IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TEXAS
WACO DIVISION

PACSEC3, LLC,	)	
Plaintiff,	)	
	)	**Civil Action No. 6:21-cv-00387**
v.	)	
	)	
JUNIPER NETWORKS, INC.,	)	**JURY TRIAL DEMANDED**
Defendant.	)	

PLAINTIFF'S ORIGINAL COMPLAINT FOR PATENT INFRINGEMENT

PacSec3, LLC ("PacSec") files this Original Complaint and demand for jury trial seeking relief from patent infringement of the claims of U.S. Patent Nos. 6,789,190 ("the '190 patent"); 7,047,564 ("the '564 patent"); and, 7,523,497 ("the '497 patent") (collectively referred to as the "Patents-in-Suit") by Juniper Networks, Inc.

I. THE PARTIES

1. Plaintiff PacSec3, LLC is a Texas Limited Liability Company with its principal place of business located in Harris County, Texas.

2. On information and belief, Juniper Networks, Inc. ("Juniper") is a California Corporation. On information and belief, JUNIPER sells and offers to sell products and services throughout Texas, including in this judicial district, and introduces products and services that perform infringing methods or processes into the stream of commerce knowing that they would be sold in Texas and this judicial district. JUNIPER can be served with process through their registered agent at CT Corporation System, 1999 Bryan St., Suite 900, Dallas, TX 75201-3136.

II. JURISDICTION AND VENUE

3. This Court has original subject-matter jurisdiction over the entire action pursuant to 28 U.S.C. §§ 1331 and 1338(a) because Plaintiff's claim arises under an Act of Congress relating to patents, namely, 35 U.S.C. § 271.

4. This Court also has original subject-matter jurisdiction over the entire action pursuant to 28 U.S.C. § 1332(a)(1) because Plaintiff is a limited liability company organized under the laws of the State of Texas and Defendant is a California Corporation with a principal, physical place of business at 1120 S Capital of Texas Hwy #120, Austin, Texas 78746. The matter in controversy exceeds the sum or value of $75,000, exclusive of interest and costs.

5. This Court has personal jurisdiction over Defendant because: (i) Defendant is present within or has minimum contacts within the State of Texas and this judicial district; (ii) Defendant has purposefully availed itself of the privileges of conducting business in the State of Texas and in this judicial district; and (iii) Plaintiff's cause of action arises directly from Defendant's business contacts and other activities in the State of Texas and in this judicial district.

6. Venue is proper in this district under 28 U.S.C. §§ 1391(b) and 1400(b). Defendant has committed acts of infringement and has a regular and established place of business in this District. Further, venue is proper because Defendant conducts substantial business in this forum, directly or through intermediaries, including: (i) at least a portion of the infringements alleged herein; and (ii) regularly doing or soliciting business, engaging in other persistent courses of conduct and/or deriving substantial revenue from goods and services provided to individuals in Texas and this District.

III. INFRINGEMENT

A. Infringement of the '190 Patent

7. On September 7, 2004, U.S. Patent No. 6,789,190 ("the '190 patent," attached as Exhibit A) entitled "PACKET FLOODING DEFENSE SYSTEM," was duly and legally issued by the U.S. Patent and Trademark Office. PacSec3, LLC owns the '190 patent by assignment.

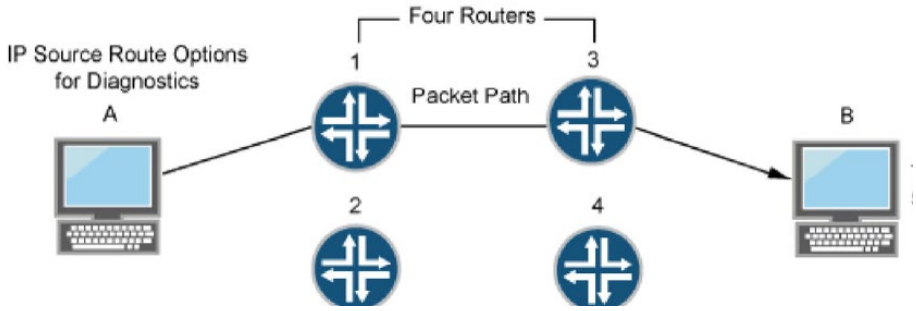
8. The '190 patent relates to a novel and improved manner and system of defense to a data packet flood attack.

