Using Policy Groups for SD-Routing Devices

First Published: 2024-04-30

Last Modified: 2024-04-30

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

© 2024 Cisco Systems, Inc. All rights reserved.

CONTENTS

CHAPTER 1 **Policy groups** 1

Feature history for policy groups 1

Policy groups 2

Policy group benefits 2

Supported devices for policy groups 3

Configure prerequisites for policy groups 3

Restrictions for policy groups 4

Add policy group 4

Policy group workflows 6

Deploy policy group workflow 6

Add devices to a policy group using rules 7

Objects and profiles 8

Configure objects and profiles 8

Policy validation for Cisco Catalyst SD-WAN 11

Troubleshooting policy group validations 12

CHAPTER 2 **Application Priority and SLA** 13

Feature history for policy groups 13

Application Priority and SLA 13

Create an application priority and SLA policy 14

Configure traffic policy 16

Advanced layout 17

Configure SLA class 18

Configure QoS policy 19

Policy sequence generation for match and action rules 19

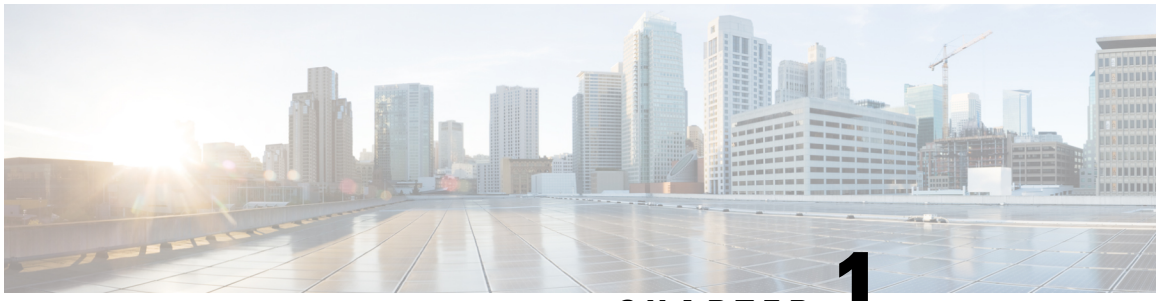
Match conditions 20

Action conditions 22
Monitor traffic flow 28

CHAPTER 3 Next-Generation Firewall (NGFW) 31
Feature history of NGFW 31
NGFW 33
Enable RBAC for NGFW policy 33
Restrictions for NGFW policy 34
Configure NGFW policy using a workflow 35
Edit NGFW policy 36
Import and export policies 42
Hit count 42
Configure an NGFW Sub-Policy 42
Configure additional settings for an NGFW policy 45
Version control for NGFW 50
Configure policy objects for an NGFW policy 50

CHAPTER 4 Secure Internet Gateway and Secure Service Edge 61
Feature history for Secure Internet Gateway and Secure Service Edge 61
Secure Internet Gateway 61
Configure a Secure Internet Gateway 62
Configure a Secure Service Edge 68

CHAPTER 5 DNS Security 77
Feature history for DNS security 77
DNS security 77
DNS security routing and fallback 78
Configure DNS security 79
Verify DNS security configurations using CLI 81



CHAPTER 1

Policy groups

- Feature history for policy groups, on page 1
- Policy groups, on page 2
- Add policy group, on page 4
- Policy group workflows, on page 6
- Objects and profiles, on page 8
- Policy validation for Cisco Catalyst SD-WAN, on page 11
- Troubleshooting policy group validations, on page 12

Feature history for policy groups

Table 1: Feature history

Feature Name	Release Information	Description
Policy Groups	Cisco IOS XE Catalyst SD-WAN Release 17.12.1a Cisco Catalyst SD-WAN Manager Release 20.12.1	This feature provides a simple, reusable, and structured approach for configuring policies in Cisco Catalyst SD-WAN. You can create a policy group, that is, a logical grouping of policies that is applied to one or more sites or devices at the site in the network. To deploy the policy group to devices, the devices must be managed by a configuration group in Cisco Catalyst SD-WAN. You can configure policies based on features that are required, recommended, or uniquely used, and then combine them to complete a policy configuration. The Deploy Policy Group workflow in Cisco Catalyst SD-WAN provides a guided method to select previously created policy groups and deploy them to sites or devices at the site that is managed by configuration groups.
Policy validation in Cisco SD-WAN	Cisco IOS XE Catalyst SD-WAN Release 26.1.1 Cisco Catalyst SD-WAN Manager Release 26.1.1.1	This feature ensures network reliability and operational efficiency by automatically validatingCisco Catalyst SD-WAN policies for accuracy, platform compliance, and alignment with network requirements before deployment.

Feature Name	Release Information	Description
Device Tagging for Policy Groups	Cisco IOS XE Catalyst SD-WAN Release 26.1.1 Cisco Catalyst SD-WAN Manager Release 26.1.1.1	With this feature you can add devices to a policy group configuration workflow using tags.

Policy groups

A policy group is a collection of policies and policy parameters that

- provides a simple, reusable, and structured approach for configuring policies and policy objects in Cisco IOS XE Catalyst SD-WAN devices
- allows you to configure basic and necessary policies with defaults to get your systems up and running through a simplified workflow, and
- can be associated with one or more sites or a single device at the site in the network and deployed on devices managed by configuration groups.

Policy group configuration options

Policy groups allow you to configure policies using different approaches:

- **Basic configuration**: Configure the basic and necessary policies with defaults through a simplified workflow
- **Advanced layout**: Switch to complete control and configure detailed policy parameters such as service-level agreement (SLA) class, Quality of Service (QoS) Maps, and Match-Action parameters pertaining to the traffic policy

After you've configured a policy group, you can deploy it on Cisco IOS XE Catalyst SD-WAN devices.

Policy group benefits

- Simplified user experience through an intuitive UI that allows you to quickly configure the basic policies that are required to get your Cisco Catalyst SD-WAN deployments up and running.
- Option to edit policy groups based on the changing needs of your network and save the configuration. You can choose to deploy these changes only when needed - during maintenance windows or in off-production hours.
- A **Preview CLI** option to preview the difference in configuration for relevant devices such as Cisco IOS XE Catalyst SD-WAN device and Cisco SD-WAN Controller in one location.
- Workflows to deploy policy groups.

Supported devices for policy groups

This feature is supported only on Cisco IOS XE Catalyst SD-WAN devices.

Configure prerequisites for policy groups

Before you begin

Before you begin configuring policy groups, ensure that these requirements are met:

- Minimum software version for Cisco IOS XE Catalyst SD-WAN devices: Cisco IOS XE Catalyst SD-WAN Release 17.8.1a

  Minimum software version for Cisco SD-WAN Manager: Cisco Catalyst SD-WAN Manager Release 20.12.1

- 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.

Follow these steps to configure RBAC for policy groups and application priority policies:

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Administration** > **Manage Users** > **User Groups**.

Ensure that the granular role-based access control (RBAC) for policy groups is specified by expanding it. With specific permissions to the usergroup, ensure that you are able to access policy groups from **Configuration** > **Policy Groups**.

Step 2 Click **Add User Group**.

Step 3 Enter **User Group Name**.

Step 4 Select the **Read** or **Write** check box against the **Policy Group** and **Device** feature that you want to assign to a user group.

Step 5 Click **Add**.

Step 6 From the Cisco SD-WAN Manager menu, choose **Administration** > **Manage Users** > **User Groups**.

Ensure that the granular RBAC for the application priority policy is specified by expanding it. With the set permissions to the usergroup, ensure that you are able to access the application priority policy from **Configuration** > **Policy Groups**.

Step 7 Click **Add User Group**.

Step 8 Enter **User Group Name**.

Step 9 Select the **Read** or **Write** check box against these features that you want to assign to a user group:

- **Feature Profile** > **Application Priority** > **Qos Policy**
- **Feature Profile** > **Application Priority** > **Traffic Policy**
- **Feature Profile** > **Policy Object** > **App List**
- **Feature Profile** > **Policy Object** > **SLA Class**
- **Feature Profile** > **Policy Object** > **TLOC**
- **Feature Profile** > **Policy Object** > **App Probe**

- **Feature Profile** > **Policy Object** > **Preferred Color Group**
- **Feature Profile** > **Policy Object** > **Class**
- **Feature Profile** > **Policy Object** > **Data Prefix**
- **Feature Profile** > **Policy Object** > **Data Ipv6**
- **Feature Profile** > **Policy Object** > **Policer**

Step 10 Click **Add**.

Restrictions for policy groups

Policy groups have several restrictions that impact configuration and deployment capabilities:

- The Application Priority and SLA workflow does not support custom applications.
- Before deploying policy groups to devices, they must first be managed by a configuration group.
- The forwarding class in localized policy is not supported.
- An error occurs when a duplicate parcel name (for example, Site27-VPN1) exists in another configuration group. Verify existing parcel names across all groups and modify the intended name to ensure exclusivity. Use descriptive naming conventions to prevent conflicts.

Add policy group

Create a policy group that can be deployed to devices to manage application priority, security policies, and other network configurations.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Policy Groups** > **+ Add Policy Group**.

Step 2 Enter a **Policy Group Name**, choose a **Solution** from the drop-down list and provide a description (optional).

Table 2: Policy group parameters

Field	Description
Policy Group 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 (_). It cannot contain spaces or any other characters.
Description	Provide a description for the policy group. It can contain up to 2048 characters including spaces.

Field	Description
Policy	
Application Priority & SLA	Choose an application priority for the policy group from the drop-down list. Click **Create New** to create a new application priority.
Embedded Security	Choose an embedded security policy from the drop-down list. Click **Create New** to create a new embedded security policy by selecting a configuration group, creating firewall policies, and other configuration settings.
Secure Internet Gateway	Configure the Secure Internet Gateway (SIG) tunnels before you apply a data policy for redirecting application traffic to an SIG. Select a Secure Internet Gateway (SIG) policy from the drop-down list. Click **Create New** to create a new SIG policy.
DNS Security	Select a DNS Security policy from the drop-down list. Click **Create New** to create a new DNS Security policy.

Step 3 Click **Create**.

Note
If you have already created a policy group, click the policy group from the list of available policy groups to edit.

Step 4 Click **Save** to save your configuration.

Step 5 Click the pencil icon to select or unselect devices to associate or dissociate with the policy group.

Note
Starting from Cisco Catalyst SD-WAN Manager Release 20.15.1, click **+Add** adjacent to **Associated** field to select or unselect devices to assoicate or dissociate with the policy group. In the associate devices workflow, you can choose devices based on **Regions** and not just **Sites**.

Step 6 Click **Deploy** to select sites and deploy the policy group.

The policy group is created and deployed to the selected devices. To delete a policy group, select the ellipsis icon (**...**) to the right of the policy group and click **Delete**.

Note Dissociating policies from policy groups do not remove the policies from the device. If you intend to remove a policy or configuration from a device, then you need to remove the policy from the policy group and redeploy to that device so that the deployment ensures that the policy is removed from that device. You can move the device to a new empty policy group with no policy profiles to refresh the controller state and to remove stale entries. Until that is done, mere dissociation will not remove any policies from the device.

Policy group workflows

A policy group workflow is a configuration management feature that

- guides you in creating a policy group for one or more sites or a single device at the site in the network that is managed by configuration groups in Cisco Catalyst SD-WAN, and
- provides you with an improved configuration and troubleshooting experience.

Policy group workflow features

The workflow has the following features:

- allows you to review the various configuration values on a single page within the workflow, and
- helps you easily identify and fix incorrect values that appear highlighted in red.

Deploy policy group workflow

You can access the workflow by choosing **Workflows** > **Deploy Policy Group** menu in Cisco SD-WAN Manager.

The **Deploy Policy Group** workflow enables you to associate devices with a previously created policy group and deploy the policy group to the selected devices. You can review device configurations to further add Site IDs and other variables that must be provided as part of a policy group before deploying the policy group.

An asterisk that is adjacent to a field name helps you identify the mandatory values within the workflow.

After deploying a policy group, any subsequent changes to the policy group will cause the Cisco SD-WAN Controller to appear in the deployment preview, even if no changes are being deployed to the controller itself.

Additionally, any modifications to the Application Priority and SLA policy are automatically pushed to all Cisco IOS XE Catalyst SD-WAN devices associated with the policy group, as well as the Cisco SD-WAN Controllers, regardless of which devices are selected in the deployment workflow. This behavior differs from NGFW, DNS Security, and SIG policies, where changes are only deployed to the selected Cisco IOS XE Catalyst SD-WAN device.

Cisco SD-WAN Controller tasks for policy group deployments

Starting with Cisco Catalyst SD-WAN Manager Release 26.1.1.1, deploying a policy group triggers a Cisco SD-WAN Controller task during the subsequent deployment in any of these scenarios:

- A device that was previously part of a classic centralized policy is newly associated with any policy group.
- A device is removed from a policy group that had Application Priority and SLA policies deployed.
- A device associated with the policy group is included in an existing Cisco SD-WAN Controller policy configuration, even if neither of the preceding conditions applies.

Only the Cisco SD-WAN Controller intent for the current policy groups, as well as the intent for any policy group involved in a device migration is included in the CLI generation.

From SD-WAN Manager 26.2.x, when you deploy a policy group, Cisco SD-WAN Manager excludes controllers from the CLI preview if no CLI differences exist for the controllers.

Policy group deployment previews in multitenant environments

Starting with Cisco Catalyst SD-WAN Manager Release 26.1.1.1, in multitenant environments, Cisco SD-WAN Manager no longer provides a preview diff for centralized policies, topology groups, policy groups, or device templates.

Instead, Cisco SD-WAN Manager shows the complete generated configuration as new. This configuration matches what is applied to the device because multitenant environments deploy the full configuration during each deployment.

In single-tenant environments, the preview diff behavior remains unchanged. Cisco SD-WAN Manager continues to show only the configuration differences.

Add devices to a policy group using rules

Before you begin

From SD-WAN Manager 26.1.1.1, you can add devices to a policy group using tags.

Ensure that you have added tags to devices. For more information about tagging, refer to the Device tagging section in the *Cisco Catalyst SD-WAN Systems and Interfaces Configuration Guide*.

