



PTAB Oral Argument

February 15, 2023

**PALO ALTO NETWORKS, INC.
CISCO SYSTEMS, INC., AND
KEYSIGHT TECHNOLOGIES, INC.**

PETITIONERS

v.

CENTRIPETAL NETWORKS, LLC

PATENT OWNER

CASE NO.: IPR2022-00182

PATENT NO.: 9,917,856

Summary of Arguments

The Claims are Patentable Because the References Fail to Teach:

1. Filtering encrypted data packets based on the claimed packet-filtering rules
2. Network-threat indicators (even under Petitioner's claim construction)
3. Routing packets to a proxy system

Petitioner's Burden of Proof

35 U.S.C. § 316(e)

"In an inter partes review instituted under this chapter, the petitioner shall have the burden of proving a proposition of unpatentability by a preponderance of evidence."

Instituted Grounds

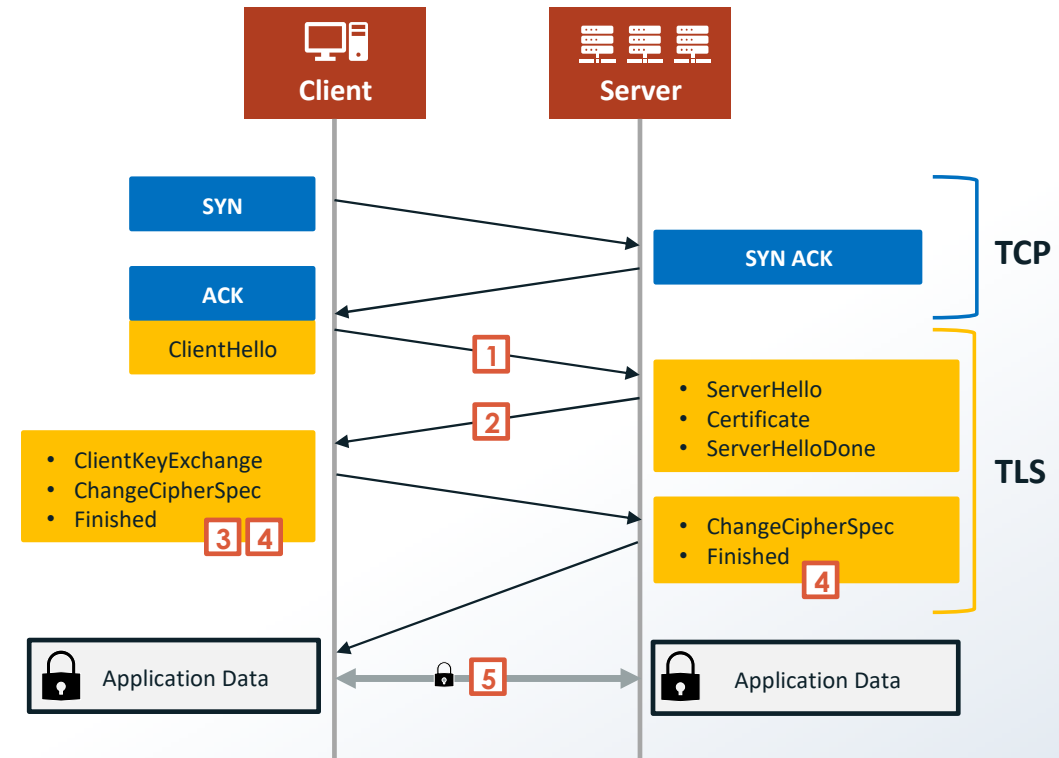
	Claims	35 USC §	References
1	1, 24, 25	103	Buruganahalli
2	1, 24, 25	103	Buruganahalli, Baehr

Technology Tutorial: Encrypted Traffic

Transport Layer Security (TLS) Protocol

1. Client initiates handshake with Server with “hello” message
2. Server responds with “hello” message and its digital certificate
3. Client validates certificate
4. Client-Server key exchange
5. Secure session begins.
Network traffic encrypted and decrypted using agreed-upon session keys

(Goodrich Decl., ¶ 32-33)



'856 Patent: Overview

- **PROBLEM:** Detecting cyberattacks in encrypted traffic
- Contemporaneous patent filings discuss the problem:

“When data on a network is encrypted (e.g., by SSL or TLS)... organizational policies cannot be applied since the data within the encrypted traffic is protected causing security functions to fail as they cannot inspect the data.”

U.S. Patent Pub. 2014/0317397 (Ex. 2005), ¶ [0018]

- Competitors (e.g., Cisco) considered this problem “unsolveable” at the time the invention was made

“a network security challenge previously thought to be **unsolveable**... to detect known attack signatures even in encrypted traffic...”

