UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

PALO ALTO NETWORKS, INC.,
FORTINET, INC.,

Petitioner,

v.

LIONRA TECHNOLOGIES LIMITED,

Patent Owner.

Case IPR2024-00099
U.S. Patent No. 7,685,436

PATENT OWNER'S PRELIMINARY RESPONSE TO PETITION

Mail Stop "PATENT BOARD"
Patent Trial and Appeal Board
U.S. Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450

TABLE OF CONTENTS

Page

CHALLENGED CLAIMS v

I. INTRODUCTION 1

II. THE '436 PATENT 1

III. THE ALLEGED PRIOR ART 7

A. U.S. Patent Publication 2003/0074473, "Scalable Network Gateway Processor Architecture," ("Pham"). 8

B. U.S. Patent No. 7,424,744, "Signature Based Network Intrusion Detection System and Method," ("Wu") 17

C. U.S. Patent No. 7,996,670, "Classification Engine in a Cryptography Acceleration Chip," ("Krishna") 18

D. U.S. Patent Publication 2002/0073316A1, "Cryptographic System Enabling Ownership of a Secure Process," ("Collins") 18

IV. CLAIM CONSTRUCTION AND A PERSON OF ORDINARY SKILL IN THE ART 19

V. ASSERTED GROUNDS OF ALLEGED UNPATENTABILITY 20

A. Ground 1: Pham in view of Wu (Claims 1-2, 9-13, 16 and 22) 21

1. Petitioner ignores packets in the crossbar switch fabric that go directly between the ingress processor and the egress processor. 21

2. Substantially all of the incoming packets and outgoing packets to the security processor will <u>not</u> transit one of the plurality of crypto processor network processors Petitioner identifies as packet engines. 25

3. Petitioner incorrectly asserts that the incoming packets and outgoing packets are provided with a tag upon ingress to

one of the crypto processor network processors and the tag determines an egress path within the security processor upon exit from a corresponding encryption/decryption engine. 30

4. It would not have been obvious to a POSITA to modify the teachings of Pham with the teachings of Wu to add an intrusion detection system to Pham's crypto processor. 32

5. Petitioner's contentions regarding dependent claims 2, 9, 10, 12, 16 and 22 fail because Pham and Wu do not disclose or teach the limitations of independent claims 1 and 13. 34

B. Ground 2: Pham in view of Wu and Collins (Claims 3, 14 and 21). 34

C. Ground 3: Pham in view of Wu, Collins and Krishna (Claims 4, 7 and 8) 35

D. Ground 4: Pham in view of Wu and Krishna (Claim 17) 35

VI. CONCLUSION 36

TABLE OF AUTHORITIES

Cases

Callaway Golf Co. v. Acushnet Co.,
576 F.3d 1331 (Fed. Cir. 2009) 34

Synqor, Inc. v. Artesyn Techs., Inc.,
709 F.3d 1365 (Fed. Cir. 2013) 34

PATENT OWNER'S EXHIBIT LIST

Exhibit No.	Description
2001	Docket Sheet, *Lionra Technologies Limited v. Fortinet, Inc.*, No. 2:22-cv-00322-JRG-RSP (Lead Case) (E.D. Tex. July 19, 2023)
2002	Order, *Lionra Technologies Limited v. Fortinet, Inc.*, No. 2:22-cv-00322-JRG-RSP (Lead Case), Dkt. No. 21 (E.D. Tex. Oct. 24, 2022)
2003	Second Amended Docket Control Order, *Lionra Technologies Limited v. Fortinet, Inc.*, No. 2:22-cv-00322-JRG-RSP (Lead Case), Dkt. No. 160 (E.D. Tex. Nov. 27, 2023)
2004	Order, *MyPort, Inc. v. Samsung Electronics Co., Ltd.*, *et al.,* No. 2:22-cv-00114-JRG (E.D. Tex. June 12, 2023)
2005	Defendants' Invalidity Contentions, *Lionra Technologies Limited v. Fortinet, Inc.*, No. 2:22-cv-00322-JRG-RSP (Lead Case) (E.D. Tex. Feb. 10, 2023)
2006	U.S. District Courts—Federal Court Management Statistics–Profiles—During the 12-Month Periods Ending September 30, 2018 Through 2023 available at https://www.uscourts.gov/sites/default/files/fcms_na_distprofile0930.2023.pdf
2007	U.S. Patent No. 7,493,659 ("Wu et al.")
2008	U.S. Patent Publication No. 2003/0014627 ("Krishna et al.)
2009	Claim Construction Order, *Lionra Technologies Limited v. Fortinet, Inc.*, No. 2:22-cv-00322-JRG-RSP (Lead Case), Dkt. No. 162 (E.D. Tex. Nov. 27, 2023)
2010	Declaration of Eric Cole, Ph.D.
2011	Curriculum Vitae of Eric Cole, Ph.D.
2012	Transcript of Jan. 10, 2024 Deposition of Mark Crovella, Ph.D.

CHALLENGED CLAIMS

Claim	Text
[i.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.
[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	Text
[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.
[7]	The security processor of claim 4 wherein the security processor handles substantially all security processing for the incoming and outgoing packets.
[8]	The security processor of claim 7 wherein the security processor further handles substantially all network processing for the incoming and outgoing packets.
[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.
[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.
[11]	The security processor of claim 1 wherein the packet engine is further operable to remove an IP header from the incoming packets.
[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.
[13.pre]	A security processing system comprising: a security processor comprising
[13.ii]	a switching system to send outgoing packets and receive incoming packets;

Claim	Text
[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.
[14]	The security processing system of claim 13 further comprising a modulo engine coupled to the local data bus.
[16]	The security processing system of claim 13 wherein the memory and the security processor are within the same cryptographic boundary.

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

I. INTRODUCTION

Patent Owner Lionra Technologies Ltd. ("Patent Owner") submits this response to Petitioner Palo Alto Networks, Inc.'s and Fortinet, Inc.'s ("Petitioner") Petition for *inter partes* review of U.S. Patent No. 7,685,436 ("the '436 patent") (Paper 3, "Pet."). As discussed below, the Petition fails on all grounds because, *inter alia*, the primary reference relied upon by Petitioner, Pham, does not disclose, teach or suggest a critical limitation of every independent claim—that "substantially all of the incoming packets and outgoing packets to the security processor transit one of the plurality of packet engines." And, as further discussed below, a Person of Ordinary Skill in the Art (POSITA) would not have been motivated to combine the Pham and Wu references to meet a different limitation of every independent claim—"an intrusion detection system coupled between the cryptographic core and the packet engine." For these reasons, Petitioner has not shown that the Petition has a reasonable likelihood of success. Accordingly, institution should be denied.

II. THE '436 PATENT

The '436 Patent, entitled "System and Method for a Secure I/O Interface," issued on March 23, 2010 and bears an earliest priority date of October 2, 2003, in light of U.S. Provisional App. No. 60/507,976. The inventors of the '436 Patent recognized that "there is a general need for a secure I/O interface system and method that improve the security of communications to and from trusted hardware, improve

communication speed, reduce the number of different systems required for secure communications, and reduce the extent of the bottleneck on the backplane bus." Ex. 1001, 2:21-26; *see also* Ex. 2010, *Combined Declaration of Eric Cole, Ph.D.*, ¶¶ 66-69. They solved this problem with a system and method for connecting a trusted piece of hardware to a network using an I/O interface or system that provides improved security for all or substantially all communications received and sent by the trusted hardware. Ex. 1001, 3:23-31; *see also* Ex. 2010, ¶¶ 70-71. "The secure I/O system of the present invention permits performing all or substantially all network processing functions and off-loads all or substantially all security functions associated with network address translation (NAT), the providing of a firewall, intrusion detection/protection system functionality, traffic proxying, and encryption from a host or network processor onto a single system or card, for example a NIC." Ex. 1001, 3:43-50; *see also* Ex. 2010, ¶ 72. The '436 Patent also teaches that certain selected networking and/or security functions may be handled by other processors such as, for example, a host processor. Ex. 1001, 3:48-51; 4:59-61; 5:36-39; *see also* Ex. 2010, ¶ 73.

Additional features described in the '436 Patent include memories to maintain for coherently storing common data, as well as providing secure buffering at the interface boundaries of the security processor. "Architecture 100 includes security processing system 102 comprising security processor 104, which may consolidate

processing of discrete or consolidated security functions and maintain relationships and integrity of the stored security context and other information in memories 106, 108, and 110." Ex. 1001, 4:4-9; *see also* Ex. 2010, ¶¶ 74-75.

