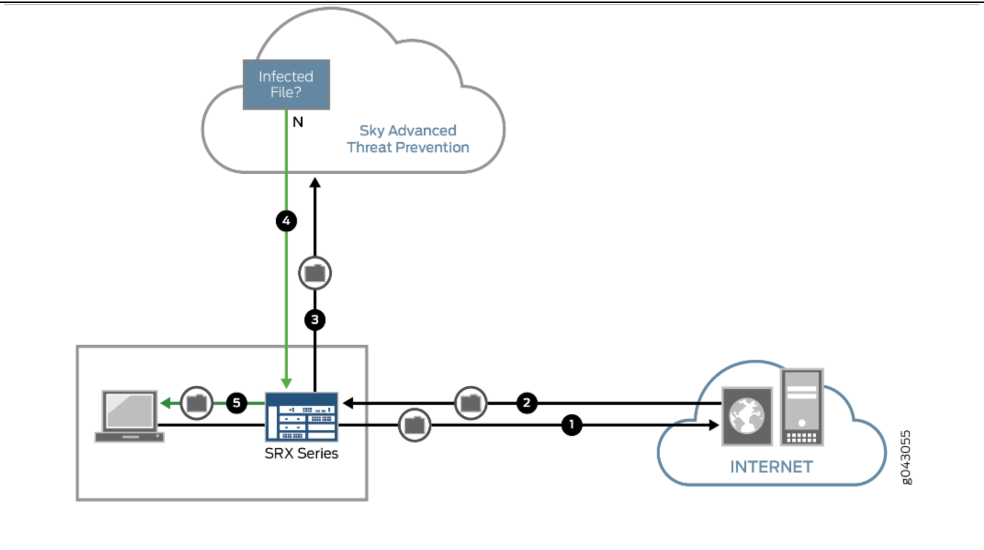
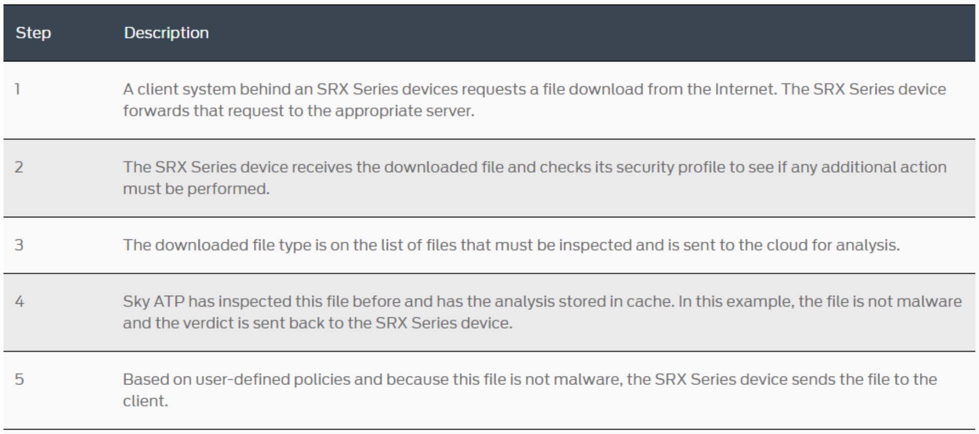
EXHIBIT 3

6,804,780	**Juniper's SRX Gateways**
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. 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] or the Advanced Threat Prevention Appliance ("ATP Appliance")[2] 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 Gateways specifically listed above infringe at least claims 1and 9 of the '780 Patent.	

Claim 1	
1a. A computer-based method for generating a Downloadable ID to identify a Downloadable, comprising:	SRX Gateways meet the recited claim language because it provides a computer-based method for generating a Downloadable ID to identify a Downloadable. 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 Gateways (either alone or in combination with Sky ATP or ATP Appliance) meet the recited claim language because SRX Gateways generates a Downloadable ID by creating malware attack profiles which include a hash to identify a Downloadable, such as malware. The analysis includes scanning the Downloadables which include references to software components required to be executed by the Downloadable (e.g., suspicious web page content containing HTML, PDFs, JavaScript, drive-by downloads, obfuscated code, or other blended web malware). SRX Gateways use the Downloadable ID to perform a hash lookup to Sky ATP or the ATP Appliance. Alternatively, SRX Gateways in combination with Sky ATP or ATP appliance meets the claim language because SRX generates a Downloadable ID and then uses Sky ATP or ATP appliance to generate a Downloadable ID for components of the Downloadable, and then generate a combined Downloadable ID for the Downloadable and the related components. As shown below, the SRX Series Services Gateway includes both hardware and software components that perform the step of receiving a Downloadable.

