Security Policy Using Policy Groups

Security Policy Using Policy Groups

Table 1: Feature History

Feature Name	Release Information	Description
Security Policy Using Policy Groups	Cisco IOS XE 17.14.1a	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. 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.

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**
- **Application Priority and SLA**
- **NGFW**
- **Secure Internet Gateway**
- **Secure Service Edge**
- **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** > **Objects and Profiles**.
2. Click the **Security Objects** 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.

Data Prefix IPv6

From Cisco IOS XE 17.18.2, you can configure an object group.

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

Rule Set

From Cisco IOS XE 17.18.2, you can configure an object group.

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

To configure rules within a rule set, see Configure Firewall Policies for SD-Routing Devices.

Object Group

From Cisco IOS XE 17.18.2, 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.

For more information on match conditions, see Configure Firewall Policies for SD-Routing Devices.

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.

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.

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.

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.

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

Signature Set

Field	Description
IPS Signature Set Name	Name of the IPS signature set.
Base Signature Set	Choose a Base Signature Set from the following options: • **Connectivity**: Delivers basic security by applying fewer rules, prioritizing higher network throughput and performance while offering less restrictive protection • **Balanced**: Provides balanced security that actively protects the system while maintaining high network throughput and minimizing false positives, ensuring strong protection without compromising performance • **Security**: Provides enhanced security with increased detection capabilities, offering greater protection than the Balanced level. Designed for administrators who are willing to accept some network latency and a low rate of false positives to identify more potential threats. • **Max-detect**: This ruleset is designed specifically for use in testing environments and is not optimized for production performance. A higher rate of false positives is anticipated and acceptable for many of the rules included in this policy. As a result, investigations into false positives will generally not be conducted. • **No-Rules-Active**: No detection rules enabled; used for testing or troubleshooting. **Note** For more information on creating custom signature sets, refer Custom IPS Signature Sets.

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

The security group of interest has the following profiles:

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

Advanced Inspection Profile

Field	Description
Profile Name	Name of the advanced inspection profile.
Description	The description of the profile.
Intrusion Prevention	Choose an intrusion prevention option from the drop-down list.
URL Filtering	Choose a URL filter from the drop-down list.
Advanced Malware Protection	Choose an advanced malware protection.
TLS Action	Choose the TLS action. The options are: • Decrypt • Pass Through • Do not Decrypt
TLS/SSL Decryption	Choose a TLS/SSL Decryption profile from the drop-down list or click **Create New** to create a new no decrypt domain list. **1.** Enter **No Decrypt Domain List Name**. **2.** Enter **No Decrypt Domain** **3.** Click **Add**.

Advanced Malware Protection Policy

Field	Description
Profile Name	Name of the advanced malware protection policy name.

Field	Description
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
File Analysis	Enable file analysis.
TG Cloud Region	Select TG Cloud region. The options are NAM and EU.
Alert Log Level	Choose the alert log level. The options are: • Critical • Warning • Info
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.

Intrusion Prevention Policy

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. • **Max-Detect**: Most restrictive; enables all detection rules for maximum protection, with the highest performance impact. • **No-Rules-Active**: No detection rules enabled; used for testing or troubleshooting, with no protection or performance impact. From 17.18.1a, you can select a previously created custom signature set or create a custom signature set by selecting **+ Create New** and customize your own signature set. For more information, refer Custom IPS signature sets.
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.
Advanced Options	
Custom Signature Set	Enable the Global custom signature set using the **radio button**.
Signature Allow List	Select a signature allow list.
Alerts Log Level	Choose the alert log level: • Error • Emergency • Alert • Critical • Warning • Notice • Info • Debug

TLS/SSL Decryption

Field Name	Description
Add TLS/SSL Decryption	Click **Add TLS/SSL Decryption**. A dialog box will appear.
Configure Certificate Authority (CA)	Click **Configure Certificate Authority** to set up the CA required for decryption. **Note** The TLS/SSL Proxy feature will now allow SAIE to decrypt encrypted connections for malware detection and to enforce security policies based on higher-layer traffic. For more information, refer Configure an SD-Routing Device as an SSL/TLS Proxy.
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	

Field Name	Description
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.
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.

TLS/SSL Profile

Field	Description
Profile Name	Name of the TLS/SSL profile.

Field	Description
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	
Decrypt Domain list	Choose the decrypt domain list or click **Create New** to create a new decrypt domain list. 1. Enter **Decrypt Domain List Name**. 2. Enter **Decrypt Domain** 3. Click **Add**.
No Decrypt Domain list	Choose the no decrypt domain list or click **Create New** to create a new no decrypt domain list. 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.

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 categories	Select one or more web categories from the drop-down list. The categories are: abortion, abused-drugs, auctions, and so on.
Allow URL list	Select an allow URL list.
Block URL list	Select a block URL list.

Field	Description
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

Configure Application Priority and SLA

The application priority and SLA policies allows you to configure the app route policy, data policy, and QoS Map policies that route and prioritize traffic for best performance. All the basic information is preconfigured. You can specify a name and description for a policy group and configure the basic policy values. You can quickly configure the basic values to get started with the traffic policy.

