IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXAS
MARSHALL DIVISION

PACSEC3, LLC,	)	
Plaintiff,	)	
	)	**Civil Action No. 2:21-cv-00141**
v.	)	
	)	
PALO ALTO 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 Palo Alto 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, Palo Alto Networks, Inc. ("Palo Alto") is a California Corporation. On information and belief, PALO ALTO 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. PALO ALTO can be served with process through their registered agent, Corporation Service Company d/b/a CSC-Lawyers Incorporation Service Company, 211 E. 7th Street, Suite 620, Austin, TX 78701 or wherever they may be found.

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 3901 North Dallas Parkway, Plano, TX 75093. 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. PALO ALTO offers for sale, sells and manufactures one or more firewall systems 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:

Exemplary Claim language	**Palo Alto Networks Evidence**
A packet flooding defense system for a network comprising a plurality of host computers, routers, communicatio	You can use Zone Protection Profiles on the firewall to configure packet-based attack protection and thereby drop IP, TCP, and IPv6 packets with undesirable characteristics or strip undesirable options from packets before allowing them into the zone. You can also configure flood protection, specifying the rate of SYN connections per second (not matching an existing session) that trigger an alarm, cause the firewall to randomly drop SYN packets or use SYN cookies, and cause the firewall to drop SYN packets that exceed the maximum rate.

n lines and transmitted data packets, said system comprising: at least one firewall, said firewall comprising:	**Pan-OS Administrator's Guide (Page 1259)** https://docs.paloaltonetworks.com/content/dam/techdocs/en_US/pdf/pan-os/10-0/pan-os-admin/pan-os-admin.pdf Palo Alto Networks: system 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;	You can use Zone Protection Profiles on the firewall to configure flood protection and thereby specify the rate of UDP connections per second (not matching an existing session) that trigger an alarm, trigger the firewall to randomly drop UDP packets, and cause the firewall to drop UDP packets that exceed the maximum rate. (Although UDP is connectionless, the firewall tracks UDP datagrams in IP packets on a session basis; therefore if the UDP packet doesn't match an existing session, it is considered a new session and it counts as a connection toward the thresholds.) **Pan-OS Administrator's Guide (Page 1263)** <https://docs.paloaltonetworks.com/content/dam/techdocs/en_US/pdf/pan-os/10-0/pan-os-admin/pan-os-admin.pdf>
… means for classifying data packets received at said firewall;,…	*Classified* DoS Protection policy rules apply the CPS thresholds defined in a classified DoS Protection profile to each individual device that matches the policy rule. For example, if you configure the classified DoS Protection profile to limit the CPS rate to 4,000, then no device in the group can accept more than 4,000 CPS. A DoS Protection policy can have one aggregate profile and one classified profile. **Pan-OS Administrator's Guide (Page 1402)** <https://docs.paloaltonetworks.com/content/dam/techdocs/en_US/pdf/pan-os/10-0/pan-os-admin/pan-os-admin.pdf>

	The reference describes means for classifying data packets received at said firewall [classify DoS Protection profile to each individual device that matches the policy rule]
means for associating a maximum acceptable transmission rate with each class of data packet received at said firewall;	DoS Protection profiles set flood protection thresholds (new CPS limits) for individual devices or groups of devices, resource protection thresholds (session limits for specified endpoints and resources), and whether the profile applies to aggregate or classified traffic. DoS Protection policy rules specify match criteria (source, destination, service ports), the action to take when traffic matches the rule, and the aggregate and classified DoS Protection profiles associated with each rule. **Pan-OS Administrator's Guide (Page 1402)** <https://docs.paloaltonetworks.com/content/dam/techdocs/en_US/pdf/pan-os/10-0/pan-os-admin/pan-os-admin.pdf> The reference describes means for associating a maximum acceptable transmission rate with each class of data packet received at said firewall [set flood protection threshold]
means for said firewall to find information for packets it receives regarding the path by which said packets came to said firewall; and	*Classified profiles can classify connections by source IP, destination IP, or both. For internet-facing zones, classify by destination IP only because the firewall can't scale to hold the internet routing table.* **Pan-OS Administrator's Guide (Page 1402)** <https://docs.paloaltonetworks.com/content/dam/techdocs/en_US/pdf/pan-os/10-0/pan-os-admin/pan-os-admin.pdf>

	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 [Classified profiles can classify connections by source IP]
whereby, said firewall can use said information to allocate the transmission rate for each class in a desired way.	*Classified* DoS Protection policy rules apply the CPS thresholds defined in a classified DoS Protection profile to each individual device that matches the policy rule. For example, if you configure the classified DoS Protection profile to limit the CPS rate to 4,000, then no device in the group can accept more than 4,000 CPS. A DoS Protection policy can have one aggregate profile and one classified profile. **Pan-OS Administrator's Guide (Page 1402)** <https://docs.paloaltonetworks.com/content/dam/techdocs/en_US/pdf/pan-os/10-0/pan-os-admin/pan-os-admin.pdf> The reference states that said firewall can use said information to allocate the transmission rate for each class in a desired way [For example, if you configure the classified DoS Protection profile to limit the CPS rate to 4,000, then no device in the group can accept more than 4,000 CPS.]