The '436 Patent discloses "[a] security processor [that] performs all or substantially all security and network processing to provide a secure I/O interface system to protect computing hardware from unauthorized access or attack. The security processor sends and receives all incoming and outgoing data packets for a host device and includes a packet engine, coupled to a local data bus, to process the incoming and outgoing packets. The processor further comprises a cryptographic core coupled to the packet engine to provide encryption and decryption processing for packets processed by the packet engine. The packet engine also handles classification processing for the incoming and outgoing packets. A modulo engine may be coupled to the local data bus." Ex. 1001, Abstract; *see also* Ex. 2010, ¶¶ 72-73.

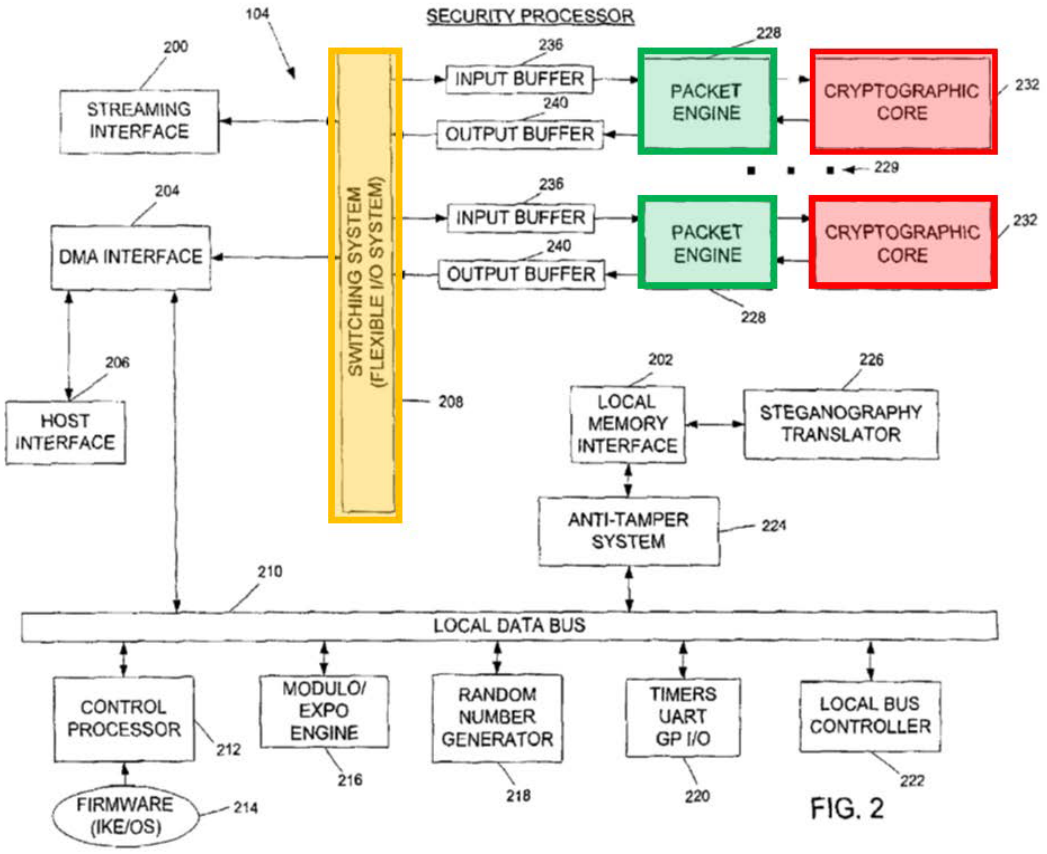


FIG. 2

Ex. 1001, Fig. 2 (highlighted). Security Processor 104 includes switching system 208 (yellow), packet engines 228 (green), and cryptographic cores 232 (red). "Security processing system 102 is preferably contained within cryptographic boundary 112 and provides a secure I/O interface for computing or communications hardware …." *Id.*, 4:20-22; *see also* Ex. 2010, ¶¶ 74-75.

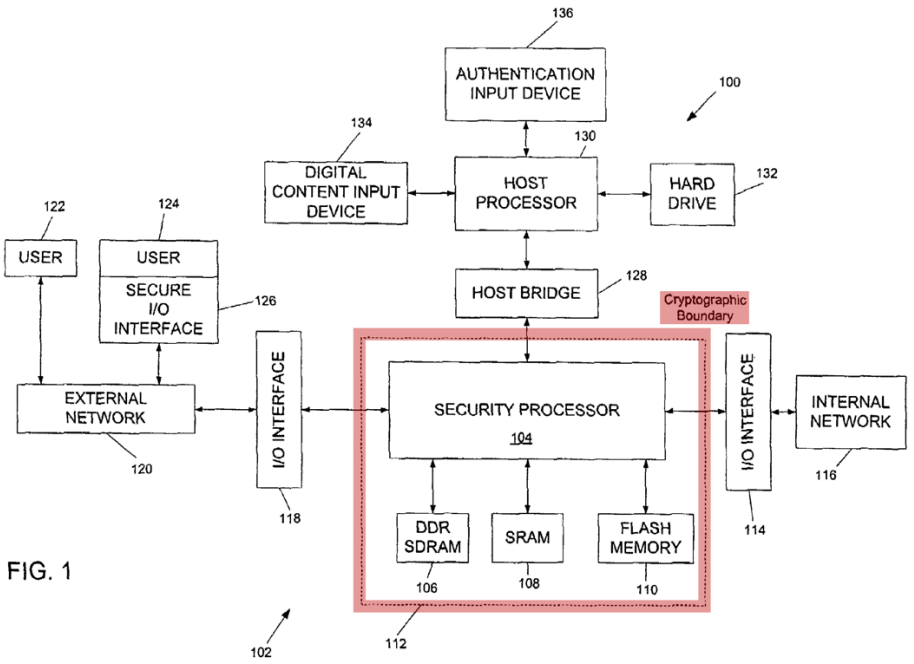
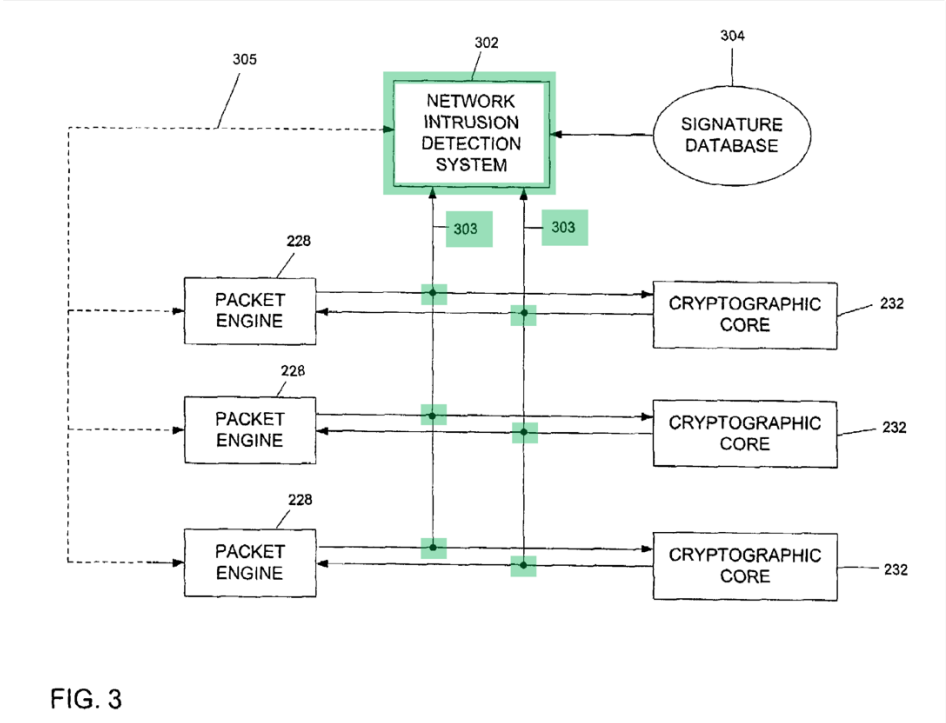


FIG. 1

Ex. 1001, Fig. 1 (annotated). "Security processor 104 preferably handles all network and security processing functions for the data packets to provide the most secure I/O interface." *Id.*, 4:56-58. "By routing all or substantially all I/O to and from host processor 130 and/or internal network 116 through security processing system 102, host processor 130 and internal network 116 are substantially protected against unauthorized access or other security breaches, protecting the security information integrity, and providing processing and storage efficiency from information consolidation." *Id.*, 4:40-47; *see also* Ex. 2010, ¶ 75.

The '436 Patent also discloses the use of an intrusion detection system to match parts of the data stream (e.g., packet header, payload, or trailer) against patterns in a signature database. *Id.*, 18:41-47; *see also* Ex. 2010, ¶ 76.