9. JUNIPER offers for sale, sells and manufactures one or more firewall systems, including its control plane denial of service protection, that infringes one or more claims of the '190 patent, including one or more of claims 1-3, literally or under the doctrine of equivalents. Defendant put the inventions claimed by the '190 Patent into service (i.e., used them); but for Defendant's actions, the claimed-inventions embodiments involving Defendant's products and services would never have been put into service. Defendant's acts complained of herein caused those claimed-invention embodiments as a whole to perform, and Defendant's procurement of monetary and commercial benefit from it.

10. Support for the allegations of infringement may be found in the following preliminary table:

Claim language	**Juniper Networks Evidence**
Claim 1. A packet flooding defense system for a network comprising a plurality of host computers, routers, communication lines and	

transmitted data packets, said system comprising: at least one firewall, said firewall comprising:	On Juniper devices, control plane DDoS protection enables the device to continue functioning while under an attack. It identifies and suppresses malicious control packets while enabling legitimate control traffic to be processed. With a single point of DDoS protection management, network administrators can customize profiles for their network control traffic. For routers, protection and monitoring persists across graceful Routing Engine switchover (GRES) and unified in-service-software-upgrade (ISSU) switchovers. Protection is not diminished as the number of subscribers increases **Control Plane Distributed Denial-of-Service (DDoS) Protection Overview (Page 1)** <https://www.juniper.net/documentation/en_US/junos/topics/concept/subscriber-managementddos-protection.html> Juniper Networks: Junos OS DDoS Protection has a packet flooding defense system for a network comprising a plurality of host computers, routers, communication lines and transmitted data packets.
… hardware and software serving to control packet transmission between said network and a host computer connected to an internal network;	Firewall filters allow you to control packets transiting the device to a network destination and packets destined for and sent by the device. You can configure firewall filters to control which data packets are accepted on and transmitted from the physical interfaces, and which local packets are transmitted from the physical interfaces and the Routing Engine. Firewall filters provide a means of protecting your device from excessive traffic. Firewall filters that control local packets can also protect your device from external aggressions, such as DoS attacks. **Junos OS Features for Device Security (Page 5)** <https://origin-www.juniper.net/documentation/en_US/junos/topics/concept/junos-software-router-security-supported-features.html>

	 **Understanding Attacker Evasion Techniques (Page 3)** <https://www.juniper.net/documentation/software/junos-security/junos-security95/ junos-security-swconfig-security/id-93100.html> The reference describes at least one firewall [Firewall filters], said firewall comprising: hardware and software serving to control packet transmission between said network and a host computer connected to an internal network [Packet Path].
… means for classifying data packets received at said firewall;,…	On Juniper devices, control plane DDoS protection enables the device to continue functioning while under an attack. It identifies and suppresses malicious control packets while enabling legitimate control traffic to be processed. With a single point of DDoS protection management, network administrators can customize profiles for their network control traffic. For routers, protection and monitoring persists across graceful Routing Engine switchover (GRES) and unified in-service-software-upgrade (ISSU) switchovers. Protection is not diminished as the number of subscribers increases. **Control Plane Distributed Denial-of-Service (DDoS) Protection Overview (Page 1)** <https://www.juniper.net/documentation/en_US/junos/topics/concept/subscriber-managementddos-protection.html> The reference describes means for classifying data packets received at said firewall [It identifies and suppresses malicious control packets while enabling legitimate control traffic to be processed].

means for associating a maximum acceptable transmission rate with each class of data packet received at said firewall;	To protect against DDoS attacks, you can configure policers for host-bound exception traffic. The policers specify rate limits for individual types of protocol control packets or for all control packet types for a protocol. You can monitor policer actions for packet types and protocol groups at the level of the device, Routing Engine, and line cards. You can also control logging of policer events. **Junos OS Features for Device Security (Page 6)** <https://origin-www.juniper.net/documentation/en_US/junos/topics/concept/junos-software-router-security-supported-features.html> The reference describes means for associating a maximum acceptable transmission rate with each class of data packet received at said firewall [The policers specify rate limits for individual types of protocol control packets or for all control packet types for a protocol].
means for said firewall to find information for packets it receives regarding the path by which said packets came to said firewall; and	Control plane DDoS policers are organized to match the hierarchical flow of protocol control traffic. Control traffic arriving from all ports of a line card converges on the Packet Forwarding Engine. Control traffic from all line cards on the router converges on the Routing Engine. Similarly, the DDoS policers are placed hierarchically along the control paths so that excess packets are dropped as early as possible on the path. This design preserves system resources by removing excess, malicious traffic so that the Routing Engine receives only the amount of traffic that it can process. **Control Plane Distributed Denial-of-Service (DDoS) Protection Overview (Page 7)** <https://www.juniper.net/documentation/en_US/junos/topics/concept/subscriber-managementddos-protection.html> The reference describes means for said firewall to find information for packets it receives regarding the path by which said packets came to said firewall [the

