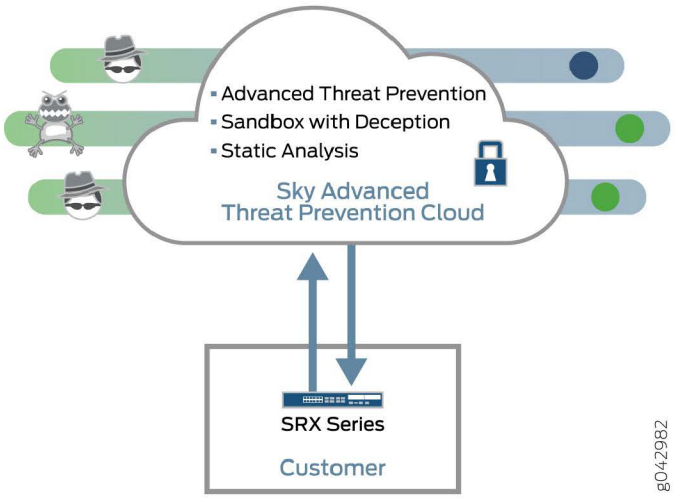
EXHIBIT 7

Juniper Networks Sky Advanced Threat Prevention

Juniper Networks Sky Advanced Threat Prevention (Sky ATP) is a security framework that protects all hosts in your network against evolving security threats by employing cloud-based threat detection software with a next-generation firewall system. See Figure 1.

Figure 1: Sky ATP Overview



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.

Sky ATP supports the following modes:

- Layer 3 mode
- Tap mode
- Transparent mode using MAC address. For more information, see Transparent mode on SRX Series devices.
- Secure wire mode (high-level transparent mode using the interface to directly passing traffic, not by MAC address.) For more information, see Understanding Secure Wire.

Sky ATP Features

Sky ATP is a cloud-based solution. Cloud environments are flexible and scalable, and a shared environment ensures that everyone benefits from new threat intelligence in near real-time. Your sensitive data is secured even though it is in a cloud shared environment. Security analysts can update their defense when new attack techniques are discovered and distribute the threat intelligence with very little delay.

In addition, Sky ATP offers the following features:

- Integrated with the SRX Series device to simplify deployment and enhance the anti-threat capabilities of the firewall.
- Delivers protection against “zero-day” threats using a combination of tools to provide robust coverage against sophisticated, evasive threats.
- Checks inbound and outbc quarantine infected systems,

- High availability to provide uninterrupted service.
- Scalable to handle increasing loads that require more computing resources, increased network bandwidth to receive more customer submissions, and a large storage for malware.
- Provides deep inspection, actionable reporting, and inline malware blocking.
- APIs for C&C feeds, whitelist and blacklist operations, and file submission. See the Threat Intelligence Open API Setup Guide for more information.

Figure 2 lists the Sky ATP components.

