UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

***Inter Partes* Review**

Cisco Systems, Inc.,
Petitioner,
v.

Lionra Technologies Ltd.,
Patent Owner.

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

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

COMBINED DECLARATION OF ERIC COLE, PH.D.

TABLE OF CONTENTS

I. INTRODUCTION 1

II. QUALIFICATIONS 2

III. SCOPE OF WORK 9

IV. LEVEL OF ORDINARY SKILL IN THE ART 9

V. LEGAL PRINCIPLES 11

A. Anticipation 11

B. Obviousness 14

VI. ASSERTED PRIOR ART 17

A. Pham 18

B. Wu 35

VII. OVERVIEW OF THE CHALLENGED PATENTS 37

A. Assumed Effective Filing and Invention Dates 37

B. The Challenged Patents 37

C. General Discussion of the Asserted Patents and the Prior Art 48

VIII. PHAM DOES NOT DISCLOSE THAT "SUBSTANTIALLY ALL OF THE … PACKETS … TO THE SECURITY PROCESSOR TRANSIT ONE OF THE PLURALITY OF PACKET ENGINES 52

IX. A POSITA WOULD NOT BE MOTIVATED TO COMBINE PHAM AND WU 59

I, Eric Cole, of Ashburn, Virginia, declare that:

I. INTRODUCTION

1. Lionra Technologies, Ltd. has retained me as an independent expert in connection with IPR2023-673 and IPR2023-00703 to provide testimony regarding the technology involved in U.S. Patent Nos. 7,685,436 (the "'436 Patent") and 8,566,612 (the "'612") (collectively, the "Challenged Patents") and how the inventions described and claimed therein compare with the asserted prior art. I have been asked to provide my technical review, analysis, insights, and opinions regarding the references set forth in the above-referenced IPRs by Petitioner Cisco Systems.

2. I am being compensated for my work in this matter at my standard hourly rate for consulting services at $700 per hour. My compensation is not dependent on the outcome of the case and does not affect the substance of my statements in this Declaration. I have no financial interest in the matter or the patents at issue.

3. I have reviewed the specification and the claims of the '612 and '436 patents, as well as the prosecution histories for these patents. I am familiar with the

technology involved therein, having practical, hands-on experience in the field for over 30 years.

II. QUALIFICATIONS

4. My academic credentials include a master's degree in computer science and a doctorate in information security, and I have worked in the cyber and technical information security industry for over twenty-five years. The details of my education and experience are summarized in my curriculum vitae ("CV"), which is attached as Exhibit 2011. My CV also includes a list of my publications over the past ten years.

5. I have worked in computer security for over twenty-five years. To briefly summarize my career, I have: 1) been responsible for the security of sensitive government projects; 2) managed security at major private sector companies; 3) consulted for major private sector companies; 4) been actively involved in designing, building, and deploying intrusion detection systems; 5) worked on protecting and securing critical information including trade secrets; 6) continually taught and written about cybersecurity.

6. I am the founder and president of Secure Anchor Consulting, LLC, located in Ashburn, Virginia. Secure Anchor Consulting provides cybersecurity

consulting services and leads research and development initiatives to advance information systems security. Many of the clients I work with are responsible for protecting sensitive client and/or consumer information and implementing effective security.

7. At Secure Anchor Consulting, I also actively work on incidents, and I have a detailed understanding of measures that organizations can take to both prevent and detect breaches. In addition, I have worked with organizations to design, build, and implement security measures that would be classified as both fixes and compensating controls, and I have detailed knowledge of the effort that is required to implement various remediation measures.

8. I worked for the U.S. government for eight years as an employee and have held various contracting jobs with government agencies, which involved working with classified information. I have worked for a wide range of government organizations, including the Federal Bureau of Investigation (FBI), the National Security Agency (NSA), the Central Intelligence Agency (CIA), the Department of Energy, the Department of Defense (DOD), the Treasury Department, the Secret Service, and the Nuclear Regulatory Commission (NRC). I have held various top-secret security clearances with the DOD, the CIA, and the NRC. I also was involved

in funded research from the Defense Advanced Research Projects Agency (DARPA), an agency of the DOD responsible for the development of new intrusion detection technologies for use by the military. During this time, I have reviewed, edited, and created numerous security policies. On several occasions, I have also reviewed the reasonableness of measures intended to protect and secure Confidential Information through various types of documentation to include policies, procedures, standards, and baselines.

9. While serving as a Senior Officer for the CIA as Program Manager / Technical Director for the Internet Program Team with the Office of Technical Services, I implemented the Internet Program Team that designs, develops, tests, and deploys internet security products in three- to six-month intervals. In this role, I received a letter of appreciation from the Director of Central Intelligence and six Exceptional Performance Awards.

10. As a member of the Information Security Assessment Team with the Office of Security at the CIA, I evaluated and performed security assessments of network operating systems to identify potential vulnerabilities and solutions. I also designed a large-scale auditing system with an automated review capability and worked on several virus investigations for the Office of Security.

11. In my role as Chief Information Officer for the American Institutes for Research, I repaired and developed IT infrastructures for various organizations. I was also responsible for building out the entire data classification program to ensure that critical and proprietary data was properly protected and secured. I was also one of the principal leads on research funding from DARPA. In this role, I was responsible for understanding the current state of the art in intrusion detection and designing and building a new cybersecurity system that could catch attacks that were targeting organizations.

12. As Chief Scientist and Senior Fellow for Lockheed Martin, I performed research and development in information systems security. I also specialized in evaluating and designing secure network design, perimeter defense, vulnerability discovery, penetration testing, and intrusion detection systems. At Lockheed Martin, I served as a technical advisor in high-profile security projects for government clients including the DOD, the FBI Sentinel case management systems, Department of Homeland Security Enterprise Acquisition Gateway for Leading Edge solutions, Jet Propulsion Labs, Hanford Labs, and FBI Information Assurance Technology Infusion programs.

13. As Chief Technical Officer for McAfee, I executed the strategy for technology platforms, partnerships, and external relationships to establish product vision and achieve McAfee's goals and business strategies. In this capacity, I worked closely with groups tasked with the development of intellectual property. While at McAfee, I worked with many business customers responsible for protecting clients' information, helping them implement effective security solutions.

14. I was a fellow and instructor for twenty years with the SANS Institute, a research and education organization consisting of information security professionals. SANS is the largest source for information security training and security certifications in the world. I am an author of several security courses, such as SEC401-Security Essentials and SEC501-Enterprise Defender. SEC401-Security Essentials is a required course for agents of the FBI and the NSA. These courses have been taken by over 30,000 people, and I have taught more than 50% of these students via live and online training. The courses that I have written have multiple modules and lessons on security policies, employee agreements, and protection of intellectual property. As one of the top-rated instructors at SANS, I have delivered keynote addresses around the world.

15. I am a member of the European InfoSec Hall of Fame, a professional membership awarded by nomination and election by a panel of industry experts.

16. I hold a Certified Information System Security Professional (CISSP) certification and was the creator of the Global Information Assurance Certification (GIAC) Security Essentials Certification (GSEC).

17. I am a contributing author of "Securing Cyberspace for the 44th President" and served as a Commissioner on cybersecurity for President Obama. My Nine books on cybersecurity include "Online Danger," "Network Security Bible - 2nd Edition," "Advanced Persistent Threat," and "Insider Threat," which have become recognized as industry-standard sources. They are used in many classrooms and colleges around the world as authoritative texts on cybersecurity. I have also published several articles in the field.

18. The focus of my work over the last ten years has been on data protection for commercial organizations. I am very familiar with best practices in cybersecurity and have developed many of the standard practices.

19. Today, my consulting efforts help organizations properly protect client information and relate to various alternative methods of security that can be implemented. This includes hardening of systems, securing servers, proper

configuration, patching, and compensating controls. In cases where a fix cannot be made because it would negatively impact the business, I have extensive experience in understanding various compensating controls as an alternative to minimize the risk to an acceptable level and how to implement those controls.

20. I routinely help clients develop and implement company-wide policies, training, and best practices to prevent potential cybersecurity incidents. My work addresses threats from both internal and external sources, including accidental and intentional incidents.

21. I have led, and been involved in working on, responses to many cybersecurity incidents. This includes performing root cause analysis, verifying the reasonableness of security measures, and validating the implementation of additional remediation measures.

22. In my consulting work and in the various positions that I have held, I have been responsible for protecting organizations to minimize and prevent data breaches, in addition to responding to breaches post detection. I have a very detailed understanding of what is and is not a reasonable level of security based on the hundreds of organizations with which I have worked and the various security task forces with which I have been involved.

III. SCOPE OF WORK

23. I have been asked to consider and provide my opinions on the claims of the Challenged Patents, including the technical subject matter and the application of various references that predate the priority date of the Challenged Patents. In particular, I have been asked to consider what one of ordinary skill in the art would have understood from the claims and specification of the Challenged Patents, whether certain references disclose or suggest the features recited in the claims of the Challenged Patents, and whether one of ordinary skill in the art would have had reason to combine certain references to arrive at the claimed subject matter.

24. As I noted previously, my compensation is in no way contingent on the nature of my findings, the presentation of my findings in testimony, or the outcome of any proceeding.

25. My opinions set forth below are based on my education, training, experience, and the content of the references considered.

IV. LEVEL OF ORDINARY SKILL IN THE ART

26. My opinions are provided based on what a person of ordinary skill in the art in the technical field of the inventions of the Challenged Patents would have understood at the time of filing of the Challenged Patents.

27. I have been informed and understand that the content of a patent and prior art should be interpreted the way a person of ordinary skill in the art would have interpreted those references at the time of filing of the patent. I understand that the person of ordinary skill is a hypothetical concept referring to one who understands the technology and associated conventional wisdom at the time.

28. I was asked to provide an opinion as to the level of one of ordinary skill in the art pertinent to the subject matter set forth in the Challenged Patents at the time of the priority date. Around October 2, 2003 (the filing date of provisional patent application 60/507,976), it is my opinion that a person of ordinary skill in the art in the field of the Challenged Patents would have been a person with a Bachelor's degree in computer science, computer engineering, or electrical engineering and at least two years of experience in computer networking, network system security and cybersecurity. Throughout this declaration, I use the term "POSITA" to refer to a person with these or similar qualifications. To have similar qualifications, an individual with additional education or additional industrial experience could still be of ordinary skill in the art if that additional education or experience compensates for a deficit in one of the other aspects of the requirements stated above. The Petitions and Dr. Crovella assert that a POSITA would have a "Bachelor's degree in computer

science, computer engineering, or a related discipline, and 3-4 of experience in computer networking with an emphasis on packet processing systems including traffic monitoring, inspection, and encryption/decryption systems." IPR2023-00673 Petition at 14-15; IPR2023-00703 Petition at 14; Ex. 1003, ¶ 50. While I disagree with the amount of experience they assert is required, I note that, applying their asserted level of skill, my opinions contained herein do not change.

