

UNITED STATES PATENT AND TRADEMARK OFFICE

---

BEFORE THE PATENT TRIAL AND APPEAL BOARD

---

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

v.

CENTRIPETAL, NETWORKS INC.  
Patent Owner.

---

IPR2023-00445  
Patent 10,785,266 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:

GERARD M. DONOVAN, ESQUIRE  
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

BRADLEY C. WRIGHT, ESQUIRE  
SCOTT M. KELLY, ESQUIRE  
JOHN R. HUTCHINS, ESQUIRE  
Banner & Witcoff, LTD.  
1100 13<sup>TH</sup> Street NW  
Suite 1200  
Washington DC 20005  
(202) 824-3160

The above-entitled matter came on for hearing on Monday, April 22, 2024, commencing at 2:51 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 TURNER: Good afternoon. This is an oral hearing for IPR2023-00445 involving U.S. Patent 10,785,266. I am Judge Turner, and I'm again joined by Judges Moore and Amundson.

All the provisos that were provided in the earlier hearing still apply to this hearing. As in the prior hearing, Petitioner will have 45 minutes to present its arguments, and Patent Owner will also have 45 minutes to present its arguments. Petitioner will go first and present its case. Thereafter Patent Owner will argue its opposition to Petitioner's case, and if there's any rebuttal from Petitioner, we will hear it after Patent Owner's opposition. Finally, we'll hear from Patent Owner's surrebuttal, if requested.

I'd like to get to the parties' appearances. Who's appearing on Petitioner's behalf?

MR. DETRIXHE: Again, Your Honor, this is Jonathan Detrixhe of Reed Smith for Petitioner Keysight Technologies. I'll be presenting. And I'm here with my colleague Gerard Donovan.

JUDGE TURNER: Okay. And do you want to reserve any time for rebuttal and how much?

MR. DETRIXHE: Yes, I expect to reserve 10 minutes, please.

JUDGE TURNER: Okay. That's 35 minutes principle then. And who do we have appearing on Patent Owner's behalf for this hearing?

MR. HANNAH: Hi, good afternoon. This is James Hannah on behalf of Centripetal. And with me is Jeffrey Price. I will be presenting for this argument.

1 JUDGE TURNER: And, Mr. Hannah, do you know how much time  
2 you want to reserve for surrebuttal at this time?

3 MR. HANNAH: Sure, we'll take 10 minutes as well.

4 JUDGE TURNER: Okay. I also wanted to find out for Petitioner  
5 Palo Alto Networks, do we have any representation from that party? Okay, I  
6 just wanted to check that.

7 Okay. Does anyone have any questions or concerns before we begin  
8 from either side? I'll start with Patent Owner. There were no questions?

9 MR. HANNAH: No questions from Patent Owner, Your Honor.

10 JUDGE TURNER: Yes, I was going to you first because Petitioner's  
11 going to start. So any questions before we begin for Petitioner?

12 MR. DETRIXHE: None from Petitioner, Your Honor.

13 JUDGE TURNER: Okay. Petitioner, you may begin when you're  
14 ready. You'll have 35 minutes. I'll give you a warning when you get close.  
15 Thank you.

16 MR. DETRIXHE: Thank you, Your Honor. Let me just start by  
17 sharing my slides, and I'll begin on slide 2. I'd like to begin by going over  
18 the Institution decision and what is in dispute in this proceeding. The  
19 Institution decision found the Petitioner had demonstrated a reasonable  
20 likelihood of prevailing on all claims of the '266 patent. The petition  
21 covered four grounds, all based on *Law* as the primary reference, and the  
22 Institution decision found a reasonable likelihood of prevailing on the  
23 ground based on *Law* alone, which was applicable to all challenged claims.  
24 So the Institution did not explicitly address the patentability challenges on  
25 the remaining three grounds.

1 In finding a reasonable likelihood, the Institution decision rejected  
2 four main arguments raised by Patent Owner in its preliminary response  
3 against the *Law* reference. Slide 3. I'll recap each one of those.

4 First, the Institution's decision rejected Patent Owner's argument that  
5 *Law* fails to teach or suggest that its firewalls 146a and b electrically  
6 provided interface across a boundary of a protected network 150.

7 Specifically, Patent Owner had argued that *Law*'s two firewalls 146a and  
8 146b do not protect a single network because Patent Owner asserted that the  
9 network 150 was actually two subnetworks 150a and 150b despite *Law*  
10 showing that those two subnetworks are joined together by network access  
11 device 149c. The Institution decision found that a POSITA would have  
12 regarded the paired LANs of *Law* as viewable as a single network when  
13 compared to the Internet, and each firewall would protect that network.

14 The Institution's decision also found that all network traffic between  
15 the joined LANs 150a and b and the Internet must pass through either  
16 firewall 146a or 146b, and that *Law*'s disclosure of an express alternative  
17 bypass embodiment where that's not the case confirms that ordinary skilled  
18 artisans would of used firewalls 146a and b as providing the entire interface  
19 across the boundary of the network.

20 Next, Patent Owner's second argument was that firewalls 146a and b  
21 would have applied different rulesets. The Institution decision rejected this  
22 argument, finding that persons of ordinary skill in the art would have  
23 understood that parameter firewalls 146a and b would have applied ruleset  
24 147 to the network traffic passing through them.

25 Slide 4. Third, Patent Owner argued that *Law* does not disclose or  
26 render obvious a security policy management server that automatically

1 creates or alters any rules within the rulesets distributed by firm 305. And  
2 this is the same argument that we have just heard previously in connection  
3 with the IPR on the '474 patent. And here again, the Institution decision  
4 rejected that argument, and, in particular, Patent Owner's argument that this  
5 limitation would not be met in view of the supposed requirement that IT  
6 personnel would have still been required to update *Law's* rulesets.

7 And lastly, as a fourth argument, the Institution decision rejected  
8 Patent Owner's argument that receiving an updated set of rules from *Law's*  
9 firm 305 following an initial operator-created ruleset would not satisfy  
10 delimitation requiring receiving a first set of packet filtering rules. And  
11 there, the Institution decision rejected Patent Owner's implicit claim  
12 construction that there must be no initial set of packet filtering rules applied  
13 by the packet security gateway such that the received first set of packet  
14 filtering rules would necessarily need to be the first set of rules ever applied  
15 by the packet security gateway.

16 Slide 5. Patent Owner's response goes and maintains all four of these  
17 arguments. I'll briefly recap them again.

18 First, Patent Owner's response makes the same argument that *Law*  
19 does not render obvious the limitations that requires "a plurality of packet  
20 security gateways that could collectively provide an entire interface across  
21 the boundary of a network, in view of Patent Owner's contention that a  
22 POSITA would not have understood *Law's* subnetworks 158a and b to have  
23 been combined as a single network."

24 Again, second, Patent Owner's response makes the same argument  
25 that "*Law* does not disclose or render obvious applying a first set of packet  
26 filtering rules to all network traversing the boundary in view of its

1 contention that the ruleset 147 applied by *Law*'s firewalls would have been  
2 different than the ruleset 147 applied by *Law*'s" other firewall.

3 Third, Patent Owner's response "repeats the argument that *Law* does  
4 not disclose or render obvious one or more first packet filtering rules that  
5 were automatically created or altered by the security policy management  
6 server," in view of their contention "that IT personnel would have still been  
7 required to update the rulesets when new threats are discovered."

8 And then finally, Patent Owner's response repeats the same argument  
9 "that *Law* does not disclose or render obvious receiving a dynamic security  
10 policy comprising a first set of packet filtering rules in view of its assertion  
11 that *Law* does not disclose receiving an initial ruleset and instead  
12 purportedly requires an operator to configure the initial ruleset."

13 Slide 6. I know we've just discussed *Law* at great length, but before I  
14 turn to the details of the substance of those arguments, I'll quickly go over  
15 again some of the relevant details regarding the *Law* records.

16 First, *Law* discloses what it calls a unified threat management system,  
17 UTMS, for securing network traffic in a process control system. Those  
18 network devices of *Law*'s process control system include devices such as  
19 firewalls that receive rulesets from an external source, which *Law* describes  
20 as a perpetual service in communication with those network devices, and the  
21 service proactively supplies the devices with rulesets in order to meet the  
22 latest security threats. Further, as shown here in the abstract, the rulesets  
23 include rules that define conditions specifying whether to accept or deny  
24 network traffic.

25 Slide 7. Specifically, *Law* discloses an embodiment with two UTMS-  
26 configured firewalls, numbered 146a and 146b, that implement one or more

1 rulesets to inspect and drop malicious packets from the network before those  
2 packets reach their intended destinations. *Law* also discloses a network 150  
3 that is protected by those firewalls. You know, first, I'll point out that *Law's*  
4 specific embodiment circumscribes with respect to a process control system,  
5 you know, such as might be used in power generation, chemical, petroleum,  
6 or other processors. But as the petition explained, *Law's* disclosure is  
7 broadly applicable to any network for which protection is desired. For  
8 example, *Law* states that the network 150 may be a standard Ethernet  
9 communications network supporting any protocol, including standard  
10 TCP/IP, and the devices protected by the network may be standard devices,  
11 including standard workspace and feeders and personal computers. And  
12 *Law* also discloses protected network 150 may comprise subnetworks 150a  
13 and 150b and may simply be a local area network implemented using any  
14 hardwired technology.

