Craig Buschmann, cbuschmann@rameyfirm.com, Utah Bar No. 10696
Attonrey for PACSEC3, LLC
5020 Montrose Blvd., Suite 800
Houston, Texas 77006
(713) 426-3923

IN THE UNITED STATES DISTRICT COURT

DISTRICT OF UTAH

PACSEC3, LLC,
        Plaintiff,
 	
v.
 	
F5 NETWORKS, INC.
        Defendant
	CASE NO 2:20-cv-00697-JCB
	
	PLAINTIFF'S ORIGINAL COMPLAINT FOR PATENT INFRINGEMENT
	
	JURY TRIAL DEMANDED

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 F5 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, F5 Networks, Inc. ("F5") is a corporation organized and existing under the laws of California, with a principal place of business located at 380 W Data Dr Ste 120, Draper, UT 84020, through its acquisition of Shape Security, Inc.. On information and belief, F5 sells and offers to sell products and services throughout Utah, 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 Utah and this judicial district. F5 can be served

with process through their Registered Agent, 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 380 W Data Dr Ste 120, Draper, UT 84020. 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 Utah and this judicial district; (ii) Defendant

has purposefully availed itself of the privileges of conducting business in the State of Utah 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 Utah 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 Utah 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. F5 offers for sale, sells and manufactures one or more firewall systems, including the BIG-IP Application Security Manager (ASM), 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	F5 Big Evidence
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:	The BIG-IP® system handles DNS attacks that use malformed packets, protocol errors, and malicious attack vectors. Protocol error attack detection settings detect malformed and malicious packets, or packets that are employed to flood the system with several different types of responses. You can configure settings to identify DNS attacks with a DoS profile. **Manual Chapter: Detecting and Preventing DNS DoS Attacks (Page 2)** F5 BIG-IP Application Security Manager (ASM) 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;	The BIG-IP Network Firewall provides policy-based access control to and from address and port pairs inside and outside of your network. By default the network firewall is configured in ADC mode, which is a default allow configuration, in which all traffic is allowed through the firewall, and any **traffic you want to block must be explicitly specified**. **F5 Candidate-produced Study Guide (Page 48)** The reference describes at least one firewall [Network Firewall], said firewall comprising: hardware and software serving to control packet transmission between said network and a host computer connected to an internal network
… means for classifying data packets received at said firewall;…	**Classification Engine** – Uses the Compiled Classifier to determine the set of rules matching a packet based on the packet contents and other relevant input. Resides in the "packet processing path, as part of TMM process". **F5 Candidate-produced Study Guide (Page 48)**

means for associating a maximum acceptable transmission rate with each class of data packet received at said firewall;	**Default Internal Rate Limit** - Use **Specify** to set a value, in packets per second, which cannot be exceeded by packets of this type. All packets of this type over the threshold are dropped. Rate limiting continues until the rate drops below the specified limit again. **F5 Candidate-produced Study Guide (Page 58)** The reference describes means for associating a maximum acceptable transmission rate with each class of data packet received at said firewall [Use Specify to set a value, in packets per second, which cannot be exceeded by packets of this type].
means for said firewall to find information for packets it receives regarding the path by which said packets came to said firewall; and	**Classification Engine** – Uses the Compiled Classifier to determine the set of rules matching a packet based on the packet contents and other relevant input. Resides in the "packet processing path, as part of TMM process". **F5 Candidate-produced Study Guide (Page 48)** 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 [determine the set of rules matching a packet based on the packet contents and other relevant input].

whereby, said firewall can use said information to allocate the transmission rate for each class in a desired way.	**Detection Threshold Percent** – Additional flag to determine the further aggressiveness of the attack, of a particular type of category. Here, AFM compares the current rate of the particular Category type's attack with Last One Hour average packet rate. For example, `if the average rate for the last hour is 1000 packets per second, and you set the percentage increase threshold to 100, an attack is detected at 100 percent above the average, or 2000 packets per second.` When the threshold is passed, an attack is logged and reported. The system then automatically institutes a rate limit equal to the average for the last hour, and all packets above that limit are dropped. The system continues to check every second until the incoming packet rate drops below the percentage increase threshold. Rate limiting continues until the rate drops below the specified limit. **F5 Candidate-produced Study Guide (Page 57)** The reference states that said firewall can use said information to allocate the transmission rate for each class in a desired way [The system then automatically institutes a rate limit equal to the average for the last hour, and all packets above that limit are dropped].