Ex. 1001, Fig. 3 (annotated). "Network intrusion detection system (NIDS) 302 has taps 303 that may couple to the input/output of each of packet engine 228 and cryptographic core 232 pair. Signature database 304 is a defined set of patterns…." *Id.*, 18:41-44; *see also* Ex. 2010, ¶ 76. "[B]y by passing all I/O traffic to host processor 130 and/or internal network 116 through security processing system 102, and including NIDS 302 within system 102, undesirable intrusions may be detected in-line with such I/O traffic, …." Ex. 1001, 18:48-52; *see also* Ex. 2010, ¶ 76. "Having a tap on each of the input and output paths to each cryptographic core 232 permits the capture of clear text packets either before or after encryption, depending on whether the packets are inbound or outbound." *Id.*, 19:5-9; *see also* Ex. 2010, ¶ 76.

The independent claims of the '436 Patent include these elements of the invention, requiring that "substantially all of the incoming packets and outgoing packets to the security processor transit one of the plurality of packet engines," *see* Ex. 1001, 24:19-21 (Cl. 1), 25:20-22 (Cl. 13), and further reciting "an intrusion detection system that is coupled between a cryptographic core and a packet engine," see id., 24:36-39 (Cl. 1); Ex. 1001, 25:38-26:2 (Cl. 13).

III. THE ALLEGED PRIOR ART

Petitioner's invalidity challenges are based on alleged obviousness based on a single primary reference in various combinations with three secondary references. The primary reference is Exhibit 1004, U.S. Patent Publication 2003/0074473, titled "Scalable Network Gateway Processor Architecture," ("Pham"). The secondary references are Exhibit 1005, U.S. Patent No. 7,424,744 titled "Signature Based Network Intrusion Detection System and Method," ("Wu"), Exhibit 1006, U.S. Patent No. 7,996,670 titled "Classification Engine in a Cryptography Acceleration Chip," ("Krishna"), and Exhibit 1008, U.S. Patent Publication 2002/0073316A1 titled "Cryptographic System Enabling Ownership of a Secure Process," ("Collins.").

Petitioner concedes that Krishna was cited by the examiner during the prosecution of the '436 Patent. Paper 3, Pet. at 21. Although Petitioner contends that Wu was not cited or applied by the examiner during the prosecution of the '436

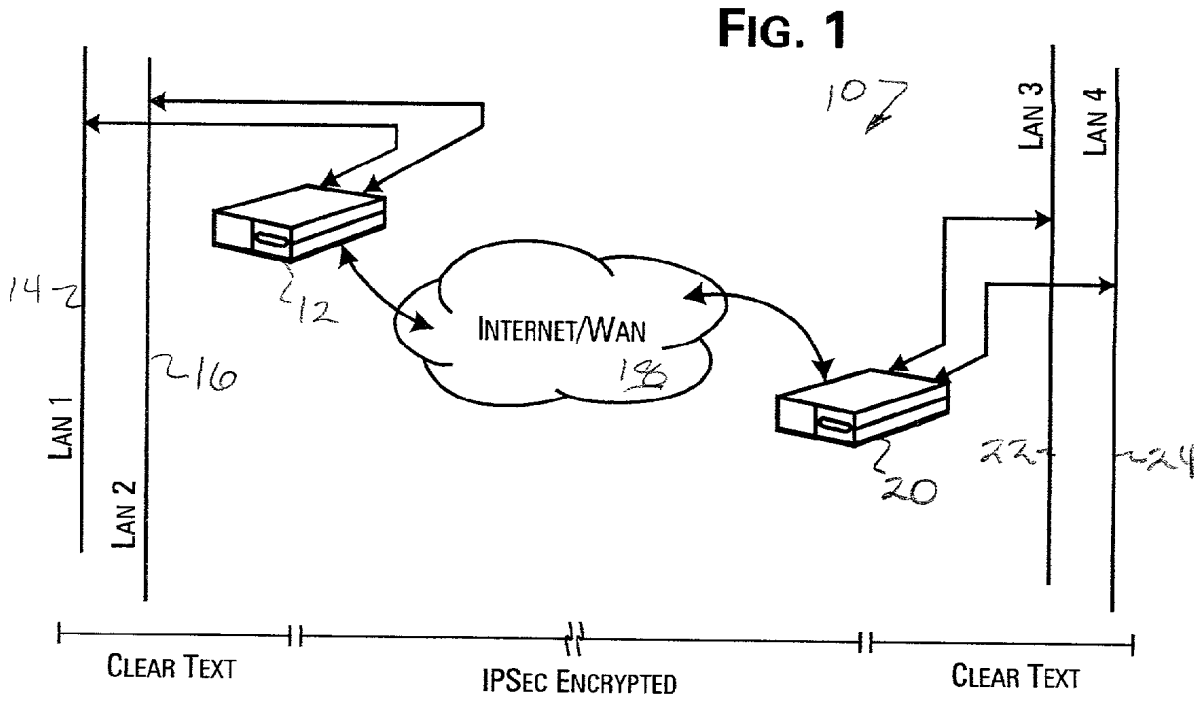
Patent, another Wu patent, U.S. Patent No. 7,493,659, commonly assigned and filed the same day with a substantially similar disclosure, is a cited reference that was applied by the examiner during the patent prosecution. *See* Ex. No. 2007, U.S. Patent No. 7,493,659 ("Wu et al."). *Compare*, *e.g.*, Ex. No. 1005, Fig. 4 *and* Ex. No. 2007, Fig. 4; Ex. No. 1005, Fig. 3 *and* Ex. No. 2007, Fig. 2; Ex. No. 1005, Fig. 6 *and* Ex. No. 2007, Fig. 5; Ex. No. 1005, 1:9-2:10 *and* Ex. No. 2007, 1:9-2:10.

A. U.S. Patent Publication 2003/0074473, "Scalable Network Gateway Processor Architecture," ("Pham").

Petitioner's primary reference, Pham, is not directed to the same problems that are addressed and solved by the inventions claimed in the '436 Patent. Pham, as its title indicates, is particularly directed to a scalable network gateway processor. Ex. 1004, [0003]. Pham teaches doing this by load balancing between data packet processors and network connection processors in "a network data processor system having a plurality of data packet processors coupled through a data switch fabric between network connection processors." *Id.*, [0013]; *see also* Ex. 2010, ¶¶ 46-49. "The data packet processors each include a data processing engine configured to perform a data processing function over data contained within predetermined data packets. The network connection processors include network interfaces coupleable to external data transmission networks and provide for the selective routing of said predetermined data packets through said data switch fabric to load balance the

processing of the predetermined data packets by the plurality of data packet processors." Ex. 1004, [0013]; *see also* Ex. 2010, ¶¶ 49-50.

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).



Ex. 1004, Fig. 1; *see also* Ex. 2010, ¶ 51. As shown in Figure 1, Pham teaches that packets going between the VPN gateways are IPsec encrypted packets travelling over a virtual private network (VPN) established between the VPN gateways 12 and 20, but there are also clear text unencrypted packets that travel between LAN 1 and LAN 2 or LAN 3 and LAN 4. These unencrypted packets do not require processing through data packet processors and are instead "bypassed between the ingress and

egress processors." Ex. 1004, [0038]-[0040]; *see also* Ex. 2010, ¶¶ 52-55; Ex. 2012, Dep. Tr., 35:4-6 ("[I]n this specific scenario, those packets would not be going through the cryptoprocesor.").

The network gateway packet processor of Pham is shown in Figure 4 below.

