

*Cisco Systems, Inc.,
Palo Alto Networks, Inc., and
Fortinet, Inc.*

v.

Lionra Technologies Ltd.

IPR2023-00673, U.S. Patent No. 7,685,436

Patent Owner's Demonstrative Exhibits

July 23, 2024

Ex. 2013

*Cisco Systems, Inc.,
Palo Alto Networks, Inc., and
Fortinet, Inc.*

v.

Lionra Technologies Ltd.

IPR2023-00703, U.S. Patent No. 8,566,612

Patent Owner's Demonstrative Exhibits

July 23, 2024

Ex. 2013

'436 Patent, Claim 1

- [1.pre] A security processor to process incoming packets and outgoing packets, the security processor comprising:
- [1.ii] a switching system to send the outgoing packets and receive the incoming packets;
 - [1.iii] 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,
 - [1.iv] 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;
 - [1.v] 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;
 - [1.vi] 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,
 - [1.vii] wherein the packet engine is interposed between the switching system and the cryptographic core;
 - [1.viii] 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.

'436 Patent, Claim 1; Ex. 1001, 24:10-39; IPR2023-00673. ("IPR-673"), Paper 14, v.

'436 Patent, Claim 13

- [13.pre] A security processing system comprising: a security processor comprising:
- [13.ii] a switching system to send outgoing packets and receive incoming packets;
 - [13.iii] 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,
 - [13.iv] 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;
 - [13.v] 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;
 - [13.vi] 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,
 - [13.vii] wherein the packet engine is interposed between the switching system and the cryptographic core;
 - [13.viii] 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
 - [13.ix] a local data bus coupled to the switching system; and;
 - [13.x] a memory coupled to the local data bus.

'436 Patent, Claim 13; Ex. 1001, 25:10-26:4; IPR2023-00673 Paper 14, vi-vii.

'612 Patent, Claim 1

- [1.pre] A security processor to process incoming packets and outgoing packets, the security processor comprising:
- [1.ii] a switching system to send the outgoing packets and receive the incoming packets;
 - [1.iii] 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,
 - [1.iv] 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;
 - [1.v] 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,
 - [1.vi] wherein the packet engine is interposed between the switching system and the cryptographic core;
 - [1.vii] 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.

'612 Patent, Claim 1; Ex. 1012, 20:54-21:11; IPR2023-00703, ("IPR-703"), Paper 13, v.

'612 Patent, Claim 13

- [13.pre] A security processing system comprising: a security processor comprising:
- [13.ii] a switching system to send outgoing packets and receive incoming packets;
 - [13.iii] 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,
 - [13.iv] 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;
 - [13.v] 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,
 - [13.vi] wherein the packet engine is interposed between the switching system and the cryptographic core;
 - [13.vii] 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
 - [13.viii] a local data bus coupled to the switching system; and;
 - [13.ix] a memory coupled to the local data bus.

'612 Patent, Claim 13; Ex. 1012, 21:49-22:11; IPR2023-00703, Paper 13, vi-vii.

Summary of Why The Petition Fails

- The prior art does not disclose, teach or suggest the claim 1 and 13 limitation that “substantially all of the incoming packets and outgoing packets to the security processor transit one of the plurality of packet engines.”
 - In all embodiments, Pham’s ingress processors perform filtering and routing.
 - Packets not requiring processing through the data packet processors are bypassed between the ingress and egress processors, without transiting a packet engine.
 - Packets directed to the VPN gateway itself or representing/initiating a new logical connection are routed to the control processor, without transiting a packet engine.
- A POSITA would not put an intrusion detection system between Pham’s crypto processor’s network processor (packet engine) and encryption/decryption engine because it could not detect bypassed or control processor packets.
- Petitioner does not show how an IDS or signature database could be formed on a single chip.

IPR-673 Paper 14, 21-35; IPR-703 Paper 13, 20-34; Exhibit 2010, ¶¶ 51-60, 87-89, 91-94, 95, 98.

Summary of Why The Petition Fails

- The prior art does not disclose, teach or suggest the '436 Patent claim limitation that “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.”
 - In all embodiments, Pham’s ingress processors perform filtering and routing.
 - Packets that are not passed across the VPN are filtered and do not have an added header (e.g., an IP tunneling (SA) header).

IPR-673 Paper 14, 30-32; Ex. 2010, ¶¶ 57,60.

Grounds 1-4: Substantially All of the Packets Do Not Transit a Packet Engine

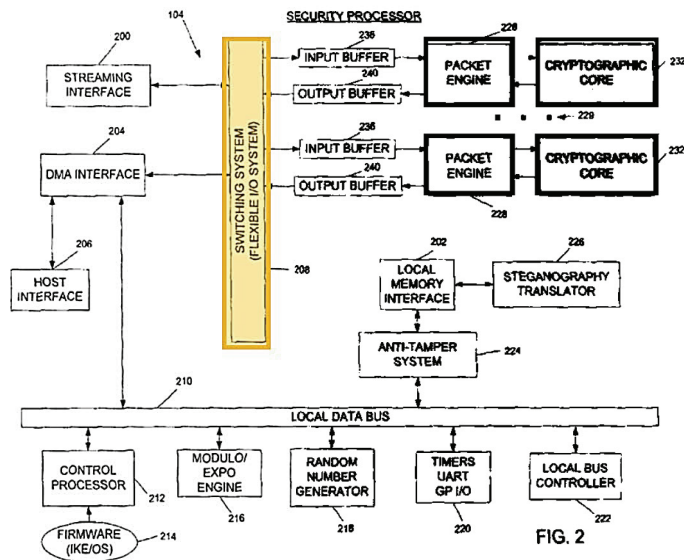
“Substantially All” is a Structural Limitation

- Claim elements [1.iv] and [13.iv] recite “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, ...”
- “Substantially all” appears in the claim body, not the preamble.
- Functional language may be used to limit the structure of an apparatus claim to the way the apparatus functions during operation.

