Trials@uspto.gov
571-272-7822

Paper 41
Date: May 11, 2015

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

APPLE INC.,
Petitioner,

v.

VIRNETX INC.,
Patent Owner.

Case IPR2014-00237
Patent 8,504,697 B2

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

EASTHOM, *Administrative Patent Judge*.

# FINAL WRITTEN DECISION
*35 U.S.C. § 318(a) and 37 C.F.R. § 42.73*

## I. BACKGROUND

Petitioner, Apple Inc., filed a Petition (Paper 1,“Pet.”) seeking an *inter partes* review of claims 1–11, 14–25, and 28–30 of U.S. Patent No. 8,504,697 B2 (Ex. 1001, “the ’697 patent”) pursuant to 35 U.S.C. §§ 311–319. After VirnetX, Patent Owner, filed a Preliminary Response (Paper 12), we instituted an *inter partes* review of claims 1–11, 14–25, and 28–30 (Paper 15, “Institution Decision” or “Inst. Dec.”).

Subsequent to institution, Patent Owner filed a Patent Owner Response (Paper 30) (“PO Resp.”), and Petitioner filed a Reply (Paper 33) (“Pet. Reply”) thereto. An Oral Hearing was conducted on February 9, 2015, and then transcribed. *See* Paper 40.

The Board has jurisdiction under 35 U.S.C. § 6(c). This Final Written Decision issues pursuant to 35 U.S.C. § 318(a) and 37 C.F.R. § 42.73.

For the reasons that follow, we determine that Petitioner has shown by a preponderance of the evidence that claims 1–11, 14–25, and 28–30 of the ’697 patent are unpatentable.

### *A. The ’697 Patent (Ex. 1001)*

The ’697 patent describes secure methods for communicating over the internet. Ex. 1001, 10:7–8. To provide a secure network, the ’697 patent system employs proxy domain name servers (DNS). The ’697 patent describes conventional DNSs as follows:

> Conventional Domain Name Servers (DNSs) provide a look-up function that returns the IP [Internet Protocol] address of a requested computer or host. For example, when a computer user types in the web name “Yahoo.com,” the user’s web browser transmits a request to a DNS, which converts the name into a four-part IP address that is returned to the user’s browser

> and then used by the browser to contact the destination web site.

Ex. 1001, 39:32–38.

To set up the secure network or Virtual Private Network ("VPN"), a proxy DNS determines whether the user has requested access to a secure site and may determine whether the user has sufficient security privileges to access that site. Ex. 1001, 40:31–37, 41:6–64. To make both determinations, the proxy DNS provides DNS look-up functions for secure hosts. *Id*. at 40:31–37. The proxy DNS may use a domain name extension or an internal table of sites, or may request security information about the user. *Id*. at 40:31–37, 41:14–27. If the user has requested access and has sufficient security privileges, the proxy DNS requests a gatekeeper to set up a secure communication link by passing a "resolved" address or "hopblocks" for the user and target addresses. *See* Ex. 1001, 40:37–65, Fig. 27. Any of various packet fields can be "hopped," for example, "IP source/destination addresses" or "a field in the header." Ex. 1001, 41:38–39. If the user lacks sufficient security privileges, the system returns a "HOST UNKNOWN" error message. Ex. 1001, Fig. 27.

In essence, the system provides security through anonymity of IP addresses—the proxy server does not send back the true IP address of the target computer. *See* Ex. 1001, 40:1–20. For example, the proxy server may receive the client's DNS request, which forwards it to a gatekeeper, which returns a "resolved" destination address to the proxy based on a "resolved" name, which then forwards the "resolved address" back to the client "in a secure administrative VPN." *See* Ex. 1001, 41:49–56.

### *B. Illustrative Claim*

Claim 1 of the ’697 patent is reproduced below:

> 1. A method of connecting a first network device and a second network device, the method comprising:
>
> intercepting, from the first network device, a request to look up an internet protocol (IP) address of the second network device based on a domain name associated with the second network device;
>
> determining, in response to the request, whether the second network device is available for a secure communications service; and
>
> initiating a secure communication link between the first network device and the second network device based on a determination that the second network device is available for the secure communications service;
>
> wherein the secure communications service uses the secure communication link to communicate at least one of video data and audio data between the first network device and the second network device.

### *C. Prior Art*

| | | | |
|---|---|---|---|
| Beser | US 6,496,867 B1 | Dec. 17, 2002 | (Ex. 1009) |

S. Kent and R. Atkinson, *Security Architecture for the Internet Protocol*, Request for Comments: 2401, BBN Corp., November 1998 (“RFC 2401”) (Ex. 1010).

### *D. Instituted Grounds of Unpatentability*

We instituted an *inter partes* review on the following grounds and claims.

| **References** | **Basis** | **Claims Challenged** |
|---|---|---|
| Beser | § 102 | 1–11, 14–25, and 28–30 |
| Beser and RFC 2401 | § 103 | 1–11, 14–25, and 28–30 |

### *E. Claim Interpretation*

In an *inter partes* review, the Board construes claim terms in an unexpired patent under their broadest reasonable construction in light of the specification of the patent in which they appear. *In re Cuozzo Speed Techs., LLC*, 778 F.3d 1271, 1281 (Fed. Cir. 2015); 37 C.F.R. § 42.100(b); *Office Patent Trial Practice Guide*, 77 Fed. Reg. 48,756, 48,766 (Aug. 14, 2012). With the exception of slight modifications to some of the terms discussed below, we adopt and incorporate the claim constructions set forth in the Institution Decision. *See* Inst. Dec. 7–15.

#### *i. Secure Communication Link*

In the Institution Decision, we determined, under the broadest reasonable construction standard, that a "secure communication link," as recited in claims 1 and 16, is "a transmission path that restricts access to data, addresses, or other information on the path, generally using obfuscation methods to hide information on the path, including, but not limited to, one or more of authentication, encryption, or address hopping." Inst. Dec. 10. Patent Owner argues that the term "secure communication link" must include encryption. *See, e.g.*, PO Resp. 10–19.

Notwithstanding Patent Owner's arguments that security requires encryption, the '697 patent Specification states that "[a] *tremendous variety* of methods have been proposed and implemented to provide security and anonymity for communications over the Internet." Ex. 1001, 1:35–37 (emphasis added). The '697 patent Specification also describes data security and anonymity as counterpart safeguards against eavesdropping that may occur while two computer terminals communicate over the Internet. *See id.* at 1:38–54. Security, in one context, may refer to protection of the data itself, to preserve the secrecy of its contents, while anonymity refers to preventing an eavesdropper from discovering the identity of a participating terminal. *See id*. at 1:40–56. Further according to the ’697 patent Specification, the concept of security generally includes “two security issues,” address (anonymity) and data security, with “a desire[] for the communications to be secure, that is, immune to eavesdropping.” *Id*. at 1:42–43, 54–56.

This understanding is also consistent with the Federal Circuit’s construction of this term in an appeal of a related case. Shortly after Patent Owner filed its Response, the Federal Circuit determined that the term does not require encryption in a related case involving VirnetX, Inc.’s patent claims of similar scope, based on similar arguments by VirnetX. *See VirnetX, Inc. v. Cisco Systems, Inc.*, 767 F.3d 1308, 1317–19 (Fed. Cir. 2014).[1] Relying on passages that also appear in the ’697 patent Specification in the same context, the court determined that a “secure communication link” (as used in the ’504 and ’211 ancestor patents, *see* note 1), is “a direct communication link that provides data security *and anonymity*.” *See Cisco*, 767 F.3d at 1319. In *Cisco*, the court found that “[b]oth the claims and the specification of the ’151 patent make clear that encryption is a narrower, more specific requirement than security.” *Id.* at 1323 (citing a passage in the ’151 patent at 1:49–50 that also appears in the

[1] The ’697 patent is a continuation of U.S. Patent No. 7,921,211 (“’211 patent”), which is a continuation of U.S. Patent No. 7,418,504 (“’504 patent”), which is a continuation-in-part of U.S. Patent No. 6,502,135 (“’135 patent”), three of the four patents at issue in *Cisco. See* 767 F.3d at 1313. Also at issue in *Cisco*, is U.S. Patent No. 7,490,151 (“’151 patent”), a division of the ’135 patent.

’697 patent at 1:57–60: “Data security is *usually* tackled using some form of data encryption.”

Central to its claim construction, the court found, based on concessions or arguments by the parties, that the ordinary meaning of the term “security,” on that record, did not apply. *See id*. at 1317 (“There is no dispute that the word ‘secure’ does not have a plain and ordinary meaning in this context, and so must be defined by reference to the specification.”).

In not requiring encryption, *Cisco* additionally found on that record that security includes “physical security.” *See Cisco*, 767 F.3d at 1322 (“VirnetX provided substantial evidence for the jury to conclude that paths beyond the VPN server may be rendered secure and anonymous by means of ‘physical security’ present in the private corporate networks connected to by VPN On Demand.”). Underlying that finding, *Cisco* noted that “VirnetX’s expert testified that one of ordinary skill would understand that the path . . . within the private network[] would be secure and anonymous owing to the protection  provided by the private network.” *Id*. at 1321.

