UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
95/001,714	08/16/2011	7,490,151 B2	43614.99	3428

137313 7590 06/23/2020
PAUL HASTINGS LLP
875 15th Street, NW
Washington, DC 20005

EXAMINER	
YIGDALL, MICHAEL J	

ART UNIT	PAPER NUMBER
3992	

MAIL DATE	DELIVERY MODE
06/23/2020	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

CISCO SYSTEMS, INC.
Requester and Cross-Appellant

v.

Patent of VIRNETX INC.
Patent Owner and Appellant

Appeal 2020-000639
Reexamination Control 95/001,714
Patent 7,490,151 B2
Technology Center 3900

Before JEFFREY B. ROBERTSON, DENISE M. POTHIER, and JEREMY J. CURCURI, *Administrative Patent Judges*.

ROBERTSON, *Administrative Patent Judge*.

DECISION ON APPEAL

I. STATEMENT OF THE CASE[1]

VirnetX Inc. ("Patent Owner") appeals under 35 U.S.C. §§ 134(b) and 315(a) (Pre-AIA) from the Examiner's decision to reject claims 1–16.[2] Third-Party Requester Cisco Systems Inc. (hereinafter "Cisco") urges that

[1] The instant reexamination proceeding was merged with Reexamination Control No. 95/001,697 filed by Apple, Inc. in a DECISION *SUA SPONTE* MERGING REEXAMINATION PROCEEDINGS entered March 15, 2012. In a "DECISION GRANTING RENEWED PETITION TO SEVER MERGER AND RENEWED PETITION TO TERMINATE REEXAMINATION PROCEEDING" entered October 16, 2019 ("Decision Severing Merger"), the merger was severed. The Decision Severing Merger concluded only that any rejection applied against claims 1–6 and 13–16 will not be further maintained by the Office "in the '1697 reexamination proceeding." Decision Severing Merger 15. This decision, however, considers rejections maintained by the Office against claims 1–6 and 13–16 for rejections as part of Reexamination Control No. 95/001,714 even though certain rejections originated from Reexamination Control No. 95/001,697. *See* DECISION ON JULY 9, 2013 PATENT OWNER PETITION FOR RELIEF FROM MAY 24, 2013 DECISION, July 7, 2014, 13–14 (explaining that Cisco is entitled to file a respondent brief that can address any of the Apple issues raised in patent owner's appellant brief because such are directed to the examiner's adopted rejections originally proposed by Apple addressed in patent owner's appellant brief); DECISION DENYING PATENT OWNER'S APRIL 2014 PETITION FOR REVIEW OF DECISION MAINTAINING MERGER OF REEXAMINATION PROCEEDINGS, September 21, 2015 13–15 (explaining the limits on appeal in merged proceedings); DECISION ON PETITIONS July 17, 2017 12 (explaining that the respondent's brief may include any arguments previously made of record that support the examiner's findings with respect to any claim addressed in the opposing party's appellant brief).

[2] *See* Patent Owner's Appeal Brief filed June 6, 2013 (hereinafter "PO Appeal Br.") vi; Examiner's Answer (mailed March 30, 2017) (hereinafter "Ans."); Right of Appeal Notice (mailed February 24, 2016) (hereinafter "RAN"); Patent Owner's Rebuttal Brief filed May 1, 2017 (hereinafter "PO Reb. Br.)".

the Examiner's decision must be affirmed.[3] Cisco cross-appeals under 35 U.S.C. §§ 134(c) and 315(b) from the Examiner's decision to withdraw several rejections of claims 1–16 on various grounds.[4] Patent Owner urges that the Examiner's decision must be affirmed.[5] We have jurisdiction under 35 U.S.C. §§ 134(b)–(c) and 315(a)–(b) (Pre-AIA).

We affirm-in-part the Examiner's decision to reject certain claims and to withdraw certain rejections. We reverse the Examiner's decision not to reject certain claims. By operation of rule, our reversal of the Examiner's decision not to reject certain claims is designated a new ground of rejection. 37 C.F.R. § 41.77(b).

II. INTRODUCTION

A. Background and Summary

United States Patent 7,490,151 B2 (hereinafter the "'151 Patent"), which is the subject of the current *inter partes* reexamination, issued to Munger et al. on February 10, 2009. *Inter partes* Reexamination was requested by Cisco ("REQUEST FOR INTER PARTES REEXAMINATION" filed on August 16, 2011, "Request"). Both Patent Owner and Cisco identify numerous related appeals and proceedings. *See* PO Appeal Br. iii–vi; Req. Appeal Br. 1–2. In particular, the Federal Circuit, in *VirnetX v. Mangrove Partners Master Fund, Ltd.*, 778 F. App'x

[3] *See* Cisco's Respondent Brief (filed August 18, 2016) (hereinafter "Cisco Resp't Br.").
[4] *See* Cisco's Appeal Brief filed June 3, 2016 (hereinafter "Cisco Appeal Br.") 3–4; Cisco's Rebuttal Brief filed May 1, 2017 (hereinafter "Cisco Reb. Br.").
[5] *See* Patent Owner's Respondent Brief filed February 27, 2017 (hereinafter "PO Resp't Br.").

897 (Fed. Cir. 2019), vacated and remanded a PTAB Final Written Decision in IPR2015-01047, an *inter partes* review of the '151 Patent.

The claims of the '151 Patent relate to secure and non-secure communications in response to a domain-name server look-up function. *See* '151 Patent, col. 36, l. 55 – col. 39, l. 46.

Claim 1, which is illustrative of the appealed subject matter, reads as follows:

> 1. A data processing device, comprising memory storing a domain name server (DNS) proxy module that intercepts DNS requests sent by a client and, for each intercepted DNS request, performs the steps of:
>
> (i) determining whether the intercepted DNS request corresponds to a secure server;
>
> (ii) when the intercepted DNS request does not correspond to a secure server, forwarding the DNS request to a DNS function that returns an IP address of a nonsecure computer, and
>
> (iii) when the intercepted DNS request corresponds to a secure server, automatically initiating an encrypted channel between the client and the secure server.

(PO Appeal Br. i, Claims App.)

B. Adopted Rejections

Patent Owner contests the Examiner's decision to reject the claims as follows (PO Appeal Br. 3; *see* RAN 7–41; Ans. 2–170):

Claim(s) Rejected	35 U.S.C. §	Reference(s)
1, 2, 5, 7, 8, 11, 13, 14	102(b)	Aventail Connect v3.01[6]
1, 2, 5, 7, 8, 11, 13, 14	102(b)	AutoSOCKS[7]
1, 2, 5, 7, 8, 11, 13, 14	103(a)	Beser,[8] Kent[9]
1–4, 7–10, 13–16	102(b)	Kiuchi[10]
5, 11	103(a)	Kiuchi, Martin[11]
1, 7, 13	103(a)	Aziz,[12] Edwards[13]
5, 11	103(a)	Aziz, Edwards, Martin
1–4, 6–10, 12–16	103(a)	Kiuchi, Edwards
5, 11	103(a)	Kiuchi, Edwards, Martin

[6] *Aventail Connect v3.01/v2.51 Administrator's Guide,* 1999 ("Aventail Connect v3.01").

[7] *Aventail AutoSOCKS v2.1 Administration & User's Guide,* 1997 ("AutoSOCKS").

[8] Beser et al., U.S. Patent No. 6,496,867, issued December 17, 2002 ("Beser").

[9] S. Kent and R. Atkinson, "Security Architecture for the Internet Protocol," Network Working Group RFC 2401, November 1998 ("Kent").

[10] Takahiro Kiuchi and Shigekoto Kaihara, C-HTTP – *The Development of a Secure, Closed HTTP-Based Network on the Internet*, PROCEEDINGS OF THE SYMPOSIUM ON NETWORK AND DISTRIBUTED SYSTEM SECURITY, IEEE 64–75 (1996) ("Kiuchi").

[11] David M. Martin Jr., *A Framework for Local Anonymity in the Internet*, Technical Report. Boston University, Boston, MA. (February 21, 1998) ("Martin").

[12] Ashar Aziz et al., U.S. Patent No. 6,119,234, issued September 12, 2000 ("Aziz").

[13] Nigel Edwards and Owen Rees, *High security Web servers and gateways*, "Computer Networks and ISDN Systems" 29 (Sept. 1997), pp. 927–938 ("Edwards").

C. Non-Adopted Rejections

Cisco contests the Examiner's decision to withdraw rejections of the claims as follows (Cisco Appeal Br. 2):

Claim(s) not Rejected	**35 U.S.C. §**	**Reference(s)**
6, 12	102(b)	Kiuchi
1–4, 6–10, 12–16	102(e)	Wesinger[14]
5, 11	103(a)	Wesinger, Martin
1, 7, 13	102(e)	Blum[15]
2–4, 6, 8–10, 12, 14–16	103(a)	Aziz, Edwards
1–4, 6–10, 12–16	103(a)	Wesinger, Edwards
5, 11	103(a)	Wesinger, Edwards, Martin

III. PATENT OWNER'S APPEAL

A. Anticipation – Kiuchi (Issue 7)[16]

1. The Examiner's Findings

The Examiner rejected claims 1–4, 7–10, and 13–16 as anticipated by Kiuchi. *See* Ans. 62–86. The Examiner found Kiuchi discloses a client (an end-user) selects and requests connection to a resource or server, which request is intercepted by the client-side proxy. *Id.* at 64–66, citing Kiuchi 64–65. The Examiner found Kiuchi discloses a client-side proxy stored on a

[14] Wesinger, Jr. et al., U.S. Patent No. 5,898,830, issued April 27, 1999 ("Wesinger").

[15] Blum et al., U.S. Patent No. 6,182,141 B1, issued January 30, 2001 ("Blum").

[16] The designation "Issue 7" is based on the labeling of rejections by the Patent Owner, Cisco, and the Examiner. We refer to these designations for convenience of the reader, although we address the "Issues" in a different order.

firewall. Ans. 65, citing Kiuchi 68. The Examiner found the client-side proxy disclosed in Kiuchi responds to a domain name inquiry by attempting to resolve the domain name to an IP address in two different ways; by (1) first requesting the IP address from a closed Hypertext Transfer Protocol-based network (C-HTTP), and if that fails, (2) requesting the IP address from an ordinary DNS. *Id.* at 65–66, citing Kiuchi 65.

As to the step of determining whether the intercepted DNS request corresponds to a secure server (the "determining step") recited in claim 1, the Examiner found Kiuchi discloses the C-HTTP-based secure server examines whether a requested server-side proxy is registered in the closed C-HTTP-based network, and when it is not, the client-side proxy receives an error status and then performs DNS lookup. *Id.* at 66–69, citing Kiuchi 64, 65, 68.

The Examiner found also Kiuchi discloses "automatically initiating an encrypted channel between the client and the secure server" as recited in claim 1. *Id.* at 71–72, citing Kiuchi 65–66. That is, the Examiner found Kiuchi discloses when the C-HTTP name server confirms the server-side proxy is an appropriate closed network member, the client-side proxy sends a request for connection, which is encrypted using the server-side proxy's public key, and that "following this request for connection, the client-side proxy (the 'client') and the server-side proxy (the 'secure server') exchange messages . . . Since the connection between the client-side proxy and the server-side proxy is established without any user involvement, the connection is initiated 'automatically.'" *Id.* at 72, citing Kiuchi 66. The Examiner found Kiuchi discloses the recited steps are performed for each request. *Id.* at 67.

2. Patent Owner's Contentions

Patent Owner contends Kiuchi fails to disclose a DNS proxy module, because Kiuchi discloses expressly that the closed HTTP-based network (C-HTTP) for communication does not involve DNS. PO Appeal Br. 35–37, citing Kiuchi 64, 68; Declaration of Angelo D. Keromytis dated May 8, 2012 ("Keromytis Decl."), ¶ 84. Patent Owner also contends Kiuchi fails to disclose the step of "determining whether the intercepted DNS request corresponds to a secure server" as recited in claim 1, because the rejection maps the "client-side proxy" to the DNS proxy module, but then maps the recited "determining" step to the "C-HTTP name server" disclosed in Kiuchi. PO Appeal Br. 37–38. Patent Owner argues Kiuchi does not disclose "automatically initiating an encrypted channel between the client and the secure server" as recited in claim 1. PO Appeal Br. 38–41. Patent Owner argues Kiuchi fails to disclose a DNS proxy module that performs the steps recited in claim 1 "for each intercepted DNS Request." PO Appeal Br. 41–42 (emphasis omitted).

