UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

CISCO SYSTEMS, INC.,
PALO ALTO NETWORKS, INC., and
FORTINET, INC.,

Petitioners,

v.

LIONRA TECHNOLOGIES LIMITED,

Patent Owner.

Case IPR2023-00703
Patent 8,566,612

PATENT OWNER'S SUR-REPLY

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

TABLE OF CONTENTS

Page

CHALLENGED CLAIMS v

I. INTRODUCTION 1

II. Pham Does Not Disclose, Teach or Suggest the Claimed Packet Engines In Any Embodiments. 3

III. The Independent Claims of the '612 Patent are limited by the structural limitation that "substantially all of the incoming packets and outgoing packets to the security processor transit one of the plurality of packet engines." 9

IV. Petitioner Does Not Address Patent Owner's Argument that a POSITA Would Not Be Motivated to Combine Wu's Intrusion Detection with Pham's Virtual Private Network Architecture. 21

V. Grounds 3 and 4 are Not Fully Supported Because Petitioner Does Not Show an Intrusion Detection System on a Chip. 21

VI. CONCLUSION 21

TABLE OF AUTHORITIES

Cases

Bicon, Inc. v. Straumann Co.,
441 F.3d 945 (Fed. Cir. 2006) 20

Haberman v. Gerber Products Co.,
236 F.Appx. 592 (Fed. Cir. 2007) 19

Hoffer v. Microsoft Corp.,
405 F.3d 1326 (Fed.Cir.2005) 19

In re Johnston,
435 F.3d 1381 (Fed. Cir. 2006) 20

In re Schreiber,
128 F.3d 1473, 44 USPQ2d 1429 (Fed. Cir. 1997) 14

Intel Corp. v. Qualcomm Inc.,
21 F.4th 801 (Fed. Cir. 2021). 10, 11

K-2 Corp. v. Salomon S.A.,
191 F.3d 1356 (Fed. Cir. 1999) 13

Lionra Technologies Ltd. v. Fortinet Inc., et al.,
Case No. 2:22-cv-00322-JRG-RSP (E.D. Tex.) 19, 20

Rowe v. Dror,
112 F.3d 473 (Fed. Cir. 1997) 12

Textron Innovations Inc. v. Am. Eurocopter Corp.,
498 F. App'x 23 (Fed. Cir. 2012) 12

Typhoon Touch Technologies, Inc. v. Dell, Inc.,
2009 WL 2243126 (E.D.Tex. July 23, 2009),
aff'd in part, rev'd in part, 659 F.3d 1376 (Fed. Cir. 2011) 13, 14

Wasica Fin. GmbH v. Cont'l Auto. Sys.,
853 F.3d 1272 (Fed. Cir. 2017) 10, 20

Other Authorities

Manual of Patent Examining Procedures § 2173.05(g). 13

PATENT OWNER'S EXHIBIT LIST

Exhibit No.	Description
2001	Order, *Lionra Technologies Limited v. Fortinet, Inc.*, No. 2:22-cv-00322-JRG-RSP (Lead Case), Dkt. No. 21 (E.D. Tex. Oct. 24, 2022)
2002	Docket Control Order, *Lionra Technologies Limited v. Fortinet, Inc.*, No. 2:22-cv-00322-JRG-RSP (Lead Case), Dkt. No. 59 (E.D. Tex. Dec. 2, 2022)
2003	Docket Sheet, *Lionra Technologies Limited v. Fortinet, Inc.*, No. 2:22-cv-00322-JRG-RSP (Lead Case) (E.D. Tex. June 28, 2023)
2004	Order, *MyPort, Inc. v. Samsung Electronics Co., Ltd.*, *et al.,* No. 2:22-cv-00114-JRG (E.D. Tex. June 12, 2023)
2005	Defendants' Invalidity Contentions, *Lionra Technologies Limited v. Fortinet, Inc.*, No. 2:22-cv-00322-JRG-RSP (Lead Case) (E.D. Tex. Feb. 10, 2023)
2006	U.S. District Courts—Federal Court Management Statistics–Profiles—During the 12-Month Periods Ending March 31, 2018 Through 2023 available at https://www.uscourts.gov/statistics/table/na/federal-court-management-statistics/2023/03/31-1
2007	U.S. Patent No. 7,493,659 ("Wu et al.")
2008	U.S. Patent Publication No. 2003/0014627 ("Krishna et al.)
2009	Claim Construction Order, *Lionra Technologies Limited v. Fortinet, Inc.*, No. 2:22-cv-00322-JRG-RSP (Lead Case), Dkt. No. 162 (E.D. Tex. Nov. 27, 2023)
2010	Declaration of Eric Cole, Ph.D.
2011	Curriculum Vitae of Eric Cole, Ph.D.
2012	Transcript of Jan. 10, 2024 Deposition of Mark Crovella, Ph.D.