15 Slide 8. *Law* discloses that updating the rulesets are required. The  
16 rulesets implemented by the firewalls are required for the rulesets to remain  
17 effective. Accordingly, *Law* discloses a third party risk for cybersecurity  
18 risk management firm 305 that generates the rules that's distributed to the  
19 firewalls. *Law* describes that the firm's ruleset construction may be  
20 performed using any type of information technology methods suitable for  
21 performing such actions using out-time (phonetic) data. And optionally,  
22 *Law* discloses that in generating the rules, that the firm 305 may include the  
23 rules based on aggregated (inaudible) data and ruleset information provided  
24 by other third party sources 315.

25 Slide 9. So, here we see where all of this comes together. Figure 3 is  
26 the embodiment relied on by the petition. It shows how the components I

1 just described are interconnected. Specifically, we see firewalls 146a and  
2 146b. These firewalls protect the network 150, which as shown here, may  
3 include a left subnetwork 150a and a right subnetwork 150b joined together  
4 by network access device 149c into a single network. And notably, as  
5 shown here, the Internet is on one side of the -- these two firewalls at  
6 number 155, and the protected network is on the other with network access  
7 device 149c simply joining together the two tasks without directly providing  
8 Internet access.

9 And we also see, as I just mentioned, the inside of the protected  
10 network. On both the left side and the right side you see most workstations  
11 and computers numbered 120 and 122. The firewalls 146a and b  
12 communicate with firm 305 over the Internet 155 to receive rulesets 147.  
13 Specifically, as we see in Figure 3, the ruleset implemented by firewall 146a  
14 can be termed ruleset 147a, whereas the ruleset implemented by firewall  
15 146b may be labeled ruleset 147b.

16 And finally, at the top we see a number of the sources 315 which all  
17 feed their own firewall threat data and ruleset data to the firm 305, which in  
18 turn constructs the rulesets and distributes those rulesets over the Internet to  
19 the firewalls.

20 Slide 10. So, I'll start by addressing Patent Owner's substantive  
21 argument that *Law* does not render obvious the limitation that recites "a  
22 plurality of active security gateways that collectively provide an entire  
23 interface across the boundary of a protected network." Patent Owner's  
24 wrong. As the petition explained and Dr. Jacobson opines, Figure 3 clearly  
25 shows that firewalls 146a and b collectively provides the entire interface  
26 separating the protected network 150 from the Internet 155.

1           Furthermore, Figure 3 shows a network access device 149c that  
2           directly joins the left subnetwork 150a and the right subnetwork 150b. And  
3           although *Law* discloses other embodiments, such as a bypass embodiment in  
4           which the network access device can serve as the perimeter device and can  
5           also implement rulesets, those don't apply to the direct access device shown  
6           in Figure 3. In particular, *Law* explicitly notes that network access device  
7           149c may or may not include a ruleset such as ruleset 151c shown in Figure  
8           3. As such, *Law's* perimeter firewalls 146a and b collectively provides the  
9           entire interface across the boundary of the network protected by the spirals  
10          and all traffic between the Internet 155 and the network was passed through  
11          those firewalls.

12          Slide 11. This is further confirmed by *Law's* explicit description of a  
13          bypass embodiment in which that is not the case. Specifically, for  
14          diagnostic purposes, *Law* discloses an alternative bypass embodiment which  
15          allows traffic to be rerouted from the firewalls using a bypass network  
16          access device. But that's not the embodiment that the petition relies on. And  
17          furthermore, the very existence of that alternative bypass embodiment  
18          further confirms to a POSITA that a POSITA would have understood *Law's*  
19          express disclosure of this embodiment does not include a perimeter UTMS  
20          firewalls 146a and b illustrated in Figure 3.

21          Slide 12. Patent Owner disputes this and makes the same argument  
22          that it did in its preliminary response, reiterating a POSITA would have  
23          understood *Law's* subnetworks 150a and b to not be joined as a single  
24          network protected by the firewalls. Patent Owner makes a number of  
25          assertions in support of that argument, so I'm going to address each in turn.

1           Starting with slide 13, first Patent Owner asserts that *Law* never uses  
2 the term "150" to refer to any combination of networks 150a and b. Instead,  
3 only uses that term when there is only one relevant network or is not  
4 necessary to distinguish between the networks. That is incorrect. Just one  
5 example, paragraph 53 of *Law* states that the process control system 100  
6 may include one or more subsystems 105a and b, one or more process  
7 control networks 150a and 150b, and one or more process controllers 110  
8 communicatively connected to one or more host workstations or computers  
9 120 through 122 over a process controlled network 150. So as you've just  
10 seen here, *Law* uses the terms "network 150a and 150b" and "network 150"  
11 in the same sentence, with the context making clear that the network 150  
12 refers to the single network formed from the combined subnetworks.

13           Slide 14. Next, Patent Owner asserts that *Law* never uses term "150  
14 to refer to any combination of networks 150a and b, and instead only uses  
15 that term where there is only one relevant network or is not necessary to  
16 distinguish between the subnetworks 150a and b." Again, that's simply  
17 incorrect. We see this in Figure 57 of *Law*, which describes a controller 110  
18 that communicates with various devices, including host computers 120  
19 through 122, as well as firewalls 146a and 146b through the network 150.

20           And so, reading that disclosure in conjunction with Figure 3, and, you  
21 know, we see that *Law*'s reference to a singular controller at 110, there's two  
22 controllers pictured here on both the left and right subnetworks, but let's  
23 take, for example, the one on the left, 150a. As shown here in this figure,  
24 communications between that controller and firewall 146a would have  
25 occurred through subnetwork 150a, whereas in blue you see the  
26 communications between that controller and the other firewall. firewall

1 146b, would have necessarily traversed the network access device and cross  
2 through both subnetworks 150a and subnetworks 150b. And so Patent  
3 Owner's assertion is simply false.

4 Next slide 15. Next, Patent Owner argues that the network access  
5 device 149c supports its assertion that a POSITA would not have considered  
6 subnetworks 150a and b to be joined as a single network. And in support of  
7 that argument, Patent Owner relies on various disclosures in *Law* that  
8 describe the network access device as implementing a ruleset or describing it  
9 as a perimeter device, but those are just particular embodiments. *Law* also  
10 discloses and what's relied on by the petition is the embodiment in Figure 3  
11 where the network access device is clearly not perimeter device. And *Law*  
12 explicitly states here in paragraph 51 that the network access device may not  
13 include a ruleset, such as ruleset 151c. So the notion that it would have  
14 needed to implement a ruleset is simply false. To the contrary, it simply  
15 joins together the two halves of a network.

16 Slide 16. Patent Owner then proceeds that *Law* renders obvious a  
17 limitation that recites "a first set of packet filtering rules to be applied to all  
18 network traversing the boundary." And specifically, this argument Patent  
19 Owner is contesting that it would have been obvious that the rulesets  
20 implemented by firewalls 146a and b may be the same ruleset. Patent  
21 Owner's wrong. A POSITA would have understood that perimeter firewalls  
22 146a and b would have applied ruleset 147 to all network traffic passing  
23 there through.

24 As one example, *Law* discloses that where the UTMS-configured  
25 device is the perimeter device, such as those firewalls, then the ruleset 147  
26 may include a global set of rules for access to any device within subsystems

1 105a and 105b. Here, the Institution's decision agreed, finding that a  
2 POSITA would have understood that the perimeter firewalls 146a and b  
3 would have applied ruleset 147 to all traffic passing there through.

4 Slide 17. Patent Owner repeats this argument in its response.  
5 Specifically, Patent Owner argues that *Law's* global ruleset must be tailored  
6 to the devices in the subsystems. And this kind of gels with the previous  
7 argument where Patent Owner's asserting that the two subsystems could be  
8 different and not part of the same network and, therefore, the rulesets could  
9 be different. To the extent it's based on the first argument, it should be  
10 rejected for all of those reasons I just explained. It should also be rejected  
11 for the same reasons as in the Institution decision.

12 Turning to slide 18. Specifically, first, Patent Owner's argument that  
13 ruleset 147 is implemented by firewall 146a is necessarily different than  
14 ruleset 147b implemented by firewall 146b is unsupported by *Law* and  
15 contrary to *Law's* description of the ruleset implemented by both firewalls as  
16 simply ruleset 147.

17 Second, Patent Owner misinterprets *Law's* disclosure where the  
18 device is a perimeter device, such as firewalls 146a and b, that ruleset 147  
19 may include a global set of rules for access to any device within the  
20 subsystems 105a and 105b. Specifically, "because *Law* permits cross-  
21 communication between subsystems 105a and b without implementing any  
22 rulesets, as I just discussed, a POSITA would have understood that the  
23 ruleset 147 implemented by both firewalls would have needed to protect all  
24 the devices in both subsystems."

25 Third, Patent Owner argues that the global ruleset is unique to the  
26 particular devices protected by the ruleset, and that that does not suggest that

1 the ruleset for subsystems 105a would have been different from the rule  
2 system for 105b. So, as the petition and reply explained, a POSITA would  
3 have understood that a single local rule applied by both firewalls would have  
4 been tailored to protect all of the devices in both subsystems 105a and b.  
5 Again, going back to the fact that they're joined together as a single network  
6 and that communications can go through either firewall to get to any of the  
7 devices in both subnetworks.

8 Slide 19. Fourth, even if one were to correctly assume that the ruleset  
9 147a is tailored only to the devices and subsystem 105a, and that ruleset  
10 147b is only tailored to the devices in system 105b, Patent Owner's  
11 argument still would not follow, specifically because there's no evidence that  
12 the devices on each subsystem are different. To the contrary, as we see in  
13 Figure 3, the illustration of the subsystems are completely identical and  
14 there's no -- and they could be different, but there certainly is no requirement  
15 that they be different.