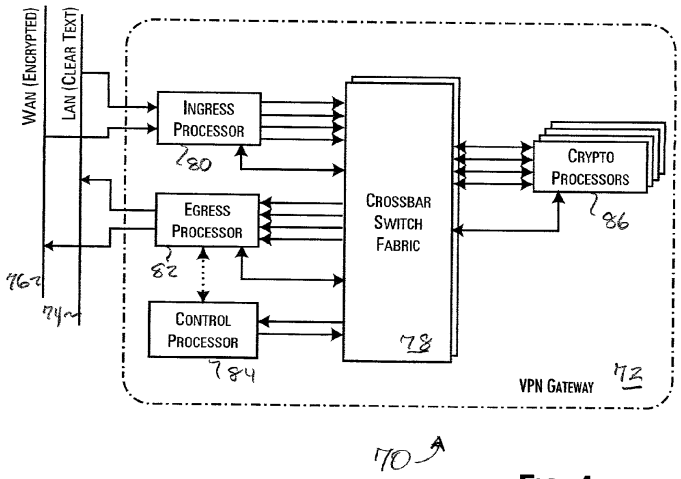
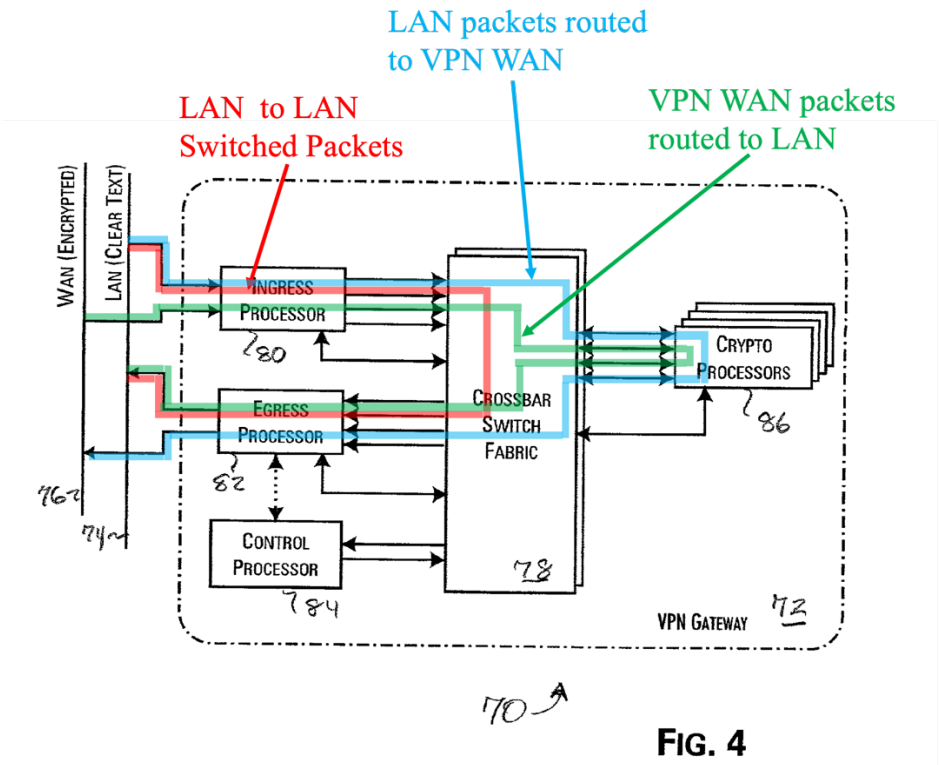


FIG. 4

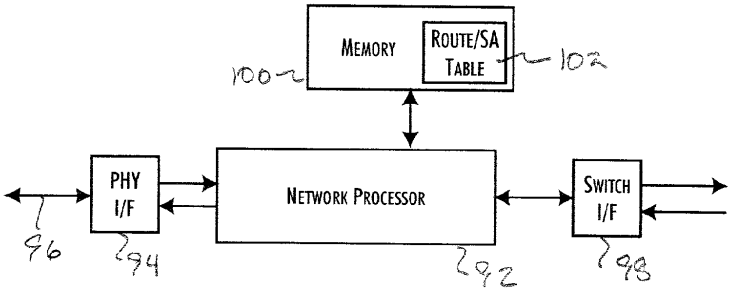
Ex. 1004, Fig. 4. In Pham's VPN gateway, there are network ingress processors, egress processors, and data packet (crypto) processors. *Id.*, [0039]. "In the preferred embodiments of the present invention, the ingress processors 30, 34 are tasked with filtering and routing functions for network data packets received on their network connections to the LAN 38 and Internet 18." *Id.*, [0038]; *see also* Ex. 2010, ¶ 53. "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." Ex. 1004, [0040]; *see also* Ex. 2010, ¶ 54. In Pham's VPN gateway, the only packets processed by the data packet (crypto) processors are those going across the WAN (e.g., VPN) because they are subject to the VPN encryption protection. Ex. 1004,

[0041]; *see also* Ex. 2010, ¶ 54. Notably, the packets that are bypassed between the ingress and egress processors are communicated across the crossbar switch fabric.



Ex. 1004, Fig. 4 (annotated to show LAN-to-LAN switching, LAN to VPN WAN routing, and VPN WAN to LAN routing).

In Pham's preferred embodiments, the ingress and egress processors utilize substantially the same implementation of a communication processor 90 as shown in Figure 5 of Pham. Ex. 1004, [0049]; *see also* Ex. 2010, ¶¶ 53-54.



90 FIG. 5

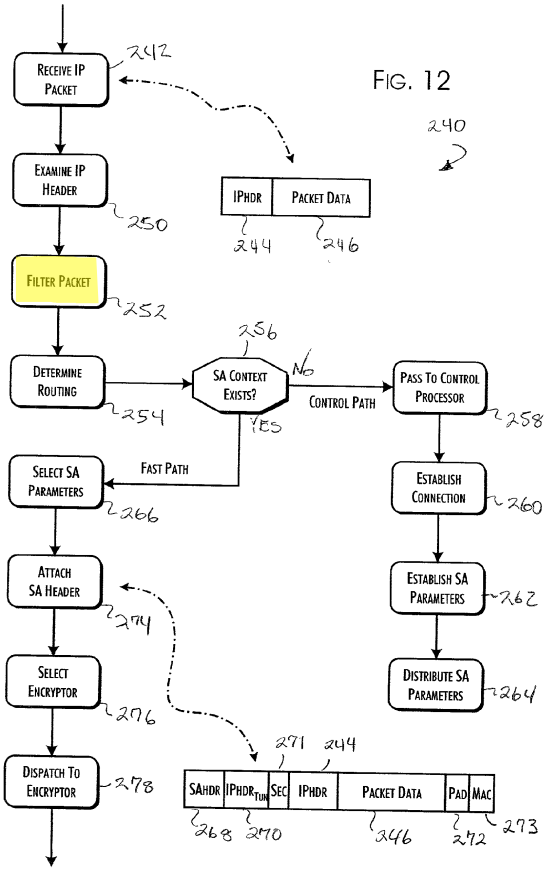
Ex. 1004, Fig. 5; *see also* Ex. 2010, ¶ 53. The network processor 92 is a programmable processor that supports Layer 2 and 3 network packet processing, filtering, and routing. Ex. 1004, [0049]; *see also* Ex. 2010, ¶¶ 53-54.

"Included within [the] memory [of the ingress processors] 100 is a data table 102 providing a dynamic data store for accumulated routing and filtering information. For implementations of the ingress processor 80 utilized in preferred embodiments of the present invention, the data table 102 also stores network connection SA [secure authority] parameter data. The route and filtering data are accumulated in a conventional manner from inspection of the attached interfaces and the source addresses of data packets received through the interfaces." Ex. 1004, [0050]. "Preferably, the SA parameter data is used by the ingress processor 80 to dynamically create and attach SA headers to each received IPsec data packet. Thus, in accordance with the preferred embodiment of the present invention, each IPsec data packet transferred to a crypto processor 86 is packaged with all of the necessary SA information needed for IPsec protocol processing." *Id.*, *see also* Ex. 2010, ¶¶ 56-57.

In Pham's preferred embodiment, the ingress processor filters data packets that are not going to be passed through the VPN. Ex. 1004, [0038] ("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."); *see also* Ex. 2010, ¶¶ 53, 56-57. Pham teaches that the ingress processor maintains the filtering responsibility even under high wire-speeds where other functions may be off-loaded. Ex. 1004, [0043] ("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. Thus, at wire-speeds in excess of about 20 Gbps, limiting the computational responsibilities of the ingress processors 52 to basic switching and filtering network data packets may be preferred."); *see also* Ex. 2010, ¶¶ 58-61.

As shown in Pham's flow diagram of ingress processor network packet processing, filtering precedes routing. "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." Ex. 1004, [0069]; *see also* Ex. 2010, ¶¶ 56-57, 59-60.

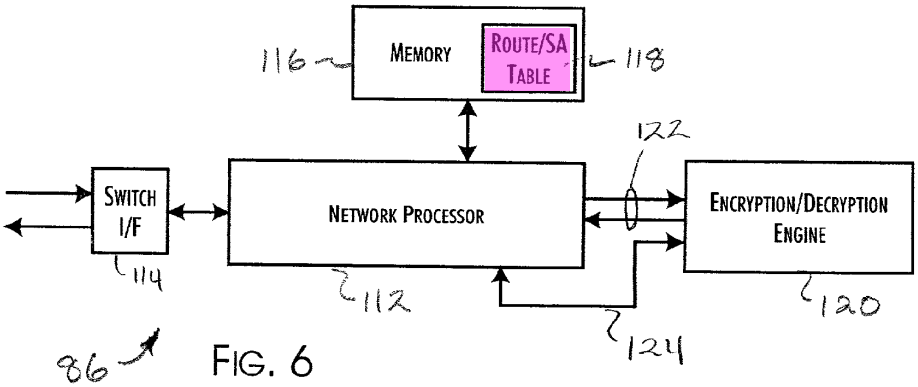


Ex. 1004, Fig. 12 (annotated to highlight filtering step). The only packets processed by the data (crypto) processor are those that are passed through the virtual private network. *Id.*, [0069]; *see also* Ex. 2010, ¶ 57.

