

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

CISCO SYSTEMS, INC.
Petitioner,

v.

LIONRA TECHNOLOGIES LTD.
Patent Owner.

U.S. Patent No. 7,685,436

Title: SYSTEM AND METHOD FOR A SECURE I/O INTERFACE

Inter Partes Review No.: IPR2023-00673

**CORRECTED PETITION FOR *INTER PARTES* REVIEW OF U.S.
PATENT NO. UNDER 35 U.S.C. §§ 311-319 and 37 C.F.R. §§ 42.1-.80,
42.100-.107**

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
I. INTRODUCTION	1
II. OVERVIEW	1
III. GROUNDS FOR STANDING (37 C.F.R. § 42.104(A))	5
IV. REASONS FOR THE REQUESTED RELIEF	5
V. BACKGROUND	5
A. Summary of the '436 Patent.....	5
B. Prosecution History	11
C. Claim Construction.....	14
D. Priority Date of the Challenged Claims	14
E. Person of Ordinary Skill in the Art	14
F. State of the Art	15
VI. IDENTIFICATION OF CHALLENGES.....	19
A. Challenged Claims	19
B. Statutory Grounds for Challenges	19
C. Prior Art Basis	20
VII. IDENTIFICATION OF HOW THE CHALLENGED CLAIMS ARE UNPATENTABLE	21
A. Ground 1: Claims 1, 2, 9-13, 16 and 22 are unpatentable over Pham in view of Wu.....	21
1. The Pham Reference	21
2. The Wu Reference	24

3.	The Motivation To Combine the Teachings of Pham with the Teachings of Wu with a Reasonable Prediction of Success	26
4.	Detailed Application of Pham and Wu	33
B.	Ground 2: Claims 3, 14 and 21 Are Unpatentable Over Pham and Wu in Further View of Collins	64
1.	The Collins Reference.....	64
2.	Detailed Application of Pham and Wu and Collins.....	65
C.	Ground 3: Claims 4, 7, and 8 Are Unpatentable Over Pham, Wu and Collins and Further In View of Krishna	69
1.	The Krishna Reference	69
2.	Detailed Application Of Pham, Wu, Collins and Krishna.....	69
D.	Ground 4: Claim 17 Is Unpatentable Over Pham and Wu and Further In View of Krishna	72
VIII.	THE BOARD SHOULD NOT EXERCISE ITS DISCRETION AND DENY INSTITUTION	73
A.	The Board Should Not Deny Institution Under 35 U.S.C. § 325(d)	73
B.	The Board Should Not Deny Institution Under 35 U.S.C. § 314(a).....	75
IX.	MANDATORY NOTICES UNDER 37 C.F.R. §42.8	78
A.	Real Party-in-Interest (37 C.F.R. § 42.8(b)(1)).....	78
B.	Related Matters (37 C.F.R. § 42.8(b)(2)).....	78
1.	JUDICIAL MATTERS	78
2.	ADMINISTRATIVE MATTERS:	79
3.	RELATED PATENTS	79

C.	Lead/Back-up Counsel (37 C.F.R. § 42.8(b)(3)):	79
D.	Notice of Service Information (37 C.F.R. § 42.8(b)(4)):	81
X.	CONCLUSION	81

TABLE OF AUTHORITIES

PAGE(S)

CASES

<i>Advanced Bionics, LLC v. MED-EL Elektromedizinische Geräte GmbH</i> , IPR2019-01469, Paper 6, (PTAB Feb. 13, 2020)((Precedential)).....	73
<i>Apple Inc. v. Fintiv, Inc.</i> , IPR2020-00019, Paper 11 (PTAB Mar. 20, 2020) (Precedential).....	75
<i>Sand Revolution II LLC v. Continental Intermodal Group – Trucking LLC</i> , IPR2019-01393, Paper 24 at 7 (June 16, 2020) (informative).....	76, 77
<i>HP Inc. v. Slingshot Printing LLC</i> , IPR2020-01084, Paper 13.....	77
<i>PEAG LLC v. Varta Microbattery GMBH</i> , IPR2020-01214, Paper 8 (Jan. 6, 2021).....	77

Petitioner's Exhibit List

<i>Exhibit #</i>	<i>Description</i>
1001	U.S. Patent No. 7,685,436 (“the ’436 Patent”)
1002	Select portions of prosecution history of the ’436 (“File History”)
1003	Declaration of Petitioner’s Expert Dr. Crovella (“Crovella”)
1004	U.S. 2003/0074473 (“Pham”)
1005	U.S. 7,424,744 (“Wu”)
1006	U.S. 7,996,670 (“Krishna”)
1007	U.S. 6,279,113 (“Vaidya”)
1008	U.S. Patent Publication 2002/0073316 (“Collins”)
1009	U.S. 7,181,017 (“Nagel”)
1010	US 2004/0039928A1 (“Elbe”)
1011	Related Patents
1012	Not used
1013	Not used
1014	Docket Control Order, <i>Lionra Technologies Limited v. Fortinet, Inc.</i> , Case No. 2:22-cv-00322 (E.D. Tex.) Document 55-1
1015	U.S. Patent Publication 2003/0145225A1 (“Bruton”)

I. INTRODUCTION

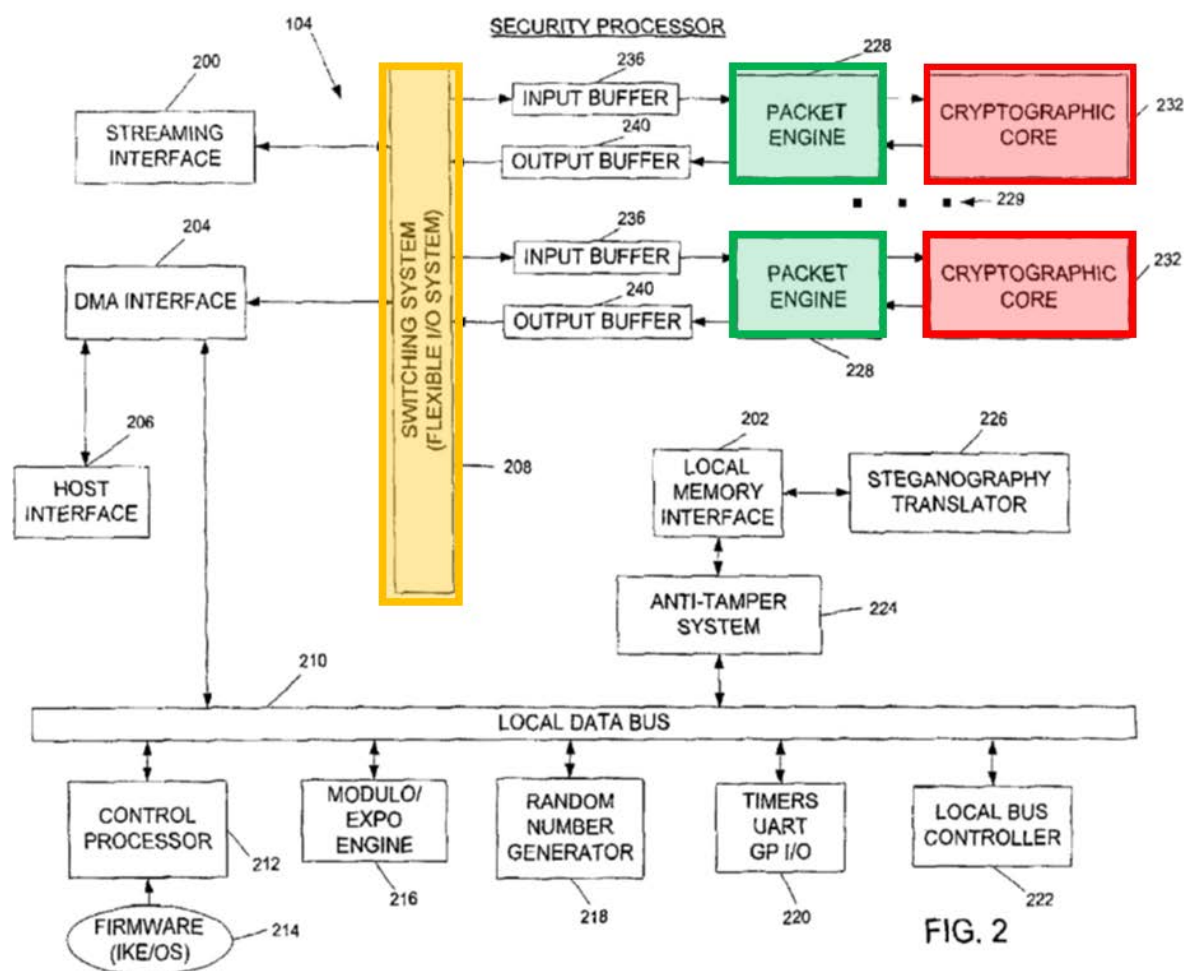
Pursuant to 35 U.S.C. §§ 311 *et seq.* and 37 C.F.R. §§ 42.1 *et seq.*, Cisco Systems, Inc. (“Petitioner”) hereby petitions for an *inter partes* review of U.S. Patent No. 7,685,436 (“the ’436 Patent”). Petitioner respectfully submits that Claims 1-4, 7-14, 16, 17, 21 and 22 (the “Challenged Claims”) of the ’436 Patent are unpatentable under 35 U.S.C. §103 in view of the prior art references discussed herein. This Petition demonstrates by a preponderance of the evidence that there is a reasonable likelihood that Petitioner will prevail with respect to at least one of these claims. Accordingly, it is respectfully requested that the Board institute an *inter partes* review of the ’436 Patent pursuant to 37 C.F.R. § 42.108.

II. OVERVIEW

The Challenged Claims are unpatentable as obvious over the prior art. The claims are directed to prior art systems and combinations of conventional components that perform conventional functions regarding processing packets for secure cryptographic communications and network intrusion detection.

Specifically, the ’436 Patent is directed to a security processor having a switching system (yellow), a cryptographic core (red) with a packet engine (green) for processing incoming and outgoing data packets interposed between the

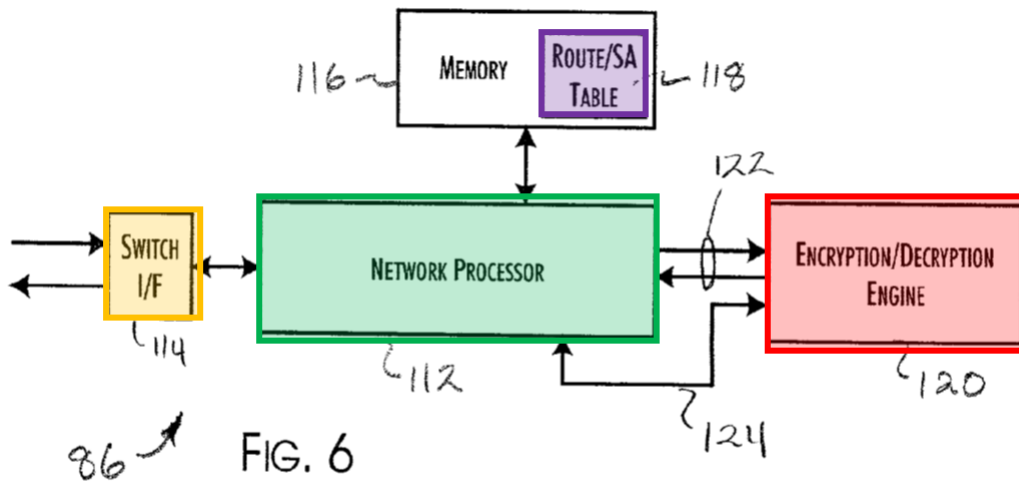
switching system and cryptographic core:



The '436 Patent also describes that an intrusion detection system using a signature database can be coupled between the packet engine and the cryptographic core to permit clear text packet capture either before or after encryption. EX-1001 19:5-8.

However, this security processor described in the '436 Patent was a combination of conventional components performing their intended purpose. Specifically, U.S. Patent Publication 2003/0074473 ("Pham") discloses a security

processor having a switching system (yellow), a cryptographic core (red) with a packet engine (green) for processing incoming and outgoing data packets interposed between the switching system and cryptographic core.



EX-1004 Fig. 6

U.S. Patent No. 7,424,744 (“Wu”) discloses an intrusion detection system. A POSA would understand that the intrusion detection system of Wu would be suitable for use with the packet engine of Pham. For example, Wu discloses a signature-based intrusion detection system with a signature database and describes that “intrusion detection system 14 may be used alone or in combination with a data monitoring and analysis device configured to perform fault and network performance management.” EX-1005 4:4-7: EX-1003 ¶ 31.

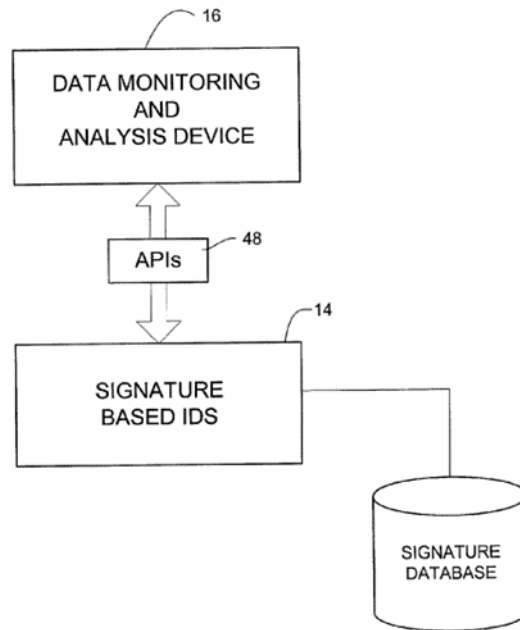


FIG. 2

EX-1005 Fig. 2: EX-1003 ¶ 31.

U.S. Patent Publication 2002/0073316 (“Collins”) discloses features recited in the dependent claims of the ’436 Patent directed to details of a cryptographic engine for performing “fast modular exponentiation” and that Collins describes that its design and operation are known to a POSA. EX-1008 [0048]; EX-1003 ¶ 32. U.S. Pat. No. 7,996,670 (“Krishna”). Krishna discloses features recited in the dependent claims of the ’436 Patent directed to a packet engine, a cryptographic core and other components of a security processor contained on a single chip. EX-1006 FIG. 2; 3:43-50; EX-1003 ¶ 32.

As will be described in detail below, because these references are all directed to the same problems described in the ’436 Patent and describe the same

solutions and features proposed in the '436 Patent, these references are analogous art and a POSA would be motivated to combine their teachings with a high likelihood of success, and the combination discloses each limitation recited in the Challenged Claims. EX-1003 ¶ 33.

III. GROUNDS FOR STANDING (37 C.F.R. § 42.104(A))

Petitioner certifies that the Patent for which review is sought is available for *inter partes* review and that Petitioner is not barred or estopped from requesting an *inter partes* review of the Challenged Claims on the grounds identified herein. 37 C.F.R. § 42.104(a). This Petition is filed pursuant to 37 C.F.R. § 42.106(a).

