

Petitioner Palo Alto Networks' Demonstratives

***Palo Alto Networks, Inc., Cisco Systems, Inc., and Keysight Technologies,
Inc. v. Centripetal Networks, Inc.***

***Inter Partes Review of
U.S. Patent No. 9,917,856
February 15, 2023***

**IPR2022-00182
Patent Trial and Appeal Board
United States Patent and Trademark Office**

**PAN EX1056
Palo Alto Networks v. Centripetal Networks
IPR2022-00182
Page 00001**

Overview of the '856 Patent

- Extract plaintext data from session-initiating unencrypted handshake message:

...common name (e.g., the domain name of the server, or the type dNSName), or the like), and rules 212 may be configured to cause rule gate 120 to one or more of identify the packets or determine that the packets comprise data corresponding to the network-threat indicators based on data included in the one or more handshake messages configured to establish session 306. In such embodiments, rules 212 may be configured to cause packet-filtering system 200 to

'856, 9:29-33; Pet. 13

- Based on the extracted handshake data, apply packet filtering rules to encrypted packets of that same session:

In step 710, the packet-filtering system may determine based on a portion of the unencrypted data corresponding to the network-threat indicators that the packets comprising encrypted data correspond to the network-threat indicators. For example, packet-filtering system 200 may determine that a domain name included in the DNS query, the reply to the DNS query, or the handshake message corresponds to the network-threat indicators, and packet-filtering system 200 may determine that one or more of the packets encrypted in accordance with the parameters of sessions 306, 308, 408, 410, 504, or 606 correlate to one or more packets comprising the DNS query, the reply to the DNS query, or the one or more handshake messages.

'856, 24:18-30; Pet. 13

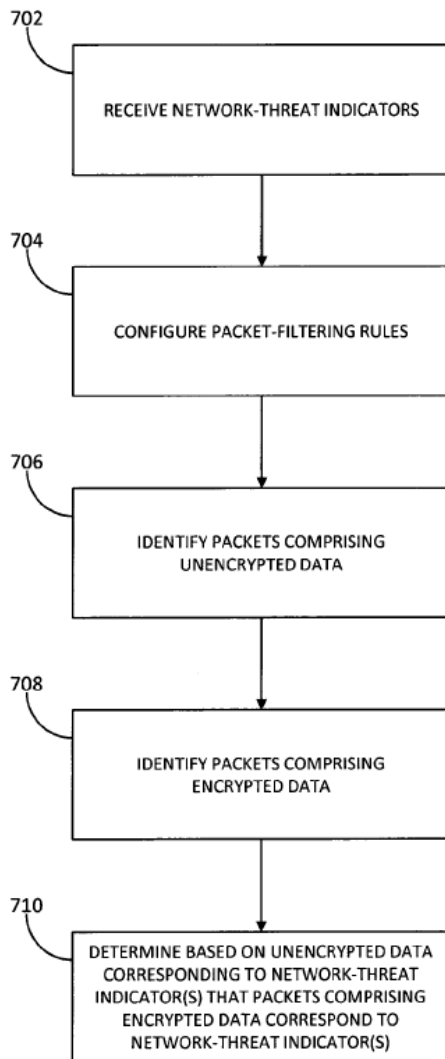


FIG. 7

Overview of the '856 Patent

- After receiving encrypted packets, the proxy device—which may comprise an ICAP client in communication with an ICAP server—may decrypt them:

Proxy device 112 may receive the packets and decrypt the data in accordance with the parameters of session 306. The packets may comprise a request (e.g., a hypertext transfer protocol (HTTP) request), and proxy device 112 may comprise an ICAP client, which, at step #20, may communicate the packets to ICAP server 132. Rule gate 126 may interface

'856, 10:15-19; Pet. 13-14; Reply 13

- ICAP servers, as well known in the art, are used to detect malware by checking for viruses.

Ex. 1051, 10; Reply 13

'856, Claim 1

[1.pre] A method comprising:

[1.a] receiving, by a packet-filtering system comprising a hardware processor and a memory and configured to filter packets in accordance with a plurality of packet-filtering rules, data indicating a plurality of **network-threat indicators**, wherein at least one of the plurality of network-threat indicators comprises a domain name identified as a network threat;

[1.b] identifying packets comprising unencrypted data;

[1.c] identifying packets comprising encrypted data;

[1.d] determining, by the packet-filtering system and based on a portion of the unencrypted data corresponding to one or more network-threat indicators of the plurality of network-threat indicators, packets comprising encrypted data that corresponds to the one or more network-threat indicators;

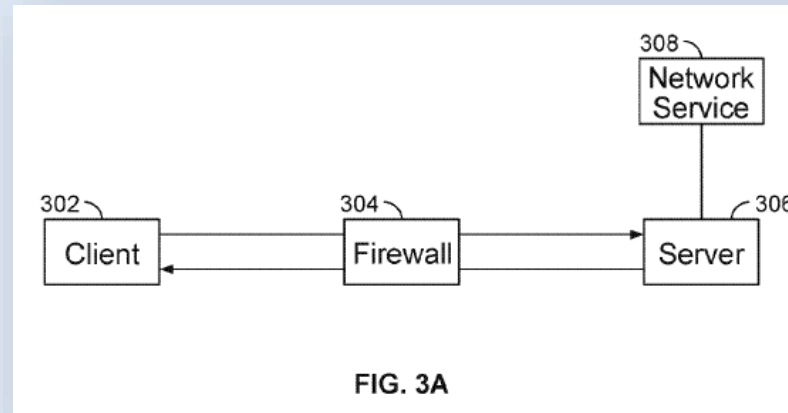
[1.e] **filtering**, by the packet-filtering system and based on at least one of a uniform resource identifier (URI) specified by the plurality of packet-filtering rules, data indicating a protocol version specified by the plurality of packet-filtering rules, data indicating a method specified by the plurality of packet-filtering rules, data indicating a request specified by the plurality of packet-filtering rules, or data indicating a command specified by the plurality of packet-filtering rules:

[1.f] packets comprising the portion of the unencrypted data that corresponds to one or more network-threat indicators of the plurality of network-threat indicators; and

[1.g] **the determined packets comprising the encrypted data that corresponds to the one or more network-threat indicators**; and

[1.h] **routing**, 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.

