Trials@uspto.gov
571-272-7822

Paper 32
Entered: February 11, 2020

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

CISCO SYSTEMS, INC.,
Petitioner,

v.

CENTRIPETAL NETWORKS, INC.,
Patent Owner.

IPR2018-01444
Patent 9,137,205 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 February 12, 2019, we instituted an *inter partes* review of claims 1–3, 5–11, 17–19, 21–27, 33–35, and 37–43 (the "challenged claims") of U. S. Patent No. 9,137,205 B2 (Ex. 1001, "the '205 patent"). Paper 7 ("Dec. to Inst."). Patent Owner filed a Patent Owner Response (Paper 18, "PO Resp."), Petitioner filed a Petitioner Reply (Paper 23, "Pet. Reply"), Patent Owner filed a Surreply (Paper 25, "PO Surreply"), and a transcript of an oral hearing held on November 12, 2019 (Paper 31, "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 '205 PATENT

The '205 patent discloses methods and systems for protecting a secured network. Ex. 1001, Abstract. Figure 1 illustrates a network environment that includes packet security gateways (PSGs) situated between networks and a security policy management server (SPMS) that communicates dynamic security policies to the PSGs. *Id.* at 4:53–55, 5:5–15, Fig. 1. The PSGs may operate in a network transparent manner, sending and receiving traffic at a link layer using an interface that is not addressed at the network layer, and simultaneously performing packet transformation functions at the network layer. *Id.* at 3:1–6. The PSG may include a management interface having a network layer address accessible at the application layer. *Id.* at 3:7–10.

The PSGs perform packet transformation functions on received packets according to rules in a dynamic security policy that specifies one or more packet transformation functions that should be performed on packets associated with specific criteria. *Id.* at 5:15–25, 6:59–62.

> 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.

Ex. 1001, 6:62–67, Fig. 3.

The '205 patent states that packet transformation functions may forward packets into or out of the network protected by the PSG (e.g., Ex. 1001, 2:47–51) or drop all packets associated with network addresses outside a specified set (*id.* at 1:65–2:4, 2:54–56). Multiple dynamic security policies may also be received from the security policy management server. *Id.* at 2:12–24. 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 15:1–7. 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 15:7–17.

Various combinations of rules may implement services, such as a blocklist service within a network environment that may include one or more rules specifying criteria for which associated packets should be blocked or denied, and at least one rule specifying that all packets outside the blocked sets should be forwarded, accepted, or allowed. *Id.* at 7:55–8:6.

III. ILLUSTRATIVE CLAIM

Claim 1 is reproduced below using the same designations for the claim limitations as those used by Petitioner.

1. A method, comprising:
[1.0] at each packet security gateway of one or more packet security gateways associated with a security policy management server:
[1.1] receiving a plurality of dynamic security policies from the security policy management server, wherein receiving the plurality of dynamic security policies comprises:
[1.2] receiving at least one rule specifying a set of network addresses for which associated packets should be forwarded and at least one rule specifying that all packets associated with network addresses outside the set of network addresses for which packets should be forwarded should be dropped;
[1.3] receiving, at a first time, a dynamic security policy specifying a first set of network addresses for which packets should be forwarded;
[1.4] receiving, at a second time, a dynamic security policy specifying a second set of network addresses for which packets should be forwarded; and receiving, at a third time, a dynamic security policy specifying a third set of network addresses for which packets should be forwarded,
[1.5] the second time being after the first time, the third time being after the second time,
[1.6] the second set of network addresses including more network addresses than the first set of network addresses, and the third set of network addresses including more network addresses than the second set of network addresses;
[1.7] receiving packets associated with a network protected by the packet security gateway; and
[1.8] performing, on a packet by packet basis, at least one of multiple packet transformation functions specified by the plurality of dynamic security policies on the packets associated with the network protected by the packet security gateway, wherein performing the at least one of the multiple packet transformation functions specified by the plurality of dynamic security policies on the packets comprises

performing at least one packet transformation function other than forwarding or dropping the packets.

Claim 17 is drawn to a system and generally parallels the limitations of claim 1. Claim 33 is drawn to a non-transitory computer readable medium and also generally parallels the limitations recited claim 1.

IV. GROUNDS OF INSTITUTION

A. Prior Art and Asserted Grounds

Petitioner asserts that the challenged claims would have been unpatentable on the following grounds:

Claim(s) Challenged	35 U.S.C. §	References/Basis
1, 5, 7, 9, 17, 21, 23, 25, 33, 37, 39, 41	103(a)	Jungck[1], Bhatia[2]
2, 3, 10, 18, 19, 26, 34, 35, 42	103(a)	Jungck, Bhatia, Ahn[3]
6, 22, 38	103(a)	Jungck, Bhatia, Ke[4]
8, 24, 40	103(a)	Jungck, Bhatia, Ingate[5], RFC 2003[6]
11, 27, 43	103(a)	Jungck, Bhatia, RFC2474[7]

V. CLAIM CONSTUCTION

In our Decision to Institute we construed the following terms.

[1] U.S. Patent Appl. Publ. No. 2009/0262741 A1, Oct. 22, 2009 (Ex. 1010)
[2] U.S. Patent Appl. Publ. No. 2007/0118894 A1, May 24, 2007 (Ex. 1011)
[3] U.S. Patent Appl. Publ. No. US 2011/0055916 A1, Mar. 3, 2011 (Ex. 1014)
[4] U.S. Patent No. 7,095,716 B1, Aug. 22, 2006 (Ex. 1015)
[5] Ingate Firewall/SIParator SIP Best Practice, Sept. 2, 2008 (Ex. 1012)
[6] IP Encapsulation within IP, Network Working Group Request for Comment: 2003, C. Perkins, IBM, October 1996 (Ex. 1016)
[7] Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers, Network Working Group Request for Comments: 2474, The Internet Society, 1998 (Ex. 1017)

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." Dec. to Inst. 7–9. Petitioner agrees with our constructions. Pet. Reply 1–3. The Patent Owner Response proposes "dynamic security policy" be construed to mean "a non-static set of one or more rules." PO Resp. 7. 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. *Id.* at 8 (citing Ex. 1001, 4:43–49). 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* 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 4:43–44) and "may include one or more rules" (*id.* at 5:61–62). 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, 7:56–57.

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. 9. According to Patent Owner, "dynamic" means "the security policy can be automatically changed or altered." *Id.* Patent Owner does not point to any use of the expression "non-static" in the '205 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, 13:8–32); 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 13:33–62). As discussed above, however, the Specification explicitly states "[a]s 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 4:43–49. As our construction is consistent with that language, we decline to adopt Patent Owner's construction, which is inconsistent with some of the embodiments in the Specification. *See On-Line Techs., Inc. v. Bodenseewerk Perkin-Elmer GmbH*, 386 F.3d 1133, 1138 (Fed. Cir. 2004) ("[A] claim interpretation that excludes a preferred embodiment from the scope of the claim is rarely, if ever, correct."). Consistent with our Decision to Institute, in this Decision we construe "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."

B. Rule/rules

In our Decision to Institute we construed "rule/rules" to mean "a condition or set of conditions that when satisfied causes a specific function to occur." Dec. to Inst. 9–10. As neither party disputes our construction and we do not discern any persuasive evidence in the full record indicating that construction is incorrect, for the reasons explained in the Decision to Institute, we apply the same construction in this Decision. *See* PO Resp. 10; Pet. Reply 1–3.

C. Security Policy Management Server (SPM)

In our Decision to Institute we construed "security policy management server" (SPM) to mean "a server configured to communicate a dynamic security policy to a packet gateway." Dec. to Inst. 10. As neither party disputes our construction and we do not discern any persuasive evidence in the full record indicating that construction is incorrect, for the reasons explained in the Decision to Institute, we apply the same construction in this Decision. *See* PO Resp. 10–11, Pet. Reply 1–3.

D. Packet Security Gateway

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. As neither party disputes our construction and we do not discern any persuasive evidence in the full record indicating that construction is incorrect, for the reasons explained in the Decision to Institute, we apply the same construction in this Decision. *See* PO Resp. 11, Pet. Reply 1–3.

E. 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. 11. 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. 11–13. 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.* at 6:5–14); 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 15:1–15). Thus, dynamic security policies and rules identify conditions that cause packet transformation functions to carry out specific operations that may differ depending upon the policy or rule that applies to detected packet conditions.

Dec. to Inst. 12–13. Patent Owner has not identified, nor are we aware of, persuasive evidence in the full record indicating that construction is incorrect. In consideration of the above, we apply the construction articulated in the Decision to Institute, for purposes of this Decision andconstrue "packet transformation function" to mean "operations performed on a packet."

VI. ANALYSIS OF PRIOR ART CHALLENGES

A. Introduction

A claim is unpatentable under § 103 if the differences between the claimed subject matter 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. *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")); *see In re Warsaw Orthopedic, Inc.*, 832 F.3d 1327, 1333 (Fed. Cir. 2016) (citing *DyStar Textilfarben GmbH & Co. Deutschland KG v. C. H. Patrick Co.*, 464 F.3d 1356, 1360 (Fed. Cir. 2006)).

B. Claim 1 As Obvious Over Jungck and Bhatia

1. Jungck

Petitioner cites Jungck as disclosing a packet interceptor apparatus that applies to intercepted packets one or more rules that execute one or more functions on a dynamically specified portion of the packet and takes one or more actions with the packets. Pet. 21 (citing Ex. 1010, Abstract). Jungck states that "[t]he apparatus is capable of analyzing any portion of the packet including the header and payload" and that the actions "include releasing the packet unmodified, deleting the packet, modifying the packet, logging/storing information about the packet or forwarding the packet to an external device for subsequent processing." Ex. 1010, Abstract. Jungck's rules may be "dynamically modified" by the external devices. *Id.*

Petitioner cites the third (Emb#3), fourth (Emb#4), and fifth (Emb5) embodiments of Jungck ("the Jungck Embodiments") as disclosing various elements of the claims of the '205 patent. Pet. 21. Petitioner notes that common to Emb#3, Emb#4, and Emb#5 is the network shown in Figure 1 having network 100 surrounded by a first boundary with points-of-presence (POPs) 116 and a second boundary with POPs 114. *Id.* According to Petitioner, Emb#3 is relevant to the challenged claims because it discloses an edge server and edge cache at every service provider or major network intersection to provide coverage of every POP. *Id.* at 23. Noting that the edge servers in Emb#3 can process packets forwarded to them by the ISPs or carrier's routing equipment, Petitioner cites Emb#4 as disclosing a packet interceptor adaptor that can interface with multiple external devices and a management interface that enables the packet interceptor adaptor to interface with particular external devices. *Id.* at 24–26. Petitioner cites Emb#5 as disclosing a device with "Intelligent Packet Adaptors" with multiple processors to perform "stateful processing tasks," e.g., determining that packets for a certain network address are consistently malicious and adding that network address to a filtering list. *Id.* at 27–29. Emb#5 also discloses an external management device for programming, controlling and maintaining the device. Pet. 29 (citing Ex. 1010 ¶ 273).

