

IN THE UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF DELAWARE

JUNIPER NETWORKS, INC.,	)	
	)	
Plaintiff,	)	
	)	
v.	)	Civ. No. 11-1258-SLR
	)	
PALO ALTO NETWORKS, INC.,	)	
	)	
Defendant.	)	

---

Jack B. Blumenfeld, Esquire and Jennifer Ying, Esquire of Morris, Nichols, Arsht & Tunnell LLP, Wilmington, Delaware. Counsel for Plaintiff. Of Counsel: Morgan Chu, Esquire, Jonathan S. Kagan, Esquire and Lisa Glasser, Esquire of Irell & Manella LLP.

Phillip A. Rovner, Esquire and Jonathan A. Choa of Potter Anderson & Corroon LLP, Wilmington, Delaware. Counsel for Defendant. Of Counsel: Daralyn J. Durie, Esquire, Ragesh K. Tangri, Esquire, Ryan M. Kent, Esquire, Sonali D. Maitra, Esquire, and Brian C. Howard, Esquire of Durie Tangri LLP.

---

**MEMORANDUM OPINION**

Dated: February 6, 2014  
Wilmington, Delaware

  
ROBINSON District Judge

## I. INTRODUCTION

On December 19, 2011, Juniper Networks Inc. (“Juniper”), a Delaware corporation involved in the design, manufacture and sale of firewall technologies, filed suit against Palo Alto Networks, Inc. (“PAN”), another Delaware-based corporation in the same industry, alleging infringement of United States Patent Nos. 8,077,723 (“the ‘723 patent”); 7,779,459 (“the ‘459 patent”); 7,650,634 (“the ‘634 patent”); 7,302,700 (“the ‘700 patent”); 7,093,280 (“the ‘280 patent”); and 6,772,347 (“the ‘347 patent”). (D.I. 1) Defendant answered plaintiff’s complaint on February 9, 2012, affirmatively asserting that the patents were invalid. (D.I. 9) On September 25, 2012, Juniper filed a first amended complaint adding claims for infringement of U.S. Patent No. 7,734,752 (“the ‘752 patent”); and 7,107,612 (“the ‘612 patent”).<sup>1</sup> (D.I. 70)

Juniper is a leading manufacturer of computer networking technologies, including firewalls. (D.I. 1 at ¶ 1) In April 2004, Juniper bought the company NetScreen, an industry innovator in high-end network security devices, for \$4 billion; NetScreen’s intellectual property rights were included as a part of this acquisition. (*Id.* at ¶ 13) Yuming Mao (“Mao”) and Nir Zuk (“Zuk”), employees of NetScreen, began working for Juniper after the acquisition. (*Id.* at ¶ 14) Zuk left Juniper in February 2005 to start PAN, which also develops firewall devices. (D.I. 21 at 3) In January of 2006, Mao left Juniper for employment at PAN. (*Id.*)

Presently before the court are several motions: Juniper’s motion for summary judgment of assignor estoppel (D.I. 172); competing motions for summary judgment of

---

<sup>1</sup>The ‘280 patent was not included in this filing.

validity of the '612 and '347 patents (D.I. 170; D.I. 204); and competing motions for summary judgment regarding infringement (D.I. 176; D.I. 202). The court has jurisdiction pursuant to 28 U.S.C. §§ 1331 and 1338(a).

## II. STANDARD OF REVIEW

“The court shall grant summary judgment if the movant shows that there is no genuine dispute as to any material fact and the movant is entitled to judgment as a matter of law.” Fed. R. Civ. P. 56(a). The moving party bears the burden of demonstrating the absence of a genuine issue of material fact. *Matsushita Elec. Indus. Co. v. Zenith Radio Corp.*, 415 U.S. 574, 586 n.10 (1986). A party asserting that a fact cannot be—or, alternatively, is—genuinely disputed must support the assertion either by citing to “particular parts of materials in the record, including depositions, documents, electronically stored information, affidavits or declarations, stipulations (including those made for the purposes of the motions only), admissions, interrogatory answers, or other materials,” or by “showing that the materials cited do not establish the absence or presence of a genuine dispute, or that an adverse party cannot produce admissible evidence to support the fact.” Fed. R. Civ. P. 56(c)(1)(A) & (B). If the moving party has carried its burden, the nonmovant must then “come forward with specific facts showing that there is a genuine issue for trial.” *Matsushita*, 415 U.S. at 587 (internal quotation marks omitted). The court will “draw all reasonable inferences in favor of the nonmoving party, and it may not make credibility determinations or weigh the evidence.” *Reeves v. Sanderson Plumbing Prods., Inc.*, 530 U.S. 133, 150 (2000).

To defeat a motion for summary judgment, the non-moving party must “do more

than simply show that there is some metaphysical doubt as to the material facts.” *Matsushita*, 475 U.S. at 586-87; see also *Podohnik v. U.S. Postal Service*, 409 F.3d 584, 594 (3d Cir. 2005) (stating party opposing summary judgment “must present more than just bare assertions, conclusory allegations or suspicions to show the existence of a genuine issue”) (internal quotation marks omitted). Although the “mere existence of some alleged factual dispute between the parties will not defeat an otherwise properly supported motion for summary judgment,” a factual dispute is genuine where “the evidence is such that a reasonable jury could return a verdict for the nonmoving party.” *Anderson v. Liberty Lobby, Inc.*, 411 U.S. 242, 247-48 (1986). “If the evidence is merely colorable, or is not significantly probative, summary judgment may be granted.” *Id.* at 249-50 (internal citations omitted); see also *Celotex Corp. v. Catrett*, 411 U.S. 317, 322 (1986) (stating entry of summary judgment is mandated “against a party who fails to make a showing sufficient to establish the existence of an element essential to that party’s case, and on which that party will bear the burden of proof at trial”).

### **III. ASSIGNOR ESTOPPEL**

The court previously found that the doctrine of assignor estoppel negated PAN’s affirmative defense of invalidity of the ‘634 patent. (D.I. 53, D.I. 54) The parties stipulated that this ruling applied to the ‘752 patent. (D.I. 80) As to the ‘700, ‘347, ‘723 and ‘459 patents, the court found that issues of material fact precluded resolution of the issue, because privity is determined based upon a balancing of the equities, a fact-sensitive inquiry that must be resolved outside the pleadings. (D.I. 80)

In *Diamond Scientific Co. v. Ambico, Inc.*, 848 F.2d 1220, 1224 (Fed. Cir. 1988),

the Federal Circuit reaffirmed the existence of the doctrine of assignor estoppel. As the court explained, “[a]ssignor estoppel is an equitable doctrine that prevents one who assigned the rights to a patent (or patent application) from later contending that what was assigned is a nullity. The estoppel also operates to bar other parties in privity with the assignor, such as a corporation founded by the assignor.” *Id.* As the Court explained, the doctrine recognizes “the implicit representation by the assignor that the patent rights that he is assigning (presumably for value) are not worthless . . . . To allow the assignor to make that representation at the time of the assignment (to his advantage) and later to repudiate it (again to his advantage) could work an injustice against the assignee.” *Id.* After concluding that assignor estoppel remained a valid defense, the Federal Circuit stated that an analysis of the doctrine “must be concerned mainly with the balance of equities between the parties.” *Id.* at 1225.

The Federal Circuit, in *Shamrock Technologies, Inc. v. Medical Sterilization, Inc.*, 903 F.2d 789, 793 (Fed. Cir. 1990), reiterated that “[a]ssignor estoppel is an equitable doctrine . . . that is mainly concerned with the balance of the equities between the parties . . . [and t]hose in privity with the assignor partake of that balance; hence, extension of the estoppel to those in privity is justified.”<sup>2</sup> The *Shamrock* Court went on to explain that, “[p]rivity, like the doctrine of assignor estoppel itself, is determined upon a balance of equities.” *Id.* In other words, “[i]f an inventor assigns his invention to his employer company A and leaves to join company B, whether company B is in privity and thus bound by the doctrine will depend on the equities dictated by the relationship

---

<sup>2</sup>As such, PAN’s arguments that the doctrine is outdated and should not be applied are not addressed.

between the inventor and company B in light of the act of infringement.” *Id.* at 793.

