Trials@uspto.gov
571-272-7822

Paper 31
Date: January 23, 2020

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

CISCO SYSTEMS, INC.,
Petitioner,

v.

CENTRIPETAL NETWORKS, INC.,
Patent Owner.

IPR2018-01386
Patent 9,565,213 B2

Before, BRIAN J. McNAMARA, J. JOHN LEE, and JOHN P. PINKERTON *Administrative Patent Judges.*

McNAMARA, *Administrative Patent Judge*.

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

I. BACKGROUND

On January 24, 2019 we instituted an *inter partes* review of claims 1–16 of U.S. Patent No. 9,565,213 B2 ("the '213 patent"). Paper 8 ("Dec. to Inst."). Patent Owner filed a Patent Owner Response (Paper 14, "PO Resp."), Petitioner filed a Petitioner Reply (Paper 20, "Pet. Reply") and Patent Owner filed a Sur-reply (Paper 26, "PO Sur-reply")). A transcript of an oral hearing held on November 12, 2019 (Paper 29, "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); 37 C.F.R. § 42.1(d).

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 '213 PATENT

The '213 patent discloses methods and systems for protecting a secured network. Ex. 1001, Abstract. Figure 1 of the '213 patent is reproduced below.

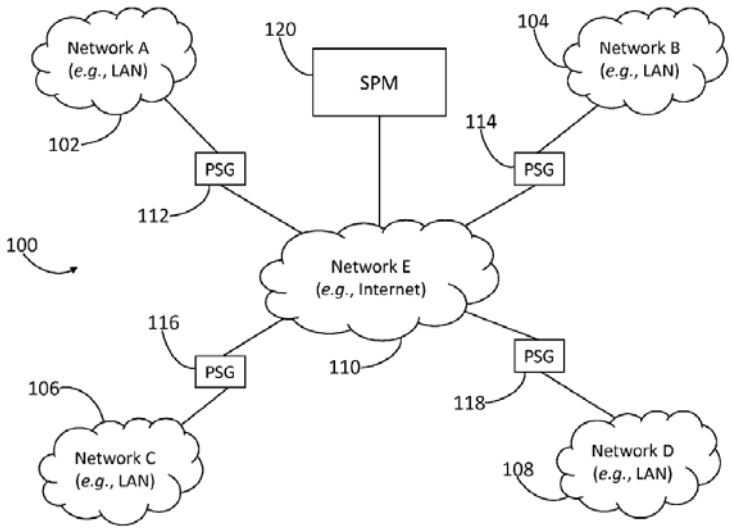


FIG. 1

Figure 1 of the ’213 patent illustrates a network environment that includes packet security gateways (PSGs) situated between networks and a security policy management (SPM) server that communicates dynamic security policies to the PSGs. *Id.* at 4:53–55, 4:66–5:3, Fig. 1. The PSGs perform packet transformation functions on received packets according to rules in a dynamic security policy in which “each rule may specify criteria and one or more packet transformation functions that should be performed for packets associated with the specific criteria.” *Id.* at 7:7–13. The patent explains that:

> The specified criteria may take the form of a five-tuple of values selected from packet header information, specifying a protocol type of the data section of the IP packet (e.g., TCP, UDP, ICMP, or any other protocol), one or more source IP addresses, one or more source port values, one or more destination IP addresses, and one or more destination ports.

Id. at 7:13–19, Fig. 3.

The ’213 patent describes packet transformation functions that forward packets into the network (e.g., Ex. 1001, 2:50–52), drop packets (e.g., *id*. at 2:57–59), or perform functions other than forwarding or dropping

the packets, (e.g., *id.* at 1:49–51). For example, rules in a dynamic security policy may specify a transformation function that routes or switches packets to a network address corresponding to a monitoring device by encapsulating the packet with a header that corresponds to the network address of the monitoring device. *Id.* at 11:14–33. The monitoring device strips the header and copies the packets, or data within the packets, for subsequent review before forwarding the packets to the destination address. *Id.* at 11:22–33.

Various combinations of rules may implement services, such as a network threat awareness service in which a packet transformation function produces a digest or log of the packet, "e.g., associated network addresses, ports, protocol types, URIs, arrival times, packet sizes, directions, interface names, media access control (MAC) addresses, matching rule IDs, metadata associated with matching rules, enforced policy names, or the like." *Id.* at 11:36–54. Such packet logs can employ a logging standard, such as syslog, and be read by awareness application servers that perform transformations to produce awareness information that can be accessed by client applications. *Id.* at 54–60.

Figure 11 of the '213 patent is reproduced below.

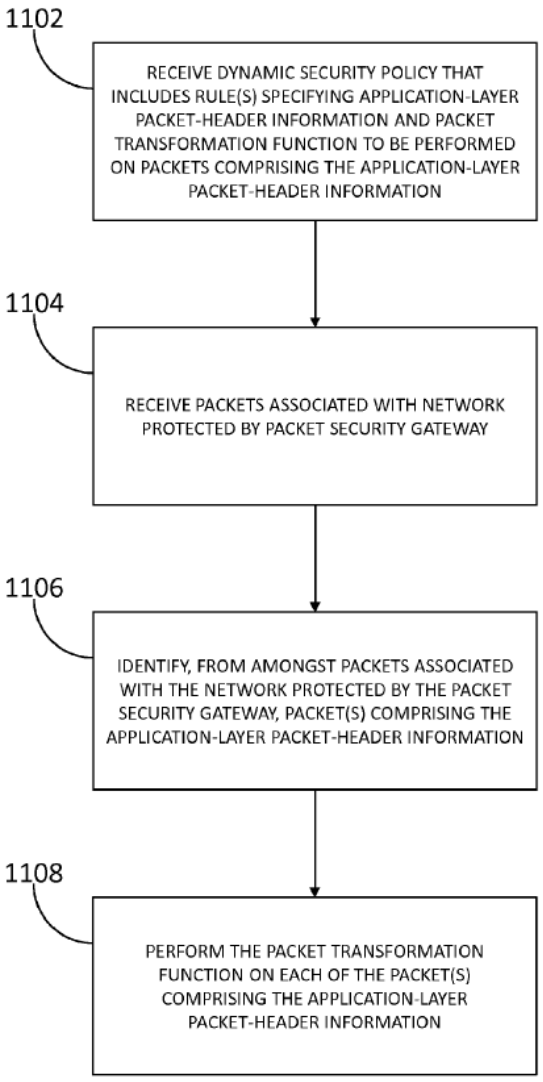


FIG. 11

"Figure 11 [of the '213 patent] illustrates an exemplary method for protecting a secured network that includes identifying packets based on application-layer packet-header information." Ex. 1001, 21:17–19. At step 1102, a plurality of PSGs (e.g., 112, 114, 116, and 118) associated with an SPM (120) receive a dynamic security policy that includes at least one rule (i.e., one or more rules) specifying application-layer packet-header information and a packet transformation function to be performed on packets comprising the application-layer packet-header information. *Id.* at 21:20–

26. For example, one or more rules of the dynamic security policy received from the SPM may specify that: (1) the application-layer packet-header information includes information that identifies one or more HTTP packets, and (2) the packet transformation function may accept or deny packets based on the specified application-layer packet-header information. *Id.* at 21:29–35.

At step 1104, a PSG receives packets from a computing device located in one of the protected networks. Ex. 1001, 21:35–43. At step 1106, the PSG identifies those packets associated with the protected network that comprise the specified application-layer packet-header information. *Id.* at 21:44–48. For example, if the rule specifies application-layer packet-header information that identifies one or more HTTP packets (e.g., one or more HTTP packets that comprise an HTTP GET method and/or an HTTP PUT method), the PSG may identify those packets as originating from and/or destined for a network address corresponding to URLs specified in the HTTP GET or HTTP PUT method call. *Id.* at 21:48–64.

At step 1108, the PSG performs the packet transformation function on each of the packets identified as comprising the specified application-layer packet-header information. Ex. 1001, 21:64–67. For example, the PSG may accept and forward the packets to their respective destinations or drop the packets. *Id.* at 21:67–22:6,

The method illustrated in Figure 12 of the ’213 patent is similar to that illustrated in Figure 11, except that instead of a dynamic security policy that performs a transformation function based on identifying application-layer packet-header information, the method illustrated in Figure 12 performs a transformation function that comprises a packet digest logging function based on specified packet identification criteria (e.g., application-layer

packet-header information and/or a five-tuple specifying one or more transport-layer protocols, a range of source addresses, a range of source ports, a range of destination addresses, and a range of destination ports). *See* Ex. 1001 22:7–28:18; *compare id.* at Fig. 11, *with id.* at Fig. 12. The packet digest logging function may generate a record comprising a subset of information for each identified packet, store the data temporarily at the PSG or send it to a different computing device, e.g., the SPMS, and may reformat the data according to a logging system standard. *Id.* at 22:60–23:18.

III. ILLUSTRATIVE CLAIMS

Independent claim 1, using the Petitioner's designation for each claim limitation as shown below, is illustrative.

1. **[1.1]** A method comprising:

receiving, by each of a plurality of packet security gateways associated with a security policy management server and from the security policy management server, a dynamic security policy that comprises at least one rule specifying application-layer packet-header information **[1.2]** and a packet transformation function comprising a packet digest logging function to be performed on packets comprising the application-layer packet-header information;

[1.3] receiving, by a packet security gateway of the plurality of packet security gateways, packets associated with a network protected by the packet security gateway;

[1.4] identifying, by the packet security gateway, from amongst the packets associated with the network protected by the packet security gateway, and on a packet-by-packet basis, one or more packets comprising the application layer packet-header information;

[1.5] performing, by the packet security gateway and on a packet-by-packet basis, the packet transformation function on each of the one or more packets comprising the application-layer packet-header information, wherein the performing the packet transformation function comprises

[1.6] identifying a subset of information specified by the packet digest logging function for each of the one or more packets comprising the application-layer packet-header information;

[1.7] generating, for each of the one or more packets comprising the application-layer packet-header information, a record comprising the subset of information specified by the packet digest logging function; and

[1.8] reformatting, for each of the one or more packets comprising the application-layer packet-header information, the subset of information specified by the packet digest logging function in accordance with a logging system standard; and

[1.9] routing, by the packet security gateway and on a packet-by-packet basis, to a monitoring device each of the one or more packets corresponding to the application-layer packet-header information in response to the performing the packet transformation function.

Id. at 25:14–55; *see* Petition ("Pet") 27–46 (including Petitioner's designation for each claim element).

Independent claim 10 generally parallels the language of independent claim 1, but recites that the dynamic security policy comprises at least one rule specifying "packet-identification criteria," instead of "application-layer packet-header information," and that the packet identifying criteria comprises a "Differentiated Service Code Point (DSCP) selector."