2. Bhatia

Bhatia discloses preventing denial of service (DoS) attacks by thwarting bad traffic before the traffic hits the session layer boundary or by providing a lower class of service until the traffic has been authenticated. Ex. 1011 ¶ 20. Petitioner cites Bhatia as disclosing methods for improved response to DoS attacks in which a packet filter, which may be a forwarding layer of an IP router or other DoS prevention device, acts as an inspection

layer between the application layer and the session layer by implementing black lists and white lists. Pet. 30–31. The packet filter in the router receives Access Control Lists (ACL) and compiles them into packet filter entries to filter packets based on IP address, protocol, network layer port, arbitrary patterns in the network layer payload, and other information useful to detecting an attack. Pet. 31; Ex. 1011 ¶ 29. When a Session Initiation Protocol (SIP) server detects a DoS attack, it propagates that information to IP router forwarding layers that may be located at the Session Border controller (SBC) to perform white list processing that selectively allows authentic packets or black list processing that selectively throws suspected attack packets. *Id.* at 32; Ex. 1011 ¶ 22. In Figure 3, the SIP server is split into two layers to create a white list. Ex. 1011 ¶ 36. Packet filter layer 34 sends received packet registration and authorization information (such as a password or biometric information) 48A to SIP session layer 20 shown in Figure 2 which creates a session and forwards the packet to SIP application layer 35 that checks and authenticates the information. *Id.* ¶¶ 36–37. If authenticated, SIP application layer 35 pushes the IP address to packet filter layer 34 and into white list 30 (shown in Fig. 2 in packet filter 13) thereby dynamically populating a white list (via ACL-Auth over path 28 in Fig. 2) that may also have static entries provided by an administrator (via ACL-Allow over path 27 in Fig. 2). *Id.* ¶¶ 33–34, 37. According to Petitioner, packet filter layer 34 and SIP application layer 35 of the SIP server interact dynamically to produce a growing white list (dynamic security policy) that provides packet filtering functionality for an IP router (i.e., a PSG, as in the '205 patent). Pet. 32–33.

3. Claim Limitations 1.0 and 1.1

Consistent with the approach taken by the parties after institution, we address claim limitations 1.0 and 1.1 together. PO Resp. 12–26; Pet. Reply 3–7. As noted by the parties, claim 17, drawn to a system, and claim 33, drawn to non-transitory computer readable media having instructions stored thereon, recite limitations that correspond to those in claim 1.

Petitioner identifies as claim element 1.0 (and as corresponding claim elements 17.0 and 33.0) the limitation that recites "at each packet security gateway of one or more packet security gateways associated with a security policy management server." Pet. 37. According to Petitioner, Jungck teaches "edge servers" as PSGs because they are located at the boundaries of a network, isolate computing devices from untrusted network traffic, and are associated with a subscribing server that acts as an SPMS. Pet. 38 (citing Ex. 1010 ¶¶ 39–40, 108–111; Ex. 1005, Declaration of Dr. Kevin Jeffay ("Jeffay Decl.") ¶¶ 216–221).

Citing Emb#4, Petitioner asserts that Jungck teaches the claimed PSGs as edge servers with packet interceptor adapters within routers or as standalone devices that apply rule sets defined by external devices to intercept packets. *Id.* (citing Ex. 1010 ¶¶ 126, 128, 130, 152–158, 160; Ex. 100, Jeffay Decl. ¶¶ 222–227).

Petitioner cites Emb#5 as teaching the claimed gateways (PSGs) as secondary processors that intercept and process packets in a device with a management adapter that associates the device and the secondary processors with an external management device acting as an SPMS that programs, controls, and maintains the device. *Id.* at 39.

Petitioner identifies as claim element 1.1 (and as corresponding claim elements 17.1 and 33.1) the limitation that recites "receiving[e/receive] a

plurality of dynamic security policies from the security policy management server, wherein receiving the plurality of dynamic security policies comprises." Pet. 40. Petitioner cites Emb#3 as disclosing subscribing server 108 as an SPMS that identifies malicious program code for monitoring by edge server 602. Pet. 41 (citing Ex. 1010 ¶¶ 108–110).

Patent Owner contends Jungck's Emb #3 fails to disclose claim limitation 1.0 because Jungck's malicious code identifications are not "dynamic security policies under either the Board's preliminary construction of the term or Patent Owner's proposed construction." PO Resp. 12–14. Therefore, as to claim limitation 1.1, Patent Owner contends that in #Emb 3 Jungck's subscribing server 108 cannot be considered a server configured to communicate dynamic security policies to a PSG. *Id*.

According to Patent Owner Jungck does not teach malicious code identifications in the form of a rule received from a server or as policy that includes such a rule. *Id.* at 13. Patent Owner cites testimony by Petitioner's expert, Dr. Jeffay, as conceding that Jungck's edge server generates filters used to monitor data transmissions for malicious program code. *Id.* at 14 (citing Ex. 1005, Jeffay Decl. ¶ 241 referencing Ex. 1010 ¶¶ 108, 111 as describing edge server 602 receiving malicious code identifications from server 108 and implementing such identifications in packet filters).

Nevertheless, as Petitioner points out, Jungck states that the subscribing server, corresponding to the claimed SPMS, identifies the malicious code (program code identified by server 108 as unwanted, harmful or destructive), which can include network addresses associated with denial of service (DoS) attacks. Patent Owner cites Dr. Jeffay's deposition testimony as conceding that network addresses associated with DoS attacks

are not themselves malicious code. PO Surreply 2–3 (citing Ex. 2019, Transcript of Deposition Testimony of Dr. Kevin Jeffay of Oct. 8, 2019 ("Jeffay Tr. II") 71:7–72:11). In addition to rules and messages, consistent with the '205 Specification, our construction of "dynamic security policy" includes any "data structure, or the like that specifies criteria corresponding to one or more packets." We do not exclude network addresses from "dynamic security policy" because network addresses are data structures that specify criteria corresponding to packets, i.e., packets originating at those certain network addresses.

Patent Owner also disputes Petitioner's contention that Jungck discloses a subscribing server that provides "an instruction that packets from these address should be dropped." PO Surreply 3 (citing Pet. Reply 4). In his Reply Declaration Dr. Jeffay stated Jungck's subscribing server would provide network addresses to the edge server along with an instruction that packets from these addresses should be eradicated. Ex. 1026, Jeffay Reply Decl. ¶ 73 (citing Ex. 1010 ¶ 111).

Jungck describes packet level filter 606 in edge server 602 as selectively intercepting traffic between clients (102, 104, 106) and subscribing servers (108, 110), monitoring transmissions for malicious program code previously identified by subscribing server 108 as unwanted, e.g., a data packet originating at an address not associated with a downstream POP 114, and recognizing and eradicating the packet or preventing it from reaching the network. Ex. 1010 ¶¶ 110–111. Even if Jungck does not identify a specific instruction to eradicate packets from such addresses is provided by the subscribing server, we are persuaded that a person of ordinary skill would have understood that, in view of the subscribing server identifying traffic from such addresses as unwanted or

harmful, it would be necessary to implement a mechanism that prevenst packets from such addresses reaching the network. *Id.* Therefore, we agree with Petitioner that Emb#3 of Jungck teaches or suggests claim limitations 1.0 and 1.1.

Petitioner also cites Emb#4 and Emb#5 of Jungck as disclosing claim element 1.1 (and corresponding claim elements 17.1 and 33.1) because they disclose dynamically updating rule sets communicated from a server to gateways. Pet. 40–41 (citing Ex. 1010 ¶¶ 153, 157). As to Emb#4, Jungck's discloses rule processor 716 comprising multiple rule sets 726 and rules 732, in which some rules may be particularized dynamically resettable rules specific to external devices 724 coupled with edge/packet interceptor device 720 and other rules may be standardized functions, e.g., provided in a library, and in which rules may be redefined or reset via management interface 722. Ex. 1010 ¶ 157.

Patent Owner argues Jungck uses external device 724 to redefine an already existing rule set, instead of sending a dynamic security policy. PO Resp. 15–18. Patent Owner also states that Jungck does not disclose receiving a plurality of dynamic policies from the SPMS, because once a rule set is defined on a router, the router receives only modifications to the rule set already implemented. *Id.* at 17. Petitioner cites Jungck's disclosure that rule sets and their rules may be defined by external devices coupled with the edge/packet interception device 702. Pet. Reply 4 (citing Ex. 1010 ¶ 157). Petitioner further notes that Jungck states rule processor 716 may contain one or more rules sets that are used by the packet analyzer. Pet. Reply 5. We agree with Petitioner that the external devices 724 (or management interface 722) may define a new rule set, which is sent to the rules processor to supplement an existing rule set (Pet. Reply 5) because

Jungck states that some rule sets may be defined by an external device 724 but can be processed entirely by rules processor 716 and rule sets and rules may be redefined or reset dynamically by rules processor 716 or external devices 724 as needed (Ex. 1011 ¶ 157). Patent Owner further argues that Jungck's Emb#4 does not disclose the claimed SPMS, because external device is not a server. PO Resp. 18. As Petitioner notes, however, the '205 patent describes a "server" as "one or more computing devices configured to perform one or more functions described herein." Pet. Reply 5–6 (citing Ex. 1001, 12:52–54).

As to Emb#5, Petitioner cites the use of management adapter 914 coupled to an external management device as disclosing an SPMS that dynamically updates invalid addresses (policies) applied by processing elements 912A, 912B (PSGs) of device 900. Pet. 40–41. Petitioner also cites Bhatia's teaching of packet filter layers receiving Access Control Lists from the SIP servers as disclosing claim element 1.1. Pet. 41–42.

Patent Owner argues that these disclosures in Jungck fail to teach receiving a plurality of dynamic security policies as claimed because, rather than acting as a server sending a plurality of dynamic security policies from an SPMS to a PSG, Jungck's management adapter 914 functions as an administrative console that directly programs the filtering functionality on device 900. PO Resp. 19–20; PO Surreply 7–8. We addressed a similar argument above concerning the server feature in the context of Emb#4 and found it unpersuasive.

Petitioner also cites Bhatia's teaching of packet filter layers receiving Access Control List (ACLs), e.g., black lists and white lists, from the SIP servers as disclosing claim element 1.1. Pet. 41. Patent Owner point outs that in Bhatia, rules are formed in the SIP server's packet filtering layer,

which Petitioner maps to the claimed PSG, rather than being received from the SIP server's application layer, which Petitioner maps to the claimed SPMS. PO Resp. 20–21 (citing Pet. 39, 41; Ex. 1011 ¶ 21; Ex. 2004, Declaration of Dr. Michael Goodrich ("Goodrich Decl.") ¶¶ 173–174). According to Patent Owner Bhatia cannot discloses a PSG receiving a dynamic security policy from an SPMS in the claimed fashion because in Bhatia the SIP packet filtering layer and the application layer are different logical components of the same device. *Id.* at 21 (citing Ex. 2004, Goodrich Decl. ¶ 174). In response, Petitioner notes Dr. Jeffay's testimony citing other embodiments where the packet filtering layer is part of a router that is a separate functional component from the SIP server that has the SIP application layer. Pet. Reply 6 (citing Ex. 2009, Transcript of Deposition Testimony of Dr. Kevin Jeffay of April 23, 2019 ("Jeffay Tr. I"), 88:6–89:20; Ex. 1026, Jeffay Reply Decl. ¶ 86.

