've discussed, right?


MR. PALYS: Objection to form.

A Sure.

Ex. 1083 at 113:16-114:12; Reply at 4

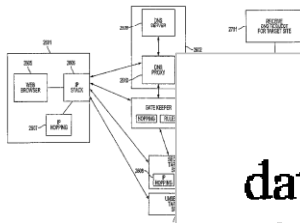
The '697 Patent, Claim 2

Construction of claim 1's "secure communication link"

 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	(51) Int. Cl. <i>G06F 15/16</i> (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.
(75) Inventors: Victor Larson, Fairfax, VA (US); Robert Dunham Short, III, Leesburg, VA (US); Edmund Colby Mungler, Crownsville, MD (US); Michael Williamson, South Riding, VA (US)	(56) References Cited U.S. PATENT DOCUMENTS 2,895,502 A 7/1950 Roper et al. 4,677,434 A 6/1987 Fissenden (Continued) FOREIGN PATENT DOCUMENTS DE 19924575 12/1999 EP 0838930 4/1988 (Continued) OTHER PUBLICATIONS Cisco Comments and Petition for Reexamination 95/001,679 dated Jun. 14, 2012. (Continued) Primary Examiner — Krisna Lim (74) <i>Attorney, Agent, or Firm</i> — McDermott Will & Emery LLP
(73) Assignee: VirnetX, Inc., Zephyr Cove, NV (US)	(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.
(*) 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.	(30) Claims, 40 Drawing Sheets
(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. 13/049,552, 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.	

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.

'697 Patent (Ex. 1001) at Claim 1



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.

'697 Patent (Ex. 1001) at Claim 2; Pet. at 8; Reply at 4

Anticipation by Beser

“at least one of video data and audio data”

US006496867B1

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

(10) Patent No.: **US 6,496,867 B1**
(45) Date of Patent: **Dec. 17, 2002**

(54) SYSTEM AND METHOD TO NEGOTIATE PRIVATE NETWORK ADDRESSES FOR INITIATING TUNNELING ASSOCIATIONS THROUGH PRIVATE AND/OR PUBLIC NETWORKS

(75) Inventors: **Nicetto B. Beser**, Evanston, IL (US),
Michael Borella, Naperville, IL (US)

(73) Assignee: **3Com Corporation**, Santa Clara, CA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. (54b) by 0 days.

(21) Appl. No.: **09/384,130**

6,381,646 B2 * 4/2002 Zhang et al. 709/227
6,400,722 B1 * 6/2002 Chuah et al. 370/401

OTHER PUBLICATIONS

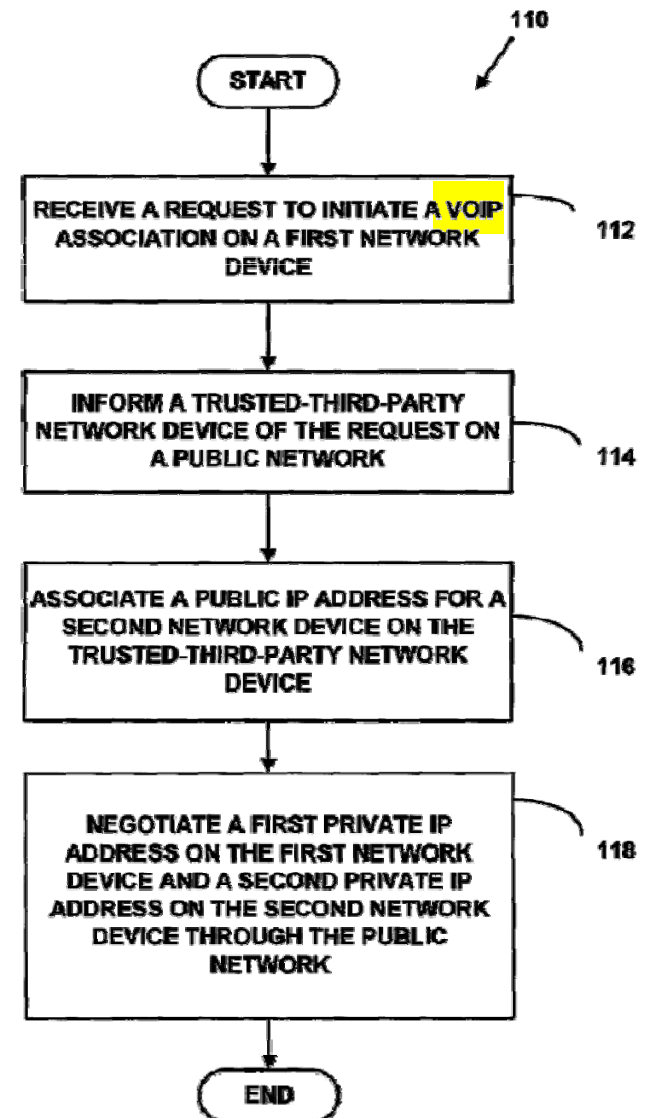
Lee et al., "The Next Generation of the Internet: Aspects of the Internet Protocol Version 6", IEEE Network, Jan./Feb. 1988, pp. 28-33.
"Internet Engineering Task Force", Request for Comments 791, Internet Protocol, Sep. 1981, pp. 1 to 45.
"Internet Engineering Task Force", Request for Comments 1853, IP in IP Tunneling, Oct. 1995, pp. 1 to 8.
"Internet Engineering Task Force", Request for Comments 1701, Generic Routing Encapsulation (GRE), Oct. 1994, pp. 1 to 8.
"Internet Engineering Task Force", Request for Comments 1241, A Scheme for an Internet Encapsulation Protocol, Jul. 1991, pp. 1 to 17.

The data network also includes network devices (24, 26) that are originating and terminating ends of data flow. In another exemplary preferred embodiment of the present invention, these network devices (24, 26) are telephony devices or multimedia devices. Multimedia devices include Web-TV sets and decoders, interactive video-game players, or personal computers running multimedia applications. Telephony devices include VoIP devices (portable or stationary) or personal computers running facsimile or audio applications. However, the ends of the data flow may be other types of network devices and the present invention is not restricted to telephony or multimedia devices.

Ex. 1009 at Fig. 5
Decision at 23-24; Pet. at 23; Ex. 1003 at ¶ 278

Petitioner Apple Inc. - Exhibit 1009, p. 1


FIG. 5



Ex. 1009 at Fig. 5

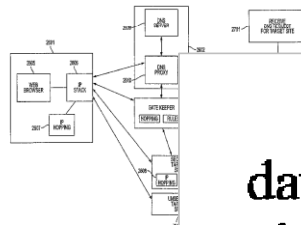
Petitioner Apple Inc. – Ex. 1084

The '697 Patent, Claim 2

 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	(51) Int. Cl. <i>G06F 15/16</i> (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.
(75) Inventors: Victor Larson, Fairfax, VA (US); Robert Dunham Short, III, Leesburg, VA (US); Edmond Colby Mlunger, Crownsville, MD (US); Michael Williamson, South Riding, VA (US)	(56) References Cited U.S. PATENT DOCUMENTS 2,895,502 A 7/19/50 Roper et al. 4,677,434 A 6/1987 Fawcenda (Continued) FOREIGN PATENT DOCUMENTS DE 19924575 12/1999 EP 0838930 4/1988 (Continued) OTHER PUBLICATIONS Cisco Comments and Petition for Reexamination 95/001,679 dated Jun. 14, 2012. (Continued) Primary Examiner — Krisna Lim (74) <i>Attorney, Agent, or Firm</i> — McDermott Will & Emery LLP
(73) Assignee: VirnetX, Inc., Zephyr Cove, NV (US)	(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.
(*) 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.	(30) Claims, 40 Drawing Sheets
(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. 13/049,552, 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.	

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.

'697 Patent (Ex. 1001) at Claim 1



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.

'697 Patent (Ex. 1001) at Claim 2

Anticipation by Beser video or audio data “is encrypted”

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

(10) **Patent No.:** US 6,496,867 B1
(45) **Date of Patent:** Dec. 17, 2002



(54) **SYSTEM AND METHOD TO NEGOTIATE PRIVATE NETWORK ADDRESSES FOR INITIATING TUNNELING ASSOCIATIONS THROUGH PRIVATE AND/OR PUBLIC NETWORKS**

(75) Inventors: **Nicetto B. Beser**, Evanston, IL (US),
Michael Borella, Naperville, IL (US)

(73) Assignee: **3Com Corporation**, Santa Clara, CA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. (54b) by 0 days.

(21) Appl. No.: **09/284,120**
(22) Filed: **Aug. 27, 1999**

(51) Int. Cl. **G06F 15/16; G06F 15/173**
(52) U.S. Cl. **709/245; 709/227; 709/225**
(58) Field of Search **709/225, 226, 227, 228, 229, 245, 218, 217, 370/401, 349; 713/201**

(56) **References Cited**
U.S. PATENT DOCUMENTS

5,159,592 A	10/1992	Perkins
5,227,778 A	7/1993	Vacou et al.
5,550,984 A	8/1996	Gelb
5,636,216 A	6/1997	Fox et al.
5,708,655 A	11/1998	Toth et al.
5,793,763 A	8/1998	Maves et al.
5,812,019 A	8/1999	Rodwin et al.
5,867,660 A	2/1999	Schmidt et al.
5,872,847 A	2/1999	Boyle et al.
6,018,767 A	1/2000	Fijolek et al.
6,236,652 B1 *	5/2001	Pesson et al.
6,253,327 B1 *	6/2001	Zhang et al.
6,377,982 B1 *	4/2002	Rat et al.
	709/218	
	370/349	
	713/201	
	709/217	

6,381,646 B2 * 4/2002 Zhang et al. 709/227
6,400,722 B1 * 6/2002 Chuah et al. 370/401

OTHER PUBLICATIONS

Lee et al., “The Next Generation of the Internet: Aspects of the Internet Protocol Version 6”, IEEE Network, Jan.-Feb. 1988, pp. 28-33.”
“Internet Engineering Task Force”, Request for Comments 791, Internet Protocol, Sep. 1981, pp. 1 to 45.
“Internet Engineering Task Force”, Request for Comments 1853, IP in IP Tunneling, Oct. 1995, pp. 1 to 8.
“Internet Engineering Task Force”, Request for Comments 1701, Generic Routing Encapsulation (GRE), Oct. 1994, pp. 1 to 8.
“Internet Engineering Task Force”, Request for Comments 1241, A Scheme for an Internet Encapsulation Protocol, Jul. 1991, pp. 1 to 17.

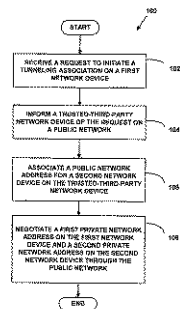
(List continued on next page.)

Primary Examiner—Le Hien Lau
(74) *Attorney, Agent, or Firm*—McDonnell, Boehnen, Hulbert & Berghoff

(57) **ABSTRACT**

A method for initiating a tunneling association in a data network. The method includes negotiating private addresses, such as private Internet Protocol addresses, for the ends of the tunneling association. The negotiation is performed on a public network, such as the Internet, through a trusted-third-party without revealing the private addresses. The method provides for hiding the identity of the originating and terminating ends of the tunneling association from the other users of the public network. Hiding the identities may prevent interception of media flow between the ends of the tunneling association or eavesdropping on Voice-over-Internet-Protocol calls. The method increases the security of communication on the data network without imposing a computational burden on the devices in the data network.