CHALLENGED CLAIMS

Claim	Text
[i.pre]	A security processor to process incoming packets and outgoing packets, the security processor comprising:
[1.ii]	a switching system to send the outgoing packets and receive the incoming packets;
[1.iii]	a packet engine, coupled to the switching system, to handle classification processing for the incoming packets received by the packet engine from the switching system and the outgoing packets sent by the packet engine to the switching system,
[1.iv]	wherein the packet engine is one of a plurality of packet engines and substantially all of the incoming packets and outgoing packets to the security processor transit one of the plurality of packet engines, and;
[1.v]	a cryptographic core, coupled to the packet engine and receiving the incoming packets from the switching system via the packet engine and communicating the outgoing packets to the switching system via the packet engine, to provide encryption and decryption processing for packets received from and sent to the packet engine,
[1.vi]	wherein the packet engine is interposed between the switching system and the cryptographic core;
[1.vii]	a signature database; and an intrusion detection system coupled between the cryptographic core and the packet engine and responsive to at least one packet matching a signature stored in the signature database.
[2]	The security processor of claim 1 wherein the packet engine is further operable to handle security context management processing for the incoming and outgoing packets.

Claim	Text
[3]	The security processor of claim 1 further comprising: a local data bus coupled to the switching system; and a modulo engine coupled to the local data bus.
[4]	The security processor of claim 3 wherein the packet engine, the cryptographic core, and the modulo engine are formed on a single chip.
[7]	The security processor of claim 4 wherein the security processor handles substantially all security processing for the incoming and outgoing packets.
[8]	The security processor of claim 7 wherein the security processor further handles substantially all network processing for the incoming and outgoing packets.
[9]	The security processor of claim 1 wherein the cryptographic core is one of a plurality of cryptographic cores coupled one-to-one to the plurality of packet engines and substantially all of the incoming and outgoing packets to the security processor transit a corresponding one of the plurality of cryptographic cores after transiting one of the plurality of packet engines.
[10]	The security processor of claim 1 wherein the packet engine is further operable to add at least one of an IP header or a MAC address to the outgoing packets.
[11]	The security processor of claim 1 wherein the packet engine is further operable to remove an IP header from the incoming packets.
[12]	The security processor of claim 1, wherein the at least one packet matching the signature stored in the signature database comprises a plain text packet.
[13.pre]	A security processing system comprising: a security processor comprising
[13.ii]	a switching system to send outgoing packets and receive incoming packets;

Claim	Text
[13.iii]	a packet engine, coupled to the switching system, to handle classification processing for the incoming packets received by the packet engine from the switching system and the outgoing packets sent by the packet engine to the switching system,
[13.iv]	wherein the packet engine is one of a plurality of packet engines and substantially all of the incoming packets and outgoing packets to the security processor transit one of the plurality of packet engines, and;
[13.v]	a cryptographic core, coupled to the packet engine and receiving the incoming packets from the switching system via the packet engine and communicating the outgoing packets to the switching system via the packet engine, to provide encryption and decryption processing for packets received from and sent to the packet engine,
[13.vi]	wherein the packet engine is interposed between the switching system and the cryptographic core;
[13.vii]	a signature database; and an intrusion detection system coupled between the cryptographic core and the packet engine and responsive to at least one packet matching a signature stored in the signature database; and
[13.viii]	a local data bus coupled to the switching system; and
[13.ix]	a memory coupled to the local data bus.
[14]	The security processing system of claim 13 further comprising a modulo engine coupled to the local data bus.
[16]	The security processing system of claim 13 wherein the memory and the security processor are within the same cryptographic boundary.
[17]	The security processing system of claim 13 wherein the security processor is formed on a single chip.

Claim	Text
[21]	The security processing system of claim 13 wherein the security processor is operable to (i) execute boot code to load firmware for execution by the security processor and (ii) authenticate the boot code using a mechanism internal to the security processor prior to operation of the security processor.
[22]	The security processing system of claim 13, wherein the at least one packet matching the signature stored in the signature database comprises a plain text packet.

I. INTRODUCTION

Patent Owner Lionra Technologies Ltd. ("Patent Owner") submits this sur-reply to Petitioner's Reply to Patent Owner's Response ("Reply," Paper 15) in the *inter partes* review of U.S. Patent No. 8,566,612 ("the '612 patent"). As discussed in Patent Owner's Response to Petition ("POR," Paper 13) and below, the Petition fails on all grounds because, *inter alia*, the primary reference relied upon by Petitioner, Pham, does not disclose, teach or suggest a critical limitation of every independent claim—that "substantially all of the incoming packets and outgoing packets to the security processor transit one of the plurality of packet engines." In order to satisfy this claim limitation, substantially all of the incoming and outgoing packets to and from the security processor would have to transit the network processors in Pham's crypto processors (which are <u>not</u> the network processors in Pham's ingress processor, egress processor, or control processor) – but they do <u>not</u>. In Pham, packets that are filtered or switched by the ingress processor are directed to the egress processor through the switch fabric, while other packets are directed to a control processor through the switch fabric. These packets never go to a crypto processor (i.e., these packets do not transit the crypto processor, including the network processor within the crypto processor).

Pham discloses several network processors, but the <u>only</u> network processors in Pham that could possibly satisfy the claim requirements for a packet engine that

is coupled to a cryptographic core and interposed between the switching system and the coupled cryptographic core are the network processors in Pham's crypto processors. And all of Pham's embodiments include ingress, egress, and control processors that filter or process packets coming into or going out of the security processor. Because these packets do not transit the network processors in Pham's crypto processors (i.e., packet engines identified by Petitioner), yet pass through the switch fabric (part of Petitioner's identified "security processor"), Pham does not disclose, teach or suggest that "substantially all of the incoming packets and outgoing packets to the security processor transit one of the plurality of packet engines."

