

PETITIONER'S TRIAL HEARING DEMONSTRATIVES

PALO ALTO NETWORKS, INC. and
FORTINET, INC.,
Petitioner,

V.

LIONRA TECHNOLOGIES LTD.,

Patent Owner.

IPR2023-00703¹

IPR2023-00673²

TRIAL HEARING

JULY 23, 2024

¹ The Board joined Palo Alto Networks, Inc. and Fortinet, Inc. as parties (Petitioner) to this proceeding via a Motion for Joinder in IPR2024-00158.

² The Board joined Palo Alto Networks, Inc. and Fortinet, Inc. as parties (Petitioner) to this proceeding via a Motion for Joinder in IPR2024-00099.

Overview of Grounds

Ground	Basis	Cited Art	'436 Claims	'612 Claims
1	103	Pham in view of Wu	1-2, 9-13, 16, 22	1-2, 9-13, 16, 22
2	103	Pham in view of Wu and Collins	3, 14, 21	3, 14, 21
3	103	Pham in view of Wu and Collins and Krishna	4, 7, 8	4, 7, 8
4	103	Pham in view of Wu and Krishna	17	17

Overview of Dispute

Dispute	Basis	'436 Claims	'612 Claims
1	Whether Pham discloses “ <i>substantially all of the incoming packets and outgoing packets to the security processor transit one of the plurality of packet engines</i> ”	1, 13	1, 13
2	Whether a POSA would be motivated to modify the teachings of Pham with the teachings of Wu	1, 13	1, 13
3	Whether a POSA would be motivated to include security functions on a single chip	4, 7, 8, 17	4, 7, 8, 17

Overview of '436/'612 Patent

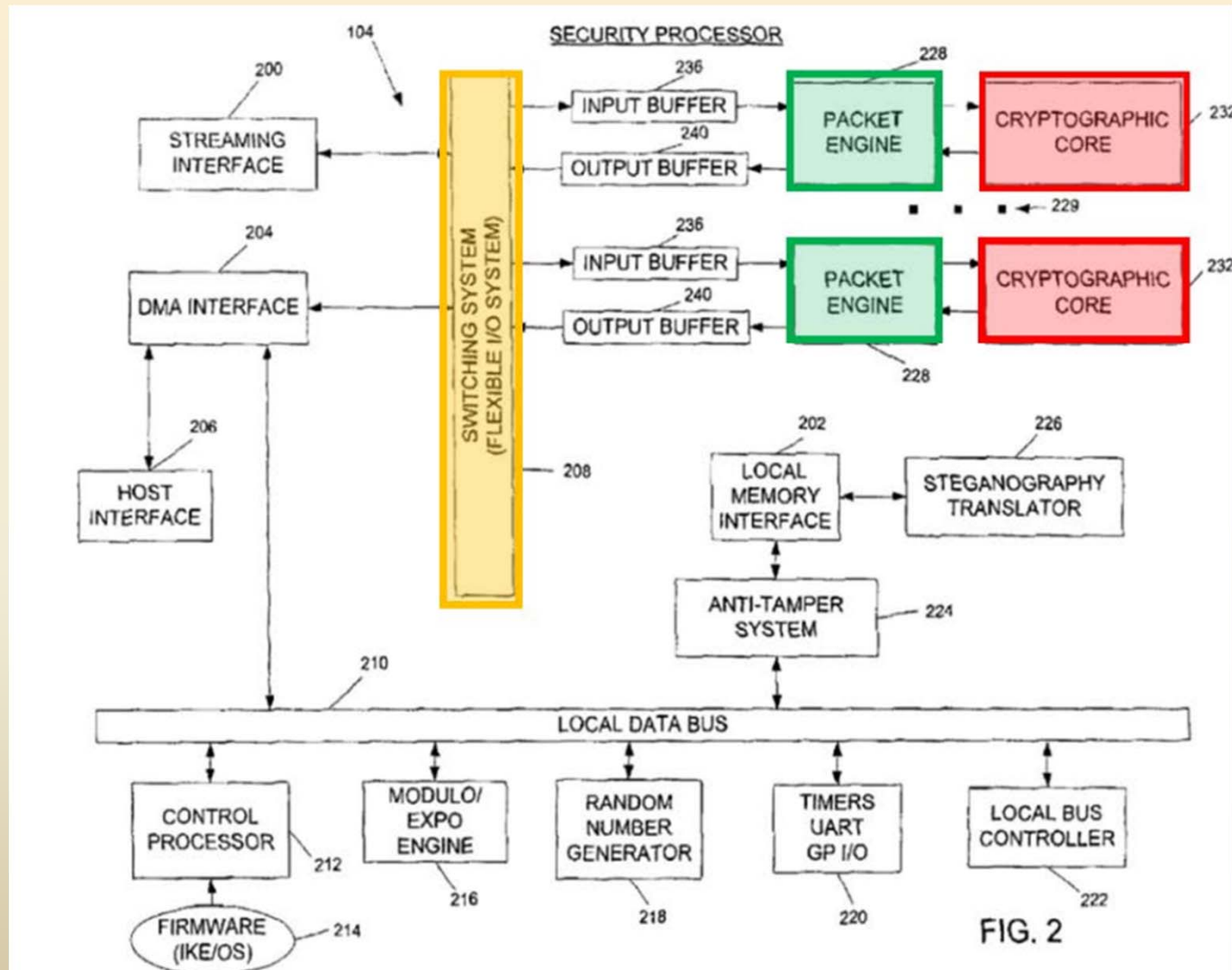
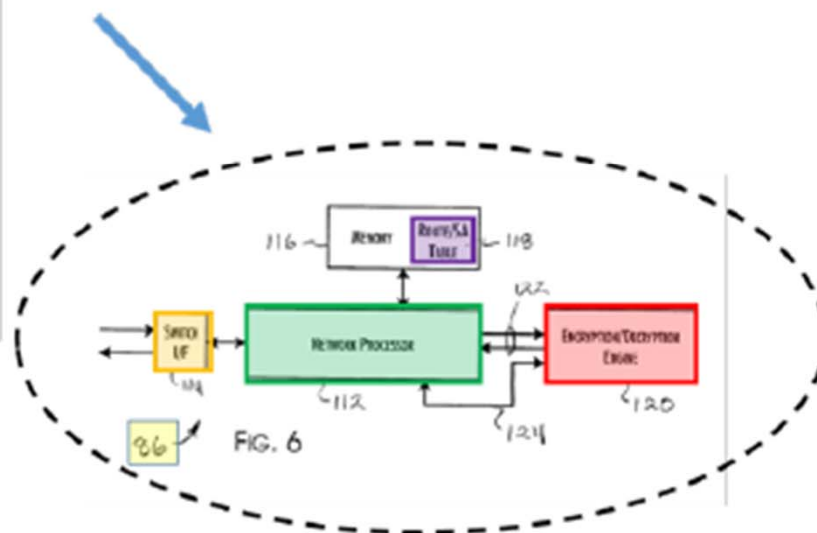
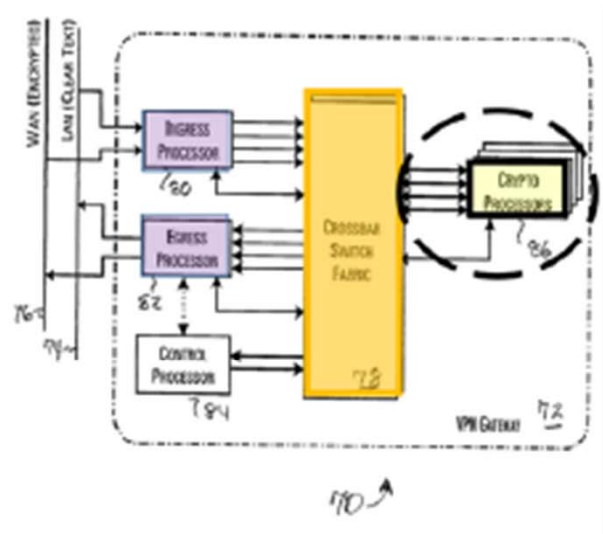


