

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

PALO ALTO NETWORKS, INC.,
Petitioner,

v.

CENTRIPETAL NETWORKS, INC.,
Patent Owner.

IPR2022-00182
Patent 9,917,856 B2

Before BRIAN J. McNAMARA, AARON W. MOORE, and
STEVEN M. AMUNDSON, *Administrative Patent Judges*.

AMUNDSON, *Administrative Patent Judge*.

DECISION

Denying Patent Owner's Request for Rehearing of
Decision Granting Institution of *Inter Partes* Review
37 C.F.R. § 42.71(d)

I. INTRODUCTION

Palo Alto Networks, Inc. (“Petitioner”) filed a Petition requesting an *inter partes* review of claims 1, 24, and 25 in U.S. Patent No. 9,917,856 B2 (Exhibit 1001, “the ’856 patent”) under 35 U.S.C. §§ 311–319. Paper 2 (“Pet.”). Centripetal Networks, Inc. (“Patent Owner”) filed a Preliminary Response. Paper 6 (“Prelim. Resp.”). Further, after receiving Board authorization, Petitioner filed a Preliminary Reply, and Patent Owner filed a Preliminary Sur-reply. Paper 9 (“Prelim. Reply”); Paper 10 (“Prelim. Sur-reply”).

After considering the submissions by the parties and the evidence of record, the Board determined that Petitioner demonstrated a reasonable likelihood of prevailing in proving claims 1, 24, and 25 unpatentable under § 103, and in May 2022, the Board instituted an *inter partes* review based on the following challenges to patentability:

Claim(s) Challenged	35 U.S.C. §	Reference(s)/Basis
1, 24, 25	103	Buruganahalli ¹
1, 24, 25	103	Buruganahalli, Baehr ²

Paper 11 (“Institution Decision” or “Inst. Dec.”) at 2, 12, 79–80, 89–91.

In June 2022, Patent Owner requested rehearing of the Institution Decision, arguing that the Board misapprehended or overlooked various matters. Paper 13 (“Req. Reh’g”) at 2–3, 10–15. In its rehearing request,

¹ U.S. Patent No. 9,680,795 B2 to Buruganahalli et al. (“Buruganahalli”), titled “Destination Domain Extraction for Secure Protocols,” and included in the record as Exhibit 1004.

² U.S. Patent No. 5,878,231 to Baehr et al. (“Baehr”), titled “System for Packet Filtering of Data Packets at a Computer Network Interface,” and included in the record as Exhibit 1005.

Patent Owner requested that the Precedential Opinion Panel (“POP”) review the Institution Decision and address the following question:

Should the Board entertain IPR petitions that collaterally attack a district court judgment when the totality of the circumstances indicates that the petition was filed to harass the patent owner?

Id. at 1; *see* Ex. 3005.

In December 2022, the POP denied the request for POP review. Paper 31, 2. The POP stated that “the original panel maintains authority over all matters, including considering the submitted rehearing request.” *Id.*

We have considered Patent Owner’s rehearing request. For the reasons explained below, the request lacks merit. Hence, we deny the request.

II. STANDARD OF REVIEW

“The burden of showing a decision should be modified lies with the party challenging the decision.” 37 C.F.R. § 42.71(d) (2022). In a rehearing request, the party challenging the decision “must specifically identify” (1) “all matters the party believes the Board misapprehended or overlooked” and (2) “the place where each matter was previously addressed” in an earlier submission. *Id.*; *see* Consolidated Trial Practice Guide at 90.³

“A rehearing request is not an opportunity for the requesting party to reargue its case or merely to express disagreement with the underlying decision.” *MicroSurgical Tech., Inc. v. Regents of Univ. of Colo.*, PGR2021-00026, Paper 14 at 2 (PTAB Aug. 12, 2021). “Nor is it an opportunity for the moving party to present new arguments that were not in its original submissions.” *Id.*

³ Available at <https://www.uspto.gov/TrialPracticeGuideConsolidated>.