3. Cisco's Contentions

Cisco responds that Patent Owner has provided no particular definition, claim interpretation, or substantive analysis that would differentiate the recited "DNS proxy module" and "DNS request" from Kiuchi's disclosure of a "domain name service" that "performs DNS lookup, behaving like an ordinary HTTP/1.0 proxy." Cisco Resp't Br. 14–16, citing Kiuchi 65. Cisco contends the client-side proxy performs the "determining step" by sending a request to the C-HTTP name server and evaluating the response received, such that the client-side proxy behaves differently depending on the received response of either receiving a secure network address, or an error message. *Id.* at 16–17. Cisco contends also that in the Examiner's analysis, the client-side proxy corresponds to the recited "client" in claim 1. *Id.* at 17–18. Cisco argues also that Kiuchi discloses that when a series of different target destinations is requested, Kiuchi discloses the client-side proxy will perform the recited steps of every request, initiating a new encrypted channel for each request. *Id.* at 18–19.

4. Analysis

We limit our discussion to claims 1 and 13–15, which is sufficient to resolve the issues associated with this rejection. *See* 37 C.F.R. § 41.67(c)(vii).

a) "Client"

We begin by addressing the Examiner's mapping of Kiuchi to the "client" recited in claim 1. In particular, as discussed above, we observe that at different points, the Examiner, in adopting Cisco's rejections, has mapped both the "user agent" as well as the "client-side proxy" disclosed in Kiuchi to the "client" recited in claim 1. *See* RAN 28–29. The Examiner's position is that regardless of whether the "user agent" or the "client-side proxy" disclosed in Kiuchi corresponds to the "client" in claim 1, claim 1 is anticipated by Kiuchi. *Id.* at 29.

We observe that the Federal Circuit, in summarizing Kiuchi, has previously equated the "user agent" disclosed in Kiuchi with a client. *VirnetX*, 778 F App'x at 905 ("[Kiuchi's] system consists of five relevant elements: a user agent (also referred to as a client), a client-side proxy, a C-HTTP name server, a server-side proxy, and an origin server."). In this regard, the Federal Circuit stated in a similar situation where Kiuchi's user agent and client-side proxy were both relied upon to correspond to the recited "client" that "[t]here is no question that these are different components in Kiuchi's system," and that a reliance on different components in Kiuchi as a disclosure of the recited "client" is not supported by substantial evidence. *Id.* at 778 F App'x at 907–908.

We are of the view that the "user agent" of Kiuchi corresponds to the "client" recited in claim 1. Kiuchi discloses a user agent requests an "HTML document" or "HTTP/1.0 request" that is encrypted and wrapped in a C-HTTP request by the client-side proxy. Kiuchi 65.

b) "Domain Name Server (DNS)"

We next address Patent Owner's argument that Kiuchi's C-HTTP techniques do not involve DNS. Cisco identifies several proceedings where the Patent Office has rejected Patent Owner's argument as insufficient to distinguish the services provided by Kiuchi's C-HTTP name server from DNS requests sent by a client. Cisco Resp't Br. 15. Although Kiuchi discloses a C-HTTP-based name service is used "instead of DNS" (Kiuchi, Abstr.), Patent Owner's arguments fail to identify a substantive difference between the DNS request recited in claim 1 and the user agent's request in Kiuchi, where the client-side proxy may perform a DNS lookup. *See* Kiuchi 65–66, Fig. c.[17] Thus, we are persuaded by the evidence that the resource name intercepted by the client-side proxy in Kiuchi is encompassed by the DNS request intercepted by the DNS proxy server recited in claim 1.

[17] We observe also that Patent Owner made similar arguments in IPR2015-01047, which the Board found to be unpersuasive. *Mangrove Partners Master Fund, LTD, Apple Inc., and Black Swamp IP, LLC v. VirnetX, Inc.*, IPR2015-01047, Paper 80 at 6–8 (PTAB Sept. 9, 2016) (Final Written Decision).

c) Each Intercepted DNS Request

We are not persuaded by Patent Owner's argument that Kiuchi fails to disclose performing the recited steps for each intercepted DNS request as recited in claim 1. In particular, as Cisco points out (Req. Resp't Br. 18–19), Kiuchi discloses a TCP connection is closed after each transaction (request and request pair). Kiuchi 65, 67. Thus, Kiuchi discloses performing the steps recited for each DNS request.

d) Steps (i) and (ii)

We are not persuaded that Kiuchi fails to disclose the recited "determining step" (i) in claim 1. At the outset, we clarify that the combination of the "client-side proxy" and the "C-HTTP name server" disclosed in Kiuchi corresponds to the DNS proxy module that performs steps (i) and (ii) recited in claim 1. That is, in Kiuchi, the client-side proxy asks the C-HTTP name server whether it can communicate with the host specified in a given URL, and if communication is not permitted, the C-HTTP server sends a status code indicating an error, which the client-side proxy receives and then performs a DNS lookup in accordance with step (ii) in claim 1. Kiuchi 65. Thus, the combined operation of the client-side proxy and C-HTTP name server in Kiuchi performs steps (i) and (ii) in claim 1. *See* Ans. 67–70, Chart E-1.1 (discussing how "examining 'whether the requested server-side proxy is registered in the closed network' shows determining whether the intercepted DNS request corresponds to a secure server a recited in the claim" and "[p]erforming 'DNS lookup' on requests that are not part of the closed network (i.e., do not correspond to a 'secure server' in the closed network) shows forwarding the DNS request to a DNS function as recited by the claim.").

e) Step (iii) "automatically initiating an encrypted channel between the client and the secure server"

We are not persuaded by Patent Owner's arguments that Kiuchi is silent as to whether the C-HTTP connections are established automatically.[18] PO Appeal Br. 38–39; Keromytis Decl. ¶¶ 88–89. Rather, we agree with the Examiner that Kiuchi, by disclosing the client-side proxy sends a request for connection to the server-side proxy and the server-side proxy sends a symmetric data exchange key for response encryption to the client-side proxy, after which connection is established, discloses "automatically initiating" as recited in the claims. RAN 28–29, citing Kiuchi 65–66. Thus, Patent Owner's assertions with respect to possible user agent involvement in establishing connections are not supported by the record.

f) Claims 1–4 and 7–10

As to the recitation in claim 1 that the encrypted channel is initiated "between the client and the secure server," the Examiner's view is that if the "user agent" in Kiuchi corresponds to the "client" recited in claim 1, the channel between the "user agent" and the "server-side proxy" is an encrypted channel, because requests from the user agent are forwarded in encrypted form from the client-side proxy to the server-side proxy and

[18] In view of the discussion of the Federal Circuit's Decision in *VirnetX v. Mangrove Partners Master Fund, Ltd.*, 778 F. App'x 897 above, we find it unnecessary to discuss Cisco's contention that Patent Owner is prohibited from arguing Kiuchi's disclosure of an encrypted link between the client-side proxy and the server-side proxy is distinguishable from the recitation in claim 1, "automatically initiating an encrypted channel between the client and the secure server," under 37 C.F.R. § 42.73, because in a final written decision in IPR2014-00482, the Board found the same argument unpersuasive. Cisco Resp't Br. 17.

responses to the user agent are forwarded from the server-side proxy to the client-side proxy "encrypted in C-HTTP format." RAN 29. In view of the discussion above, however, we are persuaded by Patent Owner's argument that Kiuchi discloses an encrypted link only between the client-side proxy and the server-side proxy. Appeal Br. 39. Kiuchi discloses only that communication between the client-side proxy and server-side proxy is encrypted while communications between a user agent and the client-side proxy or an origin server and server side proxy are performed "using current HTTP/1.0." Kiuchi, Abstract.

Accordingly, we reverse the Examiner's rejection of claims 1–4 as anticipated by Kiuchi. Because independent claim 7 contains similar language, we reverse the Examiner's rejection of claims 7–10 as anticipated by Kiuchi for similar reasons.

g) Claim 13

Independent claim 13 recites "when the intercepted DNS request corresponds to a secure server, automatically creating a secure channel between the client and the secure server." Thus, claim 13 does not require "encryption" between the client and the secure server. Kiuchi discloses "each member" of a closed group of institutions on the Internet "is protected by its own firewall." Kiuchi, Abstract, 64 § 2.1, 67 § 4.2. Therefore, we find Kiuchi discloses a secure channel as required by claim 13.

Accordingly, we affirm the Examiner's rejection of claim 13.

h) Claim 14

Claim 14 depends from claim 13 and recites, *inter alia*, "determining whether the client is authorized to access the secure server."

Patent Owner contends Kiuchi does not disclose determining whether the client is authorized to access a secure server because the client-side proxy is not synonymous with client, and while firewalls or proxies between two institutions may be authorized to communicate, individual clients and users within each institution may or may not be authorized to do so. PO Appeal Br. 43–44.

We are not persuaded by Patent Owner's argument. Rather, we agree with the Examiner's analysis, that the client-side proxy in Kiuchi, acting as a proxy for the client, determines whether the connection between the client and the secure server is permitted or not permitted, which is encompassed within the scope of "authorized" as recited in claim 14. RAN 32, citing Kiuchi 65; *see also* Kiuchi 65–66, disclosing the C-HTTP server determines whether the client-side proxy is an appropriate member of the closed network.

i) Claim 15

Claim 15 depends from claim 14, and recites "wherein step (iii) further comprises the step of: (c) when the client is not authorized to access the secure server, returning a host unknown error message to the client."

The Examiner found Kiuchi discloses an error message when the connection between the client-side proxy and server-side proxy is not permitted. Ans. 74–76, 85, citing Kiuchi 65, 68, and RFC 1035 at 27.[19]

Patent Owner contends the C-HTTP name server sends a status code that indicates an error, rather than the client-side proxy identified as the

[19] Mockapetris, P. RFC 1035, "Domain Names-Implementation and Specification," November 1987. Cisco Resp't Br., Ex. D8.

alleged DNS proxy module. PO Appeal Br. 45. Patent Owner argues also the error message is not returned to the client, but rather the client-side proxy. PO Appeal Br. 46. Patent Owner argues Cisco and the Office improperly rely on another reference, RFC 1035, in order support the position that DNS query formats and response codes include "host not found," and thus, the rejection "improperly relies on more than one reference for the claimed features" of claim 15. PO Appeal Br. 47.

We are persuaded by Patent Owner's arguments. That is, Kiuchi discloses only that the client-side proxy receives an error status when the C-HTTP name server determined the connection is not permitted, prompting it to perform a DNS lookup. Kiuchi 68. There is no indication that such an error message would be returned from the client-side proxy to the client or user agent discussed in Kiuchi. Thus, even if we were to agree that the Examiner's reliance on RFC 1035 is appropriate, such is insufficient to support the position that a "host unknown" error message would be returned to the client in the context of Kiuchi's system.

Accordingly, we reverse the Examiner's rejection of claim 15. Because claim 16 depends from claim 15, we reverse the Examiner's rejection of claim 16 as well.

In sum, we affirm the Examiner's decision to reject claims 13 and 14 as anticipated by Kiuchi. However, we reverse the Examiner's decision to reject claims 1–4, 7–10, 15, and 16 as anticipated by Kiuchi.

B. Obviousness – Claims 5 and 11 over Kiuchi and Martin (Issue 8)

Claims 5 and 11 depend from claims 1 and 7, respectively, and recite the step of initiating encrypted channel between the client and the secure server comprises establishing an IP address hopping scheme between the client and secure server. Martin is cited for disclosing an IP address hopping scheme that can co-exist with the system of Kiuchi. Ans. 90. Martin fails to cure the deficiencies identified in Kiuchi for claims 1 and 7. As a result, we reverse the Examiner's decision to reject claims 5 and 11 for similar reasons as discussed above with respect to claims 1 and 7.