FIG. 2

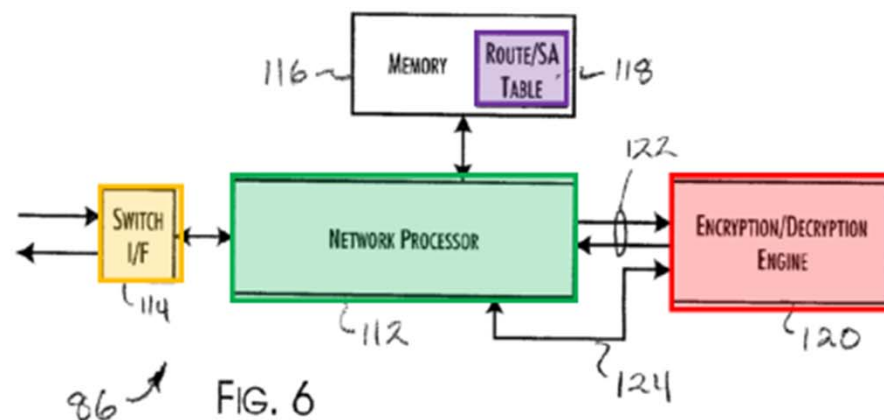
Overview of Ground 1

Overview of Pham



EX-1004, Figs. 4 and 6

Overview of Pham



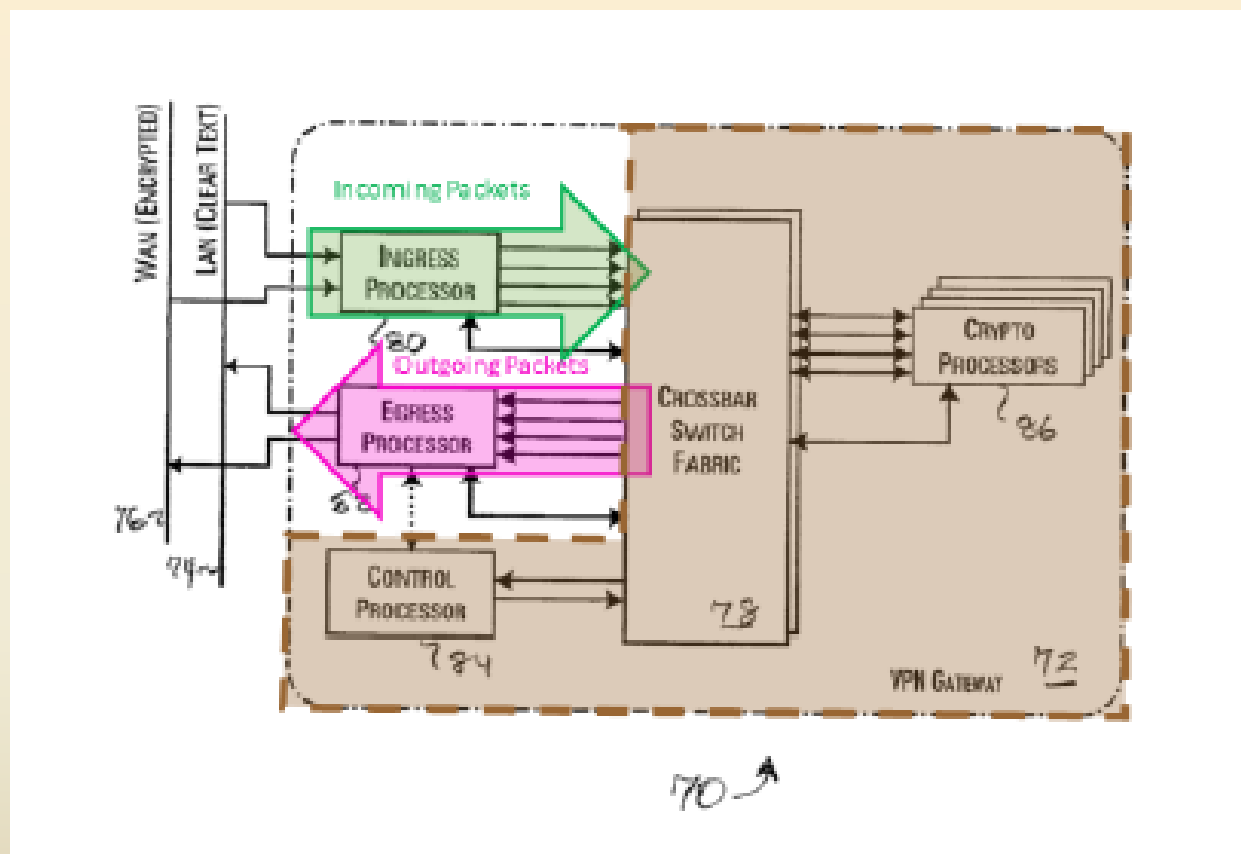
EX-1004, Fig. 6

Dispute 1: *“substantially all of the incoming packets and outgoing packets to the security processor transit one of the plurality of packet engines”*

Claim 1

- I. A security processor to process **incoming packets and outgoing packets**, the security processor comprising:
 - a switching system to send the outgoing packets and receive the incoming packets;
 - a packet engine, coupled to the switching system, to handle classification processing for the incoming packets received by the packet engine from the switching system and the outgoing packets sent by the packet engine to the switching system, wherein the packet engine is one of a plurality of packet engines and **substantially all of the incoming packets and outgoing packets to the security processor transit one of the plurality of packet engines**, and wherein the incoming packets and outgoing packets are provided with a tag upon ingress to one of the plurality of packet engines and the tag determines an egress path within the security processor upon exit from a corresponding cryptographic core;