IV. GROUNDS FOR INSTITUTION

Trial was instituted on the following grounds:

Claim(s) Challenged	35 U.S.C. §	References(s)
1–9	103	Narayanaswamy[1], Kapoor[2],

[1] U.S. Patent Appl. Publ. No. US2009/0328219 A1 (Ex. 1012)
[2] U.S. Patent Appl. Publ. No. US2008/0229415 A1 (Ex. 1013)

Claim(s) Challenged	35 U.S.C. §	References(s)
		Johnson[3] and Kjendal[4]
10–16	103	Narayanaswamy, Kapoor, Johnson, Kjendal, and the Diffserv Specification[5]

V. CLAIM CONSTRUCTION

A. Dynamic Security Policy

In our Decision to Institute, we construed "dynamic security policy" to mean "any rule, message, instruction, file, data structure, or the like that specifies criteria corresponding to one or more packets and identifies a packet transformation function to be performed on packets corresponding to the specified criteria." *See* Dec. to Inst. 7– 8. Petitioner agrees with our constructions. Pet. Reply 1–3. The Patent Owner Responses proposes "dynamic security policy" be construed to mean "a non-static set of one or more rules." PO Resp. 14. Patent Owner contends our construction alters the explicit language of the specification describing a dynamic security policy as one that *includes* any rule, message, etc. PO Resp. 14 (citing Ex. 1001, 2:58–63), PO Sur-reply 4–5. According to Patent Owner, a rule itself is not a dynamic security policy, but only part of a dynamic security policy. *Id.*

Patent Owner's proposed construction that a dynamic security policy be a *set of one or more* rules is inconsistent with its argument that a rule may not be a policy, as under Patent Owner's construction *one* rule may constitute a dynamic security policy. Our preliminary construction that *any*

[3] U.S. Patent Appl. Publ. No. US2004/0123220 (Ex. 1014)
[4] U.S. Patent No. 9,172,627 B2 (Ex. 1009)
[5] "An Architecture for Differentiated Services," Network Working Group Request for Comments 2475, The Internet Society, Dec. 1998 (Ex. 1011)

rule, message, etc., may be a dynamic security policy does not preclude a policy of more than one rule and is consistent with the Specification's description in the singular that "[a]s used herein" a dynamic security policy "includes any rule, message," etc. (*see* Ex. 1001 4:58–63) and "may include one or more rules" (*id.* at 6:11–12). Such a "dynamic security policy may utilize the combination of one or more rules to create policies for governing packets within a network environment or effectuating one or more services within a network environment." Ex. 1001, 8:34–37.

Patent Owner further argues that our construction removes any patentable weight from the word "dynamic" because it does not explicitly state that the policy is "non-static." PO Resp. 15–16. Patent Owner does not point to any use of the expression "non-static" in the '213 patent Specification. In some embodiments, a dynamic security policy may be constructed or revised manually off line and loaded into SPMS memory by an administrator (Ex. 1001, 14:23–47); in other embodiments the SPMS may be configured to add, remove, or alter one or more dynamic security policies based on information received from devices within the network known to be associated with malicious traffic (*id*. at 14:48–15:37). As discussed above, however, the Specification explicitly states "As used herein, a dynamic security policy includes any rule message, instruction, file data structures, or the like that specifies criteria corresponding to one or more packets and identifies a packet transformation function to be performed on packets corresponding to the specified criteria." *Id.* at 4:58–64. As our construction is consistent with that language, we decline to adopt Patent Owner's construction.

B. Monitoring Device

In our Decision to Institute we construed "monitoring device" to mean "a device configured to copy (or store) packets or data contained within them." *See* Dec. to Inst. 13–14. Petitioner agrees with our construction. Pet. Reply 3–4. Patent Owner contends that we should construe "monitoring device" according to its plain and ordinary meaning, which Patent Owner defines as "a device configured to monitor packets." PO Resp. 18; PO Sur-reply 5. Patent Owner's construction merely replaces the adjective "monitoring" with the infinitive form "to monitor"—it does not provide any context to the term "monitor." We further note that neither claim 1 nor claim 10 expressly states that the monitoring devices actually monitors, or in any way observes, the packets. Instead the claims merely state that packets are routed to a monitoring device, without reciting what, if anything, the monitoring device does with the packets.

In the context of the '213 patent, we construe the recited "monitoring device" In view of the Specification. As we noted in the Decision to Institute, the '213 patent describes a packet transformation function as forwarding packets to a monitoring device in the context of a voice over internet protocol (VoIP) call, where the monitoring device copies or stores packets or data contained within the packets for subsequent review, e.g., by law enforcement. Dec. to Inst. 14 (citing Ex. 1001, 16:54–17:21). We also noted that the '213 Specification discusses similar functions performed by the monitoring device in the context of logging. *Id.* (citing Ex. 1001, 11:26–31). Patent Owner has not identified any other functions performed by the claimed monitoring device. Thus, for purposes of this Decision, consistent with the Specification, we apply the construction adopted in the Decision to

institute and construe "monitoring device" to mean "a device configured to copy (or store) packets or data contained within them."

C. Packet

Neither party proposed a construction of "packet" prior to institution. The Patent Owner Response proposes that the term "packet" be construed to mean a packet at layer 2 (data link layer [L2]) or layer 3 (network layer [L3]) of the Open Systems Interconnection (OSI) seven layer model. *See* PO Resp. 9–13. Patent Owner states that, as agreed by Petitioner's expert Dr. Jeffay, packets received by the PSGs and identified on a packet-by-packet basis as including application-layer packet-header information in the '213 patent are not application-layer packets. *Id.* at 10–11 (citing Ex. 1004, Jeffay Decl. ¶ 51, including Dr. Jeffay's diagram depicting embedding of protocol data units during the transmission process). Patent Owner explains that, in one embodiment, the PSG is implemented in a network-layer transparent manner in which the PSG may send and receive traffic at the link layer using an interface not addressed at the network layer, and simultaneously perform the packet transformation function at the network layer. *Id.* at 11 (citing Ex. 1001, 3:4–9). Alternatively, the PSG includes a network interface having a network-layer addressable address. *Id.* (citing Ex. 1001, 3:10–13). Patent Owner further notes that the '213 patent explicitly states that packet transformation functions operate at the network layer, even when the PSG operates in a network-layer transparent manner. *Id.* at 12 (citing Ex. 1001, 6:38–41). Finally, Patent Owner argues that Petitioner's expert Dr. Jeffay agrees that the routing by the PSG on a packet-by-packet basis to a monitoring device refers to a process carried out by a layer-3 network interconnection, such as a router. *Id.* at 12–13 (citing Ex. 1004, Jeffay Decl. ¶ 40).

Petitioner does not oppose Patent Owner's proposed construction—instead, as discussed further herein, Petitioner argues that the asserted prior art discloses receiving Layer 2 and Layer 3 packets. Pet. Reply 6–12.

We find Patent Owner's construction of "packet," as used in the '213 patent only, to be consistent with the use of the term in the context of the '213 patent. Thus, for purposes of this Decision only we construe "packet" to mean an L2 or L3 packet.

D. Rule/Rules

In our Decision to Institute we construed "rule(s)" to mean "a condition or set of conditions that when satisfied cause a specific function to occur." Dec. to Inst. 8–10. Neither party disputes this construction, and we apply it in this Decision. Patent Owner notes that in our Decision to Institute we stated the claim language is unclear as to whether (1) the dynamic security policy includes (i) a rule specifying criteria and (ii) a packet transformation function or (2) that the dynamic security policy includes rules specifying both the criteria and the packet transformation function. PO Resp. 16–17 (citing Dec. to Inst. 9). Patent Owner argues that the latter understanding comports with the claim language. We note that the Specification states "[e]ach rule may specify criteria and one or more packet transformation functions that should be performed for packets associated with the specified criteria." Ex. 1001, 7:10–13. It is not necessary, however, for us to resolve the issue for purposes of this Decision, as only those terms which are in controversy need to be construed and only to the extent necessary to resolve the controversy. *See Vivid Techs., Inc. v. Am. Sci. & Eng'g, Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999).

E. Security Policy Management Server (SPMS)

In our Decision to Institute we construed "security policy management server (SPMS)" to mean "a server configured to communicate a dynamic security policy to a packet gateway." Dec. to Inst. 10. Neither party disputes this construction, and we apply it in this Decision.

F. Packet Security Gateway (PSG)

In our Decision to Institute we construed "packet security gateway (PSG)" to mean "a gateway computer configured to receive packets and perform a packet transformation function on the packets." Dec. to Inst. 10–11. Neither party disputes our construction, and we apply it in this Decision.

G. Packet Transformation Function

In our Decision to Institute we construed packet transformation function" to mean "operations performed on a packet." Dec. to Inst. 11–13. Although Patent Owner maintains "packet transformation function" should be construed to mean "a function that transforms one or more packets from one state to another," Patent Owner states that it applied our construction for purposes of this proceeding. PO Resp. 17. As we stated in our Decision to Institute, Patent Owner's proposed construction is not meaningful because it uses a variation of the term "transform" to define "transformation." Dec. to Inst. 12–13. Our Decision to Institute also noted:

> the packet transformation function may perform a number of operations, such as: forwarding packets to the network or an IPsec stack; dropping packets or sending them to an infinite sink (e.g., *id.* [Ex. 1001] at 6:19–31); routing packets to a network address corresponding to a monitoring device whose address may be different from the packet's destination network address, and encapsulating packets with an IP header specifying the address corresponding to the monitoring device (*id*. at 11:14– 26); and producing a digest or log of the packet information (*id.* at 11:45– 54).

Dec. to Inst. 12–13. In consideration of the above, we apply the construction articulated in the Decision to Institute, and for purposes of this Decision also construe "packet transformation function" to mean "operations performed on a packet."

H. Packet-By-Packet

Neither party proposed a construction of the term "packet-by-packet" until Patent Owner filed its Sur-reply. PO Sur-reply 1. As justification for its last minute construction proposal, Patent Owner contends that it drafted its Patent Owner Response on the basis of deposition testimony by Petitioner's expert that "packet-by-packet" means "you're working a packet at a time." *Id.* (citing PO Resp. 25; Ex. 2009, Transcript of Deposition Testimony of Dr. Kevin Jeffay ("Jeffay Depo. Tr."), 48:8–16). According to Patent Owner, although Petitioner did not dispute its expert's testimony that "working a packet at a time" is the correct construction, the Petitioner Reply asserts that "packet-by-packet" encompasses analyzing "more than one packet at a time." *Id.* (citing Pet. Reply 7; Ex. 1020, Jeffay Reply Decl., ¶12).

It is unusual that the parties have proceeded so far in this proceeding and only now are contesting the construction of "packet-by-packet." Indeed, we are not convinced that we should construe "packet-by-packet" when the phrase used in claim 1 is "on a packet-by-packet basis." Both "packet-by-packet" and "on a packet-by-packet basis" are not defined in the Specification. It is unclear from the '213 patent whether "on a packet-by-packet basis" requires inspecting every single packet, even if the preceding packet indicates there is no application-layer packet-header information in the following expected packet. On the other hand, as packets may arrive out of order, it appears that some inspection of each packet may be necessary.

In the context of claim 1, it appears that the inclusion of the term "on a packet-by-packet basis" means performing the transformation function only on those packets that comprise the application-layer packet-header information specified in a rule. For example, claim 1 recites "identifying" such packets "on a packet-by-packet basis," and then "performing . . . the packet transformation function" on such packets.

In any case, we do not apply a construction that encompasses analyzing multiple packets at one time. However, the construction "working a packet at a time" offers little insight into what "on a packet-by-packet basis" actually means. At this late stage of the proceeding, we address this issue only to the extent necessary for this Decision in our substantive analysis of the claims, as explained below.

VI. ANALYSIS OF PRIOR ART CHALLENGES

A. Introduction

In our Decision to Institute, we determined that Petitioner had demonstrated a reasonable likelihood it would succeed on its challenge to claims 1–9 as obvious over Narayanaswamy in view of Kapoor, Johnson and Kjendal (*see* Dec. to Inst. 16–37) and on its challenge to claims 10–16 as obvious over these same references and DiffServ (*see id*. at 37–42). To prevail on its challenges at this stage, Petitioner must demonstrate by a preponderance of the evidence that the claims are unpatentable. 35 U.S.C. § 316(e); 37 C.F.R. § 42.1(d). "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 never

shifts to Patent Owner. *See Dynamic Drinkware, LLC. v. Nat'l Graphics, Inc*., 800 F.3d 1375, 1378 (Fed. Cir. 2015) (*citing Tech. Licensing Corp. v. Videotek, Inc*., 545 F.3d 1316, 1326–27 (Fed. Cir. 2008)) (discussing the burden of proof in *inter partes* review). Petitioner cannot satisfy its burden of proving obviousness by employing "mere conclusory statements," but "must instead articulate specific reasoning, based on evidence of record, to support the legal conclusion of obviousness." *In re Magnum Oil Tools Int'l, Ltd.*, 829 F.3d 1364, 1380 (Fed. Cir. 2016).