	DDoS policers are placed hierarchically along the control paths so that excess packets are dropped as early as possible on the path].
whereby, said firewall can use said information to allocate the transmission rate for each class in a desired way.	To protect the Routing Engine, you can configure a firewall filter only on the device's loopback interface. Adding or modifying filters for each interface on the device is not necessary. You can design firewall filters to protect against ICMP and Transmission Control Protocol (TCP) connection request (SYN) floods and to rate-limit traffic being sent to the Routing Engine. **Junos OS Features for Device Security (Page 5)** <https://origin-www.juniper.net/documentation/en_US/junos/topics/concept/junos-software-router-security-supported-features.html> The reference states that said firewall can use said information to allocate the transmission rate for each class in a desired way [You can design firewall filters to protect against ICMP and Transmission Control Protocol (TCP) connection request (SYN) floods and to rate-limit traffic being sent to the Routing Engine].

These allegations of infringement are preliminary and are therefore subject to change.

11. JUNIPER has and continues to induce infringement. JUNIPER has actively encouraged or instructed others (e.g., its customers and/or the customers of its related companies), and continues to do so, on how to use its products and services (e.g., question and answer services on the Internet) and related services that provide question and answer services across the Internet such as to cause infringement of one or more of claims 1–3 of the '190 patent, literally or under the doctrine of

equivalents. Moreover, JUNIPER has known of the '190 patent and the technology underlying it from at least the date of issuance of the patent.

12. JUNIPER has and continues to contributorily infringe. JUNIPER has actively encouraged or instructed others (e.g., its customers and/or the customers of its related companies), and continues to do so, on how to use its products and services (e.g., question and answer services on the Internet) and related services that provide question and answer services across the Internet such as to cause infringement of one or more of claims 1–3 of the '190 patent, literally or under the doctrine of equivalents. Moreover, JUNIPER has known of the '190 patent and the technology underlying it from at least the date of issuance of the patent.

13. JUNIPER has caused and will continue to cause PacSec3 damage by direct and indirect infringement of (including inducing infringement of) the claims of the '190 patent.

B. Infringement of the '564 Patent

14. On May 16, 2006, U.S. Patent No. 7,047,564 ("the '564 patent", attached as Exhibit B) entitled "REVERSIBLE FIREWALL PACKET TRANSMISSION CONTROL SYSTEM," was duly and legally issued by the U.S. Patent and Trademark Office. PacSec3, LLC owns the '564 patent by assignment.

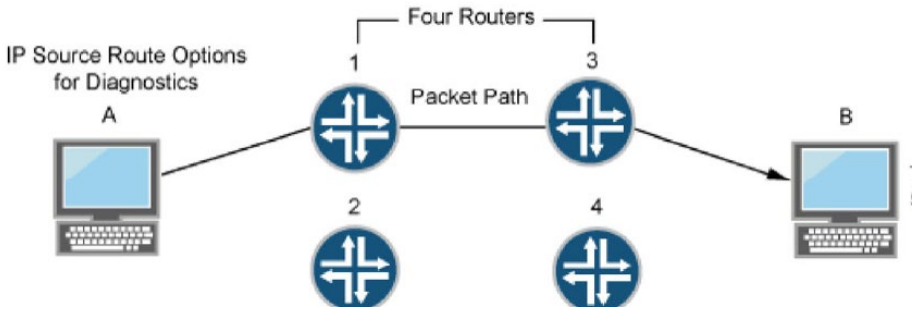
15. The '564 patent relates to a novel and improved manner and system of defense to a data packet flood attack.