 - a cryptographic core, coupled to the packet engine and receiving the incoming packets from the switching system via the packet engine and communicating the out going packets to the switching system via the packet engine, to provide encryption and decryption processing for packets received from and sent to the packet engine, wherein the packet engine is interposed between the switching system and the cryptographic core;
 - a signature database; and
 - an intrusion detection system coupled between the crypto graphic core and the packet engine and responsive to at least one packet matching a signature stored in the signature database.

Pham discloses that the networks processors 112 process substantially all the data packets received and transmitted by the VPN Gateway.



Pet. 34 (citing EX-1004 FIG. 4; EX-1003 ¶78)

PO Improperly Restricts the Teachings of Pham

- “**only** the SA parameter association task may be offloaded to crypto processor 80.” POR 26.
- Clear text does not require any processing. POR 22.

No dispute that the crypto processor is a data processor

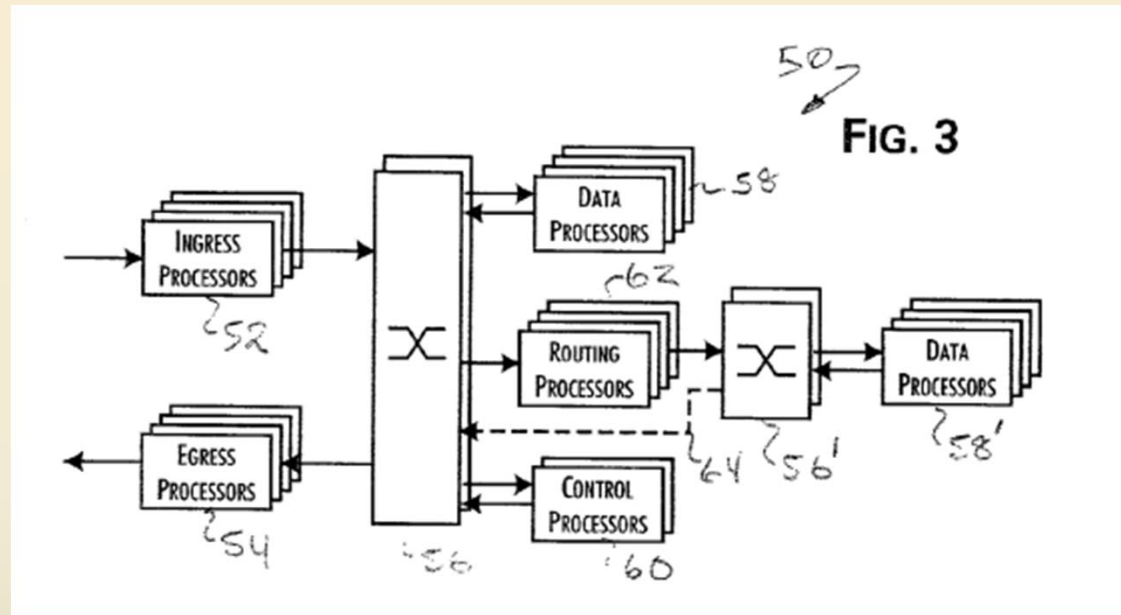
- “a plurality of data packet processors in the form of crypto processors (yellow) coupled through a data switch fabric (orange) between network connection processors (purple). Ex-1004 Abstract; EX-1003” Pet. 21
- In Pham’s VPN gateway, there are network ingress processors, egress processors, and data packet (crypto) processors. *Id.*, [0039]. POR 10.

