

Transcript of the Testimony of:

WENKE LEE

NETSKOPE, INC.

VS.

FORTINET, INC.

July 26, 2023

Volume I



I M A G I N E
R E P O R T I N G

AT UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

NETSKOPE, INC.,
Petitioner,
v.
FORTINET, INC.,
Patent Owner.

PTAB Case No. IPR2023-00030

Patent No. 10,826,941 B2

REPORTER'S TRANSCRIPT

DEPOSITION OF

WENKE LEE

Wednesday, July 26, 2023

Via Zoom Video Conferencing

9:02 a.m.

Reported by: Rachel N. Barkume, CSR, RMR, CRR
Certificate No. 13657

A P P E A R A N C E S

FOR THE PETITIONER:

PERKINS COIE LLP
By: ANDREW KLEIN
WEI YUAN
Attorneys at Law
11452 El Camino Real, Suite 300
San Diego, California 92130
(858) 720-5700
aklein@perkinscoie.com

FOR THE PATENT OWNER:

QUINN EMANUEL URQUHART & SULLIVAN LLP
By: QUINCY LU
Attorney at Law
865 South Figueroa Street, Floor 10
Los Angeles, California 90017
(213) 443-3251
quincylu@quinnemanuel.com

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25

I N D E X

	PAGE
EXAMINATION BY MR. LU	4

--o0o--

E X H I B I T S

EXHIBIT	PAGE
---------	------

(No exhibits were marked.)

1 BE IT REMEMBERED that on Wednesday, July 26,
2 2023, commencing at 9:02 a.m. thereof, via Zoom Video
3 Conferencing, before me, Rachel N. Barkume, a Certified
4 Shorthand Reporter in and for the State of California,
5 remotely appeared from Atlanta, Georgia,

6 WENKE LEE,
7 a witness called on behalf of the Patent Owner, who,
8 having been first duly sworn by me to testify the truth,
9 was examined and testified as follows:

10 EXAMINATION

11 BY MR. LU:

12 Q. Good morning, Dr. Lee. Could you spell your
13 full name for the record.

14 A. W-E-N-K-E, L-E-E.

15 Q. Thank you. And, Dr. Lee, where are you located
16 today?

17 A. I'm in Atlanta, Georgia.

18 Q. And is Atlanta your place of residence?

19 A. Yes.

20 Q. Is anyone else in the room with you today?

21 A. No. This my home office. The background is
22 not. The background is my -- whatever office
23 building.

24 Q. Okay. Understood. It's a fake background,
25 just for the record?

1 A. Yes. Right.

2 Q. Do you have any notes or documents in front of
3 you?

4 A. I printed clean copies of my declaration. It's
5 clean. And also I print -- yeah, I printed a clean copy
6 of the '941 patent, a clean copy of the Wang patent, a
7 clean copy of the Chambers patent, and a clean copy of
8 the Terrill patent. And that's it.

9 Q. Okay. And so by "clean copy," you mean there
10 are no notes or highlights on those copies?

11 A. No. Nothing.

12 Q. Okay. Thank you. So I will be referring to
13 your declaration and those prior art references
14 throughout this deposition. I may also refer to other
15 exhibits. We'll see. But since you have physical
16 copies, I think I will just reference the exhibit number
17 of those documents and just ask you to look through
18 those rather than upload them to the Zoom and having you
19 download. Unless you would prefer I upload electronic
20 copies. It's up to you.

21 A. Yeah, that's good. Although I'm not sure I can
22 remember the exhibit number so well, but if you tell me
23 which patent by the name, then it would be easier for me
24 to pick up the document.

25 Q. Oh, absolutely, yes. I will refer to the name

1 as well as the exhibit number so we have a clean record.

2 A. Okay.

3 Q. All right. So you just took an oath to tell
4 the truth; correct?

5 A. Yes, I did.

6 Q. And is there any reason you cannot tell the
7 truth today?

8 A. No.

9 Q. Is there anything that would prevent you from
10 giving truthful and accurate deposition testimony today?

11 A. No.

12 Q. Dr. Lee, have you ever had your deposition
13 taken before?

14 A. Yes, I have.

15 Q. And how many times?

16 A. About ten times.

17 Q. And how many times in the past year have you
18 had your deposition taken?

19 A. Four times.

20 Q. Four times? And were those for patent cases?

21 A. Yes.

22 Q. So all four were for patent cases; is that
23 correct?

24 A. That's correct.

25 Q. And were they for -- all four for IPR cases or

1 were there district court litigation cases as well?

2 A. I don't know -- I mean, I don't recall exact
3 detail distinction, but definitely IPR. Whether
4 district court or not, I don't remember.

5 Q. Okay. Have you ever testified at trial as a
6 witness?

7 A. Yes, I have.

8 Q. And how many times?

9 A. Once. And that time, I was scheduled, but I
10 ran out of time, so I didn't -- you know.

11 Q. Okay. And when was that time that you
12 testified as a trial witness?

13 A. I think about maybe seven years ago.

14 Q. And was that for a patent case?

15 A. Yes.

16 Q. And what was the nature of the patents, if you
17 remember?

18 A. Yeah. It was SRI versus Cisco. I was on the
19 SRI International side --

20 (Simultaneous crosstalk.)

21 BY MR. LU:

22 Q. Oh, go ahead.

23 A. Sorry. SRI, they're the patent owners, so
24 they're -- they are suing other companies for infringing
25 their patents.

1 Q. Uh-huh. And so for those patents, what was the
2 field of endeavor for those -- of those patents?

3 A. Those patents -- they were on network intrusion
4 detection, network monitoring.

5 Q. Okay. Understood. For the depositions that
6 you took in the last year, were they all with -- were
7 you represented by Perkins Coie in all of them, or were
8 there other law firms involved?

9 A. Other law firms involved, yes.

10 Q. Were any of them -- for any of those
11 depositions, were you represented by Perkins Coie?

12 A. No.

13 Q. All right. Are you being compensated for your
14 testimony in this proceeding?

15 A. As part of my work on this case, yes.

16 Q. And who is providing that compensation?

17 A. It's through Perkins Coie. I mean, we -- you
18 know, the invoice will be sent to them.

19 Q. But the -- is Fortinet paying for those
20 invoices?

21 MR. KLEIN: Object to form.

22 BY MR. LU:

23 Q. Excuse me. Is Netskope paying for those
24 invoices?

25 A. I assume so.

1 Q. And what is your hourly rate, Dr. Lee?

2 A. I think for deposition work, if I recall
3 correctly, it's about \$600 an hour.

4 Q. And so you said for deposition work, you --
5 \$600 an hour.

6 Is it also \$600 an hour for your preparation of
7 this declaration in this proceeding?

8 A. Preparation -- you know, prep work for
9 deposition, yes.

10 Q. Let me re-ask that.

11 So is it also \$600 an hour for your work in
12 preparing the declaration that you provided in this
13 proceeding?

14 A. If I recall correctly, I think for deposition,
15 maybe lower. I don't know, maybe 450 an hour. I mean,
16 I -- I don't recall the precise number.

17 Q. So you said for deposition, it was maybe 450 an
18 hour.

19 Did you mean to say for the declaration, it was
20 maybe 450 an hour?

21 A. Yes. For the declaration work, it's 450 an
22 hour. For deposition and related prep work, it's \$600
23 an hour.

24 Q. So do you typically charge a higher rate for
25 deposition work?

1 A. Yes.

2 Q. Besides your hourly rates, are you being
3 compensated in any other way?

4 A. You mean the context of this case; right?

5 Q. Yes.

6 A. No.

7 Q. How much have you billed Netskope to date for
8 your work in all of the IPR matters?

9 MR. KLEIN: Object to scope.

10 THE WITNESS: I don't recall exact number. I
11 would say dozens of hours.

12 BY MR. LU:

13 Q. All right. So the -- your counsel objected to
14 scope. Let me re-ask the question then.

15 How much have you billed Netskope to date for
16 your work in this particular IPR matter?

17 A. Like I said, I don't recall exact number. I
18 need to go back to look at my log. I do keep a log. I
19 would say, you know, dozens of hours for sure.

20 Q. So by "dozens," do you mean over 100 hours?

21 A. I am not sure. Maybe close. I would say I
22 wouldn't be surprised. Like I said, I don't know the
23 exact number.

24 Q. Would it be close to 100 hours for just this
25 case?

1 A. Well, I mean -- you mean this -- mean this
2 patent specifically?

3 Q. Yes.

4 A. That, I'm not sure. I need to -- like I said,
5 I work on multiple patents with Perkins Coie, and I have
6 a log that basically each hour doing what, on which
7 patent. I need to go there and take a look closely, you
8 know, to answer your question. But I would say that
9 even for this particular case -- would be dozens of
10 hours.

11 Q. So you understand that Netskope has filed
12 several IPR petitions against Fortinet patents; correct?

13 A. I believe that's the case, yes.

14 Q. And you -- oh, go ahead.

15 A. I believe that true, yes.

16 Q. And you have provided declarations for at least
17 some of these IPR petitions; correct?

18 A. That's correct.

19 Q. Do you remember how many?

20 A. I would say in the range of two or three.
21 Maybe three, but two for sure. I think so, yeah.

22 Q. But this is the first time you've been deposed
23 for one of these Netskope/Fortinet IPR petitions?

24 A. That's correct.

25 Q. So for the hours that you billed to Netskope,

1 does that include preparing for and appearing at this
2 deposition?

3 A. Yes.

4 Q. Dr. Lee, when were you first retained by
5 Netskope as an expert for these IPR proceedings?

6 A. I try to remember. More than year ago for
7 sure. I don't know whether it's two years or not.
8 Yeah, I mean, again, I am not -- I need to look back at
9 my log to actually track it. Yeah.

10 Q. So you would say maybe last summer or last
11 spring -- early last year or later last year?

12 A. I would say it's before last year. I mean,
13 that's how I recall it. Maybe the fall of the year
14 before last year, so that would be 2021, I think.

15 Q. Okay.

16 A. Again -- again, I'm just -- try to -- best from
17 my memory.

18 Q. Understood. Yes. If you can't remember
19 exactly, just provide the best you can.

20 A. Yeah.

21 Q. Did you do anything to prepare for this
22 deposition, Dr. Lee?

23 A. I'm sorry. Can you repeat that question again?

24 Q. Did you do anything to prepare for this
25 deposition?

1 A. What do you mean "anything"?

2 Q. Did you meet with any attorneys to prepare for
3 this deposition?

4 A. I -- I did work with the counsel, the team,
5 yeah. From Perkins Coie, yes.

6 Q. And which attorneys did you work with to
7 prepare for this deposition?

8 A. Andrew, Wei, and Babak.

9 Q. And so that's Andrew Klein, Wei Yuan, and who
10 was the third person?

11 A. Babak Tehranchi. I hope I say his name
12 correctly.

13 Q. We'll get that name later.

14 Did you meet with these attorneys multiple
15 times in preparation for your deposition?

16 A. Yeah, couple times. Yes.

17 Q. Do you know how many times?

18 A. Two times.

19 Q. And how long did you meet with them for each
20 time?

21 A. I think the first time is close to two hours.
22 The second time I would say close to four or five hours,
23 yeah.

24 Q. Okay. And when were those meetings?

25 A. I think one was last Thursday or Friday; don't

1 remember. Another one was yesterday.

2 Q. And did you review any documents during these
3 meetings with your attorneys?

4 A. I review my declaration, the patents -- patents
5 '941, the Wang, the Chambers, Terrill. I also looked at
6 the initial response from the patent owner and also the
7 Court decision as well.

8 Q. And by Court decision, you mean the Board's
9 institution decision?

10 A. That's correct. Yes.

11 Q. Okay. I'd like you to turn to Exhibit 1002,
12 which is your declaration.

13 A. Okay.

14 Q. And this is for IPR 2023-00030, Exhibit 1002
15 from that case. Now, I'd like you to turn to the last
16 page, page 136.

17 A. Okay.

18 Q. Dr. Lee, is that your signature on page 136?

19 A. Yes.

20 Q. And did you handwrite this signature, or is it
21 electronic?

22 A. I handwrite using the mouse, Microsoft Word;
23 then you can say draw. So it's my handwriting.

24 Q. I see. And you handwrote the signature on the
25 declaration, or did you provide the signature

1 electronically?

2 A. I do it, like I said, on Microsoft Word using
3 Microsoft Word's draw feature to draw it on the
4 document.

5 Q. I see. Did you write the first draft of this
6 declaration?

7 A. I work with the counsels throughout, and -- to
8 come up with this draft.

9 Q. Okay. But my question was: Did you write the
10 first draft of your declaration?

11 A. I was --

12 MR. KLEIN: Objection to the extent -- hold on,
13 Dr. Lee. Objection to the extent it calls for
14 disclosure of information covered by the attorney/client
15 privilege. But you can say yes or no to his answer --
16 or to his question.

17 THE WITNESS: Can you repeat the question
18 again?

19 BY MR. LU:

20 Q. Sure. Did you write the first draft of this
21 declaration?

22 A. Yeah.

23 MR. KLEIN: Same objection.

24 THE WITNESS: Yeah. Okay. Thank you. So I
25 was part of the writing process.

1 BY MR. LU:

2 Q. So you were part of the writing process of the
3 first draft of this declaration? Is that what you're
4 saying?

5 A. Yes.

6 MR. KLEIN: Same objection.

7 BY MR. LU:

8 Q. Did you write the entire declaration?

9 MR. KLEIN: Same objection.

10 THE WITNESS: So like I said, I -- I work with
11 the counsel throughout the -- you know, throughout the
12 process, and we discuss everything we wanted to write.
13 I was part of the writing process. I -- you know, I
14 wouldn't be able to tell you exactly which word was my
15 writing to it, but I definitely, you know, own this
16 document because, like I said, I was in the process.

17 BY MR. LU:

18 Q. Okay. Understood. Yes or no -- so you did not
19 write every single word in this declaration; correct?

20 MR. KLEIN: Same objection.

21 THE WITNESS: So like I said, I know every
22 single word is put in. Did I actually type it in? Not
23 every single word.

24 BY MR. LU:

25 Q. Okay. Thank you.

1 How many times have you ever worked as an
2 expert in a patent case before this one?

3 A. I would say around 16, 17 times.

4 Q. And over how many years would that be?

5 A. I would say over close to 20 years.

6 Q. Okay. So you began working as an expert in
7 patent cases in the early 2000s? Is that your
8 testimony?

9 A. May not be as early as -- maybe 2005 or '6 time
10 frame. I'm not -- I don't know exactly. Yeah. Maybe
11 2005, '6 time frame, yes.

12 Q. Okay. Have you ever worked for Netskope before
13 these IPR petitions?

14 A. No. I don't think so. No.

15 Q. Have you ever worked with Perkins Coie before
16 these IPR petitions?

17 A. No, I have not.

18 Q. Have you ever had any of your expert opinions
19 excluded before?

20 A. No.

21 Q. So you said you previously consulted around 16
22 or 17 times. Not all of those engagements involved
23 testifying; correct?

24 A. Not all of them. That's correct.

25 Q. And so what else were you doing if you were not

1 testifying in those engagements, just generally?

2 MR. KLEIN: I'll just caution the witness not
3 to disclose anything that might be covered by
4 confidentiality agreements. I'm not sure if there is,
5 but just in case.

6 THE WITNESS: Okay. Yeah. General expert
7 work; like, declaration kind of thing, yeah.

8 BY MR. LU:

9 Q. All right. Going back to your declaration,
10 Exhibit 1002, could you turn to paragraph 36, which
11 begins on -- excuse me, paragraph 3 -- hold on -- yes,
12 paragraph 36, which begins on page 11.

13 A. Okay.

14 Q. Let me know when you're there.

15 A. Yes, I'm here.

16 Q. All right. So here you say, "The development
17 of firewalls" -- actually, sorry. Let me back up.

18 Do you have any changes that you want to make
19 to your declaration?

20 A. No, not --

21 Q. Corrections?

22 A. No, not at this moment.

23 Q. No?

24 A. No.

25 Q. Okay. Going back to paragraph 36. So you

1 state here, "The development of firewalls was motivated
2 by the need to control what data, i.e., network traffic,
3 can be allowed to go from a local network onto the
4 internet and come from the internet into the network.
5 In other words, firewalls can screen traffic to and from
6 a network. For example, firewalls in 1989 can already,"
7 quote, "'screen packets based not only on destinations
8 but on sources or source-destination pairs,'" end quote,
9 "and with Cisco firewall systems in 1989," quote, "'one
10 could deny access to all but one host on a particular
11 network. The Cisco gateways also allow discrimination
12 based on IP protocol type and TCP or UDP port numbers,"
13 and you have a citation.

14 And then you go on and say, "That is, packet
15 filtering rules, i.e., rules for blocking or admitting
16 packets, were available prior to 1989, and firewalls
17 were developed to implement such rules."

18 Did I read that correctly?

19 A. Yes.

20 Q. And you still agree with this statement,
21 Dr. Lee?

22 A. Yes.

23 Q. Okay. So if I refer to these firewalls as
24 traditional firewalls, would you understand what I'm
25 saying?

1 A. I would say that would be the firewalls at the
2 time, like, the late 1980s.

3 Q. Did firewalls in 2018 still -- were --
4 withdrawn.

5 In 2018, were firewalls still able to provide
6 these functions that you describe in this paragraph?

7 A. Yes, and more.

8 Q. Okay. So when you say -- so -- withdrawn.

9 You would agree that these traditional
10 firewalls you described here could control the flow of
11 network traffic to or from a network?

12 A. That's correct.

13 Q. And as you say, these traditional firewalls
14 could control -- withdrawn.

15 So you would agree that such control also
16 includes traffic to and from the internet; correct?

17 A. Yes. Basically from network to network. So
18 internet is another network. At least with respect to
19 local network, yeah.

20 Q. And the internet existed in 1989?

21 A. Yeah. Even before that, yes.

22 Q. Did the World Wide Web exist in 1989?

23 MR. KLEIN: Object to form.

24 THE WITNESS: We won't call it -- we didn't
25 call it World Wide Web, but, you know...

1 BY MR. LU:

2 Q. What did you call it?

3 A. I forgot the name, but some kind of a
4 document --

5 (Reporter clarification.)

6 THE WITNESS: Document search and retrieval
7 system was already there. But we didn't call it World
8 Wide Web.

9 BY MR. LU:

10 Q. So these firewalls that you describe in
11 paragraph 36, could they automatically block traffic
12 from another network or from another domain?

13 A. Yeah, sure. If they know the IP address in
14 particular, yes, they can do that.

15 Q. So you said if they knew the IP address in
16 particular.

17 Do you mean the IP address of the network?

18 A. Meaning the domain. I'm talking about
19 domain.

20 Q. So assuming the domain had a single IP address,
21 if they know that IP address, they can block traffic
22 from it. Is that what your -- what you said?

23 A. A range of IPs. Doesn't have to be single
24 IPs.

25 Q. Correct. So if the firewall -- or if the

1 firewall administrator knows either the domain's single
2 IP address or its range of IP addresses, it could block
3 traffic from that domain; is that correct?

4 A. That's correct. And also depending on the
5 protocol, you're not sure about the IP address, meaning
6 IP address can vary from day to day. But if you know
7 exactly the domain name, you're able to actually find it
8 from the traffic, you can also block that traffic -- you
9 can also block traffic from that domain. So really
10 depending on the exact nature of the traffic.

11 Q. Excuse me. Did these firewalls use a single
12 shared network address to control traffic to and from
13 another domain?

14 A. Can you elaborate that question? I'm not sure
15 I understand.

16 Q. So the firewall you described in paragraph 36,
17 did it have its own network address?

18 A. So again, it's a complicated matter meaning
19 that depending on where you place it, you may or may not
20 need to have a so-called -- your own unique
21 internet-facing IP address. But of course, you need to
22 have -- have a way to -- to reach it in particular if
23 you are an administrator.

24 So it does have a, you know, address, whether
25 it's a internet-facing publicly-known unique IP

1 address -- again, depending on the situation. Yeah, you
2 don't have to have it, in terms of a internet-facing
3 unique IP address. Yeah. Again, those are details
4 that depending on the deployment situation.

5 Q. Right. So when you say you don't have to have
6 an IP address -- or excuse me, when you say you don't
7 have to have a publicly-known external IP address, that
8 is because not all firewalls interface with the
9 internet; is that correct?

10 A. No, that's not what I meant. I meant is
11 that -- what I meant was that you don't need to have a
12 unique IP address that's known internet -- that's
13 fixed -- that's basically fixed; hey, this IP -- this
14 firewall has to have this IP address and it's fixed.
15 That's usually -- normally doesn't have to be this way.

16 There's multiple ways to deploy and configure
17 the firewall. What it comes down to it is that what you
18 want is that -- to make sure is that when you send
19 traffic to that network, that traffic would go through
20 the firewall for that network. That's all. And then
21 multiple ways you can do this.

22 Q. And one of those ways you can do this is by
23 having the firewall have a single address; correct?

24 A. To be honest, I haven't seen such a situation
25 where say, hey, my firewall was known for this IP

1 address; it's fixed; it's known for internet. That's
2 not normally how people would do it. I mean, anybody
3 would do it that way -- like I said, I don't recall. I
4 don't recall seeing it.

5 Q. So -- yeah. I understand. I'm not actually
6 referring to a fixed address. I'm just saying -- I'm
7 just asking -- so a -- let me re-ask the question.

8 So a firewall protects a network which can
9 constitute a number of devices; correct?

10 A. Yeah, there would be devices in a network, yes.

11 Q. And external to this network -- withdrawn.

12 And this network appears as a single device
13 that has the firewall's network address; correct?

14 MR. KLEIN: Object to form.

15 THE WITNESS: No. I mean, normally, let's say,
16 we're connected to -- sorry. I say "normally" -- you
17 don't associate or identify a network by its firewall or
18 by its firewall address. Normally don't do that. You
19 just know that -- assume that if the -- if the
20 organization is, you know -- is protected or is -- if
21 the organization has network security policy mechanism,
22 you would know that when you send traffic to that -- to
23 the network of the organization, it will go through
24 firewall. That's all.

25 ///

1 BY MR. LU:

2 Q. How do you ensure that the traffic goes through
3 the firewall?

4 A. So there are a number of things you could do.
5 I mean, there's all sorts of routers, gateways, VPN
6 technologies, and so and so forth. The whole point is
7 that you make sure that before the traffic -- let's say
8 from external -- be able to reach the device internal to
9 network, the traffic would have no choice but going
10 through the firewall.

11 Q. Do you use a firewall at home for your home
12 network?

13 A. I do. I mean, I have AT&T, network comes with
14 home, you know -- home network router with a firewall.
15 I also use VPN on my laptop. In fact, right now our
16 communication is through VPN.

17 Q. And when you're not using a VPN -- well, let me
18 ask this question first.

19 So how many devices does your home network
20 have?

21 A. I would say 40 to 50.

22 Q. Oh, okay. That's quite a lot.

23 A. I have two teenage boys. What do you think?
24 Yeah.

25 Q. Yes. Everybody has iPads and iPhones and TVs.

1 A. Yeah, Xbox, whatever.

2 Q. Yeah. Understand. So -- and your laptop -- or
3 the computer that you're using right now, that is also a
4 device on your home network; is that correct?

5 A. That's correct, yes.

6 Q. And when you're not connected to a VPN, does
7 your computer have an IP address that is known to the
8 public?

9 A. Normally, you don't -- if you're in a home
10 network, your router -- whatever the ISP gives to you --
11 has a IP address that's not even permanent. It's on a
12 lease called DHCP lease. It can be hours, can be weeks,
13 can be month, depending on ISPs. And then all the
14 devices in your network essentially share the same IP
15 address to the external world.

16 Internally, you have your own set of IP
17 address, but doesn't matter. I mean that -- your home
18 router would do the so-called network address
19 translation comes in. When traffic comes in, it would
20 translate and send the correct destination. Yeah. It's
21 very similar to a -- how enterprise network set up
22 except in a smaller scale.

23 Q. So you said internally, you have your own set
24 of IP addresses, but that doesn't matter.

25 Is that because to the external world, they do

1 not know of those internal IP addresses?

2 A. They do not know and they don't need to know
3 because everything going through my home network
4 router --

5 Q. And so --

6 A. -- connected to the outside, yeah.

7 Q. I see. And so your home network router has a
8 single IP address, although it's not permanent; correct?

9 A. That's correct. Yeah.

10 Q. So in order for -- assuming you're not on a
11 VPN, in order for my laptop to communicate with your
12 computer, I would need to send a packet that has your
13 firewall's IP address; correct?

14 A. No. Like I said -- so depending on your setup,
15 your firewall may not be having an internet-facing IP
16 address. It is -- normally your router has the
17 internet-facing IP address. And normally, you couldn't
18 even find it, you know, in the case of the home network.

19 In an organization, you can always -- because
20 you know the name of the organization, you can do all
21 kind of network lookup, information lookup, you know,
22 domain lookup to know the IP address range. And then
23 from there, you can connect to it. Particularly if
24 you're able to connect to the main address, normally
25 it's the main router, you know that the router will be

1 responsible for making sure that traffic go through the
2 firewall before reaches internal.

3 So I'm not sure you can send traffic directly
4 to my machine because you don't even know the IP address
5 of my router. I don't even know because I -- can't --
6 sorry. I don't need to. So...

7 Q. Are routers -- do routers have firewall
8 functionalities?

9 MR. KLEIN: Object to form.

10 THE WITNESS: So router's main function is to
11 route packets, you know, from one network to the other.
12 Or internally, it may be responsible for doing some of
13 the, you know, function of, let's say, you know, gateway
14 or switch, whatever you want to configure it, to do
15 network address translation.

16 It will also send -- you know, make sure that
17 the -- how to put it -- the wiring is such that before
18 traffic can reach anything internal, it goes through the
19 firewall.

20 BY MR. LU:

21 Q. So going back -- excuse me -- so going back to
22 paragraph 36, do you agree that these traditional
23 firewalls were used to screen traffic to and from
24 subnetworks within a larger network?

25 A. So I think a POSITA would easy understand that,

1 you know, in particular, if you -- I mean, again,
2 depending on how you configure your network. You can
3 configure your network so that you can control traffic
4 from, let's say, one subnet to the other or from, you
5 know, one subnet to the rest of the enterprise network.
6 Yeah. That's, I would say, obvious to a POSITA.

7 Q. Would that have been obvious in 1989?

8 A. In 1989, I would think so. I mean, you --
9 again, if you have somebody who works at AT&T Bell Labs,
10 which probably was doing some of the work in
11 networking -- anyway, I think those people would know.

12 Q. Okay. But you don't --

13 A. Obvious -- would find it obvious, I think.
14 Yeah.

15 Q. But you're not actually aware of any networks
16 that were set up with subnetworks where each subnetwork
17 had its own firewall in 1989?

18 A. So I would say -- I would say in 1989, I would
19 say big enterprise would have already done this already.
20 Just because a big organization such as AT&T or IBM --
21 there's so many different locations -- Intel, you
22 know -- there's so many locations across the world. And
23 obviously, if you in different country, different
24 region, you have your own, whatever, physically
25 computers together, you form a local area network. But

1 you do want to basically communicate with each other
2 within the company's scope and also with the internet.

3 So I would say that for those organizations,
4 you can say each location is actually a subnet, you
5 know. Let's say Intel at Oregon is -- Intel in Santa
6 Clara -- that's, I would say, easily two different big
7 subnets. And then, of course, you want to put firewall
8 at each of those subnets. You know, I would say that by
9 late 1990 -- 1980s, all these big companies already
10 doing that.

11 Q. So you provided an example where -- for
12 example, at Intel, they may have a subnetwork for
13 computers in Oregon and then a subnetwork for computers
14 in Santa Clara, California?

15 A. Uh-huh. Yep.

16 Q. Is that correct?

17 A. I would say that would be for example. Right
18 now within -- within Oregon, there are so many different
19 location, different farms like this farm, that farm -- I
20 mean, they could even have subdivided the Oregon
21 location into multiple subnets again.

22 So again, the -- the concept of subnets and
23 protecting traffic from one subnet to the other -- I
24 mean, that's well understood by 19 -- by the late 1990s,
25 I would say.

1 Q. And you said the concept of subnets and
2 protecting traffic from one subnet to the other -- you
3 would use a firewall to provide that protection -- a
4 firewall on -- for the subnet; is that correct?

5 A. So again, you could say either firewall for
6 subnet -- or there's a way that you do the switch and
7 router so that you make sure that when traffic -- let's
8 say traffic from Subnet 1 goes to -- goes through Subnet
9 2, the traffic routed through the firewall that you pay
10 somewhere -- that you make sure the traffic would go
11 through that firewall and the firewall can track.

12 I mean, that's -- again, some of these are
13 implementation in house, yeah.

14 Q. So -- but for each subnet, you could have all
15 traffic for that subnet route through a single firewall;
16 correct?

17 MR. KLEIN: Object to form.

18 THE WITNESS: So like I said, depending on the
19 situation, I would say that -- you know, for example, I
20 would say that one subnet have their own switch or
21 router, for example, and then they also put a firewall
22 there. I mean, that's one -- at least one example but
23 may not be the only way to do this either.

24 BY MR. LU:

25 Q. Okay. Understood. And you would agree that a

1 subnet firewall could block traffic from another subnet
2 within the same larger enterprise network?

3 A. So again, a firewall's job is to, you know,
4 look at traffic in and out. You know, if this subnet
5 job is to protect the subnet, then this job is to
6 protect traffic in and out of this subnet. So it can be
7 a -- traffic can be from the rest of the enterprise
8 network, can be depending on the situation, can be to
9 the internet.

10 But really, the POSITA would agree that's not
11 matter. I mean, in terms of the firewall rules, you
12 write the same kind of -- essentially, you know, from a
13 technical point of view, same type of logic --

14 (Reporter clarification.)

15 THE WITNESS: From the POSITA's point of view
16 is basically whether your firewall is internet-facing
17 versus enterprise-network-facing, it's basically same
18 kind of logic and mechanism in terms of looking at the
19 traffic.

20 MR. LU: I think he said "technical point of
21 view," so could you look at the recording when you
22 finalize the transcript? Thanks.

23 THE WITNESS: Hold on. I would say from
24 POSITA's point of view is basically the same kind of
25 technologies. Let's put it that way.

1 BY MR. LU:

2 Q. Okay. Understood. All right. Let's go back
3 to your expert declaration at paragraph 37.

4 A. Okay.

5 Q. You say here that, "Firewalls also come with
6 user interfaces to allow security administrators to add,
7 delete, and modify firewall rules. Below is an example
8 of a user interface of the CheckPoint FireWall-1 system
9 in 1996."