C. Anticipation – Aventail Connect v3.01 (Issue 1)

1. The Examiner's Findings

The Examiner found, *inter alia*, Aventail Connect v3.01 discloses a proxy module that intercepts network traffic to and from a client application including DNS requests from a client application, where Aventail Connect encrypts the data on its way to the server on behalf of the application. Ans. 3–4, citing Aventail Connect v3.01 7, 12. The Examiner found Aventail Connect v3.01 discloses the channel is encrypted "at least from the application to the Aventail ExtraNet Server (a proxy server) along the path to the remote host." RAN 10. The Examiner found: "[s]pecifically, the channel between the application and the remote host is an 'encrypted channel' because the data on the channel is encrypted 'on its way' to the proxy server and when 'being returned' to the application." *Id.*

2. Patent Owner's Contentions

Patent Owner contends that Aventail Connect v3.01 has not been shown to be prior art, because there is insufficient evidence of public accessibility. PO Appeal Br. 4–7. In particular, Patent Owner argues the Declarations relied upon by the Examiner as evidence of public accessibility are uncorroborated. *Id.* at 4, citing, e.g., Declaration of James Chester.[20] Patent Owner argues the Examiner's reliance on the copyright date of 1999 in Aventail Connect v3.01 is insufficient to establish the reference as a printed publication. *Id.* at 7.

Substantively, Patent Owner contends Aventail Connect v3.01 does not disclose or suggest encrypted connections between the client and the secure server, and therefore does not disclose "automatically initiating an encrypted channel between the client and the secure server" as recited in claims 1 and 7. PO Appeal Br. 12–16. Patent Owner argues also Aventail Connect v3.01 does not disclose automatically initiating a direct channel that is encrypted between an application and a remote host, but rather the path is relayed through a server (SOCKS server). *Id.* at 16–17. Patent Owner relies on similar arguments with respect to independent claim 13. *Id.* at 17.

3. *Cisco's Contentions*

Cisco contends the status of Aventail Connect v3.01 as publically accessible is confirmed at least by the Chester Declaration in combination with the copyright date on Aventail Connect v3.01. Cisco Resp't Br. 5–6.

Cisco contends Patent Owner has not established that the claims require encryption extending to the computer/remote host. Cisco Resp't Br. 8–9.

[20] *See* Cisco Resp't Br., Evidence App., 4 citing Apple Ex. E3 Declaration of James Chester filed July 25, 2011 ("Chester Declaration").

4. Analysis

We limit our discussion to claims 1 and 13–14, which is sufficient to resolve the issues associated with this rejection. *See* 37 C.F.R. § 41.67(c)(vii).

a) Status of Aventail Connect v3.01 as Prior Art

We are not persuaded by Patent Owner's contentions that Aventail Connect v3.01 does not qualify as a printed publication due to lack of public accessibility. Aventail Connect v3.01 includes disclosures that it is a publically distributed document by including a 1996–1999 copyright notice by Aventail Corporation, a website http://www.aventail.com, and the statement "[p]rinted in the United States of America." Aventail Connect v3.01, i. Aventail Connect v3.01 provides contact information for "Aventail Technical Support." *Id.* at 5. Aventail Connect v3.01 lists Aventail protected trademarks and copyrights, the Aventail mailing and email addresses, further evidencing that Aventail Connect v3.01 is the kind of document expected to be widely disseminated. *Id.* at i.

We determine the Chester Declaration provides sufficient evidence that Aventail Connect v3.01 was accessible to the public and thus constitutes a printed publication. In particular, Mr. Chester declared that as an employee of Internal Business Machines Corporation (IBM) from 1992–2002, he evaluated network security products from vendors, and that he received a number of Aventail products. Chester Decl. ¶¶ 5–6. Mr. Chester similarly "recall[ed] that Aventail announced its AEC v3.0 product in the fall of 1998, and began distributing this product no later than mid-January 1999." *Id.* at ¶ 15. Mr. Chester declared that the AECv3.0 product included version 3.01/2.51 of the Aventail Connect software, which he received "no later than July 1998." Chester Decl. ¶¶ 16–17, Ex. C. He also testified IBM "deployed VPN solutions based on this product to more than 20,000 IBM employees domestically by March 1998 and more that 65,000 IBM employees worldwide by July 1998." *Id.* ¶ 19.

Even if corroboration is required to show public availability, "[c]orroboration does not require that every detail of the testimony be independently and conclusively supported by explicit disclosures in the pre-critical date documents or physical exhibits." *Ohio Willow Wood Co. v. Alps S., LLC*, 735 F.3d 1333, 1348 (Fed. Cir. 2013). *Willow Wood* stated a "rule of reason" test in which "the totality of the evidence . . . including circumstantial evidence" is assessed "in order to ascertain whether the testimonial assertions are credible." *Id.* "A given reference is 'publicly accessible' upon a satisfactory showing that such document has been disseminated or otherwise made available to the extent that persons interested and ordinarily skilled in the subject matter or art exercising reasonable diligence, can locate it." *SRI Int'l, Inc. v. Internet Sec. Sys., Inc.*, 511 F.3d 1186, 1194 (Fed. Cir. 2008) (quoting *Bruckelmyer v. Ground Heaters, Inc.*, 445 F.3d 1374, 1378 (Fed. Cir. 2006)).

The evidence as outlined above supports a finding that persons interested and ordinarily skilled in the subject matter of Aventail Connect v3.01 could have located them. The evidence shows that Aventail Corp. announced release of the products and they were disseminated with the manuals. Mr. Chester declared generally that "the Aventail products were distributed with installation discs and printed manuals" and of the specific availability of Aventail Connect v3.01. Chester Decl. ¶¶ 12, 15–17. Therefore, the evidence as a whole supports the Examiner's finding that

Aventail Connect v3.01was publicly accessible. Accordingly, we agree with the Examiner and Cisco that Aventail Connect v3.01 qualifies as a prior art printed publication under 35 U.S.C. § 102(b).

b) Claims 1 and 7

Regarding claims 1 and 7, we agree with Patent Owner that Aventail Connect v3.01 does not disclose "automatically initiating an encrypted channel between the client and the secure server" as recited in claims 1 and 7. Similar to the discussion above with respect to Kiuchi, encryption and decryption occurs at Aventail Connect (Aventail Connect v3.01, 1, 12), which corresponds to the DNS proxy module recited in claims 1 and 7. As such, Aventail Connect v3.01 does not disclose initiating an encrypted channel "between the client and the secure server" as recited in claims 1 and 7. Accordingly, we reverse the Examiner's decision to reject claims 1, 2, 5, 7, 8, and 11 as anticipated by Aventail Connect v3.01.

c) Claim 13

Regarding claim 13, as discussed above, claim 13 does not require an encrypted channel, but rather only requires the channel to be "secure." Aventail Connect v3.01 discloses that Aventail Connect is a "secure proxy client." Aventail Connect v3.01, 1. Accordingly, even though decryption occurs at Aventail Connect, the channel is still secure as required in claim 13. *See* RAN 11.

As to Patent Owner's argument that Aventail Connect v3.01 does not disclose a "direct" channel that is encrypted between an application and a remote host, we are not persuaded. That is, Patent Owner acknowledges the '151 Patent Specification "discloses that the communication traverses a network (or networks) through which it is simply passed or routed via various network devices such as Internet Service Providers, firewalls, and routers" and that this constitutes "'direct' communication." PO Appeal Br. 16, citing '151 Patent Figs. 2, 24, 28, 29, 33. Patent Owner's basis for contending Aventail Connect v3.01 does not disclose a "direct" channel is that in Aventail Connect v3.01, the encrypted communications channel passes through the SOCKS server, "which may create a new connection to the remote host." *Id.* at 16–17. Patent Owner alleges that "[t]his operation is different from a regular firewall or an edge router, where the traffic is destined for the target device and not for the firewall or the edge router." *Id.* at 17, citing Aventail Connect v3.01 6, 7, 12.

We observe that the Federal Circuit held with respect to U.S. Patent 6,501,135 (the "'135 Patent"), which shares a common specification with the '151 Patent, that the term "VPN between the client computer and the target computer" requires a "direct communication between the client computer and target computer" as a result of prosecution-history disclaimer. *VirnetX Inc. v. Mangrove Partners Master Fund Ltd.*, 778 F App'x at 909–910. However, the Federal Circuit did not indicate that a "direct" channel was required in the '151 Patent. *Id.* at 911 (holding "the Board erred in construing claims 1, 3–4, 7–8, 10 and 12 of the '135 Patent"). We have also not been directed to a specific definition of "direct" in the '151 Patent.

Even if the claims of the '151 Patent do require a "direct" channel, Patent Owner has not sufficiently explained how such a requirement in the claims necessarily distinguishes Aventail Connect v3.01. Although Patent Owner has referred to Internet Service Providers, firewalls, and routers as being examples of intervening devices allowed in a direct communication, given the claim language in claim 13, we do not find such examples necessarily distinguish the SOCKS server in Aventail Connect v3.01 even though the SOCKS server is disclosed as being "more than a standard security firewall." PO Appeal Br. 17; Aventail Connect v3.01 7.

The '151 Patent discloses the secure channel may be established preferably by utilizing a hopping scheme that is "preferably performed transparently to the user." '151 Patent, col. 38, ll. 62–66. The hopping scheme involves the use of Tunneled Agile Routing Protocol (TARP) packets and routers, which instead of indicating a final destination in the destination field of the IP header, points to the next-hop in a series of TARP router hops. *See* '151 Patent, col. 3, ll. 8–27; *see also* col. 31, ll. 25–42 (describing the use of edge routers and a plurality of Internet Service Providers). Aventail Connect v3.01 discloses Aventail Connect "is designed to run transparently on each workstation" and discloses the SOCKS server sends traffic to the Internet or an external network. Aventail Connect v3.01 7. We simply do not see how a requirement that the secure channel be "direct" distinguishes between the claim language in claim 13, which does not require a particular protocol or network layer for the direct connection and the disclosure in Aventail Connect v3.01.

Accordingly, we affirm the Examiner's decision to reject claim 13 as anticipated by Aventail Connect v3.01.

d) Claim 14

Regarding claim 14, the Examiner found Aventail Connect v3.01 discloses sending a proxy request to a SOCKS server, which depending on the security policy for that request, would correspond to a request for an encrypted channel between the secure server and a client. RAN 13–14, citing Aventail Connect v3.01 12.

Patent Owner contends Aventail Connect v3.01 fails to disclose "sending a request to the secure server to establish a secure channel between the secure server and the client" because the Aventail Connect software sends a proxy request to the SOCKS server, where the encryption module may not be enabled and selected by the SOCKS server, such that the proxy request is not a request to establish a secure channel. PO Appeal Br. 18–19.

Cisco contends the claims require only "sending a request" to establish an encrypted channel, and while some proxy requests in Aventail Connect v3.01 may disable encryption, such does not take away from the disclosure that certain proxy requests establish an encrypted channel. Cisco Resp't Br. 9.

As discussed above, the channel established in Aventail Connect v3.01 is "secure" as recited in claim 13. We agree with the Examiner and Cisco that Aventail Connect v3.01 discloses sending a request to a secure server as recited in claim 14. Aventail Connect v3.01, 12; *see id.* at 7. Patent Owner's contention that in some instances, the request may not be for a secure channel, does not change the disclosure in Aventail Connect v3.01 that other proxy requests are for secure channels.

Accordingly, we affirm the Examiner's decision to reject claim 14 as anticipated by Aventail Connect v3.01.

D. Anticipation – AutoSOCKS (Issue 2)

For similar reasons as discussed above for Aventail Connect v3.01, Patent Owner contends AutoSOCKS has not been shown to be publically accessible. PO Appeal Br. 5–7. We are not persuaded by Patent Owner's arguments for similar reasons as discussed above with respect to Aventail Connect v3.01, because the Chester Declaration provides similar statements with respect to AutoSOCKS as provided for Aventail Connect v3.01. *See* Chester Decl. ¶¶ 10–13, 18–19.