41 Claims, 17 Drawing Sheets



Petitioner Apple Inc. - Exhibit 1009, p. 1

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
Decision at 24; Pet. at 24; Ex. 1003 at ¶¶ 268-270, 303, 318-325

Patent Owner Assertion (Beser) video or audio data “*is encrypted*”

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
Washington, DC
Telephone: (202) 551-1996
Facsimile: (202) 551-0496
E-mail: naveenmodi@paulhastings.com

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEALS BOARD

APPLE INC.
Petitioner

v.

VIRNETX INC.
Patent Owner

Case IPR2014-00237
Patent 8,504,697

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.

Opposition at 54

Patent Owner's Expert (Beser) video or audio data "is encrypted"

Paper No. _____
Filed: August 29, 2014

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 IPR2014-00237
Patent 8,504,697

Patent Owner's Response

Q And so what Beser is saying is that it's conventional prior to Beser's invention to use IPSEC to encrypt the packets that are transmitted in an IP tunnel?

A In isolation here.

Ex. 1083 at 213:19-214:1; Reply at 14

Q So if I was concerned about the computational burden and the volume of data that's being sent over an IP tunnel with encryption in IPSEC, I could essentially choose parameters of the encryption element of IPSEC to reduce the computational burden on encrypting the traffic; is that a fair statement?

A So one possible way of addressing potentially some of the limitations expressly pointed to by Beser might be to figure out how to adapt various parameters.

Ex. 1083 at 219:8-18; Reply at 14

Obviousness over Beser and RFC 2401 video or audio data “*is encrypted*”

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

APPLE INC.
Petitioner,

v.

VIRNETX, INC. AND SCIENCE APPLICATIONS INTERNATIONAL
CORPORATION,
Patent Owners

Patent No. 8,504,697
Issued: August 6, 2013
Filed: December 28, 2011

Inventors: Victor Larson, *et al.*

Title: SYSTEM AND METHOD EMPLOYING AN AGILE NETWORK
PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN
NAMES

Inter Partes Review No. IPR2014-00237

Declaration of Michael Fratto Regarding

U.S. Patent No. 8,504,697

Petitioner Apple Inc. - Exhibit 1003, p. 1

269. Beser explains that traffic within an IP tunnel is usually encrypted using an industry standard technique called IP Security or “IPsec.” Ex. 1009 (Beser) at 1:54-55 (“Of course, the sender may encrypt the information inside the IP packets before transmission, *e.g.* with IP Security (“IPsec”)”).

270. This description of use of encryption techniques in conventional IP tunneling approaches is consistent with the guidance in the IPsec standard, RFC 2401 (Ex. 1010). For example, RFC 2401 explains:

IPsec allows the user (or system administrator) to control the granularity at which a security service is offered. For example, **one can create a single encrypted tunnel to carry all the traffic between two security gateways or a separate encrypted tunnel can be created for each TCP connection between each pair of hosts communicating across these gateways.**

Ex. 1010 (RFC 2401) at 7.

Ex. 1003 at ¶¶ 269-70
Decision at 30-31; Pet. at 34-37

Obviousness over Beser and RFC 2401 video or audio data “*is encrypted*”

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

APPLE INC.
Petitioner,

v.

VIRNETX, INC. AND SCIENCE APPLICATIONS INTERNATIONAL
CORPORATION,
Patent Owners

Patent No. 8,504,697
Issued: August 6, 2013
Filed: December 28, 2011
Inventors: Victor Larson, *et al.*

Title: SYSTEM AND METHOD EMPLOYING AN AGILE NETWORK
PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN
NAMES

Inter Partes Review No. IPR2014-00237

Declaration of Michael Fratto Regarding

U.S. Patent No. 8,504,697

Petitioner Apple Inc. - Exhibit 1003, p. 1

323. Beser states that practical concerns related to transmission of VOIP and multimedia data over an IP tunnel may lead someone to not use encryption in an IP tunnel in certain circumstances. As it states:

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 (Beser) at 1:56-67.

324. **These practical concerns are plainly linked to two particular types of high volume data transfer situations (i.e., a where because of the high volume of data being transferred, the equipment may not be able to handle the volume of traffic)**. Of course, these concerns would not be an issue for the majority of data transfer scenarios. And even in these two high data volume applications, Beser indicates that encryption ordinarily should be used. Ex. 1009 (Beser) at 2:7-13.

Beser is just saying that it *may* not be possible to encrypt every packet and maintain transmission quality due to computer power limitation (e.g., during times of high network traffic). Ex. 1009 (Beser) at 2:7-13. Based on the way Beser is describing these high volume data transfer situations, **I believe a person of ordinary skill would have read the Beser patent as indicating that encryption should be used in its IP tunneling systems other than in specific resource constrained situations.**

Ex. 1003 at ¶ 323-24, 390; Pet. at 34-36; Decision at 30-31

Patent Owner Assertion (Beser & RFC 2401) video or audio data “*is encrypted*”

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 N
Paul Has
875 15th
Washing
Telephon
Facsimile
E-mail: r

UNITED STATES PATENT AND TRADE

BEFORE THE PATENT TRIAL AND APPEALS BOARD

APPLE INC.
Petitioner

v.

VIRNETX INC.
Patent Owner

Case IPR2014-00237
Patent 8,504,697

Patent Owner's Response

The combination also does not render obvious employing encryption to audio and video packets to enhance security. The Decision cites RFC 2401 for its teaching that the IPsec protocol allows for the creation of an encrypted tunnel. (Decision at 30-31.) RFC 2401, however, is the Network Working Group document outlining the standards for the IPsec protocol, which is the very feature that *Beser* suggests not to use, as discussed above. *Beser* acknowledges the existence of the IPsec protocol, but then recognizes its problems for video or audio data, so it teaches one of ordinary skill in the art away from RFC 2401 and the proposed combination of *Beser* and RFC 2401.

Opposition at 57

Obviousness over Beser and RFC 2401 video or audio data “*is encrypted*”

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

APPLE INC.
Petitioner,

v.

VIRNETX, INC. AND SCIENCE APPLICATIONS INTERNATIONAL
CORPORATION,
Patent Owners

Patent No. 8,504,697
Issued: August 6, 2013
Filed: December 28, 2011

Inventors: Victor Larson, *et al.*

Title: SYSTEM AND METHOD EMPLOYING AN AGILE NETWORK
PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN
NAMES

Inter Partes Review No. IPR2014-00237

Declaration of Michael Fratto Regarding

U.S. Patent No. 8,504,697

Petitioner Apple Inc. - Exhibit 1003, p. 1

386. The guidance in RFC 2401 would have specifically suggested encrypting all of the IP traffic being sent over a secure IP tunnel. *See* ¶¶ 341-343, *above*. This is also specifically suggested by Beser. *See* ¶¶ 269-270, *above*.

387. Another obvious design choice that is reflected in the IPsec standard itself is to set the IPsec parameters to accommodate the particular circumstances of the implementations being discussed in Beser (*e.g.*, a high network volume implementation using equipment with limited processing capacity). *See* ¶¶ 270, 343, *above*.

388. I also note that an obvious solution to the Beser problem would be to use more powerful edge routers that can accommodate the higher volume of network traffic for VOIP or multimedia applications. As Beser itself points out, the problems with encrypting VOIP or multimedia data traffic is not linked to what the data represents, but simply is the capacity of the device to encrypt on the fly the volume of data being transferred. Another obvious design choice would be to reduce the quality of the captured signal (*e.g.*, by sampling the voice call at a lower rate or by using a lower video quality), which would reduce the volume of data that had to be transferred. These would be practical, common sense solutions to the problem that Beser identifies of limited capacity of the network devices.

Ex. 1003 at ¶¶ 386-88; Pet. at 36-37

Patent Owner's Expert (Beser) video or audio data “*is encrypted*”

Q So I understand, the computational overhead impact is because it has to encrypt a lot of data, right?

A In the context of what Beser is stating.

Q So one way of solving that problem would be to have a more powerful computer that's doing the encrypting of the traffic, right?

MR. PALYS: Objection to form. Outside the scope of direct.

A That's one possible way.

[Ex. 206:20-207:7; Reply at 15](#)

Case IPR2014-00237
Patent 8,504,697

Patent Owner's Response

Q So the VoIP scenario, you're going to capture, you're going to digitize a voice that's somebody speaking into a phone, right?

A Mm-hmm.

Q And if you capture that at a very high resolution, you're going to capture more data to represent the voice signal, right?


A Could be the case. Mm-hmm.

Q And if you used a lower resolution or lower quality recording or digitization, you would use less data to represent the same voice?

A That's conceivable.

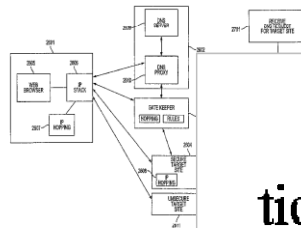
[Ex. 207:17-208:6; Reply at 15](#)

The '697 Patent, Claim 3

 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	(51) Int. Cl. <i>G06F 15/16</i> (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.
(75) Inventors: Victor Larson, Fairfax, VA (US); Robert Dunham Short, III, Leesburg, VA (US); Edmund Colby Mlunger, Crownsville, MD (US); Michael Williamson, South Riding, VA (US)	(56) References Cited U.S. PATENT DOCUMENTS 2,895,502 A 7/19/50 Roper et al. 4,677,434 A 6/1987 Fawcetta (Continued) FOREIGN PATENT DOCUMENTS DE 19924575 12/1999 EP 0838930 4/1988 (Continued) OTHER PUBLICATIONS Cisco Comments and Petition for Reexamination 95/001,679 dated Jun. 14, 2012. (Continued) Primary Examiner — Krisna Lim (74) <i>Attorney, Agent, or Firm</i> — McDermott Will & Emery LLP
(73) Assignee: VirnetX, Inc., Zephyr Cove, NV (US)	(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.
(*) 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.	(30) Claims, 40 Drawing Sheets
(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. 13/049,552, 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.	

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.

'697 Patent (Ex. 1001) at Claim 1



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

'697 Patent (Ex. 1001) at Claim 3

Institution Decision

Construction of “*virtual private network*”

Trials@uspto.gov
571-272-7822

Paper 15
Date: May 14, 2014

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

APPLE INC.
Petitioner

v.

On this record, a VPN is interpreted to mean a “secure communication link” with the additional requirement that the link includes a portion of a public network.

[Decision \(00237\) at 12](#)

EASTHOM, *Administrative Patent Judge*.

DECISION
Institution of *Inter Partes* Review
37 C.F.R. § 42.108

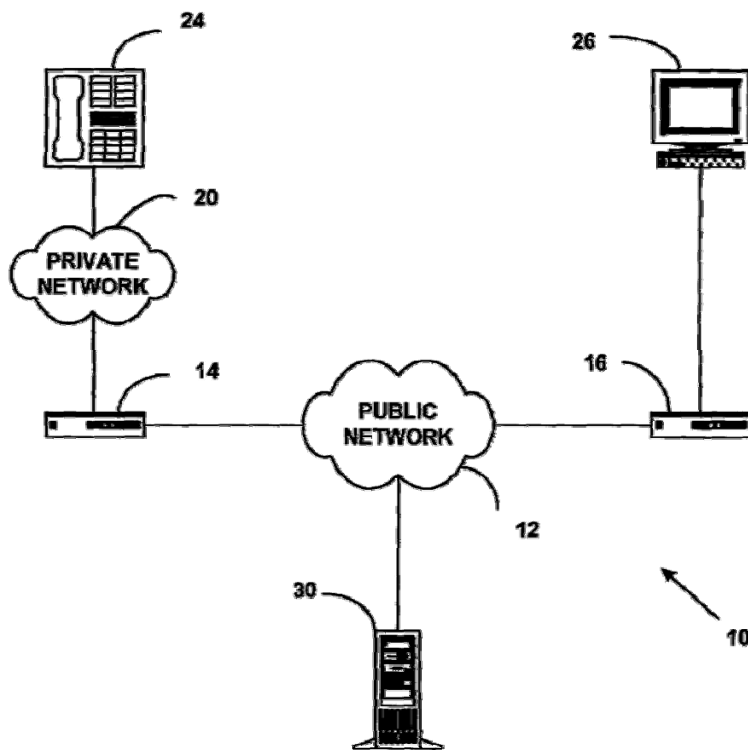
Anticipation by Beser video or audio data “is encrypted”

(12) United States Patent
Beser et al.