IPR-673 Paper 23, 12-20; IPR-703 Paper 22, 12-20; *Manual of Patent Examining Procedures* § 2173.05(g).

“Substantially All” is a Structural Limitation

- The '436 and '612 Patent specifications disclose that incoming packets are communicated to the switching system.



Streaming interface 200 may be coupled for input and output to physical I/O interfaces 114 and 118 and supports fast path data flow to security processor 104. Host interface 206 may be coupled to physical host bridge 128 and supports slow path data flow and system management by host processor 130. Host interface 206 may be coupled to DMA interface 204. Both streaming interface 200 and DMA interface 204 may be coupled to switching system 208. Although only a

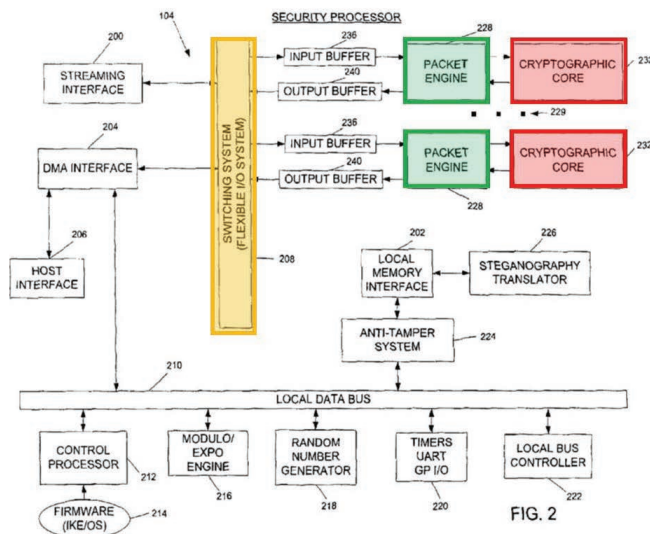
comprise two DMA interfaces. Switching system 208 may be used to provide a switching mechanism to route packets and data to and from any of the I/O interfaces of security processor 104 and local data bus 210.

Switching system 208 may provide a flexible I/O system that allows packet processing engines or packet engines 228 to communicate high-speed data with several different types of interfaces including, for example, streaming interface 200 and direct memory access (DMA) interface 204. A non-lim-

IPR-673 Paper 23, 4, 15-17; IPR-703 Paper 22, 4, 15-17; Ex 1001, 6:46-53, 58-61, 7:33-37; Ex. 1013, 6:46-53, 58-61, 7:33-37.

“Substantially All” is a Structural Limitation

- The '436 and '612 Patent specifications disclose that all packet data is passed through the switching system to a packet engine.

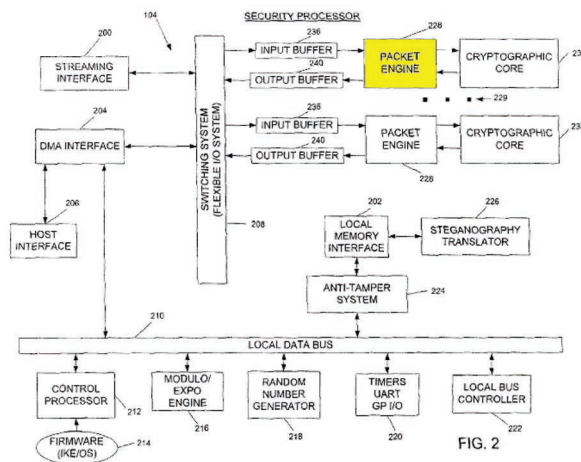


Packet flow through security processing system 102 typically begins when a packet enters switching system 208 via one of streaming interfaces 200 or DMA interfaces 204. Each packet may be inserted into an active list waiting for the next available packet engine 228. The same active list may be an insertion path for control processor 212 to direct packet traffic into a packet engine 228. Regardless of destination, whether, for example, it is to streaming interface 200, host interface 206, control processor 212, or a loop through a packet engine 228, all packet data preferably flows to a packet engine 228 and then to a corresponding cryptographic core 232. Tagging

IPR-673 Paper 23, 15-17; IPR-703 Paper 22, 15-17; Ex 1001, 3, 20:4-14; Ex. 1013, 3, 19:63-20:26.

“Substantially All” is a Structural Limitation

- The '436 and '612 Patent specifications disclose that “substantially all,” but not all, packets may be forwarded and thus transit a packet engine.



In one embodiment, all incoming packets to security processor 104 may be initially processed by one of packet engines 228. Each packet engine 228 may classify the packet based upon a lookup table result and then may apply a variety of operations including, for example, forwarding with necessary transform parameters to cryptographic core 232, or forwarding to control processor 212 for application level processing. Such operations may further include overwriting portions of the packet with new data such as, for example, the media access control (MAC) header for forwarding and the IP header for NAT, and may also include dropping the packet, or

IPR-673 Paper 23, 15-17; IPR-703 Paper 22, 15-17; Ex 1001, 3, 11:9-19; Ex. 1013, 3, 11:8-19.

