Trials@uspto.gov
571–272–7822

Paper 11
Entered: January 24, 2022

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

PALO ALTO NETWORKS, INC.,
Petitioner,

v.

CENTRIPETAL NETWORKS, INC.,
Patent Owner.

Case IPR2021-01154
Patent 10,785,266 B2

Before KEVIN F. TURNER, BRYAN F. MOORE, and
LYNNE E. PETTIGREW, *Administrative Patent Judges*.

MOORE, *Administrative Patent Judge*.

DECISION
Denying Institution of *Inter Partes* Review
37 C.F.R. § 42.108

I. INTRODUCTION

Palo Alto Networks, Inc. ("Petitioner") filed a Petition (Paper 2, "Pet.") requesting an *inter partes* review of claims 1–27 of U.S. Patent No. 10,785,266 B2 (Ex. 1001, "the '266 patent"). Centripetal Networks, Inc. ("Patent Owner") filed a Preliminary Response to the Petition. Paper 7 ("Prelim. Resp."). We have jurisdiction under 35 U.S.C. § 314, which provides that an *inter partes* review may not be instituted "unless . . . there is a reasonable likelihood that the petitioner would prevail with respect to at least 1 of the claims challenged in the petition." 35 U.S.C. § 314(a). With our authorization, Petitioner filed a Preliminary Reply (Paper 8, "*Fintiv* Reply") and Patent Owner filed a Preliminary Sur-reply (Paper 9, "*Fintiv* Sur-Reply") to address Board discretion under 35 U.S.C. § 314(a).

For the reasons explained below, we do not institute an *inter partes* review in this proceeding.

A. *Real Parties in Interest*

Petitioner identifies itself as the sole real party-in-interest. Pet. 3. Patent Owner identifies itself as the sole real party-in-interest. Paper 4, 1 (Patent Owner's Mandatory Notices).

B. *Related Proceedings*

The parties indicate that the '266 patent is the subject of the following co-pending district court case: *Centripetal Networks, Inc. v. Palo Alto Networks, Inc.*, Case No. 2:21-cv-00137-RCY-RJK (E.D. Virginia). Pet. 3; Paper 4, 1. The Petition is related to the co-pending petition for *inter partes* review in IPR2021-01153, challenging U.S. Patent No. 10,567,437 B2.

C. *The '266 Patent*

The '266 patent discloses methods and systems for protecting a

secured network. Ex. 1001, code (57). 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 4:59–5:10, 5:14–18, Fig. 1. "At each of the packet security gateways, a dynamic security policy may be received from the security policy management server, packets associated with a network protected by the packet security gateway may be received, and at least one of multiple packet transformation functions specified by the dynamic security policy may be performed on the packets." *Id.* at 3:60–4:1. "Performing the at least one of multiple packet transformation functions specified by the dynamic security policy on the packets may include performing at least one packet transformation function other than forwarding or dropping the packets." *Id.* at 2:1–6.

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 4:59–5:11, 6:24–28, 7:23–26.

> 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, 7:26–32, Fig. 3.

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 8:23–44.

D. *Illustrative Claim*

Of the challenged claims 1, 8, 15, and 21 are independent. Claim 1 is illustrative and is reproduced below.

> 1. A method of filtering packets at a packet security gateway, of a plurality of packet security gateways that collectively provide an entire interface across a boundary of a network protected by the packet security gateway and one or more networks other than the network protected by the packet security gateway, the method comprising:
>
> receiving, by the packet security gateway and from a security policy management server external from the network protected by the packet security gateway, a dynamic security policy comprising a first set of packet filtering rules to be applied to all network traffic traversing the boundary, wherein
>
> each packet filtering rule of the first set of packet filtering rules comprises at least one packet matching criterion and a corresponding packet transformation function, and
>
> one or more first packet filtering rules of the first set of packet filtering rules comprise packet matching criteria corresponding to one or more network addresses and were automatically created or altered by the security policy management server based on aggregated malicious traffic information received from at least one third party malicious host tracker service located in the one or more networks other than the network protected by the packet security gateway, that comprises network addresses that have been determined, by the at least one third party malicious host tracker service, to be associated with malicious network traffic;
>
> performing, on a packet by packet basis, packet filtering on a first portion of packets corresponding to network traffic traversing the boundary via the packet security gateway based on the first set of packet filtering rules by performing at least one packet transformation function specified by at least one packet

> filtering rule of the first set of packet filtering rules on the first portion of packets;
>
> receiving, by the packet security gateway and after performing packet filtering on the first portion of the packets, an updated second set of packet filtering rules for the dynamic security policy from the security policy management server, wherein the updated second set of packet filtering rules comprises an update to the one or more first packet filtering rules created or altered by the security policy management server based on updated malicious traffic information received from the at least one third party malicious host tracker service; and
>
> performing, on a packet by packet basis, packet filtering on a second portion of the packets corresponding to network traffic traversing the boundary via the packet security gateway based on the updated second set of packet filtering rules by performing at least one packet transformation function specified by at least one packet filtering rule of the second set of packet filtering rules on the second portion of packets.

Ex. 1001, 20:64–21:52.