To configure Application Priority & SLA, follow the steps below:

1. Click **Application Priority & SLA policy**.
2. Enter the **Policy Name** and **description**.
3. Click **Create**.

Choose one of the following options and configure the values that are based on the likely business relevance of the applications, and to give higher priority to business-relevant applications:

- **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 of the business-relevance categories, the workflow groups the applications into application lists, such as broadcast video, multimedia conferencing, VoIP telephony, and so on.

Table 2: Cisco Catalyst SD-WAN Fabric Traffic Policy

Field	Description
Preferred Path	To configure a preferred path, select one or more data plane tunnel colors from the drop-down list. Traffic will be load-balanced across all selected tunnels. If no tunnels meet the SLA requirements, data traffic is sent through any available tunnel. Preferences are applied in order of priority to determine the forwarding path or color.
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	To configure an alternate traffic path, select a backup path from the drop-down list. This path is used if the primary path fails.
Traffic Filtering	Click **Edit** to view and update application classification based on business relevance. Choose a service provider class and organize applications into classes like Gold or Bronze. Click **Save** to update the configuration.
SLA	Add the SLA class to the traffic policy. Click **Edit** to adjust the SLA class values for Loss (%), Latency (ms), or Jitter (ms).
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 3: Internet Offload Traffic

Field	Description
Secure Internet Gateway	Choose an application or family list to direct traffic through a Secure Internet Gateway. Enable fallback routing for traffic when SIG tunnels are down.

Field	Description
Direct Internet Access	Select an application or family list for direct internet access. Enable fallback routing for traffic if Direct Internet Access (DIA) is not available.

Table 4: 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 NGFW

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.

Follow the below steps to create NGFW Policy:

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Policy Groups** > **NGFW.**
2. Click **Add NGFW Policy**.
3. In the **Create NGFW Policy** dialog box, click **Let's do it**.
4. In the NGFW tab,

- Enter the **Policy Name** and **description**.
- Select **SD-Routing** as the device solution.
- Click **Next**.

5. (Optional) Select Configuration Groups – Not applicable for SD-Routing policies. Click **Next**.
6. In the Create Sub Policies tab,
   - Click **Add Sub-Policy**
   - Choose **Source Zone**
   - Choose **Destination Zone**
   - Click **Save**
7. In the **Add Rule** dialogue box, configure the following and save.

Field	Description
Rule Name	The name of the rule.
Sequence	Specify the sequence.
Match	Choose the desired match conditions from the **Add Conditions** drop-down list.
Traffic Source - Data Prefix	(Optional) Enter the Data Prefix of the Traffic Source.
Traffic Destination - Data Prefix	(Optional) Enter the Data Prefix of the Traffic Destination.
Protocol	(Optional) Select the preferred protocol.
Application	(Optional) Select the preferred application.
Action	(Optional) Choose the preferred action conditions.

8. (Optional) Click **Additional Settings** and configure the following:

Field	Description
TCP SYN Flood Limit	Specify the threshold of SYN flood packets per second for each destination address.
Max Incomplete	Specify the timeout limits for the firewall policy. A Max Incomplete timeout limit protects firewall resources and keeps these resources from being used up.
TCP Limit	Specify the maximum TCP half-open sessions allowed on a device.

Field	Description
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.
TLS/SSL Decryption	Choose the TLS/SSL decryption profile from the drop-down list
High Speed Logging Source File	Add security logging servers. You can configure 4 source interfaces for HSL
External Syslog Server	Select and configure the source interface for UTD.

- Click **Save**.
- Select **Next**.

9. In the Summary tab, verify and edit the details if required and Click **Create NGFW Policy**.

Configure a 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.

To configure a secure internet gateway, follow the below steps:

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

2. Click **Add Secure Internet Gateway (SIG)**.
3. Enter a **name** and provide a **description** (optional).
4. Click **Create**
5. Choose an **SIG Provider** from the options below:
    - Umbrella
    - Zscaler
    - Generic

Umbrella Configuration

To configure Umbrella SIG Provider, follow the these steps:

1. Select **Click here to add Umbrella credentials.**
2. In the Add **Umbrella credentials** dialog box, configure the following and click **Add**.

Table 5: Cisco Umbrella Credentials

Field	Description
Organization ID	Enter the Cisco Umbrella organization ID (Org ID) for your organization.
Scope Credentials	Enter the API Key and API Secret.
Legacy Credentials	Enter the API Key and API Secret.

Zscaler Configuration

You can access Zscaler credentials from **Administration** > **Settings** > **Cloud Provider Credentials**.

To configure Zscaler SIG Provider follow the below steps:

- Select **Click here to add Zscaler credentials**.
- In the Add **Zscaler credentials** dialog box, configure the following and click **Add**.