10 Did I read that correctly?

11 A. Yes.

12 Q. And then you have this figure, which purports
13 to be from the CheckPoint FireWall-1 system; correct?

14 A. That's correct.

15 Q. This figure came from a website; correct? You
16 did not actually own or use a CheckPoint FireWall-1
17 system to get this image?

18 A. That's correct. I -- I -- if I recalled
19 correctly, I got this figure from a document that was
20 still available online.

21 Q. Have you ever used a CheckPoint FireWall-1
22 system?

23 A. No. No.

24 Q. Okay. So this figure -- you say it depicts
25 some firewall rules; right? So let me see if I can try

1 to understand what some of these rules are.

2 So do you see in this table the first row that
3 says Number 1?

4 A. Uh-huh.

5 Q. So would I be interpreting it correctly that
6 the first rule is to reject any traffic that is going to
7 the "monk" device from any source?

8 A. Yeah.

9 MR. KLEIN: Object to form.

10 THE WITNESS: Yeah. Basically "Sources: Any,"
11 meaning from anywhere; destination is "monk"; service
12 can be -- you know, so it's being requested on monk can
13 be "any," and action is "reject." And then you also --
14 in terms of track, you basically send out alert. Yeah.
15 BY MR. LU:

16 Q. Okay. Dr. Lee, could you slow down when you
17 speak just so the court reporter can --

18 A. Okay.

19 Q. -- get everything you say. Thank you.

20 And so the second rule -- am I understanding it
21 correctly when it says -- when it's providing a rule
22 that any traffic from the monk device to any destination
23 is rejected by the firewall?

24 MR. KLEIN: Object to form.

25 THE WITNESS: So as it says here -- so the

1 source is from monk, to -- destination --

2 (Reporter clarification.)

3 THE WITNESS: So the second line -- right -- so
4 basically says source is monk; destination is any,
5 meaning to anywhere; services, again, is any, meaning
6 any services monk is requesting to any destination; and
7 action is reject; and again, alert will be sent.

8 BY MR. LU:

9 Q. Now, why would a firewall want to block -- let
10 me back up.

11 So these first two rules say that the firewall
12 is going to reject any traffic going to the monk device
13 and any traffic coming from the monk device; is that
14 right?

15 A. That's correct.

16 Q. So why would a firewall want to reject all
17 traffic going to and from the monk device?

18 MR. KLEIN: Object to form.

19 THE WITNESS: Again, depending on the security
20 policy of the organization and the role that the monk
21 device places and the risk profiles and so and so forth.
22 Right? So meaning that if it doesn't want monk to
23 interact with any other devices, okay, then you do this.

24 BY MR. LU:

25 Q. Can the monk device interact with devices

1 within this network that is protected by this
2 firewall?

3 MR. KLEIN: Object to form.

4 THE WITNESS: So again, it depends on where you
5 place the firewall, to be honest, and also how the
6 network is being architect -- how the network's being
7 configured. If this is at the switch of the -- of the
8 subnet, typically it means that "any" is outside of the
9 current subnet.

10 You know, again, monk itself can be its own
11 subnet, you know, just -- just basically right now, this
12 details that are not obvious from looking at the GUI,
13 the graphical user interface. The point is that you
14 imagine monk is some entity in the network -- is a
15 single device or subnet, we don't know.

16 So that's all I can -- I can tell you. I'm
17 just reading it, telling you monk is a destination --
18 destination -- a destination, and firewall, in
19 particularly network terms, can be a single machine or
20 can be whole subnet or can be whole network.

21 BY MR. LU:

22 Q. Okay. This figure that you provided, it does
23 not actually depict the format for the firewall rules;
24 right?

25 A. What do you mean?

1 Q. Do you understand what I mean when I say format
2 for a firewall rule?

3 A. I mean, I know in general. I would say that --
4 I mean, I've looked at firewalls. I mean, I try -- you
5 know, firewall is part of the modules that -- when I
6 teach my classes. I would say that, you know, the
7 information you see on the screen, those are the key
8 information that you would find in any firewall format,
9 how you specify rules. Basically, you know, source,
10 destination -- can be the IP address, can be the port
11 numbers. Port number, of course, covers the -- the
12 services. Sometimes you also specify UDP or TCP --

13 (Reporter clarification.)

14 THE WITNESS: Sometimes you also specify the
15 services because -- or sorry, sometimes you also specify
16 the protocol as TCP versus UDP because some service can
17 be on either. And then you say action, you know, and
18 also alert, whatever. So my point is that for the
19 firewalls -- and by the way, in the late 1990s, there's
20 this thing called Firewall Building Tool Kit. Everybody
21 can download it and build it.

22 My point is -- I actually worked on firewalls
23 and teach this firewalls in my classes. All I can tell
24 you is that I know what firewall rule format is. I
25 would say that this GUI here, the graphical user

1 interface -- the information you get by looking at this
2 user interface, it contains the -- the key elements that
3 you would see in a format -- in the firewall format.

4 BY MR. LU:

5 Q. Understood. So it can contain -- it is -- this
6 figure contains the elements of a firewall format but
7 does not actually depict the firewall format itself;
8 correct?

9 A. That's not what I said. I mean, I would say
10 that -- I cannot recall exactly which firewall, but
11 typically this how we actually explain the firewall
12 format, including some of the network intrusion
13 detection or network intrusion prevention systems. It's
14 very similar: Source, destination, service -- like I
15 said, sometimes even a protocol, and then action and
16 then log. You know, I mean -- and time, whatever.

17 I mean, so -- so my point is that this is
18 from -- if you just read from left to right, all the
19 columns, I would say that a lot of, if not all -- a lot
20 of firewall rules are formatted in similar fashion.

21 Q. What do you mean by "in similar fashion"?
22 Because all I'm looking at is a picture.

23 Are you saying that the firewall rules are
24 formatted in a picture?

25 A. As I explain to you earlier, right, if you read

1 as a line, say Rule Number 1 -- okay -- that's Line
2 Number 1, in a format, you would see source, you would
3 see destination -- you would see source, comma,
4 destination, service, comma, protocol, comma, action,
5 comma, alert, comma, and log, comma, and time, comma.

6 That's -- that's what I just said. If you read
7 it from left to right, you know, you could say, hey, I
8 imagine reading firewall rules in a text, that's what
9 you see, the fields in each line.

10 Q. Okay. Understood.

11 A. That format -- so that's a format to me.

12 Q. Okay. But this picture does not actually show
13 you that format; correct? And you've -- well, answer
14 that question first.

15 A. No, I mean, I think -- I think this is a
16 format. I mean, you know -- how to display information
17 if it's no format? What are you displaying to people?
18 If there's no format, all you see is ones and zeros. Of
19 course there's a format -- inherent format. And every
20 record here is following the same format. That's a
21 format. It -- you call it graphical format, textual
22 format, but they are formats.

23 Q. Okay. So you testified earlier that you've
24 never actually used a CheckPoint FireWall-1 system;
25 correct?

1 A. That's correct.

2 Q. So you don't actually know whether a CheckPoint
3 FireWall-1 system uses, as you say, like, a "source,
4 comma, destination, comma, service, comma" format?

5 A. I just said that most firewall rules are
6 basically formatted in similar fashion by -- in a line;
7 in each firewall rule, that kind of information. And
8 most people read from left to right. So I mean, yeah, I
9 would just say that if I were the one to design user
10 interface, I would probably come up with something very
11 similar.

12 Q. Okay. But you don't actually know whether or
13 not the CheckPoint FireWall-1 system uses this format;
14 correct?

15 A. I disagree. I mean, I can go back and look at
16 my slide -- slide deck. I mean, I actually -- one of my
17 TAs -- she was one of the engineers of CheckPoint, so I
18 am very sure that, you know -- like I said, the firewall
19 format -- if you look at any rule in a textual -- or
20 whatever medium that they choose to present would
21 contain information everybody's seeing on the screen
22 from left to right. Whether they put a comma or
23 semicolon, really, I don't think POSITA would care.

24 Q. Okay. But there are different ways to have a
25 format for a firewall rule; right? As you said, you can

1 use a comma, you could use a semicolon, you could use a
2 colon, you could use line breaks, et cetera, even have
3 different fields; isn't that right?

4 A. That's right.

5 MR. KLEIN: Object to form.

6 THE WITNESS: But a POSITA only cares that a
7 firewall rules -- they have format. You know, let's
8 say, for example, in a textual -- yes, they have a
9 textual format -- what do you mean? Meaning that each
10 line or each rule, what they represent, they are
11 fields -- the fields explain the rules.

12 And on -- if you display the rules on the
13 graphical user interface, again, there's a display
14 format. That's a format. What do you mean? I mean
15 that every record is display in a -- you know, in the
16 same format. That's a firewall rule format example they
17 were looking at.

18 BY MR. LU:

19 Q. Okay.

20 A. And that's --

21 Q. In 19 -- I'm sorry, go ahead.

22 A. I'm saying that that's -- as -- a POSITA would
23 agree with me.

24 Q. Okay. So in 1996, firewalls did not all have
25 the same format; correct?

1 MR. KLEIN: Object to form.

2 THE WITNESS: So again, I don't know what "same
3 format" do you mean. Do you mean that, oh, Firewall
4 Rule A versus Firewall B, one use comma, the other one
5 use semicolon, so hence they are different format? If
6 that's what you want to go, yeah -- what -- the case.

7 But like I said, POSITA would say if they all
8 talk about similar information like source, destination,
9 services, possibly protocol, and action and track,
10 whatever -- yeah, basically same format. People --
11 POSITA would agree they're same format pretty much, same
12 information.

13 BY MR. LU:

14 Q. Okay. Could you turn --

15 MR. LU: Actually, it's been about an hour. Do
16 you want to take a short break?

17 THE WITNESS: Yeah, that's fine.

18 MR. LU: I mean, we can keep going. It's up to
19 you.

20 THE WITNESS: It's up to you too. So how long
21 short break?

22 MR. LU: I'm not sure. I mean, I have seven
23 hours. I don't anticipate going seven hours. But I'm
24 not quite sure how much longer. At this point I can't
25 really say. So it's up to you whether or not you want

1 to take a break.

2 THE WITNESS: Yeah, we can take a break.

3 MR. KLEIN: Just take five minutes?

4 THE WITNESS: Yeah. Okay. Thank you.

5 (Off the record.)

6 MR. KLEIN: All right. Before we dive back
7 into the questions, I just want to reserve Dr. Lee's
8 right to review and sign the transcript.

9 MR. LU: All right. Understood.

10 BY MR. LU:

11 Q. Okay. Dr. Lee, we were looking at your
12 declaration, Exhibit 1002, in this IPR.

13 Could you -- do you still have that in front of
14 you?

15 A. Yes.

16 Q. All right. Could you turn to paragraph 55?

17 A. 55; right? Okay.

18 Q. Yes. It starts at page 24 of your declaration.

19 A. Yes.

20 Q. And before we continue, let me just politely
21 remind you to try to speak a little slower so the court
22 reporter can grab everything you say.

23 A. Okay. Yeah. Okay. Thank you.

24 Q. Yeah. Sure. No problem.

25 So I actually -- I wanted to ask you some

1 questions about this annotated Figure 2 that you have on
2 page 26.

3 Do you see that?

4 A. Yes.

5 Q. Does the copy of your declaration that you have
6 in front of you -- is that in color?

7 A. Yes.

8 Q. Okay. Great. So let me see if I can
9 understand what you testified in your declaration. So
10 in Figure 2, you have -- so Figure 2 depicts a -- quote,
11 "Devices in Cloud Networks 122," and it has an oval;
12 right?

13 Do you see that?

14 A. Yes.

15 Q. And you annotated this figure by coloring in
16 that oval with the color blue; is that correct?

17 A. Yes.

18 Q. Okay. And it's your assertion that this blue
19 oval represents the, quote, "enterprise network," as
20 claimed in the '941 patent?

21 A. Yes.

22 Q. Okay. And so within this network are three
23 subnets: 204, 206, 208; correct?

24 A. That's correct.

25 Q. By the way, during the break, did you talk to

1 your counsel or anybody from Perkins Coie?

2 A. No.

3 Q. Did you talk to anybody?

4 A. No.

5 Q. Okay. So one of the things Wang says is that
6 these subnets can reflect different geographical office
7 locations; is that correct?

8 A. Let me just make sure that's what we said here.
9 Yes. Yes. That's what I said in paragraph 52 in my
10 declaration. Yes.

11 Q. So for example, one of these subnets could be
12 the -- could represent the network for the office in
13 Denver; one of the subnets could be the network for the
14 office in Chicago; and one of the subnets could be the
15 network for the office in New York; is that correct?

16 A. Yeah. That's one example.

17 Q. And that's actually the example given in the
18 Wang reference?

19 A. I need to check. Did it use that kind of
20 specific geolocation?

21 Q. So -- sure. Let's -- why don't we look at the
22 Wang reference.

23 So this is Exhibit 1004 from this IPR
24 proceeding, IPR 2023-00030. It's already designated
25 Exhibit 1004.

1 Do you have that exhibit in front of you?

2 A. Yes, I have the Wang.

3 Q. So if you go to paragraph 20, which is on page
4 7 of the exhibit.

5 A. Uh-huh.

6 Q. And actually, what we're going to be looking at
7 is the very top of page 8.

8 So do you see that? This is paragraph 20.

9 A. Yep, I see.

10 Q. Okay.

11 A. Yep, I see that. "Assume a customer has three
12 branch locations: One in Denver, Colorado; one in
13 Chicago, Illinois; and one in New York City, New York."
14 Yeah.

15 Q. And then it says, "In the illustrated
16 embodiment, the branches are configured into multiple
17 and separate subnets, 204, 206, and 208 with firewall
18 protections 210, 212, 214, and 216." Correct?

19 A. Yes, I see that.

20 Q. All right. So looking back at Figure 2, the
21 one you annotated, you colored in every one of these
22 subnets, like, a green color; right?

23 A. Let me see here. Yes. Yes.

24 Q. And each of these subnets have a firewall that
25 protects the subnet; is that correct?

1 A. Let's see here. Yep. That's according to the
2 Figure 2 and also the paragraph 20 of the Wang patent.
3 Yes.

4 Q. Okay. So I want to ask you some questions
5 about -- so if I refer to firewalls 210, 212, and 214 as
6 the subnet firewalls, would you understand what I'm
7 referring to?

8 A. Yes.

9 Q. Okay. Great. Just to keep things a little
10 more -- easier to follow. All right.

11 So if you turn to Exhibit 1004, the Wang
12 reference, at paragraph 16.

13 A. 16. Okay.

14 Q. Yes. Which is also page 7.

15 A. Uh-huh.

16 Q. So why don't you read that whole paragraph to
17 yourself because it's quite long, and let me know when
18 you're done.

19 A. Okay. Okay.

20 Q. So paragraph 16 describes a resource database
21 103; correct?

22 A. Yes, it talks about 103, yes.

23 Q. And it says, "The resource database 103 may
24 store or otherwise maintain configurations for specific
25 network services corresponding to a particular customer

1 currently receiving services from a telecommunication
2 service provider and for which a firewall is required."

3 Do you see that?

4 A. Yep, I see that. Yeah.

5 Q. So Wang is referring to certain services that a
6 telecommunication service provider provides to a
7 customer; is that right?

8 A. I think this basically is example, right --
9 example of what the resource database 103 and customer
10 database 105 would store.

11 Q. Okay. But my question was in this paragraph,
12 Wang refers to services that are provided to a customer
13 by a telecommunication service provider; correct?

14 A. I would say that, yes, it says so, but I would
15 say that POSITA would see that as example of the kind of
16 information that's being stored in the resource database
17 103 and customer database 105.

18 Q. So -- but -- okay. Understood.

19 So these are examples, but an example of
20 information that is stored in this database is
21 information about the services that are provided to a
22 particular customer; correct?

23 A. Yeah, that's one of the -- you know, one of the
24 kind of information that's being stored, right. But it
25 goes on to explain, you know, some other examples in

1 this paragraph.

2 Q. So this paragraph provides two examples of
3 network services.

4 Do you see that near the bottom of that column?
5 It says, "A customer 'A' is currently purchasing two
6 network services including: One, data center services
7 that enable 24/7 secure data access to proprietary
8 content and media; and, two, content delivery services
9 that provide the proprietary content to users."

10 Do you see that?

11 A. Yes. I see that.

12 Q. And so information about those services is
13 stored in resource database 103?

14 A. So again, this example -- I mean, so
15 this examples of the kind of information that can be
16 store in 103 and 105.

17 Q. Right. And so continuing on, it says, "Thus
18 the resource database 103 stores information that
19 identifies customer A, as well as information that
20 articulates the specific configurations for the data
21 center services and content delivery services, including
22 any initial firewall policy configurations required to
23 effectively and securely provide the services."

24 Did I read that right?

25 A. Yes.

1 Q. So I want to ask you about these initial
2 firewall policy configurations.

3 Would you agree that these are stored in the
4 resource database 103?

5 A. So basically if you read the top -- the very
6 end of the paragraph 1 -- 6 -- paragraph 16, right, it
7 says, "including any initial firewall policy
8 configuration required to effectively and securely
9 provide the services." So that's the context of the
10 firewall policy configuration.

11 Basically in this example, those
12 configuration -- the configuration that required to
13 effectively and securely provide services.

14 Q. Right. So Wang is describing certain services
15 that are provided; and as part of those services, there
16 are initial firewall policy configurations needed to
17 provide those services; correct?

18 A. That's what it says here. But I will say the
19 POSITA would understand that there could be some other
20 initial firewall policy configuration that just generate
21 good for security in general that, you know, you assume
22 the firewall would -- would basically -- the principle
23 in security is called Secure-by-Default.

24 (Reporter clarification.)

25 THE WITNESS: The principle in security is

1 Secure-by-Default. So the POSITA would agree -- is that
2 you have a set of, you know, initial firewall
3 configurations that is good for security by default.
4 And the thing Wang says here is that -- give example to
5 say that if you have some specific services that have
6 some special requirements in terms of how do you
7 effectively and securely provide those services, then
8 you may have some initial policy configuration for those
9 services. That's how I read it. And also --

10 BY MR. LU:

11 Q. Okay.

12 A. And I would also add that, you know, there --
13 multiple places that the firewall -- the initial
14 firewall policy configuration could be stored so that --
15 for example, you want to update -- if you want to --
16 extension, new subnet, you have a place to -- to look at
17 and retrieve. But anyway, just -- yeah.

18 Q. Okay. Understood. I wanted to focus more on
19 the initial firewall policy configurations required to
20 effectively and securely provide the services.

21 So I understand there may be other
22 configurations as well, but I wanted to focus on the
23 ones that are required to effectively and securely
24 provide the services.

25 So are you with me?

1 A. Okay. Yes.

2 Q. All right. So for these configurations, would
3 you agree that they are firewall configurations for the
4 subnet firewalls 210, 212, and 214?

5 A. Let me see here. So first of all, I mean, 16
6 does not say that this is specifically for the firewalls
7 associated with any of the subnets. So I would say
8 POSITA would say it really depends on situation; right?
9 If your whole enterprise is the customer, then you
10 imagine this policy configuration will be in the --
11 whatever the -- the firewall for the whole enterprise,
12 which is, you know, not the specific subnet.

13 Q. So is it your testimony that it -- these
14 initial firewall policy configurations are not for the
15 subnet firewalls 210, 212, and 214?

16 A. That's not what I said. What I said is that in
17 paragraph 16, it did not say these are firewall
18 configurations specifically only for the subnet. It
19 could be for the subnet but also could be for the whole
20 enterprise. Really depending on the context of what a
21 customer is. Is a customer -- well, whatever the
22 services the customer are requesting or providing,
23 specific to that subnet, versus actually, you know, for
24 the whole organization.

25 So again, depends on situation. You may want

1 to put this policy at different places. Doesn't have to
2 be on a subnet. It didn't say so in paragraph 16.

3 Q. Okay. So it could be for the subnet firewalls,
4 right, these configurations?

5 A. So, again, depending on what customer is. Is a
6 customer that -- you know, referring to the subnet? You
7 know -- or if it is to the whole organization. So
8 really depends on -- and also depending on those
9 services that you're providing, is it involving
10 multiple, you know, subnets or a single subnet. Again,
11 those things are not discussed in paragraph 16, so I
12 don't need to read into that.

13 Q. So these initial firewall policy
14 configurations, would you agree that they are pushed to
15 the firewalls -- the necessary firewalls in order to
16 provide the services?

17 MR. KLEIN: Object to form.

18 THE WITNESS: So again, the -- I don't believe
19 the Wang patent talks about pushing the configuration --
20 policy configuration to a firewall, per se. I mean, I
21 don't recall that, but if you can point me to it, I'll
22 be happy to discuss that. Yeah.

23 BY MR. LU:

24 Q. Well, okay. So let's look at paragraph 56 of
25 your declaration.

1 A. Okay.

2 Q. 1002 -- Exhibit 1002.

3 A. Okay.

4 Q. Which is actually just the next paragraph.

5 Are you there?

6 A. Paragraph 56?

7 Q. Yes.

8 A. Yes. I'm here.

9 Q. Okay. So you say, "In this arrangement,
10 dynamic firewall controller 102 processed any input
11 defining firewall policies passed from the portal and
12 automatically configured various aspects of a firewall."
13 And you're quoting Wang paragraph 18.

14 Do you see that?

15 A. Yes.

16 Q. Okay. So you testified that the firewall
17 controller 102 automatically configures various aspects
18 of a firewall; correct?

19 A. That's what I said at paragraph 56, yes.

20 Q. And what did you mean by "automatically"?

21 MR. KLEIN: Object to form.

22 THE WITNESS: So let me read paragraph 18. So
23 paragraph 18 of the Wang patent actually specifies
24 how -- how -- you know, basically try to explain the --
25 what I quoted in my declaration. So if you allow me, I

1 can just read the relevant information here.

2 So basically say, "Referring generally again to
3 Figure 1, the dynamic firewall controller 102 may
4 process any input defining firewall policies passed from
5 the portal to dynamic firewall controller 102 and
6 automatically configure various aspects of a firewall.

7 "The dynamic firewall controller 102 may also
8 take threat inputs in threat intelligence systems, for
9 example, the 'reputation' system at Level 3, dynamically
10 generate proper firewall policies and automatically
11 configure the firewall policies for customers who
12 subscribe to threat protection service.

13 "More specifically, the dynamic firewall
14 controller 102 may automatically make one or more
15 application programming interface, API, calls to a
16 network configuration system engine, NCS 112, and/or a
17 firewall configuration system engine, FCS 114. The NCS
18 112 includes logic for configuring various aspects of
19 the routers and switches of a subnet, or otherwise, that
20 may require configuration in accordance with the
21 firewall policy.

22 "For example, if the firewall policy involves a
23 subnet, the firewall policy may include configurations
24 for router that defines an address, network ID, subnet
25 ID, subnet mask, and the like, any of which may be

1 needed to manage network traffic to and from the subnet.
2 In other embodiments, the NCS 112 may configure firewall
3 devices directly."

4 Yeah. So that's the -- that's the extent that
5 Wang actually explains automatically configure various
6 aspects of firewall in paragraph 18.

7 Q. What does "automatic" mean to you?

8 MR. KLEIN: Object to form.

9 THE WITNESS: "Automatic"? As explains here,
10 right, in Wang paragraph 18 -- for example, say, "may
11 automatically make one or more API calls"; you know,
12 that's one example of automatically.

13 BY MR. LU:

14 Q. Okay. But what does "automatically" mean in
15 that context to you?

16 A. Means calling the APIs would just be, you
17 know -- in this case, would be 102, which is the dynamic
18 firewall controller runs a process that calls the API --
19 APIs automatically. That's what I -- you know, a plain,
20 ordinary meaning, I would say, for a POSITA.

21 Q. So would it mean it calls the API in response
22 to something else?

23 A. So let me see here. So I think -- as paragraph
24 18 further explains; right? So, you know, the reason
25 you -- automatically calls the APIs to a NCS and/or a

1 FCS is the following: "The NCS includes logic for
2 configuring various aspects of the routers and switches
3 in the subnet," and so on, "that may require
4 configuration in" according -- "in accordance with the
5 firewall policy," and so on.

6 So what this says is that you call those APIs
7 to NCS, and the NCS would then perform the
8 configurations.

9 Q. So would "automatically" mean that if, for
10 example, a customer subscribes to a particular service
11 that requires certain policies, those policies are
12 automatically configured for the firewalls?

13 MR. KLEIN: Object to form.

14 THE WITNESS: So again, if you refer to
15 paragraph 18, the beginning, right, basically, it says
16 that, "The dynamic firewall controller 102 may process
17 input defining firewall policies passed from the portal
18 to the dynamic firewall controller 102." Right? And
19 then "automatically configure various aspects of a
20 firewall."

21 So what 18 says is that the dynamic firewall
22 controller may take input from the -- input defining
23 firewall policies from the portal.

24 Q. And then automatically configure various
25 aspects of the firewall; correct?

1 A. That's correct.

2 Q. And these firewalls could include the subnet
3 firewalls?

4 A. So again, paragraph 18 didn't say explicitly
5 which firewall. I would assume that any firewall.

6 Q. Well, it does give an example at the end. It
7 says, "For example, if the firewall policies involves a
8 subnet" --

9 A. Let me see. Yeah, gives one example, yes.

10 Q. So you would agree that dynamic firewall
11 controller will automatically configure subnet
12 firewalls?

13 A. So again, if you read the context of paragraph
14 18 -- first of all, the dynamic firewall controller 102
15 may process any input defining firewall policy passed
16 from the portal, right, to it. And then, for example,
17 for subnet, then it may configure certain aspects of the
18 firewalls for the subnet. Again, subnet is example
19 here.

20 Q. Correct. And these firewall policies are
21 stored in the resource database 103?

22 A. Repeat the question again.

23 MR. KLEIN: Object to form.

24 BY MR. LU:

25 Q. And these firewall policies are stored in the

1 resource database 103; correct?

2 MR. KLEIN: Object to form.

3 THE WITNESS: It didn't say so here. I know
4 that the firewall policies are stored in a database. Is
5 it only in the resource database 103? It's not clear
6 from paragraph 18. If anywhere else on the -- in the
7 patent that is -- discussed that, let me know.

8 BY MR. LU:

9 Q. Well, we just read in paragraph 16, "Firewall
10 configurations and policies accessible and definable
11 through the portal may be driven by a resource database
12 103"; correct?

13 A. Are you reading the -- let me see.

14 Q. I just read the first sentence of paragraph 16.

15 A. Okay. Let me read this again. Okay. Yeah.
16 So I think if -- the way I read this first sentence in
17 paragraph 16 of the Wang patent -- right. It says, "In
18 some embodiments, firewall configurations and policies
19 accessible and definable through the portal may be
20 driven by a resource database 103 and/or customer
21 database 105."

22 Yeah, but it -- so it didn't say that -- I
23 mean, the paragraph 16 did not talk about -- so what I'm
24 trying to say is that -- that makes sense. I mean, you
25 know, can be -- that's the -- one of the functions of

1 the resource database and customer database. Then
2 when -- and the paragraph 18 talks about, you know, then
3 if the -- if the firewall controller -- dynamic firewall
4 controller gets the input from the portal, it
5 generate -- automatically configure various aspects of
6 the firewall.

7 But paragraph 18 itself did not talk about
8 pushing the firewall policy back to 103. I'm not
9 reading it from paragraph 18.

10 Q. Okay. I mean, that wasn't my question. But I
11 believe you did answer it. So --

12 A. Okay. So again -- hold on. So I said that I
13 know the new updated firewall policies would -- is
14 stored in some database. I can probably look at my
15 declaration to see -- normally we say -- it is stored,
16 if that's the question you want to ask. Let me see
17 here. I think it says somewhere here.

18 Let me look at the '941 claims so I know where
19 to look for. Okay. Let me see. Yeah. So in paragraph
20 74 of my declaration, I did say that -- so basically 74,
21 I said -- paragraph 74 in my declaration, I said that,
22 "Additionally, these generated policies were stored in
23 resource database 103." Okay. So I probably have
24 misspoke. "Database records having fields that
25 reference specific firewall configurations." Yeah.

1 So --

2 Q. Okay. And so you --

3 A. So I'm saying that the generated database --
4 generated policies was stored in resource database 103.

5 Q. Okay. And you still agree with that statement
6 from your declaration?

7 A. Yes.

8 Q. Okay. Can we go back to the Wang reference,
9 Exhibit 1004 --

10 A. Okay.

11 Q. -- at paragraph 21.

12 A. Okay.

13 Q. So it says, "At some point, the customer may
14 want to implement a firewall policy, e.g., network layer
15 policies, that describes network traffic behaviors
16 between the subnets 204, 206, and 208, based upon
17 business needs of the customer." And then it gives an
18 example.

19 And I wanted to read later in the paragraph,
20 there's, "As another example, the resources with each
21 subnet 204, 206, and 208 may be equipped to detect
22 threats and other malicious activity for network traffic
23 coming from a particular domain, external to the
24 subnets, such as a malicious domain 218."

25 Did I read that right?

1 A. Yeah. I see that sentence, yes.

2 Q. So is it your opinion that this example where
3 each subnet 204, 206, 208 can detect threats and other
4 malicious activity coming from a malicious domain -- is
5 this describing the subnet firewalls 210, 212, and 214?

6 A. Let me -- let me look at this more carefully.
7 Okay? So -- so, I mean, if you read the beginning of
8 the first sentence of the paragraph 21, right, basically
9 says, "At some point, the customer may want to implement
10 a firewall policy, e.g., network layer policies that
11 describes network traffic behaviors between the subnets
12 204, 206 and 208, based upon" -- this is -- "based upon
13 business needs of the customer."

14 And then the next sentence give example of, you
15 know, engineering department versus human resources and
16 so on. And then as an example -- as another example
17 that you just cited -- talks about malicious domain.
18 So -- external to the subnets.

19 But, again, this is in the context of subnet to
20 subnet within a network. So --

21 Q. Okay. But this paragraph does not -- or -- are
22 you finished?

23 A. Sorry. Sorry. I mean, just saying that that's
24 what I read. Yeah.

25 Q. Okay. So this paragraph does not actually

1 refer to the subnet firewalls 210, 212, and 214;
2 correct?

3 A. It did not mention the subnet firewall
4 specifically. It talks about the subnets may be
5 equipped to detect threats and malicious activities.

6 Q. Okay. But it doesn't say that it's the subnet
7 firewalls that are detecting those threats or other
8 malicious activities; correct?

