

# Configure Traffic Steering Policies


- Traffic steering policy overview, on page 1
- Traffic steering policies, on page 2
- Traffic steering contracts, on page 6


# Traffic steering policy overview

Traffic steering policies determine which traffic is sent to the firewall in a network for security service insertion (SSI).

These policies contain

- security groups (source and destination security groups),
- firewall, and
- traffic steering contracts.

### Overview window

The traffic steering policy **Overview** window provides a summary of the security service insertion configuration.

From the main menu, choose **Policy** > **Traffic Steering Policy** to view the **Overview** window.

This table provides information about the components of this window based on the status of security service insertion.

| If security service insertion is... | Then... |
|---|---|
| disabled | this window displays the **Enable Service Insertion** option to enable security service insertion.<br>For more information, see Enable a service insertion site. |

| If security service insertion is... | Then... |
|---|---|
| enabled | this window displays these areas:<br>• **Summary**: displays the total number of:<br>  • Service insertion sites<br>  • Policies<br>  • Traffic steering contracts<br>• **Statistics by configuration**: displays this information:<br>  • Top five firewall IP addresses<br>  • Top five traffic steering contracts<br>  • Top five nodes |

# Traffic steering policies

For a service insertion site, the **Traffic steering policies** tab displays the steering policy details in the matrix view and list view.

### Matrix view

Click the icon on the top-right corner to open the matrix view. Matrix view provides an overview of all policies for all the security groups.

The matrix view contains two axes:

- Source axis: the vertical axis lists all the source security groups.
- Destination axis: the horizontal axis lists all the destination security groups.

Each cell in the matrix displays a color based on the type of policy configured for the corresponding source and destination security group:

- traffic steering policy,
- group-based policy,
- both traffic steering and group-based policies,
- no policy, or
- policies not applicable

Click to view the legend.

For the source and destination security group pairs that have a traffic steering policy configured, you can click the corresponding cell to view the traffic steering policy details and edit it. For source and destination security group pairs that do not have a traffic steering policy configured, you can click the corresponding cell to create the policy.

You can also create and deploy the traffic steering policies in this view.

### List view

Click the icon on the top-right corner to open the list view. List view provides a list of all the available traffic steering policies.

In this view, you can create, edit, view, delete, and deploy the traffic steering policies.

# Create a traffic steering policy on day zero

Use this procedure to create a traffic steering policy on day zero.

### Procedure

**Step 1** From the main menu, choose **Policy** > **Traffic Steering Policy**

**Step 2** Click the **Traffic steering policies** tab.

**Step 3** Click **Enable Service Insertion** to enable service insertion and create a traffic steering policy during the workflow.

For information about enabling service insertion, see Enable a service insertion site.

# Create a traffic steering policy on day *n*

Use this procedure to create a traffic steering policy on day *n*.

When you create a traffic steering policy, Catalyst Center creates a corresponding mirror policy automatically to reverse the traffic.

### Before you begin

- Ensure that the prerequisites are met. For more information, see Prechecks to enable a service insertion site on day zero.
- Enable security service insertion in Catalyst Center. For more information, see Enable a service insertion site.

**Note** If the security service insertion is not enabled, then Catalyst Center does not allow you to create the traffic steering policy.

- Create a traffic steering contract. For more information, see Create a traffic steering contract, on page 6.
- Create a Layer 3 virtual network. For more information, see Create a Layer 3 virtual network.

### Procedure

**Step 1** From the main menu, choose **Policy** > **Traffic Steering Policy**

**Step 2** Click the **Traffic steering policies** tab.

**Step 3** From the **Fabric site** drop-down list, choose a fabric site.

**Step 4** Click **Create policy**.

**Step 5** From the drop-down lists, choose

- a source security group,
- destination security groups, and
- a traffic steering contract.

**Note** The source and destination security groups must be different.

**Step 6** From the **Select a VN** drop-down list, choose a virtual network.

When you choose a virtual network, Catalyst Center displays the corresponding firewall name.

**Step 7** (Optional) Click the + icon to add another virtual network and firewall.

**Step 8** Under **Schedule provisioning**, choose a schedule.

a) In the **Task name** field, enter a name for the provisioning task.

b) Under **Schedule provisioning**, choose a schedule to push the policy to Cisco ISE.

| Click... | To... |
|---|---|
| **Now** | Immediately deploy the configuration. |
| **Later** | Schedule the date and time and define the time zone of the deployment. |

**Step 9** Click **Save**.

### What to do next

Deploy the policy on the device. For more information, see Deploy traffic steering policies, on page 6.

# Edit a traffic steering policy

Use this procedure to edit a traffic steering policy.

When you edit a traffic steering policy, Catalyst Center updates the corresponding mirror policy automatically. Catalyst Center uses the mirror policy to reverse the traffic.

### Procedure

**Step 1** From the main menu, choose **Policy** > **Traffic Steering Policy**

**Step 2** Click the **Traffic steering policies** tab.

**Step 3** From the **Fabric site** drop-down list, choose a fabric site.

**Step 4** In the list view ( ), check the check box next to the traffic steering policy that you want to edit.

**Step 5** Hover your cursor over **Actions** and choose **Edit**.

**Step 6** In the **Edit policy** slide-in pane, edit the required configurations.

For more information, see Create a traffic steering policy on day n, on page 3.

**Step 7** Under **Schedule provisioning**, choose a schedule.

a) In the **Task name** field, enter a name for the provisioning task.

b) Under **Schedule provisioning**, choose a schedule to push the policy to Cisco ISE.

| Click... | To... |
|---|---|
| **Now** | Immediately deploy the configuration. |
| **Later** | Schedule the date and time and define the time zone of the deployment. |

**Step 8** Click **Save**.

#### What to do next

Deploy the policy on the device. For more information, see Deploy traffic steering policies, on page 6.

