

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 IPR2022-00182
U.S. Patent No. 9,917,856

PATENT OWNER'S SUR-REPLY

TABLE OF CONTENTS

I.	BACKGROUND	1
II.	BURUGANAHALLI DOES NOT TEACH FILTERING ENCRYPTED PACKETS BASED ON THE CLAIMED PACKET- FILTERING RULES	4
A.	Buruganahalli’s Flow Lookup Is Based on IP Address and Port Number, Not the Claimed Packet-Filtering Rules	5
B.	Buruganahalli’s Technique is Not the Same as the Claimed Embodiment	8
C.	There is No Intermediate Step of Rule-Based Filtering of Encrypted Packets Between Buruganahalli’s Filtering of Unencrypted Packets and Filtering of Decrypted Data.....	9
D.	Buruganahalli’s Figures 3A and 3B Embodiments, Even Taken Together, Never Perform the Claimed Rule-Based Filtering of Encrypted Packets	12
III.	PETITIONER HAS NOT SHOWN THAT BURUGANAHALLI TEACHES THE CLAIMED “NETWORK-THREAT INDICATORS”	16
IV.	THE PRIOR ART DOES NOT TEACH THE CLAIMED ROUTING FILTERED PACKETS TO A PROXY SYSTEM.....	20
A.	Buruganahalli Does Not Disclose the Claimed Routing Filtered Packets to a Proxy System	21
B.	The Petition Provides No Rational Motivation for Why a Skilled Artisan Would Have Modified Buruganahalli in View of Baehr	22
V.	OBJECTIVE EVIDENCE OF NONOBVIOUSNESS ALSO DEMONSTRATES THAT THE CLAIMS ARE VALID	24
VI.	CONCLUSION.....	26

TABLE OF AUTHORITIES

	Page(s)
Cases	
<i>ActiveVideo Networks v. Verizon Commc'ns, Inc.</i> , 694 F.3d 1312 (Fed. Cir. 2012)	16
<i>Fox Factory, Inc. v. SRAM, LLC</i> , 944 F.3d 1366 (Fed. Cir. 2019)	25
<i>Graham v. John Deere Co. of Kan. City</i> , 383 U.S. 1 (1966).....	24
<i>Intelligent Bio-Sys., Inc. v. Illumina Cambridge, Ltd.</i> , 821 F.3d 1359 (Fed. Cir. 2016)	20
<i>KSR Int'l Co. v. Teleflex Inc.</i> , 550 U.S. 398 (2007).....	22, 23
<i>Lectrosonics, Inc. v. Zaxcom, Inc.</i> , No. IPR2018-01129, Paper 33 (P.T.A.B. Jan. 24, 2020)	24
<i>Ortho-McNeil Pharm., Inc. v. Mylan Lab'ys, Inc.</i> , 520 F.3d 1358 (Fed. Cir. 2008)	22
<i>In re Translogic Tech., Inc.</i> , 504 F.3d 1249 (Fed. Cir. 2007)	22
Other Authorities	
37 C.F.R. 42.23(b)	20

I. BACKGROUND

The '856 Patent solved the “unsolvable” problem of detecting cyber-attacks hidden within encrypted packets without decryption. Ex. 2013 at 1; *see* Paper 24 (“POR”) at 3, 4, 14-15. Earlier approaches, like those applied by the old Stealthwatch system considered in the Cisco litigation, required decrypting encrypted traffic to detect policy violations. Buruganahalli is no different. In order to determine whether encrypted packets violate Buruganahalli’s security policy, such packets must be decrypted because the firewall cannot otherwise “detect such firewall policy/rule violation(s).” Ex. 1004 (“Buruganahalli”) at 11:2-6. It is, therefore, no surprise that the Petition relied on Buruganahalli’s disclosures concerning filtering decrypted packets, not encrypted packets. Pet. at 38 (citing Buruganahalli at 4:16-22 (explaining that decryption is “needed” to monitor encrypted data communications and to apply filtering based on a policy)). The Challenged Claims are patentable, therefore, because Buruganahalli does not teach or suggest filtering encrypted packets with the rules specified in each of the Challenged Claims. POR at 4-7, 31-44.

Rather than deny institution on the basis that Buruganahalli does not disclose applying the claimed packet-filtering rules to encrypted packets, the panel instituted trial citing aspects of Buruganahalli’s “flow lookup” and a combination of Buruganahalli’s FIG. 3A and 3B embodiments, despite neither theory being raised

in the Petition.¹ See Paper 11 (“DI”) at 69-71. As Buruganahalli teaches, and Petitioner and its expert acknowledge, however, Buruganahalli’s “flow lookup” process only checks the IP address and port number for incoming encrypted packets rather than any of the criteria recited in the Challenged Claims. Buruganahalli at 9:25-32, 14:25-28; Pet. at 32; Ex. 2027 (“Weissman Tr.”) at 35:4-25. Petitioner also does not dispute that Buruganahalli’s FIG. 3A embodiment teaches either allowing a session with no further filtering of encrypted packets (whitelist processing) or blocking a nascent encrypted session (blacklist processing) before any encrypted packets are received, identified, determined, or filtered, as recited in the Challenged Claims. POR at 37-40.