“Substantially All” is a Structural Limitation

- The '436 Patent prosecution history show that the “substantially all” limitation was limiting and not merely a statement of intended use.
 - The Patent Examiner stated that pending claim 4 (“the security processor of claim 1 wherein the packet engine is one of a plurality of packet engines and substantially all of the incoming and outgoing packets to the security processor transit one of the packet engines”) would be allowable if rewritten in independent form including all of the limitations of the base claim.
 - Petitioners agreed in the district court litigation, asserting that “[t]he only way the patentee was able to get the claims of the '436 and '612 patent allowed was by amending the independent claims to include the ‘substantially all’ limitation from dependent claims.”

IPR-673 Paper 23, 18-19; IPR-703 Paper 22, 18-19; Ex. 1002, 18-19, 57, 279; *Lionra Technologies Ltd. v. Fortinet Inc.*, Case No. 2:22-cv-00322, Dkt. No. 146.

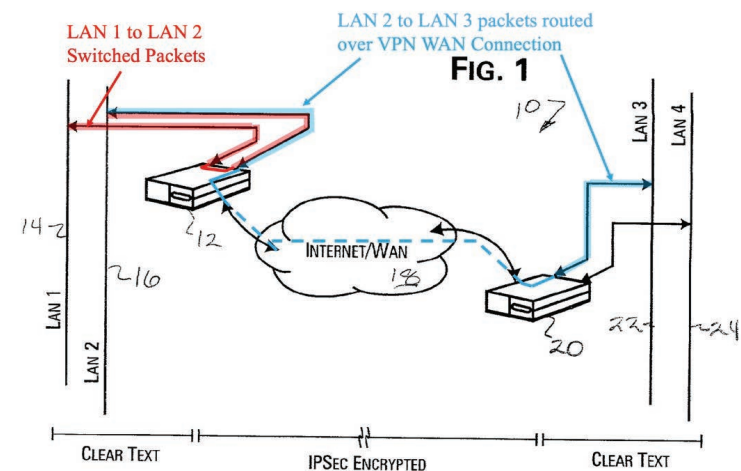
“Substantially All” is a Structural Limitation

- The '612 Patent prosecution history show that the “substantially all” limitation was limiting and not merely a statement of intended use.
 - The Patent Examiner allowed the claims after an examiner’s amendment adding “wherein the packet engine is one of a plurality of packet engines and substantially all of the incoming and outgoing packets to the security processor transit one of the packet engines” to the pending independent claims.
 - Petitioners agreed in the district court litigation, asserting that “[t]he only way the patentee was able to get the claims of the ‘436 and ‘612 patent allowed was by amending the independent claims to include the ‘substantially all’ limitation from dependent claims.”

IPR-703 Paper 22, 18-19; Ex. 1013, 20-22, 218; *Lionra Technologies Ltd. v. Fortinet Inc.*, Case No. 2:22-cv-00322, Dkt. No. 146.

Less than substantially all of the incoming packets to Pham's security processor transit one of the plurality of packet engines

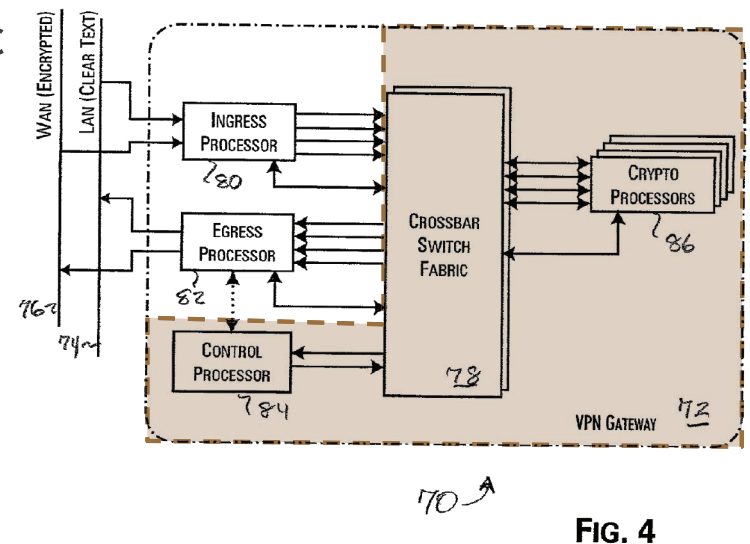
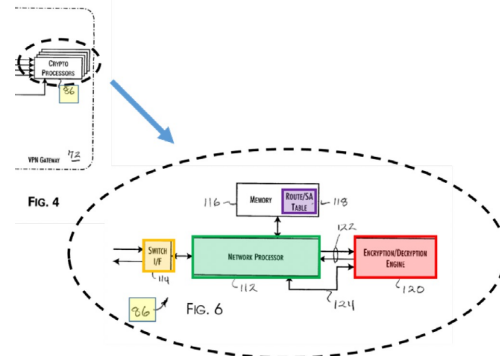
- Pham teaches a network environment utilizing network gateway switches that couple local area networks (e.g., LAN 1 and LAN 2) to each other and, through an encrypted WAN connection, to other local area networks (e.g., LAN 3 and LAN 4).
- Clear text unencrypted packets travel between **LAN 1 and LAN 2** or LAN 3 and LAN 4.
- These clear text packets are "bypassed between the ingress and egress processors."
- Ingress and egress processors are not the claimed packet engines because they are not coupled to a cryptographic engine.



IPR673 Paper 14, 8-11, 13-15, 21-25; Paper 23, 9-11, 21; IPR703 Paper 13, 8-11, 13-15, 21-25; Paper 22, 6-8; Ex. 2010, Ex. 2010, ¶¶ 94-95.

