Trials@uspto.gov
571-272-7822

Paper 29
Entered: August 12, 2024

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

CISCO SYSTEMS, INC.,
PALO ALTO NETWORKS INC., AND
FORTINET, INC.
Petitioner,

v.

LIONRA TECHNOLOGIES LTD.
Patent Owner

IPR2023-00673 (Patent 7,685,436 B2)
IPR2023-00703 (Patent 8,566,612 B2)

Record of Oral Hearing
Held: July 23, 2024

Before WILLIAM V. SAINDON, PATRICK R. SCANLON, and STEVEN M. AMUNDSON, *Administrative Patent Judges*.

APPEARANCES:

ON BEHALF OF THE PETITIONER:

PATRICK MCPHERSON, ESQUIRE
Duane Morris LLP
901 New York Avenue N.W., Suite 700 East
Washington, DC 20001-4795
Pdmcpherson@duanemorris.com
(202) 776-5214

PATRICK MULDOON, ESQ.
Pcmuldoon@duanemorris.com
(202) 776-7840

ON BEHALF OF THE PATENT OWNER:

ROBERT AUCHTER, ESQ.
Auchter PLLC
1999 K Street NW, Suite 600
Washington, DC 20006
Robert@Auchterlaw.Com

The above-entitled matter came on for hearing on Tuesday, July 23, 2024, commencing at 9:00 a.m., at the U.S. Patent and Trademark Office, 600 Dulany Street, Alexandria, Virginia.

1 P R O C E E D I N G S
2 - - - - -
3 JUDGE SAINDON: Please have a seat, good morning. Give me
4 one moment to bring this up. All right, good morning, welcome. This is a
5 hearing for IPR 2023-00673 and 703. I am Judge Saindon, with me today
6 are Judges Scanlon and Amundson. They are appearing remotely; the name
7 tags are arranged in the right spaces. We have arranged 60 minutes per side,
8 we'll allow you to break that up however you want among your time, just
9 tell me, I'll be running the clock, and I will put a time reminder up there,
10 how much time you want for your different sessions.
11 Okay, with that, let's get into introductions. Let's start with
12 Patent Owner, since Petitioner will be going first. Go ahead, Patent Owner.
13 MR. COOPER: Good morning, Your Honors, this is Brett
14 Cooper on behalf of the Patent Owner, my partner Robert Auchter who is
15 with me today will be handling the argument.
16 JUDGE SAINDON: Okay, good morning, thank you. And
17 Petitioner?
18 MR. MCPHERSON: Good morning, Your Honors, Patrick
19 McPherson for Duane Morris, I represent Fortinet, I guess the last remaining
20 Petitioner, and I have with me Patrick Muldoon and Paul Belnap. Thank
21 you.
22 JUDGE SAINDON: Good morning, and you may approach the
23 lectern. Do you have an amount of time you want to reserve for this
24 particular portion?
25 MR. MCPHERSON: Judge Saindon, I'd like to reserve 15

1 minutes for rebuttal.

2 JUDGE SAINDON: Okay.

3 MR. MCPHERSON: Judge Scanlon, Judge Amundson, can
4 you see the presentation on the computer screen, or are you using paper
5 copies, or your own copy?

6 JUDGE AMUNDSON: This is Judge Amundson; I'm using a
7 paper copy.

8 MR. MCPHERSON: Okay.

9 JUDGE SCANLON: I am as well. We should be able to
10 follow along.

11 MR. MCPHERSON: Okay, I will try to remember to say slide
12 numbers so I don't confuse anybody.

13 JUDGE SAINDON: You may begin when ready.

14 MR. MCPHERSON: Thank you, Your Honor. If we look at
15 the cover sheet, I just want to describe for our demonstratives, since this is a
16 joint proceeding, the demonstratives are reciting to the record in the 673 IPR
17 which is for the 436 Patent, and that just made the slides a little less busy.

18 If we turn to slide two, this is an overview of the four grounds
19 in this case. The claims between the 436 and the 612 Patent are nearly
20 identical. Claims one and 13 are the independent claims in both patents, and
21 it's claims one and 13 that have a slight difference between the 436 and 612,
22 and I'll point that out going forward. The four grounds shown here is
23 ground one is the only ground directed at the independent claims, one and
24 13, and some dependent claims. Ground two is directed to dependent
25 claims, ground three and ground four also to dependent claims.

26 If we turn to slide three, this is an overview of the dispute

1 between parties in both cases. These disputes are the same. The first
2 dispute is whether this claim language, which shows up in claims one and
3 13, the independent claims, whether Pham discloses substantially all of the
4 incoming packets and outgoing packets to the security processor transit one
5 of the plurality of packet engines. The next dispute, dispute two, was also
6 directed at the independent claims, and that's whether a person of ordinary
7 skill in the art would be motivated to modify the teachings of Pham with the
8 teachings of Wu. And Wu is a secondary reference which is used to show
9 the inclusion of an intrusion detection system, IDS, and a signature database.
10 And the third dispute between the parties is whether a person of ordinary
11 skill in the art would be motivated to include various components and
12 security functions on a single chip, and those are directed solely to the
13 dependent claims listed there, four, seven, eight, and 17.
14 JUDGE SAINDON: Counsel, before you move on, just a quick
15 question. The Wu issue that you have listed here, if we find for you on that
16 issue, does that subsume the need to talk about the substantially all issue, or
17 are those both independent?
18 MR. MCPHERSON: Those are both independent, both those
19 issues need to be addressed.
20 JUDGE SAINDON: Okay, thank you.
21 MR. MCPHERSON: If we turn to slide four, this is an
22 overview of the 436 and the 612 Patent, and this figure identifies the
23 architecture for which the independent claims are based upon. And if you
24 look there, there's a security processor, is what's being shown here at the
25 top, and it consists of a, or includes, a switching system, and the switching
26 system is shown in gold there, reference number 208, for receiving incoming

1 and sending outgoing packets. And then you have a packet engine
2 highlighted in green, and that does various processing, network address
3 translation, firewall, IP, security classification. And then coupled to that we
4 have a cryptographic core, and the cryptographic core provides encryption,
5 decryption, and it receives those incoming packets and sends those outgoing
6 packets via the packet engine to the switching system. And then what's not
7 shown here is an IDS system, and that IDS system is coupled between the
8 packet engine in green and the crypto core in red is just not shown in this
9 embodiment. And the 436 and 612 specification describes that each of these
10 colored components are conventional and were known in the art.
11 Turn to slide five, I'll give a brief overview of ground one. So
12 if we turn to slide six, this is the overview of Pham. And the petition
13 describes Pham using the same color coding for the common elements
14 between the patents in suit and Pham. And here we have Figure 4 on the left
15 hand side and Figure 6 on the right hand side. Figure 4 shows ingress and
16 egress processors being sent to a crypto processor via a switching system,
17 and then the crypto processor is further broken down, and you can see that in
18 Figure 6 on the right, and if we turn to the next page, it's a blow up of Figure
19 6 and it's a little easier to read. And using the same color coordination, if
20 you look at the left hand side of Figure 6 of Pham, you see there's a
21 switching interface that goes to the switching system, and that's for
22 receiving incoming and sending outgoing packets.
23 And then from there, you have a network processor 112, that's
24 shown in green, and that corresponds to the packet engine and does various
25 processing as described in the patents. And then in red we have the
26 encryption decryption engine, and that provides encryption decryption on

1 the received incoming and outgoing packages that are received through the
2 network processor. And in purple here we have identified the routing and
3 SA table, and that's the functionality that can reside in the ingress processor
4 and in one embodiment, that processing can reside in the network processor
5 through the memory. And this is the embodiment that we used in the
6 petition.
7 And then not shown here would be the intrusion
8 detection system, and that's where we modified the teachings to include an
9 intrusion detection system locating it between the network processor and the
10 encryption decryption engine, and we'll talk about that a little later. So as
11 you can see, the description and disclosure of Pham is parallel to disclosure
12 of the 612 and 436 Patents, including a description in Pham that each of
13 these color components are conventional components, and Pham actually
14 provides a model number and in some cases a part number for what those
15 conventional components are.
16 If we turn to slide eight, this is dispute number one, and this is
17 the claim language found in independent claims one and 13, and the
18 language is substantially all the incoming packets and outgoing packets at a
19 security processor transit one of the plurality of packet engines. And the
20 Patent Owner put forward several arguments, but those arguments are based
21 upon a faulty legal premise, for one, and a faulty factual premise. If we look
22 at slide nine, slide nine demonstrates the faulty legal premise. If you look at
23 the middle of the page highlighted in red is the language at issue in dispute
24 one, and it says substantially all of the incoming packets and outgoing
25 packets at a security processor transit one of the plurality of packet engines.
26 And if you look at the preamble, the preamble actually provides the