“The closer that relationship, the more the equities will favor applying the doctrine to company B.” *Id.*

In the case at bar, Mao and/or Zuk are listed as inventors on each of the ‘723, ‘459, ‘700, ‘347, and ‘612 patents. (See ‘723 patent listing Mao and Zuk as inventors; ‘459 patent listing Mao as an inventor; ‘700 patent listing Mao as an inventor; ‘347 patent listing Mao as an inventor; and ‘612 patent listing Mao as an inventor) With the exception of the ‘723 patent,<sup>3</sup> Mao and Zuk also signed inventor’s oaths averring that they were the “first” and “original” inventors of the respectively claimed subject matter.<sup>4</sup> (See D.I. 174 at exs. 1, 3, 5) Furthermore, either Mao or Zuk assigned the “entire right, title and interest” of each of the claimed inventions to either NetScreen or Juniper for “valuable consideration.”<sup>5</sup> (See D.I. 174 at exs. 1-7)

---

<sup>3</sup>Zuk did not sign an inventor’s oath or assignment for the ‘723 patent, which will be discussed below.

<sup>4</sup>In its brief, PAN emphasizes that the ‘723 and ‘459 patents issued from continuation applications that neither Zuk nor Mao ever assigned or attested to being the first inventors of and that all the patents-in-suit (except the ‘347 patent) issued after Zuk and Mao left Juniper. (D.I. 200 at 4-5) The *Diamond* Court explained that these arguments are “irrelevant” to the issue of assignor estoppel. *Diamond*, 848 F.2d at 1226. Accordingly, those facts are not addressed in any further detail.

<sup>5</sup>PAN’s argument that the assignments are void under California law is foreclosed by the contrary findings of the Federal Circuit. *Bd. of Trs. of the Leland Stanford Junior Univ. v. Roche Molecular Sys.*, 583 F.3d 832, 845-56 (Fed. Cir. 2009), *aff’d*, 131 S. Ct. 2188 (2011) (rejecting § 16600 challenge and noting that “California courts apply section 16600 to employment restrictions on departing employees, not to patent assignments”); *see also Nir Zuk et al. v. Juniper Networks, Inc.*, No. 113CV253876 (Cal. Super. January 15, 2014) (striking Zuk and PAN’s complaint, which sought to enjoin Juniper from asserting assignor estoppel in this court, alleging that Juniper’s invocation of that doctrine in this court violated California state law).

Mao requested and received the title “founder and chief architect” when he joined PAN. (D.I. 22 at ¶ 7) Zuk testified that he “is not a title person” and has no problem with Mao having the title founder. (D.I. 174, ex. 17 128:2-130:19) Mao has consistently held himself out as a founder (including to customers) and PAN’s website describes him as such. (D.I. 174, exs. 9, 11, 12, 14, 16 at 583:24-584:7, 584:20-585:3) In 2010, PAN recognized Mao as its founder and commended his efforts in its China market. (*Id.*, ex. 29) While a November 2005 presentation delivered to investors did not list Mao as a founder, a December 2005 presentation listed Mao as a member of the “Founding Team.”<sup>6</sup> (D.I. 24, ex. B at 4; D.I. 174, ex. 7) The court concludes that, while Mao requested the title of sole founder when he joined PAN, he and PAN have consistently held him out to be at least a founder. Therefore, this fact is dispositive of the issue of privity. *Diamond*, 848 F.2d at 1224 (finding that “[t]he estoppel also operates to bar other parties in privity with the assignor, such as a corporation founded by the assignor).

For completeness, the court turns to the balance of equities and the relationship of Mao and PAN. Zuk testified that he “needed Yuming Mao to work mostly on the connections between the hardware and the software, because that’s an area [he] had no expertise in . . . .”<sup>7</sup> (D.I. 174, ex. 18 at 488:24-489:25) PAN began discussions with Mao in November 2005 and Mao formally joined PAN on January 25, 2006. (D.I. 174,

---

<sup>6</sup>PAN’s argument that the metadata for the file shows that it was last modified on March 22, 2006 is not conclusive of what the content was at any moment in time.

<sup>7</sup>After listing several job functions, it is unclear what Zuk is referring to when he states that Mao “was not necessarily the right person to do that . . . .” (D.I. 489 at 489:10-14)

ex. 19 at 28:2-9, ex. 7, ex. 8) After joining PAN, Mao received an option to purchase 654,520 shares of PAN stock, which he exercised on November 22, 2006. (D.I. 174, ex. 46, 47; ex. 15 at 122:15-123:2) Mao “had the responsibility for overall architecture of the system . . . .” (D.I. 174, ex. 28 at PAN526928)

While the investment presentations outlined the core functions and schema that resulted in the PA-4000 series of products, PAN was in the early stages of product development at the time Mao started work, with “maybe 1 or 2 percent of the product . . . done . . .” and no prototype. (D.I. 201, ex. 1 at 253:24-254:16, 260:1-261:7, 264:11-266:2; D.I. 174, ex. 19 at 81:11-14, 84:15-19, ex. 27) Mao wrote an early technical specification relating to the PA-4000 series. (D.I. 174, ex. 32) That Mao could not recall if these features were implemented into the product is not dispositive, as the query is whether Mao was closely involved in the development of products and with the company. (D.I. 201, ex. 1 at 573:3-14) Mao testified to his involvement in the product’s development (including specific examples of product features) and his critical role with PAN. (See e.g., D.I. 174, ex. 15 at 289:9-290:20, 296:9-14, 300:1-10, 305:23-306:7, 516:21-519:15) Considering the balance of equities and the relationship of Mao and PAN, the evidence demonstrates that Mao is in privity with PAN, therefore, the Mao patents are subject to assignor estoppel.

As to the ‘723 patent, Zuk’s employment contract with NetScreen included an agreement to assign his inventions to NetScreen, which PAN does not dispute. (D.I. 173 at 17; D.I. 174, exs. 20, 48) Juniper diligently sought an executed assignment and oath from Zuk, however, Zuk declined to comply with the requests. Juniper filed the application with the PTO and was allowed to proceed without Zuk’s signature. The



court concludes that the employment contract properly assigned the patent to Juniper.<sup>8</sup> Therefore, as Zuk is a founder of PAN and based on the above analysis as to Mao, the '723 patent falls squarely within the holding of *Diamond* and is subject to assignor estoppel.<sup>9</sup> (D.I. 9 at ¶ 3); *Diamond*, 848 F.2d at 1224-26.

#### **IV. CLAIM CONSTRUCTION AND INFRINGEMENT STANDARDS**

##### **A. Claim Construction**

Claim construction is a matter of law. *Phillips v. AWH Corp.*, 415 F.3d 1303, 1330 (Fed. Cir. 2005) (en banc). Claim construction focuses on intrinsic evidence - the claims, specification and prosecution history - because intrinsic evidence is "the most significant source of the legally operative meaning of disputed claim language." *Vitronics Corp. v. Conceptoronic, Inc.*, 90 F.3d 1576, 1582 (Fed. Cir. 1996); *Markman v. Westview Instruments, Inc.*, 52 F.3d 967, 979 (Fed. Cir. 1995) (en banc), *aff'd*, 517 U.S. 370 (1996). Claims must be interpreted from the perspective of one of ordinary skill in the relevant art at the time of the invention. *Phillips*, 415 F.3d at 1313.

Claim construction starts with the claims, *id.* at 1312, and remains centered on the words of the claims throughout. *Interactive Gift Express, Inc. v. Compuserve, Inc.*, 256 F.3d 1323, 1331 (Fed. Cir. 2001). In the absence of an express intent to impart different meaning to claim terms, the terms are presumed to have their ordinary meaning. *Id.* Claims, however, must be read in view of the specification and

---

<sup>8</sup>Zuk has not contested inventorship of the patent before this summary judgment practice and does not advance any actual evidence to support this argument herein.

<sup>9</sup>With the application of assignor estoppel to all patents-in-suit, the competing motions for summary judgment of validity for the patents-in-suit are denied as moot.

prosecution history. Indeed, the specification is often “the single best guide to the meaning of a disputed term.” *Phillips*, 415 F.3d at 1315.

