Revised: April 6, 2026

Configure Firewall Policies for SD-Routing Devices

What's new and changed

Cisco IOS XE Release	Feature Name and Description	Supported Platforms
Cisco IOS XE 26.1.1a	**Enhancements for NGFW in Policy Groups** This feature introduces support for NGFW Policy Groups, that includes import and export of firewall policies, display of rule hit counts, drag-and-drop rule reordering to update priority, visibility of policy and object usage references in the NGFW Dashboard.	• Cisco Catalyst 8000V Edge Software • Cisco Catalyst 8500 Series Edge Platforms • Cisco Catalyst 8300 Series Edge Platforms • Cisco Catalyst 8200 Series Edge Platforms • Cisco 1000 Series Integrated Services Routers • Cisco 4000 Series Integrated Services Router • Cisco ASR 1000 Series Aggregation Services Routers • Cisco 8100 Series Secure Routers • Cisco 8200 Series Secure Routers • Cisco 8300 Series Secure Routers • Cisco 8400 Series Secure Routers • Cisco 8500 Series Secure Routers

NGFW policies for SD-Routing devices

A firewall policy is a localized security policy that allows the inspection of data traffic flows in your network. Using firewall policies, you can configure zone-based policies to protect your network against breaches and threats.

SD-Routing supports high-speed logging (HSL). When HSL is configured, a firewall provides a log of packets that flow through routing devices to an external collector or destination servers.

You can configure a source interface for HSL and a UTD syslog interface in a policy group. Also, you can define, apply, and manage firewall policies to define traffic flows between zones. You can create zones based on the interface and control all the data traffic that pass between zones.

In addition, the New Gen Firewall (NGFW) functionality in SD-Routing supports Unified Logging. It allows the stateful and stateless inspection of TCP, UDP, and ICMP data traffic that flows in your network. This functionality also allows you to effortlessly incorporate firewall solutions from the Cisco SD-WAN manager.

From 17.16.1a release onwards, you can clone, copy, and search for a rule using Cisco SD-WAN Manager.

Restrictions

- You can configure a maximum of 4 High Speed Logging (HSL) source interfaces in a firewall policy.
- VRF is not supported.
- You can configure only one external syslog server source interface for UTD.
- IPv6 rules or rulesets do not support identity.
- Only IPv4 rules with an NGFW policy support Identity. IPv4 rules with rulesets are not supported.

Before you begin

You must create a policy group from the SD-WAN Manager. For more information, see Policy Groups in the *Policy Groups Configuration Guide, Cisco IOS XE Catalyst SD-WAN Release 17.x.*

Workflow to set up firewall policy using Policy Groups

This workflow outlines the high-level steps required to set up firewall policies for your SD-Routing devices. The detailed instructions are covered in each of the sections.

Task	Detailed steps
Create an NGFW Policy	Create an NGFW policy, on page 2
Add a Sub Policy	Create a sub policy, on page 3
Review and create the policy	Review and create the policy, on page 6
Associate the NGFW policy with a Policy Group	Associate a Policy Group with the NGFW policy, on page 6

Create an NGFW policy

This task specifies the steps you must perform to create a firewall policy for your network.

Step 1 On the SD-WAN Manager main menu, go to **Configuration** > **Policy Groups**.

Step 2 On the **Policy Groups** window, click the **NGFW** tab.

Step 3 On the **Create NGFW Policy** window, specify the details for these fields:

Field	Description
Policy Name	Specify the name of the policy group. This field is mandatory and can contain only uppercase and lowercase letters, the digits 0 through 9, hyphens (–), and underscores (_). This field cannot contain spaces or any other characters.

Field	Description
Description	Provide a description for the policy group. This field can contain up to 2048 characters, including spaces.

Step 4 From the **Device Solution** radio button, select **sd-routing**.

Step 5 Click **Next** to go to the **Select Configuration Groups** page. This SD-Routing page is not applicable for SD-Routing devices. Click **Next**, again, to proceed to create a sub policy.

Create a sub policy

Perform these steps to create sub policies under a security policy.

