

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

PALO ALTO NETWORKS, INC., CISCO SYSTEMS, INC.,
and KEYSIGHT TECHNOLOGIES, INC.,
Petitioner,

v.

CENTRIPETAL NETWORKS, L.L.C.,
Patent Owner.

IPR2022-00182
Patent 9,917,856 B2

Record of Oral Hearing
Held: February 15, 2023

Before MICHELLE N. WORMMEESTER, NABEEL U. KHAN, and
AARON W. MOORE, *Administrative Patent Judges*.

APPEARANCES:

ON BEHALF OF THE PETITIONER:

SCOTT A. MCKEOWN, ESQ.
Ropes & Gray, LLP
2099 Pennsylvania Avenue, N.W.
Washington, D.C. 20006

ANDREW RADSCH, ESQ.
Ropes & Gray, LLP
1900 University Avenue, 6th floor
East Palo Alto, CA 94303

ON BEHALF OF THE PATENT OWNER:

JAMES HANNAH, ESQ.
Kramer, Levin, Naftalis & Frankel, LLP
333 Twin Dolphin Drive
Suite 700
Redwood Shores, CA 94065

The above-entitled matter came on for hearing, by video, on
Wednesday, February 15, 2023, commencing at 1:00 p.m., EDT, at the U.S.
Patent and Trademark Office.

1 PROCEEDINGS

2 - - - - -

3 JUDGE MOORE: Good day everyone. Welcome to the
4 Board. We are here for hearing in the matter IPR 2022-00182.
5 The case is now captioned Palo Alto Networks, Cisco Systems
6 and Keysight Technologies v. Centripetal Networks. I'm APJ
7 Moore. APJ's Wormmeester and Khan are also present by video.

8 Can we have appearances for the Petitioner, please?

9 MR. MCKEOWN: Good morning, Your Honors, Scott
10 McKeown of Ropes & Gray for Petitioner Palo Alto Networks.
11 I'm joined today by Andrew Radsch in our Palo Alto office and
12 James Batchelder as well.

13 JUDGE MOORE: Thank you. And for Patent Owner.

14 MR. HANNAH: Good morning or good afternoon, Your
15 Honor. This is James Hannah on behalf of Centripetal Networks
16 and with me is Jeff Price and on the line are some client
17 representatives including our chief operating officer and our
18 chief technical officer, so Jonathan Rogers and Sean Moore.

19 JUDGE MOORE: Thank you. So our primary concern
20 today is that we preserve your right to be heard in this hearing so
21 if at any time you encounter a technical problem that affects your
22 ability to participate, please let us know immediately. I'll ask
23 you to identify yourself for the court reporter each time you
24 begin speaking and also when you're not speaking that you mute
25 your connection. Also when referring to demonstratives, papers
26 or exhibits please be sure that you identify the item for the

1 record. I'll also note that this hearing is open to the public, and
2 that our Hearing Order granted each side 60 minutes. I will keep
3 the time on my end. I will ask you to let me know at the
4 beginning of your arguments if you wish to reserve time for
5 rebuttal and Petitioner, you may begin when you're ready.

6 MR. MCKEOWN: Thank you, Your Honor. I'll reserve 20
7 minutes for rebuttal and Andrew Radsch of our Palo Alto office
8 will take the podium for rebuttal.

9 So, again, good afternoon. Scott McKeown of Ropes &
10 Gray for Petitioner Palo Alto Networks. I appreciate the panel's
11 continued attention to this matter.

12 May it please the Board, the issues to be discussed here
13 today are the fifth presentation of the Patent Owner's argument
14 once on institution, once on rehearing, twice in different joint
15 hearing decisions, all of which failed. The decision here should
16 be the same based upon the same straightforward reasoning
17 throughout this record.

18 I know the panel is up to speed on the technology but I'll
19 turn very briefly to it and the claim language just so we have a
20 common foundation for the discussion today, and I would ask
21 you to start with Petitioner's slide No. 2.

22 So you'll see on slide No. 2 there is (audio interference)
23 this patent with some specification excerpts off there to the right
24 and what you can see starting with step 702 is there are what are
25 identified as network-threat indicators that are provided to the
26 system's packet filtering system. These network-threat

1 indicators are provided by vendors, well known services and
2 indicators which identify such things as domain names, for
3 example, such that packet filtering devices in step 704 can
4 configure packet filtering rules and identify packets based upon
5 what is described here as unencrypted data.

6 So in a secure communication the way that communication
7 is set up is there are some handshake messages that come
8 through. These are not encrypted. If you look into the packets
9 of those handshake messages, and this is the red underlined text
10 on the right hand side you can get some information from those
11 packets such as domain names. So once you have that domain
12 name you can then apply that to your filtering rules as you see fit
13 based upon what you want to do with that traffic in accordance
14 with your rules, and towards the bottom of figure 7 you can also,
15 as the encrypted packets start to come in on the same session,
16 correlate them to the information that was provided ahead of
17 time in the handshake message.

18 So you know something about the encrypted packets despite
19 needing to encrypt them otherwise to see the contents as to
20 where at least they're supposed to be going. So that's, you
21 know, at a high level the general idea behind the '856 patent is
22 to take this plain text data that's in the handshake message,
23 extract it and use it for filtering purposes and, again, by
24 correlation you can then indirectly operate on the encrypted
25 packets as well without decrypting them.

26 Turning to Petitioner's slide 3. Nonetheless, there is

1 decryption described in the '856 patent. It's not claimed; right?
2 All that's claimed, and we'll get to the claim language on the
3 next slide, is this idea of taking that plain text data out of the
4 handshake message and using it for filtering and then sending
5 traffic to a proxy. But at the same proxy in the '856 patent there
6 is decryption and it's for such things as scanning for viruses,
7 detecting for malware, et cetera. Just put a pin in that for a
8 moment. Again, not relevant to the claims because we just have
9 to get the traffic to the proxy, but it is relevant to the disputed
10 issues here.

11 So then I'll turn to slide 4. This is claim 1 of the '856
12 patent. We have highlighted in yellow some of the claim terms
13 and features that have been discussed in the briefing. So you'll
14 see network-threat indicators there. There's an argument about
15 the meaning of that. I will discuss that very briefly as regardless
16 of meaning the prior art would meet it in any event. So most of
17 what I'll be talking about is the filtering steps highlighted here
18 and how those packets are determined, those encrypted packets
19 are determined based upon that extracted domain name of the
20 unfiltered packets.

21 So slide 5 of Petitioner's slide deck. You see figure 3A.
22 This is the, what I'll call the Buruganahalli reference. I'm
23 probably butchering that name but that's the way it falls off my
24 tongue. Figure 3A is a domain extraction process. So you see
25 the yellow highlighted text underneath this figure. The initial
26 handshake comes in, right, same idea. Secure session is being

1 set up. We get some handshake data coming in. We can extract
2 a domain name from that plain text data without having to
3 decrypt as shown in the red underline on the rightmost passage
4 because we've gotten it from the unencrypted packet. So we
5 know where the encrypted packets are headed, just like the '856
6 patent does.

7 Then we go to figure 6 which shows on the lefthand side
8 that domain extraction technique. On the righthand side figure
9 3B is showing how data can be filtered based upon that
10 extraction and sent to a proxy. The grounds present these figures
11 in combination. So we see that Buruganahalli also provides a
12 proxy . The word proxy does not appear in Buruganahalli but
13 nevertheless we see all the features of a proxy described here and
14 that would be, for example, the language about underlined on the
15 first yellow highlighted trusted man-in-the-middle. On the other
16 side we have that the encryption functionality here is transparent
17 to the client and it's isolating that encryption, or decryption
18 rather -- excuse me.

19 JUDGE MOORE: Mr. McKeown?

20 MR. MCKEOWN: Yes.

21 JUDGE MOORE: Where exactly is the filtering taking
22 place in there?

23 MR. MCKEOWN: So the filtering is -- we have the
24 handshake come in; right? We filter the unencrypted packets for
25 the domain name and then there's a process that I'll describe
26 later, but there is a correlation with that traffic. So the way it

1 works, the handshake message comes in. We extract the domain.
2 The encrypted traffic comes in. We look at the encrypted traffic,
3 in particular its network address. We compare it to a look-up
4 table to see if it's in the blacklist and if it is, we can do one of
5 two things. We can either block it all together or we can decide
6 to forward it on to the proxy for decryption and the way that
7 that's done is through this determination step of, okay, we have
8 an encrypted packet, it has a network address. Let's look and
9 see what we did with our previous handshakes. Oh, it's on the
10 list. Let's send it to the proxy. So that's how you use the
11 domain that's been extracted from the unencrypted packets to
12 filter the encrypted packets.

13 JUDGE MOORE: Are you filtering individual packets or
14 are you filtering a session or a flow?

15 MR. MCKEOWN: It's on a packet-by-packet basis so it's
16 individual packets.

17 JUDGE MOORE: Okay.

18 MR. MCKEOWN: Each packet, because the packets come
19 in out of order; right? So different flows are coming in and as
20 each packet is coming in we're doing the look-up.

21 JUDGE MOORE: Well they do, but they come in in a
22 different order; right? But each packet comes in, you haven't
23 done anything with it yet, right, you've just looked at it. So
24 where is the filtering?

25 MR. MCKEOWN: Well, so the encrypted packet comes in
26 and we decide what to do with it which is essentially the

1 filtering. Like I said, we could block it all together or we can
2 decide to send it on to the proxy depending upon the policies that
3 are in the filtering device. So in this case if we have a domain
4 that's on the blacklist, we have that flow in our table, that
5 encrypted packet comes in. We match it up. We see it, oh, it
6 correlates to the black list. In this case we're going to route it to
7 the proxy for decryption. So that's the filtering.

8 JUDGE MOORE: So the whole flow gets routed to the
9 proxy, not just individual packets?

10 MR. MCKEOWN: Well, individual packets of the flow. If
11 the individual packets are coming in with the network address on
12 them they'll be associated with that domain name that's in the
13 table and then they're routed accordingly.