Overview of Buruganahalli



- Extract plaintext data from session-initiating unencrypted handshake message:

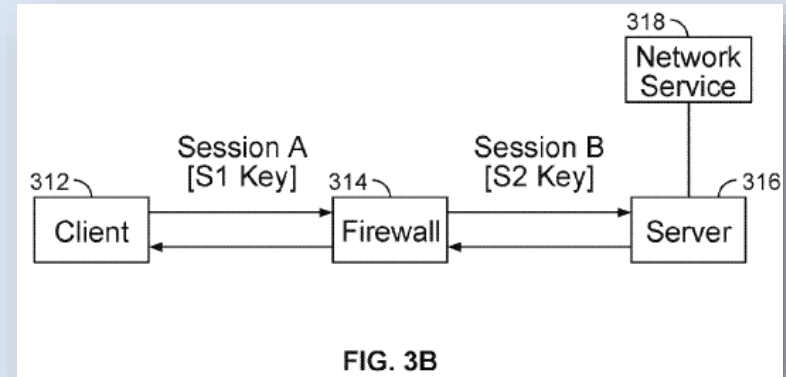
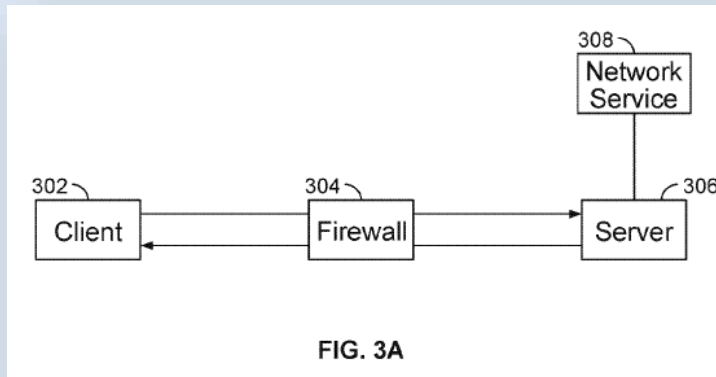
While performing various decryption techniques as described herein can facilitate applying filtering based on a policy (e.g., a security policy, such as a firewall policy), it would be desirable and efficient to further facilitate policy-based filtering on such data communication flows (e.g., sessions) prior to the set-up of the encrypted data communication for such flows (e.g., to monitor the initial unencrypted/clear text data communications exchanged as part of an initial handshake to setup a secure connection for a new session between a client and a remote server, which is prior to the establishment of the secure communication channel/tunnel after which any data communications intercepted between the client and the remote server would be encrypted).

- Based on the extracted handshake data, apply packet filtering rules to encrypted packets of that same session:

However, using various techniques described herein for destination domain extraction for secure protocols that facilitate the extraction of the destination domain by parsing the handshake traffic (e.g., parsing a client hello message to extract a hostname that identifies the destination domain being requested by the client to the remote server), the firewall 304 can apply one or more firewall policies/rules implemented by the firewall device 304 (e.g., a policy that includes requirements or rules related to destination domains that may be used for secure protocol communications) prior to and/or without having to decrypt the encrypted secure tunnel session traffic.

Overview of Buruganahalli

- Filtered packets may be allowed, blocked (dropped), or routed to a decryption engine for additional processing:

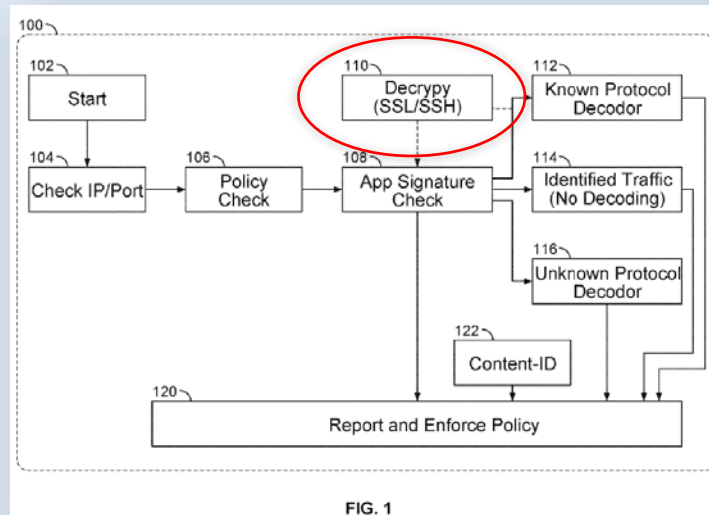


- Buruganahalli's decrypt engine functions as a transparent proxy:

As further illustrated in FIG. 1, if the monitored traffic is encrypted (e.g., encrypted using HTTPS, SSL/TLS, SSH, or another known encryption protocol), then the security device can be configured (e.g., based on a firewall policy) to decrypt the monitored traffic using a decrypt engine 110 (e.g., applying trusted man-in-the-middle techniques using a self-signed certificate). For example, in some cases, if the

firewall 314. In response, the firewall 314 performs a trusted man-in-the-middle technique by effectively splitting the SSL session between the client 312 and the remote server 316 into two half sessions shown as Session A and Session B in FIG. 3B. In Session A, the firewall 314 acts as the remote server 316 such that it is transparent to the client 312 that it is not communicating directly with the remote server 316. Session A traffic is encrypted using the session key S1 associated with the firewall device. In Session B, the firewall 314 acts as the client 312 such that it is transparent to the remote server 316 that it is not communicating directly with the client 312. Session B traffic is encrypted using the session key S2 associated with the firewall device (e.g., the firewall device can store the fingerprint from the remote server in association with that remote server IP address).

Overview of Buruganahalli

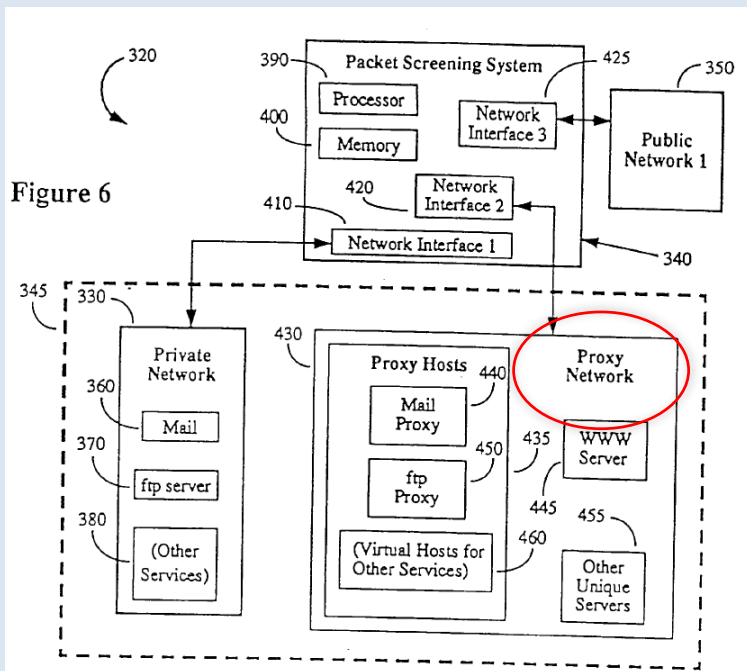


- Packets may be subject to “further potential filtering” after decryption:

For example, if a flow is initially determined to be permissible based on a policy prior to the set-up of the encrypted data communication for that flow between a client and a remote server, then the flow can be allowed, and a policy may require that the session be decrypted for further analysis and further potential filtering based on the policy. As an example, Alice who is another user (e.g., another employee)

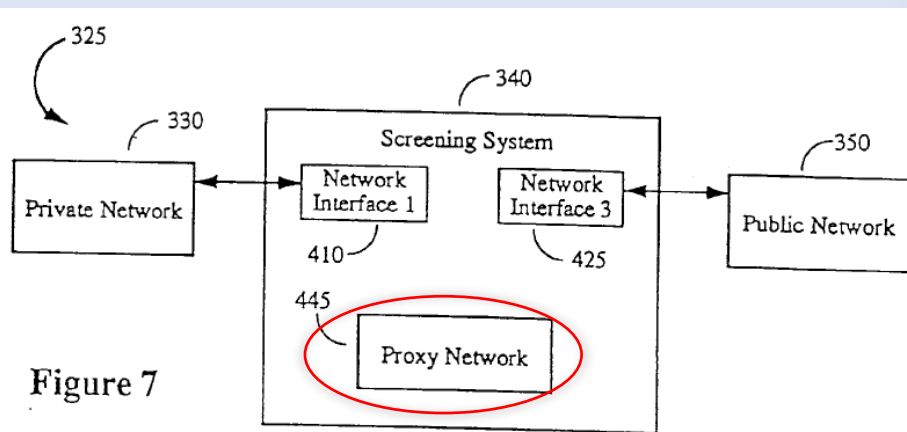
In some embodiments, destination domain extraction for secure protocols further includes decrypting the monitored encrypted network communications of a session associated with the network communications between the client and the remote server to verify that the destination domain name extracted from a server name indication matches the domain associated with a URL for the session associated with the network communications between the client and the remote server. For example, this technique can be used in order to detect malware that attempts to fool a hosting site by including false destination domain information (e.g., in the SNI field in a client hello message of an initial set-up of a TLS session).

Overview of Baehr



The screening system includes a packet filtering subsystem or module, which inspects each incoming packet and sends it to an engine, which determines, based upon the packet inspector and other information, what actions should be taken on the packet. The packet is passed to an actions subsystem or module, which executes the appropriate actions.

If the packet's intended destination is a host machine on the private network, it may instead be sent aside to a preconfigured host machine on the proxy network, which executes appropriate operations that the actual host would execute, or different operations as desired. The proxy host generates responses using the IP address of the actual host, so the existence of the proxy network is not detectable. The



Grounds

Ground	Basis	Claims	Prior Art
1	§103	1, 24-25	Buruganahalli
2	§103	1, 24-25	Buruganahalli in view of Baehr

Pet. 8.

Disputed Issues

- 1. Whether Buruganahalli teaches rule-based filtering of encrypted packets**
- 2. Whether Buruganahalli teaches “network-threat indicators”**
- 3. Whether Buruganahalli alone, or alternatively in view of Baehr, teaches routing to a proxy**
- 4. Secondary considerations**

Issue 1

Buruganahalli teaches rule-based filtering of encrypted packets

'856, Claim 1 – Filtering

[1.e] **filtering**, by the packet-filtering system and based on at least one of a uniform resource identifier (URI) specified by the plurality of packet-filtering rules, data indicating a protocol version specified by the plurality of packet-filtering rules, data indicating a method specified by the plurality of packet-filtering rules, data indicating a request specified by the plurality of packet-filtering rules, or data indicating a command specified by the plurality of packet-filtering rules:

[1.f] packets comprising the portion of the unencrypted data that corresponds to one or more network-threat indicators of the plurality of network-threat indicators; and

[1.g] **the determined packets comprising the encrypted** data that corresponds to the one or more network-threat indicators; and

Buruganahalli's Decision to Pass, Block, or Route for Decryption An Encrypted Packet Is Filtering

“Other traffic may be treated differently (*i.e.*, simply passed, or blocked), depending on the corresponding firewall policy. For example, as PO acknowledges, if the destination domain is on a whitelist, the associated encrypted traffic would simply pass without proxy processing; or, if the destination domain is on a blacklist, the associated encrypted traffic may be blocked altogether. The decision to pass, block, or route for decryption an encrypted packet is a filtering step performed on that packet.”

Reply 5

The Board recognized that the decision whether to forward encrypted traffic to Buruganahalli's decryption engine is a filtering step:

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.”

Paper 40 (Decision Denying PO's Request for Rehearing), 11;
 see also Paper 39 (Decision Granting Institution and Motion for Joinder), 20-21;
 Paper 41 ((Decision Granting Institution and Motion for Joinder), 20-21.

PO Concedes That Buruganahalli Applies Policies/Rules to Encrypted Traffic Before any Decryption May Occur

at 6:12-39). But, again, the cited portion of Buruganahalli explains that a policy may cause the firewall to initially allow a session/flow and then “require[s] that the session be *decrypted* for further analysis and further potential filtering based on the policy.” Ex. 1004 at 6:21-22.

POR 41

10:57-61. Buruganahalli’s solution to this problem is to extract a destination domain from the unencrypted handshake traffic so that its “firewall policies/rules” may be applied “*prior to and/or without having to decrypt* the encrypted secure tunnel session traffic.” *Id.* at 11:17-19. This technique, which is explained more fulsomely earlier in Buruganahalli, refers to the firewall’s ability to determine

POR 38

Buruganahalli Discloses Applying a Blacklist Policy, Based on an Extracted Destination Domain, to to All Packets (Unencrypted and Encrypted) of a Session

- Buruganahalli expressly states that a blacklist policy (i.e., packet filtering rule/rules) is applied to encrypted packets based on the extracted destination domain (e.g., URL):

In some embodiments, destination domain extraction for secure protocols further includes applying a security policy based on the destination domain to filter traffic at the security device. For example, the security policy can include a malware detection policy, a whitelist/blacklist policy (e.g., in which a session associated with the network communications between the client and the remote server are not decrypted if the destination domain is included in the whitelist, and a session associated with the network communications between the client and the remote server are decrypted if the destination domain is included in the blacklist), and/or a uniform resource locator (URL)/category filtering policy.