Of course, anonymity provides some security, as explained in *Cisco*. The claim construction in the Institution Decision also includes anonymity as a form of security, but not as a necessary requirement. Instead, our construction also includes address hopping, restricting access to addresses, and generally, obfuscation methods. This is not inconsistent with the Federal Circuit’s construction. In contrast to the broadest reasonable interpretation standard employed by the Board for an unexpired patent, the Federal Circuit employs a narrower claim construction standard when reviewing the construction of a claim applied by the district court. *See In re Rambus, Inc*., 694 F.3d 42, 46 (Fed. Cir. 2012) (contrasting the Board’s review of expired patents, which is "similar to that of a district court's review," with the Board's review of unexpired patents, which involves the broadest reasonable interpretation standard); *Cuozzo*, 778 F.3d at 1281 (broadest reasonable interpretation standard applies to AIA proceedings). In any event, anonymity is not a central issue, because the Beser reference discloses it and the parties do not raise it. *See* Ex. 1009, Abstract, 12:16–19. Accordingly, in this case, it is not necessary to determine if a secure communication link, under the broadest reasonable construction standard, necessarily includes anonymity (or a direct link).[2]

Based on the foregoing discussion, the term may include encryption, anonymity, and physical security. Therefore, we slightly modify our construction of the term as set forth in our Institution Decision. The broadest reasonable construction of a "secure communication link" is "a transmission path that restricts access to data, addresses, or other information on the path, generally using obfuscation methods to hide information on the path, including, but not limited to, one or more of anonymity, authentication, or encryption."

### *ii) Virtual Private Network (VPN) Communication Link*

Claims 3 and 17 respectively depend from claims 1 and 16 and further limit those claims by reciting "wherein the secure communication link is a virtual private network [(VPN)] communication link." In the Institution Decision, we construed a VPN to include "a secure communication link that

[2] Notwithstanding *Cisco's* "direct" component of a "secure communication link," Patent Owner argues that it "do[es] not appear relevant to the parties' disputes." PO Resp. 14 n.1. Similarly, the parties do not propose that anonymity is a requirement in their latest papers. *See* Pet. Reply 4 (suggesting anonymity is not relevant); PO Resp. 19 (same).

includes a portion of a public network." Inst. Dec. 12. The construction was based largely on the finding that the parties did not provide a clear distinction between a secure and VPN communications link, evidence of ordinary meaning provided by Petitioner (*see*, *e.g.*, Ex. 1073, 2–5), and the finding that the '697 patent Specification "explains [that] a 'secure communication link' is 'a virtual private communication link over the computer network.'" Inst. Dec. 11 (quoting Ex. 1001, 6:63–65, also relying on Ex. 1073, Ex. 1024). By way of background, one commentator generally describes a VPN as a collection of devices that can communicate (i.e., a network) over a public network with a desired level of privacy obtained by controlling access and security of data (i.e., virtually private). *See* Ex. 1073, 2–6.

Patent Owner argues that "the term VPN is not in dispute here and is not a claim term," so "the Board need not construe it." PO Resp. 19. Patent Owner characterizes the recited term, "a [VPN] communication link," as "related [to] but different" from, a VPN. *Id*. Referring to a VPN communication link, Patent Owner urges that "the Board need not construe this term . . . and [its construction] does not appear to impact any of the issues in this case." PO Resp. 21.

Nevertheless, according to Patent Owner, Beser does not disclose a VPN. PO Resp. 54. This stance mandates a construction of the term on this record. Patent Owner maintains that a "VPN communication link" is "a communication path between computers in a virtual private network." PO Resp. 21. Regarding the construction of a "VPN" as "a secure communication link with the additional requirement that the link includes a portion of the public network" (Inst. Dec. 11–12), Patent Owner "does not dispute the 'secure communication link' aspect of the Decision's construction," except to the extent that it lacks the encryption and direct link requirements discussed above in the construction of a secure communication link. *See* PO Resp. 20 & n.4. As discussed above (note 2), Patent Owner maintains that the "direct" requirement is not at issue in this proceeding, and in line with *Cisco*, we determined that encryption is not a necessary requirement of a secure communication link.

The parties do not set forth explicitly what a VPN constitutes. In *Cisco*, the court indicates, as construed in the ancestor '504 patent (*supra* note 1), that a VPN provides anonymity: "Moreover, in several instances the specification appears to use the terms 'secure communication link' and 'VPN' interchangeably, suggesting that the inventors intended the disputed term to encompass the anonymity provided by a VPN." 767 F.3d at 1318.

Although a VPN as construed by *Cisco* includes anonymity, neither party argues for that requirement in their latest papers. And as noted, Patent Owner maintains that the construction of VPN "does not appear to impact any of the issues in this case." PO Resp. 21. Claims 3 and 17 depend from claims 1 and 16, suggesting pursuant to claim differentiation that a VPN communication link is narrower than a secure communication link. Therefore, for purposes of this proceeding, the broadest reasonable construction of a "virtual private network communication link" is "a secure communication link that includes a portion of a public network," as set forth in the Institution Decision. Inst. Dec. 11–12.

### *iii) Intercepting A Request*

In the Institution Decision, we construed "intercepting a request," as recited in claim 1, as "receiving a request pertaining to a first entity at another entity." Inst. Dec. 13. Claim 16 recites a similar term (i.e., "intercept . . . a request"). Patent Owner "disagrees with this construction" (PO Resp. 23), but "believes that no construction is necessary" (*id*. at 26), because "it does not appear that the construction of 'intercepting' will bear on the outcome of the issues in this *inter partes* review" (*id*. at 23). Nevertheless, Patent Owner urges that if we construe the term, we adopt Patent Owner's construction: "receiving a request to look up an internet protocol address and, apart from resolving it into an address, preforming an evaluation on it related to establishing a secure communication link." *Id*. at 23.

To support its proposed alternative construction, Patent Owner maintains that "[t]he *Decision's construction addresses* a common aspect of *a conventional DNS and the disclosed embodiments*, namely that a request to look up an address of one entity may be received at another entity. However, the construction overlooks the aspects distinguishing the 'intercepting' phrase from conventional DNS." *Id*. at 26 (emphases added) (citation omitted). According to Patent Owner, a disclosed modified DNS "appl[ies] an additional layer of functionality to a request to look up a network address beyond merely resolving it and returning the network address." *Id*. at 25. As an "example, the DNS proxy 2610 may intercept the request and 'determin[e] whether access to a secure site has been requested.'" *Id*. (quoting Ex. 1001, 40:31–33).

Patent Owner's arguments and the record show that Patent Owner's proposed construction adds unnecessary functionality to "intercepting a request." According to Patent Owner's arguments, and as Petitioner points out, another recited phrase in claim 1 (and a similar phrase in claim 16), captures the functionality, in particular, the "determining . . . whether" phrase of claim 1, which is recited after the intercepting phrase. *See* Pet. Reply 4–5 ("Patent Owner's illogical construction . . . is actually part of the next step of the claims."); *see also* PO Resp. 26 ("The independent claims also support this [functionality], for example, by reciting that a determination is made whether the second network is available for a secure communications service . . . ."). In other words, Patent Owner argues that the "determining . . . whether" clause covers functionality that it also urges is implicit in the intercepting phrase. *See* PO Resp. 26, 29–30. Based on the foregoing discussion, the record shows that the additional functionality urged by Patent Owner should not be imported into the intercepting phrase. Accordingly, as set forth in the Institution Decision, the broadest reasonable construction of the term "intercepting a request" is "receiving a request pertaining to a first entity at another entity."

#### *iv) Determining, In Response To The Request, Whether The Second Network Device Is Available For Communication*

In the Institution Decision, we construed the above phrase, as recited in claim 1 (and similarly in claim 16), to "include[] determining,  one or more of 1) whether the device is listed with a public internet address, and if so, allocating a private address for the second network device, or 2) some indication of the relative permission level or security privileges of the requester." Inst. Dec. 15. Petitioner implicitly agrees with this construction. *See* Pet. Reply 5–6.

Patent Owner asserts that this construction "imports unnecessary language into the claims." PO Resp. 27. Patent Owner maintains that there is no reason to require "an allocation of a private address," because that step does not aid in determining availability. *See id*. at 27–28. Patent Owner also argues that the construction eliminates the requirement of the determination being made "in response to the request." *See id.* at 30. Patent Owner also maintains that "[t]he claim language is plain on its face . . . . [and] does not require construction." *See id.*

Patent Owner's arguments show persuasively that the preliminary construction was too narrow. The term "available" has an ordinary meaning of "accessible for use; at hand; usable." Ex. 3004.[3] Based on the arguments presented, the ordinary meaning of the term "available," and the '697 patent Specification, we modify our previous claim construction as follows: The term "determining, in response to the request, whether the second network device is available for secure communication," means "determining, in response to a request, whether the second network device is accessible for use, at hand, or usable for a secure communication."