16 And fifth, and lastly, Patent Owner appears to argue that network  
17 access device 149c's implementation of a ruleset 151c suggests that the rules  
18 implemented by the firewall would be different. Again, that's wrong and it  
19 appears to be based on the mistaken belief that the network access device  
20 149c needs to implement a ruleset. But, you know, the text of *Law*,  
21 paragraph 51, directly says otherwise and that the network access device  
22 does not need to implement a ruleset.

23 Slide 20. Turning to the next argument, the third argument, Patent  
24 Owner argues that *Law* does not render obvious that one or more packet  
25 filtering rules at the first set of packet filtering rules were automatically  
26 created or altered by the security policy management server. Again, Patent

1 Owner is wrong. I know we discussed related limitations with respect to the  
2 '474 patent. I'll briefly go over the same reasons here.

3 Specifically, as detailed in the petition, a POSITA would have  
4 understood that *Law*'s cybersecurity risk management firm 305 necessarily  
5 includes a server. It distributes rulesets to firewalls over the Internet, so it  
6 necessarily is a server, as Dr. Jacobson explained. And *Law* also describes  
7 firm 305 constructs rulesets using any type of information technology  
8 methods suitable for performing such actions using electronic data, that  
9 those methods include executing computer-implemented algorithms.  
10 Therefore, as Dr. Jacobson explained, a POSITA would have understood  
11 that rules are constructed "using any type of information technology  
12 methods suitable for ruleset constructing would have included methods of  
13 automatically constructing rulesets."

14 Slide 21. This is particularly the case given that *Law*'s background  
15 expressly recognized prior art techniques for creating firewall rules by  
16 automatically locating devices and generating rules by passively analyzing  
17 traffic on the network. It would have been obvious to a POSITA to  
18 incorporate such known techniques for automatically generating rules  
19 (inaudible) some of the rules in ruleset 147 created by affirmed 305.

20 Furthermore, *Law* discloses automatically updating or altering rules  
21 in response to network -- detected network conditions. And specifically,  
22 paragraph 83 of *Law* states that detection of certain network conditions may  
23 trigger an automatic update of the rulesets, which *Law* distinguishes and  
24 contrasts with an update performed in response to an alarm which prompts  
25 the user to perform a manual update.

1 Slide 22. The Patent Owner repeats -- Patent Owner argues that *Law*  
2 does not disclose or render obvious a security policy management server that  
3 automatically creates or alters any rules in the rulesets distributed by firm  
4 305. Specifically, Patent Owner appears to contend that *Law* does not  
5 disclose or render obvious that firm 305 automatically generates rulesets  
6 because firm 305 would have also included IT personnel and have been  
7 accompanied, and similarly, Patent Owner contends that IT personnel would  
8 have been required within *Law's* system to manually update the rulesets.

9 Slide 23. This is basically the exact same argument from the  
10 preliminary response, and it should continue to be rejected for the same  
11 reasons expressed in the Institution decision. As an initial reason, the claim  
12 language includes no requirement prohibiting the security policy  
13 management server from being owned by a commercial entity.

14 Slide 24. Also, Patent Owner does not meaningfully dispute the  
15 evidence I just discussed that, number one, the firm 305 may construct  
16 rulesets using any type of information technology methods using electronic  
17 data. Two, that *Law* expressly recognized such methods, including known  
18 prior art techniques for automatically generating rules. Part three, that *Law's*  
19 system discloses performing automatic updates.

20 Slide 25. Addressing Patent Owner's arguments that firm 305 would  
21 have been accompanied to include IT personnel, that fails to rebut *Law's*  
22 teaching and that techniques were automatically constructed, constructing  
23 rules were well known, and that firm 305 would have used any of those  
24 types of techniques, including computer-implemented methods for  
25 constructing these rules.

1 Slide 26. Patent Owner's main argument is relying on a background  
2 paragraph of *Law*, paragraph 16, which describes several problems with  
3 prior art approaches for managing a firewall which needed to be managed by  
4 trained IT personnel. There's numerous disadvantages expressed in this  
5 paragraph, mainly one disadvantage is that IT personnel would even be  
6 required to update the rulesets when new threats are discovered. Another  
7 disadvantage is that IT personnel would need to be trained to understand the  
8 intricacies of a process control system to understand why certain rulesets  
9 must be changed.

10 Accordingly, *Law* explains that besides a prior art firewall, those  
11 rulesets must be manually updated by IT personnel, but those rulesets may  
12 inadvertently provide less protection than desired. *Law*'s invention solves all  
13 of those problems by providing automatic updates about the necessity  
14 involving IT personnel.

15 And lastly, I'll point out that *Law* does disclose one embodiment with  
16 respect to Figure 13 that permits an operator to configure rules using a rule  
17 configuration interface. But nowhere has *Law* described that such operator  
18 involvement is a requirement to update the rules. Rather, it's an option. You  
19 know, flexibility is provided to the operator of a system and for good reason  
20 because requiring operator involvement would be contrary to *Law*'s solution  
21 and all of the disadvantages explained in paragraph 15 of requiring operators  
22 to manually update rules.

23 Turning to slide 27 --

24 JUDGE TURNER: This is Judge Turner. Just to let you know that  
25 you have five more minutes before you go to your -- into your rebuttal time,  
26 so take whatever time you need. Thank you.

1 MR. DETRIXHE: Thank you, Your Honor. There's one more  
2 substantive argument to address, which is Patent Owner's final argument that  
3 *Law* fails to disclose or render obvious the limitation that the site receiving  
4 from a security policy management server a dynamic policy comprising a  
5 first set of packet filtering rules.

6 So, specifically, Patent Owner appears to be construing this limitation  
7 to meet an initial dynamic security policy such that no prior security policy  
8 was ever installed previously on the patent security gateway. Based on that  
9 construction, Patent Owner argued that *Law* does not satisfy the claim term  
10 based on Patent Owner's contention the operators would still be required in  
11 *Law*'s system to create the initial ruleset rather than the initial ruleset being  
12 received at the distributed ruleset from firm 305. Patent Owner is wrong.  
13 This argument should be continued to be rejected for the same reasons set  
14 forth in the Institution decision.

15 Specifically, turning to slide 28, you know, first, the claim  
16 construction position is wrong. The same language simply recites a first set  
17 of packet filtering rules. That language is not limited. It does not limit a  
18 first set of rules to an initial dynamic security policy. Adding such a  
19 limitation does not find support in the claim language. Rather, Patent  
20 Owner's argument appears to be based on the claim language reciting  
21 receiving a first set of rules and then later reciting receiving a second set of  
22 rules. But the words "first" and "second" are essentially common claim  
23 drafting terms used to differentiate the first and second claims that -- or rules  
24 from one another. Not to add a negative limitation that there must have  
25 never been an initially applied ruleset.

1 Numerous cases have affirmed this principle. One, *3M Innovative* is  
2 a Federal Circuit case that stated that, "The use of the terms 'first' and  
3 'second' is a common patent law convention to distinguish between repeated  
4 instances of an element or limitation." You know, that's exactly what the  
5 claim language of the '266 patent uses, the terms "first" and "second."

6 Other cases have objected introducing an initial or first in time  
7 limitation based on plain language reciting a first of something. You know,  
8 those are mentioned here in the Reply Paper 21, pages 21 and 22. I won't go  
9 into those in detail here, but other than to point out the same results should  
10 apply here and the Board should reject Patent Owner's efforts to construe  
11 first set of packet filtering rules as being limited to some initial dynamic  
12 security policy.

13 Slide 29. Lastly, even if that construction -- incorrect construction  
14 were to be adopted, *Law* would still disclose or render obvious receiving  
15 from the firm 305 an initial dynamic security policy comprising a first set of  
16 packet filtering rules. Specifically, *Law* consistently and repeatedly  
17 describes the rulesets 147 as being constructed and distributed by the firm  
18 305. The rulesets that are implemented by *Law*'s firewall, well, there is no  
19 reason to expect otherwise for the initial ruleset.

20 And although *Law* discloses an embodiment in which rulesets may be  
21 configured by an operator, such as with respect to Figure 13, that  
22 embodiment does not suggest that the rulesets that the operator may  
23 configure are necessarily required for the initial ruleset rather than received  
24 by firm 305. In other words, nowhere does *Law* describe an embodiment in  
25 which the operator is required to create the initial ruleset.

1           And with that, unless Your Honors have any questions you'd like to  
2 address now, I'll reserve the remainder of my time for rebuttal.

3           JUDGE TURNER: It doesn't appear that there are any questions.  
4 Counsel, you will have 10 minutes for your rebuttal.

5           We'll proceed on to Patent Owner's counsel, Mr. Hannah. You can  
6 begin principal arguments when you're ready.

7           MR. HANNAH: Okay, let me just share my screen real quick. Can  
8 you see my screen?

9           JUDGE TURNER: Yes, I can.

10          MR. HANNAH: Okay, great. Thank you. Thank you, Your Honors.  
11 May it please the Board. So I want to start with the context in the disclosure  
12 of *Law*. You know, what is *Law* disclosing? We heard some of it this  
13 morning from my colleague here, from opposing counsel. And I just want to  
14 reiterate what *Law* is.