Buruganahalli, 7:39-51; Pet. 18-19, 33, 35, 38-39; Reply 7-8

- PO admits that Buruganahalli uses a destination domain to apply a filtering rule:

destination domain. *Id.* at 4:59-5:10. Buruganahalli's firewall uses this destination domain to apply a whitelist/blacklist policy. *Id.* at 7:12-51; Goodrich Decl., ¶¶ 41-

POR, 5

Determining Whether to Route to the Decryption Engine a Packet is Based on Whitelist/Blacklist Policy Applied on That Packet

The Board recognized that filtering encrypted traffic by routing it to a decryption engine is filtering:

As further illustrated in FIG. 1, if the monitored traffic is encrypted (e.g., encrypted using HTTPS, SSL/TLS, SSH, or another known encryption protocol), then the security device can be configured (e.g., based on a firewall policy) to decrypt the monitored traffic using a decrypt engine 110 (e.g., applying trusted man-in-the-middle techniques using a self-signed certificate). For example, in some cases, if the extracted destination domain is not trusted or unknown, then the firewall can be configured to decrypt the monitored traffic for further traffic monitoring and inspection based on a policy (e.g., a firewall policy). As another example, the

Paper 40 (Decision Denying PO's Request for Rehearing), 8-9;
see also Paper 39 (Decision Granting Institution and Motion for Joinder), 21;
Paper 41 ((Decision Granting Institution and Motion for Joinder), 21.

PO's Assertion Regarding Flow Lookup Does Not Distinguish the '856 Claims

PO argues: Buruganahalli's initial handling of encrypted packets is based on IP address and port number, and not with reference to any alleged "packet-filtering rules."

POSR, 7-8.

The Board recognized:

Opp. 13. Determining “which flow the packet belongs to based on the ‘IP address and port number’” corresponds to limitation [1.d] and the similar limitations in claims 24 and 25. *See* PAN Inst. Dec. 64; Ex. 1003 ¶¶ 116–121. Filtering by applying policies occurs after determining “which flow the packet belongs to based on the ‘IP address and port number.’” *See, e.g.,* PAN Inst. Dec. 66–67, 69–71. Patent Owner admits that “decoder 614 applies policies,” although Patent Owner asserts erroneously that the policies are applied only to decrypted data. Prelim. Resp. 43–44 (emphasis omitted).

Paper 39 (Decision Granting Institution and Motion for Joinder), 25-26;
Paper 41 ((Decision Granting Institution and Motion for Joinder), 25-26;
see also Pet. 19-20, 34-40; Reply 9-11.

Petitioner Did Not Rely On Flow Lookup For The Filtering Step

PO argues: Because the Petition and Board point to the flow lookup for “identifying” unencrypted and encrypted packets, it is inconsistent to rely on the same “lookup” for the “filtering” step.

POR 42-43.

“[T]he 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 10 (citing Buruganahalli, 14:25-28); Pet. 30-32.

The Board recognized:

Contrary to Patent Owner’s contentions, the analysis for limitations [1.b], [1.c], and [1.g] in the PAN IPR Institution Decision does not map the limitations to just one component in Figure 6’s security device 402, i.e., flow component 608. *See* PAN Inst. Dec. 61–62, 69; Prelim. Resp. 43. In any event, claims 1, 24, and 25 do not require that a packet-filtering system have one component for “identifying” packets and another, different component for “filtering” packets. *See* Ex. 1001, 25:14–49, 28:59–30:31; *see also Powell v. Home Depot U.S.A., Inc.*, 663 F.3d 1221, 1231–32 (Fed. Cir. 2011) (deciding that the same structure in an accused device satisfied a claim’s requirement for a “cutting box” and the claim’s requirement for a “dust collection structure”).

Buruganahalli's Figure 3A Embodiment Together With Its Figure 3B Embodiment Teaches Filtering Encrypted Traffic And Routing It To A Proxy For Decryption

PO argues: neither Figures 3A nor 3B alone teaches the claimed embodiment.

POR, 35, 37-40; POSR, 12-13.

- Buruganahalli discloses using techniques according to Figure 3A's embodiment separate or ***together with*** techniques according to Figure 3B's embodiment.

Pet. 22-23, 40 (citing Buruganahalli, 11:61-12:3, Weissman, ¶141);
DI, 71 (citing Buruganahalli, 11:7-12:3); Reply, 11-12.

- The grounds rely 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 the grounds rely on the disclosure of Figure 3B for routing filtered encrypted traffic to a proxy (*i.e.*, a decrypt engine).

Pet. 32-41; Reply, 11.

That Buruganahalli Teaches Decryption Of Encrypted Packets After Filtering Them Does Not Distinguish The Challenged Claims

PO argues: Buruganahalli teaches applying firewall rules to decrypted packets (i.e., to encrypted packets that were routed to, and then decrypted by, Buruganahalli's decrypt engine).

POR, 32-44.

- The Claims do not exclude the unclaimed extra step of decrypting encrypted packets after filtering. Rather the '856 specification describes this same unclaimed step of sending filtered encrypted packets to a proxy for purposes of decryption.

Reply, 12-14.

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).

Paper 40 (Decision Denying PO's Request for Rehearing), 9-10;
see also Paper 39 (Decision Granting Institution and Motion for Joinder), 21;
Paper 41 ((Decision Granting Institution and Motion for Joinder), 21.

Buruganahalli's Disclosures Refute PO's Assertion That, According to Figure 6, Rules Are Applied Only After Decryption

PO argues: Figure 6 of Buruganahalli shows that policies are applied (by Figure 6's decoder) only after the data has been decrypted.

POR 9-10, 43-44; POSR, 9-10.

- But Buruganahalli explains that decryption is performed only "if applicable" to a given packet, as the Board recognized, proving that policies are not applied "only after" decryption:

Buruganahalli:

various techniques described herein. If applicable (e.g., using one or more policies based on the extracted destination domain), SSL decryption is applied by SSL decryption engine 610 using various techniques as described herein. Otherwise, processing by SSL decryption engine 610 is omitted. Application identification module 612 is configured to determine what type of traffic the session involves and to

Buruganahalli, 14:33-38; see Pet. 19-20, 43; Reply 10.

The Board recognized:

Buruganahalli's disclosures that (1) decryption occurs only if "applicable" to a packet and (2) decryption is "omitted" if inapplicable refutes Patent Owner's assertion that Figure 6's security device 402 "performs decryption before using policies for filtering" and does not apply policies to packets with encrypted data. *See* Ex. 1004, 14:33-38; Prelim. Resp. 35, 43-44.