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

11. F5 has and continues to induce infringement. F5 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, F5 has known of the '190 patent and the technology underlying it from at least the date of issuance of the patent.

12. F5 has and continues to contributorily infringe. F5 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, F5 has known of the '190 patent and the technology underlying it from at least the date of issuance of the patent.

13. F5 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.

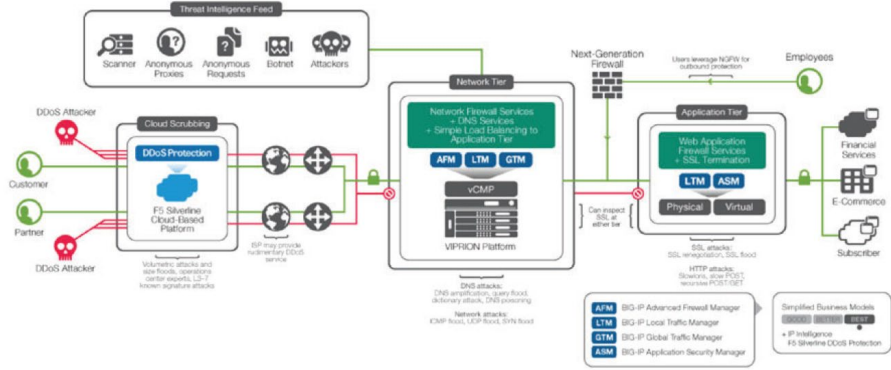## B. Infringement of the '564 Patent

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

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

16. F5 offers for sale, sells and manufactures one or more firewall systems, including the BIG-IP Application Security Manager (ASM), 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

7

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	F5 Big 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:	 **F5 Candidate-produced Study Guide (Page 46)** F5 BIG-IP Application Security Manager (ASM) 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	The BIG-IP Network Firewall provides policy-based access control to and from address and port pairs inside and outside of your network. By default the network firewall is configured in ADC mode, which is a default allow configuration, in which all traffic is allowed through the firewall, and any **traffic you want to block must be explicitly specified**.

connection between said networks and serving to control packet transmission between said networks;	**F5 Candidate-produced Study Guide (Page 48)** The reference describes at least one firewall [Network Firewall], said firewall comprising: hardware and software serving to control packet transmission between said network and a host computer connected to an internal network
means for classifying data packets received at said firewall related to the consumption of at least one resource;	**Classification Engine** – Uses the Compiled Classifier to determine the set of rules matching a packet based on the packet contents and other relevant input. Resides in the "packet processing path, as part of TMM process". **F5 Candidate-produced Study Guide (Page 48)**
means for associating a maximum acceptable transmission rate with each class of data packet received at said firewall;	Default Internal Rate Limit - Use **Specify** to set a value, in packets per second, which cannot be exceeded by packets of this type. All packets of this type over the threshold are dropped. Rate limiting continues until the rate drops below the specified limit again. **F5 Candidate-produced Study Guide (Page 58)** The reference describes means for associating a maximum acceptable transmission rate with each class of data packet received at said firewall [Use Specify to set a value, in packets per second, which cannot be exceeded by packets of this type].
means for limiting the transmission rate from the firewall to the	

maximum acceptable transmission rate for each class of data packet; and	**Detection Threshold Percent** – Additional flag to determine the further aggressiveness of the attack, of a particular type of category. Here, AFM compares the current rate of the particular Category type's attack with Last One Hour average packet rate. For example, `if the average rate for the last hour is 1000 packets per second, and you set the percentage increase threshold to 100, an attack is detected at 100 percent above the average, or 2000 packets per second.` When the threshold is passed, an attack is logged and reported. The system then automatically institutes a rate limit equal to the average for the last hour, and all packets above that limit are dropped. The system continues to check every second until the incoming packet rate drops below the percentage increase threshold. Rate limiting continues until the rate drops below the specified limit. **F5 Candidate-produced Study Guide (Page 57)** The reference states that said firewall can use said information to allocate the transmission rate for each class in a desired way [The system then automatically institutes a rate limit equal to the average for the last hour, and all packets above that limit are dropped].
whereby, packet flooding and other over usage type distributed denial of service attacks cannot be effectively launched through said non-redundant connection.	The BIG-IP® system handles DNS attacks that use malformed packets, protocol errors, and malicious attack vectors. Protocol error attack detection settings detect malformed and malicious packets, or packets that are employed to flood the system with several different types of responses. You can configure settings to identify DNS attacks with a DoS profile. **Manual Chapter: Detecting and Preventing DNS DoS Attacks (Page 2)** The reference describes packet flooding and other over usage type distributed denial of service attacks cannot be effectively launched through said non-redundant connection [DoS Protection profile to provide custom responses to malformed DNS attacks, and DNS flood attacks].