9 A. Yeah, it did talk about updating the firewall
10 policies and so on, but they didn't say that -- where
11 the firewall has to be. It didn't explicitly say where
12 the firewall is, but it did say that the subnets are
13 equipped to detect. So obviously the subnet in this
14 context would need to use the help of the firewall.

15 Q. The help of which firewall?

16 A. A subnet -- sorry. Go ahead.

17 Q. Go ahead. Go ahead.

18 A. I mean, like I said, depending on the
19 configuration and the nature of the threats, I mean,
20 some of them, you can -- you know, some of them is
21 sufficient or convenient -- or sufficient -- sufficient
22 to block the threat at the subnet firewall. I mean,
23 like I said, it really depends on the nature of the
24 threat you're talking about.

25 And some of them, you may want to have it in a

1 more, sort of, global firewall for the whole -- whole
2 corporate. It really depends on the network setup and
3 also the nature of the threat. So that's why I think in
4 paragraph 21, it did not explicitly limit where the
5 firewall has to be.

6 Q. Okay. But it's your opinion that a subnet
7 firewall can block traffic from a malicious domain into
8 that subnet?

9 A. Yes. In principle, yes.

10 Q. Okay. So why don't we look at, like, specific
11 examples. So going back to your declaration at
12 paragraph -- well, we were at paragraph 55, page 26,
13 your annotated Figure 2.

14 Are you there?

15 A. Okay. 56, yes -- paragraph 56. Yep.

16 Q. Paragraph 55, page 26.

17 A. Page -- oh, 26. I only have paragraph 56.

18 Q. Yeah, paragraph 55, like, runs into
19 paragraph --

20 A. The figure, sure, yeah.

21 Q. The figure. Yeah. Exactly.

22 A. Okay.

23 Q. So here you see a malicious domain 218;
24 correct?

25 A. Yes.

1 Q. And it's your opinion that this malicious
2 domain is outside of the enterprise network?

3 A. So this figure shows that they're outside of
4 the subnet for sure.

5 Q. Outside of the subnets.

6 Are they outside of the enterprise network?

7 A. It does not say.

8 Q. It does not say. Okay. But it's your opinion
9 that, for example, firewall 210 can block traffic from
10 the malicious domain 218 into subnet 204; correct?

11 A. Yes. Basically, the firewall 210 for subnet
12 204 can block malicious traffic into 204.

13 Q. And that includes malicious traffic from the
14 malicious domain 218?

15 A. Yes.

16 Q. Can subnet firewall 210 block traffic from
17 malicious -- let me withdraw that.

18 So subnet firewall 210 cannot block traffic
19 from malicious domain 218 to subnet 206; correct?

20 A. Yeah. So I mean, provided that the traffic --
21 malicious traffic from 218 does not go through subnet
22 204. Meaning that the traffic just, you know, go to 206
23 and nothing to do with the firewall -- nothing to do
24 with the subnet 204. That indicates firewall 210 had
25 nothing to do with that traffic because it doesn't route

1 through it.

2 Q. Okay. And suppose there were a device
3 within -- withdraw.

4 So as you -- you colored in this oval blue
5 that's labeled Devices in Cloud Networks 122. Correct?

6 A. Yes.

7 Q. And there could be devices in this cloud
8 network 122 that are not inside any of these subnets;
9 correct?

10 MR. KLEIN: Object to form.

11 THE WITNESS: So it's not in any of these -- so
12 example of the malicious domain 218 or there could be
13 other devices that are not in subnet 204, 208, 206.
14 There could be another subnet that's not being depicted
15 in Figure 2; right? So we just -- you know, for the
16 purpose of this figure, it did not show, for example,
17 218 to be in subnet 210 -- I'm sorry, in subnet 204,
18 206, or 208 but did not say whether it's outside of
19 the -- outside this network or could be in any of other
20 subnet that's not depicted. That information is just
21 not there. So I cannot draw any conclusion.

22 BY MR. LU:

23 Q. But would a POSITA looking at this figure agree
24 that there -- you could have devices within a larger
25 network that are not part of a subnetwork; right?

1 MR. KLEIN: Object to form.

2 THE WITNESS: Really depending on, you know,
3 how you define -- define network switching configuration
4 and communology [phonetic] -- how do you say what is a
5 subnet and what is not a subnet. So let's say we have
6 subnet A and the rest, well, then the rest --

7 (Reporter clarification.)

8 THE WITNESS: So I would say that suppose if
9 subnet A -- okay. You have one -- you know, say I only
10 have one subnet A in my network. In that case I would
11 say, well, maybe the rest, you could also call it a
12 subnet with itself because it's separated from subnet
13 A.

14 BY MR. LU:

15 Q. Okay. So you're saying, like, an individual
16 device could just be its own subnet? Is that what
17 you're saying?

18 A. Again, depending on how you want to switch your
19 network, traffic, and how you want to manage your
20 security policy. For example, my laptop is a subnet by
21 itself. That's why I put a VPN there. It's as good as
22 a subnet in terms of protection.

23 THE REPORTER: Counsel, could we take a break
24 when you get to a good spot?

25 MR. LU: Oh, yeah. We can take a break now.

1 That's fine.

2 (Off the record.)

3 MR. LU: Okay.

4 BY MR. LU:

5 Q. Dr. Lee, could you turn to the Wang reference
6 again, Exhibit 1004.

7 A. Okay.

8 Q. And I want to ask you some questions about
9 paragraph 26.

10 A. Okay.

11 Q. So why don't you read through that whole
12 paragraph on your own and then let me know when you're
13 finished.

14 A. Okay. Okay.

15 Q. Okay. So paragraph 26 describes a process for
16 validating proposed firewall policy changes; correct?

17 A. That's the first sentence says here, so --
18 right -- "In some embodiment, before implementing the
19 firewall policy changes, the configuration included in
20 the policy may be validated and/or otherwise verified
21 against erroneous and/or illogical automatic
22 configuration changes based on the type changes being
23 made to a particular subnet and/or devices within the
24 subnet."

25 Yeah. So it's about verifying or validating

1 the firewall policy changes.

2 Q. All right. So this is describing the way to
3 validate policy changes before they are actually
4 implemented into a firewall; correct?

5 A. That's correct.

6 Q. Wang describes this validation process as
7 optional; right?

8 A. Let me see. Are you reading some embodiment is
9 optional? Or where do you see "optional," the word?

10 Q. It says, "The configurations included in the
11 policy may be validated or otherwise verified"; correct?

12 A. So I'm not -- I'm not saying that means
13 optional versus, you know -- in computer science terms,
14 you know, you say, oh, when I say validated, I couldn't
15 tell 100 percent. It depends on how you read the
16 context. A POSITA would say, you know, maybe -- the way
17 I read it, a POSITA would be, yeah, that's one way to
18 validate. Are you guarantee 100 percent everything is
19 validated, POSITA say? Most computer scientists would
20 not answer that question or would not be able to answer
21 that question. It really depends on the complexity of
22 the policy, to be honest. So I'll stop there.

23 Q. So you said it depends on the complexity of the
24 policy.

25 Do you mean it depends on the complexity of the

1 process for validating?

2 A. So maybe I don't -- I don't see as a -- a
3 option -- or optionally you can validate, whatever. I
4 would say that it's a way to say, yeah, you can, you
5 know, validate, but, you know, just -- how to put it --
6 doesn't mean the process of validating -- it didn't say
7 that you -- it's optional. That's -- that's not how I
8 read it. May be validated, you know, against these kind
9 of illogical configuration changes based on type
10 changes, you know, and so on.

11 So I -- you know, another way to read this can
12 be -- can be -- say, hey, you know, I -- that's one way
13 of doing this. That's how I read it.

14 Q. Okay. But you would agree that at least some
15 policy changes are not validated; correct? That's what
16 the word "may be validated" indicates?

17 MR. KLEIN: Object to form.

18 THE WITNESS: That's not how I read it. It
19 says may be validated against some of these error
20 conditions. It didn't mean that -- sorry, I mean, can
21 you repeat your question again?

22 BY MR. LU:

23 Q. Are you testifying that every policy change is
24 validated?

25 A. So what I am testifying is that by reading

1 paragraph 26, Wang suggests that there's a validation
2 process -- and then using, you know, some examples to
3 say essentially when -- "may be," like, you know, to
4 me -- I'm reading it as you can -- as example, validate
5 some of these -- or check against certain error
6 conditions.

7 I don't think I read it as, oh, the process of
8 validating is optional or otherwise. Because it doesn't
9 say it that way.

10 Q. So you're saying the process of validating is
11 not optional; correct?

12 A. Again, I read what is said. It doesn't say
13 mandatory or optional. It just say -- it suggesting --
14 basically teaching his way to validate.

15 Q. Okay. But it doesn't say it's mandatory;
16 correct?

17 MR. KLEIN: Object to form.

18 THE WITNESS: Again, like I said, it didn't say
19 the word "mandatory" or "optional." It says in some
20 embodiments before implementing changes, you can try
21 what they're teaching to the validation. Is it the only
22 way to validate? A POSITA would say, yeah, maybe --
23 maybe there are other ways to validate.

24 I think that's how I -- how I interpret it.
25 "May be" is meaning that the -- the process is probably

1 more like the detail configurations of the process such
2 as virtual machines and so on. So somebody may have
3 some -- ah, validating is a good idea; I can use
4 something else. That's how I read it.

5 BY MR. LU:

6 Q. Okay. So -- oh, go ahead.

7 A. That's how I interpret "may be."

8 Q. All right. So it does say, "For example, the
9 NCS 112 may perform so-called 'dry runs' to check and
10 validate proposed firewall policy changes."

11 Do you see that?

12 A. Yes.

13 Q. And by "dry run," Wang means to check and
14 validate proposed firewall policy changes against a
15 known -- "a set of known rules without making actual
16 changes on network elements"; correct?

17 A. That's what it says here, yes.

18 Q. Right. So Wang is describing a process of
19 validating proposed changes without actually making
20 those changes on network elements; correct?

21 A. So again, a POSITA would read this to say,
22 okay, I mean, I think the network elements here would
23 refer to the actual network element and the actual
24 subnet or devices. It doesn't mean -- I mean, if I were
25 a POSITA reading this, I wouldn't say that automatically

1 means that it cannot be on any network element.

2 I mean, a lot of people identify their own test
3 bed -- test network. They have actual network elements
4 but not the actual ones that you're using on daily
5 operation. But it could be actual network elements used
6 for testing validation. So again, you know, essentially
7 teaching a principle of what dry run is referring to.
8 It doesn't say explicitly what network elements has to
9 be, has not to be.

10 Q. Okay. So you gave an example where a dry run
11 can involve, like, a test bed network but not the actual
12 network itself; correct?

13 A. Yes. That's actually very commonly done.

14 Q. Have you ever done that before?

15 A. Yeah, all the time.

16 Q. What do you mean by "all the time"?

17 A. As we speak, my research projects involve
18 actual test beds, actual network elements.

19 Q. So Wang also describes using virtual network
20 elements; correct?

21 A. Yes. He talks about them, yes.

22 Q. Actually -- so I skipped a sentence, but at the
23 bottom -- so in paragraph 26 of Wang at the very bottom
24 of page 8, there's a sentence that says, "Instead, data
25 corresponding to the execution of the firewall policy

1 change instructions is captured and analyzed to validate
2 that the proposed firewall policy changes would be
3 implemented as expected at the network elements and/or
4 devices of the subnet."

5 Did I read that correctly?

6 Was that -- did you answer?

7 A. No, no. I'm trying to read the sentences
8 before that to make sure I'm in the proper context.

9 Q. Oh, sure. Go ahead. Let me know when you're
10 done.

11 A. Okay. Okay. Yeah. I finished reading that
12 sentence. Yes.

13 Q. Okay. So it says, "Data corresponding to the
14 execution of the firewall policy changes instructions is
15 captured and analyzed."

16 What does -- to you, what does Wang mean by
17 "data corresponding to the execution of the firewall
18 policy change instructions"?

19 MR. KLEIN: Object to form.

20 THE WITNESS: I think it's what it says; right?
21 "Data corresponding to the execution of the firewall
22 policy changes instructions." So, you know, when you
23 execute something, there lot of information you can
24 capture. That's what it means. It capture any
25 information that you need for validation.

1 BY MR. LU:

2 Q. Okay. Well, could that information -- what are
3 some examples of information that you would need for
4 validation?

5 A. You know, can mean many things, can be -- you
6 know, you can see, you know -- let's say when you test
7 certain traffic, you know, you expect it to go through
8 what's being blocked; does it happen that way; was any,
9 you know, local -- impact the local -- the system that
10 runs the firewall; and so and so forth. These are just
11 examples. There are many things that you can actually
12 use to -- to capture and analyze. Yeah.

13 Q. So you gave an example where you said you can
14 test certain traffic, you know, expect it to go through
15 what's being blocked -- so I don't know if I -- that's
16 what it says on the transcript. It might be
17 mistranscribed.

18 But the question I have is one of the things
19 you could do is test, in a test bed or in a virtual
20 environment, traffic and see how the policy changes
21 respond to said traffic; is that correct?

22 A. So in principle, testing is kind of -- system
23 is basically given input. Do you see the expected
24 output? So in this case, the input is network
25 conditions. Can be normal traffic, can be simulated

1 attack traffic, whatever, and then you expect the output
2 would be based on the firewall rules, what should be
3 allowed, what should not -- what should not be allowed.

4 Then you check, you know, the logs and the --
5 and the system data, whatever, to see did the firewall
6 actually apply those rules and block or allow the
7 traffic and what shape and form and performance and all
8 that kind of things. Yeah. So it's very wide range of
9 things you can capture and analyze.

10 Q. What would be the purpose of validating in that
11 way?

12 A. So as I said previously, make sure that the
13 firewall works as intended with the new policy changes.

14 Q. So you would agree that if the firewall did not
15 work as intended, that could be a security issue;
16 correct?

17 A. May or may not be, really. I mean, if you
18 block everything, that's not security issue. You're
19 secure. It's not as available. So really depends where
20 you're looking. Yeah.

21 Q. All right. But it could, in some
22 circumstances, be -- cause security issues if a firewall
23 policy is not operating as you intended; correct?

24 A. Well, I would say -- instead of saying "as I
25 intended," I think you should say "as intended by the

1 policy"; right? Meaning that if you put in the
2 policy -- firewall policy changes, you expect how the
3 policy changes would affect, you know, the network
4 traffic, and you validate whether that is actually the
5 case. And if not, then of course there's a concern;
6 right? Can be -- can be security concern, can be
7 performance concern, can be other concerns.

8 Q. Right. And so your validate -- your validation
9 process should include all of those concerns that you
10 may have; correct?

11 MR. KLEIN: Object to form.

12 THE WITNESS: No. I mean, I think in this --
13 okay. So I think we -- if you're asking me in general
14 how I want to validate a particular system or firewall,
15 of course there are many things you could validate. But
16 in the context of 26, it talks about validating the
17 policy, you know -- basically validate the policy or
18 verified against, you know, possible errors, including
19 illogical automatic configuration changes.

20 So basically, essentially, making sure that the
21 firewall policy -- or firewall rules work as the policy
22 intend -- intends -- intends them to be. So I mean,
23 I --

24 BY MR. LU:

25 Q. What was -- what was that thing that you said?

1 "Intends them to be"?

2 A. Yeah, meaning I have a policy -- I implement
3 policy through the rules. I want to make sure that the
4 rules actually work so that the security policies -- is
5 enforced. So yeah, that's the context of 26.

6 Q. Okay. So -- and then paragraph 26 talks about
7 an embodiment where -- I'm -- and I'm going to start
8 quoting from it. "The NCS 112 may execute the proposed
9 firewall policy changes against replicated virtual
10 devices to simulate the changes in a virtual
11 environment"; right?

12 A. Uh-huh.

13 Q. I'm sorry. I missed the answer.

14 A. Yeah. I see it -- yeah, I see the sentence.
15 Yes.

16 Q. Okay. And then Wang further says, "More
17 specifically, a virtual environment that includes the
18 same network elements of the subnet, all of which
19 emulate the function of the devices in the subnet, may
20 be provisioned."

21 Did I read that right?

22 A. Yes.

23 Q. So Wang is describing a validation process that
24 involves emulating not just the subnet firewall, but all
25 of the elements in the subnet as well; correct?

1 A. It says that the -- "a virtual environment that
2 includes the same network elements of the subnet, all of
3 which emulate the function of the devices in a
4 subnet" -- that's what it says.

5 Q. Okay. So you agree that Wang is describing a
6 validation process that involves emulating the subnet
7 firewall and all of the subnet -- all of the elements in
8 the subnet as well; correct?

9 A. That's not what it says. It didn't say
10 emulating environment -- that the network elements.
11 Basically the virtual environment includes the same
12 elements of the subnet, all of which emulate the
13 function -- so basically emulate the function of the
14 devices. I think that would be the --

15 Q. Okay. So Wang is describing replicating -- or
16 withdrawn.

17 So Wang is describing a virtual environment
18 where you have virtual network devices that emulate the
19 actual devices in the subnet; correct?

20 A. It didn't use the word "virtual devices" to say
21 the virtual environment includes the network elements of
22 the subnet, all of which emulate a function of the
23 devices.

24 Q. Okay. But when it says "the same network
25 elements," do you read that as physical network elements

1 within a virtual environment?

2 A. You mean within a virtual environment, your
3 physical environment? That's not how I read it.

4 Q. Yeah.

5 A. That's not how I read it. But either way.

6 Q. So let me see if I can clarify.

7 I'm asking in a virtual environment, would it
8 have physical network elements of the subnet?

9 A. Can you repeat the question again?

10 Q. So when Wang says "a virtual environment that
11 includes the same network elements of the subnet," is it
12 referring to a virtual environment with physical network
13 elements?

14 A. So again, those are implementation details that
15 are not specified in paragraph 26. Basically say the
16 virtual environment include the same network elements of
17 the subnet. Are they the same actual elements of the
18 subnet versus, you know, you have a -- you know,
19 virtual -- within your virtual environment, a
20 separate -- how to put it -- separate instance of the
21 element to emulate -- emulate the function of the
22 devices?

23 I mean, I'd be inclined to say probably more
24 the latter, but whether those network elements in the
25 virtual environment are virtual itself versus actual,

1 physical, again, that's really implementation detail.
2 Either way would work.

3 Q. Okay. So it could be virtual; it could be
4 physical network elements within this virtual
5 environment. That's what you're saying?

6 A. Yes. That's how I define virtual network.
7 Doesn't have to be everything has to be virtual.

8 Q. I see. Okay. Okay. And then Wang goes on to
9 say, "Subsequently, the proposed firewall policy changes
10 may be executed by the NCS 112 and within the virtual
11 environment to determine how the proposed changes would
12 affect the network elements and/or devices and overall
13 subnet."

14 Did I read that right?

15 A. Yes.

16 Q. Wang does not actually describe how it would
17 determine those proposed changes would affect the
18 network elements and/or devices and overall subnet;
19 correct?

20 A. Let me read the sentence again. I mean, so
21 basically says that, you know, "Subsequently, the
22 proposed firewall policy changes may be executed by the
23 NCS 112 and within the virtual environment to determine
24 how the proposed changes would affect the network
25 elements and/or devices and overall subnet."

1 So to me, there are two things. One is what
2 NCS would do in paragraph 18 by actually making changes
3 to some of these network elements. And then, yeah, they
4 basically say, okay, let's -- let -- let those changes
5 to be executed in this virtual environment, and then you
6 see what's the effect on the network elements. That's
7 what it says.

8 Q. Okay. But it doesn't actually explain how to,
9 quote, "see what's the effect of the network elements,"
10 as you just testified; correct?

11 A. I mean -- I mean, let me see -- let me see the
12 meaning of the -- so I think we covered this in the --
13 couple minutes ago. Talked about -- so again, we
14 talked -- in the context of paragraph 26, which use, you
15 know, validation and verifying firewall changes --
16 right? So here we talk about, you know, using the NCS
17 to execute the changes to the network elements, then
18 determine whether the changes are -- how the changes
19 would affect the network elements.

20 Again, you just want to see whether the changes
21 is such that it enforces the -- the intended security
22 tracks without affecting, you know, the
23 otherwise-legitimate activities and performance. I
24 mean, that's, like, well understood by any POSITA.

25 Q. So previously you testified about, you know,

1 testing the policy change against some network traffic
2 and seeing if it responded as intended.

3 But that's not actually described here in Wang;
4 correct?

5 A. This is one example, like I said. I think I
6 said earlier that there's one example that POSITA would
7 understand what you mean by, you know, validating and
8 verifying the firewall changes. That's one example of
9 the things that you would check as a POSITA. Meaning
10 that -- does it work as intended? Okay. How? Like I
11 said, it's about looking at the input versus the output.

12 Q. Okay. But there are other examples of things
13 you would check as a POSITA?

14 A. Probably.

15 Q. Wang does not actually describe any of those
16 examples; correct?

17 A. Not in this paragraph. Maybe somewhere else,
18 if you can point me to, because I cannot recall all
19 details of Wang. But like I said, a POSITA would find
20 it so obvious what to check at a minimum.

21 Q. So you previously said you, yourself, have
22 tested firewall policies in a test bed environment;
23 correct?

24 A. I previously said that we build test -- we use
25 test bed all the time.

1 Q. Okay. What sort of tests do you run in that
2 test bed?

3 A. I actually run malware in the test bed. I have
4 the proxy also -- I have a network proxy that also
5 functions as a firewall. Yeah. So that's one example
6 in my test bed.

7 Q. So you run malware in the test bed.

8 What does that mean?

9 A. I let the malware runs and observe what it does
10 and let it go, you know, it wants connect. My proxy
11 would decide, should we let it connect to the internet
12 or not, for example.

13 Q. Are there other tests that you run on your test
14 bed?

15 A. I have other kinds of test bed, you know.

16 Q. You have other what?

17 A. I have another kinds of test beds as well.

18 Q. Okay. So you have a test bed for running
19 malware. Is that what you're saying?

20 A. That's one example, yes.

21 Q. And what other kinds of test beds do you have?

22 A. I have one test bed that runs, you know,
23 biometric-based authentication, such as face-based
24 detection.

25 (Reporter clarification.)

1 BY MR. LU:

2 Q. "Biometric" is what you're saying; right?

3 A. Biometric. Yes.

4 Q. Any other kinds of test beds that you have?

5 A. Those are examples. Yeah.

6 Q. Those -- are those the only examples of test
7 beds that you have?

8 A. Well, I mean, let me see. If you want to go --
9 yeah, I have other test bed to basically -- let's say
10 for power networks. I mean, I do many different things.
11 So all these test beds, they're both virtual and
12 physical elements, if that's what you are interested in.
13 Yeah.

14 Q. Okay. Now, Wang does not actually describe
15 anything like a malware test bed or a biometric test bed
16 or a test bed for power networks; correct?

17 A. Yeah, it does not teach -- so Wang's patent
18 does not teach any of those specific examples, but my
19 point is that a firewall validation and verification is
20 well understood, you know, what you -- what's your goal
21 and how you want to achieve it. Yeah. That's what I'm
22 going to say.

23 Q. Okay. And your testimony is that firewall
24 validation and verification is well understood, and that
25 would include these examples of test beds that you use?

1 A. Those are examples, yes. Those are examples of
2 ways that you can do a dry run. I mean, I think dry run
3 is a perfect word for this kind of thing. Yep.

4 Q. But it's not necessarily the case that you
5 would always want to run these specific tests that
6 you're doing; correct?

7 A. I mean, that's a -- how to put it -- I don't
8 know why that question is in the scope in a sense that,
9 yeah, I mean, sometimes you may choose not to even have
10 a firewall. That's your choice.

11 Q. Okay.

12 A. I mean, I don't know what -- what else I can
13 say.

14 Q. I don't think you answered my question.

15 My question is: When you're validating a
16 firewall policy, it's not necessarily the case that you
17 would run a malware check or a biometric check or a
18 check for a power network; correct?

19 A. I would say those things are not -- how to put
20 it -- depends on the situation. You may want to
21 simulate a different kind of traffic; right? So all the
22 above that I mentioned could be useful in some
23 situations.

24 So again, really depends on -- I think the key
25 word here -- I mean, the key here is to look at the -- I

1 think that the key to understand this paragraph is to
2 understand that -- for example, say a virtual
3 environment that includes the same network elements of
4 the subnet, all of which emulate a function of the
5 devices in a subnet -- so basically, it really depends
6 on what a subnet is doing and what kind of traffic
7 normally it would expect.

8 So then you would -- based on that, you would
9 determine what kind of input data you want to use in
10 your dry run. Again, it's very specific to the
11 situation, and that's why I'm -- that's why I would say
12 that all the example test beds that I gave, that could
13 be relevant example depending on what your subnet is
14 supposed to be doing.

15 Q. So you said it's very specific to the
16 situation.

17 Is it specific to the proposed policy changes
18 as well?

19 A. Definitely. I mean, again, there's --
20 paragraph 26 is talking about -- is try to validate the
21 policy changes. Of course, you want to test the policy
22 changes.

23 Q. So the sort of validation you would perform
24 depends on the sort of policy changes you're proposing;
25 correct?

1 A. Yes. But I would say that, you know, the
2 input -- right -- for example, you don't want to say,
3 hey, I want to test my -- my firewall; I only -- you
4 know, emulate malicious traffic. Nobody would do
5 this.

6 Q. You only -- oh, malicious traffic. Okay.

7 A. Yeah. POSITA would say also you emulate the
8 normal traffic that you normally expect to work as well.
9 And that's where I said that kind of -- the traffic
10 really depends on, you know, your organization, your
11 subnet, yeah. So that's what I meant.

12 Q. So I believe you previously testified that you
13 personally have tested firewall policies in your test
14 beds; correct?

15 MR. KLEIN: Object to form.

16 THE WITNESS: I don't recall where I said it.
17 I said -- with regards to firewalls, I mentioned that
18 that's part of module I teach regularly in my class --
19 in my classes. I did say that I have test beds. And my
20 test beds involve -- at least one of them involves --
21 maybe two of them actually involve having a firewall as
22 well.

23 BY MR. LU:

24 Q. When you test -- when you use these test beds,
25 do you test specific firewall policies?

1 A. Yeah, of course. You don't want the malware
2 traffic to go crazy. Of course. That's one of the key
3 requirements.

4 Q. And if a firewall policy passes your test, what
5 do you do with it?

6 A. So again, my answer would be if the firewall
7 policy does not pass the test, I would not run it, of
8 course.

9 Q. Okay. What if it does pass?

10 A. Then yeah -- then you run it. Yeah. Sure.

11 Q. I guess I should ask you: So in these test
12 beds that you use, do you ever test different kinds of
13 firewall policies to see if they're -- you know, if they
14 do what you intend them to do?

15 A. So like I said, depending on your
16 organization -- so in this case, if my test bed -- only
17 traffic that can come out of the test bed itself is
18 malware traffic, then maybe all you care about is
19 whether the malware traffic, you know, can or cannot go
20 through depending on the policy. Right?

21 And then on the other hand, if your -- if your
22 test bed emulates the normal working environment, then
23 you may want to test only the malicious traffic but also
24 maybe the legit traffic as well. So it depends. Again,
25 a POSITA would understand always this -- this is

1 actually pretty obvious.

2 Q. Right. And so my question is: If you -- in
3 your test beds, you have a firewall policy that does,
4 you know, perform well against malicious traffic as well
5 as legit traffic, it performs as intended, what do you
6 do with that firewall policy?

7 Do you, like, publish in a paper, or do you
8 tell other people this is a great firewall policy?

9 A. I haven't seen a need, but I wouldn't say
10 that's unusual, to be honest. I mean that -- a firewall
11 policy being shared. A bunch of firewall policy being
12 shared all over the world. That's well-known. I mean,
13 personally, I may give example of my policy in my paper
14 and say, yep, here's how I make sure that the unintended
15 traffic will not go to the internet. Yeah. I'll do
16 that. Yeah.

17 Q. Do you ever regularly retest the same
18 policies --

19 A. Yeah, absolutely.

20 Q. -- that you've tested before?

21 A. Yeah. Absolutely.

22 Q. And how often do you regularly retest these
23 same policies?

24 A. Well, I mean, it's like this -- every time we
25 introduce new policy into the firewall, we test

1 everything again.

2 Q. Okay. And then do you retest the old policy
3 that you used to have ever?

4 A. Absolutely. Yes.

5 Q. Okay.

6 A. We test everything -- test everything again
7 that includes our policy, yes.

8 Q. Okay. So let me re-ask it this way.

9 So you said, "Every time we introduce new
10 policy into the firewall, we test everything again."

11 My question is: There was an older policy that
12 you had with the firewalls. Do you ever reuse that old
13 policy and test it again?

14 A. So it's like this: When you introduce new
15 firewall policies, unless explicitly say I remove the
16 old policy, the old policy will still be there. So when
17 you're going to traffic, you know, some traffic may
18 trigger the old policy.

19 Q. Okay. And you specifically retest that old
20 policy when you're testing for new policies; correct?

21 A. Yeah, I mean, normally that's a good principle
22 to have. It's call -- question testing, you just, you
23 know, do that.

24 Q. And how often do you test new policies?

25 A. Like I said, every single time introduce new

1 policy, I would test.

2 Q. Okay. But do you, like, test new policies
3 every day? Or is it every month?

4 A. Really at this point depend on the progress of
5 my students. I scream at them every single week. A new
6 policy -- say, yeah, let's run a test. Right? So
7 really depends on -- that's why I'm saying it's when new
8 policy is introduced, we run through test, of course.

9 Q. Okay. So suppose last year you had a student
10 that proposed an old policy, are you still running tests
11 on that old policy from last year?

12 MR. KLEIN: Object to form.

13 THE WITNESS: So again, unless we remove the
14 policy, the policy is there. It's still there. So if
15 you read the paragraph 26, when NCS, you know, make the
16 changes to the network elements, it's -- you know,
17 adding changes. I could be adding new policies, can be
18 removing old policies.

19 So really, to understand the -- the impact of
20 the changes -- in particular, first sentence, it say
21 illogical -- or illogical configuration, that really --
22 a POSITA would say, yep, I understand, I would probably
23 run test cases that tested the firewall as a whole. And
24 that's, like, obvious.

25 ///

1 BY MR. LU:

2 Q. In your test beds, do you ever test policies
3 outside -- well, let me -- withdrawn.

4 In your test beds -- withdrawn.

5 So you previously testified that you will run
6 the test again if you have a new policy; correct?

7 A. That's correct. Yeah. I mean, I -- what I
8 said is that whenever you have a new policy that
9 automatically triggers a new round of testing, yes.