There is no dispute that the disclosure of AutoSOCKS is "substantially similar" to Aventail Connect v3.01. RAN 15–16; PO Appeal Br. 21; *see* Ans. 2–22.

Accordingly, we affirm the Examiner's rejection of claims 13 and 14 and reverse the Examiner's rejection of claims 1, 2, 5, 7, 8, and 11 for similar reasons as discussed above for Aventail Connect v3.01.

E. Obviousness – Aziz and Edwards (Issue 12)

1. The Examiner's Findings

The Examiner found Aziz discloses a DNS proxy module in the form of resolver 225. More specifically, the:

> examiner submits that Aziz teaches or suggests 'a domain name server (DNS) proxy module . . . because 'resolver 225 could follow the referral chain to the name server for the domain of inside host 140 or could pass the query on to local NS 250.' . . . Thus, it would have been obvious to those of ordinary skill in the art that the resolver of Aziz represents a DNS proxy module.

Ans. 94–95, citing Aziz, col. 6, l. 62 – col. 7, l. 7; col. 10, ll. 36–42. As the Examiner further explained, the operation of resolver 225 parallels the operation of the name server 120 in that the resolver 225 receives a query from application 215 and sends a query to the name server 120, and when the name server 120 sends a response back to the resolver 225, the resolver

225 checks for "an SX record"[21] in the response. ACP 68, citing Aziz, col. 9, ll. 54–56, col. 10, ll. 4–5, 36–39, 42–48, Figs. 3, 4A.

The Examiner found Edwards generally teaches technologies for securing HTTP web servers and related applications to prevent unauthorized access to data. Ans. 96. The Examiner found Edwards discloses a DNS proxy module (an object gateway), and the object gateway intercepts a name request sent by a client using a naming interceptor. *Id.* at 99–100. The Examiner found that Edwards discloses the object gateway includes both the proxy and the naming interceptor and determined it would have been obvious to modify the name server software of Aziz to additionally intercept name service requests, as taught by Edwards. *Id.* at 101.

The Examiner found Aziz discloses determining whether a DNS request corresponds to a secure server by checking whether the record is an associated "secure exchanger" or "SX" record. *Id.* at 104. The Examiner found Edwards discloses determining whether an intercepted name request specifies an available target, where available targets have enabled authentication and authorization, and where an administrator can adjust the access control as required. *Id.* at 104–105, citing Edwards 933. The Examiner determined it would have been obvious to one of ordinary skill in the art that a target with authentication and authorization enabled corresponds to a secure server. *Id.* at 105.

The Examiner found Aziz discloses automatically initiating an encrypted channel between the client computer and the target computer by

[21] Aziz indicates "a new resource record type" is "herein called an SX record" that responds "to requests for information needed for secure communications with protected hosts in that domain." Aziz, col. 4, ll. 9–12.

creating a tunnel map entry, which is used to encrypt messages, and after creating a tunnel map entry the application can communicate securely with the inside host 140. *Id.* at 111. The Examiner found that Aziz's disclosure of keeping secure message information up-to-date without relying on human intervention as support that Aziz discloses initiating the virtual private network "automatically." *Id.* The Examiner found Edwards discloses a domain name server proxy module in its disclosed object gateway, which intercepts name service requests. *Id.* at 99–101, citing Edwards 932, 934, Figs. 4, 6.

The Examiner determined it would have been obvious to have combined the Aziz network structure with the additional techniques disclosed in Edwards because the combination utilizes known techniques as disclosed in Edwards to improve a similar system as disclosed in Aziz in the same way. *Id.* Specifically, the Examiner determined combining the transparent encryption of Aziz with the interception of name service requests as taught by Edwards "allow[s] the Aziz network to provide its transparent encryption services with little or no client configuration required[, which] would further improve the transparency and ease of deploying the Aziz architecture." *Id.* The Examiner determined also that combining Aziz's transparent encryption with Edward's name service requests is a combination of known methods that merely produces a predictable result, such as providing transparent packet encryption in response to intercepted service requests. *Id.* at 96.

2. Patent Owner's Contentions

Patent Owner contends that although the Examiner identifies the resolver 225, which is located in authorized client 210 disclosed in Aziz as the DNS proxy module, the rejection cites to outside NS 120, separate from authorized client 210, as performing recited features of the DNS proxy module recited in claim 1. PO Appeal Br. 50. Patent Owner contends that any proposed modification of Aziz to locate resolver 225 outside NS (name server) 120 and outside of client 210 would be improper, and would render Aziz unsatisfactory for its intended purpose. *Id.* at 50–51. Patent Owner contends Edwards does not disclose or suggest the object gateway disclosed therein performs all of the features of the DNS proxy module recited in claim 1. *Id.* at 51. Patent Owner contends neither the Office nor Cisco explains how it would have been obvious to have combined the object gateway disclosed in Edwards with outside NS 120 and resolver 225 disclosed in Aziz. *Id.* at 51–52. Patent Owner contends also that both Aziz and Edwards disclose receiving, but not intercepting DNS requests, and further that it would not have been obvious to have modified Aziz to intercept DNS requests. *Id.* at 52–54. Patent Owner argues that Aziz does not disclose or suggest determining whether the intercepted DNS request corresponds to a secure server, because checking for an SX record is not the same as determining whether a DNS request corresponds to a secure server. *Id.* at 54–56. Patent Owner contends Edwards does not suggest determining whether the DNS request corresponds to a secure server. *Id.* at 56. Patent Owner argues the combination of Aziz and Edwards fails to disclose or suggest automatically initiating an encrypted channel between the client and the secure server. *Id.* at 57. In particular, Patent Owner argues Aziz's disclosure of creating a tunnel map entry does not automatically initiate an encrypted channel, and Edwards does not make up for this deficiency. *Id.* at 57–59.

3. *Cisco's Contentions*

Cisco contends Patent Owner has misconstrued the Examiner's position and the Examiner found the Aziz's resolver 225 discloses all the recited features. Cisco Resp't Br. 22. As to a DNS module that intercepts DNS requests sent by a client, Cisco contends that even under Patent Owner's interpretation of "intercept," Edwards discloses the recited limitation. *Id.* at 22–23. Cisco contends the SX records disclosed in Aziz contain an identifier of a secure exchanger, and as a result, Aziz discloses determining whether the corresponding host supports secure communications. *Id.* at 23. Cisco argues that Aziz discloses encrypted messages are sent from the host computer to the client without human intervention, and as such, are automatically initiated. *Id.* at 23–24.

4. *Analysis*

We limit our discussion to claim 1, which is sufficient to resolve the issues associated with this rejection. *See* 37 C.F.R. § 41.67(c)(vii). We are not persuaded by Patent Owner's arguments for the reasons that follow.

a) DNS Proxy Module

Aziz discloses an application 215 running on authorized client 210 (client) makes a query (DNS request) for the address of an inside host 140, which is received by a resolver 225 (DNS proxy module), and can follow a referral chain to the name server for the domain of inside host 140. Aziz, col. 10, ll. 35–41, col. 8, ll. 19–25; Figs. 1, 2A. Aziz also discloses an inside host 140 may be in protected zone 180 (secure server). *Id.* at col. 10, ll. 28–30, Fig. 1. The resolver 225 receives a response to the query checks to see if there is an "SX record," an identifier indicating there is a "secure exchanger" associated with the host name (the DNS proxy module determines whether the intercepted DNS request corresponds to a secure server as recited in claim 1). Aziz, col. 6, ll. 27–29, col. 10, ll. 42–43; Figs. 2A, 4A. Aziz discloses "[a] secure exchanger is a machine that handles secure communications for itself or for another machine (e.g. performs encryption or decryption)." Aziz, col. 6, ll. 29–33. Aziz discloses an example of a secure exchanger is firewall 110. Aziz, col. 6, ll. 36–38. Aziz discloses resolver 225 creates a "tunnel map entry," which "provides all the information that crypto-processor 230 needs to encrypt messages to inside host 140" to allow for secure communications (when the intercepted DNS request corresponds to a secure server, automatically initiating an encrypted channel between the client and the secure server as recited in claim 1). Aziz, col. 11, ll. 55–62; *see also id.,* col. 12, ll. 50–56 (disclosing the query is encrypted).

Consistent with the above discussion of Aziz, the Examiner found the resolver 225 of Aziz is the DNS proxy module, and not the combination of the resolver 225 and the outside NS 120 as asserted by Patent Owner. ACP 68; RAN 42–43; Ans. 94–95. Thus, contrary to Patent Owner's contentions, the Examiner does not rely on the combination of the resolver and the outside NS 120 as the DNS proxy module. Patent Owner's arguments focus on the joint operation of the resolver 225 with outside NS 120 and why relocating the resolver 225 would not have been obvious, without explaining what particular operation of the DNS proxy server the resolver 225 fails to perform.

b) "Intercepts DNS Requests"

We are not persuaded by Patent Owner's argument that Aziz does not disclose intercepting DNS requests. PO Appeal Br. 53. We agree with

Cisco's contention, adopted by the Examiner, that Patent Owner has not provided a sufficient explanation as to why the broadest reasonable interpretation of "intercepting" does not include receiving requests as taught by Aziz. ACP 67–68. In this regard, Patent Owner argues Cisco's construction of "intercepting" as reading on receiving a request disclosed in Aziz is inconsistent with a related proceeding where the Board allegedly determined the term "intercepting a request" "would require 'receiving and acting on' a request, the request being 'intended for' receipt at destination other than the destination at which the request is intercepted." PO Appeal Br. 53–54, quoting *Apple Inc. v. VirnetX Inc.,* IPR2014-00237, Paper No. 15 at 12 (PTAB May 14, 2014) (Decision on Institution). We observe, however, that the interpretation of "intercepting a request" as set forth by the Board under the broadest reasonable construction standard was "receiving a request pertaining to a first entity at another entity." *Apple Inc. v. VirnetX Inc.*, IPR2014-00237, Paper No. 41 at 12 (PTAB May 11, 2015) (Final Written Decision). Although this Decision was appealed, the Federal Circuit did not decide the appeal related to IPR2014-00237. *VirnetX Inc. v. Apple Inc.*, 665 F. App'x 880, 881 (Fed. Cir. 2016) ("We affirm, resolving the subject appeals on the grounds discussed by the PTAB in *VirnetX II* [IPR2014-00238].") In addition, the portions of the Specification of the patent discussed in IPR2014-00237 (US 8,504,697 B2 "the '697 Patent") are the same as in the '151 Patent. *Compare* '697 Patent, col. 40, ll. 31–33, Fig. 26, *with* '151 Patent, col. 37, ll. 60–62, Fig. 26. Thus, we do not agree with Patent Owner that the construction proposed by Cisco is inconsistent with IPR2014-00237.

c) Steps (i) and (iii)

As pointed out by the Examiner, Aziz discloses the data field of the SX record contains “the identifier (e.g., name or address) of a ‘secure exchanger’ associated with the owner of the record,” where the “secure exchanger is a machine that handles secure communications for itself or for another machine (e.g., preforms encryption or decryption).” Aziz, col. 6, ll. 27–32, col. 10, ll. 42–52. Thus, in contrast to Patent Owner’s arguments, by checking if the request contains an SX record, resolver 225 determines whether the request corresponds to a secure server. Indeed, the ’151 Patent discloses that determining whether a secure site has been requested is through “domain name extension, or by reference to an internal table of such sites.” ’151 Patent, col. 37, ll. 62–66.

We are not persuaded by Patent Owner’s argument it would not have been obvious to have modified Aziz to intercept name service requests, because there is an inadequate explanation as to how Edwards’s interception techniques would provide transparent encryption services with little or no client configuration, where Aziz already achieves this goal. PO Appeal Br. 53, citing Aziz col. 3, ll. 3–12; Keromytis Decl. ¶ 163.