Interpreting the "determining" phrase, Patent Owner directs attention to a passage in the '697 patent Specification, "'determin[ing] whether access to a secure site has been requested.'" PO Resp. 29 (quoting Ex. 1001, 40:32–33, modified by Patent Owner). The sentence immediately following this cited passage supports the view that gauging the requester's security privileges may help to determine whether a device is accessible:

> If access to a secure a secure site has been requested (as determined, for example, by a domain name extension, or by reference to an internal table of such sites), DNS proxy 2610 determines whether the user has sufficient security privileges to access the site.

Ex. 1001, 40:33–37.

[3] THE AMERICAN HERITAGE DICTIONARY OF THE ENGLISH LANGUAGE 90 (1975).

More importantly, the first quoted sentence in the passage indicates that determining whether a device is "available for a secure communication service" is broad enough to mean determining whether the device is listed on a network database that a secure network uses to obtain access to secure target devices.

Patent Owner argues that focusing on the requester's security level, and by implication, the relative security levels of the requester and the device, is not required: The "'determining' phrase *need not be limited* to the Decision's determining 'permission level or security privileges of the requester.'" PO Resp. 29 (emphasis added, citing Ex. 2025 ¶ 30). Therefore, the quoted passage from the Specification, bolstered by Patent Owner's argument, indicates that determining if a secure device is listed in an "internal table" (or similar database structure) of secure sites is sufficient to constitute a determination of availability.

As part of the disclosed process, the system returns a "resolved address" for the target device: "The address that is returned need not be the actual address of the destination computer." Ex. 1001, 40:45–49.

Another passage describes a normal DNS "look-up function":

> For DNS requests that are determined to not require secure services (e.g., an unregistered user), the DNS server transparently "passes through" the request to provide a normal look-up function and return the IP address of the target web server, provided that the requesting host has permissions to resolve unsecured sites. Different users who make an identical DNS request could be provided with different results.

Ex. 1001, 40:14–20.

In summary, according to disclosed embodiments in the '697 patent Specification, a device may be determined to be available as a secure device that the system provides, for example, by determining that the device is listed for use as part of the secure system. According to one of the above disclosed examples, which is not limiting, different users may be denied or granted access depending on that particular user's security privileges relative to the target's security level, rendering that device available or unavailable to that user.

Based on the foregoing discussion, according to the '697 patent Specification and the arguments presented, "determining, in response to a request, whether a second network device is available for secure communication," means "determining if the second network device is accessible for use, at hand, or usable, in a system that provides secure communication using that device."

## II. ANALYSIS

### *A. Beser*

Beser describes a system that establishes an IP (internet protocol) tunneling association between two end devices 24 and 26 on private networks, using first and second network devices 14 and 16, and trusted-third-party network device 30, over public network 12. *See* Ex. 1009, Abstract, Fig. 1; Pet. 16.

Figure 1 of Beser follows:

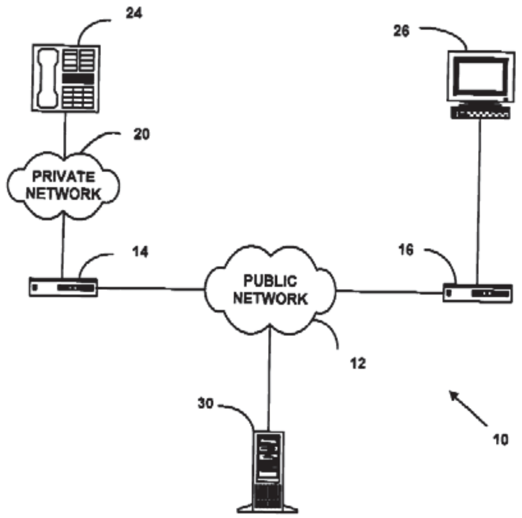

Figure 1 above represents Beser's system, which includes the Internet as public network 12, network end devices 24 and 26, private networks 20, trusted-third-party device 30, and modified router or gateway network devices 14 and 16. *See* Ex. 1009, Abstract, 3:60–4:18.

Beser's system "increases the security of communication on the data network" by providing and hiding, in packets, "private addresses" for originating device 24 and terminating device 26 on the network. *See id*. at Abstract, Fig. 1, Fig. 6. To begin the process for a secure transaction, at step 102, requesting device 24 sends to network device 14, as part of its request, an indicator that "may be a distinctive sequence of bits [that] indicates to the tunneling application that it should examine the request for its content and not ignore the datagram." Ex. 1009, 8:40–44, Figs. 1, 4. The request (which may include a series of packets) also includes a unique identifier, such as a domain name, employee number, telephone number, social security number, a public IP address 58, or other similar identifier, associated with terminating device 26. Ex. 1009, 10:37–11:8, 11:9–12. At step 104, network device 14 informs trusted-third-party network device 30 of the request. *See id*. at 7:64–8:7, 11:9–20, Fig. 4.

Trusted-third-party device 30 contains a directory of users, such as a DNS, which retains a list of public IP addresses associated at least with second network devices 16 and terminating devices 26. *See id.* at 11:32–58. At step 106 (and parallel step 116), DNS 30 associates terminating network device 26, based on its unique identifier (e.g., domain name, or other identifier) in the request, with a public IP address for router device 16 (i.e., the association of the domain name with other stored information, including Internet addresses, shows they are connected together at the edge of public network 12). *See* Ex. 1009, 11:26–36, Figs. 1, 4, 5.[4] As indicated, DNS 30 includes, in a directory database or otherwise, stored public IP addresses for router 16 and terminal device 26, and other data that associates devices 16 and 26 together. *Id*. at 11:48–52. In other words, trusted-third-party network device DNS 30, includes the "IP58 addresses for the terminating . . . device[s] 26," and uses "data structures . . . known to those skilled in the art . . . for the association of the unique identifiers [for terminating devices 26] and IP 58 addresses for the . . . network devices 16"—including domain names as unique identifiers, as noted above. *Id*. at 11: 2–5, 32–36, 48–55.

At step 108 (or step 118), Beser's system assigns, by negotiation, private IP addresses to requesting network device 24 and terminating device 26. *See id*. at 11:59–12:19, 12:38–48, Figs. 4, 5. In an exemplary embodiment, trusted-third-party network (DNS) device 30 performs the

[4] Figure 5, which includes step 116, involves a specific Voice-over-Internet-Protocol (VoIP) application of the general process of Figure 4, which includes parallel step 106. *See* Ex. 1009, 3:26–30.

negotiation for private addresses in order to further ensure anonymity of end devices 24 and 26 (though device 30 need not be involved in the negotiation in one embodiment). *Id*. at 9:29–35, 12:17–19. The negotiated private IP addresses are "isolated from a public network such as the Internet," and "are not globally routable." *Id*. at 11:63–65. "These IP 58 addresses may be stored in network address tables on the respective network devices, and may be associated with physical or local network addresses for the respective ends of the VoIP [(Voice-over- Internet-Protocol)] association by methods known to those skilled in the art." *Id*. at 12:33–37.

The negotiated private IP addresses may be "inside the payload fields 84 of the IP 58 packets and may be hidden from hackers on the public network 12." *Id*. at 12:15–16. The IP packets "may require encryption or authentication to ensure that the unique identifier cannot be read on the public network 12." *Id.* at 11:22–25; *see also* 20:11–14 (disclosing encryption or authentication of first IP 58 packet to ensure hiding the address of the public IP address of network device 16). Beser also discloses, as background prior art, known forms of encryption for "the information inside the IP packets," including IP Security ("IPSec"). *Id*. at 1:54–56.

Beser describes edge routers, such as network devices 14 and 16, as devices that route packets between public networks 12 and private networks 20. *Id*. at 4:18–24. End devices 24 and 26 include network multimedia devices, VoIP devices, or personal computers. *Id*. at 4:43–54.

### *B. RFC 2401*

According to RFC 2401, IPsec provides a "set of security services," including "access control, connectionless integrity, data origin authentication, [and] . . . confidentiality (encryption)." Ex. 1010, 4. RFC 2401 describes IPsec further, as follows:

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

*Id*. at 7.

The "security services use shared secret values (cryptographic keys) . . . . (The keys are used for authentication/integrity and encryption services)." *Id*.

### *C. Representative Claims*

As indicated above, Petitioner asserts that Beser anticipates, or alternatively, that the combination of Beser and RFC 2401 renders obvious, claims 1–11, 14–25, and 28–30. *See* Pet. 16–38. Patent Owner presents separate patentability arguments for claims 1, 2, and 3, with parallel arguments for claims 16, 17, and 24. *See* PO Resp. 36–56. Patent Owner asserts that the remaining challenged claims are patentable because they depend from claims 1 or 16. PO Resp. 52. Accordingly, this Final Written Decision focuses on claims 1, 2, and 3 as representative of the challenged claims.