Step 1 On the **Create Sub-Policy** window, click **Add Sub Policy**.

Step 2 In the **Source Zone** field, choose the zone that is the source of the data packets.

Step 3 In the **Destination Zone** field, choose the zone that is the destination of the data packets.

Step 4 On the **Add Rule** pop-up window that is displayed, configure the rules for your sub policy. This table specifies the fields under each section.

Field	Description
Add Rule or Rule with Rule Sets	
Rule Name	Specify a name for your rule.
Sequence	Specify the sequence or order of check.
Destination Zone	In the **Destination Zone** drop-down list, choose the zone to which data traffic is sent. Zones are created based on the VPNs in the configuration group selected in the create security policy workflow.
Match	
Add Conditions	To specify the match criteria or conditions for your rule, click **Add Conditions** under **Match**. From the drop-down list, choose the match conditions for your rule.
Traffic Source	
Data Prefix	Choose the **Data Prefix** from the drop-down list. This field specifies the IPv4 prefixes or IPv6 prefixes or prefix lists and/or domain names, (FQDN) or list(s). Based on the IP address type that you choose, the **Source Data Prefixes** field displays the prefix options.
Protocol	Configure the protocol match for your rule.
Application	From this drop-down list, choose one of more applications and a match condition for the rule.

Field	Description
Match (Rule Set)	You can choose the desired match conditions for a rule from the **Add Conditions** drop-down list. The available options include: Type • IPv4 • IPv6 You can configure IPv6 from Cisco Catalyst SD-W AN Manager Release 20.18.2: • Applications • Protocol • Source • Geo Location (Supported when the chosen type is IPV4 • IPv4 Prefix • Port • Destination • FQDN • Geo Location (Supported when the chosen type is IPV4 • IPv4 Prefix • Port When adding conditions for **Source** or **Destination**, select **Object** in **Data Prefix** and choose a policy object from the list. Identity User or User group is only supported for **Source**. You can create Object Groups. Object groups allow users to combine multiple objects into a single group or easier policy management. An Object Group can only be added when the other three items in the drop-down list are deselected.

Field	Description
Action	Select one of the radio buttons: • **Pass**: Allows the traffic to pass the destination zone without inspection. • **Drop**: Enables drop notifications whenever a packet is dropped. • **Inspect**: Enables inspection of the traffic in your zones. • **Log Events**: Select this check box to enable unified logging for inspect action. Select **Advanced Inspection** from the drop-down list.

Note From 17.18.2, you can pre-configure Object Groups, Data Prefix IPv6, and Rule set under **Configuration** > **Policy Groups** > **Objects and Profiles** > **Security Objects**. Once created here, the configured security objects appear as a dropdown option when adding as rule or rule set.

Step 5 Click **Additional Settings** and configure the following:

Field	Description
TCP SYN Flood Limit	Specify the threshold of SYN flood packets per second for each destination address.
Max Incomplete	Specify the timeout limits for the firewall policy. A Max Incomplete timeout limit protects firewall resources and keeps these resources from being used up.
TCP Limit	Specify the maximum TCP half-open sessions allowed on a device.
UDP Limit	Specify the maximum UDP half-open sessions allowed on a device.
ICMP Limit	Specify the maximum ICMP half-open sessions allowed on a device.
Audit Trail	Enable the Audit Trail option. This option is only applicable for rules with an inspect action.
Unified Logging	Enable the unified logging feature.
Optimized Policy	Enable the optimized policy option.
Session Reclassify Allow	Allow re-classification of traffic on policy change.
ICMP Unreachable Allow	Allow ICMP unreachable packets to pass through.
Advanced Inspection Profile	Attach a global advanced inspection profile (AIP) at a device level. All the rules in the device that match the traffic to be inspected are inspected using the advance inspection profile.

Field	Description
TLS/SSL Decryption	Choose the TLS/SSL decryption profile from the drop-down list
High Speed Logging Source File	Add security logging servers.
External Syslog Server	Select the Source Interface

Step 6 Click **Save**.