## **B. Infringement**

A patent is infringed when a person “without authority makes, uses or sells any patented invention, within the United States . . . during the term of the patent.” 35 U.S.C. § 271(a). A two-step analysis is employed in making an infringement determination. See *Markman v. Westview Instruments, Inc.*, 52 F.3d 967, 976 (Fed. Cir. 1995). First, the court must construe the asserted claims to ascertain their meaning and scope. See *id.* Construction of the claims is a question of law subject to de novo review. See *Cybor Corp. v. FAS Techs.*, 138 F.3d 1448, 1454 (Fed. Cir. 1998). The trier of fact must then compare the properly construed claims with the accused infringing product. See *Markman*, 52 F.3d at 976. This second step is a question of fact. See *Bai v. L & L Wings, Inc.*, 160 F.3d 1350, 1353 (Fed. Cir. 1998).

“Direct infringement requires a party to perform each and every step or element of a claimed method or product.” *BMC Res., Inc. v. Paymentech, L.P.*, 498 F.3d 1373, 1378 (Fed. Cir. 2007), *overruled on other grounds by* 692 F.3d 1301 (Fed. Cir. 2012). “If any claim limitation is absent from the accused device, there is no literal infringement as a matter of law.” *Bayer AG v. Elan Pharm. Research Corp.*, 212 F.3d 1241, 1247 (Fed. Cir. 2000). If an accused product does not infringe an independent claim, it also does not infringe any claim depending thereon. See *Wahpeton Canvas Co. v. Frontier, Inc.*, 870 F.2d 1546, 1553 (Fed. Cir. 1989). However, “[o]ne may infringe an independent claim and not infringe a claim dependent on that claim.” *Monsanto Co. v.*

*Syngenta Seeds, Inc.*, 503 F.3d 1352, 1359 (Fed. Cir. 2007) (quoting *Wahpeton Canvas*, 870 F.2d at 1552) (internal quotations omitted). A product that does not literally infringe a patent claim may still infringe under the doctrine of equivalents if the differences between an individual limitation of the claimed invention and an element of the accused product are insubstantial. See *Warner-Jenkinson Co. v. Hilton Davis Chem. Co.*, 520 U.S. 17, 24 (1997). The patent owner has the burden of proving infringement and must meet its burden by a preponderance of the evidence. See *SmithKline Diagnostics, Inc. v. Helena Lab. Corp.*, 859 F.2d 878, 889 (Fed. Cir. 1988) (citations omitted).

When an accused infringer moves for summary judgment of non-infringement, such relief may be granted only if one or more limitations of the claim in question does not read on an element of the accused product, either literally or under the doctrine of equivalents. See *Chimie v. PPG Indus., Inc.*, 402 F.3d 1371, 1376 (Fed. Cir. 2005); see also *TechSearch, L.L.C. v. Intel Corp.*, 286 F.3d 1360, 1369 (Fed. Cir. 2002) (“Summary judgment of noninfringement is ... appropriate where the patent owner’s proof is deficient in meeting an essential part of the legal standard for infringement, because such failure will render all other facts immaterial.”). Thus, summary judgment of non-infringement can only be granted if, after viewing the facts in the light most favorable to the non-movant, there is no genuine issue as to whether the accused product is covered by the claims (as construed by the court). See *Pitney Bowes, Inc. v. Hewlett-Packard Co.*, 182 F.3d 1298, 1304 (Fed. Cir. 1999).

For there to be infringement under the doctrine of equivalents, the accused

product or process must embody every limitation of a claim, either literally or by an equivalent. *Warner-Jenkinson*, 520 U.S. at 41. An element is equivalent if the differences between the element and the claim limitation are “insubstantial.” *Zelinski v. Brunswick Corp.*, 185 F.3d 1311, 1316 (Fed. Cir. 1999). One test used to determine “insubstantiality” is whether the element performs substantially the same function in substantially the same way to obtain substantially the same result as the claim limitation. *See Graver Tank & Mfg. Co. v. Linde Air Products Co.*, 339 U.S. 605, 608 (1950). This test is commonly referred to as the “function-way-result” test. The mere showing that an accused device is equivalent overall to the claimed invention is insufficient to establish infringement under the doctrine of equivalents. The patent owner has the burden of proving infringement under the doctrine of equivalents and must meet its burden by a preponderance of the evidence. *See SmithKline Diagnostics, Inc. v. Helena Lab. Corp.*, 859 F.2d 878, 889 (Fed. Cir. 1988) (citations omitted).

The doctrine of equivalents is limited by the doctrine of prosecution history estoppel. In *Festo Corp. v. Shoketsu Kinzoku Kogyo Kabushiki Co., Ltd.*, 535 U.S. 722 (2002) (“*Festo VII*”), the Supreme Court stated:

Prosecution history estoppel ensures that the doctrine of equivalents remains tied to its underlying purpose. Where the original application once embraced the purported equivalent but the patentee narrowed his claims to obtain the patent or to protect its validity, the patentee cannot assert that he lacked the words to describe the subject matter in question. The doctrine of equivalents is premised on language’s inability to capture the essence of innovation, but a prior application describing the precise element at issue undercuts that premise. In that instance the

prosecution history has established that the inventor turned his attention to the subject matter in question, knew the words for both the broader and narrower claim, and affirmatively chose the latter.

*Id.* at 734-735. In other words, the prosecution history of a patent, as the public record of the patent proceedings, serves the important function of identifying the boundaries of the patentee's property rights. Once a patentee has narrowed the scope of a patent claim as a condition of receiving a patent, the patentee may not recapture the subject matter surrendered. In order for prosecution history estoppel to apply, however, there must be a deliberate and express surrender of subject matter. *See Southwall Tech., Inc. v. Cardinal IG Co.*, 54 F.3d 1570, 1580 (Fed. Cir. 1995).

Once a court has determined that prosecution history estoppel applies, it must determine the scope of the estoppel. *See id.* This requires an objective examination into the reason for and nature of the surrendered subject matter. *Id.*; *see also Augustine Med., Inc. v. Gaymar Indus., Inc.*, 181 F.3d 1291, 1299 (Fed. Cir. 1999). If one of ordinary skill in the art would consider the accused product to be surrendered subject matter, then the doctrine of equivalents cannot be used to claim infringement by the accused product; i.e., prosecution history estoppel necessarily applies. *Augustine Med.*, 181 F.3d at 1298. In addition, a "patentee may not assert coverage of a 'trivial' variation of the distinguished prior art feature as an equivalent." *Id.* at 1299 (quoting *Litton Sys., Inc. v. Honeywell, Inc.*, 140 F.3d 1449, 1454 (Fed. Cir. 1998)).

"[A] narrowing amendment made to satisfy any requirement of the Patent Act" creates a presumption that "the patentee surrendered all subject matter between the broader and the narrower language" and bars any equivalents. *Festo VII.*, 535 U.S. at

736, 740; see also *Honeywell Int'l, Inc. v. Hamilton Sundstrand*, 370 F.3d 1131, 1139 (Fed. Cir. 2004) (prosecution history estoppel “bar[s] the patentee from asserting equivalents if the scope of the claims has been narrowed by an amendment during prosecution.”).

Thus, a presumption of prosecution history estoppel is established by showing that the patentee made a narrowing amendment and that “the reason for that amendment was a substantial one relating to patentability.” *Festo Corp. v. Shoketsu Kinzoku Kogyo Kabushiki Co.*, 344 F.3d 1359, 1366 (Fed. Cir. 2003) (en banc). There are three exceptions to this presumption: (1) the equivalent was “unforeseeable at the time of the narrowing amendment”; (2) the rationale for the amendment “bore no more than a tangential relation to the equivalent in question”; or (3) “some other reason suggested that the patentee could not reasonably have been expected to describe the alleged equivalent.” *Festo VII.*, 535 U.S. at 740-41.

## **V. DISCUSSION**

The patents-in-suit are directed to inventions for computer networks and systems using hardware, software, or combinations thereof. Physical hardware encompasses components such as circuits, wires, and computer chips (e.g., a central processing unit or “CPU”). One chip may contain multiple hardware components, such as electronic switches (e.g., transistors or logic gates).