A claim is unpatentable under 35 U.S.C. § 103(a) if "the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains." *KSR Int'l Co. v. Teleflex Inc*., 550 U.S. 398, 406 (2007). The question of obviousness is resolved on the basis of underlying factual determinations, including: (1) the scope and content of the prior art; (2) any differences between the claimed subject matter and the prior art; (3) the level of skill in the art; and (4) objective evidence of nonobviousness, i.e., secondary considerations. *See 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*, 550 U.S. at 418 (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")).

B. Claims 1–9 As Obvious Over Narayanaswamy in View of Kapoor, Johnson and Kjendal

1. Over view of the References

Narayanaswamy discloses it was known an Intrusion Detection and Prevention (IDP) device residing at the edge of a network could employ pattern matching to detect malicious activity, but the time and resources required for an IDP device to recognize attack patterns could delay data delivery, thereby compromising threat prevention and connectivity. Ex. 1012 ¶¶ 4–5. IDP devices in Narayanaswamy provision services offered by network security devices by automatically selecting different policies, e.g., limiting packet flows differently under different conditions, to adapt or compensate for internal resource utilizations mapped to administrator specified thresholds that balance network safety and security with connectivity. *Id.* ¶ 6.

Kapoor discloses a unified network threat management approach in which a flow processing facility uses artificial neurons, such as a self - organizing map (SOM), to recognize disparate intrusion threat types. Ex. 1013 ¶¶ 13–14. Kapoor discloses that "[s]ecurity management may include the automatic logging of any and all access (or attempted access) to any and all resources in the networked computing environment." *Id*. ¶ 136. Kapoor discloses that action rules may specify an action that occurs when a header rule or content rule matches an aspect of a transport control protocol (TCP) packet or sequence of packets, and that the action rule may trigger a database transaction that modifies a logging database containing a log of alerts, packets, data cells, or information associated with them. *See id.* ¶¶ 209–211.

Johnson discloses a framer that extracts packets from a received frame, e.g., data packets or packet data in frames in a Synchronous Optical Network/Synchronous Digital Hierarchy compliant system, and generates digests of extracted packets, in accordance with the packet classification scheme in use. Ex. 1014, Abstract ¶ 13. For example, the digest may concatenate TCP or User Datagram Protocols (UDPs) from the packet's Internet Protocol (IP) header with the source port, and destination port from a packet's transport header, or use other data, or include data not from the packet's header. *Id.* ¶ 14.

Kjendal discloses an application identification function, a dynamic mirroring function, a policy based dynamic mirroring function, and a network system controller. Ex. 1009, 6:15–18. According to Petitioner Kjendal relates to monitoring traffic for analysis and security by sending copies of certain, identified packets to a monitoring device, based on policies provided to the device. Pet. 25 (citing) Ex. 1009, Abstract, 6:15-19; Ex.1004, Jeffay Decl., ¶130. Petitioner states that Kjendal further provides for identifying packets to mirror (i.e. send to a monitoring device) by analyzing the contents of their application-layer packet-header information. *Id.* (citing) E.1009, 30:14-16; E.x1004, Jeffay Decl., ¶¶160, 227-230

2. Claim 1

Our analysis of claim 1 in the Decision to Institute addressed each of the claim 1 limitations designated by Petitioner (limitations 1.1–1.9), and the motivation to combine the references. Dec. to Inst. 16–31. The Patent Owner Response contends: (1) that Petitioner failed to demonstrate Narayanaswamy and Kapoor disclose receiving a dynamic security policy from an SPMS, as recited in claim element 1.1 (*see* PO Resp. 19–23), (2) that Petitioner failed to demonstrate Narayanaswamy in view of Kapoor,

Johnson and Kjendal discloses identifying packets with application-layer packet-header information, as recited in claim element 1.4 (*see id*. at 23), (3) that Petitioner failed to demonstrate Narayanaswamy and Kapoor disclose identifying packets on a packet-by packet basis, as recited in claim element 1.4 (*see id.* at 23–28), (4) that the classification techniques disclosed in Narayanaswamy and Kapoor do not meet the language of the challenged claims (*id*. at 28–31), (5) that Kapoor and Johnson do not disclose the claimed packet digest logging function, as recited in claim limitations 1.5–1.8 (*see id*. at 31–40), (6) that Petitioner failed to demonstrate it would have been obvious to modify Narayanaswamy with Kapoor and Johnson (see *id.* at 40–44); and (7) that Kapoor and Johnson do not disclose routing the identified packets to a monitoring device in response to performing the packet transformation function as recited in claim element 1.9 (*see id*. at 44–49).

We address each of the disputed limitations of claim 1 below. For the undisputed limitations, the parties did not submit arguments or evidence during trial indicating our analysis of those limitations at institution should be modified. Upon review of the complete record, we adopt our analysis of the undisputed limitations from the Decision to Institute, and we find that a preponderance of the record evidence indicates the asserted combination of prior art teaches those undisputed limitations.

a) Claim Limitation 1.1

Petitioner contends that claim limitation 1.1 requires that "a SPM server provision a dynamic security policy, having a rule specifying application-layer packet-header information, to multiple security packet security gateways at the edge of a network," and that during prosecution the

Examiner correctly found the combination of Narayanaswamy and Kapoor discloses this element. Pet. 27.

Petitioner cites Narayanaswamy's Policy Distribution Module that provisions security policies to IDP devices as teaching the claimed SPM server. Pet. 27–28. Petitioner argues that policies provisioned by Narayanaswamy's Policy Distribution Module use rules to match a pattern of data found within packet-header information to identify a packet with certain application-layer packet header information. *Id.* at 28 (citing Ex. 1004, Jeffay Decl. ¶ 168; Ex. 1012 ¶¶ 48–50, 102).

Patent Owner argues Petitioner relies on an overly broad construction of "dynamic security policy." PO Resp. 20. Patent Owner contends that Narayanaswamy describes static security policies "given that they can only be updated, altered, or edited manually by a human network administrator." *Id.* at 21. Patent Owner further argues that Petitioner does not contend that Kapoor's packet inspection policies are dynamic security policies. *Id.*

As discussed above, we declined to adopt Patent Owner's proposal that we construe "dynamic security policy" to mean "a non-static set of one or more rule." Although Patent Owner acknowledges that the '213 patent discloses a dynamic security policy may be created manually, in responding to Petitioner's contentions concerning Narayanaswamy Patent Owner argues "what makes it a **dynamic** security policy is that the SPM can 'automatically create or alter one or more of such rules as new network[s] addresses associated with malicious network traffic are determined.'" *Id.* 20 (quoting Ex. 1001, 14:56–59). Patent Owner cites the testimony of Petitioner's expert, Dr. Jeffay, as supporting the principle that "dynamic" and "static" relates to whether the rules of the security policy are updated automatically. *Id.* at 20–21 (citing Ex. 1004, Jeffay Decl., ¶ 106). We note, however, that

the testimony Patent Owner cites refers to the *updating* of the policy and not to the definition of a dynamic security policy. A security policy is a dynamic security policy if it can be changed either manually or automatically. The dynamic nature of the policy does not change, even if the actual updating of the policy is characterized as static or dynamic depending upon whether that updating is performed manually or automatically. Patent Owner cites no disclosure in the '213 patent to support the distinction Patent Owner advocates as to the meaning of "dynamic security policy." Indeed, the '213 patent describes a user interface that permits an administrator to update a dynamic security policy manually. Ex. 1001, 14:2–47. Thus, we agree with Petitioner that, under the correct construction of the term, Narayanaswamy teaches claim limitation 1.1.

b) Claim Limitation 1.4

As discussed above, for purposes of this Decision only, we construe the term "packet" as used in the '213 patent to mean an L2 or L3 packet. Noting the cross examination testimony of Petitioner's expert, Dr. Jeffay, that "packet-by-packet" means working on a packet at a time, Patent Owner contends that Narayanaswamy and Kapoor do not disclose identifying packets on a packet-by-packet basis because each reference discloses reassembling payloads of packets of a communication flow before determining whether a rule's criteria is triggered. PO Resp. 24–25 (citing Ex. 2009, Jeffay Depo. Tr, 48:8–16). Patent Owner emphasizes Dr. Jeffay's testimony that an application layer message may be broken into multiple parts spanning multiple packets and it is necessary "to take the parts of the message as they appear on the wire and put them back together to see what the application-layer message is." *Id.* at 25–26 (quoting Ex. 2009, Jeffay Depo. Tr., 77:9–18). According to Patent Owner, Dr. Jeffay's declaration

testimony is that "Narayanaswamy teaches identifying and inspecting HTTP application packets," but his deposition testimony acknowledges that the challenged claims do not refer to application layer packets "because you can't receive an application-layer packet." *Id.* at 26–27 (comparing Ex. 2004, Jeffay Decl, ¶ 193 with Ex. 2009, Jeffay Depo. Tr., 44:7–46:8).

Petitioner contends that Patent Owner misunderstands Dr. Jeffay's testimony. Pet. Reply 5–6. Petitioner explains that there is no dispute HTTP headers and payloads are embedded within L2 and L3 packets and argues that Patent Owner does not dispute the IDP devices in Narayanaswamy receive such L2 and L3 packets. *Id.* at 6; *see also* PO Sur-reply 8–9 [acknowledging "application-layer information does arrive at Narayanaswamy's IDP devices as the payload of L2 or L3 packets"]. According to Petitioner, a person of ordinary skill would understand that Narayanaswamy inspects application-layer information extracted from the payload of network or link packets. Pet. Reply 6 (citing Ex. 1020, Declaration of Dr. Kevin Jeffay In Support of Petitioner's Reply. ("Jeffay Reply Decl.") ¶¶ 27–41, 85—93). Petitioner cites Figure 5A of Narayanaswamy as evidence, consistent with Dr. Jeffay's deposition testimony "you're working a packet at a time" (Ex. 2009, Jeffay Depo. Tr. 48:8–16), that Narayanaswamy teaches looking at each packet to identify application layer information embedded therein. Pet. Reply 7. Petitioner points out in Figure 5A, after comparing the packet to others in a transaction flow, Narayanaswamy's IDP determines whether to forward the packet, quarantine it, or drop it. *Id.* (citing Ex. 1012 ¶ 102; Ex. 1020, Jeffay Reply Decl. ¶¶ 85–86). Petitioner further notes that Narayanaswamy's pattern matching is similar to that disclosed in the subject '213 patent concerning an

HTTP GET or HTTP PUT method call. *Id.* at 8 (citing Ex. 1001, 21:48–64, 26:12–19, 26:29–36; Ex. 1020, Jeffay Reply Decl. ¶86).

Patent Owner argues that, to the extent Narayanaswamy classifies incoming packets using application-layer decoders, it does so using reassembled application-layer communications. PO Resp. 30–31 (citing Ex. 1012 ¶ 30). According to Patent Owner, "Narayanaswamy is clear that it does not extract application layer information from **packets**, but from **application-layer communications** reassembled from multiple packets." PO Sur-reply 9 (citing Ex. 1012 ¶¶ 30–31). Patent Owner contends that Narayanaswamy's "pattern matching" does not occur on a packet-by-packet basis and that Narayanaswamy does not look at each packet, identify application-layer packet header information embedded in the packet and compare the packet to others in the transaction. *Id.* at 9.