Follow these steps to add devices to a policy group using rules:

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Policy Groups**.

Step 2 Select a policy group from the available list.

Step 3 Click the **+ Add** option adjacent to **Associated** in the **Deployment** area.

Step 4 Click **Manage rule**. You can select **Modify rules** or **Remove rules**. In the **Rules** section, choose values for the following options:

a) **Rule name**: Enter a unique name for the rule. Rule names cannot be duplicated once you create it.

b) **Rule Conditions**: Choose one of the two rules and configure the conditions: **Match All** or **Match Any**.

c) Choose one of these operators:

- **Equals**
- **Not equals**
- **Contains**
- **Not contains**
- **Starts with**
- **End with**

Note
You cannot create a new rule if it conflicts with an existing rule.

Step 5 Click **Apply**.

Based on the rule, a list of devices that will be added to or removed from the policy group appears.

Step 6 Click **Confirm** to apply the changes.

Objects and profiles

Objects and profiles provides a list of related policy objects that you can configure and call in the match or action components of a policy. Click **Objects and Profiles** to create new objects for the policy group.

In Cisco IOS XE Catalyst SD-WAN Release 17.18.x and earlier releases, **Objects and Profiles** is called **Groups of Interest**.

Configure objects and profiles

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Policy Groups**.

Step 2 Click **Objects and Profiles**.

a) Configure **Application**.

From the **Application/Application family list** drop-down, choose the required applications or application families.

A few application lists are preconfigured. You cannot edit or delete these lists.

Microsoft_Apps: Includes Microsoft applications, such as Excel, Skype, and Xbox. To display a full list of Microsoft applications, click the list in the **Entries** column.

Google_Apps: Includes Google applications, such as Gmail, Google Maps, and YouTube. To display a full list of Google applications, click the list in the **Entries** column.

b) Configure **Add App Probe Class**.

Field	Description
Probe Class Name	Enter a name for the probe class.
Forwarding Class	Choose the forwarding class from the drop-down list.
Color	Choose the color from the drop-down list.
DSCP	Enter the DSCP value.

You can add more entries if needed by clicking on + icon.

c) Configure **Color**.

Field	Description
Color List Name	Enter a name for the list.
Select Color	Choose one or more color lists types from the drop-down list.

To configure multiple colors in a single list, you can choose multiple colors from the drop-down list.

d) Configure **Community List**.

A community list is used to create groups of communities to use in a match clause of a route map. A community list can be used to control which routes are accepted, preferred, distributed, or advertised. You can also use a community list to set, append, or modify the communities of a route.

Field	Description
Community List Name	Enter a name of the community list.
Add Community	Enter one or more communities separated by commas. • **aa** : **nn** : Autonomous System (AS) number and network number. Each number is a 2-byte value with a range from 1 to 65535. For example, 65526. • **internet** : Routes in this community are advertised to the internet community. This community comprises all BGP-speaking networking devices. • **local-as** : Routes in this community are not advertised outside the local AS number. • **no-advertise** : Attaches the NO_ADVERTISE community to routes. Routes in this community are not advertised to other BGP peers. • **no-export** : Attaches the NO_EXPORT community to routes. Routes in this community are not advertised outside the local AS or outside a BGP confederation boundary. To configure multiple BGP communities in a single list, include multiple **community** options, specifying one community in each option.

e) Configure **Data Prefix** and **Data Prefix IPv6**.

Field	Description
Data Prefix List Name	Enter a name for the data prefix list.
Add Data Prefix	Enter one or more data prefixes separated by commas. Does not support: 0.0.0.0/0

f) Configure **Expanded Community List**.

Field	Description
Community List Name	Enter a name for the community list.

Field	Description
Add Community	Specify details of the expanded community list that is used to filter communities using a regular expression.

g) Configure **Forwarding Class**.

Field	Description
Forwarding Class	Enter a name for the forwarding class.
Queue	Choose a value for the queue from the drop-down list.

h) Add policer.

Field	Description
Policer List Name	Enter a name for the policer list.
Burst (bytes)	Enter the maximum traffic burst size. The range is from 15,000 to 10,000,000 bytes.
Exceed	Choose the action to take when the burst size or traffic rate is exceeded. The options are: • Drop: sets the packet loss priority (PLP) to low • Remark: sets the packet loss priority (PLP) to high
Rate	Enter the maximum traffic rate, a value from 8 through 10^11 bits per second (bps).

i) Add preferred color group.

Choose the color preference and path prefernce for the primary, secondary, and tertiary colors.

Field	Description
Preferred Color Group Name	Enter a name for the preferred color group.
Color Preference	Choose the color preference from the drop-down list. You can choose multiple colors.
Path Preference	Choose the path preference from the drop-down list. The options are: • Direct Path • Multi Hop Path • All Paths

j) Add prefix list and prefix list IPv6.

Field	Description
Prefix List Name	Enter a name for the IPv4/IPv6 prefix list.
Add Prefix	Enter one or more IPv4/IPv6 prefixes separated by commas.

k) Add SLA class.

Field	Description
SLA Class List Name	Enter a name of the SLA class list.
Loss (%)	Enter the maximum packet loss on the connection, a value from 0 through 100.
Latency	Enter the maximum packet latency on the connection, a value from 1 through 1,000 milliseconds.
Jitter	Enter the maximum jitter on the connection, a value from 1 through 1,000 milliseconds.
App Probe Class	Choose the app probe class from the drop-down list or click **Create New** to create one.
Fallback Best Tunnel	Choose this option to enable the best tunnel criteria.

l) Add TLOC list.

Field	Description
List Name	Enter a name for the TLOC list.
TLOC IP	Specify the IP address for TLOC.
Color	Choose the color from the drop-down list.
Encapsulation	Choose the value from the drop-down list. The options are: • IPSec • GRE
Preference	Choose a preference to associate with the TLOC. The range is 0 to 4294967295.

Step 3 Click **Save**.

Policy validation for Cisco Catalyst SD-WAN

Policy validation in Cisco Catalyst SD-WAN is a process that

- automatically checks if your policies are accurate,

- ensures that policies comply with platform capabilities, and
- confirms that policies align with your network requirements.

This process helps verify that all configurations operate within supported limits before deployment.

Key features of policy validation

Centralized policy checks: From Cisco IOS XE Catalyst SD-WAN Release 26.1.1 policy validation is centrally managed, enabling quicker error detection and ensuring configurations remain within supported limits.

Enhanced device alerts: Devices send detailed alerts to Cisco SD-WAN Manager for proactive monitoring.

Filters in a sequence: Each policy sequence supports up to 64 filters, giving you flexibility to define granular traffic matching criteria.

Entries in a list: You can create and modify lists with a combined total of up to 8192 entries including existing and new entries to ensure scalability for complex network requirements.

Key terms for policy validation

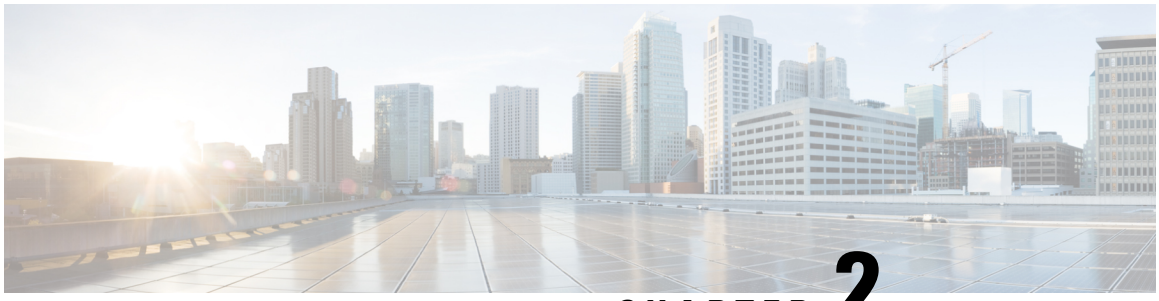
Key terms for policy validation are:

- **Application list**: An application list is a collection of applications grouped together for policy matching, allowing you to apply policies to multiple applications at once.
- **Application family**: An application family refers to a category of related applications such as Cisco Webex, Microsoft Teams, and Zoom. Application categories simplify policy management and enforcement.

Troubleshooting policy group validations

When you activate or deactivate a centralized policy or deploy a controller template, some controller-related policies associated in policy groups are deployed to prevent any errors in policy. You can avoid these validation errors using any one of the following workarounds:

- Dissociate application priority and SLA policy from any of the policy groups that have devices associated.
- Dissociate devices from any policy group that has application priority and SLA policy.
- Fix the issues in the application priority and SLA policy (In this case, you need to associate the device to a configuration group that has the selected VPNs).



CHAPTER 2

Application Priority and SLA

- Feature history for policy groups, on page 13
- Application Priority and SLA, on page 13
- Create an application priority and SLA policy, on page 14
- Configure traffic policy, on page 16
- Advanced layout, on page 17
- Policy sequence generation for match and action rules, on page 19
- Monitor traffic flow, on page 28

Feature history for policy groups

Table 3: Feature history

Feature Name	Release Information	Description
Configure Traffic and Flow Visibility for Application Priority and SLA Policy	Cisco IOS XE Catalyst SD-WAN Release 17.13.1a Cisco Catalyst SD-WAN Manager Release 20.13.1	You can configure settings to enable traffic and flow visibility for the application priority and SLA policy in Cisco Catalyst SD-WAN. This feature allows you to monitor application and traffic flow over IPv4, IPv6, or both networks at the global hierarchy level in Cisco SD-WAN Manager.
Preferred Remote Color in AAR Policy	Cisco IOS XE Catalyst SD-WAN Release 17.15.1a Cisco Catalyst SD-WAN Manager Release 20.15.1	You can set a remote preferred color in the AAR policy to control traffic routing based on the SLA criteria.

Application Priority and SLA

An application priority and SLA policy is a traffic policy group that

- configures app route policy, data policy, and QoS Map policies,

- routes and prioritizes traffic for best performance, and
- manages and customizes bandwidth allocations while prioritizing applications based on their relevance to your business.

Create an application priority and SLA policy

Follow these steps to create or edit an application priority and sLA policy.

Procedure

Step 1 Click + **Application priority & SLA policy**.l

Step 2 To edit an existing policy, click the ellipsis icon next to the policy under **Action**, and then click **Edit**.

Step 3 Choose one of these business relevance categories:

- **Gold** (Business-relevant): Likely to be important for business operations, for example, WebEx software.
- **Silver** (Default): No determination of relevance to business operations.
- **Bronze** (Business-irrelevant): Unlikely to be important for business operations, for example, gaming software.

Within each business relevance category, the workflow groups applications into application lists, such as broadcast video, multimedia conferencing, and VoIP telephony.

Note
When you upgrade Cisco SD-WAN Manager, built-in protocol pack gets updated. This might affect the existing policy groups which are using the Application priority and SLA policy in the non-advanced layout. You need to redeploy the policies when there is an upgrade. If policy is in the advanced layout, the upgrade will not affect the policy group.

Table 4: Fabric traffic policy

Field	Description
Preferred Path	To configure a preferred path, choose one or more colors of the data plane tunnel or tunnels from the drop-down list. Traffic is load-balanced across all the tunnels. If no tunnels match the SLA, data traffic is sent through any available tunnel. The preferences apply in order of priority to determine the path or color for forwarding traffic.
When SLA not met	Choose **Strict/Drop** to perform strict matching of the SLA class. If no data plane tunnel is available that satisfies the SLA criteria, traffic is dropped. Choose **Fallback to best path** to configure the best available tunnel to avoid a packet drop. This is the default. **Backup Path** : Path for traffic to use if the primary path fails.

Field	Description
Backup Path	To configure an alternate path for traffic flow, choose a path from the drop-down list.
Traffic Filtering	Click **Edit** to view and update app classification based on the business relevance. Choose a service provider class option and drag and drop the applications into different classes such as Gold or Bronze and click **Save** to update the configuration.
SLA	Add the SLA class in the traffic policy. Click **Edit** to configure the SLA class by adjusting the values for Loss (%), Latency (ms), or Jitter (ms) for the traffic policy.
QoS Queues	Click **Add QoS Policy** to add a QoS queue. Click **Edit** to configure the QoS Queues. Choose one of the following values for the QoS queuing model: • **4 Queues** • **5 Queues** • **6 Queues** • **8 Queues**

Table 5: Internet Offload Traffic

Field	Description
Secure Internet Gateway	Choose an application or application family list to tunnel traffic through a Secure Internet Gateway. Enable **Fallback to routing** for traffic to undergo normal routing if the SIG tunnels are down. Starting from Cisco Catalyst SD-WAN Manager Release 20.18.1 , you can choose a Cloud OnRamp for SaaS-capable application (Cloud OnRamp for SaaS applications with common user defined endpoints) from the **Secure Internet Gateway** dropdown.
Direct Internet Access	Select an application or application family list to allow direct internet access. Enable **Fallback to routing** for traffic to undergo normal routing if Direct Internet Access (DIA) is not available. Starting from Cisco Catalyst SD-WAN Manager Release 20.18.1 , you can choose a Cloud OnRamp for SaaS-capable application (Cloud OnRamp for SaaS applications with common user defined endpoints) from the **Direct Internet Access** dropdown.

Table 6: Apply Policy

Field	Description

Target	Configure the following parameters:
	• **Direction** : Choose the direction for applying the policy:
	  • **All** : Bidirection traffic flow
	  • **Service** : Incoming traffic from service.
	  • **Tunnel** : Incoming traffic from the tunnel.
	• **VPN** : Choose a target VPN from the drop-down list.
	• **Interface** : Specify a value or a variable for the Ethernet interface or DSL PPPoE interface type for applying the QoS policy.

Configure traffic policy

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Policy Groups** > **Application priority and SLA**.

Step 2 Click + **Application priority & SLA policy** to create a policy or edit an existing policy by clicking the ellipsis icon.

Step 3 Click the **Advanced** button on the top-right corner of the window to swtich to the advanced view.

Note
If you make changes to the application priority and SLA policies and switch to the advanced layout, the changes are retained. You cannot switch back to the default view.

