Manage Catalyst SD-WAN Security Objects and Security Profiles

An Introduction to Catalyst SD-WAN Security Objects and Security Profiles

Security objects and security profiles in Catalyst SD-WAN Manager are the foundational building blocks for defining and enforcing security NGFW policies. They ensure that your network is protected from threats while maintaining seamless connectivity and application performance.

Create new Catalyst SD-WAN Security Objects and Security Profiles

This section provides the steps to create new Catalyst SD-WAN objects and profiles using Security Cloud Control Firewall Management.

Procedure

Step 1 In the left pane, click **Manage** > **Objects**.

Step 2 Click the **WAN Branch Edge** tab.

Step 3 Click the **Create Object** (+) icon.

Step 4 Click the object or profile you want to create:

Objects:

- Application List
- Data Prefix
- FQDN
- Geolocation
- Identity
- Port
- Protocol
- Security Group Tag
- Signature
- URL Allow
- URL Block
- Zone

Profiles:

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

Step 5 Click **Save**.

The objects are created in Security Cloud Control. To see the logs in Catalyst SD-WAN Manager, navigate to **Monitor** > **Logs** > **Audit Logs** .

SDWAN Application List

The application list object groups applications into a list for use in NGFW policies.

Table 1: Application

Field	Description
Object Name	Name of the application list.
Application List	A collection of specific applications grouped together for policy configuration. It allows administrators to define and manage traffic rules for multiple applications as a single entity. For example, "Webex," "Microsoft Teams," "Zoom," and so on.

Field	Description
Application Family	The **Application Family** groups applications based on their functional category, for example, "Web," "Instant Messaging," "Network Services," and so on.

The **Selected items** field shows the items that have been chosen.

SDWAN Data Prefixes

The data prefixes are specific IP address ranges or prefixes that are used to define and manage traffic routing policies within the SD-WAN fabric.

Table 2: SDWAN Data Prefixes

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

SDWAN FQDN

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

Table 3: Application

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

SDWAN Geolocation

Allows you to configure firewall rules based on geographical locations rather than IP addresses.

Table 4: Geolocation

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

SDWAN Identity

Table 5: SDWAN Identity

Field	Description
Object Name	Name of the application list.
Users	The source of **Users** and **User Groups** is ISE AD, which is configured in Catalyst SD-WAN Manager.
User Groups	

SDWAN Port Object

A configuration element used to define and manage port-related settings for devices within the SD-WAN fabric.

Table 6: Port Object

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

SDWAN Protocol Object

Within security policies, protocols can be selected from a predefined list (for example, TCP, UDP, ICMP) to define specific rules for traffic management and security enforcement.

Table 7: Protocol Object

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

The **Selected items** field shows the items that have been chosen.

SDWAN Security Group Tag

If you use Cisco Identity Services Engine (ISE) to define and use **security group tag** (SGT) for classifying traffic in a Cisco TrustSec network, you can write access control rules that use SGT as matching criteria.

You cannot create or edit an SGT in Security Cloud Control. All SGTs must be created in ISE.

Table 8: Security Group Tag

Field	Description
Object Name	Name of the security group tag.
Security Group Tags	Select the security group tag.

The **Selected items** field shows the items that have been chosen.

SDWAN Signatures

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.

Table 9: Application

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

SDWAN URL Allow List

The URL allow list object is used to define URLs that should be explicitly permitted through the SD-WAN's URL Filtering feature.

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.

Table 10: URL Allow List

Field	Description
Object Name	Name of the URL allow object.
URL Allow	The URLs to allow.

SDWAN URL Block List

The URL block list object is used to define URLs that should be denied through the SD-WAN's URL Filtering feature.

Table 11: URL Block List

Field	Description
Object Name	Name of the URL block object.
URL Allow	The URLs to block.

SDWAN Zone

Zones are used to define security boundaries for traffic control. Zones can be configured based on **VPNs** or **Interfaces**:

- Zones can be created for specific VPNs, such as the Payment Processing Network, Corporate Users, or Local Internet for Guests. These zones allow you to apply security policies to traffic within or between VPNs.
- Interfaces can also be assigned to zones. For example, Ethernet, GigabitEthernet, or other interface types can be grouped into zones. This allows for granular control of traffic between interfaces.

Table 12: Zone

Field	Description
Object Name	Name of the zone.
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.

SDWAN Advanced Inspection Profile Policy

Apply a global Advanced Inspection Profile (AIP) at the device level. This ensures that all traffic matching the device's predefined rules is thoroughly inspected using the advanced inspection profile.

Table 13: Advanced Inspection Profile Policy

Field	Description
Object Name	Name of the advanced inspection 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

SDWAN Advanced Malware Protection Policy

Note that for some advanced configurations, a Threat Grid Server configuration is required in Catalyst SD-WAN.

Table 14: Advanced Malware Protection Policy

Field	Description
Object Name	Name of the advanced malware protection policy name.
AMP Cloud Region	**AMT Cloud Region** refers to the **Analytics, Management, and Telemetry (AMT) Cloud Region** associated with the Cisco SD-WAN cloud architecture.
Alert Log Level	All syslog messages are associated with priority levels that indicate the severity of syslog messages to save.
File Analysis	Enables file analysis on the uploaded files.
TG Cloud Region	Choose a region. This refers to the geographical region where the Threat Grid (TG) cloud services are hosted.
File Types	Choose the file types that you want to be analyzed.