US000496867B1
(10) Patent No.: US 6,496,867 B1
(45) Date of Patent: Dec. 17, 2002

FIG. 1



Ex. 1009 at Fig. 1
Decision at 17; Pet. at 16-17; Ex. 1003 at ¶ 260

FIG. 1 is a block diagram illustrating an exemplary data network 10 for an illustrative embodiment of the present invention. The data network 10 includes a public network 12 (e.g. the Internet or a campus network), a first network device 14, and a second network device 16. The public network 12 is public in the sense that it may be accessible by many users who may monitor communications on it. Additionally, there may be present multiple private networks 20. Also, a trusted-third-party network device 30 is connected to the public network 12. Data packets may be transferred to/from the first network device 14, the second network device 16, and the trusted-third-party network device 30 over the public network 12. For example, the three devices may be assigned public network addresses on the Internet. The first network device 14 and the second network device 16 may be modified routers or modified gateways. The trusted-third-party 30 may be a back-end service, a domain name server, or the owner/manager of database or directory services. Moreover, the trusted-third-party network device 30 may not be located in one physical location but may be distributed over several locations and the information may be replicated over the several locations. However, other data network types and network devices can also be used and the present invention is not limited to the data network an network devices described for an illustrative embodiment.

Ex. 1009 at 3:60-4:18
Decision at 17; Pet. at 24-25; Ex. 1003 at ¶ 255

Grounds in -00238

- Whether Claims 1-3, 8-11, 14-17, 22-25, and 38-30 of the '697 patent are anticipated by U.S. Patent No. 5,898,830 to Wesinger (Ex. 1008)
- Whether Claims 4-7 and 18-21 of the '697 patent are obvious over Wesinger in view of RFC 2543 (Ex. 1012)

Anticipation by Wesinger

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

APPLE INC.
Petitioner,

v.

VIRNETX, INC. AND SCIENCE APPLICATIONS INTERNATIONAL
CORPORATION,
Patent Owners

Patent No. 8,504,697
Issued: August 6, 2013
Filed: December 28, 2011

Inventors: Victor Larson, *et al.*

Title: SYSTEM AND METHOD EMPLOYING AN AGILE NETWORK
PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN
NAMES

Inter Partes Review No. IPR2014-00238

Declaration of Michael Fratto Regarding

U.S. Patent No. 8,504,697

Petitioner Apple Inc. - Exhibit 1003, p. 1

263. Wesinger explains that its system enables the automatic creation of a secure connection in a manner that is transparent to users:

[T]he firewalls may be configured to also **transparently** perform any of various kinds of channel processing, including various types of **encryption** and decryption, compression and decompression, etc. In this way, **virtual private networks may be established whereby two remote machines communicate securely**, regardless of the degree of proximity or separation, **in the same manner as if the machines were on the same local area network.**

Ex. 1008 (Wesinger) at 4:47-52.

264. Wesinger explains that its firewalls allow for the creation of virtual private networks:

Combining encryption capabilities with programmable transparency as described above allows for **the creation of virtual private networks-networks** in which **two remote machines communicate securely** through cyberspace in the same manner **as if the machines were on the same local area network.**

Ex. 1008 (Wesinger) at 12:23-27.

**Ex. 1003 at ¶¶ 263-64
Decision at 19; Pet. at 16**

Anticipation by Wesinger

Ex. 1008 at Fig. 1; Ex. 1003 ¶ 295;
Pet. at 16-17; Decision at 15

United States Patent [19] [11] Patent Number: **5,898,8**
Wesinger, Jr. et al. [45] Date of Patent: **Apr. 27, 19**

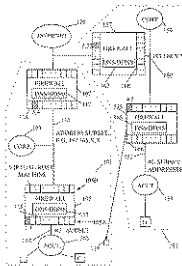


- [54] **FIREWALL PROVIDING ENHANCED NETWORK SECURITY AND USER TRANSPARENCY**
- [75] Inventors: **Ralph E. Wesinger, Jr.**, San Jose; **Christopher D. Coley**, Morgan Hill, both of Calif.
- [73] Assignee: **Network Engineering Software**, San Jose, Calif.
- [21] Appl. No.: **08/733,361**
- [22] Filed: **Oct. 17, 1996**
- [51] Int. Cl.⁴ **G06F 1/00**
- [52] U.S. Cl. **395/187.01; 395/200.55; 395/200.57**
- [58] **Field of Search** 395/186, 187.01, 395/188.01, 200.3, 200.55, 200.68, 200.57; 380/3, 4, 21, 23, 25; 340/825.3

- [56] **References Cited**
- U.S. PATENT DOCUMENTS**
- | | | | |
|-----------|---------|----------------|---------|
| 4,712,753 | 12/1987 | Boebert et al. | 364/200 |
| 4,799,153 | 1/1989 | Hann et al. | 380/25 |
| 4,799,156 | 1/1989 | Skott et al. | 364/401 |
| 5,191,611 | 3/1993 | Lang | 380/25 |
| 5,241,594 | 8/1993 | Rang | 380/4 |
| 5,416,842 | 5/1995 | Aziz | 380/50 |
- (List continued on next page.)

- OTHER PUBLICATIONS**
- Khuchi et al., "C-HTTP: The Development of a Secure, Closed HTTP Based Network on the Internet", Proceedings of SNDSS, IEEE, pp. 64-75, Jun. 1996.
- Neuman, "Proxy Based Authorization and Accounting for Distributed Systems", IEEE, pp. 283-291, 1993.
- Network Firewalls, IEEE Communications Magazine, (Ballouin et al.) pp. 50-57, Sep. 1994.
- The MITRE Security Perimeter, IEEE Communications Magazine, (Goldberg), pp. 212-218; 1994.

21 Claims, 9 Drawing Sheets



Petitioner Apple Inc. - Exhibit 1008

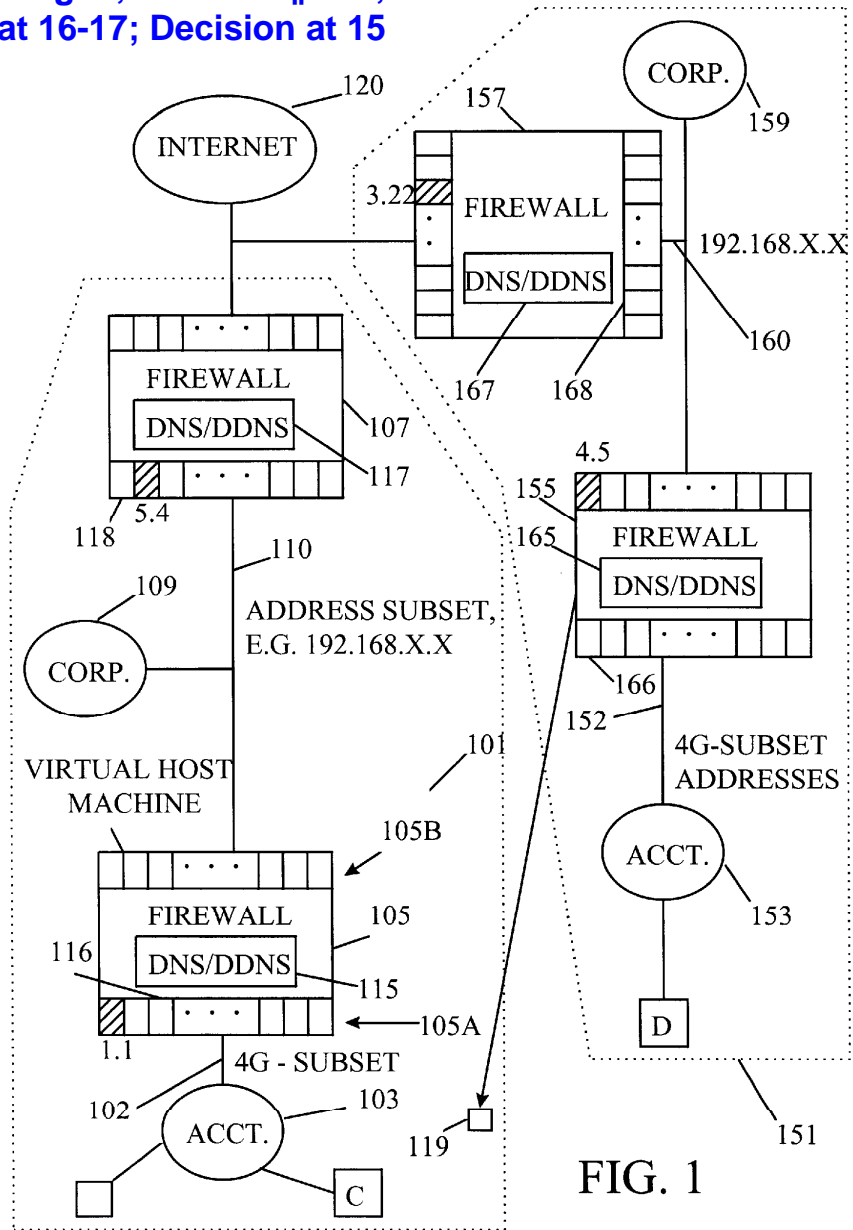



FIG. 1

The '697 Patent, Claim 1

“intercepting . . .”

 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	(51) Int. Cl. <i>G06F 15/16</i> (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.
(75) Inventors: Victor Larson , Fairfax, VA (US); Robert Dunham Short, III , Leesburg, VA (US); Edmond Colby Mungler , Crownsville, MD (US); Michael Williamson , South Riding, VA (US)	(56) References Cited U.S. PATENT DOCUMENTS 2,895,502 A 7/19/50 Roper et al. 4,877,434 A 6/1987 Fawcett (Continued) FOREIGN PATENT DOCUMENTS DE 19924575 12/1999 EP 0838930 4/1988 (Continued) OTHER PUBLICATIONS Cisco Comments and Petition for Reexamination 95/001,679 dated Jun. 14, 2012. (Continued)
(73) Assignee: VirnetX, Inc. , Zephyr Cove, NV (US)	(74) Primary Examiner — Krisna Lim (74) Attorney, Agent, or Firm — McDermott Will & Emery LLP
(*) 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.	(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
(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. 13/049,552, 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, 1999, now abandoned.	

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.

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;

'697 Patent (Ex. 1001) at Claim 1

Anticipation by Wesinger “intercepting . . .”

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

APPLE INC.
Petitioner,

v.

VIRNETX, INC. AND SCIENCE APPLICATIONS INTERNATIONAL
CORPORATION,
Patent Owners

Patent No. 8,504,697
Issued: August 6, 2013
Filed: December 28, 2011

Inventors: Victor Larson, *et al.*

Title: SYSTEM AND METHOD EMPLOYING AN AGILE NETWORK
PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN
NAMES

Inter Partes Review No. IPR2014-00238

Declaration of Michael Fratto Regarding

U.S. Patent No. 8,504,697

Petitioner Apple Inc. - Exhibit 1003, p. 1

278. Wesinger describes the benefits of using envoys and programmable transparency to facilitate the establishment of secure connections:

Normally, a prior-art proxy would have to prompt the user to enter a destination. To enable such prompting to occur, different proxy code has conventionally been required for each protocol to be proxied.

