Silver Peak

Advanced Segmentation Configuration Guide

Updated on August 07, 2020

Contents

Copyright and Trademarks

Silver Peak Advanced Segmentation 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.

Routing Segmentation Description

Segmentation Overview

Routing Segmentation (VRF) supports multiple routing tables instances – referred to as ***routing segments***, in a single appliance. Segments do not share data routes – data packets are only forwarded between interfaces within the same segment. Because routing segments are independent, overlapping IP address spaces can be used by multiple segments without conflicting.

In a typical deployment, segmentation is implemented on the provider edge (PE) while customer edge routers (CE) manage local routing. PE routers encapsulate traffic it receives from CE routers, marks it for transmission across a specific segment, and sends it across a provider backbone network. The destination PE router decapsulates the traffic and forwards it to the destination CE router. The backbone network separates end-to-end traffic customer traffic while remaining transparent to CE routers.

MGMT0 interface

When Routing Segmentation is enabled, the MGMT0 interface is not a member of any segment and there is no segment configuration for MGMT0. MGMT 0 is not accessible from any segment, including the default segment.

The MGMT0 interface can connect externally to a network on the LAN interface. In this case, the MGMT0 interface logically resides in the segment associated with the LAN interface.

When Segmentation is disabled, the behavior of the MGMT0 interface is similar to that of the interface in previous non-segmentation releases.

Silver Peak Segmentation Capacity

Silver Peak routing segmentation provide the following:

- 2000 segments that are centrally orchestrated
- 6000 Firewall zones
- 64 segments on each individual EdgeConnect appliance
- 30K IPv4 routes across SD-WAN fabric
- 30K IPv6 routes across all segments. No limit for each individual segment.
- Overlapping IP addresses in the segments
- Intra-segment traffic that supports routing isolation
- Inter-segment traffic configured through policy rules
- Source and destination network address translation (S-NAT, D-NAT)
- Per-segment site to site and local breakout policies using Business Intent Overlay (BIO) mapping
- Per-segment dynamic route learning with BGP protocol on LAN interfaces.
- Firewall zone policy configuration for intra-segment and inter-segment traffic.

Prerequisites to Routing Segmentation

Routing Segmentation is subject to the following SD-WAN fabric prerequisites:

- All EdgeConnect appliances and Unity Orchestrator must run version 9.0 or later.

  Orchestrator prevents enabling of Routing Segmentation if any appliance is not running a version that supports segmentation.

  Appliances introduced to the SD-WAN fabric (either through adding a new appliance or replacing an existing appliance) should be upgraded to a version that supports segmentation. When segmentation is enabled, the behavior of an appliance that is not running an appropriate version is unpredictable.

- All Firewall Zone Security policies must comply with enhanced Zone Based Firewall (ZBF) introduced in Version 9.0.

  Enhanced ZBF utilize security policies that include source and destination Routing Segments and specify inter-zonal traffic management for traffic traversing the specified segments. Previous versions specified zonal designations for traffic in the BIO definitions.

  Upgrading Firewall Zoning Policies describe the migration process for security policies to comply with enhanced ZBF.

Implementing Segmentation

This topic describes processes that enable Routing Segmentation and add a routing segment:

- Enable Routing Segmentation
- Add a Routing Segment

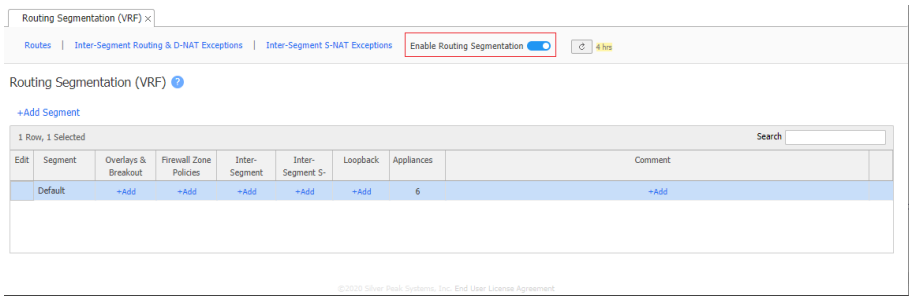
IMPORTANT When are upgrading a configuration that includes Zone-Based Firewall security policies, verify that the security policies are updated before enabling Routing Segmentation. Refer to Updating Security Policies for more information.