E. *Evidence of Record*

Petitioner cites the following references in its challenges to patentability:

Reference	Designation	Exhibit No.
U.S. Patent Appl. Publ. No. 2007/0262741 A1	Jungck	Ex. 1051
U.S. Patent Appl. Publ. No. 2007/0097976 A1	Wood	Ex. 1052
U.S. Patent Appl. Publ. No. 2009/0249482 A1	Sarathy	Ex. 1063

Pet. 5–6.

Petitioner also relies on the Declaration of Dr. Vijay Madisetti (Ex. 1004, the "Declaration").

F. *Asserted Grounds of Unpatentability*

Petitioner asserts the following grounds of unpatentability (Pet. 6):

Challenged Claims	Basis	References
1–27	§ 103[1]	Jungck, Wood
1–27	§ 103	Jungck, Sarathy, Wood

II. ANALYSIS

A. Level of Ordinary Skill in the Art

Noting that relevant experience and education can substitute for each other, Petitioner states that a person of ordinary skill in the relevant art on October 22, 2012 (the filing date of the application that matured in the '266 patent), would have had a bachelor's degree in computer science, computer engineering, or an equivalent, four years of professional experience, and a working knowledge of packet-switched networking, firewalls, security policies, communication protocols and layers, and the use of customized rules to address cyber-attack. Pet. 18 (citing Ex. 1004 [Declaration of Dr. Vijay Madisetti] ¶¶ 34–36). Petitioner's definition of a person of ordinary skill, which Patent Owner does not dispute at this stage, appears appropriate for the technology addressed by this proceeding.

[1] The Leahy-Smith America Invents Act ("AIA"), Pub. L. No. 112-29, 125 Stat. 284, 285–88 (2011), revised 35 U.S.C. § 103 effective March 16, 2013. Because the '266 patent has an effective filing date prior to the effective date of the applicable AIA amendment, we refer to the pre-AIA version of § 103.

B. Claim Construction

We construe the challenged claims by applying "the standard used in federal courts, in other words, the claim construction standard that would be used to construe the claim in a civil action under 35 U.S.C. [§] 282(b), which is articulated in *Phillips* [*v. AWH Corp.*, 415 F.3d 1303 (Fed. Cir. 2005) (en banc)]." 37 C.F.R. § 42.100(b) (2020). Under *Phillips*, the words of a claim are generally given their "ordinary and customary meaning," which is the meaning they would have to a person of ordinary skill in the art at the time of the invention, in light of the specification and prosecution history. *See Phillips*, 415 F.3d at 1312–13.

Petitioner asks the Board to adopt constructions from prior IPRs challenging related patents. Pet. 19–20. Petitioner does not explain the necessity of these constructions, nor does Patent Owner dispute them. *Id.*; *see generally* Prelim. Resp. Because we decline to institute on the basis of other claim limitations, we do not adopt Petitioner's proposed constructions.

Patent Owner requests that the preamble of independent claims 1, 8, and 15 be treated as limiting. Prelim. Resp. 16–17. These preambles provide antecedent basis for "packet security gateway," "boundary," "network," and "one or more other networks." *Id.* at 16 (citing Ex. 1001, 20:64–21:2, 22:13–18, 23:35–42). The preambles also recite the "plurality of packet security gateways that collectively provide an entire interface across a boundary of a [protected] network," which is "essential to understand" the "all traffic" limitation in the body of these claims and thus '"give life, meaning, and vitality"' to the claims. *Id.* (citing *Catalina Mktg. Int'l, Inc. v. Coolsavings.com, Inc.*, 289 F.3d 801, 808 (Fed. Cir. 2002) (citation omitted)).

The preambles provide the context for the body of the independent claims by defining the arrangement of the "plurality of packet security gateways" relative to the "boundary" of the protected network and thus the basis for applying "packet filtering rules . . . to all network traffic traversing the boundary." *Id.* (citing Ex. 1001, 20:64–21:8). The "entire interface" limitation also was relied on during prosecution of the parent '437 Patent's claims to distinguish them from the prior art. *Id.* at 16–17 (citing Ex. 2008, 254–61; *Catalina*, 289 F.3d at 808–09). Petitioner does not dispute the preambles are limiting. Pet. 18–21, 37. For, the reasons above, we construe the preambles of independent claims 1, 8, and 15 as limiting.

After review of the current record, we conclude that, other than determining the preambles are limiting, no express claim construction is necessary to determine whether to institute review of the challenged claims. *See, e.g.*, *Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co.*, 868 F.3d 1013, 1017 (Fed. Cir. 2017) (quoting *Vivid Techs., Inc. v. Am. Sci. & Eng'g, Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999)) ("[W]e need only construe terms 'that are in controversy, and only to the extent necessary to resolve the controversy.'").

C. Principles of Law

A patent claim is unpatentable under 35 U.S.C. § 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 ordinary skill in the art; and (4) objective evidence of nonobviousness. *Graham v. John Deere Co.*, 383 U.S. 1, 17–18 (1966).

In that regard, an obviousness analysis "need not seek out precise teachings directed to the specific subject matter of the challenged claim, for a court can take account of the inferences and creative steps that a person of ordinary skill in the art would employ." *KSR*, 550 U.S. at 418; *see also In re Translogic Tech., Inc.*, 504 F.3d 1249, 1259, 1262 (Fed. Cir. 2007) (quoting *KSR*, 550 U.S. at 418).