Step 4 Click + **Add Traffic Policy** to configure the traffic policy.

Table 7: Add Traffic Policy

Field	Description
Policy Name	Specify a name for the traffic-rule sequence. From Cisco IOS XE Catalyst SD-WAN Release 26.2.1, the maximum length of the policy name is 128 characters. Cisco SD-WAN Manager UI and API validation reject values longer than 128 characters.
VPN	Choose a VPN from the drop-down list.

Field	Description
Direction	• Choose the direction for applying the policy: • **All** : Bidirectional traffic flow • **Service** : Incoming traffic from service • **Tunnel** : Incoming traffic from tunnel

Step 5 Click + **Add rules** to configure rules.

Table 8: Add Rules

Field	Description
Sequence	The sequence number of the rule.
Name	Specify a name for the rule.
Protocol	Choose a protocol from the drop-down list: • **IPv4** • **IPv6** • **Both**
Match	Choose a value for the match condition from the available options. Refer to Match conditions, on page 20 table.
Action	Choose a value for the action to take if the policy matches, from the available options. Refer to Action conditions, on page 22 table.
Base Action	Choose one of the following base actions for the packets based on the rules: • **Accept** • **Drop**

To rearrange match–action pairs in the route policy, drag them to the desired position and click **Save Match and Actions**.

Advanced layout

The advanced view provides further options to configure the traffic policy along with rules, service level agreement (SLA) class, and QoS Map.

Note If you make changes to the application priority and SLA policies and switch to the advanced layout, the changes are retained. You cannot switch back to the default view.

Based on the values you configure in the workflow, a policy profile and the relevant policy objects are created in the back-end when the workflow is completed. Similarly, you can configure traffic filtering and rules by creating the match and action conditions of a policy. You can also configure the app route policy SLA class and create customized QoS queues.

The VPNs that you intend to use in policy group must be present in service or transport profile of configuration group.

You can identify the VPNs when you configure VPNs using configuration groups as VPNs are identified with VPN name. Where as, when you configure VPNs from CLI template, VPNs are identified by VPN IDs. Hence, you cannot read the VPNs in policy groups when they are configured in CLI.

Configure SLA class

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Policy Groups** > **Application Priority & SLA**.

Step 2 Create or edit an existing application priority and SLA policy and select **Advanced Mode**.

Step 3 Create a traffic policy to add your first SLA class in traffic policy.

Select the base action as **Accept**. Click **Add action** and select **SLA class**. Refer to Action conditions, on page 22.

Table 9: SLA Class Components

Parameter	Description
jitter *milliseconds*	The maximum jitter on the connection Range: 1–1000 milliseconds
latency *milliseconds*	The maximum packet latency on the connection Range: 1–1000 milliseconds
loss *percentage*	The maximum packet loss on the connection Range: 1–100 percent

Starting from Cisco IOS XE Catalyst SD-WAN Release 17.14.1a , the SLA class loss, latency, and jitter values are as follows:

- Default values: Loss 5%, latency 500 ms, jitter 500 ms
- Business relevant values: Loss 2%, latency 300 ms, jitter 60 ms
- Business irrelevant values: Loss 10%, latency 600 ms, jitter 600 ms
- Bulk data values: Loss 5%, latency 500 ms, jitter 500 ms

Step 4 Click **Save match and actions**.

Configure QoS policy

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Policy Groups** > **Application Priority & SLA**.

Step 2 Create or edit an existing application priority and SLA policy and select **Advanced Mode**.

Step 3 From the left pane, click **QoS queue**, and then click **Add QoS policy**.

Table 10: QoS Queue

Field	Description
Queuing Model	Choose a value from the drop-down list for the queuing model.
Policy Name	Provide a name for the policy.
Interface	Specify a value for the interface.
Forwarding class	Choose a value for the forwarding class from the drop-down list.
Bandwidth %	Specify the maximum bandwidth. The range is 1–99.
Drops	Choose a value for the drop type from the following options: • **Random Early** • **Tail**
Scheduling type	Specify how to prioritize data packets for transmission to the destination by configuring the schedule type. The default is Weighted Round Robin (WRR).

Step 4 Click **Save**.

Policy sequence generation for match and action rules

The workflow generates data policy and app-route policy sequences based on the match and action conditions configured in a traffic rule. The following rules apply:

- A data policy sequence is generated when the rule includes a data match condition, a data action, or both. If no match condition is configured but a data action is configured, the workflow also generates a data policy sequence.

- An app-route policy sequence is generated when the rule includes an app-route match condition, an app-route action, or both. The workflow also generates an app-route policy sequence for a common-only sequence if a data policy sequence is not already generated for that sequence.
- If the rule includes only the Cloud Monitoring action, the workflow drops the sequence. If the Cloud Monitoring action is configured with other actions, the workflow evaluates the sequence according to the data policy and app-route policy sequence generation rules.
- If both the match and action conditions are empty, the workflow generates an empty data policy sequence.
- For the Cloud OnRamp for SaaS excluded data prefix use case, if the rule includes an application list and either a destination data prefix list or destination IP address with the count action, the workflow also generates an app-route policy sequence.

Match conditions

Table 11: Match parameters - data policy and app-route policy

Match Condition	Description
Omit	Match all packets.
(Applicable only to app-route policy) **Cloud Saas Application List**	Cisco SD-WAN Manager provides a list of several cloud applications that Cisco Catalyst SD-WAN Cloud OnRamp for SaaS can use to determine the best path selection for each SaaS application. For more information on Cisco Catalyst SD-WAN Cloud OnRamp for SaaS, see the *Cisco Catalyst SD-WAN Cloud OnRamp Configuration Guide, Cisco IOS XE Release 17.x*. **Note** **Cloud Saas Application List** displays as a match condition if you specify **IPv4** as the **Protocol** option. In the drop-down list, choose a SaaS application from the drop-down list.
(Applicable only to data policy) **Packet length**	Specifies the packet length. The range is 0 through 65535; specify a single length, a list of lengths (with numbers separated by a space), or a range of lengths (with the two numbers separated with a hyphen [-]).
(Applicable only to data policy) **TCP Flag**	Specifies the TCP flag, syn.
Applications/Application Family List	Applications or application families. This match condition is available for IPv6 traffic from Cisco IOS XE Release 17.9.1a and Cisco vManage Release 20.9.1.
Destination Data Prefix	Group of destination prefixes, IP prefix and prefix length. The range is 0 through 65535; specify a single port number, a list of port numbers (with numbers separated by a space), or a range of port numbers (with the two numbers separated with a hyphen [-]).
Destination Port	Enter the port number. Specify a single port number, a list of port numbers (with numbers separated by a space), or a range of port numbers (with the two numbers separated with a hyphen [-]).

Match Condition	Description
Destination Region	Choose one of the following: • **Primary**: Match traffic if the destination device is in the same primary region (also called access region) as the source. This traffic reaches the destination using a multi-hop path, through the core region. • **Secondary**: Match traffic if the destination device is not in the same primary region as the source but is within the same secondary region as the source. This traffic can reach the destination using a direct tunnel, as described for secondary regions. • **Other**: Match traffic if the destination device is not in the same primary region or secondary region as the source. This traffic requires a multi-hop path from the source to the destination. **Note** Minimum releases: Cisco vManage Release 20.9.1, Cisco IOS XE Catalyst SD-WAN Release 17.9.1a
DNS	Specify the direction in which to process DNS packets. To process DNS requests sent by the applications (for outbound DNS queries), specify **dns request**. To process DNS responses returned from DNS servers to the applications, specify **dns response**.
DNS Application List	Enables split DNS, to resolve and process DNS requests and responses on an application-by-application basis. Name of an **app-list** list . This list specifies the applications whose DNS requests are processed. This match condition is available for IPv6 traffic from Cisco IOS XE Release 17.9.1a and Cisco vManage Release 20.9.1.
DSCP	Specifies the DSCP value.
ICMP Message	For Protocol IPv4 when you enter a Protocol value as 1, the **ICMP Message** field displays where you can select an ICMP message to apply to the data policy. Likewise, the **ICMP Message** field displays for Protocol IPv6 when you enter a Protocol value as 58. When you select Protocol as Both, the **ICMP Message or ICMPv6 Message** field displays. **Note** This field is available from Cisco IOS XE Release 17.4.1, Cisco vManage Release 20.4.1.
Packet Loss Priority (PLP)	Specifies the packet loss priority. By default, packets have a PLP value of **low**. To set the PLP value to **high**, apply a policer that includes the **exceed remark** option.
Protocol	Specifies Internet protocol number. The range is 0 through 255.
Source Data Prefix	Specifies the group of source prefixes or an individual source prefix.
Source Port	Specifies the source port number. The range is 0 through 65535; specify a single port number, a list of port numbers (with numbers separated by a space), or a range of port numbers (with the two numbers separated with a hyphen [-]).

Match Condition	Description
Traffic To	In a Multi-Region Fabric architecture, match border router traffic flowing to the access region that the border router is serving, the core region, or a service VPN. **Note** Minimum release: Cisco vManage Release 20.8.1

Action conditions

In the action, you first specify whether to accept or drop a matching data packet, and whether to count it:

Table 12: Action conditions - data policy and app-route policy

Action Condition	Description
Click **Accept**	Accepts the packet. An accepted packet is eligible to be modified by the additional parameters configured in the action portion of the policy configuration.
Click **Drop**	Discards the packet. This is the default action. When you choose this option, then only **Counter** and **Log** can be added as additional actions and all other actions are not available to select. From Cisco IOS XE Catalyst SD-WAN Release 26.2.1, IPv6 high-priority traffic follows the same behavior as IPv4 high-priority traffic. High-priority traffic is skipped by policy processing and is not dropped by a policy sequence, even when the default action is set to Drop. This behavior applies only to packets consumed by the local router. If the packets are forwarded to another device, policy processing still applies.
Counter	Counts the accepted or dropped packets. Specifies the name of a counter. Use the **show policy access-lists counters** command on the Cisco IOS XE Catalyst SD-WAN device.
Log	Minimum release: Cisco IOS XE Catalyst SD-WAN Release 17.11.1a and Cisco vManage Release 20.11.1 Click **Log** to enable logging. When (DP, AAR or ACL) data policy packets are configured with log action, logs generated and logged to syslog. Due to the global **log-rate-limit**, not all logs are logged. A syslog message is generated the first time a packet header is logged and then every 5 minutes thereafter, as long as the flow is active. For information on **policy log-rate-limit** CLI, see **policy log-rate-limit** command in the Cisco Catalyst SD-WAN Qualified Command Reference Guide.
(Applicable only to app-route policy) **Cloud SLA**	**Cloud SLA** enables traffic to use the best path selection with Cisco Catalyst SD-WAN Cloud OnRamp for SaaS. Click **Cloud SLA**.

Action Condition	Description
(Applicable only to app-route policy) **SLA Class List**	

Action Condition	Description
	Choose from the following options: **1. SLA Class List** Set the policy action for an **SLA Class List** match condition. For the SLA class, all matching data traffic is directed to a tunnel whose performance matches the SLA parameters defined in the class. The device first tries to send the traffic through a tunnel that matches the SLA. If a single tunnel matches the SLA, data traffic is sent through that tunnel. If two or more tunnels match, traffic is distributed among them. If no tunnel matches the SLA, data traffic is sent through one of the available tunnels. Click **SLA Class List**. In the **SLA Class** drop-down list, choose one or more SLA classes. **2. Preferred Color** In the **Preferred Color** drop-down list, choose the color of the data plane tunnel or tunnels to prefer. Traffic is load-balanced across all the tunnels. If no tunnels match the SLA, data traffic is sent through any available tunnel. That is, color preference is a loose matching, not a strict matching. **3. Preferred Color Group** When the **Preferred Color** is not selected, you can choose the preferered color group from the **Preferred Color Group** drop-down list. Select the preferred color group of the data plane tunnel or tunnels to prefer. You can configure up to three levels of priority based on the color or path preference. This field is available from Cisco IOS XE Catalyst SD-WAN Release 17.9.1a and Cisco vManage Release 20.9.1. **4. Restrict to Preferred Color** This option is appicable only with **Preferred Color Group**. Check the **Restrict to Preferred Color** option to drop traffic if no tunnels match the SLA in the prefered color group. **5.** When there is no SLA match you can choose the following options: **a. Strict/Drop** Click **Strict/Drop** to perform strict matching of the SLA class. If no data plane tunnel is available that satisfies the SLA criteria, traffic is dropped. **b. Fallback to best path** Click **Fallback to best path** to select the best available tunnel to avoid a packet drop. You can select the **Fallback to best path** action only when the **Fallback Best Tunnel** option is enabled while defining a SLA class. If the **Fallback Best Tunnel** option is not enabled, then

Action Condition	Description

	the following error message displays in Cisco SD-WAN Manager:
	`SLA Class selected, does not have Fallback Best Tunnel enabled.`
	`Please change the SLA class or change to Strict/Drop.`
	c. Load-balance.
	Click **Load Balance** to load balance traffic across all the tunnels.
	You can now select the **Backup SLA Preferred Color**.
	Set the policy action for a **Backup SLA Preferred Color** match condition. When no tunnel matches the SLA, direct the data traffic to a specific tunnel. Data traffic is sent out the configured tunnel if that tunnel interface is available. If that tunnel interface is not available, traffic is sent out to another available tunnel. You can specify one or more colors. The backup SLA preferred color is a loose matching condition, not a strict matching condition.
	6. Remote Preferred Color
	Set a **Remote Preferred Color** in the AAR policy to control traffic routing based on the application list. You can add multiple remote preferred colors in the AAR policy.
	Use the **Restrict to Remote Color** to restrict the tunnel to preferred TLOCs. With **Restrict to Remote Color** option, the traffic drops when the SLA is not met with the preferred remote color.