### *D. Anticipation*

#### *i) Encryption and Secure Communication Link*

Patent Owner, supported by its declarant Dr. Fabian Newman Monrose in the Monrose Declaration (Ex. 2025), argues that Beser does not disclose encryption and therefore does not disclose a "secure communication link" as required by claims 1 and 16. PO Resp. 49–52. As set forth above, according to *Cisco* and the claim construction, a secure communication link does not require encryption. Petitioner contends that even if a secure communication link requires encryption, Beser discloses at least some encryption for initial IP packets, and, in any case, also discloses anonymity. The record supports Petitioner on both theories, as we find above in Section II.A. (citing, *e.g*., Ex. 1009, 9:29–35, 11:22–25, 12:15–19 –16, Abstract).

For example, regarding encryption, "[t]he IP 58 packets may require encryption or authentication to ensure that the unique identifier cannot be read on the public network 12." Ex. 1009, 11:22–25. Patent Owner maintains that this encryption in Beser only occurs "in initiating the tunnel, not after the tunnel is established." PO Resp. 49. Given our claim construction and the holding of *Cisco* we need not decide if initial encryption of address packets of Beser is sufficient to satisfy claims 1 and 16, or if Beser otherwise discloses more encryption, because claims 1 and 16 do not require any encryption.

In any case, as Petitioner points out, Patent Owner contends that in some scenarios contemplated by the '697 patent, "hiding the address information is important while hiding the video data and/or audio data itself is not." Prelim. Resp. 21; Pet. Reply 13. The initial encryption in Beser helps to hide the address information. Patent Owner's arguments in the Preliminary Response indicate that all the data, for example a video and audio data "payload," does not need to be encrypted on a secure communication link. Prelim. Resp. 21. Patent Owner also argues that Beser's system is not yet a "secure tunnel" when encryption occurs in Beser. PO Resp. 49 (citing Ex. 2025 ¶ 54). However, even if claims 1 and 16 require encryption, if a "secure communications service" and "secure communication link" as recited therein covers passing unencrypted audio and video data, which Patent Owner's arguments imply (*see* Prelim. Resp. 21), then any encryption at any time (i.e., even if it only sets up the secure communication service and link), satisfies the disputed element of claims 1 and 16.

Moreover, Patent Owner directs attention to Beser's disclosure of encrypting "'the first IP 58 packet 272 . . . to ensure that the public IP 58 address of the second network device 16 cannot be read on the public network 12.'" PO Resp. 53 (quoting Ex. 1009, 20:11–14). Contrary to Patent Owner's characterization of this teaching in Beser as restricted to a single class of packets at a pre-tunnel stage, Beser's system also uses the public IP address for device 16 on public network 12 *after it sets up the tunnel*—in order to route packets to router device 16 (by translating the private IP address for end device 26 into a routable address for router device 16). Ex. 1009, 22:8–13, 44–48. Therefore, because Beser discloses that it hides the public address for device 16, Beser implies that it always encrypts the public IP address for network device 16—i.e., before and after the secure tunnel exists. *See* Ex. 1009, 20:11–14, 22:8–13, 44–48.

Accordingly, even if encryption is required for claims 1 and 16, Beser meets that requirement. In any event, setting aside encryption, as Petitioner contends, Beser discloses anonymity by hiding the identities of end devices 24 and 26. Pet. Reply 11–12 (citing Ex. 1009, 12:6–29). Beser hides these addresses by performing the negotiation of the private addresses "through . . . device 30 to further ensure the anonymity of the telephony devices (24, 26).” Ex. 1009, 12:16–19. Patent Owner does not dispute this disclosure of anonymity in Beser.

Based on the foregoing discussion, Petitioner shows by a preponderance of evidence that Beser discloses a secure communication link as set forth in claims 1 and 16.

*ii) Intercepting*

The first step of claim 1 recites “intercepting, from the first network device, a request to look up an internet protocol (IP) address of the second network device based on a domain name associated with the second network device.” Claim 16 recites a similar element. As construed above, the term “intercepting a request” means “receiving a request pertaining to a first entity at another entity.”

Reading the “first” and “second network device[s]” respectively on Beser’s originating and end computer devices 24 and 26, Petitioner asserts that intermediate router device 14, or trusted-third-party device 30, a DNS, intercepts a tunneling request from originating device 24 to end device 26, where the request includes a unique identifier, including a domain name, that identifies end device 26. *See* Pet. 18–19; Pet. Reply 6–8; Ex. 1009, Fig. 1. According to Beser, pursuant to the tunneling request, trusted-third-party device 30, with devices 14 and 16, or device 30 by itself, negotiates and looks up a private internet address for end device 26, in part by looking up a public internet address for device 16 based on the domain name associated with end device 26. *See* Ex. 1009, 10:37–57, 11:1–52, 12:6–19, 13:30–33.

In Beser, as discussed above in Section II.A., the “request includes” 1) an indicator having “a distinctive sequence of bits” to initiate a secure tunneling action (*id.* at 8:37–38), and 2) “a unique identifier for the terminating end [26] of the tunneling association" (*id*. at 8:1–3). This unique identifier in a request packet may be "a domain name." *See id*. at 10:37–41, 11:20–22. Pursuant to the request packets, "[a] public network address for a second network device [16] is associated with the unique identifier on the trusted-third-party network device at Step 106." *Id*. at 8:4–7. In other words, "the second network device" 16 and its public address are "associated with . . . terminating end [26] of the tunneling association" via the terminating end's "unique identifier" (a domain name), and/or any number of "database entr[ies]," that provide an association, including "public IP 58 addresses for the terminating . . . device 26." *See id*. at 8:4–9, 11:45–55. After this association between device 16 and 26, in step 108, "the second private network address is assigned to the terminating end [26] of the tunneling association." *Id*. at 8:13–15. Fig. 4.

Patent Owner contends that "[a] request to initiate a tunneling connection, even if it happens to include a domain name in some embodiments, does not convert the tunneling request into the claimed 'request to look up an internet protocol (IP) address of the second network device,' as recited in claim 1." PO Resp. 37 (citing Ex. 2025 ¶ 40). Patent Owner reasons that "the trusted-third-party network device 30 does not perform any translation into an IP address of the domain name of the terminating device 26 or otherwise treat the request as a request to look up an IP address." *Id*. at 39 (citing Ex. 2025 ¶¶ 41–42). Patent Owner also contends that trusted-third-party network device 30 does not intercept requests, because it "instead has requests intercepted from it." *Id*. at 38.

Patent Owner describes Beser's system as follows:

> After being informed of the request, trusted-third-party network device 30 associates an identifier (e.g., a domain name) of terminating device 26 with a public IP address of a second network device 16. Beser then teaches that the first and second network devices 14 and 16 "negotiate" private IP addresses themselves through the public network 12, demonstrating that the trusted-third-party network device 30 does not perform any translation into an IP address of the domain name of the terminating device 26. In another embodiment, Beser discloses that a private address of the terminating device 26 is selected and transmitted by network device 16 to trusted-third-party network device 30, which then transmits the private address of the terminating device 26 to network device [14]. Here as well, the trusted-third-party network device 30 never performs any translation into an IP address of the domain name of the terminating device 26. Thus, the request in Beser is not a "request to look up an internet protocol (IP) address," as claimed.

PO Resp. 37–38 (citations omitted).

Patent Owner's characterization of Beser reveals that there is no dispute that Beser's trusted-third-party device 30 is "informed of the request" from device 14; thereby "receiving a request pertaining to a first entity [26] at another entity [14 or 30]" and satisfying the "intercepting a request" element of claim 1 (and a similar element in claim 16). As explained above and further below, Beser's tunneling request, which includes a domain name, is a request for a look up of an IP address. As also noted above, Patent Owner concedes that "[t]he *Decision's construction* [of intercepting a request] *addresses* a common aspect of *a conventional DNS and the disclosed embodiments*, namely that a request to look up an address of one entity may be received at another entity." PO Resp. 26 (emphases added).

Patent Owner's other arguments, as quoted above, essentially reduce to the contention that the requesting portion of the intercepting phrase in claim 1 (and similarly in claim 16), requires a *single* intercepting device, i.e., Beser's DNS 30, to look up a private or public address for terminating device 26 (which Petitioner reads as the second network device of claims 1 and 16). To the contrary, the intercepting phrases of claims 1 and 16 do not require a single specific device to intercept the request *and also* perform a "look up" function. Rather, similar to method claim 1, claim 16 implies that one or more devices in a "system" may intercept a "request" for such a "look up."[5] Further, any actual "look up," if required, is due to the next claim 1 (and similar claim 16) phrase, the "determining, in response to the request, whether" phrase. That is, claim 1 recites "intercepting . . . a *request*," in particular, "intercepting, from the first network device [24], *a request* to look up an internet protocol (IP) address of the second network device [26] based on a domain name associated with the second network device" (emphases added).