Cisco Press Release (2017) (Ex. 2013) at 1

POR 3-4, 14-15; Ex. 1001 at 1:17-18; Goodrich Decl. ¶ 31

'856 Patent: Overview (cont.)

● CONVENTIONAL APPROACH:

UNDISPUTED

● Firewalls decrypted encrypted packets using man-in-the-middle techniques

● Seen in Buruganahalli and other patent references

“a trusted man-in-the-middle technique that can be used for intercepting and decoding encrypted tunneling communications to further monitor such traffic in clear text (e.g., unencrypted)”

Buruganahalli (Ex. 1004) at 11:62-65

“use of man in the middle decryption based on rules indicating which destinations should be decrypted and which should be passed directly to the Internet destination”

U.S. Patent Pub. 2014/0317397 (Ex. 2015), ¶ [0019]

POR 3-4, 14-15; Ex. 2005 at ¶ [0019]; Ex. 2015 at 2:47-59; Goodrich Decl. ¶ 31

'856 Patent: Overview (cont.)

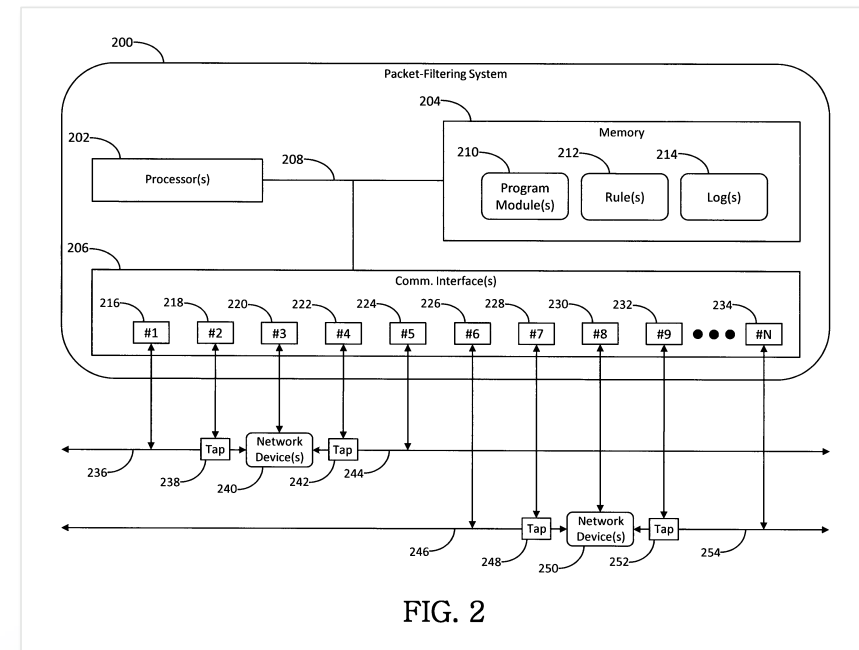
SOLUTION:

- Rule-based network-threat detection is performed on encrypted traffic without decryption.

ADVANTAGES:

UNDISPUTED

- Updated rules can be applied
- Can end a secure session that is later deemed a threat
- Can allow a secure session to pass through without further processing if rule update says not a threat



'856 Pat. at 11:2-6, 14:19-16:26, 22:20-51; POR at 14-15

'856 Patent: Claim 1

1. A method comprising:

- 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;
- identifying packets comprising unencrypted data;
- identifying packets comprising encrypted data;
- 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;
- 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:
 - 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
 - the determined packets comprising the encrypted data that corresponds to the one or more network-threat indicators; and
- 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.

Buruganahalli Does Not Teach Filtering Encrypted Data Packets Based on the Claimed Packet-Filtering Rules

The Claims Require Filtering Encrypted Data Packets Based on Certain Packet-Filtering Rules

1. A method comprising: [...]

- **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;
- **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:
- 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
- **the determined packets comprising the encrypted data** that corresponds to the one or more network-threat indicators; ...