And, as also discussed in the POR and further discussed below, a Person of Ordinary Skill in the Art (POSITA) would not have been motivated to combine the Pham and Wu references to meet a different limitation of every independent claim—"an intrusion detection system coupled between the cryptographic core and the packet engine." Petitioner's arguments to the contrary rely on both an erroneous interpretation of Pham's teachings that ignores the ingress and control processors and disregards Pham's teachings that "a general purpose microprocessor can be substituted or provided in addition to the network processor 112 to support data compression and decompression operations." Ex. 1004, [0053]. Pham explicitly teaches that its network processor would not be sufficient to support data

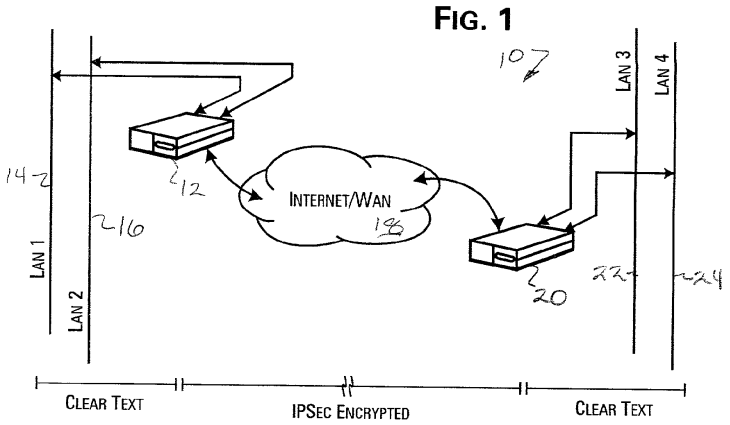
compression and decompression operations and thus would not be sufficient to support intrusion detection.

II. Pham Does Not Disclose, Teach or Suggest the Claimed Packet Engines In Any Embodiments.

Petitioner's primary reference is Exhibit 1004, U.S. Patent Publication 2003/0074473, titled "Scalable Network Gateway Processor Architecture," ("Pham"). Pham's scalable network gateway processor architecture includes ingress, egress, control and data processors and a switching fabric. Ex. 1004, [0038]. Pham's data processors can be crypto processors. *Id.*, [0045]. Petitioner identifies the network processors in the crypto processors as the claimed packet engines in Pham. Paper 15, Reply at 2. As discussed in the POR and below, unencrypted packets (and some encrypted packets), do not transit any of the crypto processor network processors in any of Pham's embodiments. Accordingly, less than "substantially all of the incoming packets and outgoing packets to the security processor transit one of the plurality of packet engines."

Petitioner's first argument, that Patent Owner's description of Pham's Figure 1 embodiment that filters unencrypted packets without transiting the cryptoprocessors lacks factual support (Reply at 2), is both conclusory and incorrect. In Figure 1, Pham shows clear text unencrypted packets that travel between LAN 1 and LAN 2 or LAN 3 and LAN 4. *See* Ex. 2010, Declaration of Eric Cole, Ph.D.,

("Cole Decl."), ¶ 51.



Ex. 1004, Fig. 1.

These unencrypted packets do not require processing through data packet processors and are instead "bypassed between the ingress and egress processors" through the switch fabric. Ex. 1004, [0038]-[0040]; Ex. 2010, Cole Decl., ¶¶ 52-55. Petitioner's expert agreed. See Ex. 2012, Dep. Tr., 35:4-6 ("[I]n this specific scenario [packets are being moved between LAN 3 and LAN4], those packets would not be going through the cryptoprocessor."). Petitioner's expert also admitted that "every incoming and outgoing packet will initially enter through the ingress processor and eventually exit through the egress processor." *Id.*, 27:16-19.

Petitioner's arguments that there are embodiments of Pham in which substantially all packets received by the security processor transit a packet engine do not withstand scrutiny. Reply at 3. Petitioner's first argument, that Pham has the capacity to process encrypted traffic in the VPN, *id.*, is a *non sequitur.* As explained

by Dr. Cole and confirmed by Dr. Crovella, clear text packets that are not be routed through a VPN WAN connection are "bypassed between ingress and egress processor" through the switch fabric. Ex. 2010, ¶ 92; Ex. 2012, 27:16-19. Moreover, Petitioner's contention that "the VPN gateways shown in FIG. 1 could work exclusively with the VPN tunnel without routing packets to the Internet," Reply at 3, disregards Pham's teaching regarding the control processor. "The control processor 84 utilizes the port connections between the control processor 84 and switch fabric 78 to transmit effectively out-of-band control information and receive status information from the ingress, egress, and crypto processors 80, 82, 86. In-band communications with external network connected devices, such as for network protocol negotiations, is accomplished by utilizing the ingress and egress processors 80, 82 as simple network access ports." Ex. 1004, [0048]. Pham's purported ability to support a VPN gateway does not refute Pham's explicit disclosure that Pham processes unencrypted packets that are not routed to a crypto processor.

All of Pham's embodiments include ingress, egress, and control processors that are not coupled to the cryptographic core in the crypto processors and are not interposed between the switch fabric and the cryptographic core. Pham's ingress, egress, and control processors filter or process packets coming into or going out of Pham's gateway by passing packets amongst themselves through the switch fabric (part of Petitioner's identified "security processor"). Because these packets do not

transit the network processors in Pham's crypto processors (i.e., packet engines identified by Petitioner), Pham does not disclose, teach or suggest that "substantially all of the incoming packets and outgoing packets to the security processor transit one of the plurality of packet engines."

