

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

KEYSIGHT TECHNOLOGIES, INC.,
Petitioner

v.

CENTRIPETAL NETWORKS, LLC,
Patent Owner.

IPR2023-00448
Patent 11,012,474 B2

Record of Oral Hearing
Held: April 22, 2024

Before KEVIN F. TURNER, AARON W. MOORE, and
STEVEN M. AMUNDSON, *Administrative Patent Judges*.

APPEARANCES:

ON BEHALF OF THE PETITIONER:

JONATHAN I. DETRIXHE, ESQUIRE
Reed Smith LLP
1301 K Street N.W.
Suite 1000-East Tower
Washington, D.C. 20005
(202) 414-9200

ON BEHALF OF THE PATENT OWNER:

JAMES HANNAH, ESQUIRE
JEFFREY H. PRICE, ESQUIRE
Kramer Levin Naftalis & Frankel LLP
333 Twin Dolphin Drive
Suite 700
Redwood Shores, California 94065
(650) 752-1712

The above-entitled matter came on for hearing on Monday, April 22, 2024, commencing at 1:00 p.m., at the U.S. Patent and Trademark Office, 600 Dulany Street, Alexandria, Virginia.

P R O C E E D I N G S

- - - - -

JUDGE AMUNDSON: All right. Is the court reporter ready to go on the record?

REPORTER: Yes, sir, I am.

JUDGE AMUNDSON: All right, very good. Let's begin. Let's go on the record. Good morning or afternoon, depending on where you are located. I'm Judge Amundson, and with me on the panel are Judges Turner and Moore. We have our final hearing in IPR2023-00448 involving U.S. Patent Number 11,012,474, between Keysight Technologies and Centripetal Networks.

Let's get the parties' appearances. Who do we have for Petitioner?

MR. DETRIXHE: Good afternoon, Your Honors. This is Jonathan Detrixhe of Reed Smith for Petitioner, Keysight Technologies.

JUDGE AMUNDSON: All right, very well. Thank you. And who do we have for the Patent Owner?

MR. HANNAH: Good morning, good afternoon. James Hannah on behalf of Patent Owner. And with me is Jeffrey Price.

JUDGE AMUNDSON: And who will be presenting the argument on Centripetal's behalf?

MR. HANNAH: For this first argument on the '474, Jeffrey -- Jeff will be doing that one.

JUDGE AMUNDSON: All right. Thank you. And welcome to everyone. Because we are conducting the hearing by video, we wanted to start by addressing a few items.

1 First, our main concern is your right to be heard. So if at any time
2 during the hearing you encounter technical or other difficulties that you feel
3 undermine your ability to adequately represent your client, please let us
4 know immediately, for example, by contacting the team members who
5 provided you with the connection information.

6 Second, when not speaking, please mute yourself.

7 Third, please identify yourself each time you speak. That will help
8 the court reporter prepare an accurate transcript.

9 Fourth, we have the entire record, including the demonstratives.
10 When referring to a demonstrative or an exhibit or a paper, please do so by
11 identifying the slide or page number. Also, please pause a little after
12 identifying the slide or page number to give others time to find it.

13 Fifth, we set forth the procedure for today's hearing in the order
14 granting the requests for oral argument. That's Paper 21, but just to remind
15 everyone the way this will work, the order granting the requests for oral
16 argument provided that each party will have 45 minutes to present
17 arguments. Petitioner bears the ultimate burden of proof and will go first,
18 and Petitioner may reserve time for rebuttal. Patent Owner will go next, and
19 Patent Owner may reserve time for surrebuttal. But Patent Owner's
20 surrebuttal must be limited to the issues in Petitioner's rebuttal.

21 Also, please do not interrupt the other party while that party is
22 presenting its argument. If you have an objection, please raise it during your
23 argument. I will keep time, and we'll try to give you a warning when you're
24 nearing the end of your time.

25 Are there any questions before we proceed?

26 MR. DETRIXHE: Not from Petitioner, Your Honor.

1 MR. HANNAH: No, Your Honor.

2 JUDGE AMUNDSON: All right, very well. Mr. Detrixhe, would
3 you like to reserve any time for rebuttal?

4 MR. DETRIXHE: I anticipate reserving approximately 10 minutes
5 for rebuttal.

6 JUDGE AMUNDSON: All right, fine. All right. You may begin
7 whenever you're ready.

8 MR. DETRIXHE: Thank you, Your Honor. Let me begin by sharing
9 the demonstratives, and I'll start on slide 2.

10 I'd like to just begin by going over the Institution Decision and what
11 is in dispute in this proceeding. Specifically, the Institution Decision found
12 that Petitioner had demonstrated a reasonable likelihood of prevailing on all
13 challenged claims, which cover all 33 claims of the '474 patent. There were
14 five grounds, all based on the combination of the *Law* and *Golnabi*
15 references, and the Institution Decision found a reasonable likelihood of
16 prevailing on each of these five grounds. And thus doing so, the Institution
17 Decision rejected three arguments raised by Patent Owner in its preliminary
18 response against the *Law* and *Golnabi* combination.

19 Slide 3. Specifically, these three arguments. First, the Institution
20 Decision rejected Patent Owner's argument that *Law* does not disclose or
21 render obvious a security policy management server that automatically
22 creates or alters any rules within the rulesets distributed by the server. And
23 in particular, the Institution decision rejected Patent Owner's argument that
24 *Law*'s firm 305 does not correspond to a security policy management server
25 that automatically creates or alters at least a portion of the rules within the

1 ruleset that it distributes, and rejected Patent Owner's argument that IT
2 personnel purportedly would still have been required to update the rulesets.

3 The second argument, the Institution Decision rejected Patent
4 Owner's argument that *Law* in view of *Golnabi* does not render obvious the
5 limitation that recites that "one or more of the packet filtering rules were
6 added, removed, or altered by the server based on a correlation between
7 portions of the malicious traffic information." And in particular, the
8 Institution Decision rejected Patent Owner's argument that a POSITA would
9 not have either recognized the problem of duplicate rules arising from *Law*'s
10 aggregation of threat data or *Golnabi*'s explicit solution to this problem.

11 And third, the Institution Decision rejected Patent Owner's argument
12 that *Law* does not render obvious a limitation that recites "wherein a first
13 packet matching rule of the packet filtering rules comprises an indication of
14 a feed." And in particular, *Law* discloses a rule table displayed to operators
15 of *Law*'s systems for purposes of seeing the rules in effect and, if desired,
16 tinkering with those rules by selecting which ones to implement. The
17 Institution Decision rejected Patent Owner's argument that a POSITA would
18 not have appreciated the desirability of displaying an identification of *Law*'s
19 sources of threat data in that table displaying rules to an operator based on
20 the threat data.

21 Slide 4. In this response, Patent Owner largely repeats each of these
22 same three arguments. Specifically, Patent Owner's response repeats the
23 argument that *Law* -- that *Law*'s firm 305 does not automatically create or
24 alter rules in view of its assertion that IT personnel still would have been
25 required.

1 Second, Patent Owner's response makes the same argument that it
2 wouldn't have been obvious in view of *Law* and *Golnabi*, too, that "one or
3 more of the rules were added, removed, or altered by the server based on a
4 correlation between portions of malicious traffic information" because a
5 POSITA "would not have recognized the problem of duplicate rules arising
6 from *Law*'s aggregation of threat data, nor *Golnabi*'s explicit solution to this
7 problem."

8 And third, the Patent Owner's response repeats the same argument,
9 that *Law* does not disclose or render obvious that "a first packet matching
10 rule may comprise an indication of a feed because a POSITA purportedly
11 would not have appreciated the desirability of displaying an identification of
12 *Law*'s sources of threat data in a table displaying rules to the operator based
13 on that threat data."

14 Slide 5. So before I get into the details and assessments of those
15 arguments, I'd like to go over some relevant details of the *Law* and *Golnabi*
16 prior art references. Starting with *Law*, *Law* discloses what it calls a unified
17 threat management system, UTMS, for securing network traffic in a process
18 control system. Network devices in *Law*'s process control system include
19 firewalls that receive rulesets from an external source, which *Law* describes
20 as a perpetual service in communication with the network devices. And this
21 perpetual service proactively supplies the network devices with rulesets in
22 order to meet the latest security threats, and the distributed rules include
23 rules that define conditions specifying whether to accept or deny network
24 traffic.