Certain Packet-Filtering Rules

Separate from the **determining** step and the filtering unencrypted packets step

Buruganahalli (Ex. 1004): Overview

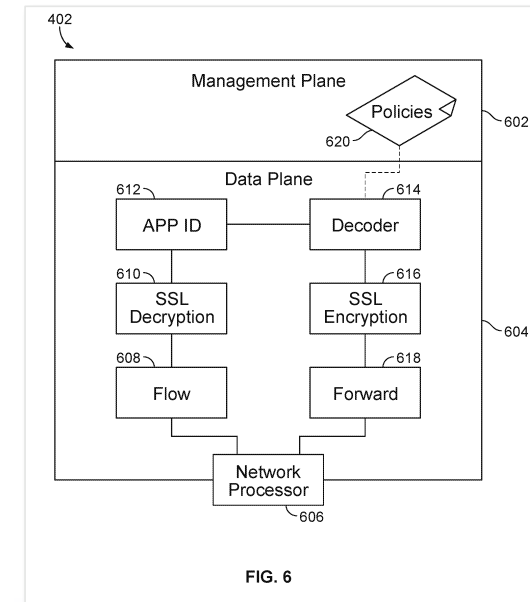
- Extracts the destination domain from an unencrypted client hello message of the TLS protocol

(Ex. 1004 at 4:45:51; POR 4-5)

- Buruganahalli's firewall uses the destination domain name when filtering unencrypted packets according to a whitelist/blacklist policy (Ex. 1004 at 7:12-51)

UNDISPUTED

- Buruganahalli teaches three scenarios for whitelisting and blacklisting (Figs. 3A-B)



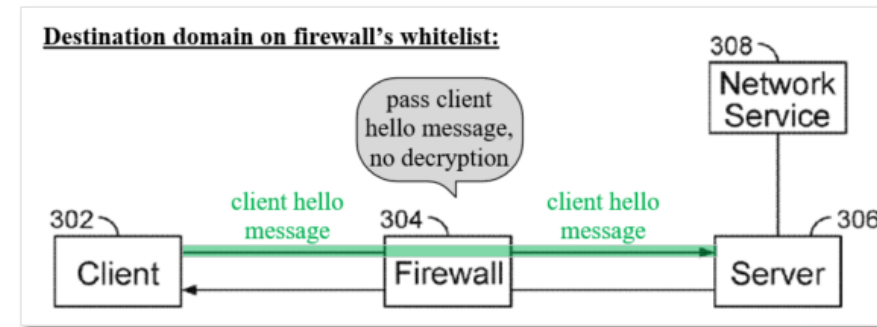
Buruganahalli only applies the alleged relevant rules to **unencrypted** packets or **decrypted** packets – never to encrypted packets.

Scenario 1: Buruganahalli's Fig. 3A Whitelist

Scenario 1 (Whitelist):

Its **Fig. 3A** Embodiment allows an encrypted session with no filtering of encrypted packets

- Petitioner does not rely on this whitelist scenario in their Petition (*Pet. 38-39, 29-30, 32-34; POR 49*)
- Whitelist embodiments are irrelevant because whitelisted domains are admittedly not network-threat indicators (*Ex. 1004 at 5:43-51, 6:1-11, 7:52-59, 10:54-11:6, 16:35-41, Fig. 3A; Goodrich Decl. at ¶ 43, 106; POR 5*)
- Encrypted packets are not subject to any rule-based filtering, only flow processing (*Ex. 1004 at 5:43-51, 5:64-6:11, 7:52-59, 10:54-11:19, 16:35-41; Goodrich Decl. at ¶ 43; POR 5*)
- Whitelisted encrypted packets are never decrypted, which is a necessary part of Petitioner's arguments for the routing step (*Goodrich Decl. at ¶ 43; POR 5*)



Ex. 1004 at Fig. 3A (annotated); POR 5

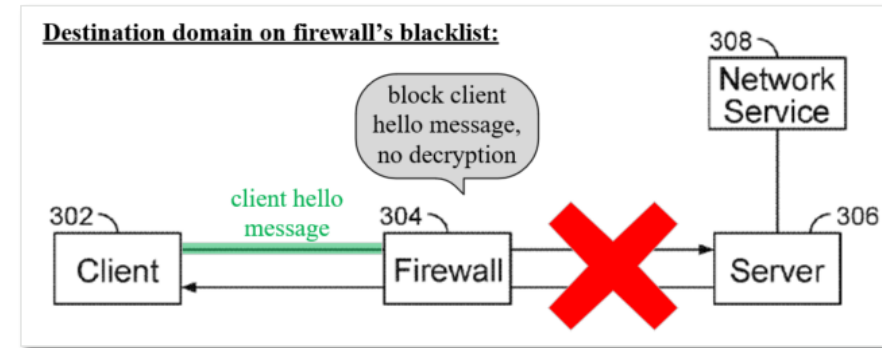
Ex. 1004 at 5:43-51, 5:64-6:11, 7:52-59, 10:54-11:19, 16:35-41; Goodrich Decl. at ¶43-45; Weissman Tr. (Ex. 2027) at 41:14-43:10; POR 5-7, 35, 37-40; Sur-Reply 2