Petitioner's contention that the speed of the BCM5840 utilized in crypto processor 86 and/or the bandwidth of the connection between ingress/egress processors and the switch fabric are evidence that all traffic is processed by the alleged packet engines is unfounded. Reply at 3. The claims do not recite a particular processing speed or connection bandwidth, and neither of those characteristics demonstrate the claimed functionality. The speed of Pham's crypto processors does not have anything to do with the system's capability to route substantially all packets to the alleged packet engines, which Pham clearly lacks.

Petitioner's second argument, directed to Figure 2 of Pham, is improper for the reasons set forth in Paper 18, Patent Owner's Motion to Strike Portions of Petitioner's Reply Brief. Petitioner's second argument also fails on the merits. As an initial matter, Petitioner ignores packets sent to control processor 46. "[T]he ingress processors 30, 34 are tasked with filtering and routing functions for network data packets received on their network connections to the LAN 38 and Internet 18. The routing function includes internally directing individual data packets through a fast processing path to the arrays of data packet processors 42, 44 <u>or through a</u>

control processing path to the control processor 46." Ex. 1004, [0038] (emphasis added).

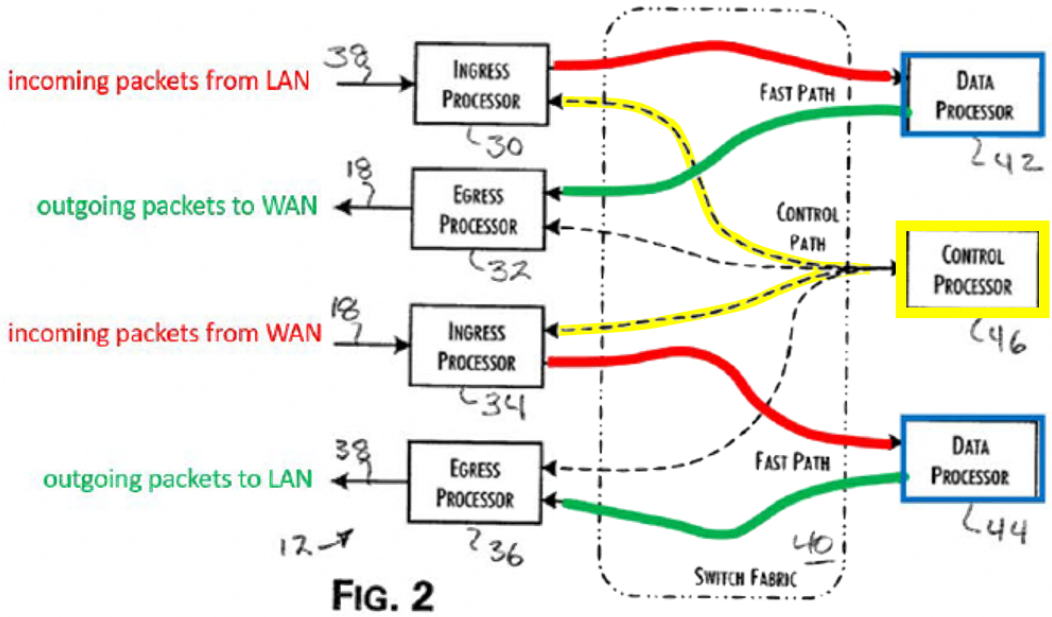


FIG. 2

Id., Fig. 2 (yellow annotations added; red/green annotations from Reply at 4). "The control path route is selected for data packets recognized as being directed to the VPN gateway 12 itself. Such data packets likely represent control commands used to configure and manage the VPN gateway 12. The control path is also selected for network data packets recognized by an ingress processor 30, 34 as representing or initiating a new logical network connection through the VPN gateway 12." *Id.*, [0039]. "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." *Id.*, [0040].

Petitioner does not suggest that control processor 46 is a packet engine as claimed. Nor does Petitioner show that the data processor 42, 44 of Pham's Figure 2 is a crypto processor, instead merely asserting that "the data processors could be crypto processors." Reply at 5. Accordingly, even if Petitioner's reliance on the embodiment of Pham shown in Figure 2 was proper, which it is not, Petitioner still has not established that "substantially all of the incoming packets and outgoing packets to the security processor transit one of the plurality of packet engines" in Pham's Figure 2 embodiment.

Petitioner's third argument, directed to Figure 4 of Pham, is based upon the same failed premise as Petitioner's first argument – that Pham's purported ability to support a VPN gateway means that Pham is nothing more than a VPN gateway, notwithstanding Pham's explicit disclosure that Pham processes unencrypted packets that are not routed to a crypto processor. Reply at 6. Petitioner's third argument fails for the same reasons Petitioner's first argument fails.