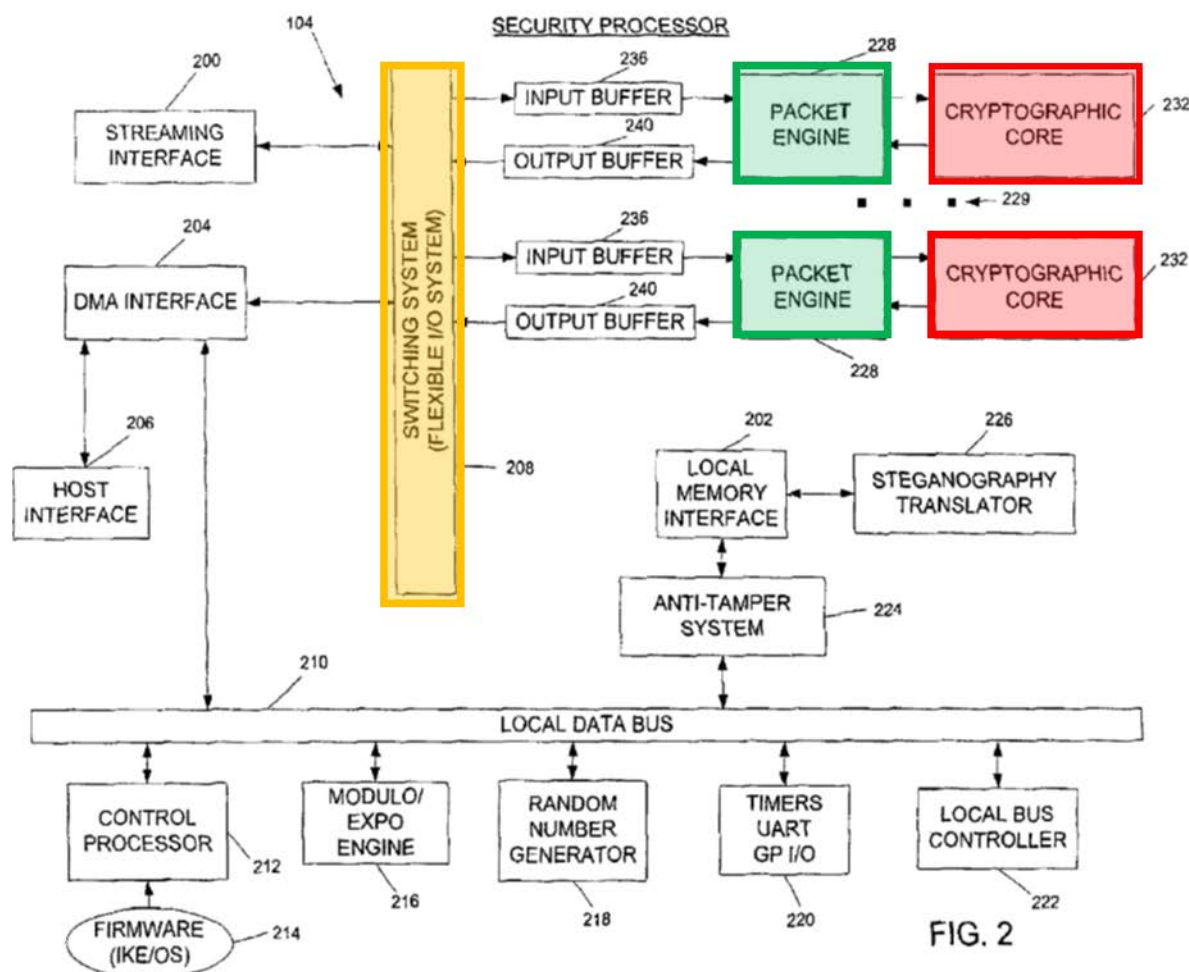
IV. REASONS FOR THE REQUESTED RELIEF

As explained in §§ II and VI-VIII of this Petition and in the attached Declaration of Petitioner's Expert, Dr. Crovella, EX-1003, the systems and methods of securing an I/O interface as described and claimed in the '436 Patent, were obvious over the prior art to a person of ordinary skill in the art ("POSA") at the time of the invention.

V. BACKGROUND

A. Summary of the '436 Patent

FIG. 2 of the '436 Patent illustrates a high-level simplified functional block diagram of one embodiment of a security processor 104. The '436 Patent describes that security processor 104 is preferably, though not necessarily, formed on a single chip. EX-1001 6:38-45; EX-1003 ¶ 34.



Switching system 208 (orange) provides 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. EX-1004 6:58-61; EX-1003 ¶ 35. The '436 Patent admits that the switching system 208 is known in the art and can be implemented using conventional switches. EX-1001 7:33-48; EX-1003 ¶ 35.

Packet engines 228 (green) may each be interposed between a cryptographic core 232 (red) and the switching system 208. Packet engines 228 may each comprise microprocessors customized for packet operations such as, for example,

packet processing and classification. The '436 Patent explains that suitable packet engines are known in the art, which process packets needing network address translation processing and firewall table processing, and process IPSec packets. Ex-1001 9:60-10:8; EX-1003 ¶ 36.

More specifically, each packet engine 228 may perform hash table lookups to a firewall connection table entry, which may contain state information, a rule to be applied to a packet, optional security association information, routing information (for example, for MAC overlay), and any application-level gateway (ALG) packet header altering to be done. EX-1001 10 8-13; EX-1003 ¶ 37.

For outbound IPSec traffic, each packet engine 228 may provide a pointer to security association data for an IP packet, load a security association database entry into a local buffer located on or off-chip, construct and add an outer IP header and IPSec header, perform lifetime checks, and update an associated security association database (SAD) entry (for example, the sequence number and byte count). EX-1001 10:14-20; EX-1003 ¶ 38.

For inbound IPSec traffic, each packet engine 228 may locate an associated SAD entry by using a security policy index (SPI) number from the IPSec header or by an SAD address provided by the classification of the destination address, protocol and SPI. In order to use the SPI number, IKE firmware 214 may define the inbound SPI number from the API provided for security processor 104 during

security association establishment. Packet engine 228 may then load the SAD entry into a local buffer, perform anti-replay checks and lifetime checks, and then update the SAD entry. Each cryptographic core 232 may remove tunnel IP headers, ESP or AH headers, and ESP trailers. The packet may then optionally be redirected through packet engine 228 for a firewall connection table lookup. EX-1001 10:21-34; EX-1003 ¶ 39.

Cryptographic cores 232 provide security processing to perform IPSec and/or SSL processing. Each cryptographic core 232 may provide high-speed fixed function encryption and authentication hash processing for packet data. Each cryptographic core 232 may receive instructions and key address information affixed to a packet for applying appropriate transforms. The '436 Patent describes that suitable cryptographic cores are known. EX-1001 11:23-47; EX-1003 ¶ 40.

The '436 Patent describes that in one embodiment, after exiting cryptographic core 232, a packet may be assigned its distribution directions (for example, to a destination of one of several streaming interfaces 200 or control processor 212) by packet engine 228 for distribution through switching system 208. EX-1001 11: 59-63; EX-1003 ¶ 41.

Initial packets for a data flow may transit from packet engine 228 and cryptographic core 232 to control processor 212 for an initial classification. Control processor 212 may perform firewall, NAT, and routing classification for

the packet, and further may create a connection table and hash entry in memory 106 for use by packet engine 228 on subsequent packets in the data flow. This may include the building of more than one connection table entry, depending on the application. Examples of this include preemptively constructing inbound and outbound entries, as well as a data channel entry for certain protocols. Control processor 212 may also trigger IKE processing as a result of the classification of the initial packet. EX-1001 12:6-18; EX-1003 ¶ 42.

The connection table entries above provide a mechanism that allows the acceleration of security operations, such as firewall or NAT decision processing for packets. Connection entries may have a relationship (for example, one-to-one or many-to-one) to IPSec SAD entries in support of IPSec operations as a result of classification. EX-1001 12:19-24; EX-1003 ¶ 43.

Switching system 208 may select the I/O port or interface, including host interface 206, to use for data packets based on the results of cryptographic or other security or network processing. For example, packets classified for forwarding to another destination after a security operation (such as encryption or new connection validation) could be directed to the proper egress port, while packet data requiring host inspection (such as IKE messages, or exception or initial packets for firewall classification) could be redirected to DMA interface 204. In contrast to prior systems that rely on external bus interfaces to re-direct packet

traffic to varying packet processing devices, the present invention may permit simplifying or collapsing the schema and protocols used, for example, in firewall, routing, NAT and IPSec processing with the result that lookups, transforms, and other application activity are more efficient. Prior systems typically require context labeling or other data envelopment or tagging to manage packet workflow among varying processing devices. Ex-1001 7:60-8:2; EX-1003 ¶ 44.

The '436 Patent issued with 22 Claims. Claims 1 and 13 are the only independent claims and recite a “security processor” and “security processing system” respectively. Claims 1 and 13 are substantially similar with Claim 13 reciting the well-known limitations of a local data bus and memory on top of the limitations of Claim 1. Claim 1 is representative:

1. **[i.pre]** A security processor to process incoming packets and outgoing packets, the security processor comprising:

[ii.] a switching system to send the outgoing packets and receive the incoming packets;

[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,

[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

[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;

[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,

[vii.] wherein the packet engine is interposed between the switching system and the cryptographic core;

[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.

B. Prosecution History

During prosecution of the '436 Patent, the examiner issued several 102 and 103 rejections resulting in a final rejection of all claims based on combinations

relying on Narad (U.S. Patent No. U.S. 6,157,955) as a primary reference, (EX-1002 FOA pp. 45-58) and allowed the claims only after entering an examiner's amendment, which further amended the independent claims to add limitations previously recited in dependent claims 6. EX-1002 Examiner's Amendment pp.16-23.

Previous claim 6 recited:

6. (Amended) The security processor of claim [[4]] 1 wherein the incoming and outgoing packets are provided with a tag upon ingress to one of the plurality of packet engines and the tag determines the egress path within the security processor upon exit from the corresponding one of the plurality of cryptographic cores.

EX-1002 After Final Amendment pp. 35-41.

Prior to the filing of the RCE, the Examiner found this limitation was disclosed by Krishna.

Applicant argued that "Also specifically with respect to claim 6, applicant draws the Examiner's attention to the fact that the cited references in the office action do not mention, the claimed 'tags'". In reply the examiner submits that Krishna et al discloses the claimed tag (The result of packet classification is a classification tag. This structure holds IPSec security association data and per-flow statistics)(paragraphs [0068],[0074], [0075]).

EX-1002 After Final Amendment pp. 35-41

The amendments to claim 1 are representative:

1. (Currently Amended) A security processor to process incoming packets and outgoing packets, the security processor comprising: a switching system to send the outgoing packets and receive the incoming packets;

a packet engine, coupled to the switching system, to handle classification processing for the incoming packets received by the packet engine from the switching system and the outgoing packets sent by the packet engine to the switching system, wherein the packet engine is one of a plurality of packet engines and substantially all of the incoming packets and outgoing packets to the security processor transit one of the plurality of packet engines, and wherein the incoming packets and outgoing packets are provided with a tag upon ingress to one of the plurality of packet engines and the tag determines an egress path within the security processor upon exit from a corresponding cryptographic core;

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

a signature database; and

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

EX-1002 Examiner's Amendment pp.16-23.

In the Notice of Allowance, the examiner's stated reason for allowances was simply a recitation of the claim terms and otherwise unremarkable. EX-1002 Examiner's Amendment pp.16-23.

C. Claim Construction

Petitioner proposes that each claim term in the Challenged Claims be given its plain and ordinary meaning in this proceeding, and that no specific construction of any claim term is required because the prior art relied on in this Petition meets each of the claim terms under any reasonable construction.

D. Priority Date of the Challenged Claims

The application that issued as the '436 Patent was filed July 30, 2004 claiming priority to Provisional application No. 60/507,976 filed on October. 2, 2003. For the purposes of this IPR, Petitioner assumes the earliest effective filing date is that of the provisional, October 2, 2003.

E. Person of Ordinary Skill in the Art

With respect to the '436 Patent, a POSA would have a Bachelor's degree in computer science, computer engineering, or a related discipline, and 3-4 years of experience in computer networking with an emphasis on packet processing systems including traffic monitoring, inspection, and encryption/decryption

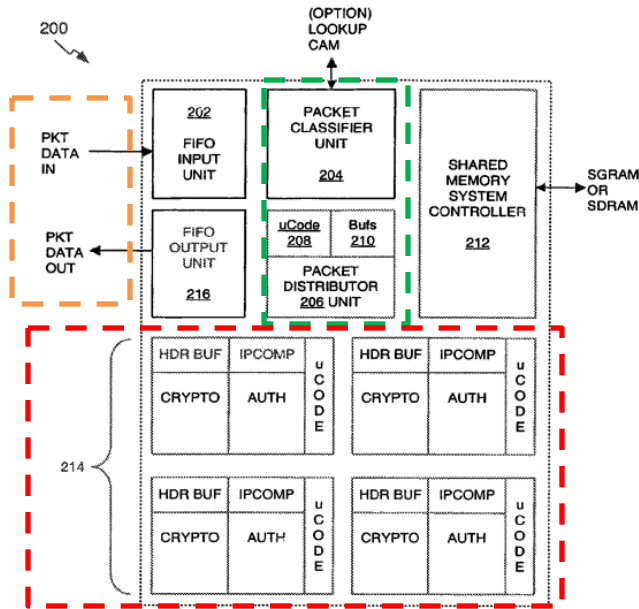
systems. More experience could compensate for less formal education and vice versa. EX-1003 ¶ 50.

F. State of the Art

The following section describes the state of the art for packet processing systems as of October 2003. EX-1003 ¶ 51. The prior art references, and the discussions of what was known to a POSA, provide the factual support for the general description of the state of the art at the time of the invention, provide additional motivation to modify or combine the references. Accordingly, these references should be considered by the Board.

1. The use of packet engines and cryptographic cores

By October 2003, the use of packet engines for handling encrypted packets was well-known. In one such system (Krishna), a packet engine (green) received packets from a switching system (orange) and provided them to a cryptographic core(red).



EX-1006 Fig 2; EX-1003 ¶ 52.

The packet engine included a packet classifier unit and a packet distributor. Packet header information from packets received from the switching system is sent to a packet classifier unit 204 where a classification engine rapidly determines security association (SA) information required for processing the packet, such as encryption keys, data, etc. The classification engine performs lookups from databases stored in associated memory and the security association information determined by the packet classifier unit 204 is sent to a packet distributor unit 206. EX-1006, 5:37-53. Packet classification and use of SA information in the Krishna system is the same as described in the '436 Patent, as discussed with respect to the prosecution history above. Krishna describes that the function of the packet classifier is to perform IPSec-specified lookup as well as IP packet fragmentation

lookup. These lookups are used by the distributor engine. EX-1006, 9:33-50; EX-1003 ¶ 53. “The distributor unit 206 determines if a packet is ready for IPSec processing, and if so, distributes the security association information (SA) received from the packet classifier unit 204 and the packet data among a plurality of cryptography processing engines 124, in this case four, on the chip 200, for security processing.” EX-1006, 5:54-60; EX-1003 ¶ 53.

Moreover, by October 2003, a POSA understood that cryptographic processing was moving away from discrete processors and was being implemented on a single chip. EX-1010, Fig. 1, Abstract; EX-1003 ¶ 54.

2. The use of intrusion and detection systems

By October 2003, the use of intrusion detection systems were well-known. In one such system, U.S. 6,279,113 (“Vaidya”), a signature based dynamic network intrusion detection system (IDS) includes attack signature profiles which are descriptive of characteristics of known network security violations. The attack signature profiles are organized into sets of attack signature profiles according to security requirements of network objects on a network. Each network object is assigned a set of attack signature profiles which is stored in a signature profile memory together with association data indicative of which sets of attack signature profiles correspond to which network objects. A monitoring device monitors network traffic for data addressed to the network objects. Upon detecting a data

packet addressed to one of the network objects, packet information is extracted from the data packet. The extracted information is utilized to obtain a set of attack signature profiles corresponding to the network object based on the association data. A processor executes instructions associated with attack signature profiles to determine if the packet is associated with a known network security violation. An attack signature profile generator is utilized to generate additional attack signature profiles configured for processing by the virtual processor in the absence of any corresponding modification of the processor. EX-1007 Abstract, 2:35-40 ; EX-1003 ¶ 55.

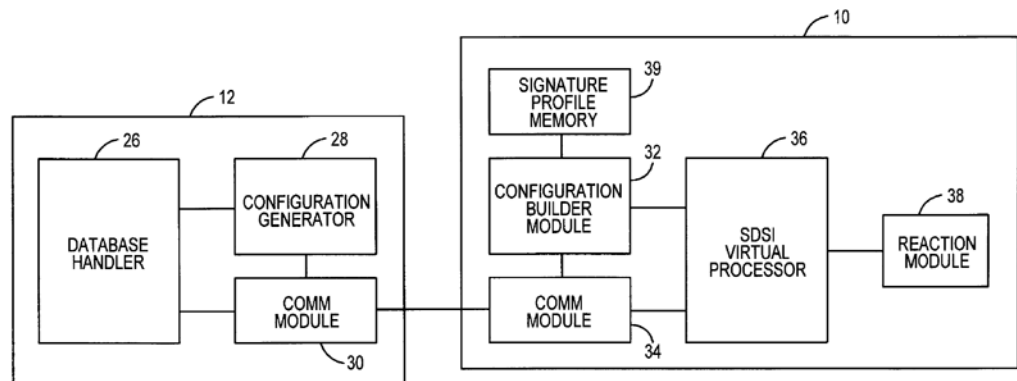


FIG. 2

EX-1007 Fig. 2; EX-1003 ¶ 55.