Paper 39 (Decision Granting Institution and Motion for Joinder), 25;
Paper 41 ((Decision Granting Institution and Motion for Joinder), 25.

There Was No Change In Petitioner's Theory

PO argues: "Petitioner altered its unpatentability theory" because Petitioner used the words "based on" the handshake processing in its PPR, but the word "after" the handshake processing in its Petition.

POR 31-32.

- A second event that is "based on" a first event necessarily comes "after" the first event.
Reply, 6
- Both Petition and PPR showed that Buruganahalli teaches extracting a destination domain to identify a firewall policy to apply to associated encrypted traffic—and the filtering of that encrypted traffic (e.g., for routing to a proxy) is based on, and comes after, that extraction of the destination domain from the handshake.

Pet. 38; PPR 5.

Issue 2

Buruganahalli teaches “network-threat indicators”

Buruganahalli Teaches “Network-Threat Indicators” Under Any Reasonable Construction

- Petitioner’s construction is consistent with the Board’s constructions of this same term in other of PO’s Patents:

PO’s Construction	Petitioner’s Construction	Board’s Prior Construction
Indicators of packets associated with network threats, such as network addresses, ports, domain names, uniform resource locators (URLs), or the like.	Indicators that represent the identity of a resource associated with a network threat.	Indicators that represent the identity of a resource associated with a network threat.

Pet. 17 (citing Ex. 1026, 8-10); POR 28-29; Reply 14

BACKGROUND

Network security is becoming increasingly important as the information age continues to unfold. Network threats may take a variety of forms (e.g., unauthorized requests or data transfers, viruses, malware, large volumes of traffic designed to overwhelm resources, and the like). Network-threat services provide information associated with network threats, for example, reports that include listings of network-threat indicators (e.g., network addresses, domain names, uniform resource identifiers (URIs), and the like). Such information may be utilized to identify network threats. Encrypted communications, however, may obfuscate data corresponding to network threats. Accordingly, there is a need for rule-based network-threat detection for encrypted communications.

Pet. 17; ‘856, 7-20

Any difference in the parties’ constructions is inconsequential; PO agrees

Buruganahalli Teaches “Network-Threat Indicators” Under Any Reasonable Construction

- It is undisputed that:
 - **Use of “network-threat indicators” to filter packets was well-known**
 - Admitted by ‘856 patent. See ‘856, 1:12-16; Pet. 2.
 - Unrebutted testimony of Dr. Weissman confirming they were well known for packet filtering. Ex.1003, ¶¶61-63 (discussing Macaulay and Moore references).
 - **Buruganahalli teaches use of a blacklist comprising destination domains.** *E.g.*, Pet. 4, 18-19; 30.
 - **Blacklists were known to be associated with malicious traffic.** Reply 16 (citing PO’s expert’s textbook, Ex. 1052 at 22.
- Whether Buruganahalli expressly states that its blacklist includes known threats is irrelevant to an obviousness ground. Reply 14.
- Even PO admits that Buruganahalli’s blacklist “comprises domains that a network administrator has identified for monitoring or blocking.” POR 50.

Buruganahalli Teaches Filtering Using a Blacklist For Security Purposes

In some embodiments, destination domain extraction for secure protocols further includes applying a security policy based on the destination domain to filter traffic at the security device. For example, the security policy can include a malware detection policy, a whitelist/blacklist policy (e.g., in which a session associated with the network communications between the client and the remote server are not decrypted if the destination domain is included in the whitelist, and a session associated with the network communications between the client and the remote server are decrypted if the destination domain is included in the blacklist), and/or a uniform resource locator (URL)/category filtering policy.

Buruganahalli, 7:39-51; Pet. 30; Reply 15.

self-signed certificate). For example, in some cases, if the extracted destination domain is not trusted or unknown, then the firewall can be configured to decrypt the monitored traffic for further traffic monitoring and inspection based on a policy (e.g., a firewall policy). As another example, the

Buruganahalli, 9:67-10:4; Reply 14.

“Because the extracted destination domain information is compared against a blacklist as specified by a ‘**security policy**’ at the security device, a POSITA would have understood, or at least found it obvious, that the blacklist contains a list of destination domains associated with network threats.”

Reply 15 (citing cross examination of Dr. Weissman)

Buruganahalli Teaches a Feedback Loop for Identifying Destination Domains Associated with Vulnerabilities and Other Threats

- Buruganahalli's teaching of a feedback loop for identifying threats and vulnerabilities reinforces the conclusion that Buruganahalli's blacklist comprises data that indicate both potential, and actual, threats:

security cloud service 410 by the security device 402. As yet another example, the security device 402 can extract destination domain information possibly along with other extracted information using various techniques, and such extracted information can be provided to the security cloud service 410 that can facilitate identification of new, zero-day threats, new vulnerabilities, prevent false positives, and/or provide a feedback loop for any of such activities or trends aggregated and correlated using the security cloud service.

Buruganahalli, 13:44-51; Pet. 30; Reply 14-15

A POSITA Would Have Known That a Blacklist is Associated With “Malicious Traffic”—i.e., Network Threats

- As PO’s own expert wrote, blacklists are associated with blocking malicious traffic:

network (or individual computer). Some network administrators choose a *blacklist approach, or default-allow ruleset*. In this configuration, all packets are allowed through except those that fit the rules defined specifically in a blacklist. This type of configuration is more flexible in ensuring that service to the internal network is not disrupted by the firewall, but is naive from a security perspective in that it assumes the network administrator can enumerate all of the properties of *malicious traffic*.

Ex. 1052 (PO’s expert’s textbook), 22; Reply 16; Pet. 30

Issue 3

Buruganahalli alone, or alternatively in view of
Baehr, teaches routing to a proxy

Buruganahalli Alone Discloses, or at Least Renders Obvious, Routing to A Proxy System

- Buruganahalli discloses that filtered packets may be sent to a “decrypt engine” of the firewall to be decrypted:

In some embodiments, destination domain extraction for secure protocols further includes applying a security policy based on the destination domain to filter traffic at the security device, in which the security policy includes a whitelist/blacklist policy, and in which a session associated with 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.

As further illustrated in FIG. 1, if the monitored traffic is encrypted (e.g., encrypted using HTTPS, SSL/TLS, SSH, or another known encryption protocol), then the security device can be configured (e.g., based on a firewall policy) to decrypt the monitored traffic using a decrypt engine 110 (e.g., applying trusted man-in-the-middle techniques using a self-signed certificate). For example, in some cases, if the

Buruganahalli, 7:59-67, 9:61-67; Pet. 20-27; Reply 17-19.