Petitioner's additional argument that Pham's disclosed crypto processor could perform additional packet processing functions beyond encryption and decryption is equally flawed. Reply at 7. First, as Petitioner admits, basic switching and filtering cannot be offloaded from the ingress processor to a data processor. Reply at 8. Basic switching and filtering is packet processing that will not be performed by a data processor, and, as discussed above, will result in packets coming into the security

processor that will not transit a claimed packet engine (identified by Petitioner as network processor 112 of crypto processor 86). Moreover, to the extent that more than the SA parameter association task is off-loaded, Pham teaches that the network processor 112 would be substituted or supplemented. "In particular, a general purpose microprocessor can be substituted or provided in addition to the network processor 112 to support data compression and decompression operations." Ex. 1004, [0053]. Accordingly, Petitioner's argument that a POSITA would understand that "packet processing performed by the network processor 92 of the ingress processor 90 would be offloaded to the network processor 112 of the crypto processor 86," Reply at 8-9, is directly contradicted by Pham's explicit teaching that off-loading tasks to the network processor 112 would not encompass basic switching or filtering and would require substitution or supplementation of the network processor with a general purpose microprocessor.

III. The Independent Claims of the '612 Patent are limited by the structural limitation that "substantially all of the incoming packets and outgoing packets to the security processor transit one of the plurality of packet engines."

Petitioner acknowledges that "substantially all of the incoming packets and outgoing packets to the security processor transit one of the plurality of packet engines" is a limitation of the independent claims. Reply at 10. However, Petitioner incorrectly asserts that this limitation is somehow subsumed by the preamble

recitation of "a security processor to process incoming packets and outgoing packets."

Under Petitioner's apparent construction, the "substantially all" limitation is meaningless. Doing so is contrary to the law and should be rejected by the Board. The Federal Circuit recently rejected a similar effort to render a claim term superfluous.

> *First*, because every buffer in our (physical) world is ultimately implemented on a physical device (*i.e.*, hardware), a "hardware buffer" must mean something more than just a "buffer implemented in hardware," as Intel urges, or else the word "hardware" would be erased from the claims. That consequence, while not inevitably disqualifying a construction in every patent, is counter to an important principle of interpretation, for patent claims as for statutes: "It is highly disfavored to construe terms in a way that renders them void, meaningless, or superfluous." *Wasica Finance GmbH v. Continental Automotive Systems, Inc.*, 853 F.3d 1272, 1288 n.10 (Fed. Cir. 2017); *see SimpleAir, Inc. v. Sony Ericsson Mobile Commc'ns AB*, 820 F.3d 419, 429 (Fed. Cir. 2016); *Stumbo v. Eastman Outdoors, Inc.*, 508 F.3d 1358, 1362 (Fed. Cir. 2007); *Phillips*, 415 F.3d at 1314; *Duncan v. Walker*, 533 U.S. 167, 174, 121 S. Ct. 2120, 150 L. Ed. 2d 251 (2001) (refusing to adopt a statutory construction that "would render the word 'State' insignificant, if not wholly superfluous"); *Salman Ranch Ltd. v. United States*, 573 F.3d 1362, 1374 (Fed. Cir. 2009) ("A cardinal rule of statutory construction is that courts should construe statutes so as to

> avoid rendering superfluous any statutory language." (cleaned up)). Here, the striking fact that Qualcomm, in its claim language, did not just say "buffer," but instead said "hardware buffer," provides a strong reason to avoid the disfavored result of rendering the word "hardware" superfluous.

Intel Corp. v. Qualcomm Inc., 21 F.4th 801, 809-10 (Fed. Cir. 2021). Petitioner mischaracterizes Patent Owner's arguments as limited to a scenario where incoming packets to the security processor do not require processing by a packet engine. Reply at 11. What Patent Owner is doing is applying the claims to Pham's disclosure in its entirety, including Pham's ingress, egress and control processors. Pham's ingress processor handles classification processing for the incoming packets, but it is not a packet engine as claimed because it does not satisfy the claim limitations for a packet engine (i.e., it is not coupled to a cryptographic core and it is not interposed between the switching system and the coupled cryptographic core).

Pham's scalable network gateway processor architecture, including ingress, egress, control and data processors, is fundamentally different from the security processor disclosed and claimed in the '612 Patent. And it is because of these differences that Pham does not disclose the limitation that "substantially all of the incoming packets and outgoing packets to the security processor transit one of the plurality of packet engines."

In the Institution Decision for *inter partes* review *Palo Alto Networks, Inc. and Fortinet, Inc. v. Lionra Technologies Ltd.*, the Board raised the issue of whether "substantially all of the incoming packets and outgoing packets to the security processor transit one of the plurality of packet engines" limits the structure of the claim or is simply a statement of intended use. *See* Paper 19 at 13-15. The Board concluded that "[o]n its face, the 'substantially all' limitation appears more akin to a statement of intended use." *Id.* at 14. Patent Owner respectfully traverses this conclusion, starting with an analysis of the Board's cited cases.

In *Textron Innovations Inc. v. Am. Eurocopter Corp.*, the Federal Circuit was addressing whether the term "replacement" in the claim *preamble* should be construed as a structural limitation or a statement of intended use. As the Court noted, "[w]hen a patentee 'uses the claim preamble to recite structural limitations of his claimed invention, the PTO and courts give effect to that usage' …. [h]owever, when a patentee 'defines a structurally complete invention in the claim body and uses the preamble only to state a purpose or intended use for the invention, the preamble is not a claim limitation.'" *Textron Innovations Inc. v. Am. Eurocopter Corp.*, 498 F. App'x 23, 27 (Fed. Cir. 2012) (citations omitted). Similarly, in *Rowe v. Dror*, 112 F.3d 473, 478-480 (Fed. Cir. 1997), the Federal Circuit addressed whether the term "angioplasty" in the *preamble* was to be construed as a structural limitation or a statement of intended use.

