



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



CONTENTS

CHAPTER 1

Policy Groups 1

- Policy Groups 1
- Information About Policy Groups 1
 - Overview of Policy Groups 1
 - Overview of Policy Group Workflows 2
 - Benefits of Policy Groups 2
- Restrictions for Policy Groups 2
- Group of Interest - Policy 2
- Add Policy Group 8

CHAPTER 2

Security Policy Using Policy Groups 9

- Security Policy Using Policy Groups 9
- Information About Security Policy 10
- Enable RBAC for Security Policy 10
- Restrictions for Security Policy 11
- Configure a Security Policy Using a Policy Group 11
- Configure a Group of Interest for a Security Policy 11
- Configure Embedded Security 20
- Configure an Embedded Security Sub-Policy 22
- Configure Embedded Security Additional Settings 24
- Configure a Secure Service Edge 29
- Configure DNS Security 34



CHAPTER 1

Policy Groups

- [Policy Groups, on page 1](#)
- [Information About Policy Groups, on page 1](#)
- [Restrictions for Policy Groups, on page 2](#)
- [Group of Interest - Policy, on page 2](#)
- [Add Policy Group, on page 8](#)

Policy Groups

Table 1: Feature History

Feature Name	Release Information	Description
Policy Groups	Cisco IOS XE 17.13.1a	This feature provides a simple, reusable, and structured approach to configuring policies for SD-Routing devices .

Information About Policy Groups

Policy groups simplify the experience of configuring and deploying various policies on SD-Routing devices. Policy groups are a collection of different policies that you can configure through workflows and associate with and deploy on different SD-Routing devices.

Overview of Policy Groups

Policy Groups provide a simple, reusable, and structured approach for configuring policies and policy objects in SD-Routing devices.

Policy groups are a collection of various policies and policy parameters that you can configure quickly through a simplified workflow. Policy groups allows you to configure the basic and necessary policies with defaults to get your systems up and running. The more advanced user can switch to the **Advanced** layout to take 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 creating a policy group, you can associate it with one or more sites or a single device at the site in the network and deploy it on devices managed by configuration groups.

After you've configured a policy group, you can deploy it by using the [Overview of Policy Group Workflows](#).

Overview of Policy Group Workflows

The policy group workflow 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 SD-Routing devices. The workflow provides you with an improved configuration and troubleshooting experience. The workflow has the following features:

- You can review the various configuration values on a single page within the workflow.
- You can easily identify and fix incorrect values that appear highlighted in red. In addition, an asterisk that is adjacent to a field name helps you identify the mandatory values within the workflow.

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.

Benefits of Policy Groups

- Simplified user experience through an intuitive UI that allows you to quickly configure the basic policies that are required to get your 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 SD-WAN device and SD-Routing device in one location.
- Workflows to deploy policy groups.

Restrictions for Policy Groups

- You cannot deploy policy groups to devices that are not already managed by a configurations group.

Group of Interest - Policy

Group of interest provides a list of related policy objects that you can configure and call in the match or action components of a policy. Click **Group of Interest** to create new objects for the policy group as described in the following sections:

Application

1. Click **Application**.

2. Click **Add Application**.
3. From the **Application/Application family list** drop-down, choose the required applications or application families.
4. Click **Save**.

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.

Color

1. Click **Color**.
2. Click **New Color List** and specify the following:

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.

3. Click **Add**.

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

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.

1. Click **Community List**.
2. Click **Add Community List** and specify the following:

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

Field	Description
Add Community	<p>Enter one or more communities separated by commas.</p> <ul style="list-style-type: none"> • 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.

3. Click **Save**.

Data Prefix

1. Click **Data Prefix**.
2. Click **Add Data Prefix**.
3. In the **Data Prefix list** dialog box, specify the following:

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.

4. Click **Save**.

Data Prefix IPv6

1. Click **Data Prefix IPv6**.
2. Click **Add Data Prefix IPv6**.
3. In the **Data Prefix List** dialog box, specify the following:

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

4. Click **Save**.

Expanded Community List

1. Click **Expanded Community List**.
2. Click **Add Expanded Community List** and specify the following:

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

Forwarding Class

1. Click **Add Forwarding Class** and specify the following:

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

2. Click **Save**.

Policer

1. Click **Policer**.
2. Click **Add Policer** and specify the following:

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: <ul style="list-style-type: none"> • 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).