Instead of rebutting Centripetal’s arguments or disputing Buruganahalli’s operation, Petitioner proceeds in an altogether different direction—now asserting that Buruganahalli’s process of “routing for decryption” satisfies the requirement that encrypted packets be filtered according to the packet-filtering rules recited in the Challenged Claims. See Paper 29 (“Reply”) at 2 (citing Buruganahalli at 9:61-

¹ Centripetal’s Request for Rehearing of the Institution Decision, which brought this issue to the panel’s attention, has been pending without a decision on the merits for nearly seven months. See Paper 13.

65).² The fatal flaw in Petitioner's new challenge is, once again, that Buruganahalli does not filter encrypted packets based on the claimed packet-filtering rules. In the ten pages of the Petitioner's Reply devoted to this issue, Petitioner argues that Buruganahalli's technique involves filtering encrypted packets "based on a firewall policy." Reply at 3; *see also id.* at 9. But the claims do not recite filtering packets "based on a firewall policy," they require filtering encrypted packets based on the specific rules recited in the Challenged Claims, and Buruganahalli is explicit that these types of rules are applied to decrypted packets because packets must be decrypted "to monitor the session traffic for firewall policy/rule compliance." Buruganahalli at 12:42-44, 12:29-32; Ex. 1003, ¶ 92.

Petitioner also fails to show that Buruganahalli teaches the claimed "network-threat indicators." POR at 49-51. Petitioner did not even apply its own unsubstantiated claim construction (from a different IPR case, involving an unrelated patent, considered under the broadest reasonable interpretation standard). Nor did Petitioner consider the district court's claim construction of the term in litigation involving the '856 Patent itself. Nor did Petitioner explain how or why a POSITA would have considered Buruganahalli's blacklisted domains as being

² This portion of Buruganahalli was not cited with respect to filtering encrypted packets in the Petition. *See* Pet. at 38-39.

associated with a network threat. The attorney argument in Petitioner's Reply neither rebuts Dr. Goodrich's testimony on this issue nor establishes that a POSITA would have understood blacklisted domains to be associated with a network threat.

With respect to Buruganahalli's failure to teach the claimed "routing" step, Petitioner relies on hand-waving and hindsight to fill Buruganahalli's considerable gaps. Petitioner's defense of its Ground 2 is similarly misguided because Petitioner cannot explain why a POSITA would have modified Buruganahalli's decryption process, which is required to carry out its firewall policy, at a proxy system, particularly given that that technique would hinder rather than help the application of the firewall's policies, as Dr. Goodrich's unrebutted testimony established.

Finally, Petitioner's Reply shirks its burden to address known objective evidence of nonobviousness. The Challenged Claims are patentable.

II. BURUGANAHALLI DOES NOT TEACH FILTERING ENCRYPTED PACKETS BASED ON THE CLAIMED PACKET-FILTERING RULES

Buruganahalli does not teach filtering encrypted packets based on the particular packet-filtering rules required by the claims. Petitioner confirms that the only place that encrypted packets are allegedly "filtered" in Buruganahalli is in its initial flow processing step before encrypted packets are decrypted. Reply at 1-3, 5. However, the only possible "rules" applied at this step check the packet's IP address and port number, which are not among the criteria (*e.g.*, "URI", "protocol version",

“method”, “request”, “command”) specified in the packet-filtering rules.³ See POR at 31-33.

A. Buruganahalli's Flow Lookup Is Based on IP Address and Port Number, Not the Claimed Packet-Filtering Rules

The Petition asserted that Buruganahalli's application of policies to decrypted data meets the claimed rule-based filtering of encrypted packets. Pet. at 38. Petitioner denies that it made this argument (Reply at 6-7), yet the Petition's first citation to Buruganahalli for limitation [1.g] (Pet. at 38) states “techniques for decrypting such secure communications are needed in order to monitor such encrypted data communications and to apply filtering based on a policy.” Buruganahalli at 4:16-22. Likewise, the Petition's second citation describes that monitoring encrypted communications involves determining that encrypted packets are part of a particular flow and then decrypting those encrypted packets for “further potential filtering based on the policy.” *Id.* at 6:12-39. Thus, after flow processing (which only checks a packet's IP address and port number) encrypted packets are decrypted before any relevant packet filtering rules might be applied. Paper 6 (“POPR”) at 46-52; POR at 33-44. Each of the other citations in this section of the

³ Those criteria from the rules are: “at least one of a uniform resource identifier (URI)”; “data indicating a protocol version”; “data indicating a method specified”; “data indicating a request”; or “data indicating a command.” '856 Patent, Claim 1.

Petition follow this format. Pet. at 38 (citing Buruganahalli at 4:31-44, 6:62-7:9, 7:12-29, 7:39-51, 7:60-67, 15:4-21).