In *K-2 Corp. v. Salomon S.A.*, the Federal Circuit addressed the patentee's argument of whether the limitation of "substantially preventing movement therebetween at least in a horizontal plane" dictated the meaning of the term "permanently affixed" in the body of a claim. *K-2 Corp. v. Salomon S.A.*, 191 F.3d 1356, 1363-64 (Fed. Cir. 1999). In reaching the conclusion that the patentee's argument would effectively expunge "permanently" from the claim, the Court first analyzed the limitation of "substantially preventing movement …" and noted that this "functional language is, of course, an additional limitation in the claim." *Id.*, 191 F.3d at 1363. In doing so, the Court further recognized that "the functional language tells us something about the structural requirements of the attachment." *Id.*; *see also Typhoon Touch Technologies, Inc. v. Dell, Inc.*, 2009 WL 2243126, at * 7 (E.D.Tex. July 23, 2009) *aff'd in part, rev'd in part*, 659 F.3d 1376 (Fed. Cir. 2011) ("Here, the structure of the 'memory' and the 'run-time executor' are defined according to their functions: e.g., storing data collection applications or executing data collection applications. Thus, the claim uses functional language that describes the structure of a 'memory' and 'run-time executor' beyond being merely 'memory' and a 'run-time executor.'").

As is clear from *K-2* and other precedents, functional language may be used to limit the structure of an apparatus claim to the way the apparatus functions during operation. *Manual of Patent Examining Procedures* § 2173.05(g). Functional

limitations can be an effective way to distinguish the claimed apparatus from the prior art. *See In re Schreiber*, 128 F.3d 1473, 1478, 44 USPQ2d 1429, 1431 (Fed. Cir. 1997) ("A patent applicant is free to recite features of an apparatus either structurally or functionally.").

In the present instance, there should be no dispute that the relevant functional language limits the structure of the claimed "packet engines" and, consequently, the claimed "security processor." More specifically, the plain language of the claims informs a POSITA of the further structural requirements of the claim, that "substantially all of the incoming packets and outgoing packets to the security processor transit one of the … packet engines." "Thus, the claim uses functional language that describes the structure of a [packet engine] and a [security processor] …. beyond being merely a [packet engine] and a [security processor]." *Typhoon Touch Technologies*, 2009 WL 2243126, at * 7; *see also Typhoon Touch Techs., Inc. v. Dell, Inc.*, 659 F.3d 1376, 1381 (Fed. Cir. 2011) (When claims include such functional language, consistent with the prosecution record, that function must be interpreted as a limitation of the claim that must be met for infringement to occur.). The plain language of the claim is entirely consistent with the specification, the prosecution history and the posture of the parties in the related district court action.

First, with respect to the specification, the '612 Patent discloses the operation of the security processor, for example, with respect to Fig. 2, which is reproduced below.

