

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

CISCO SYSTEMS, INC.,
Petitioner,

v.

LIONRA TECHNOLOGIES LTD,
Patent Owner.

IPR2023-00673
Patent 7,685,436 B2

Before WILLIAM V. SAINDON, PATRICK R. SCANLON, and
STEVEN M. AMUNDSON, *Administrative Patent Judges*.

SAINDON, *Administrative Patent Judge*.

DECISION
Granting Institution of *Inter Partes* Review
35 U.S.C. § 314

I. INTRODUCTION

A. Background and Summary

Cisco Systems, Inc. (“Petitioner”) filed a Petition (Paper 1, “Pet.”) requesting *inter partes* review of claims 1–4, 7–14, 16, 17, 21 and 22 (“the challenged claims”) of U.S. Patent 7,685,436 B2 (Ex. 1001, “the ’436 patent”). Pet. 19. Lionra Technologies Ltd. (“Patent Owner”) filed a Preliminary Response (Paper 7, “Prelim. Resp.”).

We have authority to determine whether to institute an *inter partes* review under 35 U.S.C. § 314(b) and 37 C.F.R. § 42.4(a). The standard for instituting an *inter partes* review is set forth in 35 U.S.C. § 314(a), which provides that an *inter partes* review may not be instituted unless “there is a reasonable likelihood that the petitioner would prevail with respect to at least 1 of the claims challenged in the petition.”

For the reasons provided below, we determine that Petitioner has satisfied the threshold requirement set forth in 35 U.S.C. § 314(a). Because Petitioner has demonstrated a reasonable likelihood that at least one claim of the ’436 patent is unpatentable, we institute an *inter partes* review. 37 C.F.R. § 42.108(a) (2023).

Our findings of fact, conclusions of law, and reasoning discussed below are based on the evidentiary record developed thus far, and made for the sole purpose of determining whether the Petition meets the threshold for initiating review. This decision to institute trial is not a final decision as to the patentability of any challenged claim or the construction of any claim limitation.

B. Real Parties in Interest

The parties identify only themselves as the real parties in interest.
Pet. 78; Paper 4, 2 (Patent Owner's Mandatory Notices).

C. Related Matters

The parties identify the following matters in which the '436 patent has been asserted. Pet. 78–79; Paper 4, 2:

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

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

Lionra Technologies Limited v. Palo Alto Networks, Inc., Case No. 2:22-cv-00334 (E.D. Tex.) (filed Aug. 29, 2022).

We also note that Petitioner challenges U.S. Pat. No. 8,566,612, which claims priority to the '436 patent, in IPR2023-00703.

D. Prior Art and Asserted Grounds

Petitioner's grounds rely on the following prior art references:

Name	Reference	Exhibit No.
Wu	US 7,424,744 B1, iss. Sept. 9, 2008	1005
Krishna	US 7,996,670 B1, iss. Aug. 9, 2011	1006
Collins	US PG Pub. 2002/0073316 A1, pub. June 13, 2002	1008
Pham	US PG Pub. 2003/0074473 A1, pub. Apr. 17 2003	1004

Petitioner asserts that the challenged claims would have been unpatentable on the following grounds:

Claim(s) Challenged	35 U.S.C. §	Reference(s)/Basis
1, 2, 9–13, 16, 22	103	Pham, Wu
3, 14, 21	103	Pham, Wu, Collins

Claim(s) Challenged	35 U.S.C. §	Reference(s)/Basis
4, 7, 8	103	Pham, Wu, Collins, Krishna
17	103	Pham, Wu, Krishna

E. Background and Overview of the '436 Patent

According to the '436 patent:

A security processor performs all or substantially all security and network processing to provide a secure I/O interface system to protect computing hardware from unauthorized access or attack. The security processor sends and receives all incoming and outgoing data packets for a host device and includes a packet engine, coupled to a local data bus, to process the incoming and outgoing packets. The processor further composes 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.

Figure 2 of the '436 patent shows this arrangement, and is reproduced below with highlighting added by Petitioner.