Scenario 2: Buruganahalli's Fig. 3A Blacklist

Scenario 2 (Blacklist):

Its **Fig. 3A** Embodiment blocks a nascent encrypted session before any encrypted packets are even received

- The Board misapprehends this passage in their institution decision (not relied on by the Petition): (DI 71; POR 37-38)



Ex. 1004 at Fig. 3A (annotated); POR 6

“... 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.**”

Ex. 1004 at 11:7-19

Ex. 1004 at 5:43-51, 5:64-6:11, 7:52-59, 10:54-11:19, 16:35-41; Goodrich Decl. at ¶43-45; Weissman Tr. (Ex. 2027) at 41:14-43:10 (explaining the FIG. 3A whitelist/blacklist embodiment, where whitelisted packets are passed through and blacklisted packets cause the session to be blocked before any encrypted packets are received); POR 5-7, 35, 37-40; Sur-Reply 2

Scenario 2: Buruganahalli's Fig. 3A Blacklist (cont.)

- Buruganahalli: the “typical firewall” in **Fig. 3A** “typically **cannot decrypt** the encrypted secure tunnel session traffic and, thus, cannot detect such firewall policy/rule violation(s).”

(Ex. 1004 at 11:4-6, 10:57-61)

- Buruganahalli's solution to this problem:

- Determine whether a new flow “violate[s] a policy **prior to** the set-up of the encrypted data communications” and “as early as possible” *(Ex. 1004 at 5:65-66, 4:23-26)*

- Then the “flow can be blocked and **decryption is not required**” *(Ex. 1004 at 5:67-6:1)*

“... 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.**”

Ex. 1004 at 11:7-19

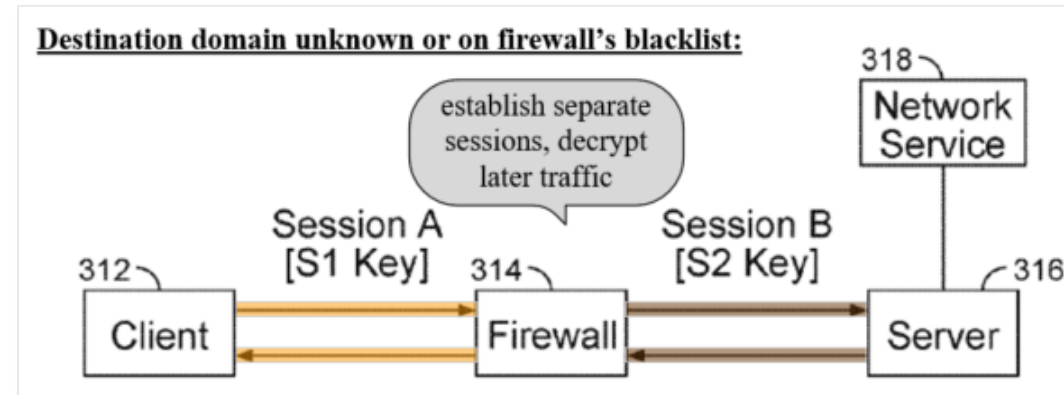
POR 37-40; Sur-Reply 11-12, 14

Scenario 3: Buruganahalli's Fig. 3B Blacklist

Scenario 3 (Blacklist):

Its **Fig. 3B** Embodiment requires encrypted packets to be decrypted before applying any packet-filtering rules

- Board agreed Fig. 3B does not involve the claimed filtering of encrypted packets (DI 70-71; POR 37)



Ex. 1004 at Fig. 3B (annotated); POR 8

Ex. 1004 at 6:12-38, 7:60-67, 8:25-44, 11:59-12:64; Goodrich Decl. at ¶ 46-50; POR 7-11, 33-40

Scenario 3: Buruganahalli's Fig. 3B Blacklist (cont.)

- Buruganahalli says nothing about combining Figs. 3A and 3B to perform the claimed rule-based filtering of encrypted packets:

“In addition, various techniques for intercepting and decoding encrypted tunneling communications from a client to a remote server are disclosed herein. For example, a trusted man-in-the-middle technique that can be used for intercepting and decoding encrypted tunneling communications **to further monitor such traffic in clear text** (e.g., unencrypted) is described below with respect to **FIG. 3B**. These decryption techniques can be used in addition to and/or in combination with the various techniques described herein for destination domain extraction for secure protocols to further enhance the various security and firewall related techniques disclosed herein.”

Ex. 1004 at 11:62-65

- Instead, Buruganahalli describes the FIG. 3B embodiment as an extension of the FIG. 3A embodiment that is used when necessary "to further monitor such traffic in clear text.”