“When rehearing a decision on petition, a panel will review the decision for an abuse of discretion.” 37 C.F.R. § 42.71(c). “An abuse of discretion occurs if a decision is based on an erroneous interpretation of law, if a factual finding is not supported by substantial evidence, or if the decision represents an unreasonable judgment in weighing relevant factors.” *Arnold P’ship v. Dudas*, 362 F.3d 1338, 1340 (Fed. Cir. 2004).

III. ANALYSIS

Patent Owner asserts that in the Institution Decision the Board:

- (A) misapprehended “what Buruganahalli’s system does when it encounters” a whitelisted packet and a blacklisted packet;
- (B) overlooked an “inconsistency” in the Board’s analyses for limitations [1.a] and [1.g]; and
- (C) “failed to give appropriate weight to the district court’s determination” about copying when considering the objective indicia of nonobviousness.

See Req. Reh’g 2–3, 10–15, 11 n.1.

A. The Board Did Not Misapprehend How Buruganahalli’s Security Devices Process Packets

As discussed above, Patent Owner asserts that the Board misapprehended “what Buruganahalli’s system does when it encounters” a whitelisted packet and a blacklisted packet. Req. Reh’g 10–11, 11 n.1 (citing Prelim. Resp. 16–18). In particular, Patent Owner contends that when Buruganahalli’s system “encounters a whitelisted packet,” the system “forwards the entire encrypted stream without decrypting or filtering encrypted packets.” *Id.* at 10 (emphasis omitted). Patent Owner also contends that when Buruganahalli’s system “encounters a blacklisted packet,” the system “either blocks the session before any encrypted packets

are received or decrypts the packets prior to filtering the packets using firewall policies/rules.” *Id.* at 10–11 (emphasis omitted). According to Patent Owner, “communications sessions are either allowed uninspected, terminated before a session is established, or (if the domain name is on the blacklist) decrypted prior to filtering.” *Id.* at 11 n.1.

Further, Patent Owner asserts that in Buruganahalli’s Figure 3A embodiment:

- (1) “encrypted packets in whitelisted sessions are forwarded without applying any packet-filtering rules”; and
- (2) “blacklisted sessions are blocked before any encrypted packets are received in the first place.”

Req. Reh’g 13 (emphasis omitted) (citing Prelim. Resp. 16–17).

Based on the current record and for the reasons discussed in the Institution Decision, we disagree with Patent Owner’s assertions about how Buruganahalli’s security devices process packets. *See, e.g.*, Inst. Dec. 57–60, 66–67, 69–71; Req. Reh’g 10–11, 13.

Buruganahalli explains that a security device may monitor network traffic by “inspecting individual packets,” for example “using pass through (e.g., in line) monitoring techniques.” Ex. 1004, 3:16–18, 9:6–15, Fig. 1; *see id.* at 3:20–21, 3:40–44, 9:25–28, 9:32–36, 14:22–28; Ex. 1003 ¶ 130. The security device may apply “a policy (e.g., a security policy) based on the destination domain” to filter inbound traffic or outbound traffic (or both). Ex. 1004, 1:33–38, 2:62–3:4, 7:25–29, code (57); *see id.* at 5:35–51, 7:8–9, 7:35–42, 7:51–67, 14:28–33, 14:61–63; Ex. 1003 ¶ 108. The security device may apply one or more of the following policies:

- (1) “a malware detection policy”; and
- (2) “a whitelist/blacklist policy”; and

- (3) “a uniform resource locator (URL)/category filtering policy.”

Ex. 1004, 7:42–51, 16:26–48; *see id.* at 7:52–67, 10:21–28; Ex. 1003 ¶¶ 90, 109.

