
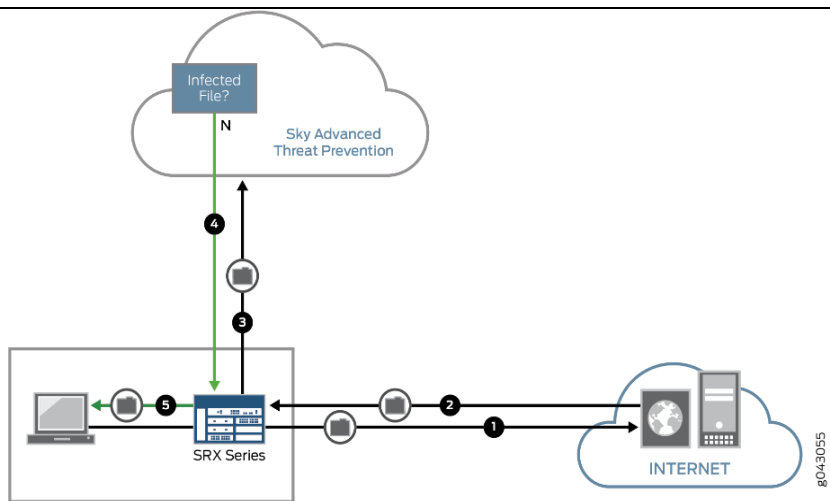


EXHIBIT 2

APPENDIX F-2

8,677,494	Juniper's Sky Advanced Threat Prevention
<p>The statements and documents cited below are based on information available to Finjan at the time this chart was created. Finjan reserves its right to supplement this chart as additional information becomes known to it.</p> <p>For purposes of this chart, "Sky ATP" is the cloud service and all support infrastructure maintained by Juniper, and includes the services and components in Exhibit A, as will be described in greater detail herein. Based on public information, Sky ATP operates identically with respect to the identified claims and only vary based on software specifications and/or deployment options.</p> <p>As identified and described element by element below, Sky ATP infringes at least claims 10, 14, 16, and 18 of the '494 Patent.</p>	
Claim 10	
<p>10a. A system for managing Downloadables, comprising:</p>	<p>Sky ATP meets the recited claim language because it includes a system for managing Downloadables.</p> <p>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."</p> <p>Sky ATP meets the recited claim language because it provides a computer system that uses a pipeline of technologies to detect malware on Downloadables received from SRX Service Series Gateways. Sky ATP manages the distribution of Downloadables within a given computer network (management system) by providing the computer network with malware determinations 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. The details of these operations are set forth in greater detail below:</p> <p>For instance, as shown in the figure below, Sky ATP identifies suspicious computer operations by extracting malicious objects and blocks them from being communicated as part of outbound C&C traffic.</p>

	 <p>Sky ATP protects your network by performing the following tasks:</p> <ul style="list-style-type: none"> • 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. <p>Juniper Networks Sky Advanced Threat Prevention.pdf at page 1.</p>
<p>10b. a receiver for receiving an incoming Downloadable;</p>	<p>Sky ATP meets the recited claim language because it includes a receiver for receiving an incoming Downloadable.</p> <p>Sky ATP meets the recited claim language because it includes software components (proxy software) that are configured to receive Downloadables from a SRX Series Services Gateway in order to detect malware. Downloadables are received by one or more computers within the cloud computing environment of Sky ATP where they can then be retrieved for malware detection purposes. The details of these operations are set forth in greater detail below:</p> <p>As shown in the figure below, software components (proxy software) resident within Sky ATP receive Downloadables for inspection when an SRX Series Services Gateway communicates the Downloadable to Sky ATP after inspection is performed by the SRX Series Services Gateway (see, e.g., Step 3 in the figure below). Downloadables received by Sky ATP are stored therein within a resident memory device where they are retrieved to perform file inspections.</p>



Step	Description
1	A client system behind an SRX Series devices requests a file download from the Internet. The SRX Series device forwards that request to the appropriate server.
2	The SRX Series device receives the downloaded file and checks its security profile to see if any additional action must be performed.
3	The downloaded file type is on the list of files that must be inspected and is sent to the cloud for analysis.
4	Sky ATP has inspected this file before and has the analysis stored in cache. In this example, the file is not malware and the verdict is sent back to the SRX Series device.
5	Based on user-defined policies and because this file is not malware, the SRX Series device sends the file to the client.

Juniper Networks Sky Advanced Threat Prevention.pdf at page 4.

To the extent that Juniper does not literally infringe this claim element, at minimum, Juniper infringes under the doctrine of equivalents. The above described functionality of ATP is at most insubstantially different from the claimed functionality and performs substantially the same function in substantially the same way to achieve substantially the same result. ATP performs the same function because it receives files that are incoming to ATP and/or were intercepted as incoming to a protected system. As such, at minimum, ATP performs the same function as receiving an incoming Downloadable. ATP perform this function same way because they utilize software and hardware to receive these incoming Downloadables through a network or other transmission mechanism. As such, at minimum, ATP performs this function the same way as receiving an incoming Downloadable. ATP achieves the same result as this element because it receives a downloadable that it incoming to the ATP and/or to a protected system. As such, at minimum, ATP achieves the same result as receiving an incoming Downloadable.

10c. a Downloadable scanner coupled with said receiver, for

Sky ATP meets the recited claim language because it includes a Downloadable scanner coupled with said receiver, for deriving security profile data for the

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.