The record shows that a domain name for terminating device 26 (i.e., "the second network device" of claims 1 and 16) in the request packet constitutes a request, intercepted by DNS 30 and device 14, to "look up an internet . . . address of second network device" 26.[6] In addition to an

[5] Claim 16 recites, in its preamble, "the system including one or more servers configured to" perform similar functions to those recited in claim 1. Patent Owner does not argue claim 16 separately, or contend specifically, that servers must perform the recited functions. Dependent claim 30 requires one or more servers to intercept the request and reads on Beser's DNS 30. *See* Pet. 32–33.

[6] Even if claims 1 and 16 require DNS 30 to look up the IP address of the second network device, as discussed above in Section II.A., Beser discloses

implied look up (i.e., an association) of the public IP address of device 26 by DNS 30 (*see supra* note 6), Beser's network device 16 looks up the private IP address of device 26—after DNS 30 and network device 14 receive the request for a look up. *See, e.g.*, Ex. 1009, 16:1–37; PO Resp. 33 (describing Beser's Fig. 9, step 156, which shows that second network device 16 "select[s] second private IP address"). Therefore, based on the foregoing discussion and Beser's disclosure, we find that either of Beser's devices 14 or 30 intercepts a request to look up an internet address of second network device 26, as required by claims 1 and 16.

In other words, even if claims 1 and 16 require an actual IP address look up to satisfy the "intercepting . . . a request" phrase, Beser discloses looking up the private and public IP addresses for end device 26. In addition to the private IP address look up of device 26 (*see* Pet. Reply 8–9), Petitioner also relies on an IP look up by DNS 30—a look up of "a public IP address for . . . device 16 [which] is associated with the unique identifier for . . . terminating telephony device' [26]." Pet. Reply 7 (quoting Ex. 1009, 11:26–28) (addition by Board).

that trusted-third-party device 30, acting as a DNS, may include a "database entry . . . includ[ing] a public IP 58 address[] *for the terminating telephony device 26*. Many data structures that are known to those skilled in the art are possible *for the association of the unique identifiers and IP 58 addresses for the second network devices 16*." Ex. 1009, 11:50–55 (emphases added); *see* Inst. Dec. 18 (discussing and quoting Ex. 1009, 11:47–52); Inst. Dec. 21–22 (discussing association of public IP addresses of 16 and 26). Therefore, in this disclosed embodiment, which merely uses more information than the generic embodiment, Beser's DNS 30 implicitly looks up the public IP 58 addresses of devices 16 and 26 based on a domain name (unique identifier) of terminating device 26—in order to associate the two devices.

As discussed, to make the association, Beser's DNS 30, a directory service, stores public IP addresses for device 26. *Supra* note 6; Ex. 1009, 11:45–55; *see also* Inst. Dec. 18 ("Beser's system includes stored public IP address for router or modem 16 and second network device 26, which are involved in the association with the domain name.") (citing Ex. 1009, 11:48–52). Therefore, Beser implies that it associates devices 16 and 26 by, among other ways, looking up the public IP addresses of both of those devices, based on the unique domain name for device 26. *Supra* note 6 (discussing Ex. 1009, 11:50–55); Ex. 1009, 11:45–55. Patent Owner does not dispute that Beser's DNS 30 associates the public IP addresses of 16 and 26 with the domain name of device 26, as discussed in the Institution Decision. *See* Inst. Dec. 18, 21–22.

In summary, Beser's system looks up a private address of end device 26, satisfying the "intercepting . . . a request" phrase. In addition, or alternatively, DNS 30 looks up (associates) either a private and public IP address of end device 26, or both, with the public IP address of device 16 (*see supra* note 6), so that looking up the public IP address for device 16 (which is associated with device 26), as Petitioner contends, also satisfies the phrase, and constitutes a request to look up an "internet protocol (IP) address of the second network device [26] based on a domain name associated with the second network device," as claim 1 requires. As Petitioner summarizes, in response to indicator bits and the unique identifier, "Beser shows a 'tunneling' request that is used to 'look[] up an [IP] address.'" Pet. Reply 8. According to Beser, "the request includes a unique identifier for the terminating telephony device 26," and the "unique identifier" includes "a domain name." Ex. 1009, 10:37–41.

Based on the foregoing discussion, Petitioner shows by a preponderance of evidence that Beser discloses "intercepting, from the first network device [24], a request to look up an internet protocol (IP) address of the second network device [26] based on a domain name associated with the second network device," as required by claim 1 and as similarly required by claim 16.

*iii) Determining*

Patent Owner contends that Beser does not teach the "determining" step recited in claim 1: "determining, in response to the request, whether the second network device is available for a secure communications service." *See* PO Resp. 43. Claim 16 recites a similar feature.

Petitioner maintains that Beser's system satisfies the determining step, for two reasons. First, Petitioner asserts that "as Patent Owner admits, the trusted-third-party network device will only initiate a tunnel if the originating device has been authenticated." Pet. Reply 12 (quoting PO Resp. 49; Ex. 1009, 11:22–25). In the alleged admission, Patent Owner actually states that "this encryption or authentication occurs in initiating the tunnel, not after the tunnel is established." PO Resp. 49 (citing Ex. 2025 ¶ 54).

The passage in Beser describing authentication follows:

> At least one of the IP 58 packets includes the unique identifier for the terminating telephone device 26 that had been included in the request message. The IP 58 packets may require encryption or authentication to ensure that the unique identifier cannot be read on the public network 12.

Ex. 1009, 11:20–25.

By authenticating or encrypting packets to hide the unique identifier (a domain name for device 26) on the public network, Beser's system effectively may grant communication access to sending device 24 (the asserted "first network device" of claims 1 and 16). However, it may do so without regard to any specified end device, such as particular end device 26, the asserted "second network device" of claim 1. For example, after authenticating the packet, thereby determining that end device 26 is accessible according to Petitioner's first reason, Beser's system thereafter may determine that DNS 30 does not list the unique identifier for a specific end device 26, according to Petitioner's second reason (discussed further below). *See* Pet. Reply 10. Therefore, Petitioner fails to show by a preponderance of evidence that *merely* authenticating at least one of the set of IP packets 58 from first network device 24 constitutes determining that "second network device" 26 is available.

Regarding the second reason, Petitioner asserts that determining the availability of network end device 26 ("the second network device" of claims 1 and 16) for secure communication service includes determining that Beser's system lists and matches a domain name for device 26, and then assigns a private IP address to it. *See* Pet. Reply 9–11. In other words, in response to a domain name and unique bits embedded in a request for a secure communication service to end device 26 (as described above, *see* Sections II.A., II.D.ii), Beser's system looks up a private IP address of end device 26, thereby satisfying the look up for an IP address as required by the determining step (i.e., which recites "in response to the request"—where the request refers back to a request to "look up . . . an internet . . . address" as introduced in the intercepting step). *See id*. at 10 (arguing that "if the domain name 'does not map to a device requiring negotiation of an IP tunnel' a private IP address is not returned") (quoting the Petition at 20–21).

Addressing Petitioner's second contention, Patent Owner argues that "no component in Beser's system ever determines that device 24 or device 26 has a private internet address assigned to it in response to a request to look up an IP address of a device based on a domain name." PO Resp. 43 (citing Ex. 2025 ¶ 46) (emphasis omitted). Patent Owner also maintains that although

> private network addresses associated with device 24 and device 26 may be selected by device 14 and device 16 in Beser, no determination in Beser is ever made in response to a request to look up an IP address of a device based on a domain name—at device 14, device 16, or trusted-third-party network device 30– as to *whether* device 24 or device 26 has a private network address assigned to it.

PO Resp. 45 (citing Ex. 2025 ¶ 47).

Patent Owner's arguments are not persuasive. Dr. Monrose's testimony largely repeats Patent Owner's arguments. *See* Ex. 2025 ¶¶ 46–47. His testimony that "*no component*" determines that device 26 has a private internet address assigned in response to a domain name request (Ex. 2025 ¶ 47 (emphasis added)) is not persuasive, because claim 1 is a method claim, and claim 16 requires "the system including one or more servers configured to" perform similar functions, as noted above. *See supra* note 5.

As indicated above in the discussion of the intercepting step, Beser's *system* makes the required determination of accessibility of end device 26. In response to the domain name of end device 26 in request packets, Beser's *system* looks up and assigns a private internet address to device 26, and also returns that address to devices 14, 24, and 30 for secure communication. Finding and returning such a private address for device 26, which occurs ultimately in response to packets that contain its domain name, satisfies the determining step under a broadest reasonable construction of the phrase (*see* section I.E.iv), because, at the least, making the device available for secure communication constitutes a determination that it is available. As discussed, Beser's DNS 30 lists the unique identifier (a domain name) for second device 26 (for example as a database or DNS entry, *see supra* note 6; Section II.A; Ex. 1009, 11:26–58). Without that domain name listing in Beser's DNS, Beser cannot return a private address for that domain name (or associate it with devices 16 and 26). We find that Beser's system returns a private address for device 26 only if it looks up its domain name and finds it. (DNS 30 also would not find (i.e., look up) a public address assigned to that domain name, which Beser discloses as a database entry (*see supra* note 6), and DNS 30 also would not return a public address for device 16 associated with that domain name.) *See* Ex. 1009, 11:8–12:19; *supra* Sections II.A, II.D.ii.