We observe that the Examiner as well as Cisco, rely on the position that Aziz discloses receiving a DNS request, and Edwards discloses it is well known in the art for an intermediary module such as Aziz’s resolver 225 to intercept requests. *See* ACP 67, citing Cisco’s comments filed on August 17, 2012, 32–33. Thus, Edwards merely provides additional support that it is well known for DNS requests to be intercepted and directed to appropriate modules for resolution. *See* Edwards 934–936 (disclosing the “proxy is configured to use the naming interceptor as its naming service” and “the naming interceptor controls whether or not a service is available to any external clients."). Moreover, Edwards discloses that there is a choice as to the placement of the object gateway, which includes the proxy and interceptors, such as on a remote machine, and also that the object gateway can share processes with many other gateway objects. Edwards, 931, 936; Fig. 6.

Patent Owner's arguments consider each reference individually rather than what one of ordinary skill in the art would have understood from the collective teachings of the references.

Thus, for these reasons, we affirm the Examiner's rejection of claims 1, 7, and 13.

F. Obviousness – Claims 5 and 11 Aziz, Edwards, and Martin (Issue 13)

Status of Martin as Prior Art

Patent Owner contends Cisco provided no evidence that Martin was publically accessible more than one year prior to the alleged earliest effective date, because there is no indication what the date of February 21, 1998 on the first page of Martin means. PO Appeal Br. 9. Patent Owner contends the additional evidence submitted by Cisco showing public accessibility should not be considered because it was not submitted with the Request. *Id.*, citing 37 C.F.R. §§ 1.947–1.948.

Cisco contends that additional evidence of record established Martin was available to the public at least as early as February 21, 1998, and the citation to such evidence is proper. Cisco Resp't Br. 7–8, Exs. I–K, and citing the Manual of Patent Examining Procedure (MPEP) § 716.01(c).

The Examiner determined Martin was a publically accessible technical report from Boston University's Computer Science Department, posted at http://www.cs.bu.edu/techreports/pdf/1997-022-lanon.pdf. ACP 8. The Examiner's conclusion is also supported by the evidence cited in Cisco's Respondent Brief, showing that Martin was catalogued with a publication date of February 21, 1998. Cisco Resp't Br. Exs., H–J.

Patent Owner does not substantively challenge the Examiner's position that Martin is prior art based on the public availability of Martin from Boston University's Computer Science Department. We agree with Cisco that Patent Owner's contentions that 37 C.F.R. §§ 1.947 and 1.948 do not allow for additional evidence are unsupported. In this instance, Patent Owner challenged the position that Martin was prior art, and in response Cisco filed additional evidence supporting that position. *See* MPEP § 2166.05(II). We do not see how Cisco's evidence would not be allowed in this situation.[22]

[22] *See* Petition Decision January 1, 2016, dismissing PATENT OWNER'S PETITION TO REOPEN PROSECUTION filed November 23, 2015 and determining that the Examiner's rejections, including those involving Martin, were not altered by the Examiner's reliance on Cisco's exhibits filed with Cisco's written comments submitted on August 12, 2012 and the online post at http://www.cs.bu.edu/techreports/pdf/1997-022-lanon.pdf, and thus did not constitute new grounds of rejection. DECISION ON PETITION entered January 20, 2016, 4–6. Although Cisco's written comments, Patent Owner's petition, and the Petition Decision all refer to "exhibits M, N, and O," our review of the record indicates that the exhibits at issue are actually Exhibits H, I, and K as attached to Cisco's Respondent Brief, with Cisco's written comments incorrectly referring to those exhibits as "exhibits M, N, and O," an error which carried through Patent Owner's petition and the Petition Decision without being identified in those documents. *See* "COMMENTS BY THIRD PARTY REQUESTER PURSUANT TO 37 C.F.R. § 1.947" filed by Cisco on August 17, 2012, at v, 4–5.

Accordingly, we agree with the Examiner that Martin constitutes publically accessible prior art.

1. Claims 5 and 11

Substantively, Patent Owner contends that claims 5 and 11 depend from claims 1 and 7, respectively and Martin does not remedy the deficiencies of Aziz and Edwards with respect to the independent claims. PO Appeal Br. 60. Accordingly, we affirm the Examiner's rejection of claims 5 and 11 as obvious over Aziz, Edwards, and Martin for similar reasons as discussed above for claims 1 and 7.

G. Obviousness – Kiuchi and Edwards (Issue 14)

We limit our discussion to claims 1, and 13–16, which is sufficient to resolve the issues associated with this rejection. *See* 37 C.F.R. § 41.67(c)(vii).

Similar to the rejection of the claims over Aziz and Edwards discussed above, the Examiner cited Edwards for the concept of incorporating naming interceptors into Kiuchi's client-side and server-side proxies in rejecting claims 1–4, 6–10, and 12–16. Ans. 136, 140–141.

Patent Owner contends Kiuchi teaches away from the features of claim 1 as discussed above for the anticipation rejection. PO Appeal Br. 61–64. Patent Owner contends Edwards does not make up for such deficiencies in Kiuchi. *See id.* at 61–62.

Cisco contends Kiuchi discloses the limitations of claim 1 and Edwards shows that it was well-known to intercept requests sent to name services, and as a result, the Examiner's rejections should be affirmed. Cisco Resp't Br. 24–26.

As discussed above, because Kiuchi only discloses encrypted communications between the client-side and server-side proxies and not between the client and secure server, we reverse the Examiner's rejection of claims 1–4, 6–10, and 12 as obvious over Kiuchi and Edwards.

However, because, as discussed above, claim 13 only requires establishing a "secure" channel between the client and secure server, we affirm the Examiner's decision to reject claim 13 as obvious over Kiuchi and Edwards.

1. Claim 14

Patent Owner presents separate arguments for dependent claim 14. PO Appeal Br. 66–67. In this regard, Patent Owner relies on the position that Kiuchi fails to disclose determining whether the client is authorized to access the secure server, which we found unpersuasive above. *Id.* at 66. Patent Owner argues additionally that the Examiner and Cisco no longer rely on additional disclosures in Edwards for the recitations in claim 14. *Id.* at 66–67.

We agree with Patent Owner, that the Examiner does not rely on any additional rationale that Edwards discloses checking a client's authorization to access a secure server. RAN 39. Thus, we affirm the Examiner's rejection of claim 14 based on the above discussion that Kiuchi discloses determining whether the client is authorized to access the secure server.

2. Claims 15 and 16

Patent Owner contends Kiuchi fails to disclose returning a "host unknown" error message to a client as recited in claim 15 and as discussed above. PO Appeal Br. 67–68. Patent Owner argues also that Edwards does not make up for the deficiencies in Kiuchi. *Id.* at 68–69. In particular, Patent Owner contends the "object not found" error disclosed in Edwards, generated when a requested name "is not in the list of available targets" even when combined with Kiuchi, would not result in returning a "host unknown" error message to the client. *Id.* at 68; Ans. 153–154; 165.

The Examiner and Cisco contends that Patent Owner's arguments are identical to the arguments regarding Kiuchi alone. RAN 40; Cisco Resp't Br. 26.

For the reasons discussed above, we agree with Patent Owner that Kiuchi does not disclose returning a "host unknown" error to the client. Further, we agree with Patent Owner that the Examiner and Cisco fail to sufficiently explain how the combination of the "object not found" error in Edwards would have remedied the deficiency identified above in Kiuchi.

As a result, we reverse the Examiner's decision to reject claim 15 as obvious over Kiuchi and Edwards.

Because claim 16 depends from claim 15, we reverse the Examiner's rejection of claim 16 as well.

In sum, we affirm the Examiner's decision to reject claims 13 and 14 as obvious over Kiuchi and Edwards. However, we reverse the Examiner's decision to reject claims 1–4, 6–12, 15, and 16 as obvious over Kiuchi and Edwards.

H. Obviousness – Claims 5 and 11 over Kiuchi, Edwards, and Martin (Issue 15)

Claims 5 and 11 depend from claims 1 and 7, respectively, and recite the step of initiating encrypted channel between the client and the secure server comprises establishing an IP address hopping scheme between the client and the secure server. Martin is cited for disclosing an IP address hopping scheme that can co-exist with the system of Kiuchi in view of Edwards. Ans. 168–169. Martin fails to cure the deficiencies identified in Kiuchi and Edwards for claims 1 and 7. As a result, we reverse the Examiner's decision to reject claims 5 and 11 for similar reasons as discussed above with respect to claims 1 and 7.

I. Obviousness – Beser and Kent (Issue 4)

1. The Examiner's Findings

The Examiner found Beser discloses a process where an IP tunnel, and encrypted channel, is established between two network devices through a third trusted network device on a public network, corresponding to a DNS proxy module as recited in claim 1. Ans. 25, citing Beser, col. 10, ll. 37–41, col. 11, ll. 32–36. The Examiner found that Beser, in an IP telephony example, discloses a domain name may be used to determine if an encrypted channel needs to be established securely, and if so, the trusted third party network device will negotiate with the first and second network devices to establish an encrypted channel between the first and second network devices. *Id.,* citing Beser, Fig. 4, col. 11, ll. 9–44, col. 11. l. 58 – col. 12, l. 19. The Examiner found Beser discloses VPNs (virtual private networks) are routinely implemented for IP tunnels and IPsec is a known technique that can be used to encrypt communications within those types of encrypted channels. *Id.* at 25–26, citing Beser, col. 1, ll. 54–57, col. 2, ll. 7–13. The Examiner found Beser discloses authentication and encryption should be used to establish IP tunnels, but Beser does not expressly require all communications between the first and second network devices to be encrypted after the IP tunnel is established, disclosing instead that in certain types of applications, the high volume of data to be transferred would make encryption of all IP packets impractical. *Id.* at 26, citing Beser, col. 11, ll. 22–24, col. 1, l. 58 – col. 2, l. 15. The Examiner found that Beser discloses IP tunneling methods ordinarily will encrypt all traffic sent between the nodes of the tunnel, and that the IPsec protocol is to be used for these encrypted IP tunnels. *Id.*, citing Beser, col. 1, ll. 54–56. Thus, the Examiner found one of ordinary skill in the art would have recognized from Beser that all communications within IP tunnel, both to initiate the tunnel and following establishment of the IP tunnel, should be encrypted other than for certain high traffic applications, and that IPsec protocol should be used to handle the encryption of the traffic being sent through the IP tunnel. *Id.*, citing Beser, col. 1, l. 54 – col. 2, l. 15. The Examiner found Beser discloses the trusted-third-party network device is a domain name server that evaluates domain names, and will take additional actions to establish the IP tunnel based on the results of the evaluation. *Id.* at 26–28, citing Beser, col. 10, ll. 37–41, col. 11, ll. 32–36, 45–49. The Examiner found that if the destination associated with the domain does not require establishment of an IP tunnel negotiated by the trusted-third-party network device, the trusted-third-party network device, as a DNS server, will return the IP address associated with the non-secure domain. *Id.* at 27–28, citing RFC 1034 at 21.[23] As to the recitation in claim 1 of "automatically initiating an encrypted channel between the client and the secure server," the Examiner found Beser discloses the trusted-third-party network device automatically negotiates with first and second devices to establish an IP tunnel therebetween. *Id.* at

[23] P. Mockapetris, "Domain Names – Concepts and Facilities," RFC 1034, October 1987. Cisco Resp't Br., Ex. D7.

28–29, citing Beser Fig. 4, col. 11, ll. 9–25, col. 12, ll. 6–19, 28–37. The Examiner found Kent discloses IPsec protocol to establish VPNs by IP tunneling, where the IPsec protocol calls for automatic encryption of all IP traffic being sent between nodes of the VPN network. *Id.* at 29–30, citing Kent 8, 13, 29–34. The Examiner determined a person of ordinary skill in the art would have relied on Kent to modify the design of Beser to incorporate IPsec to encrypt all traffic being sent in an encrypted channel between a first and a second network device in the IP tunneling procedures disclosed in Beser, rather than encrypting only traffic used to establish the encrypted channel. *Id.* at 30.

2. Patent Owner's Position

Patent Owner contends Kent has not been shown to be a printed publication because although Kent discloses "November 1998" on the first page, there is no indication Kent was publically available in November 1998. PO Appeal Br. 7–8.