# Delete traffic steering policies

Use this procedure to delete traffic steering policies.

When you delete a traffic steering policy, Catalyst Center deletes the corresponding mirror policy automatically.

### Procedure

**Step 1** From the main menu, choose **Policy** > **Traffic Steering Policy**

**Step 2** Click the **Traffic steering policies** tab.

**Step 3** From the **Fabric site** drop-down list, choose a fabric site.

**Step 4** In the list view ( ), check the check box next to the traffic steering policies that you want to delete.

**Step 5** Hover your cursor over **Actions** and choose **Delete**.

**Step 6** In the warning dialog box, click **Delete**.

### What to do next

Deploy the updates on the device. For more information, see Deploy traffic steering policies, on page 6.

# Deploy traffic steering policies

Use this procedure to deploy traffic steering policies to devices associated with the service insertion site after you create, edit, or delete traffic steering policies.

### Procedure

**Step 1** From the main menu, choose **Policy** > **Traffic Steering Policy**

**Step 2** Click the **Traffic steering policies** tab.

**Step 3** From the **Fabric site** drop-down list, choose a fabric site.

**Step 4** Click **Deploy**.

**Step 5** In the **Schedule deployment** slide-in pane, schedule the deployment.

a) In the **Task name** field, enter a name for the task.

b) Choose the required option to schedule the deployment.

| Option | Description |
|---|---|
| **Now** | Immediately deploy the configurations. |
| **Later** | Schedule the date and time, and define the time zone to deploy the configurations. |

c) Click **Deploy**.

# Traffic steering contracts

A traffic steering contract defines a set of rules that redirect specific network traffic from a source security group to destination security groups when the traffic matches a

- network application,
- transport protocol, and
- source and destination port.

# Create a traffic steering contract

Use this procedure to create a traffic steering contract to redirect the traffic.

Catalyst Center creates the contracts at a global level and doesn't assign them to any site.

### Procedure

**Step 1** From the main menu, choose **Policy** > **Traffic Steering Policy**

**Step 2** Click the **Traffic steering contracts** tab.

**Step 3** Click **Create steering contract**.

**Step 4** In the **Steering contract name** field of the **Create a steering contract** slide-in pane, enter a name for the steering contract.

**Step 5** (Optional) In the **Description** field, enter a description.

**Step 6** Click **Add Rule** to add a rule and complete these configurations:

a) Under **Application**, choose the application for which you want to apply the rule.

1. Click the pencil icon.
2. In the **Choose Application** dialog box, choose the required application.
3. Click **Confirm**.

| If you chose... | Then... |
|---|---|
| **advanced** | • Under **Transport Protocol**, from the drop-down list, choose a transport protocol for the rule.<br>• Under **Source port** and **Destination port**, enter the corresponding port numbers for the rule.<br>The valid range is from 1 to 65535. |
| other applications | based on the application that you chose, Catalyst Center displays the corresponding ports and transport protocol automatically. |

b) Use the **Enable logs** toggle button to enable or disable logging for any traffic filter rule (including the default action).

By default, logging is disabled. When logging is enabled, the device sends a syslog message when the rule is triggered.

Logging can be helpful in troubleshooting and initial testing of a policy. However, we recommend that you use it sparingly, as it may impact the resources and performance of devices.

**Step 7** (Optional) Complete these configurations:

| If you want to... | Then... |
|---|---|
| create another rule | Use one of these options:<br>• Repeat Step 6, on page 7, or<br>• under **Actions**, click the corresponding + icon and repeat 6.a, on page 7 and 6.b, on page 7. |

| If you want to... | Then... |
|---|---|
| Update the sequence of a rule. | The rules are checked in the sequence in which they are listed in the **Rules** table. Complete these steps to update the sequence:<br>**a.** Click the corresponding ⠿ icon.<br>**b.** Drag and drop the rule to the required position. |
| Enable logs for multiple rules. | **a.** Check the check box next to the required rules.<br>**b.** Click **Enable Logs**. |
| delete rules | **a.** Check the check box next to the rules that you want to delete and click **Delete**, or<br>**b.** under **Actions**, click the corresponding delete icon (🗑) for the rule that you want to delete. |

**Step 8** Click **Save**.

Catalyst Center detects any duplicate rules and merges them automatically while saving the traffic steering contract.

# Edit or duplicate a traffic steering contract

Use this procedure to edit or duplicate a traffic steering contract.

**Procedure**

**Step 1** From the main menu, choose **Policy** > **Traffic Steering Policy**

**Step 2** Click the **Traffic steering contracts** tab.

**Step 3** Check the check box next to the contract that you want to edit or duplicate.

**Step 4** Choose the required option.

| If you want to... | Then... |
|---|---|
| edit the steering contract | hover your cursor over **More Actions** and choose **Edit**. |
| duplicate the steering contract | hover your cursor over **More Actions** and choose **Duplicate**. |

**Step 5** Edit the required configurations.

For more information, see Create a traffic steering contract, on page 6.

**Step 6** Click **Save**.

# Delete traffic steering contracts

Use this procedure to delete traffic steering contracts.

### Procedure

**Step 1** From the main menu, choose **Policy** > **Traffic Steering Policy**

**Step 2** Click the **Traffic steering contracts** tab.

**Step 3** Check the check box next to the contracts that you want to delete.

**Step 4** Hover your cursor over **More Actions** and choose **Delete**.

**Step 5** In the warning dialog box, click **Yes**.