SDWAN Intrusion Prevention Policy

A security feature designed to detect and block known network attacks by leveraging predefined rules and signature.

Table 15: Intrusion Prevention Policy

Field	Description
Object Name	Name of the intrusion prevention policy.
Signature Set	Choose a signature set that defines the rules for evaluating traffic from the **Signature Set** drop-down list.
Inspection Mode	Choose the inspection mode.
Custom Signature Set:	Select one or more web categories from the drop-down list. Custom signature must be enabled from Catalyst SD-WAN Manager under **Administration > Settings > External Services > UTD Snort Subscribe Signature**.
Signature Allow List	Select a signature allow list.
Alerts Log Level	Choose the alert log level. This refers to the severity levels of logs generated by the system, which can be configured to control the granularity of information logged.

SDWAN TLS/SSL Decryption Policy

The **TLS/SSL Decryption** object refers to a feature or configuration that enables administrators to inspect and manage encrypted traffic passing through the network.

Note Before creating a **TLS/SSL Decryption** object in Security Cloud Control, you need to configure certificate authority (CA) from Catalyst SD-WAN Manager under **Configuration** > **Certificates** > **Certificate Authority**.

Table 16: TLS/SSL Decryption Policy

Field	Description
Object 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	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	
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.

SDWAN TLS/SSL Profile Policy

The TLS/SSL Profile policy is used to manage encrypted traffic within a unified security policy. To create a TLS/SSL Profile Policy in Security Cloud Control, you need to first configure the **Certificate Authority (CA) Certificate** in Catalyst SD-WAN. This is a prerequisite for enabling the TLS proxy functionality.

Table 17: TLS/SSL Profile Policy

Field	Description
Object Name	Name of the TLS/SSL profile.
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**. Supports actions based on URL reputation levels.
Decrypt Domain List	Choose the decrypt domain list.
No Decrypt Domain List	Choose the no decrypt domain list.
Fail Decrypt	Enable the fail decrypt option, if decryption fails.

SDWAN URL Filtering Policy

A security feature that allows administrators to control access to websites based on categories, reputation, and custom lists.

Table 18: URL Filtering Policy

Field	Description
Object Name	Name of the URL filtering policy.
Web Category	Choose the web category. The options are Block and Allow. The websites are classified into categories.
Web Reputation	Choose the web reputation from the drop-down list. The URLs are assigned a reputation score based on their risk level.
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. The blocked users can be redirected to a custom page or shown a message.
Alerts and Logs	Choose the alert and log type: • Blocklist • Allowlist • Reputation/Category

Modify Catalyst SD-WAN Security Objects and Security Profiles

Use this procedure to modify the values associated with the Catalyst SD-WAN security objects and security profiles from the Security Cloud Control Firewall Management.

Procedure

Step 1 In the left pane, choose **Administration** > **Integrations** > **Catalyst SD-WAN**.

Step 2 In the left pane, click **Manage > Objects**.

Step 3 Click the **WAN Branch Edge** tab.

Step 4 Check the security object or profile you want to modify. You can use the filter to search an object.

Step 5 In the **Actions** pane on the right, click **Edit**.

Modify the configurations you want.

Step 6 Click **Save** to confirm.

Delete Catalyst SD-WAN Security Objects

You can delete one or multiple Catalyst SD-WAN security objects.

- If the security object was synchronized with Catalyst SD-WAN Manager, its deletion will be reflected across both Security Cloud Control Firewall Management and Catalyst SD-WAN Manager to maintain consistency.
- Any security policies or configurations referencing the deleted object do not get deleted automatically. You must remove the references manually from the security policies before deleting the object.

- Delete actions are logged for audit purposes, ensuring traceability of changes. To view the logs:
  - In the Security Cloud Control application, choose **Monitor** > **Events & Logs** > **Logs** > **Change Log**.
  - In the Catalyst SD-WAN Manager application, choose **Monitor > Logs > Audit Logs**.

Before you begin

Make sure the Catalyst SD-WAN security objects you intend to delete are not being used or referenced in other objects, policies, or configurations.

Procedure

Step 1 In the left pane, choose **Administration** > **Integrations** > **Catalyst SD-WAN**.

Step 2 In the left pane, click **Manage > Objects**.

Step 3 Click the **WAN Branch Edge** tab.

Step 4 Check one or multiple security objects you want to delete.

Step 5 In the **Actions** pane on the right, click **Remove**.

Step 6 Click **OK** to confirm.

Selected Catalyst SD-WAN security objects are deleted. Delete actions are logged for audit purposes, ensuring traceability of changes.

To view the logs:

- In the Security Cloud Control application, choose **Monitor** > **Events & Logs** > **Logs** > **Change Log**.
- In the Catalyst SD-WAN Manager application, choose **Monitor > Logs > Audit Logs**.

Filter Catalyst SD-WAN Security Objects

The ability to filter and search for Catalyst SD-WAN security objects by **Object Type** and **Profile Type** allows users to efficiently locate, review, modify, and, when needed, delete these objects. Streamlining the management processes helps maintain optimal system performance.

Two filtering parameters used are **Object Type** and **Profile Type**.

1. In the left pane, choose **Manage > Objects**.
2. Click the **WAN Branch Edge** tab.
3. Click the filter (▼) icon and select for objects based on the object type or profile type.

You can use filters to search for the desired objects and further refine the results by typing the object name, IP address, or port number to narrow down the search within the results.