Modifications to Configuration Based on Updates

Professional Services – Security Management Framework

16 April 2019

Prepared by: *Gerardo Lastra*

Contact Information

Corporate Headquarters:

Palo Alto Networks
3000 Tannery Way
Santa Clara, CA 95054

About This Document

The Operational Enablement documents are designed to enable and inform customers on how to manage Palo Alto Networks technologies in a consistent and efficient manner. These documents assume that the reader is already familiar with Palo Alto Networks technology and they are meant to serve as sections within a runbook on how to manage the platform once deployed.

These documents do not replace other technical documentation published by Palo Alto Networks on their products and features. For more information about anything referenced in this document, see the technical documentation found at:
https://www.paloaltonetworks.com/documentation

Table of Contents

Modifying Configuration Based on Application Updates

Notifications for updated content

Palo Alto Networks releases new App-IDs on every third Tuesday of the month. As a way of letting our customers know well in advance what new App-IDs are being released, the list is published here. We highly encourage customers to look at this link and understand what new applications are being released, and if they would like to use these in their policy, to safely enable them. In addition, it's recommended to subscribe to the webpage in order to receive an email every time a new article is published.

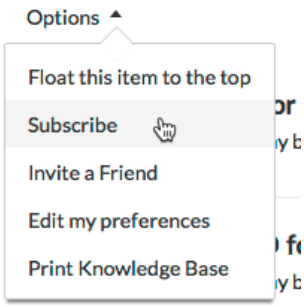

Figure 1 Subscribe option in the Customer Resources webpage

To receive an email every time our content is updated , visit the Customer Support Portal, edit your **Preferences**, and select **Subscribe to Content Update Emails**.

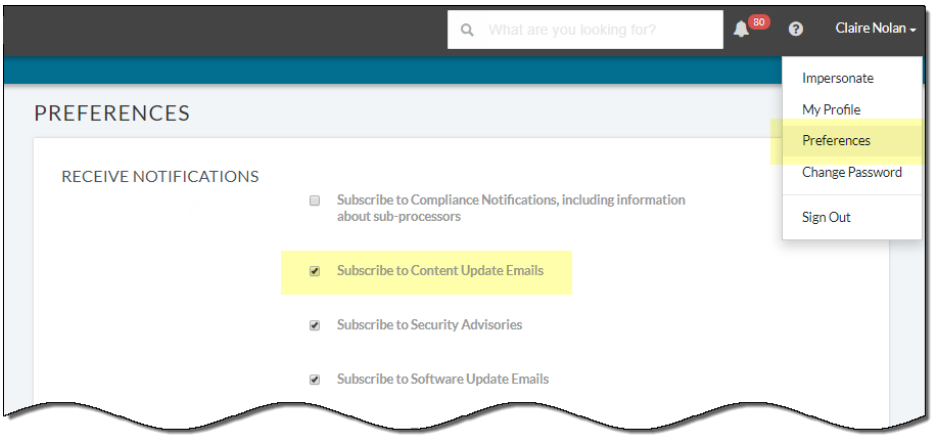

Figure 2 Subscribe option in the customer support portal

Update Security Policies Based on New or Modified Applications

Once a new application content is released, you'll need to download it to review the new and modified applications and to analyze your rulebase based on those changes. To download the latest update, go to **Device** > **Dynamic Updates** and **Download** the latest content release version.

For both downloaded and installed content updates, you can see a list of the new and modified App-IDs the update includes. Full application details are provided, and importantly, updates to applications with network-wide impact (for example, LDAP or IKE) are prominently flagged as a recommended for policy review. For modified App-IDs, application details also describe how coverage is either now expanded or more precise. The new applications need to be analyzed with the application owners to determine if any of their applications depend on them.

https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/app-id/manage-new-app-ids-introduced-in-content-releases/review-new-app-ids-since-last-content-version

Once the new applications have been reviewed you can analyze your security policies and add or remove new and modified App-IDs from the contextual menu as described in the Palo Alto Networks documentation. Performing a content update policy review before installing the new App-IDs will allow you to introduce new applications without any impact to production.
https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/app-id/manage-new-app-ids-introduced-in-content-releases/review-new-app-id-impact-on-existing-policy-rules.html#

After the policies have been modified you can install the latest version by selecting **Device** > **Dynamic Updates** and install the latest content release version.

Since new App-IDs are typically released the third Tuesday of the month, it's recommended to have a process in place to:

- Analyze the new applications. This can be done one week before (second Tuesday of the month) when the App-IDs are posted in the Customer Resources webpage.
- Modify any needed security policy based on the previous analysis.
- Install the new applications update.

Disabling and Enabling Applications

Disabling new applications needs to be used carefully as you'll need to log to every firewall to enable them once you're ready and thus this process is hard to scale.

You can disable applications in two different ways.

1. You can automatically disable new applications for every new scheduled update. On the **Device** > **Dynamic Updates** page, select **Schedule**. Choose to **Disable new apps** in content update for downloads and installations of content releases.
2. Disable one or multiple applications. **Objects** > **Applications**. Select one or more application check box and click **Disable**.

As mentioned before, to enable applications log into every firewall where the application is disabled, select **Objects** > **Applications**. Select one or more application check box and click **Enable** or open the details for a specific application and click **Enable App-ID**.

Modifying Configuration Based on Software Updates

On every major software update there are changes to the default behavior. Before upgrading to any major version, it is recommended to read the release notes to verify the changes to the default behavior and analyze if they'll require any change in the firewall settings or policies.

Examples

Changes to application-default behavior in PAN-OS 7.1 caused a review of rules with application *any* and service *application-default*.

Changes to the default authentication method for RADIUS in PAN-OS 7.1 caused some users to set it according to what the server was expecting.

Changes to the default behavior in PAN-OS versions can be found using the following links:

- PAN-OS 7.1
- PAN-OS 8.0
- PAN-OS 8.1
- PAN-OS 9.0

Document Properties

Contributors

Name	Role	Title	Contact Information
Gerardo Lastra	Consultant	Professional Services Engineer	glastra@paloaltonetworks.com

Revision History

Date	Revision	Changes By	Status	Comments
16 April 2019	1.0	Gerardo Lastra	Draft	