(Applicable only to data policy) **Cflowd**	Enables cflowd traffic monitoring.
(Applicable only to data policy) **DSCP**	DSCP value. The range is 0 through 63.
(Applicable only to data policy) **Forwarding Class**	Name of the forwarding class.
(Applicable only to data policy) **Local TLOC**	Enables sending packets to one of the TLOCs that matches the color and encapsulation. The available colors are: 3g, biz-internet, blue, bronze, custom1,custom2, custom3, default, gold, green, lte, metro-ethernet, mpls, private1 through private6, public-internet, red and silver. The encapsulation options are: **ipsec** and **gre**. By default, if the TLOC is not available, traffic is forwarded using an alternate TLOC. To drop traffic if a TLOC is unavailable, include the **restrict** option. By default, encapsulation is **ipsec**.

Action Condition	Description
(Applicable only to data policy) **NAT Pool** or **NAT VPN**	Enables NAT functionality, so that traffic can be redirected directly to the internet or other external destination. You can configure up to 31 (1–31) NAT pools per router.
(Applicable only to data policy) **Next Hop**	Sets the next hop IP address to which the packet should be forwarded. **Note** Starting from Cisco IOS XE Catalyst SD-WAN Release 17.5.1a and Cisco vManage Release 20.5.1, the **Use Default Route when Next Hop is not available** field is available next to the **Next Hop** action parameter. This option is available only when the sequence type is **Traffic Engineering** or **Custom**, and the protocol is either **IPv4** or **IPv6**, but not both.
(Applicable only to data policy) **Policer**	Applies a policer. Specifies the name of policer configured with the **policy policer** command.
(Applicable only to data policy) **Redirect DNS**	Redirects DNS requests to a particular DNS server or Umbrella. Redirecting requests is optional, but if you do so, you must specify both actions. For an inbound policy, **redirect-dns host** allows the DNS response to be correctly forwarded back to the requesting service VPN. For an outbound policy, specify the IP address of the DNS server. **redirect-dns umbrella** is only supported in Direct Internet Interface (DIA) use cases. It is not supported in SIG/SSE or overlay scenarios. When using **redirect-dns umbrella**, you do not need to explicitly configure **nat use-vpn 0**. **Note** When you upgrade to releases later than Cisco IOS XE Catalyst SD-WAN Release 17.7.1a, you must configure redirect DNS through **nat use-vpn 0** to redirect DNS to Direct Internet Interface (DIA). **Note** You can set only local TLOC preferences with redirect-dns as actions on the same sequence, but not remote TLOC. **Note** You cannot configure Redirect DNS and SIG at the same time. NAT DIA fallback and redirect-dns IP actions are supported at the same time in data policy beginning with Cisco IOS XE Catalyst SD-WAN Release 26.1.1.

Action Condition	Description
(Applicable only to data policy) **Remote Preferred Color**	Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.15.1a and Cisco Catalyst SD-WAN Manager Release 20.15.1 You can set a preferred remote color in the AAR policy to control traffic routing based on the application list. Use the **Restrict to Remote Color** option to drop traffic if the selected remote color does not meet the SLA.
(Applicable only to data policy) **Secure Internet Gateway**	Redirect application traffic to a SIG. **Note** Before you apply a data policy for redirecting application traffic to a SIG, you must have configured the SIG tunnels. For more information on configuring Automatic SIG tunnels, see Automatic Tunnels . For more information on configuring Manual SIG tunnels, see Manual Tunnels. Check the **Fallback to Routing** check box to route internet-bound traffic through the Cisco SD-WAN overlay when all SIG tunnels are down. This option is introduced in Cisco IOS XE Catalyst SD-WAN Release 17.8.1a and Cisco vManage Release 20.8.1.
(Applicable only to data policy) **Secure Service Edge**	Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.13.1a and Cisco Catalyst SD-WAN Manager Release 20.13.1 Redirect application traffic to a Secure Service Edge instance. For more information on configuring Automatic tunnels on Cisco Secure Access, see Automatic Tunnels . Check the **Fallback to Routing** check box to route internet-bound traffic through the Cisco SD-WAN overlay when all Secure Service Edge tunnels are down.
(Applicable only to data policy) **Service**	Specifies a service to redirect traffic to before delivering the traffic to its destination. The TLOC address or list of TLOCs identifies the remote TLOCs to which the traffic should be redirected to reach the service. In the case of multiple TLOCs, the traffic is load-balanced among them. The VPN identifier is where the service is located. Standard services: **FW**, **IDS**, **IDP** Custom services: **netsvc1**, **netsvc2**,**netsvc3**, **netsvc4** TLOC list is configured with a **policy lists tloc-list** list. Configure the services themselves on the Cisco IOS XE Catalyst SD-WAN devices that are collocated with the service devices, using the **vpn service** command.

Action Condition	Description
(Applicable only to data policy) **TLOC**	Direct traffic to a remote TLOC that matches the IP address, color, and encapsulation of one of the TLOCs in the list. If a preference value is configured for the matching TLOC, that value is assigned to the traffic.
(Applicable only to data policy) **VPN**.	Set the VPN that the packet is part of. Range: 1 to 65525, excluding 512. For details see the VRF range behavior change described here.

Monitor traffic flow

To enable traffic flow monitoring while configuring an application priority & SLA policy configure the following values:

This feature provides options to monitor traffic flow on incoming packets in the LAN for application and flow visibility over IPv4, IPv6, or both network addresses.

Note The Cflowd configuration applies to the global level and not the site level.

The additional settings that you configure are applied to the Cisco SD-WAN Controllers while deploying the application priority and SLA policy. For more information about configuring Cflowd, refer to Configure Cflowd section in *Cisco Catalyst SD-WAN Network Hierarchy Configuration Guide*.

Before you begin

- Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.13.1a , Cisco Catalyst SD-WAN Manager Release 20.13.1.
- Ensure that you have configured Cflowd collector details in the Cisco SD-WAN Manager menu from **Configuration** > **Network Hierarchy** > **Collectors** > **Cflowd**.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Policy Groups** > **Application Priority & SLA**.

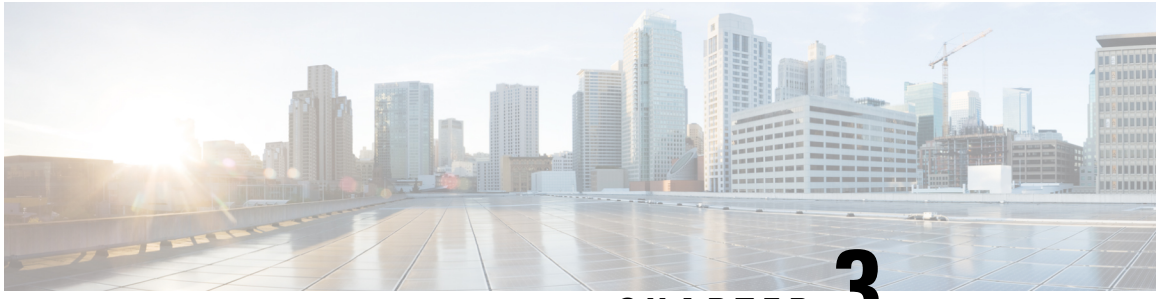
Step 2 Create or edit an existing application priority and SLA policy.

Step 3 Click **Additional settings**.

Table 13: Additional Settings

Field	Description
Application Visibility	Monitor all the applications running in all VPNs over IPv4, IPv6, or both networks in the LAN.
Flow Visibility	Monitor traffic flow over IPv4, IPv6, or both network addresses in the LAN.

Step 4 Click **Save**.



CHAPTER 3

Next-Generation Firewall (NGFW)

- Feature history of NGFW, on page 31
- NGFW, on page 33
- Enable RBAC for NGFW policy, on page 33
- Restrictions for NGFW policy, on page 34
- Configure NGFW policy using a workflow, on page 35
- Configure policy objects for an NGFW policy, on page 50

Feature history of NGFW

Table 14: Feature history

Feature Name	Release Information	Description
Security Policy Using Policy Groups	Cisco IOS XE Catalyst SD-WAN Release 17.12.1a Cisco Catalyst SD-WAN Manager Release 20.12.1	This feature provides a simple, reusable, and structured approach for configuring security policies in Cisco Catalyst SD-WAN. You can create a security policy, that is, a logical grouping of policies that is applied to one or more sites or a single device at a site in the network. To deploy the policy group to devices, the devices must be managed by a configuration group in Cisco Catalyst SD-WAN. The Deploy Policy Group workflow provides a guided method to choose previously created policy groups and deploy them to sites or a single device at a site that is managed by configuration groups.
Add Source Interface for High-Speed Logging and External Syslog	Cisco IOS XE Catalyst SD-WAN Release 17.16.1a Cisco Catalyst SD-WAN Manager Release 20.16.1	This enhancement for security logging allows you to specify the following in the additional settings of the security policy: • Source interfaces for high-speed logging (HSL) servers (up to four) • Source interface for the external syslog server

Feature Name	Release Information	Description
Enhancements to Security Policy Using Policy Groups	Cisco IOS XE Catalyst SD-WAN Release 17.15.2 Cisco Catalyst SD-WAN Manager Release 20.15.2 Cisco IOS XE Catalyst SD-WAN Release 17.16.1a Cisco Catalyst SD-WAN Manager Release 20.16.1	The following enhancements are introduced with this release: • **Embedded Security** is called **NGFW** in Cisco SD-WAN Manager. • Create copies of security policy and sub-policy. • View all configured rules for specific policies in the **NGFW** policy dashboard. • For each rule, **Clone rule**, **Add rule on top**, and **Add rule below** options are added.
Version Management for Security Policy	Cisco Catalyst SD-WAN Manager Release 20.18.1	With this feature you can track and manage changes to your security policies using the version history.
IPv6 Rule and Rule Set Support in Security Policies	Cisco IOS XE Catalyst SD-WAN Release 17.18.2 Cisco Catalyst SD-WAN Manager Release 20.18.2	You can configure IPv6 data prefix lists, rule with rule sets, and object groups in security policy using Cisco SD-WAN Manager.
Enhancements for NGFW in Policy Groups	Cisco IOS XE Catalyst SD-WAN Release 26.1.1 Cisco Catalyst SD-WAN Manager Release 26.1.1.1	The following enhancements are introduced with this release: • Import and export of the firewall policies. • Display rule hit count. • Drag and drop rules in a policy to update the priority. • Display policy and object usage reference in the NGFW policy dashboard. • Rule and policy name retention in the running CLI configuration.
Increase in FQDN Scale	Cisco IOS XE Catalyst SD-WAN Release 26.1.1 Cisco Catalyst SD-WAN Manager Release 26.1.1.1	With this feature the FQDN entries are increased to 256.

Feature Name	Release Information	Description
Discontiguous Subnet Mask Support for IPv4 Network Object Groups	Cisco IOS XE Catalyst SD-WAN Release 26.2.1 Cisco Catalyst SD-WAN Manager Release 26.2.1	Adds support for discontiguous subnet mask entries in IPv4 data prefixes and IPv4 network object groups used by NGFW Policy. You can use discontiguous subnet mask entries in IPv4 source and destination match conditions, rule sets, object groups, and data prefix variables.

NGFW

An NGFW policy is a configuration mechanism that

- simplifies the experience of configuring and deploying policies on Cisco IOS XE Catalyst SD-WAN devices using policy groups, and
- uses a workflow to configure policies and associate them with devices in the network.

Enable RBAC for NGFW policy

Follow these steps to enable RBAC for NGFW policy:

To create a policy group and security feature profiles using configuration groups, role-based access control (RBAC) must provide read and write permissions on the following profiles to access each feature. Set the permissions of the user group to enable access to policy groups from **Configuration** > **Policy Groups**.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Administration** > **Manage Users** > **User Groups**.

Step 2 Click **Add User Group**.

Step 3 Enter **User Group Name**.

Step 4 Check a **Read** or **Write** check box for the **Policy Group**, **Device** and **Deploy** feature that you want to assign to a user group.

Step 5 Check a **Read** or **Write** check box for the following features that you want to assign to a user group:

- **Feature Profile** > **DNS Security** > **DNS Policy**
- **Feature Profile** > **Sig Security** > **Sig Policy**
- **Feature Profile** > **NGFW** > **Legacy Policy**
- **Feature Profile** > **NGFW** > **NGFirewall**
- **Feature Profile** > **NGFW** > **Policy**
- **Feature Profile** > **Policy Object** > **Advanced Inspection Profile**

  The **Advanced Inspection Profile** has the following subfeature profiles:

- Advanced Malware Protection
- Intrusion Prevention
- SSL Decryption
- SSL Decryption Profile
- URL Filtering

Step 6 Click **Add**.

Restrictions for NGFW policy

IPv6 rules or rulesets

IPv6 rules or rulesets do not support identity.

IPv4 rules with rulesets

Only IPv4 rules with an NGFW policy support Identity. IPv4 rules with rulesets are not supported.

Matching traffic, custom application in a custom-defined application list

From Cisco IOS XE Catalyst SD-WAN Release 17.14.1a and Cisco Catalyst SD-WAN Manager Release 20.14.1, security policy supports matching traffic using a custom application in a custom-defined application list. In earlier releases, this is not supported.

VPNs or interfaces not present on the target device

When a security policy was deployed with zones configured to include specific VPNs or interfaces, the system would gracefully handle situations where some of these VPNs or interfaces were not present on the target device. SD-WAN Manager automatically filters out the non-existent VPNs or interfaces before pushing the configuration, allowing the policy to deploy successfully to the device for the available elements.

For policy groups, this behavior has changed. The system now strictly mandates the presence of all VPNs and interfaces specified within a zone configuration on the target device. If any configured VPN or interface is missing on the device, the security policy deployment will fail, requiring the user to ensure all referenced VPNs and interfaces exist on the device before deployment.

Example:

Consider a zone named zoneA configured to include vlan10, gigabitethernet20, and vlan1.

For security policy: If the target device only had vlan10 configured, SD-WAN Manager would filter out gigabitethernet20 and vlan1, and the policy would successfully deploy for vlan10.

For policy groups: If the target device only has vlan10, the deployment of the security policy will now fail because gigabitethernet20 and vlan1 are mandated but not present on the device.

Replacing a SIG or SSE feature policy

Replacing a SIG or SSE feature policy within the same policy group is not supported.