Table 6: Zscaler Credentials

Field	Description
Organization ID	Enter the name of the organization in Zscaler cloud.
Partner base URI	Enter Partner base URI. This is the base URI that Cisco SD-WAN Manager uses in REST API calls.
Partner Key	Enter Partner API key.
Username	Enter username of the Cisco Catalyst SD-Routing partner account.
Password	Enter username of the Cisco Catalyst SD-Routing partner account.

Generic Configuration

Tracker Configuration

To create one or more trackers to monitor tunnel health, do the following under **Tracker:**

1. Enter a **source IP address** for the probe packets.
2. Click **Add Tracker**.
3. In the **Add Tracker** dialog box, configure the following and click **Add**.

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

Tunnel Configuration

To create tunnels, do the following under **Configuration**:

1. Click **Add Tunnel**.
2. In the **Add Tunnel** dialog box, configure the following and click **Add**.

Table 7: Basic Settings

Field	Description
Tunnel Type	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.
Tunnel Destination IP Address/FQDN	The IP address of the SIG provider endpoint. The configuration of FQDN for Tunnel Destination IP address is not supported.
Preshared Key	This field is displayed only if you choose **ipsec** as the **Tunnel Type**. Enter the password to use with the preshared key. This field is displayed only if you choose ipsec as the Tunnel Type.
Advanced Options	
Shutdown	Click to enable the interface. Default: disabled.
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
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: 3600 to 1209600 seconds (1 hour to 14 days) Default: 14400 seconds

Field	Description
IKE Cipher Suite	Specify the type of authentication and encryption to use during IKE key exchange.
IKE Diffie-Hellman Group	Specify the Diffie-Hellman group to use in IKE key exchange, whether IKEv1 or IKEv2.
IKE ID for Local End Point	Specify the IKE ID for Local End Point.
IKE ID for Remote End Point	Specify the IKE ID for Remote End Point.
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, 4096. Default: 512
IPsec Cipher Suite	Specify the authentication and encryption to use on the IPsec tunnel. Default: AES 256 GCM
Perfect Forward Secrecy	Specify the PFS settings to use on the IPsec tunnel.

High Availability Configuration

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** dialog box, configure the following and click **Add**

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.
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.

Configure Secure Service Edge

Cisco Secure Access is a cloud-based platform that provides multiple levels of defense against internet-based threats. To configure Secure Service Edge (SSE), choose Cisco Secure Access as the provider in the SSE policy group in Cisco SD-WAN Manager. The SSE policy group defines IPSec tunnels and tunnel parameters. You can provision network tunnel groups in Cisco Secure Access and provide attributes to the edge devices that are needed to setup IPSec tunnels.

Before You Begin

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

To configure Secure Service Edge, follow these steps:

1. From the Cisco SD-WAN Manager menu **Configuration** > **Policy Groups** > **Secure Internet Gateway/Secure Service Edge.**
2. Click **Add Secure Service Edge(SSE)**
3. Enter a **name** and select **SD-Routing** from the Solution drop down list
4. (Optional) Provide a description.
5. Click **Create**.
6. Select **Click here to add cisco-sse credentials** and configure the following:

Field	Description
Cisco SSE Organization ID	Cisco Secure Access organization ID for your organization.
Cisco SSE API Key	Cisco Secure Access API Key.
Cisco SSE API Secret	Cisco Secure Access API Secret.

7. Click **Add**

Configure 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.

To configure DNS Security, follow the steps below:

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Policy Groups** > **DNS Security**.
2. Click **Add DNS Security Policy**.
3. Enter a **name** and provide a **description** (optional)

4. Click **Create** and configure the following:

Field	Description
Umbrella Registration Status	Displays the status of the API Token configuration.
Manage Umbrella Registration	Click **Manage Umbrella Registration** to add Cisco Umbrella Registration Key and Secret. Enter the following details: **a. Scope Credentials** • Enter **Organization ID**. • Enter **API Key** • Enter **Secret**. **b. Legacy Credentials** • Enter **API Key** • Enter **Secret** **c.** Click **Save Changes.** **Note** Note, you can edit the umbrella credentials from **Administration** > **Settings** > **Cloud Provider**.
Match All VPN	
Match All VPN	Click **Match All VPN** to keep the same configuration for all the available VPNs.
Local Domain Bypass List	Choose the local domain bypass from the drop down list or **Create New**.
DNS Server IP	Configure **DNS Server IP** from the following options: • **Umbrella Default** • **Custom DNS**
DNSCrypt	Enable or disable the DNSCrypt.
Custom VPN Configuration	
Custom VPN Configuration	choose **Custom VPN Configuration** to input the specific VPNs.
Local Domain Bypass List	Choose the domain bypass from the drop down list or **Create New**.
DNSCrypt	DNSCrypt is disabled by default.

Field	Description
Target VPN	Click **Add Target VPN** and enter the following fields: **a.** VPNs - Select the VPN from the drop-down list. **b.** DNS Server IP - Configure **DNS Server IP** from the following options: • **Umbrella Default** • **Custom DNS** **c.** Local Domain Bypass - Choose the domain bypass and **Save** changes

5. Click **Save**.