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

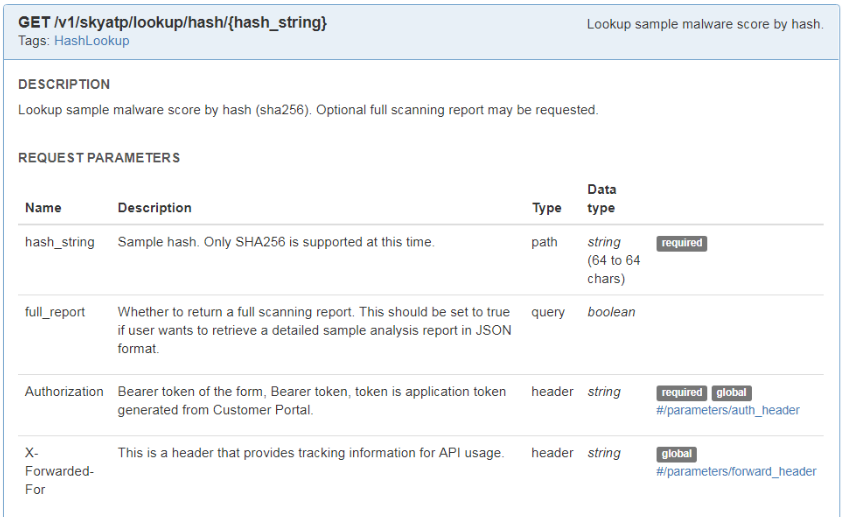




Step	Description
1	A client system behind an SRX Series devices requests a file download from the Internet. The SRX Series device forwards that request to the appropriate server.
2	The SRX Series device receives the downloaded file and checks its security profile to see if any additional action must 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.

SRX Gateways obtain a Downloadable then generates a Downloadable ID (e.g., a SHA-256 or a MD5 hash) to identify a Downloadable and send it to Sky ATP or ATP appliance to determine whether it is malicious and to return a risk score or verdict.

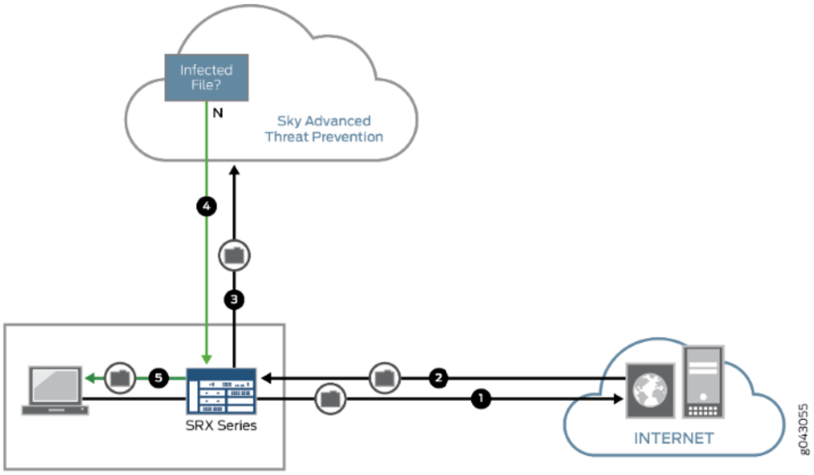
<table>
<tr>
<td></td>
<td>

<b>GET /v1/skyatp/lookup/hash/{hash_string}</b> Lookup sample malware score by hash.
Tags: HashLookup
<b>DESCRIPTION</b>
Lookup sample malware score by hash (sha256). Optional full scanning report may be requested.
<b>REQUEST PARAMETERS</b>
<table>
<tr><th>Name</th><th>Description</th><th>Type</th><th>Data type</th><th></th></tr>
<tr><td>hash_string</td><td>Sample hash. Only SHA256 is supported at this time.</td><td>path</td><td><i>string</i> (64 to 64 chars)</td><td>required</td></tr>
<tr><td>full_report</td><td>Whether to return a full scanning report. This should be set to true if user wants to retrieve a detailed sample analysis report in JSON format.</td><td>query</td><td><i>boolean</i></td><td></td></tr>
<tr><td>Authorization</td><td>Bearer token of the form, Bearer token, token is application token generated from Customer Portal.</td><td>header</td><td><i>string</i></td><td>required global
#/parameters/auth_header</td></tr>
<tr><td>X-Forwarded-For</td><td>This is a header that provides tracking information for API usage.</td><td>header</td><td><i>string</i></td><td>global
#/parameters/forward_header</td></tr>
</table>
https://www.juniper.net/documentation/en_US/release-independent/sky-atp/information-products/topic-collections/sky-atp-open-apis.html (showing a SHA-256 generated for the downloadable to indentify the downloadable).
</td>
</tr>
<tr>
<td>1b. obtaining a Downloadable that includes one or more references to software components required to be executed by the Downloadable;</td>
<td>SRX Gateways meets the recited claim language because it obtains a Downloadable that includes one or more references to software components required to be executed by the Downloadable.