No dispute that the crypto processor is a data processor

- Further, Pham discloses that crypto processor 86 in FIG. 4 is a type of data processor illustrated in FIG. 3, that can be flexibly configured to implement any of a number of different network protocol processing functions including those that are compute intensive.
 - “a preferred VPN embodiment 70 of the present invention, representing a specific implementation of the extended protocol processor architecture 50 [FIG. 3], is shown in Fig. 4.” EX-1004 [0045].

Pet. Rep. 7 (citing EX-1004 [0017], [0042] EX-1016 22:19-23:18; EX-1017 ¶14).

No dispute that the crypto processor is a data processor



Pham describes that data processors can perform compute intensive processing

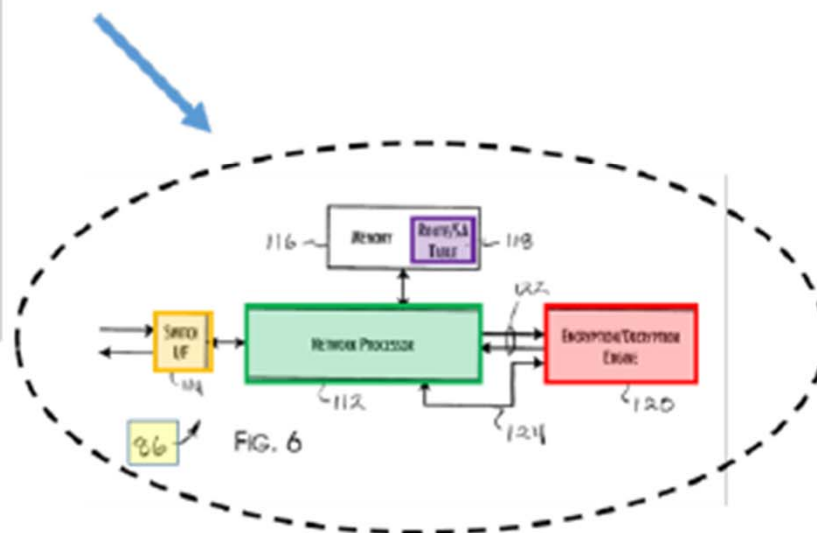
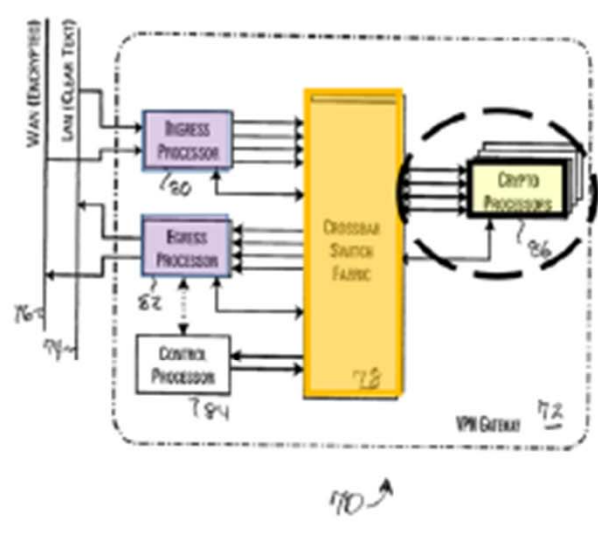
- compression
- decompression
- protocol translation
- encryption
- decryption
- routing
- load balancing
- filtering
- switching

Pet. Rep. 5 (citing EX-1004 [0042] EX-1016 22:19-29:25; EX-1017 ¶11)

Pham describes that data processors can perform multiple processes

- “data processors can be flexibly configured to handle **any number** of different protocol processing functions”
- “The individual data packet processors 58 may be configured to perform a single protocol conversion operation or **multiple related operations.**”
 - “For example, packet data can be compressed before encryption and decompressed following decryption. **Single data processors 58 can be used to perform multiple compute intensive operations** or the fast path processing of network data packets may be extended to include the transfer of data packets between multiple data packet processors 58 before finally being forwarded on to an egress processor 54.”

Pham discloses that the networks processors 112 process substantially all the data packets received and transmitted by the VPN Gateway.