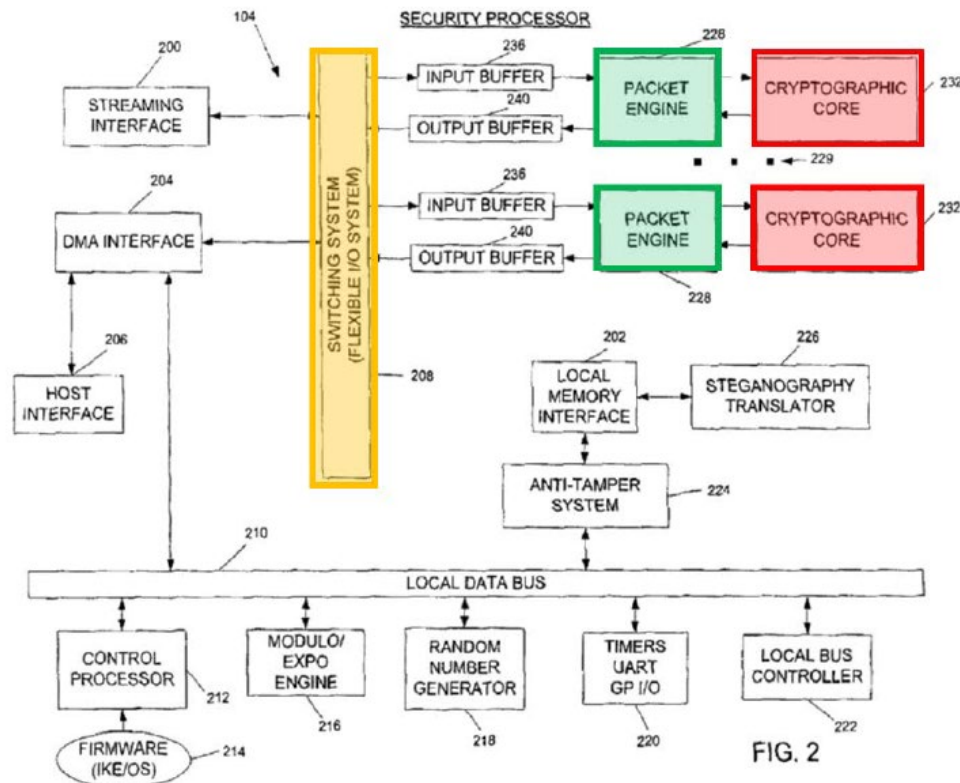


FIG. 2

Pet. 2; *see also* Ex. 1001, Fig. 2. In particular, security processor 104 includes switching system 208 (yellow), packet engines 228 (green), and cryptographic cores 232 (red).

F. Challenged Claims

Claims 1–4, 7–14, 16, 17, 21 and 22 are challenged. Claims 1 and 13 are independent. Claim 1 is reproduced below.

1. A security processor to process incoming packets and outgoing packets, the security processor comprising:

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

a packet engine, coupled to the switching system, to handle classification processing for the incoming packets received by the packet engine from the switching system and the outgoing packets sent by the packet engine to the switching

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

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

a signature database; and

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

Ex. 1001, 24:10–39.

Notably, claim 1 of the '436 patent is effectively identical to claim 1 of the '612 patent (challenged in IPR2023-00703), except claim 1 of the '612 patent removes the “tagging” limitation.

II. REQUEST FOR DISCRETIONARY DENIAL

Patent Owner asserts that we should deny institution under *Fintiv* based on the related district court matters identified above. Prelim. Resp. 1–12; *see Apple Inc. v. Fintiv, Inc.*, IPR2020-00019, Paper 11 at 11–12 (PTAB Mar. 20, 2020) (precedential) (holding that PTAB has discretion to deny institution in certain circumstances where there are parallel district court proceedings). Our analysis under *Fintiv* is guided by the USPTO Director's

Memorandum issued on June 21, 2022, titled “Interim Procedure for Discretionary Denials in AIA Post Grant Proceedings with Parallel District Court Litigation” (“Director’s Memo”). Pursuant to the Director’s Memo, we “will not discretionarily deny institution . . . where a petitioner presents a [*Sotera*] stipulation.” Director’s Memo at 3 (citing *Sotera Wireless, Inc. v. Masimo Corp.*, IPR2020-01019, Paper 12 (PTAB Dec. 1, 2020) (precedential as to § II.A)). Because Petitioner has offered a stipulation like in *Sotera*, i.e., to “not pursue in the co-pending district court litigation the specific ground asserted in the petition, or any other ground that was raised or could have been reasonably raised in an IPR (i.e., grounds that could have been raised under §§ 102 or 103 on the basis of prior art patent or printed publications)” (Paper 8, Appendix A at 2), we do not discretionarily deny institution under *Fintiv*.

