



Next-Generation Firewall (NGFW)

- [Feature history of NGFW, on page 1](#)
- [NGFW, on page 3](#)
- [Enable RBAC for NGFW policy, on page 3](#)
- [Restrictions for NGFW policy, on page 4](#)
- [Configure NGFW policy using a workflow, on page 5](#)
- [Configure policy objects for an NGFW policy, on page 20](#)

Feature history of NGFW

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.
Add Source Interface for High-Speed Logging and External Syslog	Cisco IOS XE Catalyst SD-WAN Release 17.16.1a Cisco Catalyst SD-WAN Manager Release 20.16.1	This enhancement for security logging allows you to specify the following in the additional settings of the security policy: • Source interfaces for high-speed logging (HSL) servers (up to four) • Source interface for the external syslog server

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

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

NGFW

An NGFW policy is a configuration mechanism that

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

Enable RBAC for NGFW policy

Follow these steps to enable RBAC for NGFW policy:

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

Procedure

- Step 1** From the Cisco SD-WAN Manager menu, choose **Administration > Manage Users > User Groups**.
- Step 2** Click **Add User Group**.
- Step 3** Enter **User Group Name**.
- Step 4** Check a **Read** or **Write** check box for the **Policy Group**, **Device** and **Deploy** feature that you want to assign to a user group.
- Step 5** Check a **Read** or **Write** check box for the following features that you want to assign to a user group:
 - **Feature Profile > DNS Security > DNS Policy**
 - **Feature Profile > Sig Security > Sig Policy**
 - **Feature Profile > NGFW > Legacy Policy**
 - **Feature Profile > NGFW > NGFirewall**
 - **Feature Profile > NGFW > Policy**
 - **Feature Profile > Policy Object > Advanced Inspection Profile**

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

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

Step 6 Click **Add**.

Restrictions for NGFW policy

IPv6 rules or rulesets

IPv6 rules or rulesets do not support identity.

IPv4 rules with rulesets

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

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

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

VPNs or interfaces not present on the target device

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

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

Example:

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

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

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

Replacing a SIG or SSE feature policy

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

Data policy redirecting DNS traffic

Data policy does not support both of these conditions together:

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

NGFW configurations using CLI add-on template

Ensure proper NGFW block configuration:

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

Discontiguous subnet masks in IPv4 network object-group

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

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

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

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

Configure NGFW policy using a workflow

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

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

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

Procedure

-
- Step 1** From the Cisco SD-WAN Manager menu, choose **Workflows > Workflow Library > Create Security Policy > Create NGFW Policy**. Alternatively, choose **Configuration > Policy Groups**.
- Step 2** Click **NGFW**.

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

- Step 3** On the **NGFW** page, click **Add NGFW Policy**.
This launches the NGFW policy workflow.
- Step 4** Enter **Policy Name** and **Description** and click **Next**.
- Step 5** On the **Select the optional Configuration Group to associate with the NGFW policy** page, choose the configuration groups and click **Next**.
- Step 6** Click **Add Sub-Policy**.
Refer to the steps used in the procedure, [Configure an NGFW Sub-Policy, on page 12](#).
- Step 7** Click **Submit**.

Edit NGFW policy

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

For more information on NGFW, see [Enterprise Firewall with Application Awareness](#).

Procedure

- Step 1** From the Cisco SD-WAN Manager menu, choose **Configuration > Policy Groups > NGFW**.
- Step 2** Choose an NGFW policy and click **Edit**.
- Step 3** (Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.18.2) Click **Add Rule** or **Rule with Rule Sets**.
From Cisco IOS XE Catalyst SD-WAN Release 26.1.1, you can drag and drop rules in a policy to modify the priority or sequence number of each rule.

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

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

Field	Description
Match (Rule)	

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

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

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

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

Note

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

Import and export policies

From Cisco IOS XE Catalyst SD-WAN Release 26.1.1 you can import or export the firewall policies. You can use Cisco SD-WAN Manager to export policies as a CSV file, modify the rules as needed, and then import the updated file. This process allows you to efficiently add or update existing rules.

For any NGFW sub-policy, click ... and select **Export** to download the CSV file. After making your modifications, click **Import** to upload the updated CSV file. During the import process, Cisco SD-WAN Manager validates the file and flags any errors.

Hit count

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

A rule hit count represents the total number of times a firewall rule has been accessed. This helps you to analyze rule effectiveness and identify unused rules for removal. For any NGFW sub-policy, click ... and choose **Hit count**. In the sidebar you can view the list of all the firewall rules for the sub-policy and the hit count for each rule. You can also view the hit count for all the sites or a specific site using the sites drop-down menu.