Figure 2: Sky ATP Components

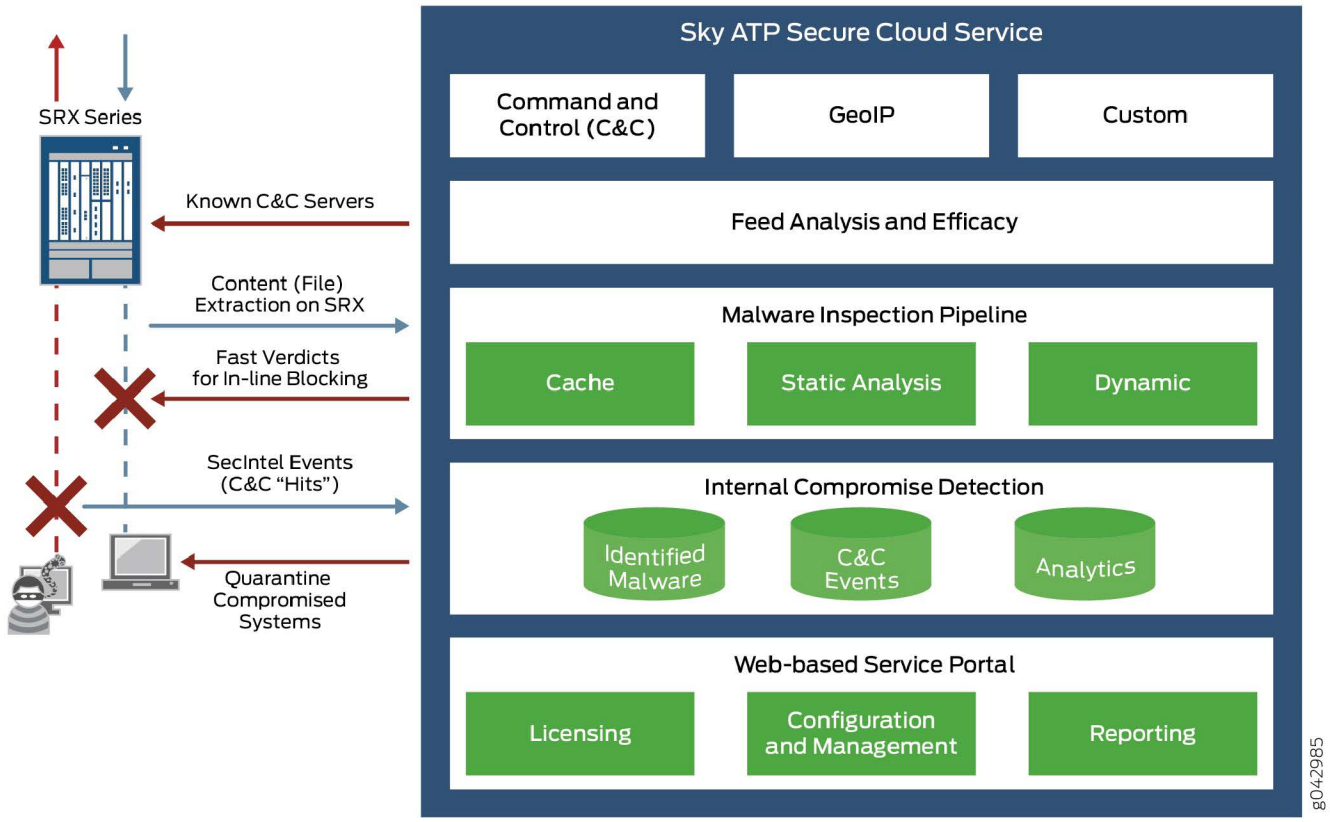


Table 1 briefly describes each Sky ATP component's operation.

Table 1: Sky ATP Components

Component	Operation
Command and control (C&C) cloud feeds	C&C feeds are essentially a list of servers that are known command and control for botnets. The list also includes servers that are known sources for malware downloads.
GeoIP cloud feeds	GeoIP feeds is an up-to-date mapping of IP addresses to geographical regions. This gives you the ability to filter traffic to and from specific geographies in the world.
Infected host cloud feeds	Infected hosts indicate local devices that are potentially compromised because they appear to be part of a C&C network or other exhibit other symptoms.

Component	Operation
Whitelists, blacklists and custom cloud feeds	A whitelist is simply a list of known IP addresses that you trust and a blacklist is a list that you do not trust. **Note:** Custom feeds are not supported in this release.
SRX Series device	Submits extracted file content for analysis and detected C&C hits inside the customer network. Performs inline blocking based on verdicts from the analysis cluster.
Malware inspection pipeline	Performs malware analysis and threat detection.
Internal compromise detection	Inspects files, metadata, and other information.
Service portal (Web UI)	Graphics interface displaying information about detected threats inside the customer network. Configuration management tool where customers can fine-tune which file categories can be submitted into the cloud for processing.