III. MERITS ANALYSIS

A. Legal Standards Used in the Merits Analysis

“In an IPR, the petitioner has the burden from the onset to show with particularity why the patent it challenges is unpatentable.” *Harmonic Inc. v. Avid Tech., Inc.*, 815 F.3d 1356, 1363 (Fed. Cir. 2016) (citing 35 U.S.C. § 312(a)(3) (requiring *inter partes* review petitions to identify “with particularity . . . the evidence that supports the grounds for the challenge to each claim”)); *Dynamic Drinkware, LLC v. Nat’l Graphics, Inc.*, 800 F.3d 1375, 1378 (Fed. Cir. 2015) (discussing the burden of proof in *inter partes* review).

A claim is unpatentable under 35 U.S.C. § 103 if “the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious . . . to a person

having ordinary skill in the art to which said subject matter pertains.” *KSR Int’l Co. v. Teleflex Inc.*, 550 U.S. 398, 406 (2007). The question of obviousness is resolved on the basis of underlying factual determinations, including: (1) the scope and content of the prior art; (2) any differences between the claimed subject matter and the prior art; (3) the level of skill in the art; and (4) when in evidence, objective evidence of non-obviousness, i.e., secondary considerations. *Graham v. John Deere Co. of Kansas City*, 383 U.S. 1, 17–18 (1966).

B. Level of Ordinary Skill in the Art

Petitioner asserts that a person of ordinary skill in the art:

would have a Bachelor’s degree in computer science, computer engineering, or a related discipline, and 3–4 years of experience in computer networking with an emphasis on packet processing systems including traffic monitoring, inspection, and encryption/decryption systems. More experience could compensate for less formal education and vice versa.

Pet. 14–15.

Patent Owner did not offer a level of ordinary skill in the art in its preliminary response. We adopt Petitioner’s definition for purposes of this Decision, which appears consistent with the level of disclosure provided in the ’436 patent and the prior art cited.

C. Claim Construction

Neither party offers any claim constructions, nor do we see a need to construe any terms in order to make this Decision. *See Realtime Data, LLC v. Iancu*, 912 F.3d 1368, 1375 (Fed. Cir. 2019) (“The Board is required to construe ‘only those terms. . . that are in controversy, and only to the extent

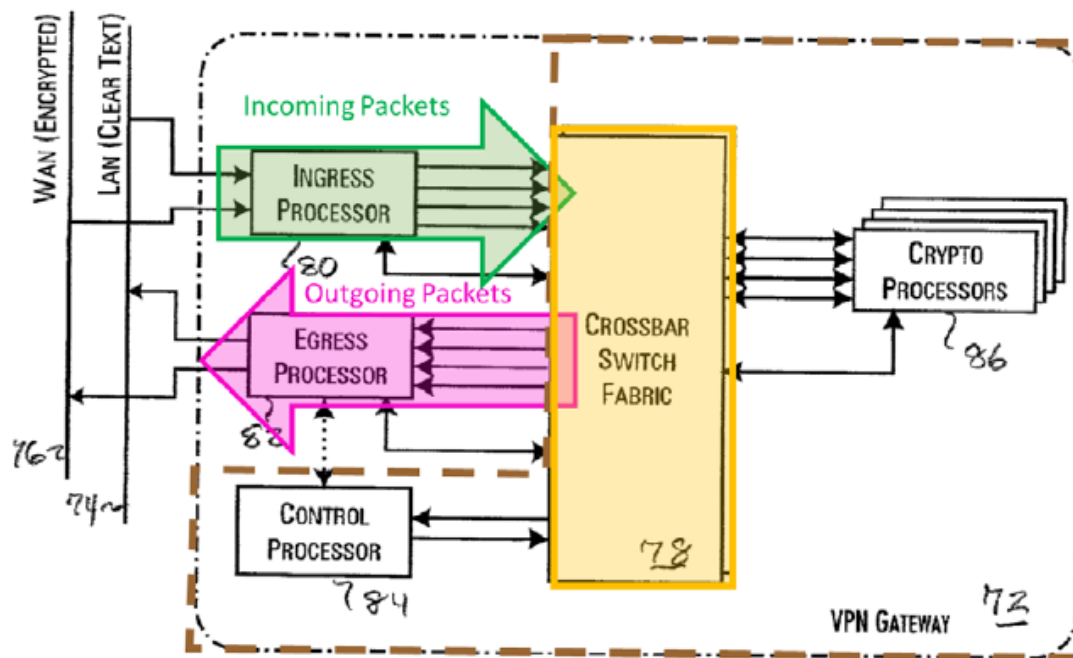
necessary to resolve the controversy.’”) (quoting *Vivid Techs., Inc. v. Am. Sci. & Eng’g, Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999)).