Patent Owner further argues that Bhatia, rather than receiving ACLs from the application layer, pushes individual IP addresses for the ACL to the corresponding white list or black list, i.e., the white lists and black lists in Bhatia are not sent anywhere but instead are maintained in place, subject to push commands. PO Resp. 22–24. Petitioner, however, cites Figure 3 of Bhatia as disclosing that the ACLs send one or more addresses, each corresponding to a packet, to the packet filter layer and each provides a transformation function by specifying that the addresses are placed on the white list such that the associated packets will be forwarded. Pet. Reply 6–7 (citing Ex. 1026, Jeffay Reply Decl. ¶ 87). According to Petitioner this constitutes sending a dynamic security policy to the packet filtering layer. *Id.* at 7. A description of the process shown in Figure 3 of Bhatia is found in paragraph 35 and 36, which states "in this manner the white list (WL) is

created." Ex. 1011 ¶¶ 37). Thus, we agree with Petitioner that Bhatia discloses the features recited in claim limitations1.0 and 1.1

Based on the arguments and evidence discussed above, we agree with Petitioner and find that Bhatia discloses the features recited in claim limitations1.0 and 1.1

4. Claim Limitation 1.2

Petitioner identifies as claim element 1.2 (and as corresponding claim elements 17.2 and 33.2) the limitation that recites "receiving/receive at least one rule specifying a set of network addresses for which associated packets should be forwarded and at least one rule specifying that all packets associated with network addresses outside the set of network addresses for which packets should be forwarded should be dropped." Pet. 42. Noting that packet filtering by blocking and forwarding packets based on network addresses was known before the '205 patent, Petitioner cites Jungck's Emb#3 as disclosing "ingress filtering," in which server 602A recognizes a forged data packet and eradicates it or prevents it from reaching network 100. *Id.* Petitioner contends that a person of ordinary skill would recognize that Emb#3 could be modified to incorporate the ingress filtering taught in Emb#5, in which all packets with an out-of-range network address are filtered out. *Id.* at 42–43. Thus, Jungck teaches one of ordinary skill an edge server that receives filtering rules with a set of network addresses associated with POPs, such that packets originating from the set of network addresses downstream from the edge server would be forwarded and all packets originating outside this set of network addresses would be eliminated. *Id.*

Patent Owner argues that Jungck's Emb#3 and Emb#5 disclosures are limited to whether a packet should be blocked, but the embodiments disclose

no rules for packets that are not eradicated, and, in particular, no rules concerning forwarding packets as recited in claim element 1.2. PO Resp. 27–28. Petitioner argues Bhatia discloses dropping invalid packets and forwarding valid ones because Bhatia states that packets originating from the set of network addresses downstream of the edge server may be transmitted to the intended subscribing server. Pet. Reply 7 (citing Ex. 1026; Jeffay Reply Decl. ¶¶ 89–90).

Petitioner also cites Bhatia as disclosing rules implementing white lists and black lists, including a rule specifying the address is to be forwarded and a catch-all or default rule specifying packets associated with all other addresses should be dropped. Pet. 43–44 (citing Ex. 1011, ¶ 35).

Patent Owner emphasizes that when Bhatia's packet filter detects an incoming packet that has no state, Bhatia employs a "rest" policy that forwards the packet to the SIP application layer where, if the packet is authenticated, the session is placed on the white list, and if the received packet is malformed, the sender's IP address is added to the black list. *Id.* at 29; Ex. 1011 ¶ 37. Paragraph 35 of Bhatia describes a "rest list" that contains entries in the universe of all possible IP addresses/ports and other rules that are not specified in the black list or the white list. Ex. 1011 ¶ 35. Patent Owner contends that Bhatia's rest list means Bhatia's black list is not the claimed rule that "specif[ies] that all packets associated with network addresses outside the set of network address for which packets should be forwarded should be dropped." PO Resp. 28–29.

As we noted in our Decision to Institute, in the case where there are no entries in the rest list, the black list meets this criteria. Pet. Reply 8 (citing Dec. to Inst. 24; Ex. 1026, Jeffay Reply Decl. ¶ 93 (citing Ex. 1011

¶¶ 37, 39)). However, as Patent Owner points out, Bhatia does not explicitly discuss a rest list with no entries. PO Resp. 30–31; PO Surreply 12 (citing Ex. 2019, "Jeffay Tr." 68:4–23 for the proposition that, as a practical matter, Bhatia's rest list is never empty). Petitioner notes and Patent Owner's expert, Dr. Goodrich, agrees, however, that any packets in the rest category are ultimately forwarded or dropped, depending upon whether they are authenticated or malformed. Pet. Reply 8 (citing Ex. 2004, Goodrich Decl. ¶¶ 183, 185; Ex. 1026, Jeffay Reply Decl. ¶ 92; Ex. 1011 ¶¶ 37, 39). Claim limitation 1.2 recites receiving at least one rule that requires dropping network addresses outside the set of addresses that should be forwarded. We agree with Petitioner that the existence of intermediate steps to determine the state of a packet does not change the fact that, if the packet is not among those that should be forwarded, that packet ultimately is dropped. Thus, we are persuaded by Petitioner's argument that Bhatia would have suggested claim limitation 1.2 to a person of ordinary skill in the art.

5. Claim Limitations 1.3–1.6

Petitioner identifies as claim element 1.3 (and as corresponding claim elements 17.3 and 33.3) the limitation that recites "receiving/receive at a first time, a dynamic security policy specifying a first set of network addresses for which packets should be forwarded." Pet. 44 *Id.* Petitioner argues that these limitations recite little more than the well-known concept of expanding or updating white lists, e.g., using techniques in which authentication of new addresses expands the white list. *Id.* Petitioner cites Bhatia as disclosing three methods of expanding white lists: (i) manually by an administrative application, (ii) dynamically by pushing addresses to the white list each time a SIP authentication is received, and (iii) both manually and automatically. *Id.* at 44–45 (citing Ex. 1011 ¶¶ 33–34, 37). Petitioner

argues that Bhatia's white list or black list updating is compatible with Jungck, which teaches executing DoS protection using a rule set in which the first rule checks the source IP address of the packet against the list of blocked IP addresses. *Id.* at 45–46. Patent Owner does not dispute explicitly that Jungck in view of Bhatia teaches claim limitation 1.3.

Petitioner identifies as claim element 1.4 (and as corresponding claim elements 17.4 and 33.4) the limitation that recites "receiving/receive, at a second time, a dynamic security policy specifying a second set of network addresses for which packets should be forwarded; and receiving, at a third time, a dynamic security policy specifying a third set of network addresses for which packets should be forwarded." Pet. 46. Petitioner contends that this limitation continues the description of expanding a white list and merely requires adding network addresses to the white list at another point in time, and then doing it again. Pet. 47. Petitioner cites the depiction in Bhatia of updating a white list repeatedly over time as teaching the use of dynamic security policies that specify a first, second, and third list of addresses at different points in time. *Id.* at 47–50. Patent Owner does not dispute explicitly that Jungck in view of Bhatia teaches claim limitation 1.4.

Petitioner identifies as claim element 1.5 (and as corresponding claim elements 17.5 and 33.5) the limitation that recites "the second time being after the first time, the third time being after the second time." Pet. 50. Petitioner cites Bhatia's disclosure of pushing updated white list rules with additional addresses over time and a time-limited black list in which blocking is disabled after a defined time period to restore normal service as disclosing claim element 1.5. *Id.* Patent Owner does not dispute explicitly that Jungck in view of Bhatia teaches claim limitation 1.5.

Petitioner identifies as claim element 1.6 (and as corresponding claim elements 17.6 and 33.6) the limitation that recites "the second set of network addresses including more network addresses than the first set of network addresses, and the third set of network addresses including more network addresses than the second set of network addresses." Pet. 50–51. Petitioner cites Bhatia as disclosing that later lists include more addresses than earlier lists and that adding addresses to a list is an obvious variation for updating the list or changing policies. *Id.*

Patent Owner notes that upon receiving an incoming packet, Bhatia authenticates the user and adds the IP address to a white list. PO Resp. 31–32 (citing Ex. 2004, Goodrich Decl. ¶ 188). Focusing on the claim's recitation of "set," Patent Owner argues that "[s]imply adding IP addresses to a white list one at a time does not meet the claim language of the claims at least because each new alleged 'set' is simply a 'set' of one new address." *Id*. at 32 (citing Ex. 2004, Goodrich Decl. ¶ 188). Patent Owner contends that, because Bhatia's packet filter receives individual addresses, it does not receive a dynamic security policy. PO Surreply 13–14.

Patent Owner's contentions concerning sets of network addresses in claim elements 1.3–1.6 focus on the mechanism of receiving successive dynamic security policies, in which each successive policy (the policy at a second time and the policy at a third time) contains more network addresses than the preceding policy. Claim elements 1.3–1.6 require only that each subsequent policy contain more addresses than the preceding one and do not preclude receiving at a second time or a third time a dynamic security policy that includes only a single new network address. As Petitioner points out, at subsequent points in time Bhatia adds network addresses to its white list. Pet. 50–51. That Bhatia implements a new dynamic security policy by

adding addresses individually does not change the fact that Bhatia suggests to one of ordinary skill a dynamic security policy that includes more network addresses at subsequent times, as recited in claim elements 1.3–1.6.

Consequently, based on the evidence and arguments presented by Petitioner, we find that the combination of Jungck and Bhatia teaches limitations 1.3–1.6

Patent Owner also argues that sending an IP address from Bhatia's application layer to the packet filtering layer "is not tantamount to sending a dynamic security policy from an SPMS to a PSG at least because the IP address does not 'identify a packet transformation function to be performed on packets corresponding to the specified criteria.'" PO Resp. 32 (citing PO Resp. Section IV.4.A.4 (Patent Owner's discussion of claim limitation 1.7)). We address this argument below in our discussion of claim limitation 1.7.

6. Claim Limitation 1.7

Petitioner identifies as claim element 1.7 (and as corresponding claim elements 17.7 and 33.7) the limitation that recites "receiving[e/receive] packets associated with a network protected by the packet security gateway." Pet. 51. Petitioner argues that a person of ordinary skill would understand that gateways must receive packets in order to filter packets. *Id*. With respect to Jungck, Petitioner argues that in each of Emb#3, Emb#4, and Emb#5, the edge server (or packet security gateway) receives packets. *Id.* Petitioner also contends that Bhatia discloses receiving packets at packet filter layer 13 of a DoS detection device. *Id*.

Patent Owner asserts the claims should not be found unpatentable because Petitioner fails to identify the network protected by the device of Jungck and Bhatia. PO Resp. 33. Petitioner responds that in Emb#3 the packets received by the edge server are associated with the protected

network containing subscribing server 108 and that Jungck discloses its edge servers form "a security barrier which isolates the core infrastructure and servers of the network/Internet from the edge where the clients are located." Pet. Reply 9 (citing Ex. 1010 ¶¶ 108–109, 116; Ex. 1026, Jeffay Reply Decl. ¶¶ 81–83, 85).