Less than substantially all of the incoming packets to Pham's security processor transit one of the plurality of packet engines

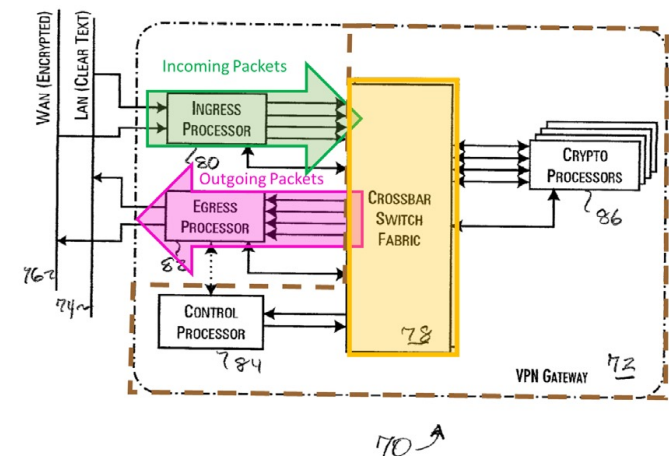
- Petitioners' identified "security processor" in Pham includes a crossbar switch fabric, control process or and crypto processors.
- Petitioners identify the crossbar switch fabric as the claimed switching system and the crypto processors as comprising the claimed packet engines.



IPR673 Paper 23, 25, IPR703 Paper 22, 25; Ex. 2010, ¶¶ 87, 89.

Less than substantially all of the incoming packets to Pham's security processor transit one of the plurality of packet engines

- All of the incoming packets come in to the VPN Gateway through an **Ingress Processor**, through the **Crossbar Switch Fabric**, and out an **Egress Processor**.
- The unencrypted clear text packets that do not require encryption or decryption do not go through the crypto processors and are bypassed between the **ingress** and **egress** processors.



IPR673 Paper 23, 9-11, 25-27; IPR703 Paper 22, 9-11, 25-27; Ex. 1004m [0038]-[0040]; Ex 2010 ¶¶ 52-55; Ex. 2012, 35:4-6.

Less than substantially all of the incoming packets to Pham's security processor transit one of the plurality of packet engines

- The **LAN to LAN Switched Packets** that are bypassed between the ingress and egress processors are communicated across the crossbar switching fabric petitioners identify as the claimed switching system.
- These **packets** are incoming packets to the security processor because they are received by the switching system.
- These **packets** are outgoing packets from the security processor because they are sent from the switching system.

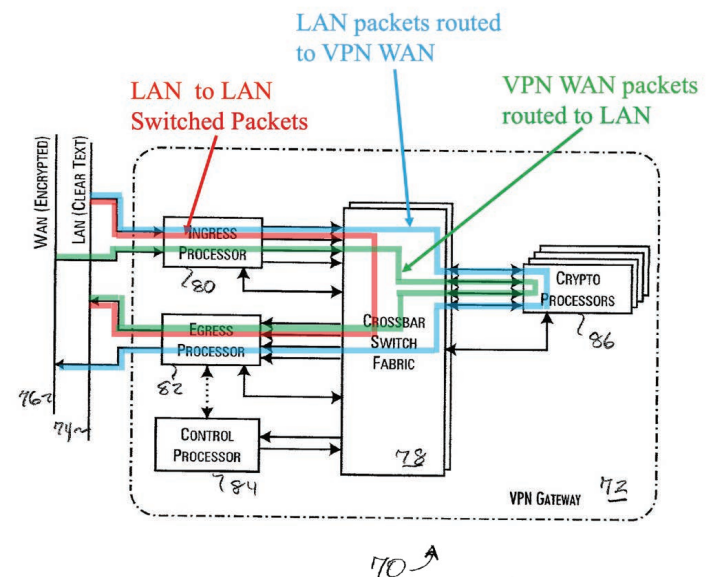


FIG. 4

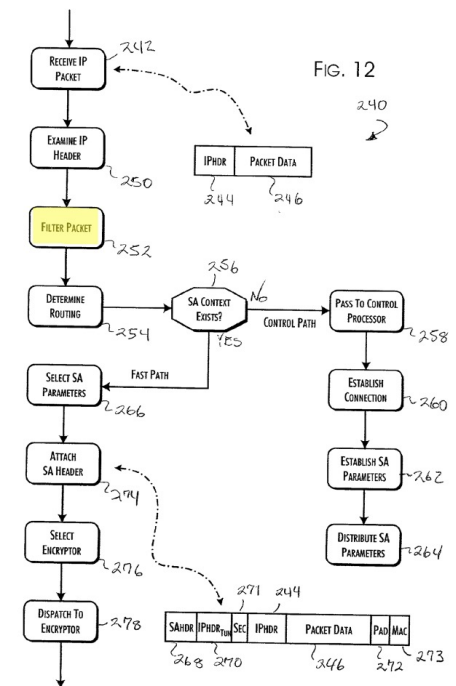
IPR673 Paper 23, 9-11, 25-27; IPR703 Paper 22, 9-11, 25-27; Ex. 1004, 3, [0038]-[0040]; Ex 2010 ¶¶ 52-55; Ex. 2012, 35:4-6.