29. The basis for my familiarity with the level of ordinary skill is my interaction with large numbers of workers in the computer security industry who were at this level of skill. In reaching this opinion as to the hypothetical person of ordinary skill in the art, I have considered the types of problems encountered in the art, the prior art solutions to those problems, the rapidity with which innovations are made, the sophistication of the technology, and the educational level and professional capabilities of workers in the field. I further note that, as of October 2, 2003, I was at least at this level of skill.

V. LEGAL PRINCIPLES

A. Anticipation

30. I understand and have been informed that in order for an inventor to be entitled to a patent, the invention must be "new," and the inventor must not have lost

his or her right to a patent by delaying filing of a patent application directed to the invention. There are a number of ways that an invention can be "anticipated"—that is, not new.

31. One such way is when the invention was already patented or described in a printed publication anywhere in the world before the date of invention by the inventor or more than one year before the earliest effective filing date of the patent application. Additionally, a patented invention may not be new if it was on sale or publicly used more than one year before the filing of an application for patent. A patented invention is also not new if it was "known" or used by others in the United States before it was invented by the patent applicants. To invalidate a patent claim based on knowledge, I understand that the knowledge must be accessible to the public. If the subject matter covered by a patent claim is found within the "four corners" of a prior art reference, the claim is said to be anticipated by that reference.

32. A patent claim can be said to be anticipated if each and every limitation of the patent claim is found either expressly or inherently in a single item of prior art. While a prior art reference need not use the same words as a patent claim to anticipate the claim, the prior art reference must describe the requirements of the claim with sufficient clarity such that a POSITA would have been able to make and

use the claimed invention based on the reference and his or her knowledge in the applicable technical field.

33. The disclosure of a feature of a claimed invention can be either "express," meaning that the text, figures, or other content of a reference actually teaches the aspects of the patent claim, or the disclosure can be "inherent." An express disclosure does not need to use the same words as the patent claim being considered and does not need to be depicted in exactly the same way, but the disclosure must actually convey the claimed invention to a POSITA using some combination of words, figures, data, or other portions of the patent. I have been informed and understand that in order to establish that an element of a claim is "inherent" in the disclosure in a prior art reference, it must be clear to a person skilled in the art that the missing element is an inevitable part of what is explicitly described in the reference, and that it would have been recognized as necessarily present by a person skilled in the art. Inherency cannot be established by probabilities or possibilities, and the mere fact that something may result from a given set of circumstances is not enough to establish inherency.

34. Finally, I further understand that to anticipate a claim, the elements of the claim must be found in the prior art reference "arranged as in the claim." I have

been informed that this means that the elements of the prior art reference may not be recombined in a way that is not taught in the prior art to arrive at the invention; instead, the prior art must teach the claimed subject matter in the arrangement required by the claims.

35. I understand that any disclosure that anticipates a claim also renders that claim obvious.

B. Obviousness

36. I have been informed and understand that subject matter claimed in a patent is obvious under 35 U.S.C. § 103 if a person of ordinary skill in the art at the time the alleged invention was made would have had reason to combine or modify the disclosures of one or more prior art references to arrive at the claimed subject matter. A claim may be unpatentable even if each and every claim limitation is not present or disclosed in a single prior art item.

37. I have been informed and understand that, under the doctrine of obviousness, a claim is unpatentable if the differences between the invention and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which the

subject matter pertains. A person of ordinary skill in the art is presumed to have knowledge of the relevant prior art at the time of the claimed invention.

38. I have been informed and understand that obviousness is based on the scope and content of the prior art, the differences between the prior art and the claim, the level of ordinary skill in the art, and secondary indicia of obviousness and non-obviousness to the extent such indicia exist.

39. I have been informed and understand the determination of whether the asserted claims would have been obvious to a person of ordinary skill in the art and, therefore, invalid is not governed by any rigid test or formula. A determination that a claim is obvious is, instead, based on a common-sense determination that the claimed invention is merely a combination of known limitations to achieve predictable results. Any of the following rationales are acceptable justifications to conclude that a claim would have been obvious: (1) the claimed invention is simply a combination of known prior art methods to yield predictable results; (2) the claimed invention is a simple substitution of one known element for another to obtain predictable results; (3) the claimed invention uses known techniques to improve similar devices (methods or products) in the same way; (4) the claimed invention applies a known technique to a known device (method or product) ready

for improvement to yield predictable results; (5) the claimed invention was "obvious to try"—choosing from a finite number of identified, predictable solutions with a reasonable expectation of success; (6) there is known work in one field of endeavor that may prompt variations of it for use in either the same field or a different one based on design incentives or other market forces if the variations would have been predictable to one of ordinary skill in the art; or (7) there is some teaching, suggestion, or motivation in the prior art that would have led one of ordinary skill in the art to modify the prior art reference to combine prior art teachings to arrive at the claimed inventions.

40. I have been informed and understand that a claim may be obvious in light of a single reference, without the need to combine references, if the elements of the claim that are not found in the reference can be supplied by the common sense or knowledge of one of ordinary skill in the art or taught in different areas of the single reference.

41. I have been informed and understand that an analysis of whether a claimed invention is obvious must not rely on a hindsight combination of prior art. The analysis must proceed in the context of the time of the invention or claimed priority date and consider whether the invention as a whole would have been obvious

to a person of ordinary skill in the art, taking into consideration any interrelated teachings of the prior art, the effects of demands known to the design community or present in the marketplace, and the background knowledge possessed by a person having ordinary skill in the art, all in order to determine whether there was an apparent reason to combine any known elements in the fashion claimed by the patent at issue.

VI. ASSERTED PRIOR ART

42. The Petitioner and its expert, Dr. Mark Crovella, have asserted that certain claims of the Challenged Patents are obvious over the combination of two or more of the following prior art references: (1) U.S. Published Patent Application No. 2003/0074473 ("Pham"); (2) U.S. Patent No. 7,424.744 ("Wu"); (3) U.S. Published Patent Application No. 2002/0073316A1 ("Collins"); and (4) U.S. Patent No. 7,996,670 ("Krishna").

43. In both IPRs, the particular combinations that the Petitioner and Dr. Crovella rely on are as follows: (1) in Ground 1, independent claims 1and 13 of the Challenged Patents, as well as dependent claims 2, 9, 10, 11, 12, 16, and 22 of the Challenged Patents, are obvious over the combination of Pham and Wu; (2) in Ground 2, dependent claims 3, 14, and 21 of the Challenged Patents are obvious over

the combination of Pham, Wu, and Collins; (3) in Ground 3, dependent claims 4, 7, and 8 of the Challenged Patents are obvious over the combination of Pham, Wu, Collins, and Krishna; and (4) in Ground 4, dependent claim 17 of the Challenged Patents are obvious over the combination of Pham, Wu, and Krishna.

44. For purposes of this declaration, I restrict my review and analysis to Ground 1 and the independent claims of the Challenged Patents and, consequently, restrict my review to the Pham and Wu references.

A. Pham

45. U.S. Patent Publication No. 2003/0074473 ("Pham") is entitled "SCALABLE NETWORK GATEWAY PROCESSOR ARCHITECTURE." *See* Ex. 1004. Pham was published on April 17, 2003 from application No. 09/976,322 filed on October 12. 2001. *See* Ex. 1004.

46. The Abstract of Pham recites:

> A network data processor system includes a plurality of data packet processors coupled through a data switch fabric between network connection processors. The data packet processors each include a data processing engine configured to perform a data processing function over data contained within predetermined data packets. The network connection processors include network interfaces coupleable to external data transmission networks and provide for the selective routing of said predetermined data packets through said data switch fabric to load balance the processing of the predetermined data packets by the plurality of data packet processors. A network control processor

> is provided to manage the other processors connected to the data switch fabric and to handle predetermined network connection processes. In the preferred embodiments of the present invention the data processing engine is preferably configured to perform hardware encryption and decryption algorithms called for by the IPsec protocol.

Ex. 1004, Abstract.

47. As part of the Field of Invention section, Pham recites that a "general purpose of the present invention is to provide a network component capable of performing compute intensive data packet processing at wire-speeds." Ex. 1004, [0003].

48. In the Description of the Related Art section, Pham describes the problem that comes within ever-increasing speeds in network technologies, and in particular connecting "remote locations and private distributed intranets at wire speed - the maximum fundamental speed of the network connecting any two sites." Ex. 1004, [0006]. Pham notes that the conventional networking equipment is capable of handling these increasing speeds. Ex. 1004, [0006]. ("Network traffic switches and routers are conventionally designed to operate at wire-speeds."). Pham then describes that the issue associated with the increasing speeds is the ability to handle computationally intensive tasks. Ex. 1004, [0007]. Pham further describes the computationally intensive tasks can include virtual private network ("VPN")

functions, secure socket layer ("SSL") functions, and packet protocol conversion functions. Ex. 1004, [0008]. Focusing on VPN function, Pham further notes the associated encryption and decryption operations are compute intensive and are typically isolated on hardware-based accelerators "to support bandwidths that are any significant fraction of a gigabit Ethernet connection." Ex. 1004, [0008]; see also Ex. 1004, [0010] ("[C]onventional network components capable of any significant in-band compute intensive processing of high-throughput rate packet data are incapable of achieving gigabit wire-speed performance ... the aggregate throughput … conventionally fall well below one Gbps and run more typically in the range of 250 to 400 Mbps. Such rates clearly fail to qualify as wire-speed in current network infrastructures.").

49. Pham consequently seeks to provide "a network component capable of performing compute intensive data packet processing at wire-speeds." Pham at [0012]. To accomplish this goal, Pham describes an array of data packet processors coupled via a switch fabric to the network processors (that provide the external component connections and can select the data packet processors based on load balancing):

> This is achieved in the present invention by a network data processor system having a plurality of data packet processors coupled through a

> data switch fabric between network connection processors. The data packet processors each include a data processing engine configured to perform a data processing function over data contained within predetermined data packets. The network connection processors include network interfaces coupleable to external data transmission networks and provide for the selective routing of said predetermined data packets through said data switch fabric to load balance the processing of the predetermined data packets by the plurality of data packet processors. A network control processor is provided to manage the other processors connected to the data switch fabric and to handle predetermined network connection processes. In the preferred embodiments of the present invention the data processing engine is preferably configured to perform hardware encryption and decryption algorithms called for by the IPsec protocol.
>
> Ex. 1004, [0013].