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

11. PALO ALTO has and continues to induce infringement. PALO ALTO 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, PALO ALTO has known of the '190 patent and the technology underlying it from at least the date of issuance of the patent.

12. PALO ALTO has and continues to contributorily infringe. PALO ALTO 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, PALO ALTO has known of the '190 patent and the technology underlying it from at least the date of issuance of the patent.

13. PALO ALTO 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. PALO ALTO offers for sale, sells and manufactures one or more firewall systems 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:

Exemplary Claim language	**Palo Alto Networks Evidence**
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:	Zone Protection profiles defend zones against flood, reconnaissance, packet-based, and non-IP-protocol-based attacks. DoS Protection profiles used in DoS Protection policy rules defend specific, critical devices against targeted flood and resource-based attacks. A DoS attack overloads the network or targeted critical systems with large amounts of unwanted traffic an attempt to disrupt network services. **Pan-OS Administrator's Guide (Page 1402)** <https://docs.paloaltonetworks.com/content/dam/techdocs/en_US/pdf/pan-os/10-0/pan-os-admin/pan-os-admin.pdf> Palo Alto Networks: Firewall 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;	You can use Zone Protection Profiles on the firewall to configure flood protection and thereby specify the rate of UDP connections per second (not matching an existing session) that trigger an alarm, trigger the firewall to randomly drop UDP packets, and cause the firewall to drop UDP packets that exceed the maximum rate. (Although UDP is connectionless, the firewall tracks UDP datagrams in IP packets on a session basis; therefore if the UDP packet doesn't match an existing session, it is considered a new session and it counts as a connection toward the thresholds.) Pan-OS Administrator's Guide (Page 1263) <https://docs.paloaltonetworks.com/content/dam/techdocs/en_US/pdf/pan-os/10-0/pan-os-admin/pan-os-admin.pdf> The reference describes 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
means for classifying data packets received at said firewall related to the consumption of at least one resource;	*Classified* DoS Protection policy rules apply the CPS thresholds defined in a classified DoS Protection profile to each individual device that matches the policy rule. For example, if you configure the classified DoS Protection profile to limit the CPS rate to 4,000, then no device in the group can accept more than 4,000 CPS. A DoS Protection policy can have one aggregate profile and one classified profile. **Pan-OS Administrator's Guide (Page 1402)** <https://docs.paloaltonetworks.com/content/dam/techdocs/en_US/pdf/pan-os/10-0/pan-os-admin/pan-os-admin.pdf> The reference describes means for classifying data packets received at said firewall [classify DoS Protection profile to each individual device that matches the policy rule]
means for associating a maximum acceptable transmission rate with each class of data packet received at said firewall;	DoS Protection profiles set flood protection thresholds (new CPS limits) for individual devices or groups of devices, resource protection thresholds (session limits for specified endpoints and resources), and whether the profile applies to aggregate or classified traffic. DoS Protection policy rules specify match criteria (source, destination, service ports), the action to take when traffic matches the rule, and the aggregate and classified DoS Protection profiles associated with each rule. **Pan-OS Administrator's Guide (Page 1402)**

	<https://docs.paloaltonetworks.com/content/dam/techdocs/en_US/pdf/pan-os/10-0/pan-os-admin/pan-os-admin.pdf> The reference describes means for associating a maximum acceptable transmission rate with each class of data packet received at said firewall [set flood protection threshold]
means for limiting the transmission rate from the firewall to the maximum acceptable transmission rate for each class of data packet; and	*Classified* DoS Protection policy rules apply the CPS thresholds defined in a classified DoS Protection profile to each individual device that matches the policy rule. For example, if you configure the classified DoS Protection profile to limit the CPS rate to 4,000, then no device in the group can accept more than 4,000 CPS. A DoS Protection policy can have one aggregate profile and one classified profile. **Pan-OS Administrator's Guide (Page 1402)** <https://docs.paloaltonetworks.com/content/dam/techdocs/en_US/pdf/pan-os/10-0/pan-os-admin/pan-os-admin.pdf> The reference describes means for limiting the transmission rate from the firewall to the maximum acceptable transmission rate for each class of data packet [For example, if you configure the classified DoS Protection profile to limit the CPS rate to 4,000, then no device in the group can accept more than 4,000 CPS.]
whereby, packet flooding and other over usage type distributed denial of service attacks cannot be effectively launched through said non-redundant connection.	Zone Protection profiles defend zones against flood, reconnaissance, packet-based, and non-IP-protocol-based attacks. DoS Protection profiles used in DoS Protection policy rules defend specific, critical devices against targeted flood and resource-based attacks. A DoS attack overloads the network or targeted critical systems with large amounts of unwanted traffic an attempt to disrupt network services. **Pan-OS Administrator's Guide (Page 1402)** <https://docs.paloaltonetworks.com/content/dam/techdocs/en_US/pdf/pan-os/10-0/pan-os-admin/pan-os-admin.pdf>

	The reference describes packet flooding and other over usage type distributed denial of service attacks cannot be effectively launched through zone protection.