POR 42-44; Sur-Reply 12-16

Petitioner's Shifting Argument

- The original Petition argued:

“Buruganahalli discloses that the encrypted data communications are filtered based on data specified in the firewall policies/rules described above. Buruganahalli, 4:16-22”

Pet. 38

“However, secure protocols can be used to evade detection by security devices, such as firewalls, by encrypting data communications between a client and a remote server (e.g., an external site, such as a remote web site/web service). As a result, techniques for decrypting such secure communications are needed in order to monitor such encrypted data communications and to apply filtering based on a policy.”

Ex. 1004 at 4:16-22

- But the cited portion is clear that decryption is needed to monitor encrypted packets

Pet. 38 (citing Ex. 1004 at 4:16-22, 4:31-44, 6:62-7:9, 7:12-29, 7:39-51, 7:60-67, 15:4-21); POR 40-41; Sur-Reply 5-8

Petitioner's Shifting Argument (cont.)

- **In Reply**, Petitioner now points to steps that occur before decryption:
 - (i) handshake processing + (ii) later flow lookup on encrypted packets

“Those encrypted packets are filtered based on the earlier handshake processing of unencrypted data”

Reply 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”

Reply 3

“The decision to pass, block, or route for decryption an encrypted packet is a filtering step performed on that packet.”

Reply 5

POR 40-41; Sur-Reply 5-8

Petitioner's Shifting Argument Fails

UNDISPUTED

- Uncontested evidence shows Buruganahalli's handling of encrypted packets is based on matching **IP address and port number** during flow lookup
- Petitioner's own expert admits this:

Expert: When an encrypted packet is received, Buru runs a rule that will basically look up this packet in the table and make a check whether there's a correlation from this packet, and a domain that is in this table, which means it's blacklisted, or not.

Q: What information is correlated from the encrypted packet to make that determination? [...]

Expert: Buru uses the IP address and port.

Ex. 2027 at 28:18-35:25

POR 31-33, 40-44, 8-10; Sur-Reply 7-8; Ex. 1004 at 13:60-65

Board's Preliminary Findings

- Board's Joinder Institution Decision misapprehends this passage:

“... Flow 608 identifies the packets as being part of a new session and creates a new session flow. Subsequent packets will be identified as belonging to the session based on a flow lookup. As described herein, an initial TLS handshake exchange of that flow can be parsed to extract a hostname to facilitate destination domain extraction for secure protocols (e.g., and to apply one or more policies if applicable based on the extracted destination domain) using 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...”

Ex. 1004 at 14:24-38

- **BUT:** The Petition relies solely on the extracted domain embodiments, so the decryption would not be “omitted”
- **ALSO:** If decryption is “omitted,” then Buruganahalli would not route packets to alleged proxy as per the rest of invalidity theory

Paper 39 at 24-26; Paper 48 at 9-12

Board's Preliminary Findings (cont.)

- Board's Joinder Institution Decision:

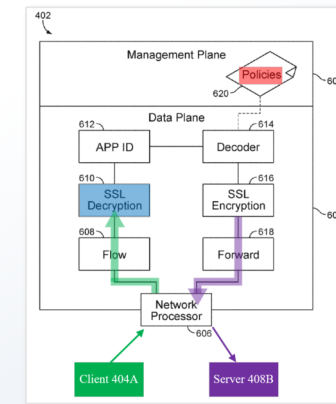
Filtering by applying policies occurs after determining “which flow the packet belongs to based on the ‘IP address and port number.’”

Paper 39 at 25 (citing DI 66-67, 69-71)

- BUT:** there is no intermediate step of rule-based filtering between Buruganahalli's flow processing and decryption of encrypted packets

“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”

Ex. 1004 at 12:29-32



Ex. 1004, Fig. 6 (annotated); Goodrich Decl., ¶ 79-82; POR 33-34, Sur-Reply 9-10; Fig

Board's Preliminary Findings (cont.)

- The Board also found in the Joinder Institution Decision:

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.

Paper 39 at 21 (citing Ex. 1003 ¶¶ 109, 134–135)

- **BUT:** the citations fail to support this position

See Ex. 1003 ¶¶ 109, 134–135.