50. Pham describes that the benefit of this approach is that the aggregated processing capability of the data packet processors can match the wire-speeds of the network processors:

> Thus, an advantage of the present invention is that computation-intensive protocol processing functions can be effectively distributed over a scalable array of data processing engines configured for the specific data processing function desired. The network connection processors manage a dynamically load balanced transfer of data to and through the data processing engines by way of a high-speed switch fabric, thereby efficiently aggregating the available bandwidth of the data processing engines. Consequently, the network data processor system of the present invention is capable of operating at or above gigabit wire-speeds utilizing only a small array of network data processors and, further, readily scaling to multiple gigabit throughput levels by, at a minimum, merely expanding the array of network data processors.

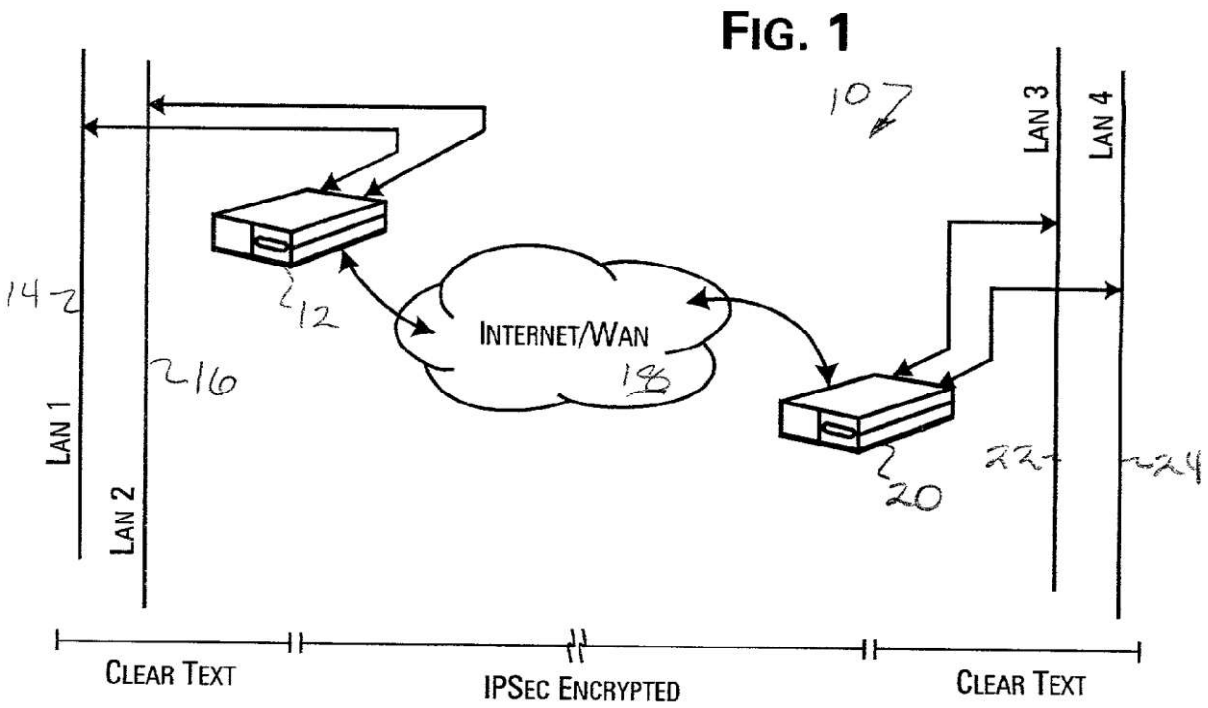
Ex. 1004, [0014].

51. Pham also describes the further benefit of "a comprehensive and centrally manageable protocol processing network gateway." Ex. 1004, [0015]. To that end, Pham describes a "VPN Gateway Switch" to handle switching/routing functionality between multiple local area networks ("LANs") and routing functionality from the LANs to a wide area network ("WAN") as part of a virtual private network ("VPN"):

> An exemplary virtual private network (VPN) application 10 of the present invention is generally shown in FIG. 1. A VPN gateway 12, constructed and operating in accordance with a preferred embodiment of the present invention, connects data packet traffic from one or more local area networks (LANs) 14, 16 through the public Internet 18. A second VPN gateway 20, also constructed and operating in accordance with a preferred embodiment of the present invention, connects data packet traffic between the Internet 18 and other LANs 22, 24. The VPN gateways 12, 20 operate to convert data conveyed by the data packets transferred through the gateways 12, 20 between clear and encrypted text, preferably consistent with the in-band encryption protocols of the IPsec standard.

Ex. 1004, [0037]; see also Ex. 1004, [0036] ("Basic operations, such as performed by network data packet switches, can easily be performed at wire-speed, here defined as the maximum bandwidth of the directly connected network."). "FIG. 1 is an illustration of networking environment utilizing network gateway switches

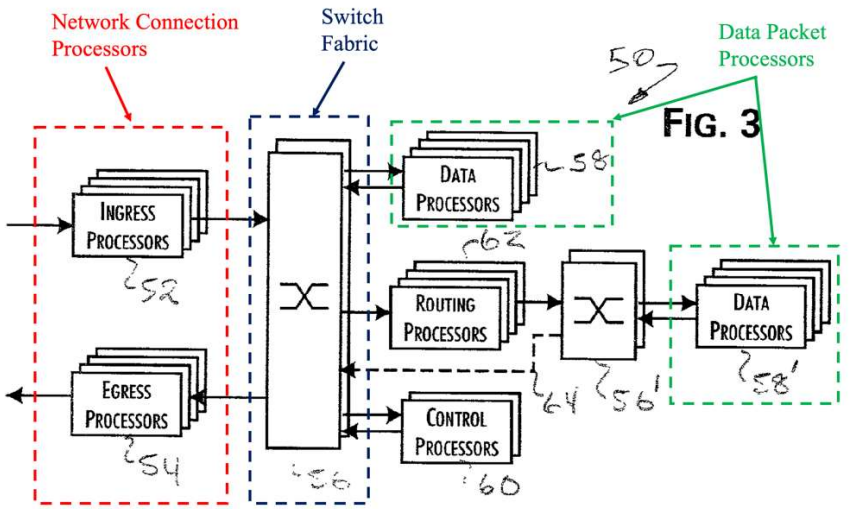
in accordance with a preferred embodiment of the present invention." Ex. 1004, [0019].



Ex. 1004, Fig. 1 (illustrating multiple LANs connected to each VPN network gateway 12).

52. As part of the proposed system, Pham proposes to segregate the compute-intensive packet operations from the network operations and interconnect. "This is achieved in the present invention by a network data processor system having a plurality of data packet processors coupled through a data switch fabric between

network connection processors." Ex. 1004, [0013]; *see also* Ex. 1004, Figs. 3 & 4 (reproduced and annotated below):



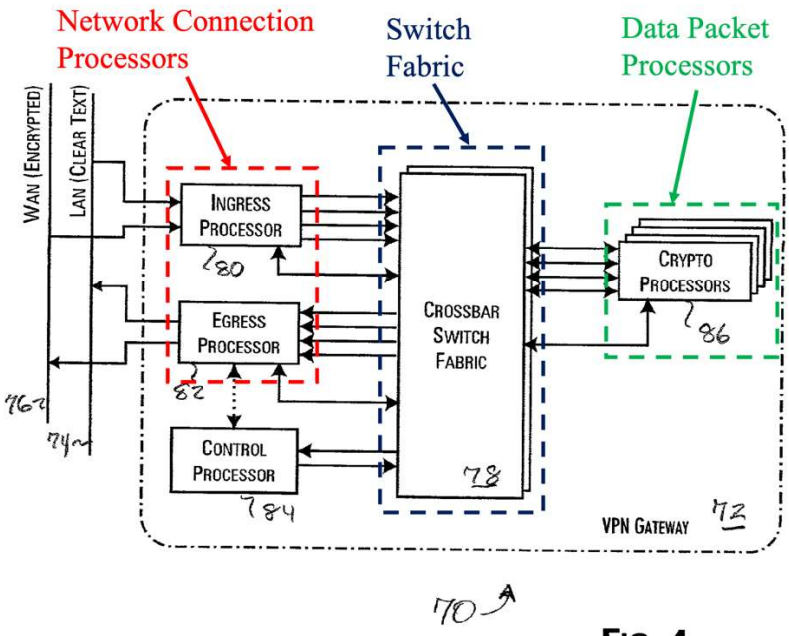


FIG. 4

53. As set forth in greater detail below, the network connection processors of Pham are responsible for (i) network switching (i.e., LAN-to-LAN packet switching); (ii) filtering of packets for computationally intensive processing; and (iii) identifying routing connections for VPN traffic through the WAN. Even though the network connection processors are of universal design, *see* Ex. 1004, Fig. 5, [0023], Pham further categorizes them as either ingress processors or egress processors. In either instance, the network connection processors can send or receive packets from/to the external network connections (LAN or WAN) and send or receive packets from/to the crossbar switch. *See* Ex. 1004, Fig. 5 (reproduced below and annotated); *see also* Ex. 1004, [0038] ("[N]etwork ingress and egress processors 30, 32, 34, 36 providing a bidirectional connection between a local LAN 38 and a wide area network (WAN), such as the Internet 18. These ingress and egress processors 30, 32, 34, 36 are interconnect through a switch fabric 40 to data packet processors 42, 44 …")

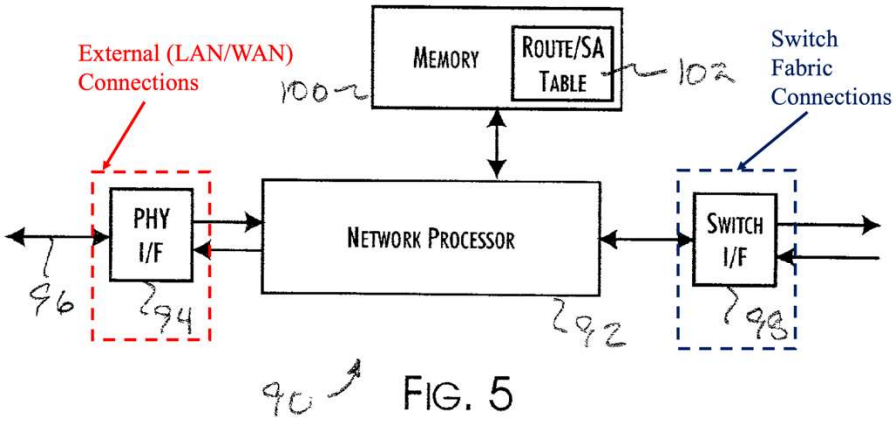


FIG. 5

Ex. 1004, Fig. 5; *see also* Ex. 1004, [0023] ("FIG. 5 provides a block diagram of an ingress/egress network processor module constructed in accordance with a preferred embodiment of the present invention"), [0049] ("While the detailed function of the ingress and egress processors 80, 82 is somewhat different, the processors 80, 82 utilize substantially the same communications processor 90 implementation, as shown in FIG. 5.")