10 Q. Okay. Do you ever test a policy that has
11 already been tested?

12 A. So again, I said that if the policy has been
13 tested -- let's call it old policy, as long as there --
14 then we test -- we normally test the firewall as a
15 whole, so that we include -- the old policy would also
16 be tested.

17 Q. That's in the context of testing a new policy
18 as well; correct?

19 A. Well, I mean -- so I will say that -- I think
20 we're talking two different things here. So we are
21 talking about when we introduce new policy, the question
22 is that -- do I test them before I install them? Yes,
23 of course.

24 And then in terms of old policy, do I ever test
25 it again even if new policy is not there? I would say

1 that when you run -- when you run traffic through
2 firewall, you know, there's a firewall log, and that
3 log's being used, actually, to monitor whether your
4 firewall is functioning properly, even though there's no
5 new policy introduced.

6 And so you could say that, hey, look, just
7 because you use a firewall, you're actually doing a live
8 test.

9 Q. Is this something that you're doing on your
10 test bed?

11 A. Yeah. I mean, we use test bed every single
12 time, every single day.

13 Q. So you're running live tests on your test bed.
14 Is that what you're saying?

15 A. Yes. Yes.

16 Q. Okay. Is it your opinion that Wang discloses
17 that firewall configurations have a predefined format?

18 A. Let me look at my declaration. Okay. So I
19 think that's a -- yeah. So I think on page 38 of my
20 declaration -- let's see here. Yeah. So on -- sorry.
21 On page 39, paragraph 74, I talk about, "Additionally,
22 these generated policies were stored in resource
23 database 103 as database records having fields that
24 reference specific firewall configurations that were
25 generated based on the user's requested modification."

1 So -- and go on to say -- that's from Wang's
2 patent, 16. And then -- let me see, further down I said
3 that the -- yeah, then I gave examples of -- of -- well,
4 let me skip that.

5 Basically, you know, when you say database
6 record -- I go on to say -- in the next sentence of
7 paragraph 74 to say that essentially, this is the
8 structure -- this is -- call it structured
9 representation. That's in -- the term of the '941
10 patent. So this basically -- database records is
11 structured representation, and that's example of
12 predefined format.

13 Q. So my question was: Is it your opinion that
14 Wang discloses that firewall configurations have a
15 predefined format? And your answer is yes?

16 MR. KLEIN: Object to form.

17 THE WITNESS: So as I said, you know, in
18 paragraph 74, I present a example of predefined formats
19 that's being used to -- to store the policy.

20 BY MR. LU:

21 Q. So in terms of validation, wouldn't it be
22 easier to simply check the policy configuration against
23 the predefined format and see if it's properly formed or
24 not formed?

25 MR. KLEIN: Objection. Scope.

1 THE WITNESS: What do you mean? In which --
2 which claim element or which one?

3 BY MR. LU:

4 Q. I'm not talking about any claim element. I'm
5 just talking about what Wang discloses in paragraph 26.

6 A. Okay.

7 Q. Wang discloses a validation process that uses
8 a -- for example, a dry run.

9 And my question is: Why not just check the
10 policy change against the predefined format that you
11 use?

12 MR. KLEIN: Objection. Scope.

13 THE WITNESS: So again, in 26, it talks
14 about -- so again, in 26 -- paragraph 26, right, he
15 talks about not checking the format -- right? It talks
16 about, you know -- the first sentence talk about, you
17 know, possible "erroneous or illogical automatic
18 configuration changes" -- "on the type changes being
19 made to a particular subnet and/or devices within the
20 subnet."

21 And then go on to say the next sentence, when
22 you do a dry run, the goal is to "check and validate
23 proposed firewall policy changes against a set of known
24 rules without making actual changes."

25 So really the goal of the validation is not to

1 check the format. It's checking the changes to the
2 network elements.

3 BY MR. LU:

4 Q. And that can't be done by simply checking the
5 format?

6 A. I guess, no. I mean, format is format. You
7 know, format is a -- how to put it -- is a syntax. So
8 in order to understand the actual effect, we talk about
9 semantic. And semantic information in this case -- you
10 actually have to run it to understand actual impact.

11 So format is really talking about the syntax of
12 the policy, how you should read and -- you know, and
13 then the actual effect is not -- is beyond just the
14 format and syntax.

15 Q. Are you an expert in databases?

16 A. I would say so, yes.

17 Q. Do you use databases in your regular work?

18 A. Right now, no, but my students do that.

19 Q. Okay. And which databases do you typically
20 use -- or your students?

21 A. I think now they use Ingres, which I'm
22 surprised is still alive. I used to be a programmer. I
23 use all kind of database when I was a programmer
24 full-time. Yeah. I'm very fairly familiar with
25 database.

1 Q. And you would agree that a database field has
2 different data types -- withdrawn.

3 And you would agree -- or withdrawn.

4 Are you familiar with the term "a database
5 schema"?

6 A. Absolutely, yes.

7 Q. And you would agree that a database schema
8 defines, for example, which rows and which columns are
9 stored in a database table; correct?

10 A. Yeah. Normally database schema would tell you
11 the fields of each -- that means what each column, you
12 know, means and how one database table would relate to
13 another table based on, you know, some keys that you can
14 use and so and so forth. Yeah.

15 Q. So you said that a database schema defines
16 which attributes -- withdrawn.

17 So you said the database schema defines the
18 attributes of each column; correct?

19 A. Yeah. Essentially, in layman's term, a
20 database schema would tell you for each table what's the
21 format of each record. A row is a record. Each column
22 is a attribute of the record. Database schema tells you
23 the format of the record of the database.

24 Q. And the database schema -- does it define the
25 type that the column -- withdrawn.

1 Does the database schema define the data type
2 of the column?

3 MR. KLEIN: Objection. Scope.

4 THE WITNESS: Yes. I mean, like I said,
5 attributes and sometimes the type can just be infer.
6 You say age; it infers a numerical.

7 BY MR. LU:

8 Q. Okay. But it can also explicitly define the
9 data type for a column; correct?

10 MR. KLEIN: Objection. Scope.

11 THE WITNESS: Could be. Could be. But, you
12 know, I don't think -- why it's important. But fine.
13 Yeah.

14 BY MR. LU:

15 Q. What sort of data types can the columns be
16 defined as?

17 MR. KLEIN: Objection. Scope.

18 THE WITNESS: Normally not a data type, per se,
19 but that's information details depending on the
20 database, technology, language you want to use, and so
21 on. But it's more like, you know, the -- like I said,
22 the attributes, like I said, you know, what -- what
23 describe a record on a database, what the fields, what
24 the attributes, and what the data represent.

25 ///

1 BY MR. LU:

2 Q. Well, I'm just trying to get some examples of
3 data types that a database can define for a column. So
4 you said previously that it could infer that a column is
5 a number because it's an age.

6 So one of the data types for a column could be
7 a number; correct?

8 A. Yeah, could be. Yes.

9 MR. KLEIN: Same objection.

10 BY MR. LU:

11 Q. It could be, for example, an integer; correct?

12 MR. KLEIN: Same objection.

13 THE WITNESS: Again, those things -- I don't
14 know why it's important, but -- just really depends on
15 implementation, you know, why do you want to do this. I
16 mean, there's also -- yeah, could you say, I'm -- you
17 know, I don't know -- somebody say I'm going to -- 19.5
18 years old, whatever. I mean, it's just, like -- it's
19 not important.

20 BY MR. LU:

21 Q. Right. I'm just asking just in general, a
22 column could be defined as having the data type of an
23 integer; correct?

24 MR. KLEIN: Object to scope.

25 THE WITNESS: Well, it wouldn't say here is

1 Column 1, what is an integer, no. That's not how we
2 define database schema. We say, hey, Column 1 is age --
3 okay -- that the most important information that you
4 should have in a database schema or the format of the
5 record. You wouldn't say, hey, it's a database record,
6 what's the format? The first field is a number, second
7 field is a string -- what are you talking about? What
8 number? What string? You're not giving information.

9 So my point is that any POSITA would understand
10 database schema will tell you, oh, here's a record --
11 here's a database schema for students -- let's say,
12 grade report. What's first field? The name. Second
13 field? ID number. What's the third field? Age --
14 probably cannot say that because private information.
15 Third field, what class you take. Fourth field would be
16 the grade. You see what I'm saying? That's the kind of
17 information we're looking at, not the data type.

18 BY MR. LU:

19 Q. Are you saying that database schemas don't
20 define the data types for these columns? So, for
21 example, the name does not -- the database schema does
22 not say that the name column has a type of string?

23 A. So --

24 MR. KLEIN: Object to scope and form.

25 THE WITNESS: Again, that depends on the

1 implementation. I would say also information that some
2 database schema may include, some database schema may
3 not include. It's not important, basically, to
4 understand what database really storing. That's --
5 those are not important things.

6 BY MR. LU:

7 Q. How long have you been using databases?

8 A. I'm old enough. That would be since the mid
9 1980s.

10 Q. So are you saying -- so withdrawn.

11 MR. LU: Actually, do you want to take a
12 short -- well, I got to -- I guess I don't have to eat
13 lunch, but I think it's time to take a break. Do you
14 want to take, like, a ten-minute break?

15 THE WITNESS: Ten minutes break.

16 MR. KLEIN: Do you want to eat, Dr. Lee? Did
17 you eat?

18 THE WITNESS: I ate half my lunch, so another
19 ten minutes would be plenty or 15 minutes.

20 MR. KLEIN: Why don't we do 15.

21 THE WITNESS: Okay. Sure. Yeah.

22 MR. LU: Sure. That's fine.

23 THE WITNESS: So I can finish second half my
24 lunch. All right. Sure. Thank you.

25 MR. KLEIN: Yep.

1 (Off the record.)

2 BY MR. LU:

3 Q. Dr. Lee, are you familiar with the database
4 MySQL?

5 MR. KLEIN: Object to scope.

6 THE WITNESS: I have heard of it, but I'm not
7 sure I used it.

8 BY MR. LU:

9 Q. What databases have you used before?

10 A. I use Oracle, Sybase, Ingres, Microsoft Access,
11 Ebase, yeah. Variety of them.

12 Q. Oracle is a pretty popular database, would you
13 agree?

14 MR. KLEIN: Object to scope.

15 THE WITNESS: Oracle is a big company. I have
16 not looked at the market share.

17 BY MR. LU:

18 Q. Are you familiar with the data types that
19 Oracle's database supports?

20 MR. KLEIN: Same objection.

21 THE WITNESS: I don't recall the details, no.

22 BY MR. LU:

23 Q. During the break, did you talk to anybody?

24 A. No.

25 Q. Okay. And in the last break, same question,

1 did you talk to anybody?

2 A. No.

3 Q. So are you familiar with the fact that Oracle
4 databases support data types like integers, floats,
5 doubles, et cetera?

6 MR. KLEIN: Object to scope. Relevance.
7 Foundation.

8 THE WITNESS: I wouldn't be surprised that they
9 support those data types. No, I wouldn't be
10 surprised.

11 MR. LU: Counsel, you can limit your objections
12 to form. Thanks.

13 MR. KLEIN: Well, if it's not -- excuse me,
14 Counsel. If it's not an objection to form but as to the
15 scope or relevance or foundation, those are not to form.
16 Those are to substance.

17 MR. LU: All right. Then go ahead and object
18 as much as you want.

19 BY MR. LU:

20 Q. Are you familiar with the fact that Oracle
21 databases support data types like character and string?

22 MR. KLEIN: Same objections.

23 THE WITNESS: Again, I wouldn't be surprised
24 that they support those data types when they have to
25 implement the logic of storing data in database, and

1 they're having a, you know, C programmer, which I used
2 to be, to program the code that process database -- you
3 should know the data types. Of course. Yeah.

4 (Reporter clarification.)

5 THE WITNESS: So what I'm trying to say is that
6 I was not surprised that Oracle supports all these data
7 types. I mean, in fact, you need -- internally, at
8 least, you need to define data types so that you know
9 you can store data properly in a computer, and then
10 programs that process this data would know what data
11 type they would expect.

12 But, you know, in the context of this -- this
13 case, I mean, to me, the most important thing is that
14 the -- the definition of the attribute. What is the
15 attribute? Is it a name? You know, a ID number? A
16 course number? Grade? Kind of example -- which is, oh,
17 this is a float, that's a integer -- it's completely
18 different levels of details that a POSITA would care
19 about.

20 BY MR. LU:

21 Q. Okay. Understood. I want to go back to your
22 declaration at paragraph 34.

23 A. Okay.

24 Q. Actually, no, we don't need to -- let's --
25 actually -- so previously you testified about funneling

1 all of the network's traffic through a firewall;
2 correct?

3 A. Funneling -- I mean, that's the objective. If
4 you want to put a firewall to protect a network, your
5 objective -- of course, you want to make sure that
6 traffic will go through that firewall -- any traffic
7 goes in and out of the network, you want it to go
8 through the firewall. Yeah. That's the objective.

9 Q. Why was -- why is it an objective that you have
10 traffic go through a single firewall? Why not just
11 have -- or I should just -- yeah. That's the question.

12 MR. KLEIN: Object to form.

13 THE WITNESS: I didn't say single firewall. I
14 just say that you want traffic to go through firewall.
15 Doesn't have to be single firewall. Some network can --
16 actually two firewalls.

17 BY MR. LU:

18 Q. Okay. But do you want -- would you --
19 withdrawn.

20 So in paragraph 34 of your declaration, you
21 state, "The internet was created to provide a resilient
22 communication infrastructure. The internet protocols
23 specify how computers can exchange information with each
24 other, even when two computers belong to different
25 networks."

1 Do you see that?

2 A. Yes.

3 Q. And then later in the paragraph, you said, "Due
4 to the lack of awareness of potential security risks and
5 that there was no major, internet-scale attack yet, the
6 internet in the 1980s was relatively open."

7 What did you mean by "relatively open"?

8 A. There were many examples -- relatively open --
9 example -- I know an instance maybe in the '70s --
10 basically the first spam. Basically, so few users on
11 internet -- at the time everybody knows everybody.
12 Everybody knows -- everybody knew everybody's mailing
13 address, e-mail address. Somebody sent a spam,
14 basically try to sell real estate, and people say, oh,
15 what the heck are you doing.

16 So that's what open stands -- everything --
17 almost everybody on the internet knows everybody else
18 and be able to access anybody -- well, not access, but
19 actually reach to everybody on the internet. That was
20 definitely in the -- you know, would be early days on
21 the internet, quite possibly in the -- into the '80s.

22 I wouldn't say that -- I would say even in the
23 early 1990s, you could still -- you could still do a lot
24 of things; now it's not imaginable. Let's put it that
25 way.

1 Q. So you just testified about e-mail.

2 Would you say that the internet in the 1980s
3 was relatively open with respect to network access?

4 A. Yes. I mean, there was instance where you can
5 use modem to connect to enterprise without proper
6 check -- without proper -- without the proper checks.
7 Yes. There has been documented somewhere, yeah.

8 Q. So later you say in this paragraph, "That is,
9 many communications and activities, e.g., a computer
10 sending to and/or receiving data from another computer
11 on the internet, were allowed because the security
12 policy and mechanisms of a computer or its network,
13 e.g., its enterprise network, were often severely
14 overlooked."

15 Do you see that?

16 A. Yes.

17 Q. And you still agree with that statement?

18 A. At that time in the '80s, yeah, sure.

19 Q. Now, today, a computer can still send or
20 receive data from another computer on the internet;
21 correct?

22 A. Today -- I mean, principle, that's your goal to
23 send data to another computer, but it's going through
24 much -- much more checks, much more security checks and
25 regulation limitations than in 1990s for sure.

1 Q. And one of those security checks would be a
2 firewall?

3 A. I would say in the -- POSITA's term would be:
4 Firewall is part of the so-called security fabric. By
5 "fabric," I mean multiple security elements and controls
6 that one would use or one would want to have. And
7 firewall is part of the -- part of the fabric.

8 Q. So I want to move on to a different topic.

9 Could you -- do you have a copy of Exhibit
10 1008, the Chambers patent application?

11 A. Yes, I do. Chambers. Yes, I have it here.
12 Yep. I have it.

13 Q. Okay. And actually, let's go back to your
14 declaration first.

15 A. Okay.

16 Q. Paragraph 166, starting at page 93.

17 A. Okay.

18 Q. Now, I'm actually looking at page 94 where you
19 have an annotated version of Figure 7B from Chambers;
20 correct?

21 A. Yes.

22 Q. And here, once again, you have colored in as
23 blue these two circles and labeled them "enterprise
24 network." Is that right?

25 A. That's correct.

1 Q. And within each of these circles, there is a
2 network access device and it includes some examples as
3 switches, routers, AP, et cetera.

4 Do you see that?

5 A. Yes, I see that. Yes.

6 Q. Actually, let me ask this question: Is it your
7 opinion that each one of these circles is its own
8 enterprise network, or is it your opinion that these two
9 circles combined are one enterprise network?

10 A. Let me -- let me see how Chambers said it --
11 explained his Figure 7B. Let me see. I mean, I would
12 say, in principle, a POSITA would agree that, you know,
13 they could be two different subnets of the same
14 enterprise, so that's why, you know, they are together
15 as the enterprise network. Yeah, they could be one.

16 Of course you can say, oh, they could just be
17 different network -- different enterprise. That's
18 possible too. I mean, doesn't have to be one or the
19 others.

20 MR. LU: Actually, can we take, like, a
21 two-minute break? Sorry.

22 THE WITNESS: Okay. All right. Sure. Yep.
23 Thank you.

24 (Off the record.)

25 ///

1 BY MR. LU:

2 Q. Okay. So Figure 7B depicts these networks, and
3 each one has network access devices; correct?

4 A. That's correct.

5 Q. And those NADs could be a firewall; is that
6 correct?

7 A. Let me see how we -- oh, by the way, I -- your
8 question regarding, you know, whether these two blue
9 bubbles are the same enterprise network -- actually, in
10 paragraph 67 of the Chambers patent, it did talk
11 about -- it explain 7B as, you know, the same
12 organization, basically. So -- so in that case,
13 basically referring to different geolocations or
14 different sites of the same organization.

15 So in this case -- just basically make sure
16 that we cover what you ask before the short break --
17 that I would consider these two blue bubbles -- they are
18 the different -- different parts of the organization at
19 different location, but together they are the -- they
20 are within the same enterprise network.

21 Okay. So -- and what's your current question
22 again? I'm sorry.

23 Q. Right. So let's look at paragraph 17 of
24 Chambers.

25 A. Okay.

1 Q. Are you there? It's on page 11.

2 A. Paragraph 17, Chambers. Yes.

3 Q. In the middle, it's -- the sentence that says,
4 "The system is designed to function with large numbers
5 of client devices, authorized for varying and
6 potentially long periods of time, and even if the
7 network access devices, NADs, e.g., routers, wireless
8 access points, network switches, or firewalls, et
9 cetera, are numerous and spread out over a large
10 geographic area."

11 Did I read that right?

12 A. Yes.

13 Q. So you would agree that these NADs include
14 firewalls; correct?

15 A. Yeah. So basically what it says -- firewall is
16 one example of NAD, yes.

17 Q. And you would agree that these firewalls could
18 include the sort of firewalls you discussed in
19 paragraph 37 and 38 of your declaration?

20 A. 37, 38.

21 MR. KLEIN: Object to form.

22 BY MR. LU:

23 Q. I should say 36 and 37 of your declaration.

24 A. Okay. So in 36 and 37, I talk about, you
25 know -- essentially, 36 and 37 -- each paragraphs are in

1 the context of the relevant technologies, and in
2 particular, I am, you know, basically citing in
3 paragraph 36 the, sort of, early version of the firewall
4 concept in the late 1980s, the reference I cite; and
5 then 37 is example of the graphical user interface of a
6 firewall in the late 1990s.

7 So again, what's your question?

8 Q. My question is: When Chambers says that these
9 NADs could be firewalls, does that include these
10 firewalls that you describe in paragraphs 36 and 37?

11 A. So again, I think, like I said before, right,
12 36 talks about the basic concepts of firewall using the
13 reference in the late 1980s, and 37 is example of the
14 graphical user interface. I would say that you know --
15 any firewall you expect to have, you know, for example,
16 these basic functionalities as described in 36, and some
17 firewall may also have the user interface as exemplified by
18 paragraph 37.

19 Q. All right. Going back to paragraph 166 --

20 A. Okay.

21 Q. -- Figure 7B.

22 A. Uh-huh.

23 Q. You also have in orange -- you also colored in
24 this management server 1001 with the color orange;
25 correct?

1 A. Yes.

2 Q. And you labeled it "system"?

3 A. Yes. I'm referring to -- it's a management
4 server that -- it's a -- it's a system. Yes.

5 Q. And it's your opinion that this management
6 server is remote from the enterprise networks; correct?

7 A. Well, as shown in Figure 7B, the management
8 server is connected to LAN 1005 and LAN 1006 through the
9 wide area network, such as the internet. So a POSITA
10 would, you know -- would see that as at least, you know,
11 in some embodiments, this server is remotely from the
12 enterprise network.

13 Q. What does ACR stand for?

14 A. I think as I explained in paragraph 167, you
15 know, I say, "According to Chambers, the device in
16 LAN 1005 and LAN 1006 were part of the same enterprise
17 company and were protected in accordance with access
18 control rules and policies, ACR and ACPs."

19 So ACR is access control rules, and ACPs are
20 access control policies.

21 Q. And what's the difference between an ACR and
22 ACP?

23 A. So it's a general concept in computer science
24 called a policy or mechanism. So access control policy,
25 by definition, policy, meaning what's allowed, what's

1 not allowed. And the rule is one example of the
2 mechanism, meaning the -- how to implement those
3 policies.

4 You say, well, you know, to implement this
5 policy, for example, you have to be authenticated with
6 the proper, you know -- so then say, okay, that's a
7 policy, and what's the exact mechanism? Well, you have
8 to provide a proper password, or maybe you cannot enter
9 the incorrect password three times in a row. So those
10 are the kind of rules, we call it mechanism -- the spec
11 of the mechanism that satisfy the policy.

12 So that's why Chambers talks about both the
13 policy and the rules, basically policy and the
14 mechanism. Likewise, firewall, same deal. Policy and
15 the rules; one's policy, one is mechanism.

16 Q. Okay. And then you say, "Chambers explained
17 that the ACRs and ACPs were transmitted from the
18 management server to multiple network access devices
19 that were associated with the same enterprise company."
20 And then you quote Chambers 49; right?

21 A. Yes. That's what I said.

22 Q. Okay. So let's turn to paragraph 49 of
23 Chambers.

24 A. Okay.

25 Q. Exhibit 1008.

1 A. All right.

2 Q. Could you read that whole paragraph and then
3 let me know when you're done?

4 A. Okay. I want to make sure I'm reading -- okay.
5 Yeah.

6 Q. Okay. So I want to start somewhere in the
7 middle of this paragraph. It says, "Referring to
8 Figure 4 at block 401, a web interface is provided at a
9 management server to allow an administrator to configure
10 a set of ACRs and/or ACPs for client devices."

11 Did I read that right?

12 A. Yes.

13 Q. Okay. And then it says -- or actually, let's
14 stay with that.

15 So Chambers is talking about providing an
16 interface so a client can modify or create ACRs and ACPs
17 that are for client devices; correct?

18 A. Let me see here. Yeah. It's -- "A web
19 interface is provided at a management server to allow an
20 administrator to configure a set of ACRs and/or ACPs for
21 client devices." Yeah. That's what it says. Yes.

22 Q. Okay. And then it says, "At block 402, the
23 ACRs and ACPs are then stored in a persistent storage of
24 the management server."

25 Do you see that?

1 A. Yes.

2 Q. And then, "At block 403, the ACRs and ACPs are
3 transmitted from the management server to multiple
4 network access devices that are associated with the same
5 enterprise company."

6 Do you see that?

7 A. Uh-huh. Yes.

8 Q. And then it says, "The network access devices
9 enforce the ACRs and ACPs to control access of the
10 associated network client devices."

11 Do you see that?

12 A. Yep.

13 Q. Would you agree that all these steps are
14 performed automatically, as in there's no human
15 intervention?

16 MR. KLEIN: Object to form.

17 THE WITNESS: Well, it's what it says. It
18 doesn't say one way or the other.

19 BY MR. LU:

20 Q. Okay. So your opinion is that this discloses
21 that after an administrator configures a set of ACRs, a
22 human instructs the ACRs and ACPs to be stored in
23 persistent storage and then transmitted?

24 A. That's not what it says. It says "are then
25 stored," so you could assume it's automatically stored.

1 Transmitted -- you could assume that's automatically
2 transmitted. But again, they didn't explicitly specify
3 that. But I --

4 Q. Understood -- oh, go ahead.

5 A. No, you go ahead.

6 Q. Yeah. I mean, I understand. But, you know,
7 from the perspective of a POSITA reading this, when it
8 says "at block 403, the ACRs and ACPs are transmitted,"
9 is that by a human or is that automatically?

10 A. You know, I would say --

11 MR. KLEIN: Object to form.

12 THE WITNESS: So again, the spec doesn't say
13 this explicitly. I would say in a lot of case,
14 transmitted -- yeah, you know, you would imagine a lot
15 of cases, why not. You know, if you can; right? In
16 some cases they may not be able to.

17 So you know, again, it's -- my point is that if
18 it's so important to say automatically, it would say so
19 in the spec. But if it didn't say specifically
20 automatically, that means it is irrelevant to what it's
21 talking about here. I think all we care about is it's
22 transmitted and stored. Okay.

23 BY MR. LU:

24 Q. Okay. But your opinion is that this disclosure
25 includes a human transmitting the ACRs and ACPs?

1 MR. KLEIN: Object to form.

2 THE WITNESS: What I'm trying to say is that it
3 doesn't affect my opinion.

4 BY MR. LU:

5 Q. You understand that the claims require a
6 computer-implemented method?

7 A. Yes.

8 Q. So it doesn't affect your opinion as to whether
9 or not these steps are performed by a computer or a
10 human?

11 A. If the spec say -- has to be transmitted by a
12 computer automatically -- did it say that?

13 Q. So it's your opinion that there's a human
14 intervention in between each of these steps in Chambers?

15 A. So, again, those are details that does not
16 affect my -- my opinion, right, because it start by
17 saying that -- the administrator enters the policy
18 and -- and the ACRs -- and then maybe the administrator
19 will click on some button and say, hey, I'm done, and
20 then kick off some storage and transmission -- whatever.

21 I mean, those things are details that does not
22 matter. The -- you know, so -- so I think that's why
23 this paragraph did not explicitly say -- have to say
24 those kind of things.

25 Well, if you read -- if you read further into

1 paragraph 49 right at the end, the last sentence say,
2 "At block 404, the management server periodically
3 transmits updates of the ACRs and ACPs to the network
4 access devices over the internet." So in this case,
5 it's giving you, you know, indication that this is
6 happened -- that transmission is happen -- is happening
7 automatically.

8 Q. Okay. So let's turn to paragraph 29 of
9 Chambers.

10 A. Okay. Okay.

11 Q. And I'm specifically looking at paragraphs 29
12 to 40 of Chambers.

13 Do you see that?

14 A. I'm sorry. I was reading -- can you repeat the
15 statement again?

16 Q. So are you -- are you at -- are you looking at
17 Chambers paragraph 29?

18 A. Yes.

19 Q. Okay. And I'm actually going to be asking
20 questions about paragraphs 29 through 40.

21 Do you see that?

22 A. Okay. Yeah. Sure.

23 Q. So paragraphs 29 through 40 -- well, let's
24 start with paragraph 29. Paragraph 29 describes a --
25 quote, "an example ACR that explicitly specifies an

1 ACP." Correct?

2 A. Yes.

3 Q. And that's paragraphs 29 through 36?

4 A. Paragraph 3 -- yes.

5 Q. Okay. And then paragraphs 37 through 40 is
6 another example of an ACR that -- this one that refers
7 to a predefined ACP; correct?

8 A. Yes.

9 Q. And you would agree that these ACRs are used to
10 modify firewall policies; correct?

11 A. Let me see what it says so or not. I couldn't
12 find the reference to firewall. I mean, looking up,
13 paragraph, let's say, 27, 28, it seems to -- referring
14 network access device, so it didn't say this has to
15 be -- this ACRs have to be firewall rules. No, it
16 didn't say so.

17 Q. Well, I didn't ask if they have to be firewall.
18 I said they can be for firewalls; correct?

19 A. It -- you know, I mean, some of these policies
20 may be -- may be able to -- involve firewalls or maybe
21 some other additional NADs as well. So really depends
22 on which -- depends on details of the policy, to be
23 honest.

24 Q. So, for example, on paragraph 36, which is part
25 of the first example, it says, "Firewall," colon, "block

1 TCP port 80."

2 Do you see that?

3 A. Yes. That's --

4 Q. Would you agree that's a firewall policy?

5 A. Yeah, that's one particular policy that the
6 firewall implement, but some others may or may not be.
7 Depend on firewall configurations.

8 Q. Okay. So you would agree that ACRs are used to
9 modify firewall policies?

10 A. I'm saying that this has example of ACRs -- or
11 the ACPs that -- that basically says firewall will do
12 this part, which is block TCP port 80. Now, there are
13 some other policy elements that may not be appropriate
14 for firewall.

15 Q. These two examples of ACRs don't actually
16 provide any definition of how the ACRs are to be
17 formatted; correct? Let me re-ask it.

18 These two ACRs -- withdrawn.

19 These two examples of ACRs don't provide any
20 definition of the syntax for the ACRs; correct?

21 A. Syntax of the ACRs. I am -- I need to look at
22 Chambers -- I mean, I think we talk about Chambers
23 format. Let me see. I think in my declaration talk
24 about formats of Chambers, so why don't we reference
25 that to see examples of that. So -- let me see here.

1 So I would say that, you know, if you look at
2 my -- my declaration, page 104, paragraph 188, I talk
3 about -- in particular, I say the -- so there I say, "A
4 POSITA would have recognized or found it obvious that
5 Chambers' ACPs and/or ACRs constituted the claimed
6 'policy digests,' at least because these ACPs and/or
7 ACRs are consistent with examples of 'policy digest'
8 provided in the '941 patent, as shown in a comparison
9 below of the example policy digest listed in Figure 4C
10 of the '941 patent with the example ACPs and ACRs
11 described in Chambers."

12 So then in -- so in -- on page 105, I put the
13 policy of Chambers, meaning paragraph 29 to 40 on the
14 left and highlighted the -- the syntax -- or the -- or
15 the format and compare that with '941 patent, Figure 4C,
16 the example policy digest.