16. JUNIPER offers for sale, sells and manufactures one or more firewall systems, including ts control plane denial of service protection, that infringes one or more claims of the '564 patent, including one or more of claims 1-6, literally or under the doctrine of equivalents. Defendant put the inventions claimed by the '564 Patent into service (i.e., used them); but for Defendant's actions, the claimed-inventions embodiments involving Defendant's products and services would never

have been put into service. Defendant's acts complained of herein caused those claimed-invention embodiments as a whole to perform, and Defendant's procurement of monetary and commercial benefit from it.

17. Support for the allegations of infringement may be found in the following preliminary table:

Claim language	**Juniper Networks Evidence**
Claim 1: A packet transmission control system for managing traffic between at least two data networks, each of said networks comprising a plurality of host computers, communication lines and transmitted data packets, said system comprising:	On Juniper devices, control plane DDoS protection enables the device to continue functioning while under an attack. It identifies and suppresses malicious control packets while enabling legitimate control traffic to be processed. With a single point of DDoS protection management, network administrators can customize profiles for their network control traffic. For routers, protection and monitoring persists across graceful Routing Engine switchover (GRES) and unified in-service-software-upgrade (ISSU) switchovers. Protection is not diminished as the number of subscribers increases. **Control Plane Distributed Denial-of-Service (DDoS) Protection Overview (Page 1)** <https://www.juniper.net/documentation/en_US/junos/topics/concept/subscriber-managementddos-protection.html> Juniper Networks: Junos OS DDoS Protection has a packet transmission control system for managing traffic between at least two data networks, each of said networks comprising a plurality of host computers, communication lines and transmitted data packets.
at least one firewall, said	

firewall comprising: hardware and software providing a non-redundant connection between said networks and serving to control packet transmission between said networks;	Firewall filters allow you to control packets transiting the device to a network destination and packets destined for and sent by the device. You can configure firewall filters to control which data packets are accepted on and transmitted from the physical interfaces, and which local packets are transmitted from the physical interfaces and the Routing Engine. Firewall filters provide a means of protecting your device from excessive traffic. Firewall filters that control local packets can also protect your device from external aggressions, such as DoS attacks. **Junos OS Features for Device Security (Page 5)** <https://origin-www.juniper.net/documentation/en_US/junos/topics/concept/junos-software-router-security-supported-features.html>  **Understanding Attacker Evasion Techniques (Page 3)** <https://www.juniper.net/documentation/software/junos-security/junos-security95/ junos-security-swconfig-security/id-93100.html> The reference describes at least one firewall [Firewall filters], said firewall comprising: hardware and software serving to control packet transmission between said network and a host computer connected to an internal network [Packet Path].

means for classifying data packets received at said firewall related to the consumption of at least one resource;	On Juniper devices, control plane DDoS protection enables the device to continue functioning while under an attack. It identifies and suppresses malicious control packets while enabling legitimate control traffic to be processed. With a single point of DDoS protection management, network administrators can customize profiles for their network control traffic. For routers, protection and monitoring persists across graceful Routing Engine switchover (GRES) and unified in-service-software-upgrade (ISSU) switchovers. Protection is not diminished as the number of subscribers increases. **Control Plane Distributed Denial-of-Service (DDoS) Protection Overview (Page 1)** <https://www.juniper.net/documentation/en_US/junos/topics/concept/subscriber-managementddos-protection.html> The reference describes means for classifying data packets received at said firewall [It identifies and suppresses malicious control packets while enabling legitimate control traffic to be processed].
means for associating a maximum acceptable transmission rate with each class of data packet received at said firewall;	To protect against DDoS attacks, you can configure policers for host-bound exception traffic. The policers specify rate limits for individual types of protocol control packets or for all control packet types for a protocol. You can monitor policer actions for packet types and protocol groups at the level of the device, Routing Engine, and line cards. You can also control logging of policer events. **Junos OS Features for Device Security (Page 6)** <https://origin-www.juniper.net/documentation/en_US/junos/topics/concept/junos-software-router-security-supported-features.html> The reference describes means for associating a maximum acceptable transmission rate with each class of data packet received at said firewall [The policers specify rate limits for individual types of protocol control packets or for all control packet types for a protocol].
means for limiting the	