Patent Owner further contends that Jungck's edge servers are not gateways for subscribing servers 108, 110 because the edge servers are not in or at the boundary of any network that includes the subscribing servers, but instead are within sub-networks of service providers 118, 120. PO Resp. 34–37 (citing Ex. 2004, Goodrich Decl. ¶ 193). As support for this assertion, Patent Owner argues that in Jungck a DDoS attack never reaches servers 108, 110. *Id.* at 35–36 (Ex 1010 ¶ 104 ("where a DDoS [distributed denial of service] attack cripples one edge server 502 and its associated sub-networks, the remaining edge servers 502 at other service providers 118, 120 (and their assocated sub-networks) can remain operational and therefore the server 108 suffers minimal impact as a result of the DDoS attack")).

According to Patent Owner, in Jungck's Emb#3 the edge servers do not protect networks, but instead protect subscribing servers 108, 110, which are only application servers that may be members of some undefined network. PO Resp. 33–34. Turning to Jungck's Emb#3, Patent Owner argues Jungck's edge servers do not protect networks, but only intercept traffic destined for the subscribing servers, allowing all other traffic to pass. *Id.* at 34. Patent Owner asserts Petitioner has a "flawed misunderstanding" of Jungck, as evidenced by Dr. Jeffay's testimony that Jungck's edge servers are intended to protect network 100 as well as networks 108, 110. PO Resp. 36; PO Surreply 15 (citing Ex. 2009, Jeffay Tr. I") 34:14–17). Patent Owner

asserts that the same arguments apply to Jungck's Emb#3 and Emb#4. *Id.* Petitioner asserts that Dr. Jeffay's testimony is correct. Pet. Reply 10.

We agree with Petitioner because Dr. Jeffay's testimony is consistent with Jungck's discussion of edge servers. Figure 6 of Jungck is shown below.

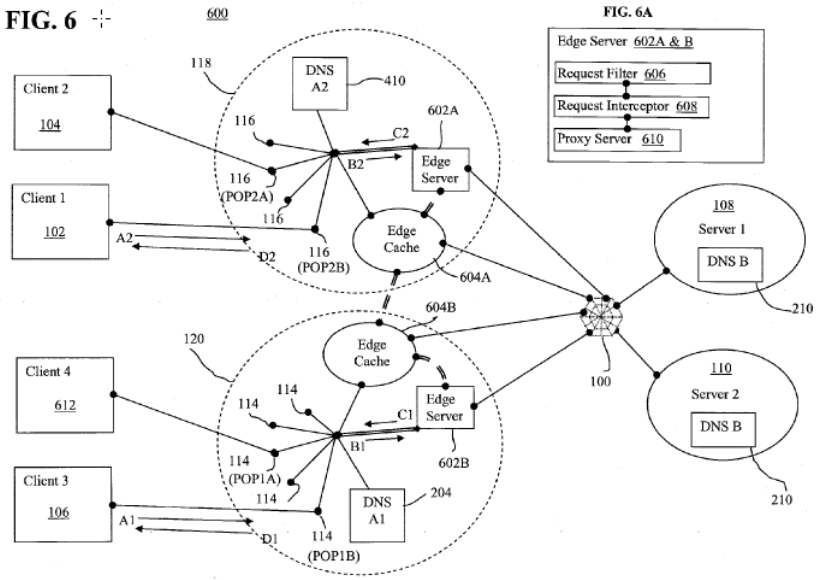


Figure 6 of Jungck illustrates Emb#3. Ex. 1010 ¶ 14. Jungck's edge servers 602A, 602B can be implemented as separate devices or integrated with other devices and may be provided at every major network 100 intersection to cover every point of presence (POP) 114 on the edge of network 100. *Id.* ¶ 107. Jungck's edge server can "intercept[ing] data traffic at the packet level based on the source or destination IP address contained within the packets flowing past the edge server 602." *Id.* ¶ 108. Any network traffic destined for a subscribing server can be intercepted by the edge server and acted upon, providing complete isolation of the subscribing server 108, 110. *Id.* In the case of subscriber "ingress filtering," packet filter 606 pre-filters traffic to first determine if the traffic it is monitoring is

associated with a subscribing/affiliated server and if not that traffic is ignored. *Id.* ¶ 113. In other circumstances, a subscription is not necessary. Jungck discloses that edge server 602 monitors transmissions from clients for previous identified malicious code and eradicates it or prevents it from reaching network 100. *Id.* ¶¶ 109–110. In this way, Jungck protects network 100. Thus, we are persuaded by Petitioner's arguments that Jungck teaches claim limitation 1.7.

Petitioner also contends that Bhatia discloses receiving packets at packet filter layer 13 of a DoS detection device. Pet. 51. According to Patent Owner, Bhatia's protection of an application layer is not protection of a network, and Bhatia fails to describe any particular networks protected by its packet filter layer. PO Resp. 39, PO Surreply 16. Petitioner, however, points out that Bhatia teaches its packet filtering layers can be implemented and executed by IP router forwarding layers and other DoS prevention devices that may be located within the Session Border Controller or at other points of the network. Pet. Reply 10 (citing Ex. 1011 ¶ 22; Ex. 1026, Jeffay Reply Decl. ¶ 102). We further note that Figure 1 of Bhatia is a diagram of "a typical network diagram undergoing a DoS attack" and that Bhatia is applicable to an "Internet type network communication system." Ex. 1011 ¶ 23, Fig. 1. Thus, we agree with Dr. Jeffay that a person of ordinary skill would have understood Bhatia discloses positioning devices at the edge of a network to intercept and filter traffic in order to protect the network. Ex. 1026, Jeffay Reply Decl. ¶ 102.

7. Claim Limitation 1.8

Petitioner identifies as claim element 1.8 (and as corresponding claim elements 17.8 and 33.8) the limitation that recites "perform/performing, on a packet by packet basis, at least one of multiple packet transformation

functions specified by the plurality of dynamic security policies on the packets associated with the network protected by the packet security gateway." Pet. 52. Petitioner argues that in each of its embodiments Jungck discloses evaluating each received packet individually and acting on it according to specific rules, for example by forwarding the packet or eradicating it. *Id*. at 52–53.

Patent Owner does not dispute explicitly that the combined teachings of Jungck and Bhatia teach claim limitation 1.8. Having reviewed the evidence of record, we are persuaded Petition has demonstrated sufficiently that the combined teachings of Jungck and Bhatia would have taught claim element 1.8 to a person of ordinary skill in the art.

8. Claim Limitation 1.9

Petitioner identifies as claim element 1.9 (and as corresponding claim elements 17.9 and 33.9) the limitation that recites "wherein performing the at least one of the multiple packet transformation functions specified by the plurality of dynamic security policies on the packets comprises performing at least one packet transformation function other than forwarding or dropping the packets." Pet. 53. Petitioner cites Emb#4 of Jungck as disclosing a variety of functions including modifying packets, replacing packets, and logging, storing and modifying the IP address and payload of the packets. Pet. 54 (citing Ex. 1010 ¶ 153). Petitioner also cites Bhatia as disclosing additional functions, such as modifying priorities in controlling packet rates, for example by queuing packets. *Id*.

Patent Owner does not dispute explicitly that the combined teachings of Jungck and Bhatia teach claim limitation 1.8. Having reviewed the evidence of record, we are persuaded Petition has demonstrated sufficiently

that the combined teachings of Jungck and Bhatia would have taught claim element 1.9 to a person of ordinary skill in the art.

9. Motivation to Combine the Teachings of Jungck and Bhatia

a) Combination of the Jungck Embodiments

Petitioner contends that a person of ordinary skill would have been motivated to combine the teachings of Emb#3, Emb#4, and Emb#5 of Jungck because all apply to the same network, and because Emb#4 provides similar functions to that of Emb#3 without introducing packet flow latency or failure points as edge/packet interception devices are added. Pet. 34 (citing Ex. 1010 ¶ 126). Petitioner contends that Emb#5 also provides similar functionality in "Optical Internet" environments that have higher traffic volume. *Id*. at 34–35 (citing Ex. 1010 ¶¶ 263–269, 275). According to Petitioner, a person of ordinary skill would have been motivated to combine the teachings of the three embodiments because Jungck's devices provide similar functions (packet filtering) to address similar problems (malicious distributed denial of service (DDoS) attacks). *Id*. (citing Ex. 1005, Jeffay Decl. ¶¶ 205–206; Ex. 1010 ¶¶ 25, 111, 182–183, 282).

Citing the differences between Figures 6 and 7 of Jungck, Patent Owner contends there would have been no reason to combine Emb#3 and Emb#4. PO Resp. 52–56. Patent Owner cites the placement of edge servers 602 such that network 100 is always to one side isolating ISP networks 118, 120 to intercept traffic destined for either subscribing server 108, 110. *Id*. at 52–53.

According to Patent Owner, Emb#4 of Figure 7 does not isolate network 100 to one side only and instead shows packet interceptor 720 with network 100 on both sides of router 702. *Id*. at 53–55.

Petitioner emphasizes that in both Emb#3 and Emb#4 packets from downstream clients flow into an edge device within an ISP, packet filters analyze the packets, and the packets may flow out of the edge device to an isolated network containing subscribing servers or their intended destinations (unless they are eradicated or prevented from reaching network 100). Pet. Reply 15–16; Ex. 1010 ¶ 111. We agree with Petitioner that, in view of the similarity in the functions performed by Emb#3 and Emb#4, the difference in the corresponding topologies relative to network 100 shown in Jungck's Figure 6 and Figure 7 does not negate the reason to combine the respective teachings to a person of ordinary skill. *Id.* Jungck states edge server 602 of Emb#3 operates similarly to edge servers 402 and 502 of the first and second embodiments. Ex. 1010 ¶ 108. In its discussion of Emb#4, Jungck states

> As can be seen from the above embodiments, edge devices generally perform the basic functions of intercepting packets from the general flow of network traffic, processing the intercepted packets and potentially releasing the original packets and/or reinserting new or modified packets back into the general flow of network traffic. In general, it is the choice of which packets to intercept and the subsequent processing performed by each edge/packet intercepting device on the intercepted packets, e.g. the application, which distinguishes each device.

Id. ¶ 125. We are persuaded that a person of ordinary skill would have had reason to combine the teachings of Emb#3 and Emb#4 to achieve the specific purpose stated in Jungck, i.e. to "decouple the interception of packets from the processing of those intercepted packets and provide a generic packet interception and pre-processing engine which can be utilized in parallel by multiple edge devices" and "[to] provide a standardized interface to a network such as the Internet for the connection of edge type or packet intercepting

device making it easier for an ISP or Carrier to offer services/enhancements of many different providers." *Id.* ¶ 126.

We also are not persuaded by Patent Owner's argument that the edge servers in Emb#3 cannot be conflated with the packet interceptor adaptor 720 of Emb#4 because they are to be used in conjunction with, but separately from, the edge servers in Emb#3. PO Resp. 55 (citing Ex. 2004, Goodrich Decl. ¶ 97). As Petitioner points out, Dr. Goodrich's testimony effectively acknowledges that Jungck discloses combining Emb #3 and Emb#4. Pet. Reply 16. Petitioner's argument is also consistent with the presence of Request Interceptor 608 in Emb#3 and with Patent Owner's acknowledgement that its arguments discussed above concerning the role played by Jungck's edge server 602 in Emb#3 apply to Emb#4 and Emb#5. PO Surreply 15. *See above* Section VI.B.6 [discussion of claim limitation 1.7].

