

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

KEYSIGHT TECHNOLOGIES, INC.,
Petitioner,

v.

CENTRIPETAL NETWORKS, LLC,
Patent Owner.

IPR2022-01525
Patent 10,284,526 B2

Before KEVIN F. TURNER, BRIAN J. McNAMARA, and
STEVEN M. AMUNDSON, *Administrative Patent Judges*.

McNAMARA, *Administrative Patent Judge*.

JUDGMENT
Final Written Decision
Determining All Challenged Claims Unpatentable
35 U.S.C. § 318(a)

I. BACKGROUND

In response to a Petition (Paper 1, “Pet.”), on April 17, 2023, we instituted an *inter partes* review of claims 1–20 of U.S. Patent No. 10,284,526 B2 (“the ’526 patent”). Paper 9 (“Dec. to Inst.”). Patent Owner filed a Patent Owner Response (Paper 13, “PO Resp.”), Petitioner filed a Petitioner Reply (Paper 18, “Pet. Reply”), Patent Owner filed a Patent Owner Sur-reply (Paper 21, “PO Sur-reply”), and a transcript of an oral hearing held on January 10, 2024 (Paper 26, “Hrg. Tr.”) has been entered into the record.

We have jurisdiction under 35 U.S.C. § 6. This Final Written Decision is issued pursuant to 35 U.S.C. § 318(a). We base our decision on the preponderance of the evidence. 35 U.S.C. § 316(e) (2018); 37 C.F.R. § 42.1(d) (2023).

Having reviewed the arguments of the parties and the supporting evidence, we conclude that Petitioner has demonstrated by a preponderance of the evidence that the challenged claims are unpatentable.

II. THE ’526 PATENT

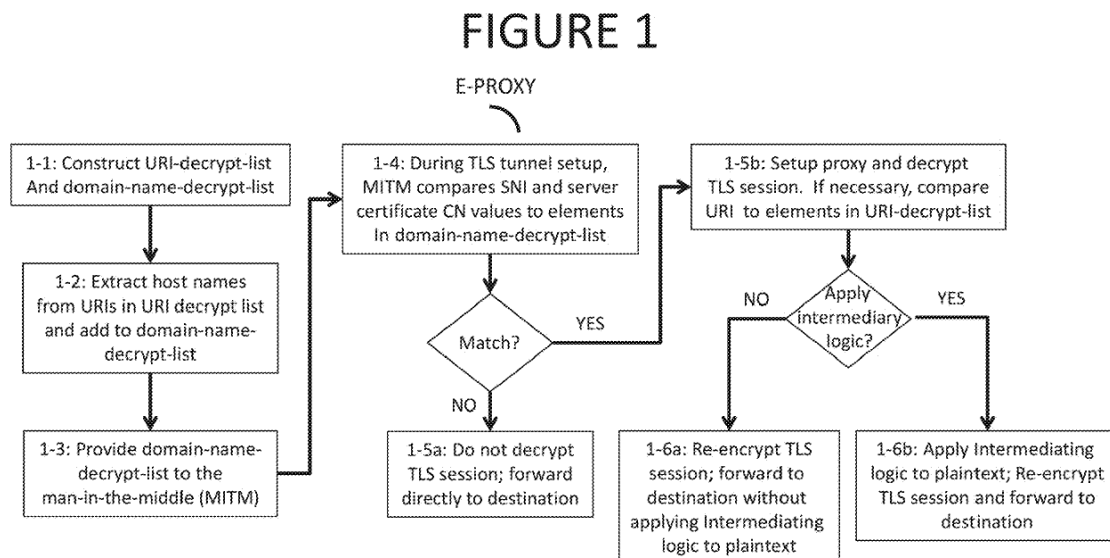
The ’526 patent issued May 7, 2019 from U.S. Patent Application No. 16/039,896, filed July 19, 2018, claiming the benefit of U.S. Provisional Patent Application No. 62/536,254, filed July 24, 2017. Ex. 1001, codes (21), (22), (45), (60), 1:6–9.

The ’526 patent describes a proxy for encrypted communications using the Secure Sockets Layer (SSL) or Transport Layer Security (TLS) protocol. Ex. 1001, code (57), 1:21–42, 1:53–2:43. According to the ’526 patent, a proxy may act as an intermediating agent for clients and servers of a network application. *Id.* at 8:5–7. For example, a web proxy may

intermediate HTTP (Hyper-Text Transfer Protocol) communication sessions between web clients and web servers. *Id.* at 8:7–8. In another example, an SSL/TLS proxy may intermediate HTTPS (Secure Hyper-Text Transfer Protocol) communication sessions between web clients and web servers encrypted by the SSL or TLS protocol. *Id.* at 8:9–10.

According to the '526 patent, an SSL/TLS proxy may intercept and decrypt an in-transit encrypted communication in order to inspect the communication's plaintext and take some action based on the plaintext content. *Id.* at 1:31–35. Typically, a conventional SSL/TLS proxy decrypts all SSL/TLS communications passing through the proxy. *Id.* at 1:35–37. The '526 patent purports to disclose an efficient SSL/TLS proxy that selectively decrypts SSL/TLS communications. *Id.* at 1:53–54.

Figure 1 of the '526 patent, reproduced below, depicts a flowchart of an exemplary operation of an efficient SSL/TLS proxy. Ex. 1001, 2:55–56, 5:44–46.



Id. Fig. 1. In Step 1-1 of Figure 1, an efficient SSL/TLS proxy constructs lists of identification data. *Id.* at 5:55–57. For example, the proxy may

construct a first list, called the “URI-decrypt-list,” of Uniform Resource Identifiers (URIs) such that, for any HTTPS sessions connecting with a URI address in the URI-decrypt-list, the HTTPS session will be decrypted. *Id.* at 5:57–61. The proxy may construct a second list, called the “domain-name-decrypt-list,” of domain names such that, for any HTTPS sessions connecting with a host whose name is in the domain-name-decrypt-list, the HTTPS session will be decrypted, whereas HTTPS sessions with hosts that are not in the domain-name-decrypt-list will not be decrypted. *Id.* at 5:61–67.

In Step 1-2, for each URI in the URI-decrypt-list, the proxy extracts the host name value, which may comprise a domain name for the host (called Fully Qualified Domain Name (FQDN)) or an IP address in the URI, and adds the extracted name values to the domain-name-decrypt-list. *Id.* at 6:1–4. In Step 1-3, the proxy provides the domain-name-decrypt-list to its agent device called “man-in-the-middle” (MITM), which observes and may act upon all network traffic on a link that transports HTTPS sessions between endpoints, e.g., HTTPS clients and HTTPS servers. *Id.* at 6:12–17.

In Step 1-4, the MITM agent compares the server’s FQDN value to the elements in the domain-name-decrypt-list. *Id.* at 6:40–42. If there is not a match or sufficient correspondence, then in Step 1-5a the MITM agent does not decrypt the session, thereby saving computational resources and possibly enforcing policies, such as privacy protection policies. *Id.* at 6:42–46. If there is a match or sufficient correspondence, then in Step 1-5b the agent may set up and use an SSL/TLS proxy function to (a) decrypt the HTTPS session and (b) inspect the plaintext of the HTTPS session. *Id.* at 6:46–50.

In Step 1-6*b*, the agent may apply some intermediating logic to the session's plaintext. *Id.* at 6:60–62. The intermediating logic may, for example, take some action on the session specified by a higher-level application (e.g., cybersecurity, privacy protection, law enforcement), such as blocking the communication, allowing the communication to proceed but logging and capturing the plaintext packets from the communication, or applying some transformation to the plaintext. *Id.* at 6:62–7:1. If the communication is not blocked by the intermediating logic, then the plaintext packets are re-encrypted and forwarded to the destination. *Id.* at 7:1–4.

III. ILLUSTRATIVE CLAIMS

Claims 1 and 11 are independent. Claim 1, drawn to a method, is illustrative of the challenged claims and is reproduced below with paragraph designations used by Petitioner (Pet. 17–24, 49–57).

1. 1[a] A method comprising:
 - 1[b] storing, by a computing device, a list of identification data and at least one corresponding action to perform on encrypted communication flows associated with corresponding identification data;
 - 1[c] receiving, by the computing device, one or more packets initiating at least one encrypted communication flow;
 - 1[d] identifying, by the computing device, flow identification data associated with the one or more packets initiating the at least one encrypted communication flow;
 - 1[e] comparing, by the computing device, the identified flow identification data with the list of the identification data; and
 - 1[f] decrypting, by the computing device and based on the comparing resulting in a match with data of the list, each packet of an encrypted communication flow associated with the match with data of the list and performing a corresponding action on each packet of the encrypted

communication flow associated with the match with data of the list; and

1[g] re-encrypting, after performing the corresponding action, each packet of the encrypted communication flow associated with the match with data of the list and transmitting each packet of the encrypted communication flow to its intended destination.

Ex. 1001, 17:63–18:21.

Claim 11 is drawn to an apparatus comprising a processor and memory storing instructions that performs substantially the same steps as those recited in method claim 1. *Id.* at 19:37–64.

IV. GROUNDS OF INSTITUTION

A. Prior Art and Asserted Grounds

We instituted trial on all of Petitioner’s grounds asserting that claims 1–20 would have been unpatentable as follows:

Claim(s) Challenged	35 U.S.C. §¹	Basis
1–4, 6–14, 16–20	102	IPUG ²
1–20	103	IPUG
1–6, 8–16, 18–20	102	Altman ³
1–6, 8–16, 18–20	103	Altman, CP ⁴
7, 17	103	Altman, IPUG

¹ The Leahy-Smith America Invents Act, Pub. L. No. 112-29, 125 Stat. 284 (2011), amended 35 U.S.C. §§ 102 and 103 effective March 16, 2013. Because the ’526 patent has an effective filing date after the effective date of the applicable AIA amendments, we refer to the AIA versions of §§ 102 and 103.

² Cisco IronPort AsyncOS 7.1 for Web User Guide, Nov. 2010 (Ex. 1008).

³ U.S. Patent Application Pub. No. 2012/0290829 A1, published Nov. 15, 2012 (Ex. 1005).

⁴ U.S. Patent Application Pub. No. 2015/0121449 A1, published Apr. 30, 2015 (Ex. 1006).

Dec. to Inst. 62.

B. Testimonial Evidence

Petitioner cites the Declaration of Dr. Atul Prakash (Ex. 1002, “Prakash Decl.”) and the Transcript of the Deposition of Dr. Michael Goodrich (Ex. 1014, “Goodrich Tr.”).

Patent Owner cites the Declaration of Dr. Michael T. Goodrich in Support of Patent Owner’s Preliminary Response (Ex. 2001, “Goodrich Decl. I”), and the Declaration of Dr. Michael T. Goodrich in Support of Patent Owner’s Response (Ex. 2002, “Goodrich Decl. II”). Patent Owner also cites the Transcript of the Deposition of Dr. Atul Prakash (Ex. 2003, “Prakash Tr.”).

V. CLAIM CONSTRUCTION

A. Claim Construction Standards

We interpret claim terms using “the same claim construction standard that would be used to construe the claim in a civil action under 35 U.S.C. 282(b).” 37 C.F.R. § 42.100(b). In this context, claim terms “are generally given their ordinary and customary meaning” as understood by a person of ordinary skill in the art in question at the time of the invention. *Phillips v. AWH Corp.*, 415 F.3d 1303, 1312–13 (Fed. Cir. 2005) (citations omitted) (en banc). “In determining the meaning of the disputed claim limitation, we look principally to the intrinsic evidence of record, examining the claim language itself, the written description, and the prosecution history, if in evidence.” *DePuy Spine, Inc. v. Medtronic Sofamor Danek, Inc.*, 469 F.3d 1005, 1014 (Fed. Cir. 2006) (citing *Phillips*, 415 F.3d at 1312–17). Extrinsic evidence is “less significant than the intrinsic record in determining ‘the legally operative meaning of claim language.’” *Phillips*,

415 F.3d at 1317 (citations omitted). Any special definition for a claim term must be set forth in the specification with reasonable clarity, deliberateness, and precision. *In re Paulsen*, 30 F.3d 1475, 1480 (Fed. Cir. 1994).

Prior to institution, neither Petitioner nor Patent Owner proposed any specific construction, other than plain and ordinary meaning, for any of the terms in the claims of the '526 patent. Dec. to Inst. 10–11 (citing Pet. 9–10; Prelim. Resp. 6). After institution, Patent Owner proposed explicit constructions for the claim terms that we address below. PO Resp. 7–19.

B. Performing a Corresponding Action

The Decision to Institute noted that Patent Owner's substantive arguments implied that "performing a corresponding action" in independent claims 1 and 11 requires some action, other than allowing a communication, such as "logging and capturing plaintext packets or some additional transformation of the plaintext when traffic is allowed." *Id.* at 24–26 (citing Pet. 23; Prelim. Resp. 23–24). The Patent Owner Response explicitly states "[t]he parties' dispute reduces down to whether the claimed 'performing a corresponding action' is satisfied by the mere transmission of re-encrypted packets to the intended destination, as taught by IPUG's *allow* feature." PO Resp. 7.

Patent Owner contends "'performing a corresponding action' should be construed to require that some action be performed in the plaintext packets after the packets have been decrypted and before the packets are re-encrypted." *Id.* Patent Owner further contends that the '526 patent describes logging and capturing or transforming the plaintext as an example of a "corresponding action" and does not limit the corresponding action to any particular action or actions. *Id.* at 10–11.

Patent Owner summarizes claim 1 as “requir[ing] four things to happen to a packet, in order 1) decrypting, 2) performing a corresponding action, 3) re-encrypting, and 4) transmitting.” *Id.* at 8–9 (citing Ex. 1001, claim 1; Ex. 2002, Goodrich Decl. II ¶ 40). According to Patent Owner, the ’526 patent discloses, but does not claim, a method in which plaintext packets are merely encrypted and transmitted; instead, the ’526 patent claims a method in which “additional corresponding action, described as ‘intermediate logic’ is performed on decrypted packets.” *Id.* at 9 (citing Ex. 1001, Fig. 1, 6:40–42, 6:46–62; Ex. 2002, Goodrich Decl. II ¶ 40).