14 JUDGE MOORE: Okay.

15 MR. MCKEOWN: So getting back to Buruganahalli.
16 That's how Buruganahalli works and I'll just preview the
17 arguments for later. That's also how the '856 patent works. The
18 '856 patent also does a correlation and a look-up on a packet-by-
19 packet basis.

20 So just closing up the discussion of Buruganahalli, we have
21 the same domain extraction; right? We have encrypted packets
22 coming in. We look them up on the same basis. We say, oh,
23 we've got a match here in our table. In the case of the '856 it's
24 a log and then based upon that we can decide to route it to the
25 proxy.

26 But just closing out the proxy issue. Buruganahalli does

1 not use the word proxy but it teaches a proxy to one of ordinary
2 skill in the art because of the features highlighted on this page,
3 it's a trusted man-in-the-middle. It's transparent to the end
4 points. It's doing the processing that the host would otherwise
5 do in an isolated environment so that we can figure out if this
6 traffic is harmful for the host before we send it on to the host.
7 So that's at Petitioner's slide 6.

8 And then on slide 7 we get to the decrypting which is the
9 point of most of the briefing and you'll see underlines here on
10 Petitioner's slide 7 about further potential filtering, further
11 decrypting, because the filtering's already done. By the time
12 you get to the decrypter you've been routed because that's the
13 only way you can get there; right? You have to be on a black list
14 and you have to do the determination, just like in the claims, and
15 you get to the decrypter by routing. That's the only way those
16 packets get there.

17 So, again, and this will go back to the decryption point I
18 made earlier about the '856 patent to put a pin in it. It's doing
19 decryption at the same time in the process for the same reason;
20 right? Once you get this traffic, you've identified it based upon
21 the threat-indicator, in this case the domain name, and you
22 decide to send it to the decrypter for further filtering or further
23 security review. In the case of the '856 it's looking for viruses
24 and decrypting for whatever other reasons it wants to decrypt.
25 But the high level takeaway here is the '856 choosing the exact
26 handshake process for unencrypted packets. It's doing a

1 correlation for the encrypted packets to determine if they
2 correspond to the threat indicator and based upon that
3 correlation, is routing it to the proxy. The fact that there's
4 decryption in both of these references later on down the line is
5 irrelevant to these claims.

6 And again, I would just highlight the reason Burgunahalli is
7 presented as a 103 and not a 102 is for the mere absence of the
8 word proxy in that reference. All of the features of the proxy are
9 nonetheless taught, so just emphasizing there how close this
10 reference really is to the claims, exact same process, exact same
11 look-ups, exact same claim text, exact same routing for the exact
12 same reasons at the exact same points in time.

13 JUDGE MOORE: Do we need to construe proxy?

14 MR. MCKEOWN: I don't believe so, Your Honor. The
15 main difference between the two parties is Petitioner just said,
16 well, proxy is well known. It doesn't need any special
17 construction. The Patent Owners have argued that, well, proxy
18 has to intervene so that seems to be the point of distinction but
19 in this case certainly the proxy intervenes; right? It's decrypting
20 the traffic before it gets to the host because that's the entire
21 point to isolate it and to be transparent to the end points and be
22 the middle man. So regardless of what the construction would be
23 whether intervening is added or not, the prior art would meet it
24 in any event.

25 JUDGE MOORE: Is the Baehr reference in the case -- in
26 case a proxy needs to be a separate system? Is that why Baehr's

1 involved?

2 MR. MCKEOWN: Right. So, and that's what I was getting
3 to on slide 8. So the Baehr reference is teaching a proxy in the
4 same field of endeavor and what we've said in the grounds as
5 well to the extent that for some reason the teaching in
6 Buruganahalli of a proxy is somehow deficient is what we said as
7 well. You know, proxies are well known and have well known
8 uses and functionality. Baehr demonstrates that in addition to a
9 number of other references that are cited throughout the briefing
10 and that one of skill in the art to the extent that Buruganahalli
11 didn't disclose a proxy would be motivated to include one for all
12 of the known benefits off-loading that decryption from the
13 firewall in the case that you wanted the proxy to be separate, for
14 example. So all of that is in the record, but the claims just
15 require a proxy, they don't require the proxy to be separate or
16 software or hardware, so the Baehr reference is just pointing out
17 that this is a fundamental building block of most of these
18 systems.

19 So that's Petitioner's slide 9. Sort of highlighting
20 Buruganahalli as the 103 ground, very close to 102 but again
21 because the word proxy is not there, it's presented as a 103 and
22 then we have the Baehr as explicitly teaching a proxy to the
23 extent the Buruganahalli was somehow found to be deficient.

24 Unless there's question on that overview, I'll now get into
25 the disputed issues. So Petitioner's slide 10. We've got these
26 disputed issues outlined there. I'm going to spend most of my

1 time on issue No. 1, whether Buruganahalli teaches rule-based
2 filtering of encrypted packets. The secondary considerations and
3 the network-threat definition, I would just characterize those
4 diplomatically as unserious in my view, so I'll only briefly
5 mention those. So I'll spend most of my time on 1, and mention
6 3 as well.

7 So Petitioner's slide 12 is the relevant claim language for
8 the filtering determination. You see [1.e] filtering based upon a
9 number of options there, the first one being the URI which is
10 what the briefing is largely focused on and then [1.g], the
11 determined packets, so this is the determined packets referencing
12 element [1.d] of the claim, the encrypted data being determined
13 as in this case correlated to the unencrypted domain name, again
14 based upon a look-up just like in the Buruganahalli reference.

15 So Petitioner's slide 13 highlights the teaching in the
16 reference and some citations to the Board's previous analysis in
17 that block on the bottom of the page. I'll just read that last
18 sentence. As discussed above, Buruganahalli discloses a security
19 device inspects newly received packets on a packet-by-packet
20 basis and may No. 2, "filter a newly received packet with
21 encrypted data destined for a black listed domain by forwarding
22 it to a decryption engine without having to decrypt the encrypted
23 secure tunnel session traffic." So that's the feature that we've
24 pointed to as corresponding to the claims. There are other
25 filtering processes going on, whitelist filtering which is allowing
26 some traffic to pass through. Some blacklist where it's rejected

1 outright and then we have this blacklist in additional security to
2 policy where the blacklist is identified by extracting that domain
3 and then as the packets come in they're correlated and we know
4 from that correlation that we should then route them on to the
5 decryption.

6 Slide 14. Patent Owner seemingly concedes this on slide
7 14. You'll see the first highlighted language. Buruganahalli
8 explains that a policy may cause the firewall to initially allow a
9 session flow and then require that the session be decrypted and I
10 would note the language that follows the yellow highlight for
11 further analysis and further potential filtering. So it's already
12 been filtered and there may be additional decryption
13 functionality just as described in the '856 patent but unclaimed,
14 so these are the Patent Owner's features, not Petitioner's.

15 And then Petitioner's slide 15 we talk about the blacklist
16 functionality operating on a domain that's not in dispute either.
17 You see that, Patent Owner points out that Buruganahalli's
18 firewall uses this destination domain to apply a whitelist or
19 blacklist policy. There's no dispute about how any of that is
20 operating.

21 And again, on Petitioner's slide 16 we see the same
22 analysis from the Board in terms of agreeing with the grounds in
23 the petition, the trial grounds. The security device can be
24 configured based on a firewall policy to decrypt the monitored
25 traffic using a decrypt engine and it goes on to talk about
26 towards the end of that yellow highlight this is for further traffic

1 monitoring and inspection based upon a policy, so there again
2 this is consistent with what is shown in Buruganahalli and
3 consistent with what has been presented in the petition in the
4 trial grounds.

5 Some of the more detailed arguments from the Patent
6 Owner can be seen on Petitioner's slide 17. They take issue with
7 the look-up process, so when an encrypted packet comes in it's
8 IP address and port number are then used to index a table and
9 we've pointed out in our briefing, and what the Board has
10 pointed out where the determining -- the determining of whether
11 the encrypted packets, you know, correspond to this policy.
12 That's in step [1.d], so it's that determination that then causes
13 the later filtering and proper forwarding that packet to the proxy
14 for decryption based upon that domain name that's been
15 previously extracted in the handshake from the plain text data.

16 So slide 18. Similar, you see the Board's specific feedback
17 on the analysis of the limitations as relating to determining. We
18 have not relied on the determining as the filtering step as shown
19 in the white box there. That is the determining of how the
20 encrypted packets are related to the domain name and the
21 unencrypted handshake. The filtering is what happens as a
22 consequence of that comparison.

23 On Petitioner's slide 19 you'll see the argument that Patent
24 Owner is arguing. Neither figure 3A, the domain name
25 extraction or figure 3B, the more detailed analysis of what
26 happens to some of the blacklist packets based upon that earlier

1 extraction. Neither one in isolation teach the claimed invention
2 or they weren't presented in isolation, they were presented in
3 combination. We see the citations there from Petitioner on slide
4 19.

5 And then finally on Petitioner slide 20 you also see the
6 point, again this was made by the Board, that this argument
7 about the relevance of Buruganahalli's decryption is misplaced.
8 All the claim requires is filtering routing to a proxy. The fact
9 that there is some decryption happening later, this is a
10 comprising claim; right? The claims don't exclude steps in the
11 future.

12 So, again, what we've got here in the prior art reference is
13 filtering based upon the plain text of the handshake message for
14 the domain. We know that's the exact same thing as the '856.
15 We correlate the encrypted packet through a look-up. We know
16 that that's the same as operating in the '856 and then we route
17 encrypted packets to the proxy for the security. Security's not
18 claimed. Both routes to the proxy, both provide additional
19 security at the proxy through decryption although unclaimed. So
20 that's the grounds, that's the mapping. That's really the
21 straightforward trial ground in this case.

22 I want to make a couple of additional points here. It may
23 be helpful at this point to switch over to the Patent Owner's
24 slides. So in addition to the fact that the reference plainly
25 shows this filtering happens in the same manner as the '856
26 patent, the Petitioner perhaps recognizing this is arguing that the

1 Petitioner has shifted their arguments and you look at that first,
2 you know, reply No. 3 that the encrypted packets are filtered
3 based on the earlier handshake processing of encrypted data.
4 They claim that's shifted. In their pending rehearings they're a
5 little bit more aggressive. They claim the Board concocted this
6 argument by plumbing the record. Again, I'll just be diplomatic
7 and say that that's counter-factual and highlight a couple of
8 points in the petition itself which plainly shows these arguments
9 starting with page 25 of the petition. So the paragraph starting
10 in the middle of the page on page 25 of the petition.