1 antecedent basis for that limitation, and that's incoming packets and
2 outgoing packets, right, a security process, incoming packets and outgoing
3 packets.
4 And so the way this claim reads is the substantially all refers
5 back to whatever packets are received by the security processor, those are
6 packets that are the subset of substantially all, recited further in the claim. If
7 you look at the preamble, there's no limit on the number of packets, the type
8 of packets, or when you consider those packets, and that is the crux of the
9 matter here, and I want to turn quickly to page 10 to show that claim one
10 reads on this limitation. Claim one reads on this embodiment for that
11 limitation.
12 If you look at this on slide 10, this is Figure 4, and it shows, we
13 have clear text coming in on the left, in one instance, going through an
14 ingress processor, going through the switch, and going through the crypto
15 processor. The crypto processor, there's processing done including
16 encryption. It is then returned from the crypto processor through the switch
17 fabric to the egress processor and goes to the WAN, as encrypted packets.
18 Or vice versa, it can come in as an encrypted packet from the WAN and
19 come into the ingress processor, go through the switch fabric, go through the
20 crypto processor for processing, including decryption, and then return from
21 the crypto processor to the crossbar switch, back to egress processor. And
22 this embodiment shown here, where the packets coming from the LAN are
23 sent to the WAN, or the packets coming from the WAN are sent to the LAN,
24 that meets the language, that those packets coming into the security
25 processor, which is shown and highlighted in brown in this figure, all of
26 those packets have a received in the brown portion, go through encryption,

1 are processed by the packet processor, and returned. This embodiment is
2 dispositive of this claim limitation, it shows that those packets that are
3 received, that go through encryption, substantially all of them received into
4 the security processor go through that encryption.
5 JUDGE SAINDON: Counsel, if I could jump in for a second.
6 MR. MCPHERSON: Yes Judge.
7 JUDGE SAINDON: Just to make sure I'm understanding how
8 you're reading this. So are you saying -- and I could see two possibilities
9 here. That depending on the nature of the packets where they're being sent
10 to, then Pham would handle substantially all because it's just, those are the
11 packets it received in that time frame and they all went through to the crypto
12 processor, that's one reading. Another reading is that only packets that are
13 intended to go through, say a VPN gateway, are to security processor,
14 therefore all the packets it receives are packets sent to it, and therefore
15 substantially all. I see those two potentially different ways that you could
16 be reading this claim, I just want to know if you're focusing on one, the
17 other, or both.
18 MR. MCPHERSON: So I think here it's not just going through
19 the VPN, if you look on slide 10 we have identified in brown what the
20 security processor is, which is a subset of the VPN. So it's those packets
21 that reach the crossbar switch fabric, which would be the entry of the
22 security processor. In this embodiment, all of them go through the crypto
23 processor and are processed.
24 JUDGE SAINDON: Because of where the packets are
25 addressed to?
26 MR. MCPHERSON: Because of where the packet are

1 addressed to.

2 JUDGE SAINDON: Okay.

3 MR. MCPHERSON: If we turn back to claim one, on slide
4 nine, in the highlighted red language, right after that there's an 'and
5 wherein' clause, and it says, "and wherein the incoming packets and
6 outgoing packets are provided with a tag upon ingress to one of the plurality
7 of packet engines and the tag determines an egress path within the security
8 processor, upon exit from a corresponding cryptographic core." That
9 language is recited in claims one and 13 of the 436 Patent, it's not recited in
10 the 612 Patent. The 612 Patent would be broader, by not having that
11 limitation in there, the example I just showed with slide 10, that's an
12 example that applies to both the 436 and the 612 packets. That language and
13 dealing with the tag, that tag is added as part of the encryption process, as
14 the processing packet engine does the beginning of crypto processing, that
15 tag is part of the encryption process, so that limitation would be met for 436
16 purposes. It's not required for 612, but the same example shown in slide 10
17 would apply for 612.

18 If we turn to slide 11 now, here are some of the faulty factual
19 premises that the Patent Owner puts forward, and one of those is that only
20 the SA parameter association task may be offloaded to a crypto processor.
21 I'll address that momentarily. And number two, that clear text does not
22 require any processing by the network processor in Pham. Now both of
23 these arguments go against the clear teachings of Pham.

24 If we turn to slide 12, both of the parties described Figure 4 of
25 Pham in the same way, and there's no dispute that the crypto processor is a
26 data processor, as described in Pham. And in the petition, we described a

1 plurality of data packet processors in the form of crypto processors,
2 highlighted in yellow in Figure 4, coupled through a data switch fabric,
3 orange, between network connection processors, purple. And in the Patent
4 Owner response, they have the same description. In Pham's VPN gateway
5 there are network ingress processors, egress processors, and data packet
6 (crypto processors). If we turn to slide 13, in Petitioner's reply, we point to
7 the specification of Pham that there's no dispute that the crypto processor is
8 a data processor, and in our reply we state, "further Pham discloses that
9 crypto processor 86, in Figure 4, is a type of data processor illustrated in
10 Figure 3 that can be flexibly configured to implement any of a number of
11 different network protocol processing functions, including those that are
12 compute intensive." And we cite specifically to Pham that says a preferred
13 VPN embodiment 70 of the present invention, representing a specific
14 implementation of the extended protocol processor architecture 50 of Figure
15 3 is shown in Figure 4.
16 And if we turn to the next slide, 14, this is the architecture 50
17 from Figure 3 where the specific embodiment that we're using is just a
18 specific implementation of the protocol shown in Figure 3, and you can see
19 there's no encryption engine shown in Figure 3, but they're part of the data
20 processors that are shown in Figure 3. If we turn to slide 15, Pham describes
21 that the data processors can perform computer intensive processes, and the
22 specification for the 436 and 612 Patent lists many examples, and during the
23 cross examination of their expert, I went through each one of those examples
24 and said, are these compute intensive processing? And he said, in the right
25 circumstances each one of these could be compute intensive processing.
26 Compression, decompression, protocol translation, encryption, decryption,

1 routing, load balancing, filtering, and switching. So these are all processes
2 that could be done in the data processors of Pham.
3 Then if we turn to slide 16, we see that Pham describes that
4 data processor can perform multiple processers. And it says in Pham, data
5 processors can be flexibly configured to handle any number of different
6 protocol processing functions. It goes on to say the individual data packet
7 processors 58 may be configured to perform a single protocol conversion
8 operation or multiple related operations, and he gives an example. For
9 example, packet data can be pressed before encryption, and decompressed
10 following decryption. Single data processors 58 can be used to form
11 multiple compute intensive operations, or the fast path processing of
12 network data packets may be extended to include the transfer of data packets
13 between multiple data packet processors before finally being forwarded onto
14 an egress processor 54. Now this directly contradicts Patent Owner's
15 argument that the network processor in Figure 6 can only perform SA
16 processing, because we know those processors are capable of performing
17 multiple processes, or they can distribute those processes over multiple data
18 processors.
19 On slide 17, this demonstrates the relationship between the
20 ingress processor and the network processor 112, and for the embodiment
21 we're using in the petition, it's a situation where processing that's normally
22 done by the ingress processor is offloaded, and that's shown in the left figure
23 as ingress processor, in purple, they can be offloaded to the network
24 processor 112. And the specific example that it gives is routing and the SA
25 tables used for encryption can be offloaded and done by the network
26 processor instead of the ingress processor there. We turn to slide 18, Pham

1 gives the example that all packet processing except basic switching and
2 filtering can be offloaded from the ingress processor to the crypto processor.
3 And it says, for example in one embodiment, Pham discloses that ingress
4 process 80, Figure 5, and network processor 112, and crypto processor 86
5 use the identical conventional processors, and identical routing and SA
6 tables to allow functions of the ingress processor to be offloaded to the
7 network processor 112, such as packet routing, SA parameter association,
8 and compression, and decompression. And gives cites. Thus, all packets
9 both clear text and cryptic can be sent to network processor for routing using
10 SA table.
11 JUDGE SAINDON: Counsel, can I jump in here? So I
12 understand your point that you can kind of load balance the functionality
13 between the front end and the back end, at least that's what I'm taking. This
14 slide here, slide 18, says that all of the processing except for the basic
15 switching and filtering can be offloaded kind of on what I'll call the back
16 end. So as I understand Patent Owner's argument, I think they're saying that
17 this in and of itself shows that not all of the packets are making it to the
18 security processor. Regardless of how much you move back there, you still
19 are going to have this residual functionality, and so I was wondering if you
20 could speak to that point.
21 MR. MCPHERSON: Yeah, so it's unclear what residual
22 functionality is remaining there.
23 JUDGE SAINDON: So let's just say switching and filtering,
24 the device needs to know whether or not the packet is address to it, in order
25 to do that it has to read it, if it wasn't, then it sends it back out, something
26 like that.