Substantively, Patent Owner argues one of ordinary skill in the art would not have combined Beser and Kent because Beser teaches away from the IPsec protocol disclosed in Kent. PO Appeal Br. 23–25. Patent Owner contends Beser does not disclose a DNS proxy module or a DNS proxy module that intercepts a DNS request by a client. *Id.* at 25–27. Patent Owner contends that the Examiner's position Beser discloses forwarding an intercepted DNS request to a DNS function when the intercepted DNS does not correspond to a secure server is not supported. *Id.* at 27–28. Patent Owner argues Beser does not disclose encryption between a client and a secure server, and Beser's disclosure of encryption relates to preliminary communications between the client and DNS proxy module, which occurs before any tunneling is established. *Id.* at 28–29.

3. *Cisco's Contentions*

Cisco contends Kent is self-dated as being available as of November 1998 and states that "[d]istribution of this document is unlimited." Cisco Resp't Br. 6. Cisco argues also Kent is an early Internet Draft by the Internet Engineering Task Force (IETF), and that the IETF's process for publishing Internet Drafts indicates that such are "'replicated on a number of Internet hosts' and 'readily available to a wide audience.'" *Id.*, quoting Ex. F at 8. In addition, Cisco contends that Dr. Keromytis, Patent Owner's expert, has repeatedly cited to Kent in his own peer-reviewed papers with a date of November 1998. *Id.* at 6–7, citing Ex. G.

Cisco argues Patent Owner is precluded from arguing Beser does not disclose a DNS proxy module under 37 C.F.R. § 42.73, because the Board considered the same argument in IPR2014-00237 and determined Beser discloses intercepting a request to look up an IP address of a network device based on a domain name. Cisco Resp't Br. 11–12, citing Ex. P, Paper 41 at 28. Even so, Cisco argues the Examiner correctly concluded Beser's VoIP (Voice over Internet Protocol) initiation request is a "DNS request." *Id.* at 12. Cisco argues Beser discloses "intercepting" a request as the Board found in IPR2014-00237. *Id.* citing Ex. P, Paper 41 at 28. Cisco argues that because Beser discloses the trusted-third-party server receives different types of requests that require different responses, it would have been obvious that Beser receives different types of requests that require different responses, where some requests require initiating an encrypted channel, and others do not require an encrypted channel. *Id.* at 12–13. Cisco argues

Patent Owner has not identified any substantive teaching of the "initiating" step that is not disclosed by Beser and Kent. *Id.* at 13.

4. Analysis

We limit our discussion to claims 1, 2, and 5, which is sufficient to resolve the issues associated with this rejection. *See* 37 C.F.R. § 41.67(c)(vii).

a) Prior Art Status of Kent

The Examiner agreed with Cisco's position that Kent was distributed and publically accessible before February 15, 2000. ACP 7.

The content of Kent is consistent with the publication process described by RFC 2026 including the date "November 1998" on the top right corner of the first page. Kent 1. The title itself, "Request for Comments," in addition to the evidence in RFC 2026 that each RFC document was made widely available "from a number of Internet hosts," constitutes sufficient evidence that Kent was intended for publication and would have been accessible to interested artisans seeking documents related to "Internet standards." Kent 1; Cisco Resp't Br., Ex. F, 6, 8. Accordingly, we find that Kent was publically accessible as of February 15, 2000.[24]

b) Teaching Away

We are not persuaded that Beser teaches away from incorporating IPsec protocol as disclosed in Kent. We agree with the Examiner's position that Beser's disclosure relates to certain limitations that with respect to the

[24] We observe that the Federal Circuit has previously determined that Kent is prior art and that VirnetX is collaterally estopped from arguing whether Kent is a printed publication. *VirnetX Inc. v. Apple, Inc.*, Appeal No. 2017-2490, 2017-2494, slip op. 2, n.1, 4 (Fed. Cir. Dec. 10, 2018).

use of encrypted packets with VoIP, including the feasibility of encrypting packets at the source and decrypting packets at a destination for certain data formats, and the amount of computing power required to encrypt or decrypt IP packets on the fly and does not amount to a teaching away. *See* Beser, col. 1, l. 58 – col. 2, l. 35. Indeed, Beser discloses the use of encryption for IP packets to ensure that the unique identifier cannot be read on the public network. Beser, col. 11, ll. 22–25, col. 20, ll. 11–14. As discussed above, Kent discloses IPsec protocol to establish VPNs by IP tunneling, where the IPsec protocol calls for automatic encryption of all IP traffic being sent between nodes of the VPN network. Kent 8, 13, 29–34; *see also id.* at 7 (disclosing IPsec allows the creation of an encrypted tunnel between each pair of hosts communicating across two security gateways). Accordingly, Beser contemplates the use of encryption in the methods disclosed in Kent, and as such, Patent Owner's argument that Beser teaches away from encryption is not persuasive.

c) Steps (i) and (ii)

We are also not persuaded by Patent Owner's argument that Beser fails to disclose that the trusted-third-party network may function as a DNS proxy module that performs the step of: "when the intercepted DNS request does not correspond to a secure server, forwarding the DNS request to a DNS function that returns an IP address of a nonsecure computer" as recited in claim 1. Beser expressly discloses the trusted-third-party network device is a domain name server. Beser, col. 11, ll. 32–36. Patent Owner points out that Beser discloses that the originating and terminating security of the connection is determined based on the private address of the requesting device 24 and the terminating device 26. Appeal Br. 22–23, citing Beser, Fig. 1, col. 2, ll. 36–39, col. 7, l. 62 – col. 8, l. 4, col. 10, ll. 2–6, col. 11, ll. 9–10, 26–32, col. 11, l. 59 – col. 12, l, 54. However, Patent Owner does not meaningfully address the Examiner's rationale discussed above that because Beser discloses domain servers, when the requesting device requests a connection to a non-secure server, such a request would be forwarded to a DNS function that would return an address of a nonsecure computer as evidenced by RFC 1034. Ans. 27. Accordingly, we are not persuaded by Patent Owner's contentions that the Examiner filled in missing limitations simply because they are not prohibited by Beser. PO Reb. Br. 7–8.

d) Claims 2, 8, and 14

Claim 2, which is representative, depends from claim 1, and recites, in pertinent part, "wherein step (iii) comprises the steps of: (a) determining whether the client is authorized to access the secure server." The Examiner found either Beser inherently discloses the limitation or Kent discloses IPsec involves an authentication step, rendering claim 2 obvious. Ans. 30–31; RAN 25, citing Kent 4, 47.[25]

Patent Owner contends that the cited portions of Beser fail to disclose requiring authenticating a client computer in conjunction with a tunneling association, and Beser discloses no reason for requiring the client be authorized or authenticated in accessing the third party network device of Beser or the secure server. PO Appeal Br. 31. Patent Owner acknowledges Beser requires authentication, but argues authentication is not the same as authorization. *Id.* Patent Owner contends the IPsec access control disclosed

[25] The cited portion of Kent attributed to page 47 appears to us to be on page 45.

in Kent does not make up for the deficiencies of Beser, because Kent is not concerned with whether a client is authorized to access a secure server. *Id.* at 32.

Cisco contends Kent discloses a variety of security services including "access control" such that one of ordinary skill in the art would have found controlling access of a client would have rendered obvious the determining whether the client is authorized as claimed. Cisco Resp't Br. 13–14, citing ACP 43; Kent 4.

We are not persuaded by Patent Owner's arguments. As discussed above, the combination of Beser and Kent discloses establishing an encrypted channel between a client and a secure server using the IPsec protocol disclosed in Kent. Beser discloses the IP packets may require authentication (Beser, col. 11, ll. 22–25), and Kent discloses access control, which is "prevention of use of a resource in an unauthorized manner." Kent 4, 45. While "authentication" and "access control" may encompass different concepts (*see* Kent 45), such does not undermine the Examiner's position that in applying the IPsec protocol of Kent to Beser, one of ordinary skill in the art would have included access control in order to determine whether the client is authorized to access the secure server as recited in claim 2. The Examiner's position is consistent with Beser's disclosure of authentication in order to ensure the security of the packets that are communicated between an originating device and a terminating device.

e) Claims 5 and 11

As discussed above, claim 5, which is representative, depends from claim 1 and recites, in pertinent part, an IP hopping scheme. The Examiner found Beser discloses Network Address Translator (NAT) protocol, which is an IP hopping scheme as recited in claim 5. Ans. 35, citing Beser, col. 2, ll. 18–27; ACP 47.

Patent Owner contends that the Examiner's position the NAT protocol disclosed in Beser satisfies the "IP hopping scheme" recited in claim 5 is conclusory and without any support. PO Appeal Br. 33. In addition, Patent Owner contends Beser teaches against the use of NAT, disclosing NAT only to show it is not to be used with VoIP applications, the technology with Beser is primarily concerned. *Id.* at 33–34.

Cisco contends the NAT protocol acts as an interface between a local network and a global network, which works by changing the originating IP address in packets before forwarding the packets to an outside server, and is an IP address hopping scheme within the meaning of claims 5 and 11. Cisco Resp't Br. 14, citing Ex. D1355 (RFC 1631). Cisco additionally contends Beser states only that NAT "may be" inappropriate for the transmission of multimedia or VoIP due to computer power limitations, and that nothing in Beser states that NAT should not be used or cannot be used in any tunneling associations, which is not a teaching away from NAT in all applications. *Id.*

We are not persuaded by Patent Owner's arguments. In particular, Patent Owner has not sufficiently explained why there is insufficient support for the Examiner's position that the NAT protocol disclosed in Beser is an IP hopping scheme as recited in the claims. Beser discloses "[a]nother method for tunneling is network address translation [(NAT)]." Beser 2, ll. 18–22. As pointed out by Cisco, the NAT protocol is understood by those skilled in the art as changing the originating IP address packets before forwarding packets to an outside server as disclosed in RFC 1631, which constitutes an

IP hopping scheme within the meaning of claims 5 and 11. Ex. D1355 (RFC 1631) 2–5.

In addition, we agree with the Examiner and Cisco that Beser does not necessarily teach away from the use of NAT protocol in all applications. Although it is true Beser discloses a number of limitations in using the NAT protocol, disclosing that use of the NAT protocol is "computationally expensive," prevents certain types of encryption from being used, is not compatible with a number of existing applications, and due to computer power limitations, "may be" inappropriate for the transmission of multimedia of VOIP packets (Beser, col. 2, ll. 18–35), such limitations would not prevent the use of the NAT protocol when these considerations were not at issue.

As a result, we affirm the Examiner's rejection of claims 1, 2, 5, 7, 8, 13, and 14 as obvious over Beser and Kent.

J. Objective Indicia of Non-Obviousness

"[T]he obviousness inquiry centers on whether 'the claimed invention as a whole' would have been obvious." *Rambus Inc. v. Rea,* 731 F.3d 1248, 1257–58 (Fed. Cir. 2013) (citation omitted). The question of obviousness is resolved on the basis of underlying factual determinations including (1) the scope and content of the prior art, (2) any differences between the claimed subject matter and the prior art, (3) the level of skill in the art, and (4) where in evidence, so-called secondary considerations. *Graham v. John Deere Co.,* 383 U.S. 1, 17–18 (1966). *See also KSR Int'l Co. v. Teleflex Inc.,* 550 U.S. 398, 406–07 (2007). Additionally, "[t]he obviousness assessment depends on what the prior art teaches and on what the non-prior-art evidence of 'secondary considerations' (or objective indicia) may indicate about whether the invention would have been obvious at the relevant time." *See Institut Pasteur & Universite Pierre et Marie Curie v. Focarino,* 738 F.3d 1337, 1344 (Fed. Cir. 2013) (citing *KSR,* 550 U.S. at 406–07).

Patent Owner contends that there is evidence of objective indicia including "Long-felt Need, Failure of Others, Skepticism, Commercial Success, and Praise and Acceptance by Others" that demonstrate non-obviousness. PO Appeal Br. 71 (emphasis omitted).