11 “Although Buruganahalli does not explicitly disclose
12 ‘routing’ to a proxy system encrypted packets of a secure session
13 directed to a blacklisted domain parenthetical (after they have
14 been filtered as being part of the secure session established by
15 the initial client request), a POSITA would have understood that
16 the filtered encrypted packets (i.e., packets identified as being
17 part of a secure session) are ‘routed’ to Buruganahalli’s decrypt
18 engine.”

19 So plainly looking at the original filtering as part of the
20 secure session, and that's before we even get to the claim charts.
21 We can start at page 32 of the claim chart or element C. In the
22 middle there that first cell,

23 “A session using a secure protocol involves ‘encrypted data
24 communication’ and the determination of how to handle the
25 encrypted data communications of the session is made by
26 applying a security policy based on handshake traffic before the

1 session is set up.”

2 Page 34 on element [1.d] towards the middle of that first
3 cell. Buruganahalli teaches,

4 “Determining encrypted packets comprising data
5 corresponding to one or more network threat indicators (.e.g., a
6 blacklisted destination domain) based on, emphasis on based,
7 data included in the hello message (e.g., destination domain and
8 associated IP address) configured to establish the encrypted
9 session as both the encrypted session and the hello message
10 would be associated with the same destination IP address of the
11 remote server.”

12 So that’s talking about the look-up based upon the earlier
13 handshake and I’ll just get one or two more in the [e] element on
14 page 35, at the end of the first paragraph there.

15 “The system applies a security rule based on the destination
16 domain extracted from the request to ‘filter traffic’ from the
17 request.”

18 And then finally on page 38 towards the bottom.

19 “A POSITA would have understood that the packets
20 communicated as part of the secure session are filtered after a
21 determination of a handshake message that initiates the session
22 includes data that corresponds to the network-threat indicator
23 (blacklisted destination domain). This is because the handshake
24 message comprises data (destination domain) that also applies,”
25 emphasis there, “to the encrypted data of the session, such that
26 the security risks associated with the handshake message and the

1 encrypted data are correlated.”

2 So it’s pretty clear that the petition argued that encrypted
3 packets are filtered based upon the earlier handshake of
4 unencrypted data. So just making sure the record’s clear on that.

5 Patent Owner’s slide 20 highlights this determination
6 argument that was made previously. They say uncontested
7 evidence shows Buruganahalli’s handling of encrypted packets is
8 based on matching IP address and port number during flow look-
9 up. Again, this relates to element [d]. This is the determination
10 step. The claim only requires that the determination is based on
11 the threat indicator and certainly when you look into a table for a
12 matching to a threat indicator, the later routing of that traffic is
13 certainly based on that threat indicator.

14 Just quickly to Patent Owner’s slide 22. They argue there’s
15 no intermediate step that of rule-based filtering between
16 Buruganahalli’s flow processing and decryption of encrypted
17 packets which begs the question then, well, how do they get
18 there; right? We, again, we are looking at the encrypted packets
19 as they come in on a packet-by-packet basis. We can key off of
20 that network address. Look up in that table, oh, that corresponds
21 to the blacklist, let’s route it to the proxy for decryption. That’s
22 the way it works. So there’s essentially two problems with this
23 argument about, you know, the IP address and port number are
24 not a rule.

25 The first problem is the claim language itself. The routing
26 just has to be based on the determination. Certainly when you

1 index a table for a network address that corresponds to a domain
2 that is on the blacklist, that is based upon that threat indicator.
3 But secondarily, and I sort of mentioned this earlier on, that's
4 exactly how the '856 patent does it and so I want to go back to
5 Petitioner's slide 2 to highlight step 710. So we're making all
6 these arguments. Patent Owner's making all these arguments
7 about the determination can't be a rule because it's an indexing
8 of a network address. Well, step 710 says that we determine
9 based upon unencrypted data corresponding to network-threat
10 indicators that packets comprising encrypted data correspond to
11 the network-threat indicators that packets comprising encrypted
12 data correspond to the network-threat indicators.

13 Well, how do we do that and you can look at that
14 description in the Buruganahalli reference itself which is at
15 column 24, lines 28 through 30 -- excuse me. Is that right,
16 column 24? Sorry, column 14, not column 24. So column 14,
17 lines 28 through 30 thereabouts,

18 "Subsequent packets will be identified as belonging to the
19 session based on a flow look-up. As described herein in initial
20 TLS handshake exchange of the flow can be parsed to extract a
21 hostname to facilitate destination domain extraction for secure
22 protocols, (e.g., to apply one or more policies if applicable based
23 on the extracted destination domain) using various techniques
24 described herein."

25 And then it goes on that the otherwise processing towards
26 -- continuing on and you'll see that this is a correlation step,

1 sorry, I am reading the wrong. Strike that.

2 It was column 24 of the ‘856 patent, sorry, not
3 Buruganahalli. So we’re looking at the support for step 710, and
4 my apologies. So column 24, lines 28 through 30 and I’m
5 reading the end of the second full paragraph that states,

6 “Packet filtering system 200 may determine that one or
7 more of the packets encrypted in accordance with the parameters
8 of sessions 306 through 606 correlate to one or more packets
9 comprising the DNS query.”

10 And if we want to know what correlate means in a little
11 more detail, we can go to column 9, lines 46 through 65, so right
12 around line 50 of column 9. Again, this is the ‘856 patent.

13 “Rules 212 may be configured to cause rule gate 126 to one
14 or more of identify the packets determined (e.g., based on one or
15 more network addresses included in the network-layer headers)
16 that the packets comprise data corresponding to network-threat
17 indicators, for example, by correlating.”

18 So this is the exact same way the ‘856 is correlating
19 encrypted packets based upon what is in a table. The
20 Buruganahalli reference is doing the same thing so there’s no
21 point of distinction here. The fact that Buruganahalli is doing
22 decryption at the same point in time as the ‘856 is not a
23 distinction. It’s the same exact way that the ‘856 provides
24 additional security and I would just highlight tellingly the Patent
25 Owner’s expert when describing the flow process of the ‘856
26 patent just completely skipped over all of the decryption and

1 seemingly pretended that it just wasn't there.

2 If there's no additional questions on the filtering, I'll just
3 briefly mention the network-threat indicator before wrapping up.
4 So I'll switch back to Petitioner's slides, I believe it's
5 Petitioner's slide 24.

6 So this lays out the differences in the proposed
7 constructions. To the extent I can make any sense of it it seems
8 as though the Patent Owner is arguing that the threat indicator
9 must be a bona fide threat and not a potential threat, that seems
10 to be the difference. That's been highlighted in the briefing, and
11 I would just highlight the background of the invention here on
12 Petitioner's slide 24 which is the first few sentences of the
13 specification highlighting that network threat services were
14 known. Highlighting that network threat indicators were known.
15 They were also known to identify domain names. You see that
16 highlighted in yellow. You see that these threats include at
17 around line 3 there on the page unauthorized requests. Certainly
18 that would be a potential threat where blacklists of course may
19 be a little more crystallized in terms of whether it's a bona fide
20 threat or not.

21 I don't know that the claims require this level of dissection,
22 potential threat, actual threat. There's no distinction made in the
23 specification. There's no distinction made in the claim and I
24 would highlight on Petitioner's slide 27 Buruganahalli talks
25 about new threats, right, new vulnerabilities, false positive,
26 right, the full realm of potential problems that you would see in

1 a network. So whether it's a potential threat or a bona fide
2 threat, the prior art would meet it in any event, so that's it for
3 network-threat indicator.

4 Quickly just finishing up on the proxy point. I'll go to
5 Petitioner's slide 32. So, again, we highlight all the features of a
6 proxy; transparent end points, trusted man-in-the-middle,
7 isolates traffic, the host doesn't know that it's there, it's
8 providing functionality that the host would otherwise perform
9 itself for the purpose of safety, all of that is taught there on slide
10 32.

11 You see in Petitioner's slide 33. No real dispute there
12 about transparency as to the end points being a main function of
13 a proxy. We've got additional references that are cited there.
14 Again, this is not a complicated issue so I'm not going to spend
15 too much time on it.

16 Certainly Petitioner's slide 35 gets to the earlier question
17 you had, Your Honor, about the differences in construction, you
18 know, whether the proxy needs to be intervening or not, whether
19 that were to be added to the construction doesn't matter. That
20 decrypter functioning as a proxy in Burganahalli is between the
21 host and the sender, that's the entire point of decrypting is so
22 that you find out about the security infirmities prior to the host
23 finding out the hard way.

24 And then I'll highlight just a few additional issues in the
25 Patent Owner's slide deck. I'll go to Patent Owner's slide 36.
26 Again, this is sticking with the proxy issue. So they argue

1 against the combination of Baehr by saying, well, there's no
2 isolation advantage over Buruganahalli because it already has
3 isolation and they say there's no reason to add a proxy to
4 Burugunahalli because it already seamless communication. So
5 they're basically arguing that Burganahalli already has a proxy
6 so why would you add a proxy, so this is one of the many
7 instances of Patent Owner just simply talking out of both sides of
8 their mouth.

9 Two more points on the Patent Owner deck before I sit
10 down here and that's Patent Owner's slide 8. So on this slide
11 deck in the pink box you see a couple of the advantages
12 highlighted here and they say, you know, these are undisputed.
13 None of these are claimed so we have no duty to dispute
14 advantages that are not recited in the claims.

15 Same holds true for Patent Owner's slides 24 and 25. They
16 say that Buruganahalli does not have certain steps. Neither do
17 the claims, so that's irrelevant. We're not matching up pieces of
18 specifications here. We're matching up the claims to the
19 teaching of the prior art.