Computer systems use memory to facilitate the storage and manipulation of software and other data. Memory comes in numerous varieties and can be shared by multiple other components in a system. There are two primary ways of sending data in

memory to parts of a computer system that need to use it. The first is to create a new copy of the data in a new memory location sometimes called “passing by value,” and the second is to communicate a “pointer” to the location in memory where the data is held, sometimes called “passing by reference.” Data may be structured or organized in memory to facilitate its use. For example, data may be grouped into larger structures of multiple (often related) data values, and formatted depending on how the data entries are to be looked up and accessed. Data elements can be organized sequentially in a “linked list,” or for fast lookup in a “hash table.”

Computers systems may be connected via networks (like the internet). Data is broken down into packets (with additional metadata) to communicate. A common format for data packets includes multiple layers of metadata information, each corresponding to a particular networking function. Firewalls are designed to permit or deny network transmissions based upon a set of rules, and are frequently used to protect networks from unauthorized access while permitting legitimate communications to pass. As such, firewalls are critical to running secure networks.

For each of the patents-in-suit, the court will discuss any specific background technology, any necessary claim construction on summary judgment, and any infringement issues on summary judgment.

#### **A. The ‘634 Patent**

The ‘634 patent describes the use of “plural security devices but only one flow table,” which “can result in faster response time” in network security. (2:13-26 and fig.1) The single flow table improves the efficiency of packet processing in a network security device. The integration of multiple security devices for network security combines the

strengths (and mitigates the limitations) of various types of security devices, for example, a firewall or an intrusion prevention system (IPS). (1:15-2:9; 2:56-3:12)

Independent claim 1 recites:

A method for inspecting data packets associated with a flow in a computer network, the computer network including two or more security devices for processing the data packets, each data packet having associated header data, the method comprising:

- receiving the data packet;
- examining the data packet;
- determining a single flow record associated with the data packet, where the determining includes:
  - determining a packet identifier using at least the associated header data;
  - evaluating a flow table for a matching flow record entry using the packet identifier;
  - when there is a matching flow record entry, retrieving the matching flow record;
  - when there is no matching flow record entry, creating a new flow record; and
  - storing the new flow record in the flow table;
- extracting flow instructions, a session ID and flow information, for the two or more security devices, from the single flow record and forwarding the flow instructions, the session ID and the flow information to the respective ones of the two or more security devices to facilitate processing of the data packet;
- receiving, from each of the two or more security devices, evaluation information, the evaluation information being generated by a respective one of the two or more security devices when processing the data packet; and
- processing the data packet using the evaluation information.

(7:10-40) Independent claim 19 recites:

A computer-readable memory device incorporating instructions for inspecting data packets associated with a flow in a computer network, the computer network including two or more security devices for processing data packets, each data packet having associated header data, the instructions to:

- receive the data packet;



examine the data packet;  
determine a single flow record associated with the data packet, where the instruction to determine the single flow packet include instructions to:  
determine a packet identifier using at least the associated header data;  
evaluate a flow table for a matching flow record entry using the packet identifier;  
retrieve a matching flow record when there is a matching flow record entry; and  
create a new flow record when there is no matching flow record entry, where the new flow record is stored in the flow record table;  
extract flow instructions, a session ID and flow information, for the two or more security devices, from the single flow record and forward the flow instructions, the session ID and the flow information to the respective ones of the two or more security devices to facilitate processing of the data packet;  
receive, from each of the two or more security devices, evaluation information, the evaluation information being generated by a respective one of the two or more security devices when processing the data packet; and  
processing the data packet using the evaluation information.

(8:34-65)

## 1. Claim limitations<sup>10</sup>

### a. “[T]wo or more security devices”

The court construes this limitation as “at least two physical devices, each of which performs a security function.” This is consistent with the specification, which provides examples of security devices, i.e., firewall, IPS, and flow based router. (See e.g., 4:19-23) Figure 9 describes “a network topology where a session module,

---

<sup>10</sup>As the court does not rely on the expert declarations submitted with claim construction (D.I. 165; D.I. 186), the court does not address the parties’ objections thereto. (D.I. 183; D.I. 197)

firewall, IPS and router are included in a single security device.” (2:48-50) According to the asserted claim language, each security device processes data<sup>11</sup> and the specification describes information being communicated to each security device, which receives information and returns results to the flow processing engine. (3:15-16, 4:32-55)

**b. “[E]xtracting flow instructions, a session ID and flow information, for the two or more security devices, from the single flow record and forwarding the flow instructions, the session ID and the flow information to the respective ones of the two or more security devices to facilitate processing of the data packet”**

“Unless the steps of a method actually recite an order, the steps are not ordinarily construed to require one. However, such a result can ensue when the method steps implicitly require that they be performed in the order written.” *Interactive Gift Express, Inc. v. Compuserve Inc.*, 256 F.3d 1323, 1342-43 (Fed. Cir. 2001). This limitation does not require that the “extracting” step occur before the “forwarding” step. The plain meaning of “forwarding” does not compel the conclusion that the “extraction” step must be performed first. *Mantech Envtl. Corp. v. Hudson Envtl. Servs., Inc.*, 152 F.3d 1368, 1375-76 (Fed. Cir. 1998) (holding that the steps of a method claim had to be performed in order, as each subsequent step referenced something logically indicating the prior step had been performed). Further, the specification states “the steps of the

---

<sup>11</sup>“Method steps of the invention can be performed by one or more programmable processors executing a computer program to perform functions of the invention by operating on input data and generating output.” (6:18-21)

invention can be performed in a different order and still achieve desirable results.” *Interactive Gift*, 256 F.3d at 1343 (directing courts to determine whether the rest of the specification “directly or implicitly requires such a narrow construction”).

## 2. Infringement

PAN’s technical and marketing documents describe the accused products as a “unique integration of software and hardware” and as “integrated by design.” (D.I. 179, ex. Q; D.I. 224, exs. BB, DD, EE) The accused products use multicore processors. (D.I. 224, exs. II at ¶¶ 6, KK) PAN argues that its accused products do not meet the “two or more security devices” claim limitation, as the PAN-OS software program is a single program and the App-ID and Content Inspection are intertwined functionalities thereof. (D.I. 211<sup>12</sup> at ¶¶ 42) However, PAN’s expert testified that he was “not sure” whether the PAN code compiled into a “single executable file.” (D.I. 224, ex. HH at 39:1-10) Juniper’s expert opined that the claim limitation is met as “the App-ID and Content Inspection are run on cores of one or more multi-core Cavium Octeon chips, and/or one or more Field Programmable Gate Arrays (FPGA).” (D.I. 178, ex. A at ¶¶ 302, 349-78) Zuk testified that “[t]he processing of a packet can happen on different cores.” (D.I. 179, ex. P at 163:2-165:6) There exists a genuine issue of material fact regarding whether the accused products meet the claim limitation. The parties’ competing motions for summary judgment are denied.

---

<sup>12</sup>PAN’s citations throughout its briefing to abbreviations (D.I. 203; D.I. 231 at iii) rather than D.I. #s is inconsistent with D. Del. LR 7.1.3(a)(6) and this judge’s preferences, added to the court’s burden in processing the papers filed in connection with the motion practice, and leaves the court wondering what PAN hoped to accomplish by randomly assigning abbreviations to some 20 documents, 18 of which had D.I. #’s.

The claim language recites, “the computer network including two or more security devices for processing data packets.” Citing to one question and answer in Juniper’s expert’s testimony,<sup>13</sup> PAN’s counsel argues that the AppID and Content Inspection are not separated from each other across a computer network, as required by this claim limitation.<sup>14</sup> (D.I. 203 at 12; D.I. 208, ex. F at 92:6-12) PAN also argues that the specification requires each device to have its own interface to the network. (D.I. 231 at 3) Similarly, with respect to the claim language requiring “extracting” and “forwarding” information, PAN offers attorney argument and citation to dictionary definitions to dispute the testimony and report of Juniper’s expert. (D.I. 203 at 14-15) Attorney argument is not evidence. PAN has not pointed to expert reports or other evidence to support its argument regarding the particular claim language at issue. Therefore, PAN, the movant, has not met its burden of persuasion. For these reasons, PAN’s motion for summary judgment is denied.