To the extent Patent Owner argues Narayanaswamy's discussion of reassembly (Ex. 1012 ¶ 30) teaches a "different technique," Petitioner states that such reassembly is an alternative or additional form of malicious traffic analysis cited by Dr. Jeffay to show Narayanaswamy teaches inspecting application-layer packet-header information, not to demonstrate packet-by-packet analysis. Pet. Reply 10–11 (citing Ex. 1020, Jeffay Reply Decl. ¶¶ 7–20, 93). Paragraph 30 of Narayanaswamy states that IDP device 4 may identify packet flows in monitored traffic and reassemble application-layer communications using protocol specific decoders to analyze the application-layer communications and identify application-layer transactions. Ex. 1012 ¶ 30. In this context, "'transaction' refers to a bounded series of related application-layer communications between peer devices." *Id.* Thus, in Narayanaswamy an IDP device may invoke an HTTP decoder to identify each request/response within a TCP connection as a different transaction in

an effort to prevent certain attack patterns from being applied across transaction boundaries. *Id.* For each transaction, a decoder may analyze the application-layer communications and extract protocol-specific elements. Thus, IDP device 4 may apply the patterns to the protocol elements extracted by the protocol decoders to detect and prevent network attacks. *Id.* ¶ 33. Narayanaswamy discloses that classifier module 26 may include the protocol decoders "to extract this application-layer information or data to classify each packet." *Id.* at ¶ 50. Thus, Narayanaswamy teaches receiving incoming traffic and classifying each packet to one of ordinary skill.

Claim limitation 1.4 is drawn to identifying on a packet-by-packet basis, packets comprising the application-layer packet-header information. The subject '213 patent does not define the meaning of the claim language "on a packet-by-packet basis" explicitly, nor does claim limitation 1.4 recite the specific steps to accomplish the claimed identification on a packet-by-packet basis. The recitation of a step to identify one or more packets that contain application-layer packet-header information indicates that not all packets contain application-layer packet-header information.

Figure 5A of Narayanaswamy illustrates the steps of receiving incoming traffic, classifying the packet, determining if the packet is part of a new information flow, and, if so, determining whether to forward the packet without further processing or if the packet is associated with a new information flow. In the latter case, the packet is processed in accordance with the rules of the policy associated with that flow and, based on a pattern match, is forwarded, dropped or subject to quarantine. *See*. Ex. 1001, Fig. 5A. Narayanaswamy uses a classifier module "that may classify each of the packets based on information extracted from each packet." Ex. 1012 ¶ 48.

In support of its position that Narayanaswamy's classification module does not identify packets that include specified application-layer packet-header information on a packet by packet basis, Patent Owner argues that Petitioner conflates packet identification based on 5-tuple values discussed in paragraphs 48 and 49 of Narayanaswamy with extracting application layer information discussed in paragraph 50. PO Sur-reply 11. One alternative is to classify each packet as belonging to a particular flow by extracting a "five-tuple" found within the header of each of the packets. *See id.* at 11–12. Another way Narayanaswamy's classifier module classifies incoming packets is to "extract application layer information, such as Session Initiation Protocol (SIP) headers and payload data and Real-time Transportation Protocol (RTP) headers and payload data," i.e., "to extract this application layer information or data to classify each packet." *Id.* ¶ 50. Based on the extracted information, the classifier module can identify whether a packet belongs to an HTTP application or FTP application, and associate the packet with the appropriate policy. Ex. 1012 ¶50.

Patent Owner argues that Narayanaswamy's protocol decoders operate on reassembled application layer communications. PO Sur-reply 11–12 (citing Ex. 1012 ¶30). The issue before us, however, is not whether Narayanaswamy discloses the exact steps claimed, but instead what Narayanaswamy would have taught or suggested to one of ordinary skill in the art. As noted above, Petitioner does not rely on the reassembly techniques discussed in paragraph 50 of Narayanaswamy to disclose packet-by-packet analysis, but to disclose inspecting application-layer packet-header information. Pet. Reply 10–11 (citing Ex. 1020, Jeffay Reply Decl. ¶¶ 7–20, 93).

We also note that claim 9, which depends from claim 1, recites the at least one rule in the dynamic security policy comprises a five-tuple used to identify the packets comprising the application packet-header information. Although we do not limit claim 1 to the features recited in claim 9, we do not construe claim 1 to exclude them.

Dr. Jeffay points out that a person of ordinary skill would understand that "any security gateway would act on a packet-by-packet basis, because any other method would not inspect all packets and would allow threats to penetrate the protected network." Ex. 1004, Jeffay Decl. ¶ 190. Paragraph 15 of Narayanaswamy discloses a method in which a network security device has a "first path for processing initial packets of new packet flow" as distinguished from "a fast path for processing packets for existing packet flows." Ex. 1012 ¶ 15. We also note that in the case of dynamic determination of policy, Narayanaswamy states "the second policy specifies that the first set of attack patterns are to be applied to all the packets of the fast path for the existing packet flow setup prior to the dynamic determination and without application to all the packets of the new flows that go through the first path after the dynamic determination." *Id.* As to Kapoor, Petitioner notes that Kapoor discloses its flow processing facility inspects "the payload of a network [application] layer packet to detect strings that match a form of invalid application layer packet header." Pet. Reply 11 (quoting Ex. 1013 ¶ 461). Patent Owner contends that the analysis of Kapoor by Petitioner's expert, Dr. Jeffay, relies on inspection of application layer packets, rather than network layer packets, and that in Kapoor, the packets must be reassembled in much the same fashion as the destination system reassembles the packets into messages. PO Resp. 27. Dr. Jeffay states more specifically in his Reply Declaration that Kapoor

teaches inspecting application layer packets within the payload of network layer packets. Pet. Reply 12, (citing Ex. 1020, Jeffay Reply Decl. ¶ 95). Petitioner also points to Figure 31 of Kapoor to emphasize that Kapoor recognizes the payload of one packet (e.g., a network layer packet) may contain a higher level packet (an application layer packet). *Id*. at 11.

Kapoor states as follows:

> in a networked computer environment using packet switching communication, *network security policies may be enforced by inspecting a packet* and, as necessary, *responding to a result of the packet inspection*. The packet inspection may be directed at a header of the packet and/or a payload of the packet. *Such packet inspection may be performed at any and all layers of a network communication protocol stack* (such as and without limitation the Internet Protocol stack). Inspecting the payload of the packet may be referred to as "deep packet inspection" or "payload inspection." In any case, any and all packet inspection may be directed at the inspection of data that encompasses a packet or flow of packets. A flow processing facility may facilitate inspecting the content of packet payloads using content matching, behavioral anomaly detection, a combination of both, and so on.

Ex. 1013 ¶ 23 (emphasis added).

Patent Owner contends that, like Narayanaswamy, Kapoor must be read in the context of Kapoor's disclosure of reassembling packet data in the same fashion as the destination system reassembles the packets into messages. PO Sur-reply 13 (citing Ex. 1013 ¶ 403). According to Patent Owner paragraph 23 of Kapoor is better understood as describing the tautological fact that the term packet inspection refers to the inspection of data within a packet or flow of packets. *Id.* Nevertheless, paragraph 23 of Kapoor is broadly written to address the enforcement of network security

policies by inspecting a packet "at any and all levels" of a network protocol stack and responding accordingly. Ex. 1013 ¶ 23.

In view of the packet-by-packet approach illustrated in Figure 5A of Narayanaswamy, the disclosure by Narayanaswamy that its classifier module extracts application layer information from each packet, and Kapoor's disclosure of inspecting individual packets, we are persuaded that Petitioner has demonstrated the combination of Narayanaswamy and Kapoor would have taught claim element 1.4 to one of ordinary skill.

c) Claim Limitation 1.5

Patent Owner does not address claim limitation 1.5 specifically. However, claim limitation 1.5 recites a transformation function comprising the steps recited in claim limitations 1.6–1.8. Patent Owner contests whether the references disclose the packet transformation function recited in claim limitations 1.6–1.8. Petitioner contends that Narayanaswamy teaches the PSG performing the packet transformation function on each of the packets comprising application-layer packet header information (claim limitation 1.5). Pet. 38 (citing Ex. 1012, Fig. 5A (steps showing processing the packet in accordance with the associated policy (step 72), including forwarding (step 78), or placing a packet in quarantine or dropping a packet (step 76))). Petitioner also contends that Kapoor's disclosure of accepting packets, denying packets or logging packets containing certain application-layer packet header information also teaches this limitation. *Id.* at 39 (citing Ex. 1004, Jeffay Decl. ¶¶ 204–205; Ex. 1013 ¶¶ [0067], [0087], [0122], [0211], [0461], [0523]-[0525]). We agree with Petitioner and find that the cited evidence indicates by a preponderance that the combination of Narayanaswamy and Kapoor would have taught performing the packet transformation function on each of the packets, as recited in claim limitation

1.5. As Patent Owner contests whether the references disclose the packet transformation function recited in claim limitations 1.6–1.8, we address those limitations below.

d) Claim Limitation 1.6

Petitioner contends that the combination of Kapoor and Johnson teaches claim element 1.6, i.e., "identifying a subset of information specified by the packet digest logging function for each of the one or more packets comprising the application-layer packet-header information." *Id.* at 39–40. Petitioner cites Kapoor as teaching system logging and suggesting that the information to be logged may be a subset of information from the application packet (*id.* at 29 (citing Ex. 1013 ¶¶ 211); Ex. 1004, Jeffay Decl. ¶¶ 207–209) and Johnson as disclosing including specified packet information in a digest (*id.* at 40 (citing Ex. 1014 ¶ 14); Ex. 1004, Jeffay Decl. ¶ 210).

Patent Owner contends that claim limitation 1.6 requires more than identifying the information to be logged—it requires "identifying a subset of information **specified by the patent digest logging function** for each of the one or more packets comprising the application layer packet-header information." PO Resp. 32–33. Patent Owner notes that implementing a packet digest logging function as claimed permits the information to be tailored to the condition matched by the rule, enhancing the ability to produce awareness information. *Id.* at 32 (citing Ex. 2004, Declaration of Dr. Michael Goodrich ("Goodrich Decl."), ¶ 156; Ex. 1001 11:34–60).

According to Patent Owner, Kapoor and Johnson lack the level of granularity and specificity enabled by the techniques claimed in the '213 patent. *Id.* Patent Owner criticizes Petitioner's argument that Kapoor suggests the information to be logged may include a subset of information

from the packet, citing the testimony of Patent Owner's expert that a person of ordinary skill would understand "information associated with" to be information related to the packet, e.g., information related to the logged packet's classification. *Id*. at 33 (citing Ex. 2004, Goodrich Decl. ¶ 157). Patent Owner further contends that Petitioner's argument concerning Kapoor logging information from an application packet means such logging is not performed on a network layer packet-by-packet basis. *Id.* at 33–34. Kapoor, however, discloses inspecting packets at all levels. Ex. 1013 ¶ 23.

Patent Owner also argues that Johnson fails to disclose the same patent logging function as recited in the claims or a packet logging digest function implemented as a packet transformation function and, instead discloses a technique to speed classification lookups, using digests made proactively for the purpose of classifying packets. *Id.* at 34–36. Although Patent Owner notes that a European Examiner found a corresponding claim allowable over Johnson, Patent Owner does not mention the European Examiner did not address the combination of Kapoor and Johnson advanced by Petitioner. *See* PO Resp. 34, Pet. Reply. 14

As Petitioner points out, Kapoor discloses logging packets identified by an "action rule" in its security policy, including packets comprising application-layer packet-header information. Pet. Reply 13 (citing Ex. 1013 ¶ 211 ("the logging database may contain a log of alerts 442, packets . . . or information associated with any of all of the foregoing")). Petitioner acknowledges Kapoor does not teach the specific subset of information to be logged, but notes Johnson discloses using a subset of specific information from a packet, or data not from the packet header, to generate a digest that can be used in a scheme that classifies packets. *Id.*; Ex. 1014 ¶ 14. Johnson also states "[m]any devices perform packet classification to tailor subsequent

processing of a packet." Ex. 1014 ¶ 8. Like Kapoor, Johnson discloses that a packet digest can include a variety of characteristics, such as data included in the packet's header(s) or payload. *Id.* ¶ 9. Thus, Johnson discloses it was known to implement a patent digest function using information specific to carrying out a particular function. Read in the context of Kapoor, we are persuaded by Petitioner's argument that a person of ordinary skill would have understood the combined teachings of Kapoor and Johnson would have taught claim limitation 1.6 to one of ordinary skill.

e) Claim Limitation 1.7

Claim element 1.7 recites "generating, for each of the one or more packets comprising the application-layer packet-header information, a record comprising the subset of information specified by the packet digest logging function."