15          So, *Law* is, first of all, not a conventional firewall system. Right?  
16 We know that from paragraph 16. Paragraph 16 says conventional firewall  
17 systems don't work. We need something different because we're dealing  
18 with nuclear reactors. We're dealing with critical infrastructure process  
19 controls that if something goes down, it's going to be catastrophic.

20          And so what does *Law* do? *Law* is trying to come up with a solution  
21 for a critical infrastructure, such as a nuclear reactor, so that the rules that  
22 are applied at the devices within that critical infrastructure are able to be  
23 implemented to prevent against threats. It's not a conventional firewall that's  
24 designed to prevent traffic from entering the network. *Law* does not disclose  
25 that. It specifically says that that stuff doesn't work.

1           So let's take a look at the diagrams of *Law* and just to get a basic  
2 understanding of what we're talking about. This is Figure 31 -- it is Figure 1  
3 that I'm showing from *Law*. And what we have, and we've seen this figure,  
4 you know, this morning, but what I want to emphasize here, and this is going  
5 to the first element that I'm going to be addressing, which is rules that have  
6 to be applied to all traffic that traverses the boundary. Okay? That's what  
7 the claim requires. It requires that you receive rules as a dynamic security  
8 policy, and that has to be applied to all traffic that traverses the boundary.

9           So what did the Petitioner point to? They pointed to these firewalls,  
10 146 and 146b. Well, what we pointed out was that the rules that are sent to  
11 the firewall are actually redistributed to the devices within the subnetwork.  
12 So the rules that we're talking about here is not just 147, we're also talking  
13 about 151a here, we're talking about 153. We're also talking about 148.  
14 Those are rules that are being implemented by the process controls  
15 themselves, the valves, the actuators. Right? Remember, we're talking  
16 about a critical infrastructure, a nuclear power plant here, and all these  
17 devices are going to have rules that are going to be specific to the actual  
18 implementation of those devices themselves.

19           So, in order for this protection to take place, *Law* discloses, and this  
20 is in paragraph 90, that it will receive the rules at the firewall, but it's going  
21 to push those rules, redistribute those rules to the various devices within the  
22 network. That tells you, because those rules are pushed down, those rules  
23 are not implemented by the firewall. Therefore, all traffic that traverses that  
24 boundary is not -- those rules are not applied to all traffic that traverses that  
25 boundary. Traffic is going to come through that firewall and it's going to get  
26 to this 152 element here. At that point, rule 153 is going to apply. That

1 rule's -- that traffic has already traversed a boundary because those rules  
2 have been pushed down to 153. That's because these are not conventional  
3 firewalls. These firewalls are designed in order to redistribute these various  
4 rules.

5 And I'll show you paragraph 90 of *Law*, that's exactly what it  
6 discloses, is when you look at -- if we get paragraph 90 here and we look at  
7 about midway through, this talks about how -- what are these firewalls going  
8 to do? We're going to receive these process control rules. The firewall can't  
9 implement those. It has no idea what to do with those. The firewall -- the  
10 counsel talked about the HART protocol and these other protocols in the  
11 previous proceeding. It's disclosed here. The *Law* patent is specific. It says  
12 that the firewalls don't know how to deal with the HART protocol. That  
13 traffic is not going to be regulated by the firewall, that's going to be  
14 regulated by the device controls themselves. Therefore, all traffic that  
15 passes through that firewall is not going -- that traverses through that  
16 boundary is not going to have rules applied at that firewall.

17 The Petitioner doesn't have any -- it doesn't have any  
18 counterarguments to this. What they pointed to is they said, okay, well,  
19 global rulesets can be applied. What does *Law* tell you? *Law* tells you that  
20 these global rulesets are the same things that are going to be redistributed to  
21 the process controls themselves to be implemented. There's just simply no  
22 disclosure -- because this is not a conventional firewall. This isn't something  
23 that you go off and you buy from a network security company today that  
24 says, hey, I'm going to protect your -- I'm going to protect the boundary of  
25 your network and I'm not going to allow Google traffic to come in or  
26 malicious sites to come in. That's not what *Law* -- *Law* is not concerned

1 with that. *Law* is concerned with protecting a nuclear reactor and pushing  
2 rules down, appropriate rules down to the particular devices within the plant,  
3 within the critical infrastructure.

4 JUDGE TURNER: Counsel?

5 MR. HANNAH: And to -- yes, Your Honor.

6 JUDGE TURNER: This is Judge Turner. So is it Patent Owner's  
7 position that 147a and 147b are basically empty, that there aren't any rules in  
8 those elements?

9 MR. HANNAH: 147a are empty? No, I think there's rules that are  
10 going to be applied to some of the traffic, but not all of the traffic. The  
11 claim requires --

12 JUDGE TURNER: But wouldn't -- let me -- maybe I can rephrase it.  
13 So if there are rules in 147a, for example, it seems like all of those -- it  
14 seems like that's going to be applied to all the traffic coming into the firewall  
15 for that subnetwork, is it not?

16 MR. HANNAH: No.

17 JUDGE TURNER: Even if it doesn't trigger anything? Oh, it's not?

18 MR. HANNAH: No, no, it doesn't even --

19 JUDGE TURNER: Maybe I'm misunderstanding about that.

20 MR. HANNAH: Yeah, it doesn't even, and I'm glad we're clarifying  
21 this, it doesn't even know what to do, for instance, with the HART protocol.  
22 Here, I'll show you, in *Law*.

23 JUDGE TURNER: I understand that the HART protocol wouldn't be  
24 in 147. Correct?

25 MR. HANNAH: It would traverse one -- it would traverse the  
26 firewall because the control system comes from the Internet. And that was

1 admitted, actually, that was in his description that we saw earlier. The  
2 control information traverses the firewall, but the HART protocol rules are  
3 not implemented until it gets to the actual device itself, the actuator, for  
4 example.

5 JUDGE TURNER: And I -- but I guess my question is, all the  
6 rulesets that are in 147a, aren't they going to be applied to the traffic coming  
7 into that firewall?

8 MR. HANNAH: No, not the HART protocol, for instance. It doesn't  
9 know it.

10 JUDGE TURNER: Now, again -- so, the HART protocol is in 147a  
11 as well?

12 MR. HANNAH: No, it's not.

13 JUDGE TURNER: Because I thought you told me it got pushed  
14 down.

15 MR. HANNAH: Exactly. It gets pushed down to be implemented.  
16 So because it does it in the --

17 JUDGE TURNER: Well, does it go in 147a then?

18 MR. HANNAH: It gets redistributed down to the -- down to the  
19 devices.

20 JUDGE TURNER: Okay. So --

21 MR. HANNAH: It does not get applied.

22 JUDGE TURNER: And perhaps this is a hypothetical, so you can  
23 take it that way (phonetic).

24 MR. HANNAH: Okay.

25 JUDGE TURNER: The rules that are in 147a, do they all -- do they  
26 get applied to all the traffic, not just the other rules? Maybe the other ones

1 may be distributed, but the rules that are just in 147a. So there are packet  
2 rules, there are filtering rules that are in 147a. The traffic comes in and the  
3 firewall just says, I don't care? I'm trying to understand. Maybe I'm missing  
4 something fundamentally here.

5 MR. HANNAH: Yeah. So let me show you. So --

6 JUDGE TURNER: Okay.

7 MR. HANNAH: -- let's see what *Law* does with information for the  
8 HART protocol, for instance. We can look at paragraph 56. If we go to 56,  
9 this is what the firewall will do with information for the Provis (phonetic),  
10 it's like -- what is it called, the PROFIBUS protocol as well as the HART  
11 commands, all the firewall will do is translate. It's going to be able to just do  
12 a simple translation. It cannot apply the rules. That's exactly -- if you -- so  
13 if you look at paragraph 56, for example, the field devices are the only ones  
14 that are going to -- or may only understand HART commands and the IO  
15 network via the PROFIBUS protocol. To this gate -- to this end, the  
16 gateway may provide bidirectional translation of the traffic. So it does not --  
17 the claim term says, apply the rules. The firewall does not apply the rules  
18 for the HART protocol.

19 Look at -- and the patent tells you why. The *Law* patent tells you  
20 why. Look at 55, 55 tells you these are implemented by the sensors  
21 themselves. That's what *Law* tells you. Using the field bus and the HART  
22 protocol, the other devices, the devices themselves, 134, are the ones that are  
23 going to drop the data, not the firewall. If *Law* said that you would drop that  
24 data at the firewall, you would never have a disclosure saying it would be  
25 done by the control valve itself. It simply wouldn't happen.

1 JUDGE TURNER: This is Judge Turner. I guess I'm game to try  
2 again. So, is there any rule that's applied at the firewall? Is the firewall just  
3 simply a sieve? It just allows everything through and everything else gets  
4 filtered on by a later element. Are there any rules that are applied by the  
5 firewall?

6 MR. HANNAH: The firewall can apply it to some traffic, but not all  
7 traffic. Yeah, I mean, it talks about how the firewall can apply it to TCP  
8 traffic, but it can't apply it to -- it can't apply it to this HART and  
9 PROFIBUS because these are specialized firewalls.

10 I think the misconception everyone's having here is that when it's this  
11 firewall, everyone thinks that they know what a firewall is, using today's  
12 conventional terms of I go purchase a firewall from a network security  
13 company. That's not what these firewalls are. You look up what Wirt does,  
14 I mean, I looked it up in preparation, but Wirt is very specific. This is the  
15 firm 305 that we'll get to, but it is very specific. The rules that it generates  
16 are for actuators, valves, like critical infrastructure, and that this whole  
17 patent is about taking these rules that are device-specific and you pass those  
18 to the appropriate devices themselves and push them to the appropriate  
19 devices themselves.