3. Click **Save**.

Preferred Color Group

1. Click **Add Preferred Color Group**.
2. In the **Preferred Color Group Name** field, enter a name for the preferred color group.
3. Choose the color preference and path preference for the primary, secondary, and tertiary colors from the **Color Preference** and the **Path Preference** drop-down lists.

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: <ul style="list-style-type: none"> • Direct Path • Multi Hop Path • All Paths

4. Click **Save**.

Prefix List

1. Click **Prefix List**.
2. Click **Add Prefix List** and specify the following:

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

3. Click **Save**.

Prefix List IPv6

1. Click **Prefix List IPv6**.
2. Click **Add Prefix List** and specify the following:

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

3. Click **Save**.

SLA Class

1. Click **SLA Class**.
2. Click **Add SLA Class** and specify the following:

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.

3. Click **Save**.

TLOC List

1. Click **TLOC List**.
2. Click **Add TLOC List** and specify the following:

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: <ul style="list-style-type: none"> • IPSec • GRE
Preference	Choose a preference to associate with the TLOC. The range is 0 to 4294967295.

3. Click **Save**.

Add Policy Group

To create a new policy group, click **Add Policy Group** and configure the values in the following table. If you have already created a policy group, click the policy group from the list of available policy groups to edit.

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.
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.

1. Click **Save** to save your configuration.
2. Click the pencil icon to select or unselect devices to associate or dissociate with the policy group.
3. Click **Deploy** to select sites and deploy the policy group.

To delete a policy group, select the ellipsis icon (...) to the right of the policy group and click **Delete**.



CHAPTER 2

Security Policy Using Policy Groups

- [Security Policy Using Policy Groups, on page 9](#)
- [Information About Security Policy, on page 10](#)
- [Enable RBAC for Security Policy, on page 10](#)
- [Restrictions for Security Policy, on page 11](#)
- [Configure a Security Policy Using a Policy Group, on page 11](#)
- [Configure a Group of Interest for a Security Policy, on page 11](#)
- [Configure Embedded Security, on page 20](#)
- [Configure an Embedded Security Sub-Policy, on page 22](#)
- [Configure Embedded Security Additional Settings, on page 24](#)
- [Configure a Secure Service Edge, on page 29](#)
- [Configure DNS Security, on page 34](#)

Security Policy Using Policy Groups

Table 3: Feature History

Feature Name	Release Information	Description
Security Policy Using Policy Groups		<p>This feature provides a simple, reusable, and structured approach for configuring security policies . 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.</p> <p>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.</p>

Information About Security Policy

Configuring security policies using policy groups simplifies the experience of configuring and deploying policies on SD-Routing devices. Use a workflow to configure policies and associate them with devices in the network.

The **Policy Groups** page includes the following:

- **Policy Group**
- **Embedded Security Configuration**
- **DNS Security Configuration**

Enable RBAC for Security 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**.

1. From the Cisco SD-WAN Manager menu, choose **Administration > Manage Users > User Groups**.
2. Click **Add User Group**.
3. Enter **User Group Name**.
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.
5. Check a **Read** or **Write** check box for the following features that you want to assign to a user group:
 - **Feature Profile > Embedded Security > Legacy Policy**
 - **Feature Profile > Embedded Security > NGFirewall**
 - **Feature Profile > Embedded Security > 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

6. Click **Add**.

Restrictions for Security Policy

Security policy does not support matching traffic using a custom application in a custom-defined application list.

Configure a Security Policy Using a Policy Group

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

1. From the Cisco SD-WAN Manager menu, choose **Workflows > Workflow Library > Create Security Policy**. Alternatively, choose **Configuration > Policy Groups**.
2. Click **Embedded Security**.
3. On the **Embedded Security** page, click **Add Security Policy**. This launches the Security Policy workflow.
4. Enter **Policy Name** and **Description** and click **Next**.
5. On the **Select the optional Configuration Group to associate with the security policy** page, choose the configuration groups and click **Next**.
6. Click **Add Sub-Policy**.
7. Click **Submit**. You can view the new security policy in the **Embedded Security** tab.