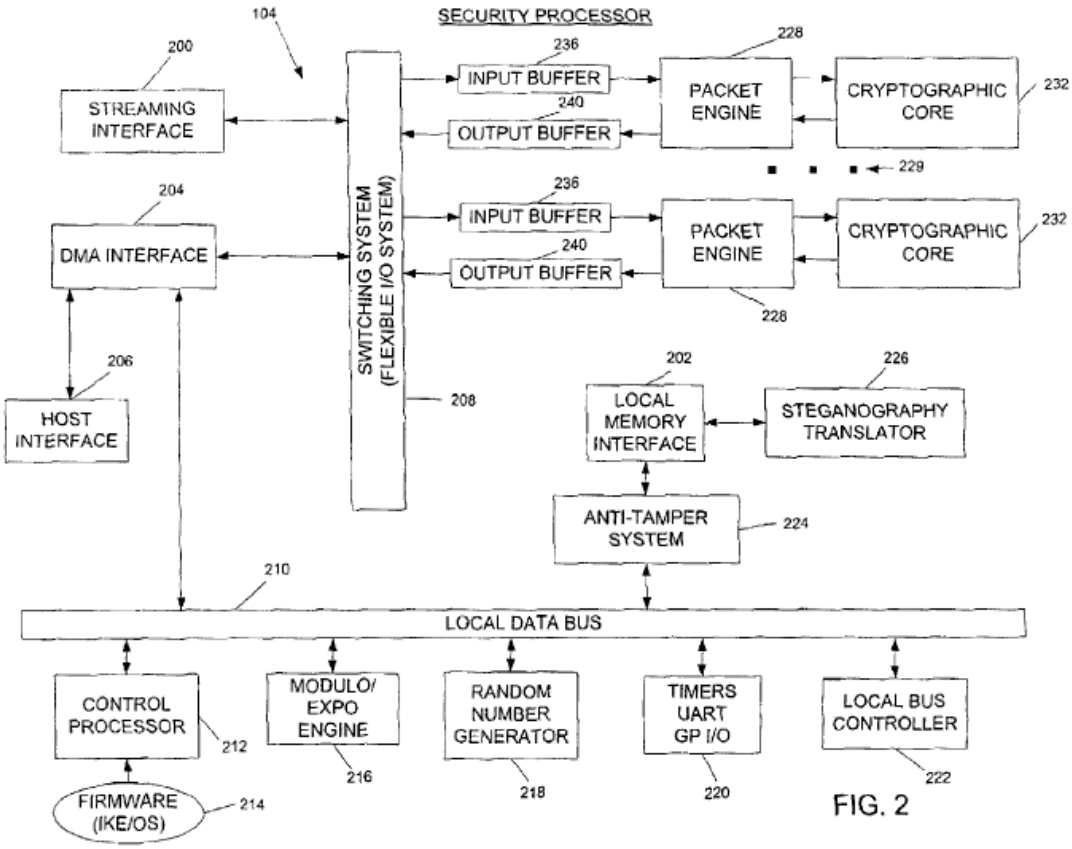


FIG. 2

Ex. 1001, Fig. 2. "Security processing system 102 may be implemented, for example, as a stand-alone system box or as a card such as, for example, a NIC, that connects to a slot in the motherboard of a host system." *Id.*, 5:37-40.

The '612 Patent describes that all incoming packets are communicated to the switching system, whether the incoming packets arrive on the streaming interface

200, the host interface 206 through the DMA interface 204, or the local data bus 210 through the DMA interface 204:

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

Id., 6:46-53; *see also id.*, 9:12-14; 9:56-59; 11:57-61 (output from switching system can be to one of several interfaces).

The '612 Patent further describes that the exemplary singular streaming and DMA interfaces are for illustrative purposes only and the number of interfaces can be significantly expanded:

> Although only a single streaming and DMA interface are illustrated, more than one interface of each type may be used. For example, in one embodiment, streaming interface 200 may comprise three 10/100 Ethernet interfaces, and DMA interface 204 may comprise two DMA interfaces. Switching system 208 may be used to provide a switching mechanism to route packets and data to and from any of the I/O interfaces of security processor 104 and local data bus 210.

Id., 6:53-61.

The '612 Patent also describes that the switching system allows numerous different types of interface standards to be used, while still providing a common interface to the packet engines:

> Switching system 208 may provide a flexible I/O system that allows packet processing engines or packet engines 228 to communicate high-

> speed data with several different types of interfaces including, for example, streaming interface 200 and direct memory access (DMA) interface 204.
>
> * * *
>
> Switching system 208 may provide a common bus interface to packet engines 228. More specifically, switching system 208 may arbitrate between streaming and DMA interfaces to provide a common interface for packet engines 228 to permit communication of differing types of data over a plurality of bus types that implement different bus protocols and/or standards.

Id., 7:33-52.

The specification of the '612 Patent describes that all packet data is passed through the switching system to a packet engine:

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

Id., 19:63-20:6 (emphasis added); *see also id.*, 12:4-12 (for initial classification, packets forwarded from packet engine to control processor); 6:29-34 (large percentage of operations handles without intervention of control processor).

Even though the specification of the '612 Patent describes that all incoming packet data is communicated through the switching system to a packet engine, the

'612 Patent notes that not all of the packet data has to pass through, i.e., transit, the packet engines. More specifically, while "all incoming packets to security processor 104 may be initially processed by one of packet engines 228," the packet engine may "classify the packet based upon a lookup table result and then may apply a variety of operations," which can "include dropping the packet, or passing the packet through security processor 104 to an egress interface, such as, for example, streaming interface 200, unchanged." *Id.*, 11:8-21; *see also id.*, 19:3-10; 11:50-53. Because the packet engine may drop a received packet, i.e., the packet engine will not forward the packet, the specification contemplates that something less than "all" of the packets, i.e., "substantially all of the packets," may be forwarded. In other words, the specification recognizes that, of the packets received at one of the packet engines, not all of the packets will be forwarded and, consequently, not all of the packets will transit the packet engines.

Second, the prosecution history unequivocally indicates that the patentees intended the claim language at issue to be limiting and not merely an intended use. In Application No. 10/903,785, which matured into the '436 Patent, originally-filed dependent claim 4, for example, recited "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." *See* Ex. 1002 at 279. The limitation of dependent claim 4, *inter alia*, was

incorporated into independent claim 1 through Examiner Amendment to secure allowance of claim 1 of the '436 Patent. *See id.* at 18-19. Similarly, in Application No. 12/697,112, which matured into the '612 Patent, dependent claim 33, filed by Preliminary Amendment, recited the same language. *See* Ex. 1013 at 218. The limitation of dependent claim 33 was incorporated into independent claim 30 through Examiner Amendment to secure allowance of claim 1 of the '612 Patent. *See id.* at 20-21. As the Petitioners collectively stated during the district court claim construction when they sought an indefiniteness finding, "[t]he only way the patentee was able to get the claims of the '436 and '612 patent allowed was by amending the independent claims to include the 'substantially all' limitation from dependent claims." *Lionra Technologies Ltd. v. Fortinet Inc. et al.*, Case No. 2:22-cv-00322-JRG-RSP, Dkt. No. 146 (*Defendants' Responsive Claim Construction Brief*), at 16 (E.D. Tex. Oct. 20, 2023); *see also Haberman v. Gerber Products Co.*, 236 F.Appx. 592, n. 3 (Fed. Cir. 2007) (Patentee is permitted to use functional language to limit the claims and overcome prior art rejections during prosecution.); *Hoffer v. Microsoft Corp.*, 405 F.3d 1326, 1329 (Fed.Cir.2005) ("[W]hen [a] 'whereby' clause states a condition that is material to patentability, it cannot be ignored in order to change the substance of the invention.").