Buruganahalli discloses that when a client attempts to access a remote server “using an encrypted session protocol,” the security device intercepts “the initial unencrypted/clear text data communications,” e.g., a TLS hello message, “exchanged as part of an initial handshake to setup a secure connection for a new session.” Ex. 1004, 4:37–40, 5:27–42, 14:21–25, 15:7–11, Figs. 6–7; *see id.* at 4:59–61, 6:39–41, 7:19–25, 11:7–12, 11:24–51, code (57); Ex. 1003 ¶¶ 103, 111–113. The security device processes the unencrypted data communications to “extract a hostname” that identifies the destination domain the client wants to connect with. Ex. 1004, 5:6–10, 9:50–57, 11:7–12, 11:47–51, 14:21–25, 14:28–31, 14:50–55, 15:11–18, code (57), Fig. 7; *see* Ex. 1003 ¶¶ 91, 111–112. For instance, the security device may analyze “an initial TLS handshake exchange” to “extract a hostname to facilitate destination domain extraction for secure protocols.” Ex. 1004, 11:47–51, 14:28–31, 14:50–55, 15:13–18; *see id.* at 5:6–10, 11:24–47; Ex. 1003 ¶ 111.

Based on the extracted hostname (destination domain), the security device “identifies the packets as being part of a new session and creates a new session flow.” Ex. 1004, 5:7, 5:35–36, 14:25–33; *see* Ex. 1003 ¶¶ 111, 115, 133. The security device uses the extracted hostname (destination domain) to “apply firewall policies or take responsive actions.” Ex. 1004, 5:35–42; *see id.* at 11:12–19; Ex. 1003 ¶ 108. For instance, the security device may use the extracted hostname (destination domain) to implement

a whitelist/blacklist policy where blacklisted items correspond to network-threat indicators. Ex. 1004, 7:39–67, 16:32–48; *see* Ex. 1003 ¶¶ 61–62, 90–91, 105, 109, 116, 120, 124, 128, 132. The security device may apply one or more policies “prior to and/or without having to decrypt the encrypted secure tunnel session traffic.” Ex. 1004, 11:12–19; *see* Ex. 1003 ¶¶ 94, 113.

As an example, a security policy may specify that “the network communications between the client and the remote server are not decrypted if the destination domain is included in a whitelist of the whitelist/blacklist policy.” Ex. 1004, 7:55–59, 16:36–42; *see id.* at 7:42–50; Ex. 1003 ¶ 90. As another example, a security policy may specify that “the network communications between the client and the remote server are decrypted if the destination domain is included in a blacklist of the whitelist/blacklist policy.” Ex. 1004, 7:63–67, 16:43–48; *see id.* at 7:42–50; Ex. 1003 ¶ 90.

According to Buruganahalli, a security device inspects individual packets, for instance, because the packets “may be received out of order.” Ex. 1004, 3:16–18, 14:50–51; *see* Ex. 1003 ¶¶ 94, 130. So, a security device implementing a whitelist/blacklist policy may:

- (1) inspect a hello message for a first session, extract a hostname corresponding to a whitelisted destination domain, and create a first session flow; and
- (2) later inspect a hello message for a second session, extract a hostname corresponding to a blacklisted destination domain, and create a second session flow (or not create the second session flow).

See Ex. 1004, 7:43–50, 14:21–26, 16:33–48; *see* Ex. 1003 ¶¶ 90, 109. When the security device subsequently receives a packet with encrypted data, the security device will inspect the packet and determine whether the packet is

correlated to (1) the hostname corresponding to the whitelisted destination domain or (2) the hostname corresponding to the blacklisted destination domain. *See* Ex. 1004, 7:39–67, 14:26–28, 14:38–40, 14:50–57, 16:36–48; Ex. 1003 ¶¶ 64, 90, 94, 109.