20 This is not about a firewall that sits at a boundary that everybody  
21 thinks about today and says, oh, I'm going to buy a firewall. It's going to  
22 protect against all the Internet traffic that comes in because this doesn't care  
23 about the Internet traffic that much. This cares about control process  
24 commands through these very specific protocols that come in and that if it  
25 bypasses the firewall, it's going to wreak havoc. And so it does not want the  
26 protection to be at the firewall. It wants it to be at the control valves

1 themselves. If there's a simple hack into the firewall and it bypasses that,  
2 your nuclear reactor goes down, plain and simple.

3         So what does this tell you? I'm not going to allow you to do that. I'm  
4 going to design a system with a very specialized firewall that doesn't apply  
5 all the rules at the boundary to all the traffic. Instead, I'm going to push the  
6 rules to the appropriate devices and make sure that those devices can  
7 implement them themselves. And that's exactly what this paragraph shows.  
8 This is, for the record, this is paragraph 55. 55 lays it out that it's the field  
9 devices themselves that are going to be implementing the control traffic or  
10 any other traffic that's going to be specific to them. At best, the firewall can  
11 do a translation, but it can't apply the rules because it doesn't know what to  
12 do. It simply doesn't because these are -- this is an industrial context. And  
13 that's from paragraph 3. Paragraph 3 of *Law* specifically said that this is an  
14 industrial context. You get to paragraph 16, it says conventional firewalls  
15 ain't going to work. So we need to have a specialized system in order to do  
16 this.

17         And so their solution to that is I'm going to be able to take rules in,  
18 push them down to the devices, have the devices do them themselves. And I  
19 think that's where we're getting a little bit lost when we talk about firewalls  
20 and all this stuff. We have to look at the context of wall and what it's about.  
21 And if you look at work security and if you look at the different disclosures  
22 that are in here, I even pulled up Your Honor's typo during the break  
23 between. I mean, that disclosure is even more, you know, that's referenced  
24 in here.

25         I mean, it's even more specific saying that this is the one that, you  
26 know, the -- Your Honor said that it was missing a one. And it says,

1 "T\traditional security solutions are based on central firewalls protecting  
2 unsecured internal devices or computers from the outside world, a design  
3 that cannot address the requirements of the industrial controlled world."  
4 That's what that reference says. That's what this context is. We have to look  
5 at this in context, and this is the industrial context and how these systems  
6 apply. This is not a traditional computer network sitting here in my *Law*  
7 firm or sitting there for the PTO. It's a completely different context.

8 JUDGE TURNER: This is Judge Turner, and I promise this is the last  
9 question I have on this particular topic.

10 MR. HANNAH: Sure.

11 JUDGE TURNER: Can you point me to where in your declarant's  
12 testimony did they say when *Law* says firewall, they don't mean firewall?

13 MR. HANNAH: Well, I mean, what he says is, this is coming into the  
14 context, I mean, we have bold heading saying that is not applied to all traffic  
15 that traverses the boundary. And what the Petitioner came back with saying  
16 was, anytime we're talking about these global rulesets. And so that's what  
17 we came back and we said, look it, global rulesets are not global rulesets in  
18 the stuff that everyone's thinking about. Global rulesets are ruleset that are  
19 going to be redistributed to the actual devices themselves. That's where this  
20 context comes in. And that's cited throughout our panel response and in our  
21 reply. Every time --

22 JUDGE TURNER: And I understand. And this is Judge Turner. I  
23 mean, I understand. I think the answer maybe you were reaching for was no.  
24 But I understand that you're making a different argument.

25 I understand your argument, but what I'm -- you seem to be saying  
26 today here, when *Law* says firewall, it doesn't mean firewall. And I'm trying

1 to look for some testimonial, you know, background for that so that I can --  
2 so if I accept your argument, you're saying when *Law* says firewall, they  
3 don't mean firewall, they mean something else. How when -- you know, if  
4 this goes up on appeal, do I support that decision? So I'm looking for any  
5 evidence that the Patent Owner has provided, perhaps testimonial evidence  
6 that says, look, when *Law* says firewall, they don't mean generic firewall or  
7 any kind of firewall. Do you have any hook there? I guess the answer is.  
8 No, but I'll let you tell me.

9 MR. HANNAH: Sure. Okay, I'll go to page 2. I'll start at page 2 of  
10 our Patent Owner response. *Law*, on the other hand, is directed to "unified  
11 threat management system for high risk or sensitive process control system,  
12 nuclear reactors, in which rulesets are initially created by operators with  
13 intimate knowledge of the process control system." I mean, that's the  
14 context, Your Honor. It's like the entire context is about nuclear control  
15 systems and the rulesets that are applied.

16 We then get into, specifically, when we talk about the global rulesets,  
17 and this is the rebut -- again, we're rebutting Petitioner. It's not our burden  
18 to point out, you know -- it's not our burden. But we say on page 28, "On  
19 the other hand, a subset of the global ruleset might only control access to a  
20 particular internal device." Again, reading that, what we're saying is that  
21 these rules are applied to particular devices within the network themselves.  
22 They're not implemented by the firewall. And this is under the heading of  
23 *Law* does not disclose "a first set of filtering rules to all," quote, "all network  
24 traversing the boundary." This is an argument we made from day one.

25 And so I'm just trying to provide the context here during oral  
26 argument, you know, in a little simpler English to show that, look, when

1 we're looking at the disclosures and we're looking at the rulesets, we have to  
2 see where those rulesets are applied. And *Law* doesn't apply the process  
3 control rules. It pushes those rules down. So, therefore, it doesn't meet the  
4 first element.

5 JUDGE TURNER: Thank you.

6 MR. HANNAH: I guess I'm also looking --

7 JUDGE TURNER: I don't want to use -- this is Judge Turner. I don't  
8 want to use up all your time, so thank you.

9 MR. HANNAH: Okay. Well, yeah, I think that when you reread the  
10 record and you specifically reread *Law*, I mean, that's what I did, when you  
11 reread *Law* and you look at it and you get the context, you say, hey, wow,  
12 this is not a conditional system. And then, you know, we actually -- well,  
13 now I'm going back, I'm thinking about more citations. We do specifically  
14 talk about paragraph 16. Petitioner even pointed it out, saying that  
15 conditional firewalls are not -- don't cut it. And that was a major argument  
16 that they had and we cited paragraph 16 all over the place in *Law* -- for *Law*.  
17 So we did argue that these are not conventional firewalls, and *Law* actually  
18 specifically says that they're not conventional firewalls and they won't work.

19 We also have paragraph 40 from Goodrich's declaration. So it's  
20 throughout the record, Your Honor. And I hope you do go through and look  
21 for that stuff to support it because this would be very good support to -- you  
22 know, for us assuming the other side of the appeal, because that is the  
23 evidence that's in the record. That's what *Law* says.

24 All right. The next element that -- the other one I just kind of wanted  
25 to just point out for the record is when we talk about paragraph 56 in *Law*,  
26 paragraph 56 also specifically talks about that PROFIBUS standard which

1 are on this IO network. Again, it's talking about how you're going to push  
2 down rules to the various devices that I showed in Figure 1 or Figure 3 for  
3 those different rulesets. All right.

4 MR. PRICE: It's paragraph 50, not 40.

5 MR. HANNAH: I'm sorry?

6 MR. PRICE: It's paragraph 50, not 40.

7 MR. HANNAH: Oh, I'm sorry. So this is also paragraph 50 of  
8 Goodrich's report. I mean, we can find citations for Your Honor, but you'll  
9 see it when we go through the record.

10 The next element I want to address is the security policy management  
11 server. Your Honor, Your Honor Turner, you asked specific questions  
12 during the previous presentation regarding the security policy management  
13 server. It is a similar element that we have in the other case. Right? You  
14 have to have a security policy management server and it has to do certain  
15 functions. It has to automatically create these rules and it has to be able to  
16 provide those rules to the packet security gateway or the firewall.

17 The -- I mean, simply put, people are not servers. Right? And I think  
18 we can all agree with that. People are not servers. Firm 305 is a person. So  
19 the argument the petition has to make is that firm 305 necessarily includes a  
20 server. Well, Your Honors showed us a definition in the previous  
21 proceeding from the technical dictionary and essentially what I wrote down,  
22 and you can correct me if I'm wrong, you probably still have it there, is that  
23 a server is a, you know, request-response mechanism in which a request is  
24 going to be sent to a server, you're going to get a response back. Right?  
25 And that's how I -- that's -- I think that was the gist of the definition.

1 JUDGE AMUNDSON: This is Judge Amundson. Yes, I think you've  
2 got the gist of it. Yes.

3 MR. HANNAH: Yeah. So, I mean, there's simply nothing in *Law*  
4 that says that they're going to ping a server to get a response back and get  
5 that response back out automatically. And now there's a rule -- there's a  
6 reason for that. We're protecting against nuclear reactors, critical  
7 infrastructure, huge data centers. You're not going to want to have a server  
8 that is going to automatically generate a rule and then you send that rule  
9 down to a nuclear reactor and it melts down. There's a reason for that.  
10 There's a reason that you have they call it firm 305 every time. This Wirt  
11 Research is a specialized group that does this. They monitor critical  
12 infrastructure and they ensure that the rules that get sent down to the various  
13 processes aren't going to melt down the nuclear reactor. So there is a reason  
14 for that. And --

15 JUDGE AMUNDSON: Excuse me, this is Judge Amundson. On the  
16 --

17 MR. HANNAH: Yeah.

18 JUDGE AMUNDSON: On that point, I mean, I have some excerpts  
19 of *Law*, but one of the excerpts from *Law* is from paragraph 66.