Data policy redirecting DNS traffic

Data policy does not support both of these conditions together:

- Data policy redirecting DNS traffic to Umbrella
- Secure Internet Gateway (SIG) configured

NGFW configurations using CLI add-on template

Ensure proper NGFW block configuration:

- Ensure that the NGFW block is moved to the end of the CLI template.
- Ensure the NGFW block is closed using the **exit** command instead of **!**.

Discontiguous subnet masks in IPv4 network object-group

A discontiguous subnet mask is used to identify which bits of an IPv4 address must be matched. A bit value of 0 indicates that the corresponding address bit is ignored, and a bit value of 1 indicates that the corresponding address bit must match.

- Discontiguous subnet mask support is applicable only to NGFW policies.
- Discontiguous subnet mask support is limited to IPv4 data prefixes and IPv4 network object groups.
- Discontiguous subnet mask support is not applicable to app-route policies or data policies.
- SD-WAN Manager supports a maximum of five discontiguous entries in an IPv4 data prefix or IPv4 network object group configured through policy objects.

  This limit is not enforced by the device. Therefore, you can use CLI add-on template to configure more than five discontiguous entries. Cisco recommends using no more than five discontiguous entries to ensure consistent behavior across SD-WAN Manager workflows.

  During policy download, attach and edit operations, the device also enforces a maximum of five discontiguous entries per IPv4 network object-group.

Configure NGFW policy using a workflow

Follow these steps to configure NGFW policy using a policy group:

Using the **Create NGFW Policy** workflow, you can create a security policy, add sub-policy, add rules to existing sub-policies, and so on.

In Cisco Catalyst SD-WAN Manager Release 20.15.1 and earlier releases, **Create NGFW Policy** is called **Create Security Policy**.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Workflows** > **Workflow Library** > **Create Security Policy** > **Create NGFW Policy**. Alternatively, choose **Configuration** > **Policy Groups**.

Step 2 Click **NGFW**.

In Cisco Catalyst SD-WAN Manager Release 20.15.1 and earlier releases, **NGFW** is called **Embedded Security**.

Step 3 On the **NGFW** page, click **Add NGFW Policy**.

This launches the NGFW policy workflow.

Step 4 Enter **Policy Name** and **Description** and click **Next**.

Step 5 On the **Select the optional Configuration Group to associate with the NGFW policy** page, choose the configuration groups and click **Next**.

Step 6 Click **Add Sub-Policy**.

Refer to the steps used in the procedure, Configure an NGFW Sub-Policy, on page 42.

Step 7 Click **Submit**.

Edit NGFW policy

In Cisco Catalyst SD-WAN Manager Release 20.15.1 and earlier releases, **NGFW** is called **Embedded Security**.

For more information on NGFW, see Enterprise Firewall with Application Awareness.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Policy Groups** > **NGFW**.

Step 2 Choose an NGFW policy and click **Edit**.

Step 3 (Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.18.2) Click **Add Rule** or **Rule with Rule Sets**.

From Cisco IOS XE Catalyst SD-WAN Release 26.1.1, you can drag and drop rules in a policy to modify the priority or sequence number of each rule.

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

Field	Description
Destination Zone	In the **Destination Zone** drop-down list, choose the zone to which data traffic is sent. The options are: • No-Zone • Corporate_Users • Local_Internet_for_Guests • Payment_Processing_Network • Physical_Security_Devices • Self • Untrusted Zones are created based on the VPNs in the configuration group selected in the create security policy workflow.

Field	Description
Match (Rule)	

Field	Description

	Match Conditions
	You can choose the desired match conditions for a rule from the **Add Conditions** drop-down list. Available options include:
	• Type
	  • IPv4
	  • IPv6
	  You can configure IPv6 from Cisco Catalyst SD-WAN Manager Release 20.18.2
	• Applications
	• Protocol
	• Source
	  • Geo Location (Supported when the chosen type is IPV4
	  • IPv4 Prefix
	  From SD-WAN Manager 26.2.1, IPv4 prefixes support discontiguous subnet mask.
	  • Port
	• Destination
	  • FQDN
	  • Geo Location (Supported when the chosen type is IPV4
	  • IPv4 Prefix
	  From SD-WAN Manager 26.2.1, IPv4 prefixes support discontiguous subnet mask.
	  • Port
	When ISE is enabled, the SGT option becomes available for both **Source** and **Destination**.
	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**.
	From Cisco Catalyst SD-WAN Manager Release 20.18.2, you can create **Object Groups**. Object groups allow users to combine multiple objects into a single group for easier

Field	Description
	policy management. You can add or select an **Object Group** only after deselecting other items in the IPv4/IPv6 rule dropdown lists.

Field	Description

Match (Rule set)	**Match Conditions**
	From Cisco Catalyst SD-WAN Manager Release 20.18.2, you can choose the desired match conditions for a rule set from the **Add Conditions** drop-down list. Available options include:
	• Type
	  • IPv4
	  • IPv6
	• Protocol
	• Source
	  • Geo Location (Supported when the chosen type is IPV4
	  • IPv4 Prefix
	  From SD-WAN Manager 26.2.1, IPv4 prefixes support discontiguous subnet mask.
	  • Port
	• Destination
	  • FQDN
	  • Geo Location (Supported when the chosen type is IPv4)
	  • IPv4 Prefix
	  From SD-WAN Manager 26.2.1, IPv4 prefixes support discontiguous subnet mask.
	  • Port
	When adding conditions for **Source** or **Destination**, select an object created from **Objects and Profiles** or create new values or objects.
	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 for easier policy management.
	You can add an **Object Group** only when you deselect all other items in the drop-down list.

Field	Description
Action	Choose the desired action conditions. The options are: • Pass • Drop • Inspect • Log Events: Unified Logging for Inspect Action. Select **Advanced Inspection Profile** from the drop-down list.

Note
From Cisco Catalyst SD-WAN Manager Release 20.18.2 you can pre-configure Object Groups, Data Prefix IPv6, and Rule set under **Policy Groups** > **Object and Profiles** > **Security Objects** . Configured security objects appear as selectable options in the drop-down list when creating rules or rule sets.

Import and export policies

From Cisco IOS XE Catalyst SD-WAN Release 26.1.1 you can import or export the firewall policies. You can use Cisco SD-WAN Manager to 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 SD-WAN Manager validates the file and flags any errors.

Hit count

From Cisco IOS XE Catalyst SD-WAN Release 26.1.1 you can view the hit count of each rule within a sub-policy.

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.

Configure an NGFW Sub-Policy

In Cisco Catalyst SD-WAN Manager Release 20.15.1 and earlier releases, **NGFW** is called **Embedded Security**.

Procedure

Step 1 From the **Configuration** > **Policy Groups**, choose **NGFW**.

Step 2 Choose an NGFW policy from the list, click **...**. Select **Edit**.

Step 3 Click **Add Sub-Policy** to add sub-policies for a security policy and enter the required details.

Table 15: Sub-Policy configuration fields

Field	Description
VPN / Interface	Specify the VPN or the interface.
Source Zone	Choose the zone that is the source of the data packets.
Zone List Name	The name of a zone list.
VPN	Choose to configure zones with zone type as **VPN**. Add the VPNs to the zones from the drop-down list. The options are: • Payment Processing Network • Corporate Users • Local Internet for Guests • Physical Security Devices
Interface	Choose to configure zones with zone type as **Interface**. Add the interfaces to the zones from the **Add Interface** drop-down list.
Rule Name	The name of the rule.
Sequence	Specify the sequence.
Destination Zone	Choose the zone to which data traffic is sent. The options are: • Any • Corporate_Users • Local_Internet_for_Guests • Payment_Processing_Network • Physical_Security_Devices • Self • Untrusted (VPN 0)

Field	Description

Match	Choose the desired match conditions from the **Add Conditions** drop-down list. The options are:
	• Applications
	• Protocol
	• Source
	  • Geo Location
	  • IPv4 Prefix
	  • Port
	• Destination
	  • FQDN
	  • Geo Location
	  • IPv4 Prefix
	  • Port
	
	From SD-WAN Manager 26.2.1, IPv4 prefixes support discontiguous subnet mask.

Action	Choose the desired action conditions. The options are: • Pass • Drop • Inspect • Log Events - Unified Logging for Inspect Action. Select **Advanced Inspection Profile** from the drop-down list.
User / User Group	An identity service engine has to be enabled to configure **User / User Group** sub policies. You can configure using **Administration** > **Integration Management** > **Identity Service Engine**.

If you edit a NGFW sub-policy and disable any rule, the variables for match conditions are still shown during the deployment process. Since the rule is disabled, these values for the variables are not applicable to the device.

If the NGFW sub-policy with disabled rules is deployed on new devices, the variables are shown in the deployment process. Enter a placeholder values in order to proceed with the deployment.

Configure additional settings for an NGFW policy

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Policy Groups** , choose **NGFW**.

In Cisco Catalyst SD-WAN Manager Release 20.15.1 and earlier releases, **NGFW** is called **Embedded Security**.

Step 2 Choose an NGFW policy from the list and click **Edit**.

Step 3 Click **Additional Settings**.

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.
High Speed Logging Source Interface	Specify the server labels of the source interface used to collect logs for high-speed logging (HSL). You can configure up to four log collector servers for HSL. Ensure that you enable security logging before specifing the source interface. For more information, see Configure Security Logging .

Field	Description
SysLog Server Source Interface	Specify the server label of the source interface associated with the external syslog server to export UTD logs. Ensure that you enable security logging before specifing the source interface. For more information, see Configure Security Logging .

Step 4 Choose the profile from the **Advanced Inspection Profile** drop-down list or click **Create New** .

Field	Description
Profile Name	The name of the profile.
Description	The description of the profile.

a) Choose the intrusion prevention from the **Intrusion Prevention** drop-down list or click **Create New**.

Field	Description
Profile Name	The name of the profile. The name can have a maximum of 32 characters.
Signature Set	Specify the signature set. The options are: • Balanced • Connectivity • Security
Inspection Mode	Specify the inspection mode. The options are: • Detection • Protection
Advanced	
Customer Signature Set	Enable customer signature set to add a new global custom signature. In the **Add New Global Custom Signature** window, choose **Download From** the following options: • Remote Server • Local Server (Not Recommended)
Select an Signature Allow List	Select an allowed signature list or **Create New** to create a new IPS signature list.

Field	Description
Alert Log Level	Choose the alert log level: • Error • Emergency • Alert • Critical • Warning • Notice • Info • Debug

Click **Add**.

b) Choose a URL filter from the **URL Filter** drop-down list or **Create New**.

Field	Description
Profile Name	The name of the profile. The name can have a maximum of 32 characters.
Web Category	Choose the web category from the drop-down list. The options are: • Block • Allow
Select one or more web categories	Choose one or more web categories from the drop-down list. The options are: abortion, abused-drugs and so on.
Web Reputation	Choose the web reputation from the drop-down list. The reputation options are: • High Risk • Suspicious • Moderate Risk • Low Risk • Trustworthy
Advanced	
Select allow url list	Select an allowed URL list or **Create New** to create a new allow URL list.

Field	Description
Select block url list	Select a blocked URL list or **Create New** to create a new block URL list.
Block Page Server	Choose the block page server from the drop-down list. The options are: • Block Page Content • Redirect URL: Specify the redirect URL
Alerts And Logs	Choose one or more file type from the drop-down list: • Blocklist • Allowlist • Reputation/Category

Click **Add**.

c) Choose the advanced malware protection profile from the **Advanced Malware Protection** drop-down list or click **Create New**.

Field	Description
Profile Name	The name of the profile. The name can have a maximum of 32 characters.
Select AMP Cloud Region	Choose the AMP cloud region. The options are: • NAM • EU • APJC
Inspection Mode	Specify the inspection mode. The options are: • Detection • Protection
Alert Log Level	Choose the alert log level: • Critical • Warning • Info
File Analaysis	Enable file analysis.

Field	Description
Select TG Cloud Region	Choose the cloud region from the drop-down list. The options are: • NAM • EU
Alert Log Level	Choose the alert log level: • Critical • Warning • Info
Select one or more file types	Choose one or more file type from the drop-down list: • All • pdf • ms-exe • new-office • rtf • mdb • mscab • msole2 • wri • xlw • flv • swf

Click **Add** .

d) Choose **TLS Action**.

Field	Description
TLS Action	Choose the web category from the drop-down list. The options are: • Decrypt • Pass Through • Do not Decrypt

Field	Description
Select an TLS/SSL Decryption	Choose the TLS/SSL decryption profile from the drop-down list or **Create New** profile.

Step 5 Click **Save**.

Version control for NGFW

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.18.1a and Cisco Catalyst SD-WAN Manager Release 20.18.1

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Policy Groups**, choose **NGFW**.

Step 2 Choose a security policy from the list and click **Edit**.

Step 3 Click **Show version control** to track and manage changes to the security policy.

Step 4 Select two versions of the security policy and click **View diff** to view the changes made in these versions.

If you have added any configurations to the security policy, it is highlighted in green. If you have removed any configuration parameters, it is highlighted in red.

Visual diff for large policy configurations is not available. You can download the configuration using the **Download config** button and compare them manually.

Step 5 Click **Revert** next to a version if you wish to move back to an older version of the security policy configuration.

For large policies, create and revert operations can take upto two minutes.

Configure policy objects for an NGFW policy

Before you begin

To save time during policy configuration and deployment, we recommend you to create single policy objects for Data Prefix, Geo Location, FQDN, Port, Protocol, and reuse it in all the common places.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Policy Groups** > **Objects and Profiles** .

In SD-WAN Manager 20.18.1 and earlier releases, **Objects and Profiles** is called **Group of Interest**.

Step 2 Click **Security objects**. The list of security objects appears.

In SD-WAN Manager 20.18.1 and earlier releases, **Security objects** is called **Security**.

- Application lists

Field	Description
Application List Name	Name of the application list. **Note** See the information about custom applications in Restrictions for Security Policy.
Applications	Choose one or more application types from the drop-down list. For example, Third Party Control, ABC News, Microsoft Teams, and so on. Choose one or more application family types from the drop-down list. For example, application-service, audio_video, authentication, behavioral, compression, database, encrypted, and so on.