17 So I would say basically in 189 -- paragraph
18 189 of my declaration, I say, "As evident from above,
19 similar to the example policy digest illustrated in
20 Figure 4C of the '941 patent, Chambers' ACRs and/or ACPs
21 were formatted according to a predefined format."

22 Q. Okay. So looking at those two excerpts that
23 you provided, the one in Chambers says, for example,
24 "Download bandwidth," colon, "2 megabits per second";
25 right?

1 A. Uh-huh. Uh-huh.

2 Q. And then the one on the right for the '941
3 patent says, "Bandwidth," underscore, "up," colon, "20."

4 A. Uh-huh.

5 Q. Right? You would agree that the syntax of
6 these examples are not the same; right?

7 A. They actually very similar. "Bandwidth up"
8 means upload bandwidth is 20. "Bandwidth down 100,"
9 that means download bandwidth is 100. It's very --

10 Q. Sure. They may be similar, but they're not the
11 same; correct?

12 A. I would say the same. They're trying to convey
13 same information, just like -- just like if you compare
14 to database, one call it student ID, the other one call
15 it -- you know, I don't know -- Georgia Tech is Buzz --
16 you know, BuzzCard ID, but they're the same thing. So I
17 mean, just -- you name it differently, doesn't really
18 matter. It's so obvious.

19 Q. Right. So one -- for the Chambers, the way to
20 indicate the upload bandwidth is to say "Upload
21 bandwidth," and then colon, then you specify "1 megabits
22 per second" --

23 A. Uh-huh.

24 Q. -- correct?

25 A. That's the example in Chambers, yes. He talks

1 about download bandwidth, yes.

2 Q. And then in the '941 patent, the way you
3 specify an upload bandwidth is you actually put, quote,
4 "bandwidth," underscore, "up," end quote, colon, space,
5 "20," comma. Right?

6 A. Yes. I think -- I think what you're getting --
7 yes, they're different format, not exactly the same
8 format, but they are conveying the same information -- I
9 mean, I think I would say in terms of the layout and the
10 information that they want to include, it's very
11 similar. I mean, anybody -- POSITA compare left and
12 right, yeah, I mean, basically very similar format, try
13 to tell you what these fields are and -- and it's like
14 this: If "bandwidth," underscore, "up," is not obvious,
15 why would they call it that way?

16 Q. I understand.

17 A. See what I'm saying? So if somebody choose to
18 "download bandwidth," colon -- somebody wanted double
19 quote, "bandwidth," under bar, "up," you know, double
20 colon, "20" -- why don't you just say BU? If you want
21 to be cute. I mean, obviously they found that
22 sufficient, and to me, it's sufficiently -- well, it's
23 very obvious to POSITA, yeah, they're basically same
24 kind of format.

25 And then I would just say that, you know, in

1 paragraph 189, I go on to say that there are examples of
2 Chambers' policy, particularly ACRs, that are
3 formatted -- for example, say, in the second sentence of
4 paragraph 189 of my declaration, I say, "As another
5 example, the ACR listing illustrated in Figure 2 of
6 Chambers shows that these ACRs were formatted to include
7 various fields, such as 'Version,' 'Network ID,' 'SSID,'
8 'MAC,' which also indicate into these ACRs are formatted
9 according to a predefined format."

10 So the point is, yeah, a POSITA would agree
11 that, yes, the -- you know, in Chambers, the ACRs and
12 ACPs, they're formatted in some predefined format. Yes.

13 Q. So looking at the left-hand excerpt from
14 Chambers, you would agree that these examples of ACRs
15 don't actually define the format of the ACR; right?
16 This is just an example.

17 A. I would say this examples likewise -- the
18 right-hand side is also examples. So --

19 Q. I'm just asking about the left-hand side.

20 A. Yeah. So normally, this indicates to you that
21 there's a format.

22 Q. There is -- it indicates there's a format, but
23 this is not the actual definition of the format;
24 correct?

25 A. Well, I mean, just like -- if you look at C

1 programming language, look at a piece of code, does it
2 have a format? Yes. By looking at that piece of code,
3 do you know the full extent of the C language format?
4 So you need to look at the manual. There's a manual to
5 look at, tell you what's the proper syntax of C, how to
6 interpret the semantic. It's two different things.

7 But looking at C code, for example, okay, yeah,
8 I need to write format in this format, otherwise won't
9 compat- -- wouldn't run. Does the example tell you
10 everything about C? No. I mean, that's -- a POSITA
11 would look at this, yep, that means these ACRs, ACPs,
12 have format. That's this -- the definition of whole
13 format? No, probably not. You could say the same thing
14 about the right-hand side.

15 Q. Okay. So in Chambers, the ACR needs to have
16 the proper format in order for it to be able to update a
17 firewall; correct?

18 MR. KLEIN: Object to form.

19 THE WITNESS: So, again, those are two
20 different things. I mean, obviously, you know, ACRs and
21 ACPs, they have formats. Yeah. And normally, anything
22 involves a process such as updates or, you know,
23 installation, whatever -- of course, you're going -- you
24 have to enforce -- follow certain format, otherwise you
25 don't even know how to process the data if you don't

1 know the format of the data. Of course you need to know
2 the format.

3 BY MR. LU:

4 Q. You need to know the format, and you need to --
5 the ACR needs to follow that format; correct?

6 A. So as I said in paragraph 188, yes, I mean,
7 the -- the -- basically, the example that we give here
8 indicates that in Chambers, the ACPs and ACRs, they
9 are -- they are formatted according to some predefined
10 format. I mean, that -- to me, again, like I said, it's
11 well understood by any POSITA. If -- POSITA would think
12 about how do they implement similar technologies, you
13 have to know -- again, like I said, in order for you to
14 process the data, the data can be -- you know, ACRs and
15 ACP in this case, you need to know the format of that
16 data. Yeah.

17 Q. Okay. And so you say in paragraph 189 that,
18 "As another example, the ACR listing illustrated in
19 Figure 2 of Chambers shows that these ARs were formatted
20 to include various fields such as 'Version,' 'Network
21 ID,' 'SSID,' 'MAC,' et cetera." Correct?

22 A. Yes.

23 Q. But these examples do not show all of the
24 fields for the predefined format; correct?

25 A. Well, paragraph 35, that's a VLAN ID. That's a

1 network ID.

2 Q. Right. So, for example, on the right-hand side
3 for '941 patent, there is a field for city, which can be
4 set to Los Angeles.

5 Do you see that?

6 A. Yes.

7 Q. But on the left-hand side, there is no such
8 field for city; correct?

9 A. That's correct. But, again, like I said
10 moments ago, that these are examples. It tells you
11 that, yes, these examples of ACRs and ACPs, they do
12 follow a predefined format. Does this include the whole
13 format requirements? No. Like I said, looking at a
14 piece of C code, you kind of understand what it -- you
15 know, what's a proper way to write C code that -- do you
16 know everything about the format requirement? Maybe
17 not. Like I said, you need to look at the complete
18 manual.

19 Q. Right. So looking just at these examples from
20 Chambers, you do not know whether or not the predefined
21 format includes -- or supports the "city" field; right?

22 A. I do not know one way or the other. I mean, it
23 may include it. It may or may not. But it doesn't
24 matter. All I care is, yes, it has a format -- it has a
25 predefined format.

1 Q. Understood.

2 A. And it provides examples of that. And
3 likewise, if you asking me for '941, is that the whole
4 possible format? I don't know. Unless the patent says
5 so.

6 Q. Okay. And so on the left-hand side for
7 Chambers, at paragraph 36, there's a field that says
8 "Firewall," and then it says, "Block TCP port 80."

9 Do you see that?

10 A. Yes, I see that. Yep.

11 Q. And actually what -- to a POSITA, what does
12 that mean?

13 A. That means that's a policy that were
14 implemented at a firewall to block port 80.

15 Q. Why would you want --

16 A. To block TCP port 80.

17 Q. Why would you want to block port 80?

18 A. What's port 80? Port 80 is a web server. You
19 don't want people to access your web server for whatever
20 reason. Okay. That's how I read it.

21 Q. So you read paragraph 36 as blocking traffic to
22 your web server?

23 A. Well, I think port 80 -- okay. Here's
24 historical note. When web -- web -- World Wide Web
25 first came out, all the web server runs on port 80.

1 Then people realize that was a huge mistake because port
2 80 is so-called a privileged port, meaning that if you
3 connect to port 80, you're able to -- that port 80 take
4 your command, that command will run as a root on your
5 machine. That's not a good idea.

6 So they move all the web server to port 8080,
7 which is a nonprivileged port. So basically, I think
8 that by -- I don't know, mid -- maybe mid -- not
9 quite -- late 1990s -- mid -- 19 -- mid to late 1990s,
10 people starting to essentially block, you know, traffic
11 to port 80, which is a privileged port, and only allowed
12 traffic to port 8080 if you're running a web server.
13 That's the historical note. Yeah.

14 Q. But today --

15 A. So I'm not surprised to see that. Yeah.

16 Q. Okay. So in this example from Chambers, it
17 does not include any field that says to block traffic
18 from a particular domain; correct?

19 A. So 36 essentially block any -- you know, if you
20 don't say -- it's like this: You know, a lot of times
21 in firewall, it's basically if you don't explicitly say
22 allow, that means you don't allowed. If you don't
23 explicitly say whichever, that means any. So in this
24 case, I would say 36 means block any traffic from
25 anywhere to my port 80. That's how I interpret it.

1 Q. Correct. But it does not say -- withdrawn.

2 But this example from Chambers does not provide
3 any example of blocking traffic from a particular domain
4 or a particular network; correct?

5 A. Let me see. Let me look at what's the MAC
6 address that it talk about here. Yeah, I mean, to your
7 question, it doesn't seem to -- so, again, I don't know.
8 I mean, for example, in paragraph 40, it says, "Policy
9 ID 105." What is that?

10 So does that -- you know, for example, maybe
11 policy ID 105 is -- is, you know -- is -- is specific
12 about a particular domain. I don't know. But it could
13 be; right? So -- yeah, it didn't say so. But again,
14 it's not -- it's not important in the sense that if
15 POSITA reads this and says, oh, 36 is example firewall
16 blocking any connection to port 80, well, in that case,
17 it's -- POSITA would find it obvious that in some other
18 situation, you can say, hey, firewall block any
19 connection from this domain to any of my machines.

20 That's pretty obvious that you can just do that
21 by looking at 36 and basically say, I have a different
22 policy to specify.

23 Q. So you would agree that in Chambers, it's
24 obvious to define a policy that blocks traffic from a
25 particular domain?

1 A. Yeah, absolutely.

2 Q. Firewall policy.

3 A. Absolutely. Yes.

4 Q. Yes. Okay.

5 So on the left, Chambers has this firewall
6 field that says, "Block TCP port 80." And the example
7 on the '941 patent, it does not have a similar policy
8 for blocking TCP port 80; correct?

9 A. Let me look at this. Yeah, that's correct. It
10 doesn't seem to explicitly talk about port 80.

11 Q. Right. It doesn't seem to specifically talk
12 about blocking any TCP port; correct?

13 A. I need to go back to -- to -- let me see. This
14 would be paragraph -- I'm going to look at how it
15 explains this Figure 4C in -- in the '941 to see whether
16 actually help me interpret what it says here. So --
17 interesting. Let me look at the Figure 4C, because I
18 look at the language of Chambers -- it's actually pretty
19 interesting. Okay. I see.

20 So I mean, again, if you read the paragraph --
21 well, it's -- you know, column 17 of the '941 patent,
22 you know, line 4 to 19, it actually explains the --
23 basically policy -- example policy digest in full. What
24 we include here in the -- on paragraph -- in -- on page
25 105 of my declaration only a snippet of that.

1 So my point is that if you read column 17,
2 page -- sorry, line 4 to line 19 of the '941 patent, it
3 actually explains further information that we did not
4 include in this example. For example, it talks about a
5 web server, talks about specified DDoS protection, and
6 so and so forth.

7 So -- and, you know, allows traffic on port 80
8 into server, you know, so and so forth. Yeah.

9 MR. LU: Okay. Why don't we take a break and
10 let me see if I have any other questions for you.

11 THE WITNESS: Okay. All right. Yep. Thank
12 you.

13 MR. LU: Actually, let's break for ten
14 minutes.

15 THE WITNESS: All right. Yep. Thank you.

16 (Off the record.)

17 BY MR. LU:

18 Q. All right. Dr. Lee, I still have a couple more
19 questions.

20 A. Okay.

21 Q. So first, during the break, did you talk to
22 anybody?

23 A. No.

24 Q. Okay. Could you turn to -- sorry, could you
25 turn to paragraph 50 of your declaration.

1 A. Okay. Paragraph 50; right? Okay.

2 Q. Yeah.

3 A. Okay.

4 Q. So there you have an annotated version of
5 Figure 1 from Wang; correct?

6 A. Yes.

7 Q. Okay. So do you see in orange -- in the color
8 orange that you colored a dynamic firewall controller
9 102?

10 A. Yes.

11 Q. And it's your opinion this is remote from the
12 enterprise network?

13 A. I'm very sure I said that in my declaration as
14 well. Yeah. So as I said in my paragraph 55, I said
15 that, "Wang described a method for protected devices in
16 cloud networks 122, enterprise network, at a dynamic
17 firewall controller 102, system, and this dynamic
18 firewall controller 102 was remote from devices in cloud
19 network 122." And then I think I cited the -- the
20 abstract as well. Yep.

21 Q. Okay. So --

22 A. Yeah.

23 Q. Okay. Great. Now, looking back at Figure 1 at
24 paragraph 50.

25 A. Uh-huh.

1 Q. There's dynamic firewall controller 102 --
2 actually, let me re-ask it this way.

3 So there's also a resource database 103,
4 correct, that you colored in pink?

5 A. Yes.

6 Q. Now, the dynamic firewall controller is not
7 directly connected to the resource database; correct?

8 A. Really depends on what you mean by "directly
9 connected," because you do see the communication network
10 130 there. I mean, I would say -- reading this, you
11 would say that they're all connected through network at
12 least.

13 Q. Okay. They're all connected to a network, but
14 it doesn't say that the firewall controller is directly
15 connected to the resource database; correct?

16 A. I mean, it doesn't matter, right, in a sense
17 that as long as they are -- they are connected through
18 the network, that's all that matters.

19 Q. Why is that all that matters?

20 A. Well, whether you're on the same LAN, same
21 location, doesn't really matter. I mean, that's the
22 whole -- whole thing about, you know, the -- you know,
23 the various virtual networks setups or enterprise
24 network setup. You know, point is that you can connect
25 anywhere from the internet as if you are right next --

1 right next office. I mean, that's the whole point.

2 Q. So you're saying that the dynamic firewall
3 controller can connect to the resource database through
4 the network, and that's just like as if the resource
5 database was right next to the controller? That's your
6 testimony?

7 A. My testimony is that they're connected through
8 the network, whether the network is local versus going
9 through the internet; doesn't really matter. That's
10 what I'm trying to say.

11 Q. What if -- withdrawn.

12 But wouldn't it be better if the resource
13 database was inside the dynamic firewall controller?

14 MR. KLEIN: Object to form.

15 THE WITNESS: I mean, again, that's not
16 something that I -- I consider in this matter. I mean,
17 to me, it doesn't really matter. I mean, all I care is
18 that the dynamic controller can store stuff in the
19 resource database because it can connect to it. You
20 know, whether it has to be part of it or right next to
21 each other, that really does not matter, to be honest.

22 BY MR. LU:

23 Q. So as long as it can connect to the network,
24 you're saying it doesn't matter if it's right next to it
25 or far away; correct?

1 A. I would say that for the -- in the context of
2 this patent or in terms of what it teaches, really,
3 that's not the important thing to consider.

4 Q. Okay. So latency is not an important thing to
5 consider?

6 A. Yeah, depend on how you define latency. How
7 are you -- are you rendering -- are you rendering
8 animation that you cannot suffer any delay versus, yeah,
9 just sending data over there, just like you read news.

10 Q. What sort of data are you -- is the dynamic
11 firewall controller using?

12 A. I'm talking about these kind of latency --
13 normally, it really, really matters if there's a very --
14 in computer terms would be very hard, real-time
15 requirements, meaning that you have to respond within
16 sort of hard limit. I just don't see in the context of
17 this patent. So that's why whatever network latency
18 talking about to me is inconsequential to teaching on
19 this patent.

20 Q. Let's turn to -- let's go to the Wang reference
21 again and turn to paragraph 16.

22 A. Okay. Wang patent. Okay. Paragraph 16.

23 Q. So the first sentence, it says, "In some
24 embodiments, firewall configurations and policies
25 accessible and definable through the portal may be

1 driven by a resource database 103 or a customer database
2 105."

3 Do you see that?

4 A. Yes, I see that. Yes.

5 Q. Now, it does not say here that the dynamic
6 firewall controller 102 can access configurations from
7 the database; correct?

8 A. I think early on we said something about -- let
9 me see. Go back to my declaration. We talk about --
10 let me see. I talk about, let's say -- in paragraph 74,
11 right, I say, "Additionally, these generated policies
12 were stored in database 103 as database records." So
13 obviously there's a way that the policies generated by
14 the dynamic controller will be transmitted and stored in
15 the original -- in the resource database 103.

16 Q. Okay. But in paragraph 74 of your declaration,
17 you're not actually testifying that the firewall
18 controller generates policies and stores them in
19 resource database 103; right?

20 A. Hold on. So I mean, in paragraph 73, right, we
21 talk about, you know, the -- I say that -- you know, in
22 73 -- paragraph 73 on page 38 of my declaration, I said,
23 "Wang explained that its dynamic firewall controller 102
24 was configured for automatic firewall policy generation
25 and configuration." So, "In particular, Wang described

1 that dynamic firewall controller 102 processed any input
2 defining firewall policies and automatically configure
3 various aspects of a firewall and also took threat
4 inputs from threat intelligence systems, dynamic
5 generated [sic] and automatically configured the
6 firewall policies," and "also disclosed that its system
7 received a modification to the firewall policy" and
8 "modify the policy."

9 But, again, then go on to paragraph 34 [sic] to
10 say, "Additionally, these generated policies were stored
11 in resource database 103 as database records having
12 fields that reference specific firewall configurations
13 that were generated based on the user's requested
14 modification," as paragraph 16 of Wang says.

15 So really, what I say here in my declaration is
16 that, first of all, the controller gets input that's
17 request from the user and then generate firewall
18 policy -- a new firewall policy or policy modification.
19 And then if you look at paragraph 16 of Wang, it talks
20 about resource database storing, you know, firewall
21 policies.

22 So the question is that -- you know, naturally,
23 POSITA would say, yeah, where those policy come from?
24 Of course, you know, reading paragraph 73, you already
25 know the policy was generated by the dynamic firewall

1 controller, at least the updates; right? Wouldn't the
2 updates also be stored in the database? Of course.
3 Because so the next time you want to make more request
4 for changes, you base on what you have. What you have
5 should be the updated policy. I mean, that's, like,
6 obvious. So obvious.

7 Q. So going back to paragraph 50 of your
8 declaration, looking at Figure 1.

9 A. Okay.

10 Q. Do you see those boxes on the -- or let me know
11 when you're there.

12 A. Paragraph 50. Okay. Yep. All right. Yeah.
13 The boxes. Which boxes?

14 Q. So on the left-hand side, you see client device
15 104, 106, 108.

16 Do you see that?

17 A. Yes.

18 Q. And you colored those in purple; correct?

19 A. Yes.

20 Q. Now, each of these client devices has a portal
21 inside of it.

22 Do you see that?

23 A. Yes, I see that.

24 Q. So when Wang 16 -- paragraph 16 says "firewall
25 configurations and policies accessible and definable

1 through the portal," isn't it talking about the portal
2 on these client devices?

3 A. I believe so, yes.

4 Q. And I believe you previously testified that
5 these configurations -- let me just pull up what you
6 testified.

7 You said, "What I say here in my declaration is
8 that, first of all, the controller gets input that --
9 request from the user and then generate firewall policy,
10 a new firewall policy or policy modification. And then
11 if you look at paragraph 16 of Wang, it talks about
12 resource database storing, you know, firewall policies."

13 Did I read that right?

14 A. Yes.

15 Q. So it's your opinion that at the client device,
16 when a client uses the portal to create or modify a
17 firewall policy, it will send that to the firewall
18 controller rather than directly store it in a database?

19 Is that -- is that your testimony?

20 MR. KLEIN: Object to form.

21 THE WITNESS: So if I read paragraph 16, right,
22 "In some embodiments, firewall configurations and
23 policies accessible and definable through the portal may
24 be driven by a resource database 103 and/or a customer
25 database 105." So what really happen here is that if

1 you call it -- what I said -- what did I say, 73 --
2 about -- you know, the input getting from the -- so when
3 I say 102, the controller getting the input, I think 106
4 here is that -- you know, when the user want to define
5 some of the, you know, changes and send a request of the
6 policy change to the controller, it can reference the
7 resource database.

8 That's -- that's all a POSITA would agree.
9 That's how, you know, this should be understood. And
10 that's why in Figure 1, you see that the portal and the
11 resource database, they're connected through the
12 network.

13 BY MR. LU:

14 Q. I guess I'm just trying to understand --
15 well -- so in Wang paragraph 16, when it talks about the
16 resource database, it does not ever mention the
17 controller; correct?

18 A. So Wang 16 talks about what information 103 and
19 105 would have. Right? And then first sentence talks
20 about -- you know, it has something to do with firewall
21 configurations and policies. So the way I would say is
22 that if a user bring up portal, say, hey, let me take a
23 look my current firewall policy configurations so that I
24 can decide what change I need to make, you know, he may
25 just connect to resource database, customer database,

1 yep, here's what you have.

2 And as explained in 16, here are the kind of
3 services that you subscribe to, here's kind of security
4 you want to provide, and then you decide, do you want to
5 add stuff? Do you want to change stuff?

6 I mean, that's the purpose of paragraph 16.
7 That's how I see it.

8 Q. Okay. But paragraph 16 does not ever mention
9 the firewall controller accessing the database; correct?

10 A. So, again, on the -- in paragraph 18, it talks
11 about, "Referring generally again to Figure 1, the
12 dynamic firewall controller 102 may process any input
13 defining policies passed from the portal to the dynamic
14 firewall controller 102 and automatically configure
15 various aspects of the firewall."

16 So really, I mean, you know -- so it goes on to
17 say, what are the changes you make and then also -- so
18 the point is following; right? It's clear that 102, the
19 firewall controller, makes changes based on input passed
20 from the portal, which, you know, the user can use the
21 portal to define that. And as the beginning of the --
22 the first sentence, 16 -- paragraph 16 says, you know,
23 you may use the resource database and the customer
24 database to locate the current policy and configuration
25 and customer information, right, to make a -- whatever

1 the appropriate or necessary request for changes.

2 The point is that after changes have been made,
3 a POSITA would absolutely agree that it's obvious that
4 then you want to update your database -- your resource
5 database, your customer database, reflecting the updated
6 policies, configurations, which paragraph 18 talks
7 about -- what changes to your configuration based on the
8 new policy. Right? So those things have to be
9 reflected in the database, so the next time you want to
10 take a look and request for changes, you're base on
11 whatever current -- the current has to be updated
12 current.

13 That's what I'm trying to say. So to me, it
14 would be so obvious for a POSITA to -- to see that
15 the -- the policy -- the new policies -- updated
16 policies produced by 102 and the new configurations will
17 be stored in the resource database. Otherwise, why do
18 you need it there? It's completely outdated. What's
19 the point of the database? It doesn't make any sense
20 otherwise.

21 Q. Okay. I understand that. You're saying --
22 you're testifying -- well, let me re-ask it this way.

23 So my question is -- I guess I'm not quite
24 clear based off of your declaration what you think --
25 what device you think is storing the configurations in

1 the resource database.

2 You previously testified that the client device
3 through the portal will access the database to get the
4 current configuration so that they can be displayed or
5 can be updated; correct?

6 A. Yeah. The database have information --
7 database records may -- so again, if you read the
8 paragraph 16, second sentence, "Stated differently, the
9 resource database 103 may store firewall policies as
10 database records having fields that reference specific
11 firewall configurations."

12 So that's what I'm trying to say is that the
13 resource database is called resource database for a
14 reason. It stores some information about the
15 configuration -- some of the information about a policy
16 that is useful for user to take a look and request the
17 appropriate updates, which the controller 102 will
18 perform, and that will result in new policies and new
19 configuration changes to your device. But that
20 information then should be reflected in your resource
21 database so the resource database is up to date, so then
22 next time when you try to take a look and request any
23 necessary changes, you are -- you're based on up-to-date
24 information. That's -- is obvious.

25 Q. Right. I understand that. I'm not asking any

1 questions about what's stored on resource database. I
2 just want to know simply -- or rather let me ask it this
3 way.

4 Wang, in paragraph 16 or paragraph 18 or really
5 anywhere in the reference, does not ever say that the
6 dynamic firewall controller can access the resource
7 database; correct?

8 A. I can check. Let me double-check.

9 Q. Sure. Take your time.

10 A. Let me look at my declaration. Okay. So
11 again, I'm going back to paragraph 50. At the moment,
12 although I did not find a specific reference explicitly
13 talking about transmitting or storing the updated
14 firewall policy to the -- to the resource database --
15 but to me is, like, you know, I think POSITA would agree
16 that the resource database need to be up to date.

17 And if, like paragraph 16 says, it contains
18 fields that indicates configuration and policy, that
19 means it need to be up to date. That means whatever the
20 updates that that dynamic firewall controller produces
21 will be stored there. You say, hey, did the dynamic
22 firewall controller push that, transmit that? To me, a
23 POSITA would say, that's such a minor detail. Any
24 POSITA would say, yeah, if you want to do that, yeah --
25 if you want the code, I can do it.

1 To me, it's obvious that things don't just
2 magically show up. I mean, if I say yes, the data has
3 to be up to date, stored there, that means, yes, most
4 logically, the dynamic firewall controller, after
5 generating the updates, validating the updates, would
6 store it after making changes, of course, to the end
7 device according to the new configuration -- new
8 firewall and all that would be making -- would be
9 storing the new configuration in the resource database.

10 To me, that's a -- a minor detail that would
11 not affect how POSITA understands the teaching of Wang.
12 Seriously.

13 Q. All right. So you said -- oh, are you done?

14 A. I'm saying that -- you know, I -- I did not
15 find explicitly Wang say it or not saying it. And if
16 you can point to me either way, I would take a look.
17 But to me, that's not important. It's --

18 Q. Well, I mean, I agree that Wang does not
19 explicitly say the controller --

20 A. Hold on. Hold on. On the other hand, I would
21 say looking at Figure 1, it talks about resource
22 database 103 and dynamic firewall controller 102,
23 they're connected through communication network. So
24 that's what I'm trying to say is so obvious to be able
25 to do this. Any POSITA would agree it's so obvious.

1 In particular, when the need to keep up to
2 date, when the need to store the latest updates to the
3 resource database so obvious, then, of course, you have
4 a network connection -- yeah, sure, just do it, what's
5 the big deal. Transmit it to it.

6 Q. I guess -- you said it's -- it would be so
7 obvious. What would be so obvious?

8 A. I said many times the -- it's very obvious the
9 need to keep the resource database up to date reflecting
10 the current firewall configuration policy, according to
11 paragraph 16. Yes. I said this many times.

12 Q. Yes. I agree.

13 A. So when you try to make request for changes,
14 you actually, you know, talking about the current
15 situation, so -- which means logically, when the
16 firewall -- dynamic firewall controller makes changes
17 and the changes are implemented locally to your subnet
18 or devices, that has to be reflected in the database --
19 resource database, so that next time when you try to
20 make more changes, again, you are using the up-to-date
21 information.

22 Again, it's very obvious that in order to keep
23 the information up to date, you need to keep up with the
24 updates. Right. So then the question is, well, Wang
25 did not explicitly say that the firewall controller

1 transmit or update the database. To me, that's, like,
2 so obvious next step that people -- a POSITA would do.
3 Why? Because logically, dynamic firewall controller
4 makes those changes. So it has today's version of the
5 firewall policy updates --

6 Q. Okay.

7 A. -- and the configuration, so and so forth, and
8 it can connect to the resource database through the
9 network. So it would be obvious and easy for POSITA to
10 do this. That's my opinion.

11 Q. All right. You keep saying -- so your
12 testimony is that the resource database needs to have
13 the most up-to-date configurations.

14 And so that would mean any changes by the
15 controller would also be reflected in the resource
16 database. My question is --

17 A. Hold on. Hold on. I want to qualify to say
18 that the database records in a resource database that
19 concern you. Let's say you are device 104. Let's say
20 in some particular case, you have a special records
21 that's really concern you. Yeah, for those things --
22 that change that affect you, yes, those things needs to
23 be up to date to you so that you can use it. Right?

24 Q. Okay.

25 A. What I'm trying to say is that if the changes

1 are to a completely different -- a different place, you
2 may not need to see it. So anyway, those are details
3 that, again, it's not important. But the key principle
4 is that the resource database should reflect the current
5 firewall policy and the current configuration. That's
6 so obvious.

7 Q. Okay. But, Dr. Lee, paragraph 16 doesn't say
8 that the controller makes any changes. It says,
9 "Firewall configurations and policies accessible and
10 definable through the portal may be driven by a resource
11 database."

12 So isn't this saying that it's the portal --
13 the client device through the portal that makes changes
14 to firewall configurations; correct?

15 A. Well, for that, I'm going to refer you to some
16 other places either in the -- in the patent or the -- or
17 the -- or my declaration that talks about portals being
18 used to make changes. So I am at this moment somewhat
19 out of sync with some of the pages. Let me see. Let me
20 see here. So can you repeat the question again or the
21 comment again so I can --

22 Q. Sure. My question -- so my question is: In
23 Wang, paragraph 16, it says, "In some embodiments,
24 firewall configurations and policies accessible and
25 definable through the portal" -- through the portal --

1 "may be driven by a resource database 103 and/or a
2 customer database 105."

3 And then if you look at paragraph 18, it says,
4 "Referring generally again to Figure 1, the dynamic
5 firewall controller 102 may process any input defining
6 firewall policies passed from the portal to the dynamic
7 firewall controller 102."

8 So my question, Dr. Lee, is: Isn't Wang saying
9 that it's the portal that makes changes to firewall
10 configurations, and then it's the portal that sends
11 those configurations to the controller? The controller
12 never accesses the database for those configurations;
13 correct?

14 A. Again, I'll try to -- I'm -- let me -- give me
15 a moment to sort through all the patents in front of me.
16 I think I'm completely out of sync now with all these
17 things. Let me just reshuffle all my documents. I
18 think that's '941. I apologize.