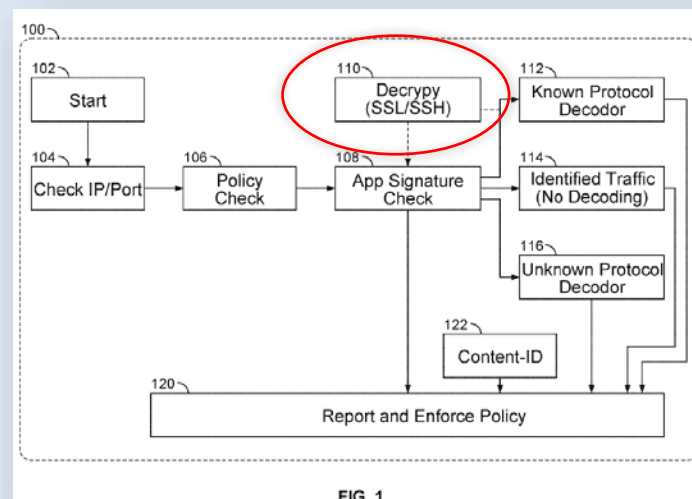


FIG. 1

Buruganahalli, Fig. 1

Buruganahalli Alone Discloses, or at Least Renders Obvious, Routing to A Proxy System

- As Dr. Weissman established, a POSITA would have understood that routing may be implemented as a software process that may be internal to a firewall:

68. It was further well-known and conventional in the art before the claimed priority date of the '856 patent for a network security system to route packets between interfaces of functional components of a security device such as a firewall. This technique was widely implemented using a software routing function.

69. For example, J. Wack et al., *Guidelines on Firewalls and Firewall Policy*, National Institute of Standards and Technology ("NIST") (Ex. 1036) describes the characteristics of an application-proxy gateway firewall. NIST discloses, "[a]pplication-proxy gateway firewalls do not require a Layer 3 (Network Layer) route between inside and outside interfaces of the firewall; the firewall software performs the routing. In the event the application-proxy gateway software

Weissman Decl. (Ex. 1003), ¶¶68, 69; Pet. 2-3, 51

- Dr. Weissman's testimony is unrebutted

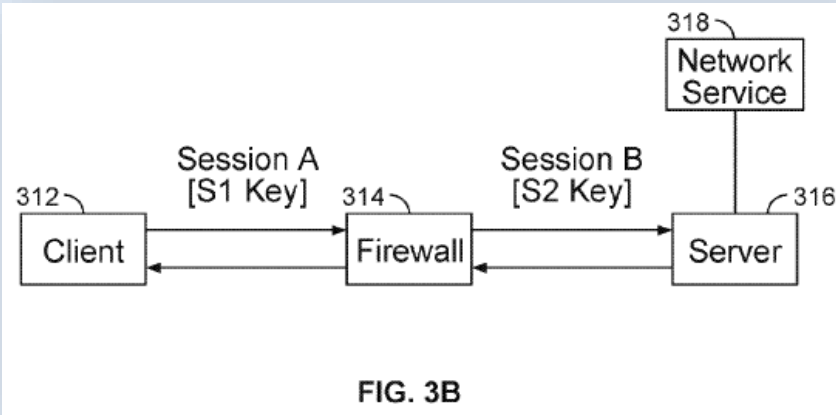
Buruganahalli’s Decrypt Engine, to Which Packets are Sent, Is A “Proxy System”

- Buruganahalli’s decrypt engine functions as a proxy because it applies trusted-man-in-the-middle techniques and operates in a transparent manner:

As further illustrated in FIG. 1, if the monitored traffic is encrypted (e.g., encrypted using HTTPS, SSL/TLS, SSH, or another known encryption protocol), then the security device can be configured (e.g., based on a firewall policy) to decrypt the monitored traffic using a decrypt engine 110 (e.g., applying trusted man-in-the-middle techniques using a self-signed certificate). For example, in some cases, if the

implemented by a firewall device 314. However, in this case, the SSL session request is intercepted and detected by the firewall 314. In response, the firewall 314 performs a trusted man-in-the-middle technique by effectively splitting the SSL session between the client 312 and the remote server 316 into two half sessions shown as Session A and Session B in FIG. 3B. In Session A, the firewall 314 acts as the remote server 316 such that it is transparent to the client 312 that it is not communicating directly with the remote server 316. Session A traffic is encrypted using the session key S1 associated with the firewall device. In Session B, the firewall 314 acts as the client 312 such that it is transparent to the remote server 316 that it is not communicating directly with the client 312. Session B traffic is encrypted using the

Buruganahalli, 9:61-67, 12:12-25; Pet. 23-25, 39-42; Reply 17-19.



Buruganahalli’s Decrypt Engine, to Which Packets are Sent, Is A “Proxy System”

A POSITA would have understood that applying a trusted man-in-the-middle technique, which is transparent to the endpoints, describes the function of a transparent proxy

Pet. 24-26, 40-41; Weissman, ¶¶ 68-76, 140-142.

As would be appreciated, the intermediary interface for the session decryption and encryption is described as “transparent” to the endpoints (*i.e.*, the client and server), and as such functions as a proxy, and more specifically, a “transparent” proxy, as was known in the art. *See, e.g.*, Wang, 8:12-19 (“In particular, because the proxy device 120 is a transparent intermediary to the client-server security session, the proxy device is able to decrypt the received traffic/packets (*e.g.*, using the session key negotiated for the client-proxy or proxy-server session, as appropriate) from each sending end device, and may re-encrypt the traffic prior to forwarding it on using the respective session key with the receiving end device.”); Ebrahimi, 1:48-52 (“[A] transparent proxy is neither known to nor configured by the clients; rather, the transparent proxy intercepts outgoing client requests to access origin servers/sites and transparently processes the requests on behalf of the clients.”); NIST, 14.

Pet. 24

Buruganahalli's Decrypt Engine, to Which Packets are Sent, Is A "Proxy System"

- PO's own expert relies on art that describes acting as a man-in-the-middle as implementing a proxy technique:

There can be no reasonable dispute that a POSITA would have understood that applying a trusted man-in-the-middle technique describes the function of a proxy. Pet. 40-41; Weissman, ¶¶140-142. Indeed, PO's expert, Dr. Goodrich, cites a patent (*see* Ex. 2026, ¶31 (citing Ex. 2015 ("Chaubey"), 2:47-5:12)), explaining that a security device acts as a man-in-the middle by implementing a proxy technique. Ex. 2015, 2:66-3:2 ("When implementing the SSL forward proxy technique, the security device may split the secure session into two parts and act as a man-in-the-middle (e.g., between the client device and the server device)."), 4:52-55 ("... by acting as a man-in-the-middle using the SSL forward proxy technique..."). The decrypt engine of Buruganahalli's firewall applying trusted man-in-the-middle techniques (which PO does not dispute) meets the claimed proxy, as would have been understood by a POSITA.