Review and create the policy

Perform this task after you add a Sub-Policy to your firewall policy.

Step 1 On the **Summary** window, review all the configuration settings for your firewall policy.

Step 2 Click **Create NGFW Policy** to create the policy.

Import and export policies

You can import or export the firewall policies using Cisco Catlyst SD-WAN Manager. Export policies as a CSV file, modify the rules as needed, and then import the updated file. This process allows you to efficiently add or update existing rules.

For any NGFW sub-policy, click **...** and select **Export** to download the CSV file. After making your modifications, click **Import** to upload the updated CSV file. During the import process, Cisco Catalyst SD-WAN Manager validates the file and flags any errors.

Hit count

You can view the hit count of each rule within a sub-policy in Cisco Catalyst SD-WAN Manager.

A rule hit count represents the total number of times a firewall rule has been accessed. This helps you to analyze rule effectiveness and identify unused rules for removal. For any NGFW sub-policy, click **...** and choose **Hit count**. In the sidebar you can view the list of all the firewall rules for the sub-policy and the hit count for each rule. You can also view the hit count for all the sites or a specific site using the sites drop-down menu.

Associate a Policy Group with the NGFW policy

Perform this task to associate the firewall policy you created with a Policy Group. If you don't have a Policy Group already, you must create one.

Step 1 On the SD-WAN Manager main menu, go to **Configurations** > **Policy Groups**.

Step 2 Select the Policy Group to which you want to associate the NGFW Policy.

Step 3 From the **NGFW** drop-down field, select the NGFW policy you created.

Step 4 Click **Save** to create an association between the NGFW Policy and the Policy Group. This association ensures that the NGFW Policy is applied to the Policy Group.

Step 5 Select the SD Routing devices on which you want to provision this policy, and click **Next**.

Step 6 Review the workflow and complete the wizard by clicking **Deploy**, to deploy the Policy Group to the device. Your device is now ready to use the NGFW Policy.

High speed logging

After you create a Policy group and a NGFW policy, you can enable High Speed Logging (HSL) for your firewall messages. When you configure HSL, a firewall provides a log of packets that flow through the SD-Routing devices to an external collector. Records are sent when sessions are created and destroyed. Session records contain the source IP address, destination IP address, source port, destination port, and protocol.

HSL allows a firewall to log records with minimum impact to packet processing. The firewall uses buffered mode for HSL. In buffered mode, a firewall logs records directly to the high-speed logger buffer, and exports of packets separately.

Enable high speed logging

Perform this procedure to configure your log server destination IP addresses to export Syslog records.

Step 1 On the SD-WAN Manager main menu, go to **Configuration** > **Network Hierarchy**.

Step 2 Under the **Collectors** tab, select the **Security Logging** toggle button.

Step 3 In the **High Speed Logging Servers** field, configure up to four labels for the source interface configured with the destination servers to collect logs for HSL. Specify the **VPN**, **Server IP**, and **Port** details for the HSL servers here.

Step 4 In the **External SysLog Server Source Interface** field, enter these details to export the UTD logs to the external syslog server:

- In the VPN field, enter the VPN that the syslog server is in.
- In the Server IP field, enter the IP address of the syslog server.

Step 5 Click **Save**.

Step 6 Add the Source Interface in the Additional Settings and associate a Policy Group with the firewall policy where you have enabled HSL.

Step 7 Preview and deploy the policy to the SD-Routing devices to use HSL.

Note If you do not configure the HSL and Syslog servers through Network Hierarchy page, a pop-up window appears for the first time under **Configuration** > **Policy Groups** > **NGFW**> **Additional Settings** to support the addition of HSL and syslog details. However, once you configure HSL and syslog, you can edit or update the settings only through Network Hierarchy page.

Verify high speed logging

After you deploy a NGFW policy with HSL and Syslog Source Interface configuration on the **CLI Pane**, verify whethere the:

a) HSL CLI **log flow-export v9 udp destination <destinationip> <port> source <interface name>** is pushed to the device.

b) UTD Syslog CLI **logging host <hostip> source-interface <interface name>** is pushed to the device.