Discussing a whitelist/blacklist policy based on domain names, but not asserting any encrypted packets are subject to filtering based on the domain name prior to decryption

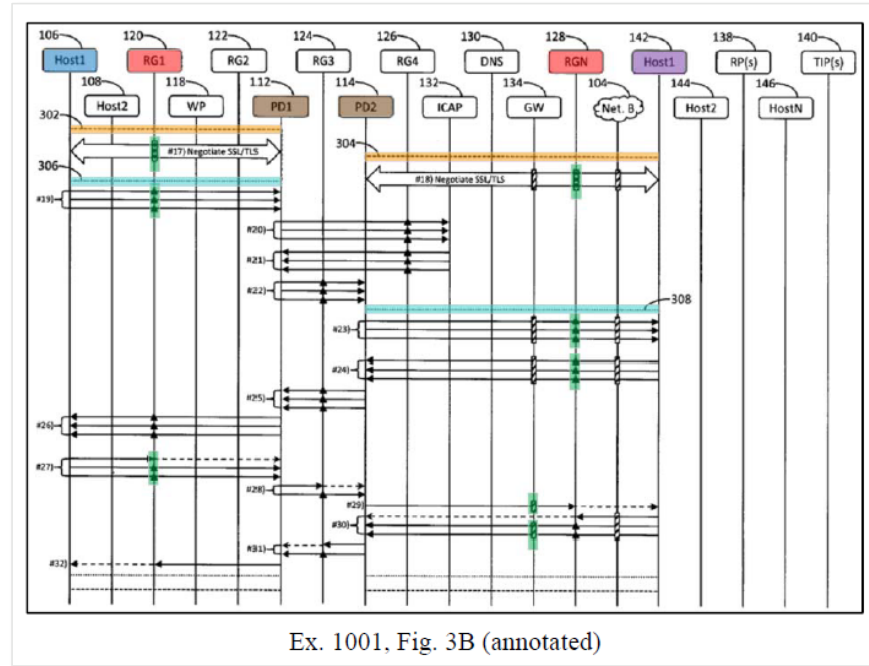
Providing string of citations to Buruganahalli that disclose applying policies to encrypted traffic only after decryption

- Petitioner has not identified a single instance where Buruganahalli teaches filtering encrypted packets based on the claimed packet-filtering rules

Paper 48 at 7-8

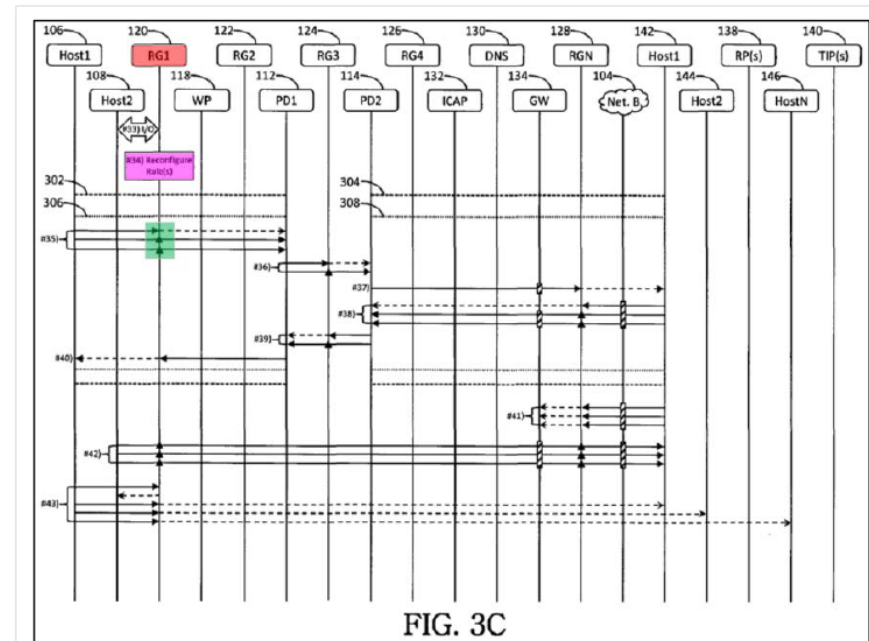
Buruganahalli's Technique Is Not the Same as the Claimed Embodiment

- Figure 3B of the '856 Patent illustrates the two distinct filtering steps
- Consistent with the claims, the spec and drawings disclose a step of rule-based filtering unencrypted packets (e.g., step #17) and then additional, separate steps of rule-based filtering encrypted packets (e.g., steps #19 and 27)
- Buruganahalli does not have steps like #19 or #27



Buruganahalli's Technique Is Not the Same as the Claimed Embodiment (cont.)

- Figure 3C of the '856 Patent shows another step of rule-based filtering encrypted packets (step #35) in addition to and separate from the step of rule-based filtering unencrypted packets (e.g., step #17).
- Note: Step #35 comes after rules are reconfigured at step #34 so it can advantageously apply updated rules to the ongoing encrypted session.
- Buruganahalli does not have a step like #35 either.