The level of ordinary skill in the art may be reflected by the prior art of record. *See Okajima v. Bourdeau*, 261 F.3d 1350, 1355 (Fed. Cir. 2001); *In re GPAC Inc.*, 57 F.3d 1573, 1579 (Fed. Cir. 1995); *In re Oelrich*, 579 F.2d 86, 91 (CCPA 1978).

D. Obviousness of Claims over Jungck and Wood

Petitioner asserts that claims 1–27 are unpatentable under 35 U.S.C. § 103(a) as obvious over Jungck and Wood. Pet. 6. To support its contentions, Petitioner provides explanations as to how the prior art allegedly teaches each claim limitation. *Id.* at 21–65. For convenience, all references cited in the grounds of the Petition are summarized below.

1. Jungck (Ex. 1051)

Jungck discloses 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. Ex. 1051, code (57). Jungck states that "[t]he apparatus is capable of analyzing any portion of the packet including the header and the

payload," and that the actions "include releasing the packet, logging/storing information about the packet or forwarding the packet to an external device for subsequent processing." *Id.* Jungck's rules may be "dynamically modified" by the external devices. *Id.*

2. Wood (Ex. 1052)

Wood is directed to improved network security by "provid[ing] real-time detection and diagnostic information" on suspect or malicious traffic associated with possible network threats. Ex. 1052 ¶ 6, code (57). Wood teaches a router and an interrogation module that detects and redirects traffic associated with one or more suspect network addresses. *Id.* ¶ 7.

Wood discloses an adaptive interrogation module 204 that is located within a protected subnetwork 202, or remotely connected; and a router 212 that is configured to redirect suspect traffic to the adaptive interrogation module for analysis. *Id.* ¶¶ 32, 40. The adaptive interrogation module 204 receives suspect addresses 206 (e.g., a suspect address list that includes "IP addresses of known threats") from one or more suspect address sources 210 that are external to the protected network. *Id.* ¶¶ 29, 32–33. Using the suspect addresses 206, the adaptive interrogation module 204 configures or reconfigures a router 212 to redirect potentially malicious traffic associated with the suspect addresses, for example, to a null address to effectively block the traffic. *Id.* ¶¶ 21, 32, 34.

Wood discloses updating the suspect addresses 206 "as any one of the suspect address sources 210 receives a change to its suspect address data (e.g., a new IP address block is legitimately allocated . . . or a new hacker site is identified)." *Id.* ¶¶ 34–36.

3. Sarathy (Ex. 1063)

Sarathy (Ex. 1063) teaches a threat management facility (purple) having "policy management facility 112 . . . to update the policies of all corporate computing assets," including access permissions, of an enterprise network 102. Ex. 1063 ¶¶ 34, 37–38, 45. Access permissions are stored as block lists, black lists, allowed lists, or white lists. *Id.* ¶ 45, Fig 1. Threat management facility, including policy management facility, is "integrated into a third-party product," where the enterprise "subscribe[s] to services through the third-party product, and threat protection to the enterprise may be provided by the threat management facility 100 through the third-party product." *Id.* ¶ 38.

4. Claim 1

> *"A method of filtering packets at a packet security gateway, of a plurality of packet security gateways that collectively provide an entire interface across a boundary of a network protected by the packet security gateway . . . comprising: a first set of packet filtering rules to be applied to all network traffic traversing the boundary. . ."*

a. Petitioner's Contentions

Petitioner relies only on Jungck for this limitation. Pet. 37–46. Petitioner relies on Jungck's disclosure of ingress filtering at plurality of edge servers 602A, 602B (packet security gateways) to provide the claimed "an entire interface across a boundary of a network protected by the packet security gateway" (hereinafter, the "entire boundary" limitation). *Id.* at 37–38. For example, Petitioner contends Jungck discloses "intercept[ing] all network traffic flowing between the POP's 114, 116 and the network 100" and "isolating the core infrastructure and servers of the network/internet

from the edge where the clients are located" across a boundary (e.g., POPs 114, 116) of a network protected by the packet security gateway (e.g., "network 100," which is a "private network") and one or more networks other than the network protected by the packet security gateway (e.g., "client 102," which is a "private network . . . coupled with the network 100"). *Id.* (citing Ex. 1051 ¶¶ 31, 38, 39, 41, 107, 113, 116, Figs 1, 6).

Petitioner also relies on Jungck's rule set 726 to show a first set of packet filtering rules. *Id.* at 41–42. Petitioner contends edge server 602 is provided with "one or more rules 732 which are applied" to "all network traffic," thus meeting the limitation of "all network traffic traversing the boundary" (hereinafter the "all traffic" limitation). *Id.* at 41–42 (citing Ex. 1051 ¶¶ 107, 111). As such, Petitioner contends Jungck discloses edge servers that "intercept all network traffic" and monitor it for "malicious program code" using rules. *Id.* at 42 (citing Ex. 1051 ¶¶ 107, 111). Petitioner also contends device 900 performs "ingress and egress filtering" on packets entering (*i.e.*, ingress) and leaving (*i.e.*, egress) the protected network. *Id.* at 43–44 (citing Ex. 1051 ¶ 269). Petitioner also contends collateral estoppel applies based on determinations made in IPR2018-01443, 1444, 1513 (the "'1443 IPR," "'1444 IPR," and '1513 IPR," respectively). *Id.* at 39, 42.