Enable Routing Segmentation

The following steps enable Routing Segmentation on the SD-WAN fabric.

1. Open Orchestrator, select the EC-Vs (Appliance menu), and open the **Routing Segmentation (VRF)** page (***Configuration > Networking > Routing > Routing Segmentation (VRF)***.
2. Slide-right the ***Enable Routing Segmentation*** button (Figure 1).

Figure 1. Enabling Routing Segmentation



When Segmentation is enabled, the page displays the default segment (which is named ***default***). The default segment becomes active when Segmentation is enabled and cannot be deleted.

Routing parameters existing when Segmentation is enabled are associated with the default segment, including:

- All interfaces
- Routes
- VRRP instances
- Firewall security zones and zone policies

Disabling Routing Segmentation

Disabling Routing Segmentation requires that all user-defined segments are previously deleted. The Default segment cannot be deleted.

Segmentation is disabled from the **Routing Segmentation** page by sliding the ***Routing Segmentation*** button left (Figure 1).

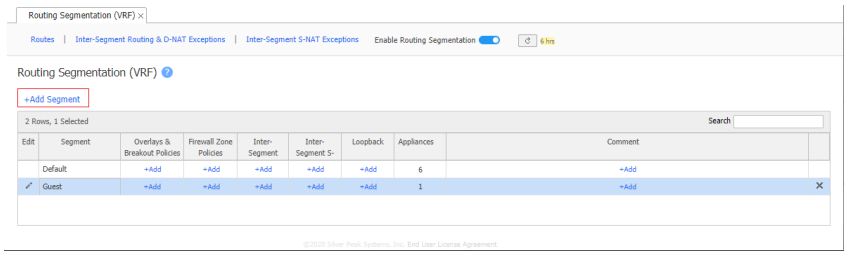
Add a Routing Segment

The following steps add a routing segment named "Guest" to the SD-WAN fabric.

1. Open Orchestrator, select the EC-Vs (Appliance menu), and open the **Routing Segmentation (VRF)** page (***Configuration > Networking > Routing > Routing Segmentation (VRF)***.
2. Click ***+Add Segment*** (Figure 1) to open the Add Routing Segment popup.
3. Enter ***Guest*** in the Segment Name field and click Save.

Figure 1 displays the new segment in the Routing Segmentation table.

Figure 2. Adding a Segment



Deleting a segment

Deleting a segment removes the segment and its configuration objects from all network appliances. These objects, which are configured from the Routing Segmentation table, include:

- The segment's overlay and break-out policy associations
- Intra-segment and inter-segment firewall zone policies
- Inter-segment routing and D-NAT rules
- Inter-segment S-NAT rules
- Loopback interfaces

These objects, located on other Orchestrator pages, are also removed:

- VTI interfaces
- All interface and VLAN associations.

All segmentation association with other configuration objects are also removed. Manual deletion of these objects may be required after the object association is removed. These objects include:

- Manually created tunnels (such as third party tunnels)
- BGP peers
- Internal subnet table rules
- Overlay ACL rules

To delete a segment, click the ***X*** in the right-most column for the segment being removed (Figure 1).

Configuring Segments

This topic describes Orchestrator processes of Configuring a Routing Segmentation:

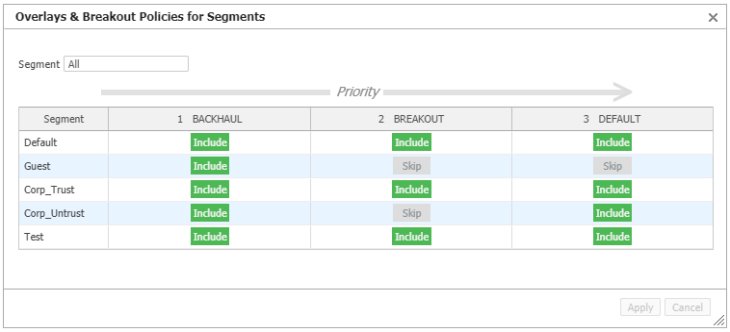
Applying Overlays and Breakout Policies

A Business Intent Overlay (BIO) is a set of policies that determine how overlay tunnels are constructed, which traffic is routed through which overlay, and how traffic that flows through each overlay uses underlay tunnel connections. The **Business Intent Overlay**s page (***Configuration > Overlays and Security > Business Intent Overlays***) displays configuration parameters of each BIO.