transmission rate from the firewall to the maximum acceptable transmission rate for each class of data packet; and	Finally, all PADR packets that are passed by the Routing Engine individual policer proceed to the Routing Engine aggregate policer. PADR packets that exceed the limit are dropped. PADR packets that are not dropped here are passed along as safe, normal traffic. **Control Plane Distributed Denial-of-Service (DDoS) Protection Overview (Page 10)** <https://www.juniper.net/documentation/en_US/junos/topics/concept/subscriber-managementddos-protection.html> The reference describes means for limiting the transmission rate from the firewall to the maximum acceptable transmission rate for each class of data packet [PADR packets that exceed the limit are dropped. PADR packets that are not dropped here are passed along as safe, normal traffic].
whereby, packet flooding and other over usage type distributed denial of service attacks cannot be effectively launched through said non-redundant connection.	To protect the Routing Engine, you can configure a firewall filter only on the device's loopback interface. Adding or modifying filters for each interface on the device is not necessary. You can design firewall filters to protect against ICMP and Transmission Control Protocol (TCP) connection request (SYN) floods and to rate-limit traffic being sent to the Routing Engine. **Junos OS Features for Device Security (Page 5)** <https://origin-www.juniper.net/documentation/en_US/junos/topics/concept/junos-software-router-security-supported-features.html> The reference states that said firewall can use said information to allocate the transmission rate for each class in a desired way [You can design firewall filters

	to protect against ICMP and Transmission Control Protocol (TCP) connection request (SYN) floods and to rate-limit traffic being sent to the Routing Engine].

These allegations of infringement are preliminary and are therefore subject to change.

18. JUNIPER has and continues to induce infringement. JUNIPER has actively encouraged or instructed others (e.g., its customers and/or the customers of its related companies), and continues to do so, on how to use its products and services (e.g., question and answer services on the Internet) and related services that provide question and answer services across the Internet such as to cause infringement of one or more of claims 1–6 of the ’564 patent, literally or under the doctrine of equivalents. Moreover, JUNIPER has known of the ’564 patent and the technology underlying it from at least the date of issuance of the patent.

19. JUNIPER has and continues to contributorily infringe. JUNIPER has actively encouraged or instructed others (e.g., its customers and/or the customers of its related companies), and continues to do so, on how to use its products and services (e.g., question and answer services on the Internet) and related services that provide question and answer services across the Internet such as to cause infringement of one or more of claims 1–6 of the ‘564 patent, literally or under the doctrine of equivalents. Moreover, JUNIPER has known of the ‘564 patent and the technology underlying it from at least the date of issuance of the patent.

20. JUNIPER has caused and will continue to cause PacSec3 damage by direct and indirect infringement of (including inducing infringement of) the claims of the ’564 patent.

C. Infringement of the ‘497 Patent

21. On April 21, 2009, U.S. Patent No. 7,523,497 ("the '497 patent", attached as Exhibit C) entitled "PACKET FLOODING DEFENSE SYSTEM," was duly and legally issued by the U.S. Patent and Trademark Office. PacSec3, LLC owns the '497 patent by assignment.

22. The '497 patent relates to a novel and improved manner and system of defense to a data packet flood attack.

23. JUNIPER offers for sale, sells and manufactures one or more firewall systems, including ts control plane denial of service protection, that infringes one or more claims of the '497 patent, including one or more of claims 1-18, literally or under the doctrine of equivalents. Defendant put the inventions claimed by the '497 Patent into service (i.e., used them); but for Defendant's actions, the claimed-inventions embodiments involving Defendant's products and services would never have been put into service. Defendant's acts complained of herein caused those claimed-invention embodiments as a whole to perform, and Defendant's procurement of monetary and commercial benefit from it.

24. Support for the allegations of infringement may be found in the following preliminary table:

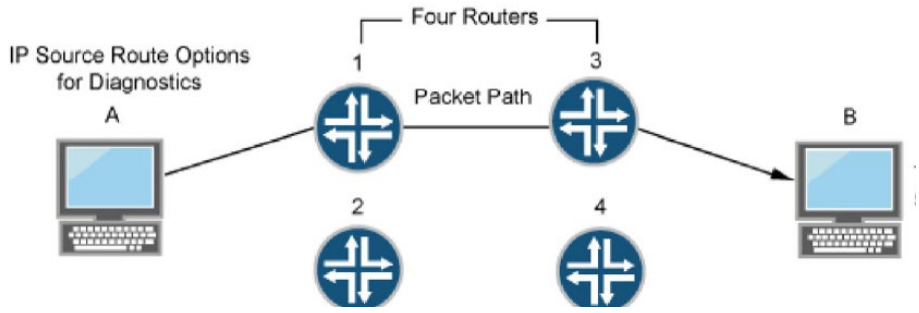
Claim language	**Juniper Networks Evidence**
Claim 7: A method of providing packet flooding defense for a network comprising a plurality of host computers, routers,	On Juniper devices, control plane DDoS protection enables the device to continue functioning while under an attack. It identifies and suppresses malicious control packets while enabling legitimate control traffic to be processed. With a single point of DDoS protection management, network administrators can customize profiles for their network control traffic. For routers, protection and monitoring persists across graceful Routing Engine switchover (GRES) and unified in-service-software-upgrade (ISSU) switchovers. Protection is not diminished as the number of subscribers increases