Configure a Group of Interest for a Security Policy

1. From the Cisco SD-WAN Manager menu, choose **Configuration > Policy Groups > Group of Interest**.
2. Click the **Security** tab. The list of security objects and profiles appears.

Use the following tables to configure a different group of lists for security policy:

Application

Field	Description
Application List Name	Name of the application list.
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.

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.

Field	Description
FQDN List Name	Name of the FQDN list.
FQDN	The URL names separated by comma. For example, cisco.com.

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 <code>Generator ID:Signature ID</code> , 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: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • 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, Antarctic, Asia, Europe, and so on.

The security group of interest has the following profiles:

- Advanced Inspection Profile
- Intrusion Prevention Policy
- URL Filtering
- Advanced Malware Protection
- TLS/SSL Profile
- TLS/SSL Decryption

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.

Field	Description
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: <ul style="list-style-type: none"> • Decrypt • Pass Through • Do not Decrypt

Intrusion Prevention Policy

Field	Description
Profile Name	Name of the intrusion prevention policy.
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. <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • 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.

Field	Description
Alerts Log Level	Choose the alert log level: <ul style="list-style-type: none"> • Error • Emergency • Alert • Critical • Warning • Notice • Info • Debug

URL Filtering Policy

Field	Description
Profile Name	Name of the URL filtering policy.
Web Category	Choose the web category. The options are Block and Allow.
Web Reputation	Choose the web reputation from the drop-down list. The reputation options are: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • Block Page Content: Enter the default content header and content body. • Redirect URL: Enter the redirect URL.

Field	Description
Alerts and Logs	Choose the alert and log type: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • NAM • EU • APJC
Alert Log Level	Choose the alert log level. The options are: <ul style="list-style-type: none"> • Critical • Warning • Info
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.

Field	Description
Reputation	Enable reputation to choose the Decrypt Threshold . The decrypt threshold options are: <ul style="list-style-type: none"> • 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. <ol style="list-style-type: none"> 1. Enter Decrypt Domain List Name. 2. Enter Decrypt Domain 3. 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. <ol style="list-style-type: none"> 1. Enter No Decrypt Domain List Name. 2. Enter No Decrypt Domain 3. 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: <ul style="list-style-type: none"> • Drop: Drop traffic • Decrypt: Decrypt traffic

Field Name	Description
Untrusted Certificate	Defines what the policy should do if the server certificate is not trusted. The options are: <ul style="list-style-type: none"> • 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 . <ul style="list-style-type: none"> • Drop: Drop traffic • Decrypt: Decrypt traffic
Unsupported Mode Checks	
Unsupported Protocol Versions	Defines the unsupported protocol versions. <ul style="list-style-type: none"> • Drop: Drop the unsupported protocol versions. • Decrypt: Decrypt the unsupported protocol versions.
Unsupported Cipher Suites	Defines the unsupported cipher suites. <ul style="list-style-type: none"> • 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.
Minimum TLS Version	Sets the minimum version of TLS that the proxy should support. The options are: <ul style="list-style-type: none"> • TLS 1.0 • TLS 1.1 • TLS 1.2
Proxy Certificate Attributes	

Field Name	Description
RSA Keypair Modules	Defines the Proxy Certificate RSA Key modules. The options are: <ul style="list-style-type: none"> • 1024 bit RSA • 2048 bit RSA • 4096 bit RSA
Ec Key Type	Defines the key type. The options are: <ul style="list-style-type: none"> • P256 • P384 • P521
Certificate Lifetime (in Days)	Sets the lifetime of the proxy certificate, in days.

Configure Embedded Security

Security is a critical element of today's networking infrastructure. Network administrators and security officers are hard pressed to defend their networks against attacks and breaches. Due to hybrid clouds and remote employee connectivity, the security perimeter around networks is disappearing.

The Enterprise Firewall with Application Awareness uses a flexible and easily understood zone-based model for traffic inspection, compared to the older interface-based model.

A firewall policy is a type of localized security policy that allows stateful inspection of TCP, UDP, and ICMP data traffic flows. Traffic flows that originate in a given zone are allowed to proceed to another zone based on the policy between the two zones. A zone is a grouping of one or more VPNs. Grouping VPNs into zones allows you to establish security boundaries in your overlay network so that you can control all data traffic that passes between zones. For more information on Embedded Security, see [Enterprise Firewall with Application Awareness](#).