In tacit recognition of the Petition's flaws, Petitioner now points to steps that occur **before** decryption as allegedly satisfying this claim element. Reply at 2-14. Specifically, Petitioner argues the claimed rule-based filtering of encrypted packets is met by Buruganahalli's (i) initial filtering of unencrypted packets during handshaking and (ii) later performance of flow lookup to decide to route associated encrypted packets to the decrypt engine.⁴ Reply at 2-5; *id.* at 3 (arguing "encrypted packets are filtered based on the earlier handshake processing of unencrypted data");

⁴ Petitioner's Reply contradicts itself by later arguing "the act of looking up a flow is not relied on for the filtering step—the flow lookup allows the security device to associate encrypted packets with unencrypted packets (e.g., from the session initiating handshake), so that the firewall policy (e.g., blacklist or whitelist) can be applied to the received encrypted packets." Reply at 10. But Petitioner identifies no other "filtering" steps between flow processing and decryption that could possibly satisfy this element. *Id.* Indeed, there are none. Buruganahalli at 12:29-32 ("After the session set-up handshaking is completed... any data that is communicated from the client 312 to the firewall 314 is decrypted... and is then inspected by the firewall").

id. at 3 (“it is the filtering of encrypted packets that separates those packets to be sent for decryption from those packets simply passed through without decryption”); *id.* at 5 (“The decision to pass, block, or route for decryption an encrypted packet is a filtering step performed on that packet.”); *id.* at 7-9 (relying on filtering during handshaking). This new attempted mapping is inconsistent with the Petition and the Challenged Claims.

Petitioner's new mapping dooms its challenge of the '856 Patent. The uncontested evidence shows Buruganahalli's initial handling of encrypted packets is based on matching IP address and port number in a flow analysis table. This fails to satisfy the challenged claims that require filtering of encrypted packets based on specific criteria (*e.g.*, “URI,” “protocol version,” “method,” “request,” “command”) that must be in the packet-filtering rules. *See* POR at 31-33, 8-10.

Petitioner's own expert explained during cross-examination that Buruganahalli builds and uses a table for checking the IP address and port number of encrypted packets. Weissman Tr. at 28:18-35:25; *id.* at 35:4-11 (“When an encrypted packet is received, then this table will be consulted.”). Petitioner's expert then admitted that “[Buruganahalli] runs a rule” that “uses the IP address and port” to “check whether there's a correlation from this packet.” *Id.* at 35:14-25; *see also* POR at 31-33. Petitioner fails to address this cross-examination testimony in its Reply. Nor did Petitioner submit a Reply Declaration to try to explain away their

expert's admission. To the extent that Petitioner now argues that filtering encrypted packets based on *any* criteria (rather than the specific criteria in packet-filtering rules recited in the claims) is sufficient to satisfy the Challenged Claims, the Board should reject such an attempt to rewrite the claim limitations to suit Petitioner's challenge.

Petitioner has not identified a single instance where Buruganahalli teaches or suggests filtering encrypted packets based on the claimed packet-filtering rules. POR at 40-44. To the contrary, Buruganahalli is explicit that encrypted packets must be decrypted in order to perform filtering based on the type of criteria recited in the Challenged Claims. Buruganahalli at 8:11-24.

B. Buruganahalli's Technique is Not the Same as the Claimed Embodiment

The difference between the Challenged Claims and Buruganahalli—filtering encrypted packets based on specific, recited criteria in packet-filtering rules—is not a pedantic difference. It represents a distinct technological advantage of the '856 Patent over the state of the art at the time the invention was made, and improves cyberthreat analysis. POR at 14-15, 22-23; Ex. 2026 ("Goodrich Decl."), ¶¶ 55-56. As just one example, the '856 Patent's approach permits a firewall to end a secure session that is later deemed to be a threat via an updated packet-filtering rule. *Id.*; '856 Patent at 14:19-16:26 (describing use of reconfigured rules), 22:20-51 (same). This is because a firewall continues to apply the packet-filtering rules with the specific claimed criteria to filter encrypted packets rather than merely use IP address

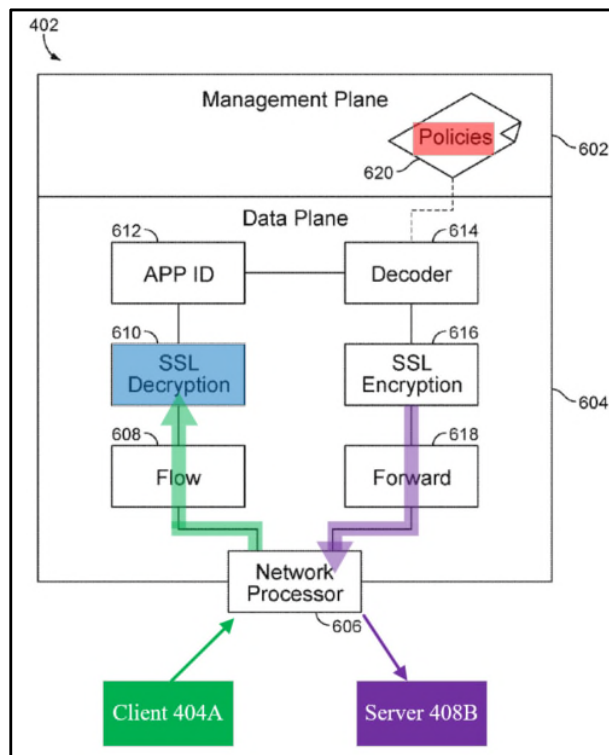
and port to associate packets in flow analysis, as described in Buruganahalli. Goodrich Decl., ¶¶ 55-56. The POR describes several other advantages of the claimed approach, none of which Petitioner attempts to rebut in its Reply. POR at 14-23.