- Data Prefix

Field	Description
Data Prefix List Name	Name of the prefix list.
Data Prefix	The data prefix value.

From SD-WAN Manager 26.2.1, IPv4 data prefixes support discontiguous subnet mask values.

- Data Prefix IPv6

From Cisco SD-WAN Manager Release 20.18.2, you can configure data prefix IPv6.

Field	Description
Name	Name of the data prefix list.
Data Prefix IPv6	The data prefix IPv6 value.

- Rule set

From Cisco SD-WAN Manager Release 20.18.2, you can configure a rule set.

Field	Description
Rule Set name	Name of the rule set.
Type	You can choose IPv6 or IPv4.

From SD-WAN Manager 26.2.1, IPv4 data prefixes support discontiguous subnet mask values.

- Object group

From Cisco SD-WAN Manager Release 20.18.2, you can configure an object group.

Field	Description
Object Group Name	Name of the object group.
Description	Description of the object group
Type	You can choose IPv6 or IPv4. From SD-WAN Manager 26.2.1, IPv4 values support discontiguous subnet mask.

- Local Domain

Field	Description
Local Domain List Name	Name of the local domain list.
Local Domain	The local domain values separated by comma. For example, cisco.com.

- FQDN (Fully Qualified Domain Name)

  The FQDN is intended to be used for matching standalone servers in data centers or a private cloud. When matching public URLs, the recommended match action is **drop** . If you use **inspect** for public URLs, you must define all related sub URLs and redirect URLs.

  Table 16:

Field	Description
FQDN List Name	Name of the FQDN list.
FQDN	The URL names separated by comma. For example, cisco.com. From Cisco Catalyst SD-WAN Manager Release 26.1.1.1 , 256 FQDN entries are supported.

- Signature

  The signature set blocks vulnerability with a Common Vulnerability Scoring System (CVSS) score that is greater than or equal to 9. It also blocks Common Vulnerabilities and Exposures (CVEs) published in the last two years and that have the rule categories: Malware CNC, Exploit Kits, SQL Injection or blocked list.

Field	Description
IPS Signature List Name	Name of the IPS signature list.
IPS Signature	The signatures in the format `Generator ID:Signature ID` , separated with commas. For example, 1234:5678. Range is 0 to 4294967295

- URL allow

  List-based filtering allows the user to control access by permitting or denying access based on allowed or blocked lists. Here are some important points to note about these lists:

  - URLs that are allowed are not subjected to any category-based filtering.
  - If the same item is configured under both the allowed and blocked list, the traffic is allowed.

- If the traffic does not match either the allowed or blocked lists, then it is subjected to category-based and reputation-based filtering.

Field	Description
Allow URL List Name	Name of the Allow URL list.
Allow URL	The URLs to allow.

- URL block

  List-based filtering allows the user to control access by permitting or denying access based on allowed or blocked lists.

Field	Description
Block URL List Name	Name of the Block URL list.
Block URL	The URLs to block.

- Zone

Field	Description
Zone List Name	Name of the zone list.
VPN	Choose to configure zones with zone type as **VPN** . Add the VPNs to the zones from the drop-down list. The options are: • Payment Processing Network • Corporate Users • Local Internet for Guests • Physical Security Devices
Interface	Choose to configure zones with zone type as **Interface** . Add the interfaces to the zones from the **Add Interface** drop-down list. The options are: • Ethernet • FastEthernet • FiveGigabitEthernet • FortyGigabitEthernet • GigabitEthernet • HundredGigE

- Port

Field	Description
Port List Name	Name of the port list.
Port	The port values separated by comma. The range is 0 to 65530.

- Protocol

Field	Description
Protocol List Name	Name of the protocol list.
Protocols	Select one or more protocol names from the drop-down list. For example, snmp, tcp, udp, icmp, echo, telnet, and so on.

- Geo Location

Field	Description
Geo Location List Name	Name of the geolocation list.
Geo Location	Select one or more geo locations from the drop-down list. For example, Africa, Antartic, Asia, Europe, and so on.

Step 3 Click **Security profiles** tab. The list of security profiles appears.

- Advanced inspection profile

Field	Description
Profile Name	Name of the advanced inspection profile.
Description	The description of the profile.
Select an Intrusion Prevention	Choose an intrusion prevention option from the drop-down list.
Select an URL Filter	Choose a URL filter from the drop-down list.
Select an Advanced Malware Protection	Choose an advanced malware protection.
TLS Action	Choose the TLS action. The options are: • Decrypt • Pass Through • Do not Decrypt

- Intrusion prevention

Field	Description
Profile Name	Name of the intrusion prevention policy.

Field	Description
Signature Set	Choose a signature set that defines the rules for an evaluating traffic from the **Signature Set** drop-down list. The following options are available. • **Balanced** : Provides protection without significant effect on system performance. • **Connectivity** : Less restrictive and provide better performance by imposing fewer rules. • **Security** : Provides more protection than Balanced but with an impact on performance.
Inspection Mode	Choose the inspection mode. The following options are available: • Detection: Choose this option for intrusion detection mode. • Protection: Choose this option for intrusion protection mode.
Custom Signature Set	Select one or more web categories from the drop-down list. The categories are: abortion, abused-drugs, auctions, and so on.
Select an Signature Allow List	Select a signature allow list.
Alerts Log Level	Choose the alert log level: • Error • Emergency • Alert • Critical • Warning • Notice • Info • Debug

• URL filtering

Field	Description
Profile Name	Name of the URL filtering policy.
Web Category	Choose the web category. The options are Block and Allow.

Field	Description
Web Reputation	Choose the web reputation from the drop-down list. The reputation options are: • High Risk • Suspicious • Moderate Risk • Low Risk • Trustworthy
Select one or more web categories	Select one or more web categories from the drop-down list. The categories are: abortion, abused-drugs, auctions, and so on.
Select allow URL list	Select an allow URL list.
Select block URL list	Select a block URL list.
Block Page Server	Choose one of the options: • Block Page Content: Enter the default content header and content body. • Redirect URL: Enter the redirect URL.
Alerts and Logs	Choose the alert and log type: • Blocklist • Allowlist • Reputation/Category

• Advanced Malware Protection Policy

Field	Description
Profile Name	Name of the advanced malware protection policy name.
Select AMP Cloud Region	Select AMT Cloud region. The options are: • NAM • EU • APJC
Alert Log Level	Choose the alert log level. The options are: • Critical • Warning • Info

Field	Description
File Analysis	Enable file analysis.
Select TG Cloud Region	Select TG Cloud region. The options are NAM and EU.
Select one or more file types	Select one or more file types. The options are, pdf, ms-exe, new-office, rtf, mdb, mscab, msole2, wri, xlw, flv, and swf.

- TLS/SSL profile

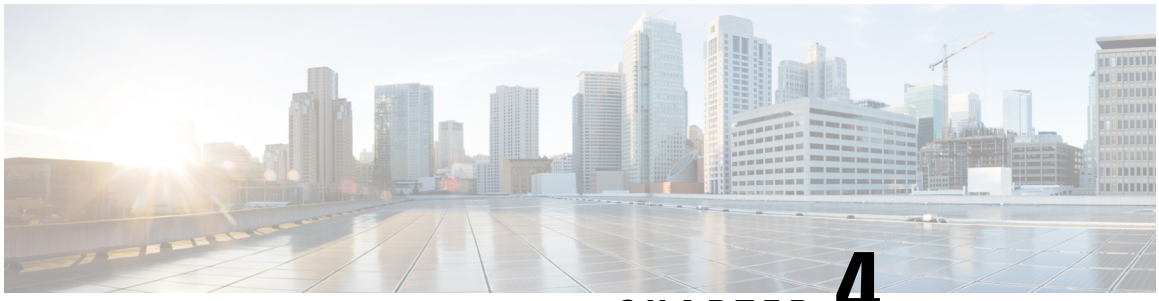
Field	Description
Profile Name	Name of the TLS/SSL profile.
Select Categories to assign action	Set the categories between the actions—Decrypt, No Decrypt, and Pass Through URL Categories. Alternatively, choose multiple categories and set the action.
Reputation	Enable reputation to choose the **Decrypt Threshold** . The decrypt threshold options are: • High Risk • Suspicious • Moderate Risk • Low Risk • Trustworthy
Advanced Options	
Select a Decrypt Domain list	Choose the decrypt domain list or click **Create New** to create a new decrypt domain list. **a.** Enter **Decrypt Domain List Name** . **b.** Enter **Decrypt Domain** **c.** Click **Add** .
Select a No Decrypt Domain list	Choose the no decrypt domain list or click **Create New** to create a new no decrypt domain list. **a.** Enter **No Decrypt Domain List Name** . **b.** Enter **No Decrypt Domain** **c.** Click **Add** .
Fail Decrypt	Enable the fail decrypt option, if decryption fails.

- TLS/SSL decryption

Field Name	Description
Policy Name	Name of the policy. The name can contain a maximum of 32 characters.
Server Certificate Checks	
Expired Certificate	Defines what the policy should do if the server certificate has expired. The options are: • **Drop** : Drop traffic • **Decrypt** : Decrypt traffic
Untrusted Certificate	Defines what the policy should do if the server certificate is not trusted. The options are: • **Drop** : Drop traffic • **Decrypt** : Decrypt traffic
Certificate Revocation Status	Defines whether the Online Certificate Status Protocol (OCSP) should be used to check the revocation status of the server certificate. The options are **Enabled** or **Disabled** .
Unknown Revocation Status	Defines what the policy does, if the OCSP revocation status is **unknown** . • **Drop** : Drop traffic • **Decrypt** : Decrypt traffic
Unsupported Mode Checks	
Unsupported Protocol Versions	Defines the unsupported protocol versions. • **Drop** : Drop the unsupported protocol versions. • **Decrypt** : Decrypt the unsupported protocol versions.
Unsupported Cipher Suites	Defines the unsupported cipher suites. • **Drop** : Drop the unsupported cipher suites. • **Decrypt** : Decrypt the unsupported cipher suites.
Failure Mode	Defines the failure mode. The options are close and open.
Certificate Bundle	Check the **Use default CA certificate bundle** checkbox to use the default CA.

Field Name	Description
Minimum TLS Version	Sets the minimum version of TLS that the proxy should support. The options are: • **TLS 1.0** • **TLS 1.1** • **TLS 1.2**
Proxy Certificate Attributes	
RSA Keypair Modules	Defines the Proxy Certificate RSA Key modules. The options are: • **1024 bit RSA** • **2048 bit RSA** • **4096 bit RSA**
Ec Key Type	Defines the key type. The options are: • **P256** • **P384** • **P521**
Certificate Lifetime (in Days)	Sets the lifetime of the proxy certificate, in days.

Step 4 Click **Save**.



CHAPTER 4

Secure Internet Gateway and Secure Service Edge

- Feature history for Secure Internet Gateway and Secure Service Edge, on page 61
- Secure Internet Gateway, on page 61
- Configure a Secure Internet Gateway, on page 62
- Configure a Secure Service Edge, on page 68

Feature history for Secure Internet Gateway and Secure Service Edge

Table 17: Feature history

Feature Name	Release Information	Description
Configure Secure Service Edge	Cisco IOS XE Catalyst SD-WAN Release 17.13.1a Cisco Catalyst SD-WAN Manager Release 20.13.1	With this feature you can configure a Secure Service Edge (SSE) profile using Cisco Secure Access as the provider. You can associate the SSE profile to a policy group to deploy to a device.

Secure Internet Gateway

Cisco Catalyst SD-WAN edge devices support routing, security, and other LAN access features that can be managed centrally. On high-end devices, you can enable all these features while providing the scale and performance required by large enterprises. However, on lower-end devices, enabling all the security features simultaneously can degrade performance. To avoid the performance degradation, integrate lower-end devices with Secure Internet Gateways (SIG) that do most of the processing to secure enterprise traffic. When you integrate a Cisco Catalyst SD-WAN edge device with a SIG, all client internet traffic, based on routing or policy, is forwarded to the SIG.

Configure a Secure Internet Gateway

Before you begin

Ensure that you enter the Umbrella and Zscaler credentials from **Administration** > **Settings** > **Cloud Provider Credentials** > **Cloud Credentials**.

Table 18: Cisco Umbrella Credentials

Field	Description
Organization ID	Enter the Cisco Umbrella organization ID (Org ID) for your organization. For more information, see the *Cisco Umbrella SIG User Guide* .
SIG Umbrella API Key	Enter the Umbrella Management API Key. Management API keys are used in SIG is **Secure Internet Gateway (SIG) - (Management)** . For more information, see the Cloud Security API documentation on the Cisco DevNet portal.
SIG Umbrella API Secret	Enter the Umbrella Management API Secret. For more information, see the Cloud Security API documentation on the Cisco DevNet portal.

Table 19: Zscaler Credentials

Field	Description
Organization	Name of the organization in Zscaler cloud.
Partner base URI	This is the base URI that Cisco SD-WAN Manager uses in REST API calls. To find this information on the Zscaler portal, see the *ZIA Help* > *ZIA API* > *API Developer & Reference Guide* > *Getting Started* .
Username	Username of the Cisco Catalyst SD-WAN partner account.
Password	Password of the Cisco Catalyst SD-WAN partner account.
Partner API key	Partner API key. To find the key in Zscaler, see Managing SD-WAN Partner Keys .

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Policy Groups** > **Secure Internet Gateway**.

Step 2 Click **Add Secure Internet Gateway**.

Step 3 Choose **SIG Provider**.

- Umbrella
- Zscaler
- Generic

Step 4 Enter a source IP address for the probe packets.

Step 5 Create one or more trackers to monitor tunnel health.

Click **Add Tracker**. In the **Add Tracker** dialog box, configure the following:

Table 20: Tracker Parameters

Field	Description
Name	Name of the tracker. The name can be up to 128 alphanumeric characters.
API url of endpoint	Specify the API URL for the SIG endpoint of the tunnel.
Threshold	Enter the wait time for the probe to return a response before declaring that the configured endpoint is down. Range: 100 to 1000 milliseconds Default: 300 milliseconds
Probe Interval	Enter the time interval between probes to determine the status of the configured endpoint. Range: 20 to 600 seconds Default: 60 seconds
Multiplier	Enter the number of times to resend probes before determining that a tunnel is down. Range: 1 to 10 Default: 3

Step 6 Create tunnels.