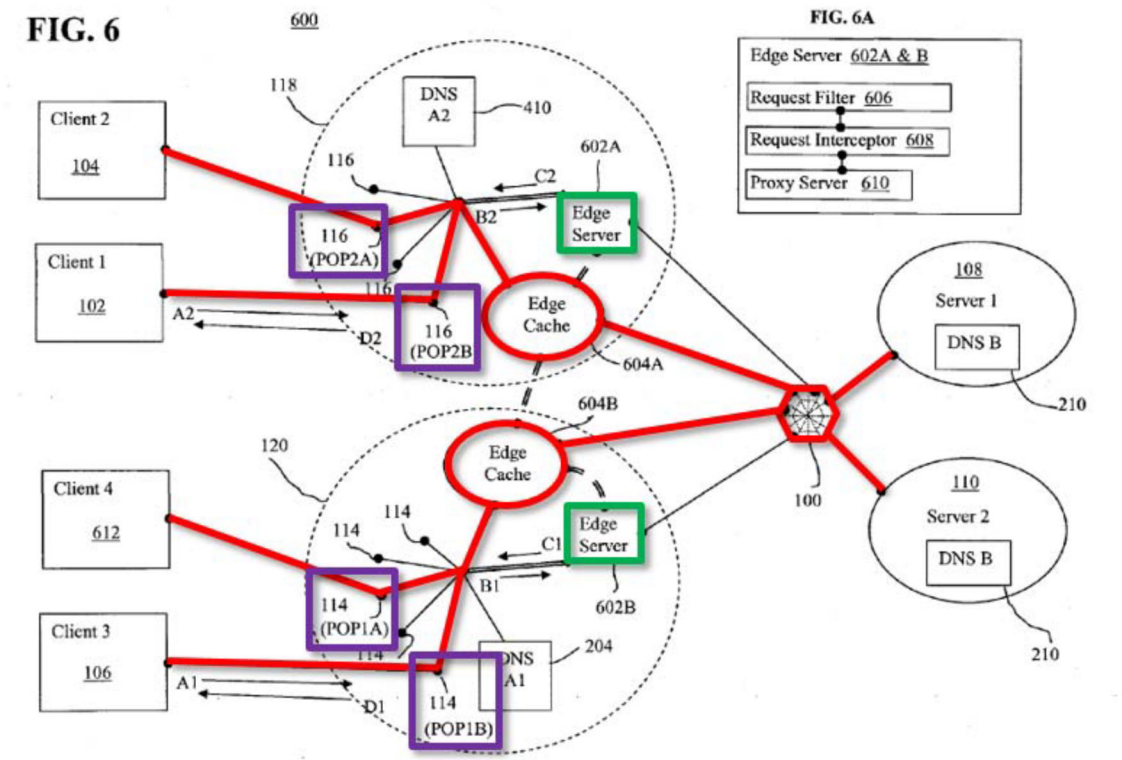
b. Patent Owner's Arguments

i. Petitioner Disregards "Edge Caches"

Patent Owner argues that "Petitioner's obviousness grounds disregard the role of *Jungck's* edge caches, which are located in network paths that

bypass the edge servers entirely." Prelim. Resp. 33.[2] We agree. In fact, Petitioner avoids reciting the words "edge cache" anywhere in the Petition. *See generally* Pet. Additionally, although Petitioner's declarant uses quotes from Jungck that recite the "edge cache," the Petition removes those references. *Compare* Ex. 1004 ¶ 221 *with* Pet. 41; *see also* Prelim. Resp. 33–34 (listing citations in the Petition that omit the term edge cache).

Patent Owner argues Jungck teaches network paths that bypass its edge servers when carrying network traffic through the POPs as shown in the annotated version of Figure 6 of Jungck. Ex. 1051, Fig. 6.



[2] We do not address Patent Owner's argument that "*Jungck* fails to disclose 'packet filtering rules to be applied to all network traffic traversing the boundary' because the client requests disclosed in *Jungck* never traverse the boundary at all." Prelim Resp. 39–40.

Patent Owner's annotated Figure 6 above, shows network paths (**red**) exist between Jungck's clients 102–106 and 612, POPs 114 and 116 (**purple**), routing equipment (206 in Figure. 5), edge caches 604A–B, network 100, and servers 108, 110—all of which Patent Owner argues bypass Jungck's edge servers (**green**). Prelim. Resp. 35 (citing Ex. 1051 ¶ 107 ("edge cache 604A, 604B coupled with the routing equipment 206"), Fig. 6). Thus, according to Patent Owner, Petitioner fails to show "an entire interface across a boundary of a network," because "*Jungck* describes network paths across the alleged 'boundary' that bypass *Jungck's* edge servers, demonstrating that the edge servers do not form the 'entire interface' across the alleged boundary." Prelim. Resp. 34. We find that Petitioner does not adequately explain the working of that boundary because it chooses not to explain or discount the contribution of the edge caches. Additionally, to the extent that this is explained in any related IPRs, Petitioner does not cite to any such explanation.