PAN argues that prosecution history estoppel prevents Juniper from arguing infringement based on the doctrine of equivalents. The original claim language required “the computer network having one or more devices for processing the packet” and “extracting flow instructions for two or more devices from the single flow record.” (D.I. 151, ex. 10 at JA-1140) The claims were amended to require “the computer network

---

<sup>13</sup>Q. . . . Are Content Inspection and application identification connected by a network? . . . A. They communicate over – in a multiprocessor system and not across a network.”

<sup>14</sup>Juniper responds that PAN’s products (with App-ID and Content-ID) are undisputedly “included” in a network as the claim language requires. (D.I. 223 at 23; D.I. 211 at ¶ 45; D.I. 178, ex. A at ¶ 299)

including two or more security devices” throughout. (*Id.* at JA-567-68) Juniper explained during reexamination that allowing “sub-components of [a] single security device” to meet the “two or more security devices” claim limitation would “effectively write[] the multiple ‘security devices’ limitation out of the claims.” (*Id.* at JA-3685) This amendment, along with the court’s construction of “two or more security devices,” precludes Juniper from arguing at trial that a single security device satisfies the “two or more security devices” claim limitations using the doctrine of equivalents. Therefore, the court grants PAN’s request for summary judgment in this regard.

### **B. The ‘347 Patent**

The ‘347 patent describes technology for efficient packet processing in a firewall, using “a first set of rules for sorting incoming IP packets into initially allowed packets and initially denied packets.” (Abstract) The initially denied packets are then processed or sorted into allowed or denied packets. (5:45-49) Denied packets are dropped, and allowed packets pass through the firewall. *Id.*

Independent claim 1 recites:

An apparatus comprising:  
a firewall engine including:  
    a first engine including a first set of rules for sorting incoming IP packets into initially allowed packets and initially denied packets; and  
    a filter including a second set of rules for receiving and further sorting the initially denied packets into allowed packets and denied packets.

(7:22-29) Independent claim 14 recites:

A method for providing network computer security,  
comprising:  
    receiving incoming packets at a firewall;

sorting the incoming packets into initially allowed packets and initially denied packets; and further sorting the initially denied packets into allowed and denied packets using rules.

(8:11-18)

## 1. Claim limitations

### a. “[Sorting/processing] ... packets into ... initially denied packets”

The specification describes “an engine for sorting incoming IP packets into initially allowed and denied packets using a fixed set of rules” and “further sort[ing] the initially denied packets into allowed packets and denied packets, using dynamically generated rules. The denied packets are dropped and the allowed packets are permitted to enter the network.” (3:5-14) Contrary to PAN’s suggestion, the term “drop” is consistently used in conjunction with finally denied packets. (*Id.*; fig.6) The court declines to construe this term, and in accordance with Juniper’s suggestion, the plain and ordinary meaning shall apply.

## 2. Infringement

Analyzing the source code, the parties’ experts reached opposing conclusions regarding whether the “default rule” satisfies the claim language. Juniper’s expert, Dr. Rubin, explained that received packets are “initially allowed” or “assigned the security action ‘deny.’ . . . An initially denied packet will ultimately be discarded, if it is not further sorted as an allowed packet, for example through the processing or sorting described below.” (D.I. 178, ex. A at ¶¶ 845-49) PAN’s expert, Dr. Mitzenmacher, explained that the “packets are not ‘initially denied’ because intra-zone packets are

allowed before a deny action is ever set for the packet.” (D.I. 211 at ¶ 157) Further, “the default action [cannot] itself be considered a set of ‘rules’ (plural), because there is only a single rule (if no other rule applies, deny the packet).” (*Id.* at ¶ 162) The court concludes that there exists a genuine issue of material fact regarding whether PAN’s accused products infringe the asserted claims. The competing motions for summary judgment are denied.<sup>15</sup>

### C. The ‘612 Patent

The ‘612 patent is a continuation of the ‘347 patent, and its claims are directed to a filter that applies “dynamically-generated rules” after the application of “fixed rules” by the ACL engine. (3:17-26, 6:35-47) The firewall engine dynamically adds or modifies rules based on a sequence of data packets received by a network. (3:9-12) The newly added or modified rules may (for example) be designed to respond to or mitigate a network attack identified based on analysis of data received.

Independent claim 1 recites:

A method, comprising:  
    establishing a set of rules for controlling access to  
    and from a network device for incoming and outgoing data  
    units;  
    receiving, at the network device, a first sequence of  
    data units; and  
    adding one or more first rules to the set of rules

---

<sup>15</sup>Juniper’s expert offered sufficient support for his theories under the doctrine of equivalents, incorporating his element by element analysis from his opinion regarding literal infringement. (D.I. 178, ex. A at ¶ 920, ex. B at ¶ 16) While PAN may disagree with these conclusions, this goes to the weight of the testimony and may be properly dealt with on cross-examination. PAN has not herein offered any evidence or expert report to contradict the opinions of Juniper’s expert. (D.I. 203 at 33-34) This lack of evidence does not meet PAN’s burden of persuasion, therefore, the court denies PAN’s motion for summary judgment as to infringement under the doctrine of equivalents.

based on data extracted from the received first sequence of data units.

(7:47-56) Independent claim 13 recites:

A network device, comprising:  
an access control engine configured to establish a set of rules for controlling access to and from the network device for incoming and outgoing data units; and  
a dynamic filter configured to add one or more first rules to the set of rules based on data extracted from a first sequence of data units received at the network device.

(8:61-67)

## 1. Claim limitations

### a. “[R]ules”

The parties agree that a “rule” must exist across multiple sessions. The background of the invention provides that “[r]ules specify actions to be applied as against certain packets.” (2:37-40) The specification distinguishes between “rules” and “look-up tables.” For example, “the firewall engine may first check a stored look-up table with criteria relating to ongoing current applications or services, before searching the rules,” and “packets . . . may be processed using the look-up table instead of a rule search.” (5:14-16, 40-42) A look-up table has “contents” and stores “information,” such as “the IP address, port and protocol corresponding to each current application or service.” (5:18-22) Further, information may be “written to the look-up table.” (5:39-40) The court construes the limitation as “actions to be applied against packets, as distinct from a look-up table, which is a data structure that stores information.”<sup>16</sup>

---

<sup>16</sup>The parties’ experts use the term “data structure” to describe flow tables. (D.I. 178, ex. A at ¶ 961; D.I. 211 at ¶ 192)



## 2. Infringement

PAN disputes (without reference to expert reports or testimony) that its products do not add rules dynamically as required by the claim language. Dr. Rubin explains that several features of the accused products, including SYN flood, Block IP and Reconnaissance Protection, perform this dynamic step. Dr. Rubin's testing showed that a new rule was added "in the event that traffic was detected attempting to download a particular file via FTP transfer." (D.I. 178, ex. A at ¶¶ 934-36, 957-58, 985)

The experts disagree on whether the Block IP feature uses entries stored in a look up table. Dr. Rubin opines that the "operation adds a block rule to the table . . ." and the entries are stored in a "hash table," which is different from a "look-up table." (D.I. 178, ex. A at ¶¶ 957-61; D.I. 149, ex. E at 90:13-15; D.I. 179, ex. B at 80:10-81:14, 82:3-83:25) On the other hand, Dr. Mitzenmacher opines that a "block table" is a "look-up table" and satisfies the claim limitation. (D.I. 211 at ¶ 192) The experts also disagree on whether the claim requires each rule to have "multiple matching criteria" and whether the rules used by the accused products contain "multiple criteria." (D.I. 178, ex. A at ¶¶ 933, 936; D.I. 211 at ¶¶ 192-193, 203) The court concludes that genuine issues of material fact exist and, therefore, the competing motions for summary judgment are denied.<sup>17, 18</sup>

---

<sup>17</sup>PAN's "practicing the prior art" defense is foreclosed by *Tate Access Floors v. Interface Archit. Resources*, 279 F. 3d 1357, 1369 (Fed. Cir. 2002). The Federal Circuit held "that there is no 'practicing the prior art' defense to literal infringement." *Id.* at 1366-69 (citing *Baxter Healthcare Corp. v. Spectramed, Inc.*, 49 F.3d 1575, 1583 (Fed. Cir. 1995)).