Patent Owner contends that a person of ordinary skill would not have been motivated to combine the teachings of Emb#5 with Emb#3 or Emb#4 because Figure 9 illustrating Emb#5 shows a topology with network 100A and 100B on both sides of device 900, which Jungck does not disclose functions as an edge server of Emb#3. PO Resp. 56–58. As Petitioner points out, however, Jungck discloses that the devices in Emb#3–Emb#5 all operate in a similar manner. Ex. 1010 ¶¶ 130–131, 268–269, 271), *cited in* Pet. Reply 17.

Patent Owner also argues that connecting intercepting devices in series introduces latency. PO Resp. 56–58. However, we credit Petitioner's expert's testimony, that in the Optical Internet, the environment for Emb#5, pipelining is a well- known means for improving throughput. Ex. 1026, Jeffay Reply Decl. ¶ 44; Ex. 1010 ¶ 278, *cited in* Pet. Reply 17.

In consideration of the above, we are persuaded that Petitioner has demonstrated a person of ordinary skill would have had reason to combine the teachings of Emb#3–Emb#5 of Jungck.

b) Combination of Jungck and Bhatia

Petitioner contends that a person of ordinary skill would have been motivated to combine the teachings of the Jungck Embodiments with those of Bhatia because both references are directed to packet filtering techniques to prevent DoS attacks in a network environment. Pet. 35. Petitioner contends that a person of ordinary skill would have recognized that Bhatia's dynamic creation and updating of white lists could provide an additional tool to implement Jungck's similar objective, i.e., combatting attacks with dynamic policies, with predictable operational results. *Id.* at 36–37.

Patent Owner argues that, because Bhatia does not have edge cache or edge server devices, its topological organization is different from that of the Jungck, requiring under experimentation to combine the teachings of the references. PO Resp. 60–61 (noting that architectural diagrams and description in Jungck are based on flows between functional components, whereas Bhatia's architecture is based on an alternate network-layer approach). Petitioner notes, however, that its proposed combination of Jungck and Bhatia does not require introducing a component in addition to the Jungck's edge device or edge adaptor/packet interceptor; instead Bhatia teaches supplementing the function of those components, i.e., logical operations that could be implemented as whitelists or blacklists as part of rule sets used by Jungck's functional components. Pet. Reply 19 (citing Ex. 1026, Jeffay Reply Decl. ¶¶ 23; Ex. 1010 ¶¶ 23, 132, 191). We find Petitioner's argument persuasive.

According to Patent Owner, Jungck also specifically teaches against using cache servers for dynamic content that cannot be cached. PO Surreply 20–21 (citing Ex. 1010 ¶ 72; Ex. 2004, Goodrich Decl. ¶¶ 119–120.

Patent Owner's argument is not persuasive. The subject matter concerning cache servers cited by Patent Owner states that conventional cache servers 208 do not alleviate completely existing net congestion problems because they have high miss rates and low hit rates that translate into minimal impact on server 108 load, response times, and network 100 bandwidth. Ex. 1010 ¶ 72. As a result, by passing missed requests to the server 108, server 108 is exposed to increased security risk from untrusted network 100. *Id.* In its various embodiments, Jungck addresses these problems with its edge server that monitors incoming traffic and, if the packet makes it to the subscribing server, a determination is made whether the request can be satisfied from the edge cache. *See, e.g.*, Ex. 1010 ¶¶ 110–113 (concerning Emb#3).

Patent Owner further argues lack of motivation to combine because adding Bhatia's blacklist, whitelist and rest-list to Jungck introduces undesirable network congestion and latency to Jungck's networks, requiring periodic whitelist and blacklist updating at every POP on the Internet. PO Resp. 59, Pet. Surreply 2 (citing Ex. 2004, Goodrich Decl. ¶ 119). We find persuasive Petitioner's argument that a person of ordinary skill would have understood updating whitelists and blacklists in a combination of Jungck and Bhatia is similar to updating routing tables in Jungck's edge devices as disclosed and, because routing updates occur at high frequencies relative to the rates at which whitelist and blacklists change, they do not add considerable congestion to the network. Pet. Reply 19 (citing Ex. 1026, Jeffay Reply Decl. ¶¶ 50–51)

Patent Owner further argues Petitioner failed to explain why a person of ordinary skill would combine Jungck's disparate embodiments with each other and with Bhatia by treating the three Jungck embodiments and Bhatia as a box of interchangeable parts. PO Resp. 55. According to Patent Owner, Petitioner's combination of the Jungck Embodiments with Bhatia encompasses as many as 12,288 distinct combinations for consideration and fails to identify Petitioner's challenge grounds with the requisite specificity. PO Resp. 51–52 (citing *Sanofi-Aventis U.S. LLC v. Astrazeneca Pharms. LP*, IPR2016-00348, Paper 10 at 6 (PTAB June 28, 2016)(Decision Denying Institution)).

We are not persuaded by Patent Owner's arguments that Petitioner treats the Jungck Embodiments and Bhatia as interchangeable parts without specifying how or why each of the Jungck Embodiments would be used with one another. The test for obviousness is not whether the features of a secondary reference may be bodily incorporated into the structure of the primary reference; nor is it that the claimed invention must be expressly suggested in any one or all of the references. Rather, the test is what the combined teachings of the references would have suggested to those of ordinary skill in the art. *MCM Portfolio LLC v. Hewlett-Packard Co.*, 812 F.3d 1284, 1294 (Fed. Cir. 2015) (citing *In re Keller*, 642 F.2d 413, 425 (CCPA 1981)). We addressed above Petitioner's assertions concerning the motivation to combine the teachings of the references. We are not persuaded by Patent Owner's arguments that Petitioner has failed to explain a proper motivation for the proposed combination of the references with the requisite specificity.

10. Objective Considerations

Before determining whether a claim is obvious in light of the prior art, we consider any relevant evidence of secondary considerations—i.e., objective indicia—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, (2) industry praise, and (3) commercial success/licensing. PO Resp. 62–71.

"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—e.g., 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)).

a) Long-Felt But Unmet Need and Failure of Others

According to Patent Owner, "the '205 Patent satisfied a long-felt need in the industry that others had failed to solve—namely, how to provide proactive network protection that could '"scale to larger networks.'" PO Resp. 68.

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. 68–69 (citing Ex. 2013, 5; Ex. 2004, Goodrich Decl. ¶ 253), PO Surreply 22–23. Patent Owner's expert, Dr. Goodrich, characterizes Jungck and Bhatia as such signature based systems, but Dr. Goodrich 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 '205 patent. Ex. 2004, Goodrich Decl. ¶ 253. In addition, the Chincheck presentation does not comment on any specific approach or technology, including that discussed in the '205 patent. Ex. 2013, 3. Thus, even if the Chincheck presentation indicates a need exists to improve certain types of signature based systems, it provides insufficient evidence that the '205 patent addresses that need, or that the approach in Jungck and Bhatia "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. 69–72 (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 71 (quoting Ex. 2006 ¶ 210). According to Patent Owner, ESG's description of Patent Owner's solution is tied to the inventions in the '205 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 71. We note, however, we do not construe a dynamic security policy as limited to one that is updated automatically, as the '205 patent describes an administrator updating the dynamic security policy manually. Ex. 1001, 13:7–33.

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 '205 patent. Pet. Reply 23 (citing Ex. 1027, Transcript of Deposition of Dr. Michael Goodrich ("Goodrich Tr.") 24:12–30:7). As Petitioner further notes, ESG's paper provides no specifics about how any of Patent Owner's products meets the claim limitations. *Id.*

In view of the above, Patent Owner does not establish a sufficient nexus between the invention claimed in the '205 patent and the purported long felt, unmet need.

b) 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. 72–73. 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. 72 (citing Ex. 2006 ¶ 7). Patent Owner states that "during its test of an embodiment of the claimed PSG (i.e., Centripetal's Threat Intelligence Gateway (TIG))" the intelligence was updated without loss. *Id.* at 71–72. Patent Owner further assets that the packet transformation function claimed in the '205 patent wwas cited in the ESG paper as helping to achieve transformation of CTI into proactive action at scale. *Id.* (citing Ex. 2004, Goodrich Decl. ¶ 258. Nevertheless, citing these generalized statements, Patent Owner does not associate this information with the specific limitations of the challenged claims. Patent Owner does not address whether or how they are part of the claimed invention or address 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 as having the "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 as using "5 million indicators simultaneously." PO Resp. 72 (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; Ex. 2004, Goodrich Decl. ¶ 263).

Similar to its arguments about ling felt unmet need, Patent Patent Owner's sole explanation of nexus based on industry praise is a conclusory assertion that "[t]he salutary benefits of Centripetal's TIG [threat interface gateway] are made possible in large part by the '205 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." PO Resp. 73 (citing Ex. 2004, Goodrich Decl. ¶ 264). Dr. Goodrich's testimony cited in support of this statement is a near-verbatim copy of this statement with no additional explanation. *See* Ex. 2004 ¶ 264; 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.

c) Commercial Success and Licensing

Patent Owner contends that the commercial success of its RuleGATE product as well as a license to U.S. Patent No. 9,565,213 ("the '213 patent") taken by Keysight Technologies are compelling secondary considerations of

non-obviousness. PO Resp. 74–75. Patent Owner argues "[t]he declaration of Jonathan Rogers, Centripetal's Chief Operating Officer, described the significant success of Centripetal's RuleGATE product, which embodies the '205 Patent." *Id.* at 74 (citing Ex. 2016, Declaration of Jonathan Rogers ("Rogers Decl.")). In fact, Mr. Rogers offers no testimony concerning the '205 patent. Mr. Rogers testified that Patent Owner's RuleGATE system has been sold to customers and that RuleGATE embodies a different patent, i.e., the '213 patent, although the record includes no technical analysis to support his testimony that RuleGATE embodies even the '213 patent. Ex. 2016, Rogers Decl. ¶¶ 3–6.

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 or the '205 patent. Ex. 2016 ¶ 3. Mr. Rogers does not state he has any personal knowledge of the '213 patent or the '205 patent or their claims; he does not state what aspects of RuleGATE embody the claims of the '213 patent or the '205 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. *See*, Ex. 2016. Indeed, Mr. Rogers does not provide any basis for his assertion that RuleGATE does, in fact, embody the claims of the '213 patent or Patent Owner's assertion that RuleGATE embodies the claims of the '205 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 that 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 in either the '213 patent or the '205 patent that is the subject of this proceeding, we do not apply a presumption of nexus in this case. As with long felt unmet need and industry praise discussed above, we also find that Patent Owner's evidence is insufficient to establish a nexus between the claimed invention and the alleged commercial success of the RuleGATE product.

As additional evidence of commercial success, Patent Owner cites a "worldwide, royalty-bearing, non-transferable, irrevocable, nonterminable, non-exclusive license to Centripetal's worldwide patent portfolio," including the '205 patent, noting the arrangement included a "one-time payment of $25 million for past damages," taken by Keysight Technologies to settle a patent infringement suit. PO Resp. 74–75 (citing Ex. 2012, 83). Patent Owner further argues that because it sells products that embody the invention of the '205 patent, and those licenses are in the same security market, a presumption exists that the commercial success of Patent Owner's products is due to the patented invention of the '205 patent. *Id.* at 75.