20 MR. HANNAH: Okay.

21 JUDGE AMUNDSON: You could maybe go to --

22 MR. HANNAH: Yep.

23 JUDGE AMUNDSON: -- paragraph 66.

24 MR. HANNAH: Yep.

25 JUDGE AMUNDSON: And the -- yeah, where is it? It says that "the  
26 UTMS-configured device or entity may receive the ruleset data and the

1 UTMS-configured process object 204e may be configured or programmed to  
2 access the ruleset data and other update data on a periodic or nonperiodic  
3 basis via any desired communication link to, dot, dot, dot, a cybersecurity  
4 risk management firm." So it seems to me there is disclosure in *Law* that the  
5 firewalls are accessing the firm 305.

6 MR. HANNAH: I agree there's accessing 305, but that's not a server.  
7 This says -- and I'm glad you pointed that out. I was going to go to 66. It  
8 says, "via any desired communication link," and it gives you an example,  
9 like an Internet connection. So, yeah, you can use the Internet in order to get  
10 the rulesets from the people, but that doesn't say that the firewalls are  
11 pinging a server and the response to that request is a ruleset that was  
12 automatically generated by the server. That's the difference.

13 And Judge Turner asked, he goes, I believe, and I don't -- you know,  
14 correct me if I'm wrong, but essentially he's like, why wouldn't you? You  
15 know, asked my colleague here, Mr. Price, why wouldn't you want to do  
16 that? And the reason is, is because you're dealing with critical infrastructure  
17 here. You have to have a firm that's online 24/7 that's going to be  
18 monitoring these power plants, data centers, critical infrastructure. And the  
19 last thing you want is a rule that gets sent down that is wrong. You can't  
20 have that here.

21 You might be able to do it to my firm. You might be able to send a  
22 block to Google to my firm, and I can't access my sports page, you know, for  
23 20 minutes. But if I get a block rule that's sent down to my actuator in my  
24 nuclear plant that's incorrect, my plant's going to blow up. So I'm going to  
25 have a firm 305 that's going to constantly monitor and make sure the rulesets  
26 are correct.

1           That's why *Law* doesn't disclose a server. I mean, it's undisputed that  
2 *Law* doesn't disclose a server. And now we're just looking for reasons why.  
3 And that's a critical reason. That's a critical reason why, and that's a critical  
4 reason why you're not going to automatically generate the ruleset by the  
5 server.

6           *Law* is very specific that you have to go in and you have to have  
7 personnel with detailed knowledge of the infrastructure in order to generate  
8 these rules. It always says you have the operators generate the rules. Right.  
9 You always -- you have to know what the valves are doing, the actuators are  
10 doing in the network. So they generate -- they're going to generate the rules.  
11 You can't have a server that's going to go -- that's going to be outside, that's  
12 going to automatically generate rules that I could potentially push through a  
13 bunch of different plants because you can't do that. All the plants are  
14 different. All the networks are different. And it would be, to say the very  
15 least, unwise to send a rule that you're not sure that's going to work in the  
16 plant. And so you can't have false positives here. You can't have a server  
17 that's going to be able to send this stuff.

18           So what does Petitioner rely upon? They rely upon inherency, right?  
19 They said, well, it's necessarily required that you have a server. Well, we  
20 know the law for inherency. It has to be necessarily present. So if you can  
21 come up with one way that is not necessarily present, then they lose.

22           You can have firm 305 on a workstation push a ruleset to a plant by  
23 themselves. There's nothing that requires a request-response architecture  
24 here at all. I have a personnel, I have an operator for my Wirt Security firm  
25 with my business, their entire business is to monitor plants, right,, not to  
26 monitor computer networks of law firms. These are to monitor critical

1 infrastructure plants using HART protocols, these other very specific things.  
2 And they generate the rules and they can send the -- or they can update rules  
3 or they can monitor those plants and send those directly. They do not need  
4 to have -- there's no need to have a server that's going to respond  
5 automatically to a request. Again, it would be foolish to do that in the sense  
6 of a nuclear processor.

7         So, there's just simply -- that's the reason that Petitioner couldn't point  
8 to anything is because *Law*, again, is not about these commercial firewalls.  
9 It's not about getting updates through, you know, in order to protect a law  
10 firm or to protect some other, you know, computer tech -- typical computer  
11 network that we would think about in the space today. *Law* is talking about  
12 protecting networks of valves.

13         I mean, this is kind of a side note, but it's also relevant. I like the  
14 figure of *Law* that shows what the typical network looks like. It's this. It  
15 kind of got, you know, passed over a little bit, but if you look at it, it's not  
16 your typical computer network. Look at this, 129b, right? This is what the  
17 network looks like. It's a firewall that's connected to a valve, that's  
18 connected to some other process control, that's connected to an actuator.  
19 This is the network we're talking about. We're not talking about typical  
20 computer networks here that operate, you know -- that are going to be  
21 ingesting and sending out Internet traffic. You're talking about a valve here  
22 that's going to be connected to some steam, you know, engine or something  
23 that's going to be generating a lot of heat. And if I got some type of attack, I  
24 got to make sure that this process control, this control valve, is going to be  
25 able to protect itself with the appropriate rules. So when you think of *Law* --

26         JUDGE TURNER: Counsel?

1 MR. HANNAH: -- this is the network that we're thinking about.

2 Yep.

3 JUDGE TURNER: Counsel, this is Judge Turner. I wanted to let you  
4 know that you have five more minutes until you go into your rebuttal time.

5 MR. HANNAH: Okay.

6 JUDGE TURNER: I also had a quick question just on that same  
7 topic. Looking at *Law* paragraph 83, the last sentence, I believe Petitioner  
8 had this up on their slides. The last sentence says, "The detection of certain  
9 network conditions may also trigger an automatic update of the rulesets 147,  
10 148, 151, and 153, or prompt a user to perform that," et cetera. It seems like  
11 that is calling for an automatic updated ruleset. How does that not support  
12 Petitioner's case?

13 MR. HANNAH: Because it still doesn't have anything about a server  
14 that's going to be -- that's going to be doing this. You have, as Petitioner  
15 pointed out, you have this service, the -- and I hope I'm not butchering the  
16 name, but I mean, I've highlighted it here. It's Wirt Security, right? But  
17 anyway, they're constantly monitoring this. And so when you -- if there's  
18 going to be something that's going to happen, they're going to be able to be  
19 triggered by it, see what's going on, and then hopefully be able to push it.  
20 This is so that you don't have to have possibly some other personnel take a  
21 look at it. But there's nothing in here that says you're going to have a server  
22 that's going to automatically generate these rules that are going to be pushed  
23 without intervention. I mean, this whole thing is about securing a plant, and  
24 so --

25 JUDGE TURNER: Okay. They're going to be automatically updated,  
26 are they not?

1 MR. HANNAH: They automatically updated, but it says nothing  
2 about a server -- that you're going to be paying doing a response -- a request-  
3 response to a server.

4 JUDGE TURNER: Okay, but they're going to -- so if it's going to  
5 update them automatically, it's just going to, I guess, just conclude. It's not  
6 going to -- you say it may be pushed, so that's the distinction you're creating.  
7 So it can update them and push them, but it's not going to serve them. Is that  
8 the distinction?

9 MR. HANNAH: Okay, there's two things, and maybe we're talking  
10 over each other. First of all, this detection of the automatic update is never  
11 going back to firm 305. Right? There's nothing in here that's saying that  
12 this is going to trigger a new ruleset that comes from firm 305. So there's  
13 simply no server in here that's going to be a request-response architecture at  
14 all. I mean, you'd agree with me with that, right? I mean, there's nothing in  
15 here that talks about firm 305 and says, okay, I'm going to ping 305 for an  
16 automatic update. Doesn't say anything about that at all. So there's no  
17 (inaudible) right here.

18 JUDGE TURNER: And I accept that. But I guess my retort would  
19 be, it seems like when we're speaking about, you know, using conventional  
20 methods and computing, it seems like if *Law* is saying, okay, well, we can  
21 automatically update, why can't 305 also automatically update? I guess  
22 would be my question if that's within, you know, what's being envisioned by  
23 *Law*.

24 MR. HANNAH: Because firm 305 is a group of people that are  
25 monitoring -- that are monitoring the nuclear plant. There's -- it -- I mean, it  
26 goes back to what I said earlier, is that every disclosure in *Law* is that --

1 that's what firm 355 is. It identifies it as people. They've never identified it  
2 as a server. And so -- and I was trying to explain is the reason they do that is  
3 because we have critical infrastructure that we're dealing with here.

4 And so that's why *Law* in paragraph 83 doesn't say that it's an  
5 automatic update to firm 305 or pinging 305 for some new rules because  
6 firm 305 talking about, you know, we're talking about lawsuits, going to get  
7 sued to oblivion if there's going to be some type of update that they're going  
8 to automatically generate, and then it destroys a nuclear plant. So that's why  
9 -- that's why *Law* doesn't do this. And so when it talks about this detection  
10 of certain network conditions that may trigger automatic updates on alarm, it  
11 has nothing about a server doing any of that. And that's -- I mean, that's the  
12 reason we're so.