Regarding the policy’s whitelist processing, if the security device determines that a newly received packet with encrypted data is correlated to the hostname corresponding to the whitelisted destination domain, the security device filters the packet by forwarding it to the remote server with the whitelisted destination domain. *See* Ex. 1004, 7:52–59, 16:36–42; Ex. 1003 ¶ 90; *see also* Ex. 1004, 6:1–11. Filtering the newly received packet with encrypted data by forwarding it to the remote server with the whitelisted destination domain occurs “without having to decrypt the encrypted secure tunnel session traffic.” Ex. 1004, 5:24–27, 5:35–42, 7:1–9, 11:7–19; *see* Ex. 1003 ¶¶ 94, 113. Further, filtering the newly received packet with encrypted data by forwarding it to the remote server with the whitelisted destination domain results from applying a packet-filtering rule (a whitelisted destination domain) to the packet.

Hence, we disagree with Patent Owner that Buruganahalli’s security devices process whitelisted packets by “forward[ing] the entire encrypted stream without . . . filtering encrypted packets.” *See* Req. Reh’g 10. We also disagree with Patent Owner that “encrypted packets in whitelisted sessions” are (1) “forwarded without applying any packet-filtering rules” and (2) “allowed uninspected.” *See id.* at 11 n.1, 13.

Regarding the policy’s blacklist processing, if the security device determines that a newly received packet with encrypted data is correlated to the hostname corresponding to the blacklisted destination domain, the

security device either blocks the packet (as Patent Owner contends) or filters the packet by forwarding it to a decryption engine. *See* Ex. 1004, 7:60–67, 9:61–67, 14:33–36, 16:43–48; Ex. 1003 ¶¶ 90–91, 94, 97, 108, 118, 127, 137; Req. Reh’g 10–11, 13. Filtering the newly received packet with encrypted data by forwarding it to a decryption engine occurs “without having to decrypt the encrypted secure tunnel session traffic.” Ex. 1004, 5:24–27, 5:35–42, 7:1–9, 11:7–19; *see* Ex. 1003 ¶¶ 94, 113, 135. Further, filtering the newly received packet with encrypted data by forwarding it to a decryption engine results from applying a packet-filtering rule (a blacklisted destination domain) to the packet and corresponds to limitation [1.g] and the similar limitations in claims 24 and 25. *See* Ex. 1003 ¶¶ 109, 134–135.

The Institution Decision explained how Buruganahalli’s security devices may filter packets comprising unencrypted data and packets comprising encrypted data according to claims 1, 24, and 25 by applying a whitelist/blacklist policy to the packets. *See, e.g.*, Inst. Dec. 57–60, 66–67, 69–71. As the Institution Decision explained and as discussed above, “for each session packets comprising unencrypted data and packets comprising encrypted data are correlated and filtered based on the hostname (destination domain) extracted from the handshake traffic, and then the correlated and filtered packets are processed separately from packets destined for other domains.” *See* Inst. Dec. 69–70; Ex. 1003 ¶¶ 109, 120–121, 133–135; Ex. 1004, 7:39–67, 8:55–60, 11:47–51, 14:21–33, 14:50–55, 16:32–48.

Buruganahalli discloses additional filtering after forwarding a newly received packet with encrypted data to a decryption engine, *e.g.*, as occurs in Buruganahalli’s Figure 3B embodiment. *See, e.g.*, Ex. 1004, 6:17–22, 9:67–10:4, 12:4–64, Fig. 3B. But claims 1, 24, and 25 use the transitional

term “comprising.” Ex. 1001, 25:14, 28:59, 29:29–30. Hence, the claims do not “exclude unrecited elements,” such as additional filtering after forwarding a newly received packet with encrypted data to a decryption engine. *See Regeneron Pharm., Inc. v. Merus N.V.*, 864 F.3d 1343, 1352 (Fed. Cir. 2017) (citing Manual of Patent Examining Procedure § 2111.03).