Figure 1 of the ’526 patent, as annotated by Patent Owner, is reproduced below,

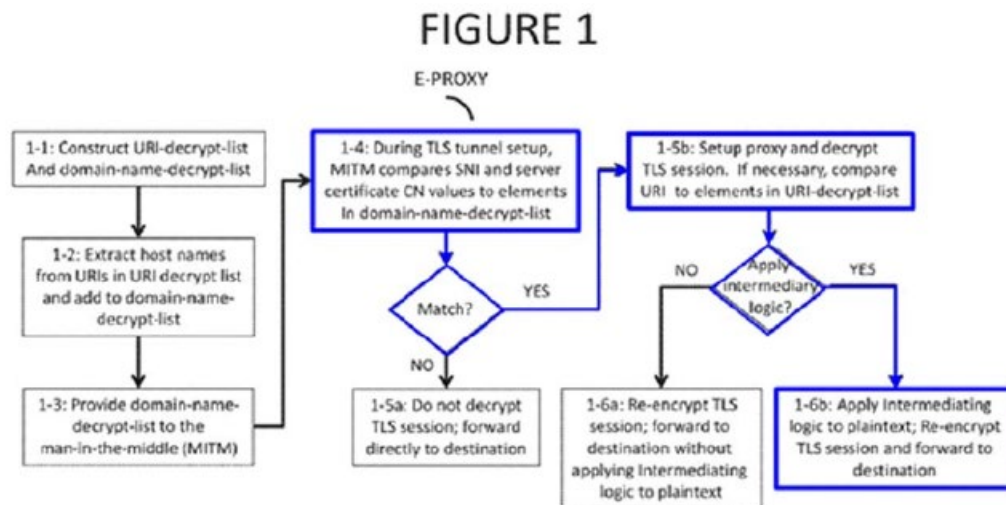


Figure 1 of the ’526 Patent as Annotated by Patent Owner

PO Sur-reply 5. Referring to its annotated Figure 1, Patent Owner argues that in step 1-5b, the proxy decrypts the encrypted session, inspects the plaintext and, based on a comparison of the plaintext to a policy, determines whether to apply intermediary logic to the session. *Id.*; see limitation 1[e]. After applying the policy, if there is no match, the packets are allowed, but if there is a match, the proxy applies intermediary logic that may take some

action on the packets comprising the session before re-encrypting the session and forwarding the packet to its destination. *Id.* at 5–6 (referencing step 1-6b in annotated Figure 1). Patent Owner contends that the “corresponding action” is performed on the packets of the claimed encrypted communication flow, i.e., the plaintext packets that are generated by the decrypting in the first part of limitation 1[f] and are not limited to encrypted packets. *Id.* at 12–13 (citing Ex. 2002, Goodrich Decl. II ¶ 44; Ex. 2003, Prakash Tr. 29:3–8 (acknowledging that “for this particular claim element, the corresponding action is performed right after decrypting”)).

Limitation 1[f] recites “decrypting . . . each packet of an encrypted communication flow” and “performing a corresponding action on each packet of the encrypted communication flow.” Ex. 1001, 18:10–16. Limitation 1[g] recites “re-encrypting, after performing the corresponding action, each packet . . . and transmitting each packet.” *Id.* at 18:17. Based on this language, we agree with Patent Owner that the claimed corresponding action is performed after decryption and before re-encryption and transmission, as recited in limitations 1[f] and 1[g].

Petitioner contends that, based on the Patent Owner’s Response, there is no claim construction dispute. Pet. Reply 4 (citing PO Resp. 11 as arguing Patent Owner does not attempt to limit the corresponding action to any particular action or actions). According to Petitioner, “because Patent Owner has abandoned any argument that ‘corresponding action’ is limited to specific examples from the specification” and “expressly states that its construction of ‘performing a corresponding action’ is ‘performing an action on packets after decryption,’ . . . there is no need for the Board to adopt an express claim construction for this term.” Pet. Reply 4–5 (citing PO Resp. 7).

The '526 patent Specification states:

If there is a match . . . the agent may apply some intermediate logic to the session's plaintext. The intermediate logic may, for example, take some action on the session specified by the higher-level application (e.g., cybersecurity, privacy protection, law enforcement), such as blocking the communication; or allowing the communication to proceed but logging and capturing the plaintext packets comprising the communication; or applying some transformation to the plaintext. If the communication is not blocked by the intermediate logic, then the plaintext packets are re-encrypted and forwarded to the destination.

Ex. 1001, 6:59–7:4. As the Specification describes the actions the intermediate logic may take as alternatives and examples, we agree with both Petitioner and Patent Owner that the term “performing a corresponding action on each packet of the encrypted communication flow associated with the match with data on the list” is not limited to the enumerated examples.

We now turn to the remaining question, i.e., whether merely allowing a packet, i.e., without performing any other transformative action on the packet, constitutes “performing a corresponding action” in the context of the '526 patent claims. As discussed above, Patent Owner contends that “performing a corresponding action on each packet,” as claimed, requires some action other than allowing the packet. The substantive arguments in the Petition indicate that Petitioner takes the opposite view. *See* Pet. 23 (arguing that IPUG “in step 3 appl[ies] an action to each packet” and that “the corresponding action depends on the application of an Access Policy, which can include block, allow, or redirect”).

Claim 1 recites that, based on comparing flow identification data with a list of identification data, a packet associated with a match is decrypted and a “corresponding action” is taken on the decrypted packet associated

with the match. *See* Ex. 1001, 18:6–16. Although the action is performed as a result of a match, the claim does not limit the action itself, i.e., any action is a “corresponding action” as long as that action is “associated with the match [of the] data on the list.” *Id.* at 18:13–16. Both parties agree that the examples of such actions in the Specification are exemplary and not limiting. *See, e.g.*, PO Resp. 11 (“[Patent Owner] did not (and does not) attempt to limit the ‘corresponding action’ to any particular action or actions.”). The ’526 patent explicitly describes “blocking” a communication as an “action.” *Id.* at 6:61–66. As “allowing” a packet is the opposite of “blocking” a packet, in the context of the ’526 patent, “allowing” a packet also constitutes an “action.”

Nevertheless, Patent Owner attempts to exclude allowing a packet from the scope of the claimed corresponding action by arguing that the differentiation between claim elements requires construing “performing a corresponding action” to mean more than simply allowing the packets. PO Resp. 10–11 (citing Prelim. Resp. 2, 23–24); PO Sur-reply 5–7. Patent Owner states that other claim limitations, e.g., “comparing the identified flow data with the list of the identification data” (step 1[e]), are recited separately from “performing a corresponding action on each packet of the encrypted communication flow associated with the match data on the list.” PO Sur-reply 7. Patent Owner argues that, for this reason, a construction of “performing a corresponding action” in step 1[f] that does not require some action, other than re-encrypting and transmitting the packets, renders the limitations superfluous. *Id.* (arguing that different claim terms are presumed to have different scope, citing *CAE Screenplates Inc. v. Heinrich Fiedler GmbH*, 224 F.3d 1308, 1317 (Fed. Cir. 2000)).

Applying Patent Owner’s principles to claim 1 leads to a different result. In the ’526 patent claims, the action taken on a packet in step 1[f], e.g., blocking or allowing and logging a communication as discussed in the patent, or merely allowing a communication (the opposite of blocking a communication), is an action on a decrypted packet that corresponds to a “packet of the encrypted communication flow associated with the match with data of the list” (step 1[e]). As Patent Owner acknowledges, the claims do not limit those actions. Thus, the comparing of step 1[e] and the action of allowing the transmission taken in step 1[f] are of different scope. Similarly (and consistent with Patent Owner’s analysis), the further steps of re-encrypting and transmitting the packet in step 1[g] are taken “after performing the corresponding action,” e.g., after allowing the packet, and are presumed to be of different scope from the allowing action in step 1[f]. Ex. 1001, 18:17. Re-encrypting and transmitting a packet that was previously decrypted as matched against flow identification criteria and determined to meet criteria allowing the packet to be transmitted without some other action, are not superfluous steps. Thus, as used in the claims of the ’526 patent, we determine that a “corresponding action” includes any action, including the action of allowing a further transmission of a packet, without further action.

C. A Computing Device (Claim 1)/ A Processor (Claim 11)

Patent Owner contends that “[t]he plain claim language and Federal Circuit precedent dictate that there must be a single computing device capable of performing each of the recited steps.” PO Resp. 16–17 (citing *Convolve, Inc. v. Compaq Comput. Corp.*, 812 F.3d 1313, 1321 (Fed. Cir. 2016), and *Salazar v. AT&T Mobility LLC*, 64 F.4th 1311, 1317–18 (Fed. Cir. 2023)). As to claim 1, Patent Owner urges that we construe claim 1 to

mean “that each step performed by ‘the computing device’ must be performed by the same computing device.” *Id.* at 18. As to claim 11, Patent Owner contends that “claim 11 requires that the same processor (or set of processors within the apparatus) be capable of performing *each* step of the steps recited therein.” *Id.* at 19. Patent Owner does not explain the distinction between its proposed construction of claim 1, requiring that each step be performed by the same computing device, and its proposed construction of claim 11, requiring that the processor (or set of processors) merely be capable of performing each step of the claim.

We begin our analysis by noting that *Convolve* and *Salazar* addressed the issue of antecedent basis for subsequent limitations—not the question of whether “a computing device” as used in the claims was in some way limited to a particular structure. *See Convolve*, 812 F.3d at 1321 (finding “the processor” recited in claim limitations to have its antecedent in the preamble of a claim drawn to “a [u]ser interface for . . . working with a processor”); *see Salazar*, 64 F.4th at 1318 (noting the general rule that “a microprocessor” does not require there be only one microprocessor, but subsequent limitations referring back to said microprocessor in the context of a claim requiring “a processor” to perform several functions (i.e., generate, create, and retrieve) require that “the processor” be capable of performing each of the recited functions).

The terms “device” and “processor” are often deemed to be nonce words or verbal constructs that do not connote sufficiently definite structure. *Williamson v. Citrix Online, LLC*, 792 F.3d 1339, 1350–51 (Fed. Cir. 2015). Patent Owner does not point to any discussion in the ’526 patent of the structure of the computing device, and Patent Owner does not explicitly argue that the term “a computing device” should be construed as a means-

plus-function term, limited to the structure disclosed in the Specification and equivalents thereof.

The '526 patent Specification guides us as to how the term “computing device” should be understood. Referencing Figure 3, the Specification states “the specific system architecture and computing devices used may vary and are secondary to the functionality that they provide, but without departing from the scope of the disclosure. For example, one or more computing devices may be distributed across a network.” Ex. 1001, 9:4–10; *see also id.* at 17:45–49 (“[T]he various methods and acts may be operative across one or more computing devices and networks. The functionality may be distributed in any manner or may be located in a single computing device (e.g., a server, client computer, or the like.”).

Although the exact nature of Patent Owner’s argument is unclear, given the disclosure in the Specification that *one* or more computing devices may be distributed across a network, we do not limit the computing device recited in claim 1, or the processor (or, as noted by Patent Owner, a set of processors) recited in claim 11 to any particular structure.

VI. ANALYSIS OF PRIOR ART CHALLENGES

A. *Principles of Law*

“In an [*inter partes* review], the petitioner has the burden from the onset to show with particularity why the patent it challenges is unpatentable.” *Harmonic Inc. v. Avid Tech., Inc.*, 815 F.3d 1356, 1363 (Fed. Cir. 2016) (citing 35 U.S.C. § 312(a)(3) (requiring *inter partes* review petitions to identify “with particularity . . . the evidence that supports the grounds for the challenge to each claim”)). This burden of persuasion never shifts to Patent Owner. *See Dynamic Drinkware, LLC v. Nat’l Graphics*,

Inc., 800 F.3d 1375, 1378 (Fed. Cir. 2015) (discussing the burden of proof in *inter partes* review).

Anticipation is a question of fact, as is the question of what a prior art reference teaches. *In re NTP, Inc.*, 654 F.3d 1279, 1297 (Fed. Cir. 2011). “A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference.” *Verdegaal Bros. Inc., v. Union Oil Co.*, 814 F.2d 628, 631 (Fed. Cir. 1987); *see also Finisar Corp. v. DirecTV Grp., Inc.*, 523 F.3d 1323, 1334 (Fed. Cir. 2008) (to anticipate a patent claim under 35 U.S.C. § 102, “a single prior art reference must expressly or inherently disclose each claim limitation”). Moreover, “[b]ecause the hallmark of anticipation is prior invention, the prior art reference—in order to anticipate under 35 U.S.C. § 102—must not only disclose all elements of the claim within the four corners of the document, but must also disclose those elements ‘arranged as in the claim.’” *Net MoneyIN, Inc. v. VeriSign, Inc.*, 545 F.3d 1359, 1369 (Fed. Cir. 2008) (quoting *Connell v. Sears, Roebuck & Co.*, 722 F.2d 1542, 1548 (Fed. Cir. 1983)).

Whether a reference anticipates is assessed from the perspective of an ordinarily skilled artisan. *See Dayco Prods., Inc. v. Total Containment, Inc.*, 329 F.3d 1358, 1368 (Fed. Cir. 2003) (“[T]he dispositive question regarding anticipation [i]s whether one skilled in the art would reasonably understand or infer from the [prior art reference’s] teaching that every claim element was disclosed in that single reference.” (quoting *In re Baxter Travenol Labs.*, 952 F.2d 388, 390 (Fed. Cir. 1991))).

Additionally, “[u]nder the principles of inherency, if the prior art necessarily functions in accordance with, or includes, the claimed limitations, it anticipates.” *MEHL/Biophile Int’l Corp. v. Milgraum*, 192

F.3d 1362, 1365 (Fed. Cir. 1999) (citation omitted); *In re Cruciferous Sprout Litig.*, 301 F.3d 1343, 1349–50 (Fed. Cir. 2002).

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 ordinary skill in the art; and (4) objective evidence of nonobviousness. *Graham v. John Deere Co.*, 383 U.S. 1, 17–18 (1966).