D. Asserted Obviousness

Petitioner asserts that claims 1, 2, 9–13, 16, and 22 would have been obvious in view of Pham and Wu. Pet. 21–64. Petitioner asserts that claims 3, 14, and 21 would have been obvious in view of Pham, Wu, and Collins (*id.* at 64–69); that claims 4, 7, and 8 would have been obvious in view of Pham, Wu, Collins, and Krishna (*id.* at 69–72); and that claim 17 would have been obvious in view of Pham, Wu, and Krishna (*id.* at 72–73). Patent Owner does not offer any arguments on the merits at this time.

We focus our analysis on claim 1. At a high level, claim 1 is directed to a security processor made of (1) a ***switching system*** to send and receive incoming packets, (2) a ***packet engine*** coupled to the switching system, (3) a ***cryptographic core*** coupled to the packet engine, and (4) a ***signature database*** sitting between the packet engine and the cryptographic core.

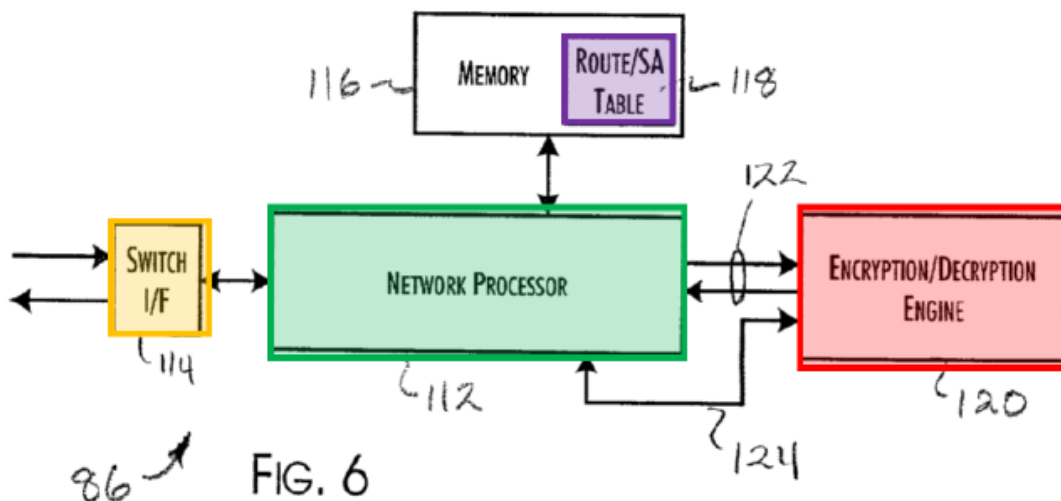
According to Petitioner, Pham discloses a security processor for ingress and egress processing of packets. Pet. 33. Petitioner asserts that Pham discloses a switching system to send the outgoing packets and receive the incoming packets. *Id.* at 33–36. In particular, Petitioner identifies crossbar switch fabric 78 as the claimed **switching system**. *Id.* at 35. This is illustrated in Figure 4 of Pham, reproduced below with highlighting and annotations by Petitioner:



Ex. 1004, Fig. 4

Pet. 36; *see also* Ex. 1004, Fig. 4. Figure 4 of Pham, as annotated by Petitioner, shows switch fabric 78 (yellow), which communicates with WAN 76 and LAN 74 through ingress processor 80 (green) and egress processor 82 (purple). Figure 4 of Pham further depicts that switch fabric 78 is connected to several crypto processors 86.