Configure an NGFW Sub-Policy

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

Procedure

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

Table 2: Sub-Policy configuration fields

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

Field	Description
Match	Choose the desired match conditions from the Add Conditions drop-down list. The options are: • Applications • Protocol • Source • Geo Location • IPv4 Prefix • Port • Destination • FQDN • Geo Location • IPv4 Prefix • Port From SD-WAN Manager 26.2.1, IPv4 prefixes support discontinuous subnet mask.
Action	Choose the desired action conditions. The options are: • Pass • Drop • Inspect • Log Events - Unified Logging for Inspect Action. Select Advanced Inspection Profile from the drop-down list.
User / User Group	An identity service engine has to be enabled to configure User / User Group sub policies. You can configure using Administration > Integration Management > Identity Service Engine.

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

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

Configure additional settings for an NGFW policy

Procedure

- Step 1** From the Cisco SD-WAN Manager menu, choose **Configuration > Policy Groups**, choose **NGFW**.
In Cisco Catalyst SD-WAN Manager Release 20.15.1 and earlier releases, **NGFW** is called **Embedded Security**.
- Step 2** Choose an NGFW policy from the list and click **Edit**.
- Step 3** Click **Additional Settings**.

Field	Description
TCP SYN Flood Limit	Specify the threshold of SYN flood packets per second for each destination address.
Max Incomplete	Specify the timeout limits for the firewall policy. A Max Incomplete timeout limit protects firewall resources and keeps these resources from being used up.
TCP Limit	Specify the maximum TCP half-open sessions allowed on a device.
UDP Limit	Specify the maximum UDP half-open sessions allowed on a device.
ICMP Limit	Specify the maximum ICMP half-open sessions allowed on a device.
Audit Trail	Enable the Audit Trail option. This option is only applicable for rules with an inspect action.
Unified Logging	Enable the unified logging feature.
Optimized Policy	Enable the optimized policy option.
Session Reclassify Allow	Allow re-classification of traffic on policy change.
ICMP Unreachable Allow	Allow ICMP unreachable packets to pass through.
Advanced Inspection Profile	Attach a global advanced inspection profile (AIP) at a device level. All the rules in the device that match the traffic to be inspected are inspected using the advance inspection profile.
High Speed Logging Source Interface	Specify the server labels of the source interface used to collect logs for high-speed logging (HSL). You can configure up to four log collector servers for HSL. Ensure that you enable security logging before specifying 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 specifying the source interface. For more information, see Configure Security Logging .

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

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

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

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

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

Click **Add**.

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

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

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

Click **Add**.

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

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

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

Click **Add** .

d) Choose **TLS Action**.

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

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

Step 5 Click **Save**.

Version control for NGFW

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

Procedure

- Step 1** From the Cisco SD-WAN Manager menu, choose **Configuration > Policy Groups**, choose **NGFW**.
- Step 2** Choose a security policy from the list and click **Edit**.
- Step 3** Click **Show version control** to track and manage changes to the security policy.
- Step 4** Select two versions of the security policy and click **View diff** to view the changes made in these versions.
- If you have added any configurations to the security policy, it is highlighted in green. If you have removed any configuration parameters, it is highlighted in red.
- Visual diff for large policy configurations is not available. You can download the configuration using the **Download config** button and compare them manually.
- Step 5** Click **Revert** next to a version if you wish to move back to an older version of the security policy configuration.
- For large policies, create and revert operations can take up to two minutes.

Configure policy objects for an NGFW policy

Before you begin

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

Procedure

- Step 1** From the Cisco SD-WAN Manager menu, choose **Configuration > Policy Groups > Objects and Profiles**.
- In SD-WAN Manager 20.18.1 and earlier releases, **Objects and Profiles** is called **Group of Interest**.
- Step 2** Click **Security objects**. The list of security objects appears.

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

- Application lists

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

- Data Prefix

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

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

- Data Prefix IPv6

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

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

- Rule set

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

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

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

- Object group

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

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

- Local Domain

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

- FQDN (Fully Qualified Domain Name)

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

Table 3:

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

- Signature

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

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

- URL allow

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

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

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

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

- URL block

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

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

- Zone

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

- Port

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

- Protocol

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

- Geo Location

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

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

- Advanced inspection profile

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

- Intrusion prevention

Field	Description
Profile Name	Name of the intrusion prevention policy.

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

- URL filtering

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

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

• Advanced Malware Protection Policy

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

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

- TLS/SSL profile

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

- TLS/SSL decryption

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

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

Step 4 Click **Save**.