Additionally, the obviousness inquiry typically requires an analysis of “whether there was an apparent reason to combine the known elements in the fashion claimed by the patent at issue.” *KSR Int’l Co. v. Teleflex Inc.*, 550 U.S. 398, 418 (2007) (citing *In re Kahn*, 441 F.3d 977, 988 (Fed. Cir. 2006) (requiring “articulated reasoning with some rational underpinning to support the legal conclusion of obviousness”)); see *In re Warsaw Orthopedic, Inc.*, 832 F.3d 1327, 1333 (Fed. Cir. 2016) (citing *DyStar Textilfarben GmbH & Co. Deutschland KG v. C.H. Patrick Co.*, 464 F.3d 1356, 1360 (Fed. Cir. 2006)).

An obviousness analysis “need not seek out precise teachings directed to the specific subject matter of the challenged claim, for a court can take account of the inferences and creative steps that a person of ordinary skill in the art would employ.” *KSR*, 550 U.S. at 418; accord *In re Translogic Tech., Inc.*, 504 F.3d 1249, 1259 (Fed. Cir. 2007). Petitioner cannot satisfy its burden of proving obviousness by employing “mere conclusory statements.” *In re Magnum Oil Tools Int’l, Ltd.*, 829 F.3d 1364, 1380 (Fed. Cir. 2016). Instead, Petitioner must articulate a reason why a person of ordinary skill in the art would have combined the prior art references. *In re NuVasive, Inc.*, 842 F.3d 1376, 1382 (Fed. Cir. 2016).

A reason to combine or modify the prior art may be found explicitly or implicitly in market forces; design incentives; the “interrelated teachings of multiple patents”; “any need or problem known in the field of endeavor at the time of invention and addressed by the patent”; and the background knowledge, creativity, and common sense of the person of ordinary skill. *Perfect Web Techs., Inc. v. InfoUSA, Inc.*, 587 F.3d 1324, 1328–29 (Fed. Cir. 2009) (quoting *KSR*, 550 U.S. at 418–21).

In determining whether a claim would have been obvious in light of the prior art, when in evidence, we consider any relevant objective evidence of non-obviousness. *See Graham*, 383 U.S. at 17. Notwithstanding what the teachings of the prior art would have suggested to one of ordinary skill in the art at the time of the invention, the totality of the evidence submitted, including objective evidence of non-obviousness, may lead to a conclusion that the challenged claims would not have been obvious to one of ordinary skill. *In re Piasecki*, 745 F.2d 1468, 1471–72 (Fed. Cir. 1984). Patent Owner does not present evidence of such objective considerations in this proceeding.

We analyze the asserted grounds of unpatentability in accordance with these principles to determine whether Petitioner has met its burden to prove unpatentability by a preponderance of the evidence.

B. Petitioner’s Contentions That IPUG Anticipates Claims 1–4, 6–14, and 16–20

1. IPUG (Ex. 1008)

a) Printed Publication Status Issues

Petitioner asserts that IPUG qualifies as a prior art printed publication because IPUG was “generally available and known to the relevant technical community more than one year before the earliest possible priority date of

the '526 Patent.” Pet. 13 (citing Ex. 1002, Prakash Decl. ¶¶ 127–135; Ex. 1010, 7–8, 17). In support of its contention, Petitioner submits the declaration of Nathaniel E. Frank-White, an administrator of the Internet Archive, which provides a service called the Wayback Machine. *See* Ex. 1010 (“Frank-White Declaration”). Citing this evidence, Petitioner contends that “the IPUG document itself was archived by the Internet Archive on October 10, 2013” (Pet. 13 (citing Ex. 1010, 17)) and that “the document was available on Cisco’s web site as indexed by the Internet Archive on March 1, 2017” (*id.* (citing Ex. 1010, 7–8)).

The determination of whether a document is a “printed publication” under 35 U.S.C. § 102 “involves a case-by-case inquiry into the facts and circumstances surrounding the reference’s disclosure to members of the public.” *In re Klopfenstein*, 380 F.3d 1345, 1350 (Fed. Cir. 2004). “Because there are many ways in which a reference may be disseminated to the interested public, ‘public accessibility’ has been called the touchstone in determining whether a reference constitutes a ‘printed publication’” *Jazz Pharm., Inc. v. Amneal Pharm., LLC*, 895 F.3d 1347, 1355 (Fed. Cir. 2018) (quoting *In re Hall*, 781 F.2d 897, 898–99 (Fed. Cir. 1986)).

The Federal Circuit has noted, “[e]xaminers use ‘The Wayback [M]achine’ as a source of information to determine when a Web reference was first made available to the public.” *Valve Corp. v. Ironburg Inventions Ltd.*, 8 F.4th 1364, 1374 (Fed. Cir. 2021) (quoting America Invents Act (AIA) Frequently Asked Questions, United States Patent and Trademark Office, available at https://www.uspto.gov/patents/laws/america-invents-act-aia/america-invents-act-aia-frequently-asked#type-browse-faqs_2998). In the same case, the Federal Circuit approved taking judicial notice of the contents of webpages available through the Wayback Machine “as facts that

can be accurately and readily determined from sources whose accuracy cannot reasonably be questioned.” *Valve*, 8 F.4th at 1374–75.

Patent Owner contends that Petitioner has not met its burden to establish by a preponderance of the evidence that IPUG was publicly accessible prior to the priority date of the ’526 patent. PO Resp. 24. Patent Owner disputes Petitioner’s reliance on the Wayback Machine as demonstrating the availability of the IPUG references on Cisco’s website arguing that Petitioner fails to shown the document was searchable or indexed in a meaningful way. *Id.* at 25 (citing *Blue Calypso, LLC v. Groupon, Inc.*, 815 F.3d 1331, 1349–50 (Fed. Cir. 2016); *Acceleration Bay, LLC v. Activision Blizzard Inc.*, 908 F.3d 765, 772–73 (Fed. Cir. 2018)). According to Patent Owner, there is no evidence that Cisco’s website was searchable or that any relevant search terms would have uncovered the IPUG document. *Id.* at 26.

Patent Owner’s emphasis on indexing is misplaced. In *Acceleration Bay*, the court affirmed the Board’s findings that the subject reference (Lin) was not meaningfully indexed because the website allowed a user to view a list of technical reports indexed only by author or year and its advanced search form was not reliable. *Acceleration Bay*, 908 F.3d at 773–74. In *Blue Calypso*, the court noted that there was no evidence a party could navigate from a university’s website concerning common subject matter to the reference itself, i.e., the personal webpage of Ratsimor. *Blue Calypso*, 815 F.3d at 1350. The facts of *Acceleration Bay* and *Blue Calypso* are distinguished from the present circumstances where Cisco’s networking products were well known to persons of ordinary skill and the reference is a page on Cisco’s own website.

The present circumstances are more akin to those in *Voter Verified, Inc. v. Premier Election Sols., Inc.*, 698 F.3d 1374, 1380 (Fed. Cir. 2012). In *Voter Verified*, the court addressed an article (Benson) posted to an on-line publication (Risks Digest) concerning the claimed subject matter (risks of computer automation), noting that Risks Digest was a prominent forum for discussing such technologies (over 100 articles relating to electronic on-line voting). *Voter Verified*, 698 F.3d at 1380–81. The article’s publication on a site interested persons of ordinary skill would have recognized as important “overcame the absence of evidence that the website at which the article was located was indexed and thereby findable by an internet search engine.” *See Blue Calypso*, 815 F.3d at 1349 (discussing *Voter Verified*); *Voter Verified*, 698 F.3d at 1380–81. In *Voter Verified* the court stated:

The Risks Digest website was undisputedly open to any internet user by the critical date. Whether or not the website itself had been indexed by 1999 (through search engines or otherwise), the uncontested evidence indicates that a person of ordinary skill interested in electronic voting would have been independently aware of the Risks Digest as a prominent forum for discussing such technologies. And upon accessing the Risks Digest website, such an interested researcher would have found the Benson article using that website’s own search functions and applying reasonable diligence. In short, the Benson article was publicly available by the critical date and therefore qualifies as a prior art “printed publication” under § 102(b).

Voter Verified, 698 F.3d at 1381. Dr. Prakash testified that a person of ordinary skill would have looked for product manuals and product descriptions concerning the relevant subject matter from other vendors in addition to Cisco, including BlueCoat, Sophos, Trend Micro, and Palo Alto Networks. Ex. 1002, Prakash Decl. ¶ 129.

We also note that IPUG states “[t]he *IronPort AsyncOS for Web User Guide* provides instructions for setting up, administering, and monitoring the IronPort Web Security appliance.” Ex. 1008, 27. Where a document’s “purpose is ‘dialogue with the intended audience,’ that purpose indicates public accessibility.” *Valve*, 8 F.4th at 1374 (quoting *Suffolk Techs., LLC v. AOL Inc.*, 752 F.3d 1358, 1365 (Fed. Cir. 2014)).

The IPUG document bears the date of November, 2010, on its title page, as well as a copyright date of 2010. Ex. 1008, 1–2; Ex. 1010, 18–19. Although Patent Owner argues the copyright date on the document is hearsay, we do not rely solely on the reference’s copyright notice. The Wayback Machine indicates IPUG was archived before the July 24, 2017 filing date of the provisional application from which the ’526 patent claims priority. Ex. 1001 (code 60), 1:6–9; Ex. 1010, Frank-White Decl. (Ex. A), 5 (Wayback Archive Page of Dec. 29, 2103 identifying IPUG as available on Cisco’s website as of Dec. 29, 2013), 6, 8 (Wayback Archive Page listing IPUG available on Cisco’s website on March 1, 2017), 11–12 (Wayback Archive Page of March 9, 2010 identifying IPUG product).

The March 9, 2010 Wayback Archive Page (1) identifies the Cisco IronPort Email Security Appliance and the Cisco IronPort Web Security Appliance, (2) describes the Cisco IronPort SenderBase network as comprising 120,000 contributing organizations with 5 billion daily queries, and (3) states that the IronPort SenderBase collects data on more than 30 percent of the world’s email and web traffic, more than 10 times larger than that of other monitoring systems. Ex. 1010, 11. Although we do not rely on these assertions for their truth or accuracy, we note that their suggestion of Cisco’s ubiquity in this subject area is consistent with Dr. Prakash’s testimony that a person of ordinary skill interested in the relevant subject

matter would have been prompted to look at Web Security Appliances on Cisco's website for examples of existing products, i.e., proxy appliances to control web access, including IronPort. Ex. 1002, Prakash Decl. ¶¶ 129–135, discussing an article by Jeff Hughes entitled “Proxy Appliances control Web Access” published on May 10, 2004 in Network World⁵; *see also*, Ex. 1007 (2010 article discussing SSL proxies); *see Valve*, 8 F.4th at 1374–76.

Patent Owner also contends that Petitioner has not demonstrated a person of ordinary skill would have had reason to delve sufficiently deep into Cisco's website to find the IPUG manual. *See, e.g.*, Hr'g Tr. 24:15–16 Patent Owner exaggerates the significance of Cisco's website structure. The Wayback Machine archive of past web pages identifies the address of the site that existed on the archive date, but does not itself describe how a user would have reached that site at that time. The archived site itself is more descriptive of how a user would have navigated to the specific page and, in this case, illustrates pages that are logically organized to facilitate user inquiry into the relevant subject matter. Ex. 1002, Prakash Decl.

¶¶ 132–135. As discussed above, a user would have had reason to navigate to Cisco's home page, to further investigate web security appliances and web proxy devices. *Id.* We are persuaded that, in order understand the capabilities of such products and how they operate, a reasonably diligent person of ordinary skill interested in this subject matter would have had reason to navigate through the site to pages with user guides for such appliances. *Id.*; *see also* Ex. 1010, Frank-White Decl. 5–8.

⁵Located on April 15, 2024 at <https://www.networkworld.com/article/883442/tech-primers-proxy-appliances-control-web-access.html>

Having considered the evidence and arguments of record, we determine the preponderance of the evidence demonstrates that, for purposes of this Decision, IPUG qualifies as a printed publication reference.

b) IPUG Disclosure

IPUG is a user guide for Cisco's Web Security appliance called "IronPort AsyncOS 7.1 for Web." Ex. 1008, 1, 27.⁶ IPUG describes that "[t]he Web Security appliance can act as a web proxy" if the Web Proxy feature is enabled by a user. *Id.* at 107. IPUG refers to the Web Proxy-enabled Web Security appliance simply as "Web Security appliance" at times. *See, e.g., id.* at 107–08; *see also id.* at 43. According to IPUG, the Web Proxy can monitor encrypted HTTPS traffic by decrypting it. *Id.* at 256.

Figure 10-4 of IPUG is reproduced below.

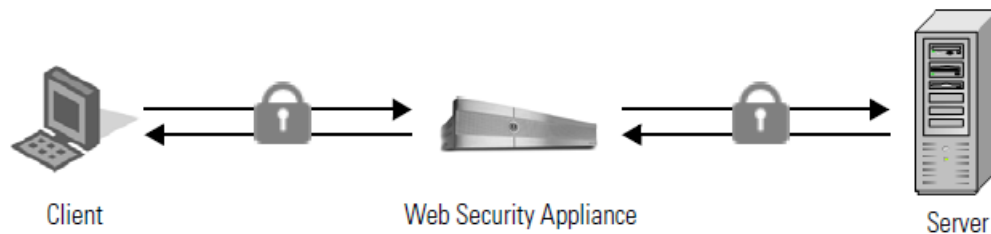


Figure 10-4 shows an HTTPS connection between a client and an HTTPS server that goes through the Web Security appliance. *Id.* at 267.

Figure 10-4 depicts the Web Security appliance acting as an intermediary (i.e., the "man in the middle") between the client and the server, intercepting the HTTPS connection to inspect the traffic between the client and the server. *Id.* IPUG describes that when acting as an intermediary for the HTTPS connection, the Web Security appliance (or the

⁶ The page numbers for Exhibit 1008 refer to the page numbers inserted by Petitioner in the bottom, right-hand corner of each page. *See* 37 C.F.R. § 42.63(d)(2).

Web Proxy) (1) receives encrypted data from the server (or the client), (2) decrypts the data, (3) applies access policies to the decrypted plain text data, (4) if the access policy allows the traffic, encrypts (i.e., re-encrypts) the data, and (5) sends the re-encrypted data to the client (or the server). *Id.* at 268–69.