25 Slide 6. Specifically, *Law* discloses an embodiment with two UTMS-
26 configured firewalls, numbered 146a and b, that implement the rulesets to

1 inspect and drop malicious packets before those packets can reach their
2 intended destination. Those firewalls protect a network 150, which may
3 include subnetworks 150a and b. That network may just be a standard
4 ethernet communications network supporting any protocol, including
5 standard TCP/IP as well as other protocols, and the device is protected on
6 this network, maybe standard devices such as workstation computers or
7 personal computers.

8 Slide 7. *Law* discloses that the rulesets implemented by the firewalls
9 require updates to remain effective. Accordingly, *Law* discloses a third-
10 party cybersecurity risk management firm 305 that generates rulesets using
11 threat data and ruleset information provided by other third party sources
12 number 315. And specifically, the cybersecurity risk management firm 305
13 may collect threat data and ruleset data 310 from the plurality of sources
14 315. Those sources create the threat data and firewall data by analyzing
15 potential unknown threats to the security of process control networks and as
16 a few examples include the Vulnerability Research Service, VRS; the
17 Computer Emergency Response Team, CERT, of Carnegie Mellon
18 University; and Secunia, to name a few examples of the sources. And then
19 *Law* discloses that the firm 305 receives the firewall rules, that data, and
20 aggregates them in constructing the ruleset 147 that is distributed to the
21 firewalls 146a and b.

22 Slide 8. So here we see a Figure which illustrates how everything
23 I've just discussed is interconnected. Specifically, we see the firewalls 146a
24 and b to protect a network, which, as shown here, may include left
25 subnetwork 150a and right subnetwork 150b joined by a network access
26 device 149c. We also see that the firewalls 146a and b communicate with

1 the firm 305 over the Internet 155. And here at the top we see a number of
2 the sources 315 all feeding in their own firewall threat data and ruleset data
3 310 to the firm 305. Specifically, it called out a few examples of the sources
4 315 that I just went over, but here we see six bubbles of such sources
5 showing that any number of sources may be combined and aggregated.

6 Slide 9. Here we see Figure 13 which provides a ruleset user interface
7 that an operator of *Law's* system could use to configure and control any
8 other rules within the ruleset 147 implemented by the firewalls.

9 Specifically, we see a number of columns, including a protocol type column
10 1302 that *Law* explains includes conventional protocols such as UDP and
11 TCP, but may also include other protocols applicable to a process control
12 environment such as ICMP, HART, or SCPI.

13 In addition to the Protocol column 1302, we also see a From address
14 column 1304 that specifies an IP address, a To address column 1306 that
15 specifies the To IP address, as well as a Port column 1308 and an Action
16 column 1310, and a Description column 1312. So the Action column may
17 specify actions such as accept or deny. And then, you know, lastly, at the far
18 left of this rule table, we see a row selection column 1324 which includes a
19 number of checkboxes. And these are what an operator may use to select
20 which rules, particular rules that the operator wants to enforce to the extent
21 the operator wants to make that selection.

22 Next slide 10. *Golnabi* is a paper titled "Analysis of Firewall Policy
23 Rules Using Data Mining Techniques." It was published by the IEEE in
24 2006. As the title suggests, *Golnabi* relates to analyzing rules that are
25 implemented by a firewall. It seeks to improve firewall performance by
26 analyzing and modifying firewall policy rules in order to optimize firewall

1 policy and efficiency. Specifically, *Golnabi* discloses a number of
2 operations that may be performed on rulesets to increase performance and
3 efficiency. Relevant here, one of those operations is combining duplicate
4 rules with similar characteristics into one generalized rule. Other operations
5 that *Golnabi* teaches are that rules may be split or reordered, and in
6 performing these operations, *Golnabi* teaches that rulesets may provide a
7 tremendous performance gain.

8 Slide 11. Turning to the substantive arguments, first Patent Owner
9 argues that *Law* does not render obvious the limitation "one or more first
10 packet filtering rules of the first set of packet filtering rules were
11 automatically created or altered by the security policy management server."
12 Patent Owner is wrong.

13 Specifically, as detailed in the petition, a POSITA would have
14 understood that while cybersecurity risk management firm 305 necessarily
15 comprises a server, the firm distributes rulesets to the firewalls over the
16 Internet, so of course it's a server. Patent Owner doesn't really appear to
17 dispute that, while it also describes that the firm 305 constructs rulesets
18 using any type of information technology methods suitable for performing
19 such actions using electronic data and also states that those methods include
20 executing computer-implemented algorithms. And as Petitioner's expert Dr.
21 Jacobson explained, a POSITA would have understood that ruleset
22 constructing using any type of information technology methods suitable for
23 ruleset construction would have included methods for automatically
24 constructing rules.

25 Slide 12. This is particularly the case given that *Law's* background
26 expressly recognized prior art techniques for creating firewall rules by

1 "automatically locating devices and generating rules by passively analyzing
2 traffic on the network." It would have been obvious to a POSITA to
3 incorporate such known techniques for automatically generating rules for at
4 least some of the rules in ruleset 147 created by the firm 305.

5 Further, *Law* discloses that the system may automatically update or
6 alter rulesets in response to detected network conditions. Specifically,
7 paragraph 83 of *Law* states that detection of certain network conditions may
8 trigger an automatic update of the rulesets 147, which is then contrasted with
9 a different embodiment of an alarm that prompts a user to perform a manual
10 update.

11 Slide 13. Patent Owner argues that *Law* does not disclose this
12 limitation, largely repeating its arguments from the preliminary response.
13 Specifically, Patent Owner contends that *Law* does not disclose or render
14 obvious the firm 305 automatically generating rulesets because firm 305
15 would be a company that includes IT personnel. Patent Owner also contends
16 the IT personnel would still be required within *Law*'s system to manually
17 update the rulesets across those control systems.

18 Slide 14. This is the same argument rejected in the Institution
19 Decision, and it should continue to be rejected. As an initial reason, the
20 claim language includes no requirement prohibiting a security policy
21 management server from being owned by a commercial entity.

22 Slide 15. Also, Patent Owner does not meaningfully dispute the
23 evidence I just discussed that, one, the firm may construct the rulesets using
24 any type of information technology methods, using electronic data; two, that
25 *Law* recognizes that such methods includes known prior art techniques for

1 automatically generating rules; or three, that *Law*'s system discloses
2 performing automatic updates.

3 Slide 16. For example, Patent Owner's arguments regarding firm 305
4 being a company that includes IT personnel fails to rebut *Law*'s teachings
5 regarding techniques that automatically construct rules were well known,
6 and the firm 305 used any type of computer-implemented methods for
7 constructing its rules.

8 Slide 17. Patent Owner's main argument appears to be relying on a
9 background paragraph of *Law*, paragraph 16, which describes problems with
10 prior art approaches that required trained IT personnel to manage firewalls.
11 Specifically, this paragraph describes a number of disadvantages to
12 traditional firewalls managed by IT personnel. Namely, one disadvantage is
13 that IT personnel would still be required to update the ruleset when new
14 threats are discovered. Another disadvantage is that IT personnel would
15 need to be trained to understand the intricacies of the process control
16 systems to understand why certain rulesets must be changed.

17 Accordingly, *Law* explains that in such a prior art firewall, those
18 rulesets must be manually updated by IT personnel. The rulesets may
19 inadvertently provide less protection than desired, for example, due to
20 mistakes by the personnel either in failing to timely update the rules or not
21 configuring the necessary rules. *Law*'s invention solves all of these
22 problems by providing automatic updates without the necessity of involving
23 IT personnel. Nonetheless, Patent Owner still relies on paragraph 16
24 extensively and attempts to impute the disadvantages of the prior art
25 firewalls that *Law* criticizes into *Law*'s embodiment. The Board should
26 continue to adjust these arguments. Notably, although *Law* describes

1 embodiments that permit an operator to configure rules such as with respect
2 to the interface shown in Figure 13, nowhere does *Law* describe that such
3 operator involvement is required to update rules, and for good reason. Such
4 requirement would be contrary to *Law's* solutions to the disadvantages of the
5 prior art firewalls described in paragraph 16.

6 Paragraph 18 -- or sorry, slide 18. Turning to Patent Owner's next
7 argument, Patent Owner contends that *Law* in view of *Golnabi* does not
8 render obvious the limitation that recites "wherein one or more of the packet
9 filtering rules were added, removed, or altered by the security policy
10 management server based on a correlation between portions of the malicious
11 traffic information." Again, the Board should continue to reject this
12 argument.