It was also well known to locate IDS systems at various locations in the networks, but in particular proximate the ingress of the network to facilitate detection prior to deeper intrusion by a malicious packet. EX-1007 5-26; EX-1003 ¶ 56. It was well known that, encryption turns malicious traffic indistinguishable from non-harmful traffic, thus the monitoring taps of the IDS are preferably placed at the endpoints where encryption and decryption are performed such that it can inspect unencrypted traffic (“the IDS function in servers 720, 740 has access to clear text data so that IDS evaluation can occur.” EX-1015 [0079]). EX-1015 [0012, 0079]; EX-1003 ¶¶ 56, 57, 58.

It was also well understood by a POSA that creating a signature database that allowed for signature matching of encrypted data was impractical given the vast number of possible combinations of bytes. EX-1003 ¶ 59.

VI. IDENTIFICATION OF CHALLENGES

A. Challenged Claims

Claims 1-4, 7-14, 16, 17, 21 and 22 of the '436 Patent are challenged in this Petition.

B. Statutory Grounds for Challenges

The Challenges are set forth in detail below and summarized as follows:

Ground	Claims	Basis	Reference
1	Claims 1-2, 9-13, 16 and, 22,	§ 103	Pham in view of Wu
2	3, 14, 21	§ 103	Pham in view of Wu and Collins

Petition for *Inter Partes* Review of U. S. Patent No. 7,685,436

3	4, 7, 8	§ 103	Pham in view of Wu and Collins and Krishna
4	17	§ 103	Pham in view of Wu and Krishna

C. Prior Art Basis

U.S. Patent Publication 2003/0074473 titled “SCALABLE NETWORK GATEWAY PROCESSOR ARCHITECTURE” published on April 17, 2003 from application No. 09/976, 322, filed October 12, 2001 (“Pham”) (EX-1004). Pham qualifies as prior art under at least §102(a) and (e). It was not cited or applied by the examiner during the ’436 Patent prosecution.

U.S. Patent No. 7,424,744 titled “SIGNATURE BASED NETWORK INTRUSION DETECTION SYSTEM AND METHOD” issued September 9, 2008 from application No. 10/992,179 filed March 5, 2002 (“Wu”)(EX-1005). Wu qualifies as prior art under §102(e). It was not cited or applied by the examiner during the prosecution of the ’436 Patent.

U.S. Patent Publication 2002/0073316A1 titled “CRYPTOGRAPHIC SYSTEM ENABLING OWNERSHIP OF A SECURE PROCESS” published on June 13, 2002 from application No. 09/949,323 filed September 7, 2001 (“Collins”)(EX-1008). Collins qualifies as prior art under at least § 102(a), (b) and (e). It was not cited or applied by the examiner during the prosecution of the ’436 Patent.

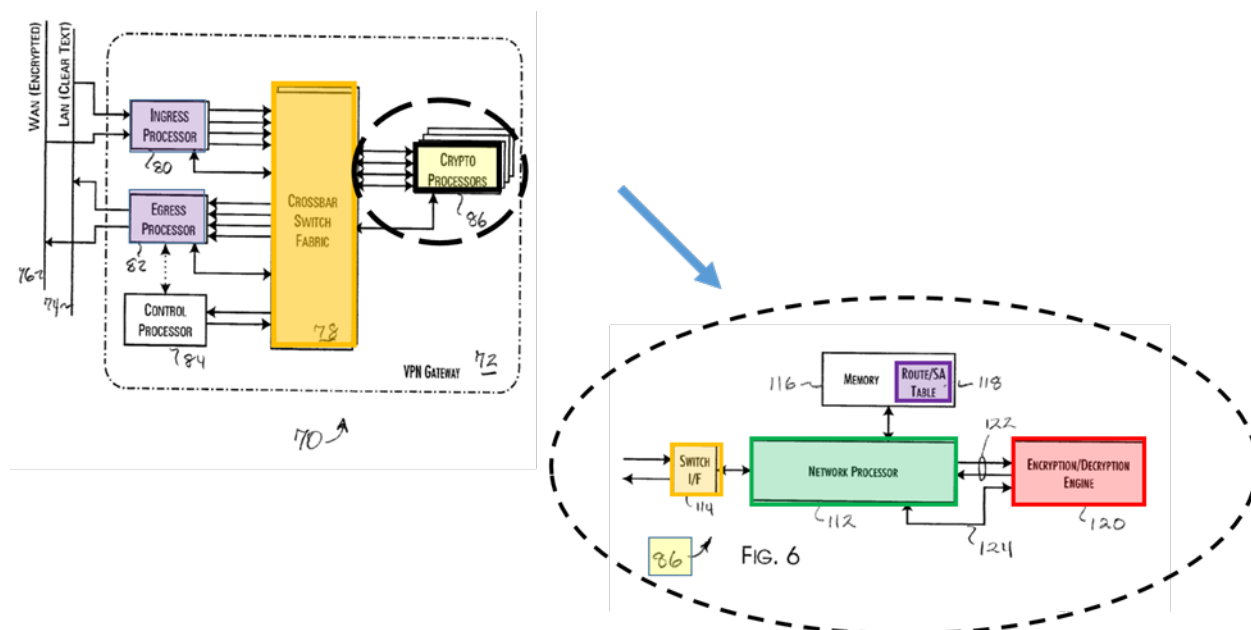
U.S. Patent No. 7,996,670 titled “CLASSIFICATION ENGINE IN A CRYPTOGRAPHY ACCELERATION CHIP” issued August 9, 2011 from application No. 09/610,722 filed July 6, 2000. (“Krishna”)(EX-1006). Krishna qualifies as prior art under §102(e). It was cited by the examiner during the prosecution of the ’436 Patent but not in combination with Pham and Wu.

VII. IDENTIFICATION OF HOW THE CHALLENGED CLAIMS ARE UNPATENTABLE

A. Ground 1: Claims 1, 2, 9-13, 16 and 22 are unpatentable over Pham in view of Wu.

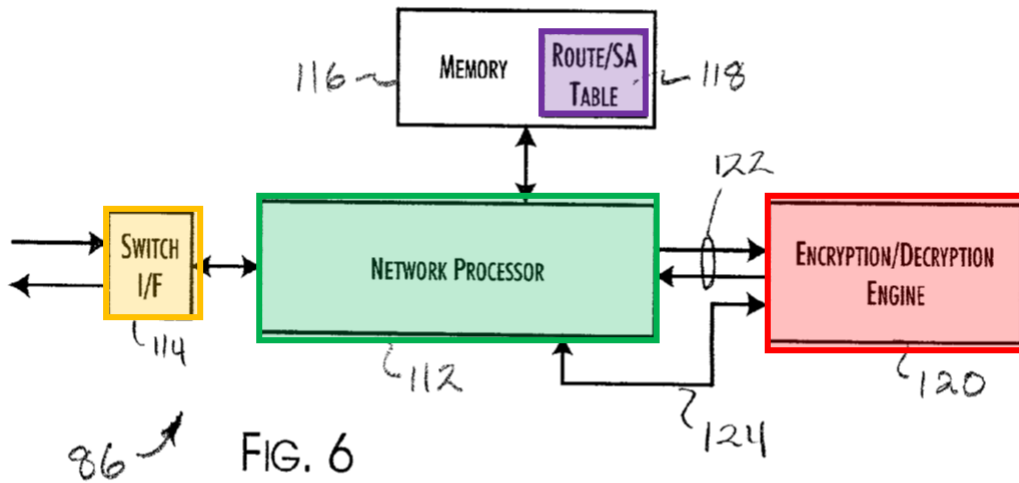
1. The Pham Reference

Pham is directed to a network data processor system in the form of a virtual private network gateway that includes a plurality of data packet processors in the form of crypto processors (yellow) coupled through a data switch fabric (orange) between network connection processors (purple). Ex-1004 Abstract; EX-1003 ¶ 62.



EX-1004 Figs. 4 and 6; EX-1003 ¶¶ 62, 63.

The crypto processors each include a data processing engine configured to perform a data processing function over data contained within predetermined data packets and to perform hardware encryption and decryption algorithms called for by the IPsec protocol. EX-1004 Abstract; EX-1003 ¶ 63. Figure 6 illustrates one embodiment of a crypto processor that corresponds to the security processing system described in the '436 Patent:



EX-1004 Fig. 6 ;EX-1003 ¶ 63.

The network processor 112 (green) connects to and supports high-speed data interchange with a dedicated encryption/decryption engine 120 (red). The network processor 112 controls and monitors the engine 120. EX-1004 [0052]; EX-1003 ¶ 64. A memory array 116 is provided for the external memory and program requirements of the network processor and provides storage space for various secure authority (SA) parameters for the encryption and decryption of data, and a SA parameter data table 118 (purple). EX-1004 [0051]; EX-1003 ¶ 64.

In one embodiment, the SA parameter association task is performed by the crypto processors 86. The control processor 84 explicitly propagates identical copies of the SA parameter data to each of the crypto processors 86, enabling the

crypto processors 86 to process any data packet received.” EX-1004 [0051]; EX-1003 ¶ 65.

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. The network processor 112 controls and monitors the encryption/decryption engine 120 via control and status lines 124. EX-1004 [0052]; EX-1003 ¶ 66.

2. The Wu Reference

Wu discloses a signature based instruction detection system that stores signature profiles identifying patterns associated with network intrusions in a signature database and generates classification rules based on the signature profiles. Data packets transmitted on the network and having corresponding classification rules are classified according to generated classification rules. Classified packets are forwarded to a signature engine for comparison with signature profiles. EX-1005 2:39-49 ;EX-1003 ¶ 67. Any problems detected are sent to an alert log 68 and appropriate action is taken. EX-1005 1-3; EX-1003 ¶ 67.

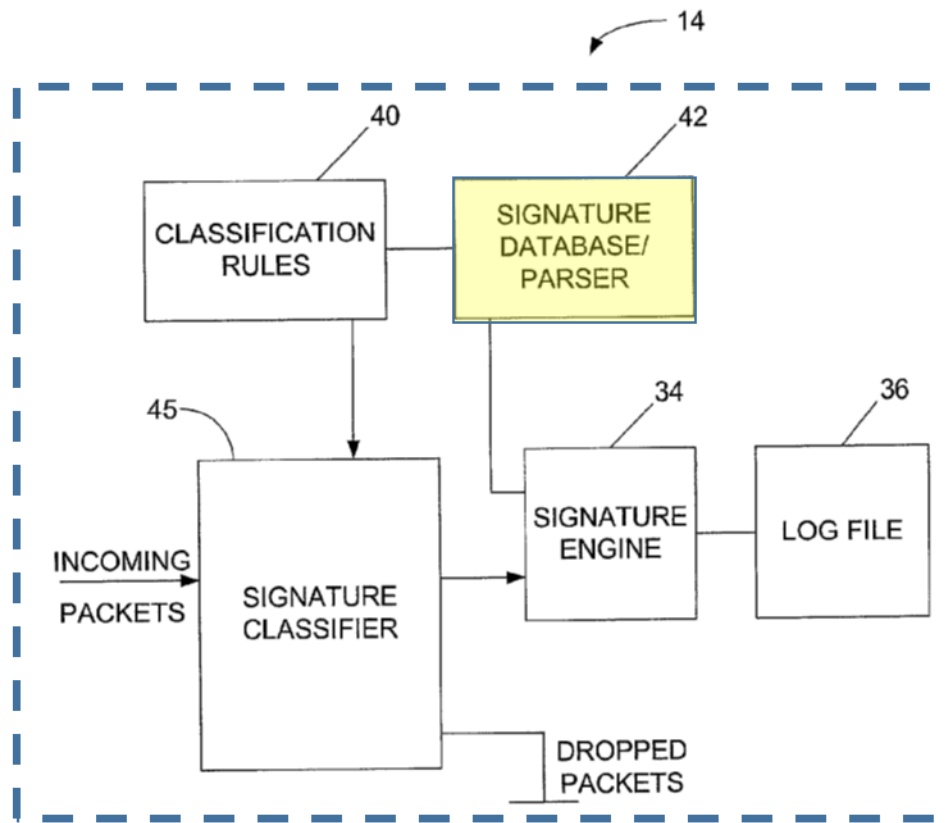


FIG. 1

EX-1005 Fig. 1; EX-1003 ¶ 67.

The system includes a signature engine 34, classification rules database 40, signature database/parser 42 (yellow), log file 36 and signature classifier 45. The signature classifier 45 filters out incoming packet streams in accordance with classification rules generated from the signature database 42. Only packets matched with the classification rules move to the signature engine 34, while no further processing is performed on the rest of packets.

The workload of the signature engine 34 is thus reduced. EX-1005 3:52-4:3; EX-1003 ¶ 68. Signatures (or patterns) of all known attacks are described in an abstract form and included within the signature database 42. EX-1005 4:4-7; EX-1003 ¶ 68.

Wu discloses that the network intrusion detection system “may be placed at key points throughout the network” and “may be used on different types of networks and placed in various locations throughout the network.” EX-1005 4:46-47; 4:66-67, EX-1015 [0012, 0079]; EX-1003 ¶ 69. A POSA understood, as discussed in the state of the art, IDS systems may be placed at various locations, but require inspection of unencrypted traffic (packets), thus any placement would be predicated on access to unencrypted data (clear text) near and preferable towards the endpoint of the local network. EX-1015 [0012, 0079]; EX-1003 ¶ 69.

3. The Motivation To Combine the Teachings of Pham with the Teachings of Wu with a Reasonable Prediction of Success

The '436 Patent, Pham and Wu are analogous art, all directed to network protection, operating at the packet level to ensure transported data to the network is secure and not malicious. Wu describes that as Internet access costs have decreased, corporations are increasingly using the Internet for corporate data and communications with external networks. EX-1005 1:8-13; EX-1003 ¶ 70. It

identifies that network security is increasingly becoming a critical issue in enterprise and service-provider networks as usage of public networks for data transport increases and new business applications such as e-commerce sites are deployed. Security measures are required, for example, to prevent hackers from gaining unauthorized access to a corporation's information resources or shutting down an e-commerce web site via a distributed denial of service attack. EX-1005 1:13-22; EX-1003 ¶ 70. Wu describes that corporations continue to deploy firewalls to prevent unauthorized users from entering their networks, but are looking for additional security technologies to protect their system's vulnerability that firewalls alone cannot address. EX-1005 1:22-26; EX-1003 ¶ 70.

Wu describes that one of these additional security measures is an intrusion detection system (IDS). Wu describes that as network attacks have increased in number and severity, intrusion detection systems have become a necessary addition to the security infrastructure of most organizations. Intrusion detection allows organizations to protect their systems from threats that come with increasing network connectivity and reliance on information systems. Intrusion detection systems include software or hardware systems that automate the process of monitoring events occurring in a computer system or network, and analyzing them for signs of security problems. Wu explains that because intruders attempt to compromise the confidentiality, integrity, availability, or to bypass the security

mechanisms of a computer or network, intrusion detection technology has become a necessary addition to every large organization's computer network security infrastructure. EX-1005 1:27-45; EX-1003 ¶ 71.

Pham also recognizes the challenges presented by the growth of the Internet and proliferation of private distributed intranets, and specifically identifies increasing the speed, security, and transactional reliability of network data transmissions as a fundamental concern and continuing consideration in the development of new network infrastructure. EX-1004 [0005]; EX-1003 ¶ 72.

Pham is directed to a virtual private network gateway having data packet processors for processing packets coming from external data networks. EX-1004 Abstract. Pham specifically identifies that its technology is useful for the type of corporate intranet environments that connect to the Internet that are identified by Wu. EX-1004 [0008]; EX-1003 ¶ 72.

A POSA would be motivated to modify the teachings of Pham to include the teachings of Wu to include an intrusion detection system to achieve the advantages expressly described above by Wu for increasing security of the network protected by Pham's gateway. Wu describes that a "signature based intrusion detection system 14 may be used alone or in combination with a data monitoring and analysis device configured to perform fault and network performance management." EX-1005 4:4-7; EX-1003 ¶ 73. In one embodiment, Wu describes

that application program interfaces (APIs) can be used to open applications of the network analysis device 16. EX-1005 4:26-27; EX-1003 ¶ 73.