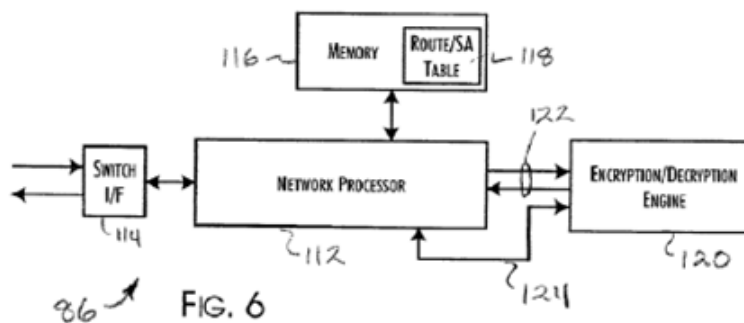
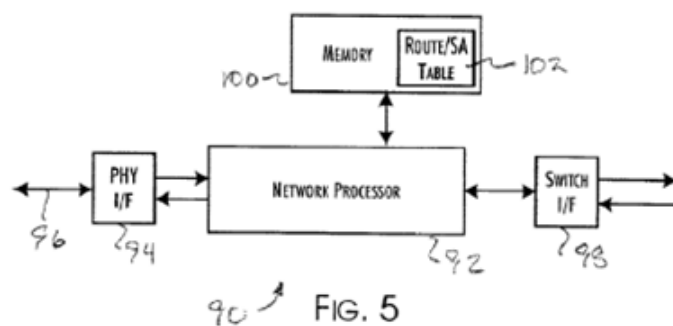


Pet. 22 (citing EX-1004 FIG. 4; EX-1003 ¶78)

All packet processing except basic switching and filtering can be offloaded from the ingress processor to the crypto processor

- For example, in one embodiment, Pham discloses that ingress processor 80 (Fig. 5) and network processor 112 in crypto processor 86 (Fig. 6) use the identical conventional processors and identical routing and SA tables to allow functions of the ingress processor to be offloaded to network processor 112, such as packet routing, SA parameter association and compression and decompression. EX-1004 Figs. 5, 6, [0049], [0051], [0053]. Thus, all packets, both clear text and encrypted can be sent to network processor 112 for routing using routing and SA table 118. EX-1003 ¶ 89.

The network processor 92 of the ingress processor 90 is identical to the network processor 112 of the crypto processor 86



EX-1004 FIGs. 5, 6; EX-1017 ¶15.

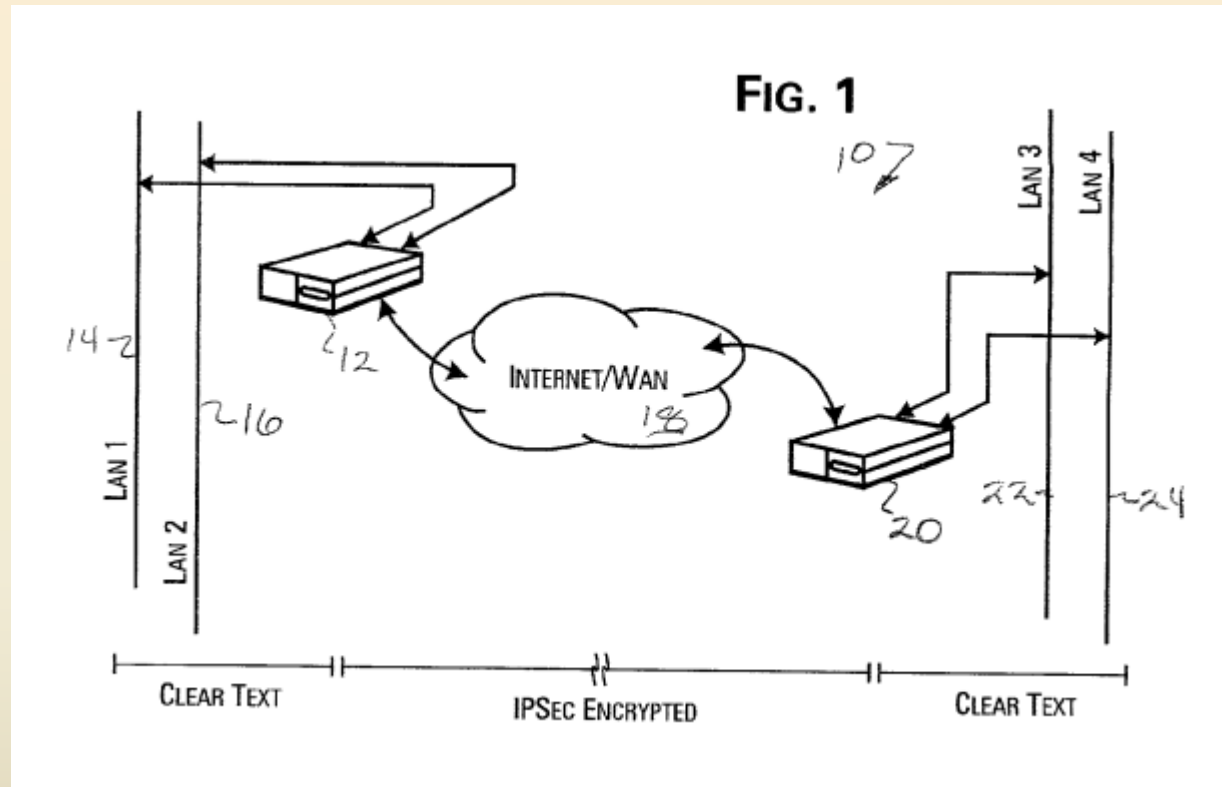
Any compute intensive tasks may be offloaded to crypto processor

- “Still another advantage of the present invention is that the network data processors can be flexibly configured to implement **any of a number of different network protocol processing functions including particularly those that are compute intensive.**” EX-1004 [0017]
- Multiple scalable arrays of data packet processors 58 can be directly connected to the switch fabrics 56 to provide **various forms of protocol data processing, characterized as involving significant computation intensive operations.** The individual data packet processors 58 may be configured to perform a single protocol conversion operation or **multiple related operations.** EX-1004 [0042]