13 As set forward in the petition, *Law* discloses receiving malicious
14 traffic information, namely threat data 310, which includes firewall ruleset
15 data from several different third party sources 315. Those sources include
16 the three examples explicitly recited by *Law*, but also include other third
17 party sources as indicated by these sources depicted in Figure 3. *Law* states
18 that -- explicitly states that the sources 315 are sources of firewall ruleset
19 data.

20 JUDGE AMUNDSON: This is Judge Amundson. I had a question on
21 that.

22 MR. DETRIXHE: Yes.

23 JUDGE AMUNDSON: And could you explain the difference
24 between the threat data provided by the sources 315 and what you call the
25 ruleset data provided by the sources 315?

1 MR. DETRIXHE: Sure. So threat data is a broader term that could
2 include other types of information, for example, the building blocks of
3 generating the rules, whereas the firewall ruleset data includes the actual
4 rules themselves, so.

5 JUDGE AMUNDSON: Could you explain, just maybe with some
6 examples, what these building blocks are?

7 MR. DETRIXHE: I mean, *Law* assumes that within, you know, the
8 knowledge of a person of ordinary skill in the art, *Law* doesn't disclose what
9 those building blocks could be other than -- other than its paragraph
10 describing, you know, how those threat data may be generated, such as by
11 prowling websites or receiving information on vulnerabilities. You know,
12 ultimately, I don't think it is material to the grounds specifically in view that
13 we're relying on the disclosures of the firewall ruleset data specifically. So
14 regardless of the outer scope of the threat data 310, as we see in paragraph
15 92, *Law* makes it explicitly clear that that threat data does include firewall
16 ruleset data.

17 And so I hope that addresses your question.

18 JUDGE AMUNDSON: Yes, thank you. Yes.

19 MR. DETRIXHE: Thank you. I'm moving on to slide 19. As the
20 petition explained, when firm 305 constructs its rulesets by processing and
21 aggregating the received threat data and ruleset data, it would have been
22 obvious to a POSITA to process the rules and remove duplicate rules using
23 *Golnabi's* technique. Specifically, *Golnabi* teaches the benefits of
24 aggregating rules by combining to get one generalized rule. And in
25 performing such actions throughout this ruleset, *Golnabi* teaches that a
26 POSITA could expect improved efficiency and even tremendous

1 performance gains. Accordingly, as the petition explained, it would have
2 been obvious to a POSITA to combine the rules, as *Golnabi* teaches, when
3 constructing rulesets, as *Law* teaches, by firm 305, using the threat data and
4 ruleset data 310 from the sources 315 because the appropriate combining of
5 rules can minimize total rules, thereby providing efficiency.

6 Slide 20. As it did in its preliminary response, Patent Owner repeats
7 this argument disputing a POSITA would have recognized that *Law's*
8 aggregation of threat data from multiple sources 315 would have given rise
9 to the problem of duplicate rules and instead asserts that Dr. Jacobson's
10 analysis was tainted by hindsight. Again, Patent Owner is wrong.

11 A POSITA's awareness that *Law's* system of aggregating threat data
12 and ruleset data from multiple independent sources would have given rise to
13 rules, that's based exclusively on the teachings of *Law* and a POSITA's
14 understanding of those teachings, not hindsight. There is no dispute that the
15 threat data and firewall ruleset data provided by the sources 315 would have
16 included duplicates, as Patent Owner's expert Dr. Goodrich admitted.
17 Specifically, Dr. Goodrich agreed that a person of ordinary skill in the art
18 would have understood there to be potential overlap in the threat data
19 provided by sources 315. Dr. Goodrich also agreed that some sources may
20 identify the same threats.

21 The only issue that appears to be in dispute is whether the
22 information provided by the sources would have included rules. As we just
23 discussed, paragraph 92 of *Law* explicitly describes that information as
24 firewall ruleset data. So the issue is whether -- whether an obvious firewall
25 ruleset data would have included rules. And I believe the answer to that, of
26 course, is yes. Dr. Jacobson explained that to be the case, but moreover, the

1 disclosure of *Law* reinforces that point, describing rulesets and ruleset data
2 interchangeably. For example, paragraph 66 of *Law* refers to ruleset data
3 147, where another paragraph, such as paragraph 51 of *Law*, refer to ruleset
4 147.

5 Slide 21. Patent Owner also disputes that a POSITA would have
6 been motivated to consider the express solution to the duplicate rule problem
7 provided by *Golnabi*. Again, Patent Owner's wrong. As explained in the
8 petition, *Golnabi* is directed to solving the same problem of removing
9 duplicate rules. In particular, *Golnabi* discloses generating policy rules for
10 firewalls designed to filter out unwanted traffic coming into or going out of a
11 secure network. And *Golnabi* expressly recognizes the importance of
12 generating a minimum number of firewall rules for reasons of efficiency.
13 And to achieve a minimum number of rules, *Golnabi* teaches merging rules
14 that have similar characteristics and combining those into one generalized
15 rule.

16 Slide 22. Next, Patent Owner asserts that even if a POSITA would
17 have been motivated to analyze *Law*'s threat data, the POSITA would have
18 found it more efficient to remove duplicate information in the threat data
19 provided by sources 315 rather than using *Golnabi*'s technique to remove the
20 duplicate rules. Again, Patent Owner's wrong. This appears to be based on
21 a misunderstanding that *Law*'s sources only provide some type of abstract
22 threat data and not the actual ruleset data, which is directly contradicted by
23 *Law*'s explicit teaching and I just went over ruleset data includes rules.

24 Slide 23. Lastly, Patent Owner argues that a POSITA setting out to
25 improve *Law*'s systems with *Golnabi*'s teachings would not have reached the
26 claimed invention in view of certain implementation details disclosed

1 *Golnabi*. Again, Patent Owner's wrong. This is similar to an argument
2 Patent Owner made in another IPR proceeding which addressed *Golnabi*
3 IPR2018-01454. There, Patent Owner argued that *Golnabi* does not disclose
4 the processing of rulesets at all, but instead discloses data mining a firewall
5 log file to extract characteristics of traffic after the traffic was already
6 received. There the Board rejected that argument, and the Board should do
7 so here for the same reasons. Specifically, a POSITA would have
8 understood that *Golnabi*'s teachings are applicable to rule optimization at
9 any time, and would have been motivated to implement *Golnabi*'s processes
10 for combining, separating, and ordering of rules in *Law*.

11 Slide 24. Addressing Patent Owner's final argument, Patent Owner
12 argues that *Law* does not render obvious the limitation that recites that "a
13 first packet matching rule comprises an indication of a feed managed by at
14 least one of the plurality of malicious host tracker services." Here, the
15 Institution Decision invited a briefing on the scope of the meaning of "an
16 indication of a feed." The Patent Owner's response acknowledged that an
17 identification of a feed is within the scope of the term. Petitioner agrees that
18 an identification of a feed is within the scope of the term and further believes
19 that *Law* renders obvious the scope under -- under that scope, under either of
20 its two theories.

21 Slide 25. Addressing the first theory, the petition explained that the
22 Protocol column 1302 in the rule table shown in Figure 13 may provide an
23 identification of a particular source 315 that generated the rule under certain
24 conditions. For example, if only one of the sources 315 provided rules with
25 a particular protocol type for a process control network, such as SCPI or
26 HART, then a listing of a rule of that protocol and the rule table would

1 identify that particular source. The Institution Decision did not agree with
2 that theory, finding that the petition had not adequately explained how a rule
3 featuring a particular protocol, such as SCPI, would have satisfied the
4 limitation's distinct requirements for the packet matching criterion, as well
5 as the identification of a feed. With respect to the packet matching criterion,
6 I would respectfully submit that although protocol 1302 is part of *Law's*
7 packet matching criterion, the packet matching criterion also includes the
8 From address column 1304, the To address column 1306, and a Port column
9 1308. So it's a much narrower set of conditions. And --

10 JUDGE AMUNDSON: I'm sorry, this is Judge Amundson. I just
11 wanted to let you know you have about five minutes left in your initial
12 allotment.

13 MR. DETRIXHE: Thank you. I'll probably go over just a little bit.

14 JUDGE AMUNDSON: Fine.

15 MR. DETRIXHE: So under this theory, only the Protocol column is
16 being relied on for the identification of the feed, whereas the Protocol
17 column as well as the From address, To address, and Port columns are relied
18 on for the packet matching criterion.