According to Petitioner, crypto processors 86 in Pham each include a network processor 112 functioning as the claimed *packet engine*. This is illustrated in Figure 6 of Pham, reproduced below with annotations by Petitioner:



Pet. 48; *see also* Ex. 1004, Fig. 6. Figure 6 shows an implementation of one of the crypto processors 86. Ex. 1004 ¶¶ 51–53; *see also id.*, Fig. 4 (noting a depiction of plural crypto processors 86 connected to switch fabric 78). Figure 6, as annotated by Petitioner above, depicts switch interface 114 (yellow), network processor 112 (green), encryption and decryption engine 120 (red), and data table 118 (purple).

Pham describes that crypto processors 86 associate received data packets with SA (secure authority) parameter data using data table 118. *Id.* ¶ 51; *see also id.* ¶¶ 71–72. According to Petitioner, network processor 112 performs the claimed tagging process when it provides the incoming and outgoing packets with header information and an IP tunneling header. Pet. 43–46. Petitioner also notes that Pham discloses the claimed *cryptographic core* (encryption/decryption engine 120), and that the packet

engine (network processor 112) is interposed between the switching system (switch fabric 78, switch fabric interface 114) and the cryptographic core. *Id.* at 46–50; *see also* Ex. 1004, Fig. 6 (noting network processor 112 (green) between switch fabric interface 114 (yellow) and encryption/decryption engine 120 (red)).

Lastly, Petitioner notes that Wu discloses the claimed ***signature database*** and intrusion detection system. Pet. 50–53. In particular, Petitioner notes that Wu discloses a “signature engine 34 [that] compares packets from the network traffic with such attack signatures such that policy violations can be discovered.” *Id.* at 52 (quoting Ex. 1005, 5:23–29). Petitioner asserts that it would have been obvious to add the intrusion detection system discussed in Wu to Pham’s network security system between the cryptographic core and the packet engine in order to gain the benefits of that intrusion detection system. *Id.* at 26–32. Petitioner explains that devices such as that disclosed in Wu should be placed where it can inspect unencrypted traffic in the first possible moment, which in the case of Pham would be adjacent the encryption/decryption engine 120 (i.e., between the cryptographic core and the packet engine, as claimed). *Id.* at 30–32.

Reviewing Petitioner’s analysis of claim 1, we determine that Petitioner has established a reasonable likelihood of success in showing that claim 1 would have been obvious in view of Pham and Wu. The three remaining grounds are also based on a similar combination of Pham and Wu, and add one or more references to address features in dependent claims. As mentioned above, Patent Owner has not argued the merits of the case at this time.

IV. CONCLUSION

For the reasons given above, we determine that Petitioner has established a reasonable likelihood of success in showing that claim 1 would have been obvious in view of Pham and Wu. Accordingly, we institute *inter partes* review on all challenged claims and grounds. 37 C.F.R. § 42.108(a) (“When instituting . . . review, the Board will authorize the review to proceed on all of the challenged claims and on all grounds of unpatentability asserted for each claim.”).

V. ORDER

In consideration of the foregoing, it is hereby:

ORDERED that *inter partes* review of claims 1–4, 7–14, 16, 17, 21 and 22 of the ’436 patent is instituted with respect to all grounds set forth in the Petition;

FURTHER ORDERED that pursuant to 35 U.S.C. § 314(a), the *inter partes* review of the ’436 patent commences on the entry date of this Decision, and pursuant to 35 U.S.C. § 314(c) and 37 C.F.R. § 42.4, notice is hereby given of the institution of a trial.

IPR2023-00673
Patent 7,685,436 B2

FOR PETITIONER:

Monté T. Squire
Patrick McPherson
Paul H. Belnap
Patrick C. Muldoon
D. Joseph English
Nicole Candelori
DUANE MORRIS LLP
mtsquire@duanemorris.com
pdmcperson@duanemorris.com
phbelnap@duanemorris.com
pcmuldoon@duanemorris.com
djenglish@duanemorris.com
ncandelori@duanemorris.com

FOR PATENT OWNER:

Brett Cooper
BC LAW GROUP, P.C.
bcooper@bc-lawgroup.com

Robert A. Auchter
AUCHTER PLLC
robert@auchterlaw.com