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

PACSEC3, LLC,	)	
Plaintiff,	)	
	)	**Civil Action No. 2:21-cv-00140-JRG**
v.	)	
	)	
MCAFEE, LLC,	)	**JURY TRIAL DEMANDED**
Defendant.	)	

PLAINTIFF'S SECOND AMENDED COMPLAINT FOR PATENT INFRINGEMENT

PacSec3, LLC ("PacSec") files this Second Amended Complaint and demand for jury trial seeking relief from patent infringement of the claims of U.S. Patent No. 7,047,564 ("the '564 patent") (referred to as the "Patent-in-Suit") by McAfee, LLC. This amended complaint is filed by agreement of the parties and pursuant to the scheduling order[1] in this matter and is filed to drop claims of infringement for U.S. Pat. Nos. 6,789,190 and 7,523,497.

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, McAfee,. LLC ("McAfee") is a California Limited Liability Company. On information and belief, MCAFEE 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. MCAFEE has appeared in this matter.

II. JURISDICTION AND VENUE

[1] Doc. No. 23.

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 Limited Liability Company 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 - Infringement of the '564 Patent

7. On May 16, 2006, U.S. Patent No. 7,047,564 ("the '564 patent", attached as Exhibit B) entitled "REVERSE 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.

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

9. MCAFEE offers for sale, sells and manufactures one or more firewall systems, including the McAfee Security Platform, 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.

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

Claim language	**McAfee Network Evidence**
A packet transmission control system for managing traffic between at least two data networks, each of said networks comprising a plurality of host	In the Manager, every rate limiting queue of a Sensor is uniquely identified by a name. The traffic management queues are configured based on Protocol, TCP ports, UDP ports, and IP Protocol Number. You can create multiple queues for each port of the sensor. The traffic management configuration in the Manager must be followed by a configuration update to the sensor. Rate limiting option is available as one of the traffic management options in the Manager. **McAfee Network Security Platform Application Notes (Page 40)** <https://docs.mcafee.com/bundle/network-security-platform-application-notes/ page/GUID-F9619079-BF06-4E81-89B8-2538B5F41A91.html>

computers, communication lines and transmitted data packets, said system comprising:	McAfee Network Security Platform 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. The
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 policies** — These are your network security policies based on which the Sensor allows or blocks traffic in and ou your network. There are two types of Firewall policies — advanced and classic. **McAfee Network Security Platform 9.1.x Product Guide** (Page 924) <https://docs.mcafee.com/bundle/network-security-platform-9.1.x-product-guide/ page/GUID-5CF9DD89-6B69-4AD5-8A8B-EF29412F36D8.html> With the source IP addresses properly classified, the Sensor can protect a network from DoS attacks. When a statistical anomaly occurs, the Sensor takes the following actions on the source IP profile in question: • The Sensor blocks all packets with source IP addresses in the bins that occupy a large percentage of the IP space, but represent a small percentage of the long-term traffic. This combats attacks that are generated with random, wide-ranging, spoofed source IP addresses. **McAfee Network Security Platform 9.1.x Product Guide** (Page 856) <https://docs.mcafee.com/bundle/network-security-platform-9.1.x-product-guide/ page/GUID-5CF9DD89-6B69-4AD5-8A8B-EF29412F36D8.html> The reference describes at least one firewall [Firewall policies], said firewall comprising: hardware and software serving to control packet transmission between said network and a host computer connected to an internal network [With the source IPs properly classified, the Sensor can now protect a network from DoS attacks].
means for classifying data packets received at	Source IP addresses classification is more effective than using devices such as firewalls that limits the rate of SYN packets on the network to block DoS attacks. The key difference in such an approach and Network Security Platform is that a rate-limiting device blocks traffic randomly. Good traffic has the same probability of being blocked as attack traffic. On the other hand, source IP address classification used by Network Security Platform attempts to differentiate good traffic from attack traffic, so attack traffic is more likely to be blocked.

said firewall related to the consumption of at least one resource;	**McAfee Network Security Platform 9.1.x Product Guide** (Page 856) <https://docs.mcafee.com/bundle/network-security-platform-9.1.x-product-guide/ page/GUID-5CF9DD89-6B69-4AD5-8A8B-EF29412F36D8.html> The reference describes means for classifying data packets received at said firewall [source IP classification used by Network Security Platform attempts to differentiate good traffic from attack traffic].
means for associating a maximum acceptable transmission rate with each class of data packet received at said firewall;	You can define a threshold value to limit the number of connections per second or the number of active connections to prevent connection based DoS attacks. The Sensor provides the ability to define threshold values to limit number of connections (three-way TCP handshakes) a host can establish. The number of connections or connection rate that is less than or equal to the defined threshold value is allowed. When this number is exceeded, the subsequent connections are dropped. This helps in minimizing the connection-based DoS attacks on server. **McAfee Network Security Platform 9.1.x Product Guide** (Page 859) <https://docs.mcafee.com/bundle/network-security-platform-9.1.x-product-guide/ page/GUID-5CF9DD89-6B69-4AD5-8A8B-EF29412F36D8.html> The reference describes means for associating a maximum acceptable transmission rate with each class of data packet received at said firewall [You can define a threshold value to limit the number of connections/ per second].
means for limiting the transmission rate from the firewall to the maximum acceptable transmission rate for each class of data packet; and	Rate limiting is very effective when applied in a specific context with full knowledge of the nature of traffic in a particular network. Rate limiting needs to be applied carefully as it might drop legitimate traffic as well. **McAfee Network Security Platform 9.1.x Product Guide** (Page 859) <https://docs.mcafee.com/bundle/network-security-platform-9.1.x-product-guide/ page/GUID-5CF9DD89-6B69-4AD5-8A8B-EF29412F36D8.html> The reference states that said firewall can use said information to allocate the transmission rate for each class in a desired way [Rate limiting is very

	effective when applied in a specific context with full knowledge of the nature of traffic in a particular network].
whereby, packet flooding and other over usage type distributed denial of service attacks cannot be effectively launched through said non-redundant connection.	Network Security Platform uses a specific choice of initial TCP number as a defense against SYN flood attacks. **McAfee Network Security Platform Application Notes (Page 38)** <https://docs.mcafee.com/bundle/network-security-platform-application-notes/ page/GUID-F9619079-BF06-4E81-89B8-2538B5F41A91.html> The reference describes packet flooding and other over usage type distributed denial of service attacks cannot be effectively launched through said non-redundant connection [Network Security Platform uses a specific choice of initial TCP number as a defense against SYN flood attacks].

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

11. MCAFEE has and continues to induce infringement. MCAFEE 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, MCAFEE has known of the ’564 patent and the technology underlying it from at least the filing date of the lawsuit.

12. MCAFEE has and continues to contributorily infringe. MCAFEE 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., computer security systems) and related services that provide computer security systems 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, MCAFEE has known of the '564 patent and the technology underlying it from at least the date of filing of the lawsuit.

13. MCAFEE 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.

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 '564 patent through selling, offering for sale, manufacturing, and inducing others to infringe by using and instructing to use at least the McAfee Security Platform, and perhaps other firewall/DDOS protection systems;

b. award PacSec3 damages in an amount sufficient to compensate it for Defendant's infringement of the Patent-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 Patent-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

CERTIFICATE OF SERVICE

Pursuant to the Federal Rules of Civil Procedure, I hereby certify that all counsel of record who have appeared in this case are being served today, October 22, 2021, with a copy of the foregoing via the Court's CM/ECF system.

/s/ William P. Ramey, III
William P. Ramey, III