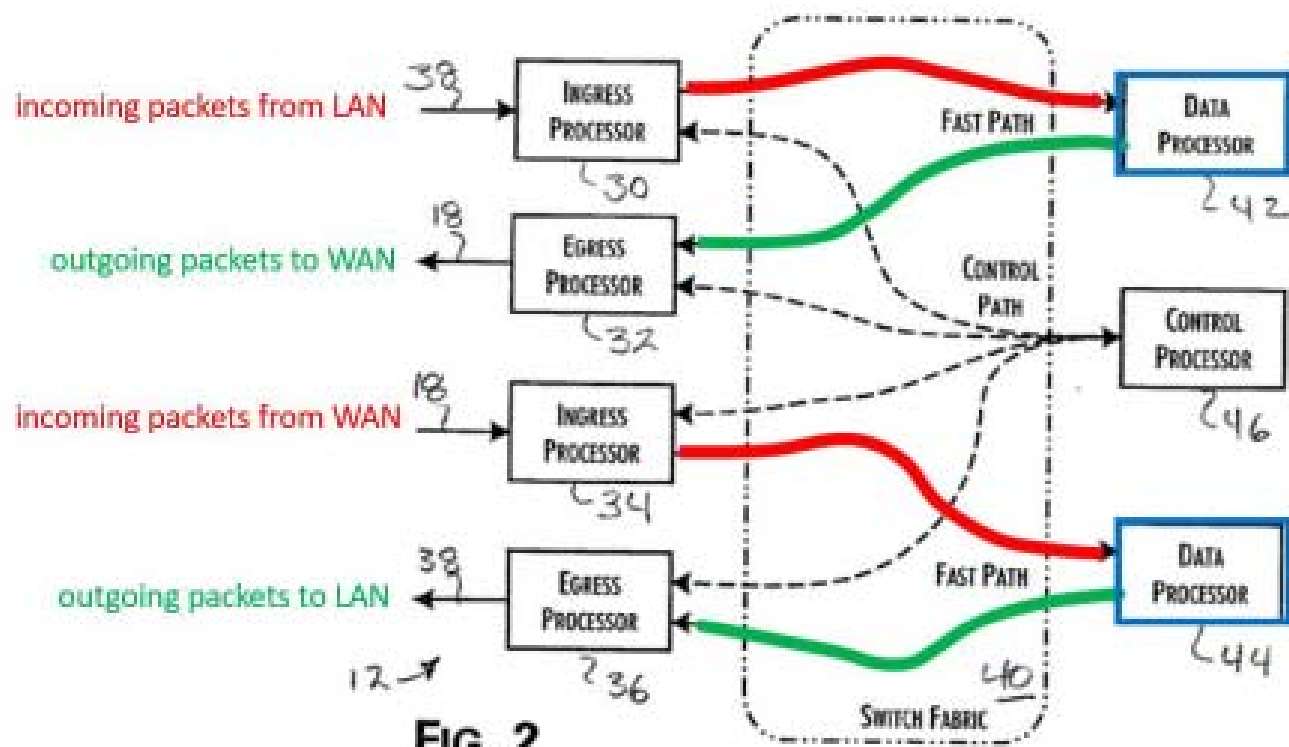
Clear text can require processing provided by crypto processor

- “With substantially increasing wire-speed, the computational capabilities of the ingress processors 52 may become insufficient to timely perform **all of the required filtering, routing and load-balancing functions.**” EX-1004 [0043]
- Although the POR restricts its analysis to an example where clear text packets are sent directly from LAN 1 to another LAN 2 to argue that no packet processing is needed, another packet processing function that would be performed by the crypto engine even for packets being sent from LAN 1 to LAN 2, would be protocol translation where LAN 1 uses a first protocol and LAN 2 uses a second protocol. This a common scenario, and yet PO’s expert did not consider this scenario. EX-1016 88:8-13.

Clear text can require processing provided by crypto processor



Pham shows embodiments where all packets are sent for processing outside ingress processor



EX-1004 FIG. 2; EX-1017 ¶9.

Pham shows embodiments where all packets are sent for processing outside ingress processor