1 MR. MCPHERSON: Right, so let's take an example where a
2 packet is clear text going from one VPN to another VPN, so it's clear text,
3 doesn't need encryption. It may need other processing, that the network
4 processor does. For example, LAN one could be IP version four, and then
5 two could be IP version six. So there has to be a conversion between those
6 two, a packet processing between those two, that's a protocol conversion.
7 And Pham says specifically, that protocol conversion, which is compute
8 intensive, could be done by the network processor in the crypto processor.
9 So it doesn't get to the encryption engine, but the packet processing still
10 needs to be done by the network processor, which is 112, Figure 6.
11 So even if you have basic switching, filtering, there are
12 many other processes that need to be done, that may not include encryption.
13 So it's not enough just to say well, as long as the ingress processor is doing
14 some type of basic switch and filtering the claim is not met, because there's
15 other processing that could be done. And that was our point, and when I
16 asked our expert that specific question he says well, I didn't consider that
17 type of protocol conversion. Well, protocol conversion is one of the types of
18 processes that can be moved, because it's compute intensive.
19 JUDGE SAINDON: Okay, yeah, and I understand that lots of
20 traffic goes through Pham, I'm just wondering about, maybe the definitions
21 of what is switching and filtering here is maybe where the confusion or
22 dispute is. You know, this Pham device is on a local network, so unlike in
23 the embodiment in the patent, it's not a network interface card, where
24 everything goes through it, all network traffic. This, some traffic doesn't
25 even, it's not even address to it, it's just on the LAN. Is that the filtering, is
26 that, you know, hey, this packet isn't even to me, just send it back out?

1 MR. MCPHERSON: That's unclear, but I would consider that
2 basic filtering, where it's not addressed to me, so I'm not going to address it
3 at all, and that happens a lot.
4 JUDGE SAINDON: Sure.
5 MR. MCPHERSON: I mean, that would be included, basic
6 filtering. The 436 and the 612 Patents don't discriminate between basic and
7 non-basic filtering. I think there's a quote where, if you're looking, it's slide
8 21, that first quote there from Pham says, "with substantially increasing wire
9 speed, the computation capabilities of the ingress processor 52 may become
10 insufficient to timely perform all of the required filtering, routing, and load
11 balancing functions." So that seems to say that there is the capability of
12 Pham to distribute that to the other data processors. And if you look at
13 Figure 3 it shows that there's a scalability function in Pham, that there are a
14 lot more data processors than there are ingress processors, and so they may
15 in fact be offloading just simple switching as well, according to this quote I
16 just read, that all of the required filtering, routing, and load balancing
17 functions can't be done by the ingress processor. Does that help answer
18 your question?
19 JUDGE SAINDON: Yeah, and I guess it goes back to my
20 original question as to whether we're looking at the packets being to the
21 processor being the ones that are intended to be processed by the processor,
22 as opposed to those that just find their way somewhere in the system.
23 MR. MCPHERSON: Right, and that's not addressed. I don't
24 think it's addressed by either of the patents or Pham, but certainly their
25 architecture allows the ingress processor to send them to the network
26 processor and the crypto processor for any of the functionality that the

1 ingress processor can do.

2 JUDGE SAINDON: Okay.

3 MR. MCPHERSON: If we look to slide 19, I think it
4 demonstrates why that's possible. At Figure 5 at the top is the ingress
5 processor, and 92 there is a network processor, and if you look below at
6 Figure 6, Figure 6 is the crypto processor, which has 112 as a network
7 processor. Those architectures are identical, and they're identical in the
8 sense that both network processors are described as IBM network
9 processors, with identical model number, identical part number in this case.
10 So the functionality between those two having the same processors is what
11 allows the ingress processor to send its processing to any one of the plurality
12 of data processors you have out there, and the data processors can use a
13 network processor, which is identical to the ingress processor, including the
14 same memory and the same access to the same deal. And the other
15 description is, is that this network processor can operate at line speed, so it
16 can operate the same as ingress processors so you don't have any slow down
17 when you offload from the ingress processor to a data processor, it's
18 operating the same line speed, but there's also multiple data processors that
19 they could be sent to.

20 And if we look at slide 20, Pham expressly touts as the
21 advantage this ability to offload these processing functions, and it says still
22 another advantage of the present invention is that the network data
23 processors can be flexibly configured to implement any number of different
24 network protocol processing functions, including particular those that are
25 compute intensive. And then beneath that, multiple scalable arrays of data
26 packet processors 58 can be directly connected to the switch fabric 56 to

1 provide various forms of protocol data processing characterized as involving
2 significant computation intensive operations. The individual data packet
3 processors may be configured to perform a single protocol conversion
4 operation or multiple related operations.
5 And then if we look at slide 21, it's the cite I just mentioned
6 before, this provides a reason why you may need to offload. And if you look
7 down below, that argument there is the same argument I just addressed
8 before, that even if you don't have encryption, there may be a reason to send
9 the packets to the network processor, the crypto processor, for example,
10 protocol conversion between IPv4 and IPv6. And on the next few pages are
11 just different embodiments of Pham, which talks about different
12 arrangement for Pham, and some of these would include embodiment where
13 all of the processing is going through the packet processor because
14 encryption is involved in it. And when you have an embodiment like that,
15 that reads on claim 1 and 13 of Patents.
16 In conclusion, for dispute one, I think the claim language is
17 dispositive that not every single packet in the world or over some set period
18 of time needs to go through the security processor, but whatever packets are
19 going through that security processor all go through the packet engine, and
20 that occurs when I have a stream of data coming in from a LAN going to a
21 WAN, every one of those packets is going to be going through the processor.
22 So substantially all of those received by the network of the security
23 processor are going through the packet engine, going through the crypto
24 engine, and going back out to the WAN. And I think that's dispositive of
25 this limitation. Are there any questions on dispute one?
26 JUDGE SAINDON: Yes, one other question. So based on the

1 timing of the joined petition, we had a DI that went out with a POPR in that
2 case, there was no POPR in this original case, the POPR in that case is
3 substantially identical to the Patent Owner response, and then there was a
4 Petitioner reply, and then the DI went out, and then there was a Patent
5 Owner sur-reply as I recall. Anyway, so you have not had any opportunity
6 to comment on the DI, what was said in there. Is there anything that you
7 need to say now?
8 MR. MCPHERSON: I don't think so, I'm probably filling out
9 some of the edges of stuff that was not drilled down upon because it was a
10 DI, and part of the stuff that we're saying now I think is stuff that was
11 addressed I think more intently in the POPR that we went after, and so some
12 of that would be that the ability of the processors to only process SA, and
13 that they couldn't process other ones, and then bringing in Figure 1 and
14 Figure 2 which was not in the POPR, and so I think some of that was just not
15 addressed in the DI, and I think it's addressed now in the papers.
16 JUDGE SAINDON: Okay, thank you.
17 MR. MCPHERSON: Slide 25 shows dispute two, and that's
18 whether a person of ordinary skill in the art would be motivated to modify
19 the teachings of Pham with the teachings of Wu. And if we look at slide 26,
20 this is a limitation in claim 1 further down, and here it's highlighted in
21 green, and the limitations are a signature database and intrusion detection
22 system coupled between the cryptographic core and the packet engine in
23 response to at least one packet matching a signature stored in a signature
24 database. And if we turn to the next slide 27, this is the overview of Wu that
25 we're really relying on here, and here, if we look at Figure 2 from Wu, it
26 shows a data monitoring and analysis device, and that's connected to the

1 network, so that's pulling in packets from the network. And then those
2 packets, through an API, sent to a signature based IDS, and the signature
3 based IDS has access to a signature database, and it does signature matching
4 to find security threats doing signature matching.
5 If we turn to slide 28, in the petition we have a state of the art
6 section, and we describe the common use of intrusion detection systems,
7 IDS, having a signature database and placing the IDS at endpoints where the
8 encryption and decryption are performed, such that it can inspect
9 unencrypted traffic. And as part of that state of the art, it expressly states
10 that it was known that security features that don't include an IDS may not be
11 sufficient. And in our motivation to combine section, which now spans six
12 pages, we identified the motivation to modify the teachings of Pham to
13 include an intrusion detection system and signature database interposed
14 between the packet engine and the cryptographic core, and exactly where it
15 should be, at the endpoint where the encryption and decryption are
16 performed. And that comes specifically from the express teachings of the
17 references, that the expert did not address the state of the art section. It was
18 unclear whether he even reviewed it.
19 We've already addressed the motivation to combine, the six
20 page of fact-based evidence that our expert used was not addressed. The
21 POR is solely based on attorney argument, and talks about increased
22 complexity and the resources required, and their expert amended that line
23 but provided no factual support for that. And here, we know that an expert
24 understands trade-offs. What's the trade-off of including an intrusion
25 detection system, does that require additional resources? The answer is yes.
26 Or does it increase complexity and resources required would prevent you