As to whether Petitioner has shown that Jungck teaches the limitation of "all network traffic traversing the boundary," Patent Owner asserts that there are pathways for content that do not include the edge server. Prelim. Resp. 34, 41. For example, Patent Owner asserts Jungck's edge servers redirect clients to request content from the edge caches or send content request packets to the edge caches for handling. *Id.* at 34, 41 (citing Ex. 1051 ¶¶ 69, 74, 95 ("[T]his effectively redirects the client 102, 104 to make all of its content requests from the edge cache" . . . "edge cache . . . attempt[s] to satisfy content requests from its cache storage"), 109 ("requests will be redirected and served from the edge cache 604"), 113).

Patent Owner also argues that "after a client request[s] content from server 108, the edge server translates server 108's domain name into the IP address of the edge cache so that the client communicates directly with the edge cache instead of either the edge server or server 108." *Id.* at 36 (citing Ex. 1051 ¶¶ 95, 111); *see Fintiv* Sur-Reply 9.[3] In sum, Patent Owner asserts "[t]here are many circumstances in which traffic bypasses the edge servers via the edge caches." Prelim. Resp. 35–36.

We agree with Patent Owner that the Petition's avoidance of the operation of edge caches when edge caches are important in the processing of traffic flowing across the boundary undermines this ground of the Petition. If Petitioner wished to rely on an embodiment or configuration in which the edge caches were irrelevant, the edge caches were redundant to the edge server, or the edge caches were unnecessary, it was incumbent upon Petitioner to explain sufficiently how and why that was the case. Petitioner was aware of the edge caches because it appears to have omitted all references to them in the Petition yet did not explain why this was done.

Additionally, although Petitioner's declarant does include references to edge caches, its declarant also does not explain sufficiently the relevance of those edge caches. Ex. 1004 ¶¶ 148, 212, 214, 215, 227, 323. Additionally, Petitioner's references to collateral estoppel do not relieve Petitioner from the burden to describe its contentions regarding obviousness in the Petition.

---

[3] Patent Owner also relies on Jungck's treatment of a cache miss. Because Patent Owner's other evidence is sufficient we do not rely on Patent Owner's arguments regarding a cache miss. *See* Prelim. Resp. 42.

ii. Petitioner's Reliance on Device 900 is Insufficient

Patent Owner also argues Petitioner's apparent alternative reliance on the fifth embodiment of Jungck is insufficient to cure the deficiencies of its other contentions as to the "all traffic" limitation. Prelim. Resp. 43. For example, as explained above, Petitioner's analysis of the "all traffic" limitation also mentions "ingress and egress filtering" and the use of "blocklists" by Jungck's fifth embodiment.[4] Pet. at 43–44 (citing Ex. 1051 ¶ 269). Specifically, Petitioner's complete contention is that:

> **Jungck** discloses device 900, coupled to network 100 (*e.g.*, upstream network 100A and downstream network 100B), which includes primary processing elements 904A and 904B that "may be consolidated into a single processing element." Jungck, [0266], [0268]. Elements 904A/904B perform "ingress and egress filtering" on packets entering (*i.e.*, ingress) and leaving (*i.e.*, egress) the protected network. Jungck, [0269]. Device 900 maintains "block lists" that include a range of network addresses of upstream and downstream network devices. Jungck, [0269]. The network addresses of incoming packets are compared to the "block lists" and filtered out of the packet stream if they are "out of range." Jungck, [0269]. A POSITA would have understood that all packets entering or leaving the protected network would be compared against the blocklists (or another rule) to "ensur[e] that packets arriving from a particular portion of the network actually came from that portion of the network," or at minimum would have found that to have been obvious, because applying filtering rules to all packets entering and leaving a network was well-known, and a POSITA would have been motivated to apply filtering rules to all such packets to prevent malicious intrusions into the network, and to block devices inside the network from accessing known malicious sites or devices outside of the network. Jungck, [0269]; Madisetti, ¶¶238-241.

[4] We note that Petitioner does not cite to the fifth embodiment to meet the "entire boundary" limitation. *See* Pet. 37–41.

Id.

Patent Owner argues the discussion quoted above regarding device 900 is untethered to the claim language and only describes filtering packets within network 100, and not traversing any network boundary. Prelim. Resp. 43 (citing Ex. 1051 ¶¶ 108, 112, 269, Fig. 9). Patent Owner also argues that paragraph 269 from Jungck, cited by Petitioner, merely discusses filtering packets by a single device ("device 900") that "intercept[s] and process[es]" all packets that the device happens to receive, not "all packets entering and leaving" Jungck's network as a whole. *Id.* at 43 (citing Ex. 1051 ¶¶ 266, 268). We agree with both arguments.[5] The discussion of device 900 above is not tied to the rules and filtering done by the edge servers on which Petitioner relies.

iii. Petitioner's Reliance on "All Traffic" Being "Well Known" is Insufficient

We find Petitioner's discussion of device 900 quoted above appears to be presented as support for the proposition that "applying filtering rules to all packets entering and leaving a network" was "well-known." Pet. 44 (citing Ex. 1051 ¶ 269). In further support of that proposition, Petitioner states also that "POSITA would have been motivated to apply filtering rules to all such packets to prevent malicious intrusions into the network, and to block devices inside the network from accessing known malicious sites or devices outside of the network." *Id.* We are not persuaded by this contention.