When Segmentation is not enabled, overlays are applied to an appliance through the **Apply Overlay** page (***Configuration > Overlays and Security > Apply Overlays***). When Segmentation is enabled, the Default segment is assigned the overlay specified for the appliance in this page.

The **Overlays and Breakout Policies for Segments** popup (Figure 1) displays and configures Overlay associations for each segment.

Figure 3. Overlays and Breakout Policies for Segments popup



The following steps configure the BIO assignment for Routing Segments.

1. Open Orchestrator, select the EC-Vs (Appliance menu), and open the **Routing Segmentation (VRF)** page (***Configuration > Networking > Routing > Routing Segmentation (VRF)***.
2. In the Segment table, click the hyper-text under the Overlays & Breakout Policies column (Figure 3) to open the **Overlays and Breakout Policies for Segments** popup.

   Each column corresponds to a BIO. Each row corresponds to a segment. Cell contents define the BIO association status for the specified segment.
3. Configure each Routing Segment by clicking cells in its corresponding row as follows:
   - **Associate a BIO to a segment**: Click the BIO cell until it displays a green ***Include*** text box.
   - **Dissociate a BIO from a segment**: Click the BIO cell until it displays a grey ***Skip*** text box.
4. Click ***Apply*** to save popup changes and return to the **Routing Segmentation** page.
   Click ***Cancel*** to discard popup changes and return to the **Routing Segmentation** page.

Configuring Firewall Zone Policies

Firewall Zone Policies manage traffic between zone-based firewalls. The **Securities Policies** page (***Configuration > Overlays & Security > Security > Firewall Zone Security Policies***) configure and display policies for selected appliances regardless of the Routing Segment enabled status.

Inter-segment routing policy requires a corresponding Firewall Zone policy. Scope of a zone is limited to a segment. Zones in two segments are distinct even if they share the same name: for example, “default” zone in Segment A and “default” zone in Segment B are different zones even though the zone label is identical.

In segment “A”, no Firewall Zone policy is required for traffic to flow between sites in the “default” zone. A Firewall Zone policy is required for traffic to flow in the “default” zone from segment A to segment B.

The **Segment (VRF) Firewall Zones Policies** popup displays and configures policies for each Segment. To access this popup from the Routing Segmentation page, click the hyper-text under the Firewall Zone Policies column.

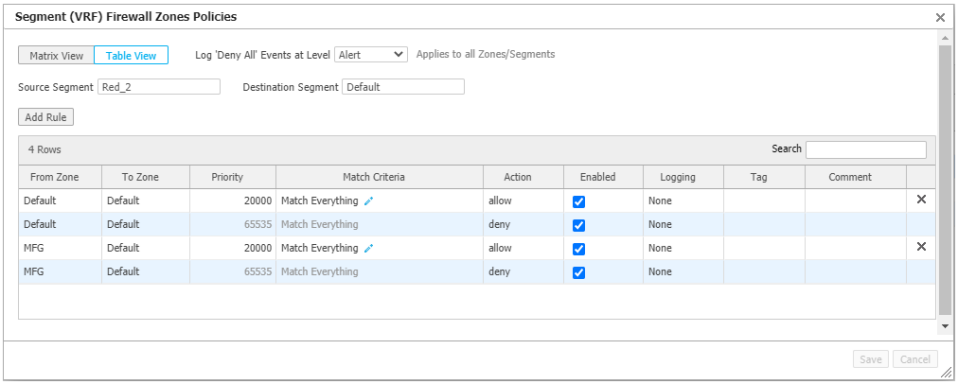
The popup provides two viewing options.

- Matrix view provides a visual representation of policies configured for all segments. The popup opens into the Matrix view (Figure 3).

Figure 4. Segment (VRF) Firewall Zones Policies popup – Matrix View

- Table view lists all policies for a specified Segment (Figure 3).

Figure 5. Segment (VRF) Firewall Zones Policies popup – Table View



  - Click on ***Table View*** (upper-left corner) to display policies for a specified segment.
  - Click on a *Matrix* cell to display the specified Segment policies for an individual zone.

You can add, remove, or modify polices from the popup Table View.

- Click ***Save*** in the bottom right corner to save all popup changes.
- Click ***Cancel*** to discard all popup changes.

To delete a segment, click the ***X*** in the right-most column for the policy being removed (Figure 3).