54. Pham further describes how the ingress processors can determine where to pass a packet to through the switch fabric, either to a data packet processor when encryption or decryption is required or to an egress processor when data pocket processing is not required, e.g., when passing "clear text" packets from LAN to LAN:

> Fast path routing is selected for those network data packets that are recognized by the ingress processors 30, 34 as belonging to a previously

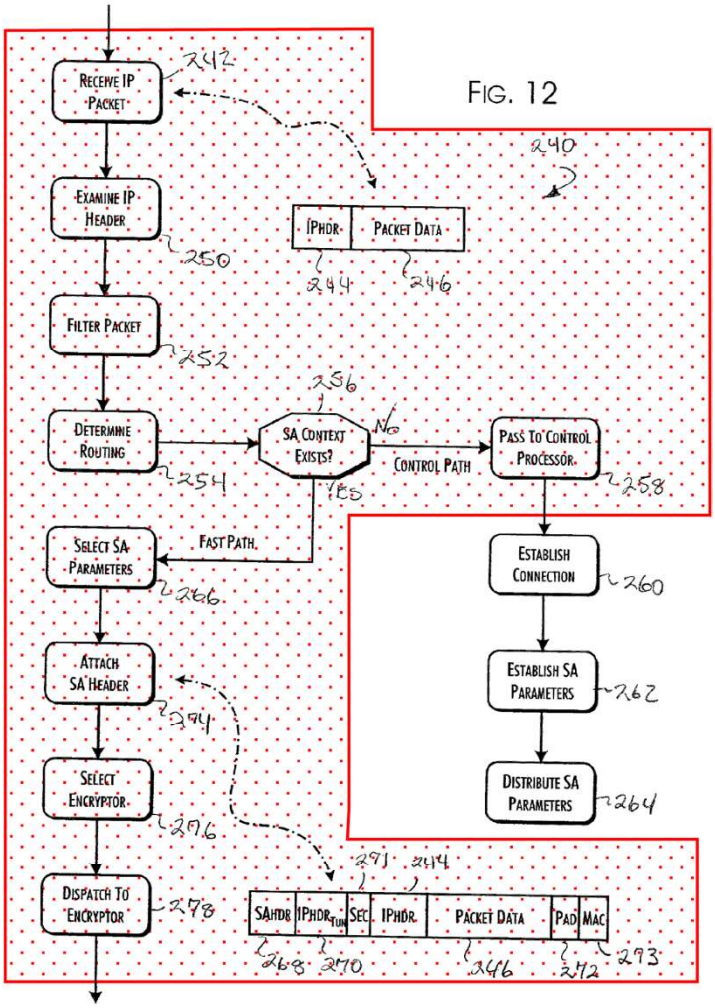
> established network connection. In the preferred embodiments of the present invention, *the further choice of fast path routing of data packets is determined by the type of data packet processing required, such as data encryption or decryption*, and the relative availability of the data packet processors 42, 44 to receive and process data packets. In particular, ***packets not requiring processing through the data packet processors 42, 44 are bypassed between the ingress and egress processors*** 30, 32, 34, 36."

Ex. 1004, [0040] (emphasis added); *see also* Ex. 1004, [0049] (describing "a programmable processor with hardware support for Layer 2 and 3 network packet processing, filtering and routing operations at effective throughputs of up to 4 Gbps"). In Pham, only the "packets forwarded from the LAN 38 through the VPN gateway 12" are "subject to the VPN encryption protection." Ex. 1004, [0041]. These packets "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." Ex. 1004, [0041].

55. "Multiple ingress processors 52 and egress processors 54 can be provided as part of the architecture 50 to support aggregation of network data traffic from multiple LANs through a single gateway device. This also allows the ingress and egress processors 52, 54 to extend the functionality of the architecture 50 to include data compression, network data traffic switching and routing, and other

compute intensive packet processing operations on a single gateway device implementing the architecture 50." Ex. 1004, [0042].

56. "FIG. 12 provides a flow diagram describing the network packet processing operation 240 of an ingress processor 80 for network data packets received from a clear text network in accordance with a preferred embodiment of the present invention. An ordinary network data packet, as received 242, includes a conventional IP header 244 and data packet payload 246. The IP header is examined 250 to discriminate and filter out 252 data packets that are not to be passed through the VPN gateway 72." Ex. 1004, [0069]; see Ex. 1004, Fig. 12:



Ex. 1004, Fig. 12 (annotated to highlight steps performed by ingress processor)

57. With respect to Fig. 12, Pham describes the steps taken by the ingress processor:

- Receiving the IP Packet at step 242, Ex. 1004, [0069];

- The IP Header is examined at step 250 "to discriminate and filter out 252 data packets that are not to be passed through the VPN gateway," Ex. 1004, [0069];

- Filtered out packets will bypass packet processing and be passed through the switch fabric to an egress processor, *see* Ex. 1004, [0040]. These packets do not require the addition or attachment of additional fields or information, as compared to the packets to be encrypted which require the attachment of SA parameter data;

- At step 254, a routing connection is identified for data packets that are to be passed through the VPN gateway, *see* Ex. 1004, [0069], and, at step 256, a determination is made as to whether a secure authority (SA) context exists in the ingress processor's data table, *see* Ex. 1004, [0069];

- "Where a SA context is found 256 in the data table 102 by an ingress processor 80, fast path processing is selected. The relevant SA parameters are retrieved 266 from the SA context store and formatted into a SA header 268. A tunneling IP header 270, IPsec control fields 271, padding field 272, and Message Authentication Code (MAC) field 273 are also created. These fields are then attached 274 to the network data packet." Ex. 1004, [0071].

- At step 276, the destination data packet processor or crypto processor is selected using the load-balancing algorithm running on the ingress processor, *see* Ex. 1004, [0071]. The network data packet and attachments are then passed to the selected data packet processor or crypto processor via the switch fabric, *see* Ex. 1004, [0071].

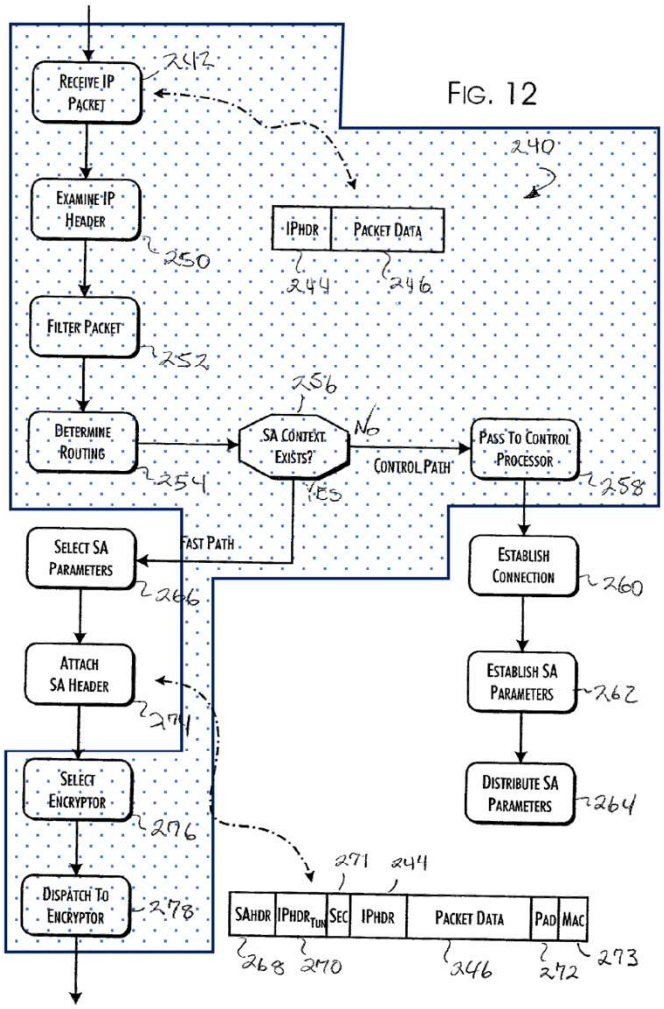
- Where a SA content is not found in the data table, the ingress processor passes the packet to the control processor for negotiation of an IPsec connection, *see* Ex. 1004, [0070]. When the SA parameters for the connection are authenticated, the control processor will update the data tables in the ingress processors with the routing and SA parameter context information, *see* Ex. 1004, [0070].

58. Pham also describes, as an alternate embodiment, a scenario where the SA parameter data is also stored in the memory associated with the network processor of the data packet processor / crypto processor. *See* Ex. 1004, [0051]. In this alternate embodiment, Pham describes that only "the SA parameter association task is off-loaded from the ingress processors 80 and performed by the crypto processors 86." Ex. 1004, [0051]. Pham describes the reason for off-loading of this task from the ingress processor, which still maintains its basic switching and filtering functions:

> "With substantially increasing wire-speed, the computational capabilities of the ingress processors 52 may become insufficient to timely perform all of the required filtering, routing and load-balancing functions. Thus, at wire-speeds in excess of about 20 Gbps, ***limiting the computational responsibilities of the ingress processors 52 to basic switching and filtering network data packets*** may be preferred."
>
> Ex. 1004, [0043] (emphasis added).