Ex. 1001, Fig. 3C (annotated)

(POR 14-15, 19-20, 22-23; Sur-Reply 8-9)

Buruganahalli Does Not Teach Network-Threat Indicators

All Claims Require Network-Threat Indicators

1. A method comprising:

- 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**;
- identifying packets comprising unencrypted data;
- identifying packets comprising encrypted data;
- 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**;
- 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:
- 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
- the determined packets comprising the encrypted data that corresponds to the one or **more network-threat indicators**; and
- 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**.

Claim Construction: “network-threat indicators”

- Petitioner fails to address prior claim construction under *Phillips* standard

District Court’s Construction	Petitioner’s 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

POR 28-29; Sur-Reply 16-17; Ex. 1027 at 39

Buruganahalli Does Not Teach Network-Threat Indicators

- Petitioner points to the destination domains on Buruganahalli's blacklist for "network-threat indicators" *(Pet. 29-30, 32-34; POR 49-51)*
- **BUT:** Buruganahalli's blacklist is simply a list of domains that a network administrator has identified for monitoring or blocking
- Even Petitioner's Expert characterized Buruganahalli's blacklist as a list of domains that represents merely **potential** threats:

Q: [M]y question is, does the fact that a URL or URI is on a blacklist necessarily mean that that URL or URI has been determined to be associated with a network threat?

A: ... 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. ...

Ex. 2027 at 60:12-22; see also id. at 59:15-22

Buruganahalli Does Not Teach Network-Threat Indicators (cont.)

- **Reply Arg:** destination domain on the blacklist is “not trusted” (Reply 14; Ex. 1004 at 9:67-10:4)

- **BUT:** the full quote is:

“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).”

Ex. 1004 at 9:67-10:4

- **ALSO:** Petitioner’s own evidence discloses all Internet traffic is considered untrusted

“It is now an accepted fact that the Internet is a vast network of **untrusted** and potentially malicious machines”

“the Internet is considered an **untrusted** zone”

Ex. 1052 at 21

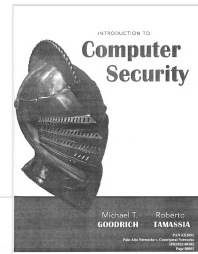
- Buruganahalli's blacklist is used to identify all domains that are not fully trusted, not those known to be associated with network threats (Ex. 1025 at 21)

(POR 50; Sur-Reply 17-18)

Buruganahalli Does Not Teach Network-Threat Indicators (cont.)

- Petitioner belatedly cites PO's expert Dr. Goodrich's textbook

(Reply 14; Ex. 1052 at 22)



Blacklists and White Lists

There are two fundamental approaches to creating firewall policies (or *rule-sets*) to effectively minimize vulnerability to the outside world while maintaining the desired functionality for the machines in the trusted internal 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.

- **BUT:** Petitioner did not bother to present this evidence to Dr. Goodrich before/during his deposition
- **ALSO:** Passage describes the “blacklist approach” as a “default-allow ruleset” that allows all packets “except those that fit the rules defined specifically in a blacklist.”

(Sur-Reply 18-19)

Buruganahalli and Baehr Do Not Teach Routing to a Proxy System

'856 Patent: Claim 1

1. A method comprising: [...]

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.

Claim Construction: “proxy system”

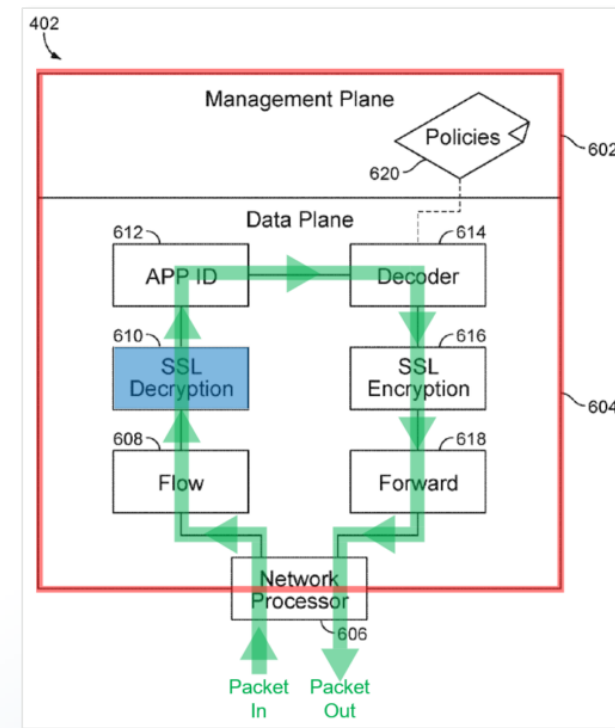
- Petitioner fails to address prior claim constructions under *Phillips* standard