*B. The Board Did Not Overlook an “Inconsistency”
in the Board’s Analyses for Limitations [1.a] and [1.g]*

As discussed above, Patent Owner asserts that Board overlooked an “inconsistency” in the Board’s analyses for limitations [1.a] and [1.g]. Req. Reh’g 10; *see id.* at 2, 11, 13–14. In particular, Patent Owner contends that “the ‘firewall rules/policies’ applied to blacklisted packets, which allegedly correspond to the ‘packet-filtering rules’” of limitation [1.a], “are only applied to decrypted or unencrypted packets, but not the encrypted packets recited in” limitation [1.g]. *Id.* at 10 (emphases omitted). Patent Owner contends that Buruganahalli “never applies” any “firewall policies/rules to encrypted packets without decrypting them.” *Id.* at 11; *see id.* at 2. Further, Patent Owner asserts that the Board relied on “firewall policies/rules associated with Buruganahalli’s blacklist processing” for limitation [1.a] but pointed to “irrelevant disclosures that do not use these policies/rules” for limitation [1.g]. *Id.* at 11 (emphases omitted) (citing Inst. Dec. 60, 68, 71).

Contrary to Patent Owner’s assertion, the Institution Decision pointed to “Buruganahalli’s blacklist processing” for limitation [1.g] by quoting Dr. Weissman’s testimony that the “encrypted data communications are filtered after it is determined that information extracted from the handshake traffic matches with those on a blacklist, and thus corresponds to a network-threat indicator.” Inst. Dec. 69 (quoting Ex. 1003 ¶ 135).

Additionally, we disagree with Patent Owner’s contention that Buruganahalli “never applies” any “firewall policies/rules to encrypted packets without decrypting them.” *See* Req. Reh’g 11. As discussed above, Buruganahalli discloses that a security device inspects newly received packets on a packet-by-packet basis and may:

- (1) filter a newly received packet with encrypted data destined for a whitelisted domain by forwarding it to the remote server with the whitelisted domain “without having to decrypt the encrypted secure tunnel session traffic”; and
- (2) filter a newly received packet with encrypted data destined for a blacklisted domain by forwarding it to a decryption engine “without having to decrypt the encrypted secure tunnel session traffic.”

Ex. 1004, 5:24–27, 5:35–42, 7:1–9, 11:7–19; *see* Ex. 1003 ¶¶ 94, 113, 130–135; *supra* § III.A.

*C. The Board Did Not Fail to Give Appropriate Weight
to the District Court’s Determination About Copying*

As discussed above, Patent Owner asserts that Board “failed to give appropriate weight to the district court’s determination” about copying when considering the objective indicia of nonobviousness. Req. Reh’g 3; *see id.* at 14–15.

As background, Patent Owner filed a complaint in 2018 against Cisco Systems, Inc. (“Cisco”) in the Eastern District of Virginia alleging infringement of several patents, including the ’856 patent. Ex. 1027, 1–2; *see* Ex. 1028, 11.⁴ In 2020, the district court conducted a bench trial and

⁴ For Exhibit 1028 (Cisco’s Non-Confidential Opening Brief in the Appeal to the Federal Circuit), we cite to the page numbers appearing in the brief rather than the page numbers that Petitioner applied to the exhibit.

subsequently issued an opinion and order with findings of fact and conclusions of law concerning infringement, validity, and damages. Ex. 1027, 1, 3, 22. Among other things, the court found that various combinations of Cisco's products infringed the asserted claims in four patents, including the '856 patent. *Id.* at 22–23, 29, 41, 57, 78–79, 95, 107, 110, 123, 160, 166.

The district court also found that:

- (1) “Cisco was provided with demonstrations of the product and confidential information regarding” Patent Owner's proprietary algorithms;
- (2) “[w]ithin a year of these meetings, Cisco released the ‘network of the future,’ involving the release of older products embedded with new software functionality that was outlined and detailed to them by disclosure of the patents and multiple technical discussions and demonstrations” by Patent Owner;
- (3) Cisco's release of products with Patent Owner's “functionality within a year of these meetings goes beyond mere coincidence”; and
- (4) Cisco “copied software functionality from the [infringed] patents” and embedded the copied software functionality in “switches, routers and firewalls.”