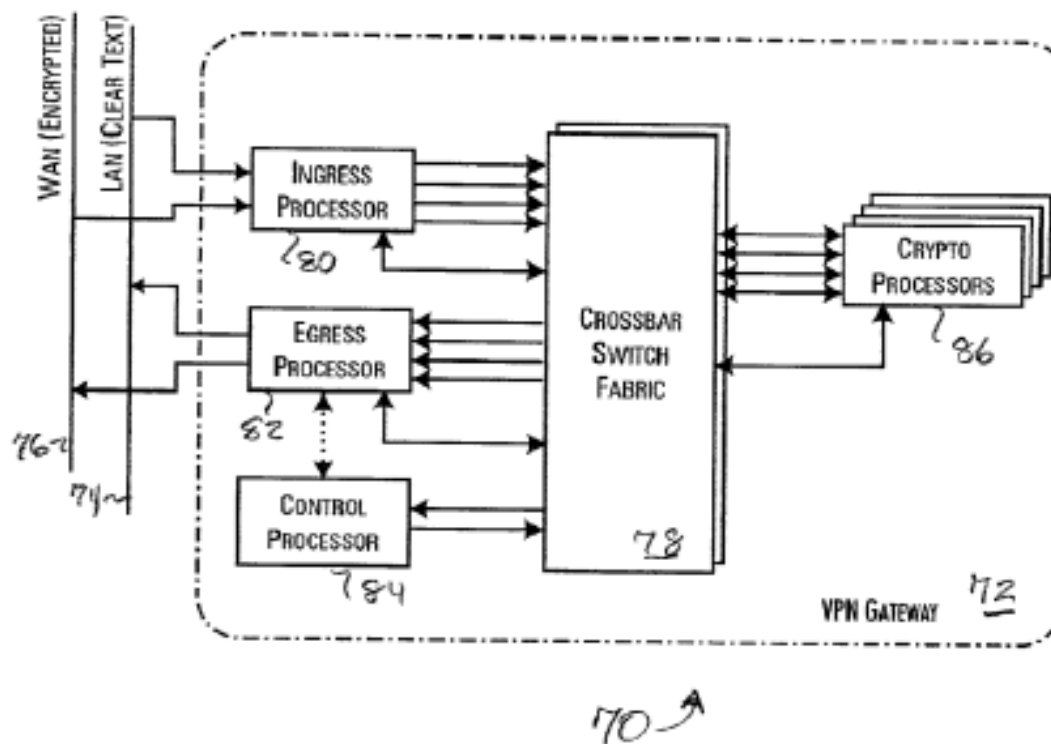


FIG. 4

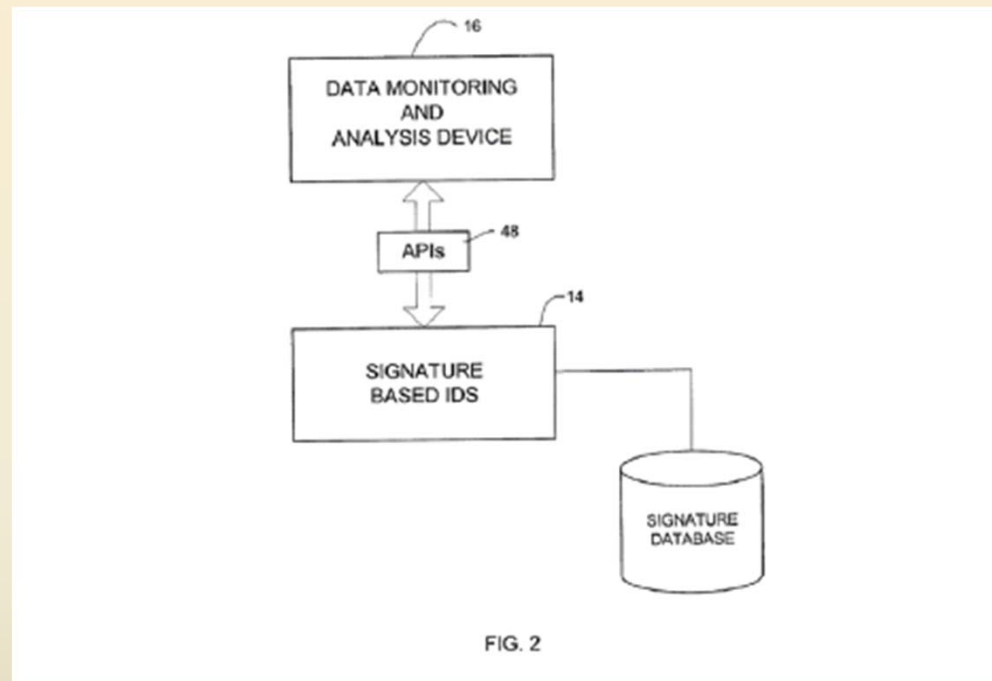
EX-1004 FIG. 4; EX-1017 ¶13.

Dispute 2: Whether a POSA would be motivated to modify the teachings of Pham with the teachings of Wu

Claim 1

- I. A security processor to process incoming packets and outgoing packets, the security processor comprising:
 - a switching system to send the outgoing packets and receive the incoming packets;
 - a packet engine, coupled to the switching system, to handle classification processing for the incoming packets received by the packet engine from the switching system and the outgoing packets sent by the packet engine to the switching system, wherein the packet engine is one of a plurality of packet engines and substantially all of the incoming packets and outgoing packets to the security processor transit one of the plurality of packet engines, and wherein the incoming packets and outgoing packets are provided with a tag upon ingress to one of the plurality of packet engines and the tag determines an egress path within the security processor upon exit from a corresponding cryptographic core;
 - a cryptographic core, coupled to the packet engine and receiving the incoming packets from the switching system via the packet engine and communicating the outgoing packets to the switching system via the packet engine, to provide encryption and decryption processing for packets received from and sent to the packet engine, wherein the packet engine is interposed between the switching system and the cryptographic core;
 - a signature database; and
 - an intrusion detection system coupled between the cryptographic core and the packet engine and responsive to at least one packet matching a signature stored in the signature database.

Overview of Wu



EX-1005, Fig. 2

Motivation to Combine Pham and Wu

- State of the Art
 - Common use of intrusion detection systems (IDS) having a signature database, and placing the IDS “at endpoints where encryption and decryption are performed such that it can inspect unencrypted traffic.”
Pet. 15-19 (citing EX-1015; EX-1003 ¶¶51-59))
- Motivation to Combine
 - Motivation to modify the teachings of Pham to include an intrusion detection system and signature database interposed between the packet engine and the cryptographic core, e.g., at the endpoint where encryption and decryption are performed.
Pet. 26-32 (citing EX-1003 ¶¶70-76).

Motivation to Combine Pham and Wu

- Petitioner's evidence is un rebutted
 - PO expert did not address State of the Art section or motivation to combine
 - POR is based solely on attorney argument
 - “increased complexity and resources required”
 - Same clear text argument from Dispute I

Dispute 3: Whether a POSA would be motivated to include security functions on a single chip

Single Chip Limitations

4. The security processor of claim 3 wherein the packet engine, the cryptographic core, and the modulo engine are formed on a single chip.