19 Slide 26. So under this theory, there would be at least some
20 occasions, not all occasions, but some, where one of the sources 315 would
21 have been the only source providing rules under a particular protocol, such
22 as SCPI, and on those occasions, that unusual protocol would have been
23 sufficient to identify that particular source to a user.

24 Slide 27. In any event, the petition also explained that Figure 13 of
25 *Law* illustrates the ruleset user interface, including protocol rule table 1300
26 that allows a user to access an interface to configure and control any other

1 rules within the ruleset 147. So, given *Law's* disclosure of receiving threat
2 data and ruleset data 310 from several sources 315, it would have been
3 obvious to a POSITA that information identifying such sources 315 of each
4 rule may be helpful to a user when using the ruleset interface to configure
5 and control the rules within the rulesets. For example, a POSITA would
6 have understood that some sources 315 may be more trustworthy or reliable
7 than others, and, therefore, it would have been obvious to communicate that
8 information to a user, such as by adding a column to the rule table 1300 to
9 indicate for each rule the source or sources 315 on which the rule is based.

10 Slide 28. Patent Owner disputes this, first arguing that Petitioner fails
11 to recognize -- reconcile how a combination of rule parameters can even
12 identify a particular source when various sources provide the same rules and
13 rule parameters. And that argument appears to be directed to the first theory.
14 But it's not Petitioner's position that it would always be the case that the
15 rules within the rulesets with particular protocols would include protocols
16 unique to a particular source, just that it would sometimes be the case, and
17 when it is, that protocol would identify the particular source.

18 Slide 29. Next, Patent Owner asserts that a POSITA would not have
19 been motivated to modify the rules as provided by firm 305 to include
20 information indicating the sources 315 the updates are from. *Law* already
21 explicitly discloses an embodiment, as we saw back in Figure 3, in which the
22 sources may deliver threat data and ruleset data directly to the firewalls,
23 thereby identifying the source of the ruleset data to those firewalls. So it
24 simply would have been obvious to include that same identifying
25 information in the rulesets distributed by firm 305.

1 Slide 30. "Lastly, Patent Owner appears to dispute that a POSITA
2 would have understood that some sources 315 are more trustworthy or
3 reliable than others. To the extent the Patent Owner is arguing that a
4 POSITA would have understood all of *Law's* sources 315, both named and
5 unnamed, to necessarily be equally trustworthy and reliable, Patent Owner is
6 simply wrong. For example, given that *Law* names exemplary sources, such
7 as Assurent, Secunia, and Carnegie Mellon, as well as disclosing additional
8 unnamed sources, a POSITA would have understood that it's impossible to
9 say that the unnamed sources are equally as reliable and trustworthy as the
10 named sources.

11 Furthermore, "a POSITA would have understood the possibility of
12 errors in the ruleset information provided by the sources," as Dr. Goodrich
13 agreed. Patent Owner's expert Dr. Goodrich agreed that the data provided
14 by any of the sources would not necessarily be correct. And "given the
15 possibility for errors in the information provided by the sources," which goes
16 to its trustworthiness, "a POSITA would have understood that all possible
17 sources 315 are not necessarily equally trustworthy, reliable, or error prone."
18 Accordingly, Patent Owner's stated reasons for disputing the obviousness of
19 including identifying information of the sources 315 have no merit.

20 I'll reserve the remainder of my time for rebuttal. Thank you.

21 JUDGE AMUNDSON: All right. So are you done with your
22 arguments and your opening?

23 MR. DETRIXHE: Yes, Your Honor.

24 JUDGE AMUNDSON: All right. So there was something I wanted
25 to ask about. If you could go to page 3 in the petition, the grounds table.

26 MR. DETRIXHE: Yes.

1 Speaker A: The grounds table. Ground 1, *Law* and *Golnabi*.

2 MR. DETRIXHE: Yes.

3 JUDGE AMUNDSON: So, I want to ask about five dependent
4 claims: claim 6, claim 14, claim 22, claim 30, and claim 33, which are
5 included in ground 1. I did not see in the petition any arguments on those
6 five dependent claims. You could scroll up to the second page of the table of
7 contents, and you'll see some dependent claims that are listed there. But --
8 yeah, right there at the top of that second page of the table of contents. But
9 you don't see claims 6, 14, 22, 30, and 33. And then I didn't see anywhere in
10 the petition where there was an argument on those five dependent claims. So
11 I was wondering if I missed something there.

12 MR. DETRIXHE: Hold on. Sorry, Your Honor, could you repeat the
13 claim numbers?

14 JUDGE AMUNDSON: Okay. It's 6, 14, 22, and 30, and they're all
15 similar in scope. And then claim 33.

16 MR. DETRIXHE: Got it. Yes. This, I believe (phonetic), I'm
17 looking at claim 6, is a limitation addressed by the dependent claims and the
18 other grounds. Specifically, I believe that is the combination.

19 Well, Your Honor, actually, let me address that in my rebuttal time.
20 I'll look at it --

21 JUDGE AMUNDSON: All right.

22 MR. DETRIXHE: -- and get back to you more.

23 JUDGE AMUNDSON: So the question is just if it's there, where is
24 it? That's my question, okay?

25 All right. Very well. Okay. So I think you have about nine minutes
26 left in the -- for the rebuttal.

1 MR. DETRIXHE: Thank you, Your Honor.

2 JUDGE AMUNDSON: Mr. Price, would you like to reserve time for
3 surrebuttal?

4 MR. PRICE: Yes, Your Honor, I will reserve 10 minutes for
5 surrebuttal.

6 JUDGE AMUNDSON: All right, very well. You may begin when
7 you're ready.

8 MR. PRICE: Thank you, Your Honor. And may it please the Board,
9 Your Honor, we also could not find any basis in the petition challenging the
10 dependent claims that you brought up at the end of the -- at the end of the
11 case. And, you know, I think on those claims we would say that Petitioner
12 hasn't even attempted to meet its burden and that the Board should find those
13 claims patentable.

14 JUDGE AMUNDSON: This is Judge Amundson. I understand that,
15 but could you explain why you didn't say why Centripetal didn't say
16 anything about those five dependent claims in its briefs?

17 MR. PRICE: Yeah. I think, Your Honor, there was no obviousness
18 analysis put, you know, into those claims. And, you know, how could we
19 rebut anything that's not made of record for us to look at? It's always
20 Petitioner's burden to identify the grounds, which they did, and then explain
21 with particularity why the claims are invalid under the grounds that were
22 identified. Again, we have the grounds, we have the claims, and we don't
23 have any proof. And that means that those claims -- the Petitioner has not
24 met his burden on those claims.

25 JUDGE AMUNDSON: All right, thank you.

1 MR. PRICE: So I'm on page 2 of our demonstratives, and I'll just run
2 through quickly the map of the arguments that we'll be making. First, we'll
3 be going over the grounds, as we just spoke about, then the overview of the
4 '474 patent, and then we'll get into the three main reasons why all of the
5 claims in this case are patentable.

6 First, the firm 305 disclosed in *Law* is not a security policy
7 management server. There has been no server identified in firm 305 and
8 certainly not a server that does the things that the server of the '474 patent
9 has to do. One of the main reasons for that is that IT personnel in firm 305
10 are there, and they are there to ensure that the rules that are provided to the
11 devices are suitable to protect the systems that they protect, which, as Your
12 Honors are aware, are not, you know, just running in those systems, but
13 they're nuclear reactors. They're, you know, they're very, very
14 individualized and important process control networks.

15 Next, we'll move on to why Petitioner's argument that *Law* in view of
16 *Golnabi* teaches the limitations about correlating malicious traffic
17 information. Your Honor, I mean, basically, there's no disclosure in *Law* or
18 *Golnabi* about correlating malicious traffic information. Petitioner's -- you
19 know, this problem that Petitioner says existed in the art was not recognized
20 in *Golnabi*, nor were any solutions. And the solutions provided in *Golnabi*
21 have nothing to do with correlating malicious traffic information. So what's
22 missing from *Law* is not found in *Golnabi*. It's not found in the knowledge
23 of a person of ordinary skill in the art. And what we'll show is that all of the
24 arguments as to how *Law* alone or with *Golnabi* reached this limitation are
25 based fully on ex-post reasoning, based on the benefits disclosed in -- of this
26 technique disclosed in the '474 patent. And what a Petitioner can't do is

1 come in and say, well, this invention has these certain benefits that were
2 recognized. Therefore, those benefits render the claims obvious, which is
3 what Petitioner has done in this case.