communication lines and transmitted data packets, said method comprising the steps of:	**Control Plane Distributed Denial-of-Service (DDoS) Protection Overview (Page 1)** <https://www.juniper.net/documentation/en_US/junos/topics/concept/subscriber-managementddos-protection.html> Juniper Networks: Junos OS DDoS Protection has a method of providing packet flooding defense for a network comprising a plurality of host computers, routers, communication lines and transmitted data packets.
determining a path by which data packets arrive at a host computer via packet marks provided by routers leading to said host computer; said path comprising all routers in said network via which said packets are routed to said computer;	Rich packet processing enables the M Series to support multiple levels of granular quality of service (QoS) per-port, per-logical circuit (DLCI, VC/VP, VLAN), and per-channel (to DS0) for traffic prioritization. These comprehensive QoS functions include classification, rate limiting, shaping, weighted round-robin scheduling, strict priority queuing, weighted random early detection, random early detection, and packet marking. For network convergence applications, Layer 2 class of service (CoS) can be mapped to Layer 3 CoS on a per-DLCI, per-VP/VC, or per-VLAN basis. Simultaneously, extensive statistics can be collected and diagnostics performed at this same level of granularity to enable flexible billing, traffic planning, and rapid troubleshooting. **M Series Multiservice Edge Routers (page 2)** <https://web.archive.org/web/20110807093018/https://www.juniper.net/us/en/ local/pdf/datasheets/1000042-en.pdf> The reference describes determining a path by which data packets arrive at a host computer via packet marks provided by routers leading to said host computer [QoS functions include classification, rate limiting, shaping, weighted roundrobin scheduling, strict priority queuing, weighted random early detection, random early detection, and packet marking].

Source routing was designed to allow users at the source of an IP packet transmission to specify the IP addresses of the devices (also referred to as "hops") along the path that they want an IP packet to take on its way to its destination. The original intent of the IP source route options was to provide routing control tools to aid diagnostic analysis. If, for example, the transmission of a packet to a particular destination meets with irregular success, you might first use either the record route or timestamp IP option to discover the addresses of devices along the

Understanding Attacker Evasion Techniques (Page 2)

<https://www.juniper.net/documentation/software/junos-security/junos-security95/ junos-security-swconfig-security/id-93100.html>



Understanding Attacker Evasion Techniques (Page 3)

<https://www.juniper.net/documentation/software/junos-security/junos-security95/ junos-security-swconfig-security/id-93100.html>

The reference describes said path comprising all routers in said network via which said packets are routed to said computer [along the path that they want an IP packet to take on its way to its destination].

classifying data packets received at said host computer into wanted data packets and unwanted data packets by path;	On Juniper devices, control plane DDoS protection enables the device to continue functioning while under an attack. It identifies and suppresses malicious control packets while enabling legitimate control traffic to be processed. With a single point of DDoS protection management, network administrators can customize profiles for their network control traffic. For routers, protection and monitoring persists across graceful Routing Engine switchover (GRES) and unified in-service-software-upgrade (ISSU) switchovers. Protection is not diminished as the number of subscribers increases. **Control Plane Distributed Denial-of-Service (DDoS) Protection Overview (Page 1)** <https://www.juniper.net/documentation/en_US/junos/topics/concept/subscriber-managementddos-protection.html> The reference describes means for classifying data packets received at said firewall [It identifies and suppresses malicious control packets while enabling legitimate control traffic to be processed].
associating a maximum acceptable processing rate with each class of data packet received at said host computer; and	To protect against DDoS attacks, you can configure policers for host-bound exception traffic. The policers specify rate limits for individual types of protocol control packets or for all control packet types for a protocol. You can monitor policer actions for packet types and protocol groups at the level of the device, Routing Engine, and line cards. You can also control logging of policer events. **Junos OS Features for Device Security (Page 6)** <https://origin-www.juniper.net/documentation/en_US/junos/topics/concept/junos-software-router-security-supported-features.html> The reference describes means for associating a maximum acceptable transmission rate with each class of data packet received at said firewall [The policers specify rate limits for individual types of protocol control packets or for all control packet types for a protocol].