13 JUDGE TURNER: Counsel, you're at 35 minutes, so you have 10  
14 more minutes. But that would be using up some of your rebuttal, so --

15 MR. HANNAH: Okay.

16 JUDGE TURNER: -- you may proceed as you see fit..

17 MR. HANNAH: Let me just -- I'll just raise a couple -- a couple of  
18 more points and reserve the rest for rebuttal. See what's said.

19 You know, we have this in our papers. It's, you know, it's all over the  
20 place. You know, I hope Your Honors take a look at it with regard to the  
21 two networks. *Law* discloses two different separate networks. The only  
22 argument that -- I mean, the only real argument the other side raises is  
23 Figure 3, saying that this network access device shows that these are actually  
24 one network. I think that it shows the opposite.

25 A network access device is something that accesses two different  
26 networks, plain and simple. And so you wouldn't have to have a network

1 access device if you had a single network here. And that's what *Law*  
2 discloses.

3 And the reason that you want these isolated is, again, comes back to  
4 this critical infrastructure problem. You don't want to have critical  
5 infrastructure that's going to be, you know, connected in some unsecure way.  
6 And so you have this network access device. I think it proves exactly  
7 opposite what Petitioner was saying. I think it actually proves that there are  
8 two networks, because otherwise it would show them -- show them  
9 combined.

10 And then finally, and I'll reserve the rest, we talk about this no  
11 dynamic security policy. And I just want to make sure that we get this clear  
12 in terms of what the argument is. The argument here is not, as Petitioner  
13 puts it. The argument is that the dynamic security policy required by the  
14 claims has to be generated by the security policy management server. *Law*,  
15 that secured that dynamic security policy that gets generated is done by the  
16 operators within the -- within the plant, within the nuclear plant themselves.  
17 It's never generated by a server. And I think that's the point of the dynamic  
18 security policy argument is that it's done in the wrong place. And the reason  
19 that *Law* does that is because these networks are so specific and so critical  
20 and unique that you have to give firm 305 essentially a mapping of what you  
21 have. And so you're not going to have a server that's going to dynamically --  
22 or generate the dynamically secured -- dynamic security policy.

23 JUDGE AMUNDSON: This is Judge Amundson. On that point,  
24 though, I just wanted to ask about a couple of disclosures in *Law*. And one  
25 of them -- one of them is in paragraph 90, where it indicates that a user's  
26 graphic display may include a number of preconfigured network security

1 profiles. And then the other one is in paragraph 102, where it indicates that -  
2 - where *Law* indicates that -- that the rule -- that the rule profiles may be  
3 generated by a manufacturer of process control equipment. So how do those  
4 disclosures comport with your theory that it's the system operators who  
5 create the initial ruleset?

6 MR. HANNAH: I think -- I love paragraph 90. It's one of my  
7 favorite paragraphs because it has the rule distribution in there.

8 Yeah, I think that that's -- and I'll take a look during the break here,  
9 but I think that's actually proven our point, right, is this is configurable by an  
10 operator or other personnel from a graphic display. Right? That's the third  
11 line. So it specifically says that the operator is using the graphic display and  
12 not firm 305.

13 See, their point, that's where this -- the misconception comes in.  
14 They're pointing to firm 305 as the security policy management server. First  
15 of all, it doesn't include a server. Second of all, nothing originates from  
16 there. Right? Anything that they're pointing to for the dynamic security  
17 policy actually originates by the operators of the system themselves within  
18 the plant. That's paragraph 90.

19 What was the other one, Your Honor?

20 JUDGE AMUNDSON: 102, paragraph 102, where it indicates that  
21 the rule profiles can be generated by a manufacturer of process control  
22 equipment.

23 MR. HANNAH: Oh, yeah. Yeah. So, again, so that's within the  
24 plant itself. Right? So that's not firm 305. The manufacturer of the  
25 equipment is the valve, the company that makes the valves. Right? And  
26 they say, okay, here's a graphical user interface for the valves, so the

1 operators can look at the valves. But that's not a disclosure of firm 305  
2 doing it. The firm 305 is not the manufacturer. Right? They're just a  
3 security firm that sits out -- a nontraditional security firm, or this is specific  
4 to critical infrastructure, but they're a security -- "security" firm that sits out,  
5 that's going to be monitoring. They're not manufacturers of anything.

6 So I think that 90 and 102 actually support our cause, saying, yeah,  
7 you're not going to generate a dynamic security policy by firm 305. You're  
8 doing it within the plant.

9 JUDGE AMUNDSON: All right. Thank you.

10 MR. HANNAH: (Inaudible) within the plant. Yeah, all right. With  
11 that, if you don't have any other further questions, Your Honor, I'll reserve  
12 the rest of my time.

13 JUDGE TURNER: Okay. You will have five minutes for surrebuttal.  
14 Back to Petitioner, you have 10 minutes for rebuttal again. You may begin  
15 when you're ready.

16 I think you may be on mute.

17 MR. DETRIXHE: Thank you, Your Honor. I was.

18 So, where to begin? Almost everything we just heard from Mr.  
19 Hannah is a new argument that wasn't explained in Patent Owner's response.  
20 I'll do my best to address those arguments.

21 In particular the argument that Counsel spent the most of his time  
22 presenting, which, as I understand it, Counsel, the Patent Owner contended  
23 that contrary to *Law's* teaching, that *Law's* firewalls did not actually  
24 implement its ruleset, namely ruleset 147. Instead, Counsel appears to argue  
25 that the firewall simply passed through the rules to particular devices  
26 without actually implementing the rules.

1 First, this is an entirely new argument. Counsel relied extensively on  
2 paragraph 90 of *Law* in making this argument about taking rules that are  
3 device-specific and pushing those rules to devices, but that isn't argued in  
4 Patent Owner's response at all. To the contrary, paragraph 90 isn't even  
5 cited in the section of Patent Owner's response that disputes that the  
6 firewalls apply the same rules. To the contrary, paragraph 90 of *Law* is only  
7 mentioned in the context of the third and fourth arguments, namely the  
8 arguments regarding automatically updating rules and the argument  
9 regarding provisioning the initial ruleset. And there the context was citing  
10 paragraph 90 to argue that IT personnel would have been required, not this  
11 new argument about not implementing the rules.

12 But regardless of it being completely new, it's also completely wrong,  
13 and a desperate attempt to say that that is clearly invalid. As the petition  
14 explained extensively, *Law*'s firewalls 146 implement and enforce the  
15 rulesets 147. *Law* explains that the enforcement of the rulesets, you know,  
16 the action field in the rule table, accept or deny, it's enforcing those rules  
17 drop packets. And, you know, at bottom, Patent Owner appears to be  
18 conflating enforcement of the ruleset with this optional feature where  
19 additional rulesets -- a subset of rulesets can be distributed to the internal  
20 devices.

21 So essentially, Patent Owner is conflating the actual enforcement of  
22 the ruleset with the fact that you can also distribute a subset of the ruleset.  
23 And the latter being able to distribute a subset of the rulesets in no way  
24 implies that the firewalls itself wouldn't implement the rulesets 147, which  
25 include all of the rules, including the specific device component rules.

1           This is explained in the petition, but there would be no reason to let  
2 traffic pass through the boundaries of the firewalls, especially in a sensitive  
3 environment such as the nuclear process environment, and only enforce  
4 these important rules at some internal point in the network. One, that's not  
5 disclosed by *Law*, but it'd be completely contrary to *Law*'s disclosures that  
6 are relied on by the petition.

7           And we also heard the entirety of Mr. Hannah's argument about  
8 nuclear control systems. First, that was not a theme in Patent Owner's  
9 response. They mentioned the idea that *Law* is applicable to nuclear process  
10 environments twice: first in the introduction and then again in the  
11 background of *Law*. Not any substantive arguments. So to hear this as like  
12 a central theme of how Mr. Hannah's responds and everything he's arguing is  
13 directed to this nuclear embodiment, is a little bit baffling to say the least.

14           But, you know, it's also, in addition to being a completely new  
15 argument, it's also wrong. Yeah, sure, *Law* has one or two instances that  
16 discuss a potential application to nuclear environments, but, as the petition  
17 explained, you know, *Law* is much more broadly applicable. Paragraph 3 of  
18 *Law* states that, you know, example process control systems that are relevant  
19 to *Law* dimensions include those used in power generation by any means,  
20 not just nuclear: chemical, petroleum, and other processors.

21           Also, *Law* repeatedly discloses enforcement of its rulesets and  
22 enforcing the rules to drop packets. So not only does *Law* explicitly disclose  
23 that firewalls enforce and implement rules and explain in detail in the  
24 petition, it's just baffling the notion that *Law*'s firewalls would allow traffic  
25 to pass without implementing its own ruleset, which is a completely  
26 unsupportive proposition.

1           And now -- I'd now like to turn to this whole idea that the firm 305  
2   does not necessarily comprise the server. I'm having trouble understanding  
3   this argument. You know, *Law* explicitly discloses that the firm 305 uses  
4   computer-implemented algorithms to construct the ruleset and then  
5   distributes the rulesets over the Internet. It's not clear, you know, first of all,  
6   Patent Owner didn't make this argument in his response, but it's not clear  
7   what they're now contending, that, you know, people mail the information in  
8   the ruleset rather than sending it over the Internet. Or, more precisely, as  
9   Counsel seemed to be saying is that unless there is a request and distributing  
10   the rulesets in response to that request, then there isn't the client-server  
11   relationship that would be necessary for a server, and that's contradicted by  
12   the actual teachings of *Law*. As Your Honor mentioned, paragraph 83 of  
13   *Law* explicitly discloses detecting network conditions that would trigger an  
14   automatic update of the ruleset 147 applied by the firewalls.