Click **Add Tunnel**. In the **Add Tunnel** dialog box configure the following:

Table 21: Add tunnel

Field	Description
Tunnel Type	Umbrella: (Read only) **ipsec** Zscaler: Click **ipsec** or **gre** . Generic: Click **ipsec** or **gre** .
Interface Name (1..255)	Name of the interface.
Description	Description for the interface.
Tracker	By default, a tracker is attached to monitor the health of tunnels.

Field	Description
Tunnel Source Interface	Name of the source interface of the tunnel. This interface should be an egress interface and is typically the internet-facing interface.
Source Public IP	(Automatic GRE tunnels to Zscaler only) Public IP address of the tunnel source interface that is required to create the GRE tunnel to Zscaler. Default: Auto We recommend that you use the default configuration. With the default configuration, the Cisco IOS XE SD-WAN device finds the public IP address assigned to the tunnel source interface using a DNS query. If the DNS query fails, the device notifies Cisco SD-WAN Manager of the failure. Enter the public IP address only if the DNS query fails.
Data-Center	For a primary data center, click **Primary** , or for a secondary data center, click **Secondary** . Tunnels to the primary data center serve as active tunnels, and tunnels to the secondary data center serve as back-up tunnels.
Tunnel Destination IP Address/FQDN	(Manual tunnels only) The IP address of the SIG provider endpoint. The configuration of FQDN for Tunnel Destination IP address is not supported.
Preshared Key	(Manual tunnels only) This field is displayed only if you choose **ipsec** as the **Tunnel Type** . Enter the password to use with the preshared key.
Advanced Options	
Shutdown	Click **No** to enable the interface; click **Yes** to disable. Default: No
IP MTU	Specify the maximum MTU size of packets on the interface. Range: 576 to 2000 bytes Default: 1400 bytes
TCP MSS	Specify the maximum segment size (MSS) of TPC SYN packets. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented. Range: 500 to 1460 bytes Default: None
DPD Interval	Specify the interval for IKE to send Hello packets on the connection. Range: 10 to 3600 seconds Default: 10

Field	Description
DPD Retries	Specify the number of seconds between DPD retry messages if the DPD retry message is missed by the peer. After one DPD message is missed by the peer, the router changes the state and sends a DPD retry message at a faster retry interval, which is the number of seconds between DPD retries if the DPD message is missed by the peer. The default DPD retry message is sent every 2 seconds. Five DPD retry messages can be missed before the tunnel is marked as down. Range: 2 to 60 seconds Default: 3
IKE	
IKE Rekey Interval	Specify the interval for refreshing IKE keys. Range: 300 to 86400 seconds (1 hour to 14 days) Default: 14400 seconds
IKE Cipher Suite	Specify the type of authentication and encryption to use during IKE key exchange. Choose one of the following: • AES 256 CBC SHA1 • AES 256 CBC SHA2 • AES 128 CBC SHA1 • AES 128 CBC SHA2 The IPsec Cipher Suite defaults vary by the type of the SIG: • Umbrella: AES 256 GCM • Zscaler: None • Generic: NULL SHA 512

Field	Description
IKE Diffie-Hellman Group	Specify the Diffie-Hellman group to use in IKE key exchange, whether IKEv1 or IKEv2. • 2 1024-bit modulus • 14 2048-bit modulus • 15 3072-bit modulus • 16 4096-bit modulus The IKE group defaults vary by the type of the SIG: • Umbrella: 14 2048-bit modulus • Zscaler: 2 1024-bit modulus • Generic: 16 4096-bit modulus
IPSec	
IPsec Rekey Interval	Specify the interval for refreshing IPsec keys. Range: 300 to 1209600 seconds (1 hour to 14 days) Default: 3600 seconds
IPsec Replay Window	Specify the replay window size for the IPsec tunnel. Options: 64, 128, 256, 512, 1024, 2048, 4096. Default: 512
IPsec Cipher Suite	Specify the authentication and encryption to use on the IPsec tunnel. Options: • AES 256 CBC SHA1 • AES 256 CBC SHA 384 • AES 256 CBC SHA 256 • AES 256 CBC SHA 512 • AES 256 GCM • NULL SHA1 • NULL SHA 384 • NULL SHA 256 • NULL SHA 512 Default: AES 256 GCM

Field	Description
Perfect Forward Secrecy	Specify the PFS settings to use on the IPsec tunnel. Choose one of the following Diffie-Hellman prime modulus groups: • Group-2 1024-bit modulus • Group-14 2048-bit modulus • Group-15 3072-bit modulus • Group-16 4096-bit modulus • None: disable PFS The Perfect Forward Secrecy defaults vary by the type of the SIG: • Umbrella: None • Zscaler: None • Generic: Group 16

Note
When a security policy associated with Zscaler is removed from a device and a new configuration group is deployed, the corresponding tunnel entry sometimes fails to be deleted from Zscaler's cloud services. As a result, attempting to establish a new tunnel may result in a DUPLICATE_ITEM error due to the presence of the existing entry. To resolve this issue, manually delete the stale tunnel entry from the Zscaler cloud whenever a security policy is removed from a device.

Step 7 Configure high availability to designate active and back-up tunnels and distribute traffic among tunnels.

Click **Add Interface Pair**. In the **Add Interface Pair** dialog box, configure the following:

Field	Description
Active Interface	Choose a tunnel that connects to the primary data center.
Active Interface Weight	Enter weight (weight range 1 to 255) for load balancing. Load balancing helps in distributing traffic over multiple tunnels and this helps increase the network bandwidth. If you enter the same weights, you can achieve ECMP load balancing across the tunnels. However, if you enter a higher weight for a tunnel, that tunnel has higher priority for traffic flow. For example, if you set up two active tunnels, where the first tunnel is configured with weight of 10, and the second tunnel with weight configured as 20, then the traffic is load-balanced between the tunnels in a 10:20 ratio.
Backup Interface	To designate a back-up tunnel, choose a tunnel that connects to the secondary data center. To omit designating a back-up tunnel, choose **None** .

Field	Description
Backup Interface Weight	Enter weight (weight range 1 to 255) for load balancing. Load balancing helps in distributing traffic over multiple tunnels and this helps increase the network bandwidth. If you enter the same weights, you can achieve ECMP load balancing across the tunnels. However, if you enter a higher weight for a tunnel, that tunnel has higher priority for traffic flow. For example, if you set up two back-up tunnels, where the first tunnel is configured with weight of 10, and the second tunnel with weight configured as 20, then the traffic is load-balanced between the tunnels in a 10:20 ratio.

Configure a Secure Service Edge

Before you begin

Create the Cisco SSE credentials from **Administration** > **Settings** > **Cloud Credentials** .

Gateway Options

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Policy Groups** > **Secure Internet Gateway/Secure Service Edge**.

Step 2 Click **Add Secure Service Edge**.

Step 3 Choose the **SSE Provider**.

- Cisco Secure Access
- (Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.14.1) Zscaler

Step 4 Enable context sharing for VPN and SGT to allow Cisco IOS XE Catalyst SD-WAN device s to share context information with SSE.

Table 22: Context Sharing

Field	Description
VPN	Enable sharing of VPN information with SSE.
SGT	Enable sharing of SGT information with SSE.

Step 5 Configure trackers.

While creating automatic tunnels, Cisco SD-WAN Manager creates and attaches a default tracker endpoint with default values for failover parameters. However, you can also create customized trackers with failover parameters that suit your requirements.

a) In the **Source IP Address** field, enter a source IP address without a subnet mask.
b) Click **Add Tracker**. In the **Add Tracker** pop-up window, configure the following:

Table 23: Tracker Parameters

Field	Description
Name	Name of the tracker. The name can be up to 128 alphanumeric characters.
API url of endpoint	Specify the API URL for the Secure Service Edge endpoint of the tunnel. Default: service.sig.umbrella.com
Threshold	Enter the wait time for the probe to return a response before declaring that the configured endpoint is down. Range: 100 to 1000 milliseconds Default: 300 milliseconds
Probe Interval	Enter the time interval between probes to determine the status of the configured endpoint. Range: 20 to 600 seconds Default: 60 seconds
Multiplier	Enter the number of times to resend probes before determining that a tunnel is up or down. Range: 1 to 10 Default: 3

Step 6 Create tunnels.

Click **Add Tunnel**. In the **Add Tunnel** pop-up window, under **Basic Settings** , configure the following:

Table 24: Basic Settings

Field	Description
Tunnel Type	• Cisco Secure Access: (Read only) **ipsec** • (Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.14.1) Zscaler: **ipsec** or **gre**
Interface Name (1..255)	Name of the interface.
Description	Enter a description for the interface.
Tracker	By default, a tracker is attached to monitor the health of tunnels.
Tunnel Source Interface	Name of the source interface of the tunnel. This interface should be an egress interface and is typically the internet-facing interface. The tunnel source interface supports loopback.

Field	Description
Source Public IP	(Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.14.1) Public IP address of the tunnel source interface that is required to create the GRE tunnel to Zscaler. Default: Auto. We recommend that you use the default configuration. With the default configuration, the Cisco IOS XE Catalyst SD-WAN device finds the public IP address assigned to the tunnel source interface using a DNS query. If the DNS query fails, the device notifies Cisco SD-WAN Manager of the failure. Enter the public IP address only if the DNS query fails.
Data-Center	For a primary data center, click **Primary** , or for a secondary data center, click **Secondary** . Tunnels to the primary data center serve as active tunnels, and tunnels to the secondary data center serve as back-up tunnels.
Advanced Options (Optional)	
Shutdown	Click the radio button to enable this option. Default: Disabled
Enable Tracker	Click the radio button to enable this option.
IP MTU	Specify the maximum MTU size of packets on the interface. Range: 576 to 2000 bytes Default: 1400 bytes
TCP MSS	Specify the maximum segment size (MSS) of TPC SYN packets. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented. Range: 500 to 1460 bytes Default: None
DPD Interval	Specify the interval for Internet Key Exchange (IKE) to send Hello packets on the connection. Range: 10 to 3600 seconds Default: 10

Field	Description
DPD Retries	Specify the number of seconds between Dead Peer Detection (DPD) retry messages if the DPD retry message is missed by the peer. If a peer misses a DPD message, the router changes the state and sends a DPD retry message. The message is sent at a faster retry interval, which is the number of seconds between DPD retries. The default DPD retry message is sent every 2 seconds. The tunnel is marked as down after five DPD retry messages are missed. Range: 2 to 60 seconds Default: 3
IKE	
IKE Rekey Interval	Specify the interval for refreshing IKE keys. Range: 3600 to 1209600 seconds (1 hour to 14 days) Default: 14400 seconds
IKE Cipher Suite	Specify the type of authentication and encryption to use during IKE key exchange. Choose one of the following: • AES 256 CBC SHA1 • AES 256 CBC SHA2 • AES 128 CBC SHA1 • AES 128 CBC SHA2 Default: AES 256 CBC SHA1
IKE Diffie-Hellman Group	Specify the Diffie-Hellman group to use in IKE key exchange, whether IKEv1 or IKEv2.
IPSec	
IPsec Rekey Interval	Specify the interval for refreshing IPsec keys. Range: 3600 to 1209600 seconds (1 hour to 14 days) Default: 3600 seconds
IPsec Replay Window	Specify the replay window size for the IPsec tunnel. Options: 64, 128, 256, 512, 1024, 2048, or 4096 packets. Default: 512

Field	Description
IPsec Cipher Suite	Specify the authentication and encryption to use on the IPsec tunnel. Options: • AES 256 CBC SHA1 • AES 256 CBC SHA 384 • AES 256 CBC SHA 256 • AES 256 CBC SHA 512 • AES 256 GCM Default: AEM 256 GCM
Perfect Forward Secrecy	Specify the Perfect Forward Secrecy (PFS) settings to use on the IPsec tunnel. Choose one of the following Diffie-Hellman prime modulus groups: • Group-2 1024-bit modulus • Group-14 2048-bit modulus • Group-15 3072-bit modulus • Group-16 4096-bit modulus • None: disable PFS

Step 7 Applicable only to Cisco Secure Access: **Region** : When you choose the region, a pair of primary and secondary region is selected. Choose the primary region that Cisco Secure Service Edge provides from the drop-down list and the secondary region is auto-selected in Cisco SD-WAN Manager . If the primary region with a unicast IP address is not reachable then the secondary region with a unicast IP address is reachable and vice versa. Cisco Secure Access ensures that both the regions are reachable at all times.

Note
You can configure any DNS server on the device which connects to HTTPS to get the public IP address. To configure a source interface for HTTPS, use the **ip http client source-interface** command on Cisco SD-WAN Manager .

Step 8 Configure high availability to designate active and back-up tunnels and distribute traffic among tunnels.

Click **Add Interface Pair**. In the **Add Interface Pair** pop-up window, configure the following:

Table 25: Add interface pair

Field	Description
Active Interface	Choose a tunnel that connects to the primary data center.

Field	Description
Active Interface Weight	Enter weight (weight range 1 to 255) for load balancing. Load balancing helps in distributing traffic over multiple tunnels and this helps increase the network bandwidth. If you enter the same weights to both the tunnels, you can achieve ECMP load balancing across the tunnels. However, if you enter a higher weight for a tunnel, that tunnel has higher priority for traffic flow. For example, if you set up two active tunnels, where the first tunnel is configured with weight of 10, and the second tunnel with weight configured as 20, then the traffic is load-balanced between the tunnels in a 10:20 ratio.
Backup Interface	To designate a back-up tunnel, choose a tunnel that connects to the secondary data center. To omit designating a back-up tunnel, choose **None** .
Backup Interface Weight	Enter weight (weight range 1 to 255) for load balancing. Load balancing helps in distributing traffic over multiple tunnels and this helps increase the network bandwidth. If you enter the same weights, you can achieve ECMP load balancing across the tunnels. However, if you enter a higher weight for a tunnel, that tunnel has higher priority for traffic flow. For example, if you set up two back-up tunnels, where the first tunnel is configured with weight of 10, and the second tunnel with weight configured as 20, then the traffic is load-balanced between the tunnels in a 10:20 ratio.

