EXHIBIT G

JUNIPER NETWORKS

Sky Advanced Threat Prevention Administration Guide

Modified: 2017-09-08

Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

Sky Advanced Threat Prevention Administration Guide

The information in this document is current as of the date on the title page.

YEAR 2000 NOTICE

Juniper Networks hardware and software products are Year 2000 compliant. Junos OS has no known time-related limitations through the year 2038. However, the NTP application is known to have some difficulty in the year 2036.

END USER LICENSE AGREEMENT

The Juniper Networks product that is the subject of this technical documentation consists of (or is intended for use with) Juniper Networks software. Use of such software is subject to the terms and conditions of the End User License Agreement ("EULA") posted at http://www.juniper.net/support/eula/. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

CHAPTER 8

Scanning Email Attachments

Email Management Overview

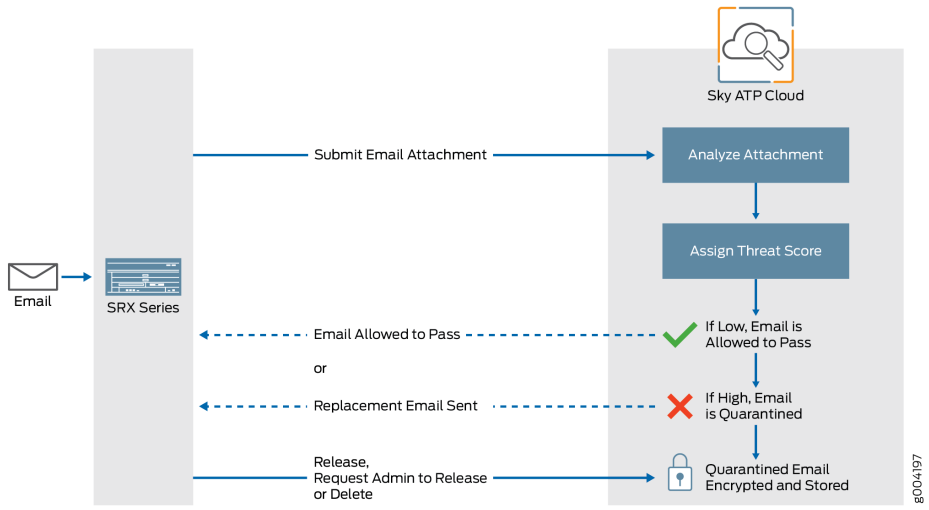
With Email Management, enrolled SRX devices transparently submit potentially malicious email attachments to the cloud for inspection. Once an attachment is evaluated, Sky ATP assigns the file a threat score between 0-10 with 10 being the most malicious.

NOTE: If an email contains no attachments, it is allowed to pass without any analysis.

Configure Sky ATP to take one of the following actions when an email attachment is determined to be malicious:

- Quarantine Malicious Messages—If you select to quarantine emails with attachments found to be malicious, those emails are stored in the cloud in an encrypted form and a replacement email is sent to the intended recipient. That replacement email informs the recipient of the quarantined message and provides a link to the Sky ATP quarantine portal where the email can be previewed. The recipient can then choose to release the email by clicking a Release button (or request that the administrator release it) or Delete the email.
- Deliver malicious messages with warning headers added—When you select this option, headers are added to emails that most mail servers recognize and filter into Spam or Junk folders.
- Permit—You can select to permit the email and the recipient receives it intact.

Figure 18: Email Management Overview



Quarantine Release

If the recipient selects to release a quarantined email, it is allowed to pass through the SRX series with a header message that prevents it from being quarantined again, but the attachments are placed in a password-protected ZIP file. The password required to open the ZIP file is also included as a separate attachment. The administrator is notified when the recipient takes an action on the email (either to release or delete it).

If you configure Sky ATP to have the recipient send a request to the administrator to release the email, the recipient previews the email in the Sky ATP quarantine portal and can select to Delete the email or Request to Release. The recipient receives a message when the administrator takes action (either to release or delete the email.)

Blacklist and Whitelist

Emails are checked against administrator-configured blacklists and whitelists using information such as Envelope From (MAIL FROM), Envelope To (RCPT TO), Body Sender, Body Receiver. If an email matches the whitelist, that email is allowed through without any scanning. If an email matches the blacklist, it is considered to be malicious and is handled the same way as an email with a malicious attachment.

Related Documentation

- Email Management: Configure SMTP on page 52
- Email Management: Configure Blacklists and Whitelists on page 55
- SMTP Quarantine Overview on page 55

Email Management: Configure SMTP

Access this page from **Configure** > **Email Management** > **SMTP**.

- Read the "Email Management Overview" on page 51 topic.