4 A very similar analysis will apply to the last main argument that we
5 have, which are about the indication of a feed. Now, it's not disputed that
6 *Law* doesn't disclose an indication of a feed. It's not disputed that *Golnabi*
7 doesn't teach an indication of a feed. So what we have are attempts, ex-post
8 reasoning, trying to justify a situation in which a person of ordinary skill in
9 the art, might be able to determine where a rule came from, which is not an
10 indication of a feed.

11 JUDGE AMUNDSON: On that, this is Judge Amundson, on that
12 point, could you explain Centripetal's position on what an indication of a
13 feed is?

14 MR. PRICE: It has to indicate the feed. It has to tell you what the
15 feed is. And that's just what the language is, right? There has to be
16 information that tells you the feed that this rule was based on. I mean, that's
17 just the plain meaning of an indication. Right? It has to actually indicate the
18 feed. It's not something, you know, where, you know, if you have exactly
19 the right information and you put the sleuths, you know, and your team on
20 there, they might be able to figure out within some, you know, error bar,
21 right, that, you know, maybe it came from this feed originally. That's, you
22 know, that's not an indication of a feed.

23 JUDGE AMUNDSON: Could you give us maybe a couple of
24 examples of what would be an indication of a feed?

25 MR. PRICE: Sure. You know, for example, in, you know, the
26 Carnegie Mellon example, right, in *Law*, if that qualifies as a feed for

1 malicious traffic information, you would have an indication saying Carnegie
2 Mellon.

3 JUDGE AMUNDSON: All right, thank you.

4 MR. PRICE: Sure. Okay, I'm now on slide 4. This is just a summary
5 of the IPR grounds. As you can see, the Petitioner included the claims that
6 Your Honor identified, including 6 and 22 and 26 and 30 in this table, but
7 has provided no proof that these claims are actually obvious over the
8 references.

9 Just giving a slight background on the '474 patent. This patent is all
10 about Centripetal's techniques for operationalizing threat intelligence data
11 and how to make that data actionable at a security device, at a network
12 security device. On page 5 -- page 6 here, we just have highlighted the
13 abstract, but just to give Your Honors a little bit of background here. There
14 are these feeds out on the Internet. They were at the time of the invention.
15 And what they would do is they would provide information about malicious
16 traffic on the Internet.

17 You know, for example, there might be some suspicious IP addresses
18 that are collected. But prior to Centripetal's inventions these data were not
19 used proactively to prevent a network from being harmed. And the reason
20 for that is the amount of data that comes in from these feeds has to be
21 translated into rules, and then the rules have to be provisioned to the devices
22 in order for them to actually be actionable. And so what Centripetal had
23 done was they created a technique where you could, you know, have a
24 security policy management server, which is a server that manages security
25 policies. It takes in all of this information from different sources and
26 automatically creates the rules that are going to be pushed to the network

1 protection devices. And the reason that it has to be automatic is because this
2 data changes very quickly. So an IP address that might be suspicious one
3 day, might not be suspicious the next day. And what the security policy
4 management server does is it makes sure that all of the, you know, the
5 information is automatically, right, because there is no manual way of
6 handling the amount of data and the types of data and putting that -- you
7 know, getting it to the network protection devices in a timely manner, so
8 Centripetal developed algorithms for automatically generating rules and also
9 automatically making the rulesets more -- I'm sorry, and making the rulesets
10 more efficient.

11 So how is that different from what *Law* is doing? *Law* is a system,
12 like we just talked about earlier, where it's a process control network, you
13 know, for potentially, you know, a nuclear reactor. And what *Law* was
14 concerned with was this idea that you would have specifically trained
15 operators on the system who know the process control network inside and
16 out. And what the prior art was missing was the ability for a person sitting
17 on that network, on that process control network, one of these operators, to
18 be able to manage the security of the network. Because in the old system,
19 you would have these trained IT personnel who had to become experts in the
20 process control system in order for them to make rules that would
21 adequately protect that system.

22 So what did *Law* do? *Law* said, well, we really want our operators to
23 have more control over this. We don't want to be relying, you know,
24 completely on the IT personnel at this third party firm because they're not
25 going to know the ins and outs of our process control network. So *Law* is all
26 about keeping firm 305 in place, keeping, you know, their IT personnel over

1 there. What *Law* does and says is you don't have to be as specifically trained
2 on each process control network, IT personnel at firm 305, because we're
3 going to have our operators handle the network-specific stuff.

4 And so what they do is those operators generate the first ruleset.
5 They send it up to 305 to get updated with, you know, additional security
6 rules. Because what *Law* also says is that these operators are not security
7 experts. Right? They're experts on the process control network, they're not
8 experts on network security. So what *Law* has is these two different sources
9 for rules. One is the operators who create the initial ruleset, and then one is
10 the IT personnel at firm 305 who take in the information, make sure that
11 when the rules are generated are going to adequately protect the network,
12 and then they put the rules in and they send that security policy back to the
13 device for implementation. So that background of *Law* will come up a lot
14 throughout the rest of the presentation.

15 So, on page 7, I just have a diagram of the kind of network overview
16 what the network architecture is going to look like. You have a security
17 management -- a security policy management server that's connected to the
18 network, the Internet, and then you have, you know, various networks, local
19 area networks, for example, that are each protected by a PSG, a packet
20 security gateway. So what the '474 does is it has the security policy
21 management server, takes in this feed data, automatically generates the rules,
22 makes them more efficient, and then sends them off to be implemented.

23 Okay. Moving on to page 10, the first argument is firm 305 is not a
24 security policy management server. So firm 305 is a commercial entity.
25 Right? It's a company, it has hardware infrastructure and it has IT
26 personnel. And so firm 305 itself is not a server. There are various things

1 that firm 305 does that a security policy management server, certain things,
2 not all of the things, but certain things that the firm 305 will do that the
3 security policy management server does, but what Petitioner has not
4 identified is the server that does these things. That indication of a server that
5 does these things is missing from the petition.

6 Now, all of the -- we have many, many arguments about why it
7 wouldn't have been obvious to do these things on a server. What, you know,
8 what the problems would, you know, would have been if we buy into
9 Petitioner's obviousness argument that all these things would happen on a
10 server. But what we don't have as, you know, baseline -- as the baseline
11 here is the identification of a server in 305 that does the things that the
12 security policy management server has to do.

13 Now, it is of utmost importance that the Petitioners adhere to the
14 requirement to identify with particularity the evidence that supports the
15 grounds for each claim. And there is no server identified that does what the
16 security policy management server of the 305 -- of the '474 patent has to do.

17 JUDGE AMUNDSON: I had a question on that. I have the Microsoft
18 Dictionary, Fifth Edition, 2005. And if I go to page 474 and look at the
19 definition of server, it states the second definition, "On the Internet or other
20 network, a computer or program that responds to commands from a client."
21 So with that understanding of a server, and then I note that *Law* in
22 paragraphs 88 and 90 discloses that a ruleset can be a data file, my question
23 is, how would firm 305 distribute a ruleset data file to a firewall if firm 305
24 did not include a server like a file server or an email server?

25 MR. PRICE: Okay, so, Your Honor, was that, that of record?

1 JUDGE AMUNDSON: Well, it is now, but it hasn't been until now.
2 But if you got a different definition of a server you want to advance, let's
3 hear it.

4 MR. PRICE: Okay, so a couple things. Obviously, the definition is
5 not of record. I'm not saying it's wrong, I'm not saying it's right. I'm saying
6 we haven't had the opportunity to, before the hearing today, conceptualize
7 the case in terms of that definition. However, what I would say is there's a
8 big difference between a computer that sends a ruleset and the security
9 policy management server that has to generate rules. Right? So to the
10 extent that there is a computer that actually is involved in sending this thing,
11 there are a lot of other limited -- a lot of other things that the security policy
12 management server has to do that are not just sending a data file to a process
13 control network.

14 And, you know, Centripetal never took the position that firm 305
15 wouldn't have any servers. Right? The idea that, you know, firm 305 would
16 have, you know, hardware, infrastructure components as part of, you know,
17 its oeuvre is going to be -- that's not in dispute. What's in dispute is there
18 has been no server identified that does the things that a security policy
19 management server has to do in the '474 patent.

20 JUDGE AMUNDSON: All right. I think I understand your position
21 about a specific identification. But as I understand the record, Dr. Jacobson
22 testified in his initial declaration that firm 305 would necessarily include a
23 server. Is there evidence in the record that contradicts his testimony?