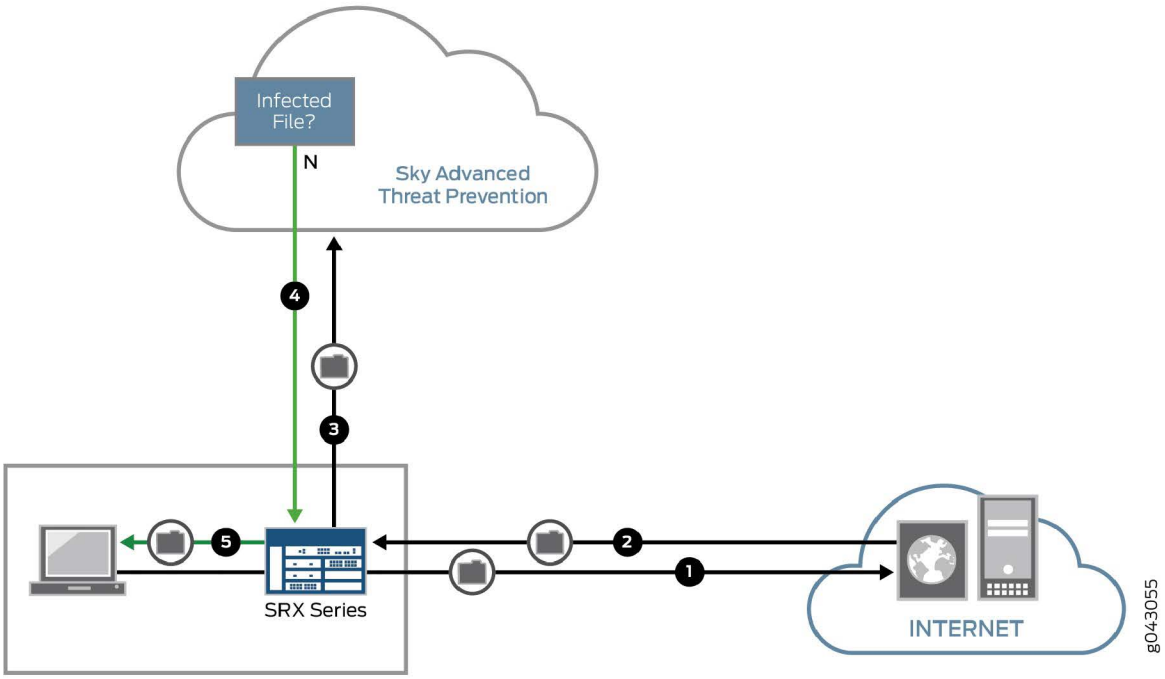
How the SRX Series Device Remediates Traffic

The SRX Series devices use intelligence provided by Sky ATP to remediate malicious content through the use of security policies. If configured, security policies block that content before it is delivered to the destination address.

For inbound traffic, security policies on the SRX Series device look for specific types of files, like .exe files, to inspect. When one is encountered, the security policy sends the file to the Sky ATP cloud for inspection. The SRX Series device holds the last few KB of the file from the destination client while Sky ATP checks if this file has already been analyzed. If so, a verdict is returned and the file is either sent to the client or blocked depending on the file's threat level and the user-defined policy in place. If the cloud has not inspected this file before, the file is sent to the client while Sky ATP performs an exhaustive analysis. If the file's threat level indicates malware (and depending on the user-defined configurations) the client system is marked as an infected host and blocked from outbound traffic. For more information, see How is Malware Analyzed and Detected?.

Figure 3 shows an example flow of a client requesting a file download with Sky ATP.

Figure 3: Inspecting Inbound Files for Malware



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.

For outbound traffic, the SRX Series device monitors traffic that matches C&C feeds it receives, blocks these C&C requests, and reports them to Sky ATP. A list of infected hosts is available so that the SRX Series device can block inbound and outbound traffic.

Sky ATP Use Cases

Sky ATP can be used anywhere in an SRX Series deployment. See Figure 4.

Figure 4: Sky ATP Use Cases