59. As to the "basic switching and filtering" functions of the ingress processor that will be maintained in the alternate embodiment, a POSITA would readily recognize the ingress processor steps, as shown in Fig. 12, that must be maintained for operation of Pham's VPN gateway switch. Below I provide another annotated version of Fig. 12 to illustrate the steps, consistent with Pham's

description in [0051] about only the SA parameter association task being off-loaded, that must be maintained by the ingress processor:



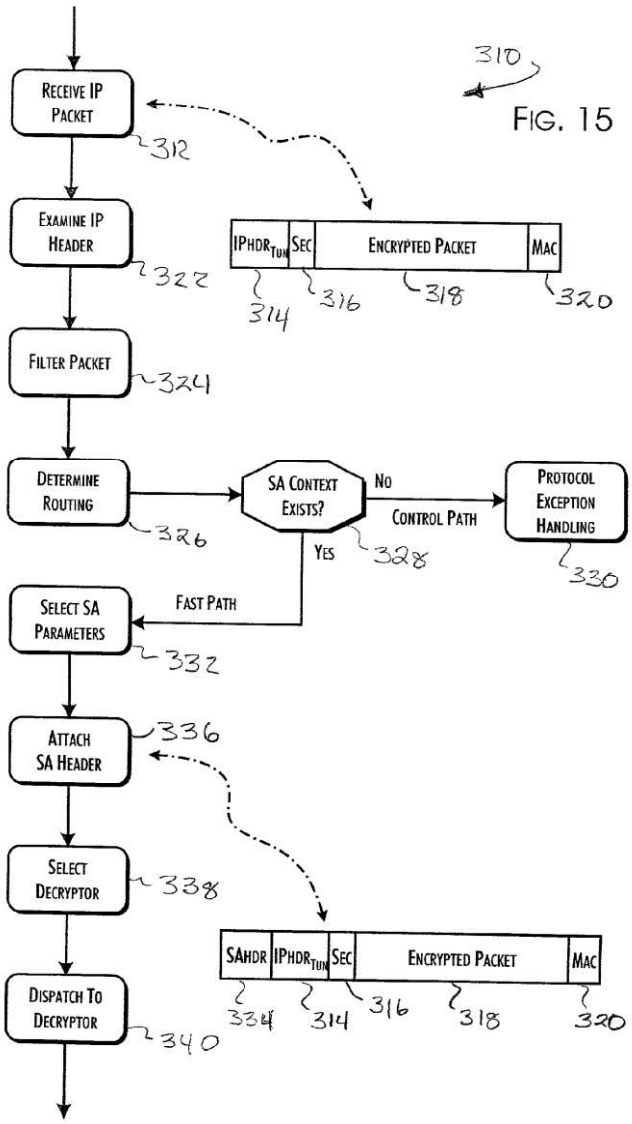
Ex. 1004, Fig. 12 (annotated to highlight steps performed by ingress processor in alternate embodiment)

60. With respect to Fig. 12 and the alternate embodiment, the ingress processor of Pham must take the steps of:

- Receiving the IP Packet at step 242, Ex. 1004, [0069];
- Examining the IP Header at step 250 to filter out packets that are not going to be passed through the VPN gateway and, therefore, do not need to be passed to a data packet processor / crypto processor;
- Passing filtered out packets through the switch fabric to an egress processor. These packets do not require the addition or attachment of additional fields or information, as compared to the packets to be encrypted which require the attachment of SA parameter data;
- Identifying a routing connection at step 254 and whether a SA context exists at step 256 for data packets that are to be passed through the VPN gateway. The ingress processor must make this identification in order to take the appropriate next step of passing the network data packet to a data packet processor / crypto processor (for "fast path processing" of known VPN connections) or the control processor (to setup the appropriate VPN connection). To the extent the Petitioner argues that all packets after filtering can be passed to a data packet processor / crypto processor for these determinations, I do not find such an approach feasible because the load balancing algorithm is dependent upon the estimated completion time for each crypto processor. *See* Ex. 1004, [0060]. The estimated completion time is based on the size of the packet and the identity of the crypto processor, *see* Ex. 1004, [0061]; *see also* Ex. 1004, [0067]. If the data packet processor / crypto processor needs to send a packet to the control processor to establish a connection, it becomes impossible for the ingress processor to reliably estimate the completion time, causing the load-balancing algorithm to destabilize.
- For packets with a known SA context, selecting a data packet processor / crypto processor at step 276 using the load-balancing algorithm running on the ingress processor and sending the network data packet to the selected data packet processor / crypto processor at step 278;

- For packets without a known SA context passing the packet to the control processor for negotiation of an IPsec connection.

61. Pham also describes, with respect to Fig. 15 (reproduced below), the operational flow for an ingress processor that receives a network data packet from the WAN. Notably, this operation flow includes a filtering step 324. Similar to the ingress processor operation on the LAN side, a POSITA would understand this filtering step to apply to identify "clear text" packets such as non-encrypted IPsec control plane communications between the control processors. *See* Ex. 1004, [0048] ("In-band communications with external network connected devices, such as for network protocol negotiations, is accomplished by utilizing the ingress and egress processors 80, 82 as simple network access ports.").



Ex. 1004, Fig. 15.

B. <u>Wu</u>

62. U.S. Patent No. 7,424,744 ("Wu") is entitled "SIGNATURE BASED NETWORKINTRUSION DETECTION SYSTEM AND METHOD." *See* Ex.

1005. Wu issued on September 9, 2008 from application No. 10/992,179 filed on March 5,2002. *See* Ex. 1005.

63. The Summary of Invention section of Wu recites:

> A signature based intrusion detection method and system are disclosed. A method for detecting intrusions on a network generally comprises storing signature profiles identifying patterns associated with network intrusions in a signature database and generating 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, 2:39-48.

64. The Summary of Invention section of Wu further recites:

> An intrusion detection system of the present invention generally comprises a signature classifier having a first stage classifier operable to classify packets according to at least one packet field into groups and a second stage classifier operable to classify the packets within each of the groups according to packet type or size. A signature database is provided for storing signature profiles identifying patterns associated with network intrusions. The system further includes a flow table configured to support table lookups of actions associated with classified packets and a signature engine operable to perform a table lookup at the flow table to select an action to be performed on the packet based on its classification. One of the actions is comparing the packets to at least a subset of the signature profiles.
>
> In another aspect of the invention, a computer program product for detecting intrusions on a network generally comprises code that stores signature profiles identifying patterns associated with network intrusions in a signature database, code that generates classification rules based on the signature profiles, code that receives packets

> transmitted on the network, code that classifies the packets according to at least one packet field into groups, code that classifies the packets within each of the groups according to packet type or size, and code that performs a table lookup to select an action to be performed on the packet based on its classification. One of the actions is comparing the packets to at least a subset of the signature profiles. A computer-readable storage medium is provided for storing the codes.

Ex. 1005, 2:49-3:9.

VII. OVERVIEW OF THE CHALLENGED PATENTS

A. Assumed Effective Filing and Invention Dates

65. The '436 Patent is entitled "System and method for a secure I/O interface" and was filed on July 30, 2004. *See* Ex. 1001. The '436 Patent claims priority to provisional patent application No. 60/507,976 that was filed on October 2, 2003. *See* Ex. 1001. The '612 Patent is also entitled "System and method for a secure I/O interface" and was filed on January 29, 2010 as a continuation of the application that led to the '436 Patent. *See* Ex. 1012. The '612 Patent claims priority to provisional patent application No. 60/507,976. *See* Ex. 1012. Consistent with Dr. Crovella, *see* Ex. 1003, ¶ 49, I assume the priority date for the Challenged Patents is the filing date of the provisional patent application, October 2, 2003.

B. The Challenged Patents

66. As noted in the Background of the Invention section of the Challenged Patents, trusted internal computer networks are usually protected by external

computer networks or systems with individual firewalls and methods. *See* Ex. 1001, 1:24-26; Ex. 1012, 1:24-26. Computer networks often rely on similar systems to provide more protection. However, as the number of systems attached to the computer network increases, vulnerability increases proportionally. Further, using the firewalls, processing, and security functionalities of external systems, each designed and manufactured by different organizations and methods, lead to unoptimized performance, unnecessarily draining resources and creating redundancies that lack any true purpose, as well as openings and vulnerabilities to potential bad actors. As a result, the use of different systems to perform different portions of security and network processing is both inefficient and more vulnerable as a whole to attacks and exploitations.

67. Usually, the end-users are primarily concerned with the speed and relative- security at which communication are transmitted to and from the trusted computer. "However, providing firewall, network processing and security functionalities in different systems, which are often made by different manufacturers, provides increased opportunities for snooping or other techniques that may permit an unauthorized person to gain access to ongoing communications or to discover key or other security data when it is exchanged between subsystems.

For example, if certain security functions associated with securing communications over a NIC are handled by the computer's host processor and/or by other computers on the internal network, then the communications may be more easily attacked or otherwise accessed or interfered with by an unauthorized person, who may attempt to exploit easier snooping access or other vulnerabilities presented by the processing of security functions by a host processor or another server on the network." Ex. 1001, 1:46-60; Ex. 1012, 1:46-60. "Network interface cards (NIC) often provide a computer's physical connection to its trusted internal network. More specifically, a NIC connects a personal computer, server or workstation to a local area network (LAN) and has two primary interfaces: the network interface and the host bus interface. NICs are typically low-cost ASIC-based products designed for simple buffering and data transfer." Ex. 1001, 1:37-43; Ex. 1012, 1:37-43.

68. "The use of different systems to perform different portions of security and network processing also requires additional processing and interfaces for coordinating communications processing between the systems. Such additional processing and interfaces increase processing demands, which limits communication speed and increases the size of the chips and systems necessary to implement secure communications." Ex. 1001, 1:61-67; Ex. 1012, 1:61-67.

69. The industry standard process leads to encryption and decryption vulnerabilities when an internal network relies on an external and foreign system to handle encryption and decryption services. When connected to the "backplane bus of a host" and "using external security processors and I/O cards," "input encrypted data is typically transferred using Direct Memory Access (DMA) from the I/O card," and then by DMA to the security processor. Ex. 1001, 2:1-7; Ex. 1012, 2:1-7. After decryption, a "key is generated," and "data is transferred by DMA … to memory," and "then to the I/O card for output to another destination." Ex. 1001, 2:8-11 Ex. 1012, 2:8-11. As a result of the network relying on external systems, as shown in this example, the transfer process takes longer and is significantly more vulnerable to attacks during the process due to more openings, as well as bottlenecking the backplane bus. *See* Ex. 1001, 2:11-14 Ex. 1012, 2:11-14.

70. In order to reduce potential redundancies and security issues posed by using external systems for protection and processing, the Challenged Patents describe a system and method which may improve the security, speed, and efficiency of communications between trusted hardware, reduce the number of required systems, and reduce vulnerabilities to bad actors. *See* Ex. 1001, 2:20-26 Ex. 1012, 2:20-26.