24 MR. PRICE: Yeah, a couple of things, Your Honor. One, in *Law*, in
25 this paragraph that we're talking about, 88, there's no -- there's no disclosure

1 here of it being, you know, a client server response as opposed to just a
2 push. That's one thing.

3 But the -- Dr. Jacobson said that firm 305 necessarily includes a
4 server, but that was conclusory testimony. There was nothing backing it up.
5 He just said it. So I understand that's evidence, but it's conclusory evidence
6 that can't support a finding that will be upheld on appeal under substantial
7 evidence standard, because conclusory expert testimony like that is not
8 evidence -- is not evidence that can -- is not substantial evidence for
9 decision. You know, I think this is a theme here is that we, you know, we
10 recognize, Petitioner recognizes that these limitations are not in the art. And
11 what we are trying to do now is finding ways to bridge the gap between the
12 art and the record, all based on ex-post reasoning or conclusory testimony.
13 And that's what we have here.

14 JUDGE AMUNDSON: All right, thank you. I think I understand the
15 position.

16 MR. PRICE: Okay, change the clicker's number. Okay.

17 Moving up to slide 12. We do have testimony from Dr. Jacobson who
18 says that you have to have the staff to manage the infrastructure and that the
19 staff needs to know about the threats. Right. So, in addition to the hardware
20 infrastructure that is part of firm 305, *Law* also teaches that firm 305 is made
21 up of people. And these people, the IT personnel, are critical to ensuring
22 that the rules that end up getting sent to the process control networks are --
23 will adequately protect the system.

24 So *Law* explains over and over again how and why IT personnel must
25 be involved in managing the security of the process control network. So
26 starting at paragraph 16. I know my friend said that, you know, our

1 argument was based entirely on paragraph 16 and paragraph 16 is about the
2 prior art commercial off-the-shelf firewall system. Now, this is true to an
3 extent that this is talking about what's in the prior art, that in these old
4 systems, the off-the-shelf firewall systems, IT personnel were required to
5 update the ruleset when new threats are discovered or upgrades are -- to the
6 software components are implemented. Now, what my friend is trying to
7 suggest is that this was the old way of doing things. Now we don't need IT
8 personnel at all.

9 Slide 15 says differently. So slide 15, looking at paragraph 21 of
10 *Law*, this tells you what the problem was that *Law* was trying to solve. This
11 says -- you know, it talks about this Byres application. And I will come
12 back to this paragraph 21 and talking about this Byres application because
13 it's one of the pieces of state of the art evidence that Petitioner's relying on
14 for automatic rule generation. However, I haven't been able to find Byres. I
15 look for it. It doesn't seem to exist. I look for it by the inventor's name. I
16 looked for it by the title. I looked for it by the application, by the supposed
17 publication number. It doesn't exist as far as I can tell.

18 JUDGE AMUNDSON: This is Judge Amundson. All right. There's
19 an error in the patent application publication number specified in paragraph
20 21. In particular, the last digit of the publication number is missing. It's the
21 digit 1. So if you added a digit 1 to that publication number, you could find
22 it.

23 MR. PRICE: Okay. It is not of record, obviously.

24 JUDGE AMUNDSON: Okay. All right.

25 MR. PRICE: You know, we should spend a little bit of time talking
26 about what's happening here. So, first of all, what's not happening here is

1 automatic ruleset generation based on what's disclosed -- what's in this
2 paragraph. The word "automatic" is in here, but what's done automatically
3 is locating the devices on the network. I think my friend is trying to suggest
4 that the word "automatically" modifies both locating devices and generating
5 rules, but that's not what this says. Because what's happening here, based on
6 this disclosure, is that you passively analyze traffic on the network. And
7 what that can do is give you an indication that, hey, there's a new device on
8 this network, and we're going to have to do something to figure out how to
9 protect this device. Or it might be that they recognize a new device on the
10 network that shouldn't be there and, hey, we better call these guys up and
11 say, you know, it looks like there's a problem here. There's nothing about
12 automatic rule generation here.

13 And why? Because what *Law* is saying here, the problem with this
14 solution is that, yeah, you still need IT personnel to do what the IT personnel
15 always do. But what you want to have is more control by the operators on
16 the system who are, you know -- who know the system in and out. These
17 operators in the system still are not IT personnel. They're not security
18 experts. They're experts on their process control network, which is why you
19 still have firm 305 in the loop for the security portions of this. And, you
20 know, there is no disclosure that they can be taken out of the loop when it
21 comes to generating the rules that go back to the process control network.

22 Okay. And so now moving on to slide 16, we're talking about, okay,
23 would it have been obvious to modify firm 305 so that you could do this
24 automatically without the input of the IT personnel? And what we have here
25 in 88 is no disclosure of how or why you would modify what *Law* is actually
26 teaching in order to do this automatically. It's a missing disclosure. Right?

1 So, you know, it's Petitioner arguing that this would have been
2 obvious, but everything from *Law*, which -- and you have to take *Law* in its
3 entirety, everything from *Law* is telling you that we need the IT personnel.
4 They're important. They're the ones who are making sure that the security is
5 maintained on these process control networks. There are no disclosures of
6 any methods that could forego the required manual input of it personnel.

7 JUDGE TURNER: Counsel, this is Judge Turner. I guess -- I'm
8 sorry, can you go back to the previous slide?

9 MR. PRICE: Yeah.

10 JUDGE TURNER: So, if we take -- if we look at the sentence, let's
11 say it's actually off of your highlighted section, that it may be performing
12 any type of information technology methods suitable for performing such
13 action using electronic data. Seems like that's broader. And it seems like
14 that's what Petitioner is sort of bootstrapping their way off of saying, well, if
15 I'm one of ordinary skill in the art, why wouldn't automation be obvious?

16 MR. PRICE: Okay, so a couple things. One, for state of the art
17 evidence, we don't have it. You know, so, you know, when we're talking
18 about, you know, the argument that it would have been obvious to do this
19 automatically, what we don't have -- we have reliance solely on state of the
20 art, but not an argument as to how and why a person of ordinary skill in the
21 art would have done it given the disclosure of *Law*. Right? And what *Law*
22 tells you and what -- what the *Law* tells you is you can't focus in narrowly
23 on, you know, one specific aspect while forgetting about the rest of the
24 disclosures.

25 So, yes, *Law* a hundred percent says that any suitable technology
26 methods for performing these actions using electronic data are within the

1 scope of *Law*. What we don't see is any state of the art information saying
2 that you're automatically generating rules using the information that is in our
3 claims. Right?

4 So, you know, if we pull up the '474 claims, what do we have? "One
5 or more of the packet filtering rules of the dynamic security policy were
6 automatically created or altered by the security policy management server."
7 And here it is "based on malicious traffic information received from a
8 plurality of malicious host tracker services." Now, what we don't have is
9 any state of the art evidence that it was known how to generate these kinds
10 of rules, right, based on the malicious traffic information received from a
11 plurality of malicious host tracker services that could stand in for the
12 nondisclosure in *Law*. Right?

13 So are there techniques for automatically generating rules? I don't
14 see that in the record as state of the art evidence. I don't. But what we
15 definitely don't see is any rules automatically created based on malicious
16 traffic information received from a plurality of malicious host tracker
17 services. So there's still a gap. You know, even granting the idea that some
18 kind of automatic rule generation was known, you don't have any evidence
19 in the record that says that these kinds of rules were known to be generated
20 automatically.

21 JUDGE TURNER: And this is Judge Turner. Again, let me come
22 back. And it also doesn't say in the record that, you know, how I learn an IP
23 address, I manually write it down, all the numbers down with my pen, and I
24 go to a different computer and I manually enter all those in. I think at some
25 point we have to take, you know, take what one of ordinary skill in the art
26 would do. And, you know, I'm sure, you know, I could bang rocks and

1 communicate. I mean, there's all kinds of things that I think we have to sort
2 of be within the realm here when they're talking about, you know, suitable
3 for performing the actions and those methods. I mean, that's fairly broad. I
4 understand you're saying, well, they didn't specifically point out, well, you
5 know, we don't have, you know, voluminous records here where, you know,
6 we're citing the Library of Congress. You know, at some point, we have to
7 sort of say, one of ordinary skill in the art would have known.

8 So I take your argument. I understand what you're saying, but I feel
9 the need to sort of push back and say, why wouldn't it be obvious to do this
10 in an automatic fashion? And again, it's not really creation, but it's also, you
11 know, alteration.