<sup>18</sup>Ensnarement bars a patentee from asserting a scope of equivalency that would encompass, or "ensnare," the prior art. See *Wilson Sporting Goods Co. v. David*

#### D. The '752 Patent

The '752 patent is directed to an apparatus and method for sharing information between primary and secondary security systems, which provide protection “upon a failover event.” (Abstract) Specifically, the two security systems each store information for flows that they are actively processing, as well as flow information synchronized from the other security system. (8:17-29) By doing so, each system can take over processing that ordinarily would be performed by the other, if the other system experiences a failover event. (*Id.*) Only when a failover event occurs does the system activate the “secondary portion” of the flow table and move the records from that portion into the “primary portion.” (9:59-61) When these records are moved into the “primary portion,” the system can label them, so they can be cleared from that portion in the event the failed system is recovered. (9:65-10:3)

Independent claim 1 recites:

A method in a computer network, comprising:  
processing packets, by a primary security system, the  
primary security system including a first device-implemented  
session module to maintain flow information for the primary

---

*Geoffrey & Assoc.*, 904 F.2d 677, 683 (Fed. Cir. 1990), overruled in part on other grounds, *Cardinal Chem. Co. v. Morton Int'l, Inc.*, 508 U.S. 83, 92 n.12 (1993). The accused infringer must first satisfy its burden to go forward “by presenting prior art which shows that the asserted range of equivalence would encompass the prior art . . . .” *Streamfeeder, L.L.C. v. Sure-Feed Sys., Inc.*, 175 F.3d 974, 983 (Fed. Cir. 1999).

PAN asserts that Juniper's doctrine of equivalents arguments would ensnare the prior art reference, Baraka. However, neither PAN nor its expert provides analysis for this proposition or matches the prior art element by element to any asserted claim. (D.I. 203 at 38-39; D.I. 211 at ¶ 204) As this is a matter of law for the court to decide, should PAN wish to move forward with this argument, it will need to provide the court with a proffer before trial. The burden would then shift to Juniper “to prove that the range of equivalents which it seeks would not ensnare the prior art.” *Wilson Sporting Goods*, 904 F.2d at 685.

security system to facilitate processing of the packets, where the first device-implemented session module includes a first flow table having a primary portion that stores information associated with the operation of the first device-implemented session module, when the primary security system is functioning in a primary security system mode, and a secondary portion that stores information associated with the operation of the first device-implemented session module, when the primary security system is functioning in a failover mode;

designating a secondary security system for processing packets upon a failover event, the secondary security system including a second device-implemented session module to maintain flow information for the secondary security system to facilitate processing of the packets, where the second device-implemented session module includes a second flow table having a primary portion that stores information associated with the operation of the second device-implemented session module, when the secondary security system is functioning in a primary security system mode, and a secondary portion that stores information associated with the operation of the second device-implemented session module, when the secondary security system is functioning in a failover mode;

sharing flow records from the primary security system with the secondary security system;

sharing flow records from the secondary security system with the primary security system;

using the primary security system to provide failover support for the secondary security system, based on the information stored in the secondary portion of the first flow table; and

using the secondary security system to provide failover support for the primary security system, based on the information stored in the secondary portion of the second flow table.

(12:22-63) Independent claim 13 recites:

A system, comprising:

a processor-implemented primary security system to process packets, the primary security system including a first device-implemented session module to maintain flow information for the primary security system to facilitate processing of the packets, where the first

device-implemented session module includes a first flow table having a primary portion that stores information associated with an operation of the first device implemented session module, when the primary security system is functioning in a primary security system mode, and a secondary portion that stores information associated with an operation of the first device-implemented session module, when the primary security system is functioning in a failover mode; and

a secondary security system to process packets upon a failover event, the secondary security system including a second device-implemented session module to maintain flow information for the secondary security system to facilitate processing of packets, where the second device-implemented session module includes a second flow table having a primary portion that stores information associated with an operation of the second device implemented session module, when the secondary security system is functioning in a primary security system mode, and a secondary portion that stores information associated with an operation of the second device-implemented session module, when the secondary security system is functioning in a failover mode,

where the primary security system and the secondary security system share flow records, and

where the primary security system is to provide failover support for the secondary security system, based on the information stored in the secondary portion of the first flow table and the secondary security system is to provide failover support for the primary security system, based on the information stored in the secondary portion of the second flow table.

(13:45-14:19)

## **1. Claim limitations**

**a. “[A] primary portion that stores information associated with the operation of the first device-implemented session module, when the primary security system is operating in a primary security mode”**

The court adopts PAN's proposed construction, "the portion of the flow table that stores information for processing packets when all security devices are operational." This construction finds support in the specification, which explains that a "session module . . . may also facilitate the operation of the security devices by communicating flow information to a respective device for processing a given packet." (4:54-57) The primary portion "store[s] flow information for which the session module is actively participating in the processing of the packets." (8:20-22)

**b. "[A] secondary portion that stores information associated with the operation of the first device-implemented session module, when the primary security system is functioning in a failover mode"**

The court construes this limitation as "a separate portion of the same flow table that stores information for processing packets if there is a failover event." While the primary and secondary portions "may be integrated in [a] flow table," the specification and claims distinguish the "secondary portion" from the "primary portion" of the flow table. (8:27-29, fig.10) The secondary "portion of the flow table [is] dedicated to stor[ing] information related to the operation of the given session module as a secondary security system." (8:23-25) A flow table may contain "multiple secondary portions corresponding to multiple primary security systems for which a given session module may be providing failover support." (8:30-32)

## **2. Infringement**

The parties' experts disagree on whether the flow tables in the accused products satisfy the claim limitation requiring a primary portion and a secondary portion. The

specification describes “records of the primary and secondary portions” being integrated in a flow table. Further, “the record may include a label indicating to which security system the record belongs.”<sup>19</sup> (9:61-67) In connection with the accused products, Dr. Rubin explains that “the flow table in each unit maintains different information for processing of packets by that unit in its ordinary operation . . . and for processing packets . . . in the event of the failover,” pointing to groups of entries in the source code designated by “flags.” (D.I. 178, ex. A at ¶ 96) Dr. Mitzenmacher disagrees, opining that the flags do not indicate different portions, but are labels. As such, “if any combination of flag values could denote a portion of the flow table, in practice there would be thousands of possible portions . . . .” (D.I. 211 at ¶ 114) The experts further disagree on whether the information in the secondary portion of the flow table provides “failover support.” (D.I. 178, ex. A at ¶¶ 101, 103, 114; D.I. 211 at ¶¶ 116-118) The court concludes that genuine issues of material fact exist and, therefore PAN’s motion for summary judgment is denied.<sup>20</sup>

Juniper’s original claims required “a primary security system” and “a secondary security system” for processing packets and the security systems were “operable to maintain flow information . . . to facilitate processing of the packets.” (D.I. 153, ex. 13 at

---

<sup>19</sup>Contrary to PAN’s argument, the prosecution history does not “confirm[] that the use of labels cannot denote portions.” Juniper described the prior art as disclosing a server with a database containing session data and “an affinity scheme that directs all requests sharing a session ID to the same clone in a server group.” (D.I. 153, ex. 13 at JA-2159) Juniper concluded that this prior art reference did not disclose a flow table having portions. (*Id.*)

<sup>20</sup>The parties disagree on the admissibility of a document, “PAN-OS Active/Active High Availability.” (D.I. 233; D.I. 223 at 28 n.43 (citing D.I. 208, ex. J)) The court will consider this issue in context at trial.

JA-2144) Juniper amended the claims to include “a primary portion” and “a secondary portion” of a flow table. (*Id.*) This amendment narrowed the scope of the claim to require a flow table with two portions, and Juniper argued that the prior art did not disclose

a first device-implemented session module that includes a first flow table having a primary portion that stores information associated with the operation of the first device-implemented module, when the primary security system is functioning in a primary security system mode, and a secondary portion that stores information associated with the operation fo the first device-implemented session module, when the primary security system is functioning in a failover mode.