Configuring Inter-Segment Routing

A segment's traffic is isolated, by default, from traffic routed through all other segments. Inter-Segment Routing and D-NAT policies facilitate inter-segment routing, or routing across two segments. This is similar to route-leaking between VRFs in traditional router deployments.

EdgeConnect Inter-Segment routing is policy driven, as opposed to advertising routes between segments. If the destination subnet for traffic originating in a (source) segment matches an Inter-Segment Routing policy rule, traffic transfers to the destination segment at the source appliance. Route lookup and traffic forwarding over the SD-WAN fabric is in context of the destination segment.

The **Inter-Segment Routing and D-NAT Exceptions** page defines routes between segments. Routes between a source and destination segment is configured on the **Inter-Segment Routing & D-NAT Exceptions** popup.

- To access the **Inter-Segment Routing & D-NAT Exceptions** page, click ***Inter-Segment S-NAT Exceptions*** in the menu bar of the **Routing Segmentation (VRF)** page.
- To access the *popup* from the **Routing Segmentation** page, click the hyper-text under the **Inter-Segment Routing & D-NAT** column. You can also click an edit-column *icon* in the ***Inter-Segment Routing & D-NAT Exceptions*** page.

The popup provides two viewing options.

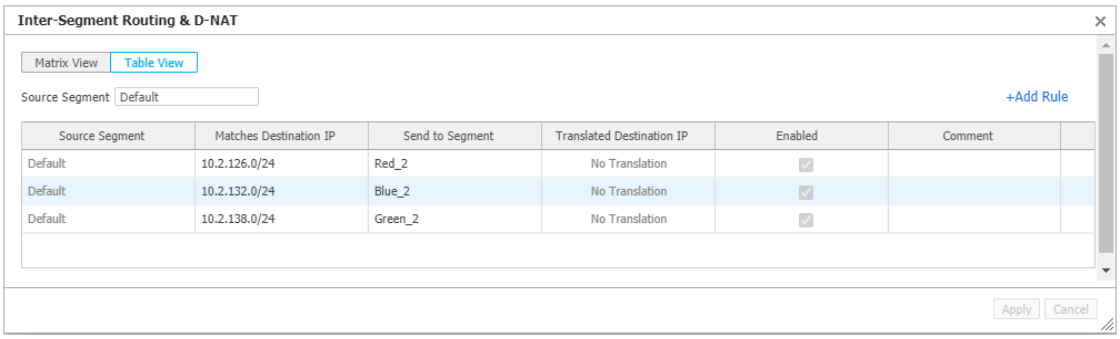
- ***Table view*** lists the IP address spaces that are routed to a destination segment. The popup opens in Table view for the selected Segment.

  Column parameter values include:

  - **Source Segment**: Segment where traffic originates.
  - **Matches Destination IP**: Address space to which destination address must match. Valid settings include a subnet (172.16.10.0/24) or a IP address range (172.16.10.200-255)
  - **Send to Segment**: Destination Segment for traffic that matches the rule.
  - **Translated Destination IP**: Destination IP subnet for 1:1 D-NAT. Should be used when source and destination segments IP addresses that overlap.

    Also used to increase security when destination IP space is not visible to source segment.
  - **Enabled**: Activity status of the rule.
  - **Comment**: User reference description text.

Figure 6. Inter-Segment Routing and D-NAT popup – Table View



- ***Matrix view*** provides a visual representation of all inter-segment route rules.

The following steps add a route between Routing Segments:

1. In the route's source segment row, click the hypertext in the ***Inter-Segment S-Net*** cell.
   The **Inter-Segment Routing and S-NAT** popup opens for the source segment.
2. Click ***+Add Rule*** (above table, right-side of popup)
   A new rule is added at the bottom of the table.
3. Enter translation parameters, including the following:
   - IP Address space to be routed,
   - Destination segment,
   - IP address translation,
   - Check Enabled to immediately activate the route.
4. Continue adding rules as required.
5. Click ***Save*** at the bottom of the popup to save the rules and close the popup.
   Click ***Cancel*** to discard the new rules and close the popup.

To delete a rule, click the ***X*** in the right-most column for the rule being removed.

Inter-Segment S-NAT

The **Inter-Segment S-NAT Exceptions** page lists all S-NAT between segments. The **Inter-Segment S-NAT popup displays and configures S-NAT** status between segments.

- To access the **Inter-Segment S-NAT Exceptions** page, click ***Inter-Segment S-NAT Exceptions*** in the menu bar of the **Routing Segmentation (VRF)** page. This page lists the routes defined between Segments.