When receiving encrypted communications, the Web Proxy applies decryption policies to determine whether “to decrypt or not to decrypt” the communication traffic. *Id.* at 164. Access Policies define how the Web Proxy handles HTTP and FTP requests and decrypted HTTPS connections for network users. *Id.* at 222. For an HTTP request or a decrypted HTTPS request, the Web Proxy can perform the following “actions”: monitor, allow, block, and redirect. *Id.* at 222–23. The allow, block, and redirect actions are called “final actions” because the Web Proxy stops comparing the transaction to control settings. *Id.* at 223. The monitor action is called an “intermediary action,” as the Web Proxy continues to compare the transaction to other control settings. *Id.* When a control setting matches “monitor” and the transaction is ultimately allowed, the Web Proxy logs the monitored setting in access logs. *Id.* at 224. In addition, access logs for decrypted HTTP transactions are saved to disk. *Id.* at 269.

2. *Claim 1*

a) *Preamble 1[a]*

The preamble of claim 1 recites “[a] method comprising.” Ex. 1001, 17:63. Petitioner asserts that, to the extent that the preamble is limiting, IPUG discloses a method. Pet. 17. Petitioner argues that “IPUG discloses the IronPort Web Security Appliance, which is an apparatus that performs

the specified methods using software.” *Id.* (citing Ex. 1008, 107⁷ (“A web proxy is a computer system or software The web proxy service monitors and controls traffic.”)). Patent Owner does not dispute that IPUG discloses claim 1’s preamble. We determine that Petitioner has demonstrated that IPUG discloses claim 1’s preamble.

b) Limitation 1[b]

Claim 1 recites “storing, by a computing device, a list of identification data and at least one corresponding action to perform on encrypted communication flows associated with corresponding identification data.” Ex. 1001, 17:64–67. Petitioner identifies this limitation as claim element 1[b]. Pet. 18.

Petitioner asserts that IPUG discloses element 1[b] because “[IPUG’s] Decryption Policies and Access Policies are lists of identification data and at least one corresponding action to perform on encrypted communication flows.” Pet. 18. According to Petitioner, Decryption Policies and Access Policies can make use of URL categories, which may include a list of sites defined by IP address, domain name, hostname, or partial hostname. *Id.* at 18–19 (citing Ex. 1008, 228, 288, 415; Ex. 1002 ¶¶ 155, 194–196). Petitioner argues that IP address, domain name, and hostname are all

⁷ Petitioner cites the original page numbers for IPUG throughout the Petition. Patent Owner in its Preliminary Response, on the other hand, used the page numbers inserted by Petitioner in the bottom-right corner of each page. To avoid confusion and because Exhibit 1008 is missing original page numbers on some pages, we directed the parties to use the page numbers inserted by Petitioner in the bottom, right-hand corner of each page of Exhibit 1008. Dec. to Inst. 19 (citing 37 C.F.R. § 42.63(d)(2)). Some citations do not comply with our direction. In those cases, we identify the citation to Exhibit 1008 by specifying the cited page numbers in accordance with our direction.

specific examples of “identification data” described in the ’526 patent. *Id.* at 19 (citing Ex. 1001, 2:7–10). Petitioner asserts, therefore, IPUG’s Decryption Policies and Access Policies include “a list of identification data.” *Id.*

Petitioner further contends that “IPUG discloses that both Decryption Policies and Access Policies are associated with a specific action to perform on communication flows associated with the identification information.” Pet. 19. For example, Petitioner asserts that IPUG Decryption Policies are associated with one of the actions “decrypt,” “pass through,” or “block” (*id.* (citing Ex. 1008, 257; Ex. 1002 ¶ 196)) and that IPUG Access Policies are associated with the actions “allow,” “block,” and “redirect” (*id.* (citing Ex. 1008, 223; Ex. 1002, Prakash Decl. ¶¶ 196, 225)).

In addition, Petitioner argues that IPUG discloses a computer system. Pet. 17 (citing Ex. 1008, 107 (“A web proxy is a computer system or software The Web Security appliance can act as a web proxy”)).

Patent Owner does not dispute that IPUG discloses claim limitation 1[b]. We determine that Petitioner has demonstrated that IPUG discloses this limitation.

c) Limitation 1[c]

Claim 1 recites “receiving, by the computing device, one or more packets initiating at least one encrypted communication flow.” Ex. 1001, 18:1–2. Petitioner identifies this limitation as claim element 1[c]. Pet. 19.

Petitioner asserts that IPUG discloses element 1[c] because IPUG discloses that the appliance acts as a “man-in-the-middle” HTTPS web proxy and that the appliance receives HTTPS requests in the form of packets. Pet. 20 (citing Ex. 1008, 107, 123; Ex. 1002 ¶ 202). Petitioner further argues “IPUG also discloses that an HTTPS request ‘initiates at least

one encrypted communication flow.” *Id.* (citing Ex. 1008, 262; Ex. 1002 ¶ 204).

Patent Owner does not dispute that IPUG discloses limitation 1[c].
We determine that IPUG discloses this limitation.

d) Limitation 1[d]

Claim 1 recites “identifying, by the computing device, flow identification data associated with the one or more packets initiating the at least one encrypted communication flow.” Ex. 1001, 18:3–5. Petitioner identifies this limitation as claim element 1[d]. Pet. 20.

Petitioner contends that IPUG discloses element 1[d] because “IPUG expressly discloses that the appliance utilizes specific information from an HTTPS request (the packets initiating the at least one encrypted communication flow) to create an ‘identity’ for the request.” Pet. 20 (citing Ex. 1008, 186 (“When a client sends a request to a server, the Web Proxy receives the request, evaluates it, and determines to which Identity group it belongs.”); Ex. 1002 ¶ 215). Petitioner further asserts “IPUG discloses that the identification data extracted from the HTTPS request includes a URL category, which is determined by the IP address and hostname of the destination for HTTPS connection.” *Id.* at 21 (citing Ex. 1008, 398; Ex. 1002 ¶ 215).

Patent Owner does not dispute that IPUG discloses limitation 1[d].
We determine that IPUG discloses this limitation.

e) Limitation 1[e]

Claim 1 recites “comparing, by the computing device, the identified flow identification data with the list of the identification data.” Ex. 1001, 18:6–8. Petitioner identifies this limitation as claim element 1[e]. Pet. 21.

Petitioner asserts that IPUG discloses element 1[e] because “IPUG [] discloses comparing the URL category (one example of the identified flow identification data) in both Decryption Policies and Access Policies.” Pet. 22 (citing Ex. 1008, 226, 283; Ex. 1002 ¶¶ 220–222). Petitioner further argues that IPUG also discloses comparing the IP address directly with the request in connection with Bypass Lists. *Id.* (citing Ex. 1008, 123; Ex. 1002 ¶ 210).

Patent Owner does not dispute that IPUG discloses limitation 1[e]. We determine that IPUG discloses this limitation.

f) Limitations 1[f] and 1[g]

Limitation 1[f] recites

decrypting, by the computing device and based on the comparing resulting in a match with data of the list, each packet of an encrypted communication flow associated with the match with data of the list and performing a corresponding action on each packet of the encrypted communication flow associated with the match with data of the list; and

and limitation 1[g] recites

re-encrypting, after performing the corresponding action, each packet of the encrypted communication flow associated with the match with data of the list and transmitting each packet of the encrypted communication flow to its intended destination.

Ex. 1001, 18:9–20.

The Petition asserts that IPUG discloses elements 1[f] and 1[g] because IPUG discloses that when encrypted data in an HTTPS connection are received, the appliance (1) decrypts the received encrypted data, if the URL category (the claimed “identified flow identification data”) matches the data in the Decryption Policies, (2) applies the Access Policies to the decrypted plaintext traffic, (3) if the Access Policies allow the traffic,

encrypts (i.e., re-encrypts) data, and (4) sends the encrypted data to their intended destination. Pet. 23–24 (citing Ex. 1008, 257, 268–69; Ex. 1002 ¶¶ 224–229, 232–233).

The Petition notes that, after comparing the packet to the list, as recited in limitation 1[e], IPUG takes certain actions, i.e., IPUG allows the packet to pass, blocks the packet, or redirects the packet. Pet. 23 (citing Ex. 1008, 268–69; Ex. 1002, Prakash Decl. ¶ 226). As claim limitation 1[g] recites re-encrypting and transmitting the packet to its intended destination, the actions of blocking or redirecting the packet do not satisfy limitation 1[g]. The remaining question before us is whether, after completing the comparison recited in limitation 1[e], merely allowing a packet to be re-encrypted and transmitted to its destination, as taught by IPUG, is “performing a corresponding action” according to limitation 1[f].

According to Patent Owner “[t]he parties’ dispute reduces down to whether the claimed ‘performing a corresponding action’ is satisfied by the mere transmission of re-encrypted packets to the intended destination, as taught by IPUG’s *allow* feature.” PO Resp. 7; *see* Section V.B herein. Patent Owner states that “[w]hen IPUG applies the ‘allow’ function to a decrypted communication, it simply ‘permits the connection without interruption’ by re-encrypting and retransmitting the packets.” PO Resp. 35 (citing Ex. 1008, 222; Ex. 2003, Prakash Tr. 58:21–59:6). Patent Owner contends that “[p]ermitting a connection without interruption does not result in ‘performing a corresponding action on each packet,’” but instead “means *no* corresponding action is performed ‘on each packet.’” *Id.*

Patent Owner also contends that, notwithstanding Petitioner’s assertion there is no claim construction dispute, Petitioner’s Reply implies a new construction of the term “corresponding action performed on each

packet of the communication flow.” PO Sur-reply 3–4 (citing Pet. Reply 5–6, 12–14). According to Patent Owner, by arguing that IPUG’s application of its Access Policies discloses the claimed corresponding action, Petitioner applies a construction that is inconsistent with the ’526 patent Specification and claims. *Id.* at 6–7. Patent Owner states “the plain language of the claims further reinforces the conclusion that matching traffic against a list is not an action, let alone a corresponding action.” *Id.* at 7.

The Petition states “the corresponding action depends on the application of an Access Policy, which can include block, allow, or redirect.” Pet. 23 (citing Ex. 1008, 223; Ex. 1002 ¶ 228). Although it is unclear from the sentence whether Petitioner intended the phrase “which can include block, allow, or redirect” to modify the term “corresponding action” or “Access Policy,” the Petition explicitly states that “the corresponding action *depends on the application of* an Access Policy.” Pet. 23 (citing IPUG at 8-3 as teaching “actions allowed in Access Policy”; Ex. 1002 ¶ 228). The Petition does not assert that matching the traffic against the list is the corresponding action. Patent Owner acknowledges this position advanced in the Petition, stating “Petitioner recognized that the ‘action’ is not the application of the security policy itself, it is the action taken on the session as a result of applying the policy.” PO Sur-reply 7–8 (citing Pet. 23).

The Petitioner Reply takes the same position. Pet. Reply 5–6 (quoting pages 15 and 23 of the Petition). The Petitioner Reply reproduces the following five-step process disclosed in IPUG, which also appears on page 23 of the Petition:

After the two separate HTTPS connections are established, the following actions occur:

1. Encrypted data is received from the server.
2. The temporary, symmetric key negotiated with the server is used to decrypt the data.
3. Access Policies are applied to the decrypted traffic as if it were a plaintext HTTP connection. For more information about Access Policies, see [Access Policies, page 8-1](#).
4. Assuming the Access Policy group allows the client to receive the data, the data is encrypted using the temporary, symmetric key negotiated with the client.
5. Encrypted data is sent to the client.

Pet. Reply 6 (citing Ex. 1008, 268–269). The above five-step process specifies actions that occur after the two separate HTTPS connections are established.

The Petitioner Reply states “IPUG discloses in the third step applying the access policy, which results in the decision to block, allow or redirect.” *Id.* Thus, the Petition and the Petitioner Reply are consistent in their assertion that applying the policy (limitation 1[e]) generates a decision that causes the system to perform a corresponding action (limitation 1[f]).

As we discussed in our claim construction analysis, there is no limit on the scope of the corresponding action that is performed after completing the comparison recited in limitation 1[e]—thus blocking, redirecting, or allowing the packet (with or without logging it or taking any other action) are corresponding actions, as recited in limitation 1[f].

Re-encrypting and transmitting in IPUG corresponds to limitation 1[g]. Thus, we determine that, because Petitioner has demonstrated IPUG discloses all the limitations recited in claim 1, IPUG anticipates claim 1.

3. *Claim 11*

Claim 11 is drawn to an apparatus comprising a processor and a memory storing instructions for performing substantially the same steps as those recited in method claim 1. *Id.* at 19:37–64. Petitioner contends that IPUG anticipates claim 11 for the same reasons IPUG anticipates claim 1. Pet. 17–24. Patent Owner does not advance separate arguments addressed to claim 11. We agree with Petitioner that, in substance, claims 1 and 11 are of similar scope. For the same reasons as those discussed above with respect to claim 1, we determine that Petitioner has demonstrated IPUG discloses all the limitations of claim 11.

4. *Claims 2–4 and 12–14*

Claims 2 and 12 depend from claims 1 and 11, respectively, and recite the computing device (or processor) creating the list of identification data (recited in claim 1) based on a list of network address and domain names the computing device (or processor) receives from a security application. Ex. 1001, 18:22–28, 19:65–20:5. Petitioner cites IPUG as disclosing the use of Web Reputation Filters in connection with Decryption Policies and Access Policies to determine an action based on a received web reputation score. Pet. 25–26.

IPUG’s Web Reputation Filters function as “a security filter that analyzes web server behavior and assigns a reputation score to a URL to determine the likelihood that it contains URL-based malware.” Ex. 1008, 469; *see id.* at 103. Petitioner contends IPUG discloses “receiving . . . a list of one or more network addresses and/or domain names,” as claimed, because “IPUG discloses that the appliance (the computing device / the apparatus) receives [a] list of one or more network addresses or domain names associated with a reputation score from a security application.” Pet.

25 (citing Ex. 1008, 470; Ex. 1002, Prakash Decl. ¶ 250). According to Petitioner, IPUG’s Decryption Policies and Access Policies use Web Reputation Filters—which involve a list of URLs associated with a particular reputation score (*id.* (citing Ex. 1008, 469, 472; Ex. 1002 ¶¶ 237–241))—and “[t]he web reputation filtering component periodically receives updates to its database tables from the IronPort update server” (*id.* (quoting Ex. 1008, 470)). Petitioner further argues that IPUG discloses “creating the list of the identification data based on the received list of [] network addresses and/or domain names” because “IPUG discloses creating a list of identification data (sites) with corresponding actions (the action associated with their specific web reputation score).” Pet. 26 (citing Ex. 1002 ¶¶ 248–249).