As we agree with Petitioner the combination of Kapoor and Johnson teaches or suggests the logging function recited in claim limitation 1.6, we are not persuaded by Patent Owner's argument that claim limitation is not taught because claim element 1.6 is not taught. PO Resp. 32. For the reasons discussed above relative to claim element 1.6, we also are not persuaded by Patent Owner's argument that Johnson fails to cure Kapoor's deficiencies because Johnson does not create packets digests as a packet digest logging function. *Id.* at 37.

Petitioner contends that Kapoor teaches modifying a logging database and that making such a modification involves generating a record. Pet. 41. Petitioner further argues that, even if Kapoor does not disclose this feature, Johnson discloses generating a record containing a subset of information identified from the packet. *Id.* at 42 (citing Ex. 1004 ¶ 217; Ex. 1004, Jeffay Decl. ¶ 15)

Patent Owner contends there is insufficient evidence to support Dr. Jeffay's assertions, arguing there is no basis to believe a person of ordinary skill would generate a record when modifying a database. PO Resp. 37 (citing Ex. 2004, Goodrich Decl. ¶ 161). Dr. Jeffay replies that information in a database is referenced commonly as a "record" and that a modification of such information must generate a new record, e.g., adding an entry to a logging database would involve generating a record that includes information to be added to the log. Ex. 1020, Jeffay Reply Decl. ¶ 103. Recognizing that in the absence of a new record, a database is not modified, we find Dr. Jeffay's testimony that modifying a database implicates generating a new record to be credible. Thus, we are persuaded that Petitioner has demonstrated the combination of Kapoor and Johnson teaches claim limitation 1.7

f) Claim Limitation 1.8

Claim limitation 1.8 recites "reformatting, for each of the one or more packets comprising the application-layer packet-header information, the subset of information specified by the packet digest logging function in accordance with a logging system standard." As we have determined above that the combination of references teaches claim limitations 1.6 and 1.7, we are not persuaded by Patent Owner's arguments that claim limitation 1.8 is not taught because claims limitations 1.6 and 1.7 are not taught. PO Resp. 38.

Petitioner argues that the '213 Specification acknowledges "standard" logging formats, such as Syslog, and cites at least Kapoor as teaching sending log information to a central Security Event Information Management (SEIM) repository that accepts log information in a variety of standard formats, such as Syslog. Pet. at 43–44 (citing Ex. 1013, ¶¶ 532; Ex.

1004 ¶ 221). Petitioner further argues a person of ordinary skill would understand that the packet digest created in Johnson by selectively shifting bits of the packet into a register as the packet bits are output by the framer could be reformatted into a standard format such as Syslog. *Id*. at 44 (citing Ex. 1014 ¶ 15; Ex. 1004 ¶ 217).

Referring to Kapoor's logging database, Patent Owner contends that a person of ordinary skill would not have reformatted the subset of information in accordance with a logging standard prior to modifying the database because "a database is not a log." PO Resp. 38. (citing Ex. 2004 ¶164. Petitioner replies that Kapoor states explicitly that "[t]he logging ***database*** may contain of ***log*** of alerts, 442, packets 402, data cells 408, or information associated with any and all of the foregoing." Pet. Reply 15–16 (citing Ex. 1013 ¶ 211).

Patent Owner further argues that Kapoor receives "event information," such as information regarding a flow processing facility encountering a failure, and Petitioner fails to establish that any information sent to Kapoor's SEIM would include the subset of information specified by the packet digest logging function. PO Resp. 39 (citing Ex. 2004, Goodrich Decl. ¶ 165). Petitioner replies that reading paragraph 532 of Kapoor a person of ordinary skill would recognize "security events" are sent to the SEIM, not information about encountering a system failure. Pet. Reply 16 (citing Ex. 1020, Jeffay Reply Decl., ¶¶ 107–108). Petitioner's characterization comports with Kapoor's description of the network security infrastructure as including an SEIM maintained in a management server "to provide central logging for security events." Ex. 1013 ¶ 532.

We also are not persuaded by Patent Owner's argument that the existence of an SEIM as taught by Kapoor does not imply the reformatting

data in accordance with a logging system standard because many SEIMs use proprietary logging systems. PO Resp. 40 (citing Ex. 2004, Goodrich Decl. ¶ 168). As Petitioner points out, there is no requirement for SEIMs to use a proprietary logging system, and, in the context of an obviousness analysis, formatting data to implement an SEIM using well-known system would have been an obvious design choice. *See* Pet. Reply 16.

We find that the evidence cited by Petitioner establishes that a person of ordinary skill would have been taught by the combination of Kapoor and Johnson to practice limitation 1.8, for the reasons presented in the Petition and Petitioner's Reply, as discussed above.

g) Claim Limitation 1.9

Claim limitation 1.9 recites "routing, by the packet security gateway and on a packet-by-packet basis, to a monitoring device each of the one or more packets corresponding to the application-layer packet-header information in response to the performing the packet transformation function." Petitioner cites Kapoor as disclosing generally the act of routing a packet to a monitoring device and Kjendal as describing a system for routing to a monitoring device. Pet. 46. Petitioner notes Kapoor's disclosure that at least one copy of the data flow proceeds to machine learning logic and another to a data flow router as evidence that a person of ordinary skill would understand Kapoor teaches routing on a packet-by-packet basis a packet or copy of a packet both toward its destination and to a network monitoring facility. Pet. 45 (citing Ex. 1013 ¶ 478; Ex. 1004, Jeffay Decl,, ¶ 225). Petitioner further cites Kapoor as disclosing circumstances for routing packets to a monitoring device, e.g., to monitor packets from a device attempting to spread a virus. *Id.* (citing Ex. 1013 ¶¶ 501; Ex. 1004, Jeffay Decl. ¶ 226). Petitioner cites Kjendal as teaching packets may be

routed or forwarded to a monitoring device, i.e., mirrored, based on factors, including application-layer packet-header information. *Id.* (citing Ex. 1009, 8:59–9:3)

Patent Owner contends that Kapoor directs one copy of the data flow to machine learning logic, but does not route packets on a packet-by-packet basis. PO Resp. 44–45. Patent Owner further contends that Petitioner has not demonstrated that Kapoor's machine learning logic is a monitoring device, as claimed, or that Kapoor's data flows are sent to the machine learning logic in response to performing a packet transformation function specified by a rule of a dynamic security policy. *Id.* at 45. Patent Owner further contends that because Kjendal's techniques also are directed to mirroring flows rather than packets on a packet-by-packet basis, Kjendal does not cure the deficiencies in Kapoor.

According to Patent Owner, even if the teachings of Kapoor and Kjendal were combined, the combined system would not result in routing packets to a monitoring device, because Kapoor's machine learning logic is a classifier that classifies packets prior to applying any packet transformation function. *Id.* at 46 (citing Ex. 2004, Goodrich Decl. ¶ 176).

As Petitioner points out, Kapoor discloses that a web client attempting to propagate a virus detected by a flow processing facility (the claimed PSG) may have all further packets associated with that web client dropped or directed to a security port for further analysis. Pet. Reply 18–19; Ex. 1013 ¶ 501. Petitioner notes that, by directing the selected packets to the security port, Kapoor teaches performing a transformation function on each packet. *Id.* at 18 (citing Ex. 1013 ¶501). As Dr. Jeffay testifies, a person of ordinary skill would understand that packets sent to the security port would be routed to a monitoring device for further analysis. Ex. 1020, Jeffay Reply Decl.

¶ 119. We are also persuaded by Dr. Jeffay's testimony that within the flow processing facility the logic that applies the security policy would be separate from the logic that acts as the monitoring device. Pet. Reply 19 (citing Ex. 1020, Jeffay Reply Decl. ¶¶ 118, 123).

Kapoor also discloses that when a data flow facility receives a data flow, that data flow may be sent to a router through a delay and almost simultaneously provided to machine learning logic that classifies the data flow. Ex. 1013 ¶¶ 478–479. The router receives the classifications or application identifiers and security policies and decides further information flow. *Id.* ¶¶ 479–480. Petitioner notes that accepting the packets in the information flow and forwarding them to the machine logic constitutes an "accept packet" transformation function. Pet. Reply 18.

In consideration of the above, we are persuaded that Petitioner has demonstrated the disputed limitations of claim 1 would have been taught by the combination of the Narayanaswamy, Kapoor, Johnson, and Kjendal.

h) Motivation to Combine the Teachings of Narayanaswamy, Kapoor, Johnson, and Kjendal

Petitioner contends that a person of ordinary skill would have been motivated to combine the teachings of the references because each reference teaches specific software-based implementations of systems generally referred to by the other references. Pet. 25 (citing Ex. 1002, 434–35; Ex. 1004 ¶¶ 147–159).

Petitioner further contends that Johnson teaches implementing a known technique (packet digesting) that Narayanaswamy and Kapoor refer to generally. *Id.* at 26. Patent Owner contends Petitioner effectively abandoned this argument in the Petitioner Reply. PO Sur-reply 17.

Patent Owner contends Petitioner misrepresents the teachings of Narayanaswamy and Kapoor because neither the references nor paragraph 159 of the Jeffay Declaration cited by Petitioner refers to packet digesting. PO Resp. 40–41 (citing Ex. 2004, Goodrich Decl. ¶ 103). According to Patent Owner, Dr. Jeffay does not identify any disclosure in Narayanaswamy or Kapoor relating to packet digesting. *Id.* at 42.

Patent Owner further contends Petitioner's arguments that it would have been obvious to modify Narayanaswamy with Kapoor and Johnson are "boilerplate" and fail to provide a reason a person of ordinary skill would have combined particular elements of the prior art to reach the claimed invention. *Id.* at 41–42 (citing *Heart Failure Techs., LLC v. CardioKinetix, Inc.*, IPR2013-00183, Paper No. 12 at 9 (PTAB July 31, 2013) (citing *KSR Int'l Co. v. Teleflex, Inc.*, 550 U.S. 398, 418 (2007)). Patent Owner presents similar arguments in disputing a motivation for combining the teaching of Kjendal with those of Narayanaswamy, Kapoor, and Johnson. *Id.* at 47.

Patent Owner further argues the case for combining the teachings of Narayanaswamy with Kapoor and Johnson lacks foundation because Petitioner provides few details from Narayanaswamy about implementing alerts based on intrusion detection and because system level alerts in Narayanaswamy are based on utilization of internal resources and an IDP, not whether a packet matches a rule in a dynamic security policy. PO Resp. 42–43.