[5] We find not that Petitioner fails to provide a rationale to combine or motivation to combine, but rather that Petitioner fails to explain sufficiently how device 900 relates to the specific limitations of the claims.

Whether or not this was known as a general proposition does not address reasons why Jungck's traffic appears to bypass the edge servers upon which Petitioner relies and why a person of ordinary skill would have modified Jungck's operation to apply its rules to all traffic or why a person of ordinary skill would have modified Jungck's operation to use device 900 instead of the edge servers and what effect that would have on the rest of the operation of Jungck. Also, Petitioner does not rely on device 900 to meet the "entire boundary" limitation. *See* Pet. 37–41.

Petitioner also appears to rely on its declarant who testifies it was well-known to block all incoming traffic. *Fintiv* Reply (citing Ex. 1004 [Declaration of Dr. Vijay Madisetti] ¶¶ 72–73). Nevertheless, this section of the Declaration was not cited in the Petition but rather is referred to indirectly in a portion of the Declaration which *is* cited in the Petition. Pet. 44 (citing Ex. 1004 ¶ 241). Paragraph 241 of the Declaration states "*as discussed in Section IV*, applying filtering rules to all packets entering and leaving a network was well-known," but does not refer to paragraphs 72 and 73. As the Court of Appeals for the Seventh Circuit has explained, "[a] brief must make all arguments accessible to the judges, rather than ask them to play archaeologist with the record." *DeSilva v. DiLeonardi*, 181 F.3d 865, 867 (7th Cir. 1999); *see also United States v. Dunkel*, 927 F.2d 955, 956 (7th Cir. 1991) ("Judges are not like pigs, hunting for truffles buried in briefs.").

Additionally, paragraph 72 of the Declaration contains new argument regarding "firewall" and "standard networking practice" based on references (Bharali and Wood) not cited for that proposition in the Petition. Ex. 1004 ¶ 72. We find the Petition improperly incorporates this section of the Declaration by reference because the basis of the "firewall" argument is not

explained sufficiently in the Petition. *Cisco Systems, Inc., v. C-Cation Technologies, LLC*, IPR2014-00454, Paper 12 at 8 (PTAB Aug. 29, 2014) (informative opinion) (describing the proper course of action as "to not consider arguments that are not made in the Petition, but are instead incorporated by reference").

iv. Collateral Estoppel Does Not Apply

1. Collateral Estoppel in the Petition

Petitioner also suggests in conclusory fashion that collateral estoppel may apply to its contentions as to the "entire boundary" limitation (Pet. 38 ("***Collateral estoppel applies.*** 1513 FWD, *19-33, *43, *45-47; 1443 FWD, *49-50, *52-54.")) and the "all traffic" limitation" (Pet. 41 ("***Collateral estoppel applies.*** 1443 FWD, *13-18, *42, *49-50, *52-54; 1444 FWD, *13-19, *42.")).

Our reviewing court has held that "[c]ollateral estoppel protects a party from having to litigate issues that have been fully and fairly tried in a previous action and adversely resolved against a party-opponent." *Nestle USA, Inc. v. Steuben Foods, Inc.*, 884 F.3d 1350, 1351–1352 (Fed. Cir. 2018) (quoting *Ohio Willow Wood Co. v. Alps S., LLC*, 735 F.3d 1333, 1342 (Fed. Cir. 2013)). "It is well established that collateral estoppel, also known as issue preclusion, applies in the administrative context." *MaxLinear, Inc. v. CF CRESPE LLC*, 880 F.3d 1373, 1376 (Fed. Cir. 2018) (citations omitted); *Webpower, Inc. v. WAG ACQUISITION, LLC*, Case IPR2016-01239, Paper 21 at 26–28 (PTAB Dec. 26, 2017).

"Issue preclusion [i.e., collateral estoppel] is appropriate only if: (1) the issue is identical to one decided in the first action; (2) the issue was actually litigated in the first action; (3) resolution of the issue was essential

to a final judgment in the first action; and (4) plaintiff had a full and fair opportunity to litigate the issue in the first action." *In re Freeman*, 30 F.3d 1459, 1465 (Fed. Cir. 1994); *see also MaxLinear, Inc.*, 880 F.3d at 1377 (citing *Blonder-Tongue Labs., Inc. v. Univ. of Illinois Found.*, 402 U.S. 313, 91 S. Ct. 1501, 28 L.Ed. 2d 788 (1971) (finding collateral estoppel applies to a patentee who had a full and fair opportunity to litigate the validity of a patent in a prior federal case.)).

Patent Owner points out that the claims at issue in IPR2018-01443, 1444, 1513 ("prior IPRs") did not include the "entire boundary" or "all traffic" limitations. Prelim. Resp. 26–27, 32, 44. We agree. Collateral estoppel does not apply because there are differences between the claim limitation at issue here and the adjudicated claim limitations at issue in the prior IPRs. *See In re Freeman*, 30 F.3d at 1465; *accord MaxLinear, Inc.*, 880 F.3d at 1377–1378; *cf. In re Arunachalam*, 709 F. App'x 699, 702 (Fed. Cir. 2017) (unpublished) (finding collateral estoppel applies to an adjudicated claim that is not "materially different" than the adjudicated claims).