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 '205 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 '205 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 '205 patent. *See id.*

Petitioner points out that Keysight was sued on other patents beyond the '205 patent. Pet. Reply 25. Petitioner also points out that Mr. Rogers identifies only three sales of RuleGATE, does not state how much revenue was received from these sales, whether Centripetal made a profit on these sales, how much of Centripetal's total revenue is tied to these RuleGATE sales, the level of Centripetal's market share, or how the sales revenues for RuleGATE compare to competitor products. *Id.* at 24.

In consideration of the above, we are not persuaded Petitioner has shown a nexus between the '205 patent and commercial success of its products.

11. Conclusion as to Claim 1

In consideration of the above, we are persuaded Petitioner has demonstrated sufficiently that the person of ordinary skill would have had reason to combine the teachings of Jungck and Bhatia as asserted in the Petition. We find that Petitioner has demonstrated by a preponderance of the evidence that claim 1 is unpatentable under 35 U.S.C. 103(a) as obvious over the combined teachings of Jungck and Bhatia.

C. Claims 17 and 33

Petitioner treats together the elements of independent method claim 1 and the corresponding elements of independent claim 17, drawn to a system, and independent claim 33, drawn to non-transitory computer readable media having stored instructions. Pet. 37. Patent Owner treats claims 17 and 33 the same way. PO Resp. 12–39. For the same reasons as those applicable to claim 1, we find that Petitioner has shown by a preponderance of the evidence that independent claims 17 and 33 are unpatentable under 35 U.S.C. 103(a) as obvious over Jungck in view of Bhatia..

D. Claims 5, 21, and 37 as Obvious Over Jungck and Bhatia

Petitioner analyzes claims 5, 21, and 37 together, treating claim 5 as illustrative. Pet. 55. Claim 5 depends from claim 1 and recites in part "receiving, by the security policy management server, information associated with a Voice over Internet Protocol (VoIP) session." Petitioner notes that both Jungck and Bhatia explicitly teach applicability to VO IP systems. Pet. 55–56 (citing Ex. 1010 ¶¶ 31, 119, 191; Ex. 1011 ¶ 27). Claim 5 also recites "creating or altering, by the security policy management server and based on the information associated with the VoIP session, the at least one rule specifying the set of network addresses for which associated packets should be forwarded." *Id.* at 56. Petitioner notes that Jungck teaches techniques to prevent DDoS and other network attacks that are generally applicable to voice, video and data services and using a communication session to update a packet filter. *Id.* at 57. Petitioner cites Bhatia as teaching the use of information associated with a Vo IP session to create or alter a white list. *Id.* at 56 (citing Ex. 1011 ¶¶ 22, 27, 34–37).

Patent Owner does not respond explicitly to Petitioner's contentions concerning claims 5, 21, and 37 as obvious over the combined teachings of Jungck and Bhatia. We further determine that our analyses for claim 1 regarding motivation to combine and secondary considerations also apply to these claims. Having reviewed the entire record, and based on the evidence discussed above, we are persuaded Petitioner has demonstrated by a preponderance of the evidence that claims 5, 21, and 37 are unpatentable as obvious under 35 U.S.C. § 103(a) over the combined teachings of Jungck and Bhatia.

E. Claims 7, 23, and 39 as Obvious Over Jungck and Bhatia

Noting that claims 7, 23, and 39 relate to rerouting a packet based on a packet parameter, Petitioner analyzes these claims together, treating claim 7 as illustrative. Pet. 58. Claim 7 depends from claim 1 and recites in part "receiving the plurality of dynamic security policies comprises receiving at least one rule specifying a parameter." Petitioner cites Jungck as describing packet filtering rules that specify a parameter, such as a particular report number. *Id*. Claim 7 further recites "routing, by the one or more packet security gateways, at least one packet of the packets that matches the parameter to a network address different from a destination network address specified by the at least one packet." Petitioner cites Jungck as disclosing a rule that based on a parameter in an intercepted packet an action may be taken that modifies the destination IP address to an alternate destination and releases the packet. *Id*. at 58–59.

Patent Owner does not respond explicitly to Petitioner's contentions concerning claims 7, 23, and 39 as obvious over the combined teachings of Jungck and Bhatia. We further determine that our analyses for claim 1 regarding motivation to combine and secondary considerations also apply to these claims. Having reviewed the entire record, and based on the evidence discussed above, we are persuaded Petitioner has demonstrated by a preponderance of the evidence that claims 7, 23, and 39 are unpatentable as obvious under 35 U.S.C. § 103(a) over the combined teachings of Jungck and Bhatia

F. Claims 9, 25, and 41 as Obvious Over Jungck and Bhatia

Petitioner analyzes claims 9, 25, and 41 together, treating claim 9 as illustrative. Pet. 59. Petitioner notes that claims 9, 25, and 41 are substantively identical, and specify that the packet transformation function is

one of four functions recited in the claim, and that Jungck performs at least three of these functions: forwarding packets into (ingress) and out of (egress) the network protected by the Gateway, and dropping or deleting packets. Pet. 59 (citing Ex 1005, Jeffay Decl. ¶¶ 308–311).

Patent Owner does not respond explicitly to Petitioner's contentions concerning claims 9, 25, and 41 as obvious over the combined teachings of Jungck and Bhatia. We further determine that our analyses for claim 1 regarding motivation to combine and secondary considerations also apply to these claims. Having reviewed the entire record, and based on the evidence discussed above, we are persuaded Petitioner has demonstrated by a preponderance of the evidence that claims 9,25, and 41 are unpatentable as obvious under 35 U.S.C. § 103(a) over the combined teachings of Jungck and Bhatia.

G. Claims 2, 18, and 34 as Obvious Over Jungck, Bhatia and Ahn

Petitioner analyzes claims 2, 18, and 34 together, treating claim 2 as illustrative. Claim 2 recites in part "the one or more packet security gateways comprise at least two packet security gateways configured in series." Petitioner contends that each of the firewalls in Ahn constitutes a PSG because it receives packets and performs packet transformation functions on the packets. Pet. 64–65. Petitioner further notes that Ahn discloses firewalls including processors and packet filters in a serial configuration that could be readily incorporated into Jungck, which specifically describes using multiple processors for subdividing and serializing the processing of packets. *Id*. at 65 (citing Ex. 1005, Jeffay Decl., ¶¶ 325–332; Ex. 1014, Fig. 2; Ex. 1010 ¶¶ 278, 306). Claim 2 also recites forwarding packets from the first gateway to the second gateway, and the second gateway receiving the forwarded packets. Petitioner notes that, as

discussed above, this feature is taught by Ahn's serial configuration. *Id.* at 65–66.

Patent Owner contends that a person of ordinary skill would not have been motivated to combine the teachings of Ahn with those of Jungck Emb#3, Emb#4, Emb#5, and Bhatia because such a series connection would reduce the system's capability to operate at wire speed. PO Resp. 39–41 (citing Ex. 2004, Goodrich Decl. ¶ 219).

Petitioner comments on Dr. Goodrich's testimony concerning the combined teachings of Bhatia and Ahn, but notes its proposed combination is Ahn with the teachings of Jungck, not Bhatia. Pet. Reply 19. The Patent Owner Response does not argue Dr. Goodrich's testimony concerning combining Bhatia with Ahn. PO Resp. 39—41.

Petitioner contends a motivation to combine the teachings of Jungck and Ahn would have existed because Ahn's use of serial gateways can improve the efficiency of Jungck's packet analysis. Pet. 63–64; Ex. 1026, Jeffay Reply Decl. ¶¶ 58–62. Although Patent Owner correctly notes that Jungck points out the presence of additional intercepting devices introduces latency as to Emb#3 (PO Resp. 40; Ex. 1010 ¶ 124), Emb#4 of Jungck presents an edge adapter/packet interceptor system "without introducing additional network latency . . . with the addition of each such edge/packet interception device" (Ex. 1010 ¶ 126). Dr. Jeffay notes that Jungck's discussion of Emb#5 states there are both benefits and costs to implementing devices in series, rendering such decisions a matter of design choice. Ex. 1026 ¶ 60 (citing Ex. 1010 ¶ 278; Ex. 1029, Goodrich Tr. 93, 11–94:14) (acknowledging "there could be tradeoffs in serial processing" using serial processors to subdivide the processing task). Patent Owner also does not

rebut Dr. Jeffay's testimony that Ahn can improve the efficiency of Jungck's packet analysis. *See* Ex. 1026, Jeffay Reply Decl. ¶¶ 58–62.

In consideration of the above, we are persuaded Petitioner has demonstrated that a person of ordinary skill would have been motivated combine the teachings of Jungck and Ahn and that the combined teachings of Jungck, Bhatia, and Ahn teach the limitations of claims 2, 18, and 34. We further determine that our analyses for claim 1 concerning motivation to combine and secondary considerations of non-obviousness also apply to these claims. Therefore, we find that Petitioner has demonstrated by a preponderance of the evidence that claims 2, 18, and 34 are unpatentable under 35 U.S.C.

§ 103(a) over the combined teachings of Jungck, Bhatia, and Ahn.

H. Claims 3, 19, and 35 as Obvious Over Jungck, Bhatia, and Ahn

Petitioner analyses claims 3, 19, and 34 together, treating claim 3 as illustrative. Claim 3 depends from claim 2 and recites that a first of at least two packet security gateways performs a packet transformation function specified by the first of at least two rules, and the second of the packet security gateways performs a packet transformation specified by the second of at least two rules. Petitioner notes that Ahn discloses a firewall policy that includes an ordered set of packet filtering rules in a dynamic security policy that includes at least two rules. Pet. 67. Petitioner cites paragraphs 20–21 of Ahn as disclosing that rules in subset A 208 are executed before the rules in subset B 210, where the rules in subset B 210 are applied by the second gateway. *Id.* at 69.

Patent Owner repeats the unpersuasive arguments it made as to claims 2, 18, and 34. PO Resp. 42. Patent Owner also argues that, although Dr. Jeffay points to Jungck Emb#4 as processing rules sets in a prioritized

manner, Jungck does not disclose rules are executed by different PSGs. *Id.* Petitioner notes that Ahn teaches this feature. Pet. Reply 12 (citing Ex. 1026, Jeffay Reply Decl. ¶ 116 (testifying "that is exactly what is disclosed by Ahn," citing Ex. 1014 ¶¶ 7, 16–17, 21–22, 31, Fig.2). Patent Owner also states Jungck Emb#4 teaches against the serial configuration of packet filtering devices. PO Resp. 42 (citing Ex. 2004, Goodrich Decl. ¶ 224). Noting Jungck's teaching of benefits and costs to implementing devices in series, Petitioner repeats its persuasive design choice arguments. Pet. Repl. Decl. 11; *see* Ex. 1026, Jeffay Reply Dec;. ¶ 116.