In his Declaration, Dr. Prakash states that Figure 10-9 of IPUG “shows two different decision points that involve the web reputation score of the destination server. The web reputation score of the server is evaluated only once, but the result is applied at two different points in the decision flow.” Ex. 1002, Prakash Decl. ¶¶ 247–249. Petitioner and Dr. Prakash rely on the second instance of applying the web reputation score shown near the bottom of Figure 10-9, i.e., the step labeled “Does the reputation score of the destination server indicate pass through or decrypt the connection?” Dr. Prakash testifies that this step “corresponds to confirming that the IP address of the destination server in the HTTPS request matches with a reputation score.” Ex. 1002, Prakash Decl. ¶ 248. Dr. Prakash further states that “IPUG discloses that the appliance maintains a local database of web reputations, whose tables are updated from the update server. The items in this local database constitute a list of identification data.” *Id.* ¶ 249. Thus, according to Dr. Prakash, “IPUG discloses creating a list of identification

data based on the received list so that an incoming HTTPS request can be matched against the list as illustrated in IPUG Figure 10-9.” *Id.* ¶ 247.

Patent Owner contends that Decryption Policies and Access Policies are not created using Web Reputation Filters, but are generated manually by an administrator. PO Resp. 38–39 (citing Ex. 1008, 227; Pet. 26 (noting that the IPU administrator can configure Web Reputation Filter thresholds for each policy group)). Patent Owner further argues that in IPUG, although the administrator may set a range for a web reputation score in a Decryption or Access Policy, the administrator’s action is not based on any received list of domain names. *Id.* at 39 (citing Ex. 2002, Goodrich Decl. II ¶ 68; Ex. 1008, 232, 474–75). Arguing that the ’526 patent differentiates lists input by a user from a “received list” from a subscription service, Patent Owner contends that neither IPUG’s Access nor its Decryption Policies are created based on the Web Reputation Filter, let alone a received list of domain names involved with the filter. *Id.* at 40. Instead, according to Patent Owner, the Web Reputation Filter is merely a selectable setting within an Access or Decryption Policy that an administrator sets to a range of reputation values to allow, scan, or block. *Id.* (citing Ex. 1008, 471–72, 474–75; Ex. 2002, Goodrich Decl. II ¶ 73). According to Patent Owner, the Web Reputation Filter is based on a numeric value, i.e., the Web Reputation Score, rather than a network address or domain name. *Id.* Patent Owner notes that the Petition relies on a match of a URL Category within the Access Policy and Decryption Policy. *Id.* (citing Pet. 22). Patent Owner contends that to be consistent with its mapping of claim limitation 1[e], the list of identification data that is created from a received list of domain names in limitation 2[c], must include the same URL Category, but the Petition

does not mention this URL category in its analysis of claim 2–4 and 12–14. *Id.* at 41 (citing Pet. 22).

These arguments by Patent Owner are unavailing. We see no inconsistency in Petitioner’s arguments concerning limitations 1[e] and 2[c] as limitation 1[e] (“comparing, by the computing device, the identified flow identification data with the list of identification data”) does not recite the source of the identification data or specific categories of URLs. The Petition refers to URL category as “one example of identified flow identification data in both Decryption and Access Policies.” Pet. 22. The Petition cites IPUG’s disclosure that “[t]he proxy bypass list works by **matching the IP addresses of the request** [flow identification data] **to an IP address in the proxy bypass list** [the list of identification data].” *Id.* (quoting Ex. 1008, 824 (emphasis by Petitioner)); *see* Ex. 1002, Prakash Decl. ¶ 210.

As to the limitations of claim 2, Petitioner notes that IPUG expressly discloses receiving and updating a list of network addresses or domain names corresponding to web reputation scores. Pet. Reply 15–16; *see* Ex. 1008, 469–70 (disclosing that (i) “[t]he Web Security appliance collects information and maintains a filtering database,” (ii) “periodically receives updates to its database tables from the IronPort update server,” (iii) “updates are automated and the update interval is set by the server as opposed to the appliance,” and (iv) “[u]pdates to database tables . . . require no administrator intervention”).

IPUG also discloses installing and setting up the Web Security appliance invokes “default settings for Web Reputation Scores” that one “can modify threshold settings for web reputation scoring” and “configure web reputation filter settings for each policy group.” Ex. 1008, 473–74 (describing how to edit reputation filter settings for an Access Policy group

“to change the range for URL block, scan, and allow actions”). Thus, although IPUG describes that an administrator can configure settings for Decryption Policies and Access Policies (*see* Pet. 26 (citing Ex. 1008, 474–75)), IPUG also discloses that the appliance creates Decryption Policies and Access Policies based on Web Reputation Filter settings, as configured by the administrator (Ex. 1008, 474–75; *see also id.* at 168 (describing Access Policies Table and Decryption Policies Table, both of which include Web Reputation Filters)). Having considered the arguments and evidence of record, we determine that Petitioner has demonstrated IPUG discloses the limitations of claim 2 and 12.

Claims 3 and 13 depend from claims 1 and 11, respectively, and recite creating the list of identification data based on a list of network addresses and/or domain names the computer device (or processor) receives via a subscription service. Ex. 1001, 18:30–33, 20:9–11. Claims 4 and 14 similarly recite receiving a list of network addresses and/or domain names from a privacy protection application. *Id.* at 18:45–47, 20:19–21.

Petitioner cites IPUG’s disclosure of a Web Proxy Appliance configured to participate and share data with a SenderBase Network. Pet. 27–28. Petitioner asserts that IPUG discloses that the Web Reputation Scores are received from the SenderBase Network, which Petitioner contends is a “cyber threat intelligence provider that provides intelligence on cyber threats associated with URLs, including IP addresses and domain names.” *Id.* at 27 (quoting Ex. 1008, 46) (citing Ex. 1002 ¶ 258). Petitioner further contends that the SenderBase Network is also a privacy protection application because “IPUG expressly discloses that the Web Reputation Filters, which make use of the Web Reputation score received from (or derived from) the SenderBase Network, ‘protect against URL-based

malware that threatens end-user privacy and sensitive corporate information.”” *Id.* at 30 (citing Ex. 1008, 469; Ex. 1002 ¶¶ 269–274). Citing the testimony of Dr. Prakash, Petitioner argues that the SenderBase Network is a subscription service because a person of ordinary skill in the art would understand that sharing data with the SenderBase Network and acceptance of a license agreement required by the SenderBase Network would constitute a subscription service. *Id.* at 28 (citing Ex. 1008, 47–48, 471; Ex. 1002 ¶¶ 259–262).

Patent Owner contends Petitioner failed to cite any disclosure in IPUG that establishes the SenderBase Network is a subscription service. PO Resp. 42. As Petitioner points out, however, there is no requirement for a prior art reference to use the identical language to disclose a claim limitation. Pet. Reply 17 (citing *ADASA Inc. v. Avery Dennison Corp.*, 55 F.4th 900, 913 (Fed. Cir. 2022)). IPUG explicitly describes levels of participation in the SenderBase Network available via the Web Security appliance as none, Basic - enabled by default, or Standard (enhanced participation). Ex. 1008, 47–48. One must agree to participate in the network by selecting a level of participation using the Security Services > SenderBase page. *Id.* at 48 (stating “[i]f you agree to participate in the SenderBase Network, data sent from your IronPort appliance is transferred via HTTPS. Sharing data improves IronPort’s ability to react to web-based threats and protect your corporate environment from malicious activity.”). We agree with Petitioner that IPUG describes a subscription service, at least because IPUG provides the Web Security appliance’s owner the ability to opt out or select a level of participation by providing information to SenderBase from which the Web Security appliance receives or derives Web Reputation scores. Having considered the arguments and evidence of record, we determine that

Petitioner has demonstrated that IPUG discloses the limitations of claim 3 and 13.

Claims 4 and 14 depend from claims 1 and 11, respectively, and recite creating the list of identification data based on the list of network addresses and/or domain names received from a privacy application. Ex. 1001, 18:37–43, 20:16–26. Petitioner notes that claims 4 and 14 are similar to claims 2 and 12, except that claims 4 and 14 recite receiving the list of network addresses and domain names from a “privacy” application, instead of a “security” application. Petitioner argues that IPUG expressly discloses Web Reputation Filters that make use of the Web Reputation score received from the SenderBase Network to “protect against URL-based malware that threatens privacy and sensitive corporate solutions.” Pet. 30 (citing Ex. 1008, 221; Ex. 1002, Prakash Decl. ¶¶ 269–274, 278–279). Petitioner further argues that, even if IPUG does not disclose the limitation expressly, it would have been obvious because the origin of the list received from the computing device would not alter the method or design of the apparatus, i.e., it would have been obvious to modify IPUG’s teaching to implement the receipt of the list of addresses from any source, without experimentation. *Id.* at 29–31. Having considered the arguments and evidence of record, we determine that Petitioner has demonstrated IPUG discloses the limitations of claim 4 and 14.

5. *Claims 6–10 and 16–20*

Claims 6 and 16 depend from claims 1 and 11, respectively, and recite forwarding the packets associated with a particular communication flow to their intended destinations wherein the plurality of packets are not decrypted prior to forwarding. Ex. 1001, 18:51–56, 20:34–41. Petitioner cites IPUG as disclosing Decryption Policies may be associated with actions that pass

through all encrypted information flows and the use of Bypass Lists that cause traffic streams to bypass the proxy server entirely. Pet. 34 (citing Ex. 1008, 10–31; Ex. 1002, Prakash Decl. ¶¶ 294–298). The Patent Owner Response does not respond explicitly to Petitioner’s contentions. We determine that Petitioner has cited sufficient evidence to demonstrate that IPUG discloses the limitations of these claims.

Claims 7 and 17 depend from claims 1 and 11, respectively, and recite the computing device receiving a first list of network addresses/domain names from which corresponding communication flows are to be decrypted and a second list of network addresses/domain names whose corresponding communication flows are not to be decrypted, assigning different priorities to the first and second lists, and creating identification data from the first and second lists. Ex. 1001, 18:57–19:13, 20:42–66. Petitioner cites IPUG as disclosing the creation of decryption policies that assign one or more URL categories the action of “decrypt,” i.e., the claimed first list, and one or more URL categories the action of “pass through,” the claimed second list, and the creation of a combined list (the final Decryption Table or Access Policy Table). Pet. 36–38 (citing Ex. 1008, 288, 413, 415; Ex. 1002, Prakash Decl. ¶¶ 300–314). Petitioner also cites IPUG as disclosing each policy group is required to have a different priority table. *Id.* at 38 (citing Ex. 1008, 281; Ex. 1002 ¶ 314). The Patent Owner Response does not respond explicitly to Petitioner’s contentions. We determine that Petitioner has cited sufficient evidence to demonstrate that IPUG discloses the limitations of these claims.

Claims 8 and 18 depend from claims 1 and 11, respectively, and recite, by comparing the identification flow data with the list of identification data, determining that the list of identification data does not comprise the identified flow identification data, and performing an action

other than the action indicated by the list of identification data. Ex. 1001, 19:14–26, 20:67–21:12. Petitioner cites IPUG’s disclosure of Bypass Lists and Decryption Policy Tables. Pet. 38–39 (citing Ex. 1008, 113, 257; Ex. 1002, Prakash Decl. ¶ 317). In the context of Bypass Lists, Petitioner notes IPUG’s disclosure that when identification data extracted for an HTTPS request does not match data on the proxy bypass list, the flow does not bypass the web proxy and is processed according to the decryption and access policies configured on the web proxy. *Id.* at 39–40 (citing Ex. 1008, 5–17; Ex. 1002, Prakash Decl. ¶¶ 319–323). Petitioner also notes that in the context of decryption policies and access tables, IPUG discloses a global policy applied when an HTTPS request does not match any specific policy groups, such that IPUG preforms an action specified by the global policy, i.e., an action other than the action associated with the identification data, when there is no match with the specific policy groups. *Id.* at 40 (citing Ex. 1008, 226, 283; Ex. 1002, Prakash Decl. ¶ 324). The Patent Owner Response does not respond explicitly to Petitioner’s contentions. We determine that Petitioner has cited sufficient evidence to demonstrate that IPUG discloses the limitations of these claims.

Claims 9 and 19 depend from claims 8 and 18, respectively, and recite that the action indicated by the list of identification data comprises terminating the encrypted communication flow. Ex. 1001, 18:27–29, 21:13–16. Petitioner cites IPUG’s disclosure of a global policy applied whenever an HTTPS request does not match a specific policy group as preforming an action, other than the action associated with the identification data (including drop and block actions) when there is no match. Pet. 41 (citing Ex. 1008, 226, 283; Ex. 1002, Prakash Decl. ¶ 329).

The Patent Owner Response does not respond explicitly to Petitioner's contentions. We determine that Petitioner has cited sufficient evidence to demonstrate that IPUG discloses the limitations of these claims.

Claims 10 and 20 depend from claims 8 and 18, respectively, and recite the action indicated by the list comprises logging packets associated with the encrypted communication and forwarding the packets to their respective indicated destination. Ex. 1001, 18:30–36, 21:17–24. Petitioner cites IPUG as disclosing a packet capture facility that could be used by an administrator at any time for logging traffic to or from a specific address or all traffic if no IP address was specified. Pet. 42 (citing Ex. 1008, 726–28; Ex. 1002, Prakash Decl. ¶¶ 332–335). The Patent Owner Response does not respond explicitly to Petitioner's contentions. We determine that Petitioner has cited sufficient evidence to demonstrate that IPUG discloses the limitations of these claims.

6. Conclusion

Having reviewed the arguments and evidence of record, we determine that Petitioner has demonstrated that IPUG is a prior art reference and that all the limitations of claims 1–4, 6–14, and 16–20 are disclosed by IPUG. Thus, we determine that Petitioner has shown by a preponderance of the evidence that claims 1–4, 6–14, and 16–20 are anticipated by IPUG.