Using programmable transparency, the destination is provided to an envoy using DNS and/or DDNS as described more fully

hereinafter. There is therefore no need to always prompt the user for a destination and no need for the user to always enter a destination (although a mode of operation may be provided in which the user is prompted for and does enter a destination). Instead of a collection of conventional protocol-specific proxies, a single generic envoy program may be used.

Ex. 1008 (Wesinger) at 9:36-51 (emphasis added). Here, Wesinger shows that an envoy is the program that works with each virtual host to associate the virtual host with a destination IP address and to move data across the firewall.

Ex. 1003 at ¶ 278
Pet. at 17-18; see Decision at 15-16

Patent Owner Assertion (Wesinger)

“*intercepting . . .*”

Case No. IPR2014-00238

Paper No.

Fi

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 LL

875 15th Street N

Washington, DC

Telephone: (202)

Facsimile: (202)

E-mail: naveenm

UNITED STATES PATENT AND TRADEMARK

BEFORE THE PATENT TRIAL AND APPEAL

APPLE INC.
Petitioner

v.

VIRNETX INC.
Patent Owner

Case IPR2014-00238
Patent 8,504,697

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.”

Opposition at 49

***Wesinger*, however, does not disclose combining the name prompts (i.e., the Decision’s alleged “request”) of the prior art embodiment with its allegedly inventive disclosed embodiments.**

Opposition at 50

Anticipation by Wesinger “intercepting . . .”

UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE PATENT TRIAL AND APPEAL BOARD

APPLE INC.
Petitioner,
v.
VIRNETX, INC. AND SCIENCE APPLICATIONS INTERNATIONAL
CORPORATION,
Patent Owners

Patent No. 8,504,697
Issued: August 6, 2013
Filed: December 28, 2011
Inventors: Victor Larson, *et al.*
Title: SYSTEM AND METHOD EMPLOYING AN AGILE NETWORK
PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN
NAMES

Inter Partes Review No. IPR2014-00238

Declaration of Michael Fratto Regarding

U.S. Patent No. 8,504,697

Petitioner Apple Inc. - Exhibit 1003, p. 1

278. Wesinger describes the benefits of using envoys and programmable transparency to facilitate the establishment of secure connections:

Normally, a prior-art proxy would have to prompt the user to enter a destination. To enable such prompting to occur, different proxy code has conventionally been required for each protocol to be proxied.

Using programmable transparency, the destination is provided to an envoy using DNS and/or DDNS as described more fully

hereinafter. There is therefore no need to always prompt the user for a destination and no need for the user to always enter a destination (although a mode of operation may be provided in which the user is prompted for and does enter a destination). Instead of a collection of

conventional protocol-specific proxies, a single generic envoy program may be used.

Ex. 1008 (Wesinger) at 9:36-51 (emphasis added). Here, Wesinger shows that an envoy is the program that works with each virtual host to associate the virtual host with a destination IP address and to move data across the firewall.

Ex. 1003 at ¶ 278
Pet. at 17-18; see Decision at 15-16

Anticipation by Wesinger “intercepting . . .”

UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE PATENT TRIAL AND APPEAL BOARD

APPLE INC.
Petitioner,

v.
VIRNETX, INC. AND SCIENCE APPLICATIONS INTERNATIONAL
CORPORATION,
Patent Owners

Patent No. 8,504,697
Issued: August 6, 2013
Filed: December 28, 2011

Inventors: Victor Larson, *et al.*
Title: SYSTEM AND METHOD EMPLOYING AN AGILE NETWORK
PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN
NAMES

Inter Partes Review No. IPR2014-00238

Declaration of Michael Fratto Regarding

U.S. Patent No. 8,504,697


Petitioner Apple Inc. - Exhibit 1003, p. 1

267. Wesinger overcomes this problem with prior art systems using a firewall that intercepts a user’s request to initiate a connection and automatically establishes a connection with the remote host. Ex. 1008 (Wesinger) at 4:12-16 (“Using envoys, the added burden associated with prior-art proxy systems is avoided so as to achieve full transparency—the user can use standard applications and need not even know of the existence of the firewall.”), 4:32-38 (“The full transparency attribute of a single firewall system remains unchanged in a multi-layered system: a user may, if authorized, access a remote host multiple network layers removed, without knowing of the existence of any of the multiple firewalls in the system.”).

Ex. 1003 at ¶ 267
Pet. at 17; see Decision at 15-16

The '697 Patent, Claim 1

“determining . . .”

 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	(51) Int. Cl. <i>G06F 15/16</i> (2006.01)
(75) Inventors: Victor Larson, Fairfax, VA (US); Robert Dunham Short, III, Leesburg, VA (US); Edmund Colby Mungler, Crownsville, MD (US); Michael Williamson, South Riding, VA (US)	(52) U.S. CL. USPC 709/227
(73) Assignee: VirneX, Inc., Zephyr Cove, NV (US)	(58) Field of Classification Search USPC 709/223-227 See application file for complete search history.
(*) 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.	(56) References Cited U.S. PATENT DOCUMENTS 2,895,502 A 7/19/50 Roper et al. 4,677,434 A 6/19/87 Fawcetta (Continued)
(21) Appl. No.: 13/339,257	FOREIGN PATENT DOCUMENTS DE 19924575 12/1999 EP 0838930 4/1988 (Continued)
(22) Filed: Dec. 28, 2011	OTHER PUBLICATIONS Cisco Comments and Petition for Reexamination 95/001,679 dated Jun. 14, 2012. (Continued)
(65) Prior Publication Data US 2012/0102204 A1 Apr. 26, 2012	Primary Examiner — Krisna Lim (74) Attorney, Agent, or Firm — McDermott Will & Emery LLP
Related U.S. Application Data	(57) ABSTRACT
(63) Continuation of application No. 13/049,552, 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.	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.
(60) Provisional application No. 60/106,261, filed on Oct. 30, 1998, provisional application No. 60/137,704, filed on Jun. 7, 1999.	30 Claims, 40 Drawing Sheets

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.

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

'697 Patent (Ex. 1001) at Claim 1

Anticipation by Wesinger “determining . . .”

using envoys. Establishment of an envoy may be subjected to a myriad of tests to “qualify” the user, the requested communication, or both. Therefore, a high level of security may be achieved.

Ex. 1008 at 3:58-61; Ex. 1003 ¶ 301;
Decision at 16-17; Pet. at 18-19

United States Patent [19] [11] P
Wesinger, Jr. et al. [45] D

[54] FIREWALL PROVIDING ENHANCED NETWORK SECURITY AND USER TRANSPARENCY

[75] Inventors: Ralph E. Wesinger, Jr., San Jose; Christopher D. Coley, Morgan Hill, both of Calif.

[73] Assignee: Network Engineering Software, San Jose, Calif.

[21] Appl. No.: 08/733,361

[22] Filed: Oct. 17, 1996

[51] Int. Cl.⁷ G06F 1/00

[52] U.S. Cl. 395/187.01; 395/200.55; 395/200.57

[58] Field of Search 395/186, 187.01, 395/188.01, 200.3, 200.55, 200.68, 200.57; 380/3, 4, 21, 23, 25; 340/825.3

[56] References Cited

U.S. PATENT DOCUMENTS

4,712,753	12/1987	Bosbert et al.	364/200
4,799,153	1/1989	Hann et al.	380/225
4,799,156	1/1989	Skott et al.	364/401
5,191,611	3/1993	Lang	380/225
5,241,594	8/1993	Kang	380/4
5,416,842	5/1995	Aziz	380/30

(List continued on next page.)

OTHER PUBLICATIONS

Khuchi et al., “C-HTTP: The Development of a Secure, Closed HTTP Based Network on the Internet”, Proceedings of SNDSS, IEEE, pp. 64-75, Jun. 1996.

Neuman, “Proxy Based Authorization and Accounting for Distributed Systems”, IEEE, pp. 283-291, 1993.

Network Firewalls, *IEEE Communications Magazine*, (Ballouin et al.) pp. 50-57, Sep., 1994.

The MITRE Security Perimeter, *IEEE Communications Magazine*, (Goldberg), pp. 212-218, 1994.



IpAccess—A
Installations;
pp. 31-41; 1
Remote Cod
SNMP, *IEEE*
pp. 673-667;
Firewall's In
Corporation.
Primary Exa
Attorney, Ag
Beighoff

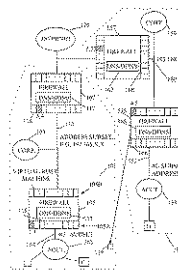
[57]

ABSTRACT

The present invention, generally speaking, provides a firewall that achieves maximum network security and maximum user convenience. The firewall employs “envoys” that exhibit the security robustness of prior-art proxies and the transparency of the firewall by being the firewall that traffic. It uses envoys to a myriad of communications systems to achieve transparency not even known in full transparent sets of virtual hosts, each set of hosts is of the firewall that interface be achieved hosts to virtual herein as

The foregoing discussion has focused on the programmable transparency aspects of the present firewall. Of course, a primary function of a firewall is to selectively allow and disallow communications. Hence, in the course of establishing a connection, each virtual host examines a configuration table to determine, based on the particulars of the requested connection—source, destination, protocol, time-of-day, port number, etc.—whether such a connection will be allowed or disallowed. The process by which con-

Ex. 1008 at 9:52-60; Ex. 1003 ¶ 301;
Decision at 16-17; Pet. at 18-19



Anticipation by Wesinger “determining . . .”

occur and which users are authorized. The access rules database may have an Allow portion, a Deny portion or both. Processing with respect to the Allow database is performed prior to processing with respect to the Deny database. Therefore, if there is an entry for a the requested connection in the Allow database and no entry for that connection in the Deny database, then the connection will be allowed. If there is no Allow database and no entry in the Deny database, then the connection will also be allowed. If there is an entry for the requested connection in the Deny database, then the connection will be denied regardless. Machines may be specified by name or by IP address, and may include “wildcards,” address masks, etc., for example: MisterPain.com, *.srmc.com, 192.168.0.*, 192.168.0.0/24, and so on.

Ex. 1008 at Fig. 7, 15:32-46; Ex. 1003 ¶ 287, 299;
Decision at 16; Pet. at 18-19

United States Patent [19]
Wesinger, Jr. et al.

[11] Patent Number:
[45] Date of Patent:



[54] FIREWALL PROVIDING ENHANCED NETWORK SECURITY AND USER TRANSPARENCY
[75] Inventors: Ralph E. Wesinger, Jr., San Jose; Christopher D. Coley, Morgan Hill, both of Calif.
[73] Assignee: Network Engineering Software, San Jose, Calif.
[21] Appl. No.: 08/733,361
[22] Filed: Oct. 17, 1996
[51] Int. Cl.⁷ G06F 1/00
[52] U.S. Cl. 395/187.01; 395/200.55; 395/200.57
[58] Field of Search 395/186, 187.01, 395/188.01, 200.3, 200.55, 200.68, 200.57; 380/3, 4, 21, 23, 25; 340/825.3

[56] References Cited
U.S. PATENT DOCUMENTS
4,713,753 12/1987 Bosbert et al. 364/200
4,799,153 1/1989 Finn et al. 380/25
4,799,156 1/1989 Skovet et al. 364/401
5,191,611 3/1993 Lang 380/25
5,241,594 8/1993 Kang 380/4
5,416,842 5/1995 Aziz 380/30

(List continued on next page.)