In consideration of the above, we are persuaded Petitioner has demonstrated that a person of ordinary skill would have been motivated combine the teachings of Jungck and Ahn and that the combined teachings of Jungck, Bhatia, and Ahn teach the limitations of claims 3, 19, and 35. We further determine that our analyses for claim 1 concerning motivation to combine and secondary considerations of non-obviousness also apply to these claims. Therefore, we find that Petitioner has demonstrated by a preponderance of the evidence that claims 3, 19, and 35 are unpatentable under 35 U.S.C.
§ 103(a) over the combined teachings of Jungck, Bhatia, and Ahn.

I. Claims 10, 26, and 42 as Obvious Over Jungck, Bhatia, and Ahn

Petitioner analyzes claims 10, 26, and 42 together, treating claim 10 as illustrative. Claim 10 depends from claim 1 and recites "receiving at least one rule comprising a five-tuple specifying one or more protocols, one or more Internet Protocol (IP) source addresses, one or more source port values, one or more IP destination addresses, and one or more destination port values." Petitioner cites the testimony of Dr. Jeffay that a five-tuple is a

long known standard method of identifying packets for implementing policies, and is fundamental to TCP/IP and other protocols. Pet. 69 (citing Ex. 1005 ¶ 346). Petitioner further cites Jungck and Ahn as disclosing use of the well-known five-tuple parameters for packet filtering. *Id*. at 70 (citing Ex 1010 ¶ 149; Ex. 1014 ¶ 30).

Patent Owner does not respond explicitly to Petitioner's contentions concerning claims 10, 26, and 42 as obvious over the combined teachings of Jungck, Bhatia and Ahn. We agree with Petitioner's arguments and evidence, and find that the asserted combination of art teaches the limitations of these claims. We further determine that our analyses for claim 1 regarding motivation to combine and secondary considerations of non-obviousness also apply to these claims. Having reviewed the entire record, and based on the evidence discussed above, we are persuaded Petitioner has demonstrated by a preponderance of the evidence that claims 10, 26, and 42 are unpatentable as obvious under 35 U.S.C. § 103(a) over the combined teachings of Jungck and Bhatia.

J. Claims 6, 22, and 38 as Obvious Over, Jungck, Bhatia, and Ke

Petitioner analyzes claims 6, 22, and 38 together, treating claim 6 as illustrative. Pet. 74. Claim 6 depends from claim 1 and recites in part "the plurality of dynamic security policies specify that a first portion of the packets should be placed in a first forwarding queue and a second portion of the packets should be placed in a second forwarding queue." Ke relates to an Internet security system. Ex. 1015, 1:12. Noting that Jungck teaches treating packet traffic differently to differentiate service offerings, Petitioner cites Ke as disclosing quality of service (QoS) based on priority queuing rules for detecting, intercepting, dropping, and logging unwanted packets implemented by an Internet security device, e.g., to "queue packets in a

priority queue so that certain packets get priority over others." Pet. 74 (citing Ex. 1015, 4:51–57).

Claim 6 further recites "the first forwarding queue having a higher forwarding rate than the second forwarding queue," and "placing, by the one or more packet security gateways, the first portion of the packets in the first forwarding queue; and placing by the one or more packet security gateways, the second portion of the packets in the second forwarding queue." Petitioner notes that Ke discloses a high priority queue for some packets, such as control packets, and other queues for normal packets. *Id*. at 74–75 (citing Ex. 1015, 4:50–57; Ex. 1005, Jeffay Decl. ¶¶ 358–361). In addition, Petitioner notes that the purpose of the queues is to differentiate packets into different queues based on policies. *Id.*

Patent Owner contends that Ke does not disclose the first and second forwarding queues, but instead uses a single data structure, i.e., a layer 2 FIFO (first in first out memory), a splitter and priority queuing logic unit. PO Resp. 42–43 (citing Ex. Fig. 3, 4:49–57). According to Patent Owner, Ke's priority structure is a single queue that processes elements according to priority rather than the FIFO protocol. *Id.* at 43–44 (citing Ex. 2004, Goodrich Decl. ¶ 234). Petitioner contends Patent Owner's assertion that Ke does not teach multiple queues is incorrect because a person of ordinary skill would have understood that the priority queueing logic could be implemented using a single queue, as argued by Patent Owner, or as multiple queues connected to the output of an interconnection device. Pet. Reply 12 (citing Ex. 1005, Jeffay Decl. ¶¶ 354, 360; Ex. 1026, Jeffay Reply Decl. ¶ 119).

Patent Owner contends Petitioner is wrong because the splitter in Figure 3 of Ke merely determines which MAC port a packet should be

forwarded on, rather than teach the first and second queues recited in claims 6, 22, and 38. Pet. Surreply 17 (citing Ex. 1015, 6:10–20).

Patent Owner's citation to Ke does not address Petitioner's assertion that a person of ordinary skill would have known about connecting multiple queues to an interconnection device. Dr. Jeffay testifies "[t]o support 'real time' applications, network interconnection devices may provide multiple queues for an output interface and use these queues to implement a priority transmission scheme." Ex. 1005 ¶ 354. According to Dr. Jeffay, an interconnection device capable of recognizing a high-priority application can place arriving transmission units into a higher priority queue than transmission units that are not so recognized. *Id.*

We further note claims 6, 22, and 38 are not drawn to any particular structure. Claims 6, 22, and 38 recite first and second portions of the packets are placed in first and second forwarding queues with the first forwarding queues having a higher forwarding rate than the second forwarding queues. Method claim 6 recites the PSGs placing the packets in the queues, system claim 22 recites the PSGs "are configured" to place the packets in the queues, and computer readable media claim 38 recites the instructions when executed cause the PSG to place the packets in the queues. The claims do not limit how the queues are formed. Patent Owner does not dispute Dr. Jeffay's testimony that Ke's transmission logic at the output interface transmits high priority packets, i.e., session control packets first, resulting in such packets having a higher transmission rate, and transmits normal packets only when the output interface is available.

In consideration of the above, we are persuaded that Petitioner has demonstrated the combined teachings of Jungck, Bhatia, and Ke teach the limitations of claims 6, 22, and 38 to a person of ordinary skill in the art and

that such a person would have had reason to combine these teachings. We further determine that our analyses for claim 1 concerning secondary considerations of non-obviousness, also apply to these claims. Therefore, we find that Petitioner has demonstrated by a preponderance of the evidence that claims 6, 22, and 38 are unpatentable under 35 U.S.C. § 103(a) over the combined teachings of Jungck, Bhatia, and Ke.

K. Claims 8, 24, and 40 as Obvious Over Jungck, Bhatia, Ingate, and RFC2003

Petitioner analyzes claims 8, 24, and 40 together, treating claim 8 as illustrative.

a) The Printed Publication Status of Ingate

We turn first to Patent Owner's contentions that Petitioner failed to demonstrate Ingate is a printed publication for prior art purposes. PO Resp. 45–50. As evidence Ingate is a printed publication, the Petition included the Declaration of Scott Beer (Ex. 1023, "Beer Decl. 1"). Patent Owner did not dispute whether Ingate is a printed publication in its Preliminary Response in this proceeding. *See* Paper 6. In a related case, Patent Owner disputed Petitioner demonstrated Ingate is a printed publication, arguing that Beer Decl. 1 failed to provide sufficient evidence Ingate was available to the public. *See Cisco Systems, Inc. v. Centripetal Networks, Inc.*, IPR2018-01505 ("Cisco I"), Paper 6 at 22–25. In that case, we agreed with Patent Owner and declined to institute *inter partes* review on the basis that Petitioner had failed to show Ingate was a printed publication. *See* Cisco I, Paper 7 (Decision Denying Institution), Paper 10 (Decision Denying Petitioner's Request for Rehearing).

After we denied institution in Cisco I, in this proceeding Petitioner filed, and we granted, Petitioner's Motion to file Supplemental Information.

See Papers 10, 11, 14. Petitioner then filed the Supplemental Declaration of Scott Beer (Ex. 1024 ("Beer Decl. 2")) and a page from the Wayback Machine (Ex. 1025). Paper 15. Patent Owner contends that Petitioner again failed to carry its burden of demonstrating Ingate is a printed publication because Petitioner failed to show Ingate was accessible by the public as of the '205 patent's critical date. PO Resp. 44 (citing *Acceleration Bay, LLC v. Activision Blizzard Inc.*, 908 F.3d 765, 772 (Fed. Cir. 2018) (petitioner's burden to prove reference is a printed publication and "public accessibility" has been called the touch-stone in determining whether a reference is a "printed publication")).

Beer Decl. 2 repeats much of the testimony from Beer Decl. 1 concerning Mr. Beer's role as author of Ingate and his participation in its purported publication, but provides additional detail not found in Beer Decl. 1. *See generally,* Ex. 1024, Beer Decl. 2. Mr. Beer states that Ingate was published and available on or around September 2, 2008 and, although he was not personally responsible for placing Ingate on the website, Ingate's process for posting an article to its website included a review of the article by a supervisor and an update to the website by an administrator. Beer Decl. 2 ¶ 5. Although Patent Owner emphasizes that Mr. Beer, did not post the article himself, we are not persuaded by Patent Owner's argument that there is no evidence of Ingate's business practices to corroborate Mr. Beer's testimony about the timing of the publication because Mr. Beer could not produce a document process for publishing articles. PO Resp. 46–47 (citing Ex. 2018, Transcript of Deposition Testimony of Scott Beer (Beer Tr., 31:18–20). Although such documentary could add further persuasive weight to Mr. Beer's testimony, we find that testimony itself to be credible evidence of the process Ingate followed to post Mr. Beer's article to Ingate's website.

Mr. Beer states he would typically check to confirm the website was updated correctly and that the article was available. *Id.* Even more persuasive is Mr. Beer's testimony that he saw Ingate on the website shortly after it was published in September 2008. *Id.*

Patent Owner further contends that Mr. Beer failed to provide evidence that the Ingate reference was meaningfully indexed, such that an interested person exercising reasonable diligence would have found it. PO Resp. 46 (citing *Acceleration Bay*, 890 F.3d at 774). As the Federal Circuit points out, our inquiry into public accessibility is not limited to indexing—"[w]hile cataloging and indexing have played a significant role in our cases involving library references, we have explained that neither cataloging nor indexing is a necessary condition for a reference to be publicly accessible." *In re Lister*, 583 F.3d 1307, 1312 (Fed. Cir. 2009) (citing *In re Klopfenstein*, 380 F.3d 1345, 1348 (Fed. Cir. 2004)).

As evidence of public dissemination and accessibility, Mr. Beer testifies he accessed the Ingate website with customers. Ex. 1024, Beer Decl. 2 ¶ 6. Although Mr. Beer does not state explicitly that he accessed the Ingate reference with customers, he provides as Exhibit 2 to his second declaration, a Wayback Machine page that includes a link to the Ingate reference present on the Ingate website in December 2008. *Id.*, Ex. 2. As further evidence that the Ingate reference was accessible to website visitors, Mr. Beer testifies there is no reason to believe the link ever was broken, and that the Ingate reference is accessible at the same URL today. Ex. *Id.* ¶ 6. He also testifies that "the Ingate reference was one of only about five papers available" at the link, making it easy to find. *Id.*

As further evidence the Ingate reference was made accessible to the public, Mr. Beer testified that he prepared an April 2009 "Knowledge Base"

article entitled "More About SIP Protocol Security: SIP Compliancy" that includes the URL linking to the Ingate reference under the heading "Want More Information." *Id.* ¶ 7, Ex. 3; Ex. 2018, Beer Tr. 43:16–44:8). According to Mr. Beer, this article would have been disseminated as a printed handout at various conferences, although Mr. Beer's declaration is not specific about how and where this Knowledge Base article was distributed.