C. Petitioner's Contentions That Claims 1–20 Would Have Been Obvious over IPUG

1. Claims 1–4, 6–14, and 16–20

As to claims 1–4, 6–14, and 16–20, Patent Owner argues that, because Petitioner has not separately “explained why a [person of ordinary skill] would have found it obvious to modify IPUG to reach the Challenged Claims, the obviousness arguments rise and fall with the anticipation

argument.” PO Resp. 43. Referencing its response to Petitioner’s anticipation arguments, Patent Owner again argues that Decryption Policies of Access in IPUG are not created based on Web Reputation Filters and that Petitioner’s analysis of the dependent claims contradicts its positions on the independent claims that rely on a match to a URL Category. *Id.* at 45–46. We addressed these arguments in our analysis of Petitioner’s anticipation challenge and determined Petitioner had demonstrated the claimed limitations are disclosed by IPUG. *See* Section VI.B herein.

2. *Claims 5 and 15*

Claims 5 and 15 recite the list of identification data of network addresses and/or domain names is received from a law enforcement wiretapping application. Ex. 1001, 18:44–50, 20:25–33. Petitioner notes that claims 5 and 15 are similar to claims 2 and 12, which recite that the list of identification data is received from a security application. Pet. 31; Ex. 1001, 18:22–28, 19:65–20:5. Petitioner contends that a person of ordinary skill would have understood that a law enforcement application could provide the list because the source of the list would not in any way change the design of the computing apparatus. Pet. 31–32 (citing Ex. 1002, Prakash Decl. ¶¶ 278–279). Patent Owner asserts that “Petitioner’s proposed modification of the origin or source of the list does not cure the failure to show that IPUG teaches all of the elements of claims 1 and 11,” (PO Resp. 45–46), but we do not find those arguments to be availing, per our discussion of IPUG above. *See* Section VI.B herein. We agree with Petitioner that a person of ordinary skill would have understood a wiretapping law enforcement application could be used to provide the requisite list of networks addresses and domain names, as a law enforcement wiretapping application is merely a type of security application.

3. Conclusion

We determine that, because Petitioner has demonstrated that IPUG teaches or suggests all the limitations of claims 1–4, 6–14, and 16–20 as well as claims 5 and 15 to a person of ordinary skill, as discussed above, Petitioner has demonstrated by a preponderance of the evidence that claims 1–20 are unpatentable as obvious over IPUG.

D. Petitioner’s Contentions That Claims 1–6, 8–16 and 18–20 Are Anticipated by Altman and/or Obvious over Altman and CP

1. Altman (Ex. 1005)

Altman describes “methods and systems for inspection of encrypted network traffic.” Ex. 1005 ¶ 13. Altman discloses that

In an example embodiment, a Network Monitor Center (NMC) analyzes plain (unencrypted) data that relates to users of a communication network according to predefined analysis rules. Based on the analysis, the NMC dynamically establishes a list of rules for selection of encrypted data connections. For example, an analysis rule may specify a network access login-name the [sic] of a target user, and a resulting selection rule would specify a temporary IP address that the network allocates to the target user once he or she logs in to the network. The NMC provides this list, as a “rule table to a Secure data Inspection Appliance (SIA) and keeps updating this table upon changes in the list. The SIA accepts some or all of the network user encrypted traffic and checks it against the rule table. The SIA transfers transparently the encrypted connections that do not match the rule table. However, when detecting an encrypted connection that matches the rule table, the SIA decrypts the connection and provides a copy of the connection plain data to the NMC. The NMC then inspects the plain data for security threats. Once a security threat is found in a connection, the NMC applies predefined consequent actions to this connection.

Id. ¶ 14. Altman also discloses: “As an example [of the predefined consequent actions], sensitive information leaks, as well as malwares, can be

blocked. As another example, predefined information types that relate to target users may be copied and logged.” *Id.* ¶ 33.

Altman further describes that “the SIA functions as a Man In The Middle (MITM),” maintaining separate SSL/TLS connections between a client and a server, “while decrypting the encrypted data that it receives from each end party and re-encrypting it back-to-back toward the opposite party.” *Id.* ¶ 32. According to Altman, “[t]he SIA thus constitutes an SSL proxy for secure connections.” *Id.*

2. CP (Ex. 1006)

CP describes methods and systems for malicious application blocking in a network environment. Ex. 1006 ¶ 1. CP discloses that

Embodiments are configured to receive metadata of a process intercepted on an end host when attempting to access a network. The metadata includes a hash of an application associated with the process and an endpoint reputation score of the application. Embodiments are configured to request a threat intelligence reputation score based on the hash of the application, to determine an action to be taken by the end host based, at least in part, on one or more policies and at least one of the threat intelligence reputation score and the endpoint reputation score, and to send a response indicating the action to be taken by the end host. Further embodiments request another threat intelligence reputation score based on another hash of a dynamic link library module loaded by the process on the end host, and the action is determined based, at least in part, on the other threat intelligence score.

Id., Abstract. In an embodiment, CP describes that “[t]he metadata includes a tuple of connection information, which includes the network address (e.g., IP address) and port of end host 130, the network address (e.g., IP address) and port of the destination node, and the protocol used (e.g., TCP/IP).” *Id.* ¶ 54.

3. *Reasons to Combine the Teachings of Altman and CP*

Citing the testimony of Dr. Prakash, Petitioner argues that a person of ordinary skill in the art would have been motivated to combine the teachings of Altman and CP because “both patents are directed to rule-based interception of traffic, and CP provides details of a specific method for performing the matching step identified by Altman.” Pet. 55 (citing Ex. 1002 ¶ 408).⁸ Patent Owner contends that Petitioner fails to explain adequately how and why Altman and CP would be combined. PO Resp. 60.

Petitioner relies on CP as disclosing limitations 1[d] and 11[f], which concern identifying flow identification data with the one or more packets initiating communication flow. Pet. 55. According to Patent Owner, Petitioner’s assertion that CP provides details of a specific matching step identified by Altman is unconnected to the subject matter of limitations 1[d] and 11[f]. PO Resp. 60–61. Patent Owner further contends that the Petition is silent as to whether an ordinarily skilled artisan would have reasonably expected success in combining Altman and CP to arrive at limitations 1[d] and 11[f] and that the Petition does not explain how Altman’s rules used to determine whether a communication session is to be selected for decryption would be combined with CP’s transmitted metadata (IP addresses) to identify the flow identification data. *Id.* at 61.

The Petition cites testimony of Dr. Parkash stating that a person of ordinary skill would have had reason to combine the teachings of Altman and CP to the extent a person of ordinary skill in the art (POSITA) needed to understand the finer details of the matching disclosed in step 216 of Altman.

⁸ The cited testimony of Dr. Prakash appears to be included in paragraph 407 of his Declaration. *See* Ex. 1002, Prakash Decl. ¶ 407.

Pet. 55 (citing Ex. 1002, Prakash Decl. ¶¶ 407–408). Noting that the subject matter of both Altman and CP is directed to intercepting traffic between clients and servers based on policies and rules, Dr. Prakash explicitly states that a person of ordinary skill would have been motivated to combine the teachings of Altman and CP “because using the metadata disclosed by CP is one of only a few potential methods for performing the matching taught by Altman . . . [and] the metadata disclosed by CP offers more potential options to complete the matching step disclosed in Altman.” Ex. 1002, Prakash Decl. ¶ 407.

On this record, we determine that Petitioner has described with sufficient specificity why a person of ordinary skill would have looked to CP to provide details of performing Altman’s matching step and how the features of CP would have been combined with Altman. Pet. 55.

4. *Patent Owner’s Single Processor Arguments*

The Patent Owner Response contends that neither Altman nor CP discloses a computing device that performs each step (claim 1) or causes the apparatus to perform all recited operations (claim 11) with a single processor. PO Resp. 53–58. Referencing Figure 2 of Altman, Patent Owner notes the distinction between steps performed by the SIA and those performed by the NMC. *Id.* at 53–55. According to Patent Owner, Altman expressly states that its NMC and SIA are separate devices and in Figure 1 illustrates NMC 128 on one side of network switch 126 and SIA 136 on the other side of the switch. *Id.* at 55–56 (citing Ex. 1005, Fig. 1, ¶ 26). Patent Owner argues there is no teaching in Altman that functions of the NMC and SIA can be combined in a suitable processor. *Id.* at 57 (citing Ex. 1005 ¶ 27 (as disclosing that the NMC functionality may be carried out by any suitable computing device that correlates between the SIA and AAA server)).

Notwithstanding Altman’s disclosure that the disclosed techniques can be carried out by any suitable processor or processors, Patent Owner further argues that Petitioner has not shown inherency for purposes of anticipation, because the Petition does not demonstrate that Altman necessarily includes a single device that would perform all recited steps/operations. *Id.* at 58. As to CP, Patent Owner argues that Petitioner has not demonstrated that either CP or Altman suggest combining the NMC and SIA into a single device. *Id.*

Petitioner contends that we should reject Patent Owner’s single processor arguments because none of the Challenged Claims is limited to a single computer embodiment, where all functions are performed by the same processor. Pet. Reply 20. We agree with Petitioner. As noted in our claim construction analysis, the ’526 patent explicitly states that “the various methods and acts may be operative across one or more computing devices and networks. The functionality may be distributed in any manner or may be located in a single computing device (e.g., a server, client computer, or the like.” *See* Section V.C herein; Ex. 1001, 17:45–49.

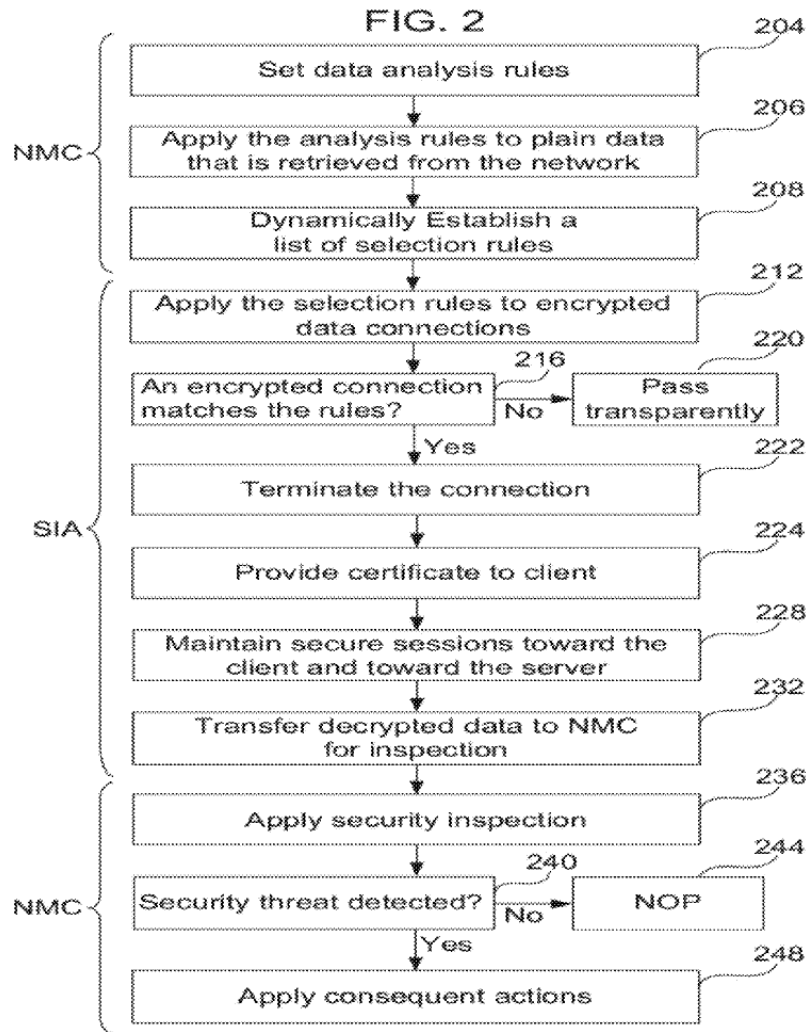
Petitioner further argues that, even if we adopted Patent Owner’s proposed single computing device/single processor construction, Altman expressly teaches that an embodiment with a separate SIA and NMC is exemplary. Pet. Reply 21 (citing Ex. 1005 ¶ 26). On this point, we agree with Petitioner. Paragraph 27 of Altman is cited by Patent Owner as demonstrating the functions of Altman’s NMC can be carried out by any suitable computing device. PO Resp. 57. Immediately preceding paragraph 26 of Altman explicitly states that both NMC 128 and “[t]he configurations of systems 100” in Figure 1 are “example configurations” and “the disclosed techniques can be carried out by any suitable processor or processors, typically located at any suitable location en-route from the client devices to

the servers that offer encrypted communications.” Ex. 1005 ¶ 26. Having considered the evidence and arguments of record, we determine that Petitioner has sufficiently demonstrated a person of ordinary skill would have had reason to combine the teachings of Altman and CP and that in combination they disclose a computing device that performs each step (claim 1) or causes the apparatus to perform all recited operations (claim 11) with a single processor.

5. *Analysis of Petitioner’s Arguments That Altman Anticipates Claims 1–6, 8–16, and 18–20 or That Altman in View of CP Render the Claims Obvious*

Petitioner addresses independent claims 1 and 11 together asserting that “claim 11 is substantively identical to claim 1, except that it claims an apparatus comprising a processor and at least one memory storing instructions that perform the method of claim 1.” Pet. 49. As discussed above, we agree that claims 1 and 11 recite substantially similar substantive limitations. Unless otherwise noted, our analysis below applies equally to corresponding limitations of both independent claims 1 and 11.

Petitioner contends Altman teaches the elements of claims 1 and 11; as to the limitations reciting “identify[ing], by the computing device, flow identification data associated with the one or more packets initiating the at least one encrypted communication flow,” Petitioner alternatively relies on CP in combination with Altman. *Id.* at 49–57. Petitioner relies on Figure 2 of Altman. *Id.* Figure 2 of Altman is reproduced below.



Ex. 1005, Fig. 2. Figure 2 of Altman is a flowchart that illustrates an exemplary method for selective SSL inspection. Ex. 1005 ¶¶ 10, 30.