(*Id.* at JA-2158-59) This amendment, along with the court’s construction requiring that the secondary portion be separate from the primary portion, prevents Juniper from arguing at trial that a flow table without portions satisfies the claim language under the doctrine of equivalents. Contrary to Juniper’s assertion that this difference “bear[s] no more than a tangential relation” to the asserted basis for equivalency, the court concludes that the “portioning” of the flow table is integral to Juniper’s argument. PAN’s motion for summary judgment in this regard is granted.

#### **E. The ‘723 Patent**

Conventional networks include different packet processing engines such as a firewall, an intrusion detection system, or a flow-based router. (1:48-60) Each of these processing engines can examine different layers within a packet. (1:38-40) The different engines work together to allow “efficient processing of packets at different network levels.” (3:63-64) After processing, tags may be attached to packets, which include information that is useful to other engines when they are processing or routing

the packet. (5:19-33)

Independent claim 1 recites:

A system comprising:  
a first engine to:  
    route a packet to a second engine, and  
    route the packet to a third engine, after receiving the  
packet from the second engine;  
the second engine to:  
    process the packet, and  
    associate a tag with the packet, the tag including  
information about the processing of the packet; and  
the third engine to:  
    process the packet using the information included in  
the tag,  
where the second engine and the third engine comprise a  
firewall processing engine, an intrusion detection system, or  
a network address translation (NAT) engine,  
where the second engine is different than the third engine,  
and  
where the second engine and the third engine are included  
on one integrated circuit.

(11:35-54) Independent claim 9 recites:

A method comprising:  
    routing, using a first engine, a packet to a second  
engine that is different than the first engine;  
    processing, using the second engine, the packet;  
    associating, using the second engine, a tag with the packet,  
    where the tag includes information associated with  
the processing of the packet using the second engine;  
    routing, using the first engine and based on the  
information included in the tag, the packet to a third engine,  
after receiving the packet from the second engine,  
    where the third engine is different than the first engine  
and the second engine; and  
    processing, using the third engine and based on the  
information included in the tag, the packet,  
    where the second engine and the third engine include  
a firewall processing engine, an intrusion detection system,  
or a network address translation (NAT) engine.

(12:20-36)



## 1. Claim limitations

### a. “[F]irst engine” and “second engine”

The claim language requires that the first, second, and third engines be “different.” The specification recites a “multiple processor system,” “packet processing devices,” and “a group of processing engines.” (2:20-36; 4:11-12) Particularly, the specification calls out “a first processor” and “a second processor.” The court construes the limitations respectively as, “a first processor” and “a second processor.”

### b. “[R]out[e] ... [a/the] packet”

The court agrees with Juniper that this limitation does not require construction. The term “route” in the context of the claims is understood by its plain and ordinary meaning. The court clarifies that “routing” does not exclude the use of pointers. The ‘634 patent was incorporated by reference (1:11-12) and provides for “a pointer to a location of a given packet . . . in memory and a pointer to information containing the relative position of the packet in a flow.”<sup>21</sup> (‘634 patent, 5:23-39, fig.6 (“pointer to packet” and “pointer to relative position of packet”))

### c. “a tag” and “associat[e] ... a tag”

The court adopts Juniper’s construction of “a tag,” which is “a structure for holding data.” Contrary to PAN’s argument, the specification does not require that the tag necessarily be “sent along” with the packet. Tags may be sent over different paths or over a common path. (5:4-8) “[I]f the firewall processing engine determines that a

---

<sup>21</sup>The court is not bound by, nor did it find persuasive the examiner’s comments directed to a single prior art reference, made during reexamination, and identified by PAN. (D.I. 155, ex. 15 at JA-2415)

packet is part of an attack, a tag including a communication action flag can be sent to flow engine . . . informing flow engine . . . not to route any more packets from the same session as the packet.” (7:51-55)

PAN’s construction for “associate . . . a tag” is adopted, “form a connection with a tag.” A tag may be “attached” to a packet or “appended or prepended to the packet.” (2:60-61, 4:23)

## **2. Infringement**

Dr. Mitzenmacher performed an experiment and concluded that “slow path and fast path processing for a single packet can indeed run on the same core of the Cavium.” (D.I. 211 at ¶ 84) However, Dr. Rubin analyzed the source code and opined that “the Slowpath Engine and the Fastpath Engine can be run on different cores of the Cavium chip.” (D.I. 178, ex. A at ¶ 656)

The parties’ experts also disagree on whether the first engine “routes” packets to other engines. Dr. Mitzenmacher explains that “neither the packet information, nor the pointer to the packet in the [Work Queue Entry] WQE, is sent from a source to a destination in this process by the scheduler. . . . Thus, not even the pointer to the packet is “routed” . . . .” (D.I. 211 at ¶ 80) However, Dr. Rubin opines that “after a packet is received by the SSO Unit in the accused PAN products, it is packaged into a data structure called a Work Queue Entry . . . . the Cavium accesses and processes the packet by reference to the WQE, including its ‘pointer to the Packet Data Buffer.’”

The claims require that the “second engine . . . associate a tag with the packet.” PAN asserts through attorney argument and by reference to Dr. Rubin’s expert report and testimony, that Dr. Rubin’s opinion is incorrect because the WQE is the “data

structure” that holds session and group data and “the WQE is associated with the packet before the SSO receives it.”<sup>22</sup> (D.I. 203 at 22; D.I. 208, ex. F at 167:1-169:11) Dr. Mitzenmacher asserts that “[t]he WQE is associated with a packet when the packet is first received by the Cavium - which is before the scheduler/SSO receives the WQE (let alone assigns the WQE to a core).” (D.I. 211, ex. 2 at ¶ 147) Dr. Rubin’s opinion, however, offers an alternative explanation for this process and concludes that the source code evidences that the accused products meet this claim limitation. (D.I. 178, ex. A at ¶¶ 613-631) The court concludes that several issues of material fact remain unresolved as to whether the accused products infringe the asserted claims. Therefore, the court denies the competing motions for summary judgment.<sup>23</sup>

#### **F. The ‘700 and ‘459 Patents**

The ‘700 patent shares a specification with the ‘459 patent, as described below.

Independent claim 2 of the ‘700 patent recites:

An L2 device comprising:  
a controller to determine for each packet received whether the received packet is to be transferred intra-zone or inter-zone, each zone representing a distinct security

---

<sup>22</sup>After several questions and answers, Dr. Rubin testified that “So on this first sentence the document reference does seem to indicate that the – that the WQE is associated with the packet before the SSO receives it.” (D.I. 208, ex. F at 169:8-11) The deposition follows with clarifying questions and answers that do not provide concrete answers. (*Id.* at 169-177)

<sup>23</sup>PAN moves for summary judgment regarding the doctrine of equivalents, arguing that Juniper’s theories are cursory and do not establish a disputed issue of fact regarding infringement. Juniper’s expert offered sufficient support for his theories based on the court’s adoption of PAN’s constructions. PAN’s lack of analysis does not meet its burden of persuasion on this issue, therefore, the court denies PAN’s motion for summary judgment regarding the doctrine of equivalents.

domain and having an associated policy for use in inspecting packets entering and exiting an associated zone;  
a firewall engine to inspect and filter received inter-zone packets using a zone specific policy; and  
an L2 switching engine operable to:  
route to an intra-zone port, without the inspection by the firewall engine, received intra-zone packets using a table of MAC addresses and corresponding ports, and  
route to an inter-zone port inspected inter-zone packets that are retained after the inspection by the firewall engine.

(‘700 patent, 11:1-18) During prosecution of the ‘700 patent, Juniper amended the claims to add “associated with intra-zone transfer, without inspection by the firewall engine,” and argued that the prior art did not disclose transferring intra-zone packets “without inspection by the L2 device’s firewall engine.” (D.I. 152, ex. 11 at JA-1285) When allowing the claims, the examiner agreed with Juniper that “the prior art of record do[es] not teach the limitation ‘wherein intra-zone packets are not inspected by the firewall’ (see similar, but not identical language),” and “do[es] not teach the limitation ‘transfer[ing] noninspected packets within the first or second security zones’ (see similar, but not identical language).” (*Id.* at JA-1171-72.)