Although Patent Owner contends that Mr. Beer's testimony only demonstrates Ingate was technically accessible and is not evidence Ingate could have been located by others (PO Surreply 18), Mr. Beer also testified that the presence of the term "partner" in the title "Ingate-Partner Information Guide" is evidence that the article was intended for customers, as Ingate referred to its customer as "partners." Ex. 1024 ¶ 4.

Patent Owner cites Mr. Beer's testimony that in order to access Ingate, a customer would have to create an account as evidence weighing against public accessibility. *Id.* at 46 (citing *SRI Int'l, Inc. v. Internet Sec. Sys., Inc.*, 456 F. Supp. 2d 623, 631 (D. Del. 2006) (placement of document on a password protected site suggests that it was not in the public domain). *See*, Ex. 2018, Beer Tr. 35:14–17, 36:12–18, 43:9–11. We note, however, that Mr. Beer testified that at an IT Expo in 2008 he gave a presentation concerning the concepts discussed in the Ingate reference. Ex. 1028, Beer Tr. 39:15–40:7. According to Mr. Beer, "[t]he document is not a very good presentation, but the concepts I would have used, absolutely. **The document itself would have been just on a table in the back**." *Id.* at 40:4–7 (emphasis added).

Having weighed the evidence including that the Ingate reference was posted to the Ingate website as a matter of routine, Mr. Beer's testimony that

saw the Ingate reference on the website in September 2008, the Wayback Mchine evidence that links to the article were present on the website in December 2008, testimony that the Ingate reference is accessible at that same link today, and the testimony that the Ingate reference was available in paper form to participants at the IT Expo in 2008, we are persuaded that Petitioner has demonstrated the Ingate reference was accessible to the public and is a printed publication for prior art purposes.

b) Analysis of Claims 8, 24, and 40

As noted above, Petitioner treats claims 8, 24, and 40 together. Ingate discloses securing an enterprise network as an edge device, e.g., firewall, using a deep packet inspection functionality that provides intrusion detection and intrusion prevention that handle attacks while the service and other Session Initiation Protocol (SIP) devices in the network can still be used. Ex. 1012, 11–12. Ingate notes that in the SIP application layer protocol requests and responses are SIP URIs with addresses in the form of an IP address or a domain name. *Id.* at 1. SIP requests and responses are written in plain text. *Id.* SIP is not secure implicitly and is communicated in the clear over the Internet. *Id.* Ingate discloses using the SIP URI in a Dial Plan that applies rules to all incoming SIP traffic to ensure that only predefined SIP Traffic is processed. *Id.* at 10.

RFC 2003 discloses altering the normal IP routing for datagrams by delivering them to an intermediate destination that would otherwise not be selected by the network part of the IP destination address field in the original IP header. Ex. 1016, 1. Encapsulation, in which an IP datagram maybe carried as a payload within another IP datagram, is suggested as a means to alter the normal IP routing. *Id.*

According to Petitioner, a person of ordinary skill would recognize that the packet filtering technology in Jungck and Bhatia could be modified to filter VoIP packets based on Ingate's SIP URI parameter because both Jungck and Bhatia teach packet filtering in VoIP systems, which use SIP. Pet. 77. Petitioner further argues that a person of ordinary skill would have recognized that packets can be routed to new destinations based on packet filtering criteria, as disclosed in Jungck, and that encapsulating packets for routing to new destinations as taught by RFC 2003 was a standard implementation for packet rerouting. *Id*. at 78.

Claim 8 depends from claim 7 and recites in part, "the parameter comprises a Session Initiation Protocol (SIP) Uniform Resource Identifier (URI)." Ingate teaches filtering packets based on a SIP URI parameter to address DDoS attacks, among other SIP vulnerabilities. *See* Pet. 78–79.

Claim 8 further recites, "the network address different from the destination network address specified by the at least one packet corresponds to a network device configured to copy information contained in the at least one packet and forward the at least one packet to the destination network address specified by the at least one packet." Petitioner cites Jungck as disclosing routing packets that match a parameter to network addresses different from the destination network address specified by the packet, and that such a packet may also be logged. *Id*. at 79–80.

Claim 8 still further recites, "routing the at least one packet comprises encapsulating the at least one packet with a header containing the network address different from the destination network address specified by the at least one packet." Based on the disclosure discussed above, Petitioner cites RFC 2003 as teaching this claim element. *Id*. at 80–81.

Patent Owner contends that Ingate does not cure Jungck's deficiencies concerning serial processing by packet filtering devices. PO Resp. 50 (citing its arguments concerning the combination of Jungck, Bhatia, and Ahn). As discussed above, we are not persuaded by Patent Owner arguments on this issue. *See above,* Section IV.B.G–I.

Our analysis of claim 8 applies to claims 24 and 40, as well. In consideration of the above, we are persuaded that Petitioner has demonstrated the combined teachings of Jungck, Bhatia, Ingate and RFC 2003 teach the limitations of claims 8, 24, and 40 to a person of ordinary skill in the art and that such a person would have has reason to combine these teachings. Further, we determine that our analyses discussed above concerning motivation to combine and secondary considerations of non-obviousness also apply to these claims. Therefore, we find that Petitioner has demonstrated by a preponderance of the evidence that claims 8, 24, and 40 are unpatentable under 35 U.S.C. § 103(a) over the combined teachings of Jungck, Bhatia, Ingate and RFC 2003.

L. Claim 11, 27, and 43 as Obvious Over Jungck, Bhatia, and RFC 2472

Petitioner analyzes claims 11, 27, and 43 together, treating claim 11 as illustrative. Pet. 83. Petitioner cites RFC 2474 as disclosing "differentiated services enhancements to the Internet protocol are intended to enable scalable service discrimination in the Internet without the need for per-flow state and signaling at every hop." Pet. 81 (citing Ex. 1017, 1). Petitioner notes that such services may include specifying the differential treatment of individual packets. *Id*. at 82. Noting that Jungck discloses enabling network operators to deploy traffic treatment algorithms of their own design to differentiate service offerings, Petitioner argues that a person of ordinary

skill would have recognized the standard set forth in RFC 2474 describes the implementation of a DSCP field for specifying such differentiated services. *Id*. (citing Ex. 1010 ¶¶ 191, 207; Ex. 1017, 1).

Claim 11 depends from claim 1 and recites, "receiving the plurality of dynamic security policies comprises receiving at least one rule comprising a Differential Service Code Point (DSCP) selector that maps to a DSCP field in an Internet protocol (IP) header of the packets." *Id*. at 83. Petitioner cites Emb#4 of Jungck for the proposition that packet filtering rules can be based on packet header information, and RFC 2474 as disclosing that the IP header can contain a differentiated services field that identifies packets for differentiated services. *Id.*

Patent Owner does not respond explicitly to Petitioner's contentions concerning claims 11, 27, and 43 as obvious over the combined teachings of Jungck, Bhatia and RFC 2474. Having reviewed the entire record, and based on the evidence discussed above, we find that the asserted combination of prior art teaches the limitations of these claims, that a person of ordinary skill would have been motivated to combine them in the manner alleged, and that Patent Owner's evidence of secondary considerations of non-obviousness is insufficient to be accorded significant weight. Consequently, we are persuaded Petitioner has demonstrated by a preponderance of the evidence that claims 11, 27, and 43 are unpatentable as obvious under 35 U.S.C. § 103(a) over the combined teachings of Jungck, Bhatia, and RFC 2474.

VII. CONCLUSION[8]

For the reason discussed above, we conclude that Petitioner has demonstrated by a preponderance of the evidence that:

Claims 1, 5, 7, 9, 17, 21, 23, 25, 33, 37, 39, and 41 are unpatentable under 35 U.S.C. § 103(a) as obvious over Jungck in view of Bhatia;

Claims 2, 3, 10, 18, 19, 26, 34, 35, and 42 are unpatentable under 35 U.S.C. § 103(a) as obvious over Jungck in view of Bhatia and Ahn;

Claims 6, 22, and 38 are unpatentable under 35 U.S.C. § 103(a) as obvious over Jungck in view of Bhatia and Ke;

Claims 8, 24, and 40 are unpatentable under 35 U.S.C. § 103(a) as obvious over Jungck, in view of Bhatia, Ingate and RFC 2003;

Claims 11, 27, and 43 are unpatentable under 35 U.S.C. § 103(a) as obvious over Jungck in view of Bhatia and RFC 2474.

In summary:

Claims	35 U.S.C. §	Basis	Claims Shown Unpatentable	Claims Not shown Unpatentable
1, 5, 7, 9, 17, 21, 23, 25, 33, 37, 39, 41	103(a)	Jungck, Bhatia	1, 5, 7, 9, 17, 21, 23, 25, 33, 37, 39, 41	

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

2, 3, 10, 18, 19, 26, 34, 35, 42	103(a)	Jungck, Bhatia, Ahn	2, 3, 10, 18, 19, 26, 34, 35, 42	
6, 22, 38	103(a)	Jungck, Bhatia, Ke	6, 22, 38	
8, 24, 40	103(a)	Jungck, Bhatia, Ingate, RFC 2003	2, 24, 40	
11, 27, 43	103(a)	Jungck, Bhatia, RFC 2004	11, 27, 43	
Overall Outcome			1–3, 5–11, 17–19, 21–27, 33–35, and 37–43	

VIII. ORDER

In consideration of the above, it is

ORDERED that claims 1, 5, 7, 9, 17, 21, 23, 25, 33, 37, 39, and 41 are unpatentable under 35 U.S.C. § 103(a) as obvious over Jungck in view of Bhatia;

FURTHER ORDERED that claims 2, 3, 10, 18, 19, 26, 34, 35, and 42 are unpatentable under 35 U.S.C. § 103(a) as obvious over Jungck in view of Bhatia and Ahn;

FURTHER ORDERED that claims 6, 22, and 38 are unpatentable under 35 U.S.C. § 103(a) as obvious over Jungck in view of Bhatia and Ke;

FURTHER ORDERED that claims 8, 24, and 40 are unpatentable under 35 U.S.C. § 103(a) as obvious over Jungck, in view of Bhatia, Ingate and RFC 2003;

FURTHER ORDERED that claims 11, 27, and 43 are unpatentable under 35 U.S.C. § 103(a) as obvious over Jungck in view of Bhatia and RFC 2474; 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 W. McDonald
Jeffrey D. Blake
Kathleen E. Ott
Michael S. Wagner
Christopher C. Davis
MERCHANT & GOULD P.C.
dmcdonald@merchantgould.com
jblake@merchantgould.com
kott@merchantgould.com
mwagner@merchantgould.com
cdavis@merchantgould.com

FOR PATENT OWNER:

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

Bradley C. Wright
BANNER & WITCOFF, LTD.
bwright@bannerwitcoff.com

kis