Citing its discussion of claim limitation 1.6, Patent Owner argues a person of ordinary skill would not have had reason to combine the teachings of Kapoor and Johnson. PO Resp. 40. In its discussion of claim element 1.6, Patent Owner disputes Petitioner's assertion that a person of ordinary skill would have had reason to combine the teachings of Kapoor and

Johnson because Johnson provides specific examples of the suggestions of Kapoor. *Id.* at 35–36. According to Patent Owner (1) a person of ordinary skill would not have understood Kapoor to disclose identifying a subset of information from a packet when making a modification to a logging database and, therefore, would not have been motivated to seek out a technique for generating a packet digest to assist Kapoor in modifying its logging database; and (2) Johnson is not concerned with packet logging. *Id.*

We addressed claim limitation 1.6 in detail above, noting that Kapoor discloses logging packets identified by an "action rule" in its security policy, including packets comprising application-layer packet-header information (Ex. 1013 ¶ 211), and Johnson states "[m]any devices perform packet classification to tailor subsequent processing of a packet" (Ex. 1014 ¶ 8). As our discussion of claim limitation 1.6 demonstrates, we agree with Petitioner that, in view of these disclosures a person of ordinary skill would have been motivated to combine the teachings of Kapoor and Johnson.

In assessing the motivation to combine the teachings of the references, we do not take lightly the fact that the Examiner considered Narayanaswamy and Kapoor during examination of the application that led to issuance of the '213 patent, and concluded a skilled artisan would have been motivated to combine their teachings. *See, e.g.*, Ex. 1002, 443–447. The Examiner explicitly states:

> Kapoor and Narayanaswamy are analogous art as they are in the same field of endeavor of information security. It would have obvious to one of ordinary skill in the art before the effective filing date of the claimed invention to receive a dynamic security policy that includes at least one rule (as disclosed by Narayanaswamy) specifying application-layer packet-header information (as taught by Kapoor) and a packet transformation function to be performed on packets (as disclosed by

> Narayanaswamy) comprising the application-layer packet-header information (as taught by Kapoor). The motivation/suggestion would have been to address patterns relevant to a variety of types types of network and data integrity threats that relate to computer system (Kapoor, Abstract).

Ex. 1002, 435–436. "Prior art is analogous where either (1) 'the art is from the same field of endeavor, regardless of the problem addressed' or (2) even if the reference is not within the same field of endeavor, 'the reference still is reasonably pertinent to the particular problem with which the inventor is involved.'" *In re Ethicon, Inc.*, 844 F.3d 1344, 1349 (Fed. Cir. 2017) (quoting *In re Clay*, 966 F.2d 656, 658–59 (Fed. Cir. 1992)). Applying the Federal Circuit's standard, we agree with the Examiner that Narayanaswamy and Kapoor are analogous art.

As discussed above, Petitioner also asserts Johnson as a basis for its challenge to claims 1–9. Patent Owner argues Petitioner has not established it would have been obvious to implement the combined system of Kapoor and Johnson with Narayanaswamy. PO Sur-reply 16. Petitioner notes that Kapoor teaches packet logging. Pet. Reply 17 (citing Ex. 1013 ¶¶ 87, 211 ("logging database may contain a log of alerts 442, **packets 402**, data cells 408, or **information associated with any and all of the foregoing**"). Petitioner points out that Johnson's implementation of packet digest logging (Ex. 1014 ¶ 14) would be used as part of the packet-by-packet analysis performed on packet flows in Narayanaswamy. Pet. Reply 17. Patent Owner acknowledges that this argument by Petitioner is "apparent motivation for combining Johnson directly with Narayanaswamy," but argues it does not cure any identified deficiency with Narayanaswamy. PO Sur-reply 16–17. We discuss Narayanaswamy extensively above, and are not persuaded that Narayanaswamy is deficient as a reference. Johnson

states "a digest can be used in a scheme that classifies packets" and "[o]ther digests can include other data."

As to Kjendal, Patent Owner contends if a person of ordinary skill used Kjendal's techniques to route data flows to Kapoor's machine learning logic, the combined system would not route packets to a monitoring device. PO Resp. 46. We addressed this argument in our discussion of claim limitation 1.9 above and did not find it persuasive.

Patent Owner argues that Narayanaswamy, Kapoor, Johnson, and Kjendal are disparate systems that one of ordinary skill would not have been motivated to combine. PO Resp. 47.

We are not persuaded that Narayanaswamy, Kapoor, Johnson, and Kjendal are "disparate." Narayanaswamy seeks to allow an administrator to balance network safety and security with network connectivity, for example using a "first path for processing initial packets of new packet flow and a fast path for processing packets for existing packet flows." Ex. 1012 ¶¶ 1006, 1015. Kapoor also teaches a flow processing facility to provide security and protection to a computer or computer system based on inspecting packets. Ex. 1013, Abstract, ¶ 23. We discuss the specific teachings of Narayanaswamy and Kapoor, extensively above and there is an apparent motivation to combine the teachings of Johnson with Narayanaswamy. We are further persuaded by Petitioner's arguments that a person of ordinary skill would have looked to the teachings of Kjendal, as that reference is not only in the same field, but deals specifically with network security via packet inspection. Pet. 26.

In view of the above, we are persuaded that a person of ordinary skill would have been motivated to combine the teachings of Narayanaswamy, Kapoor, Johnson, and Kjendal.

C. Claims 2–9

Our Decision to Institute addresses explicitly claims 2–9, which all depend from independent claim 1. Dec. to Inst. 32–37. Patent Owner contends that claims 2–9 are patentable, based on its arguments that claim 1 is patentable, but does not respond specifically to Petitioner's challenges to claims 2–9. PO Resp. 49. As explained further below, we have reviewed the record and find that, based on the same reasoning considered in our Decision to Institute, Petitioner has demonstrated by a preponderance of the evidence that claims 2–9 would have been taught by the combination of Narayanaswamy, Kapoor, Johnson, and Kjendal.

1. Claim 2

Claim 2 depends from claim 1 and recites "the at least one rule indicates performing an accept packet transformation function on the packets comprising the application-layer packet-header information, and wherein the performing the packet transformation function comprises forwarding, by the packet security gateway, the each of the one or more packets comprising the application-layer packet-header information toward its respective destination." We are persuaded by Petitioner's arguments that Narayanaswamy discloses identifying certain packets via policy and accepting and forwarding acceptable packets, as illustrated in Figure 5A. Pet. 47–48 (citing Ex. 1012 ¶¶ 11–15, 62, 72, 78, 93, Fig. 5A; Ex. 1004, Jeffay Decl. ¶ 234). We are also persuaded by Petitioner's arguments that Kapoor discloses embodiments with actions (transformation) of forwarding acceptable identified packets. *Id.* at 48 (citing Ex. 1013 ¶¶ 210, 590, Ex. 1004, Jeffay Decl. ¶¶ 236–237).

2. Claim 3

Claim 3 depends from claim 1 and recites "the at least one rule indicates performing a deny packet transformation function on the packets comprising the application layer packet-header information, and wherein the performing the packet transformation function on comprises dropping, by the packet security gateway, the each of the one or more packets comprising the application-layer packet-header information." Similar to its analysis of claim 2, Petitioner persuasively argues Narayanaswamy and Kapoor disclose denying and dropping packets. Pet. 49–50.

3. Claim 4

Claim 4 depends from claim 1 and recites "the application-layer packet-header information identifies one or more hypertext transfer protocol (HTTP) packets, and wherein identifying the one or more packets comprising the application-layer packet-header information comprises determining by the packet security gateway that the one or more packets comprising the application-layer packet-header information are amongst the one or more HTTP packets." Petitioner persuasively argues that Narayanaswamy teaches "identifying HTTP packets to locate anomalies in the packet-header information to prioritize between packet types." Pet. 50–51 (citing Ex. 1012 ¶¶ 31–32; Ex. 1004, Jeffay Decl. ¶¶ 246–247). Petitioner also persuasively argues that Kapoor teaches scanning data flow of an HTTP session and scanning packets for certain URLs within application-layer packet-header information associated with an HTTP GET request. *Id.* at 51 (citing Ex. 1013 ¶ 156; Ex. 1004, Jeffay Decl. ¶¶ 248–249).

4. Claim 5

Claim 5 depends from claim 4 and recites "the one or more HTTP packets comprise an HTTP GET method call, and wherein determining that the one or more packets comprising the application-layer packet-header information are amongst the one or more HTTP packets comprises determining that the one or more packets comprising the application-layer packet-header information are associated with the HTTP GET method call." Petitioner persuasively argues Kapoor discloses that a system may process a data flow in order to recognize patterns that suggest the presence of a URL, or request access to a URL, such as one that is blacklisted or suspect, where the request is embodied in an HTTP GET. Pet. 52 (citing Ex. 1013 ¶ 603; Ex. 1004, Jeffay Decl. ¶¶ 252–253).

5. Claim 6

Claim 6 depends from claim 5 and recites "the HTTP GET method call specifies a uniform resource identifier (URI), and wherein determining that the one or more packets comprising the application-layer packet-header information are associated with the HTTP GET method call comprises determining that the one or more packets comprising the application-layer packet-header information originated from or are destined for a network address corresponding to the URI." Petitioner notes that claim 5 recites a rule using a required feature of an HTTP GET packet and cites Kapoor as disclosing filtering on URI/URL. Pet. 53 (citing Ex. 1004, Jeffay Decl. ¶¶ 254–257). Thus, we are persuaded Petitioner has demonstrated claim 6 would have been taught by the combination of the references.

6. Claim 7

Claim 7 depends from claim 4 and recites "the one or more HTTP packets comprise an HTTP PUT method call, and wherein determining that

the one or more packets comprising the application-layer packet-header information are amongst the one or more HTTP packets comprises determining that the one or more packets comprising the application-layer packet-header information are associated with the HTTP PUT method call." Petitioner notes that claim 7 recites a long-known HTTP request method, i.e., PUT, in which an HTTP packet asks a web server to create or replace content at the list URL with data found within the body of the HTTP packet. Pet. 54. Petitioner persuasively argues Kapoor teaches identifying HTTP application packets and performing transformations based on the Request Method found therein. *Id.* (citing Ex. 1013 ¶ 458; Ex. 1004, Jeffay Decl. ¶¶ 139–145, 258–259).

7. Claim 8

Claim 8 depends from claim 7 and recites "the HTTP PUT method call specifies a uniform resource identifier (URI), and wherein determining that the one or more packets comprising the application-layer packet-header information are associated with the HTTP PUT method call comprises determining that the one or more packets comprising the application-layer packet-header information originated from or are destined for a network address corresponding to the URI." Petition persuasively argues that Kapoor discloses the features of claim 8 for the same reasons it discloses the features of claim 6 concerning HTTP GET packets and claim 7 concerning the HTTP PUT method. Pet. 55 (citing Ex. 1004, Jeffay Decl. ¶ 260).

8. Claim 9

Claim 9 depends from claim 1 and recites "the at least one rule comprises a five-tuple specifying one or more transport-layer protocols, a range of source addresses, a range of source ports, a range of destination addresses, and a range of destination ports, and wherein identifying the one

or more packets comprising the application-layer packet-header information comprises determining by the packet security gateway that each of the one or more packets comprising the application-layer packet-header information corresponds to at least one of the one or more transport-layer protocols, has a source address within the range of source addresses, a source port within the range of source ports, a destination address within the range of destination addresses, and a destination port within the range of destination ports." As Petitioner notes Narayanaswamy, Kapoor, and Kjendal each disclose using a five-tuple in the process of identifying packets. Pet. 56 (citing Ex. 1012 ¶¶ 48, 53, 91, 101; Ex. 1013 ¶ 209; Ex. 1009, 8:64–9:2, 18:17–32; Ex. 1004, Jeffay Decl. ¶¶ 265-268).

D. Claims 10–16 As Obvious Over Narayanaswamy in View of Kapoor, Johnson, Kjendal and DiffServ

1. Claim 10

Petitioner notes that claim 10 generally parallels the language of claim 1, but recites the dynamic security policy comprises at least one rule specifying "packet-identification criteria," as opposed to the more specific term "application-layer packet-header information," and that the packet-identifying criteria comprises a "Differentiated Service Code Point (DSCP) selector." Pet. 56, 59. The Petition addresses each of the limitations of claim 10 individually, noting that in most cases the same analysis as that applicable to claim 1 applies. Pet. 59–67.