Petitioner ignores these disclosures and advantages, not to mention the plain language of the claims, when contending that “[t]he ’856 patent filters encrypted packets in the same way as Buruganahalli.” Reply at 5 (citing ’856 Patent at 9:19-33 and claims 18 and 20). The cited disclosure is irrelevant to the issue raised in the POR, however, because it relates to the separately claimed “determining...packets comprising encrypted data that corresponds to the one or more network-threat indicators” element, not the claimed rule-based filtering of encrypted packets. *See, e.g.,* ’856 Patent, Claim 1. Petitioner’s failure to understand (or mischaracterization of) the claimed embodiment undermines its argument.

C. There is No Intermediate Step of Rule-Based Filtering of Encrypted Packets Between Buruganahalli’s Filtering of Unencrypted Packets and Filtering of Decrypted Data

Understanding that both the Petition grounds and the “trial grounds” are meritless, Petitioner suggests that there is some *other* filtering step in between Buruganahalli’s flow processing and decryption. Reply at 10 (citing Buruganahalli at 14:25-28) . No such step exists. *See* Buruganahalli at 12:29-32 (“After the session set-up handshaking is completed for each of Session A and Session B, any data that

is communicated from the client 312 to the firewall 314 is decrypted using a session key S1 and is then inspected by the firewall 314.”) Indeed, the unexplained citation accompanying Petitioner’s assertion explicitly states that when “using one or more policies based on the extracted domain[], *SSL decryption is applied by SSL decryption engine.*” Buruganahalli at 14:34-36 (emphasis added). This process is illustrated in FIG. 6, reproduced below:



Buruganahalli, Fig. 6 (annotated)

Id. at 14:8-15:3, Fig. 6. If Buruganahalli’s firewall determines, based on unencrypted handshake traffic, to further monitor a session, then it performs flow lookup, decrypts the encrypted packets, and then applies policies 620. *Id.*; POR at 33-34.

Petitioner further misunderstands (or mischaracterizes) Buruganahalli's passage at 9:61-67. *See* Reply at 9. Buruganahalli refers to filtering *unencrypted* packets to determine whether to employ the man-in-the-middle configuration of Figure 3B. Buruganahalli at 9:61-67, 11:59-12:61. When Figure 3B is employed, subsequently received encrypted packets are subject to flow lookup and then decrypted before any policy rules are applied to the decrypted data. POR at 7-10, 33-35. Indeed, the Board correctly agreed that Figure 3B does *not* teach the rule-based filtering of encrypted packets. DI at 70; POR at 35-37.

Petitioner argues: "The Board also recognized that Buruganahalli describes a process for filtering both the handshake traffic **and** the encrypted packets of the session." Reply at 9 (emphasis in original). But, the Institution Decision's preliminary finding was based on an incorrect understanding of Buruganahalli's "without having to decrypt" language (Buruganahalli at 11:7-19). POR at 37-40. That language only reflects that encrypted packets are prevented from being received by filtering *unencrypted* handshake messages. *Id.* Notably, Petitioner makes no attempt to rebut this and never directly (only indirectly via citations to the Institution Decision) relies on that portion of Buruganahalli for teaching rule-based filtering of encrypted packets. Reply at 9.

Centripetal has also never "concede[d] that policies are applied to encrypted traffic in Buruganahalli." Reply at 9. Centripetal's statements that "a policy may

cause the firewall to initially allow a session/flow” and “‘policies/rules’ may be applied ‘*prior to and/or without having to decrypt*’” explain how Buruganahalli filters *unencrypted* handshake traffic to block a secure session from being established so that no encrypted packets are even received, let alone filtered according to the claimed packet-filtering rules. POR at 38, 41. Petitioner does not dispute that Buruganahalli teaches this scenario. Nor does Petitioner dispute that none of the three scenarios disclosed in Buruganahalli involve rule-based filtering of encrypted packets. See POR at 5-8.

D. Buruganahalli’s Figures 3A and 3B Embodiments, Even Taken Together, Never Perform the Claimed Rule-Based Filtering of Encrypted Packets

Buruganahalli’s Figures 3A and 3B embodiments, even taken together, never perform the claimed rule-based filtering of encrypted packets. POR at 5-8, 42-44. Buruganahalli’s Figure 3A embodiment either blocks unencrypted handshake packets (blacklist processing) or passes encrypted packets without any filtering (whitelist processing). *Id.* Buruganahalli then switches from the FIG. 3A embodiment to the FIG. 3B embodiment when it determines, based on filtering unencrypted handshake traffic, that man-in-the-middle techniques should be applied to decrypt encrypted packets before applying policies. POR at 42. These two embodiments work together seamlessly and do not suggest the conclusion that the Board reached in its Institution Decision, namely that an unarticulated combination

of Figs. 3A and 3B results in applying filtering rules recited in limitation [1.g] to encrypted packets “without ‘having to decrypt’” the encrypted communications. DI at 71. Petitioner does not dispute any of these facts in its Reply or attempt to support the conclusion that the panel reached. *See* Reply at 11-12.

Instead, Petitioner attempts to twist the Board's *sua sponte* combination, which it describes as the “trial grounds” to differentiate them from grounds raised in the Petition, to support its new unpatentability theory. Reply at 11. Specifically, Petitioner suggests that the panel “rel[ied] on the disclosure of Figure 3A for applying a policy to extract a destination domain in an unencrypted hello message that is used to filter the associated encrypted traffic by comparing the domain to a blacklist, and on the disclosure of Figure 3B for routing filtered encrypted traffic to a proxy (*i.e.*, a decrypt engine).” *Id.* The problems with this statement are manifold.