71. Having a security processor perform all or substantially all security and network processing to provide a secure I/O interface directly reduces the dependency of a network on external, unprotected, and inefficient processing commonly plaguing the industry during the time period prior to October, 2003. In addition, the system and method proposed by the Challenged Patents reduce the bottleneck existing around the backplane bus by the inclusion of a packet engine connected to the local data bus. Further, the Challenged Patents' use of a cryptographic core provides the system an internal and faster method of encrypting and decrypting data without the need of an external processor, which greatly mitigates the vulnerability associated with the industry standard process. The Challenged Patents also leave room for further optimization with the inclusion of the modulo engine connected to the local data bus.

72. The Challenged Patents resolve the known issues within the field and improve the speed and security at which communications are transmitted. More specifically, the Challenged Patents recite:

> The secure I/O system of the present invention permits performing all or substantially all network processing functions and off-loads all or substantially all security functions associated with network address translation (NAT), the providing of a firewall, intrusion detection/ protection system functionality, traffic proxying, and encryption from

a host or network process or onto a single system or card, for example a NIC.

Ex. 1001, 3:43-50; Ex. 1012, 3:43-50.

73. As further described in the Challenged Patents, the "security processor performs all or substantially all … network processing to provide a secure I/O interface system to protect computing hardware from unauthorized access or attack." Ex. 1001, Abstract; Ex. 1012, Abstract. "The security processing performed by the secure I/O system typically may include encryption, decryption, signing and verification of packets at, for example, 100 megabits per second full duplex and greater speeds." Ex. 1001, 3:52-55; Ex. 1012, 3:52-55. "The security processor sends and receives all incoming and outgoing data packets for a host device and includes a packet engine, coupled to a local data bus, to process the incoming and outgoing packets. The processor further comprises a cryptographic core coupled to the packet engine to provide encryption and decryption processing for packets processed by the packet engine. The packet engine also handles classification processing for the incoming and outgoing packets." Ex. 1001, Abstract; Ex. 1012, Abstract. The secure I/O system of the Challenged Patents may be on single system or card, such as a Network Interface Card (NIC), or certain selected networking and/or security functions may be handled by other processors such as, for example,

a host processor. Ex. 1001, 3:48-51; 4:59-61; 5:36-39; Ex. 1012, 3:48-51; 4:59-61; 5:36-39

74. Additionally, the security processor "may consolidate processing of discrete or consolidated security functions and maintain relationships and integrity of the stored security context and other information in memories." Ex. 1001, 4:6-9; Ex. 1012, 4:6-9. The Challenged Patents describe how the memories can "store, for example, cryptographic keys and other data used in security functions by the security processor," Ex. 1001, 4:11-13; Ex. 1012, 4:11-13, and "also store security associations and connection entries used in maintaining multiple security sessions with other computers," Ex. 1001, 4:13-15; Ex. 1012, 4:13-15. The memories may also be "used to buffer inbound and outbound data packets awaiting security processing by the security processor." Ex. 1001, 4:16-17; Ex. 1012, 4:16-17. The security processing system also "is preferably contained within a cryptographic boundary" and "provides a secure I/O interface for computing and communications hardware." Ex. 1001, 4:20-22; Ex. 1012, 4:20-22. Such a boundary "preferably complies with Federal Information Processing Standards Publication" issued in 2001 by the National Institute of Standards and Technology (NIST). Ex. 1001, 4:24-26; Ex. 1012, 4:24-26.

75. Additionally, the security processing systems may be coupled to an internal network and to an external network by the I/O interface. *See* Ex. 1001, 4:29-31; Ex. 1012, 4:29-31. Such interfaces "may perform physical (PHY) layer processing to convert a digital bit stream to or from an analog or photonic signal for transmission over a physical medium such as, e.g., copper wire pairs, co-axial cable, fiber or air." Ex. 1001, 4:31-35; Ex. 1012, 4:31-35. "By routing all or substantially all I/O to and from a host processor 130 and/or internal network 116 through [the] security processing system, [the] host processor 130 and internal network 116 are substantially protected against unauthorized access or other security breaches, [thereby] protecting the security information integrity, and providing processing and storage efficiency from information consolidation." Ex. 1001, 4:40-47; Ex. 1012, 4:40-47. *See* Ex. 1001, Fig. 1; Ex. 1012, Fig. 1:

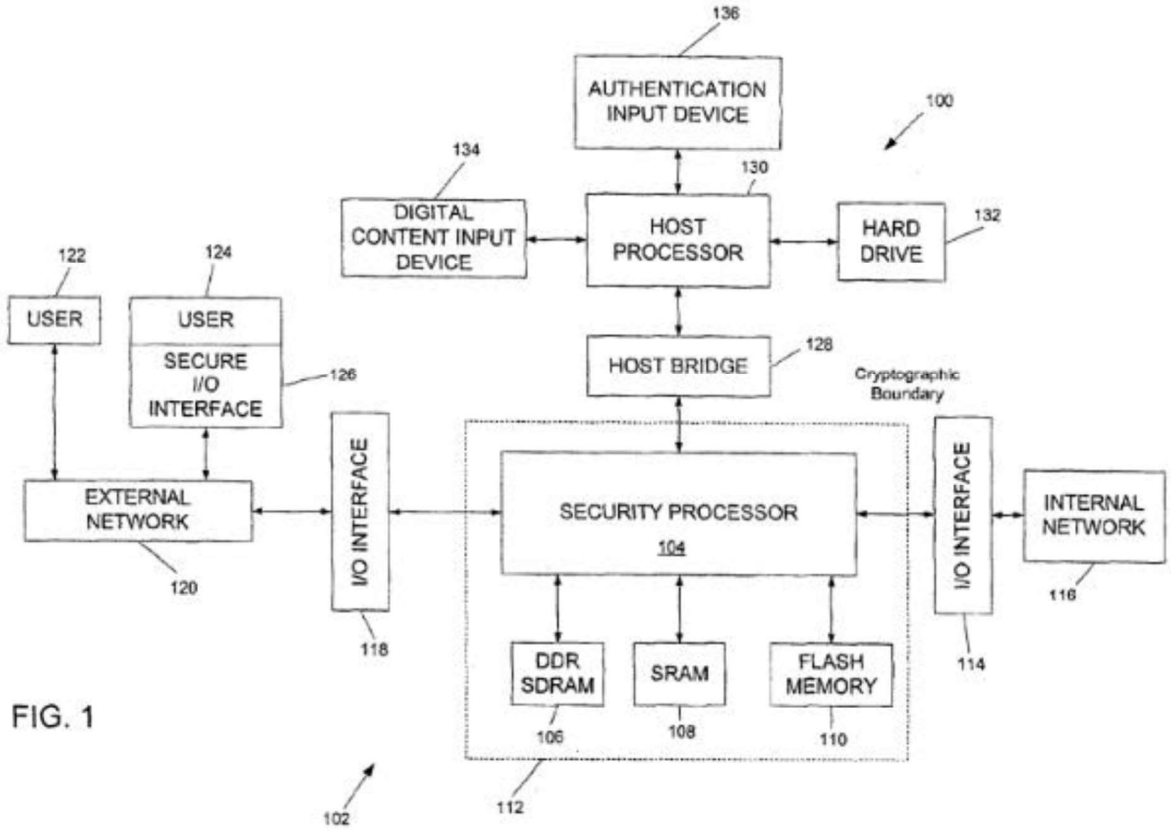


FIG. 1

See also Ex. 1001, Fig. 2; Ex. 1012, Fig. 2:

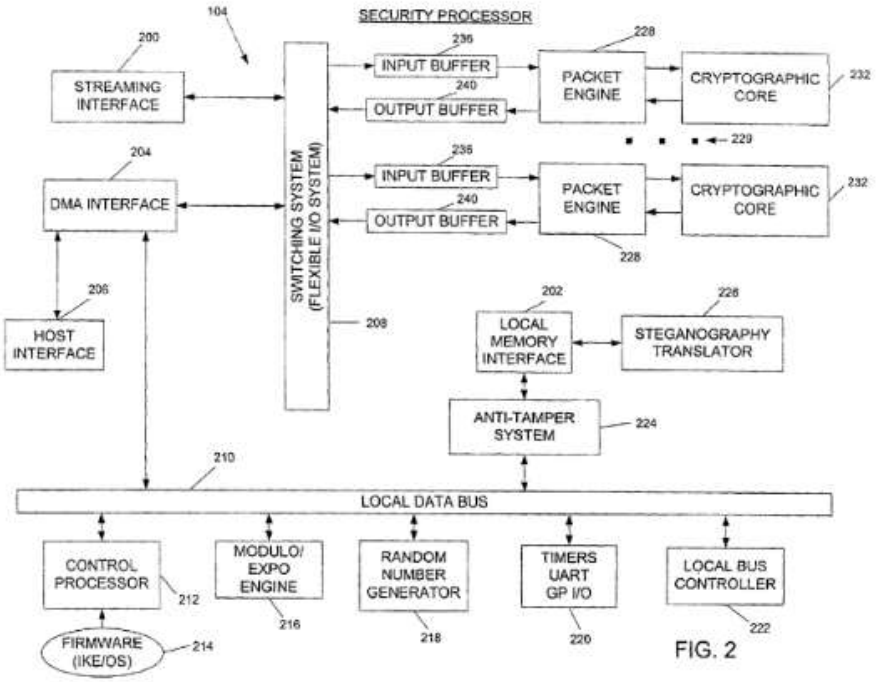
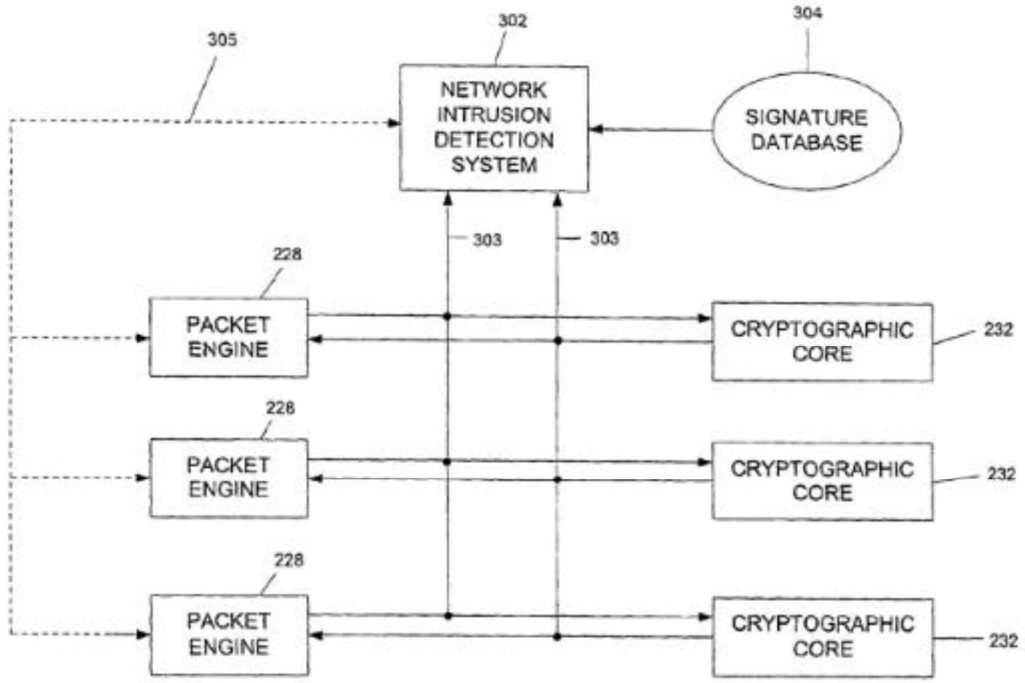