Petitioner contends that Altman teaches “storing, by a computing device, a list of identification data and at least one corresponding action to perform on encrypted communication flows associated with corresponding identification data,” as recited in claim limitation 1[b] and similarly recited in limitation 11[d], because, as shown in Figure 2 (step 208), Altman “dynamically establishes a list of rules for selection of encrypted data connections.” Pet. 50–53 (reproducing Figure 2 of Altman, as annotated by Dr. Prakash) (citing Ex. 1005 ¶ 14; Ex. 1002 ¶ 392). According to

Petitioner, “Altman discloses that the [SIA] receives this dynamic rule list from the NMC.” *Id.* at 53 (citing Ex. 1005 ¶¶ 14, 22; Ex. 1002 ¶ 397). Petitioner further asserts that “Altman discloses that the dynamic rule list can include . . . IP addresses and other identification data.” *Id.* (citing Ex. 1005 ¶ 30 (rule table may include “client IP addresses” and “server URLs”); Ex. 1002 ¶¶ 393–396). Petitioner further argues that “Altman also discloses a corresponding action to be performed on encrypted communication flows associated with the identification data, in step 248 of Figure 2.” *Id.* Petitioner asserts that “Altman describes exemplary actions as including: ‘sensitive information leaks, as well as malwares, can be blocked [and] predefined information types that relate to target users may be copied and logged.’” *Id.* (citing Ex. 1005 ¶ 33; Ex. 1002 ¶¶ 398–401). The Patent Owner Response does not explicitly dispute that Altman discloses limitations 1[b] and 11[d]. Having reviewed the arguments and evidence of record, we agree with Petitioner that Altman discloses these limitations.

Petitioner further asserts that Altman teaches “receiving, by the computing device, one or more packets initiating at least one encrypted communication flow,” as recited in claim limitation 1[c] and similarly recited in claim limitation 11[e], because Altman discloses that “the SIA (computing device) ‘accepts some or all of the network user encrypted traffic.’” Pet. 53–54 (citing Ex. 1005 ¶ 14; Ex. 1002 ¶¶ 402–404). Petitioner asserts that “Altman further discloses that matching with the rules table is performed ‘for each new encrypted connection.’” *Id.* at 54 (citing Ex. 1005 ¶ 31). The Patent Owner Response does not explicitly dispute that Altman discloses limitations 1[c] and 11[e]. Having reviewed the arguments and evidence of record, we agree with Petitioner that Altman discloses these limitations.

Petitioner next contends that Altman teaches “identifying, by the computing device, flow identification data associated with the one or more packets initiating the at least one encrypted communication flow” (limitations 1[d] and 11[f]) because Altman discloses that the SIA (in step 212 of Figure 2) applies selection rules to flows and that the selection rules include identification data, such as IP addresses and URLs. Pet. 54 (citing Ex. 1005 ¶¶ 30–31; Ex. 1002 ¶¶ 392–395). Citing the testimony of Dr. Prakash, Petitioner argues “[a person of ordinary skill in the art] would understand that in order to apply the selection rules, like items must be compared to like (e.g. IP addresses from the flow request to IP addresses in the rule table).” *Id.* (citing Ex. 1002 ¶¶ 405, 412). Thus, according to Petitioner, applying selection rules by the SIA teaches “identifying . . . flow identification data” as recited in claims 1 and 11. *Id.*

Petitioner additionally asserts that the combination of Altman and CP teaches “identifying . . . flow identification data.” Pet. 55. Petitioner contends that CP discloses identifying metadata for connections, which includes “a tuple of connection information, which includes the network address (e.g., IP address) and port of end host 130, the network address (e.g., IP address) and port of the destination node, and the protocol used (e.g., TCP/IP).” *Id.* (citing Ex. 1006 ¶ 54; Ex. 1002 ¶ 407). We have already addressed Patent Owner’s arguments that Petitioner has not sufficiently demonstrated reasons an ordinarily skilled artisan would have combined the teachings of Altman and CP and agree with Petitioner. *See* Section VI.D.3 herein. The Patent Owner Response does not explicitly dispute that Altman and/or CP discloses the substance of limitations 1[d] and 11[f]. Having reviewed the arguments and evidence of record, we agree with Petitioner that Altman and/or CP discloses these limitations.

Petitioner contends that Altman teaches “comparing, by the computing device, the identified flow identification data with the list of the identification data,” as recited in claim limitation 1[e] and similarly recited in claim 11, because, as discussed above, Altman discloses accepting encrypted traffic and checking new encrypted connections “against the rule table.” Pet. 55 (citing Ex. 1005 ¶ 14; Ex. 1002 ¶ 396). Petitioner again argues that “[d]ue to the nature of comparisons, a [person of ordinary skill in the art] would have understood that Altman’s disclosed comparison necessarily involved comparing the identification data in the rule table with corresponding information from the communication flow.” *Id.* (citing Ex. 1002 ¶ 412). Having reviewed the arguments and evidence of record, we agree with Petitioner that Altman discloses these limitations.

Petitioner further asserts that Altman teaches “decrypting, by the computing device and based on the comparing resulting in a match with data of the list, each packet of an encrypted communication flow associated with the match with data of the list and performing a corresponding action on each packet of the encrypted communication flow associated with the match with data of the list,” as recited in claim 1 (element 1[f]) and similarly recited in claim 11 (element 11[h]). Pet. 56. According to Petitioner, Altman discloses “when detecting an encrypted connection that matches the rule table, the SIA decrypts the connection and provides a copy of the connection plain data to the NMC.” *Id.* (citing Ex. 1005 ¶ 14; Ex. 1002 ¶ 416). Petitioner further argues that “Altman also expressly discloses performing a corresponding action on the communication flow; specifically, Altman discloses that the computing device inspects the plain data after decrypting them for security threats and then applying predefined consequent actions to this connection.” *Id.* (citing Ex. 1005 ¶ 14; Ex. 1002

¶¶ 417–418). Petitioner asserts that “Altman describes exemplary actions as including: ‘sensitive information leaks, as well as malwares, can be blocked [and] predefined information types that relate to target users may be copied and logged.’” *Id.* at 53 (citing Ex. 1005 ¶ 33; Ex. 1002 ¶¶ 398–401).

Petitioner also argues that Altman teaches “re-encrypting, after performing the corresponding action, each packet of the encrypted communication flow associated with the match with data of the list and transmitting each packet of the encrypted communication flow to its intended destination,” as recited in claim 1 (limitation 1[g]) and similarly recited in claim 11 (limitation 11[i]). Pet. 57 (citing Ex. 1005 ¶ 32, stating that the SIA decrypts encrypted data it receives from each party and re-encrypts it “back-to-back toward the opposite party”).

Patent Owner focuses its arguments on claim limitations 1[g] and 11[i]. Patent Owner contends that neither Altman nor CP discloses, after performing the corresponding actions, re-encrypting each packet of the encrypted communication flow, as recited in limitations 1[g] and 11[i]. PO Resp. 46–53. As to the disclosures in CP, Patent Owner states that “Petitioner proffers an obviousness argument only for Limitations 1[d] and 11[f]” and relies upon Altman as disclosing limitations 1[g] and 11[i]. *Id.* at 50–51. We focus our analysis of limitations 1[g] and 11[i] on the parties’ arguments based on Altman.

Referencing Figure 2 of Altman, Patent Owner argues that “Altman does not teach re-encrypting each packet after performing the corresponding action on each packet, as recited in the ’526 patent claims.” *Id.* at 48–49. According to Patent Owner, “[i]n contrast to the claimed invention, Altman’s step 228 (the alleged ‘re-encrypting’) is performed *before* step 248 (the alleged ‘performing the corresponding action.’).” *Id.* at 50 (citing

Ex. 1005, Fig. 2, ¶¶ 30–33; Pet. 56–57). Based on its analysis of Figure 2, Patent Owner states that in contrast to the claims of the ’526 patent, “communications in Altman are decrypted, re-encrypted, and transmitted to their intended destination (step 228) without any ‘corresponding action’ performed on the packets of the communication.” *Id.* (citing Ex. 2002, Goodrich Decl. II ¶ 81).

Petitioner argues that Patent Owner misunderstands two aspects of Altman’s Figure 2. Pet. Reply 18. First, according to Petitioner, Patent Owner incorrectly identifies the “corresponding action” solely as step 248. *Id.* at 19. Petitioner cites both the Petition and Dr. Prakash’s Declaration as evidence that Altman discloses the corresponding action in steps 236–248. *Id.* (citing Pet. 56; Ex. 1002, Prakash Decl. ¶ 416 (stating that “[t]he corresponding action on each packet of the encrypted communication flow associated with the match is to inspect the plain data after decrypting it for security threats and then applying predefined consequent actions to this connection, which can include at least blocking the connection and logging the traffic”))).

Petitioner states that Patent Owner’s first misunderstanding leads to its second misunderstanding, i.e., Patent Owner’s assertion that the re-encryption Altman describes in its discussion of step 228 occurs before steps 232–248. Pet. Reply 19 (citing PO Resp. 50). According to Petitioner, Altman describes step 228 as an ongoing process. *Id.* at 19–20. Petitioner cites Altman’s description of step 228 as one that “maintains separate secure connections” by “decrypting the encrypted data that [SIA 136] receives from each end party and re-encrypting it back-to-back toward the opposite party.” *Id.* at 19 (citing Ex. 1005 ¶ 32). Petitioner asserts that Altman clearly describes step 228 as ongoing because one potential consequent action in

step 248 is that “sensitive information leaks, as well as malwares, can be blocked.” *Id.* at 19–20 (citing Ex. 1005 ¶ 33). Petitioner emphasizes that Patent Owner’s expert, Dr. Goodrich, agreed that it would be impossible to block the communication if step 248 (applying the consequent actions) occurs only after re-encryption. *Id.* at 20 (citing Ex. 1014, Goodrich Tr. 38:16–39:17). Thus, Altman discloses performing the consequent action, e.g., making a decision to block or re-transmit a packet with or without logging it, before re-encryption, such that re-encryption and re-transmission occurs after performing the corresponding action, as recited in claims 1 and 11. *Id.*

According to Patent Owner, the “Network Monitoring Center (NMC) receives a copy of the decrypted traffic for analysis, but then drops the traffic after analysis, never re-encrypting the traffic and sending it to intended destination.” PO Resp. 47 (citing Ex. 1005, Abstract, ¶ 14, Fig. 1; Ex. 1002, Prakash Decl. ¶ 145; Ex. 1007, 6, Fig. 5b). Dr. Goodrich testified that, in Altman “the NMC drops the traffic after analysis rather than re-encrypting it and transmitting it to intended destination.” Ex. 2002, Goodrich Decl. II ¶ 85.

Patent Owner’s argument that the NMC drops the traffic after analysis and never re-encrypts is unavailing, as further evidenced by Dr. Goodrich’s deposition testimony. Altman’s NMC does not function to re-encrypt and transmit traffic, but instead uses unencrypted data from the SIA to determine whether to instruct the SIA, which functions as the Man-In-The-Middle, to block or re-encrypt and transmit packets. *See* Ex. 1005 ¶¶ 31–33; Ex. 1014, Goodrich Tr. 42:18–22 (agreeing that Altman does not describe the NMC itself as accepting or processing encrypted communications), 38:12–15 (agreeing that the SIA responds to instructions from the NMC).

The Decision to Institute determined that Petitioner had demonstrated sufficiently that Altman at least suggests re-encrypting the decrypted traffic after performing the corresponding action as recited in claim limitations 1[f] and 1[g]. Dec. to Inst. 49–50. As discussed below, having reviewed the arguments and evidence of record, we are also persuaded that a skilled artisan would reasonably understand or infer limitation 1[g] from Altman’s disclosure. *See Dayco Prods.*, 329 F.3d at 1368 (stating that “the dispositive question regarding anticipation is whether one skilled in the art would reasonably understand or infer from the prior art reference’s teaching that every claim element was disclosed in that single reference”).

Patent Owner’s citation to Exhibit 1007 (Netronome) as “showing a similar out-of-band⁹ analysis” informs our understanding of what a person of ordinary skill would reasonably understand or infer from Altman. PO Resp. 47; Ex. 1005 ¶ 12. Netronome, incorporated into Altman by reference, discloses an embodiment for plaintext inspection of SSL-encrypted flows, using a proxy to examine and inspect the SSL-encrypted content before entering or exiting an enterprise. Ex. 1007, 2; Ex. 1005 ¶ 12. In one Netronome embodiment, each individual session terminates on the SSL inspector, but TCP connections are retained end-to-end. Ex. 1007, 6. Terminating and re-originating SSL allows the appliance to obtain plaintext in the encrypted signal that is sent to an adjacent security appliance in a regenerated TCP stream; the data remains encrypted on both the connection

⁹ Neither the ’526 patent nor Altman uses the term “out of band.” Ex. 1014, Goodrich Tr. 35:19–25. As to Altman, Dr. Goodrich appears to be referring to copies of data flows decrypted by the SIA and received by the NMC as “out of band” content. *Id.* at 46:11–16 (noting that the NMC is never disclosed as processing flows where it would be sending packets back to a destination); *see also id.* at 36:3–22.

from the client to the SSL inspector and from the SSL inspector to the Web server. Ex. 1007, 6.

Petitioner's Altman-based challenges do not rely on Netronome, where the TCP connections are retained end-to-end, but instead, cite Altman's explicit disclosure of "decrypting the encrypted data that it receives from each end party and re-encrypting it back-to-back toward the opposite party." Pet. 57 (quoting Ex. 1005 ¶ 32); Pet. Reply 19–20. As Petitioner points out, this encryption and re-encryption is performed by the SIA (not the NMC) as part of ongoing step 228. Pet. Reply 18–20; Ex. 1005 Fig. 2 (indicating that the SIA performs steps 212–232 and the NMC preforms steps 236–248). Altman states that, when an encrypted connection matches the rule table, the "SIA decrypts the connection and provides a copy of the connection plain data to the NMC . . . [and t]he NMC then inspects the plain data for security threats . . . [and] applies predefined consequent action to this connection." Ex. 1005 ¶ 14. In one method, upon a match, at termination step 222, SIA 136 substitutes the matching connection with a pair of separate TCP connections, one toward the client and one toward a related server 124. *Id.* ¶ 31. "At a session maintaining step 228, SIA 136 maintains separate secure connections, typically SSL/TLS based . . . connections, while decrypting the encrypted data it receives from each party and re-encrypting it back-to-back toward the opposite party." *Id.* ¶ 32. The SIA "constitutes an SSL proxy for the secure communications it terminates." *Id.* At step 232, the SIA transfers decrypted data to the NMC for inspection. *Id.*

"At decision step 240, the NMC determines the method step that follows the inspection. If no security threat is detected then no further action is required regarding the inspected connection. This case is indicated by a

no-operation step 244.” *Id.* ¶ 33. If a security threat is detected, the NMC applies predefined consequent actions. *Id.* No-operation step 244 refers to no-operation at the NMC, which operates on decrypted data. *See* Ex. 1014, Goodrich Tr. 42:18–21.