1 from using an IDS when you want to increase your security? And I think
2 with the architecture as we've described in Pham, where you have these data
3 processors that are specifically identified as having the ability to compute
4 intensive processing, they could easily do compute intensive processing for
5 the IDS.
6 And then on top of that, there's also a description by Wu of
7 using databases, the central base database, while we know the network
8 processors have access to the memory, to the databases, and can do a lookup
9 just like they do a lookup for the SA tables. So we describe how it fits
10 nicely in there, and all we got back was increased complexity and resources
11 required, separate in part from their argument in dispute one that no, the
12 packet processor only does encrypted text, and therefore you'd never have
13 access to clear text, and that's just not accurate. And that's all I wanted to
14 address with respect to dispute two. So are there any questions regarding
15 dispute two?
16 If we turn to the next slide, slide 30, that's dispute three, and
17 this is whether a person of ordinary skill in the art would be motivated to
18 include security functions on a single chip. And the claims we're talking
19 about now, really, this is where the language shows up, claim 4, the security
20 processor of claim 3, wherein the packet engine to cryptographic core and
21 the modulo engine are formed on a single chip. And claim 17, the security
22 processing system of claim 13, wherein the security processor is formed on a
23 single chip. In this case, we relied on secondary reference of Krishna, and
24 Krishna discloses a packet engine, a cryptographic core, and other
25 components of the security processor upon a single chip, in Figure 2. And
26 we provided that color coded chip there. And Krishna further describes

1 incorporating components on this single chip may increase performance.
2 And to set it up, we have a state of the art section. And in that
3 state of the art we state, it was known to put security processing functions on
4 a single chip, and that cryptographic processing was moving away from
5 discrete processors and was being implemented on a single chip. And it
6 includes an illustration including a packet engine, including database
7 lookups and cryptographic engines, and that these discrete processors were
8 implemented on a single chip. This is all part of the state of the art at the
9 time. And so in our motivation to combine, our expert goes on, in giving the
10 teachings in the state of the art, combined with express teachings of Krishna,
11 that single chip processors' overall performance can be enhanced, a person
12 of ordinary skill in the art would be motivated to include security functions
13 on a single chip. That rationale applies to all security functions including in
14 IDS, and not just those discrete elements recited in claim 13, the packet
15 engine, the crypto core, and the modulo engine.
16 Well, in response to those arguments, the Patent Owner's expert
17 did not address our description of the state of the art or the rationale that we
18 provided in our motivation to combine. The Patent Owner response is based
19 solely on attorney argument, a terse description of Krishna. And our
20 description of Krishna was terse because it says that we're moving to put
21 these functions on a single chip, that a single chip can enhance performance.
22 And if you look at the 436 and 612 Patents, their description of whether all
23 these functions can be performed on a chip or not was described in the
24 alternative, and preferably can be performed on a single chip. But there was
25 no description in the patents that this is some new blockbuster thing, they
26 talk about it in the alternative and didn't really assign any patentability to it

1 at all, and we think that's because our state of the art description was right
2 on, that at that point in time it was known you could do this on a single chip.
3 Then their secondary argument is the same clear text argument that no
4 further processing is required if it's not encrypted. And that's the third
5 dispute, and that's all I was planning on covering right now. Are there any
6 questions?
7 JUDGE SAINDON: I have no more questions for you. I have
8 five and a half minutes that will be added back to your 15. Okay, so Patent
9 Owner, now you can set up.
10 MR. AUCHTER: Thank you, Your Honor.
11 JUDGE SAINDON: Okay, and then you may also reserve
12 some time for your sur-rebuttal, if you would like.
13 MR. AUCHTER: Thank you Your Honor, ten minutes please.
14 JUDGE SAINDON: Okay, all right, you may begin when
15 ready.
16 MR. AUCHTER: Thank you, Your Honor. If we could, I'd
17 like to turn to slide number seven, please. And just to reiterate where we
18 are, our position is that the Petitioner's petition fails because the petition
19 fails to disclose the limitation that's substantial at all of the incoming and
20 outgoing packets transiting one of the packet engines, and that is for two
21 reasons. First, because the clear text packets that go across a LAN go
22 directly from an ingress processor to an egress processor, are bypassed in the
23 language used in Pham. They go through the security processor because
24 they go through the switch fabric, but at no time do they go to any of the
25 crypto processors, they're filtered out. Second reason is because there are
26 packets that are directed to the control processor. Those packets come

1 across the LANs and they also come from the WAN, those packets are used
2 to establish a security connection. Those are clear text packets because they
3 have to be before you can establish a secure connection. Both of those
4 touched packets are going to exist in all the embodiments disclosed. They
5 will constitute --
6 JUDGE AMUNDSON: This is Judge Amundson; I have a
7 question on this. So I think I understand your point about the clear text
8 packets going from LAN to LAN, but what's your response to the argument
9 that there could be a protocol conversion required for those clear text
10 packets that could be offloaded from the ingress processor?
11 MR. AUCHTER: A couple of issues, Your Honor. First off,
12 even if there was a protocol conversion, there's no reason why that particular
13 operation would be offloaded to the crypto processor. Another issue which I
14 will get into in just a minute is that Pham itself teaches that when you're
15 doing certain types of compute intensive operations you would either replace
16 or supplement the crypto processor with a general purpose microprocessor,
17 and that is because once you reach a certain level of computation they say, at
18 least Pham teaches us, that that exceeds the capability of the IBM network
19 processor that is disclosed.
20 Furthermore, even in that case, you still have the control packet
21 processes, the control processor packets, rather, that are going to amount to a
22 substantial number of packets, and Pham discloses that those packets are
23 packets that are directed to the VPN gateway itself, for any number of
24 administrative or in band communication functions, as well as those packets
25 that are used to establish secure connection, if one does not exist in the SA
26 table. Consequently, some packets, so a significantly large number that

1 substantially all of the packets won't go to through crypto processor, will
2 either go to the control processor or bypass and go directly to the egress
3 processor, even in the situation where you are performing a protocol
4 conversion. And if you are performing a protocol conversion and you are
5 supplementing or replacing the network processor that's in the crypto
6 processor, as taught by Pham, then you would no longer have a packet
7 engine coupled to a crypto engine as required by the claims of the 436 and
8 the 612 Patents.
9 JUDGE AMUNDSON: All right, all right, thank you, I think I
10 understand your position.
11 MR. AUCHTER: And those would be the first, second, and
12 third sub-points and our first point in slide number seven, that the ingress
13 processors always perform filtering, there's no disclosure of filtering ever
14 becoming a responsibility of the crypto processors, and they also perform
15 basic switching functions.
16 JUDGE SAINDON: Counsel, if I could ask a question.
17 MR. AUCHTER: Yes, Your Honor.
18 JUDGE SAINDON: So you had mentioned something about
19 there being a substantial number of packets going into the control side. In
20 general, how many packets need to go to the crypto processor or not for it to
21 be substantially all?
22 MR. AUCHTER: Well, if one looks at the disclosure of the
23 436 and the 612 Patents, Your Honor, the system of the Davis patents, that's
24 the first named inventor of the 436 and the 612 Patents, it's directed to
25 creating a secure system. And in order to do that, they're saying look, there
26 used to be, there's a system out there where everybody has something over

1 here, something over there, it's inefficient, it has holes in it. What we're
2 trying to do in this invention is provide a system that captures everything, or
3 almost everything. In the Davis patent's disclosure they talked about, we
4 may drop a few packets, but the point is to not have holes in your security
5 system, to have a truly secure system that could be used for military
6 purposes, or any purpose where you want to maintain a trusted system and
7 maintain the security. So those kinds of packets that we're talking about that
8 would be directed at the control processor, those are exactly the kind that
9 would probably want to be captured by the Davis system, because those are
10 coming from the outside, those are clear text packets, and are being used to
11 establish a secure connection, that would be an opportunity to hacking or
12 spoofing. So it's not necessarily a specific number, because again, the Davis
13 patents are teaching let's try and capture every packet and only drop a few,
14 whereas Pham isn't concerned about that. Pham is concerned about
15 establishing a VPN gateway, which is why they have this opening to the
16 control processor, and between the ingress and egress processor, where they
17 wouldn't look at these systems. Of course, he also doesn't have an IDS, he
18 just discloses the basic switching systems.
19 JUDGE SAINDON: Okay, and I guess to follow up, what in
20 the challenged patents is enacting this or causing this to happen? Is it some
21 arrangement of structures, is it some sort of code, what is the structure kind
22 of underlying all of this?
23 MR. AUCTHER: The structure underlying all of this, Your
24 Honor, in the 436 and the 612 Patents is the configuration either embodied
25 in NIC, a network interface card, or an external device, that is intended to
26 capture all packets coming from any location and put them through the