Patent Owner first contends that Petitioner fails to demonstrate that its combination of references discloses receiving a dynamic security policy from an SPMS, as recited in independent claim 10, for the same reasons receiving a dynamic security policy is not disclosed with respect to claim1 PO Resp. 49–50. As discussed above, we are persuaded that Petitioner has

demonstrated this limitation in claim 1 is taught by the combination of the references and, accordingly, we reach the same conclusion for the corresponding limitation of claim 10. Patent Owner presents similar arguments grounded in its arguments from claim 1 concerning whether this combination of references teaches identifying packets with packet-identification criteria on a packet-by-packet basis, as recited in independent claims 1 and 10 (*id*. at 52–53), and whether this combination of references discloses routing to a monitoring device, as recited in claims 1 and 10 (*id.* at 52–54). Our analysis for the relevant limitations of claim 10 is the same as for the corresponding limitations of claim 1, and we reach the same conclusions.

Turning to the new subject matter in claim 10, Petitioner notes that DSCP selector standards known at the time use classifiers to allow a system to assign priority to some packets over others, e.g. giving higher routing priority to VoIP packets over HTTP because VoIP packets are more susceptible to delay that would be noticed on a live telephone call. *Id.* at 58. Petitioner asserts that the DiffServ classifier rules qualify as packet identification criteria for purposes of claim 10 and its dependent claims. *Id.* 60. Petitioner further notes that Narayanaswamy and Kjendal both refer to relevant quality of service (QoS) indicators and implementations, thereby motivating a person of ordinary skill to employ the Diffserv rules in similar applications. *Id.* at 59.

Patent Owner contends that Petitioner's combination of references fails to disclose receiving a dynamic security policy with a rule that includes a DSCP selector as the packet identification criteria, as recited in independent claim 10. PO Resp. 50–52. Patent Owner argues to the extent Narayanaswamy and DiffServ disclose using DSCP data, it is used for

packet classification and not as packet identification criteria specified by a dynamic security policy. *Id.* at 50 (citing Ex. 2004, Goodrich Decl. ¶ 197). Patent Owner contends that Narayanaswamy's IDP device monitors quality of service (QoS) not as packet-identification criteria, but to determine which policy should be applied to packet flows. *Id.* at 51 (citing Ex. 2004, Goodrich Decl. ¶ 198). According to Patent Owner, Petitioner's assertion that DiffServ's classifier rules qualify as packet identification criteria is not supported by the references because DiffServ's packet classifiers would be used by Narayanaswamy's classifier module, rather than being packet identification criteria in a dynamic security policy. *Id.* (citing Ex. 2004, Goodrich Decl. ¶199).

Noting Patent Owner's acknowledgement that the combination of Narayanaswamy and DiffServ teach using DSCP data to implement QoS, Petitioner argues that Patent Owner construes dynamic security narrowly to exclude packet classification prior to the application of any security policy and not as the packet-identification criteria applied by a dynamic security policy. Pet. Reply 21. Patent Owner contends the DSCP selector must be specified in a rule of the dynamic security policy because the claim language requires the rule specify the packet-identification criteria as comprising a DSCP selector. PO Sur-reply 20.

Petitioner points out that Narayanaswamy's IDP device can use QoS as a parameter that is part of the dynamic security policy, meaning the IDP can classify packets in a data flow using QoS as a packet identification criterion. Pet. Reply 21–22 (citing EX 1012 ¶¶ 7, 48, 72–73). In that case, the security policy is applied to each packet on a packet-by-packet basis given the classification. *Id.* at 22 (citing Ex. 1012 ¶¶ 49, 51). Patent Owner argues that the cited disclosure from Narayanaswamy states packet

classification based on QoS is used only when determining the application of policies, i.e., which policy to use, and not as packet-identification criteria in a rule of a policy as claimed, and that in some cases no policy at all is applied. PO Sur-reply 21 (citing Ex. 1012 ¶¶ 48, 50, 72–73).

Claim 10 recites that a rule of the dynamic security policy (the at least one rule) specifies packet identification criteria that comprise a DSCP selector, and that a packet digest logging function (the packet transformation function) is performed on packets corresponding to the criteria in the rule. The discussion in paragraphs 72 and 73 of Narayanaswamy is directed to characteristics a classifier in an IDP can use to differentiate between information flows based on criteria, such as QoS, application, or application priority. Ex. 1012 ¶72. As an example, in Narayanaswamy an administrator can configure a dynamic security manager to cause classifier 26 to forward without further processing HTTP applications and process further FTP applications. *Id.* In our discussion of claim element 1.4 we noted Petitioner's argument that Figure 5A of Narayanaswamy teaches analyzing the packets to identify application-layer packet-header information. Paragraph 72 of Narayanaswamy expands that analysis to other criteria, but still applies a transformation function (e.g., forwarding an HTTP message (i.e. its packets) without further processing, or performing further processing in the case of FTP). Petitioner cites Narayanaswamy as disclosing a QoS architecture and DiffServ as identifying packets based on the content of some part of the packet header and selecting packets based on the DS codepoint only. Pet. 61 (citing Ex. 1011 § 2.3.1; Ex. 1004, Jeffay Decl. ¶¶ 286–287). DiffServ states "[c]lassifiers are used to 'steer' packets matching some specified rule to an element of a traffic conditioner for further processing." Ex. 1011 § 2.3.1. In view of these disclosures, we

agree with Petitioner that a person of ordinary skill would have had reason to combine the teachings of Narayanaswamy and DiffServ to arrive at a dynamic security policy that includes a rule that performs a transformation function on packets meeting a specified DSCP criterion.

E. Claims 11–16

Our Decision to Institute addressed claims 11–16, which all depend from independent claim 10. Dec. to Inst. 37–42. Patent Owner contends that claims 11–16 are patentable, based on its arguments that claim 10 is patentable, but does not respond specifically to Petitioner's challenges claims 11–16. PO Resp. 50. We have reviewed the record and find that, based on the same reasoning considered in our Decision to Institute, Petitioner has demonstrated by a preponderance of the evidence that claims 11–16 would have been taught by the asserted combination of references. We summarize the evidence presented by Petitioner that supports our conclusion concerning claims 11–16 below.

1. Claim 11

Claim 11 depends from claim 10 and recites "the subset of information comprises at least one of a portion of data from the packet, a source address of the packet, a source port of the packet, a destination address of the packet, a destination port of the packet, a transport-protocol type of the packet, a uniform resource identifier (URI) from the packet, an arrival time of the packet, a size of the packet, a flow direction of the packet, an identifier of an interface of the packet security gateway that received the packet, or one or more media access control (MAC) addresses associated with the packet." As evidence that claim 11 is would have been taught, Petitioner persuasively cites Diffserv as disclosing that a system should generate a log for auditable events during the packet transformation process,

including at least three of the options recited in claim 11 (date/time the packet was received, the source and destination address and the DS codepoint that caused failure). Pet. 67–68 (citing Ex. 1011 § 6.1).

2. Claim 12

Claim 12 depends from claim 10 and recites "temporarily storing data in a memory of the packet security gateway, the data comprising the subset of information specified by the packet digest logging function for each of the one or more packets corresponding to the packet-identification criteria; and utilizing, by the packet security gateway, the data to generate a message comprising the subset of information specified by the packet digest logging function for each of the one or more packets corresponding to the packet-identification criteria." Petitioner cites Kapoor as disclosing temporarily storing the subset of information in memory, generating a message for a remote logging database, and using the syslog format for sending remote messages. Pet. 68–69 (citing Ex. 1013 ¶¶ 211, 617, 87; Ex. 1004 ¶¶ 315–318). We agree with Petitioner that a person of ordinary skill would have known that to send remote alerts or messages as taught by Kapoor, the information is first stored temporarily in a memory record. *Id.* (citing Ex. 1004, Jeffay Decl. ¶ 318).

3. Claim 13

Claim 13 depends from claim 12 and recites "communicating, by the packet security gateway and to the security policy management server, the message comprising the subset of information specified by the packet digest logging function for each of the one or more packets corresponding to the packet identification criteria." Petitioner persuasively argues that a person of ordinary skill would have known a centralized log is one of a limited number of design options and cites Kapoor as teaching a database log

provided and/or maintained by a management server. Pet. 69 (citing Ex. 1013 ¶ 211; Ex. 1004, Jeffay Decl. ¶¶ 320–321).

4. Claim 14

Claim 14 depends from claim 13 and recites "reformatting the subset of information specified by the packet digest logging function in accordance with the logging system standard comprises reformatting the subset of information specified by the packet digest logging function in accordance with a syslog logging system standard." As discussed above with respect to claim 12, Petitioner persuasively cites Kapoor as teaching the information can be reformatted into the Syslog system standard, and notes that the '213 Specification acknowledges Syslog was known in the art. Pet. 70.

5. Claim 15

Claim 15 depends from claim 10 and recites "the packet-identification criteria comprises a five-tuple specifying one or more transport-layer protocols, a range of source addresses, a range of source ports, a range of destination addresses, and a range of destination ports, and wherein identifying the one or more packets corresponding to the packet-identification criteria comprises determining by the packet security gateway that each of the one or more packets corresponding to the packet-identification criteria corresponds to at least one of the one or more transport-layer protocols, has a source address within the range of source addresses, a source port within the range of source ports, a destination address within the range of destination addresses, and a destination port within the range of destination ports." Noting that claim 15 recites the use of a five-tuple for the same purpose as claim 9 recites the use of a five-tuple, Petitioner persuasively cites Narayanaswamy, Kapoor and Kjendal for the same reasons as discussed with respect to claim 9. Pet. 71.

6. Claim 16

Claim 16 depends from claim 10 and recites "the packet-identification criteria comprises application-layer packet-header information, and wherein identifying the one or more packets corresponding to the packet-identification criteria comprises determining by the packet security gateway that each of the one or more packets corresponding to the packet-identification criteria comprises at least a portion of the application-layer packet-header information." Petitioner persuasively relies on its discussion and cited evidence pertaining to claim 1 as the basis for its contentions that claim 16 is unpatentable. Pet. 71–72.

F. Objective Indicia of Nonobviousness

Before determining whether a claim is obvious in light of the prior art, we consider any relevant evidence of secondary considerations 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 presents evidence of three such considerations: (1) long-felt but unmet need, (PO Resp. 56–61) (2) industry praise (*id.* at 61–63), and (3) commercial success/licensing (*id*. at 63–64).

"In order to accord substantial weight to secondary considerations in an obviousness analysis, the evidence of secondary considerations must have a nexus to the claims, i.e., there must be a legally and factually sufficient connection between the evidence and the patented invention." *Fox Factory, Inc. v. SRAM, LLC*, 944 F.3d 1366, 1373 (Fed. Cir. 2019) (internal

quotations omitted). A nexus is presumed when "the patentee shows that the asserted objective evidence is tied to a specific product and that product 'embodies the claimed features, and is coextensive with them.'" *Id.* (quoting *Polaris Indus., Inc. v. Arctic Cat, Inc.*, 882 F.3d 1056, 1072 (Fed. Cir. 2018)). If the product is not coextensive with the claims at issue—for example, if the patented invention is only a component of the product—the patentee is not entitled to a presumption of nexus. *See id.* (citing *Demaco Corp. v. F. Von Langsdorff Licensing Ltd.*, 851 F.2d 1387, 1392 (Fed. Cir. 1988)).