Less than substantially all of the incoming packets to Pham's security processor transit one of the plurality of packet engines

- The Ingress Processor filters out data packets that are not passed through the VPN Gateway (e.g., LAN to LAN packets) before routing.

processors, and a control processor 46. In the preferred embodiments of the present invention, the ingress processors 30, 34 are tasked with filtering and routing functions for network data packets received on their network connections to the LAN 38 and Internet 18. The routing function includes

[0069] FIG. 12 provides a flow diagram describing the network packet processing operation 240 of an ingress processor 80 for network data packets received from a clear text network in accordance with a preferred embodiment of the present invention. An ordinary network data packet, as received 242, includes a conventional IP header 244 and data packet payload 246. The IP header is examined 250 to discriminate and filter out 252 data packets that are not to be passed through the VPN gateway 72. For data packets that



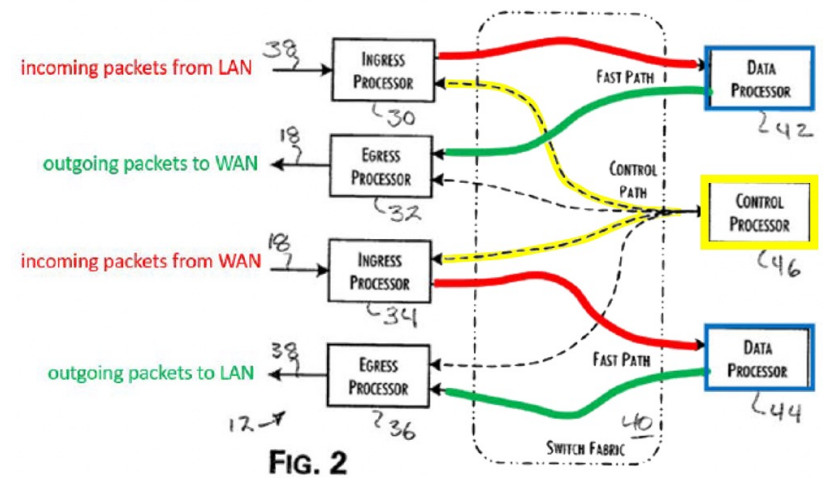
IPR673 Paper 23, 13-14, 26-30; IPR703 Paper 22, 13-14, 26-30; Ex. 1004 7, [0038], [0069]; Ex 2010 ¶¶ 51-60, 67, 91-94.

Less than substantially all of the incoming packets to Pham's security processor transit one of the plurality of packet engines

- Pham discloses sending packets to the Control Processor, which is not a claimed “packet engine.”

[0039] The control path route is selected for data packets recognized as being directed to the VPN gateway 12 itself. Such data packets likely represent control commands used to configure and manage the VPN gateway 12. The control path is also selected for network data packets recognized by an ingress processor 30, 34 as representing or initiating a new logical network connection through the VPN gateway 12.

the control processor 84 utilizes the port connections between the control processor 84 and switch fabric 78 to transmit effectively out-of-band control information and receive status information from the ingress, egress, and crypto processors 80, 82, 86. In-band communications with external network connected devices, such as for network protocol negotiations, is accomplished by utilizing the ingress and egress processors 80, 82 as simple network access ports. Both the in-band and out-of-band communi-



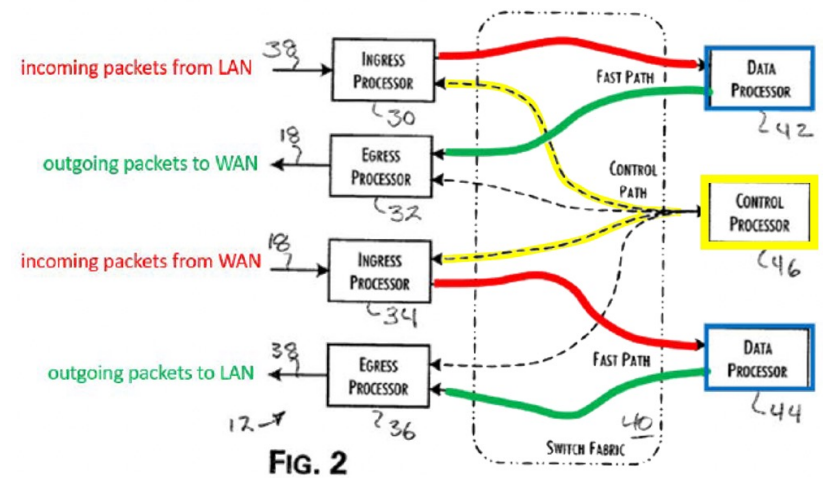
IPR673 Paper 23, 4-8, IPR703 Paper 22, 4-8; Ex. 1004, 2, [0039], [0048].

Less than substantially all of the incoming packets to Pham's security processor transit one of the plurality of packet engines

- Pham's Figure 2 embodiment sends incoming packets to the control processor and the egress processor.

[0039] The control path route is selected for data packets recognized as being directed to the VPN gateway 12 itself. Such data packets likely represent control commands used to configure and manage the VPN gateway 12. The control path is also selected for network data packets recognized by an ingress processor 30, 34 as representing or initiating a new logical network connection through the VPN gateway 12.

and process data packets. In particular, packets not requiring processing through the data packet processors 42, 44 are bypassed between the ingress and egress processors 30, 32, 34, 36.



IPR673 Paper 23, 6-8, IPR703 Paper 22, 6-8; Ex. 1004, 2, [0039]-[0040].

