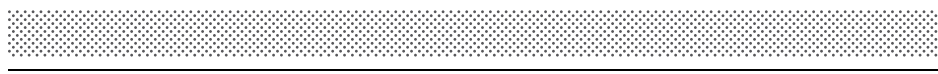


EXHIBIT 9



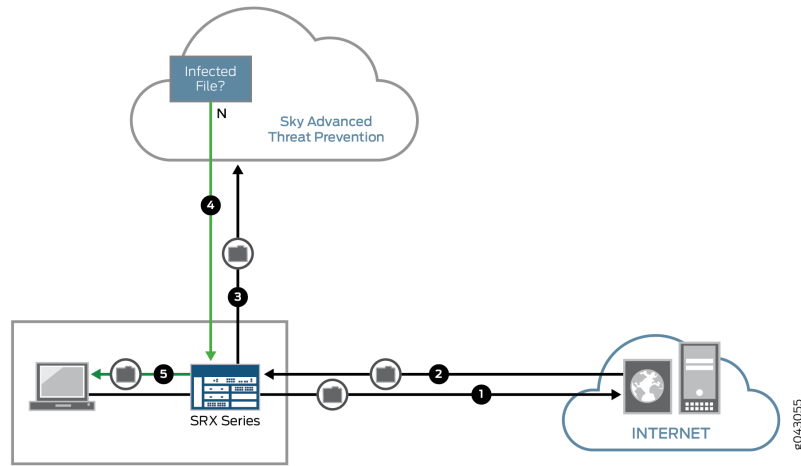
Sky ATP

Sky Advanced Threat Prevention Administration Guide



Modified: 2017-12-21

Figure 3: Inspecting Inbound Files for Malware



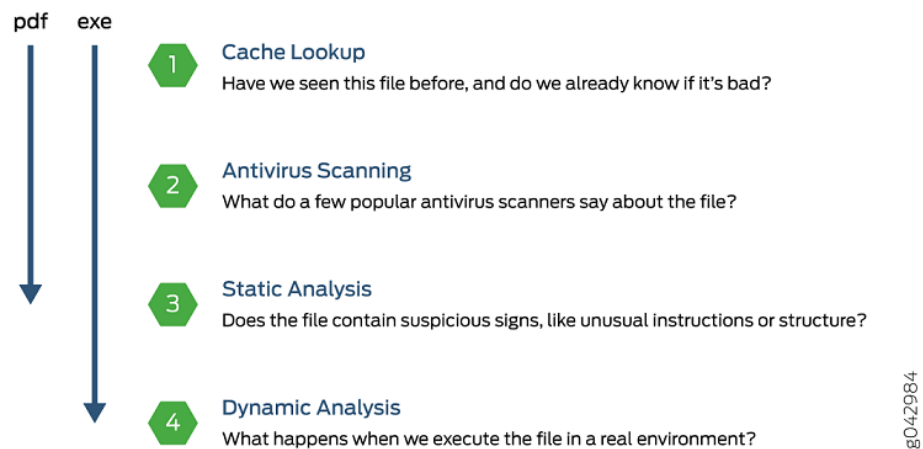
Step	Description
1	A client system behind an SRX Series devices requests a file download from the Internet. The SRX Series device forwards that request to the appropriate server.
2	The SRX Series device receives the downloaded file and checks its security profile to see if any additional action must 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 on page 8](#).

Figure 5: Example Sky ATP Pipeline Approach for Analyzing Malware



Each analysis technique creates a verdict number, which is combined to create a final verdict number between 1 and 10. A verdict number is a score or threat level. The higher the number, the higher the malware threat. The SRX Series device compares this verdict number to the policy settings and either permits or denies the session. If the session is denied, a reset packet is sent to the client and the packets are dropped from the server.

Cache Lookup

When a file is analyzed, a file hash is generated, and the results of the analysis are stored in a database. When a file is uploaded to the Sky ATP cloud, the first step is to check whether this file has been looked at before. If it has, the stored verdict is returned to the SRX Series device and there is no need to re-analyze the file. In addition to files scanned by Sky ATP, information about common malware files is also stored to provide faster response.

Cache lookup is performed in real time. All other techniques are done offline. This means that if the cache lookup does not return a verdict, the file is sent to the client system while the Sky ATP cloud continues to examine the file using the remaining pipeline techniques. If a later analysis returns a malware verdict, then the file and host are flagged.

Antivirus Scan

The advantage of antivirus software is its protection against a large number of potential threats, such as viruses, trojans, worms, spyware, and rootkits. The disadvantage of antivirus software is that it is always behind the malware. The virus comes first and the patch to the virus comes second. Antivirus is better at defending familiar threats and known malware than zero-day threats.

Sky ATP utilizes multiple antivirus software packages, not just one, to analyze a file. The results are then fed into the machine learning algorithm to overcome false positives and false negatives.

samples and thousands of goodware samples. It learns what malware looks like, and is regularly re-programmed to get smarter as threats evolve.

Threat Levels

Sky ATP assigns a number between 0-10 to indicate the threat level of files scanned for malware and the threat level for infected hosts. See [Table 4 on page 11](#).

Table 4: Threat Level Definitions

Threat Level	Definition
0	Clean; no action is required.
1 - 3	Low threat level.
4 - 6	Medium threat level.
7 - 10	High threat level.

For more information on threat levels, see the Sky ATP Web UI online help.

Related Documentation

- [Juniper Networks Sky Advanced Threat Prevention on page 3](#)
- [Dashboard Overview on page 36](#)
- [Sky Advanced Threat Prevention License Types on page 11](#)

Sky Advanced Threat Prevention License Types

Sky ATP has three service levels:

- **Free**—The free model solution is available on all supported SRX Series devices (see the [Supported Platforms Guide](#)) and for customers that have a valid support contract, but only scans executable file types (see *Sky Advanced Threat Prevention Profile Overview*). Based on this result, the SRX Series device can allow the traffic or perform inline blocking.
- **Basic**—Includes executable file scanning and adds filtering using the following threat feed types: Command and Control, GeoIP, Custom Filtering, and Threat Intel feeds. Threat Intel feeds use APIs that allow you to injects feeds into Sky ATP.
- **Premium**—Includes all features provided in the Free and Basic licenses, but provides deeper analysis. All supported file types are scanned and examined using several analysis techniques to give better coverage. Full reporting provides details about the threats found on your network.



NOTE: You do not need to download any additional software to run Sky ATP.

[Table 5 on page 12](#) shows a comparison between the free model and the premium model.