FIG. 2

See also Ex. 1001, Fig. 3; Ex. 1012, Fig. 3:



76. As shown in Fig. 3, above, the Challenged Patents also describe an intrusion detection system that has "taps … couple[d] to the input/output each of packet engine 228 and cryptographic core 232 pair." Ex. 1001, 18:41-43; Ex. 1012, 18:33-35. "[B]y passing all I/O traffic to host processor 130 and/or internal network 116 through security processing system 102, and including NIDS 302 within system 102, undesirable intrusions may be detected in-line with such I/O traffic … [b]y being in-line in this manner, intrusions identified by NIDS 302 may be stopped in the I/O traffic flow" Ex. 1001, 18:48-55; Ex. 1012, 18:40-47. As part of intrusion detection, a "signature database" of "a defined set of patterns" is maintained in

memory, *see* Ex. 1001, 18:43-45; Ex. 1012, 18:35-37, and signature matching is performed on clear text packets "either before or after encryption, depending on whether the packets are inbound or outbound," *see* Ex. 1001, 19:5-9; Ex. 1012, 18:64-19:1.

C. General Discussion of the Asserted Patents and the Prior Art

77. Pham consists of a network data processor system that includes a plurality of data packet processors coupled through a data switch fabric between network connection processors. The network data processor is preferably configured to perform hardware encryption and decryption algorithms called for by the IPsec protocol. *See* ¶¶ 49, 51, above.

78. Pham also describes the data packet processors as each including a data processing engine configured to perform a data processing function over data contained within predetermined data packets. *See* ¶¶ 46, 49, 52-54, 56, 57, 60, 61, above. Additionally, the network connection processors include network interfaces coupleable to external data transmission networks and provide for the selective routing of said predetermined data packets through said data switch fabric to load balance the processing of the predetermined data packets by the plurality of data packet processors. Furthermore, a network control processor is provided to manage

the other processors connected to the data switch fabric and to handle predetermined network connection processes. *See* ¶¶ 46, 49, 57, 60, 61, above.

79. The Challenged Patents substantially differ from Pham in that they are not merely adding data processing capabilities to a known network gateway switch architecture, but are directed to a security processor with packet engines that perform network processing on "substantially all" of the packets that transit the security processor.

80. Pham describes adding multiple data processing engines to a switch, where the data processing engines are exclusively configured to handle data packets requiring compute intensive processing, for example hardware encryption and decryption algorithms called for by the IPsec protocol, whereas the Challenged Patents describe and claim a security processor with packet engines processing "substantially all" of the packets that transit the security processor, with cryptographic cores tightly coupled to the packet engines.

81. The Challenged Patents make improvements over the prior art, such as Pham, by combining security and network processing into a single, tightly integrated unit. Previously, the use of different systems to perform different portions of security and network processing required additional processing and interfaces for

coordinating communications between the systems, which resulted in increasing processing demands. The increased demand in turn resulted in limited communication speeds and increases in the size of chips and systems necessary to implement secure communications.

82. Pham is primarily concerned with the processing speed of compute intensive data packets, whereas the Challenged Patents improve the security of the system, consolidates the resources needed for communications and thereby also increases the speed at which the communications are received and sent. As part of the improvement, the Challenged Patents claim a security processor with packet engines where "substantially all of the incoming packets and outgoing packets to the security processor transit one of the plurality of packet engines," whereas Pham, as noted in ¶ 80, above, describes data packet processors that handle only *predetermined* network data packets, i.e., those data packets requiring compute intensive processing. More specifically, in Pham's VPN Gateway Switch, which handles LAN switching and WAN VPN routing functionality, the basic LAN switching functions (that are not compute intensive) do not reside on the data packet processors. *See* ¶¶ 53-60, above.

83. Additionally, the Challenged Patents describe and claim an integrated intrusion detection system. Because Pham does not disclose any intrusion detection functionality the Petition proposes the combination of a Pham with Wu because Wu describes a signature based intrusion detection method and system. Wu is primarily concerned with detecting intrusions by storing signature profiles and having classification rules that correspond to data packets being transmitted over a network. The signature profiles identifying patterns associated with network intrusions are stored in a signature database and classification rules are generated based on the signature profiles. Data packets transmitted on the network and having corresponding classification rules are classified according to generated classification rules.

84. The Petition and Dr. Crovella propose combining Pham and Wu such that Wu's intrusion detection functionality is integrated into the data packet processor of Pham. *See* IPR2023-00673 Petition at 53; IPR2023-00703 Petition at 48; Ex. 1003, ¶ 107. As set forth in detail below, a POSITA would not be motivated to make this proposed combination because the combination does not address the Pham's VPN Gateway Switch greatest vulnerability from unencrypted packets arriving on the WAN interface.

VIII. PHAM DOES NOT DISCLOSE THAT "SUBSTANTIALLY ALL OF THE … PACKETS … TO THE SECURITY PROCESSOR TRANSIT ONE OF THE PLURALITY OF PACKET ENGINES

85. Each of independent claims 1 and 13 of the '436 Patent requires that "substantially all of the incoming packets and outgoing packets to the security processor transit one of the plurality of packet engines." *See* Ex. 1001, 24:19-21 ('436 Patent, Cl. 1); Ex. 1001, 25:20-22 ('436 Patent, Cl. 13). Similarly, each of independent claims 1 and 13 of the '612 Patent requires that "substantially all of the incoming and outgoing packets to the security processor transit one of the plurality of packet engines." *See* Ex. 1012, 20:63-65 ('612 Patent, Cl. 1); Ex. 1012, 21:59-61 ('612 Patent, Cl. 13).[1]

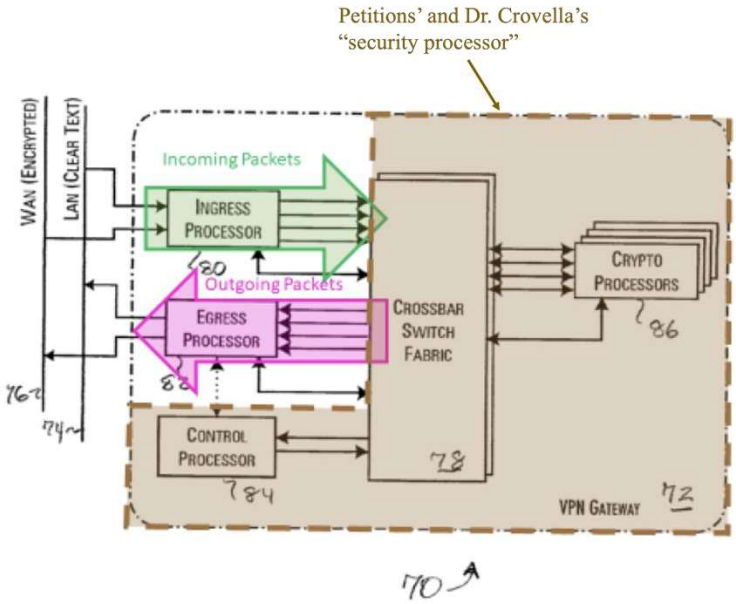
86. As noted above, in ¶ 77, the network processing engine of Pham's data packet processor / crypto processor, upon which the Petitions and Dr. Crovella rely to show that the "packet engine" limitation of independent claims 1 and 13 of the Challenged Patents is met, only operate on *predetermined* data packets. *See also* ¶¶ 46, 49, 52-54, 56, 57, 60, 61, above. Those *predetermined* data packets are network data packets that will be encrypted according to the IPsec protocol for

---

[1] As Dr. Crovella did, *see* Ex. 1003, ¶ 48, I have interpreted this limitation under its plain and ordinary meaning.

transmission across the WAN. Because the network processing engine of Pham's data packet processor / crypto processor does not see substantially all of the data packets "to the security processor," Pham cannot satisfy the claim requirement that "substantially all of the … packets to the security processor transit one of the plurality of packet engines." I will explain in greater detail below.

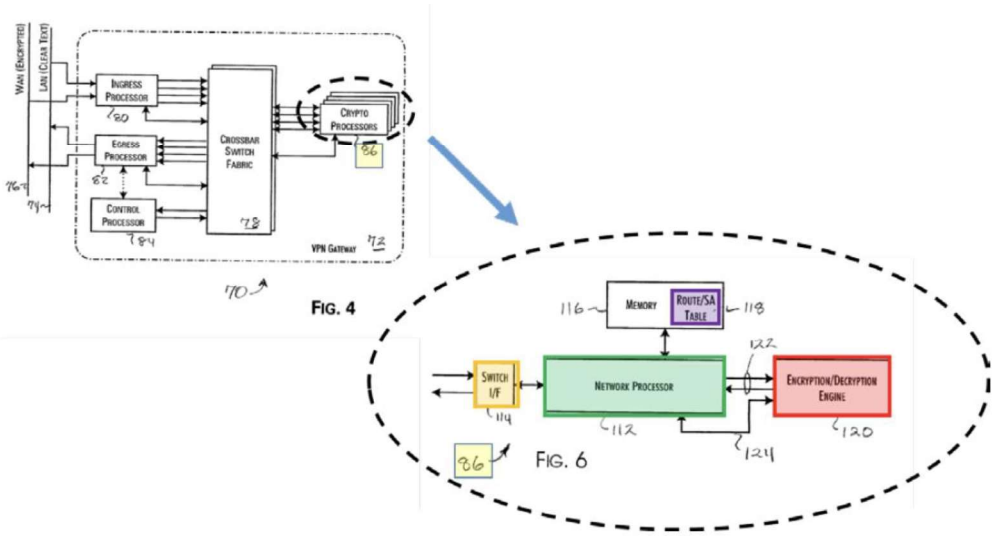
87. For the claimed "security processor," the Petitions and Dr. Crovella identify a portion of Pham's VPN Gateway Switch:



IPR2023-00673 Petition at 33-34; IPR2023-00703 Petition at 32-33; Ex. 1003, ¶ 78.