First, the Board's *sua sponte* combination of Figs. 3A and 3B is entirely different than the combination that Petitioner describes in the Reply. The Board relied on the Fig. 3A embodiment, along with a statement that the two embodiments may be used “separately or together,” to conclude that the firewall rules/policies applied in Fig. 3B can be applied to encrypted packets “without ‘having to decrypt’ encrypted communications.” DI at 71. Petitioner's assertion that the Board's discussion of Fig. 3B in this context actually referred to routing packets to a proxy baldly misstates the record. Reply at 11.

Second, the record shows that the panel's combination, developed on the limited pre-institution record, read Buruganahalli's statement about applying policies without having to decrypt encrypted communications out of context. POR at 37-39. In fact, Petitioner does not dispute either how the FIG. 3A embodiment is capable of applying firewall policies without having to decrypt encrypted communications, *i.e.*, by either allowing the session without any further filtering (whitelist processing) or blocking the session before any encrypted packets are ever received (blacklist processing). *Id.* at 5-7, 37-39. In both of these scenarios, encrypted packets are never decrypted or filtered whatsoever, and Petitioner does not muster any rebuttal to this fact. *Id.*; Reply at 11-12.

Third, Petitioner did not raise this argument in the Petition. In its Reply, Petitioner coyly claims that “*a* combination of Figures 3A and 3B... is explicitly relied on in the Petition.” Reply at 11 (emphasis added) (citing Pet. at 22-23, 40, Ex. 1003 at ¶ 141). Whether or not the panel can suss out “*a* combination of Figures 3A and 3B” in the cited portions of the Petition (Centripetal cannot), it certainly was not the combination described in the Petition. Thus, although the Petition cites text from both embodiments, it never asserts a combination that produces a new step in which the claimed packet-filtering rules are applied to encrypted packets without having to decrypt the encrypted communications. *See* Pet. at 22-23, 40. To the contrary, Buruganahalli is consistently explicit (as the Board recognized in the

Institution Decision) that encrypted packets must be decrypted “to monitor the session traffic for firewall policy/rule compliance.” DI at 755 (citing Buruganahalli at 12:29-32, 12:42-44).

The first cited text (Pet. at 22-23) of the Petition are an overview of Buruganahalli that simply describes Figures 3A and 3B with no hint that Petitioner's obviousness theory relied on a combination of the two embodiments that would result in applying the claimed packet-filtering rules to encrypted packets without having to decrypt them. In fact, the term “without having to decrypt” is not found anywhere in the Petition, let alone in this cited portion. The other citations (Pet. at 40, Ex. 1003 at ¶ 141) are directed to an entirely different limitation (*i.e.*, routing to a proxy system), and are irrelevant to the issue of whether Buruganahalli teaches filtering encrypted packets using the claimed rules with or without having to decrypt the encrypted communications. As described in detail throughout the POR and this paper, it does not.

Further, the Petition provides no description of how or why these two embodiments would be combined to reach the claimed invention, let alone a description of what the combined system would do. *See* Pet. at 22-23, 40. Yet a description of “how any specific combination would operate or read on the asserted claims” and why a POSITA would have combined such elements in the way that the claimed invention does at the time of the invention is the bare minimum required to

show that a patent claim is obvious. *See ActiveVideo Networks v. Verizon Commc'ns, Inc.*, 694 F.3d 1312, 1327-28 (Fed. Cir. 2012).

* * *

Like the old Stealthwatch system asserted against the '856 Patent in the Cisco litigation, Buruganahalli requires that encrypted packets be decrypted “to monitor the session traffic for firewall policy/rule compliance.” Buruganahalli at 12:29-32; Ex. 1027 at 61; POR at 24-25. Buruganahalli does not, therefore, teach or suggest filtering encrypted packets with packet-filtering rules specifying a URI, protocol version, method, request, or a command, as recited in each of the Challenged Claims. The Challenged Claims are patentable.

III. PETITIONER HAS NOT SHOWN THAT BURUGANAHALLI TEACHES THE CLAIMED “NETWORK-THREAT INDICATORS”

The term “network-threat indicator” has already been construed under the *Phillips* standard in the context of the '856 Patent to mean “indicators of packets associated with network threats, such as network addresses, ports, domain names, uniform resource locators (URLs), or the like.” POR at 28 (citing Ex. 1027 at 39). Yet, Petitioner attempts to fault Centripetal for not applying a construction that was arrived at in the context of unrelated patents under the broadest reasonable interpretation (“BRI”) standard. Reply at 14. This remarkable statement appears calculated to distract from the fact that Petitioner did not even apply its own construction of the term in the Petition. *See* Pet. at 29-30.

Ultimately it is immaterial whether the Board adopts the district court's construction or Petitioner's construction because the Petition still failed to show that destination domains on Buruganahalli's blacklist are "network-threat indicators" under any construction of the term. POR at 49-51; Goodrich Decl., ¶¶ 105-09. Buruganahalli never characterizes the blacklist as being associated with "network threats." POR at 49-51; Goodrich Decl., ¶ 106. A POSITA would understand that a blacklist in Buruganahalli is simply a list of domains that a network administrator has identified for monitoring or blocking (for any number of reasons). Goodrich Decl., ¶ 107 (citing Buruganahalli at 5:64-6:38; Ex. 2006 at 1:25-36; Ex. 2007 at ¶ 0007). This testimony stands unrebutted. In Reply, Petitioner belatedly raises new arguments and evidence in an attempt to cure the deficiencies in its Petition. Reply at 14-16.