20 So just in wrapping up, the claims are overwhelmingly
21 obvious. We have the same plain text, domain extraction, we
22 have the same look-up, we have the same routing to a proxy and
23 even the unclaimed feature of decryption is also there. So we're
24 doing the same things at the same time for the same reasons.
25 There is no distinction here. There's no magic here. There's no
26 unsolvable problem; right? We routing encrypted packets based

1 upon what we learned from unencrypted packets. Buruganahalli
2 is doing the exact same thing; right? It's filtering the plain text
3 handshake for a domain, correlating the encrypted packets come
4 in that have a network address that matches that domain through
5 a look-up triggering saying, oh, they're on the blacklist, we have
6 policy for that. Let's route it to the proxy for decryption, and
7 that's all on point with exactly what the '856 patent is doing.

8 So unless there are further questions, I'll reserve what's
9 left for rebuttal.

10 JUDGE MOORE: Very good. Thank you. You've got
11 about 21 minutes left.

12 MR. MCKEOWN: Thank you.

13 JUDGE MOORE: And Mr. Hannah, are you ready?

14 MR. HANNAH: Yes, Your Honor. Can you hear me?

15 JUDGE MOORE: We can.

16 MR. HANNAH: Okay, great. Thank you. May it please
17 the Court. James Hannah on behalf of Centripetal and first off,
18 we would like to thank you. Thank you for your time and your
19 consideration in this matter and in re-reviewing this record and I
20 believe that based on a full record and based on the arguments
21 that you will hear today there's several elements that are missing
22 from the Buruganahalli reference with regard to the '856 and
23 we'll dive into those, and I think one of the main ones is that
24 filtering step that Your Honor alluded to and the specific criteria
25 that are within that filtering. Also the network-threat indicators.
26 There's no such network-threat indicators in the routing to a

1 proxy is missing as well.

2 But let me back up and just do a little recap of Centripetal
3 and --

4 JUDGE MOORE: Actually, Mr. Hannah?

5 MR. HANNAH: Yes, Your Honor.

6 JUDGE MOORE: I'm sorry. Did you want to reserve time
7 for rebuttal?

8 MR. HANNAH: Oh, I'm sorry. Yes, can I reserve 20
9 minutes, please?

10 JUDGE MOORE: Of course.

11 MR. HANNAH: Thank you very much. So let me just
12 recap a little bit about Centripetal. Centripetal is a company
13 based in Reston, Virginia with deep ties to the government and
14 to the military. Several of its founders, the founding members of
15 the company, come from a long stand with the government and in
16 the military and based on that experience they recognized that
17 there were certain gaps in cyber security that just simply were
18 not able to be solved at the time and that's where Centripetal
19 really came into play.

20 Centripetal came into play to solve these unsolvable
21 problems. I mean, several people, several companies, even the
22 government issued a mandate and issued statements saying we
23 need a solution to these problems. We need to be able to protect
24 these large networks from these threats because at the time they
25 were simply not be able to be addressed and that's what
26 Centripetal did. Centripetal came up with the technology, solved

1 the unsolvable problem and what they did is they started -- they
2 were a small company so they reached out to partners in order to
3 try to integrate their technology, try to get it out into the world
4 and one of the players that they approached was Cisco. Cisco
5 was a big player in the market and they said, hey, and they
6 opened up their books. They opened up their books. They
7 opened up their patents to Centripetal and the said, hey, let's
8 partner, let's make this reality and Cisco turned around and they
9 say, thanks, but no thanks, we're not interested and what
10 happened is Cisco put Centripetal's technology in its products, in
11 its major products and so what did Centripetal have to do? It's
12 left with the recourse it has to sue Cisco because Cisco is not
13 even coming to the table anymore to talk to Centripetal. It has to
14 sue one of the largest players in the field and what happened
15 during discovery? We learned in internal emails, we have emails
16 that say we need to study Centripetal's claims, study the claims
17 in order to come up with our solution and that's exactly what
18 they did and that's what resulted in this large verdict for
19 Centripetal after the Cisco case.

20 Well, Cisco was not the only company that Centripetal
21 approached. It also approached Palo Alto Networks and lo and
22 behold the exact same thing happened. Centripetal's technology
23 ended up in their products. Instead of attacking Centripetal
24 based on the patents that were actually asserted in the litigation,
25 PAN took a different approach. It took a different approach by
26 trying to file this IPR against a patent that was never asserted

1 against PAN and the reason it did that was to get leverage
2 against Centripetal because this was part of the large Cisco
3 verdict that Centripetal had, and this is why as you go through
4 there's a lot of briefing based on these tactics that we view as
5 predatory and ironically Cisco and Keysight (indiscernible)
6 petitioners joined this and are now part of this proceeding and
7 the ironic part of that they both knew the reference here,
8 Buruganahalli. The knew about it and they decided not to bring
9 it into the -- in front of the jury or in front of the Judge because
10 there's several issues with it and the overall issue with this
11 reference is that it simply is talking about the old technology of
12 analyzing unencrypted data in order to make decisions. It must
13 decrypt the data in order to do any type of filtering. This is the
14 old technology. The unsolvable problem that Centripetal solved
15 which is being able to analyze encrypted traffic without
16 decrypting it.

17 And if you look at this, you can see -- I'm looking at slide
18 2 if you can see my screen. I'm sorry, can you see my screen,
19 Your Honors? Did I put it on there? All right. Thank you. You
20 see on my screen these are the main reasons that the reference
21 fails. No. 1, there is no filtering of encrypted data packets based
22 on the packet filtering rules. During the presentation by the
23 Petitioner, we did not hear any argument regarding the criteria
24 that is required in the claims for the filtering of the packet
25 filtering rules. There was no discussion of a uniform source
26 identifier, no discussion of a protocol version, no discussion of a

1 method that was specified by the packet filtering rules. No
2 discussion of a data indicating a request or data indicating a
3 command. It is simply absent from the Buruganahalli reference.
4 It's not there. Every time when you look and you study this
5 record, and you study the reference you will not see a reference,
6 you will not see any disclosure of the claimed packet filtering
7 rules with the necessary criteria. The Petitioner simply skips
8 over it every single time and even during the presentation that
9 we just heard.

10 No. 2, there's no network --

11 JUDGE MOORE: Counsel?

12 MR. HANNAH: Yes.

13 JUDGE MOORE: Isn't that filtering basically the
14 correlating, isn't what's happening in each case that you identify
15 a plain text, domain name, and then you then filter all the
16 packets that correlate with that packet that had the unencrypted
17 concerning domain name?

18 MR. HANNAH: Okay. So no, Your Honor. So first of all,
19 there's talk about what Buruganahalli actually teaches. So first
20 you extract the domain name from the unencrypted handshake;
21 right? And I can just jump to -- there's three scenarios in
22 Buruganahalli; right? No. 1 is the whitelist scenario. So you
23 extract the domain name from the unencrypted handshake and
24 then you say, okay, everything here -- everything in this flow is
25 going to pass on. So now everyone's gone; right? There's no
26 routing in scenario 1 so that is completely irrelevant to the

1 claims here.

2 Scenario No. 2 is the blacklist. You look at the handshake
3 message. You extract the domain and then you block the session
4 from ever forming. No analysis of any encrypted packets; right?

5 No. 3. This is where you look at the handshake message.
6 You see that it's on the unencrypted -- from the unencrypted data
7 you see the domain name and then the flow is going to be
8 forwarded to be decrypted; right? Only the unencrypted
9 handshake is analyzed and policies are applied, and only the
10 decrypted data is applied.

11 Now, what they're trying to say is, well, and as Your Honor
12 just said, isn't this their argument that they're saying, well, we'll
13 just do a correlation between the unencrypted handshake and the
14 later encrypted packets. Well, that's wrong for several reasons.
15 Let me just look at the claims. There is still not filtering of the
16 encrypted data based on one of these criteria. One of these
17 criteria is completely absent to look at the encrypted data.

18 JUDGE MOORE: But aren't those the criteria that allow
19 you to correlate?

20 MR. HANNAH: No.

21 JUDGE MOORE: I mean, correlate criteria, for lack of a
22 better word?

23 MR. HANNAH: No, no, no. So what happens is you
24 extract a domain name and you say, okay, I'm going to decrypt
25 this flow. Then you do a look-up of the IP address and the port
26 number. That's not here. The IP address and the port number is

1 not shown in this step and Your Honor asked a very good
2 question. You said, well, aren't you actually just looking at the
3 flow, not individual packets and that's exactly right because
4 what you do is you look at the IP address and the port number
5 and you associate that packet with the flow. You don't apply
6 any policy to it and then once you associate it with that flow,
7 then that flow is just sent to be decrypted so that you can
8 actually do exactly what the prior art has done for decades is
9 decrypt the data in order to see what's in the data itself. So
10 there is --

11 JUDGE MOORE: So you would say the problem is that
12 that list in the middle there on slide 11 doesn't say and an IP
13 address and a port?

14 MR. HANNAH: Exactly.

15 JUDGE MOORE: Okay.

16 MR. HANNAH: Exactly. Absolutely, Your Honor, and it
17 doesn't say domain either, domain name either; right? So none
18 of that is there. The domain name comes when you do the
19 determination of the network-threat earlier in the claim. So this
20 is on slide 9 which is the claim here. You look at the network-
21 threat indicator and that comprises the domain name. But when
22 you do the filtering, that's on the specific criteria that is
23 nowhere to be found. It's simply absent.

24 So when you go through those three scenarios, one, the
25 whitelist doesn't apply. The blacklist where it blocks the
26 communication doesn't apply because encrypted packets aren't

1 ever analyzed, and then when you're going to send traffic to be
2 decrypted, all you're doing is looking at the unencrypted data
3 and the handshake, looking at the domain name. Say, okay, I'm
4 going to have this traffic be decrypted. Subsequent packets, it's
5 a flow look-up and we know page 10 of their reply, I've got that
6 memorized, the Petitioner specifically says that flow look-up is
7 not applying the packet filtering rules. They say it as clear as
8 can be and so there is no filtering of the encrypted packets and
9 that is the problem, that is the unsolvable problem that we've
10 both been referring to now that is simply missing. I mean --

11 JUDGE MOORE: It's solved a different way in the
12 reference, right, they just use the look-up instead of these other
13 criteria on your slide?