The preferred embodiment of a data packet (crypto) processor in Pham has some similarities to the network ingress/egress processors, and preferably uses the same NP4GS3 Network Processor. Ex. 1004, [0051]. "The network processor 112 is also preferably an NP4GS3 Network Processor, including a switch fabric interface

114. A memory array 116 is provided for the external memory and program requirements of the network processor." *Id.*

Pham also teaches an alternative embodiment in which "the memory array 116 [of the data packet (crypto) processor] also provides storage space for an SA parameter data table 118. In this alternate embodiment, the SA parameter association task is off-loaded from the ingress processors 80 and performed by the crypto processors 86." *Id.*; *see also* Ex. 2010, ¶ 58.



Ex. 1004, Fig. 6 (annotated to highlight alternative embodiment SA Table). "The network processor 112 connects to and supports high-speed data interchange with a dedicated encryption/decryption engine 120 through a direct data transfer bus 122." *Id.*, [0052].

In the preferred embodiment of Pham, the SA parameter association task is performed at the ingress processor. "The relevant SA parameters are retrieved 266 from the SA context store and formatted into a SA header 268. A tunneling IP header 270, IPsec control fields 271, padding field 272, and Message Authentication Code

(MAC) field 273 are also created. These fields are then attached 274 to the network data packet." Ex. 1004, [0071]; *see also* Ex. 2010, ¶ 57. The network data packet and attached fields are then sent to the data packet (crypto) processor. "The network data packet received 282 by a crypto processor 86 preferably includes the SA header 268, tunneling IP header 270, IPsec control fields 271, padding field 272, and MAC field 273, as well as the original network data packet 244, 246." Ex. 1004, [0072]; *see also* Ex. 2010, ¶ 57. The packet intended for the VPN is encrypted and sent to the egress processor. Ex. 1004, [0072]-[0073]. "The operational protocol conversion of encrypted network data packets to clear text data packets closely parallels that of the clear text to encrypted conversion operations 240, 280, 300." Ex. 1004, [0074]. In the alternate embodiment of Pham, *see id.*, [0051], the SA parameter association task is "off-loaded" from the ingress processor and performed at the data packet (crypto) processor. The ingress processor maintains its "basic switching and filtering" functions on data packets, as well as determining whether an SA context exists (to choose where to forward the packet to, i.e., to a data packet (crypto) processor for "fast path processing" or a control processor) and performing load-balancing amongst the plurality of data packet (crypto) processors. *See id.*, [0043], Ex. 2010, ¶¶ 58-60.

B. U.S. Patent No. 7,424,744, "Signature Based Network Intrusion Detection System and Method," ("Wu")

The secondary reference that Petitioner relies on for every ground, Wu, was substantively considered and applied by the patent examiner during the prosecution of the '436 Patent. *See, e.g.*, Ex. 1002, 21. Specifically, the Patent Examiner applied a very similar Wu patent, U.S. Patent No. 7,493,659, commonly assigned and filed the same day with a substantially similar disclosure. *See* Ex. No. 2007, U.S. Patent No. 7,493,659 ("Wu et al."). *Compare*, *e.g.*, Ex. No. 1005, Fig. 4 *and* Ex. No. 2007, Fig. 4; Ex. No. 1005, Fig. 3 *and* Ex. No. 2007, Fig. 2; Ex. No. 1005, Fig. 6 *and* Ex. No. 2007, Fig. 5; Ex. No. 1005, 1:9-2:10 *and* Ex. No. 2007, 1:9-2:10; Ex. No. 1005, 5:40-6:3 *and* Ex. 2007, 5:43-6:3. Nevertheless, the claims of the '436 Patent were allowed. *See* Ex. 1002, 21-22.

Notably, Wu teaches that "[t]he [network intrusion detection and analysis] system preferably receives raw network packets and uses a network adaptor that listens and analyzes all traffic in real-time as it travels across the network. The packets are received at receiving port (RX) 50 at the MAC (Medium Access Control) layer 52." Ex. 1005, 5:41-45. A POSITA would not position an intrusion detection system where only a limited number of packets could be analyzed. As Dr. Cole explains, locating an intrusion detection system where only encrypted WAN packets were analyzed, "it would monitor secure VPN traffic for intrusions, it would miss

Pham's much greater vulnerability to unencrypted traffic arriving over the WAN, as well as unencrypted traffic arriving over a LAN." Ex. 2010, ¶ 99. *See also* Ex. 2010, ¶¶ 83-84, 97-99.

C. U.S. Patent No. 7,996,670, "Classification Engine in a Cryptography Acceleration Chip," ("Krishna")

As an initial matter, Krishna does not directly pertain to whether independent claims 1 and 13 would have been obvious over Pham and Wu. Furthermore, Petitioner concedes that Krishna was cited by the examiner during the prosecution of the '436 Patent. Paper 3, Pet. at 21. Nevertheless, the claims of the '436 Patent were allowed. *See* Ex. 1002, 21-22. Krishna does not disclose, teach or suggest an intrusion detection system, and Petitioner does not assert that it does. Moreover, Petitioner does not explain how an intrusion detection system could be coupled between a cryptographic core and a packet engine in Krishna's classification engine in a cryptography acceleration chip.

D. U.S. Patent Publication 2002/0073316A1, "Cryptographic System Enabling Ownership of a Secure Process," ("Collins")

As an initial matter, Collins does not directly pertain to whether independent claims 1 and 13 would have been obvious over Pham and Wu. The Collins reference is directed to "methods of using public key cryptography." Ex. 1008, [0003]. Accordingly, Collins "provide[s] an efficient cryptographic system for implementing public key cryptography with multiple prime factors." *Id.*, [0013].

Collins does not disclose or suggest a virtual private network such as is disclosed in Pham.

IV. CLAIM CONSTRUCTION AND A PERSON OF ORDINARY SKILL IN THE ART.

Patent Owner contends that the terms of the challenged claims should be construed in accordance with their plain and ordinary meaning to a person of ordinary skill in the art (POSITA) in light of the specification and the prosecution history. The Board should be aware that the terms of the '436 Patent were construed by the District Court in the active consolidated district court case involving the '436 patent pending in the Eastern District of Texas: *Lionra Technologies Limited v. Fortinet, Inc.*, No. 2:22-cv-00322-JRG-RSP (Lead Case). This case was consolidated with Member Cases *Lionra Technologies Limited v. Cisco Systems, Inc.*, No. 2:22-cv-00305-JRG-RSP (E.D. Tex.) and *Lionra Technologies Limited v. Palo Alto Networks, Inc.*, No. 2:22-cv-00334-JRG-RSP (E.D. Tex.). *See* Ex. 2002, Order, *Lionra Technologies Limited v. Fortinet, Inc.*, No. 2:22-cv-00322-JRG-RSP (Lead Case), Dkt. No. 21 (E.D. Tex. Oct. 24, 2022) (Consolidating cases). *See* Ex. 2009, Claim Construction Order, *Lionra Technologies Limited v. Fortinet, Inc.*, No. 2:22-cv-00322-JRG-RSP (Lead Case), Dkt. No. 162 (E.D. Tex. Nov. 27, 2023). Patent owner contends that the District Court's construction of the terms of the '436

Patent is consistent with the plain and ordinary meaning of these terms to a person of ordinary skill in the art.

Patent Owner contends that a POSITA would have, at the time of the respective inventions, either (1) a bachelor's degree in computer science or computer engineering including at least two years of experience in computer networking, system security and authentication or (2) equivalent work experience in the design and/or implementation of systems involving computer networking, security, and authentication. As reflected in the level of ordinary skill, a person of ordinary skill can have equivalent education and work experience.

V. ASSERTED GROUNDS OF ALLEGED UNPATENTABILITY

Petitioner asserts that the challenged claims are unpatentable as obvious based on four grounds.

Ground	Claims	Basis	References
1	1-2, 9-13, 16 and 22	§ 103	Pham in view of Wu
2	3, 14 and 21	§ 103	Pham in view of Wu and Collins
3	4, 7 and 8	§ 103	Pham in view of Wu and Collins and Krishna
4	17	§ 103	Pham in view of Wu and Krishna

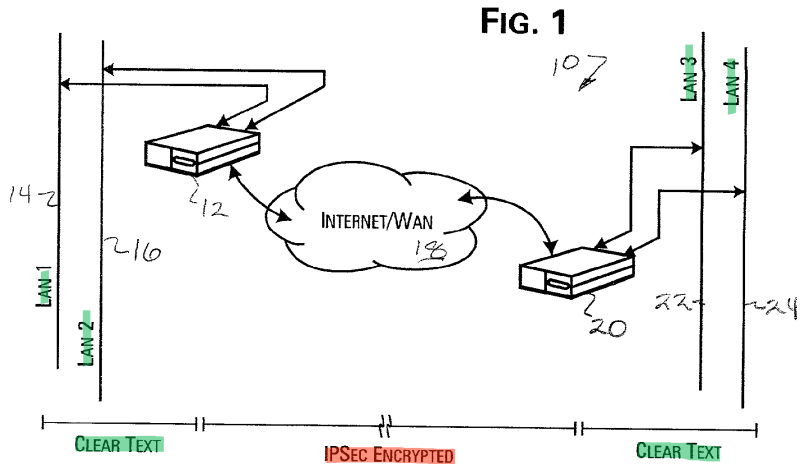
All of Petitioner's grounds rely upon Pham as the primary reference and Wu as a secondary reference. Grounds 2 and 3 also rely on the Collins reference, and grounds 3 and 4 also rely on the Krishna reference.