To the extent that Petitioner has some theory why a prior proceeding regarding a different patent with different claim limitations would be considered a proper basis for collateral estoppel, Petitioner should have explained that theory in its Petition – a mere string citation is insufficient. *See, e.g.*, *Trading Techs. Int'l, Inc. v. IBG LLC*, 921 F.3d 1378, 1385 (Fed. Cir. 2019) (holding that a conclusory assertion with no analysis was not adequately developed); *Novartis AG v. Torrent Pharms.*, 853 F.3d 1316, 1326 n.2 (Fed. Cir. 2017) (finding that an argument presented in one conclusory sentence and a string cite was "far from sufficient to raise a

meaningful challenge" and "amount[ed] to little more than a request that the Board peruse the cited evidence and piece together a coherent argument on Novartis' behalf").

2. *Collateral Estoppel in the Fintiv Reply*

In its Reply to Patent Owner's arguments regarding discretionary denial under § 314(a), Petitioner responds to Patent Owner's argument that the Petition fails to show that Jungck meets the "entire boundary" and "all traffic" limitations. *Fintiv* Reply 8–9.[6] As an initial matter, we note that our authorization of a responsive brief regarding *Fintiv* is not an invitation to respond to all issues on the merits raised in a Patent Owner preliminary response. Also, Petitioner's *Fintiv* Reply does not relieve it of the burden of explaining sufficiently its contentions, including contentions based on collateral estoppel, in its Petition. "In an IPR, the petitioner has the burden from the onset to show with particularity why the patent it challenges is unpatentable." *Harmonic Inc. v. Avid Tech., Inc.*, 815 F.3d 1356, 1363 (Fed. Cir. 2016).

Nevertheless, we address Petitioner's *Fintiv* Reply arguments here. Petitioner asserts "as the Board previously found, Jungck 'broadly teach[es] *protecting entire networks*' such that the 'edge servers located at the POPs

[6] Petitioner argues that Patent Owner "incorrectly suggest[s] that an edge cache necessarily bypasses the edge server 'in the event that there is a cache miss." *Fintiv* Reply. 8–9 (citing Prelim. Resp. 34 (citing Ex. 1051, 96, 112)). Patent Owner does not rely solely on the cache miss but, as explained above, relies on Figure 6 and other disclosures including Ex. 1051 ¶ 95 to show that the edge caches bypass the edge servers. We do not rely on Patent Owner's cache miss argument, but rather we rely on the other arguments cited above. Petitioner does not address Figure 6, Ex. 1051 ¶ 95, or the other arguments Patent Owner makes.

are . . . capable of 'intercept[ing] *all network traffic*,'" citing the Final Written Decision in the '1513 IPR ("'1513 FWD"). *Fintiv* Reply 8 *(*citing Ex. 1012, 24, 29). Thus, according to Petitioner, "Jungck teaches providing 'an entire interface' that protects entire networks by filtering 'all network traffic.'" *Id.* We examine the '1513 FWD's discussion of the "entire network" and "all traffic" limitations, respectively, below.

We begin with the limitation of "an entire interface across a boundary of a network protected by the packet security gateway." In the '1513 IPR, Patent Owner argued "Jungck only protects 'subscribing servers,' i.e., servers that pay a fee for protection, and not other, non-subscribing servers on the network." Ex. 1012 ['1513 FWD], 23. The Board found, however, "Patent Owner does not sufficiently explain how the claim language and intrinsic record support its view that protecting only subscribing servers in a network is excluded from the scope of claim 1 . . . Petitioner need only show that Jungck *teaches or suggests* a network protected by a plurality of devices." *Id.* at 23–24. Only after making this determination does the Board suggest that "omitting restrictions based on subscriptions is simpler and advantageously protects the entire network." *Id.* at 24.

Thus, although the Board referenced the term "entire network," it was not necessary for the ultimate finding of non-obviousness because the Board had already declined to adopt Patent Owner's claim construction. *In re Freeman*, 30 F.3d at 1465 (collateral estoppel applies to issues the "resolution of [which] was essential to a final judgment in the first action"). For that reason, collateral estoppel does not apply and the statement relied on by the Petition was arguably dicta. Additionally, the pages cited by

Petitioner do not address the relationship between edge servers and edge cache which is at issue in this IPR.

In the '1513 FWD, the Board also stated the edge servers located at the POPs are described as capable of "intercept[ing] all network traffic flowing between the POPs 114, 116 and the network 100." Ex. 1012 ['1513 FWD], 29 (citing IPR2018-01513, Ex. 1008 ¶ 107 [Jungck]). As an initial matter, the text portion of Jungck cited and relied on in the '1513 FWD actually states "service providers 118, 120 each include an edge server 602A, 602B ***and an edge cache 604A, 604B*** coupled with the routing equipment 206 of the service providers 118, 120 so as to be able to intercept all network traffic" and, thus, the '1513 IPR does not address the issue in this case regarding the distinction between the operation of the edge server and edge cache. Ex. 1051 ¶ 107 (emphasis added).

Additionally, because the issue in the '1513 FWD was simply whether the claimed boundary existed in Jungck between the protected network and one or more other networks, so the Board did not need to determine whether all traffic goes through the edge servers to reach a decision on obviousness. Ex. 1012 ['1513 FWD], 29; *In re Freeman*, 30 F.3d at 1465 (collateral estoppel applies to issues the "resolution of [which] was essential to a final judgment in the first action"). For that reason, collateral estoppel does not apply and the reference to "all network traffic" was arguably dicta.