14 MR. HANNAH: Right. But I mean I would take it a step
15 further and say that they solved it in a different way in that they
16 still required decryption to apply the policies. But they
17 absolutely did not use their criteria that's specified in the claims.
18 That is, I mean that's clear because it's nowhere to be found, and
19 that really boils down -- I mean, that is one of the main
20 arguments. I think, you know, I didn't hear anything about it in
21 the opening. I looked in the reply. They don't really hit it head
22 on either and it is these criteria, as we've put into our Patent
23 Owner response and we put into our surreply that these criteria --
24 every time we say the claimed filtering rules, that's what we're
25 talking about is the criteria that's applied to the encrypted
26 packets.

1 The Petitioner pointed to this slide 20 and, again, I always
2 love it when the other side kind of uses our slides, but this just
3 shows exactly the problem with their argument is that the
4 encrypted packets is based on the matching of the IP address and
5 the port number during the flow look-up. That's what they're
6 pointing to. But then in the reply they say that's not packet
7 filtering rules. So we don't have any filtering. We simply don't
8 have any filtering, especially based on the claim criteria that we
9 keep discussing.

10 In slide 22 here. We address the Joinder Institution
11 decision in talking about, you know, based on the incomplete
12 record that had been before the Board saying that, you know, the
13 flow look-up, that the filtering and the policies occurs after
14 determining which flow it belongs to, but there's no intermediate
15 step and then also the Petitioner confirmed that in the reply and
16 then we emphasized it in our surreply. But Buruganahalli is
17 clear that after you sped up the session and it's complete, then
18 that data is communicated to the firewall and it's decrypted
19 using the session key. So it's simply a flow look-up associating
20 the packet with a flow. There's no check on the blacklist domain
21 which they keep saying. That's nowhere to be found either. It's
22 just simply taking the packet associated with the flow and the
23 flow is going to be decrypted and the session that's going to be
24 there is going to be decrypted. But there's simply no application
25 of any type of rules or any policy to that traffic before it's
26 decrypted.

1 On 23 we just point out again that in the Institution
2 decision based on an incomplete record there were certain
3 citations about filtering the newly received packet with the
4 encrypted packet by forwarding it to the decryption engine. But
5 if you look at the actual citations that are provided by the
6 Petitioner and in the record, again, there is not a single instance
7 where it teaches this filtering of the encrypted packets based on
8 the claimed packet filtering rules with the criteria. It's just
9 simply absent and you're not going to find it in the record. You
10 won't find it in the petition. You're not going to find it in the
11 reference. You're not going to find it in the reply. It's just
12 absent.

13 Unless Your Honors have questions I think that you -- I
14 mean, I think you understand the issue that we have here is that
15 the criteria is simply missing. I'd invite any questions or any
16 clarifications or citations, you know, to the record that we can
17 explain but I think that that really hits the nail on the head in
18 terms of the issue.

19 JUDGE MOORE: Okay.

20 MR. HANNAH: So, Your Honor, I'll move on to the
21 network-threat indicator. So with the network-threat indicator, it
22 really does come down to the claim construction and how one of
23 ordinary skill in the art is going to understand this term.

24 This term's been construed. It's been construed in the
25 District Court. Petitioner offered a construction for it in
26 previous proceedings. As you see here on slide 28 it's an

1 indicator of a packet associated with a network-threat and so
2 actually it has to be associated with a network threat. The
3 Petitioner said, well, it could be a potential threat or something
4 of that nature but that's not what the construction says. This is
5 an indicator of a packet that's associated with a network threat
6 and even there says indicators that represent the identity of a
7 resource associated with a network-threat. Buruganahelli doesn't
8 talk about any type of known network-threats that are being
9 associated and so they're simply not comparing that and it's not
10 on the blacklist.

11 JUDGE MOORE: Counsel, you don't think that a person
12 skilled in the art is going to recognize that at least some of those
13 things in the blacklist are there because they, at least somebody
14 thought they would represent a threat to a network?

15 MR. HANNAH: I mean, no, I don't think so, Your Honor,
16 because I think that -- everything in Buruganahelli specifically
17 says that it's going to be something that's going to be set up by
18 the administrator. A blacklist that's going to be set up by the
19 administrator, and there's no confirmation in there that it's
20 actually a network-threat indicator and then, again, that's why
21 we kind of put up the testimony of their expert who said it's a
22 potential threat that comes up. But the network-threat indicator
23 actually has to be associated with the network-threat and it can't
24 simply just be a blacklist that could identify, for example, gmail.
25 I mean, my firm unfortunately has other blacklist gmail because
26 they don't want us using our personal email accounts associated

1 with the firm business. I think it's great for clients, great for the
2 firm, tough for me to check my email but that's on our blacklist.
3 I don't think there's any one of skill in the art who's going to
4 say that gmail is associated with a network-threat and so based
5 on what my firm's policy is that gmail is an untrusted -- is not
6 trusted and it's also unknown in terms of what we're going to do
7 with gmail, how we're going to be using that and so that could
8 be something that's going to be on a blacklist.

9 Buruganahelli doesn't specify that it actually has to be
10 some type of network-threat. It could be gmail that's on the
11 blacklist and that would -- that's going to satisfy, you know,
12 whatever issues that they're going to have with gmail or any
13 other service that they're going to put on there.

14 So their comeback to this is that, well, you know, all
15 internet traffic is considered untrusted. I mean, this is what their
16 actual evidence is that they cited, and we have the citation here
17 on slide 30. Well, that means it's going to be unworkable at that
18 point. If all internet traffic is considered untrusted, then no
19 traffic is going to get through or everything is going to have to
20 be decrypted and you're going to slow everything down. So it
21 becomes a simply unworkable system based on the evidence that
22 they cite and so the blacklist in Buruganahelli is something
23 that's set up by the administrator. It can be based on a variety of
24 decisions that the administrator wants to make but there's no
25 disclosure that it's actually associated with a network-threat as
26 specifically detailed in the '856 patent as the '856 patent has and

1 as the Petitioner even pointed out that these are associated with a
2 network-threat and you have to have that criteria and that's what
3 you're going to be using in the claims.

4 One tactic that the Petitioner used here was they tried to
5 use Dr. Goodrich's book against him but they didn't actually
6 show it to him during his deposition. They brought it in
7 afterwards in reply. But even this shows that if you look at the
8 plain language that they have here it even says that it's naïve
9 from a security perspective in that it assumes that the network
10 administrator can enumerate all the properties in malicious
11 traffic. So even Dr. Goodrich's textbook specifies that using a
12 blacklist approach to be able to use it for security is naïve.
13 You're not going to be able to use it. So rather than support the
14 notion that blacklists are going to always have network threats or
15 something that's associated with the network-threat and it
16 actually specifies that it would be naïve to use this blacklist
17 approach in conjunction with a blacklist.

18 Do Your Honors have any questions regarding our position
19 on the network-threat indicators?

20 JUDGE MOORE: I don't think so.

21 MR. HANNAH: Okay.

22 JUDGE MOORE: Thank you.

23 MR. HANNAH: So now I'll turn to the routing to a proxy
24 system. The claims here require this routing to a proxy system.
25 These are the filtered packets that are specified in the claims.
26 Again, there's an issue with claim construction. Your Honor

1 asked does this term need to be construed? I would say yes, it
2 needs to be construed consistent with the construction that's
3 already been offered under the Phillips standard and that's what
4 the District Court construction is here on this screen on slide 34.
5 It's a proxy system which intervenes to prevent threats in
6 communication in its devices.

7 Petitioner's construction, they offered no construction, you
8 know for this term and so for a variety of reasons that's a
9 problem. But with the proper construction and how this is
10 understood, is that I think the key term here is that it has to
11 intervene to prevent threats. The only thing that they point to
12 for the proxy system in the Buruganahalli reference is the
13 decryption engine. Well, the decryption engine does exactly
14 what it says. It decrypts. There's no notion that it's intervening
15 between anything to perform any type of -- preventing any type
16 of threat from the communications. There's no disclosure of
17 that. It just simply decrypts the traffic and then allows the
18 process to continue.

19 JUDGE MOORE: Mr. Hannah, aren't they pointing also or
20 are they pointing to figure 3D as the --

21 MR. HANNAH: 3D?

22 JUDGE MOORE: -- as the proxy system?

23 MR. HANNAH: 3B, Your Honor?

24 JUDGE MOORE: Yes, 3B of Buruganahalli where 314 the
25 firewall would be acting as a proxy.

26 MR. HANNAH: In terms of -- so 3B where it does the

1 decryption of the traffic?

2 JUDGE MOORE: Yes. The firewalls, it's between the two
3 sessions. So it's decrypting, right, and then I guess analyzing,
4 then re-encrypting and the client and the server think they're
5 talking to each other but they're actually -- you've got that
6 firewall in the middle.

7 MR. HANNAH: Right. And I think that's exactly what
8 this figure is showing on figure 6 is just a blown-up version of
9 how that would work in that the firewall has the decryption
10 engine within it and so 3B is just a higher level view of the
11 system but when you dive down into see, okay, what is the
12 firewall actually doing, you know, what they did here is they just
13 kind of pointed to the random SSL decryption box as being the
14 proxy and, again, there's no disclosure that it's preventing
15 threats or doing anything of that nature. It is just simply
16 decrypting and then the flow continues and that's what we show
17 on slide 35.

18 JUDGE MOORE: Isn't it applying the policies that are
19 shown there in that figure on slide 35? Isn't that why there's a
20 (audio interference).

21 MR. HANNAH: But the policies that are applied by the
22 decoder with regard to -- let's see here. So the policies right
23 here on 620 are applied right here with the decoder. If you look
24 at the petition and you look at the reply, the only thing that
25 they're pointing to for the proxy is the SSL decryption 610 and
26 so there's no -- and the reason they do this is because they have

1 to try and show some type of routing and I don't think this is
2 showing routing to a proxy at all. But they're trying to show
3 some type of traffic flow that goes through but the thing that
4 they point to there is the SSL decryption 610.