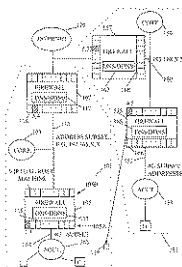
OTHER PUBLICATIONS

Khachi et al., “C-HTTP: The Development of a Secure, Closed HTTP Based Network on the Internet”, Proceedings of SNDSS, IEEE, pp. 64-75, Jun. 1996.
Neuman, “Proxy Based Authorization and Accounting for Distributed Systems”, IEEE, pp. 283-291, 1993.
Network Firewalls; IEEE Communications Magazine; (Ballouin et al.) pp. 50-57, Sep., 1994.
The MITRE Security Perimeter; IEEE Communications Magazine; (Goldberg), pp. 212-218; 1994.

IpAccess—An Internet Service Ac Installations; IEEE Communicatio pp. 31-41; 1995.
Remote Control of Diverse Ne SNMP; IEEE Communications M pp. 673-667, 1995.
Firewall's Information is Money! Corporation.
Primary Examiner—Joseph Palys Attorney, Agent, or Firm—McDon Beighoff [57] ABSTRACT

The present invention, generally a wall that achieves maximum user convenience. The firewa exhibit the security robustness of transparency and ease-of-use of pri bining the best of both worlds. Ne the firewall unless the firewall has that traffic. Both connection-orien tionless (e.g., UHP-based) se using envoys. Establishment of an to a myriad of tests to “qualify” communication, or both. Therefore may be achieved. The usual added systems is avoided in such a transparency—the user can use stand not even know of the existence of full transparency, the firewall is ce sets of virtual hosts. The firewa boomed,” each home being indepen set of hosts responds to addresses o of the firewall. Another set of hosts a second network interface of the programmable transparency is a DNS mappings between remote hos one of the network interfaces and r that interface. In another aspect, ant be achieved using code for dyna hosts to virtual hosts in accordance to herein as dynamic DNS, or DD

21 Claims, 9 Drawi



Anticipation by Wesinger “determining . . .”

United States Patent [19] [11]
Wesinger, Jr. et al. [45]

[54] FIREWALL PROVIDING ENHANCED NETWORK SECURITY AND USER TRANSPARENCY
[75] Inventors: Ralph E. Wesinger, Jr., San Jose; Christopher D. Coley, Morgan Hill, both of Calif.
[73] Assignee: Network Engineering Software, San Jose, Calif.
[21] Appl. No.: 08/733,361
[22] Filed: Oct. 17, 1996
[51] Int. Cl.⁶ G06F 1/00
[52] U.S. Cl. 395/187.01; 395/200.55; 395/200.57
[58] Field of Search 395/186, 187.01, 395/188.01, 200.3, 200.55, 200.68, 200.57; 380/3, 4, 21, 23, 25; 340/825.3

[56] References Cited
U.S. PATENT DOCUMENTS
4,713,753 12/1987 Bosbert et al. 364/200
4,799,153 1/1989 Finn et al. 380/25
4,999,156 1/1989 Skovet et al. 364/401
5,191,611 3/1993 Lang 380/25
5,241,594 8/1993 Kang 380/4
5,416,842 5/1995 Aziz 380/50

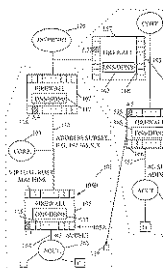
(List continued on next page.)

OTHER PUBLICATIONS

Khuchi et al., “C-HTTP: The Development of a Secure, Closed HTTP Based Network on the Internet”, Proceedings of SNDSS, IEEE, pp. 64-75, Jun. 1996.
Neuman, “Proxy Based Authorization and Accounting for Distributed Systems”, IEEE, pp. 283-291, 1993.
Network Firewalls; *IEEE Communications Magazine*; (Ballouin et al.) pp. 50-57, Sep., 1994.
The MITRE Security Perimeter; *IEEE Communications Magazine*; (Goldberg), pp. 212-218; 1994.



IpAccess—Installation pp. 31-41; Remote C. SNMP; *IEEE* pp. 673-68
Firewall’s Corporate Primary E. Attorney, / Beighoff [57]
The present wall that i. morn user exhibit the transparent the firewall that traffic netionless using enve to a myrii communic may be act systems p. transparency—the user can use standard applications and need not even know of the existence of the firewall. To achieve full transparency, the firewall is configured as two or more sets of vi boomed,” ei set of hosts of the firew a second i program; DNS mapp one of the that interfa be achieve hosts to vii to herein s



Petition

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; Ex. 1003 ¶ 284; Decision at 16; Pet. at 18-19; Reply at 7

Once the connection has been allowed, the virtual host process invokes code 818 that performs protocol-based connection processing and, optionally, code 823 that performs channel processing (encryption, decryption, compression, decompression, etc.). When processing is completed, the connection is closed, if it has not already been closed implicitly.

Ex. 1008 at 17:1-7; Reply at 12

Anticipation by Wesinger “determining . . .”

Channel processing may be performed using existing standard software modules. In the case of encryption and decryption, for example, modules for DES, RSA, Cylink, SET, SSL, and other types of encryption/decryption and authentication may be provided on the firewall. In the case of compression and decompression, standard modules may include MPEG, JPEG, LZ-based algorithms, etc. Based on information contained in the configuration files, information passing through the firewall may be processed using one or more such modules depending on the direction of data flow.

Ex. 1008 at 11:51-60; Ex. 1003 ¶ 301;
Decision at 16-17; Pet. at 16

United States Patent [19] [11]
Wesinger, Jr. et al. [45]

[54] FIREWALL PROVIDING ENHANCED NETWORK SECURITY AND USER TRANSPARENCY
[75] Inventors: Ralph E. Wesinger, Jr., San Jose; Christopher D. Coley, Morgan Hill, both of Calif.
[73] Assignee: Network Engineering Software, San Jose, Calif.
[21] Appl. No.: 08/733,361
[22] Filed: Oct. 17, 1996
[51] Int. Cl.⁷ G06F 1/00
[52] U.S. Cl. 395/187.01; 395/200.55; 395/200.57
[58] Field of Search 395/186, 187.01, 395/188.01, 200.3, 200.55, 200.68, 200.57; 380/3, 4, 21, 23, 25; 340/825.3

[56] References Cited
U.S. PATENT DOCUMENTS
4,713,753 12/1987 Bosbert et al. 364/200
4,799,153 1/1989 Finn et al. 380/225
4,799,156 1/1989 Skovet et al. 364/401
5,191,611 3/1993 Lang 380/25
5,241,594 8/1993 Kang 380/4
5,416,842 5/1995 Aziz 380/50

(List continued on next page.)

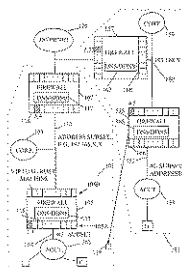
OTHER PUBLICATIONS

Khuchi et al., “C-HTTP: The Development of a Secure, Closed HTTP Based Network on the Internet”, Proceedings of SNDSS, IEEE, pp. 64-75, Jun. 1996.
Neuman, “Proxy Based Authorization and Accounting for Distributed Systems”, IEEE, pp. 283-291, 1993.
Network Firewalls; *IEEE Communications Magazine*; (Ballouin et al.) pp. 50-57, Sep., 1994.
The MITRE Security Perimeter; *IEEE Communications Magazine*; (Goldberg), pp. 212-218; 1994.

IpAccess—Installation pp. 31-41; Remote C. SNMP; *IEEE* pp. 673-68
Firewall’s Corporate Primary E. Attorney, / Beighoff [57]
The present wall that i. mern user exhibit the transparen bining the the firewal that traffic nectionless using enrv to a myri communicate may be act systems e transparent not even k full transpi sets of vi boomed,” e; set of hosts of the firew a second i program; DNS mapp

one of the network interfaces and respective virtual hosts on that interface. In another aspect, automatic transparency may be achieved using code for dynamically mapping remote hosts to virtual hosts in accordance with a technique referred to herein as dynamic DNS, or DDNS.

21 Claims, 9 Drawing Sheets



Petitioner Apple Inc. - Exhibit 1008, p. 1

Patent Owner Assertion (Wesinger)

“determining . . .”

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 Mod

Paul Hasting

875 15th Stre

Washington,

Telephone: (

Facsimile: (

E-mail: nave

***Wesinger* describes two separate processes, each responsive to a unique request and having unique characteristics. The first is a “transparent” DNS resolution process, which is set off by “DNS queries” or “name request[s].” (Ex. 1008 at 9:16-19, 13:9-14.) The second is non-transparent firewall allow/disallow processing, which is set off by a separate “ensuing connection request.” (Id.; Ex. 2025 at 21, ¶ 32, Monroe Decl.)**

Opposition at 32

UNITED STATES PATENT AND TRADEM

BEFORE THE PATENT TRIAL AND APPEAL BOARD

Wesinger is silent on how the connection request might arise following the DNS query, but is clear that a DNS query is not a connection request. *Wesinger*

Opposition at 35

Anticipation by Wesinger “determining . . .”

United States Patent [19] [11] Patent Number: 5,898,830
Wesinger, Jr. et al. [45] Date of Patent: Apr. 27, 1999



[54] FIREWALL PROVIDING ENHANCED NETWORK SECURITY AND USER TRANSPARENCY
[75] Inventors: Ralph E. Wesinger, Jr., San Jose; Christopher D. Coley, Morgan Hill, both of Calif.
[73] Assignee: Network Engineering Software, San Jose, Calif.
[21] Appl. No.: 08/733,361
[22] Filed: Oct. 17, 1996
[51] Int. Cl.⁷ G06F 1/00
[52] U.S. Cl. 395/187.01; 395/200.55; 395/200.57
[58] Field of Search 395/186, 187.01, 395/188.01, 200.3, 200.55, 200.68, 200.57; 380/3, 4, 21, 23, 25; 340/825.3

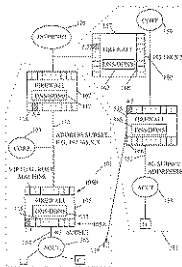
[56] References Cited
U.S. PATENT DOCUMENTS
4,713,753 12/1987 Boebert et al. 364/200
4,799,153 1/1989 Finn et al. 380/25
4,799,156 1/1989 Skovet et al. 364/401
5,191,611 3/1993 Lang 380/25
5,241,594 8/1993 Kang 380/4
5,416,842 5/1995 Aziz 380/30

(List continued on next page.)

OTHER PUBLICATIONS

Khuchi et al., “C-HTTP: The Development of a Secure, Closed HTTP Based Network on the Internet”, Proceedings of SNDSS, IEEE, pp. 64-75, Jun. 1996.
Neuman, “Proxy Based Authorization and Accounting for Distributed Systems”, IEEE, pp. 283-291, 1993.
Network Firewalls; *IEEE Communications Magazine*; (Ballouin et al.) pp. 50-57, Sep., 1994.
The MITRE Security Perimeter; *IEEE Communications Magazine*; (Goldberg), pp. 212-218; 1994.

21 Claims, 9 Drawing Sheets



Petitioner Apple Inc. - Exhibit 1008, p. 1

1. A method of establishing a connection between a first computer and a second remote computer along a route from the first computer to the second computer through a first intermediate system having a first interface to a first computer network and a second interface to a second computer network, without requiring a user to know of the intermediate system, the method comprising the steps of:

configuring the first intermediate system as a plurality of virtual hosts, each responsive to a network address used on one of the first and second computer networks;

mapping from a name of the second computer to a network address of one of the virtual hosts of the first intermediate system, said one of the virtual hosts being associated with the first interface;

issuing a request for a connection from the first computer to the second computer by specifying the name of the second computer;

receiving the request at the first interface and routing the request to said one of the virtual hosts in accordance with said mapping;

establishing a first bi-directional connection from the first computer to said one of the virtual hosts;

establishing a second bi-directional connection from said one of the virtual hosts to the second computer on behalf of the first computer; and

passing data between the first computer and the second computer using the first and second bi-directional connections.

