Silver Peak

Zone-Based Firewall Configuration Guide

Updated on August 07, 2020

Contents

Copyright and Trademarks

Silver Peak Zone-Based Firewall Configuration Guide

Date: August 07, 2020

Trademark Notification

Warranties and Disclaimers

Silver Peak Systems, Inc.
2860 De La Cruz Boulevard
Santa Clara, CA 95050

1.877.210.7325 (toll-free in USA)
+1.408.935.1850

http://www.silver-peak.com/support

Support

For product and technical support, contact Silver Peak Systems at either of the following:

1.877.210.7325 (toll-free in USA)
+1.408.935.1850
www.silver-peak.com/support

We're dedicated to continually improving the usability of our products and documentation.

- If you have suggestions or feedback for our documentation, send an e-mail to techpubs@silver-peak.com.
- If you have comments or feedback about the interface, send an e-mail to usability@silver-peak.com.

Related Documentation

- **Release Notes** provide information on new software features, system bugs, and software compatibility.
- All user documentation is available at https://www.silver-peak.com/support/user-documentation.

Zone-Based Firewall Description

Zone-Based Firewall Introduction

Version 9.0 enhances Zone Based Firewall (ZBF) feature to simplify configuration of end-to-end security policies across the SD-WAN fabric. The new firewall zoning behavior is optional and activated from the **Firewall Zone Security Polices** page (***Configuration > Overlays & Security > Security > Firewall Zone Security Policies***).

Changes to Firewall Zoning

Previous to Version 9.0, end-to-end zone security required the configuration of intra-zone and inter-zone Firewall Zone Security Policies through BIO zones where a zone spans across the SD-WAN fabric. For instance, sender on site Zone 1> BIO-X zone policy requires that traffic is permitted to enter the SD-WAN fabric, while the receiver side must require BIO-X zone > Zone 2 policy to exit the fabric and be permitted in the Zone 2. This is how Zone 1-> Zone 2 desired security posture is achieved.

Enabling Version 9.0 New Firewall Zoning results in the following:

- The zone configuration on BIO page is not available: BIO zones configuration is not required
- Firewall Zone Security policies consist of zones associated with only LAN or WAN interfaces.
- Using only LAN and WAN interface zones to configure Zone 1-> Zone 2 Firewall Zone Security policy achieves the desired outcome.
- SD-WAN fabric routes and packet header carry necessary zone information to enforce the security policies across the SD-WAN fabric.

Enhanced Zone-Based Firewall Prerequisites

Enhanced Zone-Based Firewall requires Version 9.0 on Orchestrator and all EdgeConnect appliances.

- When Orchestrator is upgraded to 9.0 version, **New Firewall Zoning** is disabled.
  Users can enable features as required, as instructed in this guide and on configuration screens.
- For New Orchestrator installations, **New Firewall Zoning** is enabled by default.

Mixed Versions Environment

When any EdgeConnect appliance uses a software version older than Version 9.0, Orchestrator prevents then enabling of the Enhanced Zone-Based Firewall and displays a message to upgrade all appliances.

Upgrade from 8.3/8.2/8.1.9/8.1.7 to 9.0

Because enhanced Firewall zoning is initially disabled, behavior does not change after upgrade. Users can continue using the existing firewall zone security configuration and templates without making changes.

Implementing Zone-Based Firewalls

The following sections describe Version 9.0 scenarios for using Enhanced Zone-Based Firewall scenarios.

Using Legacy Zone-Based Firewall

After upgrading to Version 9.0, Enhanced Zone-Based Firewall (ZBF) and Segmentation remains disabled until it is explicitly enabled or until Routing Segmentation is enabled. When Enhanced Firewall is disabled, Firewall behavior remains unchanged from previous versions.

Migrating to Enhanced Firewall Zoning

Enhanced ZBF security policies differ from legacy security policies. It is highly encouraged to migrate existing policies before enabling enhanced ZBF. When the enhanced behavior is enabled, zone configuration is removed from the BIO page because it is not applicable to the new behavior and enhanced policies reflect this change.

IMPORTANT It is recommended to perform this operation during the service maintenance window. Switching back and forth between the old and new behaviors should be avoided.

IMPORTANT Do not enable Segmentation or Firewall Zoning until before performing these steps:

The following steps migrate security policies to the new firewall zone behavior.

1. Review existing security policies (***Configuration > Overlays & Security > Security > Firewall Zone Security Policies***).
2. Create a Security template group (***Configuration > Templates & Policies > Templates***).
3. Copy the desired security policies from an existing template to the new Security group.
   Use the ***Save As*** option at the bottom of the Templates page to copy and paste the policies.
4. Delete all rules in the old security policy template, using the ***REPLACE*** option.
5. Save changes to the old security policy template.
   Saving changes in Orchestrator deletes all security policy rules on appliances associated to the security policy template.
6. Disassociate old security templates (***Configuration > Templates and Policies > Apply Template Group***).
7. Apply new security policy templates (***Configuration > Templates and Policies > Apply Template Group***).

8. Enable ***New firewall zoning***.

   Enhanced Zone-Based Firewall is enabled from the Firewall Zone Policies page.

The **Apply Template Group** page includes a copy-paste tool that copies policies cell by cell, pastes content into the cells. Modify as necessary and use ***Save as*** to place them in a new template group.

Enabling Zone-Based Firewall With segmentation

Enabling Routing Segmentation also enables enhanced Zone-Based Firewall. When Segmentation is enabled, Firewall Zone Security Policies do not require Firewall Zone Security templates. Security policies are configured from ***Configuration > Routing Segmentation > Firewall Zone Policies***.

No existing Firewall Zone policies

When there are no Firewall Security policies after the Version 9.0 upgrade, no additional action is required before enabling Enhanced Zone-Based Firewalls. Firewall zone policies created from ***Configuration > Routing Segmentation > Firewall Zone Policies*** after the upgrade implement the enhanced behavior.

Existing Firewall Zone policies

To enable segmentation with existing firewall zone policies, create new firewall zone security policies as described in Using Legacy Zone-Based Firewall. Failure to do so before enabling segmentation results the applying of all existing firewall zone policies to Default segment. Using legacy security policies with Enhanced Zone Based Firewall may lead to unpredictable behavior.

The following steps are recommended to migrate from old to new security zone policies to support segmentation:

1. Use the steps described in Using Legacy Zone-Based Firewall to delete the old Firewall Zone Security policies.

   Do not create new Firewall Zone policies (yet).
2. Enable Segmentation
3. Configure new security policies (***Configuration > Routing Segmentation > Firewall Zone Policies***).

Although highly discouraged, It is possible to use the Firewall Zone Security template with segmentation enabled. If used, the template group is applied to the “Default” segment. We recommended that all Firewall Zone Security policies are maintained in one place and configured from the Routing Segmentation menu.