1 system, specifically through the switching network there, into the packet
2 engine, to the crypto core, scanning them into an IDS, and making sure that
3 they capture every possible packet to avoid having that kind of leakage. It's,
4 if I may, Your Honor, I have a slide on that, Your Honor, where we discuss
5 some of the places where it's disclosed, and then if you give me a second I'll
6 take a minute and find where I've actually identified every place within the
7 patent disclosure where it explains why they're looking for all of the packets
8 or substantially all the packets.
9 JUDGE SAINDON: Okay, and so maybe we'll bump across
10 that next. So I guess just to follow up what you've said, it's embodied in the
11 fact that it's a NIC, a network interface card, which I understand is,
12 everything has to pass through because there's no other way through, right,
13 is the claim limited to a network interface card?
14 MR. AUCHTER: No, Your Honor, and neither is disclosure.
15 The disclosure mentions that it could be something else besides the network
16 interface card, they're just using a network interface card as an example to
17 show where you would capture every single packet that would be going
18 through the device.
19 JUDGE SAINDON: So it's a device that by nature of how it's
20 installed, for lack of a better word, where everything has to go through it.
21 MR. AUCHTER: Yes, Your Honor.
22 JUDGE SAINDON: Because Pham, being a gateway and a
23 switch, and all these other functions, just sitting on a network, things are
24 going to be bouncing all over the place, and that is why Pham doesn't
25 address all the packets, aside from the control packets that you've
26 mentioned, but some of them simply aren't sent to it, or bypassing it. And

1 so do your claims not cover that type of arrangement, or is there something
2 more specific to Pham?
3 MR. AUCHTER: The claims of the Davis patent would not
4 cover that type of arrangement because the key limitation and the limitation
5 that was added, or actually it was brought up from a dependent claim, to
6 obtain the allowance of the claims, was limitation of substantially all of the
7 packets transiting the packet engine. Pham doesn't do that, and that's a
8 critical limitation added during prosecution, so that the claims would be
9 allowed in both the 436 and the 612 Patents.
10 JUDGE SAINDON: Okay, and I know one of your arguments
11 was that the Pham, even, however much it offloads, it still performs basic
12 filtering, and I forget what the other --
13 MR. AUCHTER: Basic switching.
14 JUDGE SAINDON: Switching. Yeah, so could you explain
15 what is going on in those processes? Is a filter just, you know, some
16 gateways are configured not to pass onto certain IP addresses, doesn't allow
17 it out, is that basic filtering?
18 MR. AUCHTER: Your Honor, Pham does not go into great
19 detail as to what it means by filtering, other than it filters out certain packets,
20 and that is in particular, if I may, slide 20. Slide 20 shows Figure 12 as a
21 similar flow chart in Figure 15 of Pham, where it discusses filtering out the
22 data packets in particular with respect to Pham. And as they say here, this is
23 in paragraph 69 of Pham, an ordinary network data packet, as received 242
24 includes a conventional IP header, 244, and data packet payload 246. The IP
25 header is examined 250, step 250, to discriminate and filter out data packets
26 that are not to be passed through the VPN gateway 72. That is the filtering

1 function that is being performed by the ingress processor as disclosed in
2 Figure 12 of Pham.
3 And then it also shows in this same figure, in 256, where they
4 examine the SA table, the IP table, to determine whether or not there's an
5 existing security association, and if there is not a security association, it goes
6 on what they call the control path, as shown in there, 256 here, the decision
7 box. And that directs the packet to the control processor, as shown in 258,
8 to establish the connection. And that would be an example of filtering in the
9 case of 252 and basic switching in the case of 256, where it's sending it to
10 the control processor if there is no SA table entry showing an existing
11 security path, so it has to create one.
12 JUDGE SAINDON: Okay, and I guess that raises a question,
13 and it's similar to the question I asked Petitioner's counsel, so is a packet to
14 the security processor, in your view, one that touches any of the different
15 features that are part of the security processor? Or is it one that's intended to
16 be completely processed by the security processor?
17 MR. AUCHTER: It is our position, Your Honor, that it is one
18 that goes through the security processor, i.e. goes through the switching
19 fabric, which would include all the packets that come from the ingress
20 processor and are bypassed to the egress processor, but it would also include
21 packets that are directed to the control processor, because Pham explicitly
22 discloses that packets that are directed to the VPN gateway itself will be
23 routed and handled by the control processor. And the control processor is
24 shown in the brown section I believe we referred to, as to what Petitioner
25 identifies as the security processor.
26 JUDGE SAINDON: So if it goes into any part of the brown

1 section from that figure, then it is to the security processor?
2 MR. AUCHTER: Yes Your Honor, it's going through the
3 switch fabric, it's got into the security processor, presumably it would go
4 out, unless it's malevolent or something, I guess it would be dropped as is
5 disclosed, for example, in 436, you drop packets.
6 JUDGE SAINDON: Okay, understood.
7 MR. AUCHTER: And just to expand a little, if we could turn
8 to slide 21 please, Pham explicitly discloses the routing or switching of
9 packets to the control processor, and this is where they specifically say in
10 paragraph 39 that such data packets likely represent control commands used
11 to configure and manage the VPN gateway 12. So in other words, these are
12 packets that are being directed to the VPN gateway itself specifically, and
13 those would go into the security processor, but they would never go into the
14 crypto processors, and that would be part of the packets that are making
15 Pham a device where substantially all the packets do not transit a crypto
16 processor. And Pham again repeats, in the context of slide 22, that packets
17 not requiring processing for the data packet processors 42 and 44 are
18 bypassed between any number of ingress and egress processors.
19 Going on to slide 23, to show the point I was making
20 previously. Pham teaches that if you are going to offload a significant
21 number of the operations to the network processor within the crypto
22 processor -- and by the way, Pham's a little confusing in this sense, in that
23 the network processor is in the ingress processor, it's also an egress
24 processor, to sometimes refer to those as network processors, and it's also
25 referring it to the small IBM processor that's within the crypto processor and
26 the ingress and egress processors. But in this case, we're referring to the

1 network processor that's within the crypto processor, and Pham specifically
2 teaches us that if you're going to move the functions to the crypto processor,
3 in particular a general purpose microprocessor can be substituted or
4 provided in addition to the network processor 112 to support data
5 compression and decompression operations. And those compression and
6 decompression operations in Pham are similar to the kind of signature
7 matching that is performed, because they talked about how you would be
8 looking up the entries in the decompression table, which is similar to
9 protocol conversions and signature matching if you had an IDS in Pham's
10 embodiment.
11 If we could go back to slide 19, just for some additional
12 clarification, you could see where the LAN to LAN switch packets or the
13 clear text packets, which in accordance with Pham's disclosure would not be
14 routed to the crypto processors, but would be routed through the crossbar
15 switch fabric, and therefore would go into and out of the security processor
16 as part of that operation.
17 JUDGE SAINDON: Counsel, is that the bypass language that I
18 remember seeing?
19 MR. AUCHTER: Yes, Your Honor. To go back to a previous
20 question you asked, Your Honor, about where it's disclosed in the Davis
21 patents, that is reflected in slide 11. And slide 11 shows the basic
22 embodiment of the security processor in the 436 and 612 Patents, and it
23 shows that in the Davis patents they contemplate that all of the packets are
24 going to be routed through this switching system and then ultimately into the
25 packet engine of the cryptographic core, as a function of the design of the
26 Davis system to make sure that it captures all of the packets and not just

1 ones that are specifically in need of encryption or decryption.
2 And if you look at slide 12, you see where they specifically
3 address the issue. Regardless of destination, whether for example it is to
4 streaming interface 200, host interface 206, control processor 212, or a loop
5 through a packet engine 228, all packet data preferably flows to a packet
6 engine 228 and then to a corresponding cryptographic core 232. That's a
7 fundamentally different way of operating than is disclosed in Pham. And
8 then on slide 13, Davis discusses the concept of why it's not all packets,
9 because they show that you may also include dropping the packet.
10 JUDGE SAINDON: Counsel, is that a -- I hate to use the word
11 conscious choice, but a design choice or is that just an error and it gets lost?
12 MR. AUCHTER: Why a packet would be dropped, Your
13 Honor?
14 JUDGE SAINDON: Yes.
15 MR. AUCHTER: I think it's two or three situations, possibly,
16 Your Honor. I think it's one, if it gets tagged by the IDS then it would be
17 dropped because it's deemed to be harmful, two, there are lots of situations
18 where you drop packets including congestion in your buffers, it's damaged,
19 you can't read the data and what have you, but nevertheless there are going
20 to be some packets in any system that are not going to go through, which is
21 why an aspect of the claim language is substantially all, rather than all
22 packets, because all packets would not go through in the real world, some of
23 them are going to be dropped for the aforementioned reasons, buffer
24 overflow, corruption, or being flagged as being harmful by the IDS.
25 JUDGE SAINDON: Do you know, and you might not have the
26 answer now, and you can do that later, does the expert testify on those

1 particular examples, or similar examples?

2 MR. AUCHTER: I believe so. I believe it's at paragraph 73 at

3 Exhibit 2010. I believe that's the closest he got to testifying on that

4 particular point, Your Honor.