Ex. 1008 at 17:17-46; Reply at 6-7

Patent Owner's Expert (Wesinger)

“determining . . .”

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) 551-1996
Facsimile: (202) 551-0496
E-mail: naveenmodi@paulhastings.com

UNITED STATES PATENT AND TRADEMARK

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 Response

Case

File

Q Okay. So the connection request originates on the first computer and it has the name of the second computer in the name of the connection request, right?

MR. PALYS: Objection to form.

BY MR. KUSHAN:

Q According to this step.

MR. PALYS: Same objection.

A It has an identifier that it's trying to connect to.

BY MR. KUSHAN:

Q And that identifier is the name of the second computer, according to the claim, right?

A In the claim.

Ex. 1083 at 258:4-259:12; Reply at 6-7

Anticipation by Wesinger “determining . . .”

United States Patent [19] [11] Patent Number: 5,898,830
Wesinger, Jr. et al. [45] Date of Patent: Apr. 27, 1999



[54] FIREWALL PROVIDING ENHANCED NETWORK SECURITY AND USER TRANSPARENCY

[75] Inventors: Ralph E. Wesinger, Jr., San Jose; Christopher D. Coley, Morgan Hill, both of Calif.

[73] Assignee: Network Engineering Software, San Jose, Calif.

[21] Appl. No.: 08/733,361

[22] Filed: Oct. 17, 1996

[51] Int. Cl.⁶ G06F 1/00

[52] U.S. Cl. 395/187.01; 395/200.55; 395/200.57

[58] Field of Search 395/186, 187.01, 395/188.01, 200.3, 200.55, 200.68, 200.57; 380/3, 4, 21, 23, 25; 340/825.3

[56] References Cited

U.S. PATENT DOCUMENTS

4,713,753	12/1987	Bosbert et al.	364/200
4,799,153	1/1989	Hann et al.	380/225
4,799,156	1/1989	Skovet et al.	364/401
5,191,611	3/1993	Lang	380/25
5,241,594	3/1993	Kang	380/4
5,416,842	5/1995	Aziz	380/30

(List continued on next page.)

OTHER PUBLICATIONS

Khuchi et al., “C-HTTP: The Development of a Secure, Closed HTTP Based Network on the Internet”, Proceedings of SNDSS, IEEE, pp. 64-75, Jun. 1996.

Neuman, “Proxy Based Authorization and Accounting for Distributed Systems”, IEEE, pp. 283-291, 1993.

Network Firewalls; *IEEE Communications Magazine*; (Ballouin et al.) pp. 50-57, Sep., 1994.

The MITRE Security Perimeter; *IEEE Communications Magazine*; (Goldberg), pp. 212-218; 1994.

IpAccess—An Intern...
Installations; *IEEE C...*
pp. 31-41; 1995.

Remote Control of
SNMP; *IEEE Commu...*
pp. 673-667, 1995.

Firewall's Informati...
Corporation.

Primary Examiner...
Attorney, Agent, or I...
Beighoff

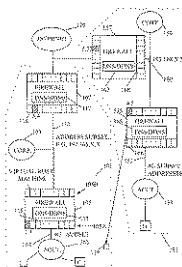
[57]

The present inventio...
wall that achieves a...
mum user convenien...
exhibit the security t...
transparency and eas...
bing the best of be...
the firewall unless th...
that traffic. Both co...
nectionless (e.g., U...
using envoys. Establ...
to a myriad of test...
communication, or b...
may be achieved. Th...
systems is avoided...
transparency—the use...
not even know of th...
full transparency, th...
sets of virtual hosts...
homed,” each home...
set of hosts respons...
of the firewall. Anot...
a second network in...
programmable trans...
DNS mappings betwe...
one of the network...
that interface. In an...
be achieved using c...
hosts to virtual hosts...
to herein as dynamic

21 Cla

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; Reply at 5



Anticipation by Wesinger “determining . . .”

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. The DNS server for D returns the network address of D to a virtual host on the firewall 155. The virtual host returns its network address to the virtual host on the firewall 157 from which it received the lookup request, and so on, until a virtual host on the firewall 105 returns its network address (instead of the network address of D) to the client C. This activity is all transparent to the user.

Ex. 1008 at 9:16-25; Ex. 1003 at ¶ 283-85; Pet. at 19; Reply at 7-8; Decision at 16

each protocol to be proxied. Using programmable transparency, the destination is provided to an envoy using DNS and/or DDNS as described more fully hereinafter. There is therefore no need to always prompt the user for a destination and no need for the user to always enter a destination (although a mode of operation may be provided in which the user is prompted for and does enter a destination). Instead of a collection of conventional

Ex. 1008 at 9:42-49; Ex. 1003 at ¶ 278; Decision at 16; Pet. at 19; Reply at 7

United States Patent [19] Patent Number: 5,898,831
Wesinger, Jr. et al. [45] Date of Patent: Apr. 27, 1999

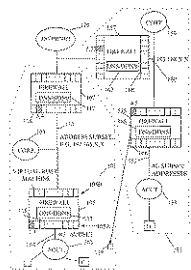


[54] FIREWALL PROVIDING ENHANCED NETWORK SECURITY AND USER TRANSPARENCY
[75] Inventors: Ralph E. Wesinger, Jr., San Jose; Christopher D. Coley, Morgan Hill, both of Calif.
[73] Assignee: Network Engineering Software, San Jose, Calif.
[21] Appl. No.: 08/733,361
[22] Filed: Oct. 17, 1996
[51] Int. Cl.⁷ G06F 1/00
[52] U.S. Cl. 395/187.01; 395/200.55; 395/200.57
[58] Field of Search 395/186, 187.01, 395/188.01, 200.3, 200.55, 200.68, 200.57; 380/3, 4, 21, 23, 25; 340/825.3

[56] References Cited
U.S. PATENT DOCUMENTS
4,712,753 12/1987 Boebert et al. 364/200
4,799,153 1/1989 Finn et al. 380/225
4,799,156 1/1989 Skovet et al. 364/401
5,191,611 3/1993 Lang 380/225
5,241,594 8/1993 Kang 380/4
5,416,842 5/1995 Aziz 380/30
(List continued on next page.)

OTHER PUBLICATIONS
Khuchi et al., “C-HTTP: The Development of a Secure, Closed HTTP Based Network on the Internet”, Proceedings of SNDSS, IEEE, pp. 64-75, Jun. 1996.
Neuman, “Proxy Based Authorization and Accounting for Distributed Systems”, IEEE, pp. 283-291, 1993.
Network Firewalls; IEEE Communications Magazine; (Ballouin et al.) pp. 50-57, Sep., 1994.
The MITRE Security Perimeter; IEEE Communications Magazine; (Goldberg), pp. 212-218; 1994.

21 Claims, 9 Drawing Sheets



Petitioner Apple Inc. - Exhibit 1008,

Patent Owner's Expert (Wesinger)

“determining . . .”

Case No. IPR2014-00238

Paper No.
Filed: August 2014

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 Response

Q That's not based on something Wesinger actually says; that's based on your analysis of how you understand Wesinger; is that fair to say?

MR. PALYS: Objection to form.

A No, it's based on -- it's saying that there is a -- that the virtual hosts for -- the DNS virtual host receives the connection requests, propagates processing of the DNS queries, Wesinger also that in the usual way, and later says there is these ensuing connections that are received by a daemon, and then spawn a separate virtual host.

And I agree with you, these other virtual hosts have the ability to read a configuration file and do some channel processing.

[Ex. 1083 at 275:16-276:6; Reply at 6](#)

Patent Owner's Expert (Wesinger)

“determining . . .”

Case No. IPR2014-00238

Paper No. _____
Filed: August 29, 2014

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 Response

Q And why -- so you're saying that that reading that I just gave you is not at all logical based on the fact that the front end of that paragraph is referring to the physical firewall machines managing and sharing the aggregate processing load of current connections?

MR. PALYS: Objection to form.

A So my understanding of -- and I think it's in keeping with one of ordinary skill in the art, would have interpreted what's here, in light of the specifications, it says there are these two separate things, right? One is on the ensuing connection, one is on a DNS query. In that paragraph, when I see it merging the two, then I'm assuming this ensuing connection it's talking about is very different than anything that has to do with the DNS request.

[Ex. 1083 at 283:13-284:6; Reply at 6](#)

Patent Owner's Expert (Wesinger)

“determining . . .”

Case No. IPR2014-00238

Paper No. _____
Filed: August 29, 2014

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 Response

Q I may have misspoken. Let me just make that clear. So at the time that the connection request is issued by the first computer under the claim, there has not been any DNS resolution yet, right?

A That's correct.

Q All right. So after that first connection request has occurred, that will then prompt a DNS lookup?

A On that firewall, that virtual host, to find a path through the network.

[Ex. 1083 at 254:14-255:2; Reply at 6](#)

Patent Owner's Expert (Wesinger)

"determining . . ."

Case No. IPR2014-00238

Paper No. _____
Filed: August 29, 2014

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 Response

Q The way you introduce that, you say, "Client C transmits a DNS query to its local firewall DNS server 115," right? And by that, are you saying the client C transmits a DNS query containing the name of D to its local firewall DNS server 115?

A So the specification says that the client transmits a DNS query to a local DNS server.


Q Right. And so the DNS query that we're talking about is the one that's in that first line from the paragraph that says "When client C tries to initiate a connection to host D," it's going to have the name of D in the query, right?

A Correct. And then DNS operates in its usual manner to propagate that.

[Ex. 1083 at 258:21-259:12; Reply at 9](#)

The '697 Patent, Claim 1

“initiating . . .”

 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	(51) Int. Cl. <i>G06F 15/16</i> (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.
(75) Inventors: Victor Larson, Fairfax, VA (US); Robert Dunham Short, III, Leesburg, VA (US); Edmond Colby Mungler, Crownsville, MD (US); Michael Williamson, South Riding, VA (US)	(56) References Cited U.S. PATENT DOCUMENTS 2,895,502 A 7/1950 Roper et al. 4,677,434 A 6/1987 Fawcetta (Continued) FOREIGN PATENT DOCUMENTS DE 19924575 12/1999 EP 0838930 4/1988 (Continued) OTHER PUBLICATIONS Cisco Comments and Petition for Reexamination 95/001,679 dated Jun. 14, 2012. (Continued)
(73) Assignee: VirnetX, Inc., Zephyr Cove, NV (US)	(74) Attorney, Agent, or Firm — Krisna Lim LLP (74) Attorney, Agent, or Firm — McDermott Will & Emery LLP
(*) 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.	(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 com-
(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. 13/049,552, 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) Provis 30, 1 filed e	

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

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;

'697 Patent (Ex. 1001) at Claim 1

Anticipation by Wesinger “initiating . . .”

United States Patent [19] [11]
Wesinger, Jr. et al. [45]

[54] FIREWALL PROVIDING ENHANCED NETWORK SECURITY AND USER TRANSPARENCY
[75] Inventors: Ralph E. Wesinger, Jr., San Jose; Christopher D. Coley, Morgan Hill, both of Calif.
[73] Assignee: Network Engineering Software, San Jose, Calif.
[21] Appl. No.: 08/733,361
[22] Filed: Oct. 17, 1996
[51] Int. Cl.⁶ G06F 1/00
[52] U.S. Cl. 395/187.01; 395/200.55; 395/200.57
[58] Field of Search 395/186, 187.01, 395/188.01, 200.3, 200.55, 200.68, 200.57; 380/3, 4, 21, 23, 25; 340/825.3

[56] References Cited
U.S. PATENT DOCUMENTS
4,713,753 12/1987 Bosbert et al. 364/200
4,799,153 1/1989 Finn et al. 380/225
4,799,156 1/1989 Skovet et al. 364/401
5,191,611 3/1993 Lang 380/225
5,241,594 8/1993 Kang 380/4
5,416,842 5/1995 Aziz 380/50

(List continued on next page.)