- To access the *popup* from the **Routing Segmentation** page, click the hyper-text under the **Inter-Segment Routing and D-NAT** column. You can also click an edit-column icon in the **Inter-Segment Routing & D-NAT Exceptions** page.

The following steps modify the S-NAT state between routing segments:

1. In the row of the desired source segment, click the hypertext on the ***Inter-Segment S-Net*** cell.
   The **Inter-Segment S-NAT** popup opens for the source segment. The popup table contains rows for all other defined Route Segments, which configures the S-NAT On/Off state between Segments.
2. To modify the on-off state, click the text box in the S-NAT cell for the desired destination segment
3. Continue modifying segments as required.
4. Click ***Save*** at the bottom of the popup to save the changes and close the popup.
   Click ***Cancel*** to discard the new rules and close the popup.

Local Internet breakout from non-default segment

All the WAN links including Internet links are in the "default segment". Internet bound traffic originated from the non-default segment gets mapped to one of the Business Intent Overlay (BIO) included in the "Overlay and Breakout policies for the segment". The EdgeConnect treats this traffic as inter-segment traffic (non-default segment to Internet interfaces in the default segment). No inter-segment routing policy is required for local breakout traffic but for security reasons, security policies from non-default segment's source zone to default segment's appropriate destination zone must be configured.

By default, all WAN interfaces are in the default segment, default zone. WAN interface segments are not configurable and it's recommended to keep WAN interface zones in the "default" zone.

Applying a Loopback Interface

Loopback interfaces allow routing protocols to stay active as long as the segment is available even when the outbound interface is down. The Loopback interface from the default segment is used by all management applications when Segmentation is enabled.

Loopback interfaces are assigned to segments from the **Loopback Orchestration** page. To access the Loopback Orchestration page:

- Select ***Configuration > Networking > Loopback Orchestration*** from the main menu.
  This option opens the page for all segments. To display loopbacks and activate configuration options for a single segment, enter the segment's name in the **Segment** field. The drop-down auto-populates when the field is cleared.
- Open the **Routing Segmentation (VRF)** page and click the text in the ***Loopback*** cell for the desired segment.

To add a Loopback to a segment:

1. Open the **Loopback Orchestration** page for the desired segment.
2. Click ***+Add Loopback Interface*** (left-side of page above segment table).
   The **Loopback Interface – Segment** popup opens for the specified segment.
3. Select the desired **Label** and **Zone** (firewall) from the respective drop-down menus.
4. Click Add (bottom-right corner).
   The popup closes and the interface appears in the Loopback Orchestration table.

Deploying Segments

A segment is deployed by associating it to a LAN interface, then assigning a FW zone and an IP address to the interface. Segments can only be assigned to LAN interfaces in Router mode.

The following steps deploy a routing segment.

1. Open Orchestrator, select the EC-Vs (Appliance menu), and open the **Deployment** page (***Configuration*** > ***Networking*** > ***Deployment***.
2. Click an *edit* column icon for the appliance where the segment is to be deployed.

   The **Deployment** popup opens for the specified appliance.
3. Select a LAN interface.

   If necessary, add a VLAN branch to an existing interface by clicking ***+IP*** below a desired LAN interface.
4. Enter the following information for the new interface:
   - **VLAN**: For interfaces deploying multiple segments, enter a unique VLAN number (1-4094)
   - **FW Zone**: (drop-down) Select a Firewall Zone
   - **Segment**: (drop-down): Select the Routing Segment being configured.
   - **Label**: (drop-down) Select the data type.
   - **IP/Mask**: Enter an IPv4 address and mask in CIDR notation
   - **Next Hop**: (Optional) Enter an IPv4 address in the space listed under **IP/Mask**. Default is first available address in the specified IP/Mask address.
5. Configure WAN and Inbound / Outbound parameters as required.
   - While these parameters are not directly affected by Routing Segments, adjustments may be necessary, depending on your deployment.
6. Click ***Apply*** to save popup changes and return to the **Deployment** page.

   Click ***Cancel*** to discard popup changes and return to the **Deployment** page.

