Next-Generation Firewall

Configure Service Routes

Previous
Configure Virtual Routers
Next
Static Routes

Where Can I Use This?

- NGFW

What Do I Need?

One of these licenses for Strata Cloud Manager managed NGFWs:

- Strata Cloud Manager Essentials
- Strata Cloud Manager Pro

The firewall uses the management (MGT) interface by default to access external services, such as DNS servers, external authentication servers, Palo Alto Networks® services such as software, URL updates, licenses and AutoFocus. An alternative to using the MGT interface is to configure a data port (a regular interface) to access these services. The path from the interface to the service on a server is known as a `service route`. The service packets exit the firewall on the port assigned for the external service and the server sends its response to the configured source interface and source IP address.

You can configure service routes globally for the firewall or customize service routes for a virtual system on a firewall enabled for multiple virtual systems so that you have the flexibility to use interfaces associated with a virtual system. Any virtual system that does not have a service route configured for a particular service inherits the interface and IP address that are set globally for that service.

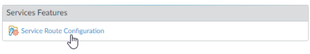
The following procedure enables you to configure service routes to change the interface that the firewall uses to send requests to external services such as the Palo Alto Network cloud services or for log forwarding. For firewalls in a high availability (HA) configuration, the service route configuration is synchronized across the HA peers

For firewalls in an active/passive high availability (HA), the service route you configured to leverage an external service or for log forwarding sees activity only on the **`active`** HA peer while the **`passive`** HA peer sees no activity if you configured an Ethernet interface as the **Source Interface**. For example, you configure a service route with Ethernet 1/3 as the source interface to forward logs to Strata Logging Service. In this scenario, all logs are forwarded from the **`active`** HA peer but no logs, including the system and configuration logs, are forwarded from the **`passive`** HA peer. However, if you configure the MGT interface as the service route **Source Interface**, activity occurs on both the **`active`** and **`passive`** HA peers.

PAN-OS & Panorama | Strata Cloud Manager

STEP 1 - Configure service routes.

1. Select **Device > Setup > Services > Global** (omit Global on a firewall without multiple virtual system capability), and in the Services Features section, click **Service Route Configuration**.



2. To force all firewall service communication with external servers through the management (MGT) interface, select **Use Management Interface for all** and click **OK**.

> When a service request originates from a firewall that has IPv6 enabled and has both IPv4 and IPv6 configured, the firewall behaves as a dual-stack host. Consequently, if the DNS resolution returns an IPv6 address as the first result, the firewall attempts to use that as the destination address.

> Additionally, in cases where the management interface is configured with only an IPv4 address and lacks a valid IPv6 configuration, if the DNS resolution returns an IPv6 address as the first result, the firewall doesn't **Use Management Interface for all** (which would be an IPv4 address). The firewall instead uses a dataplane IPv6 interface address as the source for the service request. Thus the service route has an IPv6 address at each end of the route.

3. As an alternative to using the MGT interface, select **Customize** and do one of the following to create a service route:
   - For a predefined service:
     - Select **IPv4** or **IPv6** and click the link for the service for which you want customize the service route.

> To easily use the same source address for multiple services, select the checkbox for the services, click **Set Selected Routes**, and proceed to the next step.

     - To limit the list for Source Address, select a **Source Interface**; then select a **Source Address** (from that interface) as the service route. An Address Object can also be referenced as a Source Address if it is already configured on the selected interface. Selecting **Any** Source Interface makes all IP addresses on all interfaces available in the Source Address list from which you select an address. Selecting **Use default** causes the firewall to use the management interface for the service route, unless the packet destination IP address matches the configured Destination IP address, in which case the source IP address is set to the **Source Address** configured for the **Destination**. Selecting **MGT** causes the firewall to use the MGT interface for the service route, regardless of any destination service route.

> The Service Route Source Address does not inherit configuration changes from the referenced interface and vice versa. Modification of an Interface IP Address to a different IP address or Address Object will not update a corresponding Service Route Route Source Address. This may lead to commit failure and require you to update the Service Route(s) to a valid Source Address value.

     - Click **OK** to save the setting.
     - Repeat this step if you want to specify both an IPv4 and IPv6 address for a service.
   - For a destination service route:
     - Select **Destination** and **Add** a **Destination** IP address. In this case, if a packet arrives with a destination IP address that matches this configured **Destination** address, then the source IP address of the packet will be set to the **Source Address** configured in the next step.
     - To limit the list for Source Address, select a **Source Interface**; then select a **Source Address** (from that interface) as the service route. Selecting **Any** Source Interface makes all IP addresses on all interfaces available in the Source Address list from which you select an address. Selecting **MGT** causes the firewall to use the MGT interface for the service route.
     - Click **OK** to save the setting.
4. Repeat the prior steps for each service route you want to customize.
5. Click **OK** to save the service route configuration.

STEP 2 - **Commit**.

Previous
Configure Virtual Routers
Next
Static Routes