19 Okay. I may have '941. I really apologize
20 because we've shuffled around. It just completely threw
21 me out of sync.

22 Q. That's all right. So why don't I try to make
23 this a little simpler for you. I'm just looking at the
24 Wang reference. You don't need to worry about anything
25 else.

1 A. Okay.

2 Q. So Wang -- let's look at paragraph 16. Right?

3 A. Okay. Paragraph 16. All right. Let me see --
4 try to find paragraph 16 of Wang. That's where I'm --
5 how could it be -- paragraph 16.

6 Q. Let me know when you're there.

7 A. I couldn't even find the whole page. Maybe
8 it's, like, stuck somewhere in my declaration. That's
9 my guess. Yeah. It's bad. I should have stick with
10 them.

11 MR. KLEIN: Do you want to take a break so he
12 can collect his docs?

13 THE WITNESS: Yeah. Give me two minutes. I
14 just shuffle all of them together maybe. Yeah.

15 MR. LU: Okay.

16 (Off the record.)

17 MR. LU: Back on the record.

18 BY MR. LU:

19 Q. Okay. So, Dr. Lee, let's -- I'll try to keep
20 this simple. You only need to have Wang in front of
21 you.

22 A. Okay.

23 Q. Of course you can always refer to your
24 declaration if you want.

25 A. Okay.

1 Q. So paragraph 16 of Wang, the first sentence, it
2 says, "In some embodiments, firewall configurations and
3 policies accessible and definable through the portal may
4 be driven by a resource database 103 and/or a customer
5 database 105."

6 Do you see that?

7 A. Yes. Yeah.

8 Q. Do you agree that Wang says that firewall
9 configurations are accessible and definable through the
10 portal?

11 A. Yeah, through a portal, yeah, and portal
12 normally is accessible to the users too. Yeah. I mean,
13 I can see that. Yes.

14 Q. And you would agree that this does not say that
15 the firewall controller can define or access any
16 firewall configurations; correct?

17 A. So not in paragraph 16, but then in paragraph
18 18, right, it talks about how you automatically
19 configure the firewall -- various aspect of the
20 firewall.

21 Q. Sure.

22 A. Yeah.

23 Q. Yeah. We can go to paragraph 18. So in
24 paragraph 18, it says, "Referring generally again to
25 Figure 1, the dynamic firewall controller 102 may

1 process any input defining firewall policies passed from
2 the portal to the dynamic firewall controller 102 and
3 automatically configure various aspects of a firewall."

4 Do you see that?

5 A. Yep. So first of all, that means that
6 normally, at least what is being said in paragraph 18,
7 the dynamic firewall controller gets the input defining
8 the policy -- firewall policies from the portal.

9 Q. Right.

10 A. And then, of course -- then it goes on to
11 update.

12 Q. Right. So paragraph 18 says, "The input that
13 defines the firewall policies is passed from the
14 portal"; correct?

15 A. Yes.

16 Q. It does not say that the firewall controller
17 defines the firewall policy; correct?

18 A. It didn't say one way or the other; right?
19 Meaning that it gets the input defining the policy --
20 firewall policy. That means -- from the portal -- and
21 then the question -- then really means if you ask, hey,
22 what's being transmitted from the portal? Firewall
23 policies.

24 Does it mean that dynamic firewall controller
25 would not add or modify or improve some of the policies?

1 It did not say so one way or the other. In fact, let me
2 read the next sentence. "Dynamic firewall controller
3 102 may also take threat inputs from threat intelligence
4 systems, e.g., the "reputation" at Level 3 [sic],
5 dynamically generate proper firewall policies and
6 automatically configure the firewall policies for
7 customers who subscribe to threat protection service."

8 So what really it says here is that -- this
9 input -- the user say, hey, I would rather have this
10 type of protection. And they say, here's my request for
11 some kind of new firewall policies. And then the
12 firewall controller say, yeah, I got it, but I need some
13 information. Tell me how you define your policy,
14 improve your policy to even better and more proper
15 protection. That's what the sentence says.

16 So my point is that, you know, just because the
17 input from portal is policy doesn't mean that dynamic
18 firewall controller itself does not, you know, produce
19 or define new policies.

20 Q. Okay. Understood. And again, it's your
21 opinion that even though Wang does not disclose it, the
22 firewall controller will upload these policies to the
23 resource database through the communications network?

24 MR. KLEIN: Object to form.

25 THE WITNESS: Yeah, I think -- I think I said

1 this multiple times. If you read paragraph 18 as a
2 whole, right, it talks about, you know -- you know, more
3 specifically -- in the middle of paragraph 18, "More
4 specifically, the dynamic firewall controller 102 may
5 automatically make one or more application program
6 interface API" --

7 (Reporter clarification.)

8 THE WITNESS: -- "programming interface, API
9 calls to a network configuration system engine, NCS 112,
10 and/or a firewall configuration system engine, FCS 114.
11 The NCS 112 includes logic for configuring various" --
12 "various aspects of the routers and switches of a
13 subnet, or otherwise, that may require configuration in
14 accordance with the firewall policy."

15 And then, "For example, if the firewall policy
16 involves a subnet, the firewall policy may include
17 configurations for router that defines an address,
18 network ID, subnet ID, subnet mask, and the like, any of
19 which may be needed to manage network traffic to and
20 from the subnet." In some -- "In other embodiments, the
21 NCS 112 may configure firewall device directly."

22 So I mean, it goes on in -- paragraph 19 also
23 talks about an FCS also -- make changes to the various
24 aspects of firewalls that require configuration. So
25 really, a POSITA reading paragraph 18 would agree that

1 the dynamic firewall controller, as I said in the -- in
2 the first sentence -- at the end of -- at the end of the
3 sentence, right -- it says "automatically configure
4 various aspects of the" -- of a firewall according to
5 new policy, essentially.

6 So that's well understood, you know. And then
7 give examples of through the API calls to the NCS and
8 FCS to -- you know, to change -- you know, to change the
9 logic or the configures -- so then the logic for the
10 devices and the subnets and so on.

11 So really what I'm trying to say is that
12 paragraph 18 talks about getting input from the portal,
13 improving the policy, making changes, okay, by directly
14 causing some changes, including some new configuration.
15 So then the point is if you read 16, when the portal's
16 being used to, let's say, define -- to look at the
17 current policy configuration or make requests for
18 changes, you are -- you want to refer to resource
19 database 103, then obviously resource database 103
20 should include those new changes, including the new
21 configurations, as indicated in paragraph 18.

22 MR. LU: All right. Give me one second. All
23 right. I pass the witness.

24 MR. KLEIN: All right. Give us about 15
25 minutes just to run through our notes, but if we have

1 any redirect, it won't be much.

2 THE WITNESS: Okay. 15 minutes.

3 MR. KLEIN: Yeah.

4 THE WITNESS: Okay. All right. Thank you.

5 (Off the record.)

6 MR. KLEIN: Mr. Lee, we have no questions.

7 Thank you for your time.

8 THE WITNESS: Okay. All right. Thank you.

9 MR. LU: Thank you, Dr. Lee.

10 THE WITNESS: Thank you.

11 MR. KLEIN: Thanks, Quincy. Do we have
12 anything to handle?

13 MR. LU: No, Dr. Lee, you can leave. Rachel,
14 can I get a rush on both the rough and the final?

15 (Discussion off the record.)

16 THE REPORTER: Mr. Klein, did you want a copy?

17 MR. KLEIN: Yes, please.

18 (The proceedings were concluded at
19 2:41 p.m.)

20

21

22

23

24

25

1 CERTIFICATE OF STENOGRAPHIC REPORTER

2
3
4 I, RACHEL N. BARKUME, a Certified Shorthand
5 Reporter of the State of California, hereby certify that
6 the witness in the foregoing deposition,

7 WENKE LEE,
8 was by me duly sworn to tell the truth, the whole truth,
9 and nothing but the truth in the within-entitled cause;
10 that said deposition was taken at the time and place
11 therein named; that the testimony of said witness was
12 stenographically reported by me, a disinterested person,
13 and was thereafter transcribed into typewriting.

14 Pursuant to Federal Rule 30(e), transcript
15 review was requested.

16 I further certify that I am not of counsel or
17 attorney for either or any of the parties to said
18 deposition, nor in any way interested in the outcome of
19 the cause named in said caption.
20

21 DATED: July 30, 2023.

22
23 

24 Rachel N. Barkume, CSR No. 13657, RMR, CRR
25

WITNESS SIGNATURE PAGE

I, WENKE LEE, do declare under penalty of perjury under the laws of the State of California that the foregoing is my deposition under oath; are the questions asked of me and my answers thereto; that I have read the deposition and have made the necessary corrections, additions, or changes to my answers that I deem necessary.

_____ I have no changes to my deposition.

_____ Following are the changes I wish to make:

Page	Line	Change
------	------	--------

_____	_____	_____
-------	-------	-------

_____	_____	_____
-------	-------	-------

_____	_____	_____
-------	-------	-------

_____	_____	_____
-------	-------	-------

_____	_____	_____
-------	-------	-------

_____	_____	_____
-------	-------	-------

_____	_____	_____
-------	-------	-------

_____	_____	_____
-------	-------	-------

_____	_____	_____
-------	-------	-------

_____	_____	_____
-------	-------	-------

23

24 _____

25 SIGNATURE

DATE

\$	105 48:10,17 49:16 59:21 123:12 132:9,11 133:25 139:2 142:25 143:19 152:2 154:5	189 123:17,18 126:1,4 128:17	21 61:11 62:8 64:4	38 94:19 112:19, 20 139:22
\$600 9:3,5,6,11, 22		19 30:24 41:21 131:9 133:22 134:2 157:22	210 46:18 47:5 52:4,15 62:5 63:1 65:9,11,16,18,24 66:17	39 94:21
1	106 141:15 143:3	19.5 100:17	212 46:18 47:5 52:4,15 62:5 63:1	4
1 31:8 34:3 39:1,2 50:6 55:3 101:1,2 124:21 135:5,23 141:8 143:10 144:11 148:21 152:4 154:25	108 141:15	1980s 20:2 30:9 102:9 107:6 108:2 113:4,13	214 46:18 47:5 52:4,15 62:5 63:1	4 116:8 133:22 134:2
100 10:20,24 69:15,18 124:8,9	11 18:12 112:1	1989 19:6,9,16 20:20,22 29:7,8, 17,18	216 46:18	40 25:21 120:12, 20,23 121:5 123:13 132:8
1001 113:24	112 55:16,18 56:2 72:9 78:8 81:10, 23 157:9,11,21	1990 30:9	218 61:24 64:23 65:10,14,19,21 66:12,17	401 116:8
1002 14:11,14 18:10 43:12 54:2	114 55:17 157:10	1990s 30:24 37:19 107:23 108:25 113:6 131:9	24 43:18	402 116:22
1004 45:23,25 47:11 61:9 68:6	122 44:11 66:5,8 135:16,19	1996 33:9 41:24	24/7 49:7	403 117:2 118:8
1005 114:8,16	130 136:10	2	26 4:1 44:2 64:12, 16,17 68:9,15 71:1 73:23 77:16 78:5,6 80:15 82:14 87:20 92:15 96:5,13,14	404 120:2
1006 114:8,16	136 14:16,18	2 31:9 44:1,10 46:20 47:2 64:13 66:15 123:24 126:5 128:19	27 121:13	450 9:15,17,20,21
1008 109:10 115:25	15 102:19,20 158:24 159:2	20 17:5 46:3,8 47:2 124:3,8 125:5,20	28 121:13	49 115:20,22 120:1
102 54:10,17 55:3,5,7,14 56:17 57:16,18 58:14 135:9,17,18 136:1 139:6,23 140:1 143:3 144:12,14, 18 145:16 146:17 148:22 152:5,7 154:25 155:2 156:3 157:4	16 17:3,21 47:12, 13,20 50:6 52:5, 17 53:2,11 59:9, 14,17,23 95:2 138:21,22 140:14, 19 141:24 142:11, 21 143:15,18 144:2,6,8,22 146:8 147:4,17 149:11 151:7,23 153:2,3,4,5 154:1, 17 158:15	2000s 17:7	29 120:8,11,17,20, 23,24 121:3 123:13	4C 123:9,15,20 133:15,17
103 47:21,22,23 48:9,17 49:13,16, 18 50:4 58:21 59:1,5,12,20 60:8, 23 61:4 94:23 136:3 139:1,12, 15,19 140:11 142:24 143:18 146:9 148:22 152:1 154:4 158:19	166 109:16 113:19	2005 17:9,11	2:41 159:19	5
104 123:2 141:15 150:19	167 114:14	2018 20:3,5	3	50 25:21 134:25 135:1,24 141:7,12 147:11
	17 17:3,22 111:23 112:2 133:21 134:1	2021 12:14	3 18:11 55:9 121:4 156:4	52 45:9
	18 54:13,22,23 56:6,10,24 57:15, 21 58:4,14 59:6 60:2,7,9 82:2 144:10 145:6 147:4 152:3 154:18,23,24 155:6,12 157:1,3, 25 158:12,21	2023 4:2	34 105:22 106:20 140:9	55 43:16,17 64:12, 16,18 135:14
	188 123:2 128:6	2023-00030 14:14 45:24	35 128:25	56 53:24 54:6,19 64:15,17
		204 44:23 46:17 61:16,21 62:3,12 65:10,12,22,24 66:13,17	36 18:10,12,25 21:11 22:16 28:22 112:23,24,25 113:3,10,12,16 121:3,24 130:7,21 131:19,24 132:15, 21	6 17:9,11 50:6
		206 44:23 46:17 61:16,21 62:3,12 65:19,22 66:13,18	37 33:3 112:19,20, 23,24,25 113:5, 10,13,18 121:5	67 111:10
		208 44:23 46:17 61:16,21 62:3,12 66:13,18		7
				7 46:4 47:14
				70s 107:9
				73 139:20,22 140:24 143:1

74 60:20,21 94:21 95:7,18 139:10,16 7B 109:19 110:11 111:2,11 113:21 114:7 8 8 46:7 73:24 80 122:1,12 130:8, 14,16,17,18,23,25 131:2,3,11,25 132:16 133:6,8,10 134:7 8080 131:6,12 80s 107:21 108:18 9 93 109:16 94 109:18 941 5:6 14:5 44:20 60:18 95:9 123:8,10,15,20 124:2 125:2 129:3 130:3 133:7,15,21 134:2 152:18,19 9:02 4:2 A a.m. 4:2 absolutely 5:25 90:19,21 91:4 98:6 133:1,3 145:3 abstract 135:20 access 19:10 49:7 103:10 107:18 108:3 110:2 111:3 112:7,8 114:17, 19,20,24 115:18 117:4,8,9 120:4 121:14 130:19 139:6 146:3 147:6 154:15	accesses 152:12 accessible 59:10,19 138:25 141:25 142:23 151:9,24 154:3,9, 12 accessing 144:9 accordance 55:20 57:4 114:17 157:14 accurate 6:10 achieve 85:21 ACP 114:22 121:1,7 128:15 ACPS 114:18,19 115:17 116:10,16, 20,23 117:2,9,22 118:8,25 120:3 122:11 123:5,6, 10,20 126:12 127:11,21 128:8 129:11 ACR 114:13,18, 19,21 120:25 121:6 126:5,15 127:15 128:5,18 ACRS 115:17 116:10,16,20,23 117:2,9,21,22 118:8,25 119:18 120:3 121:9,15 122:8,10,15,16, 18,19,20,21 123:5,7,10,20 126:2,6,8,11,14 127:11,20 128:8, 14 129:11 action 34:13 35:7 37:17 38:15 39:4 42:9 activities 63:5,8 82:23 108:9 activity 61:22 62:4 actual 72:15,23 73:3,4,5,11,18 79:19 80:17,25 96:24 97:8,10,13 126:23	add 33:6 51:12 144:5 155:25 adding 92:17 additional 121:21 Additionally 60:22 94:21 139:11 140:10 address 21:13, 15,17,20,21 22:2, 5,6,12,17,21,24 23:1,3,6,7,12,14, 23 24:1,6,13,18 26:7,11,15,17,18 27:8,13,16,17,22, 24 28:4,15 37:10 55:24 107:13 132:6 157:17 addresses 22:2 26:24 27:1 administrator 22:1,23 116:9,20 117:21 119:17,18 administrators 33:6 admitting 19:15 affect 77:3 81:12, 17,24 82:19 119:3,8,16 148:11 150:22 affecting 82:22 age 99:6 100:5 101:2,13 agree 19:20 20:9, 15 28:22 31:25 32:10 41:23 42:11 50:3 51:1 52:3 53:14 58:10 61:5 66:23 70:14 76:14 79:5 98:1,3,7 103:13 108:17 110:12 112:13,17 117:13 121:9 122:4,8 124:5 126:10,14 132:23 143:8 145:3 147:15 148:18,25 149:12 154:8,14 157:25	agreements 18:4 ahead 7:22 11:14 41:21 63:16,17 72:6 74:9 104:17 118:4,5 alert 34:14 35:7 37:18 39:5 alive 97:22 allowed 19:3 76:3 108:11 114:25 115:1 131:11,22 analyze 75:12 76:9 analyzed 74:1,15 and/or 55:16 56:25 59:20 68:20,21,23 74:3 81:12,18,25 96:19 108:10 116:10,20 123:5,6,20 142:24 152:1 154:4 157:10 Andrew 13:8,9 Angeles 129:4 animation 138:8 annotated 44:1, 15 46:21 64:13 109:19 135:4 anticipate 42:23 AP 110:3 API 55:15 56:11, 18,21 157:6,8 158:7 APIS 56:16,19,25 57:6 apologize 152:18,19 appeared 4:5 appearing 12:1 appears 24:12 application 55:15 109:10 157:5	apply 76:6 architect 36:6 area 29:25 112:10 114:9 arrangement 54:9 ARS 128:19 art 5:13 articulates 49:20 aspect 154:19 aspects 54:12,17 55:6,18 56:6 57:2, 19,25 58:17 60:5 140:3 144:15 155:3 157:12,24 158:4 assertion 44:18 associate 24:17 assume 8:25 24:19 46:11 50:21 58:5 117:25 118:1 assuming 21:20 27:10 AT&T 25:13 29:9, 20 ate 102:18 Atlanta 4:5,17,18 attack 76:1 107:5 attorney/client 15:14 attorneys 13:2,6, 14 14:3 attribute 98:22 105:14,15 attributes 98:16, 18 99:5,22,24 authenticated 115:5 authentication 84:23 authorized 112:5 automatic 56:7,9 68:21 77:19 96:17
---	---	---	--	--

139:24 automatically 21:11 54:12,17,20 55:6,10,14 56:5, 11,12,14,19,25 57:9,12,19,24 58:11 60:5 72:25 93:9 117:14,25 118:1,9,18,20 119:12 120:7 140:2,5 144:14 154:18 155:3 156:6 157:5 158:3 aware 29:15 awareness 107:4	32:16,17,24 34:10,14 35:4 36:11 37:9 40:6 42:10 48:8 50:5, 11,22 54:24 55:2 57:15 60:20 62:8 65:11 71:14 75:23 77:17,20 79:11,13 80:15 81:21 82:4 85:9 87:5 95:5,10 102:3 107:10,14 111:12,13,15 112:15 113:2 115:13 122:11 123:17 125:12,23 128:7 131:7,21 132:21 133:23 bed 73:3,11 75:19 83:22,25 84:2,3,6, 7,14,15,18,22 85:9,15,16 89:16, 17,22 94:10,11,13 beds 73:18 84:17, 21 85:4,7,11,25 87:12 88:14,19, 20,24 89:12 90:3 93:2,4 began 17:6 beginning 57:15 62:7 144:21 begins 18:11,12 behalf 4:7 behaviors 61:15 62:11 Bell 29:9 belong 106:24 big 29:19,20 30:6, 9 103:15 149:5 billed 10:7,15 11:25 biometric 85:2,3, 15 86:17 biometric-based 84:23 block 21:11,21 22:2,8,9 32:1 35:9 63:22 64:7 65:9, 12,16,18 76:6,18	116:8,22 117:2 118:8 120:2 121:25 122:12 130:8,14,16,17 131:10,17,19,24 132:18 133:6 blocked 75:8,15 blocking 19:15 130:21 132:3,16 133:8,12 blocks 132:24 blue 44:16,18 66:4 109:23 111:8,17 Board's 14:8 bottom 49:4 73:23 boxes 141:10,13 boys 25:23 branch 46:12 branches 46:16 break 42:16,21 43:1,2 44:25 67:23,25 102:13, 14,15 103:23,25 110:21 111:16 134:9,13,21 153:11 breaks 41:2 bring 143:22 BU 125:20 bubbles 111:9,17 build 37:21 83:24 building 4:23 37:20 bunch 90:11 business 61:17 62:13 button 119:19 Buzz 124:15 Buzzcard 124:16	C California 4:4 30:14 call 20:24,25 21:2,7 39:21 57:6 67:11 91:22 93:13 95:8 115:10 124:14 125:15 143:1 called 4:7 26:12 37:20 50:23 114:24 146:13 calling 56:16 calls 15:13 55:15 56:11,18,21,25 157:9 158:7 capture 74:24 75:12 76:9 captured 74:1,15 care 40:23 89:18 105:18 118:21 129:24 137:17 carefully 62:6 cares 41:6 case 7:14 8:15 10:4,25 11:9,13 14:15 17:2 18:5 27:18 42:6 56:17 67:10 75:24 77:5 86:4,16 89:16 97:9 105:13 111:12,15 118:13 120:4 128:15 131:24 132:16 150:20 cases 6:20,22,25 7:1 17:7 92:23 118:15,16 causing 158:14 caution 18:2 center 49:6,21 Certified 4:3 cetera 41:2 104:5 110:3 112:9 128:21	Chambers 5:7 14:5 109:10,11,19 110:10 111:10,24 112:2 113:8 114:15 115:12,16, 20,23 116:15 119:14 120:9,12, 17 122:22,24 123:11,13,20,23 124:19,25 126:6, 11,14 127:15 128:8,19 129:20 130:7 131:16 132:2,23 133:5,18 Chambers' 123:5 126:2 change 70:23 74:1,18 83:1 96:10 143:6,24 144:5 150:22 158:8 character 104:21 charge 9:24 check 45:19 71:5 72:9,13 76:4 83:9, 13,20 86:17,18 95:22 96:9,22 97:1 108:6 147:8 checking 96:15 97:1,4 Checkpoint 33:8,13,16,21 39:24 40:2,13,17 checks 108:6,24 109:1 Chicago 45:14 46:13 choice 25:9 86:10 choose 40:20 86:9 125:17 circles 109:23 110:1,7,9 circumstances 76:22 Cisco 7:18 19:9, 11
--	---	--	---	---

citation 19:13	collect 153:12	company's 30:2	18:4	connected 24:16 26:6 27:6 114:8 136:7,9,11,13,15, 17 137:7 143:11 148:23
cite 113:4	colon 41:2 121:25 123:24 124:3,21 125:4, 18,20	compare 123:15 124:13 125:11	configuration 50:8,10,12,20 51:8,14 52:10 53:19,20 55:16, 17,20 57:4 63:19 67:3 68:19,22 70:9 77:19 92:21 95:22 96:18 139:25 144:24 145:7 146:4,15,19 147:18 148:7,9 149:10 150:7 151:5 157:9,10, 13,24 158:14,17	connection 132:16,19 149:4
cited 62:17 135:19	color 44:6,16 46:22 113:24 135:7	comparison 123:8	configurations 47:24 49:20,22 50:2,16 51:3,19, 22 52:2,3,14,18 53:4,14 55:23 57:8 59:10,18 60:25 69:10 72:1 94:17,24 95:14 122:7 138:24 139:6 140:12 141:25 142:5,22 143:21,23 145:6, 16,25 146:11 150:13 151:9,14, 24 152:10,11,12 154:2,9,16 157:17 158:21	consistent 123:7
citing 113:2	Colorado 46:12	compat- 127:9	configure 23:16 28:14 29:2,3 55:6, 11 56:2,5 57:19, 24 58:11,17 60:5 116:9,20 140:2 144:14 154:19 155:3 156:6 157:21 158:3	constitute 24:9
city 46:13 129:3, 8,21	colored 46:21 66:4 109:22 113:23 135:8 136:4 141:18	compensated 8:13 10:3	configures 54:17 117:21 158:9	constituted 123:5
claim 96:2,4	coloring 44:15	compensation 8:16	configuring 55:18 57:2 157:11	consulted 17:21
claimed 44:20 123:5	column 49:4 98:11,18,21,25 99:2,9 100:3,4,6, 22 101:1,2,22 133:21 134:1	complete 129:17	connect 27:23,24 84:10,11 108:5 131:3 136:24 137:3,19,23 143:25 150:8	content 49:8,9,21
claims 60:18 119:5	columns 38:19 98:8 99:15 101:20	completely 105:17 145:18 151:1 152:16,20		context 10:4 50:9 52:20 56:15 58:13 62:19 63:14 69:16 74:8 77:16 78:5 82:14 93:17 105:12 113:1 138:1,16
Clara 30:6,14	combined 110:9	complexity 69:21,23,25		continue 43:20
clarification 21:5 32:14 35:2 37:13 50:24 67:7 84:25 105:4 157:7	comma 39:3,4,5 40:4,22 41:1 42:4 125:5	complicated 22:18		continuing 49:17
clarify 80:6	command 131:4	computer 26:3,7 27:12 69:13,19 105:9 108:9,10, 12,19,20,23 114:23 119:9,12 138:14		control 19:2 20:10,14,15 22:12 29:3 114:18,19, 20,24 117:9
class 88:18 101:15	commencing 4:2	computer- implemented 119:6		controller 54:10, 17 55:3,5,7,14 56:18 57:16,18,22 58:11,14 60:3,4 135:8,17,18 136:1,6,14 137:3, 5,13,18 138:11 139:6,14,18,23 140:1,16 141:1 142:8,18 143:3,6, 17 144:9,12,14,19 146:17 147:6,20, 22 148:4,19,22 149:16,25 150:3, 15 151:8 152:5,7, 11 154:15,25 155:2,7,16,24 156:2,12,18,22 157:4 158:1
classes 37:6,23 88:19	comment 151:21	computers 29:25 30:13 106:23,24		controls 109:5
clean 5:4,5,6,7,9 6:1	commonly 73:13	concept 30:22 31:1 113:4 114:23		convenient 63:21
clear 59:5 144:18 145:24	communicate 27:11 30:1	concepts 113:12		
click 119:19	communication 25:16 106:22 136:9 148:23	concern 77:5,6,7 150:19,21		
client 112:5 116:10,16,17,21 117:10 141:14,20 142:2,15,16 146:2 151:13	communication s 108:9 156:23	concerns 77:7,9		
close 10:21,24 13:21,22 17:5	communology 67:4	concluded 159:18		
closely 11:7	companies 7:24 30:9	conclusion 66:21		
cloud 44:11 66:5, 7 135:16,18	company 103:15 114:17 115:19 117:5	conditions 70:20 71:6 75:25		
code 105:2 127:1, 2,7 129:14,15 147:25		Conferencing 4:3		
Coie 8:7,11,17 11:5 13:5 17:15 45:1		confidentiality		

convey 124:12	18:21	20 73:24 74:13, 17,21 76:5 87:9 98:2 99:1,9,15,18, 24 100:3,6,22 101:17,20 103:18 104:4,9,21,24,25 105:3,6,8,9,10 108:10,20,23 127:25 128:1,14, 16 138:9,10 148:2	deal 115:14 149:5	definition 105:14 114:25 122:16,20 126:23 127:12
conveying 125:8	correctly 9:3,14 13:12 19:18 33:10,19 34:5,21 74:5	database 47:20, 23 48:9,10,16,17, 20 49:13,18 50:4 58:21 59:1,4,5,11, 20,21 60:1,14,23, 24 61:3,4 94:23 95:5,10 97:23,25 98:1,4,7,9,10,12, 15,17,20,22,23,24 99:1,20,23 100:3 101:2,4,5,10,11, 19,21 102:2,4 103:3,12,19 104:25 105:2 124:14 136:3,7,15 137:3,5,13,19 139:1,7,12,15,19 140:11,20 141:2 142:12,18,24,25 143:7,11,16,25 144:9,23,24 145:4,5,9,17,19 146:1,3,6,7,9,10, 13,21 147:1,7,14, 16 148:9,22 149:3,9,18,19 150:1,8,12,16,18 151:4,11 152:1,2, 12 154:4,5 156:23 158:19	decide 84:11 143:24 144:4	delay 138:8
copies 5:4,10,16, 20	counsel 10:13 13:4 16:11 45:1 67:23 104:11,14	DDOS 134:5	decision 14:7,8,9	delete 33:7
copy 5:5,6,7,9 44:5 109:9 159:16	counsels 15:7		deck 40:16	delivery 49:8,21
corporate 64:2	country 29:23		declaration 5:4, 13 9:7,12,19,21 14:4,12,25 15:6, 10,21 16:3,8,19 18:7,9,19 33:3 43:12,18 44:5,9 45:10 53:25 54:25 60:15,20,21 61:6 64:11 94:18,20 105:22 106:20 109:14 112:19,23 122:23 123:2,18 126:4 133:25 134:25 135:13 139:9,16,22 140:15 141:8 142:7 145:24 147:10 151:17 153:8,24	Denver 45:13 46:12
correct 6:4,23,24 11:12,17,18,24 14:10 16:19 17:23,24 20:12,16 21:25 22:3,4 23:9, 23 24:9,13 26:4,5, 20 27:8,9,13 30:16 31:4,16 33:13,14,15,18 35:15 38:8 39:13, 25 40:1,14 41:25 44:16,23,24 45:7, 15 46:18,25 47:21 48:13,22 50:17 54:18 57:25 58:1, 20 59:1,12 63:2,8 64:24 65:10,19 66:5,9 68:16 69:4, 5,11 70:15 71:11, 16 72:16,20 73:12,20 75:21 76:16,23 77:10 78:25 79:8,19 81:19 82:10 83:4, 16,23 85:16 86:6, 18 87:25 88:14 91:20 93:6,7,18 98:9,18 99:9 100:7,11,23 106:2 108:21 109:20,25 111:3,4,6 112:14 113:25 114:6 116:17 121:1,7, 10,18 122:17,20 124:11,24 126:24 127:17 128:5,21, 24 129:8,9 131:18 132:1,4 133:8,9, 12 135:5 136:4,7, 15 137:25 139:7 141:18 143:17 144:9 146:5 147:7 151:14 152:13 154:16 155:14,17	couple 13:16 82:13 134:18		depend 92:4 122:7 138:6	depending 22:4, 10,19 23:1,4 26:13 27:14 29:2 31:18 32:8 35:19 52:20 53:5,8 63:18 67:2,18 87:13 89:15,20 99:19
Corrections	court 7:1,4 14:7,8 34:17 43:21		declarations 11:16	depends 36:4 52:8,25 53:8 63:23 64:2 69:15, 21,23,25 76:19 86:20,24 87:5,24 88:10 89:24 92:7 100:14 101:25 121:21,22 136:8
	cover 111:16		default 51:3	depict 36:23 38:7
	covered 15:14 18:3 82:12		definable 59:10, 19 138:25 141:25 142:23 151:10,25 154:3,9	depicted 66:14, 20
	covers 37:11		define 67:3 81:6 98:24 99:1,8 100:3 101:2,20 105:8 126:15 132:24 138:6 143:4 144:21 154:15 156:13,19 158:16	depicts 33:24 44:10 111:2
	crazy 89:2		defined 99:16 100:22	deploy 23:16
	create 116:16 142:16		defines 55:24 98:8,15,17 155:13,17 157:17	deployment 23:4
	created 106:21		defining 54:11 55:4 57:17,22 58:15 140:2 144:13 152:5 155:1,7,19	deposed 11:22
	crosstalk 7:20			deposition 5:14 6:10,12,18 9:2,4, 9,14,17,22,25 12:2,22,25 13:3,7, 15
	current 36:9 111:21 143:23 144:24 145:11,12 146:4 149:10,14 151:4,5 158:17			depositions 8:5, 11
	customer 46:11 47:25 48:7,9,12, 17,22 49:5,19 52:9,21,22 53:5,6 57:10 59:20 60:1 61:13,17 62:9,13 139:1 142:24 143:25 144:23,25 145:5 152:2 154:4			describe 20:6 21:10 81:16 83:15
	customers 55:11 156:7			
	cute 125:21			
	D			
	daily 73:4			
	data 19:2 49:6,7,			