5 JUDGE SAINDON: Okay, thank you.

6 MR. AUCHTER: Going to the issue I raised earlier regarding

7 prosecution history, that's addressed in slide 14. And the point here is that

8 in the case law, for a limitation to be a structural limitation and not merely a

9 statement of intended use, one of the factors that is considered is whether or

10 not the limitation was relevant to allow ability of the patent during

11 prosecution. In this case, in showing slide 14, this is referring to the 436

12 Patent prosecution, and again, what I meant when I said earlier that the

13 limitation was added is it was in allowable claim four if, which was objected

14 to, but they bonded into claim 1 and made the claim allowable by doing that

15 with respect to the 436 Patent, and Petitioners, in the district court litigation,

16 agreed with that, where they asserted that the only way the patentee was able

17 to get the claims of the 436 and 612 Patent allowed was by amending the

18 independent claims to include the substantially all limitation from dependent

19 claims. Looking at slide number 15, you see that that also occurred in the

20 612 Patent prosecution history, essentially the same limitation being brought

21 into the independent claims, to make the claims allowable over the prior art.

22 Just to go back to a point raised by the Petitioner, we do believe

23 that dispute one is not based on a faulty legal premise, I believe that the

24 claims clearly require, in the specifications it clearly discloses an

25 implementation in which all or substantially all of the packets go through the

26 system, through the claimed crypto engine, through the claimed packet

1 engine, and through the claimed IDS, and that's not what's disclosed in
2 Pham in any of the embodiments, and it's not appropriately limited to what
3 if you had just two packets going through situation, this is an apparatus in
4 which you're functioning and operating. And even in that situation, if you
5 had just the VPN, you would still have to establish the VPN, and that would
6 still require communications to the control processor, which would not, as
7 shown, ever get to any of the crypto processors, so it's not substantially all
8 would not go through the crypto processor in those embodiments. And that
9 doesn't even address bypassing, going through the switching fabric to the
10 egress processor.
11 JUDGE SAINDON: Just to follow up on that, my question that
12 I think I asked Petitioner before was, if Pham was installed in a certain way,
13 would it effectively be like a network interface card where there's only one
14 way traffic going through it, and -- or one device's traffic going through it,
15 so it's not a switch for multiple devices, it is just a VPN. It sounds like your
16 position is that the control messages still would mean that it does not meet
17 the claim limitations?
18 MR. AUCHTER: That's correct, Your Honor, because of the
19 control processor, Pham explicitly teaches that those packets would be sent
20 to a control processor and not to the crypto processor.
21 JUDGE SAINDON: Okay, are there other reasons, or is
22 control your chief --
23 MR. AUCHTER: No, Your Honor, the other reasons would be
24 the packets that go directly to the ingress and then to the egress processor
25 and bypass the crypto processors. And even in the case of the network
26 interface card, there's still going to be traffic, administrative traffic,

1 management traffic, LAN management traffic, et cetera, that would be going
2 across the network that would necessarily be seen and then just moved on or
3 ignored by the network interface card.
4 JUDGE SAINDON: I guess I was providing the example
5 where Pham was installed between one PC, a VPN, and then the internet,
6 there's no other LAN, there's no LAN, they're just in that configuration.
7 MR. AUCHTER: Even in that situation, Your Honor, there
8 would still be the control packets.
9 JUDGE SAINDON: Right, okay, I understand.
10 MR. AUCHTER: Do Your Honors have any further questions
11 on Pham in and of itself, and substantially all?
12 JUDGE SAINDON: No.
13 MR. AUCHTER: With respect to the so-called second dispute,
14 the expert did address whether or not there would be a motivation to
15 combine Wu with Pham, and the issues that were addressed, Your Honor, in
16 paragraphs 96 through 99 of Exhibit 2010, which is Dr. Cole's declaration in
17 support, and specifically we discussed, Dr. Cole discussed the issue of where
18 you would put it, and whether or not you would even need it if you were
19 talking about just a VPN connection, as we understood Petitioner to be
20 arguing. If you are discussing just a VPN connection, then you have a
21 secure connection and you would not be worried about intrusion detection.
22 If you didn't have just a pure VPN connection and you were worried about
23 intrusion detection, then you would not place it between the packet engine
24 and the crypto engine in the crypto processor/data processor of Pham, rather
25 you would place it in the ingress processor, where you would see the clear
26 text packets that would be coming through and would be more likely to have

1 intrusion characteristics, because those are coming from the internet to
2 establish a network, your secure connection, or anywhere, could be spoofed,
3 what have you. And you never see those in Pham's embodiment, because in
4 Pham's embodiment those would go to the control processor and would
5 never be looked at by the IDS that was positioned in between the packet
6 engine and the crypto engine in the crypto processors. And he specifically
7 addressed that in paragraph 98.
8 And there is obviously a tradeoff in complexity, but the position
9 here is that Pham teaches that it's not just increasing the complexity of your
10 operations and your code, Pham teaches that you may have to substitute or
11 add an additional general purpose microprocessor if you're going to perform
12 those kinds of processing steps in the crypto processor, which is
13 substantially more than just a little bit of increased complexity, it's basically
14 making sure you have an added processor within your system for each one
15 of your data processors and crypto processors, and that's what we're
16 referring to by the increased complexity that would be required. Do Your
17 Honors have any further questions regarding the combination of Wu and
18 Pham?
19 JUDGE AMUNDSON: This is Judge Amundson, I did have a
20 follow up question on that, and Petitioner's counsel said yes, it's going to be
21 more complex, but there's going to be tradeoffs, but you want to go with the
22 increased complexity because you're getting a lot more security. What's
23 your response to that point?
24 MR. AUCHTER: Our response to that point, Your Honor, is
25 that it's not just a little bit of increased complexity, it's actually adding an
26 extra processor to each one of your data processor nodes, and the delays that

1 would be incurred by having an additional data path, the increased costs and
2 expense of having an additional microprocessor, general purpose
3 microprocessor coordinating with the IBM network processor would be
4 significant, significant enough that that would lead a person of ordinary skill
5 in the art at the time to not add an intrusion database in accordance with the
6 teachings of Pham, inasmuch as Pham teaches that you're going to have to
7 add an extra processor, or replace your network processor with a general
8 purpose processor, in which case you have issues of bandwidth processing
9 capability and what have you, because the IBM MP is designed basically, it
10 appears based on the description of Pham, to just handle processing packets.
11 JUDGE AMUNDSON: All right, thank you, I think I
12 understand your position.
13 MR. AUCHTER: One other point, and this is just with respect
14 to the 436 Patent, Your Honor, if you look at slide 26, you see that the 436
15 Patent as Petitioner noted also includes providing a tag upon ingress. And
16 turning to slide 28, fundamentally the same issue here is that substantially all
17 the packets aren't going to be going through the crypto processor of the
18 identified network processor to have an SA header or an IP tunneling header
19 added if they're looking at the embodiment which you're using the SA table
20 within the network processor within the crypto processor, and not in the
21 ingress processor. And with that being the case, you would not have a tag
22 added in either a clear text packet that is bypassed or a packet that is directed
23 to the control processor. And that is again shown on slide 29, where we
24 talked about the filtering and the SA context, and why you would move it to
25 the control processor in order to add or create an SA path in the case that it
26 didn't exist, and those are again, limitations of claims 1 and 13 in the 436

1 Patent only.

2 Going on to grounds three and four, Your Honors, and looking
3 at slide 37 to start with claim four, the issue here is that the Petitioner failed
4 to show how one would implement the security processor on a single chip,
5 and in essence there was a conclusory statement that a person of ordinary
6 skill in the art would be motivated to do so, but there was no showing as to
7 how that would be done within the Petition. So if you look at slide 40, the
8 issue there is, on the right there is the drawing of Krishna that's provided in
9 the Petition, and as you can see there's essentially what's identified as a
10 packet engine or a packet classifier that the crypto engine down below,
11 presumably the switching is the packet data in, packet data out, although it's
12 not clear, but there's no showing as to how you would have an intrusion
13 detection system coupled between the crypto core and the packet engine
14 within this embodiment, whether or not it would be on the chip, off chip, or
15 how it would be done, and it's simply a failure of proof and meeting the
16 burden on showing how that particular limitation or those limitations in
17 claims 4, 7, and 8 would be met.

18 JUDGE SAINDON: Counsel, just so I understand here, are
19 you saying that this isn't within the level of ordinary skill to implement it, or
20 are you just saying we don't actually know what Petitioner's proposed
21 combination is?