88. I note that this identification includes the switch fabric, the control processor and the plurality of data packet processors / crypto processors of Pham's VPN Gateway Switch while excluding the ingress processors and egress processors.

89. For the claimed "plurality of packet engines," the Petitions and Dr. Crovella identify the network processors of the plurality of data packet processors / crypto processors:



IPR2023-00673 Petition at 37; IPR2023-00703 Petition at 36; Ex. 1003, ¶ 83.

90. The Petitions and Dr. Crovella further state:

> 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.

I note that the reference to the "network processor includ[ing] the association of secure authority (SA) parameters task" to be to the alternate embodiment of the ingress processor operation discussed above in ¶¶ 58-60.

91. For the claimed requirement that "substantially all of the … packets to the security processor transit one of the plurality of packet engines," the Petitions and Dr. Crovella conclude that "Pham discloses that the network processors 112 process substantial all the data packet received and transmitted by the VPN Gateway." IPR2023-00673 Petition at 42; IPR2023-00703 Petition at 41; Ex. 1003, ¶ 89. As support for this conclusion, the Petitions and Dr. Crovell assert:

> 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.

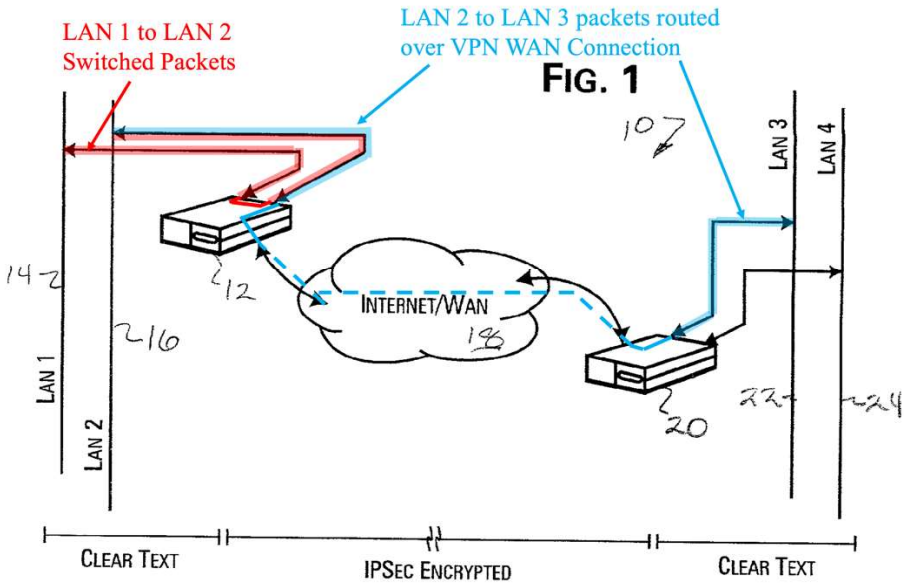
IPR2023-00673 Petition at 42; IPR2023-00703 Petition at 41; Ex. 1003, ¶ 89 (emphasis added)

92. The assertion that "all packets … can be sent to network processor 112" is not supported by the disclosure of Pham, either in the preferred embodiment or the alternative embodiment of ingress processor operation. *See* ¶¶ 53-60, above. Pham clearly teaches that clear text packets that are not to be routed through a VPN WAN connection "are bypassed between ingress and egress processor." *See* ¶ 54, above. The only "bypass" mechanism that Pham discloses is through the switch fabric. *See* ¶ 53, above. Furthermore, Pham makes clear that, when certain aspects of ingress processor operation are "off-loaded" to the network processor of the data packet processor / crypto processor, the ingress processor maintains the "basic switching and filtering" functions. *See* ¶ 53, above.

93. A POSITA would realize that the assertion that "all packets" would be forwarded to the network processor of the data packet processor / crypto processor is untenable because the ingress processors are expected to operate at wire-speed while the data packet processors / crypto processors are expected to operate at a small fraction of wire-speed. *See, e.g.*, Ex. 1004, [0036]. A POSITA would also realize that passing "all packets" to network processor of the data packet processor / crypto processor would double the load on the switch fabric for LAN-to-LAN switched packets. Instead of a packet's single traversal of the switch fabric in going

from ingress processor to egress processor, the Petitions' misreading of Pham requires a traversal from ingress processor to data packet processor / crypto processor ***plus*** a traversal from data packet processor / crypto processor to egress processor. This too is untenable.

94. As further illustrated below, Pham's VPN Gateway Switch is expected to switch packets from LAN-to-LAN, to route LAN packets through a VPN WAN connection, and to route VPN WAN packets to a LAN:



Ex. 1004, Fig. 1 (annotated to show LAN-to-LAN switching and LAN to VPN WAN routing).

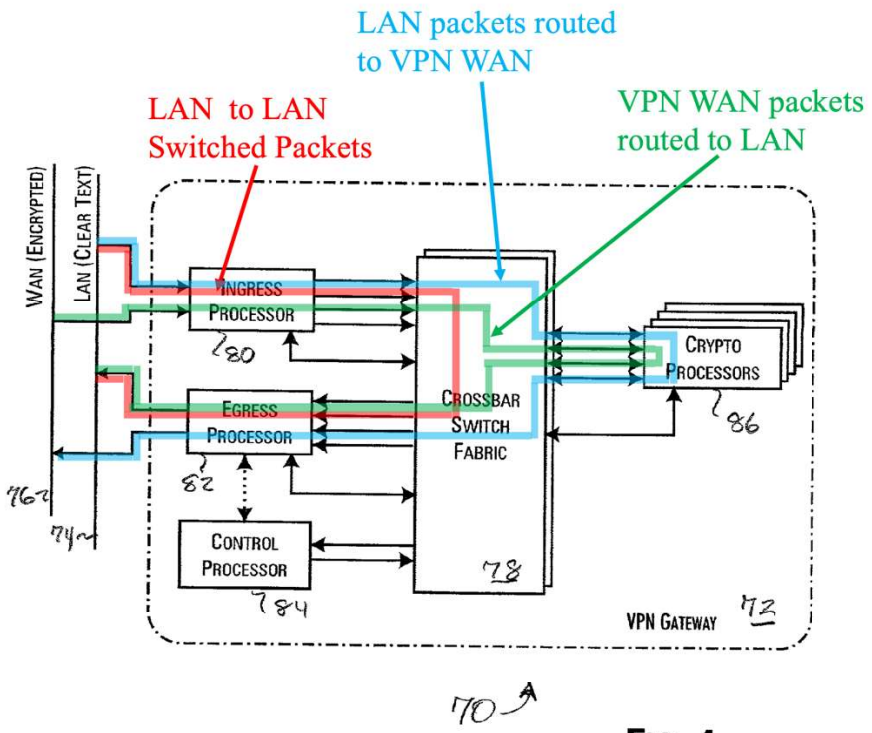


FIG. 4

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

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

IX. A POSITA WOULD NOT BE MOTIVATED TO COMBINE PHAM AND WU

96. Each of independent claims 1 and 13 of the Challenged Patents requires "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." *See* Ex. 1001, 24:35-39 ('436 Patent, Cl. 1); Ex. 1001, 25:37-26:2 ('436 Patent, Cl. 13); Ex. 1012, 21:7-11 ('612 Patent, Cl. 1); Ex. 1012, 22:4-8 ('612 Patent, Cl. 13).

97. The Petitions and Dr. Crovella assert that, to meet these requirements of the claims "[i]t would have been obvious to modify the teachings of Pham with the teachings of Wu to add an intrusion detection system and signature database to the network data processor system AND to functionally locate the IDS between the network processor (*packet engine*) and the encryption/decryption engine (*cryptographic core*)." IPR2023-00673 Petition at 53; IPR2023-00703 Petition at 48; Ex. 1003, ¶ 107. I disagree.

98. Because Pham discloses a closed system in which the only connections to the internet are through secure connections and a virtual private network, a POSITA would have to consider the increased complexity and resources in modifying Pham as the Petitions and Dr. Crovella suggest. Neither the Petitions nor

Dr. Crovella discuss the complexities and required resources in relation to Pham. For example, would the network processor of Pham's data packet processor / crypto processor be replaced by a general purpose microprocessor, as Pham already suggests for data compression purposes, *see* Ex. 1004, [0053], to implement the intrusion detection and databases features. Because the Petitions do not address the impact on the overall design of Pham's system, a POSITA would not be motivated to combine Pham and Wu as the Petitions and Dr. Crovella suggest.

99. More importantly, a POSITA would not be motivated to combine the teachings of Wu between the network processor and the encryption/decryption engine on Pham's data packet processor / crypto processor. While such a placement would monitor secure VPN traffic for intrusions, it would miss Pham's much greater vulnerability to unencrypted traffic arriving over the WAN, as well as unencrypted traffic arriving over a LAN. As described above in ¶ 61, Pham maintains "simple network access ports" for WAN communication with "external network connected devices," *see* Ex. 1004, [0048], for example, to allow for set up of IPsec VPN connections. By placing Wu's intrusion detection system on Pham's data packet processor / crypto processor, the much greater vulnerability from unencrypted WAN and/or LAN traffic is missed because Pham filters out such traffic at ingress and does

not pass associated packets to data packet processor / crypto processor. If a POSITA were motivated to combine Pham's VPN Gateway Switch with Wu's intrusion detection system, the proper location within Pham's VPN Gateway Switch to place the intrusion detection would be at Pham's egress processor. Only placement at the egress processor would allow for comprehensive protection against intrusion to and from Pham's LANs. For at least this reason, a POSITA would not be motivated to add Wu's intrusion detection system to Pham's data packet processor / crypto processor.

I declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true, and that these statements were made with knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, undersection 1001 of Title 18 of the United States Code.

Date: January 22, 2024

Eric Cole, Ph.D.