85:14 99:23 113:10 describes 47:20 61:15 62:11 68:15 69:6 73:19 120:24 describing 50:14 62:5 69:2 72:18 78:23 79:5,15,17 design 40:9 designated 45:24 designed 112:4 destination 26:20 34:11,22 35:1,4,6 36:17,18 37:10 38:14 39:3, 4 40:4 42:8 destinations 19:7 detail 7:3 72:1 81:1 147:23 148:10 details 23:3 36:12 80:14 83:19 99:19 103:21 105:18 119:15,21 121:22 151:2 detect 61:21 62:3 63:5,13 detecting 63:7 detection 8:4 38:13 84:24 determine 81:11, 17,23 82:18 87:9 developed 19:17 development 18:16 19:1 device 24:12 25:8 26:4 34:7,22 35:12,13,17,21,25 36:15 66:2 67:16 110:2 114:15 121:14 141:14 142:15 145:25 146:2,19 148:7 150:19 151:13 157:21	devices 24:9,10 25:19 26:14 35:23,25 44:11 56:3 66:5,7,13,24 68:23 72:24 74:4 78:10,19 79:3,14, 18,19,20,23 80:22 81:12,18,25 87:5 96:19 111:3 112:5,7 115:18 116:10,17,21 117:4,8,10 120:4 135:15,18 141:20 142:2 149:18 158:10 DHCP 26:12 difference 114:21 differently 124:17 146:8 digest 123:7,9, 16,19 133:23 digests 123:6 directly 28:3 56:3 136:7,8,14 142:18 157:21 158:13 disagree 40:15 disclose 18:3 156:21 disclosed 140:6 discloses 94:16 95:14 96:5,7 117:20 disclosure 15:14 118:24 discrimination 19:11 discuss 16:12 53:22 discussed 53:11 59:7 112:18 discussion 159:15 display 39:16 41:12,13,15 displayed 146:4	displaying 39:17 distinction 7:3 district 7:1,4 dive 43:6 docs 153:12 document 5:24 15:4 16:16 21:4,6 33:19 documented 108:7 documents 5:2, 17 14:2 152:17 domain 21:12,18, 19,20 22:3,7,9,13 27:22 61:23,24 62:4,17 64:7,23 65:2,10,14,19 66:12 131:18 132:3,12,19,25 domain's 22:1 double 125:18,19 double-check 147:8 doubles 104:5 download 5:19 37:21 123:24 124:9 125:1,18 dozens 10:11,19, 20 11:9 draft 15:5,8,10,20 16:3 draw 14:23 15:3 66:21 driven 59:11,20 139:1 142:24 151:10 152:1 154:4 dry 72:9,13 73:7, 10 86:2 87:10 96:8,22 Due 107:3 duly 4:8 dynamic 54:10 55:3,5,7,13 56:17	57:16,18,21 58:10,14 60:3 135:8,16,17 136:1,6 137:2,13, 18 138:10 139:5, 14,23 140:1,4,25 144:12,13 147:6, 20,21 148:4,22 149:16 150:3 152:4,6 154:25 155:2,7,24 156:2, 17 157:4 158:1 dynamically 55:9 156:5 E e-mail 107:13 108:1 e.g. 61:14 62:10 108:9,13 112:7 156:4 earlier 38:25 39:23 83:6 early 12:11 17:7,9 107:20,23 113:3 139:8 easier 5:23 47:10 95:22 easily 30:6 easy 28:25 150:9 eat 102:12,16,17 Ebase 103:11 effect 82:6,9 97:8,13 effectively 49:23 50:8,13 51:7,20, 23 elaborate 22:14 electronic 5:19 14:21 electronically 15:1 element 72:23 73:1 80:21 96:2,4 elements 38:2,6	72:16,20,22 73:3, 5,8,18,20 74:3 78:18,25 79:2,7, 10,12,21,25 80:8, 11,13,16,17,24 81:4,12,18,25 82:3,6,9,17,19 85:12 87:3 92:16 97:2 109:5 122:13 embodiment 46:16 68:18 69:8 78:7 embodiments 56:2 59:18 71:20 114:11 138:24 142:22 151:23 154:2 157:20 emulate 78:19 79:3,12,13,18,22 80:21 87:4 88:4,7 emulates 89:22 emulating 78:24 79:6,10 enable 49:7 end 19:8 50:6 58:6 120:1 125:4 148:6 158:2 endeavor 8:2 enforce 117:9 127:24 enforced 78:5 enforces 82:21 engagements 17:22 18:1 engine 55:16,17 157:9,10 engineering 62:15 engineers 40:17 ensure 25:2 enter 115:8 enterprise 26:21 29:5,19 32:2,7 44:19 52:9,11,20 65:2,6 108:5,13 109:23 110:8,9,
---	--	---	--	---

14,15,17 111:9,20 114:6,12,16 115:19 117:5 135:12,16 136:23	126:1,14,17,18 128:23 129:10,11, 19 130:2 158:7	91:15 99:8 118:2, 13 119:23 120:25 131:21,23 133:10 147:12 148:15,19 149:25	20,21 65:3 66:15, 16,23 109:19 110:11 111:2 113:21 114:7 116:8 123:9,15,20 126:5 128:19 133:15,17 135:5, 23 141:8 143:10 144:11 148:21 152:4 154:25	60:3,6,8,13,25 61:14 62:10 63:3, 9,11,12,14,15,22 64:1,5,7 65:9,11, 16,18,23,24 68:16,19 69:1,4 72:10,14 73:25 74:2,14,17,21 75:10 76:2,5,13, 14,22 77:2,14,21 78:9,24 79:7 81:9, 22 82:15 83:8,22 84:5 85:19,23 86:10,16 88:3,13, 21,25 89:4,6,13 90:3,6,8,10,11,25 91:10,15 92:23 93:14 94:2,4,7,17, 24 95:14 96:23 106:1,4,6,8,10,13, 14,15 109:2,4,7 111:5 112:15 113:3,6,12,15,17 115:14 121:10,12, 15,17,25 122:4,6, 7,9,11,14 127:17 130:8,14 131:21 132:15,18 133:2,5 135:8,17,18 136:1,6,14 137:2, 13 138:11,24 139:6,17,23,24 140:1,2,3,6,7,12, 17,18,20,25 141:24 142:9,10, 12,17,22 143:20, 23 144:9,12,14, 15,19 146:9,11 147:6,14,20,22 148:4,8,22 149:10,16,25 150:3,5 151:5,9, 14,24 152:5,6,7,9 154:2,8,15,16,19, 20,25 155:1,2,3,7, 8,13,16,17,20,22, 24 156:2,5,6,11, 12,18,22 157:4, 10,14,15,16,21 158:1,4
enterprise- network-facing 32:17	excerpt 126:13 excerpts 123:22 exchange 106:23 excluded 17:19 excuse 8:23 18:11 22:11 23:6 28:21 104:13 execute 74:23 78:8 82:17 executed 81:10, 22 82:5 execution 73:25 74:14,17,21 exhibit 5:16,22 6:1 14:11,14 18:10 43:12 45:23,25 46:1,4 47:11 54:2 61:9 68:6 109:9 115:25 exhibits 5:15 exist 20:22 existed 20:20 expect 75:7,14 76:1 77:2 87:7 88:8 105:11 113:15 expected 74:3 75:23 expert 12:5 17:2, 6,18 18:6 33:3 97:15 explain 38:11,25 41:11 48:25 54:24 82:8 111:11 explained 110:11 114:14 115:16 139:23 144:2 explains 56:5,9, 24 133:15,22 134:3 explicitly 58:4 63:11 64:4 73:8	extension 51:16 extent 15:12,13 56:4 127:3 external 23:7 24:11 25:8 26:15, 25 61:23 62:18 F fabric 109:4,5,7 face-based 84:23 fact 25:15 104:3, 20 105:7 156:1 fairly 97:24 fake 4:24 fall 12:13 familiar 97:24 98:4 103:3,18 104:3,20 farm 30:19 farms 30:19 fashion 38:20,21 40:6 FCS 55:17 57:1 157:10,23 158:8 feature 15:3 field 8:2 98:1 101:6,7,12,13,15 129:3,8,21 130:7 131:17 133:6 fields 39:9 41:3, 11 60:24 94:23 98:11 99:23 125:13 126:7 128:20,24 140:12 146:10 147:18 figure 33:12,15, 19,24 36:22 38:6 44:1,10,15 46:20 47:2 55:3 64:13,	filed 11:11 filtering 19:15 final 159:14 finalize 32:22 find 22:7 27:18 29:13 37:8 83:19 121:12 132:17 147:12 148:15 153:4,7 fine 42:17 68:1 99:12 102:22 finish 102:23 finished 62:22 68:13 74:11 firewall 19:9 21:25 22:1,16 23:14,17,20,23,25 24:8,17,18,24 25:3,10,11,14 27:15 28:2,7,19 29:17 30:7 31:3,4, 5,9,11,15,21 32:1, 11,16 33:7,25 34:23 35:9,11,16 36:2,5,18,23 37:2, 5,8,20,24 38:3,6, 7,10,11,20,23 39:8 40:5,7,18,25 41:7,16 42:3,4 46:17,24 48:2 49:22 50:2,7,10, 16,20,22 51:2,13, 14,19 52:3,11,14, 17 53:13,20 54:10,11,12,16,18 55:3,4,5,6,7,10, 11,13,17,21,22,23 56:2,6,18 57:5,16, 17,18,20,21,23,25 58:5,7,10,14,15, 20,25 59:4,9,18	60:3,6,8,13,25 61:14 62:10 63:3, 9,11,12,14,15,22 64:1,5,7 65:9,11, 16,18,23,24 68:16,19 69:1,4 72:10,14 73:25 74:2,14,17,21 75:10 76:2,5,13, 14,22 77:2,14,21 78:9,24 79:7 81:9, 22 82:15 83:8,22 84:5 85:19,23 86:10,16 88:3,13, 21,25 89:4,6,13 90:3,6,8,10,11,25 91:10,15 92:23 93:14 94:2,4,7,17, 24 95:14 96:23 106:1,4,6,8,10,13, 14,15 109:2,4,7 111:5 112:15 113:3,6,12,15,17 115:14 121:10,12, 15,17,25 122:4,6, 7,9,11,14 127:17 130:8,14 131:21 132:15,18 133:2,5 135:8,17,18 136:1,6,14 137:2, 13 138:11,24 139:6,17,23,24 140:1,2,3,6,7,12, 17,18,20,25 141:24 142:9,10, 12,17,22 143:20, 23 144:9,12,14, 15,19 146:9,11 147:6,14,20,22 148:4,8,22 149:10,16,25 150:3,5 151:5,9, 14,24 152:5,6,7,9 154:2,8,15,16,19, 20,25 155:1,2,3,7, 8,13,16,17,20,22, 24 156:2,5,6,11, 12,18,22 157:4, 10,14,15,16,21 158:1,4 firewall's 24:13 27:13 32:3 Firewall-1 33:8, 13,16,21 39:24

40:3,13	96:10,15 97:1,5,6, 7,11,14 98:21,23 101:4,6 122:23 123:15,21 125:7, 8,12,24 126:9,12, 15,21,22,23 127:2,3,8,12,13, 16,24 128:1,2,4,5, 10,15,24 129:12, 13,16,21,24,25 130:4	G	good 4:12 5:21 50:21 51:3 67:21, 24 72:3 91:21 131:5	156:9
firewalls 18:17 19:1,5,6,16,23,24 20:1,3,5,10,13 21:10 22:11 23:8 28:23 33:5 37:4, 19,22,23 41:24 47:5,6 52:4,6,15 53:3,15 57:12 58:2,3,12,18 62:5 63:1,7 88:17 91:12 106:16 112:8,14,17,18 113:9,10 121:18, 20 157:24	formats 39:22 95:18 122:24 127:21	gateway 28:13	grab 43:22	higher 9:24
firms 8:8,9	formatted 38:20, 24 40:6 122:17 123:21 126:3,6,8, 12 128:9,19	gateways 19:11 25:5	grade 101:12,16 105:16	highlighted 123:14
fixed 23:13,14 24:1,6	formed 95:23,24	gave 73:10 75:13 87:12 95:3	graphical 36:13 37:25 39:21 41:13 113:5,14	highlights 5:10
float 105:17	Fortinet 8:19 11:12	general 18:6 37:3 50:21 77:13 100:21 114:23	great 44:8 47:9 90:8 135:23	historical 130:24 131:13
floats 104:4	found 123:4 125:21	generally 18:1 55:2 144:11 152:4 154:24	green 46:22	hold 15:12 18:11 32:23 60:12 139:20 148:20 150:17
flow 20:10	foundation 104:7,15	generate 50:20 55:10 60:5 140:17 142:9 156:5	guarantee 69:18	home 4:21 25:11, 14,19 26:4,9,17 27:3,7,18
focus 51:18,22	Fourth 101:15	generated 60:22 61:3,4 94:22,25 139:11,13 140:5, 10,13,25	guess 89:11 97:6 102:12 143:14 145:23 149:6 153:9	honest 23:24 36:5 69:22 90:10 121:23 137:21
follow 47:10 127:24 128:5 129:12	frame 17:10,11	generates 139:18	GUI 36:12 37:25	hope 13:11
forgot 21:3	Friday 13:25	generating 148:5	H	host 19:10
form 8:21 20:23 24:14 28:9 29:25 31:17 34:9,24 35:18 36:3 41:5 42:1 53:17 54:21 56:8 57:13 58:23 59:2 66:10 67:1 70:17 71:17 74:19 76:7 77:11 88:15 92:12 95:16 101:24 104:12,14, 15 106:12 112:21 117:16 118:11 119:1 127:18 137:14 142:20 156:24	front 5:2 43:13 44:6 46:1 152:15 153:20	generation 139:24	half 102:18,23	hour 9:3,5,6,11, 15,18,20,22,23 11:6 42:15
format 36:23 37:1,8,24 38:3,6, 7,12 39:2,11,13, 16,17,18,19,20, 21,22 40:4,13,19, 25 41:7,9,14,16, 25 42:3,5,10,11 94:17 95:12,15,23	full 4:13 127:3 133:23	geographic 112:10	hand 89:21 148:20	hourly 9:1 10:2
	full-time 97:24	geographical 45:6	handle 159:12	hours 10:11,19, 20,24 11:10,25 13:21,22 26:12 42:23
	function 28:10, 13 78:19 79:3,13, 22 80:21 87:4 112:4	geolocation 45:20	handwrite 14:20, 22	house 31:13
	functionalities 28:8 113:16	geolocations 111:13	handwriting 14:23	huge 131:1
	functioning 94:4	Georgia 4:5,17 124:15	handwrote 14:24	human 62:15 117:14,22 118:9, 25 119:10,13
	functions 20:6 59:25 84:5	give 51:4 58:6 62:14 90:13 128:7 152:14 153:13 158:7,22,24	happen 75:8 120:6 142:25	I
	funneling 105:25 106:3	giving 6:10 101:8 120:5	happened 120:6	i.e. 19:2,15
		global 64:1	happening 120:6	IBM 29:20
		goal 85:20 96:22, 25 108:22	happy 53:22	ID 55:24,25 101:13 105:15 124:14,16 126:7 128:25 129:1 132:9,11 157:18
			hard 138:14,16	ID,' 128:21
			heard 103:6	idea 72:3 131:5
			heck 107:15	
			hey 23:13,25 39:7 70:12 88:3 94:6 101:2,5 119:19 132:18 143:22 147:21 155:21	

identifies 49:19	129:12,23 131:17	input 54:10 55:4	157:6,8	IP 19:12 21:13,15,
identify 24:17	133:24 134:4	57:17,22 58:15	interfaces 33:6	17,20,21 22:2,5,6,
73:2	157:16 158:20	60:4 75:23,24	internal 25:8 27:1	21,25 23:3,6,7,12,
Illinois 46:13	included 68:19	83:11 87:9 88:2	28:2,18	13,14,25 26:7,11,
illogical 68:21	69:10	140:1,16 142:8	internally 26:16,	14,16,24 27:1,8,
70:9 77:19 92:21	includes 20:16	143:2,3 144:12,19	23 28:12 105:7	13,15,17,22 28:4
96:17	55:18 57:1 65:13	152:5 155:1,7,12,	International	37:10
illustrated 46:15	78:17 79:2,11,21	19 156:9,17	7:19	ipads 25:25
123:19 126:5	80:11 87:3 91:7	158:12	internet 19:4	iphones 25:25
128:18	110:2 118:25	inputs 55:8 140:4	20:16,18,20 23:9,	IPR 6:25 7:3 10:8,
image 33:17	129:21 157:11	156:3	12 24:1 30:2 32:9	16 11:12,17,23
imaginable	including 38:12	inside 66:8	84:11 90:15	12:5 14:14 17:13,
107:24	49:6,21 50:7	137:13 141:21	106:21,22 107:6,	16 43:12 45:23,24
imagine 36:14	77:18 158:14,20	install 93:22	11,17,19,21	IPS 21:23,24
39:8 52:10 118:14	inconsequential	installation	108:2,11,20 114:9	irrelevant 118:20
impact 75:9	138:18	127:23	120:4 136:25	ISP 26:10
92:19 97:10	incorrect 115:9	instance 80:20	137:9	ISPS 26:13
implement 19:17	indication 120:5	107:9 108:4	internet-facing	issue 76:15,18
61:14 62:9 78:2	individual 67:15	institution 14:9	22:21,25 23:2	issues 76:22
104:25 115:2,4	infer 99:5 100:4	instructions	27:15,17 32:16	
122:6 128:12	infers 99:6	74:1,14,18,22	internet-scale	
implementation	information	instructs 117:22	107:5	J
31:13 80:14 81:1	15:14 27:21 37:7,	integer 100:11,23	interpret 71:24	
100:15 102:1	8 38:1 39:16 40:7,	101:1 105:17	72:7 127:6 131:25	job 32:3,5
implemented	21 42:8,12 48:16,	integers 104:4	133:16	July 4:1
69:4 74:3 130:14	20,21,24 49:12,	Intel 29:21 30:5,	interpreting 34:5	
149:17	15,18,19 55:1	12	intervention	K
implementing	66:20 74:23,25	intelligence 55:8	117:15 119:14	
68:18 71:20	75:2,3 97:9 99:19	140:4 156:3	introduce 90:25	key 37:7 38:2
important 99:12	101:3,8,14,17	intend 77:22	91:9,14,25 93:21	86:24,25 87:1
100:14,19 101:3	102:1 106:23	89:14	introduced 92:8	89:2 151:3
102:3,5 105:13	124:13 125:8,10	intended 76:13,	94:5	keys 98:13
118:18 132:14	134:3 143:18	15,23,25 82:21	intrusion 8:3	kick 119:20
138:3,4 148:17	144:25 146:6,14,	83:2,10 90:5	38:12,13	kind 18:7 21:3
151:3	15,20,24 149:21,	intends 77:22	invoice 8:18	27:21 32:12,18,24
improve 155:25	23 156:13	78:1	invoices 8:20,24	40:7 45:19 48:15,
156:14	infrastructure	interact 35:23,25	involve 73:11,17	24 49:15 70:8
improving	106:22	interested 85:12	88:20,21 121:20	75:22 76:8 86:3,
158:13	infringing 7:24	interesting	involved 8:8,9	21 87:6,9 88:9
inclined 80:23	Ingres 97:21	133:17,19	17:22	97:23 101:16
include 12:1	103:10	interface 23:8	involves 55:22	105:16 115:10
55:23 58:2 77:9	inherent 39:19	33:8 36:13 38:1,2	58:7 78:24 79:6	119:24 125:24
80:16 85:25 93:15	initial 14:6 49:22	40:10 41:13 55:15	88:20 127:22	129:14 138:12
102:2,3 112:13,18	50:1,7,16,20 51:2,	113:5,14,17	157:16	144:2,3 156:11
113:9 125:10	8,13,19 52:14	116:8,16,19	involving 53:9	kinds 84:15,17,21
126:6 128:20	53:13			85:4 89:12

Kit 37:20	12,17	location 30:4,19, 21 111:19 136:21	112:22 117:19 118:23 119:4 128:3 134:9,13,17 137:22 143:13 153:15,17,18 158:22 159:9,13	66:12 88:4,6 89:23 90:4
Klein 8:21 10:9 13:9 15:12,23 16:6,9,20 18:2 20:23 24:14 28:9 31:17 34:9,24 35:18 36:3 41:5 42:1 43:3,6 53:17 54:21 56:8 57:13 58:23 59:2 66:10 67:1 70:17 71:17 74:19 77:11 88:15 92:12 95:16,25 96:12 99:3,10,17 100:9,12,24 101:24 102:16,20, 25 103:5,14,20 104:6,13,22 106:12 112:21 117:16 118:11 119:1 127:18 137:14 142:20 153:11 156:24 158:24 159:3,6, 11,16,17	latest 149:2 law 8:8,9 layer 61:14 62:10 layman's 98:19 layout 125:9 lease 26:12 leave 159:13 Lee 4:6,12,15 6:12 9:1 12:4,22 14:18 15:13 19:21 34:16 43:11 68:5 102:16 103:3 134:18 151:7 152:8 153:19 159:6,9,13 Lee's 43:7 left 38:18 39:7 40:8,22 123:14 125:11 133:5 left-hand 126:13, 19 129:7 130:6 141:14 legit 89:24 90:5 Level 55:9 156:4 levels 105:18 likewise 115:14 126:17 130:3 limit 64:4 104:11 138:16 limitations 108:25 listed 123:9 listing 126:5 128:18 litigation 7:1 live 94:7,13 local 19:3 20:19 29:25 75:9 137:8 locally 149:17 locate 144:24 located 4:15	logically 148:4 149:15 150:3 logs 76:4 long 13:19 42:20 47:17 93:13 102:7 112:6 136:17 137:23 longer 42:24 looked 14:5 37:4 103:16 lookup 27:21,22 Los 129:4 lot 25:22 38:19 73:2 74:23 107:23 118:13,14 131:20 lower 9:15 LU 4:11 7:21 8:22 10:12 15:19 16:1, 7,17,24 18:8 21:1, 9 25:1 28:20 31:24 32:20 33:1 34:15 35:8,24 36:21 38:4 41:18 42:13,15,18,22 43:9,10 51:10 53:23 56:13 58:24 59:8 66:22 67:14, 25 68:3,4 70:22 72:5 75:1 77:24 85:1 88:23 93:1 95:20 96:3 97:3 99:7,14 100:1,10, 20 101:18 102:6, 11,22 103:2,8,17, 22 104:11,17,19 105:20 106:17 110:20 111:1	lunch 102:13,18, 24 M MAC 126:8 128:21 132:5 machine 28:4 36:19 131:5 machines 72:2 132:19 made 68:23 96:19 145:2 magically 148:2 mailing 107:12 main 27:24,25 28:10 maintain 47:24 major 107:5 make 18:18 23:18 25:7 28:16 31:7, 10 45:8 55:14 56:11 74:8 76:12 78:3 90:14 92:15 106:5 111:15 116:4 141:3 143:24 144:17,25 145:19 149:13,20 151:18 152:22 157:5,23 158:17 makes 59:24 144:19 149:16 150:4 151:8,13 152:9 making 28:1 72:15,19 77:20 82:2 96:24 148:6, 8 158:13 malicious 61:22, 24 62:4,17 63:5,8 64:7,23 65:1,10, 12,13,14,17,19,21	malware 84:3,7, 9,19 85:15 86:17 89:1,18,19 manage 56:1 67:19 157:19 management 113:24 114:3,5,7 115:18 116:9,19, 24 117:3 120:2 mandatory 71:13,15,19 manual 127:4 129:18 market 103:16 mask 55:25 157:18 matter 10:16 22:18 26:17,24 32:11 119:22 124:18 129:24 136:16,21 137:9, 16,17,21,24 matters 10:8 136:18,19 138:13 meaning 21:18 22:5,18 34:11 35:5,22 41:9 56:20 65:22 71:25 77:1 78:2 82:12 83:9 114:25 115:2 123:13 131:2 138:15 155:19 means 36:8 56:16 69:12 72:13 73:1 74:24 98:11, 12 118:20 124:8,9 127:11 130:13 131:22,23,24 147:19 148:3 149:15 155:5,20, 21 meant 23:10,11 88:11 mechanism 24:21 32:18 114:24 115:2,7, 10,11,14,15
knew 21:15 107:12				
L				
L-E-E 4:14 labeled 66:5 109:23 114:2 Labs 29:9 lack 107:4 LAN 114:8,16 136:20 language 99:20 127:1,3 133:18 laptop 25:15 26:2 27:11 67:20 large 112:4,9 larger 28:24 32:2 66:24 late 20:2 30:9,24 37:19 113:4,6,13 131:9 latency 138:4,6,				

mechanisms 108:12	modules 37:5	Netskope/ fortinet 11:23	114:6 135:16 136:23	objections 104:11,22
media 49:8	moment 18:22 147:11 151:18 152:15	network 8:3,4 19:2,3,4,6,11 20:11,17,18,19 21:12,17 22:12,17 23:19,20 24:8,10, 11,12,13,17,21,23 25:9,12,13,14,19 26:4,10,14,18,21 27:3,7,18,21 28:11,15,24 29:2, 3,5,25 32:2,8 36:1,6,14,19,20 38:12,13 44:19,22 45:12,13,15 47:25 49:3,6 55:16,24 56:1 61:14,15,22 62:10,11,20 64:2 65:2,6 66:8,19,25 67:3,10,19 72:16, 20,22,23 73:1,3,5, 8,11,12,18,19 74:3 75:24 77:3 78:18 79:2,10,18, 21,24,25 80:8,11, 12,16,24 81:4,6, 12,18,24 82:3,6,9, 17,19 83:1 84:4 86:18 87:3 92:16 97:2 106:4,7,15 108:3,12,13 109:24 110:2,8,9, 15,17 111:3,9,20 112:7,8 114:9,12 115:18 117:4,8,10 120:3 121:14 126:7 128:20 129:1 132:4 135:12,16,19 136:9,11,13,18,24 137:4,8,23 138:17 143:12 148:23 149:4 150:9 156:23 157:9,18, 19	news 138:9	objective 106:3, 5,8,9
medium 40:20	moments 129:10		nonprivileged 131:7	observe 84:9
meet 13:2,14,19	monitor 94:3		normal 75:25 88:8 89:22	obvious 29:6,7, 13 36:12 83:20 90:1 92:24 123:4 124:18 125:14,23 132:17,20,24 141:6 145:3,14 146:24 148:1,24, 25 149:3,7,8,22 150:2,9 151:6
meetings 13:24 14:3	monitoring 8:4		note 130:24 131:13	
megabits 123:24 124:21	monk 34:7,11,12, 22 35:1,4,6,12,13, 17,20,22,25 36:10,14,17		notes 5:2,10 158:25	
memory 12:17	month 26:13 92:3		number 5:16,22 6:1 9:16 10:10,17, 23 24:9 25:4 34:3 37:11 39:1,2 100:5,7 101:6,8, 13 105:15,16	office 4:21,22 45:6,12,14,15 137:1
mention 63:3 143:16 144:8	morning 4:12		numbers 19:12 37:11 112:4	older 91:11
mentioned 86:22 88:17	motivated 19:1		numerical 99:6	one's 115:15
method 119:6 135:15	mouse 14:22		numerous 112:9	online 33:20
Microsoft 14:22 15:2,3 103:10	move 109:8 131:6		O	open 107:6,7,8, 16 108:3
mid 102:8 131:8,9	multiple 11:5 13:14 23:16,21 30:21 46:16 51:13 53:10 109:5 115:18 117:3 157:1			operating 76:23
middle 112:3 116:7 157:3	Mysql 103:4			operation 73:5
minimum 83:20	N			opinion 62:2 64:6 65:1,8 94:16 95:13 110:7,8 114:5 117:20 118:24 119:3,8, 13,16 135:11 142:15 150:10 156:21
minor 147:23 148:10	NAD 112:16		oath 6:3	opinions 17:18
minutes 43:3 82:13 102:15,19 134:14 153:13 158:25 159:2	NADS 111:5 112:7,13 113:9 121:21		object 8:21 10:9 20:23 24:14 28:9 31:17 34:9,24 35:18 36:3 41:5 42:1 53:17 54:21 56:8 57:13 58:23 59:2 66:10 67:1 70:17 71:17 74:19 77:11 88:15 92:12 95:16 100:24 101:24 103:5,14 104:6,17 106:12 112:21 117:16 118:11 119:1 127:18 137:14 142:20 156:24	option 70:3
missed 78:13	naturally 140:22		objected 10:13	optional 69:7,9, 13 70:7 71:8,11, 13,19
misspoke 60:24	nature 7:16 22:10 63:19,23 64:3	network's 36:6 106:1	objection 15:12, 13,23 16:6,9,20 95:25 96:12 99:3, 10,17 100:9,12 103:20 104:14	optionally 70:3
mistake 131:1	NCS 55:16,17 56:2,25 57:1,7 72:9 78:8 81:10, 23 82:2,16 92:15 157:9,11,21 158:7	networking 29:11		Oracle 103:10,12, 15 104:3,20 105:6
mistranscribed 75:17	needed 50:16 56:1 157:19	networks 29:15 44:11 66:5 85:10, 16 106:25 111:2		Oracle's 103:19
modem 108:5	necessarily 86:4,16			orange 113:23,24 135:7,8
modification 94:25 140:7,14,18 142:10	needed 50:16 56:1 157:19			order 27:10,11 53:15 97:8 127:16
modify 33:7 116:16 121:10 122:9 140:8 142:16 155:25	Netskope 8:23 10:7,15 11:11,25 12:5 17:12			
module 88:18				