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

18. F5 has and continues to induce infringement. F5 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, F5 has known of the '564 patent and the technology underlying it from at least the date of issuance of the patent.

19. F5 has and continues to contributorily infringe. F5 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, F5 has known of the '564 patent and the technology underlying it from at least the date of issuance of the patent.

20. F5 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. F5 offers for sale, sells and manufactures one or more firewall systems, including the BIG-IP Application Security Manager (ASM), 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	F5 Big Evidence
A method of providing packet flooding defense for a network comprising a plurality of host computers, routers, communication lines and transmitted data packets, said method comprising the steps of:	The BIG-IP® system handles DNS attacks that use malformed packets, protocol errors, and malicious attack vectors. Protocol error attack detection settings detect malformed and malicious packets, or packets that are employed to flood the system with several different types of responses. You can configure settings to identify DNS attacks with a DoS profile. **Manual Chapter: Detecting and Preventing DNS DoS Attacks (Page 2)** F5 BIG-IP Application Security Manager (ASM) 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;	The BIG-IP® system handles DNS attacks that use malformed packets, protocol errors, and malicious attack vectors. Protocol error attack detection settings detect malformed and malicious packets, or packets that are employed to flood the system with several different types of responses. You can configure settings to identify DNS attacks with a DoS profile. **Manual Chapter: Detecting and Preventing DNS DoS Attacks (Page 2)** 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 [detect malformed and malicious packets]. The reference describes said path comprising all routers in said network via which said packets are routed to said computer [packets that are employed to flood the system].
classifying data packets received at said host computer into wanted data packets and unwanted data packets by path;	**Classification Engine** – Uses the Compiled Classifier to determine the set of rules matching a packet based on the packet contents and other relevant input. Resides in the "packet processing path, as part of TMM process". **F5 Candidate-produced Study Guide (Page 48)**
associating a maximum acceptable processing rate with each class of data packet received at said host computer; and	**Default Internal Rate Limit** - Use **Specify** to set a value, in packets per second, which cannot be exceeded by packets of this type. All packets of this type over the threshold are dropped. Rate limiting continues until the rate drops below the specified limit again. **F5 Candidate-produced Study Guide (Page 58)**

	The reference describes means for associating a maximum acceptable transmission rate with each class of data packet received at said firewall [Use Specify to set a value, in packets per second, which cannot be exceeded by packets of this type].
allocating a processing rate less than or equal to said maximum acceptable processing rate for unwanted data packets.	**Detection Threshold Percent** – Additional flag to determine the further aggressiveness of the attack, of a particular type of category. Here, AFM compares the current rate of the particular Category type's attack with Last One Hour average packet rate. For example, `if the average rate for the last hour is 1000 packets per second, and you set the percentage increase threshold to 100, an attack is detected at 100 percent above the average, or 2000 packets per second.` When the threshold is passed, an attack is logged and reported. The system then automatically institutes a rate limit equal to the average for the last hour, and all packets above that limit are dropped. The system continues to check every second until the incoming packet rate drops below the percentage increase threshold. Rate limiting continues until the rate drops below the specified limit. **F5 Candidate-produced Study Guide (Page 57)** The reference describes allocating a processing rate less than or equal to said maximum acceptable processing rate for unwanted data packets [The system then automatically institutes a rate limit equal to the average for the last hour, and all packets above that limit are dropped].

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

25. F5 has and continues to induce infringement. F5 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, F5 has known of the '497 patent and the technology underlying it from at least the date of issuance of the patent.

26. F5 has and continues to contributorily infringe. F5 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, F5 has known of the '497 patent and the technology underlying it from at least the date of issuance of the patent.

27. F5 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 at least the BIG-IP Application Security Manager (ASM), and perhaps other firewall 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/Craig Buschmann
Craig Buschmann
Utah Bar No. 10696
5020 Montrose Blvd., Suite 800
Houston, Texas 77006
(713) 426-3923 (telephone)
(832) 900-4941 (fax)

16

cbuschmann@rameyfirm.com

Attorneys for PacSec3, LLC