5 JUDGE MOORE: If they were pointing to everything in
6 reference No. 402 in that figure, would that be a proxy system?

7 MR. HANNAH: Then you don't -- then you're also taking
8 into account the flow that's there. So you have a problem then if
9 you're going to go too, you know, you draw your box too broad
10 then what's the distinction between the other claim elements that
11 are required in order to do the determining and the filtering of
12 that nature and then you have to route to the proxy system. You
13 see what I'm saying? So if you draw your box that big and the
14 whole thing is the proxy system, then you don't have anything
15 else that's doing the first, you know all of those steps before
16 that. Because now you're encompassing everything so --

17 JUDGE MOORE: Oh, but I thought you had two steps.
18 The first step you do the thing where you look at the plain text
19 domain and you, you know, flag the whole flow and then if it's
20 on the list you send the whole flow to the firewall into the
21 system shown in figure 3B of Buruganahalli where it decrypts all
22 of the communications and looks at them and then, you know,
23 decrypts them and sends them on. Isn't that --

24 JUDGE HANNAH: Correct. So that first part that you just
25 talked about? That's all done on the firewall. The whole thing
26 of looking at the traffic that comes in, extracting the domain and

1 then subsequent packets associating with the flow, that's all
2 happening on the firewall. So that whole part is happening on
3 the firewall.

4 So my point was if you draw your box around -- I believe
5 this was your question, I might have misunderstood it, but I
6 thought you said if you draw your box around 402 and label that
7 as the proxy, then the issue is you're not encompassing
8 essentially the whole firewall and so there's not a proxy system
9 in which you're routing the packets to, if that makes sense.

10 JUDGE MOORE: I mean, it may. Does it have to be on a
11 different device or does it have to be a different process, for lack
12 of a better word, in the same device?

13 MR. HANNAH: I don't think it necessarily has to be on a
14 different device but I do think that it has to have the
15 functionality that's required by the claim language in which
16 you're going to prevent threats in the communications between
17 devices and so going with their mapping which is the 610 as a
18 cell description as provided in the petition, there's -- I keep
19 trying to use the pointer, I'm sorry about that on my screen here
20 -- this is just simply doing a decryption. It's not used to prevent
21 threats in the communications between the devices and then if
22 they try to broaden this and, you know, they start including three
23 boxes or four boxes, I mean it just -- at what point do you have,
24 it just keeps shifting in terms of like they're drawing anything
25 across it, you know, a router to be a proxy device.

26 So that's our issue with the proxy is that it doesn't meet the

1 claim language. I think the term does have to be construed. It
2 has been construed in previous proceedings under the same
3 standard and in fact it was construed in the Keysight litigation as
4 well. So Keysight as the joined party is well aware and I believe
5 that -- I'd have to double check the record to see whether they
6 agreed to it or not but it's definitely a construction used in that
7 proceeding as well and they just simply don't apply that
8 construction and they draw it around a box that is not doing
9 anything that's required by the construction. So that's our issue
10 with regards to the proxy, the identified proxy within the
11 Buruganahalli reference.

12 Buruganahalli doesn't really help you because the only,
13 like the Petitioner said, the only reason they point to Baehr is for
14 the word proxy which the word proxy appears in Baehr but there
15 is no reason that you're going to use the proxy in Baehr to do
16 anything. I mean, the decryption is already happening at the
17 firewall so why would you need to send it to an external device
18 because their position is that you're going to have the decryption
19 done on an external device and therefore you're going to use the
20 proxy or the proxy that's identified in Baehr in order to do that
21 decryption. So there's just really no reason to do that, so when
22 we say there's no isolation advantage over Buruganahalli that's
23 why there is no isolation advantage Why would you send traffic
24 in order, to another device, in order to do some decryption when
25 the firewall is already going to be doing it and firewalls have
26 been doing that, have been doing decryption for a while at that

1 point. So one of skill in the art's not going to --

2 JUDGE MOORE: Counsel?

3 MR. HANNAH: Yes, Your Honor.

4 JUDGE MOORE: Might you just want to offload that more
5 processor intensive work somewhere else so that most of the
6 traffic doesn't get, you know, encumbered by all of that activity?

7 MR. HANNAH: I mean, I don't -- there's no advantage to
8 that. All you're going to do is still slow down the system
9 because the traffic is either going to be decrypted or not
10 decrypted. So if it's decrypted, it's just going to go. If it's
11 going to be -- I mean, if it's not decrypted, I'm sorry -- it's just
12 going to go through. If it's decrypted and you're offloading the
13 processing it's still going to be a bottleneck in passing it into the
14 network. So there's no advantage there. It's not like it's a, you
15 know, some type of process that's happening and that you're
16 allowing the traffic to still continue and then you're going to be
17 decrypting it and analyzing it some other way in order to do
18 whatever. I don't know whatever reason you would do it for.
19 It's still a bump in the road, I'll put it that way. It's still a bump
20 in the road that you're going to have to decrypt at some point,
21 and so offloading it to one device or five devices actually is
22 going to slow it down because that device is now going to have
23 to process the incoming traffic in a similar manner so you're
24 almost duplicating the efforts and, again, this is something that's
25 been in firewalls for a while so one of skill in the art's not going
26 to look and say, okay, it's going to be an advantage to me to

1 break up this firewall and put the decryption engine on
2 someplace else. It doesn't make sense in terms of efficiency or
3 anything of that nature which is, you know, in our view it's very
4 conclusory what they cite but, you know, in terms of efficiency,
5 in terms of the network and stuff like that but if you actually
6 think about it, it makes it less efficient to put it on a separate
7 box.

8 JUDGE MOORE: Why does the patent use a proxy, do you
9 know?

10 MR. HANNAH: Why does the patent use a proxy? You
11 can do additional further analysis. Actually they talk about a
12 bunch of different things so you can deal with it, with a proxy. I
13 can get you citations in terms of specifics on what it does but in
14 terms of routing it to the proxy you can have a number of actions
15 that are just going to perform this additional analysis that I was
16 talking of. You can generate -- there's an issue about generating
17 log information, yes, so you can log data. If you look at column
18 14, line 65 I think it talks about how the proxy device can
19 generate logs so there's a bunch of different information that you
20 can use. Actually column 14 talks about it a lot where it talks
21 about you can, even on 31, where you can log data generated by
22 the packet filtering system. You can log the, you know, whether
23 packets are dropped. Column 15 kind of talks about that similar
24 thing. So one, to answer your question directly, one specific
25 thing is that you can do some logging information. I can find
26 additional things but, again, that's not shown in any reference.

1 So, you know, and that's when we get down to this last
2 point here where it says, the sub-bullet point, where it says
3 doesn't show anything about how the combination would
4 preserve the computing of resources or achieve load balancing or
5 maximized performance for the very reason I just discussed is
6 that it actually will increase the resources that are required is
7 going to -- serves as another bottleneck and in the reply none of
8 these were addressed. I mean, they simply weren't addressed in
9 terms of in the reply about how the system was actually going to
10 be more efficient and I think that's because they were double
11 downing on the Buruganahalli reference, you know, for this
12 notion rather than bring in Baehr.

13 Unless Your Honors have any questions regarding the
14 proxy limitation, so I'd quickly like to talk about the objective
15 evidence of nonobvious. It is true unfortunately for my client
16 that the District Court's opinion was vacated in this matter, or
17 not this matter I should say but at the Federal Circuit and so, you
18 know, obviously that is still an issue that is outstanding but it
19 does not -- that does not vacate the underlying trial transcript
20 record.

21 So let me just back that up a little bit in that what
22 happened in the Federal Circuit was after the trial was
23 completed, after all the witnesses had been presented, after all
24 credibility determinations had been made by the Judge,
25 essentially a lot of them on the record, the trial transcript was
26 closed and so the evidence was in. During the time that he was

1 writing, Judge Morgan, who unfortunately since has passed
2 away, was writing his opinion it was learned about the Cisco
3 stock issue and so the trial transcript itself and all of the
4 evidence that was in there and the determinations that he made
5 on the trial record stand and that's the evidence that -- we're
6 relying on that same evidence and so that's what we talk about
7 when we say, you know, they tried to solve this unsolvable
8 problem and they were using Centripetal's technology and in that
9 trial record Judge Morgan specifically references that. So the
10 underlying evidence is still there and this is some of the
11 evidence that we cited in the slide, on slide 37 where we talk
12 about, this is Exhibit 2013, where they're able to look at known
13 threats in the encrypted traffic without encrypting it. The
14 information about how Centripetal gave the technology to Cisco
15 and they copied the claims, they actually said we have to analyze
16 the claims. So all that underlying evidence is still there in terms
17 of the long felt need, the industry praise and the copying.

18 So I know the Petitioner makes, you know, kind of made
19 this categorical statement that, well, the opinion was vacated and
20 therefore you don't look at it anymore. That's not right. The
21 underlying evidence in the trial record is still in place and that's
22 what we're dealing with now, and so that was not vacated. That
23 is still in place. That's still in play and that's the evidence that
24 we're relying upon for the objective evidence of the
25 nonobviousness.

26 If Your Honors don't have any questions, I'll reserve the

1 rest of my time for rebuttal.

2 JUDGE MOORE: Okay. Looks like no questions. Thank
3 you very much, Mr. Hannah.

4 MR. HANNAH: Your Honor, may I ask how much time I
5 have left?

6 JUDGE MOORE: Yes, sorry, 20 minutes and 16 seconds.

7 MR. HANNAH: Okay, thank you.

8 JUDGE MOORE: Mr. McKeown, when you're ready,
9 please.

10 MR. MCKEOWN: Andrew, you're on mute.

11 MR. RADSCH: Can you hear me now? Okay. Thank you.

12 Good afternoon. This is Andrew Radsch from Ropes &
13 Gray for Petitioner Palo Alto Networks and may it please the
14 Board. I'll be presenting the rebuttal arguments today.

15 I'd like to start with the last piece that Mr. Hannah
16 addressed because it does (indiscernible) with the very beginning
17 part of his comments which is about the record and the Cisco
18 litigation. To be clear, that trial record is not in this proceeding.
19 It's not in evidence here. I believe they submitted the trial
20 transcript but all of the exhibits and the underlying evidence has
21 not been submitted here.