Cisco contends the Board has reviewed essentially the same evidence as presented in the instant reexamination in another reexamination, and found it to be insufficient to outweigh the evidence of obviousness. Cisco Resp't Br. 27, citing Ex. R, Decision on Appeal in Reexamination Control 95/001,792 (Appeal No. 2014-000591) of US Pat. 7,188,180, 18–23.

The Examiner determined the evidence presented by Patent Owner was entitled to little weight and thus did not outweigh the evidence of obviousness on the record. RAN 53–54; ACP 84.

We agree with the Examiner and Cisco that the evidence of objective indicia does not outweigh the evidence supporting a conclusion of obviousness discussed *infra*. Our reasoning for this determination follows.

1. Long-Felt Need

Patent Owner contends evidence of record demonstrates the computer-security and internet-security industries have had a long-felt need to easily and conveniently establish secure communications links, and the inventions claimed in the '151 Patent combine both the ease of use and the security aspects of a VPN, without sacrificing one or the other. Appeal Br. 71–72, citing Short Decl.[26] ¶¶ 3, 4–9, 11; Exs. B-1, B-2, B-4.

Cisco contends Patent Owner has not provided any analysis that any claim or claim term actually recites or incorporates the notion of easily and conveniently establishing VPN communications. Cisco Resp't Br. 28.

We are of the view that Patent Owner has not provided sufficient evidence of a persistent, long felt need or failure of others for establishing encrypted or secure communication links in an easy manner. The evidence provided by Patent Owner only establishes that secure communications was an area of interest. That is, although Patent Owner points to the Short Declaration and the Exhibit thereto "Living in your own private Idaho" for support that access to secure communications in an easy manner represented long-felt need (Short Decl. ¶¶ 8–9, citing Ex. B-4, 1 (VNET00219638)), such does not support Patent Owner's position because the claimed invention does not recite any particular ease associated therewith in initiating encrypted or secure communications. In addition, the assertions by Patent Owner that the Defense Research Projects Agency (DARPA) funded programs "were focused on the need to provide easy-to-enable secure communications" by significantly funding various research programs (Short Decl. ¶ 4) is not supported by the evidence cited. In particular, the Exhibits pointed to in the Short Declaration, while directed to secure communications, do not appear to discuss any particular aspect of easily enabling such communications. Short Decl. ¶¶ 4–5; Ex. B-1,

[26] Declaration of Dr. Robert Dunham Short III, dated July 19, 2012 ("Short Decl.").

VNET00219302, 319–321; Ex. B-2, VNET00219244, 284, 298–299, 593, 625; Ex. B-3, 1 (VNET00219634). Patent Owner's reference to relationships between In-Q-Tel and SAIC and investments in technology allegedly resulting in the '151 Patent, while evidence of the commitment to the technology, does provide any particular evidence that the '151 Patent claims provide a solution to a long-felt unfulfilled need.

2. *Failure of Others*

Patent Owner contends others attempted to create easy-to-enable secure communications, which attempts failed. PO Appeal Br. 72, citing Short Decl. ¶¶ 4, 5, 10, 11; Ex. B-3 "Dynamic Coalitions" program.

Cisco contends Patent Owner has failed to explain how any of program goals from the Dynamic Coalitions program, which relate to "provid[ing] 'continuous network operations even after a cyberattack' and supporting 'distributed rather than hierarchical coalition security policies,'" relate to the claims and how any alleged failure of these programs address a need for quick and easy secure communications. Cisco Resp't Br. 28, citing Ex. B-3, 1–2.

We agree with Cisco in this regard. In addition to the discussion above with respect to long-felt need, Patent Owner's evidence does not support Patent Owner's contentions. That is, the evidence simply describes the goals of the Dynamic Coalitions program, to ensured continued communications when the composition of a coalition changes or when an ad hoc area network is attacked. Ex B-3 VNET00219634. Patent Owner does not point out with any particularity where the evidence discusses easy-to-enable secure communications, such that, even if we were to agree that the claims of the ’151 Patent embody such a system, there is no indication of failure to achieve such a system from the Dynamic Coalitions program.

3. Skepticism

Patent Owner contends the technology of the ’151 Patent was met with skepticism by those skilled in the art. PO Appeal Br. 72–73, citing Short Decl. ¶¶ 13–15.

Cisco contends Patent Owner has not provided sufficient details to support Patent Owner’s arguments of skepticism. Cisco Resp’t Br. 28.

We are not persuaded by the statements made in the Short Declaration that the claims of the ’151 Patent were contrary to the accepted wisdom, a belief reinforced by the IT offices of many large companies and institutions. Short Decl. ¶¶ 13–14. The evidence cited by the Short Declaration does not discuss difficulties with VPN systems being not easily or conveniently enabled, but rather discusses the ability of VPNs to be used “without requiring companies to rip out existing gear.” PO Appeal. Br. Ex. B-5, 2.

Regarding the statements made in the Short Declaration regarding certain conversations between one Sami Saydjari, alleged to be a program manager for DARPA, and Edmund Munger, a co-inventor of the ’151 Patent (Short Decl. ¶ 15), we accord these statements little weight as such amount to unverified third-party conversations.

4. Commercial Success

Patent Owner contends the claims of the ’151 Patent have experienced commercial success in view of licensing agreements with multiple companies. PO Appeal Br. 73, citing Short Decl. ¶ 12; Ex A-8 1.

Cisco contends Patent Owner has presented no evidence that the broad portfolio licenses provide evidence that the claims under reexamination were a primary motivating factor for the licensing agreements. Cisco Resp't Br. 29.

We agree with Cisco. The alleged licensing agreements apparently include multiple patents, and there is insufficient evidence that such agreements were as a result of the particular features recited in the claims of the '151 Patent. As a result, Patent Owner has provided insufficient nexus between the claims of the '151 Patent and commercial success.

5. *Praise and Acceptance by Others*

Patent Owner argues those in the industry have praised the inventions either by stating praise or investing in the technology or licensing it. PO Appeal Br. 73–74, citing Short Decl. ¶¶ 7, 12, 16.

Cisco contends Patent Owner presents no documentary evidence that the '151 Patent claims were praised or accepted by the industry, only third-hand statements.

We agree with Cisco. The statements made in the Short Declaration regarding the alleged investments made by SAIC in the technology leading to the '151 Patent as well as the statement that SAIC spent one-third of its total patent portfolio efforts on a patent portfolio including the '151 Patent (Short Decl. ¶ 7) are uncorroborated and do not particularly address any particular praise for the features in the claims of the '151 Patent. In addition, portfolio licensing agreements (Short Decl. ¶¶ 12, 16) do not demonstrate praise for the particular features recited in the claims of the '151 Patent. With respect to the alleged study done by CSMG praising the inventors and alleged praise and significant interest expressed by Jim Rutt at Network Solutions (Short Decl. ¶ 16), such statements are uncorroborated and do not relate any praise or acceptance to the particular features of the claims of the '151 Patent.

6. *Weighing the Evidence of Objective Indicia*

After considering the evidence both in favor of non-obviousness and in favor of obviousness, we determine that in view of the deficiencies discussed above with respect to the evidence of non-obviousness, the evidence of obviousness carries more weight. That is, the combinations of prior art discussed above (the combinations of Aziz and Edwards; Kiuchi and Martin; Aziz, Edwards, and Martin; Kiuchi and Edwards; Kiuchi, Edwards, and Martin; and Beser and Kent) are stronger than the evidence tending to show claims of the '151 Patent would not have been obvious for the reasons previously discussed.

IV. CISCO'S APPEAL

A. *Anticipation – Wesinger (Issue 9)*

The Examiner withdrew the rejection of claims 1–4, 6–10, and 12–16 as anticipated by Wesinger, finding Patent Owner's argument persuasive that Wesinger's disclosure of determining what security rules to apply based on a host (domain) name is not the same as "determining whether the intercepted DNS request corresponds to a secure server." Ans. 92. The Examiner stated that a DNS entry for the "accessing machine" in Wesinger is not the same as a DNS request sent by the client as recited in the claims. *Id.* at 92–93.

Cisco contends the Examiner incorrectly withdrew the rejection of the claims because Wesinger discloses a firewall performs an allow or deny determination as part of the DNS request process. Cisco Appeal Br. 5–8, citing Wesinger Fig. 7. In particular, Cisco argues Wesinger discloses an "access rules database" that, as Cisco points out, "govern[s] access to and through the virtual host, i.e., which connections will be allowed and which connections will be denied." Cisco Appeal Br. 5, citing Wesinger col. 15, ll. 19–28 (emphasis omitted).

Patent Owner contends Wesinger's process occurs when the firewall receives a connection request and is not based on any DNS request. PO Resp't Br. 3, citing Wesinger col. 16, ll. 22–28, col. 9, ll. 16–24, and col. 15, ll. 5–19; Keromytis Decl. ¶¶ 112–113. Patent Owner contends Wesinger's firewall system makes no determination whether a connection request corresponds to a secure server, because every server in Wesinger is supported by a firewall and presumably secure, where Wesinger implements a security policy for each virtual host. *Id.* at 3–4, citing Keromytis Decl. ¶¶ 114–117. Patent Owner argues "at best, Wesinger analyzes whether the remote host (i.e., client) requesting a connection is secure . . . [b]ut [Wesinger] does not additionally disclose determining whether a connection request, much less a DNS request, corresponds to a secure server." *Id.* at 4, citing Keromytis Decl. ¶ 117 (emphases omitted).

We agree with the Examiner and Patent Owner that Wesinger fails to disclose analyzing the remote host (host requesting connection or client) in order to determine whether it is secure and that Wesinger fails to disclose determining whether a DNS request corresponds to a secure server. In particular, Wesinger discloses in addition to checking the remote host requesting the connection (client) to determine the level of access scrutiny, checking the virtual host (destination server) to determine whether the remote host (client) is allowed access via the allow and deny databases. Wesinger, col. 16, ll. 43–60. In other words, although Wesinger determines whether the client is allowed to access a secure server, such a determination does not depend on whether the requested server is secure or nonsecure, but rather whether the client has sufficient privileges to access the requested server. Thus, Wesinger does not disclose determining whether the virtual host itself corresponds to a secure server; rather, Wesinger only discloses evaluating the security privileges pertaining to the host requesting connection (i.e., the client). In this regard, Cisco's citation to Figure 7 of Wesinger to illustrate certain allow/deny "rules" (Cisco Appeal Br. 6–8) does not speak to whether the server itself is secure, but rather only determines under what particular conditions the remote host (client) may access the virtual host (secure server).

Accordingly, we affirm the Examiner's determination that Wesinger does not anticipate the claims.

B. Obviousness – Wesinger and Edwards (Issue 16)

Cisco relies on the same arguments for the combination of Wesinger and Edwards as discussed above for the anticipation rejection based on Wesinger (Issue 9). Cisco Appeal Br. 14–16. Accordingly, for similar reasons as discussed above, we affirm the Examiner's decision to withdraw the rejection of the claims as obvious over Wesinger and Edwards.

C. Obviousness – Claims 5 and 11 Wesinger or Wesinger in view of Edwards and Martin (Issues 10 and 17)

As discussed above, claims 5 and 11 depend from claims 1 and 7, respectively. As pointed out by Patent Owner, Martin is not relied upon to remedy any deficiencies of Wesinger or Wesinger and Edwards. PO Resp't Br. 6, 13. Accordingly, we affirm the Examiner's decision not to reject claims 5 and 11 for the reasons discussed above with respect to claims 1 and 7.

D. Anticipation – Blum (Issue 11)

The Examiner found that Blum discloses determining only whether a server is local or remote, and does not disclose determining whether a server is secure, and as such Blum further fails to disclose forwarding a DNS request to a DNS function that returns an IP address of a nonsecure computer when the DNS request does not correspond to a secure server. Ans. 93–94; ACP 62–64.

Cisco contends Blum discloses intercepting a DNS request, determining whether the DNS request corresponds to a remote server, and then determining if there is a protocol filter, such as a Secure Sockets Layer (SSL) protocol associated with the connection request. Cisco Appeal Br. 9–10, citing Blum, col. 1, ll. 46–48, col. 3, ll. 42–44, col. 5, ll. 23–27, col. 6, ll. 50–51, col. 9, ll. 19–23, 33–35.