District Court Construction	Petitioner’s Construction
A proxy system which intervenes to prevent threats in communications between devices	Nothing

POR 28-29; Sur-Reply 20-24; Ex. 1027 at 39

Buruganahalli Does Not Teach Routing to a Proxy System

1. Petitioner equates Buruganahalli's "decrypt engine" with "proxy system" (*Pet. 39*)
 - **BUT:** the decrypt engine (610) performs one step (decryption) of the firewall's own filtering process without "interven[ing[] to prevent threats in communication between devices"
2. Petitioner argues Fig. 3B for disclosing proxy-like functionality (*Pet. 39*)
 - **BUT:** the Board has recognized Fig. 3B cannot satisfy the challenged claims because it decrypts encrypted packets before applying any firewall policies/rules (*DI 70-71*)



POR 53-55; Sur-Reply 21-22; Ex. 1004 at Fig. 6 (annotated)

No Motivation to Combine Buruganahalli/Baehr

- Petitioner's fallback argument (Ground 2) is a combination with Baehr *(Ex. 1005)*
- **BUT:** Petitioner fails to provide a persuasive reason to combine with Baehr
 - There is no isolation advantage over Buruganahalli *(POR 61; Ex. 1004 at 12:4-55, Goodrich Decl. at ¶ 126)*
 - Buruganahalli's firewall already provides seamless communication with the server as if it was communicating with the client *(POR 61; Ex. 1004 at 12:4-55, Goodrich Decl. at ¶¶ 126-27)*
 - Minuscule or nonexistent load reduction if proxy function handed off
(POR 62-63; Ex. 1005 at 4:20-63, Goodrich Decl. at ¶¶ 128-29)
 - Petitioner's Ex. 1036 does nothing to show how the combination would "preserv[e] computing resources," "achiev[e] load balancing," or "maximiz[e] performance"
(POR 63-65; Goodrich Decl. at ¶¶ 130-36)
- Petitioner failed to rebut these criticisms in its Reply *(Reply 21-23)*

POR 55-67; Sur-Reply 22-24

Objective Evidence of Nonobviousness

- Cisco Press Release (Ex. 2013) demonstrates long-felt need and industry praise of their copied Encrypted Traffic Analysis product
- Acknowledged the problem of rule-based detection of threats in encrypted traffic as a “a network security challenge previously thought to be unsolveable”
- “identify[ing] the fingerprints of known threats even in encrypted traffic, without decrypting it and impacting data privacy” *(Ex. 2013 at 1)*
- District Court’s opinion (Ex. 1027), while vacated, still provides underlying evidence of copying, including when Centripetal disclosed its technology to Cisco and when Cisco launched an infringing product *(Ex. 1029 at 31:7-32:3; Ex. 2016 at 258:21-25, 260:2-18; Ex. 2017 at 1128:8-1129:5; Ex. 2018 at 1220:1-1222:25)*

POR 67-70; Sur-Reply 24-26; Ex. 1027 at 149-152, 155-157, 160

Extra Slides

'856 Patent: Claim 24

24. A packet-filtering system comprising:

- at least one hardware processor; and
- memory storing instructions that when executed by the at least one hardware processor cause the packet-filtering system to:
 - receive data indicating a plurality of network-threat indicators, wherein at least one of the plurality of network-threat indicators comprise a domain name identified as a network threat;
 - identify packets comprising unencrypted data;
 - identify packets comprising encrypted data;
 - determine, 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;
 - filter, based on at least one of a uniform resource identifier (URI) specified by a 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:
 - packets comprising the portion of the unencrypted data corresponding to one or more network-threat indicators of the plurality of network-threat indicators; and
 - the determined packets comprising the encrypted data that corresponds to the one or more network-threat indicators; and
- 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.

'856 Patent: Claim 25

25. One or more non-transitory computer-readable media comprising instructions that when executed by at least one hardware processor of a packet-filtering system cause the packet-filtering system to:

- receive data indicating a plurality of network-threat indicators, wherein at least one of the plurality of network-threat indicators comprise a domain name identified as a network threat;
- identify packets comprising unencrypted data;
- identify packets comprising encrypted data;
- determine, 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;
- filter, by the packet-filtering system and based on at least one of a uniform resource identifier (URI) specified by a

plurality of packet-filtering rules indicating one or more of the plurality of network-threat indicators, 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:

- packets comprising the portion of the unencrypted data corresponding to one or more network-threat indicators of the plurality of network-threat indicators; and
- the determined packets comprising the encrypted data that corresponds to the one or more network-threat indicators; and
- 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.