Manage Catalyst SD-WAN Security Policies

An Introduction to Catalyst SD-WAN NGFW Security Policies

The NGFW security policies in Catalyst SD-WAN Manager are a set of rules and configurations designed to protect systems, networks, and data from unauthorized access, misuse, or threats. Catalyst SD-WAN Manager provides a comprehensive framework for both implementing and managing NGFW security policies.

Manage Existing Catalyst SD-WAN NGFW Security Policies

Note that you cannot delete an NGFW policy from Security Cloud Control Firewall Management that is already associated with a policy group in Catalyst SD-WAN.

Procedure

Step 1 In the left pane, click **Manage** > **Policies** > **WAN Branch Edge**.

Step 2 Navigate to the policy and click the ellipsis (…) under the **Action** column.

Step 3 Click **View**, **Edit**, **Delete**, or **Copy**.

Create Catalyst SD-WAN Security Policies

Before you begin

Ensure that these devices are deployed and managed using a configurations group. For more information about creating configuration groups, see Configuration Groups and Feature Profiles.

Procedure

Step 1 In the left pane, click **Manage** > **Policies** > **WAN Branch Edge**.

Step 2 On the **Catalyst SD-WAN NGFW Policies** page, click **Add NGFW Policy**.

This launches the Create NGFW policy workflow.

Step 3 On the **Security Policy Name** tab, enter **Policy Name** and **Description**, and under **Device Solution**, select the **sdwan** radio button and click **Next**.

Step 4 On the **Select the optional Configuration Group to associate with the security policy** page, choose the configuration group to associate with the NGFW policy and click **Next**.

Step 5 On the **Create Sub-Policies** tab, click **+Add Sub-Policy** to add sub-policies for a security policy.

Field	Description
VPN / Interface	Specify the VPN or the interface.
Source Zone	Choose the zone that is the source of the data packets. The options are: • Corporate_Users_zone • Local_Internet_for_Guests_zone • No_zone • Payment_Processing_Network_zone • Physical_Security_Devices_zone • Self • Untrusted To create a new Source Zone, click **+ Create New**. Enter the **Name** and select the **VPN**. Note that multiple VPNs can be selected within a Source Zone.

Field	Description
Destination Zone	Select the zone/s to which data traffic is sent. The options are: • Corporate_Users_zone • Local_Internet_for_Guests_zone • No_zone • Payment_Processing_Network_zone • Physical_Security_Devices_zone • Self • Untrusted To create a new Destination Zone, click **+ Create New**. Enter the **Name** and select the **VPN**. Note that multiple VPNs can be selected within a Source Zone.

Step 6 Click **Additional Settings** to configure additional settings for a security policy. Refer to the steps used in the procedure, Configure NGFW Additional Settings. Click **Save**.

Step 7 Click on the ellipsis (...) at the top left corner of the existing sub-policy to **Edit**, **Delete**, or **Copy** it.

Step 8 To add a rule to a sub-policy, navigate to the sub-policy and click **+ Add Rule**.

Field	Description
Rule Name	The name of the rule.
Sequence	Specify the sequence.

Field	Description

Match	Choose the desired match conditions from the **Add Conditions** drop-down list. The options are:
	• Source
	  • Geo Location
	  • IPv4 Prefix
	  • Port
	• Destination
	  • FQDN
	  • Geo Location
	  • IPv4 Prefix
	  • Port
	• Protocol
	• Applications
	When ISE is enabled, then SGT option is available in the **Source** and **Destination**. Identity User or User group is only supported for **Source**.

Action	Choose the desired action conditions. The options are: • Pass • Drop • Inspect • Log Events: Unified Logging for Inspect Action.

Step 9 To modify an existing rule, click the pencil icon to **Edit**, **Disable**, **Delete**, **Clone rule**, **Add rule on top**, or **Add rule below**.

Associate a Policy Group to Catalyst SD-WAN NGFW Policy

Procedure

Step 1 In the left pane, click **Manage** > **Policies** > **WAN Branch Edge**.

Step 2 Navigate to the policy you want to associate with a policy group. Click the ellipsis (…) under the **Action** column and click **Associate Policy Group**.

Step 3 Select the policy and click **Save**.

Deploy Policy Group from Catalyst SD-WAN Manager

A policy group in Catalyst SD-WAN refers to a logical grouping of related items or configurations that are used in Next-Generation Firewall (NGFW) security policies. These groups are created to simplify the process of applying policies across multiple devices or sites.

NGFW policy modifications, including security objects and profiles, from Security Cloud Control Firewall Management, must be deployed to Secure Router devices using the Catalyst SD-WAN Manager.

You can access the workflow by choosing **Workflows** > **Deploy Policy Group** menu in Catalyst SD-WAN Manager. The **Deploy Policy Group** workflow enables you to associate Secure Router devices and deploy the policy group to the selected devices.

For more information, refer to the *Deploy Policy Group Workflow* section in the Policy Groups Configuration Guide, Cisco IOS XE Catalyst SD-WAN.