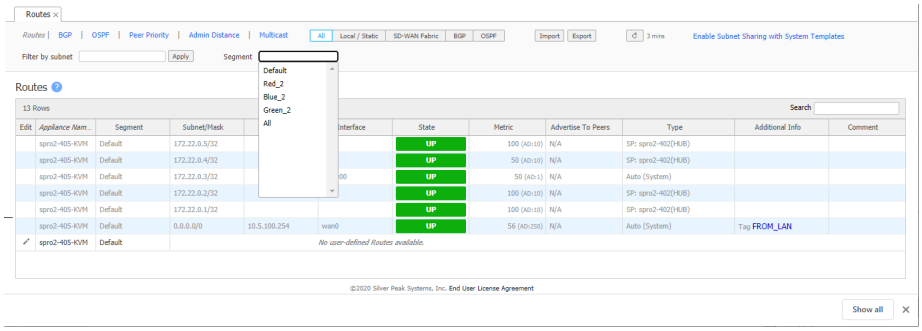
Segment Routes

The **Routes** page (Figure 7) displays all routes for the specified segments and is accessed by the following methods:

- Select ***Configuration > Routing > Routes*** from the main Orchestration menu.
- Select ***Routes*** from the top menu bar of the **Routing Segmentation (VRF)** page.

The **segment** field determines which routes are displayed. To change the segment name, clear field contents to auto-populate the drop-down menu. Select ***All*** to view all routes on selected appliances.

Figure 7. Routes Page

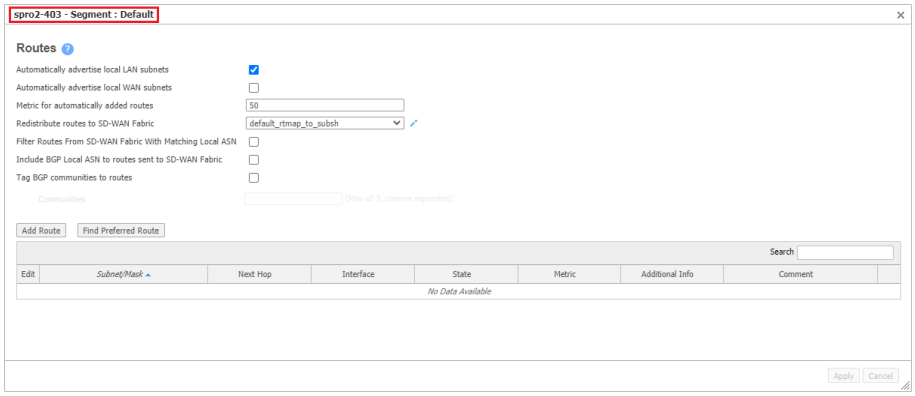


Configuring Route Parameters

Static Routes

Static routes can be defined and configured for each routing segment. To create a static route, open the **Routes** popup by clicking the *edit-column* icon for the ***appliance – source segment*** where the route will originate. The appliance and segment name appear in the title bar (Figure 7).

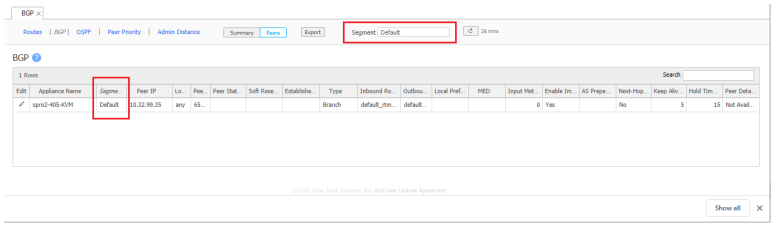
Figure 8. Routing Popup for the Default Segment



BGP Routes

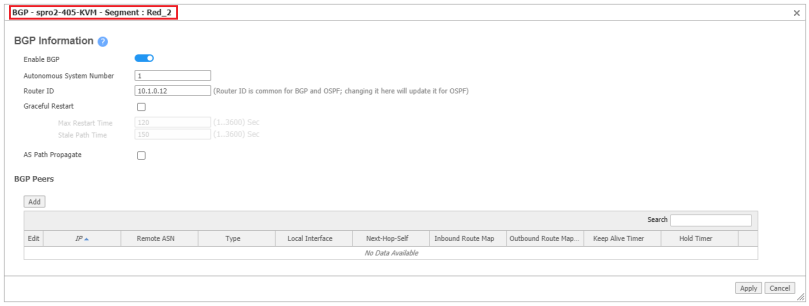
BGP can be enabled and peers added to each route segment. The **BGP** page (***Configuration > Routing > BGP***) includes a Segment field that filters BGP peers based on individual segments.