Therefore, Beser's system determines that device 26 is available for secure communications because it makes that device available for those communications, by assigning it a private address after it finds the domain associated therewith listed in DNS 30. According to Beser, "[t]he . . . system . . . may help ensure that the addresses of the ends of the tunneling association are hidden on the public network and may increase the security of communication." Ex. 1009, 3:5–9. Stated differently, Beser's system or method determines that device 26 is available for secure communications as required by claims 1 and 16, because the system or method provides secure communications by returning private addresses for that secure communication only after determining that DNS 30 lists device 26. Moreover, Beser contemplates, in some embodiments, a secure system that accesses only private systems 20 attached to public network 12. *See* 4:21–23 (disclosing that edge routers 14 and 16 connect between public network 12 and private networks such as 20).

Contending otherwise, Patent Owner asserts that "Beser does not disclose what would happen if a valid domain name . . . were not present in a tunnel initiation request." PO Resp. 46. Patent Owner also contends that Petitioner "intermingles" normal DNS functions and Beser's "tunnel-establishment process," when they "would be compartmentalized and separate." *Id*. at 46–47.

In support of its position, Patent Owner relies on its declarant, Dr. Monrose, who states that

> the DNS server in Beser could return an error message, could discard the request, could do nothing, or could wait until the domain name does map to a device requiring negotiation of an IP tunnel. Even if [Petitioner's] proposed manner of operating the DNS server in Beser could actually be implemented, it would be one of several possibilities and is not necessarily present in Beser's system.

Ex. 2025 ¶ 45.

Setting aside, momentarily, the "wait" possibility that Dr. Monrose alleges, as Petitioner essentially contends, the first three possibilities that Dr. Monrose outlines merely describe conventional DNS functions, and Beser discloses coventional DNS functions and other functions. *See* Pet. Reply 11; Ex. 1009, 11:33–34 ("network device 30 is a . . . domain name server").[7]

[7] *See supra* note 6, *see also* Ex. 1009, 1:50–53 ("For example, an appropriate Domain Name Server ('DNS') inquiry may correlate the IP address with a domain name, and domain names are typically descriptive of the user, location, or the user's organization."); 10:55–57 ("Other possibilities are that the unique identifier . . . is a domain name . . . used to initiate the VoIP

Dr. Monrose's testimony  implies that Beser's DNS only maps a public IP address, and then helps to negotiate private IP addresses, which devices 14 and 16 look up, only if the domain name for 26 is listed in the DNS and elsewhere.  That is, it must be listed for it to be mapped—there must be something (i.e., the unique domain name) "to correlate" or "to provide a look-up function" (*supra* note 7).  *See also* note 6 (additional DNS disclosures).  Otherwise, assuming Patent Owner is correct, the DNS "return[s] an error message, . . . discard[s] the request, [or does] . . . nothing."  *See id*.  In essence, the record shows that Beser discloses a conventional DNS modified to additionally perform tunnel negotiation for private IP addresses.

Tracking Patent Owner's arguments, Dr. Monrose characterizes Beser as disclosing "an embodiment where *Beser*'s trusted-third- party network device is part of a domain name server, [and] any DNS functionality and *Beser*'s disclosed tunnel-establishment functionality would be compartmentalized and separate."  Ex. 2025 ¶ 50.  This testimony does not describe a claim distinction:  Claims 1 and 16 simply do not preclude the typical DNS functions and negotiating functions from being "compartmentalized and separate."  Regarding the "wait" possibility alleged, to the extent that Dr. Monrose contends that Beser's DNS may return a private address for an *unrequested* device (i.e., "wait until the domain name

association." ): 10:37–41 (similar).  Similarly, according to the '697 patent, "[c]onventional Domain Name Servers (DNSs) provide a look-up function that returns the IP address of a requested computer or host."  Ex. 1001, 39:29–34.  In addition, according to this conventional scheme, "[w]hen a user enters the name of a destination host, a request DNS REQ is made . . . to look up the IP address associated with the name."  *Id*. at 39:42–44.

does map to a device requiring negotiation of an IP tunnel" as quoted above), Dr. Monrose does not provide credible, if any, evidence or rationale, to support this characterization of Beser's DNS, or any typical DNS. Neither Patent Owner nor Dr. Monrose directs attention to a citation of Beser that supports the testimony or shows that Beser's DNS returns an address for an *unrequested* device.

Therefore, Beser's look-up and negotiation procedure, or as supplemented by the authentication procedure outlined above, determines, after an initial request using a unique identifying domain name, that terminating device 26 is accessible or usable by the system for secure communications, under the broadest reasonable construction of the determining phrase. The record shows that only devices 26 having a domain name listed in Beser's DNS and elsewhere would be associated with a routing device 16 after a look up of a public address of device 16 and a look up of a private address of device 26, rendering device 26 available for secure communication, because Beser discloses a method and system for providing a secure tunneling system to such devices. Device 16 looks up (i.e., finds, in a table, or otherwise), and assigns to end device 26, a private address from a "pool," which it would not do unless device 16 has a valid domain name listed in Beser's secure system, according to the findings above. *See also* Ex. 1009, 16:6–7, 1–16 (discussing the "private address pool"), Fig. 9 (device 16 selects the second private IP address in step 156).

In a similar scenario described in *Cisco*, the court determined that Apple's "VPN On Demand" system infringed claims in the '135 and '151 patents which included a similar "determining . . . whether" phrase. *See* 767 F.3d at 1315, 1320. Specifically, in *Cisco*, claim 1 of the '135 patent recited "determining whether the DNS request transmitted in step (1) is requesting access *to a secure web site*." *Id*. at 1315 (emphasis added).

Determining that Apple's VPN On Demand system infringed claim 1, the court found as follows:

> Here, the evidence presented at trial supports the conclusion that Apple's VPN On Demand product infringes the asserted claim limitation in its normal configuration. In particular, VirnetX's expert testified that Apple's technical design documents and internal technical presentations relating to the VPN On Demand system . . . make clear that a VPN connection should only be established for private web addresses. . . .
>
> Moreover, this description of the VPN On Demand feature is consistent with how the claimed functionality is described in the specification. *For example, in one embodiment, the DNS proxy determines whether a request is for a secure site by checking the domain name against a table or list of domain names*. '135 patent, col. 38 ll. 23–30. In other words, the *proxy identifies a request for "access to a secure site ... by reference to an internal table of such sites*." *Id.* That is precisely how the VPN On Demand feature operates.
>
> We therefore conclude that the jury's finding that the VPN On Demand product infringes the "determining whether" limitation was supported by substantial evidence.

767 F.3d at 1320–21 (emphases added).

These passages in *Cisco* provide illumination, because VPN On Demand, the invention disclosed in the '697 patent, and Beser, operate similarly by checking domain names to determine availability. Moreover, claim 1 of the '135 patent involved in *Cisco* requires determining whether "access to *a secure* web site" (emphasis added) is requested. In contrast, claims 1 and 16 involved here merely require determining whether the second network device is *available* for secure communications—i.e., the end device need not be secure before it is determined to be available. In any event, Beser's system only lists secure end devices (i.e., those on private networks 20) for one of its embodiments, and for all embodiments, makes all listed end devices secure by providing private IP addresses and anonymity. Determining that a particular end device 26 in Beser is listed for use in Beser's secure DNS system by finding its domain name and assigning a private address to it, and thereby making the listed end device secure, under the rationale of *Cisco*, is sufficient to satisfy the determining phrase in claims 1 and 16 of the '697 patent.

Based on the foregoing discussion, Petitioner shows by a preponderance of evidence that Beser discloses the "determining . . . whether" and "determine . . . whether" clauses of claims 1 and 16.

*iv) Remaining clauses*

The Institution Decision initially finds, based on the Petition and Beser, that Beser discloses the initiating and wherein clauses of claim 1, and similar parallel clauses in claim 16. *See* Inst. Dec. 25–32. Patent Owner does not argue with particularity in its Patent Owner Response that Beser fails to disclose these final two clauses of claims 1 and 16. In summary, these clauses require the initiation of a secure communication link based on a determination that the second network devices is available for communication, wherein the secure communication service uses the link to communicate at least one of audio and video data. According to the description of Beser above in Section II.A., and the discussions above of the related clauses, as supplemented by the findings in the Institution Decision, we find that Beser's system initiates the link based on determining availability, and provides the secure communication service to communicate one of audio and video data, as required by claims 1 and 16. *See, e.g.*, Ex. 1009, Abstract (disclosing VoIP secure communications by initiating a tunnel between end devices over a public network), Fig. 1.

Based on the foregoing discussion, Petitioner shows by a preponderance of evidence that Beser anticipates claims 1 and 16.

### *E. Beser, or Beser and RFC 2401*

#### *1. Claims 1, 2, 16, and 24*

Claims 2 and 24 respectively depend from claims 1 and 16 and require encryption of audio or video data. To the extent claims 1 and 16 require more encryption of information than Beser discloses under a narrow claim construction of a secure communication link or secure communication service, the following analysis of claims 2 and 24 applies also to claims 1 and 16.