allocating a processing rate less than or equal to said maximum acceptable processing rate for unwanted data packets.	Finally, all PADR packets that are passed by the Routing Engine individual policer proceed to the Routing Engine aggregate policer. PADR packets that exceed the limit are dropped. PADR packets that are not dropped here are passed along as safe, normal traffic. **Control Plane Distributed Denial-of-Service (DDoS) Protection Overview (Page 10)** <https://www.juniper.net/documentation/en_US/junos/topics/concept/subscriber-managementddos-protection.html> The reference describes means for limiting the transmission rate from the firewall to the maximum acceptable transmission rate for each class of data packet [PADR packets that exceed the limit are dropped. PADR packets that are not dropped here are passed along as safe, normal traffic].

These allegations of infringement are preliminary and are therefore subject to change.

25. JUNIPER has and continues to induce infringement. JUNIPER has actively encouraged or instructed others (e.g., its customers and/or the customers of its related companies), and continues to do so, on how to use its products and services (e.g., question and answer services on the Internet) and related services that provide question and answer services across the Internet such as to cause infringement of one or more of claims 1–18 of the '497 patent, literally or under the doctrine of equivalents. Moreover, JUNIPER has known of the '497 patent and the technology underlying it from at least the date of issuance of the patent.

26. JUNIPER has and continues to contributorily infringe. JUNIPER has actively encouraged or instructed others (e.g., its customers and/or the customers of its related companies), and continues to do so, on how to use its products and services (e.g., question and answer services on

the Internet) and related services that provide question and answer services across the Internet such as to cause infringement of one or more of claims 1–18 of the '497 patent, literally or under the doctrine of equivalents. Moreover, JUNIPER has known of the '497 patent and the technology underlying it from at least the date of issuance of the patent.

27. JUNIPER has caused and will continue to cause PacSec3 damage by direct and indirect infringement of (including inducing infringement of) the claims of the '497 patent.

IV. JURY DEMAND

PacSec3 hereby requests a trial by jury on issues so triable by right.

V. PRAYER FOR RELIEF

WHEREFORE, PacSec3 prays for relief as follows:

a. enter judgment that Defendant has infringed the claims of the '190 patent, the '564 patent and the '497 patent through selling, offering for sale, manufacturing, and inducing others to infringe by using and instructing to use Junos OS DDoS Protection, and perhaps other firewall/DDOS protection systems;

b. award PacSec3 damages in an amount sufficient to compensate it for Defendant's infringement of the Patents-in-Suit in an amount no less than a reasonable royalty or lost profits, together with pre-judgment and post-judgment interest and costs under 35 U.S.C. § 284;

c. award PacSec3 an accounting for acts of infringement not presented at trial and an award by the Court of additional damage for any such acts of infringement;

d. declare this case to be "exceptional" under 35 U.S.C. § 285 and award PacSec3 its attorneys' fees, expenses, and costs incurred in this action;

e. declare Defendant's infringement to be willful and treble the damages, including attorneys' fees, expenses, and costs incurred in this action and an increase in the damage award pursuant to 35 U.S.C. § 284;

f. a decree addressing future infringement that either (i) awards a permanent injunction enjoining Defendant and its agents, servants, employees, affiliates, divisions, and subsidiaries, and those in association with Defendant from infringing the claims of the Patents-in-Suit, or (ii) awards damages for future infringement in lieu of an injunction in an amount consistent with the fact that for future infringement the Defendant will be an adjudicated infringer of a valid patent, and trebles that amount in view of the fact that the future infringement will be willful as a matter of law; and

g. award PacSec3 such other and further relief as this Court deems just and proper.

Respectfully submitted,

Ramey & Schwaller, LLP

/s/William P. Ramey
William P. Ramey, III
Texas Bar No. 24027643
5020 Montrose Blvd., Suite 800
Houston, Texas 77006
(713) 426-3923 (telephone)
(832) 900-4941 (fax)
wramey@rameyfirm.com

Attorneys for PacSec3, LLC