Ex. 1027, 157, 160. The court determined that “the fact that Cisco's system mirrors the functionality of the [infringed] patents is compelling evidence that damages should be enhanced for copying.” *Id.* at 157.

Cisco appealed to the Federal Circuit. Ex. 1028, 4–5.

The Institution Decision noted that “Patent Owner does not identify information allowing us to evaluate whether copying occurred.” Inst. Dec. 78 (citing Prelim. Resp. 16, 54–56). The Institution Decision accorded

“little weight” to the evidence about copying in the record before the Board.
Id.

Patent Owner asserts that the Board “should have considered the district court’s determination and the underlying evidence of copying.” Req. Reh’g 15. Patent Owner also asserts that the Board “‘ideally should not arrive at a different conclusion’ if it faces the same evidence and argument as a district court.” *Id.* (quoting *In re Baxter Int’l, Inc.*, 678 F.3d 1357, 1365 (Fed. Cir. 2012)).

Patent Owner does not explain why issue preclusion permits the Board to hold the district court’s finding that Cisco “copied software functionality from the [infringed] patents” against Petitioner. *See* Prelim. Resp. 16, 54–56; Req. Reh’g 3, 14–15. Issue preclusion “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) the party defending against preclusion “had a full and fair opportunity to litigate the issue in the first action.”

SynQor, Inc. v. Vicor Corp., 988 F.3d 1341, 1353 (Fed. Cir. 2021). Patent Owner does not address any of these requirements for issue preclusion. *See* Prelim. Resp. 16, 54–56; Req. Reh’g 3, 14–15.

As for Patent Owner’s assertion that the Board “‘ideally should not arrive at a different conclusion’ if it faces the same evidence and argument as a district court,” the Board does not have the same evidence about copying as the district court. *See Cisco Sys., Inc. v. Centripetal Networks, Inc.*, IPR2022-01151, Paper 2 at 73 (PTAB June 24, 2022). Patent Owner

did not submit to the Board all of the evidence about copying cited by the district court. *See* Ex. 1027, 149–61 (citing PTX-99, PTX-102, PTX-134, PTX-528, PTX-547, PTX-548, PTX-550, PTX-570, PTX-1046, PTX-1215); Prelim. Resp. vi (Patent Owner’s Exhibit List) (not listing PTX-99, PTX-102, PTX-134, PTX-528, PTX-547, PTX-548, PTX-550, PTX-570, PTX-1046, PTX-1215).

For these reasons, the Institution Decision did not give insufficient weight to the evidence about copying in the record before the Board.

Additionally, the Federal Circuit in June 2022 vacated the district court’s opinion and order concerning infringement, validity, and damages. Ex. 1050, 2–3, 26–27. The Federal Circuit determined that the district judge “was disqualified from hearing the case once he became aware of his wife’s ownership of Cisco stock.” *Id.* at 2. The Federal Circuit remanded the case for reassignment to a new district judge and directed the new district judge to “decide the case without regard for” the vacated opinion and order. *Id.* at 2–3, 26–27. Thus, there is no “final judgment in the first action” to provide a foundation for issue preclusion.

IV. CONCLUSION

For the reasons discussed above, Patent Owner has not demonstrated that the Board abused its discretion when instituting an *inter partes* review of claims 1, 24, and 25 in the ’856 patent.

V. ORDER

Accordingly, it is

ORDERED that Patent Owner’s Request for Rehearing is denied.

IPR2022-00182
Patent 9,917,856 B2

For PETITIONER:

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

For PATENT OWNER:

James Hannah
Jeffrey H. Price
Jenna Fuller
KRAMER LEVIN NAFTALIS & FRANKEL LLP
jhannah@kramerlevin.com
jprice@kramerlevin.com
jfuller@kramerlevin.com
svdocketing@kramerlevin.com

Bradley C. Wright
Scott M. Kelly
John R. Hutchins
BANNER & WITCOFF, LTD.
bwright@bannerwitcoff.com
skelly@bannerwitcoff.com
jhutchins@bannerwitcoff.com