First, Petitioner changes course from the arguments set out in the Petition, latching onto the term "not trusted" in Buruganahalli to suggest the blacklisted destination domain indicates network threats. Reply at 14 (citing Buruganahalli at 9:67-10:4). Moreover, the full quote from Petitioner's citation describes the blacklist as representing an "extracted destination domain [that] is not trusted ***or unknown.***" Buruganahalli at 9:67-10:4 (emphasis added) The full quote indicates Buruganahalli's blacklist is used to identify all domains that are not fully trusted

(i.e., whitelisted domains), not those that are known to be associated with a network threat.

Second, Petitioner's own evidence discloses that all Internet traffic is untrusted, so this does not mean—or even imply—that all untrusted traffic is associated with a network threat. Ex. 1052 at 21 (“It is now an accepted fact that the Internet is a vast network of untrusted and potentially malicious machines” and “the Internet is considered an untrusted zone”). To the contrary, network-threat indicators do not represent “untrusted and potentially malicious machines.” That’s a description that applies to every Internet connection computer. Even under Petitioner’s construction, network-threat indicators must “represent the identity of a resource associated with a network threat.” Accordingly, Dr. Weissman’s testimony that Buruganahalli’s blacklist represents “things you should be worried about as a *potential* network threat” does not even facially support Petitioner’s argument. See Reply at 15 (citing Weissman Tr. at 59:5-13).

Centripetal already addressed Petitioner’s other argument about the “identification of new, zero-day threats” in the POR. Reply at 15 (citing Buruganahalli at 13:44-51)). In particular, domains associated “new, zero-day threats” cannot possibly be network-threat indicators because they are, by definition, not already known to be associated with a network threat. POR at 51. Instead, Buruganahalli discloses reporting detected security violations detected at the

firewall to a cloud service that “can facilitate identification of new, zero-day threats.” Buruganahalli at 13:44-51. This means that the domain was not associated with a network threat at the time the firewall encountered it and, therefore, that the domain was not associated with a network threat. POR at 51; Goodrich Decl. at ¶¶ 108-109. Accordingly, Petitioner’s reliance on Buruganahalli’s security cloud service undermines its argument. *See* Reply at 16 (citing Pet. at 30; Ex. 1003 at ¶ 109).

Petitioner also argues that the very name “security policy” in Buruganahalli means “a POSITA would have understood... that the blacklist contains a list of destination domains associated with network threats.” Reply at 15-16. The only support Petitioner can muster for this new argument is from its expert’s cross-examination testimony. *Id.* (citing Weissman Tr. at 59:5-13, 59:14-22). But the cited testimony itself is unsupported, conclusory, and in conflict with other testimony, which accurately characterized Buruganahalli’s blacklist as a list of domains that represent ***potential*** threats Weissman Tr. at 60:12-22 (“To me, then, the domain name, URI, is -- Buru is -- the blacklists in question here are potential network threats. Because it's not necessarily blocking every blacklist.”); *id.* at 59:15-22 (acknowledging Buruganahalli does not even use the word threat in its detailed description).

Finally, the Board should disregard Petitioner’s belated introduction of new evidence to support its prima facie case because it should have been submitted with

the Petition. Reply at 16 (citing Ex. 1052). Incredibly, Petitioner did not present this evidence to Dr. Goodrich before or during his deposition so that he could comment on it. *See generally* Ex. 1049. Petitioner's attempt to sandbag this proceeding is not well taken and contrary to law. *See Intelligent Bio-Sys., Inc. v. Illumina Cambridge, Ltd.*, 821 F.3d 1359, 1369-70 (Fed. Cir. 2016); 37 C.F.R. 42.23(b).

In any event, Petitioner's belated evidence does not support its contentions because the "blacklist approach" described in Dr. Goodrich's textbook does not describe a blacklist as representing domains associated with a network threat, as required even under Petitioner's construction of the term. Instead, it describes the "blacklist approach" as a "default-allow ruleset" that allows all packets "except those that fit the rules defined specifically in a blacklist." Ex. 1052 at 22. This description is not even consistent with Buruganahalli's use of the term, which extends to traffic that is initially *allowed*, albeit subject to decryption and further monitoring. Buruganahalli at 7:43-50, 7:60-67. Accordingly, Petitioner's belatedly entered evidence fails to establish Buruganahalli's blacklist meets even its own broad interpretation of the term "network-threat indicator."

IV. THE PRIOR ART DOES NOT TEACH THE CLAIMED ROUTING FILTERED PACKETS TO A PROXY SYSTEM

Each challenged claim recites "[routing/route], by the packet-filtering system, filtered packets to a proxy system based on a determination that the filtered packets

comprise data that corresponds to the one or more network-threat indicators” (the “routing step”). ’856 Patent, Claims 1, 24, 25. Buruganahalli, alone or in combination with Baehr, fails to disclose the routing of filtered packets to a proxy system.