128:13 149:22	13 59:6,9,14,17, 23 60:2,7,9,19,21 61:11,19 62:8,21, 25 64:4,12,15,16, 17,18,19 68:9,12, 15 71:1 73:23 78:6 80:15 82:2, 14 83:17 87:1,20 92:15 94:21 95:7, 18 96:5,14 105:22 106:20 107:3 108:8 109:16 111:10,23 112:2, 19 113:3,18,19 114:14 115:22 116:2,7 119:23 120:1,8,17,24 121:4,13,24 123:2,13,17 126:1,4 128:6,17, 25 130:7,21 132:8 133:14,20,24 134:25 135:1,14, 24 138:21,22 139:10,16,20,22 140:9,14,19,24 141:7,12,24 142:11,21 143:15 144:6,8,10,22 145:6 146:8 147:4,11,17 149:11 151:7,23 152:3 153:2,3,4,5 154:1,17,23,24 155:6,12 157:1,3, 22,25 158:12,21	passes 89:4	person 13:10	114:18,20 115:3 121:10,19 122:9 138:24 139:11,13, 18 140:2,6,10,21 141:25 142:12,23 143:21 144:13 145:6,15,16 146:9,18 151:9,24 152:6 154:3 155:1,8,13,23,25 156:5,6,11,19,22
ordinary 56:20		password 115:8, 9	personally 88:13 90:13	
Oregon 30:5,13, 18,20		past 6:17	perspective 118:7	
organization 24:20,21,23 27:19,20 29:20 35:20 52:24 53:7 88:10 89:16 111:12,14,18		patent 4:7 5:6,7, 8,23 6:20,22 7:14, 23 11:2,7 14:6 17:2,7 44:20 47:2 53:19 54:23 59:7, 17 85:17 95:2,10 109:10 111:10 123:8,10,15,20 124:3 125:2 129:3 130:4 133:7,21 134:2 138:2,17, 19,22 151:16	petitions 11:12, 17,23 17:13,16	
organizations 30:3		patents 7:16,25 8:1,2,3 11:5,12 14:4 152:15	phonetic 67:4	
original 139:15		pay 31:9	physical 5:15 79:25 80:3,8,12 81:1,4 85:12	
otherwise- legitimate 82:23		paying 8:19,23	physically 29:24	
outdated 145:18		people 24:2 29:11 39:17 40:8 42:10 73:2 90:8 107:14 130:19 131:1,10 150:2	pick 5:24	
output 75:24 76:1 83:11		percent 69:15,18	picture 38:22,24 39:12	
oval 44:11,16,19 66:4		perfect 86:3	piece 127:1,2 129:14	
overlooked 108:14		perform 57:7 72:9 87:23 90:4 146:18	pink 136:4	
owner 4:7 14:6		performance 76:7 77:7 82:23	place 4:18 22:19 36:5 51:16 151:1	
owners 7:23		performed 117:14 119:9	places 35:21 51:13 53:1 151:16	
P		performs 90:5	plain 56:19	
p.m. 159:19	paragraphs 112:25 113:10 120:11,20,23 121:3,5	periodically 120:2	plenty 102:19	
packet 19:14 27:12	part 8:15 15:25 16:2,13 37:5 50:15 66:25 88:18 109:4,7 114:16 121:24 122:12 137:20	periods 112:6	point 25:6 32:13, 15,20,24 36:13 37:18,22 38:17 42:24 53:21 61:13 62:9 83:18 85:19 92:4 101:9 118:17 126:10 134:1 136:24 137:1 144:18 145:2,19 148:16 156:16 158:15	
packets 19:7,16 28:11	parts 111:18	Perkins 8:7,11,17 11:5 13:5 17:15 45:1	points 112:8	
pages 151:19	pass 89:7,9 158:23	permanent 26:11 27:8	policies 54:11 55:4,10,11 57:11, 17,23 58:7,20,25 59:4,10,18 60:13, 22 61:4,15 62:10 63:10 78:4 83:22 88:13,25 89:13 90:18,23 91:15, 20,24 92:2,17,18 93:2 94:22	
pairs,' 19:8	passed 54:11 55:4 57:17 58:15 144:13,19 152:6 155:1,13	persistent 116:23 117:23		
paper 90:7,13				
paragraph 18:10,11,12,25 20:6 21:11 22:16 28:22 33:3 43:16 45:9 46:3,8 47:2, 12,16,20 48:11 49:1,2 50:6 52:17 53:2,11,24 54:4,6, 13,19,22,23 56:6, 10,23 57:15 58:4,				

popular 103:12 port 19:12 37:10, 11 122:1,12 130:8,14,16,17, 18,23,25 131:1,2, 3,6,7,11,12,25 132:16 133:6,8, 10,12 134:7 portal 54:11 55:5 57:17,23 58:16 59:11,19 60:4 138:25 141:20 142:1,16,23 143:10,22 144:13, 20,21 146:3 151:10,12,13,25 152:6,9,10 154:3, 10,11 155:2,8,14, 20,22 156:17 158:12 portal's 158:15 portals 151:17 POSITA 28:25 29:6 32:10 40:23 41:6,22 42:7,11 48:15 50:19 51:1 52:8 56:20 66:23 69:16,17,19 71:22 72:21,25 82:24 83:6,9,13,19 88:7 89:25 92:22 101:9 105:18 110:12 114:9 118:7 123:4 125:11,23 126:10 127:10 128:11 130:11 132:15,17 140:23 143:8 145:3,14 147:15, 23,24 148:11,25 150:2,9 157:25 POSITA's 32:15, 24 109:3 possibly 42:9 107:21 potential 107:4 potentially 112:6 power 85:10,16 86:18 precise 9:16	predefined 94:17 95:12,15,18,23 96:10 121:7 123:21 126:9,12 128:9,24 129:12, 20,25 prefer 5:19 prep 9:8,22 preparation 9:6, 8 13:15 prepare 12:21,24 13:2,7 preparing 9:12 12:1 present 40:20 95:18 pretty 42:11 90:1 103:12 132:20 133:18 prevent 6:9 prevention 38:13 previously 17:21 76:12 82:25 83:21,24 88:12 93:5 100:4 105:25 142:4 146:2 principle 50:22, 25 64:9 73:7 75:22 91:21 108:22 110:12 151:3 print 5:5 printed 5:4,5 prior 5:13 19:16 private 101:14 privilege 15:15 privileged 131:2, 11 problem 43:24 proceeding 8:14 9:7,13 45:24 proceedings 12:5 159:18 process 15:25	16:2,12,13,16 55:4 56:18 57:16 58:15 68:15 69:6 70:1,6 71:2,7,10, 25 72:1,18 77:9 78:23 79:6 96:7 105:2,10 127:22, 25 128:14 144:12 152:5 155:1 processed 54:10 140:1 produce 156:18 produced 145:16 produces 147:20 profiles 35:21 program 105:2 157:5 programmer 97:22,23 105:1 programming 55:15 127:1 157:8 programs 105:10 progress 92:4 projects 73:17 proper 55:10 74:8 108:5,6 115:6,8 127:5,16 129:15 156:5,14 properly 94:4 95:23 105:9 proposed 68:16 72:10,14,19 74:2 78:8 81:9,11,17, 22,24 87:17 92:10 96:23 proposing 87:24 proprietary 49:7, 9 protect 32:5,6 106:4 protected 24:20 36:1 114:17 135:15 protecting 30:23 31:2	protection 31:3 55:12 67:22 134:5 156:7,10,15 protections 46:18 protects 24:8 46:25 protocol 19:12 22:5 37:16 38:15 39:4 42:9 protocols 106:22 provide 12:19 14:25 20:5 31:3 49:9,23 50:9,13, 17 51:7,20,24 53:16 106:21 115:8 122:16,19 132:2 144:4 provided 9:12 11:16 30:11 36:22 48:12,21 50:15 65:20 116:8,19 123:8,23 provider 48:2,6, 13 providing 8:16 34:21 52:22 53:9 116:15 provisioned 78:20 proxy 84:4,10 public 26:8 publicly-known 22:25 23:7 publish 90:7 pull 142:5 purchasing 49:5 purple 141:18 purports 33:12 purpose 66:16 76:10 144:6 push 147:22 pushed 53:14 pushing 53:19	60:8 put 16:22 28:17 30:7 31:21 32:25 40:22 53:1 67:21 70:5 77:1 80:20 86:7,19 97:7 106:4 107:24 123:12 125:3 Q qualify 150:17 question 10:14 11:8 12:23 15:9, 16,17 22:14 24:7 25:18 39:14 48:11 58:22 60:10,16 69:20,21 70:21 75:18 80:9 86:8, 14,15 90:2 91:11, 22 93:21 95:13 96:9 103:25 106:11 110:6 111:8,21 113:7,8 132:7 140:22 145:23 149:24 150:16 151:20,22 152:8 155:21 questions 43:7 44:1 47:4 68:8 120:20 134:10,19 147:1 159:6 Quincy 159:11 quote 19:7,8,9 44:10,19 82:9 115:20 120:25 125:3,4,19 quoted 54:25 quoting 54:13 78:8 R Rachel 4:3 159:13 ran 7:10 range 11:20 21:23 22:2 27:22 76:8
---	---	---	--	---

rate 9:1,24	received 140:7	region 29:24	45:12 99:24	13,20,21 147:1,6, 14,16 148:9,21 149:3,9,19 150:8, 12,15,18 151:4,10 152:1 154:4 156:23 158:18,19
rates 10:2	receiving 48:1 108:10	regular 97:17	representation 95:9,11	
re-ask 9:10 10:14 24:7 91:8 122:17 136:2 145:22	recognized 123:4	regularly 88:18 90:17,22	represented 8:7, 11	
reach 22:22 25:8 28:18 107:19	record 4:13,25 6:1 39:20 41:15 43:5 68:2 95:6 98:21,22,23 99:23 101:5,10 103:1 110:24 134:16 153:16,17 159:5, 15	regulation 108:25	represents 44:19	resources 61:20 62:15
reaches 28:2	records 60:24 94:23 95:10 139:12 140:11 146:7,10 150:18, 20	reject 34:6,13 35:7,12,16	reputation 55:9 156:4	respect 20:18 108:3
read 19:18 33:10 38:18,25 39:6 40:8 47:16 49:24 50:5 51:9 53:12 54:22 55:1 58:13 59:9,14,15,16 61:19,25 62:7,24 68:11 69:15,17 70:8,11,13,18 71:7,12 72:4,21 74:5,7 78:21 79:25 80:3,5 81:14,20 92:15 97:12 112:11 116:2,11 119:25 130:20,21 133:20 134:1 138:9 142:13,21 146:7 156:2 157:1 158:15	redirect 159:1	rejected 34:23	request 140:17 141:3 142:9 143:5 145:1,10 146:16, 22 149:13 156:10	respond 75:21 138:15
reading 36:17 39:8 59:13 60:9 69:8 70:25 71:4 72:25 74:11 116:4 118:7 120:14 136:10 140:24 157:25	reference 5:16 45:18,22 47:12 60:25 61:8 68:5 94:24 113:4,13 121:12 122:24 138:20 140:12 143:6 146:10 147:5,12 152:24	relevance 104:6, 15	requested 34:12 94:25 140:13	responded 83:2
reads 132:15	references 5:13	relevant 55:1 87:13 113:1	requesting 35:6 52:22	response 14:6 56:21
real 107:14	referring 5:12 24:6 47:7 48:5 53:6 55:2 73:7 80:12 111:13 114:3 116:7 121:13 144:11 152:4 154:24	remember 5:22 7:4,17 11:19 12:6, 18 14:1	requests 158:17	responsible 28:1,12
real-time 138:14	refer 5:14,25 19:23 47:5 57:14 63:1 72:23 151:15 153:23 158:18	REMEMBERED 4:1	require 55:20 57:3 119:5 157:13,24	rest 29:5 32:7 67:6,11
realize 131:1	reference 5:16 45:18,22 47:12 60:25 61:8 68:5 94:24 113:4,13 121:12 122:24 138:20 140:12 143:6 146:10 147:5,12 152:24	remind 43:21	required 48:2 49:22 50:8,12 51:19,23	result 146:18
reason 6:6 56:24 130:20 146:14	references 5:13	remote 114:6 135:11,18	requirement 129:16	retained 12:4
recall 7:2 9:2,14, 16 10:10,17 12:13 24:3,4 38:10 53:21 83:18 88:16 103:21	referring 5:12 24:6 47:7 48:5 53:6 55:2 73:7 80:12 111:13 114:3 116:7 121:13 144:11 152:4 154:24	remotely 4:5 114:11	requirements 51:6 89:3 129:13 138:15	retest 90:17,22 91:2,19
recalled 33:18	refers 48:12 121:6	remove 91:15 92:13	requires 57:11	retrieval 21:6
receive 108:20	reflect 45:6 151:4	removing 92:18	research 73:17	retrieve 51:17
	reflected 145:9 146:20 149:18 150:15	rendering 138:7	reserve 43:7	reuse 91:12
	reflecting 145:5 149:9	repeat 12:23 15:17 58:22 70:21 80:9 120:14 151:20	reshuffle 152:17	review 14:2,4 43:8
		replicated 78:9	residence 4:18	right-hand 126:18 127:14 129:2
		replicating 79:15	resilient 106:21	risk 35:21
		report 101:12	resource 47:20, 23 48:9,16 49:13, 18 50:4 58:21 59:1,5,11,20 60:1, 23 61:4 94:22 136:3,7,15 137:3, 4,12,19 139:1,15, 19 140:11,20 142:12,24 143:7, 11,16,25 144:23 145:4,17 146:1,9,	risks 107:4
		represent 41:10		role 35:20
				room 4:20
				root 131:4
				rough 159:14
				round 93:9
				route 28:11 31:15 65:25
				routed 31:9
				router 25:14

26:10,18 27:4,7, 16,25 28:5 31:7, 21 55:24 157:17 router's 28:10 routers 25:5 28:7 55:19 57:2 110:3 112:7 157:12 row 34:2 98:21 115:9 rows 98:8 rule 34:6,20,21 37:2,24 39:1 40:7, 19,25 41:10,16 42:4 115:1 rules 19:15,17 32:11 33:7,25 34:1 35:11 36:23 37:9 38:20,23 39:8 40:5 41:7,11, 12 72:15 76:2,6 77:21 78:3,4 96:24 114:18,19 115:10,13,15 121:15 run 72:13 73:7,10 84:1,3,7,13 86:2, 5,17 87:10 89:7, 10 92:6,8,23 93:5 94:1 96:8,22 97:10 127:9 131:4 158:25 running 84:18 92:10 94:13 131:12 runs 56:18 64:18 72:9 75:10 84:9, 22 130:25 rush 159:14 S Santa 30:5,14 satisfy 115:11 scale 26:22 scheduled 7:9 schema 98:5,7, 10,15,17,20,22,24	99:1 101:2,4,10, 11,21 102:2 schemas 101:19 science 69:13 114:23 scientists 69:19 scope 10:9,14 30:2 86:8 95:25 96:12 99:3,10,17 100:24 101:24 103:5,14 104:6,15 scream 92:5 screen 19:5,7 28:23 37:7 40:21 search 21:6 secure 49:7 76:19 Secure-by- default 50:23 51:1 securely 49:23 50:8,13 51:7,20, 23 security 24:21 33:6 35:19 50:21, 23,25 51:3 67:20 76:15,18,22 77:6 78:4 82:21 107:4 108:11,24 109:1, 4,5 144:3 sell 107:14 semantic 97:9 127:6 semicolon 40:23 41:1 42:5 send 23:18 24:22 26:20 27:12 28:3, 16 34:14 108:19, 23 142:17 143:5 sending 108:10 138:9 sends 152:10 sense 59:24 86:8 132:14 136:16 145:19	sentence 59:14, 16 62:1,8,14 68:17 73:22,24 74:12 78:14 81:20 92:20 95:6 96:16, 21 112:3 120:1 126:3 138:23 143:19 144:22 146:8 154:1 156:2,15 158:2,3 sentences 74:7 separate 46:17 80:20 separated 67:12 server 113:24 114:4,6,8,11 115:18 116:9,19, 24 117:3 120:2 130:18,19,22,25 131:6,12 134:5,8 service 34:11 37:16 38:14 39:4 40:4 48:2,6,13 55:12 57:10 156:7 services 35:5,6 37:12,15 42:9 47:25 48:1,5,12, 21 49:3,6,8,12,21, 23 50:9,13,14,15, 17 51:5,7,9,20,24 52:22 53:9,16 144:3 set 26:16,21,23 29:16 51:2 72:15 96:23 116:10,20 117:21 129:4 setup 27:14 64:2 136:24 setups 136:23 severely 108:13 shape 76:7 share 26:14 103:16 shared 22:12 90:11,12 short 42:16,21 102:12 111:16	Shorthand 4:4 show 39:12 66:16 128:23 148:2 shown 114:7 123:8 shows 65:3 126:6 128:19 shuffle 153:14 shuffled 152:20 sic 140:5,9 156:4 side 7:19 126:18, 19 127:14 129:2,7 130:6 141:14 sign 43:8 signature 14:18, 20,24,25 similar 26:21 38:14,20,21 40:6, 11 42:8 123:19 124:7,10 125:11, 12 128:12 133:7 simple 153:20 simpler 152:23 simply 95:22 97:4 147:2 simulate 78:10 86:21 simulated 75:25 simultaneous 7:20 single 16:19,22, 23 21:20,23 22:1, 11 23:23 24:12 27:8 31:15 36:15, 19 53:10 91:25 92:5 94:11,12 106:10,13,15 sites 111:14 situation 23:1,4, 24 31:19 32:8 52:8,25 86:20 87:11,16 132:18 149:15 situations 86:23	skip 95:4 skipped 73:22 slide 40:16 slow 34:16 slower 43:21 smaller 26:22 snippet 133:25 so-called 22:20 26:18 72:9 109:4 131:2 sort 64:1 84:1 87:23,24 99:15 112:18 113:3 138:10,16 152:15 sorts 25:5 source 34:7 35:1, 4 37:9 38:14 39:2, 3 40:3 42:8 source- destination 19:8 sources 19:8 34:10 space 125:4 spam 107:10,13 speak 34:17 43:21 73:17 spec 115:10 118:12,19 119:11 special 51:6 150:20 specific 45:20 47:24 49:20 51:5 52:12,23 60:25 64:10 85:18 86:5 87:10,15,17 88:25 94:24 132:11 140:12 146:10 147:12 specifically 11:2 52:6,18 55:13 63:4 78:17 91:19 118:19 120:11 133:11 157:3,4 specifies 54:23 120:25
---	--	---	--	--

spell 4:12	storing 102:4 104:25 140:20 142:12 145:25 147:13 148:9	158:10	sync 151:19 152:16,21	TAS 40:17
spot 67:24		subnetwork 29:16 30:12,13 66:25	syntax 97:7,11, 14 122:20,21 123:14 124:5 127:5	TCP 19:12 37:12, 16 122:1,12 130:8,16 133:6,8, 12
spread 112:9	string 101:7,8,22 104:21	subnetworks 28:24 29:16	system 21:7 33:8,13,17,22 39:24 40:3,13 55:9,16,17 75:9, 22 76:5 77:14 112:4 114:2,4 135:17 140:6 157:9,10	teach 37:6,23 85:17,18 88:18
spring 12:11	structure 95:8	subscribe 55:12 144:3 156:7		teaches 138:2
SRI 7:18,19,23	structured 95:8, 11	subscribes 57:10		teaching 71:14, 21 73:7 138:18 148:11
SSID 126:7 128:21	stuck 153:8	Subsequently 81:9,21		team 13:4
stand 114:13	student 92:9 124:14	substance 104:16	systems 19:9 38:13 55:8 140:4 156:4	Tech 124:15
stands 107:16	students 92:5 97:18,20 101:11	suffer 138:8		technical 32:13, 20
start 78:7 116:6 119:16 120:24	stuff 137:18 144:5	sufficient 63:21 125:22	T	technologies 25:6 32:25 113:1 128:12
starting 109:16 131:10	subdivided 30:20	sufficiently 125:22	table 34:2 98:9, 12,13,20	technology 99:20
starts 43:18	subnet 29:4,5 30:4,23 31:2,4,6, 8,14,15,20 32:1,4, 5,6 36:8,9,11,15, 20 46:25 47:6 51:16 52:4,12,15, 18,19,23 53:2,3,6, 10 55:19,23,24,25 56:1 57:3 58:2,8, 11,17,18 61:21 62:3,5,19,20 63:1, 3,6,13,16,22 64:6, 8 65:4,10,11,16, 18,19,21,24 66:13,14,17,20 67:5,6,9,10,12,16, 20,22 68:23,24 72:24 74:4 78:18, 19,24,25 79:2,4,6, 7,8,12,19,22 80:8, 11,17,18 81:13, 18,25 87:4,5,6,13 88:11 96:19,20 149:17 157:13,16, 18,20	suggesting 71:13	talk 42:8 44:25 45:3 59:23 60:7 63:9 82:16 94:21 96:16 97:8 103:23 104:1 111:10 112:24 122:22,23 123:2 132:6 133:10,11 134:21 139:9,10,21	teenage 25:23
state 4:4 19:1 106:21		suggests 71:1		Tehranchi 13:11
Stated 146:8		suing 7:24	talked 82:13,14	telecommunicati on 48:1,6,13
statement 19:20 61:5 108:17 120:15		summer 12:10	talking 21:18 63:24 87:20 93:20,21 96:4,5 97:11 101:7 116:15 118:21 138:12,18 142:1 147:13 149:14	telling 36:17
stay 116:14		support 104:4,9, 21,24	talks 47:22 53:19 60:2 62:17 63:4 73:21 77:16 78:6 96:13,15 113:12 115:12 124:25 134:4,5 140:19 142:11 143:15,18, 19 144:10 145:6 148:21 151:17 154:18 157:2,23 158:12	tells 98:22 129:10
step 150:2		supports 103:19 105:6 129:21		ten 6:16 102:15, 19 134:13
steps 117:13 119:9,14		suppose 66:2 67:8 92:9		ten-minute 102:14
stick 153:9		supposed 87:14		term 95:9 98:4,19 109:3
stop 69:22		surprised 10:22 97:22 104:8,10,23 105:6 131:15		terms 23:2 32:11, 18 34:14 36:19 51:6 67:22 69:13 93:24 95:21 125:9 138:2,14
storage 116:23 117:23 119:20	subnets 30:7,8, 21,22 31:1 44:23 45:6,11,13,14 46:17,22,24 52:7 53:10 61:16,24 62:11,18 63:4,12 65:5 66:8 110:13	switch 28:14 31:6,20 36:7 67:18		Terrill 5:8 14:5
store 47:24 48:10 49:16 95:19 105:9 137:18 142:18 146:9 148:6 149:2		switches 55:19 57:2 110:3 112:8 157:12		test 73:2,3,11,18 75:6,14,19 83:22, 24,25 84:2,3,6,7, 13,15,17,18,21,22 85:4,6,9,11,15,16, 25 87:12,21 88:3, 13,19,20,24,25
stored 48:16,20, 24 49:13 50:3 51:14 58:21,25 59:4 60:14,15,22 61:4 94:22 98:9 116:23 117:22,25 118:22 139:12,14 140:10 141:2 145:17 147:1,21 148:3		switching 67:3		
stores 49:18 139:18 146:14		sworn 4:8		
		Sybase 103:10		

89:4,7,11,12,16, 17,22,23 90:3,25 91:6,10,13,24 92:1,2,6,8,23 93:2,4,6,10,14,22, 24 94:8,10,11,13	140:3,4 156:3,7 threats 61:22 62:3 63:5,7,19 threw 152:20 Thursday 13:25 time 7:9,10,11 11:22 13:20,21,22 17:9,11 20:2 38:16 39:5 73:15, 16 83:25 90:24 91:9,25 94:12 102:13 107:11 108:18 112:6 141:3 145:9 146:22 147:9 149:19 159:7	86:21 87:6 88:4,6, 8,9 89:2,17,18,19, 23,24 90:4,5,15 91:17 94:1 106:1, 6,10,14 130:21 131:10,12,17,24 132:3,24 134:7 157:19 transcript 32:22 43:8 75:16 translate 26:20 translation 26:19 28:15 transmission 119:20 120:6 transmit 147:22 149:5 150:1 transmits 120:3 transmitted 115:17 117:3,23 118:1,2,8,14,22 119:11 139:14 155:22 transmitting 118:25 147:13 trial 7:5,12 trigger 91:18 triggers 93:9 true 11:15 truth 4:8 6:4,7 truthful 6:10 turn 14:11,15 18:10 42:14 43:16 47:11 68:5 115:22 120:8 134:24,25 138:20,21 TVS 25:25 two-minute 110:21 type 16:22 19:12 32:13 68:22 70:9 96:18 98:25 99:1, 5,9,18 100:22 101:17,22 105:11 156:10	types 98:2 99:15 100:3,6 101:20 103:18 104:4,9, 21,24 105:3,7,8 typically 9:24 36:8 38:11 97:19 U UDP 19:12 37:12, 16 Uh-huh 8:1 30:15 34:4 46:5 47:15 78:12 113:22 117:7 124:1,4,23 135:25 underscore 124:3 125:4,14 understand 11:11 19:24 22:15 24:5 26:2 28:25 34:1 37:1 44:9 47:6 50:19 51:21 83:7 87:1,2 89:25 92:19,22 97:8,10 101:9 102:4 118:6 119:5 125:16 129:14 143:14 145:21 146:25 understanding 34:20 understands 148:11 understood 4:24 8:5 12:18 16:18 30:24 31:25 33:2 38:5 39:10 43:9 48:18 51:18 82:24 85:20,24 105:21 118:4 128:11 130:1 143:9 156:20 158:6 unintended 90:14 unique 22:20,25 23:3,12 unusual 90:10 up-to-date 146:23 149:20	150:13 update 51:15 127:16 145:4 150:1 155:11 updated 60:13 141:5 145:5,11,15 146:5 147:13 updates 120:3 127:22 141:1,2 146:17 147:20 148:5 149:2,24 150:5 updating 63:9 upload 5:18,19 124:8,20 125:3 156:22 user 33:6,8 36:13 37:25 38:2 40:9 41:13 113:5,14,17 140:17 142:9 143:4,22 144:20 146:16 156:9 user's 94:25 140:13 users 49:9 107:10 154:12 V validate 69:3,18 70:3,5 71:4,14,22, 23 72:10,14 74:1 77:4,8,14,15,17 87:20 96:22 validated 68:20 69:11,14,19 70:8, 15,16,19,24 validating 68:16, 25 70:1,6 71:8,10 72:3,19 76:10 77:16 83:7 86:15 148:5 validation 69:6 71:1,21 73:6 74:25 75:4 77:8 78:23 79:6 82:15 85:19,24 87:23 95:21 96:7,25
--	---	--	---	--

Variety 103:11 vary 22:6 varying 112:5 verification 85:19,24 verified 68:20 69:11 77:18 verifying 68:25 82:15 83:8 version 109:19 113:3 126:7 128:20 135:4 150:4 versus 7:18 32:17 37:16 42:4 52:23 62:15 69:13 80:18,25 83:11 137:8 138:8 Video 4:2 view 32:13,15,21, 24 virtual 72:2 73:19 75:19 78:9,10,17 79:1,11,17,18,20, 21 80:1,2,7,10,12, 16,19,25 81:3,4,6, 7,10,23 82:5 85:11 87:2 136:23 VLAN 128:25 VPN 25:5,15,16, 17 26:6 27:11 67:21 W W-E-N-K-E 4:14 Wang 5:6 14:5 45:5,18,22 46:2 47:2,11 48:5,12 50:14 51:4 53:19 54:13,23 56:5,10 59:17 61:8 68:5 69:6 71:1 72:13, 18 73:19,23 74:16 78:16,23 79:5,15, 17 80:10 81:8,16 83:3,15,19 85:14 94:16 95:14 96:5,	7 135:5,15 138:20,22 139:23, 25 140:14,19 141:24 142:11 143:15,18 147:4 148:11,15,18 149:24 151:23 152:8,24 153:2,4, 20 154:1,8 156:21 Wang's 85:17 95:1 wanted 16:12 43:25 51:18,22 61:19 125:18 ways 23:16,21,22 40:24 71:23 86:2 web 20:22,25 21:8 116:8,18 130:18,19,22,24, 25 131:6,12 134:5 website 33:15 Wednesday 4:1 week 92:5 weeks 26:12 Wei 13:8,9 well-known 90:12 WENKE 4:6 whichever 131:23 wide 20:22,25 21:8 76:8 114:9 130:24 wireless 112:7 wiring 28:17 withdraw 65:17 66:3 withdrawn 20:4, 8,14 24:11 79:16 93:3,4 98:2,3,16, 25 102:10 106:19 122:18 132:1 137:11 word 14:22 15:2 16:14,19,22,23 69:9 70:16 71:19	79:20 86:3,25 Word's 15:3 words 19:5 work 8:15 9:2,4,8, 11,21,22,25 10:8, 16 11:5 13:4,6 15:7 16:10 18:7 29:10 76:15 77:21 78:4 81:2 83:10 88:8 97:17 worked 17:1,12, 15 37:22 working 17:6 89:22 works 29:9 76:13 world 20:22,25 21:7 26:15,25 29:22 90:12 130:24 worry 152:24 write 15:5,9,20 16:8,12,19 32:12 127:8 129:15 writing 15:25 16:2,13,15 X Xbox 26:1 Y year 6:17 8:6 12:6,11,12,13,14 92:9,11 years 7:13 12:7 17:4,5 100:18 yesterday 14:1 York 45:15 46:13 Yuan 13:9 Z zeros 39:18 Zoom 4:2 5:18		
---	--	--	--	--