1. Long Felt Unresolved Need and the Failure of Others

Patent Owner points to a U.S. Naval Research Laboratory presentation by Stanley Chincheck as evidence of a long felt, unresolved need recognized as early as 2010 to improve signature based network security systems. PO Resp. 56–57 (citing Ex. 2013, 5–6; Ex. 2004, Goodrich Decl. ¶ 208), PO Sur-reply 22–23. Patent Owner's expert, Dr. Goodrich, characterizes Narayanaswamy and Kapoor as such signature based systems, but does not explain the basis for his characterization and does not explain why the techniques in these references would be less effective than that claimed in the '213 patent. Ex. 2004, Goodrich Decl., ¶ 208. In addition, the Chincheck presentation does not comment on any specific approach or technology, including that discussed in the '213 patent. Ex. 2013, 3. Thus, even if the Chincheck presentation indicates a need exists to improve certain types of signature based systems, it provides no evidence that the '213 patent addresses that need, or that the approach in Narayanaswamy and Kapoor "failed" to do so.

Patent Owner cites statements in a May 2018 paper titled "Centripetal Networks Threat Intelligence Gateway" by Tony Palmer, a paper Patent

Owner commissioned from the Enterprise Strategy Group (ESG), concerning its CleanINTERNET intelligence-led managed security service using its RuleGATE enforcement point. PO Resp. 58–61 (citing Ex. 2006). Although we do not dismiss the ESG paper out of hand because it was commissioned by Patent Owner, we also cannot overlook the potential implications arising from this fact.

Patent Owner notes ESG's assertion that Patent Owner's "**goal is nothing less that the transformation of CTI (cyber threat intelligence) into protective action at scale**" and that Patent Owner "**does this by converting indicators to rules that drive actions** across a risk spectrum, i.e., **logging, content capture, mirroring, redirection**, shielding, and advanced threat detection." *Id.* at 59 (quoting Ex. 2006, ¶ 210). According to Patent Owner, ESG's description of Patent Owner's solution is tied to the inventions in the '213 patent that are directed to receiving a dynamic security policy, as distinguished from prior art security policies by its automatic updating when new CTI is received. *Id.* at 59, PO Sur-reply 24. We note, however, as discussed above, the '213 patent does not limit a dynamic security policy to one that is updated automatically, as the '213 patent describes an administrator updating the dynamic security policy manually. Ex. 1001, 14:23–47.

As Petitioner notes, Patent Owner's expert, Dr. Goodrich acknowledges that the ESG paper does not disclose whether the products it discusses embody the claims of the '213 patent. Pet. Reply 24 (citing Ex. 1021, Deposition Transcript of Dr. Michael Goodrich ("Goodrich Tr.") 24:12–30:7). Petitioner further notes that ESG's paper contains only a single general reference to "logging" and does not refer to the claimed packet digest logging function or routing packets to a monitoring device. *Id.*

In view of the above, Patent Owner does not establish a sufficient nexus between the invention claimed in the ’213 patent and the purported long felt, unmet need.

2. Industry Praise

Patent Owner cites the ESG Paper (Ex. 2006) as well as a Gartner article (Ex. 2007) and an American Banker article (Ex. 2011) as evidence of industry praise. PO Resp. 61–62. Similar to its long-felt need contentions, however, Patent Owner does not provide sufficient analysis or explanation to establish the requisite nexus. Patent Owner provides no analysis demonstrating that any of its product is coextensive with the challenged claims, so no presumption of nexus is applied. *See Fox Factory*,944 F.3d at 1373–74. Additionally, the cited praise of Patent Owner’s products is not linked sufficiently to the challenged claims, due in part to Patent Owner’s failure to address lauded features with no relationship to the claims.

For example, Patent Owner cites the ESG Paper as describing Patent Owner’s TIG (Threat Intelligence Gateway) as having the “highest performance network filter that ESG has tested or seen in action to date.” PO Resp. 61 (citing Ex. 2006, 7). Patent Owner also cites the ESG Paper as stating patent Owner’s TIG processed over 140 Gbps of network traffic at wire speed, and distributing, ingesting, synthesizing into a network policy, and enforcing over five million complex network filtering rules with each complex filtering rule containing at-least a dozen unique fields. *Id.* (citing Ex. 2006, 7). Patent Owner does not associate this information with the limitations of the challenged claims. Patent Owner does not address whether they are part of the claimed invention or, if not, their relative contribution to the industry praise compared to any actual features of the claimed invention.

Regarding the Gartner article, Patent Owner notes that Gartner praises Patent Owner's product's "ability to instantly detect and prevent malicious connections based on millions of threat indicators at 10-gigabit speeds," as having "the largest number of third-party threat intelligence service integrations," and using "5 million indicators simultaneously." PO Resp. 62 (citing Ex. 2007, 5). Again, insufficient analysis is presented to address how these features relate to the challenged claims. Patent Owner's reference to the American Banker article similarly suffers from a lack of explanation. *Id.* (citing Ex. 2011, 14)

Patent Owner's sole nexus explanation is a conclusory assertion that "the salutary benefits of Centripetal's TIG [threat interface gateway] are made possible in large part by the '213 patent's dynamic security policies, which are automatically managed and distributed by the claimed SPM, as well as its network layer packet-by-packet rule enforcement, packet digest logging function and packet transformation function for routing packets to a monitoring device." PO Resp. 62 (citing Ex. 2004, Goodrich Decl. ¶217). Dr. Goodrich's testimony cited in support of this statement is merely a near-verbatim copy of this conclusory statement with no additional explanation. *See* Ex. 2004 ¶ 112; 37 C.F.R. § 42.65(a) ("Expert testimony that does not disclose the underlying facts or data on which the opinion is based is entitled to little or no weight."). As a result, we find that Patent Owner has not established a sufficient nexus between the cited industry praise and the invention of the challenged claims.

3. Commercial Success and Licensing

Patent Owner contends that the commercial success of its RuleGATE product as well as a license to the '213 Patent taken by Keysight Technologies are compelling secondary considerations of non-obviousness.

PO Resp. 63–64. Jonathon Rogers, Patent Owner's Vice President of Operations and COO, testified that Patent Owner's RuleGATE system has been sold to customers and that RuleGATE embodies the '213 patent, although the record includes no technical analysis to support his testimony that RuleGATE embodies the '213 patent. Ex. 2016 ¶¶ 3–6.

Petitioner responds that Patent Owner does not provide an element by element analysis to support Mr. Rogers' claim. Pet. Reply 25–26. Patent Owner argues that no such element by element analysis is required and that, given Mr. Rogers' testimony, which Petitioner failed to cross-examine, nexus is presumed. PO Sur-reply 25–26.

Although Patent Owner argues it was incumbent on Petitioner to put forth evidence to rebut the presumption, we are not persuaded that Mr. Roger's bald assertion, without any factual basis, constitutes adequate evidence of nexus. Mr, Rogers states he is familiar with Patent Owner's licensing practices and assists in licensing Patent Owner's patented technologies, but he provides no foundation for his assertion that RuleGATE embodies the 213 patent. Mr. Rogers does not state he has any personal knowledge of the '213 patent or its claims; he does not state what aspects of RuleGATE embody the claims of the '213 patent; he does not state whether he draws on any personal technical background for his testimony; and he does not state whether his assertion is based on a legal assessment of counsel. Indeed, Mr. Rogers does not provide any basis for his assertion that RuleGATE does, in fact, embody the claims of the '213 patent. As an employee of Patent Owner, Mr. Rogers' testimony, without foundation or corroboration of any kind, is unreliable.

"Whether a product is coextensive with the patented invention, and therefore whether a presumption of nexus is appropriate in a given case, is a

question of fact." *Fox Factory*, 944 F.3d at 1373. Although the patentee is not required to prove perfect coextensiveness, the patentee is required to demonstrate the product is essentially the claimed invention. *Id.* at 1374. As Patent Owner has provided insufficient factual evidence to demonstrate RuleGATE is the claimed invention, we do not apply a presumption of nexus in this case.

As additional evidence of commercial success, Patent Owner cites a "worldwide, royalty-bearing, non-transferable, irrevocable, nonterminable, nonexclusive license to Centripetal's worldwide patent portfolio," including the '213 patent, taken by Keysight Technologies to settle a patent infringement suit. PO Resp. 63–64 (citing Ex. 2012, 83). Petitioner points out that Keysight was sued on the '213 patent and ten other patents. Pet. Reply 27. Patent Owner provides no information about the relevant details of this license—e.g., how many patents comprise the portfolio, or the relative contribution of the '213 patent to the value of the license—such that we could discern whether Keysight took the license "out of recognition and acceptance of the subject matter claimed" in the '213 patent. *See In re GPAC Inc.*, 57 F.3d 1573, 1580 (Fed. Cir. 1995). As such, we find that Patent Owner has not provided sufficient evidence to establish the requisite nexus between the Keysight license and the '213 Patent. *See id*.

G. Conclusion As to Obviousness

As discussed above, Petitioner has shown by a preponderance of the evidence that the combined teachings of Narayanaswamy, Kapoor, Johnson and Kjendal teach each limitation of each challenged claims 1–9 and the combined teachings of Narayanaswamy, Kapoor, Johnson, Kjendal, and the Diffserv Specification teach the limitations of claims 10–16 to a person of ordinary skill in the art. We further determine that Petitioner's showing that

the claims are taught by the references was very strong, particularly in comparison to Patent Owner's showing with respect to the asserted secondary considerations of obviousness. As discussed above, we find that Patent Owner has not established the requisite nexus between the challenged claims and any of the asserted secondary considerations. As such, we are unable to accord them any substantial weight. See *Fox Factory*, 944 F. 3d at 1373–74. Therefore, in weighing the totality of the evidence of record and the strength of the parties' showings on the inquiries underlying the question of obviousness, we conclude that Petitioner has met its overall burden of proving by a preponderance of the evidence that each of the challenged claims would have been obvious in view of the cited prior art.

VII. CONCLUSION[6]

In consideration of the above, we find that Petitioner has demonstrated by a preponderance of the evidence (1) that claims 1–9 are unpatentable under 35 U.S.C. § 103 as obvious over Narayanaswamy, Kapoor, Johnson and Kjendal and (2) that claims 10–16 are unpatentable under 35 U.S.C. § 103 as obvious over Narayanaswamy, Kapoor, Johnson, Kjendal, and the Diffserv Specification.

[6] 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. mSee* 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).

In summary:

Claims	35 U.S.C. §	References	Claims Shown Unpatentable	Claims Not shown Unpatentable
1–9	103	Narayanaswamy, Kapoor, Johnson, Kjendal	1–9	
10–16	103	Narayanaswamy, Kapoor, Johnson, Kjendal, Diffserv Specification	10–16	
Overall Outcome			1–16	

VIII. ORDER

In consideration of the foregoing, it is hereby:

ORDERED that claims 1–9 of the ’213 patent are held unpatentable as obvious under 35 U.S.C. § 103 over Narayanaswamy, Kapoor, Johnson and Kjendal;

FURTHER ORDERED that claims 10–16 of the ’213 patent are held unpatentable as obvious under 35 U.S.C. § 103 over Narayanaswamy, Kapoor, Johnson, Kjendal, and the Diffserv Specification; and

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

FOR PETITIONER:

Daniel McDonald
Jeffrey Blake
Kathleen Ott
Christopher Davis
MERCHANT & GOULD
dmcdonald@merchantgould.com
jblake@merchantgould.com
kott@merchantgould.com
cdavis@merchantgould.com

FOR PATENT OWNER:

James Hannah
Jeffrey Price
Michael Lee
KRAMER LEVIN NAFTALIS & FRANKEL LLP
jhannah@kramerlevin.com
jprice@kramerlevin.com
mhlee@kramerlevin.com

Bradley Wright
BANNER & WITCOFF
bwright@bannerwitcoff.com