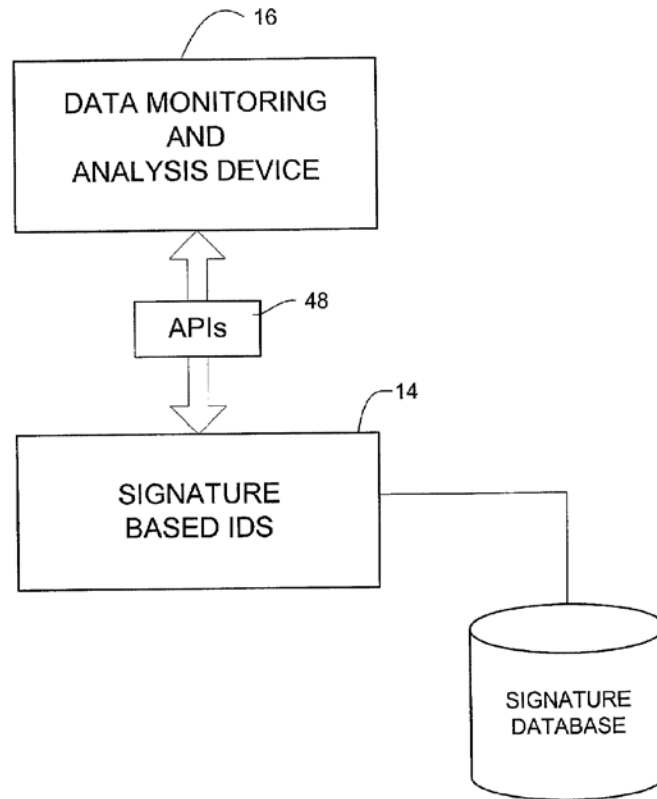


FIG. 2

EX-1005 Fig. 2; EX-1003 ¶ 73.

The APIs are used to parse, generate and load signatures, invoke corresponding signature detection methods from appropriate protocol contexts, access states required for stateful intrusion detection, and access alerts/alarms management facilities. Wu also teaches in another embodiment that the signature based intrusion detection system 14 may be used without the network analysis

device 16, and instead perform the function of device 16, such as packet decoding.

EX-1005 4:28-38; EX-1003 ¶ 74.

Pham describes that the network processor 112 connects to and supports high-speed data interchange of incoming and outgoing packets with a dedicated encryption/decryption engine controls and monitors the engine encryption/decryption 120. EX-1004 [0052]; EX-1003 ¶ 75. A memory 116 is provides for the external memory and program requirements of the network processor. EX-1004 [0051]; EX-1003 ¶ 75. A POSA understood that to implement the teachings of Wu with Pham, the IDS would be coupled between the network processor 112 and the cryptographic core because Wu expressly discloses that network intrusion detection system may be “placed in various locations throughout the network” (EX-1005 4:65-67), and “may be used alone or in combination with a data monitoring and analysis device configured to perform fault and network performance management.” EX-1005 4:4-7; EX-1003 ¶ 75. Placing the intrusion system inline with the network processor of Pham is advantageous because it allows actions to be taken on packets that match a signature in the signature database before the packet is accepted into a network or sent to a network. Importantly as discussed in the state of the art, IDS systems such as Wu must necessarily be placed where it can inspect unencrypted traffic (packets), thus placement between the encryption engine and the network

processor would have allowed access to unencrypted data (clear text) near and endpoint of the local network. EX-1015 [0012, 0079]; EX-1003 75. As noted in Wu, the IDS is configured to analyze packets flowing through a network that may be overlooked by the firewall's simplistic filtering rules. EX-1005 1:50-54; EX-1003 ¶ 75. For incoming encrypted packets, a tap location between the Pham's network processor 112 and encryption/decryption engine 120 is the first instance a clear text packet may be analyzed, conversely for outgoing packets that will be encrypted, the tap location between the network processor 112 and the encryption/decryption engine 120 is the last opportunity to analyze the packets prior to encryption and transmission out of the LAN. EX-1004 Fig. 6; EX-1003 75.

Further, external memory 116 of Pham is described as including a data table to store and share other information between the crypto processors and, generically, data processors. EX-1004 [0053]; EX-1003 ¶ 75. Thus, a POSA understood that the signature database could be included in memory 188, as contemplated by Pham, or as a standalone database. EX-1003 ¶ 75.

In view of the above, a POSA would be motivated to combine the teachings of Pham with Wu, with a reasonable expectation of success because:

- i. Wu expressly provided the teaching, suggestion, and motivation that “intrusion detection technology has become, a necessary addition to every large

organization's computer network security infrastructure” and would have led a POSA to modify Pham’s network data processor with an intrusion detection system with a signature database before allowing a data packet to enter the internal network to increase security and achieve the benefits expressed described by Wu.

ii. The general knowledge in the art that the use of intrusion detection systems and signature databases to protect internal networks from external threats was an accepted, known and predictable mechanism to increase the security of Pham’s network processor.

iii. Wu’s known technique of using APIs in conjunction with a network processor to implement the intrusion detection system would readily improve the security of the network processor taught by Pham with predictable results; and,

iv. The location between the network processor and the encryption/decryption engine allows the IDS access to the unencrypted packet at a point near the endpoint at the first possible point after decryption thus allowing the earliest indication of an incoming threat and allows action to be taken before a malicious packet is received into the network. Similarly, this location allows the IDS access to the unencrypted packet at a point near the endpoint at the last possible point prior to encryption thus allowing action to be taken before a malicious packet is sent into to another network. EX-1003 ¶ 76.

4. Detailed Application of Pham and Wu

a. Claim 1

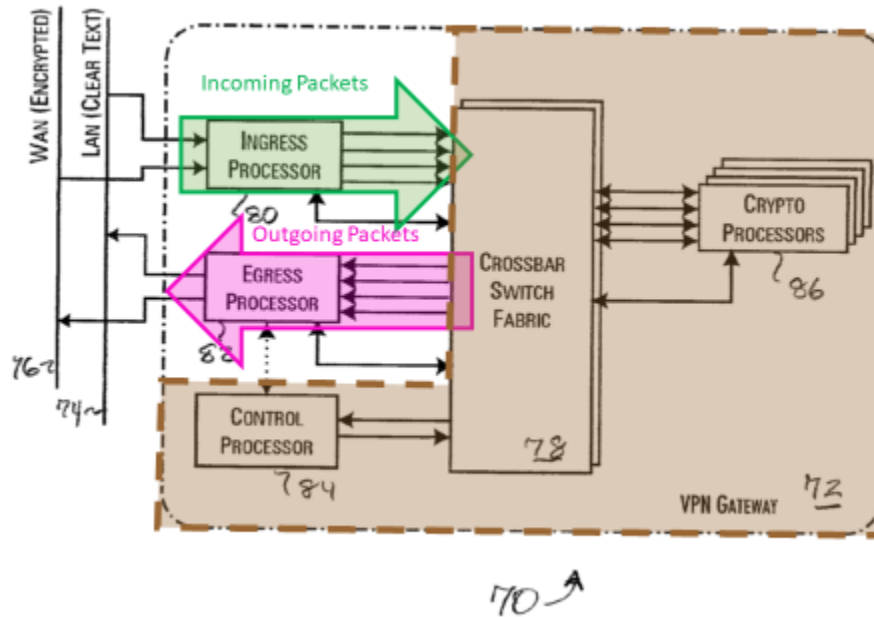
- i. [pre] A security processor to process incoming packets and outgoing packets, the security processor comprising:*

To the extent the preamble is limiting, Pham discloses a security processor for ingress and egress processing of packets (*process incoming packets and outgoing packets*).

A VPN gateway 72 provides a single physical LAN 74 connection supporting multiple logical connections over a local clear text network and a single physical WAN 76 connection, extending encrypted network connections over the Internet. The VPN gateway 72 utilizes IBM Packet Routing Switches PRS28.4G (IBM Part Number IBM3221L0572), available from IBM Corporation, Armonk, N.Y., as the basis for a central crossbar switch fabric 78 interconnecting an ingress processor 80, an egress processor 82, a control processor 84 and an array of two to sixteen crypto processors 86.

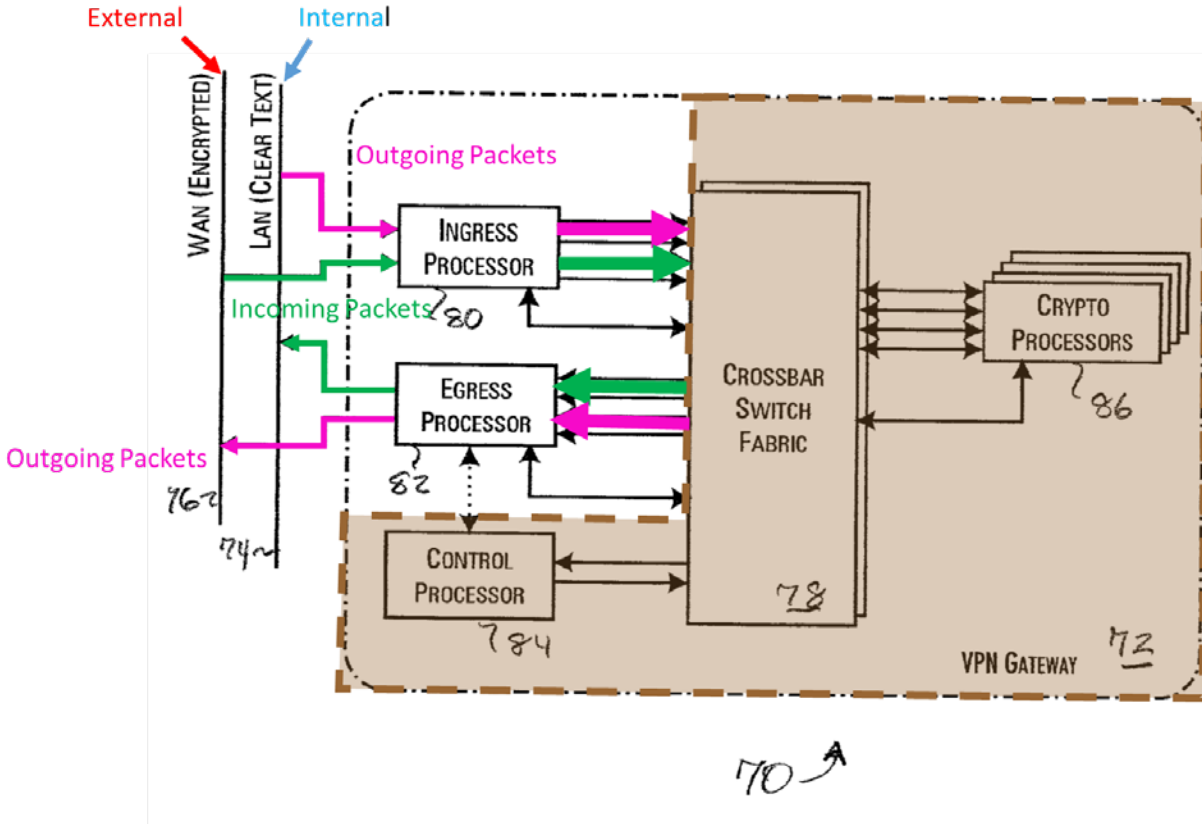
EX-1004 [0045]; EX-1003 ¶ 77.

In Pham, as shown in annotated Fig. 4, the security processor (**brown**) processes incoming packets (**green**) and outgoing packets (**pink**).



EX-1004 Fig. 4; EX-1003 ¶ 78.

Alternatively, to the extent PO argues the incoming/outgoing packet distinction is with respect to the internal/external network perspective, the incoming packets may be the encrypted packets received from the external network (i.e. the WAN 76) and the outgoing packets may be the clear text packets received from the internal network (i.e. the LAN 74). EX-1003 ¶ 79.



EX-1004 Fig. 4; EX-1003 ¶ 79.

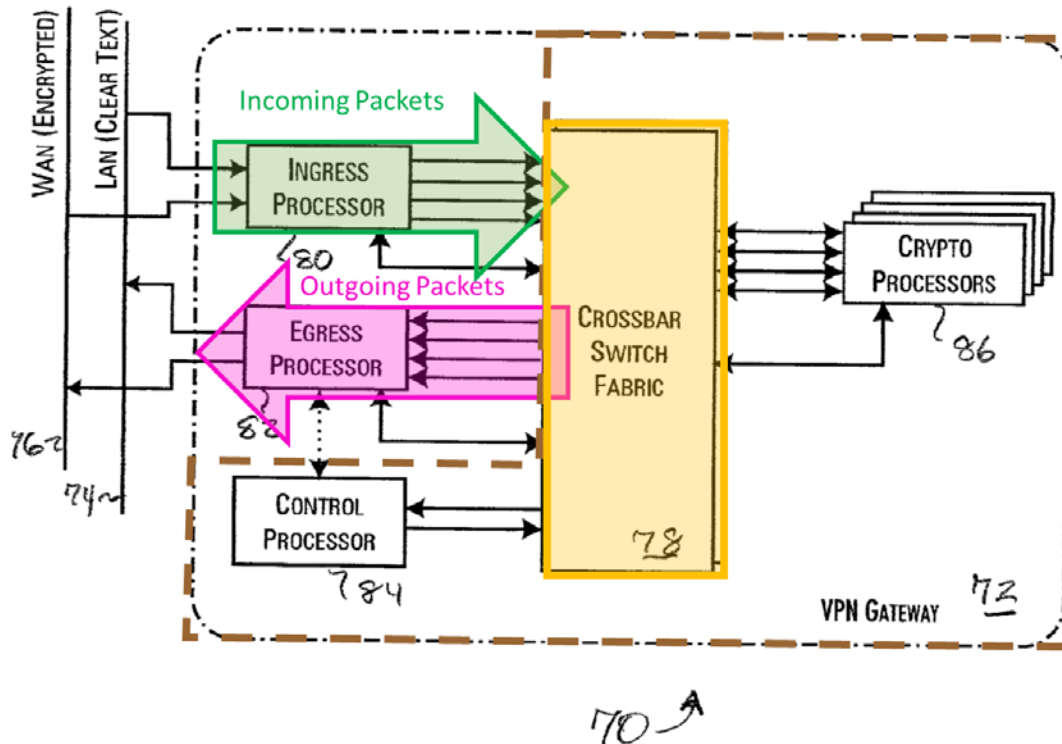
ii. a switching system to send the outgoing packets and receive the incoming packets;

Pham discloses a switch fabric 78 (*switching system*) to send the egress packets (*outgoing packets*) and received in ingress packets (*incoming packets*).

Thus, for 4 Gbps network 74, 76 connections, each ingress processor 80 implements at least three port connections to the switch fabric 78. Likewise, each egress processor 82 receives at least three output port connections to the switch fabric 78.

EX-1004 [0047]; EX-1003 ¶ 80.

As shown in Fig 4. The switch fabric 78 (orange) sends outgoing packets (pink) and receives incoming packets (green).



EX-1004 Fig. 4; EX-1003 ¶ 81.

Pham discloses that the switch fabric is made up of conventional packet routing switches (EX-1004 [0045]), which is consistent with the disclosure of the '436 Patent that the switching system 208 is known in the art and can be implemented using conventional switches. EX-1001 7:33-48; EX-1003 ¶ 82.

