

Network Analysis Policies

This chapter provides an insight into network analysis policy basics, prerequisites, and how to manage network analysis policies. It also provides information on custom network analysis policy creation and network analysis policy settings.

- Network analysis policies, on page 1
- Manage network analysis policies, on page 2
- Snort 3 definitions and terminologies for network analysis policies, on page 3
- Custom network analysis policy creation for Snort 3, on page 5
- Network analysis policy settings and cached changes, on page 33
- Generate Snort 3 recommendations, on page 33

Network analysis policies

A *network analysis policy* is a traffic preprocessing configuration that

- governs many traffic preprocessing options and is invoked by advanced settings in your access control policy,
- performs preprocessing after Security Intelligence matching and SSL decryption, and
- completes processing before intrusion or file inspection begins.

Default and custom network analysis policies

By default, the system uses the *Balanced Security and Connectivity* network analysis policy to preprocess all traffic handled by an access control policy. However, you can choose a different default network analysis policy to perform this preprocessing. For your convenience, the system provides a choice of several non-modifiable network analysis policies, which are tuned for a specific balance of security and connectivity by the Talos Intelligence Group. You can also create a custom network analysis policy with custom preprocessing settings.

Note System-provided intrusion and network analysis policies are similarly named but contain different configurations. For example, the Balanced Security and Connectivity network analysis policy and the Balanced Security and Connectivity intrusion policy work together and can both be updated in intrusion rule updates. However, the network analysis policy governs mostly preprocessing options, whereas the intrusion policy governs mostly intrusion rules. Network analysis and intrusion policies work together to examine your traffic.

You can also tailor traffic preprocessing options to specific security zones, networks, and VLANs by creating multiple custom network analysis policies, then assigning them to preprocess different traffic.

Manage network analysis policies

This task allows you to perform various management operations on network analysis policies, including creation, editing, deletion, comparison, and report generation.

Under your user name in the toolbar, the system displays a tree of available domains. To switch domains, choose the domain you want to access.

Note Snort 2 is not supported on threat defense version 7.7. For information on Snort 2 features that are supported in versions earlier than 7.7, refer to the management center guide that matches your threat defense version.

Procedure

Step 1 Choose one of these paths to access the network analysis policy.

- **Policies** > **Security policies** > **Access Control**, and then click **Network Analysis Policy**
- **Policies** > **Security policies** > **Intrusion**, and then click **Network Analysis Policies**

Note If your custom user role limits access to the first path listed here, use the second path to access the policy.

Step 2 Manage your network analysis policy:

- Create—If you want to create a new network analysis policy, click **Create Policy**.

  Two versions of the network analysis policy are created, a **Snort 2 Version** and a **Snort 3 Version**.

  - For the Snort 2 version, see *Custom Network Analysis Policy Creation for Snort 2* in the *Cisco Secure Firewall Management Center Configuration Guide*.
  - For the Snort 3 version, see Custom network analysis policy creation for Snort 3, on page 5.

- Delete—If you want to delete a network analysis policy, click the **Delete** icon, then confirm that you want to delete the policy. You cannot delete a network analysis policy if an access control policy references it.

  If the controls are dimmed, the configuration belongs to an ancestor domain, or you do not have permission to modify the configuration.

- Edit—If you want to edit an existing network analysis policy, click the **Edit** icon.

  If **View** ( ) appears instead, the configuration belongs to an ancestor domain, or you do not have permission to modify the configuration.

- Report—Click the **Report** icon; see *Generating Current Policy Reports* in the *Cisco Secure Firewall Management Center Configuration Guide*.

Snort 3 definitions and terminologies for network analysis policies

This table lists the Snort 3 concepts and terms used in the Network Analysis Policy.