22 The Board noted that in its Institution decision that the
23 Patent Owner had not submitted that record of evidence in this
24 proceeding and did not subsequently submit that either and I
25 believe the Patent Owner's counsel stated that the determinations
26 made on that trial record stand. That's just false. All of the

1 determinations that the Court made subsequent to that trial have
2 been vacated and so the whole introductory comments about
3 alleged copying by Cisco, none of that evidence is in the record
4 here. That's all attorney argument. There's some comments too
5 made about similar fact pattern had occurred at Palo Alto
6 Networks. Again, that's just false. None of the alleged evidence
7 has been submitted here. It's just attorney argument and can be
8 ignored.

9 So what I'd like to do is just jump into the arguments about
10 the disclosures of the prior art starting with the discussion that
11 we spent most of our time on today which is the filtering that's
12 done by Buruganahalli and there's a number of comments made
13 by Patent Owner's counsel that the filtering does not occur nor
14 does it occur based upon the recited criteria.

15 If we just look at the claim language again, that's on
16 Petitioner's slide No. 3, sorry, slide No. 4 you see the list of
17 criteria. Among those listed criteria are uniform resource
18 identifier, again that's filtering based on URI. URI is a superset
19 that includes a URL. We showed throughout the record that the
20 filtering here is based upon a URL. I can point you to just a
21 couple of places in Buruganahalli where that is absolutely clear.
22 For example, this is discussed in the record in the petition and
23 also in the reply at column 5, lines 5 through 10. This is
24 Buruganahalli discusses the use of the SNI extension to the TOS
25 protocol and that extension includes the requested host name,
26 e.g., the destination domain for the connection. So it's that from

1 the initial handshake message setting up the TLS connection.
2 The destination domain, for example, the host name is extracted
3 and that is used to filter both the unencrypted packets and the
4 subsequently received encrypted packets, that URL. We see that
5 same information also shown at column 11 starting at lines 34
6 through about 53. It shows this handshake with the destination
7 domain, the URL.

8 JUDGE MOORE: Counsel, I thought the URL was only
9 exposed in the handshake message, the first one? It is exposed
10 in any others?

11 MR. RADSCH: That's correct, Your Honor. You see that
12 in column 11 there. The destination domain, the URL, is
13 exposed there in the handshake. It's extracted. A policy is
14 applied. The blacklist or whitelist policy that is applied. That
15 same blacklist or whitelist policy is applied to all of the
16 subsequently received packets of that session. This is absolutely
17 crystal clear in Buruganahalli. That blacklist policy which is
18 based upon that extracted destination domain which here we have
19 an example of the URL, is applied to the encrypted packets.

20 Now there's discussion --

21 JUDGE MOORE: So the filtering can be -- the filtering of
22 both types of packets can be done by the URL even if the URL
23 only exists, is only found in the first packet data (phonetic)?

24 MR. RADSCH: That's right. The claim language says it's
25 based upon one of those criteria. So you extract the URL and
26 you identify what is your corresponding policy and your rule is

1 then based upon, or your policy -- they're used interchangeably -
2 -- in Buruganahalli but your rule is based upon that destination
3 domain. That same rule is applied to both the unencrypted
4 packets and all subsequently received packets whether encrypted
5 or not of that session. That determines --

6 JUDGE MOORE: It's not that the filtering is done based
7 on the URL, it's the filtering is done based on the rule that's
8 being applied because of the URL that was in the first packet?

9 MR. RADSCH: Well, I'd say it's based upon the URL
10 because you select the rule that you apply. The blacklist rule is
11 based upon that URL. So the filtering is based upon that URL
12 because you're determining am I going to apply this blacklist to
13 a decryption engine? That answer is dependent upon whether the
14 destination domain is on that blacklist. So from that perspective
15 it's based on that destination domain.

16 There was the discussion about the use of the IP address
17 and the port number and as the Board recognized, and I can point
18 you to Petitioner's slide No. 17. As the Board correctly
19 recognized, and this is exactly how it works in the '856 patent,
20 the IP address and port number of the encrypted packets are used
21 to determine what session, what flow does this encrypted packet
22 want to so that it can apply the same filtering policy to that
23 encrypted packet that was previously applied to the unencrypted
24 handshake packets. It's precisely what's done with the '856
25 patent. So the flow look-up can simply say what session does
26 this packet belong to? That doesn't tell you what to do with it,

1 it's because that session correlates to the blacklist policy that's
2 based on the URL that tells you where to send that packet and,
3 again, we know this is exactly like the '856 patent because the
4 '856 patent says so. The word correlate appears over 50 times in
5 the '856 patent because what the '856 patent does is it correlates
6 the encrypted packets to the unencrypted packet to determine
7 what session it belongs to and I think Mr. McKeown pointed to
8 the same place in the '856 patent but it's worth repeating.

9 Column 5 of the '856 patent starting around line 33, the log that
10 is used to correlate the encrypted packets with the unencrypted
11 handshake include such information as the IP address and the
12 port number because it's that correlation into the log or in the
13 case of Buruganahalli a table that allows you to determine what
14 policy to apply and we see this, again, turning back to
15 Buruganahalli.

16 I mean, the thesis that I think that Patent Owner is
17 presenting here is that you extract the URL at the time of the
18 handshake and just discard it. You don't use it anymore. That's
19 exactly the opposite of what Buruganahalli teaches. You extract
20 the URL in order to select your policy and that policy, that
21 filtering rule is applied to all subsequently received packets of
22 that session. It's applied on a packet-by-packet basis. It's
23 applied to the whole session. You see that, for example, at the
24 bottom of column 9 of the Buruganahalli reference. This is with
25 reference to figure 1 of Buruganahalli. It says, and this is
26 starting at line 60,

1 “As further illustrated in figure 1 if the monitored traffic is
2 encrypted,” I’ll skip the parens, “then the security device can be
3 configured, e.g., based on a firewall policy to decrypt the
4 monitored traffic using a decrypt engine 110.”

5 It then goes on to state,

6 “For example, in some cases if the extracted destination
7 domain,” that would be the URL, “is not trusted or unknown,
8 then the firewall could be configured,” again that’s by a firewall
9 policy or rule, “to decrypt the monitored traffic for further
10 traffic monitoring.”

11 So the encrypted packets are filtered based upon that earlier
12 extracted destination domain and as we showed throughout the
13 record here, among the criteria listed in claim 1 includes URL.
14 That’s expressly recited throughout the claims. The URL is
15 extracted and it’s used to filter the encrypted and unencrypted
16 packets.

17 Now the Patent Owner in its slides points to the three
18 different scenarios it says that Burunganahalli discloses that is a
19 whitelist process by which packets are sent. A blacklist which
20 just simply blocks the packets from the session from even being
21 initiated and therefore it drops the session, or a blacklist that
22 would route the packets to a decrypt engine. That is filtering
23 right there, according to their own slides. Different packets are
24 going to be treated different ways depending on whether it’s on a
25 whitelist or a blacklist. The criteria includes a URL which is
26 among those recited criteria in the claim language. So it’s doing

1 exactly what the '856 discloses, exactly what it claims,
2 according to the precise criteria recited in the claim language for
3 filtering. Again, to be clear the IP address and the port -- as the
4 Board recognizes, this is again at slide 17 of Petitioner's slides
5 -- that's simply for the determining step that's used to determine
6 if the encrypted packet correlates to the unencrypted handshake,
7 then further filtering takes place according to that domain name
8 based firewall policy.

9 There was a statement by Patent Owner's counsel again that
10 policy applied to "only" to the unencrypted packets. Again,
11 that's not true. We see that again in the bottom of column 9 of
12 Buruganahalli where it says starting around line 63,

13 "The security device can be configured, e.g., based on a
14 firewall policy to decrypt the monitored traffic that's applying a
15 policy to the encrypted packets."

16 And again that policy is a domain name based policy that
17 includes such criteria as a URL as recited in the claims.

18 Turning briefly to network-threat indicators because there
19 was some extensive discussion about that by the Patent Owner.
20 I'd like to turn to Petitioner's slide 25 on that. You know, just
21 to be clear, it's stated in the slide, there's no dispute that
22 network-threat indicators were known. The '856 patent says that
23 expressly. Starting at column 1 of the '856, it says network-
24 threat indicators were used for security purposes and a threat
25 includes something as benign as an unauthorized request. It's
26 exactly what a blacklist is, unauthorized requests to access the

1 network, unauthorized communications, and as communicated on
2 slide 25 there's unrebutted testimony from Dr. Weissman that
3 confirming that such criteria as network-threat indicators were
4 known to be used for packet filtering purposes.

5 There was some discussion about gmail that a blacklist with
6 gmail and that gmail itself may not be a threat. It may be a
7 threat to some organizations and in any event, this claim is a
8 comprising claim. Just because the blacklist may also include
9 domains that are not deemed a threat, doesn't take away from the
10 fact that Buruganahelli specifically discusses using this blacklist
11 for security, discusses identifying threats, a feedback loop to
12 identify new threats and vulnerabilities, all of this ties in to
13 blocking threatening traffic and in response to the textbook from
14 its own expert and that excerpt is on slide No. 28 of Petitioner's
15 demonstratives.

16 Again, Patent Owner's expert's textbook he is tying a
17 blacklist malicious traffic. Patent Owner's counsel's argument
18 was that it would be naïve to use the backlist because it's
19 difficult to identify all malicious traffic or all properties of
20 malicious traffic. Whether it's naïve or not, Buruganahalli
21 expressly discloses the use of a blacklist and this textbook just
22 confirms that it was known to a person of ordinary skill in the art
23 that a blacklist corresponds to known malicious traffic.

24 Moving on to the arguments about the proxy system. I'd
25 like to just, you know, there's a lot of argument about
26 Buruganahalli's teachings with respect to figure 6 and this is on

1 Patent Owner's slide No 35. You know, what it omits from this
2 discussion and it's focused a lot of its attention on figure 6, but
3 figure 6 is one embodiment. There's other embodiments. Again,
4 figure 6 is a functional diagram. Figure 1 is another
5 embodiment. In their corresponding passages Buruganahalli
6 talks about the decryption engine of figure 1. But this notion of
7 that decrypt process is not intervening to prevent threats, it's
8 really difficult to understand because what Buruganahalli
9 specifically says is that it acts as a trusted man-in-the-middle,
10 right, and it's swapping out it's own self-signed certificate for
11 the public certificate in the communication so that it can decrypt
12 and re-encrypt that communication without either endpoint
13 knowing and it does that precisely to apply security policies,
14 additional security policies to prevent malicious traffic. That
15 certainly is intervening in a communication to prevent threats.