1. From the Cisco SD-WAN Manager **olicy Groups** > **Embedded Security**.
2. Choose a security policy and click **Edit**.
3. Click **Add Rule**.

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

Field	Description
Destination Zone	<p>In the Destination Zone drop-down list, choose the zone to which data traffic is sent. The options are:</p> <ul style="list-style-type: none"> • No-Zone • Corporate_Users • Local_Internet_for_Guests • Payment_Processing_Network • Physical_Security_Devices • Self • Untrusted <p>Zones are created based on the VPNs in the configuration group selected in the create security policy workflow.</p>
Match	<p>Choose the desired match conditions from the Add Conditions drop-down list. The options are:</p> <ul style="list-style-type: none"> • Applications • Protocol • Source <ul style="list-style-type: none"> • Geo Location • IPv4 Prefix • Port • Destination <ul style="list-style-type: none"> • FQDN • Geo Location • IPv4 Prefix • Port <p>When ISE is enabled, then SGT option is available in the Source and Destination. Identity User or User group is only supported for Source.</p>

Field	Description
Action	Choose the desired action conditions. The options are: <ul style="list-style-type: none"> • Pass • Drop • Inspect • Log Events: Unified Logging for Inspect Action. Select Advanced Inspection Profile from the drop-down list.

Configure an Embedded Security Sub-Policy

1. From the **Configuration > Policy Groups**, choose **Embedded Security**.
2. Choose a security policy from the list and click **Edit**. and enter the following details.
3. Click **Add Sub-Policy** to add sub-policies for a security policy.

Field	Description
VPN / Interface	Specify the VPN or the interface.
Source Zone	Choose the zone that is the source of the data packets.
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: <ul style="list-style-type: none"> • 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.

Field	Description
Destination Zone	Choose the zone to which data traffic is sent. The options are: <ul style="list-style-type: none"> • Any • Corporate_Users • Local_Internet_for_Guests • Payment_Processing_Network • Physical_Security_Devices • Self • Untrusted (VPN 0)
Match	Choose the desired match conditions from the Add Conditions drop-down list. The options are: <ul style="list-style-type: none"> • Applications • Protocol • Source <ul style="list-style-type: none"> • Geo Location • IPv4 Prefix • Port • Destination <ul style="list-style-type: none"> • FQDN • Geo Location • IPv4 Prefix • Port
Action	Choose the desired action conditions. The options are: <ul style="list-style-type: none"> • Pass • Drop • Inspect • Log Events - Unified Logging for Inspect Action. Select Advanced Inspection Profile from the drop-down list.

Field	Description
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 .

Configure Embedded Security Additional Settings

1. From the Cisco SD-WAN Manager menu, choose **Configuration > Policy Groups**, choose **Embedded Security**.
2. Choose a security policy from the list and click **Edit** and enter the following details.
3. Click **Additional Settings** to configure additional settings for a security policy.

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.

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.
Select an Intrusion Prevention	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.

5. Choose the intrusion prevention from the **Select an 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: <ul style="list-style-type: none"> • Balanced • Connectivity • Security
Inspection Mode	Specify the inspection mode. The options are: <ul style="list-style-type: none"> • Detection • Protection
Advanced	

Field	Description
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: <ul style="list-style-type: none"> • 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.
Alert Log Level	Choose the alert log level: <ul style="list-style-type: none"> • Error • Emergency • Alert • Critical • Warning • Notice • Info • Debug

6. Click **Add**.
7. Choose the advanced malware protection profile from the **Select an 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: <ul style="list-style-type: none"> • NAM • EU • APJC
Inspection Mode	Specify the inspection mode. The options are: <ul style="list-style-type: none"> • Detection • Protection

Field	Description
Alert Log Level	Choose the alert log level: <ul style="list-style-type: none"> • Critical • Warning • Info
File Analysis	Enable file analysis.
Select TG Cloud Region	Choose the cloud region from the drop-down list. The options are: <ul style="list-style-type: none"> • NAM • EU
Alert Log Level	Choose the alert log level: <ul style="list-style-type: none"> • Critical • Warning • Info
Select one or more file types	Choose one or more file type from the drop-down list: <ul style="list-style-type: none"> • All • pdf • ms-exe • new-office • rtf • mdb • mscab • msole2 • wri • xlw • flv • swf