A. Buruganahalli Does Not Disclose the Claimed Routing Filtered Packets to a Proxy System

Under the first ground, Petitioner asserts that the decryption engine within Buruganahalli’s firewall is the claimed “proxy system.” Pet. at 39; Reply at 17-19. But, as discussed above in detail, the “decrypt engine” cannot be said to be routed filtered packets because no filtering of encrypted packets—using the claimed rules—occurs until after the encrypted packets have been decrypted. POR at 52, 33-37; Goodrich Decl., ¶¶ 110-11. Thus, Buruganahalli’s decrypt engine cannot satisfy the claimed proxy system.

Petitioner also chafes at addressing the proper construction of the term “proxy system,” and mislabels “a proxy system which intervenes to prevent threats in communications between devices” as “PO’s narrow construction.” Reply at 18-19. Petitioner forgets that this construction is in fact the district court’s construction from litigation involving the ’856 Patent and can be found in Petitioner’s own exhibits. *See* Ex. 1027 at 39; Ex. 1030 at 33-34, 36. Nevertheless, Petitioner reasserts in its Reply that the decrypt engine, described with respect to Buruganahalli’s Figure 3B and its “man-in-the-middle” techniques, allegedly discloses proxy-like functionality.

Reply at 18-19. However, as explained in the Patent Owner Response, the decrypt engine performs one step in firewall's own filtering process without "interven[ing] to prevent threats in communications between devices." POR at 53-54 (citing Buruganahalli at 14:21-60; Goodrich Decl., ¶¶ 114-15).

For at least these reasons, Buruganahalli does not teach or render obvious the routing to a "proxy system."

B. The Petition Provides No Rational Motivation for Why a Skilled Artisan Would Have Modified Buruganahalli in View of Baehr

Under the second instituted ground, Petitioner has failed to show that a POSITA would have been motivated to combine Buruganahalli and Baehr. POR at 55-67. Centripetal showed that Baehr does not provide a reason for offloading encryption from a firewall to a proxy. POR at 61. Petitioner overstates the holding of *KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398 (2007) by implying that the absence of an express teaching, suggestion, or motivation in Baehr is irrelevant and "rejected" by the courts. Reply at 21. But, the Federal Circuit has explained in post-*KSR* rulings that "a flexible approach to the TSM test" still remains, which can "prevent[] hindsight and focuses on evidence before the time of invention." *In re Translogic Tech., Inc.*, 504 F.3d 1249, 1260 (Fed. Cir. 2007); *see also Ortho-McNeil Pharm., Inc. v. Mylan Lab'ys, Inc.*, 520 F.3d 1358, 1364-65 (Fed. Cir. 2008) (finding that a "flexible TSM test remains the primary guarantor against . . . hindsight analysis").

Nor did Centripetal end its analysis after noting the absence of any express teaching, suggestion, or motivation in the references. POR at 61. Contrary to Petitioner's suggestion (Reply at 22), Centripetal did dispute each alleged "advantage" and "motivation" to combine Buruganahalli and Baehr:

- isolating a private network (POR at 61; Buruganahalli at 12:4-55, Goodrich Decl. at ¶ 126);
- providing seamless communications with outsiders (POR at 61; Buruganahalli at 12:4-55, Goodrich Decl. at ¶¶ 126-27);
- reducing load on a firewall (POR at 62-63; Ex. 1005 ("Baehr") at 4:20-63, Goodrich Decl. at ¶¶ 128-29); and
- preserving computing resources, achieve load balancing, and maximizing performance (POR at 63-65; Goodrich Decl. at ¶¶ 130-36).

In its Reply, Petitioner's criticism that these counterarguments are attacking the references individually is without merit. Reply at 22. The Supreme Court's discussion in *KSR* warns that "rejections on obviousness grounds cannot be sustained by mere conclusory statements." *KSR*, 550 U.S. at 1741 (citation omitted). Instead, there must be some articulated reasoning with "some rational underpinning" to support the legal conclusion of obviousness. *Id.* In this case, Centripetal has demonstrated that the brainstorm list of alleged advantages recited in the Petition lack a rational underpinning when examined in the context of a POSITA's view of

Buruganahalli and Baehr. There simply is no showing that a skilled artisan would have been motivated to or reasonably expected the proposed combination of Buruganahalli and Baehr to yield the “routing” to a “proxy system” step.

V. OBJECTIVE EVIDENCE OF NONOBVIOUSNESS ALSO DEMONSTRATES THAT THE CLAIMS ARE VALID

Centripetal demonstrated significant objective indicia of nonobviousness with nexus to the challenged claims. POR at 67-71. Centripetal is not “attempt[ing] to shift the burden to Petitioner.” See Reply at 25. The burden to show obviousness is always Petitioner’s, and the obviousness analysis requires consideration of objective evidence of nonobviousness. See *Graham v. John Deere Co. of Kan. City*, 383 U.S. 1, 17-18 (1966); *Lectrosonics, Inc. v. Zaxcom, Inc.*, No. IPR2018-01129, Paper 33 at 72 (P.T.A.B. Jan. 24, 2020) (citing *Graham*) (precedential).