22 MR. AUCHTER: A combination of the two, Your Honor,
23 although more accurately that would pertain to the next slides, in claim 17,
24 because claims 4, 7, and 8 don't necessarily include the signature database,
25 which would be, we believe, a difficult implementation issue, but it's more
26 that they just don't show how you would do it, whether we should do it

1 inside the chip, we should do it with a connection interposed in between the
2 crypto core and the packet engine in Krishna, how would you do it, where
3 would you do it, and none of that is shown, it simply says that a person of
4 ordinary skill in the art would have modified what is shown here to add this
5 additional functionality, including the IDS.
6 JUDGE SAINDON: I guess I put out those two alternatives,
7 one being level of skill, because I don't think the challenged patents say
8 much on this either, is that correct, presuming that it is known in the art how
9 to do these types of things?
10 MR. AUCHTER: That is correct, Your Honor, they show how
11 it would be done, and they claim it on a single chip and they say you could
12 do this, but they don't necessarily show how you would do it. Although,
13 within the challenged patents they're saying, take what we're showing you
14 here in the drawings of the entire system and including fairly detailed
15 discussions of buffering and various kinds of memory structures and what
16 have you, how that would be done within their system, so they are at least
17 providing an example of a specific construction and not saying, you know,
18 put it anywhere, rather they're saying okay, here's what we have, here are
19 some various memory configurations that we've got for, I think it's the
20 extended data out, and some other kinds of data out in the operations, and
21 that's why you could do it on a single chip, which is more information that is
22 provided by Krishna.
23 JUDGE SAINDON: Okay, understood.
24 JUDGE AMUNDSON: This is Judge Amundson, I had a
25 question on this issue, and it concerns the state of the art, and on the
26 Petitioner's slide 33, they have a quote, the cryptographic processing was

1 moving away from discrete processors and was being implemented on a
2 single chip. So my question is, does Patent Owner dispute that as a factual
3 matter?
4 MR. AUCHTER: No, Your Honor, Krishna shows
5 cryptographic processing on a single chip, but Krishna does not show an
6 intrusion detection system or a signature database on a single chip.
7 JUDGE AMUNDSON: All right, thank you.
8 MR. AUCHTER: And then moving on to slide 43, which is
9 dependent from claim 13, and the issue here is that, for claim 17, is the
10 security processor is formed on a single chip. And if one looks back on slide
11 42, the security processor that's claimed includes, of course switching
12 system, packet engine, cryptographic core, a signature database, an intrusion
13 detection system, a local data bus and memory, all of which are part of the
14 so-called, the claimed security processor. And more emphatically than with
15 respect to the claims that are dependent from claim 1, there's no disclosure
16 as to how you would implement the entire security processor on a single
17 chip, and that's in grounds four. Are there any further questions, Your
18 Honors?
19 JUDGE SAINDON: None from me.
20 MR. AUCHTER: Then we'd like to reserve our additional time
21 for rebuttal, please, thank you.
22 MR. MCPHERSON: Your Honors, you heard a lot of language
23 about what the intention of the patent was, and he started off explaining that
24 their intention was there's no holes. But we're not dealing with the intention
25 of the patent, I've got to deal with the claim language, and I don't see this
26 'no holes' claim language in the claims.

1 Specifically, the preamble does not limit it to every single
2 packet, it's just the packets that are going to the security processor, and that
3 in fact literally reads on two packets coming from the LAN going to the
4 encryption processor. That's the end of discussion, that's dispositive.
5 That's the scope of the claim, the scopes of the claims read on our
6 embodiment, which shows in Figure 6, both for the 436 and the 612 Patent.
7 There's also a disconnect between what the patents in suit are
8 saying and what their arguments are. On their slide 12, they read a passage
9 to you, and it says regardless of destination, whether for example it is to
10 streaming interface 200, host interface 206, control processor 212, or a loop
11 around the packet engine 228, all packet data preferably flows to a packet
12 engine 228, and then to a corresponding cryptographic core 232, all right?
13 But in their patents, if they're not encrypted, they don't go to the
14 cryptographic core. So them pointing to this and saying of all packets, right,
15 all packets are being processed and then going to a cryptographic core, that
16 doesn't cover all their situations, because they have packets that don't go to
17 a cryptographic core. The patents aren't sending packets that don't need to
18 be encrypted to a cryptographic core, either in Pham or in theirs. So trying
19 to use that language to bootstrap that everything has to go to the packet
20 engine in the crypto core, that's not the corresponding disclosure in their
21 patents.
22 Judge Saindon, you asked a question regarding the DI, and the
23 DI did raise an issue that was kind of academic when you look at the claim
24 language they use, but what's the structural difference between a packet
25 engine processing all the packets or a subset of packets? How is that a
26 structural limitation, that they only process some of them? There's no

1 method claims in any of these patents, right, we're dealing with structural
2 limitations, and how is that a structural limitation, that I'm only going to
3 receive some packets? When you're not even talking about the processing
4 being done, other than the 436 which talks about tagging it, classifying and
5 tagging it, right, we're not even talking about encrypting and decrypting, we
6 just say we have a cryptographic core. So it comes down to, are these just
7 really capability claims?
8 And at the outset, and the end of the day it's kind of academic,
9 because we've shown that Pham is a parallel disclosure, that for each
10 component they recite in the claims of claim one, there's a corresponding
11 component situated the exact same way in Pham. And they can say oh, but
12 it's a network interface card. Well, the claims aren't limited to a network
13 interface card. And their disclosure about whether to be a network interface
14 card is a throwaway line, if you look at that. And he goes back to his last
15 comments about grounds three and four, that there is no disclosure in the
16 packets of how to arrange an IDS and a database on a chip, or how you
17 arrange some components, but not the IDS, as he admitted it would be very
18 difficult to do. What's their claims? There's no disclosure in there, and
19 there's no disclosure because it was well known to one of ordinary skill in
20 the art, which is why we had the state of the art section in there. So they
21 don't get to throw stones at us and say well Pham doesn't disclose how you
22 do that, when their own patents don't disclose how to do that, and yet we
23 have a section that discloses why there's no description in there, and that's
24 all we're required to do, is to describe what one of ordinary skill in the art
25 would do and a rationale for it, and they have not come back with any
26 response from their expert citing to the facts that we're incorrect.

1 There's also some language about how the patent got allowed.
2 For the 436 Patent, which was the first patent, as we discuss on page 12 of
3 the petition for the 436, the claim was only allowed after the Examiner did
4 an examiner's amendment. That examiner's amendment was directed at the
5 tag, the classification and the tag, that's why the claim was allowed. And
6 the Examiner should have not allowed the 612 Patent, it didn't have a
7 limitation in there, because that's why he allowed the 436. So I just want to
8 make the record clear on that.
9 And there was also some discussion about the limits of Pham,
10 and it could only do compression if it uses an additional general purpose
11 computer, and that's one embodiment that's described, but that ignores the
12 teaching of Pham that I went though, where compression, decompression, all
13 the functions. So Pham describes that each one of these processes are
14 compute intensive, and each one of those can be done on the data packets,
15 the data processors, and each one of those can be offloaded --
16 JUDGE AMUNDSON: This is Judge Amundson, if I could
17 interrupt, it seems like you're referring to something in Pham, or I'm not
18 sure what you're referring to.
19 MR. MCPHERSON: I'm on slide 15 of Petitioner's
20 demonstratives, I apologize.
21 JUDGE AMUNDSON: All right, very good, thank you.
22 MR. MCPHERSON: This is a listing of the processes that
23 Pham describes as compute intensive. And I went through each one of these
24 and I asked our expert, was this compute intensive, is this the type of process
25 that would be offloaded from the ingress processor to a data packet
26 processor? And if you look, Pham describes about scaling up, having data

1 processors that can perform more than one of these operations, and also
2 having the ability to send the packets from one data processor to the next
3 data processor. And so the capability to do that is described right in Pham,
4 and if that's the complexity that wasn't contemplated by Pham, we disagree.
5 We think Pham discloses that, and would include, this is not exhaustive,
6 would include an intrusion detection system. That's a compute intensive,
7 and Pham already has a database, it does look-ups, and Krishna describes
8 that look-ups can be done, a table look-up can be done on a chip, and so that
9 was all within the broad disclosure of Pham. And what we keep hearing is
10 this narrowing down that Pham only does this, Pham only does that, Pham
11 has the ability to do everything the 612 and the 436 Patents do. And unless
12 there are any more questions, I have no more points.
13 JUDGE SAINDON: I do, I have some questions. Okay, so
14 let's go back to the substantially all limitation. We have the security
15 processor, which has the switching system and the packet engine, and the
16 packet engine basically sees all of the, substantially all of the incoming and
17 outgoing packets. As I understand, they don't necessarily make it to the
18 cryptographic core, which is a point you were making earlier, so I want to
19 make sure I understand what you're saying there. So in the challenged
20 patents it sounds like it's okay if it goes into the switching system, to the
21 packet engine, and then back out without going to the cryptographic core,
22 that still substantially all make it to the packet engine. Do I understand that
23 correct?
24 MR. MCPHERSON: In the patents themselves?
25 JUDGE SAINDON: Yeah.
26 MR. MCPHERSON: And the patents themselves describe, in