Less than substantially all of the incoming packets to Pham's security processor transit one of the plurality of packet engines

- Even if Pham's crypto processor performed packet processing beyond encryption and decryption, packets would still be filtered by the ingress processor.
- Pham teaches using a general-purpose microprocessor for or with a network processor if more than the SA parameter association task is off-loaded.

processors, and a control processor 46. In the preferred embodiments of the present invention, the ingress processors 30, 34 are tasked with filtering and routing functions for network data packets received on their network connections to the LAN 38 and Internet 18. The routing function includes

[0053] In alternate embodiments of the present invention, the data table 118 can be used to store and share other information between the crypto processors 86 and, generically, data processors 58. In particular, a general purpose microprocessor can be substituted or provided in addition to the network processor 112 to support data compression and decompression operations. Compression symbols are iden-

IPR673 Paper 23, 8-9, IPR703 Paper 22, 8-9; Ex. 1004, [0038], [0053].

Substantially all of the incoming packets to Pham's security processor do not transit one of the plurality of packet engines

- Because less than “substantially all of the incoming packets and outgoing packets to the security processor transit one of the plurality of packet engines” in any of Pham's disclosed embodiments, the prior art does not disclose, teach or suggest independent claim limitations [1.iv] or [13.iv] of the '436 and '612 Patents.
- Because the prior art does not teach limitations of independent claims 1 and 13, it does not render obvious dependent claims 2-4, 7-12, 14, 16-17 and 20-21.
- *Synqor, Inc. v. Artesyn Techs., Inc.*, 709 F.3d 1365, 1375 (Fed. Cir. 2013) (“Th[e] court need not consider Defendants' arguments that certain dependent claim limitations would have been obvious where the base claim has not been proven invalid.”).
- *Callaway Golf Co. v. Acushnet Co.*, 576 F.3d 1331, 1344 (Fed. Cir. 2009) (a judgment is irreconcilably inconsistent where a dependent claim is found obvious and the independent claim from which it depends is nonobvious).

IPR673 Paper 14, 21-30, 34-36; IPR703 Paper 13, 20-30, 32-34; Ex. 2010, Ex. 2010, ¶¶ 94-95.

Grounds 1-4: The Incoming and Outgoing Packets are Not Provided with a Tag ('436 Patent Only)

'436 Patent, Claim 1

- [1.pre] A security processor to process incoming packets and outgoing packets, the security processor comprising:
- [1.ii] a switching system to send the outgoing packets and receive the incoming packets;
 - [1.iii] 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,
 - [1.iv] 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;
 - [1.v] 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;
 - [1.vi] 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,
 - [1.vii] wherein the packet engine is interposed between the switching system and the cryptographic core;
 - [1.viii] 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.

'436 Patent, Claim 1; Ex. 1001, 24:10-39; IPR2023-00673. ("IPR-673"), Paper 14, v.

'436 Patent, Claim 13

- [13.pre] A security processing system comprising: a security processor comprising:
- [13.ii] a switching system to send outgoing packets and receive incoming packets;
 - [13.iii] 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,
 - [13.iv] 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;
 - [13.v] 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;
 - [13.vi] 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,
 - [13.vii] wherein the packet engine is interposed between the switching system and the cryptographic core;
 - [13.viii] 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
 - [13.ix] a local data bus coupled to the switching system; and;
 - [13.x] a memory coupled to the local data bus.

'436 Patent, Claim 13; Ex. 1001, 25:10-26:4; IPR2023-00673 Paper 14, vi-vii.

The incoming packets to Pham's security processor are not all provided with an SA Header (tag)

- Petitioners identify an SA header or an IP tunneling header as the claimed “tag” provided “upon ingress to one of the plurality of packet engines.”
- An SA header or IP tunneling header is not provided to a packet in Pham if the packet is a clear text packet that is not routed through the VP.
- An SA header or IP tunneling header is not provided to a packet in Pham if the packet is passed to the control processor.

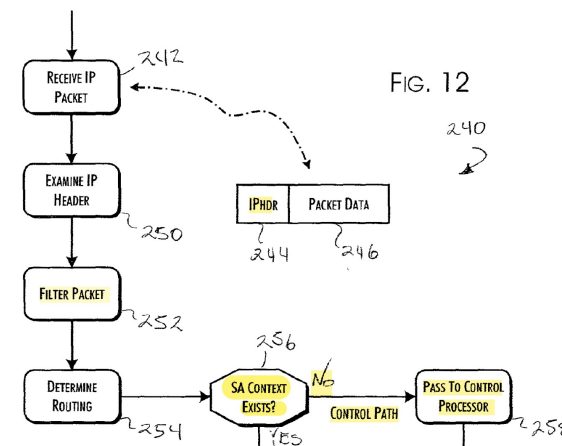
IPR673 Paper 14, 13-16, 30-31; Ex 2010 ¶¶ 56-57.

The incoming packets to Pham's security processor are not all provided with an SA Header (tag)

- The Ingress Processor filters out data packets that are not passed through the VPN Gateway (e.g., LAN to LAN packets) before routing.
- Packets that are not filtered but do not have associated SA context are passed to Control Processor.

[0069] FIG. 12 provides a flow diagram describing the network packet processing operation 240 of an ingress processor 80 for network data packets received from a clear text network in accordance with a preferred embodiment of the present invention. An ordinary network data packet, as received 242, includes a conventional IP header 244 and data packet payload 246. The IP header is examined 250 to discriminate and filter out 252 data packets that are not to be passed through the VPN gateway 72. For data packets that

[0070] Where an applicable connection route or SA parameter context is not found in the data table 102, indicating that the network data packet received corresponds to an implied new connection request, the data packet is forwarded 258 through the control path to the control processor 84 for negotiation of an IPsec connection. The negotiation is conducted through the appropriate network



IPR673 Paper 14, 13-16, 30-31; Ex. 1004 7, [0069]-[0071]; Ex 2010 ¶¶ 56-57.