12 MR. PRICE: So, thank you, Your Honor. A couple things there.
13 First of all, it wouldn't have been obvious, and for the reasons that I'm going
14 to get to, that *Law* specifically says that -- you know, requires its IT
15 personnel to be in the loop for all the reasons that *Law* says.

16 The other thing, Your Honor, is that Petitioner had the opportunity to
17 cite anything of relevance. Yeah, I mean, you talked about it voluminous
18 record, but Petitioner is in control of the record. If Petitioner had state of the
19 art evidence that said it was known to do this, right, which is what you use
20 state of the art evidence for, then it was incumbent on them to identify that
21 evidence. If you don't need that, then I don't know what we're doing here,
22 because these decisions have to be based on evidence in the record.

23 Otherwise, there's nothing for the Patent Owner to address. Right?

24 The burden is always on the Petitioner to come up with this evidence,
25 to put it in the record, and to explain how it gets the claims to be obvious.
26 And, you know, reliance on, you know, this one sentence in *Law* talking

1 about, you know, any time of -- any kind -- type of information technology
2 methods suitable, they haven't demonstrated that there was an information
3 technology method suitable for doing what the claims require.

4 JUDGE AMUNDSON: This is Judge Amundson. I just wanted to
5 point out you probably have about five minutes left in your initially
6 requested allotment of time.

7 MR. PRICE: Okay, thank you. I'm going to move on. So, slide 17,
8 this was another piece of evidence that a Petitioner tried to parlay into an
9 argument that would have been obvious for firm 305 to automatically
10 generate or update rules. But this isn't -- this paragraph 83 is not about firm
11 305. This paragraph is about detecting a particular network condition at the
12 process control network and either manually updating rules to deal with that
13 network condition or requesting an automatic update. Right? So, you know,
14 maybe firm 305 has an update ready to go and they can go and, you know,
15 request that or it gets sent. It's not entirely clear, but what it's not saying is
16 that firm 305 is doing anything automatically.

17 And returning to the state of the art techniques on page 18. Again,
18 these are two key legal premises that, you know, can't get lost in the shuffle
19 here. The prior art has to be considered for all its teachings, not selectively.
20 So when we're talking about the known information technology techniques
21 that you can use, you're not going to do something that's antithetical to what
22 *Law* is teaching. You're not going to cut the IT personnel out of the loop
23 just because, you know, if there was the state of the art evidence in the
24 record, just because that state of the art evidence is in there. And the
25 Petitioner has to provide adequately developed explanations and not just,
26 you know, wave their hands at these vague statements.

1 So, again, you know, on page 19 -- I'm going to move on so I can get
2 to -- I think I made my point there.

3 All right, *Law* and *Golnabi*. I'm on page 23 now. So there's no
4 dispute that neither *Law* nor *Golnabi* discloses correlating threat data. That's
5 missing from the record. So what do we have here? We have another ex-
6 post explanation as to why a person of ordinary skill in the art would have
7 done what the claims teach.

8 However, the problem and the solution both come from the '474
9 patent. Right? There is no, you know, indication in *Law* that, you know,
10 these duplicate rules and the threat data were a problem that he or she even,
11 you know, was aware of. And *Law* did not provide a solution to that. *Law*
12 certainly didn't provide a solution to that by correlating the threat data.
13 *Golnabi* doesn't either.

14 *Golnabi* has its own technique. *Golnabi* has this technique where
15 you're looking -- you're running traffic through a firewall, submitting it to
16 rules. You create firewall logs, and then you do, you know, some ruleset
17 efficiency work there. So *Golnabi* doesn't have the piece that *Law* is
18 missing.

19 JUDGE AMUNDSON: This is Judge Amundson. I just -- I wanted
20 to follow up on that. And if you could go, I think it's, yeah, it's page 312 in
21 *Golnabi*, Exhibit 1009. Do you have that?

22 MR. PRICE: I'm getting it. I'll be there when -- go ahead.

23 JUDGE AMUNDSON: All right. In the lower left column, as I
24 understand it, and correct me if I'm wrong, this is in Figure 10, the Linux
25 firewall rules that *Golnabi* used when it created the log and then applied its

1 data mining rule and then its data mining algorithm, and then applied the
2 FRG algorithm after that.

3 So here's my question. If instead of using the Figure 10 ruleset, an
4 ordinarily skilled artisan replaced it with a ruleset from firm 305, why
5 wouldn't they get to the claimed invention?

6 MR. PRICE: So, all right. First of all, is this an argument that was
7 made in the record or this is a hypothetical that you're asking me about now?

8 JUDGE AMUNDSON: As I understand the Petitioner's theory of
9 combining the teachings of *Golnabi* and *Law*, this is one way an ordinarily
10 skilled artisan would have done it.

11 MR. PRICE: So a couple things then. So, first, we got to think about
12 where is this ruleset coming from in *Law*, right, that would then be, you
13 know, involved in *Golnabi*'s techniques? This ruleset initially comes from
14 the process control network, right? It's the operator control -- the operator-
15 generated ruleset that gets sent to firm 305 to be updated. So there's not
16 going to be any duplicate rules. There's not going to be anything in there,
17 you know, for *Golnabi*'s techniques to work on because it's just, you know,
18 the original stuff that the operator said should be in there, and it has nothing
19 to do with the rules that were, you know, generated based on the alleged
20 malicious traffic information.

21 But I don't know what else to say about your question, because I'm
22 not entirely sure what Your Honor is suggesting would happen differently.
23 In that case --

24 JUDGE AMUNDSON: Well, here, this is what I -- this is -- correct
25 me if I'm wrong, if the way I understand *Law*, at some point you're going to
26 get an updated ruleset from firm 305 and it's going to be based on malicious

1 traffic information. You're going to get an updated ruleset. And if a person
2 of ordinary skill in the art wanted to make that better, according to *Golnabi*,
3 why wouldn't they take that updated ruleset from firm 305 and do what
4 *Golnabi* does with its MLF algorithm and its FRG algorithm? And then
5 when it does that, when the person of ordinary skill would do that, why
6 wouldn't they combine rules according to the claims?

7 MR. PRICE: So, a couple of things. For *Golnabi*'s technique to
8 actually be instantiated in the system, you would have to send the ruleset
9 back to the process control network first so that you could run traffic through
10 it. Then you don't have the security policy management server doing the
11 things that it needs to do. Right? Because now the ruleset is sitting at
12 process control network 150 in order for it to actually generate the live data.
13 Right?

14 JUDGE AMUNDSON: Okay.

15 MR. PRICE: So then you don't have a security policy management
16 server that's doing the updating the -- you know, we're at firm 305, you don't
17 have that doing that anymore. But, you know, more fundamentally, you
18 don't have -- using *Golnabi* in this way or the way that the Petitioner used it
19 doesn't have anything to do with correlating threat data. Right? So even if a
20 person of ordinary skill in the art was presented with *Law*, was presented
21 with *Golnabi*, they have a map for how to combine these things. Right? It
22 has nothing to do with correlating threat data, right, which is what the claims
23 say. So, you know, that's the main point that we want, you know, to get
24 across here is that this idea that you would do what *Golnabi*'s teaching, you
25 know, combining rules, whatever, by correlating threat data is missing from

1 the art. And all of the arguments as to how and why you would put it
2 together are based on ex-post reasoning from the '474 patent.

3 Again, we have claim language that says do it in this specific way.
4 The art doesn't do that. And now we're trying to backfill reasoning for how
5 and why a person of ordinary skill in the art would have done it this way, but
6 you don't have that. So, that's on page 24, "At best, a person of ordinary
7 skill in the art would have removed duplicate data from the analyzed threat
8 data, not from the dynamic security policy."

9 Just before I run out of time, I want to get to the indication of a feed
10 argument. There are two arguments. One is that you would be able to
11 somehow figure out who was responsible for sending this feed based on
12 some information in the rules themselves. You know, I think that doesn't
13 reach the claims. It's not an indication of a feed. Right? You know, what's
14 in a particular rule is not -- what's in a particular rule has nothing to do with
15 -- it doesn't indicate what feed it was.

16 We asked Dr. Jacobson about this during his deposition, you know,
17 because Petitioner made this, you know, this big case about how the SCPI
18 protocol, you know, is -- you know, it's not used very often, so it would
19 probably only be, you know, sent out by one feed and maybe then you could
20 figure out who sent it. Dr. Jacobson doesn't even know what the SCPI feed
21 is, so, you know, I don't think that that argument holds any water.