SRX Gateways (either alone or in combination with Sky ATP or ATP Appliance) meets the recited claim language because SRX Gateways obtain suspicious traffic flows for analysis through a application program interface, and the content in these traffic flows include Downloadables such as web page and/or email attachments. These Downloadables include references to software components required to be executed by the Downloadable (e.g. suspicious web page content containing HTML, PDFs, JavaScript, drive-by downloads, obfuscated code, or other blended web malware).

Downloadables that includes one or more references to software components required to be executed by the Downloadable include a web page that includes references to JavaScript, visual basic script, ActiveX, injected iframes; and a PDF that includes references to JavaScript, swf files or other executables. Typically, Juniper characterizes them as drive-by-downloads or droppers as such Downloadables are usually programmed to take advantage of a browser, application, or OS that is out of date and has a security flaw. The initial downloaded code is often small enough that it wouldn’t be noticed, since its job is often simply to contact another computer where it can pull down the rest of the code on to the computer. In particular, such software components are usually programmed to be downloaded and run in the background in a manner that is invisible to the user and without the user taking any conscious actions as just the act of viewing a web-page that harbors this malicious code is typically enough for the download and execution to occur.

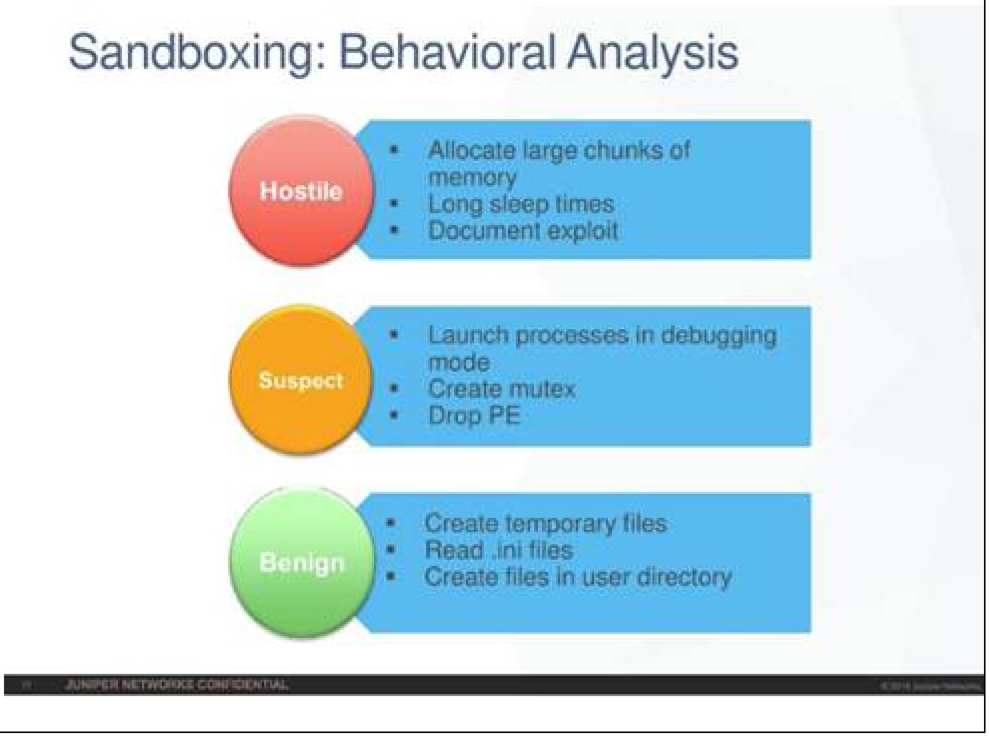
SRX Gateways obtain and scan Downloadables that may include malware embedded in images, JavaScript, text and Flash files. As shown below, SRX</td>
</tr>
</table>

Gateways obtain and conducts analysis on Downloadables such as Executable files (e.g., ".bin, .com, .dat, .exe, .msi, .msm, .mst"), PDF files, Java (e.g., ".class, .ear, .jar, .war"), MS Office file types, Flash and Silverlight applications, Script files, and installer files through an application program interface.



(showing SRX intercepting downloadables and sending them to Sky ATP) see also https://www.juniper.net/documentation/en_US/release-independent/sky-atp/topics/reference/general/sky-atp-profile-overview.html.

In infringement scenarios involving SRX Gatway with Sky ATP, Sky ATP performs behavioral analysis such as potential dropper infection for Downloadables. Potential dropper infections "Drop PE" (e.g., references to software components required to be executed by the Downloadable).



Sandboxing: Behavioral Analysis

Hostile
- Allocate large chunks of memory
- Long sleep times
- Document exploit

Suspect
- Launch processes in debugging mode
- Create mutex
- Drop PE

Benign
- Create temporary files
- Read .ini files
- Create files in user directory

JUNIPER NETWORKS CONFIDENTIAL

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.

WHAT WILL YOU BUILD? | sales@docketalarm.com | 1-866-77-FASTCASE

Smarter legal research.