The incoming packets to Pham's security processor are not all provided with an SA Header (tag)

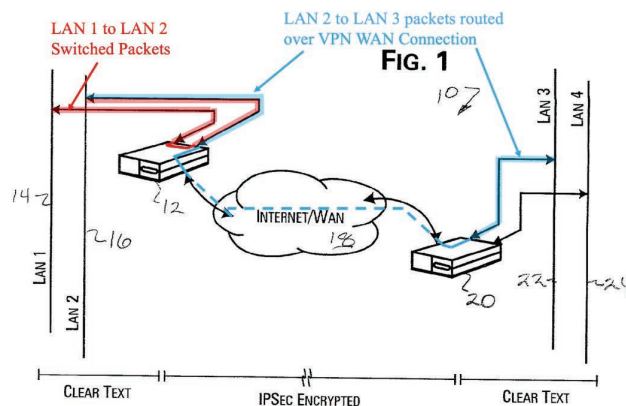
- Petitioners identify an SA header or an IP tunneling header as the claimed “tag” provided “upon ingress to one of the plurality of packet engines.”
- An SA header or IP tunneling header is not provided to a packet in Pham if the packet is (1) a clear text packet that is not routed through the VPN or (2) passed to the control processor.
- Because “the incoming packets and outgoing packets are **[NOT]** provided with a tag upon ingress to one of the plurality of packet engines” in any of Pham's disclosed embodiments, the prior art does not disclose, teach or suggest independent claim limitations [1. v] or [13.v] of the '436 Patent.

IPR673 Paper 14, 13-16, 30-31.

Grounds 1-4: A POSITA Would Not Add an IDS to Pham's Crypto-Processor

A POSITA would not be motivated to combine Pham's VPN Gateway with an intrusion detection system.

- Pham discloses a closed system with the only internet connections through secure connections on a virtual private network.
- Pham teaches using a general-purpose microprocessor instead of or with a network processor if the crypto-processor is performing additional tasks.

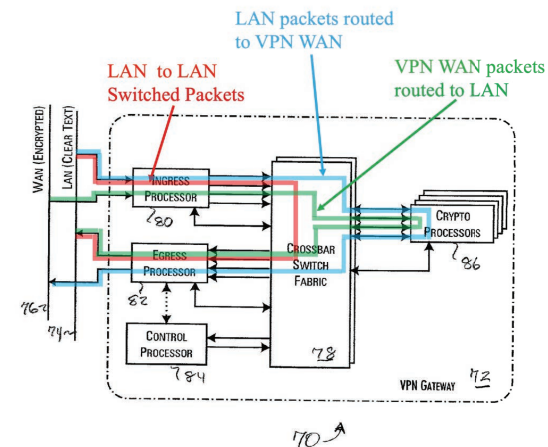
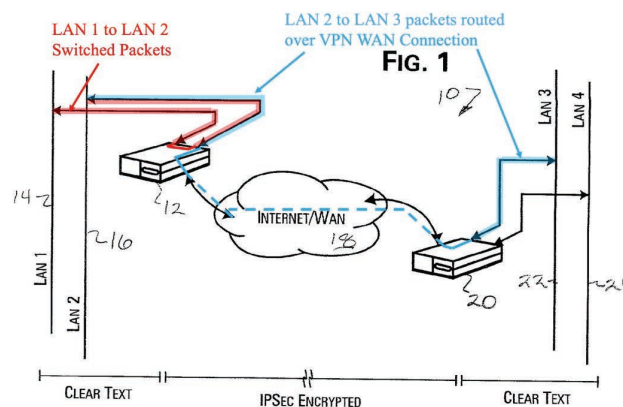


[0053] In alternate embodiments of the present invention, the data table 118 can be used to store and share other information between the crypto processors 86 and, generically, data processors 58. In particular, a general purpose microprocessor can be substituted or provided in addition to the network processor 112 to support data compression and decompression operations. Compression symbols are iden-

IPR673 Paper 14, 23, 32-34; IPR703 Paper 13, 24, 30-32; Ex. 2010, ¶¶ 61, 96-99; Ex. 1004, 2, [0053].

A POSITA would not modify Pham's VPN Gateway with an intrusion detection system in a crypto-processor.

- A POSITA would not locate the IDS between the network processor (*packet engine*) and the encryption/decryption engine (*cryptographic core*) because doing so would only monitor **traffic passing over the secure virtual private network** while ignoring the **clear text packets** filtered by the ingress processor.



IPR673 Paper 14, 23-24, 32-34; IPR703 Paper 13, 23-24, 30-32; Ex. 2010, ¶¶ 61, 96-99; Ex. 1004, 2-3.

The incoming packets to Pham's security processor are not all provided with an SA Header (tag)

- Because Pham discloses a closed system and adding an intrusion detection system would increase the complexity of the crypto-processor by requiring a general-purpose microprocessor instead of or with a network processor a PHOSITA would not be motivated to combine the teachings of Pham and Wu.
- A PHOSITA would not put an intrusion detection system in a crypto-processor because it would not detect clear text packets.
- The prior art does not disclose, teach or suggest independent claim limitations [1.viii] or [13.viii] of the '436 Patent or [1.vii] or [13.vii] of the '612 Patent.
- Because the prior art does not teach limitations of independent claims 1 and 13, it does not render obvious dependent claims 2-4, 7-12, 14, 16-17 and 20-21

IPR673 Paper 14, 23-24, 32-34; IPR703 Paper 13, 23-24, 30-32; Ex. 2010, ¶¶ 61, 96-99.