22 So what's the next argument? The next argument is it would have
23 been obvious to stick this thing in there. And again, what we're -- we're not
24 looking at any disclosures in the art. What we're looking at is, well, the '474
25 patent disclosed this. It claimed this. It gives the operator, you know, the
26 network administrator some additional information. That's great. And then

1 uses that as an argument that it would have been obvious to do this in the
2 first place. This is ex-post reasoning, it's hindsight, and it's forbidden.

3 And so with that, I'll reserve the rest of my time.

4 JUDGE AMUNDSON: All right. I think you have about five
5 minutes or so for the surrebuttal.

6 MR. PRICE: Thank you, Your Honor.

7 JUDGE AMUNDSON: Mr. Detrixhe, you can begin your rebuttal
8 whenever you're ready.

9 MR. DETRIXHE: Thank you, Your Honor. First, I would like to
10 address Your Honor's question regarding claims 6, 14, 22, and 30. Each of
11 those claims recite the packet security gateway is a LAN switch. The
12 petition could have been more clear, but those limitations are addressed in
13 the petition. Specifically, as we've been over numerous times, the packet
14 feed security gateway corresponds to firewalls 146a and b. The petition also
15 cites paragraph 54 of *Law* numerous times on pages 12, 15, and 21. And
16 there *Law* states that a network device 146 includes one or more of a
17 network switch and a firewall. So that's explicitly equating the packet
18 security gateway 146 with a firewall.

19 So the substance of the claims was addressed in petition. I apologize,
20 the petition certainly could have been more clear on that point, but thank you
21 to Your Honors for raising that issue.

22 And I'd also point out that the scheduling order cautions Patent
23 Owner that any patentability arguments not raised in the response may be
24 deemed waived.

25 Next, I'd like sort of address Your Honor's question regarding claim
26 33. That one recites that the packet transformation function is configured to

1 route packets to a monitoring device. There, that was just a typo. That was
2 fully addressed in the petition on page 73, where it explains it would have
3 been obvious in view of *Law* to route a subset of information on the
4 identified packet to a packet monitoring device, citing paragraph 168 of Dr.
5 Jacobson's declaration, Exhibit 1003, as well as paragraph 1003 of *Law* that
6 states that other actions may include, but are not limited to log, notify, and
7 reroute.

8 I'd like to turn to some of Patent Owner's arguments very briefly.
9 You know, first, the whole notion distinguishing *Law* with the idea that *Law*
10 requires you to have trained operators to know that the process control
11 system inside and out, and that's exactly contradictory to the problem
12 solving. Again, that goes back to paragraph 16 of *Law*, which in great detail
13 explains the problems of that approach and it's what *Law* was trying to solve
14 by having a system for doing automatic updates. It doesn't mean -- you
15 know, sure, it would be nice to have specifically trained personnel who
16 know the process control system inside and out. And *Law* provides the
17 capability to tinker with the rulesets if you have an operator who wants to do
18 so. But *Law* is by no means limited to requiring such a trained IT personnel
19 in order to function.

20 You know, regarding the description and the background in
21 paragraph 21 regarding the reference that discloses techniques for automatic
22 ruleset generation being known, and there I would point out, you know, the
23 petition isn't relying on a combination of *Law* and that reference. The
24 petition is relying on the express acknowledgement in that background that
25 automatic ruleset generation techniques were well known and that's stated on
26 the basis of *Law* itself in describing that patent.

1 I'd also point out that even the '474 patent itself assumes that
2 techniques to generate -- automatically generate rulesets were well known.
3 Specifically, there's only a single sentence in the entire specification at
4 column 15, line 7, that states that the security policy management server 120
5 may be configured to automatically create or alter one or more of such rules
6 as new network addresses associated with malicious network traffic are
7 determined. That's the extent of the disclosure.

8 The '474 patent assumes a person of skill in the art would understand
9 how to automatically generate rules using known techniques, just as *Law*. In
10 fact, *Law* provides more description by the reference in the background in
11 paragraph 21 to the techniques disclosed there, as well as its statement in
12 paragraph 88 to generate rulesets using any information technology
13 methods.

14 There was some discussion that in paragraph 21 that the automatic
15 was only modifying, locating, and not just generating, you know. I'd say
16 that's not the case, and it's certainly not what the disclosure would be
17 considered for obviousness purposes, especially in view of the description of
18 it being passive. If automatic did not also modify the generation of rules, it
19 simply wouldn't be a passive system as is disclosed there.

20 You know, next, on the notion that firm 305 is not a server, I agree
21 that it's broader than a server, but it certainly includes a server. You know,
22 that's in the petition. And Dr. Jacobson pointed out that firm 305 necessarily
23 includes a server. And I'm still confused at how the firm 305 electronically
24 processes rules and distributes them over the Internet without being a server.
25 That's completely ridiculous for Patent Owner to even make this argument.
26 It's just otherwise. But in any event, supported by Dr. Jacobson's testimony

1 is more than sufficient to explain why the firm 305 necessarily includes the
2 server, including that it would be necessary to perform those functions I just
3 mentioned, generating the rules that's being distributed to the firewalls over
4 the Internet.

5 And then lastly, I'd like to address what counsel discussed regarding
6 correlating threat data as being completely missing from the art. Again, I
7 think this is based on the mistaken notion that threat data does not include
8 rule data. As I went over earlier, the threat data 310 provided by *Law's*
9 sources 315 are explicitly described in paragraph 92 as including ruleset
10 data. And so the combination of *Law* in view of *Golnabi*, you know, in
11 order to determine the duplicate rules and the overlap, as Dr. Jacobson
12 explained that it necessarily would have entailed correlating those rules to
13 determine the duplicates.

14 So, that's all I have to rebuttal. I cede the remainder of my time.
15 Thank you, Your Honors.

16 JUDGE AMUNDSON: All right, thank you. Mr. Price, you can
17 begin whenever you're ready.

18 MR. PRICE: Okay, thank you, Your Honor. In terms of the
19 automatic generation of rules, again, what we don't have is an -- is really any
20 evidence of state of the art, including automatic rule generation. But even if
21 we gave the most broad reading to *Law* as possible, what we don't have is
22 automatic rule generation based on this data, the malicious traffic
23 information data. I know, Your Honor, in the Institution Decision mentions
24 a -- the *Ke* reference which was cited during prosecution of the '474 patent.
25 That was about using -- not about basing this on malicious traffic

1 information data. That was about automatically creating rules with virus
2 signatures, which is different.

3 So again, what we don't have is any disclosure state of the art
4 knowledge in the record of automatically generating or updating rules based
5 on malicious traffic information. It's missing.

6 My friend said that the -- there's this idea of maybe the threat
7 information including rules. That doesn't help them get to the limitation,
8 because what does it require? It requires correlating. Right? It requires that
9 the rules be generated at the SPMS, right, not received from the threat data
10 sources. Right? So already we're not in the realm of the claims if we're
11 talking about receiving rules from, you know, one of these third party
12 sources. But it doesn't -- it also has nothing to do with, you know,
13 modifying what they're calling the dynamic security policy, which is the
14 thing that was generated at the process control network and sent over to firm
15 305. So just because -- even granting this argument that these threat sources
16 are going to have, you know, data in the form of rules has nothing to do with
17 whether or not you would automatically generate rules, right, because if
18 you've received them, then you're not generating them. So, you know, I'm a
19 little bit at a loss as to what that argument is even about.

20 I think I also heard a new argument based on the disclosure of the
21 '474 patent in terms of automatically updating rules. Again, I don't know
22 what that argument is all about other than that there's this disclosure of
23 automatically generating rules in the '474 patent. And we are also claiming
24 that. I didn't hear any rebuttals on the *Golnabi* motivation to combine or the
25 indication of a feed. So, I think if Your Honors have any questions, I'd be
26 happy to answer them. Yeah.

1 JUDGE AMUNDSON: It looks like that there are no further
2 questions from the panel. So, with that, our hearing is concluded, but we
3 thank both parties for your time and your helpful presentations.
4 The case is submitted and the hearing is adjourned. But please stay
5 on the line to see if the court reporter wants us assistance with any spellings.
6 And with that, let's go off the record.
7 (Whereupon, the proceedings at 2:41 p.m. were concluded.)

IPR2023-00448
Patent 11,012,474 B2

PETITIONER:

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

PATENT OWNER:

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

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