- 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*

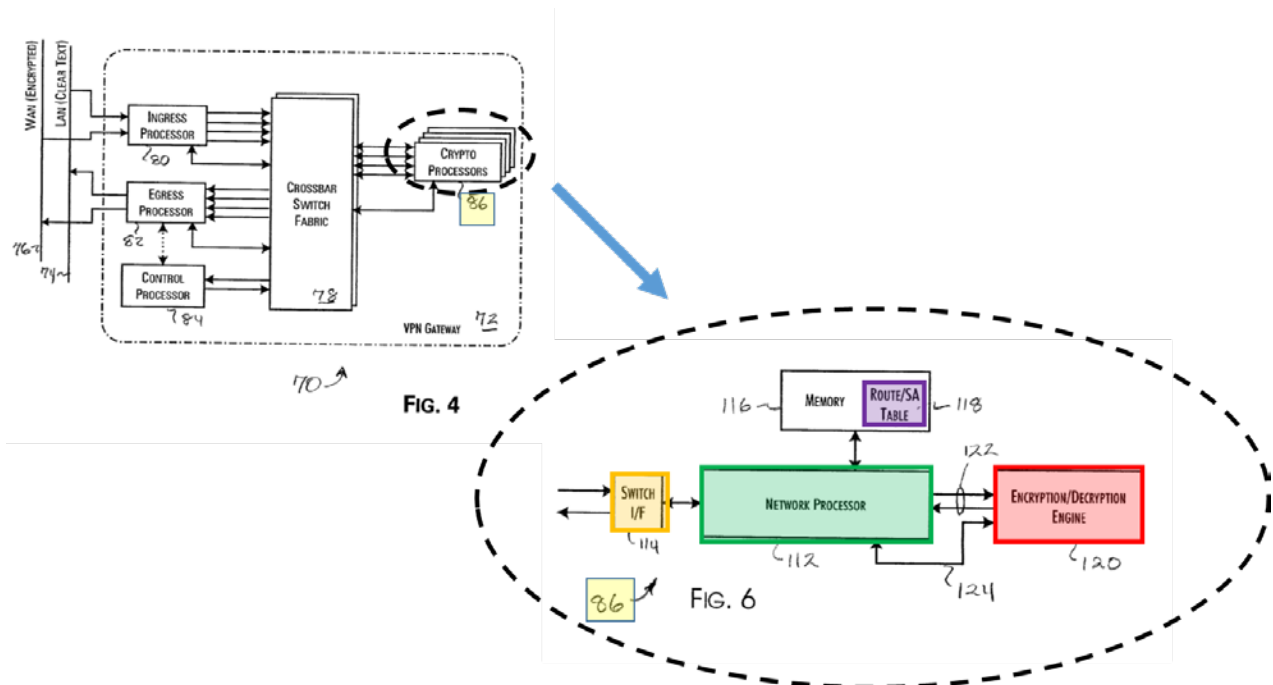
packets sent by the packet engine to the switching system,

Pham discloses an implementation of a crypto processor 86 which includes a network processor 112 (*packet engine*) coupled to the switch fabric 78 (switching system).

The preferred implementation of a crypto processor 86 is shown in.

FIG. 6.

EX-1004 [0051]; EX-1003 ¶ 83.



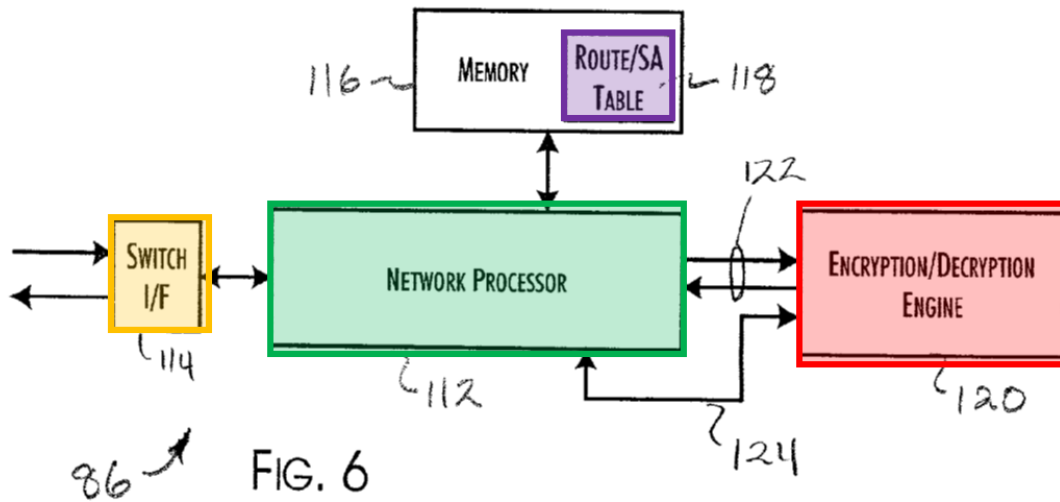
EX-1004 Figs. 4 and 6; EX-1003 ¶ 83.

Pham discloses the network processor 112 (*packet engine*) processes the incoming packets received from the switch fabric (*switching system*) and the outgoing packets sent to the switch fabric (*switching system*). The

network processor includes the association of secure authority (SA) parameters task (*classification processing*). The SA parameter data from table 118 is used to dynamically create and attach SA headers to each received IPsec data packet to allow for IPsec protocol processing by encryption/decryption engine 120. EX-1004 [0049]-[0051]; EX-1003 ¶ 84.

Pham's description of classification processing is consistent with the '436 Patent's disclosure that packet classification generally involves matching information from an incoming packet to a table of connection entries (which may include state and context elements, and relations to encryption associations) stored in, for example, memory 106 or 108. EX-1001, 5:23-35; EX-1003 ¶ 85

As shown in Fig. 6, the network processor 112 (**green**) is connected to the switching fabric 78 via the switch fabric interface 114 (**orange**) (the interface 114 may be considered part of the switching fabric 78) and processes the incoming and outgoing packets (green and pink) for association with the SA parameters stored in the memory 116/ SA parameter data table 118 (**purple**). An encryption/decryption engine 120 (**red**) is connected to the network processor.



EX-1004 Fig. 6; EX-1003 ¶ 86.

Pham describes that the network processor 112 can be a commercially available processor including a switch fabric interface 114, *e.g.*, IBM PowerNP NP4GS3 Network Processor. EX-1004 [0049], [0051]; EX-1003 ¶ 87. Pham's disclosure of a conventional network processor is consistent with the '436 Patent's disclosure that suitable packet engines are known in the art, process packets needing network address translation processing and firewall table processing, and process IPSec packets. Ex-1001 9:60-10:8; EX-1003 ¶ 87.

- 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*

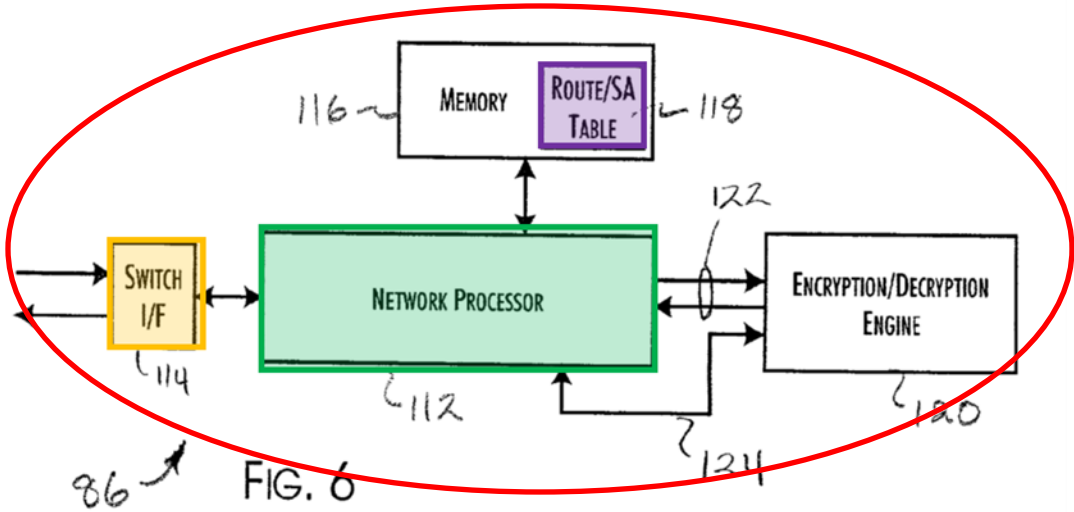
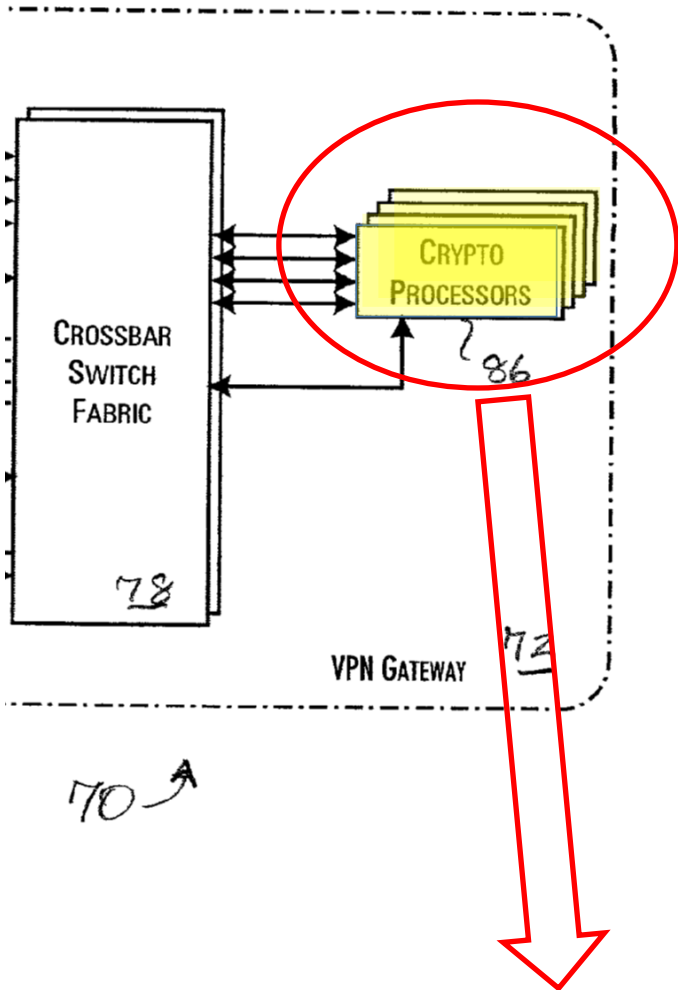
Pham discloses multiple crypto processors 86 which each include a respective network processor (*packet engines*).

The VPN gateway 72 utilizes IBM Packet Routing Switches PRS28.4G (IBM Part Number IBM3221L0572), available from IBM Corporation, Armonk, N.Y., as the basis for a central crossbar switch fabric 78 interconnecting an ingress processor 80, an egress processor 82, a control processor 84 and an array of two to sixteen crypto processors 86.”

EX-1004 [0045]; EX-1003 ¶ 88.

The preferred implementation of a crypto processor 86 is shown in FIG. 6.

EX-1004 [0051]; EX-1003 ¶ 88.



EX-1004 Figs. 4 and 6; EX-1003 ¶ 88.

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

Further, as discussed below, when the intrusion detection system is interposed in line with the network processor between the network processor and the cryptographic core, all incoming and outgoing packets would be sent through the intrusion detection system, via the network processor to ensure that malicious packets can be identified before being sent into or from the network. EX-1003 ¶ 90.

- 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;

Pham discloses the incoming packets and outgoing packets are provided with SA header information and an IP tunneling header (*tag*) upon ingress to one of the plurality of network processors (*packet engines*). Pham also discloses the SA header including the IP tunneling header (*tag*) determines the egress path within the security processor to an appropriate egress processor upon exit from the encryption/decryption engine 120 (*cryptographic core*). EX-1004 [0051, 0071 and 0072];EX-1003 ¶ 92.

Pham, with respect to one embodiment, discloses adding an IP tunneling header to the packet at the ingress processor using the routing and SA parameter table:

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.

EX-1004 [0071]; EX-1003 ¶ 93.

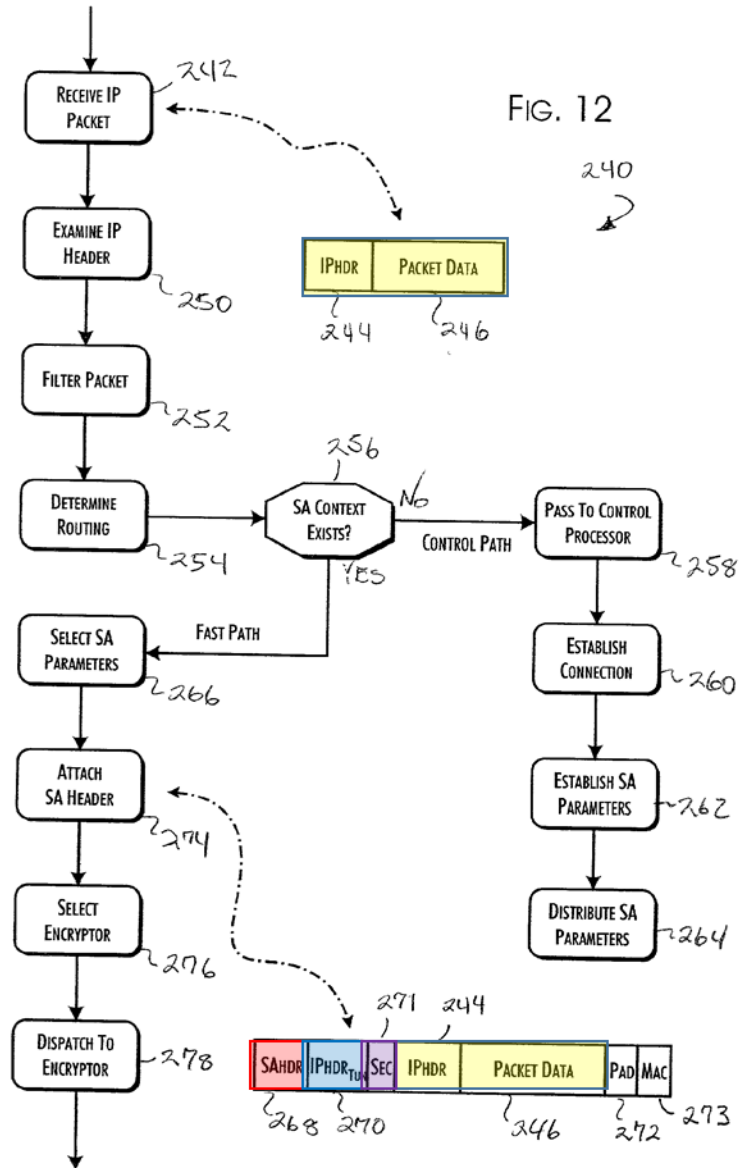
Figure 12 of Pham illustrates the use of the routing and SA table (102) used by the ingress processor (Figure 5) upon receipt of a clear text packet. However, Pham discloses that in an alternative embodiment, the routing and SA table 118 of

the crypto processor can be used (Fig. 6) in the network processor 112 and associated memory 116 with route/SA 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. The control processor 84 explicitly propagates identical copies of the SA parameter data to each of the crypto processors 86, enabling the crypto processors 86 to process any data packet received. EX-1004 [0051]; EX-1003 ¶ 94.

Thus, Figure 12 applies equally to a clear text data packet received at network processor 112 using routing and SA table 118, and discloses the creation and attachment of the headers to each data packet by network processor 112 in a crypto processors 86 for each packet received (*upon ingress to one of the plurality of packet engines*) rather than by the ingress processors. EX-1003 ¶ 95.

The headers added to the ingress packet (yellow) as disclosed in Pham include at least the SA header (red) and tunneling IP header (blue) and the IPsec control fields (purple), i.e. SAHDR (268) IPHDR_{TUN} (270) and SEC (271). EX-1004 [0072], Figs. 12, 13; EX-1003 ¶ 96.



EX-1004 Fig. 12; EX-1003 ¶ 96.

Pham discloses the SA Header includes a tunneling IP header 270 (*tag*) that determines an egress path within the security processor upon exit from a corresponding encryption/decryption engine 120 (*cryptographic core*).

The selection of an appropriate egress processor 82, where multiple egress processors 82 are present, is determined by the crypto

processor 86 from the route identification information contained in the tunneling IP header 270.

EX-1004 [0072]; EX-1003 ¶ 97.

The tunneling IP header disclosed in Pham corresponds to the identification of the IPsec tunnels described in the '436 Patent. Similarly the routing and SA parameter table of Pham corresponds with the connection flow table and security policy/association data" of the '436 Patent. EX-1001, 5:7-14, 20:21-26; EX-1003 ¶ 98.