In addition to arguing Blum only discloses determining whether a server is local or remote, Patent Owner contends Blum does not address the security of the remote servers at all, and that the SSL protocol is used in client programs not in communication processes with remote servers. PO Resp't Br. 6–8, citing Keromytis Decl. ¶¶ 150–151.

Ultimately, we agree with the Examiner that Blum does not disclose the specific arrangement recited in claim 1. That is, we agree with the Examiner that Blum fails to disclose forwarding a DNS request to a DNS function that returns an IP address of a nonsecure computer when the DNS request does not correspond to a secure server as recited in the claim.

Contrary to Patent Owner's arguments and the statements made in the Keromytis Declaration, Blum does not limit the application of protocol filters to local communications. In particular, Blum discloses "the transparent proxy application 355 checks to see if there is a protocol filter 520 associated with the native protocol of the connection request ***or with a port indicated in the connection request***." Blum, col. 9, ll. 33–35 (emphasis added); Fig. 5. Blum then discloses the protocol filter is applied and if the communication is allowed to be established, the connection is established "between the requesting client application 325 ***and the remote server identified in the communication request***." *Id.* at col. 9, ll. 35–46 (emphasis added). Blum discloses well-known protocols include Secure Sockets Layer (SSL) protocols. *Id.* at col. 1, ll. 46–50.

However, Blum does not provide any particular discussion regarding the use of SSL protocols in the context of the method described therein, nor does Blum particularly disclose forwarding a DNS request to a DNS function following a determination that a DNS request does not correspond to a secure server. In an anticipation rejection, "'the [prior art] reference must clearly and unequivocally disclose the claimed [invention] or direct those skilled in the art to the [invention] without *any* need for picking, choosing, and combining various disclosures not directly related to each other by the teachings of the cited reference.'" *Net MoneyIN v. Verisign, Inc.*, 545 F.3d 1359, 1371 (Fed. Cir. 2008) (quoting *In re Arkley*, 455 F.2d 586, 587 (CCPA 1972)) (alterations in original).

As a result, we affirm the Examiner's decision to withdraw the rejection of the claims as anticipated by Blum.

E. Obviousness – Claims 2–4, 6, 8–10, 12, 14–16 Aziz and Edwards (Issue 12)

1. Claims 2–4, 8–10, and 14–16

Claim 2 is representative of the limitations argued by Cisco, and recites, in pertinent part,

> [t]he data processing device of claim 1, wherein step (iii) comprises the steps of: (a) determining whether the client is authorized to access the secure server; and when the client is authorized to access the secure server, sending a request to the secure server to establish an encrypted channel between the secure server and client.

Cisco argues the Examiner improperly withdrew the rejection of claim 2, because the Examiner overlooked Aziz discloses that when the client computer needs to communicate via an encrypted channel with the inside host 140, but does not have the necessary record for inside the host 140, the resolver makes additional inquiries. Cisco Appeal Br. 12, citing Aziz, col. 11, l. 63 – col. 12, l. 33, Fig. 4C. Cisco argues also additional queries are sent to inside name server 130, located behind a firewall, which renders obvious "sending a request to the secure server to establish an encrypted channel between the secure server and the client." *Id.*, citing Aziz, col. 12, ll. 9–11.

Patent Owner contends Aziz does not disclose sending a request to the secure server to establish an encrypted channel and Cisco's position that inside name server 130 corresponds to the claimed secure server is unsupported. PO Resp't Br. 10. Patent Owner contends Edwards also does not disclose or suggest this feature. *Id.*

Although we do not agree with Patent Owner's position that inside name server 130 does not correspond to the secure server recited in claim 2, we agree with the Examiner and Patent Owner that Aziz fails to disclose sending a request to a secure server after determining whether the client is authorized to access the secure server. Aziz discloses only that "resolver 225 makes additional queries (not shown in Fig. 4C) as necessary." Aziz, col. 12, ll. 25–27. Moreover, Aziz discloses the authorized client "will be used herein to refer to a client that is configured to use the invention and whose communications will be allowed through by the firewall for the protected hosts with which the authorized client communicates." *Id.* at col. 3, ll. 62–67. Thus, we agree with Patent Owner that Cisco's position Aziz discloses sending a request to access a secure server is not sufficiently supported.

Because claims 3, 4, 9, 10, 15, and 16 depend either directly or indirectly from claims 2, 8, and 14, respectively, we affirm the Examiner's decision to withdraw the rejection of those claims for similar reasons as discussed for claims 2, 8, and 14.

2. *Claims 6 and 12*

Claims 6 and 12 recite "the secure server avoids sending a true IP address of the secure server to the client."

Cisco contends Edwards discloses service interceptors, which provides a way to avoid sending a true address of a requested service to the client by preventing services in the internal network accidently subverting security by handing object references to a client in the outside network. Cisco Appeal Br. 13, citing Edwards 932, 936. Cisco argues because Aziz discloses an embodiment where the network topology behind firewall 110 is hidden, it would have been obvious to improve Aziz's system by using the further topology-hiding technique of Edwards. *Id.*, citing Aziz, col. 11, ll.

64–65. Thus, Cisco contends rather than returning the true IP address of a requested server, the combination of Aziz and Edwards suggest returning a false IP address corresponding to a service interceptor. *Id.*

Patent Owner contends Cisco only considers part of the claims, the portion reciting not sending a true IP address, and the combination of Aziz and Edwards does not disclose "automatically initiating the encrypted channel between the client and the secure server." PO Resp't Br. 11–12.

The Examiner determined Aziz discloses the authorized client needs the information including the hosts address. ACP 72, citing Aziz, col. 3, ll. 38–44, col. 5, ll. 57–60.

We are persuaded by Cisco's arguments. In particular, as Cisco points out, Edwards discloses a name service receives a request from the CORBAweb plugin to resolve a name, it will return a reference to a service interceptor instead of the actual service, which is consistent with the disclosure in Aziz that the network topology behind the firewall 110 is hidden. Edwards 932, 936; Aziz, col. 11, ll. 64–65. Thus, in view of our discussion above that the combination of Aziz and Edwards renders obvious claim 1, we are of the opinion that the additional disclosure in Edwards that the naming service interceptor prevents services in the internal network accidently subverting security (Edwards 936), renders obvious avoiding sending a true IP address of the secure server to the client.

Accordingly, we reverse the Examiner's decision not to reject claims 6 and 12.

F. Anticipation – Claims 6 and 12 Kiuchi (Issue 7)

Claims 6 and 12 depend from claims 1 and 7, respectively. As discussed above, we reversed the Examiner's rejection of claims 1 and 7 as anticipated by Kiuchi. Accordingly, we affirm the Examiner's decision not to reject claims 6 and 12 for similar reasons.

V. CONCLUSION

In summary, the status of the Adopted Rejections is as follows:

Claim(s) Rejected	35 U.S.C. §	Reference(s)/Basis	Affirmed	Reversed
1, 2, 5, 7, 8, 11, 13, 14	102(b)	Aventail Connect v3.01	13, 14	1, 2, 5, 7, 8, 11
1, 2, 5, 7, 8, 11, 13, 14	102(b)	AutoSOCKS	13, 14	1, 2, 5, 7, 8, 11
1, 2, 5, 7, 8, 11, 13, 14	103(a)	Beser, Kent	1, 2, 5, 7, 8, 11, 13, 14	
1–4, 7–10, 13–16	102(b)	Kiuchi	13, 14	1–4, 7–10, 15, 16
5, 11	103(a)	Kiuchi, Martin		5, 11
1, 7, 13	103(a)	Aziz, Edwards	1, 7, 13	
5, 11	103(a)	Aziz, Edwards, Martin	5, 11	
1–4, 6–10, 12–16	103(a)	Kiuchi, Edwards	13, 14	1–4, 6–10, 12, 15, 16
5, 11	103(a)	Kiuchi, Edwards, Martin		5, 11
Overall Outcome Adopted Rejections			**1, 2, 5, 7, 8, 11, 13, 14**	**3, 4, 6, 9, 10, 12, 15, 16**

The status of the Non-Adopted Rejections is as follows:

Claim(s) not Rejected	35 U.S.C. §	Reference(s) /Basis	Affirmed	Reversed	New Ground Of Rejection
6, 12	102(b)	Kiuchi	6, 12		
1–4, 6–10, 12–16	102(e)	Wesinger	1–4, 6–10, 12–16		
5, 11	103(a)	Wesinger, Martin	5, 11		
1, 7, 13	102(e)	Blum	1, 7, 13		
2–4, 6, 8–10, 12, 14–16	103(a)	Aziz, Edwards	2–4, 8–10, 14–16	6, 12	6, 12
1–4, 6–10, 12–16	103(a)	Wesinger, Edwards	1–4, 6–10, 12–16		
5, 11	103(a)	Wesinger, Edwards, Martin	5, 11		
Overall Outcome Non-Adopted Rejections			**1–5, 7–11, 13–16**	**6, 12**	**6, 12**

NEW GROUND OF REJECTION

This decision contains new grounds of rejection pursuant to 37 C.F.R. § 41.77(b) which provides that "[a]ny decision which includes a new ground of rejection pursuant to this paragraph shall not be considered final for judicial review." Correspondingly, no portion of the decision is final for purposes of judicial review. A requester may also request rehearing under 37 C.F.R. § 41.79, if appropriate; however, the Board may elect to defer issuing any decision on such request for rehearing until such time that a final decision on appeal has been issued by the Board.

For further guidance on new grounds of rejection, *see* 37 C.F.R. § 41.77(b)–(g). The decision may become final after it has returned to the Board. 37 C.F.R. § 41.77(f).

37 C.F.R. § 41.77(b) also provides that the Patent Owner, WITHIN ONE MONTH FROM THE DATE OF THE DECISION, must exercise one of the following two options with respect to the new grounds of rejection to avoid termination of the appeal as to the rejected claims:

(1) *Reopen prosecution.* The owner may file a response requesting reopening of prosecution before the examiner. Such a response must be either an amendment of the claims so rejected or new evidence relating to the claims so rejected, or both.

(2) *Request rehearing*. The owner may request that the proceeding be reheard under § 41.79 by the Board upon the same record. . . .

Any request to reopen prosecution before the examiner under 37 C.F.R. § 41.77(b)(1) shall be limited in scope to the "claims so rejected." Accordingly, a request to reopen prosecution is limited to issues raised by the new ground(s) of rejection entered by the Board. A request to reopen prosecution that includes issues other than those raised by the new ground(s) is unlikely to be granted. Furthermore, should the patent owner seek to substitute claims, there is a presumption that only one substitute claim would be needed to replace a cancelled claim.

A requester may file comments in reply to a patent owner response. 37 C.F.R. § 41.77(c). Requester comments under 37 C.F.R. § 41.77(c) shall be limited in scope to the issues raised by the Board's opinion reflecting its decision to reject the claims and the patent owner's response under paragraph 37 C.F.R. § 41.77(b)(1). A newly proposed rejection is not permitted as a matter of right. A newly proposed rejection may be appropriate if it is presented to address an amendment and/or new evidence properly submitted by the patent owner, and is presented with a brief explanation as to why the newly proposed rejection is now necessary and why it could not have been presented earlier.

Compliance with the page limits pursuant to 37 C.F.R. § 1.943(b), for all patent owner responses and requester comments, is required.
The examiner, after the Board's entry of a patent owner response and requester comments, will issue a determination under 37 C.F.R. § 41.77(d) as to whether the Board's rejection is maintained or has been overcome.
The proceeding will then be returned to the Board together with any comments and reply submitted by the owner and/or requester under 37 C.F.R. § 41.77(e) for reconsideration and issuance of a new decision by the Board as provided by 37 C.F.R. § 41.77(f).

AFFIRMED-IN-PART; 37 C.F.R. § 41.77(b)

ELD

PATENT OWNER:

PAUL HASTINGS LLP
875 15th Street, NW
Washington, DC 20005

THIRD PARTY REQUESTER:

SIDLEY AUSTIN LLP
2021 McKinney Avenue, Suite 2000
Dallas, TX 75201