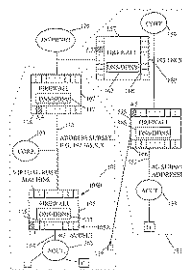
OTHER PUBLICATIONS

Khuchi et al., “C-HTTP: The Development of a Secure, Closed HTTP Based Network on the Internet”, Proceedings of SNDSS, IEEE, pp. 64-75, Jun. 1996.
Neuman, “Proxy Based Authorization and Accounting for Distributed Systems”, IEEE, pp. 283-291, 1993.
Network Firewalls; *IEEE Communications Magazine*; (Ballouin et al) pp. 50-57, Sep., 1994.
The MITRE Security Perimeter; *IEEE Communications Magazine*; (Goldberg), pp. 212-218; 1994.



IpAccess—
Installation
pp. 31-41;
Remote C
SNMP; *IE*
pp. 673-69
Firewall's
Corporate
Primary E
Attorney,
Beighoff
[57]

The preser
wall that i
man user
exhibit the
transparen
bing the
the firewal
that traffic
nectionless
using encri
to a myri
communi
may be act
systems e
transparen
not even k
full transp
sets of vi
boomed,” e
set of hosts
of the firew
a second i
program;
DNS mappings between remote hosts to be accessed through one of the network interfaces and respective virtual hosts on that interface. be achieved e hosts to virtual to herein as d



Petitioner

Channel processing may be performed using existing standard software modules. In the case of encryption and decryption, for example, modules for DES, RSA, Cylink, SET, SSL, and other types of encryption/decryption and authentication may be provided on the firewall. In the case of compression and decompression, standard modules may include MPEG, JPEG, LZ-based algorithms, etc. Based on information contained in the configuration files, information passing through the firewall may be processed using one or more such modules depending on the direction of data flow.

Ex. 1008 at 11:51-60; Ex. 1003 ¶ 301;
Decision at 16-17; Pet. at 16

Once the connection has been allowed, the virtual host process invokes code 818 that performs protocol-based connection processing and, optionally, code 823 that performs channel processing (encryption, decryption, compression, decompression, etc.). When processing is completed, the connection is closed, if it has not already been closed implicitly.

Ex. 1008 at 17:1-7; Reply at 12

Anticipation by Wesinger “initiating . . .”

United States Patent [19] [11]
Wesinger, Jr. et al. [45]

[54] FIREWALL PROVIDING ENHANCED NETWORK SECURITY AND USER TRANSPARENCY
[75] Inventors: Ralph E. Wesinger, Jr., San Jose; Christopher D. Coley, Morgan Hill, both of Calif.
[73] Assignee: Network Engineering Software, San Jose, Calif.
[21] Appl. No.: 08/733,361
[22] Filed: Oct. 17, 1996
[51] Int. Cl.⁶ G06F 1/00
[52] U.S. Cl. 395/187.01; 395/200.55; 395/200.57
[58] Field of Search 395/186, 187.01, 395/188.01, 200.3, 200.55, 200.68, 200.57; 380/3, 4, 21, 23, 25; 340/825.3

[56] References Cited
U.S. PATENT DOCUMENTS
4,713,753 12/1987 Bosbert et al. 364/200
4,799,153 1/1989 Hinn et al. 380/225
4,799,156 1/1989 Skovet et al. 364/401
5,191,611 3/1993 Lang 380/225
5,241,594 8/1993 Kang 380/4
5,416,842 5/1995 Aziz 380/30

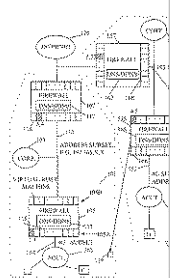
(List continued on next page.)

OTHER PUBLICATIONS

Khuchi et al., “C-HTTP: The Development of a Secure, Closed HTTP Based Network on the Internet”, Proceedings of SNDSS, IEEE, pp. 64-75, Jun. 1996.
Neuman, “Proxy Based Authorization and Accounting for Distributed Systems”, IEEE, pp. 283-291, 1993.
Network Firewalls; *IEEE Communications Magazine*; (Ballouin et al.) pp. 50-57, Sep., 1994.
The MITRE Security Perimeter; *IEEE Communications Magazine*; (Goldberg), pp. 212-218; 1994.



IpAccess—Installation pp. 31-41; Remote C. SNMP; *IEEE* pp. 673-69
Firewall’s Corporate Primary E. Attorney, / Beighoff [57]
The preser wall that i man user exhibit the transparen bining the the firewal that traffic netionless using enryp to a myrii communic may be act systems e transparen not even k full transp sets of vi boomed,” ei set of hosts of the firew a second i program; DNS map one of the that interfa be achieve hosts to vii to herein a



Petition

Encryption and decryption are particularly important to realizing the potential of the Internet and network communications. In the example just described, on the network segment between firewall 105 and 107, DES encryption might be used, in accordance with the configuration file on firewalls 105 and 107. Across the Internet, between firewall 107 and firewall 155, triple DES may be applied. On the network segment between firewall 155 and 157 RSA encryption may be used. Alternatively, encryption could be performed between firewalls 105 and 155 and also between 107 and 155 and also between 157 and 155. Thus the firewall 157 may then decrypt the cumulative results of the foregoing multiple encryptions to produce clear text to be passed on to host D. Combining encryption capabilities with programmable transparency as described above allows for the creation of virtual private networks—networks in which two remote machines communicate securely through cyberspace in the same manner as if the machines were on the same local area network.

Ex. 1008 at 12:9-28; Ex. 1003 ¶ 299; Decision at 17; Pet. at 19-20

Anticipation by Wesinger “initiating . . .”

UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE PATENT TRIAL AND APPEAL BOARD

APPLE INC.
Petitioner,

v.

VIRNETX, INC. AND SCIENCE APPLICATIONS INTERNATIONAL CORPORATION,
Patent Owners

Patent No. 8,504,697
Issued: August 6, 2013
Filed: December 28, 2011

Inventors: Victor Larson, *et al.*

Title: SYSTEM AND METHOD EMPLOYING AN AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE NAMES

Inter Partes Review No. IPR2014-00238

Declaration of Michael Fratto Regarding

U.S. Patent No. 8,504,697


Petitioner Apple Inc. - Exhibit 1003, p. 1

292. Each firewall between the client and the destination spawns a virtual host to process the request. Ex. 1008 (Wesinger) at 9:15-25. When the virtual host is created, it will load the configuration file and access rules. When the firewall spawns a virtual host, it loads the configuration file for the client and destination. Ex. 1008 (Wesinger) at 10:13-16, 24-28. The virtual host will verify that the connection is permitted before processing the request and returning its IP address. Ex. 1008 (Wesinger) at 15:54-57 (“All access rules must be satisfied in order to gain access to a virtual host.”).

Ex. 1003 at ¶ 292
Pet. at 19-20; see Decision at 17

The '697 Patent, Claim 1

“wherein . . .”

 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	(51) Int. Cl. <i>G06F 15/16</i> (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.
(75) Inventors: Victor Larson , Fairfax, VA (US); Robert Dunham Short, III , Leesburg, VA (US); Edmond Colby Munger , Crownsville, MD (US); Michael Williamson , South Riding, VA (US)	(56) References Cited U.S. PATENT DOCUMENTS 2,895,502 A 7/19/50 Roper et al. 4,677,434 A 6/1987 Fawcett (Continued) FOREIGN PATENT DOCUMENTS DE 19924575 12/1999 EP 0838930 4/1988 (Continued) OTHER PUBLICATIONS Cisco Comments and Petition for Reexamination 95/001,679 dated Jun. 14, 2012. (Continued)
(73) Assignee: VirnetX, Inc. , Zephyr Cove, NV (US)	(74) Primary Examiner — Krisna Lim (74) Attorney, Agent, or Firm — McDermott Will & Emery LLP
(*) 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.	(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 com-
(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. 13/049,552, 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) Provis 30, 1 filed e

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

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.

'697 Patent (Ex. 1001) at Claim 1

Anticipation by Wesinger “wherein . . .”

UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE PATENT TRIAL AND APPEAL BOARD

APPLE INC.
Petitioner,

v.

VIRNETX, INC. AND SCIENCE APPLICATIONS INTERNATIONAL CORPORATION,
Patent Owners

Patent No. 8,504,697
Issued: August 6, 2013
Filed: December 28, 2011

Inventors: Victor Larson, *et al.*

Title: SYSTEM AND METHOD EMPLOYING AN AGILE NETWORK
PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE
NAMES

Inter Partes Review No. IPR2014-00238

Declaration of Michael Fratto Regarding

U.S. Patent No. 8,504,697

Petitioner Apple Inc. - Exhibit 1003, p. 1

306. Wesinger explains that channel processing can leverage existing encryption software modules, as well as media processing software modules:

Channel processing may be performed using existing standard software modules. **In the case of encryption and decryption, for example, modules for DES, RSA, Cylink, SET, SSL, and other types of encryption/decryption and authentication may be provided on the firewall. In the case of compression and decompression, standard modules may include MPEG, JPEG, LZ-based algorithms, etc.**

Ex. 1008 (Wesinger) at 11:51-60. **MPEG is a well-known video compression technique, and JPEG a well-known image compression technique.**

Ex. 1003 at ¶ 306
Pet. at 20-21; see Decision at 17-18

The '697 Patent, Claims 8, 9, 22, 23

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

(10) **Patent No.:** US
(45) **Date of Patent:**



US008504697E

(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. 13/049,552, 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

(58) **Field of Classification Search**
USPC
See application file for complete search history.

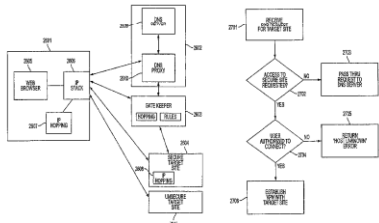
(56) **References Cited**
U.S. PATENT DOCUMENTS
2,895,502 A 7/19/50 Roper
4,677,434 A 6/1987 Fauscent
(Continued)

FOREIGN PATENT DOCUMENTS
DE 19924575 12/1996
EP 0838930 4/1998
(Continued)

OTHER PUBLICATIONS
Cisco Comments and Petition for Reexamination 95/001,679 dated Jun. 14, 2012.
(Continued)
Primary Examiner—Krisna Lim
(74) **Attorney, Agent, or Firm**—McDermott Will & Emery LLP

(57) **ABSTRACT**
A system and method connect a first network device to a second network device by initiating a secure communication link. The system includes one or more network devices. A first network device receives, from the first network device, a network address of the second network device. The first network device identifies the second network device based on the network address. In response to the request, when the second network device is available for a secure communication link, the first network device initiates a secure communication link with the second network device. The second network device receives the secure communication link. The second network device initiates a secure communication link with the first network device. The second network device communicates at least one of video data and audio data with the first network device and the second network device.

30 Claims, 40 Drawings



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.

'697 Patent (Ex. 1001) at Claims 8 & 9

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.

'697 Patent (Ex. 1001) at Claims 22 & 23

Anticipation by Wesinger

Claims 8, 9, 22, and 23

UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE PATENT TRIAL AND APPEAL BOARD

APPLE INC.
Petitioner,

v.
VIRNETX, INC. AND SCIENCE APPLICATIONS INTERNATIONAL CORPORATION,
Patent Owners

Patent No. 8,504,697
Issued: August 6, 2013
Filed: December 28, 2011
Inventors: Victor Larson, *et al.*
Title: SYSTEM AND METHOD EMPLOYING AN AGILE NETWORK
PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE
NAMES

Inter Partes Review No. IPR2014-00238


Declaration of Michael Fratton Regarding
U.S. Patent No. 8,504,697

Petitioner Apple Inc. - Exhibit 1003, p. 1

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.