Reply 19

Buruganahalli Discloses a “Proxy System” Even Under PO’s Construction

- PO contends: “proxy system” should be construed as “a proxy system which intervenes to prevent threats in communications between devices.”
POR, 53
- PO admits that its proposed construction is not plain and ordinary meaning:

Regardless whether the Board adopts the district courts’ construction or applies the plain and ordinary meaning, Buruganahalli, alone or in combination with Baehr, fails to teach “routing, by the packet-filtering system, filtered packets to a proxy system” as claimed. *See* §IV.C, *infra*.

POR, 30

- Regardless, Buruganahalli’s decryption engine intervenes to prevent threats by performing trusted man-in-the-middle techniques, e.g., to detect malware.
Buruganahalli, 8:11-24, 9:61-10:4; Reply 18
- PO’s expert agrees that such technique involves “intercepting” communications:

0019; Ex. 2015 at 2:47-59. Such a firewall functions as a “trusted man-in-the-middle,”² intercepting, decrypting, analyzing, and then re-encrypting the encrypted communications. Ex. 2015 at 2:47-5:12. But decryption and re-encryption is

Ex. 2026, ¶31; Reply 18

Buruganahalli Teaches Routing Filtered Packets To A Proxy System

PO argues: “Buruganahalli’s decrypt engines 110, 610 are not a proxy” because they perform only decryption.

POR 53-55.

- Buruganahalli’s decrypt engines perform the same functions as the ’856 patent’s disclosed proxy that receives and decrypts encrypted packets.

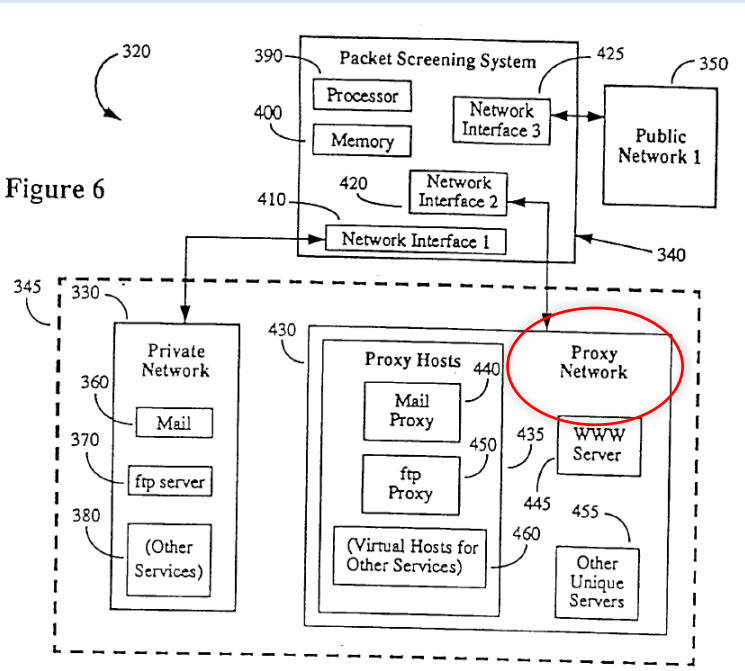
Reply, 17; see also Pet. 40, Weissman, ¶140.

Buruganahalli, 9:61-67	'856, 10:15-16
“... the security device can be configured (<i>e.g.</i> , based on a firewall policy) to decrypt the monitored traffic using a decrypt engine 110 (<i>e.g.</i> , applying trusted man-in-the-middle techniques using a self-signed certificate).”	“Proxy device 112 may receive the packets and decrypt the data in accordance with the parameters of session 306”

Issue 3

Buruganahalli alone, or alternatively **in view of Baehr**, teaches routing to a proxy

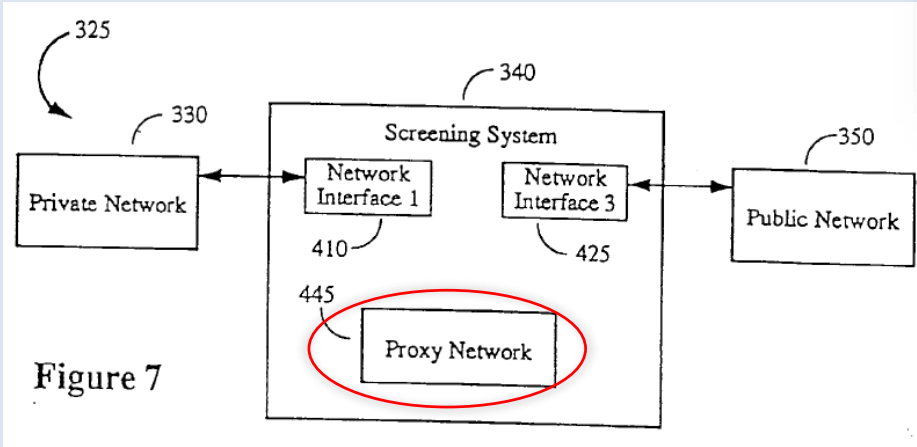
There Is No Dispute That Baehr Teaches a Separate Proxy System



The screening system includes a packet filtering sub-system or module, which inspects each incoming packet and sends it to an engine, which determines, based upon the packet inspector and other information, what actions should be taken on the packet. The packet is passed to an actions subsystem or module, which executes the appropriate actions.

If the packet's intended destination is a host machine on the private network, it may instead be sent aside to a preconfigured host machine on the proxy network, which executes appropriate operations that the actual host would execute, or different operations as desired. The proxy host generates responses using the IP address of the actual host, so the existence of the proxy network is not detectable. The

Baehr, 2:18-32; Pet. 44-47



The Petition Explains How Baehr Is Relied Upon for its Teaching of Routing to a Separate Proxy System

PO argues: the Petition fails to explain “how” the combination in trial ground 2 meets the claims.

Compare POR 55-56 with POPR 35-36.