The Petition never met this burden because it failed to address known and publicly available evidence of nonobviousness that contributed to an enhanced verdict of willful infringement in the Cisco litigation. POR at 68. This failure was exacerbated by Petitioner’s false statement that “the underlying evidence is not publicly available and Petitioner does not have access to such evidence” (Pet. at 50), despite the Cisco press release (Ex. 2013) twice appearing in Petitioner’s own exhibit (Ex. 1027). POR at 68. Petitioner seeks to rely on the vacatur of the district court’s opinion to relieve it of its burden. See Reply at 25. But, that vacatur came after the Petition was filed and had nothing to do with adequacy of the objective

evidence. Nor did it impact the availability of evidence known to be probative of nonobviousness.

In any event, the Cisco press release (Ex. 2013) demonstrates long-felt need and industry praise of the Encrypted Traffic Analytics product that is coextensive with the Challenged Claims. POR at 68-69. Petitioner does not dispute that Ex. 2013 evidences long-felt need and industry praise, just that there is no nexus. Petitioner's focus on the presumption of nexus and coextensiveness (*see, e.g.*, Reply at 24-25) is irrelevant because the POR's evidence of objective indicia is the "direct result of the unique characteristics of the claimed invention." *Fox Factory, Inc. v. SRAM, LLC*, 944 F.3d 1366, 1374 (Fed. Cir. 2019) (citation omitted). For example, Petitioner ignores the description in the Cisco press release (Ex. 1027 at 64) of "identify[ing] the fingerprints of known threats even in encrypted traffic, without decrypting it and impacting data privacy." *Id.* This description embodies the novel features of the '856 Patent, which includes filtering encrypted packets according to packet-filtering rules specifying network-threat indicators. *Id.* There is nexus between the **Encrypted** Traffic Analytics and the claimed rule-based filtering of **encrypted** packets—the very same feature that distinguishes over the prior art (*see* Section II, *above*).

Further, the district court's opinion, *albeit* vacated, still provides the underlying objective evidence of nonobviousness, including when Centripetal

disclosed its technology to Cisco and when Cisco launched the infringing product. POR at 69-70 (citing Ex. 1027 at 149-152, 155-157, 160). And, Centripetal also provided additional evidence of copying (POR at 69 (citing Exs. 1029, 2016-2018)), which Petitioner ignores (Reply at 25).

VI. CONCLUSION

For these reasons, Centripetal respectfully requests that the Board find each of the Challenged Claims patentable.

Respectfully submitted,

Dated: December 30, 2022

/James Hannah/
James Hannah (Reg. No. 56,369)
Jenna Fuller (Reg. No. 74,212)
Paul Andre (*pro hac vice* pending)
Kramer Levin Naftalis & Frankel LLP
333 Twin Dolphin Drive, Suite 700
Redwood Shores, CA 94065
Tel: (650) 752-1700 Fax: (650)752-1800

Jeffrey H. Price (Reg. No. 69,141)
Kramer Levin Naftalis & Frankel LLP
1177 Avenue of the Americas
New York, NY 10036
Tel: (212) 715-7502 Fax: (212)715-8302

Scott M. Kelly (Reg. No. 65,121)
Bradley C. Wright (Reg. No. 38,061)
John R. Hutchins (Reg. No. 43,686)
BANNER & WITCOFF, LTD.
1100 13th Street, NW, Suite 1200
Washington, DC 20005
Tel: (202) 824-3000 Fax: (202) 824-3001

(Case No. IPR2022-00182)

Attorneys for Patent Owner

CERTIFICATE OF COMPLIANCE

The undersigned hereby certifies that the portions of the above-captioned PATENT OWNER'S SUR-REPLY specified in 37 C.F.R. § 42.24 has 5,600 words in compliance with the 5,600-word limit set forth in 37 C.F.R. § 42.24(c)(4). This word count was prepared using the Microsoft Word word-processing system used to prepare this paper.

Dated: December 30, 2022

By: /James Hannah/
James Hannah (Reg. No. 56,369)
Jenna Fuller (Reg. No. 74,212)
Paul Andre (*pro hac vice* pending)
Kramer Levin Naftalis & Frankel LLP
333 Twin Dolphin Drive, Suite 700
Redwood Shores, CA 94065
Tel: (650) 752-1700 Fax: (650) 752-1800

Jeffrey H. Price (Reg. No. 69,141)
Kramer Levin Naftalis & Frankel LLP
1177 Avenue of the Americas
New York, NY 10036
Tel: (212) 715-7502 Fax: (212) 715-8302

Scott M. Kelly (Reg. No. 65,121)
Bradley C. Wright (Reg. No. 38,061)
John R. Hutchins (Reg. No. 43,686)
BANNER & WITCOFF, LTD.
1100 13th Street, NW, Suite 1200
Washington, DC 20005
Tel: (202) 824-3000 Fax: (202) 824-3001

Attorneys for Patent Owner

CERTIFICATE OF SERVICE

The undersigned certifies, in accordance with 37 C.F.R. § 42.6(e), and pursuant to agreement by the parties that filing with the Board through the Patent Trial and Appeal Case Tracking System (P-TACTS) constitutes electronic service, that service was made on Petitioner as detailed below.

<i>Date of service</i>	December 30, 2022
<i>Manner of service</i>	Electronic Filing with the Board
<i>Documents served</i>	PATENT OWNER'S SUR-REPLY
<i>Persons served</i>	ROPES & GRAY LLP Scott A. McKeown Mark D. Rowland James Batchelder Andrew Radsch Keyna Chow

/James Hannah/
James Hannah
Registration No. 56,369
Lead Counsel for Patent Owner