15           JUDGE AMUNDSON: This is Judge Amundson here. I had a  
16   question on that, on paragraph 83.

17           MR. DETRIXHE: Yes, Your Honor.

18           JUDGE AMUNDSON: As I understand Centripetal's position, it's  
19   that, okay, paragraph 83 says or discloses triggering an automatic update,  
20   but paragraph 83 does not disclose what entity triggers that automatic  
21   update. And Petitioner hasn't shown that it's firm 305 that's going to trigger  
22   that automatic update. Could you maybe respond to that?

23           MR. DETRIXHE: Yes. So paragraph 83 states, and this is in the  
24   context of the process control system 100, so, you know, on the internal side  
25   of the network protected by firewalls, not talking about firm 305. And the  
26   final sentence of that paragraph states, "Detection of certain network

1 conditions may also trigger an automatic update of the rulesets 147 or an  
2 alarm to prompt a user to perform a manual update of the ruleset for other  
3 actions to fully secure the system 100." The system 100 is the process  
4 control system. It's not talking about the firm 305. Nor would it make sense  
5 for the detected network conditions within the process control system to  
6 refer to firm 305. I mean, *Law* discloses the alternative embodiment in  
7 which the process control system 100 is sending information up to the server  
8 305 so that it may use that information in addition to all of the other  
9 information coming from sources 315, as well as, you know, any other  
10 information from the computer-implemented methods for constructing rules,  
11 all of those may be used by firm 305 in constructing the rulesets.

12 But with respect to this disclosure in paragraph 83 about protecting  
13 network conditions to perform an automatic update, you know, that occurs  
14 within the process control system itself, which goes to the point that when  
15 those conditions are detected, it would necessarily be sending a request to  
16 the server 305 and getting the current updated ruleset in response. There's  
17 no other explanation for how that would work. I mean, the firm 305 doesn't  
18 magically coincidentally know to send the update when those conditions are  
19 detected. It's implied, as stated in the petition, that there's a server there that  
20 sends those rules in response to the automatic update request.

21 I'd also like to address Counsel's suggestion that -- and he makes a  
22 bunch of wild unsupported statements regarding *Law*'s disclosure. Perhaps  
23 the most wild is that the firm 305 only includes people. I mean, look at  
24 paragraph 88. The firm 305 executes computer-implemented algorithms. I  
25 mean, is Counsel seriously suggesting that are the people in firm 305 are  
26 manually writing down on a sheet of paper the rulesets or somehow trying to

1 figure out how a computer would have implemented the instructions to  
2 generate the rulesets? I mean, that's contradictory to the text in paragraph 88  
3 of *Law* and is a way wild speculation. Again, it is not found anywhere in  
4 Patent Owner's response.

5 JUDGE TURNER: Counsel, you're at time. You may -- you may  
6 finish.

7 MR. DETRIXHE: Thank you. That was all I had, Your Honor,  
8 unless you had any other questions for me.

9 JUDGE TURNER: Let me survey the panel, see if we have any  
10 questions. Doesn't look like it. So thank you very much. We will go back  
11 to Mr. Hannah.

12 Mr. Hannah, you have four minutes and I'll be liberal. I was liberal  
13 with Petitioner's counsel as well, so please begin when you're ready.

14 MR. HANNAH: Oh, sure. Thank you, Your Honors. I appreciate it.

15 So I did look for a couple more citations during our break, as  
16 Petitioners are trying to say that we didn't raise this argument saying that  
17 rules are applied to particular devices. Additional support, you can -- and I  
18 was looking specifically for Dr. Goodrich. Your Honor Turner, you asked  
19 for that. Right. And so for Goodrich's declaration, we have at least 69 and  
20 70 are some places to take a look. And then those are citations to *Law*  
21 paragraphs 59 and 88, where he explains how those rulesets are applied and  
22 they are to the particular devices, and, therefore, it doesn't apply to all the  
23 traffic that traverses the boundary.

24 So with that, you know, with that, I'd like to address some of  
25 Petitioner's counterarguments. So, Petitioner made an argument saying that  
26 it wouldn't make sense for the firewall not to implement rules for control

1 valves at the firewall. Well, as we pointed out, there is a reason for that,  
2 because the firewall doesn't know what to do with that traffic. Specifically,  
3 as I pointed out, the only disclosure in *Law* is that the traffic will be  
4 translated by the firewall, but there's no indication that there will be rules.

5 And if you think about it, it doesn't make sense that if *Law* was  
6 implementing those rules at the perimeter, then why the heck does paragraph  
7 90 say that you distribute the rules to the various devices? It doesn't make  
8 sense. If those rules are going to be enforced, then they don't need to be  
9 distributed. You don't need to use that extra computation and that power in  
10 order to enforce those rules.

11 The reason is, is because the firewall can't enforce those rules, and so  
12 it has to send those rules to the control valves, to the actuators, to the various  
13 devices in order for them to implement it. And that's exactly what the  
14 paragraphs say that we were talking about earlier, which describes how the  
15 devices themselves will implement the rules in order to protect against  
16 malicious traffic.

17 So I would disagree that it would be baffling that the firewall would  
18 not implement the rules. It's not baffling if the firewall can't, and that the  
19 disclosure in *Law* actually specifically says that you're going to send those  
20 down.

21 The other point that Counsel addressed from Your Honors was  
22 paragraph 83. And I think, based on the admissions that we have on the  
23 record, that there's no longer a dispute that the automatic generation or the  
24 automatic updating happens within the process control system. Because it  
25 happens within the process control system, that means that firm 305 is not  
26 doing any type of automatic updating or generating of the rules. And that's

1    why my whole point was that paragraph 83 doesn't disclose firm 305  
2    because that's what they point to as the security policy management server.

3            And so, I believe, and we can go back and look at the record, that it is  
4    now crystal clear that any -- the only disclosure that we have about  
5    automatically updating rules is in paragraph 83. And it's undisputed now  
6    that that automatic updating or generating of rules does not happen within  
7    firm 305. So I think that's an important point that we need to look at for the  
8    record, especially the discussion that happened there during the -- during the  
9    rebuttal.

10           And then, you know, finally, you know, Counsel made some  
11    arguments saying that we're trying to say that firm 305 doesn't use  
12    computers. I think the Panel understands that that's not the point. The point  
13    is firm 305. The people who write the rules, who are monitoring the system,  
14    are people. They might use computers, but the people that are monitoring  
15    the rules, they are not servers. They are not security policy management  
16    servers as required by the claims that will automatically generate and send  
17    rules to the packet security gateways. And that's the point. That's the point.

18           And every disclosure that you see when it talks about computer  
19    algorithms, when it specifically talks about that, the computer algorithms are  
20    there for the person, the IT person, to test the rule before the IT person sends  
21    the rule. There's never a disclosure that there's a request-response  
22    architecture in which a request is sent, a server is going to automatically  
23    generate a rule, and then the response is going to be the updated ruleset.  
24    And that's what -- that's what the claim is requiring the server to be able to  
25    do that.

1           With that, Your Honor, that concludes my presentation, but I'm happy  
2   to answer any questions.

3           JUDGE AMUNDSON: This is Judge Amundson.

4           JUDGE TURNER: You're at time, but I'll let Judge Amundson ask  
5   his question. Sure.

6           MR. HANNAH: Thank you.

7           JUDGE AMUNDSON: I'm looking at *Law's* Figure 3.

8           MR. HANNAH: Yes.

9           JUDGE AMUNDSON: And just focus on the left side where --

10          MR. HANNAH: In Figure 3?

11          JUDGE AMUNDSON: Yeah.

12          MR. HANNAH: I have it on the screen.

13          JUDGE AMUNDSON: Right. We've got process control subsystem  
14   105a. And I understand your argument about pushing all these things down  
15   to the valves and the actuators and the whatevers, but here, what I don't  
16   understand is why wouldn't the firewall 146a still have some rules to protect  
17   the workstation 122 and the whatever, the workstation 120 and workstation  
18   122?

19          MR. HANNAH: Your Honor, it might. But the point is that the  
20   ruleset that's applied here has to be applied to all traffic that traverses the  
21   boundary. So if traffic is getting analyzed, that goes to the workstation that  
22   some ruleset that's going to apply to the workstation, there's going to be rules  
23   that are going to be applied just to the control valves. And this firewall  
24   distributes that rule to the valve. And the disclosure in *Law* says that if that  
25   information comes in, the firewall will not do anything to it but translate it.

1           So the point is that this is not the conventional firewall that exists  
2 today in which you have a security profile that comes in from some  
3 management server, and I'm going to be protecting my network against all  
4 the Internet traffic that comes in. That's the point that I was trying to make,  
5 is that this is a very specific application in that this firewall will apply some  
6 rules, but it will not apply all the rules. It will send those rules down to the  
7 various devices. And because of that, those rules are not implemented at the  
8 boundary. That's all the traffic that traverses that boundary.

9           JUDGE AMUNDSON: All right. I think I understand. Yes. Thank  
10 you.

11          JUDGE TURNER: This is Judge Turner. I thank the parties for their  
12 arguments and attendance. The case is submitted. We'll go off the record  
13 and see if the court reporter needs any spellings or clarifications at this time.

14          (Whereupon, the proceedings at 4:31 p.m. were concluded.)

IPR2023-00445  
Patent 10,785,266 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  
svdocketing@kramerlevin.com

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