- But as the Petition explained:

A POSITA would have been motivated and found it obvious to implement Buruganahalli’s system in view of the teachings of Baehr to route the filtered packets to a proxy system separate from the firewall, such that Buruganahalli’s

Pet., 47

- And the Board already found PO’s argument meritless:

We disagree with Patent Owner’s assertion that Petitioner fails “to specify where each claim element is found in the combination.” See Prelim. Resp. 36. For the ground based on Buruganahalli and Baehr, Petitioner explains how Buruganahalli teaches most of the limitations in claims 1, 24, and 25 and how Baehr teaches limitation [1.h] and the similar limitations in claims 24 and 25. Pet. 42–50; see Ex. 1003 ¶¶ 147–158; *supra* §§ IV.D.2(b)–(h), IV.D.3; see also Pet. 28–39; Ex. 1003 ¶¶ 101–135. Contrary to Patent Owner’s contention, there is no “basis for denial” under 37 C.F.R. § 42.104(b)(4). See Prelim. Resp. 36.

DI, 87-88.

PO's Argument That The Petition Fails To Describe "How" The Combination Meets The Challenged Claims Lacks Merit

PO argues: the Petition does not specify whether the proxy would be implemented as a physically separate device or merely a logically separate device.

POR 58-59.

- The Claims do not require the proxy to be implemented in one form or the other
- Either implementation meets the claim language
- A proxy is a basic component in any network system—it is merely a matter of implementation as to which approach would be desired in a given system.

Reply 21.

A POSITA Would Have Combined The Teachings Of Buruganahalli And Baehr

PO argues: the Petition does not provide a reason “why” a POSITA “would combine Buruganahalli with Baehr in the claimed manner”—Baehr “does not provide a reason for offloading encryption from a firewall to a proxy” to “fix the issues with Buruganahalli.”

POR, 60-65.

- Baehr does not need to supply such a reason: the suggestion that the art itself must provide the express teaching, suggestion, or motivation was rejected years ago.

KSR Int’l Co. v. Teleflex Inc., 550 U.S. 398 (2007).

- The Petition provided multiple rationales for why a POSITA would have been motivated to modify Buruganahalli with the teachings of Baehr’s separate proxy:

discussed above, a POSITA would have been motivated and found it obvious to implement **Buruganahalli**’s techniques describing a proxy in a dedicated system for the advantages of preserving computing resources, achieving load balancing, and maximizing performance, as recognized in **Buruganahalli** (Buruganahalli, 3:5-15, 4:7-15) and in the prior art generally. *See, e.g.*, NIST, 14 (“Typically, dedicated proxy servers are used to decrease the work load on the firewall...” and “can be used to secure less time-sensitive services...”). The teachings of **Baehr** further provide the added advantages of isolating the proxy system, which handles high-risk or suspicious packets and is particularly vulnerable to attacks, from the private network. *Baehr, Abstract* (“The proxy network is isolated from the private network, so it cannot be used as a jumping off point for intruders”). For example, *Baehr*

Pet. 47-48; *see also Weissman* ¶¶155-156.

A POSITA Would Have Combined The Teachings Of Buruganahalli And Baehr

PO argues: the cost and complexity of adding a proxy system to Buruganahalli would “far outweigh any benefit.”

POR, 65.

The modification to implement the decrypt engine as a proxy would be obvious despite economic costs.

Reply 22-23.

- *In re Farrenkopf*, 713 F.2d 714, 718 (Fed. Cir. 1983) (affirming the Board’s finding that the additional expense associated with a modification would not discourage a POSITA from seeking the advantage provided by the modification);
- *Medichem, S.A. v. Rolabo, S.L.*, 437 F.3d 1157, 1165 (Fed. Cir. 2006) (“The fact that the motivating benefit comes at the expense of another benefit, however, should not nullify its use as a basis to modify the disclosure of one reference with the teachings of another...”)
(citation omitted).

Issue 4

There is No Evidence of Secondary Considerations

PO Fails To Establish Any Secondary Considerations

PO argues: “[o]bjective evidence of nonobviousness, including satisfaction of a long-felt need and industry praise, contributed to the court’s validity determination and enhanced verdict of willful infringement in the Cisco litigation.”

POR 68 (*citing* vacated district court opinion and order); POSR 25-26.

- PO’s objective indicia of non-obviousness arguments are based on a vacated district court opinion and fail for that reason alone.

Reply 23.

Order denying Cisco’s Motion for Miscellaneous Relief (ECF No. 619), *see Recusal Op.*, 492 F. Supp. 3d 615, we vacate the Opinion & Order re Infringement and Damages (ECF No. 621), *see Merits Op.*, 492 F. Supp. 3d 495, and the Opinion & Order Denying Post-Judgment Motions & De-

Ex. 1050, 27.

Cisco Sys., Inc., 492 F. Supp. 3d 615 (E.D. Va. 2020) (“*Recusal Op.*”), vacate all orders and opinions of the court entered on or after August 11, 2020, including the final judgment, and remand for further proceedings before a different district court judge.

Ex. 1050, 2-3.

PO Fails To Establish A Presumption Of Nexus To The Purported Evidence

PO argues: “the nexus between this evidence and the ’856 patent claims was [] established by way of the court’s finding that Cisco’s Encrypted Traffic Analytics technology, which claimed to solve the unsolvable problem, infringed the ’856 Patent. Ex. 1027 at 30-57.”

POR 68-69; POSR 24.

- PO fails to show that Cisco’s Encrypted Traffic Analytics solution is **coextensive** with the ’856 claims
- The cited press release describes Cisco’s Encrypted Traffic Analytics only in general terms, with no reference to the ’856 Patent or any claimed step/technique:

Cisco unveils network of the future that can learn, adapt and evolve

© June 20, 2017



Plaintiff’s Trial Exhibit

PTX-1135

Case No. 18-cv-00094-HCM

■ **Encrypted Traffic Analytics** (<http://www.cisco.com/c/en/us/solutions/enterprise-networks/enterprise-network-security/index.html>). Today, almost half of cyber-attacks are hidden in encrypted traffic and this number keeps growing. By utilizing Cisco’s Talos cyber intelligence and machine learning to analyze metadata traffic patterns, the network can identify the fingerprints of known threats even in encrypted traffic, without decrypting it and **impacting** data privacy. Only Cisco can enable IT to detect threats in encrypted traffic with up to 99% accuracy, with less than 0.01% false positives. As a result, the new network provides security while maintaining privacy.

Reply 24; Ex. 2013, 1, 2

PO Fails To Show Copying

PO argues: “the district court found that the ’856 Patent had been copied by Cisco.”

POR 69.

- The district court finding was vacated and cannot provide evidence of copying.
- PO failed to supply here the same evidence of alleged copying relied upon in the district court:

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).

Paper 40 (Decision Denying PO’s Request for Rehearing), 13-14.