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

18. PALO ALTO has and continues to induce infringement. PALO ALTO 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, PALO ALTO has known of the '564 patent and the technology underlying it from at least the date of issuance of the patent.

19. PALO ALTO has and continues to contributorily infringe. PALO ALTO 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, PALO ALTO has known of the '564 patent and the technology underlying it from at least the date of issuance of the patent.

20. PALO ALTO 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. PALO ALTO offers for sale, sells and manufactures one or more firewall systems 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:

Exemplary Claim language	**Palo Alto Networks Evidence**
A method of providing packet flooding defense for a network comprising a plurality of host computers,	You can use Zone Protection Profiles on the firewall to configure packet-based attack protection and thereby drop IP, TCP, and IPv6 packets with undesirable characteristics or strip undesirable options from packets before allowing them into the zone. You can also configure flood protection, specifying the rate of SYN connections per second (not matching an existing session) that trigger an alarm, cause the firewall to randomly drop SYN packets or use SYN cookies, and cause the firewall to drop SYN packets that exceed the maximum rate.

routers, communication lines and transmitted data packets, said method comprising the steps of:	**Pan-OS Administrator's Guide (Page 1259)** https://docs.paloaltonetworks.com/content/dam/techdocs/en_US/pdf/pan-os/10-0/pan-os-admin/pan-os-admin.pdf Palo Alto Networks: system 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;	Flood Protection Configure Flood Protection settings based on the number of packets you want to allow to each service behind the firewall. Settings apply to all traffic that enters the network through any interface in the zone on which the Zone Protection Profile is active, but a separate counter is maintained for each source IP/destination IP/destination port tuple. **Advanced Threat Prevention Deployment Tech Note PAN-OS 7.0 (Page 46)** 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 [counter is maintained for each source IP/destination IP/destination port tuple]. The reference describes said path comprising all routers in said network via which said packets are routed to said computer [traffic that enters the network].
classifying data packets received at said host computer into	

wanted data packets and unwanted data packets by path;	One particular feature of App-ID is its ability to classify unknown traffic as unknown-tcp, unknown-udp or unknown-p2p. This can be leveraged to block connections where the underlying application cannot be identified, as is often the case with custom outbound C2 channels. As such, App-ID can assist in disrupting the kill-chain at the Command-and-Control stage. **Advanced Threat Prevention Deployment Tech Note PAN-OS 7.0 (Page 9)** The reference describes classifying data packets received at said host computer into wanted data packets and unwanted data packets by path [classify unknown traffic].
associating a maximum acceptable processing rate with each class of data packet received at said host computer; and	DoS Protection profiles set flood protection thresholds (new CPS limits) for individual devices or groups of devices, resource protection thresholds (session limits for specified endpoints and resources), and whether the profile applies to aggregate or classified traffic. DoS Protection policy rules specify match criteria (source, destination, service ports), the action to take when traffic matches the rule, and the aggregate and classified DoS Protection profiles associated with each rule. **Pan-OS Administrator's Guide (Page 1402)** <https://docs.paloaltonetworks.com/content/dam/techdocs/en_US/pdf/pan-os/10-0/pan-os-admin/pan-os-admin.pdf> The reference describes associating a maximum acceptable transmission rate with each class of data packet received at said firewall [set flood protection threshold]
allocating a processing rate less than or equal to said maximum acceptable processing rate for unwanted data packets.	Maximal Rate When the Maximal Rate threshold is exceeded, any further packets that match the DoS Protection rule and classification criteria (in case of a classified profile) will be dropped for the block duration specified. The default value for SYN-cookie is 1.000.000 which will prevent it from being triggered in almost any environment. You should adjust this value to match your environment in the following scenarios: **Advanced Threat Prevention Deployment Tech Note PAN-OS 7.0 (Page 42)**

	The reference describes allocating a processing rate less than or equal to said maximum acceptable processing rate for unwanted data packets [When the Maximal Rate threshold is exceeded, any further packets that match the DoS Protection rule and classification criteria (in case of a classified profile) will be dropped].

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

25. PALO ALTO has and continues to induce infringement. PALO ALTO 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, PALO ALTO has known of the '497 patent and the technology underlying it from at least the date of issuance of the patent.

26. PALO ALTO has and continues to contributorily infringe. PALO ALTO 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, PALO ALTO has known of the '497 patent and the technology underlying it from at least the date of issuance of the patent.

27. PALO ALTO 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 Pan-OS and/or 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 (if) 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