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 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.

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.
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
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.

Feature Name	Release Information	Description
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	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.
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	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	With this feature the local domain bypass entries are increased to 256.
Increase in FQDN Scale	Cisco IOS XE Catalyst SD-WAN Release 26.1.1 Cisco Catalyst SD-WAN Manager Release 26.1.1	With this feature the FQDN entries are increased to 256.

Information About Security Policy

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

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

- **Policy Group** (see Policy Group chapter)
- **Application Priority & SLA** (see Policy Group chapter)

- **NGFW**

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

- **Secure Internet Gateway (SIG)**
- **DNS Security**

Version management for security policies

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

With this feature Cisco SD-WAN Manager supports multiple versions of the same security policy. You can view and revert to an older version of the feature configuration at any point. Before making any new changes you do not need to copy or backup the feature configurations manually.

Every time you make changes to the security policy, a new version of the policy is generated, and the older versions are maintained in Cisco SD-WAN Manager. Cisco SD-WAN Manager saves only the last 30 versions.

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** > **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

6. Click **Add**.

Restrictions for Security 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

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**. Refer to the steps used in the procedure, Configure an NGFW Sub-Policy, on page 21.
7. Click **Submit**.You can view the new security policy in the **Embedded Security** tab.

Configure policy objects for a Security policy

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

   Group of Interest is now called as **Objects and Profiles**.
2. Click the **Security Objects** tab. The list of security objects and profiles appears.

   Security is now called as **Security Objects**.

Note 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.

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. **Note** See the information about custom applications in Restrictions for Security Policy.

Field	Description
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 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.

To configure rules within a rule set, see Configure NGFW.

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.

Field	Description
Description	Description of the object group
Type	You can choose IPv6 or IPv4.

To see more information on the match conditions, see Configure NGFW.

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. From Cisco Catalyst SD-WAN Manager Release 26.1.1, 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

Field	Description
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.

Click **Security profiles** to configure 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.
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 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. • **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.

Field	Description
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 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: • 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.

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

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
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.

Field	Description
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. 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. 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: • **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: • **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.
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	

Field Name	Description
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.

Configure NGFW

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

Cisco SD-WAN NGFW policy offers comprehensive protection for enterprise networks, integrating features such as Application Firewall, IPS, URL Filtering, AMP, TLS Proxy, and DNS security. These policies enable organizations to create rules that manage traffic flow between defined zones. A zone is a group of one or more VPNs, which helps establish security boundaries within the overlay network, allowing control over all data traffic that passes between zones.

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

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Policy Groups** > **NGFW**.
2. Choose a security policy and click **Edit**.
3. Click **Add Rule** or **Rule with Rule Sets**.

   From Cisco Catalyst SD-WAN Manager Release 20.18.2, you can add a rule set within a rule.

   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
	  • Port
	• Destination
	  • FQDN
	  • Geo Location (Supported when the chosen type is IPV4
	  • IPv4 Prefix
	  • 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 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
	  • Port
	• Destination
	  • FQDN
	  • Geo Location (Supported when the chosen type is IPV4
	  • IPv4 Prefix
	  • 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

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

   In Cisco Catalyst SD-WAN Manager Release 20.15.1 and earlier releases, **NGFW** is called **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: • 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

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 NGFW Additional Settings

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**.

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.
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.

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: • Balanced • Connectivity • Security

Field	Description
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.
Alert Log Level	Choose the alert log level: • 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: • NAM • EU • APJC

Field	Description
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.
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

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: • 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.
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

10. Click **Add**.
11. 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
Select an TLS/SSL Decryption	Choose the TLS/SSL decryption profile from the drop-down list or **Create New** profile.

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 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.

Access Umbrella credentials from **Administration** > **Settings** > **Cloud Credentials**.

To configure a secure internet gateway:

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Policy Groups** > **Secure Internet Gateway**.
2. Click **Add Secure Internet Gateway**.
3. Choose **SIG Provider**. The options are:
    - Umbrella
    - Zscaler
    - Generic

Umbrella Configuration

Table 2: 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.

Zscaler Configuration

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

Table 3: Zscaler Credentials

Field	Description
Organization	Name of the organization in Zscaler cloud.

