EXHIBIT 1

APPENDIX F-1

8,677,494	Juniper's SRX Series Services Gateways
The statements and documents cited below are based on information available to Finjan, Inc. at the time this chart was created. Finjan reserves its right to supplement this chart as additional information becomes known to it. For purposes of this chart, "SRX Gateways" include at least the following appliance models listed in Exhibit A. For purposes of this chart, "SRX Gateways" are SRX Series Services Gateway appliances, either alone, or when used in conjunction with other products or services as a system. For example, SRX Gateways perform the infringing procedures in combination with Juniper Sky Advanced Threat Prevention ("Sky ATP")[1], the Advanced Threat Prevention Appliance ("ATP Appliance")[2], and/or the Space Security Director[3] as an integrated distributed system, as will be described in greater detail herein. Based on public information, SRX Gateways all operate identically with respect to the identified claims and only vary based on software specifications and/or deployment options. As identified and described element by element below, the one or more of the SRX Series Services Gateways infringe at least claims 10, 14, 16, and 18 of the '494 Patent.	
Claim 10	
10a. A system for managing Downloadables, comprising:	SRX Series Services Gateways meet the recited claim language because they include a system for managing Downloadables. As used herein, and throughout these contentions, Downloadable is "an executable application program, which is downloaded from a source computer and run on the destination computer." SRX Series Services Gateways meet the recited claim language because they selectively determine whether files received from a source computer (Downloadables), that were inspected for malware by an SRX Series Services Gateway, should be communicated to Sky ATP as a destination computer (management system). In another scenario, SRX Series Services Gateways, in combination with Sky ATP, meet the recited claim language because they provide a distributed computer system that that uses a pipeline of technologies to detect malware on Downloadables received from SRX Service Series Gateways. The distributed system of SRX Series Services Gateways and Sky ATP manage the distribution of Downloadables within a given computer network (management system) by providing the computer network with malware determinations ("verdicts") that enable the computer network to determine whether a web client or Internet application should receive a particular Downloadable that is requested. Notably, Internet applications include web browsers, FTP or file download clients, messaging clients, and email client applications. In another scenario, SRX Series Services Gateways, in combination with ATP Appliance, meet the recited claim language because they provide a distributed

[1] Sky ATP includes the components and services in Exhibit A.
[2] ATP Appliance includes the appliance models listed in Exhibit A.
[3] Space Security Director includes the appliance models listed in Exhibit A.

	computer system to detect malware on Downloadables received from SRX Service Series Gateways, which are used as "collectors" that are dispersed across different points within a given network. The distributed system of SRX Series Services Gateways and ATP Appliance manage the distribution of Downloadables within a given computer network (management system) by providing the computer network with malware determinations. The details of these operations are set for in greater detail below: For instance, as discussed in the excerpt below, SRX Series Services Gateways manage Downloadables because, they each receive downloaded content and perform security functions related to that content within a security system when they provide "perimeter security, content security, application visibility, tracking and policy enforcement, user role-based control, threat intelligence through integration with Juniper Networks Spotlight Secure, and network-wide threat visibility and control." The content such files is a "Downloadable" because it is of the type that is downloaded from a source computer (e.g. web server) to be run on a destination computer (e.g., web client or Internet application). Notably, Internet applications include web browsers, FTP or file download clients, messaging clients, and email client applications. • SRX Series for the branch provides perimeter security, content security, application visibility, tracking and policy enforcement, user role-based control, threat intelligence through integration with Juniper Networks Spotlight Secure*, and network-wide threat visibility and control. Using zones and policies, network administrators can configure and deploy branch SRX Series gateways quickly and securely. Policy-based VPNs support more complex security architectures that require dynamic addressing and split tunneling. The SRX Series also includes wizards for firewall, IPsec VPN, Network Address Translation (NAT), and initial setup to simplify configurations out of the box. SRX Series Service Gateways For the Branch.pdf at page 1. As shown in the figure below, SRX Series Services Gateways manage Downloadables when they operate with Sky ATP because they identify suspicious computer operations by extracting malicious objects and blocks them from being communicated as part of outbound C&C traffic.

Sky ATP protects your network by performing the following tasks:

- The SRX Series device extracts potentially malicious objects and files and sends them to the cloud for analysis.
- Known malicious files are quickly identified and dropped before they can infect a host.
- Multiple techniques identify new malware, adding it to the known list of malware.
- Correlation between newly identified malware and known Command and Control (C&C) sites aids analysis.
- The SRX Series device blocks known malicious file downloads and outbound C&C traffic.

Juniper Networks Sky Advanced Threat Prevention.pdf at page 1.

Additionally, as shown in the excerpt below, SRX Series Services Gateways and ATP Appliance act in combination as Downloadable managers because they act as file collectors that upload "suspicious files" to the ATP Appliance for management.

ATP Appliance with SRX Series Services Gateways as Collectors

When using SRX Series Services Gateways as collectors, the ATP Appliance is ideal for organizations that have already deployed, or are planning to deploy, SRX Series firewalls in their environment and are specifically looking for an on-premise solution for advanced threat detection and analysis. Unlike standalone mode, in this deployment the SRX Series firewalls act as collectors, uploading suspicious files to the SmartCore analytics engine for analysis. Standalone collectors are optional and can be deployed in conjunction with those running on the SRX Series gateways. In this mode, the ATP Appliance also provides threat intelligence to the SRX Series firewalls to block callbacks to malicious C&C servers. The ATP Appliance also sends a list of infected hosts requiring immediate attention so the SRX Series can isolate those devices. The SRX Series device and security policies can be configured on Juniper Networks Junos Space® Security Director to quarantine or block identified threats.

3510633-en.pdf at page 5.

Additionally, the distributed computer system of a SRX Series Services Gateway and Junos Space Security Director meets the recited claim language because it

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS

Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS

Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS

Sync your system to PACER to automate legal marketing.