Figure 9. BGP Page



To enable BGP for a segment, open the **BGP** popup by clicking the *edit-column* icon for the desired ***appliance – source segment***. The appliance and segment name appear in the title bar

Figure 10. BGP Popup



OSPF Routes

OSPF is not configurable on a routing segment basis. OSPF configuration parameters apply to all routing segments.

Peer Priority

Peer Priority is not configurable on a routing segment basis. Peer Priority configuration parameters apply to all routing segments.

Admin Distance

Admin Distance (route preference value) is not configurable on a routing segment basis. Admin Distance configuration parameters apply to all routing segments.

Upgrading Firewall Zoning Policies

Version 9.0 introduces enhanced Zone Based Firewall (ZBF) that simplifies configuring end to end security policies across the SD-WAN fabric. Enhanced ZBF is mandatory for Routing Segmentation.

This topic describes the process of migrating polices for enhanced ZBF.

Updating Security Policies

No Existing Firewall Zone Policies

If an SD-WAN fabric does not include Firewall Zone policies when a network is upgraded to Version 9.0, no action is required. New policies created after an upgrade (***Configuration > Routing Segmentation > Firewall Zone Policies***) are compatible with enhanced ZBF.

Existing Firewall Zone Policies

Before enabling segmentation with existing firewall zone policies, create a new security template group and copy existing policies into the new group.

The following steps create and deploy the security policies:

IMPORTANT We recommend performing this process during a service maintenance window. Transmitting data when changing firewall behavior should be avoided.

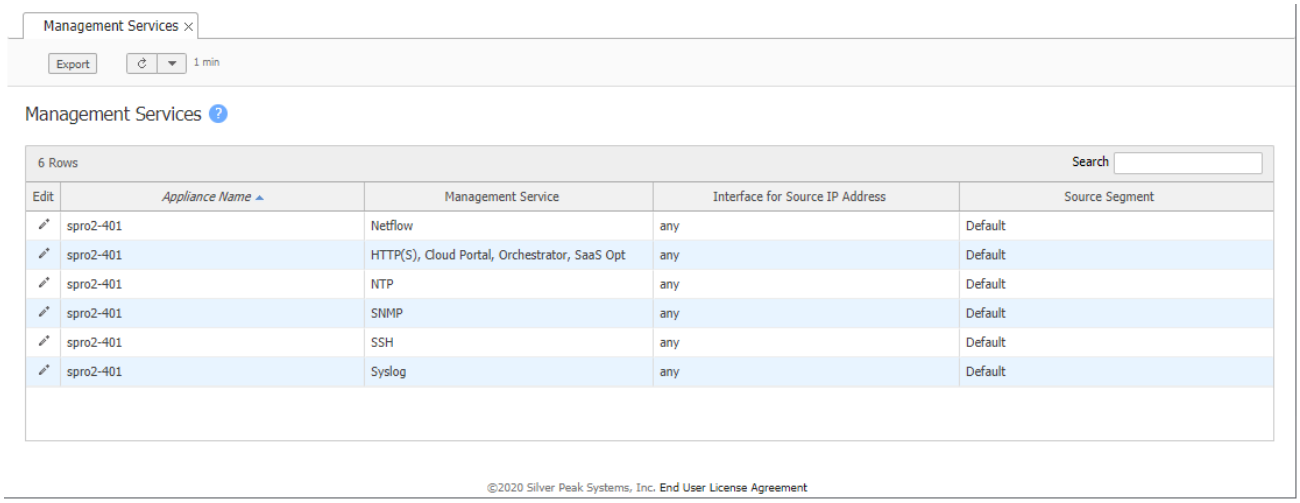
IMPORTANT Do not enable Segmentation or Firewall Zoning until before performing these steps:

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***.

Routing Segmentation and Management Services

Management services are a set of subsidiary protocols and applications that implement essential connectivity, monitoring, startup, and management tasks. Services supported include Netflow, HTTP (HTTPS), Cloud Portal, Orchestrator, SaaS Opt, NTP, SNMP, SSH, and Syslog. Management services egress packets coordinate processes between the appliances and the server providing the services. Orchestrator designates the IP address these packets through the **Management Services** page (***Configuration > Routing > Management Services***).