The ‘459 patent is a direct continuation of, and shares a specification with, the ‘700 patent. The ‘459 patent describes the use of zone-specific policies, which allow security systems to differentiate between inter-zone packets (i.e., packets sent between two or more security zones) and intra-zone packets (i.e., packets that stay in the same security zone). (6:62-65, 10:42-59) “Packets are either directly processed (e.g., intra-zone packets) or processed after a security screening (e.g., for inter-zone packets).” (6:25-27) The specification explains that “communications that are

intra-zone ... will not require inspection,” while inter-zone communications “will invoke an inspection process.” (8:26-31) For example, the ‘459 patent describes ways to bypass one or more types of security screening for intra-zone packets traveling within a distinct security domain, to increase processing efficiency. The examiner allowed the claims for “substantially similar . . . reasons” to the ‘700 patent.

Independent claim 1 of the ‘459 patent recites:

In a network device, a method comprising:  
receiving a packet via a network that includes a plurality of distinct security domains;  
determining whether the packet is to remain within a first one of the distinct security domains or pass between two of the distinct security domains;  
performing, based on a first determination that the packet is to pass between the two distinct security domains security [sic], security screening on the packet before routing the screened packet to an egress port of the network device for forwarding on the network; and  
routing, based on a second determination that the packet is to remain within the first distinct security domain, the packet to an egress port of the network device for forwarding on the network without performing the security screening on the packet.

(10:43-59) Independent claim 12:

A network device comprising:  
an ingress port to receive a packet via a network that includes a plurality of distinct security domains;  
a controller to determine whether the network device is to transfer the packet within a first one of the distinct security domains or between two of the distinct security domains;  
a security device to perform security screening, based on a first determination that the packet is to be forwarded between the two distinct security domains security [sic], on the packet before routing the packet to an egress port of the network device for forwarding on the network; and  
an engine to route the packet, based on a second

determination that the packet is to be forwarded within the first distinct security domain, to an egress port of the network device for forwarding on the network without performing the security screening on the packet.

(11:24-50)

## **1. Claim limitations of the '459 patent**

### **a. “[S]ecurity screening”**

The court construes the limitation as “inspection by applying one or more security policies.” The specification supports this construction, providing that “policies can be established for inspecting or otherwise screening packets” and, if “an inspection is to occur, an appropriate policy is retrieved.” (7:19-21; 9:5-6)

### **b. “[W]ithout performing the security screening”**

The court construes the limitation as “without inspection.” The specification states, “communications that are intra-zone . . . will not require inspection.” (8:26-29) The packets are evaluated “to determine if inspection is required.” (9:27-28) This construction makes clear that the inspection process is not performed. “Screening engine . . . examines each packet received from a respective port . . . and determines whether security screening is to be performed.” (6:45-47) This construction is also consistent with the prosecution history discussed above.<sup>24</sup> While Juniper argues that the specification discloses embodiments where intra-zone packets are screened, the court disagrees. (8:33-36, 8:64-65) One embodiment discloses three different security zones, “v1-trust, v1-untrust and v1-dmz zones,” and provides that intra-zone packets do

---

<sup>24</sup>As discussed below regarding the doctrine of equivalence, the prosecution history of the '700 patent is relevant to the claim construction of this limitation.

“not require inspection.” (8:20-29) The other embodiment goes on to describe that “the packet's ingress and egress ports are compared to determine if the packet is passing to another zone. Assuming that an inspection is to occur, an appropriate policy is retrieved . . . .” (9:3-6) Moreover, a claim does not have to encompass all disclosed embodiments. *TIP Systems, LLC v. Phillips & Brooks/Gladwin, Inc.*, 529 F.3d 1364, 1373 (Fed. Cir. 2008) (citing *PSN III., LLC v. Ivoclar Vivadent, Inc.*, 525 F.3d 1159, 1167 (Fed. Cir. 2008) (reiterating that “read in the context of the specification, the claims of the patent need not encompass all disclosed embodiments”).

## **2. Infringement**

The parties' experts disagree on whether the “without performing the screening” limitation is met by the accused products. Dr. Mitzenmacher explains that all incoming packets are subject to inspection of information in the header to determine whether the packet should be discarded, prior to policy look up. (D.I. 211 at ¶ 230) Further, the look up policy “is called for intra-zone packets” as well, therefore, Dr. Mitzenmacher opines that the accused products do not meet the claim limitation. For the '459 patent, Juniper argues that the incoming packet inspection is irrelevant as it occurs prior to policy look up and is not the infringement contention at issue. Dr. Rubin explains that the application of a “deny” security policy to inter-zone packets, when the product runs in default mode, infringes the claim limitation. (D.I. 178, ex. A at ¶¶ 1249, 1265, 1276) Dr. Mitzenmacher opines that to determine whether the default rule applies requires that a security inspection be performed. (D.I. 211 at ¶ 225-227)

Relying on the same arguments described above, PAN argues that the claims of the '700 patent “require that packets traveling within a security zone (‘intra-zone

packets') are routed 'without the inspection by the firewall engine' or specify that such intra-zone packets are to remain 'non-inspected.' In response, Juniper advances the opinions of its expert that the accused products employ a "zone specific security approach." (D.I. 178, ex. A at ¶¶ 1103, 1122) After reviewing the expert reports, the court concludes that a classic battle of the experts exists with respect to the asserted claim limitations of the '459 and '700 patents, resulting in genuine issues of material fact. The parties' competing motions for summary judgment are denied.<sup>25</sup>

PAN moves for summary judgment of non-infringement of the '459 and '700 patents under the doctrine of equivalents. The asserted claims of the '700 patent route intra-zone packets "without inspection by the firewall engine," and the asserted claims of the '459 patent do so "without performing the security screening." The prosecution history for the '700 patent discussed above and the court's construction forecloses argument by Juniper that intra-zone packets may be inspected and still meet these claim limitations under the doctrine of equivalents. See e.g., *Invitrogen Corp. v. Clontech Laboratories, Inc.*, 429 F.3d 1052, 1078 (Fed. Cir. 2005) (recognizing that "an amendment to a related limitation in the parent application [that] distinguishes prior art and thereby specifically disclaims a later (though differently worded) limitation in the continuation application" can create estoppel) (citing *Elkay Mfg. Co. v. EBCO Mfg. Co.*, 192 F.3d 973, 978-79 (Fed. Cir. 1999)). The court grants PAN's motion for summary judgment in this regard.

---

<sup>25</sup>The parties disagree on the admissibility of a document, "PAN-OS: Day in the life of a packet." (D.I. 233; D.I. 223 at 14 n.23 (citing D.I. 208, ex. G)) The court will consider this issue in context at trial.



## **G. Other Claim Limitations**

Juniper moves for partial summary judgment for approximately 73 “undisputed claim elements” found in 56 of the 65 asserted claims, arguing that Dr. Rubin’s report<sup>26</sup> explains how each of these elements are satisfied for the purposes of infringement. Further, Juniper requests partial summary judgment on 36 asserted dependent claims,<sup>27</sup> asserting that PAN’s expert did not address the dependent claims and the non-infringement claim charts do not present any material disputes of fact. (D.I. 177 at 27-34) Not surprisingly, PAN disagrees and supplies the court with citations to Dr. Mitzenmacher’s expert report and responses to interrogatories to establish that there are material facts in dispute. (D.I. 203 at 46-50) Juniper has not provided any analysis other than conclusory statements and references to its expert report, which PAN and its expert dispute. The court declines to undertake the exercise of comparing the competing expert reports without context and, therefore, Juniper’s motion for summary judgment of infringement is denied in this regard.

## **VI. CONCLUSION**

The court has provided a construction in quotes for the claim limitations at issue. The parties are expected to present the claim construction to the jury consistently with any explanation or clarification herein provided by the court, even if such language is not included within the quotes.

For the foregoing reasons, Junipers’ motion for summary judgment of assignor

---

<sup>26</sup>Citing to some 275 paragraphs of his expert report.

<sup>27</sup>Citing to some 220 paragraphs of Dr. Rubin’s report.

estoppel (D.I. 172) is granted and the competing motions for summary judgment of validity of the patents-in-suit (D.I. 170, D.I. 204) are denied as moot. Juniper's motion for summary judgment of infringement is denied. (D.I. 176) PAN's motion for summary judgment of non-infringement is granted in part and denied in part. (D.I. 202)