16 As to the question of whether that term needs to be
17 construed, I would point you to Petitioner's slide No. 35. On
18 slide 35 as shown in the first highlighted box of text there,
19 Patent Owner admits that its proposed construction here deviates
20 from plain and ordinary meaning. It contrasts the District
21 Court's construction with plain and ordinary meaning, and if you
22 look at the record the cited evidence from the Keysight case that
23 they cite for their construction you'll see that Patent Owner itself
24 argued that no construction was necessary and the Board only
25 adopted the construction that Patent Owner now proposes
26 because the Court said the term would not be familiar to a lay

1 person. It's just adding extra clarity to a lay person. That's all
2 in the cited evidence. I believe that's Exhibit 1030, and that's
3 why the Court adopted that construction over Patent Owner
4 saying no construction was needed. It should be accorded its
5 plain meaning. Here again we see in the briefing Patent Owner
6 has admitted that the Court's construction is not plain meaning, it
7 adds something additional. They say oh, it doesn't matter
8 because Buruganahalli's proxy intervenes. It takes those patents,
9 it decrypts them, replaces the certificates with its own
10 certificate, re-encrypts them and performs processing on them in
11 order to prevent malicious communications, for example, from
12 continuing on or prevent malware from being transmitted.

13 Whether the functionality has to be a separate device or not
14 is not claimed. It can be a separate functional component. The
15 Buruganahalli reference itself, this is at column 2, discusses that
16 its firewall can be a device or a system. That's at lines 14
17 through 15, and also at lines 50 through 53 it discusses that its
18 firewall is typically a device or a set of devices or a software
19 executed on a device. So it certainly contemplates these
20 functionalities being done in a single device in separate devices,
21 in separate logical components, and as Patent Owner has stated
22 and its expert has stated nothing in Buruganahalli restricts these
23 functionalities from being performed on a single processor, for
24 example, so they can be and it's understood by a person of skill
25 in the art to be separate components.

26 There was some argument by Patent Owner about a lack of

1 motivation to combine also Buruganahalli with Baehr to the
2 extent that's even necessary. I would point you to their expert's
3 own statement in his declaration. This is Exhibit 2026 and this
4 is at paragraph 31 where Dr. Goodrich states,

5 "Decryption and re-encryption is difficult to perform in
6 real time and undesirably slows down network traffic and
7 consumes computing resources."

8 This goes directly to the question that Your Honor was
9 asking. A person of ordinary skill in the art, as Dr. Weissman
10 testified to and showed through other secondary references,
11 would be motivated to offload that computationally intensive
12 process to a dedicated machine. That does not slow down the
13 process as Patent Owner claims. The firewall in Buruganahalli,
14 it's acting on many sessions. It has both blacklisted flows,
15 whitelisted flows, and those that are being blacklisted and routed
16 for decryption. So to offload that intensive decryption and re-
17 encryption process as was known in the art through separate
18 proxy would have been obvious to a person of ordinary skill in
19 the art.

20 Among other things we cited the NIST reference that
21 discusses the benefits of a dedicated proxy for these very
22 reasons, to offload processing and specific tasks to a separate
23 proxy. So it takes that a separate proxy is needed for routing to
24 a proxy element. Baehr teaches that and there's ample
25 motivation to do so.

26 And just to circle back on I think the final point about the

1 arguments that Patent Owner made, circling back to the argument
2 about the filtering. Again, they rely upon, you know, in their
3 slides they touched upon steps that they claimed just are not in
4 Buruganahalli. This is on slides 24 and 25 of their
5 demonstratives. On 24 they say there's no separate step, like 19
6 or 27 in Buruganahalli there's no step like 19 or 27 of the '856
7 patent. Again, those specific steps are not claimed but in any
8 event there is a similar step. Again, packets, the handshake
9 message is filtered to extract a URL. That URL-based policy is
10 applied to all subsequently received packets of the session such
11 that subsequently received encrypted packets are filtered
12 according to that same URL. Again, it's that association of the
13 flow, the (indiscernible) support that allows the firewall to
14 determine what to do with that packet. Should it be passed
15 because it's on a whitelist? Should it be routed because it's on
16 the blacklist? Those policies are based upon recited criteria in
17 the claims. There is no distinction over the '856 patent. It's
18 exactly the same.

19 Unless Your Honors have any further questions, I will sit
20 down.

21 JUDGE MOORE: Seeing none, thank you very much.

22 MR. RADSCH: Thank you.

23 JUDGE MOORE: Patent Owner, you've got 28 minutes.

24 MR. HANNAH: Thank you, Your Honor. I'd like to start
25 with a fundamental technical misunderstanding. The URL is not
26 contained in the handshake message. Counsel said it several

1 times. He said that the URL is in the handshake message. It is
2 not. The only thing that's in the handshake message is the
3 domain name. The URL is not there and that's why I kept
4 emphasizing that there is no packet filtering using the criteria
5 disclosed in Buruganahalli. Buruganahalli makes that clear that
6 the URL is not in the handshake message and in order to
7 determine where the URL is you have to decrypt the traffic.

8 I'll show it on the screen here. In order to look at the URL
9 and compare it to the domain name, Buruganahalli specifically
10 says that you have to decrypt the data. It is not in the handshake
11 message. This would be completely irrelevant if the URL was in
12 the handshake message. That understanding is so technically
13 wrong. You will not find it anywhere in the papers. This is the
14 first time that we're hearing it today. You can scour the record.
15 You can look in the petition. You can look at all the
16 declarations. You can look in the reply. The Petitioner never
17 makes the argument that the URL is in the handshake message
18 and furthermore, never makes an argument that a domain name is
19 a URL, because it's not. A URL, and this is cited in Dr.
20 Goodrich's declaration. He even cites the Wikipedia page about
21 the encrypted protocol. But the URL includes the method or
22 protocol use retrieve the file, the host name, the port and the
23 path. The domain name does not include any of that.

24 If you want to look at the additional evidence that's in the
25 record, we can look at the Magee reference -- I'm also putting
26 that on the screen -- and it shows you the difference between a

1 URL, which I'm showing here and this is Exhibit 1037, and the
2 domain name. Here the domain name is simply mynetwork.com.
3 That's the only thing that you're going to see in that handshake
4 message. You are not going to see the URL and so all of this
5 argument that Petitioner made saying that, okay, we're going to
6 use the URL from the handshake message and then use that for
7 filtering is completely wrong because you can't do it.

8 So that is why when I started out before the panel here
9 when I say that they can't point to anything, that says that you're
10 going to filter based on the claimed criteria, filter based on the
11 URI or any of these other criteria that is simply not disclosed in
12 Burgunahalli, that's because it's not. The only thing that they
13 look at, that Burgunahalli looks at, is the domain name and the
14 unencrypted data in the handshake message. That's it. It never
15 filters based on anything else and it absolutely never filters the
16 encrypted packets based on any of this criteria, and you won't
17 see it in the record and it's really that simple that it's not
18 (indiscernible).

19 If you look at their testimony from their expert even. So
20 this is Exhibit 1003. Their expert specifically says that the URL
21 is found in the encrypted application layer data. So it can't be in
22 the handshake message. It's encrypted in the application layer
23 data. This is found in paragraph 64 and paragraph 127. So all of
24 the argument that we've heard today simply falls apart because
25 they do not filter based on the criteria that's found in the claims.

26 Unless Your Honors have any other questions -- I'd love to

1 answer any questions Your Honors have about the handshake
2 message or anything of that nature because I think that this is a
3 very important point and this is the crux of the Petitioner's
4 argument, and once you actually dive into the technology and
5 look at the reference and look at Buruganahalli even which says
6 that you have to decrypt the packets to find the URL to make that
7 comparison, their entire argument falls apart. It's an important
8 point. I'm sorry, I didn't hear you, Your Honor.

9 JUDGE MOORE: Apologies. I think we understand your
10 arguments.

11 MR. HANNAH: Okay.

12 JUDGE MOORE: Do you have anything further?

13 MR. HANNAH: Well, with regard to the claim
14 constructions and the other positions that were taken, typically in
15 a situation in which we offer a construction and the District
16 Court comes back and says you lose, we're going to go with
17 another construction, that's the construction that we're stuck
18 with and that's the one that we go with. So I think that's
19 common sense in terms of how we proceed and that's why we
20 offer the constructions and we think that we need to stick to
21 those constructions in this case, and that sticks to both network-
22 threat identifiers and the proxy system as articulated here.

23 But other than that, Your Honor, I'll leave it with that point
24 that, you know, Burgunahalli simply does not filter based on the
25 criteria and they still have not, even in their rebuttal, have not
26 shown that encrypted packets themselves are actually filtered

1 based on that criteria, or filtered at all. They're simply just
2 associated with a flow, as we pointed out earlier.

3 JUDGE MOORE: Okay. Well, thank you very much and
4 thank you everyone else. It was a very interesting afternoon.
5 Everybody's extremely well prepared and we certainly appreciate
6 it. So we are adjourned and order we'll issue in due course.
7 We'll ask the parties to stay on for a minute in the event that the
8 court reporter has any questions. Thank you very much.

9 (Whereupon, at 2:54 p.m., the oral hearing was
10 concluded.)

PETITIONER:

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

Theodore Foster
David McCombs
Gregory Huh
HAYNES AND BOONE, LLP
ipr.theo.foster@haynesboone.com
david.mccombs.ipr@haynesboone.com
gregory.huh.ipr@haynesboone.com

Gerard Donovan
Peter Chassman
Jonathan Detrixhe
Sidharth Kapoor
REED SMITH LLP
gdonovan@reedsmith.com
pchassman@reedsmith.com
jdetrixhe@reedsmith.com
skapoor@reedsmith.com

IPR2022-00182
Patent 9,917,856 B2

PATENT OWNER:

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

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