Finally, there has been no dispute raised by any Petitioner that the functional language at issue is merely an intended use. For example, as noted in the prior

paragraph, the Petitioners sought a finding of the language as indefinite during the district court claim construction. As a further example, Petitioner Palo Alto Networks moved for summary judgment of non-infringement based on the functional language of the claim. *See Lionra Technologies Ltd. v. Fortinet Inc. et al.*, Case No. 2:22-cv-00322-JRG-RSP, Dkt. No. 268, at 10 (E.D. Tex. Feb. 27, 2024) ("[E]very Asserted Claim requires 'substantially all of **the incoming** and outgoing **packets to the security processor** transit one of the plurality of packet engines.'") (emphasis in original).

There should be no question that the functional language of "substantially all of the incoming packets and outgoing packets to the security processor transit one of the plurality of packet engines" in the claims of the '612 Patent limits the structure of the claims and is not a statement of intended use.

This Board should not effectively remove the "substantially all" limitation from the claims. Construing a limitation in a way that effectively removes it from the claim "would make [it] optional or potentially nonexistent. *See In re Johnston*, 435 F.3d 1381, 1384 (Fed. Cir. 2006). It is highly disfavored to construe terms in a way that renders them void, meaningless, or superfluous. *See Bicon, Inc. v. Straumann Co.*, 441 F.3d 945, 950-51 (Fed. Cir. 2006) (refusing to construe claim terms in a way that made other limitations meaningless)." *Wasica Fin. GmbH v. Cont'l Auto. Sys.*, 853 F.3d 1272, 1288 n.10 (Fed. Cir. 2017).

IV. Petitioner Does Not Address Patent Owner's Argument that a POSITA Would Not Be Motivated to Combine Wu's Intrusion Detection with Pham's Virtual Private Network Architecture.

Petitioner's contentions with respect to the combination of Pham and Wu, Reply at 11-13, do not address Pham's clear text packets or why a POSITA would not need an intrusion detection system for a secure virtual private network. As stated in the POR at 32-34, Pham discloses a closed system with a secure VPN and any intrusion would not come from the VPN.

V. Grounds 3 and 4 are Not Fully Supported Because Petitioner Does Not Show an Intrusion Detection System on a Chip.

Petitioner's terse discussion of the teachings of Krishna omits any discussion of how limitation [1.vii] of independent claim 1 ("an intrusion detection system coupled between the cryptographic core and the packet engine") or limitation [13.vii] of independent claim 13 ("an intrusion detection system coupled between the cryptographic core and the packet engine") could or would be satisfied if the security processor was formed on a single chip. Doing so requires more than identifying intrusion detection systems that were implemented in networks, but not on an integrated circuit, in the prior art.

VI. CONCLUSION

As set forth above and in the POR, Pham does not disclose that "substantially all of the incoming packets and outgoing packets to the security processor transit one

of the plurality of packet engines" as required by limitations [1.iv] and [13.iv] of the independent claims of the '612 Patent. Furthermore, as also set forth above and in the POR, a person of ordinary skill in the art would not be motivated to combine Pham with Wu as the Petition asserts. Accordingly, the prior art does not teach or suggest "an intrusion detection system coupled between the cryptographic core and the packet engine" as required by limitations [1.vii] and [13.vii] of the independent claims of the '612 Patent. For these reasons, and all of the other reasons set forth above, Patent Owner respectfully requests that all challenged claims be found not unpatentable.

Date: June 3, 2024

Respectfully submitted,

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

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

The undersigned hereby certifies that the word count in this Patent Owner's Sur-reply is 4,811 words, as counted by the word-processing program Microsoft Word that was used to generate this Patent Owner's Sur-reply, where such word count excludes the table of contents, table of authorities, mandatory notices, certificate of service, appendix of exhibits, claim listing, and this certificate of word count. This Patent Owner's Sur-reply is in compliance with the 5,600-word limit set forth in 37 C.F.R. § 42.24(c)(4).

Date: June 3, 2024

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

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

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

The undersigned hereby certifies that the above document was served on June 3, 2024, by filing this document through the Patent Trial and Appeal Case Tracking System as well as delivering a copy via electronic mail upon the following attorneys of record for the Petitioner:

Patrick McPherson (Reg. No. 46,255)
PDMcPherson@duanemorris.com
Patrick C. Muldoon (Reg. No. 47,343)
PCMuldoon@duanemorris.com
D. Joseph English (Reg. No. 42,514)
DJEnglish@duanemorris.com
Paul H. Belnap (Reg. No. 73,106)
PHBelnap@duanemorris.com
Nicole Candelori (Reg. No. 77,218)
NCandelori@duanemorris.com
DUANE MORRIS LLP
901 New York Ave. NW, Suite 700 East
Washington, D.C. 20001-4795

Monté T. Squire (Reg. No. 80,123)
MTSquire@duanemorris.com
DUANE MORRIS LLP
201 North Market Street, Suite 501
Wilmington, DE 19801

Date: June 3, 2024
BC Law Group, P.C.
200 Madison Avenue, 24th Floor
New York, NY 10016
(212) 951-0100

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