Petitioner generally relies on Beser's disclosure that describes known encryption techniques. *See* Pet. 23–24; Pet. Reply 13–14. Petitioner relies further on RFC 2401 as suggesting encryption of data, by using the IPsec protocol, the same encryption protocol that Beser discloses. *See* Pet. 35–36; Ex. 1009, 1:54–56; Ex. 1010, 4. Petitioner contends that RFC 2401 provides automatic encryption for traffic traveling through security gateways over a public network, and that Beser employs edge routers and similar gateways, thereby at least suggesting encryption for a secure tunnel. *See* Pet. 34–37; Ex. 1010, 4–6, 30. RFC 2401 describes an IPsec goal as providing "confidentiality (encryption)." Ex. 1010, 4.

In response, Patent Owner contends that the combination of Beser and RFC 2401 fails to render obvious the use of encryption of audio or video data as claims 2 and 24 require, or to establish a secure communication link, as Patent Owner contends that claims 1 and 16 require. *See* PO Resp. 49–

52, 56. According to Patent Owner, Beser teaches away from using the IPsec protocol of RFC 2401 for audio or video data. *Id.* at 56–57. Patent Owner explains that Beser describes encryption as requiring increased power for "packets on the fly," and also describes it as aiding hackers by allowing them to decrypt packets accumulated in a buffer during encryption according to the IPsec protocol. *Id.* at 57 (citing Ex. 2025 ¶¶ 62–63; Ex. 1009, 1:58–66).

Petitioner replies by noting that Patent Owner's declarant, Dr. Monrose, agreed, during his deposition, that "the implementation challenges that Beser identifies in using encryption can easily be navigated." Pet. Reply 15 (citing Ex. 1083, 206:20–208:6). At the cited deposition passage, during questioning about teaching away in Beser, Dr. Monrose agrees that sending voice data with lower resolution would have been "conceivable" (Ex. 1083, 208:6), and that using a more powerful computer would constitute "one possible way" (*id.* at 207:7) to implement Beser's system and use encryption. Therefore, as Petitioner contends, Dr. Monrose effectively concedes that Beser does not teach away from encryption when performed in higher power computers that do not accumulate a large number of packets at a node buffer—i.e., video or audio packets that capture a relatively lower resolution of voice or audio than other multimedia may capture. *See* Pet. Reply 15.

In general, Beser's system hides addresses on the public network, which "may *increase* the *security* of communication without an *increased* computational burden." Ex. 1009, 3:5–9 (emphases added). Hiding, in packets, "private addresses" is a form of tunneling that provides anonymity. *See* Ex. 1009, Abstract ("hiding the identity"), 12:16–19 (negotiating the private addresses "through . . . device 30 to further ensure the anonymity of the telephony devices (24, 26)"). By "increasing" security without an increased computational burden, Beser's tunnel techniques at least suggest adding a layer of security to known security methods—for example, by adding Beser's anonymity method to the encryption of voice or audio data.

Beser also describes prior art systems that encrypt data, hide addresses by encapsulating and encrypting them in the payloads of packets, or otherwise hide addresses by translating them. *See* Ex. 1009, 1:40–2:40.[8] Beser describes potential hacking concerns due to accumulating a large number of packets at a source so that a hacker "may" be able to decrypt the packets and obtain source information. PO Resp. 57; Ex. 1009, 1:57, 54–58. However, as Dr. Monrose concedes and as Petitioner argues, lower resolution of audio or video data redounds to a lower accumulation of data packets. In addition, Beser does not describe a hacker problem as occurring when a scheme like Beser's hides or encapsulates private address information inside a packet–a tunneling technique. Rather, in relation to Beser's description of a prior art VPN (discussed further below), Beser only describes power concerns, instead of hacker concerns: "The tunneled IP packets . . . may need to be encrypted before the encapsulation in order to hide the source IP address. Once again, *due to computer power limitations*, this *form of tunneling may* be inappropriate for the transmission of multimedia or VoIP packets." Ex. 1009, 2:12–17 (emphases added).

[8] As discussed above, Beser specifically discloses encrypting at least some IP packets, although Patent Owner contends that this occurs only at tunnel initialization. *See* Ex. 1009, 11:22–25; PO Resp. 52–53 (citing Ex. 2025 ¶¶ 58).

Beser's similar *tunnel solution* hides the source (and terminating end) by sending private addresses inside of packet payloads. *See id*. at 9:49–51, 12:13–16. Beser's tunnel solution also includes encrypting packets to hide the unique identifier and public IP addresses on the public network. *Id*. at 11:22–25, 20:11–14. Beser suggests that any problems associated with encryption in tunnels, including with multimedia, may be overcome by providing more computer power. *Id*. at 2:13–17. Specifically, Beser cautions that using IPSec for "streaming data flows, such as multimedia or . . . ('VoIP'), may require a great deal of computer power to encrypt or decrypt IP packets on the fly." *Id*. at 1:60–62. Beser adds that "[t]he expense of added computer power might also dampen the customer's desire to invest in VoIP equipment." *Id*. at 1:65–67.

Therefore, skilled artisans would have recognized that Beser's system overcomes prior art hacking problems, and also that Beser suggests encryption of at least low resolution audio or video data packet information, as encompassed by claims 2 and 24. Even if hacking is a concern for streaming flows, as Petitioner argues, the claims do not require streaming data flows, and "would cover transfer of video file[s] via other means." Pet. Reply Br. 15. As argued, video or audio data covered by the claims need not be streamed live, but could have been sent at a desired speed so that the information can be stored for later usage. Therefore, any teaching away is not commensurate in scope with the challenged claims, or would be overcome by increasing computer power, coupled with Beser's tunneling solution.

Finally, Beser characterizes some prior art systems as creating "*security problems by preventing certain types of encryption from being* *used*." Ex. 1009, 2:23–24 (emphasis added). And Beser's system "increase[s] . . . security." *Id*. at 3:7. Therefore, skilled artisans would have recognized that Beser implies or suggests solving these security problems by providing compatibility with known audio or video data encryption techniques, thereby enhancing security. The record shows that artisans of ordinary skill would have recognized that the combination of Beser and RFC 2401 at least suggests that encrypting audio or video likely would be "productive," and a skilled artisan "would [not] be led in a direction divergent from the path that was taken by the applicant." *See In re Gurley,* 27 F.3d 551,553 (Fed. Cir. 1994).

Based on the foregoing discussion, Petitioner shows by a preponderance of evidence that Beser renders obvious claims 1, 2, 16, and 24. The conclusion of obviousness renders it unnecessary to decide if Beser anticipates claims 2 and 24. *Cf. In re Gleave*, 560 F.3d 1331, 1338 (Fed. Cir. 2009) (not reaching obviousness after finding anticipation).

### *2. Claims 3 and 17*

Claim 3 depends from claim 1 and requires the secure communication link to be a VPN communication link. Claim 17 depends from claim 16 and recites a similar feature. Petitioner argues that Beser's secure IP tunnels constitute VPNs because they allow end devices to communicate over a secure and anonymous channel. *See* Pet. 24–25, 37–38; Pet. Reply 14. Petitioner contends that Beser anticipates claims 3 and 17. Alternatively, even if a VPN communication link requires encryption, Petitioner contends that Beser in view of RFC 2401 would have rendered claims 3 and 17 obvious. *See* Pet. 24–25, 37–38.

Patent Owner contends that Beser criticizes a VPN as "'[a] form of tunneling [that] may be inappropriate for the transmission of multimedia or VoIP packets' . . . , immediately before introducing Beser's tunnel as a solution to the problems posed by VPNs for VoIP." PO Resp. 55 (quoting and citing Ex. 1009, 2:6–17, 2:43–66). Therefore, according to Patent Owner, Beser "expressly teaches that its tunnel is not a VPN communication link." *Id*. (citing Ex. 2025 ¶ 60).

Patent Owner's characterization fails to account for the broadest reasonable construction of a VPN communication link (as explained above in Section I.E.ii), and it mischaracterizes Beser's teachings. As to the first point, Beser's tunnel provides anonymity over a public network, rendering it a VPN under the broadest reasonable (and a narrower) construction the term. *See* Ex. 1009, Abstract, 12:16–19 (negotiating the private addresses "through . . . device 30 to further ensure the anonymity of the telephony devices (24, 26)."). Beser similarly refers to a VPN as "a tunneling connection between edge routers on [a] public network," which uses "encapsulation" (and which "may" require encryption) to "hide the source IP address." *See* Ex. 1009, 2:9–14.