Figure 11. Management Services page



When route segmentation is enabled, the Management Services page includes a **Source Segment** column. The IP address used for egress packets is based on the interface assigned to the specified service – the source segment column indicates the segment that is assigned to the interface in the **Deployment** page. When ***any*** is assigned to a service, Orchestrator designates an interface and source IP address based on route lookup for the service. Assigning an interface to a service provides a defined IP address for the service.

The following sections describe Management Service behavior when routing segmentation is enabled.

Management Traffic Routing

Routing of the management services traffic and source IP address used in the egress packets depend upon user configuration as described in these sections:

- Routing Segmentation and Management Services
- Interface for Source IP Address – Loopback or Data Path Interface

Interface for Source IP Address – Any

When **Interface for Source IP Address** is set to ***any***, user has no control over the source IP address used for management services egress packets.

Depending upon route lookup, the corresponding source IP address configured in the **Management Routes** table is used as the packet's source IP address. If the Source IP address is not configured (or set to 0.0.0.0) in the **Management Routes** table for the selected route, the egress interface's IP address is used as the source IP address.

Previous versions supported the ***ip mgmt-ip <ip address>*** CLI command, which specified a static IP address for managements services. This CLI command is not available in Version 9.0.

Interface for Source IP Address – Loopback or Data Path Interface

Default Segment

The **Management Routes** table is associated with the default segment. When a Management Service source segment is set to ***default***, the route used for service traffic is determined as follows:

- The egress interface is the data path of the default segment in the default segment's table when 1) MGMT0 is down; or 2) the data path has a metric value less than the metric value of the MGMT0 interface.
- The egress interface is MGMT0 if it is up and it has a metric value greater than the metric value of the data path of the default segment that was in the default segment's route table.

User Defined Segments

When **Interface for source IP address** is set to a loopback interface or any data path interface (lo100, lan0, lan0:100), the egress interface is determined through a route look up in the associated segment's data path route table.

Because the **Management routes** table is associated with the ***default*** segment, it is never used for traffic of a user-defined segment.

Orchestrator and Cloud Portal Management

Public IP address discovery of NAT interfaces

When segmentation is enabled, public IP address discovery is performed through all interfaces regardless of segment association.

Cloud Portal connectivity – Cloud Portal DNS resolution

EdgeConnect attempts to resolve the Cloud Portal DNS address (cloudportal.silver-peak.com) from all interfaces.

Cloud Portal connectivity – Portal reachability & WebSocket connection

Cloud portal reachability test and WebSocket connection are established only through the segment associated with the interface configured in **Interface for Source IP Address**. User-configured IP address in **Interface for Source IP address**, is not used for Cloud Portal reachability and WebSocket connections.

Connectivity from the interface specified in **Interface for Source IP Address** can result in established Cloud Portal WebSocket connectivity with all segment interfaces.

Packet forwarding for Cloud Portal

Cloud Portal reachability test specifies the interface through which Cloud Portal is reachable. This results in establishing the WebSocket connection over that interface, bypassing the route lookup.

Application Management

DHCP Server

Users can configure DHCP address ranges per segment because each interface is associated with the segment. Overlapping IP subnet/masks across two segments is not supported.

- When Segment A's segment interface is configured with 192.168.10.0/24 and the same or overlapping range is used to configure interface in Segment B, clients from both segments receive IP addresses allocated from a single range.
- When two ranges are configured for segments 192.168.10.1-99 and 192.168.10.200-250, the range configured last is used for both interfaces even if they are in different segments

DHCP Relay

DHCP relay is supported only in the default segment.

SSH, NetFlow, SNMP, NTP, and Syslog

These services are available only in the segment associated with the **Interface for the source IP Address** setting. Source IP address and traffic routing are described in Management Traffic Routing.

Management Services template

Version 9.0 adds a Management services template to the Default Template group. The **Interface for the source IP Address** default is ***any*** for all management services.

Users should plan for potential changes in behavior before applying the Management Services template if there are changes to the **Management Routes** page.

Because SSH management is configurable in the management services template, the existing CLI template excludes ***ssh server listen interface lo***. By default, **SSH service** is set to ***any*** – this allows users to SSH into an EdgeConnect appliance through the IP address of any interface.

Accessing services from multiple segments

When services are configured to run in a specific segment by selecting specific "Interface for source IP Address", these services are only available in that specific segment. Users can configure appropriate inter-segment rules to make these services accessible from the other segments.

CLI Session

CLI session usage requires the following management services are configured with the same segment:

- HTTP(s), Cloud Portal, Orchestrator, SaaS Opt
- SSH