1 the passages I showed that all that make it to the packet engine, all go to a
2 crypto core, in the embodiment described there.
3 JUDGE SAINDON: Okay, but it doesn't have to, according to
4 the claims? We just need to go to the packet engine, and that's as far as we
5 need to go?
6 MR. MCPHERSON: Correct.
7 JUDGE SAINDON: Okay, okay. I'm trying to think if I have
8 any more questions on substantially all, because I see that as kind of the
9 biggest issue here. I can't think of any.
10 MR. MCPHERSON: I mean, if the Patent Owner wanted to,
11 and wanted to capture this 'no holes,' they could have filed a motion to
12 amend and amended the preamble, because the substantially all comes off
13 the preamble, and it's really the preamble they're arguing, is that, what is the
14 security processor receiving? All, or whatever it is, over a stream, over three
15 days, over this network, from this network, but none of that made it in there,
16 so they're trying to shoehorn it in by saying the substantially all down here.
17 Well, that substantially all is just referring back to whatever packets we're
18 talking about in the security processor, and we're allowed to limit that to two
19 packets, or ten packets, or 12 packets, and it's only substantially all of those
20 two packets, or 10 packets, or 12 packets, need to go to the security
21 processor. And when you have this situation where all the packets are going
22 from a LAN and going to a WAN, or vice versa, substantially all of them are
23 going to go through the processing engine to the crypto core, and that's why
24 the claim read on Pham.
25 JUDGE SAINDON: And Patent Owner had spoken quite a bit
26 about the control -- I forget the exact language.

1 MR. MCPHERSON: The control processor.

2 JUDGE SAINDON: Yes.

3 MR. MCPHERSON: That's the same argument as saying well,
4 if it's just going from one LAN to the other LAN, it doesn't need to go
5 through processing. And the question is, well, in my example, Pham is only
6 talking about packets that do need that, and that's where the invalidity comes
7 from, from the example provided in Pham, where all the packets do need
8 crypto processing, kind of like the same example that I just read from the
9 patent, where all the packets go from the packet engine to crypto processing.
10 That's an example of that. And the claim would read on that embodiment,
11 or specification.

12 JUDGE SAINDON: I have no further questions. From the
13 panel? Okay, thank you. And Patent Owner, I have 16 minutes left for you
14 if you'd care to use that.

15 MR. AUCHTER: Thank you, Your Honor. So to go back to a
16 question you had asked earlier, if I could just, citing to Exhibit 1001, the 436
17 Patent, and where it discusses and discloses specifically that all or
18 substantially all of the packets, a transitive packet engine in the disclosure,
19 first off, that is in the abstract, in the first five lines, where it specifically
20 says that the security processor performs all or substantially all security
21 network processing, the security processor sends and receives all incoming
22 and outgoing data packets. And that is also in -- and I'm just referring to the
23 436 patent disclosure, and not the 612 and the 436, because they're
24 substantially identical, but there is some difference in line numbering
25 throughout.

26 In column three, line 28, they talk about the I/O interface or

1 system that provides improved security for all or substantially all
2 communications received and sent by trusted hardware, further I'm
3 describing that through line 34 of column three. In addition, it discusses at
4 column three, lines 43 to 49 the secure I/O system of the present invention
5 permits performing all or substantially all network processing functions. It's
6 further described in the context of all or substantially all in column four,
7 lines 40 to 45, and lines 56 to 58, security processor 104 preferably handles
8 all network and security processing functions from the data packets to
9 provide the most secure I/O interface.
10 It's further described in column six, lines 29 through 36 by
11 performing all or most security and networking processing for I/O
12 communications, also it's further described and discussed at column 11,
13 lines nine through 11, all incoming packets to security processor 104 may be
14 initially processed by one of package engines 228. Further, in column 11
15 and line 52 through line 59, accordingly all or substantially all packet and
16 data flow may return to the corresponding packet engine 228 from the
17 cryptographic core 232, prior to output. It's also further described into
18 column 12, lines two through five, control processor 212 and firmware 214
19 may provide all or substantially all of control. It's also further described at
20 column 18, lines 48 to 53, according to the present invention, by passing all
21 I/O traffic to host processor, at column 20, line 10, regardless of destination,
22 whether for example it is streaming interface 200, host interface 206, control
23 processor 212, or a loop through a packet engine 228, all packet data
24 preferably flows from packet engine 228 and then to a corresponding
25 cryptographic core 232, and that's column 20, lines 10 through 14.
26 JUDGE SAINDON: Counsel, can we go back to one of those, I

1 am trying to find it again. Column six, line 33 or so, where it gives a
2 percentage, could you put that into context for me?
3 MR. AUCHTER: Sure. By performing all or most security and
4 networking processing for I/O communications to host processor 130 and
5 security processing system 102, a large proportion for example of greater
6 than about 50-90% of VPN and firewall I/O data loops may be handled in
7 secure processing system 102 without intervention by host processor 103. In
8 addition, all or most security and network exception processing may be
9 hemmed by security processing system 102. That's discussing the situation
10 where the host processor may provide additional support or systems in the
11 situation, it's not talking about all the processing, it's the data loops within,
12 as I understood that paragraph to be referring.
13 JUDGE SAINDON: 130, the host processor, being -- is that the
14 CPU?
15 MR. AUCHTER: The host processor is, if you look on Figure
16 3, which I believe is -- it's on one of our slides as well. If you look through
17 it, Your Honor --
18 JUDGE SAINDON: Figure 2, slide 12?
19 MR. AUCHTER: Figure 2 shows there's a host processor,
20 should be -- I think it's connected to the host interface, but I'm not sure.
21 JUDGE SAINDON: I see the host processor in Figure 1 of the
22 436 Patent.
23 MR. AUCHTER: There we go, yes, that's it, and that goes
24 through the host bridge, which is what was shown in the Figure 3 that I was
25 looking at. And that's the discussion of -- it has the limitations of the local
26 data bus, and also having the modular engine attached to the local data bus

1 and the dependent claims, I think it's three and four, or three and five, but
2 I'm not sure off the top of my head. So, there are a lot of claims, it's hard to
3 memorize them all.
4 JUDGE SAINDON: So in any event, this 50-90% isn't talking
5 about substantially all of the packets?
6 MR. AUCHTER: No, Your Honor, I do not understand that as
7 being substantially all of the packets going through, I think substantially all
8 of the packets going through means substantially all of the packets.
9 JUDGE SAINDON: Okay.
10 MR. AUCHTER: Directing your attention to claim 3, I'm
11 sorry, not claim three, slide three, my apologies. Pointing out that the
12 preamble of claim 1 is a security processor to process incoming packets and
13 outgoing packets, and then it's claim four, or claim element four, rather,
14 which is in the body of the claim, where you see substantially all appearing.
15 It's not a preamble limitation, it's a limitation in the body, and that's one of
16 the reasons why it is not a statement of intended use, or why we believe that
17 the case law that's directed to the preamble is not directly pertinent because
18 it's a limitation within the body of the claim.
19 I would also point out that at least the claims in the 436 Patent
20 do require that the packets do go through the cryptographic core as well as
21 the packet engine, because it says in claim limitation V, the tag determines
22 an egress path within a security processor upon exit from a corresponding
23 cryptographic core. Now that limitation does not appear in the 612 Patent,
24 but it is in the independent claims of the 436 Patent. And then this point,
25 regarding the preamble, we make in slide number 10 as well. And the point
26 here being that it is appropriate to use functional language to limit the

1 structure, the case law that we discussed in the sur-reply, it goes to that at
2 some lengths, I won't go there this morning unless Your Honor wishes me to
3 do so. And the fact that it's a structural limitation is further reflected in
4 slides 11, 12, and 13. Are there any further questions, Your Honors?
5 JUDGE SAINDON: I have no further questions, looks like the
6 panel does not either.
7 MR. AUCHTER: Thank you, Your Honors.
8 JUDGE SAINDON: All right, thank you. The panel would
9 like to thank both parties for their presentation today. It was very helpful
10 discussion. We are adjourned.
11 (Whereupon, the above-entitled matter went off the
12 record at 10:56 a.m.)

PETITIONER:

Patrick McPherson
Patrick Muldoon
Paul Belnap
Donald English
Nicole Candelori
Monte Squire
DUANE MORRIS LLP
pdmcpherson@duanemorris.com
pcmuldoon@duanemorris.com
phbelnap@duanemorris.com
djenglish@duanemorris.com
ncandelori@duanemorris.com
mtsquire@duanemorris.com

Eric Buresh
Mark Lang
ERISE IP, P.A.
eric.buresh@eriseip.com
mark.lang@eriseip.com

PATENT OWNER:

Brett Cooper
BC LAW GROUP, P.C.
bcooper@bc-lawgroup.com

Robert A. Auchter
AUCHTER PLLC
robert@auchterlaw.com