Field	Description
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.

Generic Configuration

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

Parameter Scope	Scope Description
Device Specific (indicated by a host icon)	Use device-specific value for the parameter. For device-specific parameters, you cannot enter value in the feature template. Enter the value when you add a device to the configuration group. To change the default key, type a new string and move the cursor out of the **Enter Key** box.
Global (indicated by a globe icon)	Enter value for the parameter, and apply that value to all devices.

1. Click **Add Tunnel**.
2. In the **Add Tunnel** dialog box, under **Basic Settings** configure the following:

Table 4: Basic Settings

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.
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.

Field	Description
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

3. Click **Add**.

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.

Tracker Configuration

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

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

Table 5: 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.

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 down. Range: 1 to 10 Default: 3

4. Click **Add**.

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:

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.

3. Click **Add**.

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

Enable Context Sharing

Enable context sharing for VPN and SGT to allow Cisco IOS XE Catalyst SD-WAN devices to share context information with SSE:

Table 6: Context Sharing

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

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 7: 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

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 8: 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.

Field	Description
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.
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

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:

Table 9: Add interface pair

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 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.

3. Click **Add**.

Advanced Settings

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

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.

Zscaler Location

Table 10: 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.

Gateway Options

Table 11: 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

Field	Description
Enable Firewall	See *ZIA Help > Traffic Forwarding > Location Management > Configuring Locations*. Default: Off

Bandwidth Control

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

Table 12: 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*.

Sub-Locations

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

Table 13: 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

Field	Description
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
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

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.

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.
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 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 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 the following: • **Name** • **Description** (optional) • **Local domain** From Cisco Catalyst SD-WAN Manager Release 26.1.1, 256 local domain bypass entries are supported.
DNS Server IP	Configure **DNS Server IP** from the following 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.

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.

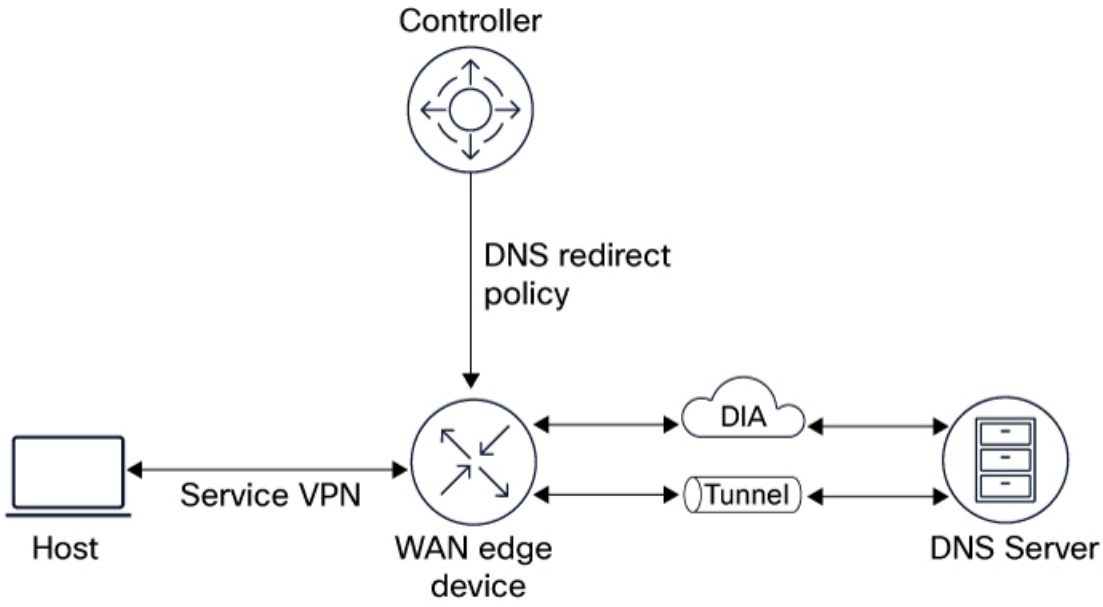
Integration with NAT trackers

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



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
```