- 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,*

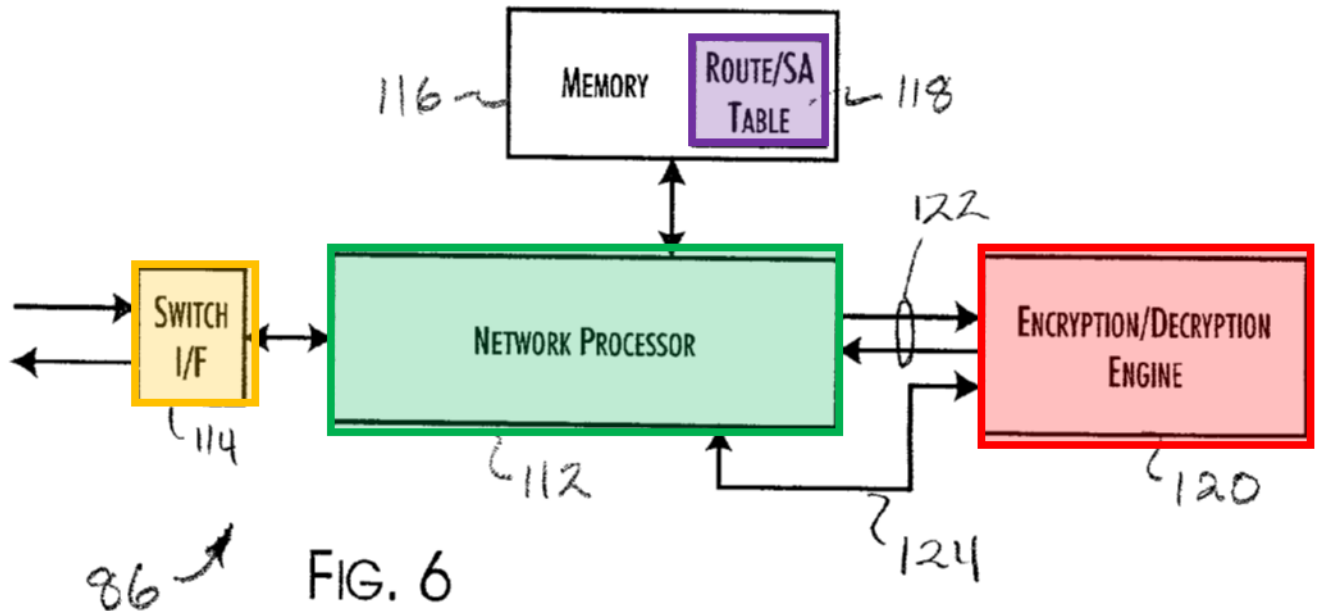
Pham discloses the crypto processor 86 includes an encryption/decryption engine 120 (*cryptographic core*) coupled to the network processor 112 (*packet engine*) which receives incoming packets from the switch fabric 78 (*switching system*) via the network processor 112 and communicating the outgoing packets to the switch fabric 78 via the network processor 112, and provides encryption and decryption processing of packets received from and sent to the network processor.

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. The network processor 112 controls and monitors the engine 120 via control and status lines 124. Preferably, the engine 120 is a BCM5840 Gigabit Security Processor, available from Broadcom Corporation, Irvine, Calif. The BCM5840 processor implements a highly integrated symmetric cryptography engine providing hardware support for IPsec encryption and decryption operations. Utilizing the BCM5840, each crypto processor 86 is capable of a minimum sustained effective IPsec encryption/decryption and IPsec authentication rate of 2.4 Gbps.

EX-1004 [0052]; EX-1003 ¶ 99.

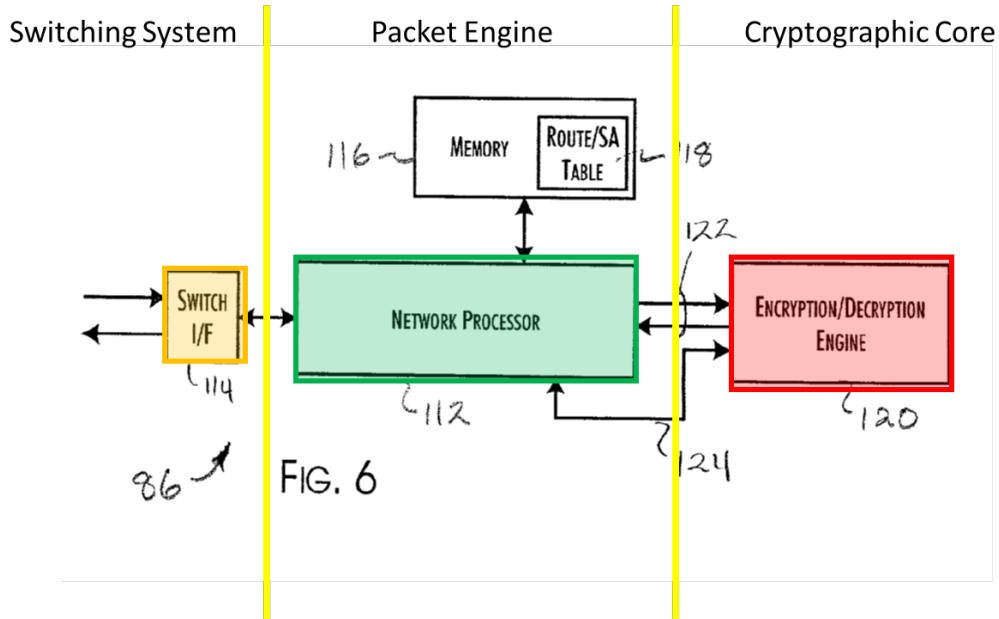
Fig. 6 illustrates the arrangement of the encryption/decryption engine 120 (red) and flow of packets with respect to the network processor (green), and switch fabric/interface (orange).



EX-1004 Fig. 6; EX-1003 ¶ 100.

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

Pham discloses the network processor (*packet engine*) is interposed between the switch fabric/interface (*switching system*) and the encryption/decryption engine (*cryptographic core*).

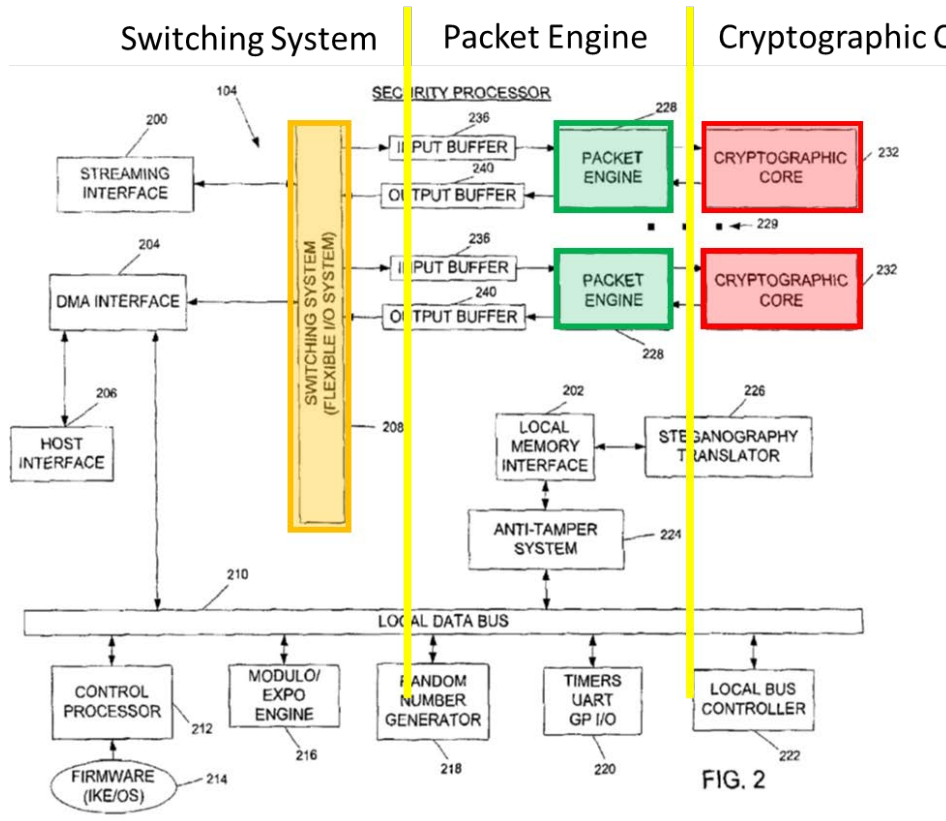


EX-1004 Fig. 6; EX-1003 ¶ 101.

Pham's arrangement shown in Fig. 6 corresponds with the architecture disclosed in the '436 Patent which the applicant argued demonstrated the "Packet engines 228 may each be interposed between/coupled to a cryptographic core 232 and the switching system 208 as shown in Figure 2."

The specification has been updated to include the "interposed" language in light of the objection to the specification. This change is supported by the originally filed specification. For example, Figure 2 illustrates packet engines 228 interposed between the switching system 104 and cryptographic cores 232.

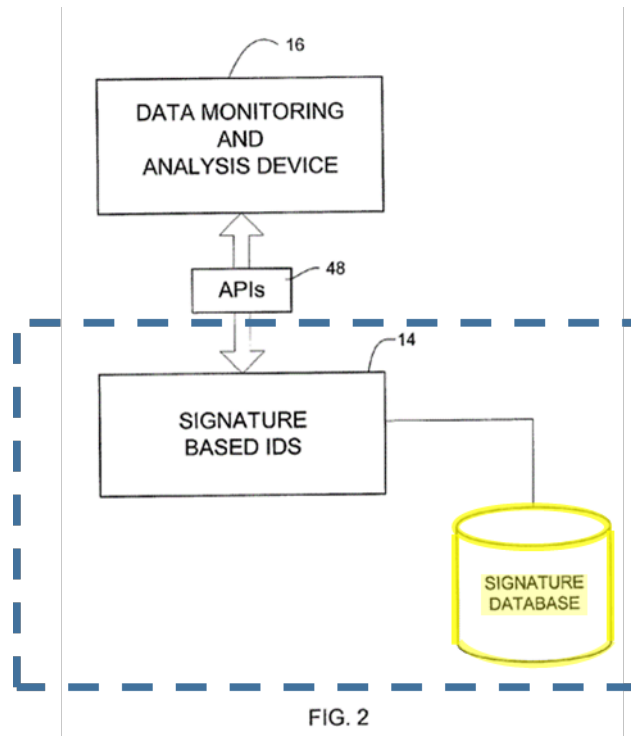
EX-1002 OA response pp. 68-77; EX-1003 ¶ 102



EX-1001, Fig. 2; EX-1003 ¶ 102.

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.

Wu discloses a signature based intrusion detection system 14 (blue) with a signature database (yellow).



EX-1005 Fig. 2; EX-1003 ¶ 103.

Wu discloses a signature based instruction detection system 14 including a signature database 42. EX-1005 3:52-4:3; EX-1003 ¶ 104.

The system of Wu is responsive to captured packets matching a signature stored in the signature database.

Signatures (or patterns) of all known attacks are described in an abstract form and included within the signature database 42. These patterns are used to identify an intrusion. Additional signatures are identified by studying system audit information in order to find matching patterns of known system intrusions. In a similar manner indications of other attacks can be figured out. They are represented in a specified form and coded to the intrusion detection system. A signature analysis or pattern matching algorithm is used upon the packets, wherein the packets are compared to “attack signatures”, or

signatures of known policy violations or patterns of misuse. Signature engine 34 compares monitored traffic with attack signatures. Attack signatures can comprise, for example, a rules-based hierarchy of traffic signatures of known policy violations. The signature engine 34 compares packets from the network traffic with such attack signatures such that policy violations can be discovered.

EX-1005 5:23-39; EX-1003 ¶ 105.

Wu discloses locating the intrusion detection system at key locations in the network and notes that the system may be “placed in various locations throughout the network.” EX-1005 4:65-67; EX-1003 ¶ 106.

The network intrusion detection system (NIDS) 18 may be placed at key points throughout the network. The units monitor network traffic, perform local analysis of the traffic, and report attacks to a central management station (e.g., system administrator). The network intrusion detection systems 18 are preferably placed on the network perimeter including both sides of a firewall 20 (e.g., between router 22 and the Internet), near a web server 26, and on links to internal or partner networks (e.g., between router 28 and internal corporate network 24). For example, NIDS 1 monitors all traffic passing into and out of the internal network. NIDS 1 provides an early warning since it detects reconnaissance port scans that typically indicate the start of hacker activity. From this point, NIDS1 can document the number and types of attacks originating on the Internet that target the network. NIDS 2 monitors traffic that has passed through the firewall 20. NIDS 3 monitors traffic passing into and out of internal corporate

LAN 24. It is to be understood that the network of FIG. 3 is only one example illustrating placement of NIDSs within a network and that the present invention may be used on different types of networks and placed in various locations throughout the network.

EX-1005 4:46-67; EX-1003 ¶ 106.

It 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 engine*) and the encryption/decryption engine (*cryptographic core*) as discussed in Section VIIA.3 above. EX-1003 ¶ 107.

b. Claim 13

- i. [pre] A security processing system comprising: a security processor comprising:*

Pham discloses a security processing system including a security processor.

See Claim 1 [pre]

- ii. a switching system to send outgoing packets and to receive incoming packets;*

See Claim 1.ii

- 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,*

See Claim 1.iii

- 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*

See Claim 1.iv

- v. *wherein the incoming and outgoing packets are provided with a tag upon ingress to one of the plurality of packet engines and the tag determines an egress path within the security processor upon exit from a corresponding cryptographic core;*

See Claim 1.v

- 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,*

See Claim 1.vi

- vii. *wherein the packet engine is interposed between the switching system and the cryptographic core;*

See Claim 1.vii

- 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*

Wu discloses an intrusion detection system meeting the limitation as described in detail above with respect to Claim 1.viii limitation.

It would have been obvious to a POSA to combine Pham and Wu as described above to arrive at the claimed invention for the same reasons as described above with respect to Claim 1. EX-1003 ¶ 116.

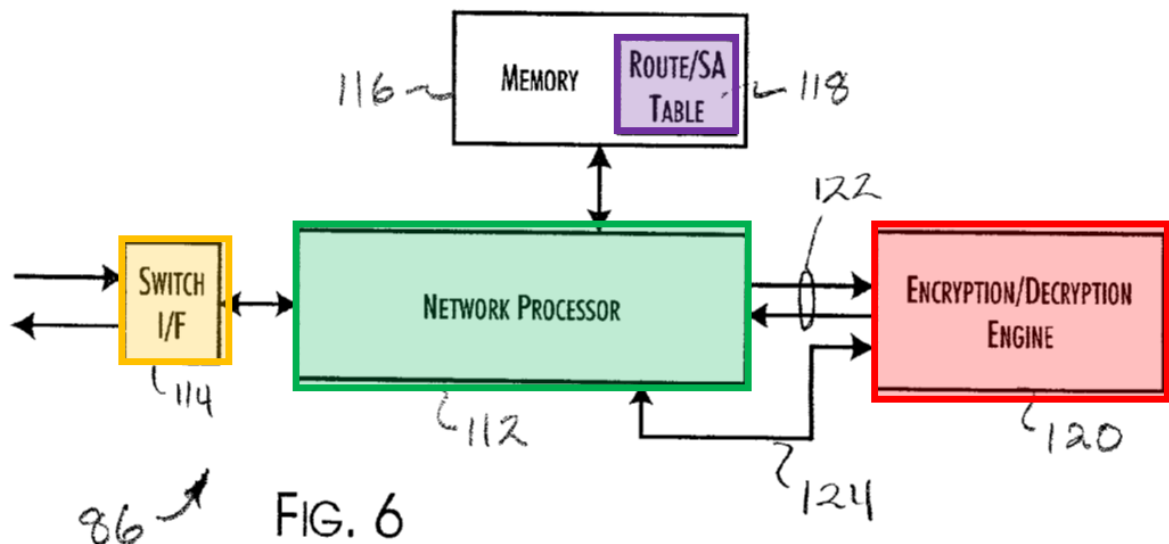
***ix. a local data bus coupled to the switching system;
and***

Pham discloses a direct data transfer bus 122 (*local data bus*).

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.”

EX-1004 [0052]; EX-1003 ¶ 117.

The direct data transfer bus 122 is coupled to the switch fabric 78 (*switching system*) via the network processor 112.



EX-1004 Fig. 6; EX-1003 ¶ 118.

This is consistent with the '436 Patent's use of the word "coupling" with respect to the data bus, in that it includes direct coupling as well as coupling through an intermediate element. For example, the '436 Patent describes that in Figure 2, local memory interface 202 is "coupled to local data bus 210" even though it is coupled through anti-tamper system 224. EX-1001 6:63-64; EX-1003 ¶ 119.

To the extent PO argues the local data bus must be directly coupled to switching system, it would have been obvious to a POSA to provide a direct data transfer bus as taught by Pham between the network processor and encryption/decryption engine to handle packets between the switching fabric and other entities in the security processor of Pham, such as to connect the network processor and/or memory 116. A POSA would have been motivated to provide the bus to effectively handle data transfers between the switch fabric, network processor and memory as is known in the art, furthermore being downstream of the switch fabric, the local data bus fails to be subject to the deleterious saturation issues noted by Pham regarding prior art peripheral buses. EX-1004 [0010]; EX-1003 ¶ 120.

x. a memory coupled to the local data bus.