As the Petition and Dr. Prakash point out, the SIA, which maintains the secure connections, decrypts the encrypted data it receives from each party and re-encrypts it toward the opposite party. Pet. 56; Ex. 1002, Prakash Decl. ¶¶ 415–416; Ex. 1005 ¶ 32. A person of ordinary skill would have been familiar with Netronome, cited by Patent Owner, where re-encryption is not required. That same ordinarily skilled artisan would have understood Altman’s explicit disclosure of a method requiring re-encryption to the opposite party to be different from that in Netronome.

Figure 2 of Altman explicitly indicates that steps 212–232 are performed by the SIA and steps 236–248 are performed by the NMC. Ex. 1005, Fig. 2. As Petitioner points out, the NMC determines, based on its analysis of unencrypted data, what action should be taken, e.g., no action (allowing the packet to proceed, where no threat is detected), blocking information leaks and the packet, or logging and copying the packet. Pet. 56–57; Pet. Reply 19; Ex. 1005 ¶¶ 32–33. Although Altman does not explicitly state when the re-encryption occurs, an ordinarily skilled artisan would infer that the SIA’s re-encryption toward the opposite party occurs after the NMC signals a decision to allow the packet. *See* Ex. 1014, Goodman Tr. 29:12–17 (agreeing that Altman’s SIA blocks packets based on instructions from the NMC), 42:18–22 (agreeing that Altman does not describe the NMC as accepting or processing encrypted packets).

Altman also discloses an alternative embodiment in which the SIA decrypts the connection data without terminating it and proceeds directly to

step 232 to transfer decrypted data to the NMC. Ex. 1005 ¶ 31. In this embodiment, Altman skips steps 222 through 228 and does not maintain a secure session between the client and server. In that case, if the NMC determines the data is safe to transmit, in order to transmit the data safely, an ordinarily skilled artisan would reasonably infer that the SIA, as the Man-In-The-Middle, re-encrypts the data it de-crypted after the NMC performs the corresponding action by instructing the SIA to allow the packet. Ex. 1005 Fig. 1, ¶ 19.

Thus, applying the standard articulated in *Dayco*, we agree with Petitioner that Altman anticipates claims 1 and 11 because Altman discloses to an ordinarily skilled artisan a method and apparatus in which re-encryption and transmission of the data occur after performing the corresponding action, as recited in the claims. We also determine that Altman's teachings in combination with the teachings of CP would have at least suggested that if no security threats are detected upon the NMC's inspection of the decrypted plaintext, the traffic is allowed and re-encrypted to be sent to its destination.

6. Conclusion – Claims 1 and 11

Having considered all the arguments and evidence of record, we determine that Petitioner has demonstrated by a preponderance of the evidence that Altman discloses all the limitations of method claim 1 and corresponding apparatus claim 11 of the '526 patent and that claims 1 and 11 are anticipated by Altman.¹⁰ We further determine that Petitioner has demonstrated that a person of ordinary skill would have had reason to

¹⁰ The Petition does not assert, as separate ground, that claims 1 and 11 are unpatentable as obvious over Altman alone.

combine the teachings of Altman and CP and that, because the combined teachings of Altman CP would have taught all the limitations of claim 1 and 11 to an ordinarily skilled artisan, Petitioner has demonstrated by a preponderance of the evidence claims 1 and 11 are unpatentable as obvious over Altman and CP.

7. *Claims 2–6, 8–10, 12–16, and 18–20*

Claims 2 and 12 recite receiving a list of addresses and/or domain names from a security application and, based on the received list, creating a list of identification data. Ex. 1001, 18:22–28, 19:65–20:5. Petitioner cites Altman as disclosing a security application and the SIA receiving a rule table that contains network addresses from the NMC. Pet. 56–57 (citing Ex. 1005 ¶ 27). Petitioner also cites Altman as disclosing creating a list of identification data based on the received list and the SIA receiving the rule table from the NMC and creating a local copy. *Id.* at 58 (citing Ex. 1002, Prakash Decl. ¶ 58).

Claims 3 and 13 recite receiving a list of network addresses and/or domain names via a subscription service. Ex. 1001, 18:29–36, 20:9–11. Claims 4 and 14 similarly recite receiving a list of network addresses and/or domain names from a privacy protection application. *Id.* at 18:45–47, 20:19–21. Petitioner cites Altman as disclosing the NMC functionality can be provided by any number of tools, including systems operated by a “service provider.” Pet. 59 (citing Ex. 1005 ¶ 27). Petitioner states that such a service provider would be a “cyber threat intelligence provider” because “the information in the application is expressly designed to eliminate cyber threats such as malware.” *Id.* (citing Ex. 1005 ¶ 33). Petitioner further argues that CP also discloses receiving identification information from a threat intelligence server operated by a third party. *Id.* (citing Ex. 1006

¶ 47). Noting that Altman incorporates Netronome by reference, Petitioner cites Netronome as disclosing spyware was a specific concern in network monitoring. *Id.* at 62. Petitioner also notes that a person of ordinary skill would have had reason to combine the teachings of Altman and CP to cross-communicate with multiple data sources and improve operation of the resultant system and because receiving such a list from any source would not change the operation of the system or require experimentation. *Id.* at 60, 62.

Petitioner contends that because claims 5 and 15 recite a law-enforcement wiretapping application with features similar to those recited in claims 2 and 12, claims 5 and 15 are unpatentable for the same reasons that claim 2 and 12 are unpatentable. Pet. 63–64.

Claims 6 and 16 recite forwarding packets that are not decrypted prior to being forwarded to their intended destinations. Ex. 1001, 18:51–56, 20:34–41. Petitioner cites Altman as disclosing the limitations of claims 6 and 16 because Altman discloses that the SIA “transfers transparently” all encrypted connections that do not match the rules table. Pet. 65 (citing Ex. 1005 ¶ 15]. Petitioner notes that Altman uses the term “transfers transparently” to refer to forwarding the communication flow without decryption. *Id.* (citing Ex. 1002, Prakash Decl. ¶ 447).

Claims 8 and 18 recite, by comparing the identification flow data with the list of identification data, determining that the list of identification data does not comprise the identified flow identification data, and performing an action other than the action indicated by the list of identification data. Ex. 1001, 19:14–26, 20:67–21:12. Petitioner cites Altman as disclosing that, when there is no match with the rules table, the action associated with the identification information (step 248) is not performed, but instead, at step 220 the communication flow passes transparently. Pet. 66–67.

Claims 9 and 19 recite that the action indicated by the list of identification data comprises terminating the encrypted communication flow. Ex. 1001, 18:27–29, 21:13–16. Petitioner cites Altman as disclosing a greylist in which data that matches a first criterion (a match with the rules table) is decrypted for further processing at steps 222–248, and data that does not match the first criterion is passed on. Pet. 67 (citing Ex. 1002, Prakash Decl. ¶ 457). Arguing that Altman discloses this limitation as exemplary, Petitioner further argues that a person of ordinary skill would have understood that it would be straightforward to use the rules table to implement a “whitelist” in which the items matching the rules tables are not decrypted, and all other traffic is decrypted and inspected. *Id.* at 68 (citing Ex. 1002, Prakash Decl. ¶ 457). Petitioner further argues that Netronome, incorporated by reference in Altman, discloses such a “whitelist.” *Id.* at 69 (citing Ex. 1007, 5; Ex. 1002, Prakash Decl. ¶ 458).

Claims 10 and 20 recite that the action indicated by the list comprises logging packets associated with the encrypted communication and forwarding the packets to their respective indicated destination. Ex. 1001, 18:30–36, 21:17–24. Petitioner cites Altman as disclosing possible actions at step 248 in Figure 2 including “copy and log” information that relates to specific users and that ongoing activity in step 228 includes forwarding the packets associated with the encrypted communication flow to their intended destination. Pet. 69–70 (citing Ex. 1005, Fig. 2, ¶¶ 32–33; Ex. 1002, Prakash Decl. ¶ 466).

Patent Owner does not explicitly respond to Petitioner’s contentions concerning the limitations recited in claims 2–6, 8–10, 12–16, and 18–20. Having reviewed the evidence and arguments of record, as discussed above, we determine that Petitioner has demonstrated Altman discloses all the

limitations of claims 2–6, 8–10, 12–16, and 18–20 and has shown by a preponderance of the evidence that Altman anticipates claims 2–6, 8–10, 12–16, and 18–20.¹¹

We further determine that Petitioner has demonstrated that a person of ordinary skill would have had reason to combine the teachings of Altman and CP and that, because the combined teachings of Altman CP would have taught all the limitations of claims 2–6, 8–10, 12–16, and 18–20 to an ordinarily skilled artisan, Petitioner has demonstrated by a preponderance of the evidence that claims 2–6, 8–10, 12–16, and 18–20 are unpatentable as obvious over Altman and CP.

E. Petitioner’s Contentions That Claims 7 and 17 Would Have Been Obvious over Altman in View of IPUG

Claims 7 and 17 recite the computing device receiving first and second lists of network addresses and/or domain names, assigning different first and second priorities to the lists and creating an ordered list of identification data from the first and second lists. Ex. 1001, 1856–19:13, 20:43–69. Petitioner contends that dependent claims 7 and 17 would have been obvious over the combination of Altman and IPUG. Pet. 71–75.

Petitioner persuasively argues that a person of ordinary skill in the art would have been motivated to combine Altman and IPUG because “a person designing a system according to the teachings of Altman would have looked to systems providing a similar functionality, such as IPUG, for teachings on implementation details of such a system.” *Id.* at 74 (citing Ex. 1002 ¶¶ 496, 502). Noting that Altman incorporates Netronome by reference, Petitioner cites Netronome’s whitelist of bank servers for which communications

¹¹ The Petition does not assert, as a separate ground, that claims 2–6, 8–10, 12–16, and 18–20 are unpatentable as obvious over Altman alone.

should not be encrypted as Altman's disclosure of a second list. *Id.* at 72. Petitioner argues that Netronome indirectly discloses assigning different priorities to the different lists, because Netronome teaches two different policies, each with a set of rules. *Id.* at 73 (citing Ex. 1007, 5; Ex. 1002, Prakash Decl. ¶ 492). Petitioner states that Netronome discloses the Traffic Diversion Policy has a higher priority than the Inspection Policy, because the purpose of the Traffic Diversion Policy is to reduce the load on the SSL inspector. *Id.*

Petitioner cites IPUG as expressly disclosing assigning different priorities to first and second lists because IPUG discloses (i) each custom URL must include a unique priority, (ii) IPUG Decryption Policies are applied in priority order, and (iii) IPUG creates a combined list (the final Decryption Policy) that includes both identification data from the first list (policies assigned the action decrypt) and identification data from the second list (policies assigned the action pass through). Pet. 73–75 (citing Ex. 1002, Prakash Decl. ¶¶ 309, 492, 496–501; Ex. 1008, 281, 413).

Patent Owner does not respond explicitly to the substance of Petitioner's contentions concerning the teachings of Altman and IPUG relating to claims 7 and 17. Having considered the evidence and arguments of record, we determine that Petitioner has demonstrated that a person of ordinary skill would have had reason to combine the teachings of Altman and IPUG and that, because the combined teachings of Altman and IPUG teach all the limitations of claims 7 and 17 to an ordinarily skilled artisan, Petitioner has demonstrated by a preponderance of the evidence that claims 7 and 17 are unpatentable as obvious over Altman and IPUG.

VII. CONCLUSION¹²

Having considered all the evidence of record we determine that Petitioner has demonstrated by a preponderance of the evidence that all the challenged claims are unpatentable.

In summary:

Claims	35 U.S.C. §	Basis	Claims Shown Unpatentable	Claims Not shown Unpatentable
1–4, 6–14, 16–20	102	IPUG	1–4, 6–14, 16–20	
1–20	103	IPUG	1–20	
1–6, 8–16, 18–20	102	Altman	1–6, 8–16, 18–20	
1–6, 8–16, 18–20	103	Altman, CP	1–6, 8–16, 18–20	
7, 17	103	Altman, IPUG	7, 17	
Overall Outcome			1–20	

VIII. ORDER

In consideration of the above it is:

ORDERED that claims 1–20 of the '526 patent are unpatentable;

¹² Should Patent Owner wish to pursue amendment of the challenged claims in a reissue or reexamination proceeding subsequent to the issuance of this Decision, we draw Patent Owner's attention to the April 2019 *Notice Regarding Options for Amendments by Patent Owner Through Reissue or Reexamination During a Pending AIA Trial Proceeding*. See 84 Fed. Reg. 16,654 (Apr. 22, 2019). If Patent Owner chooses to file a reissue application or a request for reexamination of the challenged patent, we remind Patent Owner of its continuing obligation to notify the Board of any such related matters in updated mandatory notices. See 37 C.F.R. § 42.8(a)(3), (b)(2).

FURTHER ORDERED that, because this is a Final Written Decision, 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.

IPR2022-01525
Patent 10,284,526 B2

FOR PETITIONER:

Peter Chassman
Michael Forbes
Gerard Donovan
Jonathan Detrixhe
REED SMITH LLP
pchassman@reedsmith.com
mforbes@reedsmith.com
gdonovan@reedsmith.com
jdetrixhe@reedsmith.com

FOR PATENT OWNER:

James Hannah
Jeffrey Price
Jenna Fuller
Bradley Wright
Scott Kelly
KRAMER LEVIN NAFTALIS & FRANKEL LLP
jhannah@kramerlevin.com
jprice@kramerlevin.com
jfuller@kramerlevin.com
bwright@bannerwitcoff.com
skelly@bannerwitcoff.com