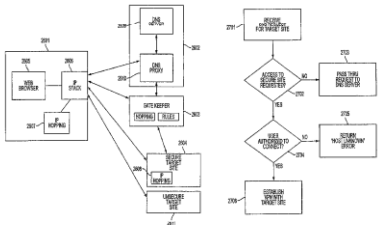
Ex. 1003 at ¶ 270
Pet. at 24-25; see Decision at 18-19

Obviousness by Wesinger and RFC 2543 Claims 4-7 and 18-21



US008504697

<p>(12) United States Patent Larson et al.</p> <p>(54) SYSTEM AND METHOD EMPLOYING AN AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES</p> <p>(75) Inventors: Victor Larson, Fairfax, VA (US); Robert Dunham Short, III, Leesburg, VA (US); Edmond Colby Mlunger, Crownsville, MD (US); Michael Williamson, South Riding, VA (US)</p> <p>(73) Assignee: VirnetX, Inc., Zephyr Cove, NV (US)</p> <p>(*) 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.</p> <p>(21) Appl. No.: 13/339,257</p> <p>(22) Filed: Dec. 28, 2011</p> <p>(65) Prior Publication Data US 2012/0102204 A1 Apr. 26, 2012</p> <p>Related U.S. Application Data</p> <p>(63) Continuation of application No. 13/049,552, 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.</p> <p>(60) Provisional application No. 60/106,261, filed on Oct. 30, 1998, provisional application No. 60/137,704, filed on Jun. 7, 1999.</p>	<p>(10) Patent No.: U</p> <p>(45) Date of Patent:</p> <p>(51) Int. Cl. G06F 15/16 (2006)</p> <p>(52) U.S. CL. USPC</p> <p>(58) Field of Classification Search USPC See application file for complete search history.</p> <p>(56) References Cited</p> <p>U.S. PATENT DOCUMENTS 2,895,502 A 7/19/50 Roper 4,677,434 A 6/1987 Finsen (Continued)</p> <p>FOREIGN PATENT DOCUMENTS DE 19924575 12/19 EP 0838930 4/19 (Continued)</p> <p>OTHER PUBLICATIONS Cisco Comments and Petition for Reexamination Jun. 14, 2012. (Continued)</p> <p>Primary Examiner — Krisna Lim (74) Attorney, Agent, or Firm — McDERMOTT WILL & EMERY LLP</p> <p>(57) ABSTRACT A system and method connect a first network device to a second network device by initiating a secure communication link. The system includes one or more network devices that receive, from the first network device, a network address of the second network device and a second network identifier associated with the second network device. In response to the request, the second network device is available for a secure communication link. The system initiates a secure communication link between the first network device and the second network device and the second network device initiates a secure communication link with the first network device. The second network device and the first network device communicate at least one of video data and audio data over the secure communication link.</p> <p>30 Claims, 40 Drawings</p>
--	--



- 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.
- 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).

'697 Patent (Ex. 1001) at Claims 4-7

- 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).

'697 Patent (Ex. 1001) at Claims 18-21

Obviousness by Wesinger and RFC 2543

Claims 4-7 and 18-21

UNITED
BEFOR
VIRNETX, INC
Title: SYSTEM
PROTOCOL FOR

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 ¶¶ 309-313. That person also would have had a motivation to support such services using a common communication platform, because doing so would enable an organization to consistently implement and regulate security and access control measures. Ex. 1003 ¶¶ 309-313. The person also would have known that RFC 2543 supported standard telephony and video conferencing services, and that implementing these services on the Wesinger architecture would have been simple and straightforward from a technical perspective. Ex. 1003 ¶¶ 309-313, 364-368. Wesinger in view of RFC 2543 thus would have made implementing a video conferencing service on the Wesinger architecture obvious in February of 2000.

Pet. at 30; see also Ex. 1003 at ¶¶ 309-313, 364-368

Obviousness by Wesinger and RFC 2543

Claims 4-7 and 18-21

310. One common architecture was to have a firewall and a SIP server (described in Ex. 1012 (RFC 2543)). The SIP server could be located on either side of the firewall, and the firewall could regulate access to the server. For example, the SIP server might be located outside of the firewall and be integrated with the organization's PBX, which is conventional phone system. Wesinger's transparent firewall could regulate a user's ability to place certain types of phone calls. For example, the firewall could permit a client to dial restrict a client's ability to place an international call. Where the SIP server was located inside the firewall, the firewall could restrict incoming calls.

Ex. 1003 at ¶ 310; see generally ¶¶ 309-313
Pet. at 29-30

Obviousness by Wesinger and RFC 2543 Claims 4-7 and 18-21

UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE PATENT TRIAL AND APPEAL BOARD

APPLE INC.
Petitioner,

v.

VIRNETX, INC. AND SCIENCE APPLICATIONS INTERNATIONAL CORPORATION,
Patent Owners

Patent No. 8,504,697
Issued: August 6, 2013
Filed: December 28, 2011

Inventors: Victor Larson, *et al.*

Title: SYSTEM AND METHOD EMPLOYING AN AGILE PROTOCOL FOR SECURE COMMUNICATIONS USING SEVERAL NAMES

Inter Partes Review No. IPR2014-00238

Declaration of Michael Fratto Regarding

U.S. Patent No. 8,504,697

Petitioner Apple

309. Wesinger shows that its transparent firewalls can be used in the corporate setting for connecting different offices across a LAN or the Internet. Ex. 1008 (Wesinger) at 1:38-40 (“Corporate Intranets have become a strong driving force in the marketplace of network products and services”), Figure 1 (showing CORP and ACCT sub-networks). In February 2000, it was common for organizations to incorporate a VOIP server into such a configuration.

310. One common architecture was to have a firewall and a SIP server (described in Ex. 1012 (RFC 2543)). The SIP server could be located on either side of the firewall, and the firewall could regulate access to the server. For example, the SIP server might be located outside of the firewall and be integrated with the organization’s PBX, which is conventional phone system. Wesinger’s transparent firewall could regulate a user’s ability to place certain types of phone calls. For example, the firewall could permit a client to dial restrict a client’s ability to place an international call. Where the SIP server was located inside the firewall, the firewall could restrict incoming calls.

Ex. 1003 at ¶ 309-10
Pet. at 29-32; Reply at 14-15; Decision at 21-22

Obviousness by Wesinger and RFC 2543

Claims 4-7 and 18-21

UNITED STATES PATENT AND TRADEMARK
BEFORE THE PATENT TRIAL AND APPEAL

APPLE INC.
Petitioner,

v.

VIRNETX, INC. AND SCIENCE APPLICATIONS INTERNATIONAL CORPORATION,
Patent Owners

Patent No. 8,504,697
Issued: August 6, 2013
Filed: December 28, 2011
Inventors: Victor Larson, *et al.*
Title: SYSTEM AND METHOD EMPLOYING AN AG
PROTOCOL FOR SECURE COMMUNICATIONS USING
NAMES

Inter Partes Review No. IPR2014-00238

Declaration of Michael Fratto Regarding

U.S. Patent No. 8,504,697

Petitioner Ag

311. A SIP server would have been used to provide phone service to an organization's employees. RFC 2543 shows that, in addition to VOIP calls, SIP also supports a variety of other types of communications. For example SIP supports Internet-to-PSTN calls. Ex. 1012 (RFC 2543) at 9. It was well-known that voice data transmitted via a PSTN would be modulated using TDM. *See* ¶¶ 189, *above*.

312. RFC 2543 also shows that SIP servers support video conferencing and other multimedia calls. Ex. 1012 (RFC 2543) at 1, 7 (explaining that a SIP “session” “include[s] Internet multimedia conferences, Internet telephone calls and multimedia distribution”).

313. It would have been obvious to a person of ordinary skill in the art that a VOIP system such as that described in RFC 2543 could be incorporated into Wesinger's system.

**Ex. 1003 at ¶ 311-12
Pet. at 29-32; Reply at 14-15; Decision at 21-22**

Michael Fratto

9. I have been studying, evaluating, testing and describing networking, networking security and related technologies for more than 15 years. Since well before 1999, I have had an extensive background and experience in network systems, software and related technologies, with a particular focus on network security.

Ex. 1003 at ¶ 9

VIRNETX, INC. AND SCIENCE APPLICATIONS INTERNATIONAL
CORPORATION
Patent C
Patent No.
Issued: Aug
Filed: Decem
Inventors: Vict
Title: SYSTEM AND METHOD EM
PROTOCOL FOR SECURE COMMUNI
NAN

Inter Partes Review

Declaration of Micha
U.S. Patent N

10. I also have extensive hands-on experience with wide range of networking and networking security products developed and sold in the 1993 to 2002 time frame. This came from my various positions with Network Computing, where I reviewed, tested and described these products in a technical publication devoted to this field. I also wrote articles about network infrastructure, data center, and network access control items that were published by Network Computing. I also am very familiar with Internet standards governing networking and security, which I discuss below.

Ex. 1003 at ¶ 10

Michael Fratto

Patent Owner's challenge to Mr. Fratto's credentials is baseless. Mr. Fratto has over 15 years of experience in studying, evaluating, testing, and describing networking, networking security and related technologies. Ex. 1003 ¶ 9. In the early 1990s he was writing computer programs as part of an IT consulting business that provided remote office automation. Ex. 1081 (Fratto Dep. Tr.) at 13:4-14:7. He can write computer programs in several languages including "C, Pascal, Turbo Pascal, PERL, PHP, JAVA, Javascript, [and] a little bit of Python," all of which were self-taught. Ex. 1081 at 13:11-14:19. These subject areas are directly relevant to understanding the state of the art as it relates to the '697 patent, and more than qualify Mr. Fratto as an expert in these proceedings.

Reply at 1-2

Patent Owner's Expert

1

2 UNII

3 BEFC

4 APPLE INC.

5 v.

6 VIRNETX, I

7 APPLICATIO

8 CORPORATIO

9 Depos

Q So if I was -- let's say I don't have a master's degree, but then I go to work for Lucent, and 20 years later, let's say I started in 1980 at Lucent, in the year 2000, after 20 years of working at Lucent, building and deploying and conducting research in these systems, do you think that person would have the same amount of knowledge that a person with a master's degree would have?

Ex. 1083 at 48:8-49:9; Reply at 2

10 Job No.: 6

11 Pages: 1 - 296

12 Reported By: Lee Bursten, RMR, CRR

Patent Owner's Expert

MR. PALYS: Objection, form.

A That's so many things, so many what-ifs here. I mean, it really depends on the types of things they were doing during that period. You know, so -- so if they were doing things that are really relevant to understanding what the state of the art is, and they were getting all that necessary exposure, going through the technologies very closely, understanding the problems, the solutions, etc., I think it's conceivable.

As I said, just gauging on, as a proffer, and my own experience and folks that I've interacted with throughout the academic career, throughout my internships, this is my opinion on what I think would be necessary to understand the relevant art at the time. There could be others.

[Ex. 1083 at 48:8-49:9; Reply at 2](#)

1 UNITED STATES

2 BEFORE THE PAT

3 -----
4 APPLE INC.,

5 Petitione

6 v.

7 VIRNETX, INC. AND SO

8 APPLICATION INTERNA

9 CORPORATION,

10 Patent Ov

11 -----
12 Deposition of

13
14
15 Thursda

16
17
18
19
20 Job No.: 68382

21 Pages: 1 - 296

22 Reported By: Lee Bu