Pham discloses a memory array 116. EX-1004 [0051]; Fig. 6; EX-1003 ¶ 121.

A memory array 116 is provided for the external memory and program requirements of the network processor. Optionally, in accordance with an alternate embodiment of the present invention, the memory array 116 also provides storage space for an SA parameter data table 118.

EX-1004 [0051]; EX-1003 ¶ 121.

The memory array 116 is coupled to the local data bus via the network processor 112. EX-1004 Fig. 6; EX-1003 ¶ 122.

To the extent the PO argues the memory must be directly coupled to the local data bus, it would have been obvious to directly couple the local data bus to both the memory and switching fabric as discussed above. EX-1003 ¶ 123.

c. Claim 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.

As discussed above with respect to Claim element 1.iii, Pham describes the network processor (*packet engine*) provides SA parameters (*security context management processing*) for the ingress and egress packets (*incoming and outgoing packets*).

The preferred implementation of a crypto processor 86 is shown in FIG. 6. 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. Optionally, in accordance with an alternate embodiment of the present invention, the memory array 116 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. The control processor 84 explicitly propagates identical copies of the SA parameter data to each of the crypto processors 86, enabling the crypto processors 86 to process any data packet received.

EX-1004 [0051]; EX-1003 ¶ 124.

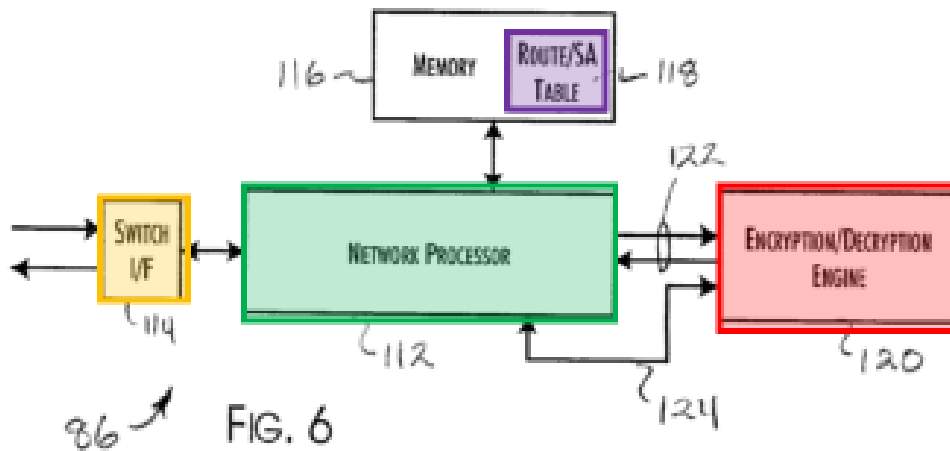
d. **Claim 9.**

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.

As described with respect to Claim 1, Pham discloses multiple crypto processors 86 which each include a respective network processor [green] (*packet engines*) and encryption/decryption engine [red] (*cryptographic cores*)

The VPN gateway 72 utilizes IBM Packet Routing Switches PRS28.4G (IBM Part Number IBM3221L0572), available from IBM Corporation, Armonk, N.Y., as the basis for a central crossbar switch fabric 78 interconnecting an ingress processor 80, an egress processor 82, a control processor 84 and **an array of two to sixteen crypto processors 86.**

EX-1004 [0045]; EX-1003 ¶ 125.



EX-1004 Fig. 6; EX-1003 ¶ 125.

Pham discloses that respective ones of the network processors 112 and encryption/decryption engines process substantially all the data packet received and transmitted. For example, in one embodiment, Pham discloses that ingress processor 80 (Fig. 5) and network processor 112 in crypto processor 86 (Fig. 6) use the identical conventional processors and identical routing and SA tables to allow functions of the ingress processor to be offloaded to network processor 112, such

as packet routing, SA parameter association and compression and decompression. EX-1004 Figs. 5, 6, [0049], [0051], [0053]. Thus, all packets, both clear text and encrypted can be sent to network processor 112 for routing using routing and SA table 118. EX-1003 ¶ 126.

e. **Claim 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.

Pham discloses the network processor (packet engine) adds at least an IP_{tun} header (*IP header*) to the outgoing packets. See Claim 1 VI.A.4.a.v; EX-1003 ¶ 127.

f. **Claims 12 and 22**

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.

Pham in view of Wu discloses an intrusion detection system including the signature database connected between the network processor and the encryption/decryption engine that “listens and analyzes all traffic in real-time as it travels across the network” for packets matching stored signatures as discussed above with respect Claims 1 and 13. Pham further discloses passing encrypted data packets and clear text data packets to the encryption/decryption engine.

For the preferred IPsec processing embodiments of the present invention, clear text data packets forwarded from the LAN 38 through the VPN gateway 12 subject to the VPN encryption protection are routed by the ingress processor 30 through the Switch fabric 40 to an available encryption data packet processor 42. The encrypted data packet is then returned through the Switch fabric 40 to the egress processor 32 and passed onto the Internet 18. Conversely, encrypted data packets received from the Internet 18 are routed by the ingress processor 34 through the Switch fabric 40 to a decryption data packet processor 44. The resulting clear text data packet is then passed to the egress processor 36 for transferred onto the LAN 38.

EX-1004 [0041]; EX-1003 ¶ 128.

Wu further discloses its IDS, like conventional IDS, matches packets traversing the network against signatures in the signature database. EX-1005 2:11-13, 2:44-48, 7:51-67; EX-1003 ¶ 129.

Conventional signature based network intrusion detection systems treat signatures as passive items. When a packet is inspected, it is matched against a list of signatures.

EX-1005 2:11-13; EX-1003 ¶ 129.

Data packets transmitted on the network and having corresponding classification rules are classified according to generated classification rules. Classified packets are forwarded to a signature engine for comparison with signature profiles.

EX-1005 2:44-48; EX-1003 ¶ 129.

The 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.

EX-1005 5:41-44; EX-1003 ¶ 129.

Signatures (or patterns) of all known attacks are described in an abstract form and included within the signature database 42. These patterns are used to identify an intrusion.

EX-1005 5:23-25; EX-1003 ¶ 129.

Signature matching 66 is performed based on packet classifications to detect network intrusion. Any problems detected are sent to an alert log 68 and appropriate action is taken.

EX-1005 5:67-6:1; EX-1003 ¶ 129.

Action may include, for example, match packet with Subset of signatures (step 116), drop packet (step 118), generate alarm (120), or drop packet and update field of flow table (step 122).

EX-1005 7:64-67; EX-1003 ¶ 129.

g. Claim 16.

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

Pham discloses the security processor and memory are within the same cryptographic boundary. A POSA understands a cryptographic boundary to mean an explicitly defined continuous perimeter that establishes the physical bounds of a cryptographic module and contains all hardware, software, and/or firmware components of a cryptographic module. EX-1003 ¶ 130. Pham discloses the memory 116 is within the security processor (**brown**) which forms the cryptographic module or part of the cryptographic module.

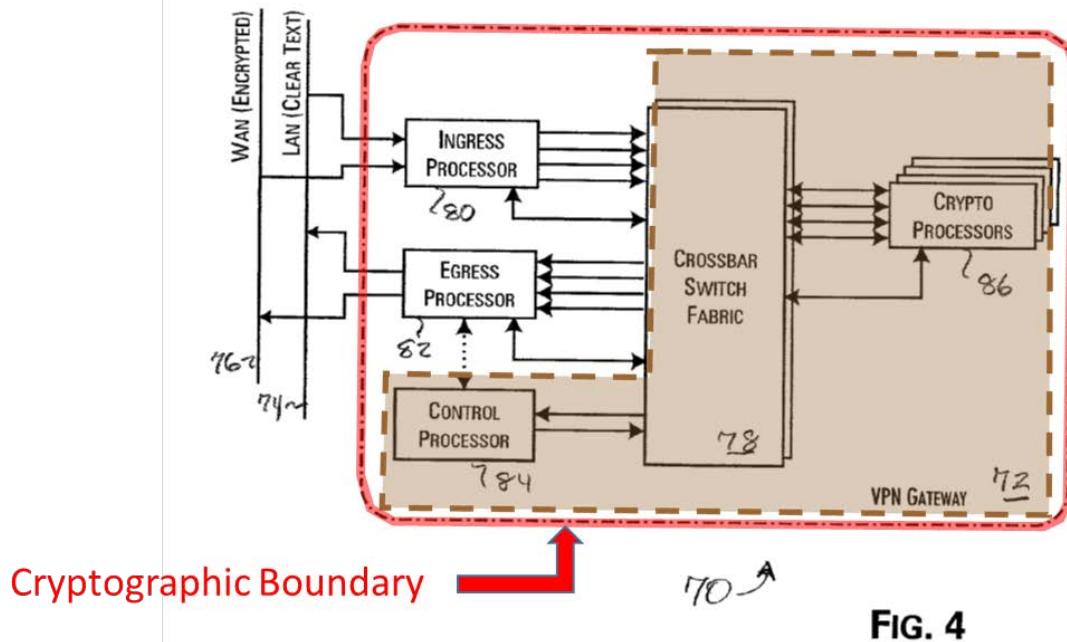
A preferred VPN embodiment 70 of the present invention, representing a Specific implementation of the extended protocol processor architecture 50, is shown in FIG. 4. A VPN gateway 72 provides a single physical LAN 74 connection supporting multiple logical connections over a local clear text network and a single physical WAN 76 connection, extending encrypted network connections over the Internet. The VPN gateway 72 utilizes IBM Packet Routing Switches PRS28.4G (IBM Part Number IBM3221L0572), available from IBM Corporation, Armonk, N.Y., as the basis for a central crossbar Switch fabric 78 interconnecting an ingress processor 80, an egress processor 82, a control processor 84 and an array of two to sixteen crypto processors 86.

EX-1004 [0045]; EX-1003 ¶ 130.

The security processor as described previously includes the network processor 112, the encryption/decryption engine 120, and switch matrix 78 which

enables the routing and processing of packets for encryption/decryption. The security processor and memory 116 is within the cryptographic boundary (red).

EX-1004 [0045]; EX-1003 ¶ 131.



EX-1004 Fig. 4; EX-1003 ¶ 131.

B. Ground 2: Claims 3, 14 and 21 Are Unpatentable Over Pham and Wu in Further View of Collins

1. The Collins Reference

Collins describes a cryptographic system which includes an RSA engine. Collins describes that the RSA engine is a special purpose arithmetic unit designed and structured to perform “fast modular exponentiation” and that its design and operation are known to a POSA. EX-1008 [0048]; EX-1003 ¶ 132. Collins explains that the RSA engine allows tasks to be performed in parallel to speed up the operation of the cryptographic system. EX-1008 [0050]; EX-1003 ¶ 132.

2. Detailed Application of Pham and Wu and Collins

a. Claims 3 and 14

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.

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

Pham in view of Wu renders Claims 1 and 13 obvious as discussed above.

As described in Claim 13, Pham discloses a direct data transfer bus 122 (*local data bus*). EX-1004 [0052]; EX-1003 ¶ 133.

Pham and Wu do not explicitly disclose a modulo engine. However, a POSA understood that it was common to use a modulo engine to increase the speed of the cryptographic process, and Collins discloses such a modulo engine. EX-1003 ¶ 134.

Collins discloses an arithmetic unit/exponentiation cells (*modulo engine*) to “perform fast modular exponentiation” for use in cryptographic processing coupled to a bus.

The RSA engine 260 is a special purpose arithmetic unit designed and structured to perform fast modular exponentiation. In the Specific embodiment, it performs 10 exponentiations per Second on a 1024 bit value. Its design and operation will be understood by one of skill in the art. If another encryption method besides RSA public key

cryptography is provided by the System, other types of arithmetic units may be provided along with or instead of RSA engine 260.

EX-1008 [0048]; EX-1003 ¶ 135.

As FIG. 3 further shows, the I/O controller router 310 of the cryptographic co-processor 115 is coupled by a data/control bus 320 to a DES cell 330 and a number of exponentiation cells 340.

EX-1008 [0057]; EX-1003 ¶ 135.

A POSA understood the arithmetic unit/exponentiation cell described in Collins to be a modulo engine. EX-1003 ¶ 136.

It would have been obvious to a POSA to use the arithmetic unit (modulo engine) described in Collins to aid in the encryption/decryption of Pham. A POSA would be motivated to use a special purpose arithmetic unit to speed the encryption/decryption processes as expressly described by Collins as a benefit by allowing parallel processing, moreover it would have been obvious to a POSA to couple the arithmetic unit to the direct data bus of Pham to allow the transfer of data to and from the arithmetic unit. EX-1003 ¶ 137.

b. Claim 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.

Pham in view of Wu renders Claim 13 obvious as discussed above. Neither Pham nor Wu disclose executing and authenticating boot code. However, Collins does.

Collins discloses executing a loader program (*boot code*) on the cryptographic processor 110 (*security processor*) to load user applications programs (*firmware*). EX-1008,[0026, 58, 66]; EX-1003 ¶ 139.

FIG. 6 is a flow diagram of a loader program (e.g., black-boot) that may be used to load user applications.

EX-1008 [0026]; EX-1003 ¶ 139.

The black-boot program's main function is to load other user-application programs into flash memory 124, or to Start an application from flash memory 124 (if it is already there).

EX-1008 [0086]; EX-1003 ¶ 139.

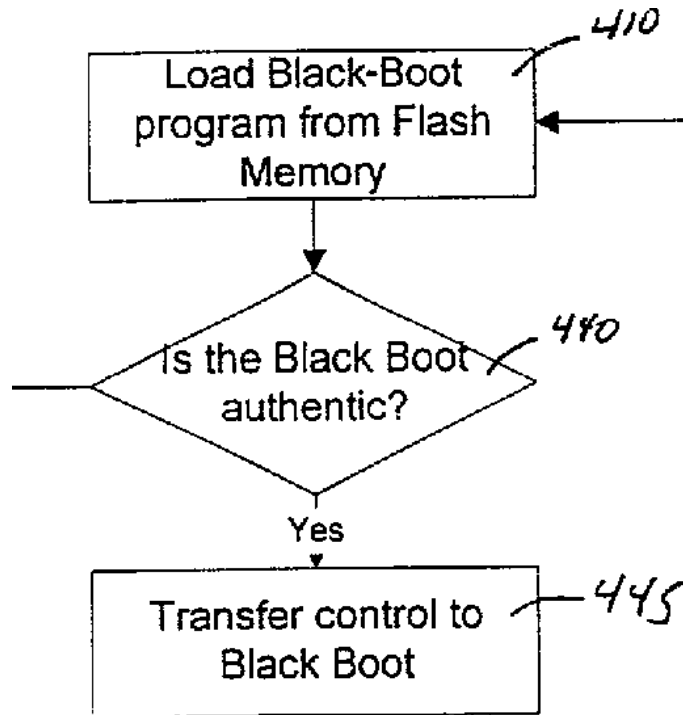
Collins discloses the loader program is loaded and authenticated by the cryptographic processor (*security processor*) prior to transferring control (*operation of the security processor*)

CPU 210 proceeds to step 410 in which it loads a black-boot program from flash memory.

EX-1008 [0068]; EX-1003 ¶ 140.

Referring again to FIG. 4, in step 440, once the black-boot program is loaded, CPU 210 determines if the black-boot is authentic using the same technique described above in Step 424. If it is not authentic, then operation is aborted to step 427 and the keys are zeroed (erased) and the cryptographic System 100 is placed in a non-functioning State awaiting a reset. If it is authentic, then the black-boot program is loaded into RAM, and control of CPU 210 is transferred to the black-boot program.

EX-1008 [0087]; EX-1003 ¶ 140.



EX-1008 Fig. 4; EX-1003 ¶ 140.

It would have been obvious to a POSA to implement the boot authentication protocol taught by Collins into the security system of Pham and Wu. A POSA

would have been motivated to implement the teachings of Collins in order to “provide a level of confidence” that boot code has not be altered or replaced by a fraudulent program” and “allows a great amount of flexibility, while still providing security” as expressly taught by Collins. EX-1008 [0081]. A POSA would have been confident of success implementing Collins authentication protocol given its use of well-known processes such as comparing the length of the program file, starting address, and hashes with known values. EX-1008 [0072]; EX-1003 ¶ 141.