As to the second point, as Patent Owner states, Beser discloses that "'[o]ne method of thwarting [a] hacker is to establish a Virtual Private Network ('VPN') by initiating a tunneling connection between edge routers on the public network.'" PO Resp. 55 (quoting Ex. 1009, 2:6–8). Beser then discusses problems with such a VPN if it employs encryption, but Beser does not state that a VPN has insurmountable problems, if any, or that

Beser's tunnel is not a VPN.[9] For example, as discussed above, Beser teaches that "[o]nce again, *due to computer power limitations*, this form of [VPN] tunneling [that uses encryption] may be inappropriate for the transmission of multimedia or VoIP packets." *Id*. at 2:15–17. Even if a VPN communication link requires encryption, Beser discloses or suggests, or Beser and RFC 2401 suggest, that feature as discussed in connection with claims 1, 2, 16, and 24, and in any case, this prior art discloses or renders obvious the VPN communication link required by claims 3 and 17.

Based on the foregoing discussion, Petitioner shows by a preponderance of evidence that Beser anticipates, or Beser with RFC 2401 renders obvious, claims 3 and 17.

### *F. Summary and Dependent Claims 4–11, 14, 15, 18-23, 25, and 28–30*

Based on the foregoing discussion, and a review of the record, Petitioner demonstrates by a preponderance of evidence that Beser anticipates, or that Beser with RFC 2401 renders obvious, claims 1–3, 16, 17, and 24. In the Institution Decision, we initially found and determined that Petitioner shows that Beser, and Beser with RFC 2401, respectively anticipates or renders obvious, the remaining challenged claims, claims 4–11, 14, 15, 18–23, 25, and 28–30. *See* Inst. Dec. 25–32; Pet. 25–38. In

[9] Patent Owner does not argue that a VPN requires Beser's "example" of a VPN that refers to "encapsulating the IP packet to be tunneled within the payload field for another packet that is transmitted over the public network." *See* Ex. 1009, 2:8–13. In any event, Beser describes placing "the private network address . . . as the payload in data packets" (Ex. 1009, 9:48–52), and sending those over a public network, which, on this record, constitutes a form of tunneling and a VPN, based on anonymity. *See* Ex. 1009, 11:2–25, 18:11–14.

response, Patent Owner relies on arguments presented for patentability of claims 1–3, 16, 17, and 24. *See* PO Resp. 52, 56–58.

For example, claims 4 and 18 require the secure communications service includes a video conferencing service. Claim 18 recites a similar feature. Petitioner asserts that Beser discloses or renders obvious video conferencing, because Beser discloses VoIP traffic, and multimedia content in the form of audio and video data. Pet. 25; Ex. 1009, 4:43–54. In addition to multimedia devices, Beser also discloses VoIP and the International Telecommunications Union-Telecommunication Standardization Sector ("ITU") standard H.323, which involves audio and video teleconferencing. Ex. 1009, 9:67–10:2, Fig. 5; Ex. 1074, 1, 5 (describing ITU-T H.323 standards, which include multimedia communications such as multipoint conferences). On this record, Beser contemplates video conference services according to well-known conferencing standards disclosed by Beser.

Claim 5 depends from claim 1 and recites "wherein the secure communications service is a telephony service." Claim 6 depends from claim 5 and recites "wherein the telephony service uses modulation." Claims 19 and 20 depend from claim 16 and respectively are similar to claims 5 and 6. Claims 8 and 22 respectively depend from claims 1 and 16 and similarly require a mobile device. Petitioner asserts that Beser, which employs modems, and discloses wireless mobile devices, implicitly or necessarily uses modulation. *See* Pet. 26–28. Beser's system employs telephony, mobile devices, and multimedia devices, using known standards, such as Wireless Internet  Protocol ("WAP"), VoIP, Institute of Electrical and Electronic Engineers ("IEEE"), and ITU. *See* Ex. 1009, 4:18 – 5:14. These devices generally convert voice and other media to data, receive and transmit the data at internet frequencies, and thereby implicitly or necessarily employ known modulation standards. *See id*. Petitioner establishes by a preponderance of evidence that Beser anticipates or renders obvious claims 5, 6, 8, 19, 20, and 22.

Claim 7 depends from claim 1 and requires the modulation to be based on specific modulation types, Frequency-Division Multiplexing ("FDM"), Time- Division Multiplexing ("TDM"), or Code Division Multiple Access ("CDMA"). Claim 21 depends from claim 16 and recites a similar feature. Petitioner relies on Beser's disclosure of using WAP standards, which include standards for wireless devices and well-known wireless multiplexing or modulation schemes, including Web-TV and other multimedia. *See* Pet. 26–27; Ex. 1009, 4:55–62. Beser contemplates or renders obvious the well-known modulation techniques for transmitting and receiving data according to known standards incorporated by Beser's disclosure for exchanging information over the internet. *See id*.

Claim 9 recites "wherein the mobile device is a notebook computer." Claim 23 recites a similar limitation. Beser discloses "portable or stationary" personal computer devices. *See* Ex. 1009, 4:43–54. According to Petitioner, a skilled artisan would have recognized that a personal computer includes different types of such computers, including stationary desktop computers and portable laptop or notebook computers. *See* Pet. 28. Beser contemplates a notebook computer as a well-known type of portable personal computer.

Claim 10 recites that "intercepting the request consists of receiving the request to determine whether the second device is available for the secure communications service." Claim 29 recites a similar feature. Similar to the assertions involving claim 1, Petitioner asserts that Beser discloses that the trusted third-party network device intercepts a request for a second network device and determines if that device is available for the secure service. *See* Pet. 21–22, 28–29. Also similar to the assertions regarding claim 1, Petitioner asserts that "[u]nder the inherent operation of the Beser process, if a domain name specifies a destination that is unavailable or unknown to the trusted third-party network device, the request will not be routed further." *Id*. at 29. As found in the discussion of claim 1, Beser discloses intercepting a request and determining the availability of a second network device, based on unique identification, or domain name, of the second device, which leads at least to a private internet addresses for that device.

Claim 11 depends from claim 1 and requires the secure communication link to support data packets. Claim 25 depends from claim 16 and recites a similar feature. Petitioner asserts that Beser discloses packets, including in the form of IP addresses, which necessarily involves data packet transmission. Pet. 30. Beser generally discloses packets on the internet, including VoIP and other forms. Ex. 1009, Figs. 3, 5, 14; 1:26–30, 11:10–12. Beser also discloses that "[t]he payload field 84 of the IP 58 packet 80 typically comprises the data that is sent from one network device to another." *Id.* at 7:10–12. Therefore, Beser discloses a link that supports data packets, as recited in claims 11 and 25.

Claim 14 recites "determining that the second device is available for a secure communications service is a function of a domain name lookup." Claim 28 recites a similar feature. Petitioner asserts that Beser discloses using a trusted third-party network device that can be a domain name server that stores domain names associated with IP addresses. *See* Pet. 30–32. As noted above in the discussion of claim 1, Beser discloses determining the availability of a second network device based on unique identification that includes a domain name associated therewith.

Claim 15 recites that "intercepting the request occurs within another network device that is separate from the first network device." Claim 30 recites a similar feature. Petitioner maintains, as discussed in connection with claim 1, that Beser's trusted-third-party network, a distributed device, intercepts the request and constitutes a device that is separate from the first device. *See* Pet. 32–33; Ex. 1009, Figs. 1, 5, 6.

As noted, Patent Owner generally does not dispute Petitioner's contentions except in connection with claims 1–3, 16, 17, and 24. Based on the foregoing discussion, and a review of the record, Petitioner demonstrates by a preponderance of evidence that Beser anticipates, or that Beser with RFC 2401 renders obvious, claims 4–11, 14, 15, 18–23, 25, and 28–30. *See* Inst. Dec. 25–31; Pet. 25–38; PO Resp. 52, 56–58.

### *G. Declaration of Michael Fratto*

Patent Owner argues that the Declaration of Michael Fratto (Ex. 1003) should not be given any weight. *See, e.g.*, PO Resp. 1–8. We do not rely on the testimony of Mr. Fratto to reach this Final Written Decision. Therefore, Patent Owner's argument is moot.

## III. CONCLUSION

Petitioner has demonstrated, by a preponderance of the evidence, that claims 1, 3–11, 14–23, 25, and 28–30 are anticipated by Beser under 35 U.S.C. § 102, and that claims are 1–11, 14–25, and 28–30 are unpatentable over Beser and RFC 2401, under 35 U.S.C. § 103(a).

## IV. ORDER

In consideration of the foregoing, it is hereby

ORDERED that claims 1–11, 14–25, and 28–30 of U.S. Patent No. 8,504,697 B2 are unpatentable; and

FURTHER ORDERED that, because this is a Final Written Decision, the parties to the proceeding seeking judicial review of the decision must comply with the notice and service requirements of 37 C.F.R. § 90.2.

PETITIONER:

Jeffrey P. Kushan
Joseph A. Micallef
SIDLEY AUSTIN LLP
jkushan@sidley.com
jmicallef@sidley.com

PATENT OWNER:

Joseph E. Palys
Naveen Modi
PAUL HASTINGS LLP
josephpalys@paulhastings.com
naveenmodi@paulhastings.com

Jason E. Stach
FINNEGAN, HENDERSON, FARABOW, GARRETT & DUNNER, LLP
jason.stach@finnegan.com