17. The security processing system of claim 13 wherein the security processor is formed on a single chip.

Motivation to Combine Pham and Krishna

- Krishna
 - Krishna discloses a packet engine (green), a cryptographic core(red) and **other components of a security processor** upon a single chip in FIG. 2.
 - Krishna further describes incorporating components on a single chip may increase performance.

EX-1006 1:66-2:2; EX-1003 ¶ 145

Motivation to Combine Pham and Krishna

- State of the Art
 - It was known it was known to put security processing functions on a single chip, and that “cryptographic processing was moving away from discrete processors and was being implemented on a single chip.”
 - Includes an illustration including a packet engine, including database lookups and cryptographic engines and that these discrete processors were implemented on a single chip
Pet. 15-19 (citing EX-1006; EX-1010; EX-1003 ¶¶51-59))

Motivation to Combine Pham and Krishna

- Motivation to Combine
 - Given the teaching in the State of the Art, and combined with the express teaching of Krishna that single chip processor's overall performance can be enhanced, a POSA would be motivated to **include security functions on a single chip**. That rationale applies to all security functions, including an IDS, and not just those discrete elements recited in Claim 3, e.g., packet engine, cryptographic core and the modulo engine.

Pet. 69-71 (citing EX-1006; EX-1003 ¶¶142-150).

Motivation to Combine Pham and Krishna

- Petitioner's evidence is unrebutted
 - PO expert did not address State of the Art section or motivation to combine
 - POR is based solely on attorney argument
 - “terse description of Krishna”
 - Same clear text argument of Dispute I

Claims

Claim 2

2.The security processor of claim 1 wherein the packet engine is further operable to handle security context management processing for the incoming and outgoing packets.

Claim 3

3. The security processor of claim 1 further comprising: a local data bus coupled to the switching system; and a modulo engine coupled to the local data bus.

Claim 4

4. The security processor of claim 3 wherein the packet engine, the cryptographic core, and the modulo engine are formed on a single chip.

Claim 5

5. The security processor of claim 4 further comprising a control processor, coupled to the local data bus, for exception handling of the incoming and outgoing packets.

Claim 6

6. The security processor of claim 4 further comprising a key management engine coupled to the local data bus.

Claim 7

7. The security processor of claim 4 wherein the security processor handles substantially all security processing for the incoming and outgoing packets.

Claim 8

8. The security processor of claim 7 wherein the security processor further handles substantially all network processing for the incoming and outgoing packets.

Claim 9

9. The security processor of claim 1 wherein the cryptographic core is one of a plurality of cryptographic cores coupled one-to-one to the plurality of packet engines and Substantially all of the incoming and outgoing packets to the security processor transit a corresponding one of the plurality of cryptographic cores after transiting one of the plurality of packet engines.

Claim 10

10. The security processor of claim 1 wherein the packet engine is further operable to add at least one of an IP header or a MAC address to the outgoing packets.

Claim 11

11. The security processor of claim 1 wherein the packet engine is further operable to remove an IP header from the incoming packets.

Claim 12

12. The security processor of claim 1, wherein the at least one packet matching the signature stored in the signature database comprises a plain text packet.

Claim 13

13.A security processing system comprising:

(a) a security processor comprising:

a switching system to send outgoing packets and to receive incoming packets;

a packet engine, coupled to the switching system, to handle classification processing for the incoming packets received by the packet engine from the switching system and the outgoing packets sent by the packet engine to the switching system,

wherein the packet engine is one of a plurality of packet engines and substantially all of the incoming packets and outgoing packets to the security processor transit one of the plurality of packet engines, and wherein the incoming and outgoing packets are provided with a tag upon ingress to one of the plurality of packet engines and the tag determines an egress path within the security processor upon exit from a corresponding cryptographic core;

a cryptographic core, coupled to the packet engine and receiving the incoming packets from the switching system via the packet engine and communicating the outgoing packets to the switching system via the packet engine, to provide encryption and decryption processing for packets received from and sent to the packet engine,

wherein the packet engine is interposed between the switching system and the cryptographic core;

a signature database; and

an intrusion detection system coupled between the cryptographic core and the packet engine and responsive to at least one packet matching a signature stored in the signature database; and

a local data bus coupled to the Switching system; and

(b) a memory coupled to the local data bus.

Claim 14

14. The security processing system of claim 13 further comprising a modulo engine coupled to the local data bus.

Claim 15

15. The security processing system of claim 14 further comprising a key management engine coupled to the local data bus.

Claim 16

16. The security processing system of claim 13 wherein the memory and the security processor are within the same cryptographic boundary.

Claim 17

17. The security processing system of claim 13 wherein the security processor is formed on a single chip.

Claim 18

18. The security processing system of claim 13 further comprising:

- a memory interface coupled to the local data bus, wherein the memory is coupled to the local data bus using the memory interface; and

- a translator coupled to the memory interface to perform translation of data received by the memory interface from the memory.

Claim 19

19. The security processing system of claim 18 wherein the translator performs steganographic translation of the received data.

Claim 20

20. The security processing system of claim 18 wherein the translator performs encryption translation of the received data.

Claim 21

21. The security processing system of claim 13 wherein the security processor is operable to

- (i) execute boot code to load firmware for execution by the security processor and
- (ii) authenticate the boot code using a mechanism internal to the security processor prior to operation of the security processor.

Claim 22

22. The security processing system of claim 13, wherein the at least one packet matching the signature stored in the signature database comprises a plain text packet.