C. Ground 3: Claims 4, 7, and 8 Are Unpatentable Over Pham, Wu and Collins and Further In View of Krishna

1. The Krishna Reference

Krishna is directed to cryptographic processing on a single chip. EX-1006; EX-1003 ¶ 142.

2. Detailed Application Of Pham, Wu, Collins and Krishna

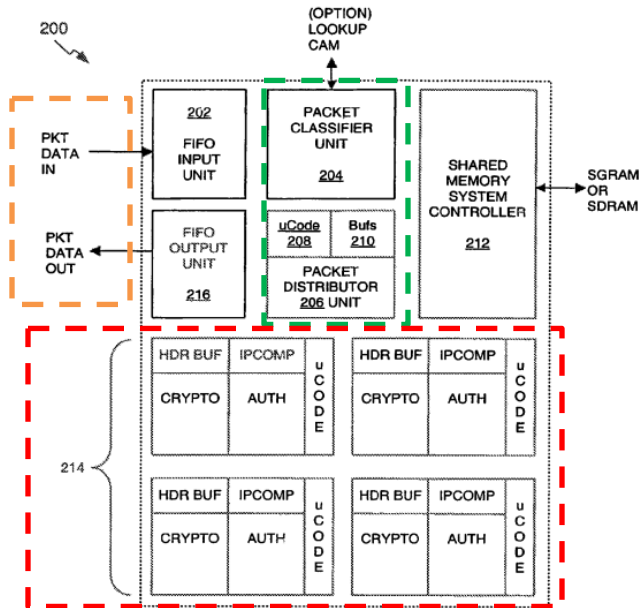
a. Claim 4

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

Pham, Wu and Collins render Claim 3 obvious as described above including disclosing a network processor (*packet engine*), encryption/decryption engine (*cryptographic core*) and arithmetic unit (*modulo engine*). Pham, Wu and Collins do not explicitly disclose the packet engine, cryptographic core and modulo engine

are formed on a single chip. However, Krishna discloses forming discrete components of the security processor on a single chip. EX-1003 ¶ 143

Krishna discloses a packet engine (green), a cryptographic core(red) and other components of a security processor upon a single chip. EX-1003 ¶ 144.



EX-1006, Fig 2; EX-1003 ¶ 144.

Krishna further describes incorporating components on a single chip may increase performance.

By incorporating both encryption and authentication functionality in a single accelerator chip, over-all system performance can be enhanced.

EX-1006 1:66-2:2; EX-1003 ¶ 145

It would have been obvious to a POSA to form the network processor, encryption/decryption engine, and the arithmetic unit of Pham, Wu and Collins

onto a single chip as taught by Krishna. A POSA would have been motivated to do so to increase performance as described by Krishna. As discussed in the State of the Art section, by October 2003 cryptographic processing had moved away from discrete processors to implementing on a single chip. EX-1010 Abstract; EX-1003 ¶ 146.

A POSA would also be confident of success given Krishna's teaching and the ubiquitous nature of special purpose chips. EX-1003 ¶ 147

b. Claims 7 and 8

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.

Pham discloses the security processor includes network processor 112 that performs security processing and network processing. Pham also discloses that “[a]ll network traffic that is to be processed can be routed to and through the network gateway.” EX-1004 [0015]; EX-1003 ¶ 148.

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. The network processor 112 controls and monitors the engine 120 via control and status lines 124. Preferably, the engine 120 is a BCM5840 Gigabit Security Processor,

available from Broadcom Corporation, Irvine, Calif. The BCM5840 processor implements a highly integrated symmetric cryptography engine providing hardware Support for IPsec encryption and decryption operations.

EX-1004 [0052]; EX-1003 ¶ 148.

For example, in one embodiment, Pham discloses that ingress processor 80 (Fig. 5) and network processor 112 in crypto processor 86 (Fig. 6) use the identical conventional processors and identical routing and SA tables to allow functions of the ingress processor to be offloaded to network processor 112, such as packet routing, SA parameter association and compression and decompression. EX-1004 Figures 5, 6, [0049], [0051], [0053]; EX-1003 ¶ 149.

D. Ground 4: Claim 17 Is Unpatentable Over Pham and Wu and Further In View of Krishna

a. Claim 17.

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

Pham and Wu render obvious Claim 13 as described above. Pham and Wu do not explicitly disclose whether the security processor is formed on a single chip. Krishna as discussed above with respect to Claim 4 discloses forming a security processor including a switching system, a packet engine and a cryptographic core as well as other functions on a single chip. It would have been obvious to combine

the teachings of Krishna with the system of Pham in view of Wu for the same reasons discussed above with respect to Claim 4. EX-1003 ¶ 150.

VIII. THE BOARD SHOULD NOT EXERCISE ITS DISCRETION AND DENY INSTITUTION

A. The Board Should Not Deny Institution Under 35 U.S.C. § 325(d)

When determining whether to exercise discretion under § 325(d), “the Board uses the following two-part framework: (1) whether the same or substantially the same art previously was presented to the Office or whether the same or substantially the same arguments previously were presented to the Office; and (2) if either condition of first part of the framework is satisfied, whether the petitioner has demonstrated that the Office erred in a manner material to the patentability of the challenged claims.” *Advanced Bionics, LLC v. MED-EL Elektromedizinische Geräte GmbH*, IPR2019-01469, Paper 6, p. 8 (Feb. 13, 2020) (designated: March 24, 2020).

The ’436 Patent has not been challenged in any other IPR or post-grant review (PGR) proceeding or in reexamination. The combination of art in the present grounds, and the arguments related thereto were not previously presented to the Office.

During prosecution, the examiner did cite to U.S. Pat. No. 7,493,659 (the ’659 Patent). The ’659 Patent was filed the same day as Wu and includes an overlap in inventorship, and subject matter with Wu. The ’659 Patent was cited for

disclosing “a network intrusion detection and analysis processor which further discloses 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.” In response, the applicant did not present any arguments that the ‘659 Patent did not disclose 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, but instead rewrote the independent claims to include the limitations from dependent claims that the examiner found to be allowable. However, the examiner never identified nor considered the Pham primary reference used herein and thus did not consider the Wu reference in combination with the Pham disclosure nor the arguments as presented in Grounds 1-4. Thus, the Office erred by not considering the combination of Pham and Wu which is material to the patentability of the challenged claims.

The present Petition uses Krishna in Grounds 3 and 4 for disclosing that the security processor is formed on a single chip. During prosecution, the examiner cited U.S. Pat Publication No. 2003/0014627 (“627 Publication”). The 627 Publication includes an overlap in inventorship, and subject matter with Krishna. However, the examiner did not cite to the 627 Publication for disclosing the security processor is formed on a single chip, and never identified the Pham

reference and thus did not consider the Krishna reference in combination with the Pham and Wu references as presented in Grounds 3-4. Thus, the Office erred by not considering the combination of Krishna, Pham and Wu which is material to the patentability of the challenged claims.

B. The Board Should Not Deny Institution Under 35 U.S.C. § 314(a)

The Board has discretion to deny *inter partes* review under 35 U.S.C. § 314(a). In *Apple Inc. v. Fintiv, Inc.*, the Board set forth six non-dispositive factors intended to guide that discretionary decision of whether efficiency, fairness, and the merits support the exercise of authority to deny institution in view of an earlier trial date in the parallel proceeding. On June 21, the Director issued interim procedure regarding application of the *Fintiv* factors (Interim Guidance). The Interim Guidance stated that “the PTAB will not deny institution of an IPR or PGR under *Fintiv* (i) when a petition presents compelling evidence of unpatentability” Here, the Petition is particularly strong and presents compelling evidence of unpatentability of the Challenged Claims. Specifically, the Petition explains how the primary reference, Pham, in combination with the other references, discloses the claimed limitations. The evidence presented, if unrebutted in trial, would plainly lead to a conclusion that one or more claims are unpatentable by a preponderance of the evidence. Thus, under the Interim Guidance, the Board should not deny institution.

Nevertheless, the Board's decision in *Sotera Wireless, Inc. v. Masimo Corp.*, IPR2020-01019, Paper 12 (Dec. 1, 2020) (precedential as to § II.A) instructs that a holistic view of the remaining *Fintiv* factors also weighs in favor of institution.

Factor 1 is neutral because no request for stay has been filed *Sand Revolution II LLC v. Continental Intermodal Group – Trucking LLC*, IPR2019-01393, Paper 24 at 7 (June 16, 2020) (informative).

Under factor 2, the trial date has been set for all defendants in the Related Litigation for May 2024. According to the most recent statistics on median time-to-trial for civil actions in the (https://www.uscourts.gov/sites/default/files/data_tables/fcms_na_distprofile0930.2022.pdf), the median time from filing to trial is 21 months. The Related Litigation was filed on August 8, 2022 and thus would be expected to go to trial shortly after May 8, 2024 according to the median time to trial statistics. A Final Written Decision is expected in the present matter August 2024. Considering the inherent uncertainties of litigation scheduling, particularly where multiple trials are scheduled for the same date this factor weighs against discretionary denial.

Factor 3 favors institution. The co-pending litigation is in its early stages, and the investment in it has been minimal. The parties have not exchanged proposed claim terms or constructions, and will not complete claim construction briefing until October 2023. EX-1014, 2. The *Markman* hearing is not until

November 2023. EX-1014, 3. Fact discovery is not set to close until December 8, 2023, and expert discovery is not set to close until February 5, 2024. EX-1014 3; *see PEAG LLC v. Varta Microbattery GMBH*, IPR2020-01214, Paper 8 at 17 (Jan. 6, 2021) (finding that since no claim construction hearing had yet been held and discovery was not completed, the little investment in the parallel proceeding weighed against discretionary denial).

Under factor 4, Petitioner stipulates that if the IPR is instituted, it will not pursue the same grounds in the district court litigation. *Sand Revolution II* at 7. In addition to the stipulation that Petitioner issued to PO, PO has only identified a subset of the claims that are being challenged in the present Petition. Thus, it is unlikely the district courts will be addressing the validity of all of the claims challenged by this Petition.

Under factor 5, Petitioner is a defendant in the Related Litigations. While some cases favor institution where petitioner is not a defendant, nothing within *Fintiv* suggests that the same party between the proceedings weighs in favor of discretionary denial. *See HP Inc. v. Slingshot Printing LLC*, IPR2020-01084, Paper 13 at 9 (having the “same parties as parallel proceeding” makes factor 5 “neutral”)

Under factor 6, other circumstances weigh in favor of institution. Here, the merits of the Petition are particularly strong. For example, the primary reference Pham discloses the very limitation (*i.e. the... packets are provided with a tag upon*

ingress....and the tag determines an egress path) by which the '436 Patent gained allowance (See V.B and VI.A.4.a.v. above). Further, the secondary reference, Wu, discloses the same conventional IDS system presented by the Examiner to meet the claimed IDS system during prosecution to which the PO acquiesced, rather following up with a narrowing amendment directed to the number of packet engines. EX-1002, FOA pp.45-58, After Final Amendment pp. 35-42 (See also V.B and VII.A above).

When viewed holistically, the timing of the present Petition was reasonable, there has been relatively limited investment in the related litigation, and there is minimal overlap between the present IPR and the Related Litigations. Further, coupling these *Fintiv* considerations with compelling evidence of unpatentability presented in the Petition, the efficiency and integrity of the IPR process is best served by instituting review.

IX. MANDATORY NOTICES UNDER 37 C.F.R. §42.8

A. Real Party-in-Interest (37 C.F.R. § 42.8(b)(1))

The real party-in-interest in this Petition is CISCO SYSTEMS, INC.

B. Related Matters (37 C.F.R. § 42.8(b)(2))

1. JUDICIAL MATTERS

As of the filing date of this Petition and to the best knowledge of Petitioner, the '436 Patent is involved in the following litigations:

Petition for *Inter Partes* Review of U. S. Patent No. 7,685,436

Lionra Technologies Limited v. Fortinet, Inc., Case No. 2:22-cv-00322 (E.D. Tex.) (filed Aug. 19, 2022) (ongoing).

Lionra Technologies Limited v. Cisco Systems, Inc., Case No. 2:22-cv-00305 (E.D. Tex.) (filed Aug. 8, 2022) (ongoing).

Lionra Technologies Limited v. Palo Alto Networks, Inc., 2:22-cv-00334 (E.D. Tex.) (filed Aug. 29, 2022) (ongoing)

2. ADMINISTRATIVE MATTERS:

As of the filing date of this Petition and to the best knowledge of Petitioner, the '436 Patent was not subject to any *inter partes* reviews or reexamination.

3. RELATED PATENTS

See Exhibit 1011.

C. Lead/Back-up Counsel (37 C.F.R. § 42.8(b)(3)):

Lead Counsel:

Patrick D. McPherson, USPTO Reg. No. 46,255

PDMcPherson@duanemorris.com

DUANE MORRIS LLP

901 New York Avenue NW, Suite 700-East

Washington, D.C. 20001

P: 202.776.5214, F: 202.776.7801

Back-Up Counsel:

Patrick C. Muldoon, USPTO Reg. No. 47,343

PCMuldoon@duanemorris.com

DUANE MORRIS LLP

901 New York Avenue NW, Suite 700-East

Washington, D.C. 20001

P: 202.776.7840, F: 202.776.7801

D. Joseph English, USPTO Reg. No. 42,514

DJEnglish@duanemorris.com

DUANE MORRIS LLP

901 New York Avenue NW, Suite 700-East

Washington, D.C. 20001

P: 202.776.5228, F: 202.776.7801

Monté T. Squire USPTO Reg. No. 80,123

MTSquire@duanemorris.com

Duane Morris LLP

1201 North Market St, Suite 501

Wilmington, DE 19801

P: : +1 302 657 4918

Paul H. Belnap USPTO Reg. No. 73,106

PHBelnap@duanemorris.com

Duane Morris LLP

901 New York Avenue N.W., Suite 700 East

Washington, DC 20001-4795

P: +1 202 776 7879

Nicole Candelori* USPTO Reg. No. 77,218

DUANE MORRIS LLP

NCandelori@duanemorris.com

901 New York Avenue NW, Suite 700-East

Washington, D.C. 20001

P: 202-776-5284, F: 202.776.7801

*Not admitted in D.C. Practice in D.C. limited to matters and proceedings
before the U.S. Patent and Trademark Office and federal courts

D. Notice of Service Information (37 C.F.R. § 42.8(b)(4)):

Please direct all correspondence to lead and back-up counsel at the above
addresses. Petitioner consents to electronic service at the email addresses above.

X. CONCLUSION

For the reasons set forth above, Petitioner has established a reasonable
likelihood of prevailing with respect to all Challenged Claims of the '436 Patent
and requests the Board institute *inter partes* review and then cancel all claims as
unpatentable.

Respectfully submitted,

DUANE MORRIS LLP

BY: /Patrick D. McPherson/
Patrick D. McPherson, USPTO Reg.
No. 46,255
PDMcPherson@duanemorris.com
DUANE MORRIS LLP
901 New York Avenue NW, Suite
700-East
Washington, D.C. 20001.

Dated: March 9, 2023

CERTIFICATION OF SERVICE ON PATENT OWNER

Pursuant to 37 C.F.R. §§ 42.6(e), 42.8(b)(4) and 42.105, the undersigned certifies that on the March 9, 2023, a complete and entire copy of this Petition for *Inter Partes* Review of U.S. Patent No. 7,685,436 and all supporting exhibits were served via Federal Express, postage prepaid, to Lionra Technologies LTD. by serving the correspondence address of record for the '436 Patent:

Kiklis and Clark, PLLC

Harris Corporation

1800 Diagonal Road

Suite 600

Alexandria, VA 22314

UNITED STATES

/Patrick D. McPherson/

Patrick D. McPherson, Reg. No. 46,255
901 New York Ave. NW suite 700 East
Washington, D.C. 20001

P: (202) 776-7800

F: (202) 776-7801

PDMcPherson@duanemorris.com

ATTORNEY FOR PETITIONER

CERTIFICATE OF COMPLIANCE

Pursuant to 37 C.F.R. § 42.24 *et seq.*, the undersigned certifies that this document complies with the type-volume limitations. This document contains 12,941 words as calculated by the “Word Count” feature of Microsoft Word 2010, the word processing program used to create it.

Dated: March 9, 2023

By: Patrick D. McPherson
Patrick D. McPherson
Reg. No. 46,255
Duane Morris LLP
901 New York Ave. NW suite 700 East
Washington D.C., 20001
P: (202) 776-7800
F: (202) 776-7801
PDMcPherson@duanemorris.com