A. Ground 1: Pham in view of Wu (Claims 1-2, 9-13, 16 and 22)

Petitioner relies on the Pham reference for every limitation of the challenged claims except for [1.viii], [12], [13.vii] and [22] ("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" "wherein the at least one packet matching the signature stored in the signature database comprises a plain text packet."). Petitioner's reliance on Pham fails because Pham does not disclose [1.iv] or [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.**" Ex. 1001, 24:19-21 (Cl. 1), 25:20-22 (Cl. 13) (emphasis added).

1. Petitioner ignores packets in the crossbar switch fabric that go directly between the ingress processor and the egress processor.

The Petition identifies Pham's crossbar switch fabric 78 as the claimed switching system. Paper 3, Pet. at 35-36. As discussed above, 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).



Id., Fig. 1. As shown in Figure 1, Pham discloses transmission of both clear text (green) and encrypted (red) packets. The only encrypted packets in Pham are IPsec Encrypted packets travelling over a virtual private network (VPN) established between the VPN gateways 12 and 20. A substantial number of the packets traversing Pham's VPN gateways are clear text unencrypted packets that travel between LAN 1 and LAN 2 or LAN 3 and LAN 4. *See* Ex. 2010, ¶¶ 51-55. These unencrypted packets do not require processing through data packet (crypto) processors, so the unencrypted packets are filtered to bypass the data packet (crypto) processors and move between the ingress and egress processors that handle classification processing (highlighted in yellow below) through the crossbar switch fabric. Ex. 1004, [0038]-[0040]; Ex. 2010, ¶¶ 51-55.

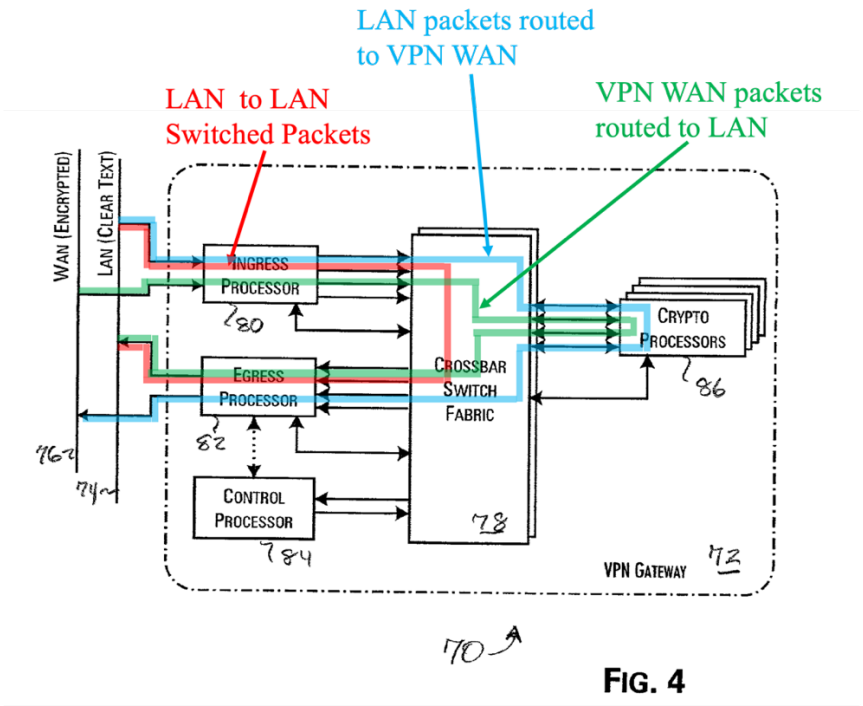
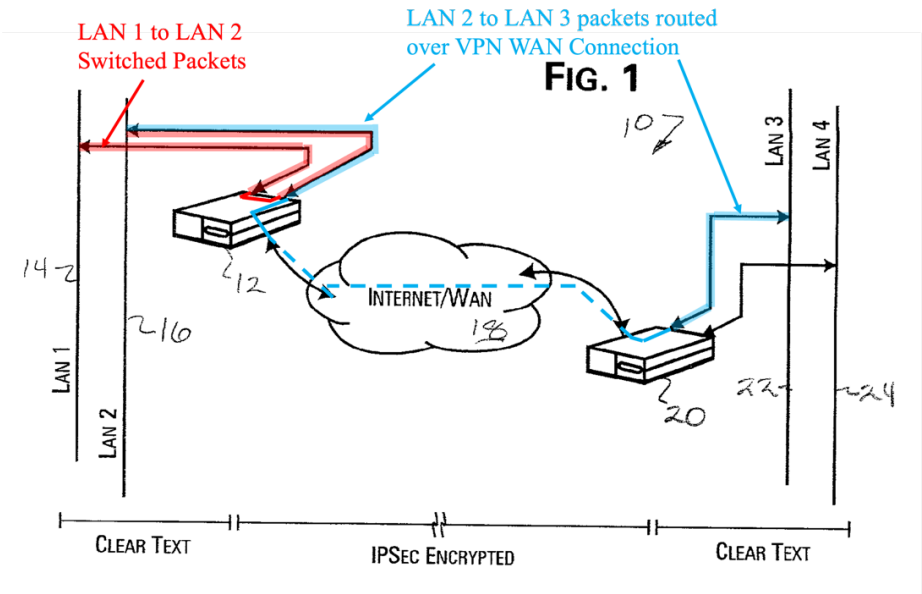


FIG. 4

Ex. 1004, Fig. 4 (annotated to show LAN-to-LAN switching, LAN to VPN WAN routing, and VPN WAN to LAN routing). The Petition does not address these unencrypted packets that necessarily transit the crossbar switch fabric identified by Petitioner as the claimed switching system. But, as Petitioner admits, Pham discloses incoming packets from the LAN and the WAN and outgoing packets to the LAN and the WAN, all of which go through the ingress processor and the egress processor. *See* Paper 3, Pet. at 34 (annotated Figure 4 of Pham showing green incoming packets and pink outgoing packets). By excluding the packets that go directly from the ingress processor to the egress processor via the crossbar switch fabric (Petitioner's identified "switching system"), the Petition disregards that a substantial number of the incoming and outgoing packets will not be processed by

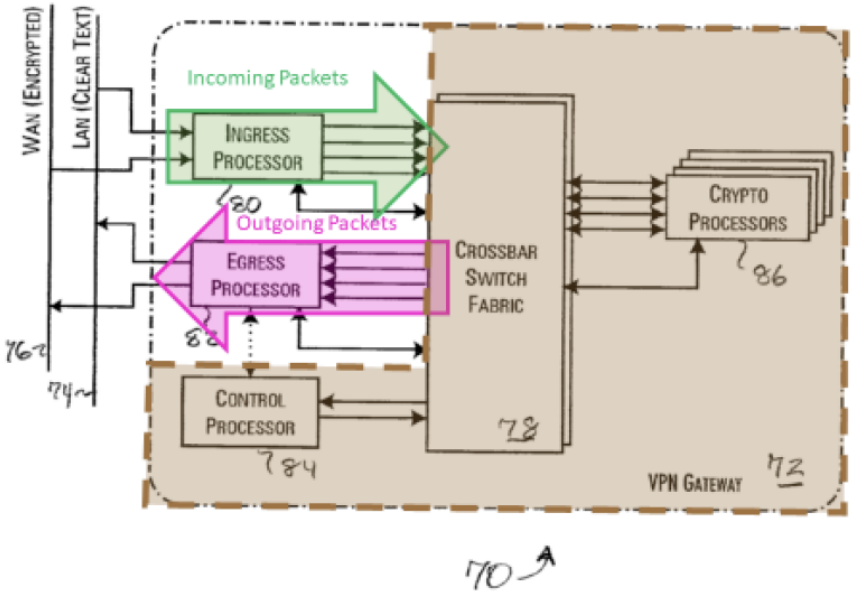
what Petitioner identifies as the claimed packet engine. *See* Ex. 2010, ¶ 94. As Dr. Cole illustrates in his declaration, Petitioner ignores the "LAN to LAN Switched Packets" (highlighted in red):



Id. As Dr. Cole explains, "a POSITA would expect Pham's VPN Gateway Switch to switch a substantial amount of packets from LAN-to-LAN. Those packets would pass through Pham's switch fabric but not pass through the data packet processor / crypto processor and, therefore, a substantial amount of packets would pass through the identified 'security processor' but not through the identified 'packet engine.' Pham does not describe that "substantially all" packets pass through the 'packet engine.'" *Id.*, ¶ 95.