Ground 3: Petitioner Does Not Show How an IDS Could be Coupled Between the Cryptographic Core and the Packet Engine on a Single Chip

'436 Patent, Claim 1

- [1.pre] A security processor to process incoming packets and outgoing packets, the security processor comprising:
- [1.ii] a switching system to send the outgoing packets and receive the incoming packets;
 - [1.iii] 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,
 - [1.iv] 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;
 - [1.v] 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;
 - [1.vi] 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,
 - [1.vii] wherein the packet engine is interposed between the switching system and the cryptographic core;
 - [1.viii] 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.

'436 Patent, Claim 1; Ex. 1001, 24:10-39.

'436 Patent, Claim 4

[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.

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

'436 Patent, Claims 3 and 4; Ex. 1001, 24:44-49.

'612 Patent, Claim 1

- [1.pre] A security processor to process incoming packets and outgoing packets, **the security processor comprising:**
- [1.ii] a switching system to send the outgoing packets and receive the incoming packets;
 - [1.iii] 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,
 - [1.iv] 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;
 - [1.v] 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,
 - [1.vi] wherein the packet engine is interposed between the switching system and the cryptographic core;
 - [1.vii] **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.

'612 Patent, Claim 1; Ex. 1012, 20:54-21:11.

'612 Patent, Claim 4

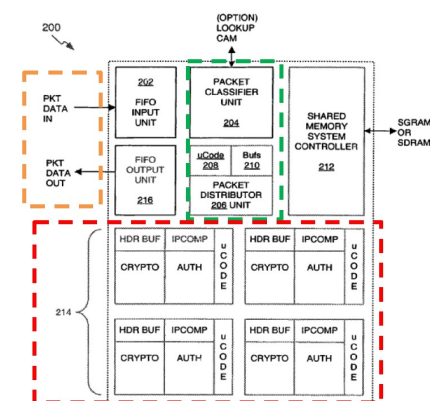
[3] The security processor of claim 1 further comprising: a local data bus coupled to the switching system; and a modulo engine coupled to the local data bus.

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

'612 Patent, Claims 3 and 4; Ex. 1012, 21:16-21.

Petitioner does not show how a security processor with an intrusion detection system could be on a single chip.

- Petitioners' terse discussion of the teachings of Krishna omits any discussion of how limitation [1.vii]/[1.viii] of independent claim 1 ("an intrusion detection system coupled between the cryptographic core and the packet engine") could or would be satisfied if the packet engine, cryptographic core and modulo engine are formed on a single chip.
- Because Petitioners have not shown how the limitations of claims 1 are met, they have not shown how the limitations of claims 4, 7 and 8 are met.



IPR673 Paper 14, 35; IPR703 Paper 13, 33; IPR673, Paper 3, 70.

Ground 4: Petitioner Does Not Show How a Security Processor comprising a Signature Database and an IDS Coupled between the Cryptographic Core and the Packet Engine Could Be On a Single Chip

'436 Patent, Claim 13

- [13.pre] A security processing system comprising: a security processor comprising:
- [13.ii] a switching system to send outgoing packets and receive incoming packets;
 - [13.iii] 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,
 - [13.iv] 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;
 - [13.v] 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;
 - [13.vi] 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,
 - [13.vii] wherein the packet engine is interposed between the switching system and the cryptographic core;
 - [13.viii] 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
 - [13.ix] a local data bus coupled to the switching system; and;
 - [13.x] a memory coupled to the local data bus.

'436 Patent, Claim 13; Ex. 1001, 25:10-26:4.

'436 Patent, Claim 17

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

'436 Patent, Claims 17; Ex. 1001, 26:13-14.

'612 Patent, Claim 13

- [13.pre] A security processing system comprising: a security processor comprising:
- [13.ii] a switching system to send outgoing packets and receive incoming packets;
 - [13.iii] 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,
 - [13.iv] 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;
 - [13.v] 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,
 - [13.vi] wherein the packet engine is interposed between the switching system and the cryptographic core;
 - [13.vii] 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
 - [13.viii] a local data bus coupled to the switching system; and;
 - [13.ix] a memory coupled to the local data bus.

'612 Patent, Claim 13; Ex. 1012, 21:49-22:10.

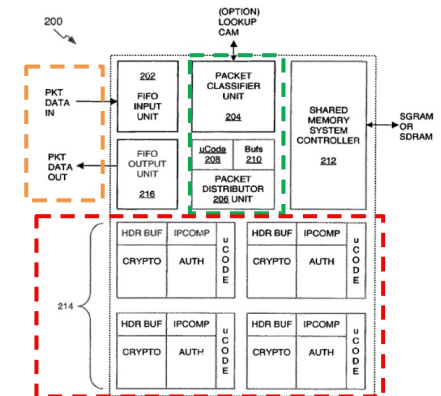
'612 Patent, Claim 17

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

'612 Patent, Claim 17; Ex. 1012, 22:20-21.

Petitioner does not show how a security processor with an intrusion detection system could be on a single chip.

- Petitioners' terse discussion of the teachings of Krishna omits any discussion of how limitation [3.vii]/[13.viii] of independent claim 13 ("a signature database; and an intrusion detection system coupled between the cryptographic core and the packet engine") could or would be satisfied if the packet engine, cryptographic core and modulo engine are formed on a single chip.
- Because Petitioners have not shown how the limitations of claims 13 are met, they have not shown how the limitations of claim 17 are met.



IPR673 Paper 14, 35-56; IPR703 Paper 13, 34; IPR673, Paper 3, 70.