8. Click **Add**.
9. 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: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • 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.
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: <ul style="list-style-type: none"> • Block Page Content • Redirect URL: Specify the redirect URL
Alerts And Logs	Choose one or more file type from the drop-down list: <ul style="list-style-type: none"> • Blocklist • Allowlist • Reputation/Category

10. Click **Add**.

11. Choose **TLS Action**.

Field	Description
TLS Action	Choose the web category from the drop-down list. The options are: <ul style="list-style-type: none"> • Decrypt • Pass Through • Do not Decrypt
Select an TLS/SSL Decryption	Choose the TLS/SSL decryption profile from the drop-down list or Create New profile.

Configure a Secure Service Edge

Before You Begin

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

Configure a Secure Service Edge

Choose the **SSE Provider**. The options are:

- Cisco Secure Access

Configure a Tracker

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.

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

Table 4: 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

Field	Description
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

4. Click **Add**.

Configure Tunnels

To create tunnels, click **Configuration** and do the following:

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

Table 5: Basic Settings

Field	Description
Tunnel Type	• Cisco Secure Access: (Read only) ipsec
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.
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)	

Field	Description
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
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

Field	Description
IKE Cipher Suite	<p>Specify the type of authentication and encryption to use during IKE key exchange.</p> <p>Choose one of the following:</p> <ul style="list-style-type: none"> • AES 256 CBC SHA1 • AES 256 CBC SHA2 • AES 128 CBC SHA1 • AES 128 CBC SHA2 <p>Default: AES 256 CBC SHA1</p>
IKE Diffie-Hellman Group	<p>Specify the Diffie-Hellman group to use in IKE key exchange, whether IKEv1 or IKEv2.</p>
IPSec	
IPsec Rekey Interval	<p>Specify the interval for refreshing IPsec keys.</p> <p>Range: 3600 to 1209600 seconds (1 hour to 14 days)</p> <p>Default: 3600 seconds</p>
IPsec Replay Window	<p>Specify the replay window size for the IPsec tunnel.</p> <p>Options: 64, 128, 256, 512, 1024, 2048, or 4096 packets.</p> <p>Default: 512</p>
IPsec Cipher Suite	<p>Specify the authentication and encryption to use on the IPsec tunnel.</p> <p>Options:</p> <ul style="list-style-type: none"> • AES 256 CBC SHA1 • AES 256 CBC SHA 384 • AES 256 CBC SHA 256 • AES 256 CBC SHA 512 • AES 256 GCM <p>Default: AEM 256 GCM</p>

Field	Description
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: <ul style="list-style-type: none"> • Group-2 1024-bit modulus • Group-14 2048-bit modulus • Group-15 3072-bit modulus • Group-16 4096-bit modulus • None: disable PFS

3. Click **Add**.

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.

Configure High Availability

To designate active and back-up tunnels and distribute traffic among tunnels, click **High Availability** and do the following:

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

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

Field	Description
Active Interface Weight	<p>Enter weight (weight range 1 to 255) for load balancing.</p> <p>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.</p> <p>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.</p>
Backup Interface	<p>To designate a back-up tunnel, choose a tunnel that connects to the secondary data center.</p> <p>To omit designating a back-up tunnel, choose None.</p>
Backup Interface Weight	<p>Enter weight (weight range 1 to 255) for load balancing.</p> <p>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.</p> <p>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.</p>

3. Click **Add**.

Configure DNS Security

The 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.

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

Field	Description
Create New	Displays the DNS Security Policy wizard.
Policy Name	Enter a name for the policy.
Umbrella Registration Status	Displays the status of the API Token configuration.
Manage Umbrella Registration	<p>Click Manage Umbrella Registration to add Cisco Umbrella Registration Key and Secret. Specific network-devices keys are used in DNS.</p> <ul style="list-style-type: none"> • Enter Organization ID. • Enter Registration Key. • Enter Secret. <p>You can edit the umbrella credentials from Administration > Settings > Cloud Provider.</p>
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.
Local Domain Bypass List	Choose the domain bypass.
DNS Server IP	<p>Configure DNS Server IP from the following options:</p> <ul style="list-style-type: none"> • Umbrella Default • Custom DNS
DNSCrypt	Enable or disable the DNSCrypt.