In its *Fintiv* Reply, Petitioner also asserts "PO does not even address the evidence that it was well-known to filter both inbound and outbound traffic." *Fintiv* Reply 9 (citing Pet. 43–44; Ex. 1004 ¶¶ 72–73, 238–241). As noted above, Patent Owner does respond to the "well-known" argument and we are persuaded by Patent Owner's response. Petitioner also cites to

portions of the Declaration (Ex. 1004 ¶¶ 72–73) to support the "well-known" argument. *Id.* However, as explained above, those paragraphs of the Declaration are not cited or explained in the Petition. *Id.*

c. Summary of Claim 1

In sum, Petitioner does not explain how the edge cache devices contribute or detract from Jungck's ability to teach or suggest the "entire boundary" and "all traffic" limitations of the challenged claims. The evidence of device 900 and claims of collateral estoppel do not remedy this deficiency. In the absence of such evidence, Petitioner has failed to "identif[y], in writing and with particularity, . . . the evidence that supports the grounds for the challenge." *See Intelligent Bio-Sys., Inc. v. Illumina Cambridge Ltd.*, 821 F.3d 1359, 1369 ("It is of the utmost importance that petitioners in the IPR proceedings adhere to the requirement that the initial petition identify 'with particularity' the 'evidence that supports the grounds for the challenge to each claim.'") (quoting 35 U.S.C. § 312(a)(3)); 37 C.F.R. § 42.104(b). For the reasons above, Petitioner has not shown sufficiently that the combination of Jungck and Wood meets the limitation of "[a] method of filtering packets at a packet security gateway, of a plurality of packet security gateways that collectively provide an entire interface across a boundary of a network protected by the packet security gateway . . . comprising: a first set of packet filtering rules to be applied to all network traffic traversing the boundary."

d. Independent Claims 8, 15, and 21 and Dependent Claims 2–7, 9–14, 16–20, 22–27

Petitioner asserts that Jungck and Wood teach the limitations of independent claims 8, 15, and 21 and dependent claims 2–7, 9–14, 16–20, 22–27. These claims also recite the "entire boundary" and "all traffic"

limitations and thus, for the same reasons as above, Petitioner has not demonstrated a reasonable likelihood of success in establishing the unpatentability of any of independent claims 1, 8, 15, and 21, and claims 2–7, 16–20, and 22–27 which depend therefrom, as having been obvious over Jungck and Wood.

E. Obviousness of Claims over Jungck, Sarathy, and Wood

Petitioner asserts that claims 1–27 are unpatentable under 35 U.S.C. § 103(a) as obvious over Jungck, Sarathy, and Wood. Pet. 6. To support its contentions, Petitioner provides explanations as to how the prior art allegedly teaches each claim limitation. *Id.* at 65–68.

Petitioner's contentions that Jungck, Sarathy, and Wood teach the limitations of independent claims 8, 15, and 21 and dependent claims 2–7, 9–14, 16–20, 22–27 do not cure the deficiencies discussed above as to the "entire boundary" and "all traffic" limitations. Thus, for the same reasons as above, Petitioner has not demonstrated a reasonable likelihood of success in establishing the unpatentability of any of independent claims 1, 8, 15, and 21, and claims 2–7, 16–20, and 22–27 which depend therefrom, as having been obvious over Jungck, Sarathy, and Wood.

F. Summary

For the foregoing reasons, we determine that Petitioner has not demonstrated a reasonable likelihood of success in establishing the unpatentability of any of independent claims 1, 8, 15, and 21, and claims 2–7, 16–20, and 22–27 which depend therefrom, on the obviousness grounds asserted in the Petition.

G. *Discretionary Denial Under 35 U.S.C. § 314(a) and/or 325(d)*

Because we deny institution upon consideration of the merits of Petitioner's challenges, we need not address Patent Owner's arguments that we should exercise our discretion under 35 U.S.C. § 314(a) and/or § 325(d) to deny institution.

II. CONCLUSION

Petitioner has not demonstrated a reasonable likelihood of prevailing with respect to any of claims 1–27 of the '266 patent under any of the proffered grounds.

III. ORDER

For the reasons given, it is:

ORDERED that, pursuant to 35 U.S.C. § 314(a), an *inter partes* review is not instituted for claims 1–27 of U.S. Patent No. 10,785,266 B2.

PETITIONER:

Scott A. McKeown
Mark D. Rowland
James R. Batchelder
Andrew Radsch
ROPES & GRAY LLP
scott.mckeown@ropesgray.com
mark.rowland@ropesgray.com
james.batchelder@ropesgray.com
andrew.radsch@ropesgray.com

PATENT OWNER:

James Hannah
Jeffrey H. Price
KRAMER LEVIN NAFTALIS & FRANKEL, LLP
jhannah@kramerlevin.com
Jprice@kramerlevin.com

Bradley C. Wright
Scott M. Kelly
Blair A. Silver
BANNER & WITCOFF, LTD.
bwright@bannerwitcoff.com
skelly@bannerwitcoff.com
bsilver@bannerwitcoff.com