Step 9 (Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.14.1) Configure advanced settings.

Applicable only to Zscaler:

Field	Description
Primary Datacenter	Cisco SD-WAN Manager automatically selects the primary data center closest to the WAN edge device. To route traffic to a specific Zscaler data center, choose the data center from the drop-down list.
Secondary Datacenter	Cisco SD-WAN Manager automatically selects the secondary data center closest to the WAN edge device. To route traffic to a specific Zscaler data center, choose the data center from the drop-down list.

Table 26: Zscaler location

Field	Description
Zscaler Location	Enter the name of a location that is configured on the ZIA Admin Portal. If you do not enter a location name, the Zscaler service detects the location based on the received traffic. From Cisco Catalyst SD-WAN Manager Release 20.18.1 , enter unique location name for primary and secondary routers. For more information about locations, see *ZIA Help > Traffic Forwarding > Location Management > About Locations* .
Country	You can enable or disable this option only if either primary or secondary data center is set to Auto. When you choose Auto, the data center selected is within the country of the device.

Table 27: Gateway options

Field	Description
Authentication Required	See *ZIA Help > Traffic Forwarding > Location Management > Configuring Locations* . Default: Off
Enable Caution	See *ZIA Help > Traffic Forwarding > Location Management > Configuring Locations* . Default: Off
Enable AUP	See *ZIA Help > Traffic Forwarding > Location Management > Configuring Locations* . Default: Off
XFF Forwarding	See *ZIA Help > Traffic Forwarding > Location Management > Configuring Locations* . Default: Off
Enable IPS Control	See *ZIA Help > Traffic Forwarding > Location Management > Configuring Locations* . Default: Off
Enable Firewall	See *ZIA Help > Traffic Forwarding > Location Management > Configuring Locations* . Default: Off

(Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.15.1)

Table 28: Bandwidth control

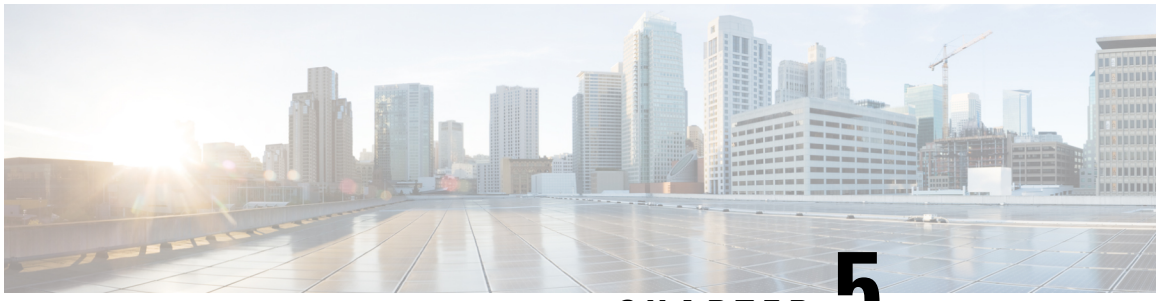
Field	Description
Enforce Bandwidth Control	Enable to enforce bandwidth control on the location. • **Download (Mbps)** : Specify the maximum bandwidth limits for download. • **Upload (Mbps)** : Specify the maximum bandwidth limits for upload. For more information about locations, see *ZIA Help > Traffic Forwarding > Location Management > About Locations* .

(Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.15.1)

Table 29: Sub-locations

Field	Description
Name	Enter a name for the sub-location.
Service VPN	Select a service VPN from the drop-down menu.
IP Address	Enter an IP address or a range of IP addresses for the service VPN.
Authentication Required	See *ZIA Help > Traffic Forwarding > Location Management > Configuring Locations* . Default: Off
Enable Caution	See *ZIA Help > Traffic Forwarding > Location Management > Configuring Locations* . Default: Off
Enable AUP	See *ZIA Help > Traffic Forwarding > Location Management > Configuring Locations* . Default: Off
XFF Forwarding	See *ZIA Help > Traffic Forwarding > Location Management > Configuring Locations* . Default: Off
Enable IPS Control	See *ZIA Help > Traffic Forwarding > Location Management > Configuring Locations* . Default: Off

Field	Description
Enable Firewall	See *ZIA Help > Traffic Forwarding > Location Management > Configuring Locations* . Default: Off
Enforce Bandwidth Control	Choose one of the following: • **Location Bandwidth** : Uses bandwidth of the parent location on the sub-location. The download and upload maximum bandwidth limits are the same as specified for the parent location. A percentage of the parent location bandwidth is allocated to the sub-location based on the allocations of other sub-locations. For more information, see *Secure Internet and SaaS Access (ZIA) Help > Traffic Forwarding > Location Management > Configuring Sub-Locations* . • **Override** : Overrides the bandwidth of the parent location. Specify the maximum bandwidth limits for **Download (Mbps)** and **Upload (Mbps)** . This bandwidth is dedicated to the sub-location and not shared with other sub-locations. • **Disable** : Disables the sub-location traffic from any bandwidth management



CHAPTER 5

DNS Security

- Feature history for DNS security, on page 77
- DNS security, on page 77
- DNS security routing and fallback, on page 78
- Configure DNS security, on page 79
- Verify DNS security configurations using CLI, on page 81

Feature history for DNS security

Table 30: Feature history

Feature Name	Release Information	Description
DNS Security with Cisco Secure Access	Cisco IOS XE Catalyst SD-WAN Release 26.1.1 Cisco Catalyst SD-WAN Manager Release 26.1.1.1	This feature monitors and controls the DNS requests by blocking access to unauthorized domains and applies consistent DNS-based security policies across devices. DNS security fallback ensures that DNS security policy routing is determined by device routing configurations. In the event of a failover where the NAT Direct Internet Access (DIA) route is unavailable, connectivity is maintained by service vpn routing, ensuring continued reachability.
Increase in Local Domain Bypass Scale	Cisco IOS XE Catalyst SD-WAN Release 26.1.1 Cisco Catalyst SD-WAN Manager Release 26.1.1.1	With this feature the local domain bypass entries are increased to 256.

DNS security

The Cisco Catalyst SD-WAN Umbrella Integration feature enables the cloud-based security service by inspecting the Domain Name System (DNS) query that is sent to the DNS server through the device.

The security administrator configures policies on the Umbrella portal to either allow or deny traffic toward the fully qualified domain name (FQDN). The router acts as a DNS forwarder on the network edge, transparently intercepts DNS traffic, and forwards the DNS queries to the Umbrella cloud.

DNS security routing and fallback

A DNS security routing fallback mechanism is an implementation that

- ensures device configurations dictate the egress path of packets,
- maintains symmetric routing based on the device's routing table, and
- data policy configurations takes precedence over the local DNS security policy.

DNS security uses the service VPN route configuration to establish connectivity to DNS servers, ensuring that device routing tables determine the egress path.

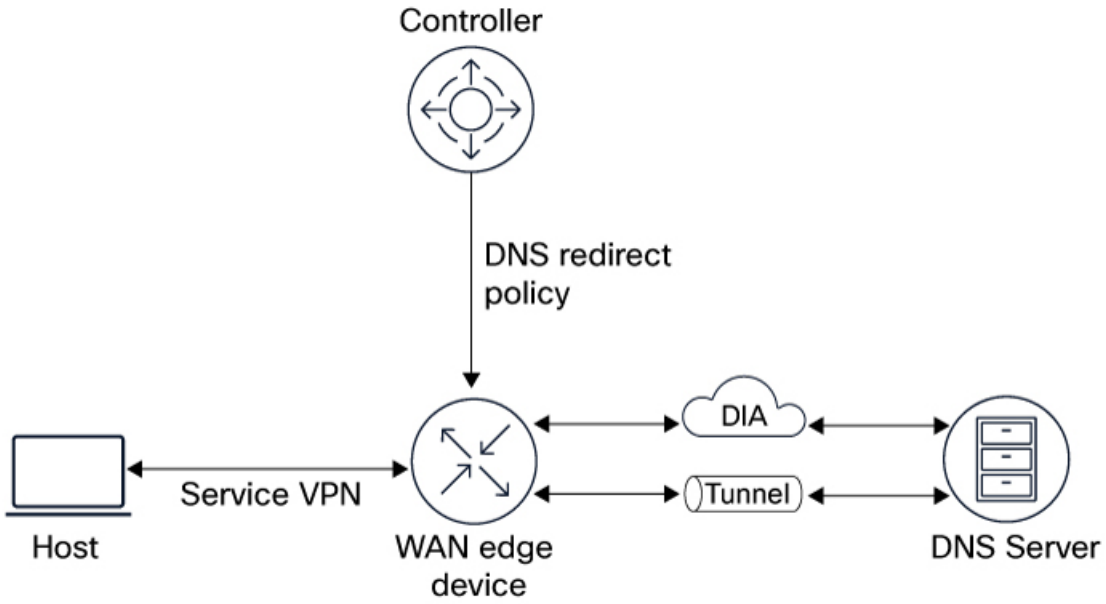
If you want to continue with the DNS security where traffic egresses via the global VRF, then configure a NAT DIA route for the Umbrella IP addresses 208.67.222.222 and 208.67.220.220.

Integration with NAT trackers

You can configure a NAT tracker and monitor the availability of the path.

- If the path is healthy: The DNS traffic uses the NAT route.
- If the path fails: The NAT tracker detects the failure, withdraws the route, and the device automatically performs a new route lookup to find an alternative path (like the overlay).

Figure 1: DNS security fallback



Configure DNS security

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Policy Groups** > **DNS Security**.

Step 2 Click **Add DNS Security Policy**.

Field	Description
Add DNS Security Policy	From the **Add DNS Security Policy** drop-down list, select **Create New** to create a new DNS Security Policy policy.
Create New	Displays the DNS Security Policy wizard.
Policy Name	Enter a name for the policy.
Select Provider	Minimum supported release: Cisco Catalyst SD-WAN Manager Release 26.1.1.1 Choose from: • **Cisco Secure Access** • **Umbrella**
Registration Status	Displays the status of the API Token configuration.
Manage Cisco Secure Access Registration	Enter the following details: • **Organization ID**: Cisco Secure Access organization ID for your organization. For more information, see *Find Your Organization ID* in the Cisco Secure Access User Guide. • **API Key**: Cisco Secure Access API Key. • **Secret**: Cisco Secure Access API Secret.

Field	Description
Manage Umbrella Registration	• Enter the Cisco Umbrella organization ID (**Organization ID**) for your organization. For more information, see *Find Your Organization ID* in the *Cisco Umbrella SIG User Guide*. Do one of the following: • In the Legacy Credentials pane, enter the **Registration Key**. It is the Umbrella Management API Key, which is part of DNS security policy under unified security policy. Then, enter the Umbrella Management API **Secret**. • For Legacy Credentials, navigate to **Legacy Keys** and select Umbrella Network Devices to obtain the key and secret Or • From Cisco Catalyst SD-WAN Manager Release 20.15.1, in the **Scope Credentials** pane, enter the **Registration Key**. It is the Umbrella Management API Key, which is part of DNS security policy under unified security policy. Then, enter the Umbrella Management API **Secret**. For Scope Credentials, go to **API Keys** and choose the appropriate key scope based on your requirements. Ensure that **Tunnels** and **Network Devices** are selected in the deployments tab (these API Keys are read/write keys). to add Cisco Umbrella Registration Key and Secret. Specific network-devices keys are used in DNS. Also see Information About Cisco Umbrella Scope Credentials. You can edit the umbrella credentials from **Administration** > **Settings** > **Cloud Provider** > **Cloud Credentials**.
Match All VPN	Click **Match All VPN** to keep the same configuration for all the available VPNs.
Custom VPN Configuration	choose **Custom VPN Configuration** to input the specific VPNs.

Field	Description
Local Domain Bypass List	Perform one of these actions: • Choose a local domain from the drop-down list • Choose **Create New**. If you click **Create New**, configure these options: • **Name** • **Description** (optional) • **Local domain** From Cisco Catalyst SD-WAN Manager Release 26.1.1.1, 256 local domain bypass entries are supported.
DNS Server IP	Configure **DNS Server IP** from these options: • **Umbrella Default** • **Custom DNS** The DNS security fallback feature is not supported for custom DNS. You must configure an explicit NAT route to the DNS server for the custom DNS redirect to work.
DNSCrypt	Enable or disable the encryption of DNS packets. The DNS security fallback feature is not supported for DNSCrypt.

Step 3 Click **Save**.

Verify DNS security configurations using CLI

DNS security configuration example

The following is a sample configuration of the DNS security with Cisco Secure Access..

```
parameter-map type dns-defense global
local-domain test
dnscrypt
api-key apikey
orgid 1111111
secret 6 ehB_GFUYBFN]SAJM]eQPdOiJGWfRTDDdJLLPQB]JHCa]HHNgIYLbbPOJKMTdUVWHRhVgF
vrf 1
dns-resolver umbrella
match-local-domain-to-bypass
```

```
vrf 2
dns-resolver umbrella
match-local-domain-to-bypass
```

View VRFs registration

The **show sdwan dns-defense info** command displays how many VRFs requested registration, how many were successfully registered, and whether DNSCrypt is enabled.

```
Device# show sdwan dns-defense info

REGISTRATIONS REQUESTED        REGISTRATIONS COMPLETED        DNSCRYPT        LAST SUCCESS ATTEMPT
-------------------------------------------------------------------------------------------------------
11
10                                    True                         10/25/25 21:12:01
```

View registration status

The **show sdwan dns-defense device-registration** command displays the device ID and the registration status, indicating whether registration was successful or failed for any reason. The response also provides information about the cause of any failure.

```
Device# show sdwan dns-defense device-registration

VRF ID                  RESP CODE          TAG                  DEVICE_ID                  DESCRIPTION
-------------------------------------------------------------------------------------------------------
1
201 created         vpn1                    f3384af554cefba2         Device Id received successfully
2
201 created         vpn2                    f3382ad2f8a37dc6         Device Id received successfully
```