2. Substantially all of the incoming packets and outgoing packets to the security processor will <u>not</u> transit one of the plurality of crypto processor network processors Petitioner identifies as packet engines.

Claim limitations [1.iv] and [13.iv] recite "wherein the packet engine is one of a plurality of packet engines and <u>substantially all</u> of the incoming packets and outgoing packets to the security processor transit one of the plurality of packet engines, …." Ex. 1001, 24:19-21 (Cl. 1), 25:20-22 (Cl. 13). As to the claimed "security processor," the Petition identifies a portion of Pham's VPN Gateway Switch (highlighted in brown in figure below):



Paper 3, Pet. at 33-34; *see also* Ex. 2010, ¶ 87. The Petition also identifies the network processors in the crypto processors as the claimed packet engines. Paper 3, Pet. at 37-38, 40; *see also* Ex. 2010, ¶ 89.

Petitioner asserts that "Pham discloses that the network processors 112 process substantial [sic] all the data packet [sic] received and transmitted by the VPN gateway." Paper 3, Pet. at 41; *see also* Ex. 2010, ¶ 91. In support of this assertion, Petitioner points to Pham's use of identical processors in "ingress processor 80 (Fig. 5) and network processor 112 in crypto processor 86 (Fig. 6)," and further asserts that the use of "identical routing and SA tables" allows "functions of the ingress processor to be offloaded to network processor 112, such as packet routing, SA parameter association and compression and decompression." Paper 3, Pet. at 42. Petitioner then concludes that "all packets, both clear text and encrypted can be sent to network processor 112." *Id.*

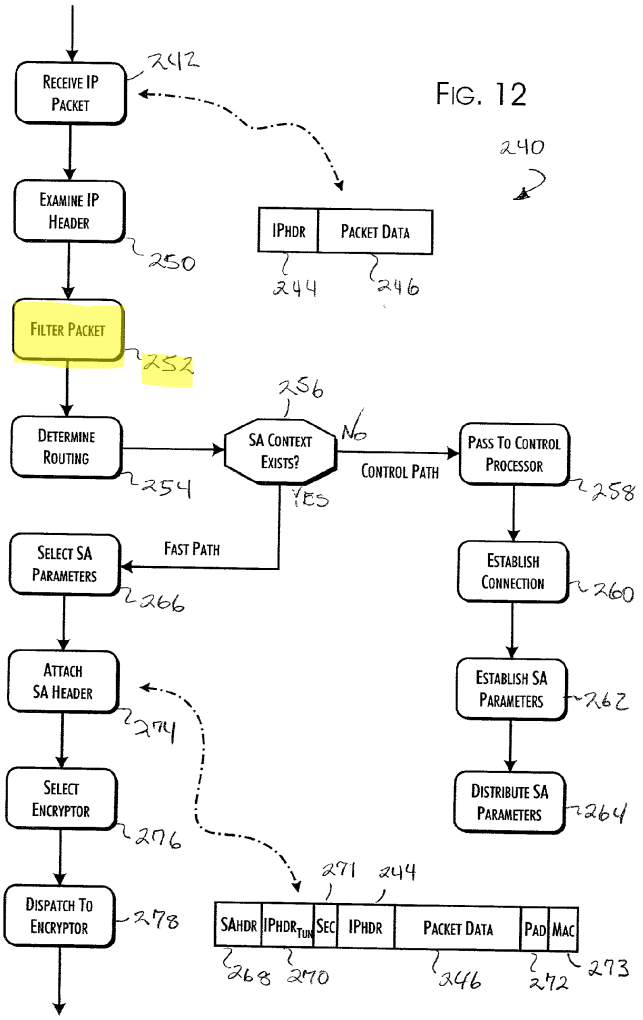
Petitioner is incorrect. Pham's ingress processor filters data packets that are not going to be passed through the VPN connection on the WAN. Ex. 1004, [0038] ("In the preferred embodiments of the present invention, the ingress processors 30, 34 are tasked with filtering and routing functions for network data packets received on their network connections to the LAN 38 and Internet 18."); *see also* Ex. 2010, ¶¶ 51-57. The alternate embodiment that Petitioner relies on does not change this. In that embodiment, Pham discloses that the ingress processor maintains this filtering function and that **only** the SA parameter association task may be off-loaded to crypto processor 80. Ex. 1004, [0051] ("In this alternate embodiment, the SA parameter association task is off-loaded from the ingress processors 80 and

performed by the crypto processors 86."); *see id.*, [0043] ("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. Thus, at wire-speeds in excess of about 20 Gbps, limiting the computational responsibilities of the ingress processors 52 to basic switching and filtering network data packets may be preferred."); *see also* Ex. 2010, ¶¶ 58-60.

Consequently, Petitioner's assertion that "all packets, both clear text and encrypted can be sent to network processor 112," Paper 3, Pet. at 42, finds no support in Pham. *See* Ex. 2010, ¶¶ 59-60. Pham's ingress processors filter out data packets not destined for a WAN VPN connection and transmit those packets to an egress processor through the crossbar switch fabric (part of Petitioner's alleged "security processor"). *See id.*, ¶¶ 91-94. Because a substantial portion of the data packets transiting Pham's crossbar switch fabric are **not** processed by the network processors in the crypto processors (Petitioner's alleged "packet engine"), Pham does not describe that "substantially all of the incoming packets and outgoing packets to the security processor transit one of the plurality of packet engines." *See id.*, ¶ 95.

As discussed above and as shown in Pham's flow diagram of ingress processor network packet processing, filtering precedes routing. "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." Ex. 1004, [0069]. A POSITA would understand that Pham teaches filtering by the ingress processor, even with the alternate embodiment where an SA parameter table is stored in the memory of a crypto processor. *See* Ex. 2010, ¶¶ 58-60. The only packets processed by the data (crypto) processor are those that are passed across the WAN using a virtual private network connection. Ex. 1004, [0069].



Id., Fig. 12 (Filter packet step 252 precedes and is separate from step 254, determine routing, and evaluation of the SA parameters).[1]

A POSITA would understand that because Pham teaches packet filtering by the ingress processor and the filtered packets necessarily transit what Petitioner

[1] The Petition also incorrectly asserts that Pham teaches network processor 112 performs compression and decompression. Paper 3, Pet. at 42. Pham actually teaches that "[i]n particular, a general purpose microprocessor can be substituted or provided in addition to the network processor 112 to support data compression and decompression operations." Ex. 1004, [0053].

identifies as the claimed "switching system" (crossbar switch fabric), in both the preferred and alternate embodiments, substantially all of the incoming packets and outgoing packets in the security processor would **not** transit one of the plurality of crypto processor network processors. *See* Ex. 2010, ¶ 95. Therefore, Ground 1 fails as to all the independent claims because Pham does not disclose [1.iv] or [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.**"

3. Petitioner incorrectly asserts that the incoming packets and outgoing packets are provided with a tag upon ingress to one of the crypto processor network processors and the tag determines an egress path within the security processor upon exit from a corresponding encryption/decryption engine.

Claim limitation [1.v] recites "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; …." Petitioner's assertion that this claim limitation is taught by Pham's disclosure of an IP tunneling header is incorrect. Petitioner's discussion of Pham's teachings regarding an IP tunneling header is misleading because petitioner's citation to Pham omits a critical prerequisite. *See* Paper 3, Pet. at 43. As taught by Pham, the relevant SA parameters are only retrieved

where a SA context is found in the data table. "Where a SA context is found 256 in the data table 102 by an ingress processor 80, fast path processing is selected. The relevant SA parameters are retrieved 266 from the SA context store and formatted into a SA header 268." Ex. 1004, [0071]. A POSITA would understand that clear text data packets that are not routed through the VPN would not have an SA header. *See, e.g.*, Ex. 2010, ¶¶ 57, 60.

Petitioner ignores the filtering step 252. As taught by Pham, "[a]n 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*." Ex. 1004, [0069] (emphasis added); *see also* Ex. 2010, ¶¶ 57, 60.

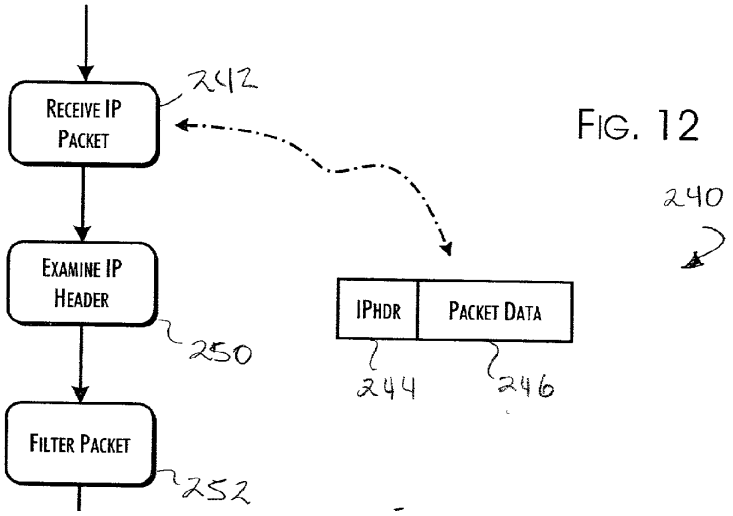


FIG. 12

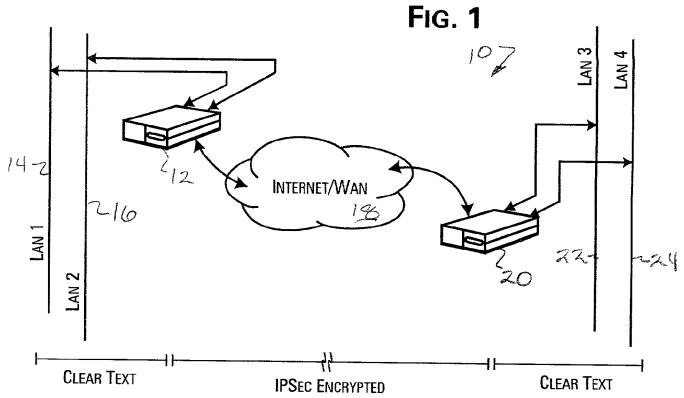
Ex.1004, Fig. 12. Because data packets that are not to be passed through the VPN gateway are filtered out by the ingress processor, those data packets do not have headers added to the "ingress packet" identified by Petitioner, including, but not

limited to, an SA header or a tunneling IP header. *See* Paper 3, Pet. at 44; *see also* Ex. 2010, ¶¶ 57, 60. Therefore, Ground 1 fails as to all the independent claims because Pham does not disclose [1.v] or [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."

4. It would not have been obvious to a POSITA to modify the teachings of Pham with the teachings of Wu to add an intrusion detection system to Pham's crypto processor.

Claim limitations [1.vii] and [13.vii] recite "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." Ex. 1001, 24:35-39 (Cl. 1); Ex. 1001, 25:37-26:2 (Cl. 13). Petitioner's contention that "[i]t would have been obvious to modify the teachings of Pham with the teachings of Wu to add an intrusion detection system and signature database to the network data processor system AND to functionally locate the IDS between the network processor (*packet engi*ne) and the encryption/decryption engine (*cryptographic core*)" is incorrect. *See* Paper 3, Pet. at 53.

As an initial matter, Pham discloses a closed system in which the only connections to the internet are through secure connections and a virtual private network. Ex. 1004, Fig. 1.



Because Pham teaches a closed system, a POSITA would have to consider the increased complexity and resources required to modify the teachings of Pham with the teachings of Wu, something which Petitioner does not address. For example, Pham teaches that simply adding support for compression or decompression would require supplementing or replacing the preferred network processor. "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." Ex. 1004, ¶ 53. A POSITA would accordingly not be motivated to combine the teachings of Pham and Wu. *See* Ex. 2010, ¶ 98.

And, even if a POSITA were motivated to combine the teachings of Pham and Wu, a POSITA would not locate the IDS between the network processor (*packet engi*ne) and the encryption/decryption engine (*cryptographic core*) because doing so would only monitor traffic passing over the secure virtual private network while ignoring all of the clear text packets filtered by the ingress processor as discussed above. *See* Ex. 2010, ¶ 99.

Therefore, Ground 1 fails as to all the independent claims because Petitioner fails to show that [1.vii] or [13.vii] is obvious in view of Pham and Wu.

5. Petitioner's contentions regarding dependent claims 2, 9, 10, 12, 16 and 22 fail because Pham and Wu do not disclose or teach the limitations of independent claims 1 and 13.

Because the prior art does not teach or disclose limitations of each of the independent claims, it does not anticipate or render obvious any of the dependent claims of the '436 patent. *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."); s*ee also Callaway Golf Co. v. Acushnet Co.*, 576 F.3d 1331, 1344 (Fed. Cir. 2009) (holding verdict irreconcilably inconsistent where jury found dependent claim obvious and found independent claim nonobvious).

B. Ground 2: Pham in view of Wu and Collins (Claims 3, 14 and 21).

Claim 3 depends from independent claim 1 and claims 14 and 21 depend from independent claim 13. As discussed in Section V.A., Pham and Wu do not teach or disclose the limitations of each of these independent claims. Petitioner makes no argument that the additional teachings of Collins remedy that fundamental deficiency. Paper 3, Pet., 64-69. Therefore claims 3, 14, and 21 are not rendered obvious by the teachings of Pham in view of Wu and Collins.

C. Ground 3: Pham in view of Wu, Collins and Krishna (Claims 4, 7 and 8)

Claim 4 depends from claim 3 which depends from independent claim 1. Claim 7 depends from claim 4 and claim 8 depends from claim 7. As discussed in Section V.A., Pham and Wu do not teach or disclose the limitations of independent claim 1. Petitioner makes no argument that the additional teachings of Collins remedy that fundamental deficiency. Paper 3, Pet., 69-72. Therefore claims 4, 7 and 8 are not rendered obvious by the teachings of Pham in view of Wu, Collins, and Krishna.

Moreover, petitioner's terse discussion of the teachings of Krishna omits any discussion of how limitation [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. *Id.* Petitioner has therefore failed to show that claim 4 would have been obvious to a POSITA over Pham, Wu and Collins in view of Krishna.

D. Ground 4: Pham in view of Wu and Krishna (Claim 17)

Claim 17 depends from independent claim 13. As discussed in Section V.A., Pham and Wu do not teach or disclose the limitations of independent claim 13. Petitioner makes not argument that the additional teachings of Krishna remedy that

fundamental deficiency. Paper 3, Pet., 72-73. Therefore claim 17 is not rendered obvious by the teachings of Pham in view of Wu and Krishna.

Moreover, petitioner's terse discussion of the teachings of Krishna omits any discussion of how limitation [13.viii] of independent claim 13 ("an intrusion detection system coupled between the cryptographic core and the packet engine") could or would be satisfied if the security processor was formed on a single chip. *Id.* Petitioner has therefore failed to show that claim 13 would have been obvious to a POSITA over Pham, Wu, and Krishna.

VI. CONCLUSION

Pham does not disclose that "substantially all of the incoming packets and outgoing packets to the security processor transit one of the plurality of packet engines" as recited by limitations [1.iv] and [13.iv] of the independent claims of the '436 Patent. Furthermore, a person of ordinary skill in the art would not be motivated to combine Pham with Wu as the Petition asserts. For these reasons, and all of the other reasons set forth above, Patent Owner respectfully requests that the Board deny institution.

Respectfully submitted,

/Brett Cooper/
Brett Cooper, Reg. No. 55,085
Lead counsel for Patent Owner

Date: February 22, 2024

CERTIFICATE OF WORD COUNT (37 C.F.R. § 42.24(d))

The undersigned hereby certifies that the word count in this Patent Owner Response to Petition is 6,606 words, as counted by the word-processing program Microsoft Word that was used to generate this Patent Owner Preliminary Response, where such word count excludes the table of contents, table of authorities, mandatory notices, certificate of service, appendix of exhibits, claim listing, and this certificate of word count. This Patent Owner Response to Petition is in compliance with the 14,000-word limit set forth in 37 C.F.R. § 42.24(b)(1).

Date: February 22, 2024

/Brett Cooper/

BC Law Group, P.C.
200 Madison Avenue, 24th Floor
New York, NY 10016
(212) 951-0100

Brett Cooper
Reg. No. 55,085
Attorney for Patent Owner

CERTIFICATE OF SERVICE (37 C.F.R. § 42.6(e))

The undersigned hereby certifies that the above document was served on February 22, 2024, by filing this document through the Patent Trial and Appeal Case Tracking System as well as delivering a copy via electronic mail upon the following attorneys of record for the Petitioner:

Eric A. Buresh, Reg. No. 50,394
eric.buresh@eriseip.com
PTAB@eriseip.com

Mark C. Lang, Reg. No. 55,356
mark.lang@eriseip.com

Patrick D. McPherson, Reg. No. 46,255
PDMcPherson@duanemorris.com

Patrick C. Muldoon, Reg. No. 47,343
PCMuldoon@duanemorris.com

Date: February 22, 2024

/*Brett Cooper*/

Brett Cooper, Reg. No. 55,085
Attorney for Patent Owner

BC Law Group, P.C.
200 Madison Avenue, 24th Floor
New York, NY 10016
(212) 951-0100