Table 1: Snort 3 definitions and terminologies for network analysis policy

Term	Description
Inspectors	Inspectors are plugins that process packets (similar to the Snort 2 preprocessor).
Binder inspector	The binder inspector defines the flow when a particular inspector must be accessed and considered. When the traffic matches the conditions defined in the binder inspector, only then do the values and configurations for that inspector come into effect. For more information, see *Binder Inspector* in Custom network analysis policy creation for Snort 3, on page 5.
Singleton inspectors	Singleton inspectors contain one instance. These inspectors do not support adding more instances like multiton inspectors. Settings for a singleton inspector apply to all traffic that matches the inspector, not just a specific traffic segment. For more information, see *Singleton Inspectors* in Custom network analysis policy creation for Snort 3, on page 5.

Term	Description
Multiton inspectors	Multiton inspectors contain multiple instances which you can configure as needed. These inspectors support configuring settings based on specific conditions, such as network, port, and VLAN. One set of supported settings is called an instance. For more information, see *Multiton Inspectors* in Custom network analysis policy creation for Snort 3, on page 5.
Schema	The schema file is based on the OpenAPI JSON specification, and it validates the content that you upload or download. You can download the schema file and open it using any third-party JSON editor, such as Swagger editor. The schema file helps you to identify what parameters can be configured for inspectors with their corresponding allowed values, range, and accepted patterns to be used. For more information, see Customize the network analysis policy, on page 13.
Sample file	It is a pre-existing template that contains example configurations to help you with configuring the inspectors. You can refer to the example configurations included in the sample file and make any changes you require. For more information, see Customize the network analysis policy, on page 13.
Full configuration	You can download the entire inspector configurations in a single file. All information regarding the inspector configuration is available in this file. The full configuration is a merged configuration of the default configuration (provided as part of the LSP updates by Cisco Talos) and the custom NAP inspector configurations. For more information, see Customize the network analysis policy, on page 13.

Term	Description
Overridden configuration	In the **Snort 3 Version** of the network analysis policy page: • Under **Actions** > **Upload**, you can click **Overridden Configuration** to upload the JSON file that contains the overridden configuration. • Under **Actions** > **Download**, you can click **Overridden Configuration** to download the inspector configuration that has been overridden. If you have not overridden any inspector configuration, then this option is disabled. When you override the inspector configuration, then this option is enabled automatically to allow you to download. For more information, see Customize the network analysis policy, on page 13.

Related Topics

Custom network analysis policy creation for Snort 3, on page 5
Customize the network analysis policy, on page 13
Network analysis policy mapping, on page 11

Custom network analysis policy creation for Snort 3

A custom network analysis policy creation for Snort 3 is a data-driven configuration process that

- enables advanced users to customize the default network analysis policy for specific network requirements or to optimize performance, and
- utilizes JSON and JSON Schema based on the OpenAPI specification to configure inspectors and settings.

Network analysis policy customization overview

The default network analysis policy is tuned for typical network requirements and optimal performance. In most situations, you do not need to customize the policy. However, when you have a specific network requirement or when you are facing performance issues, the default network analysis policy can be customized. Note that customizing the network analysis policy is an advanced configuration that should only be done by advanced users or Cisco Support.

In Snort 3, the list of inspectors and settings are not in a one-to-one mapping with the Snort 2 list of preprocessors and settings. The number of inspectors and settings available in Firewall Management Center forms a subset of those that Snort 3 supports. See https://snort.org/snort3 for more information on Snort 3. See https://www.cisco.com/go/snort3-inspectors for more information on the inspectors available in Firewall Management Center.

Note

- While upgrading the Firewall Management Center to the 7.0 release, the changes that were done in the Snort 2 version of the network analysis policy are not migrated to Snort 3 after the upgrade.
- Unlike the intrusion policy, there is no option to synchronize Snort 2 network analysis policy settings to Snort 3.

Default inspector updates

Lightweight Security Package (LSP) updates may contain new inspectors or modifications to integer ranges for existing inspector configurations. After you install an LSP, new inspectors or updated ranges will be available under **Inspectors** in the **Snort 3 Version** of your network analysis policy.

Binder inspector

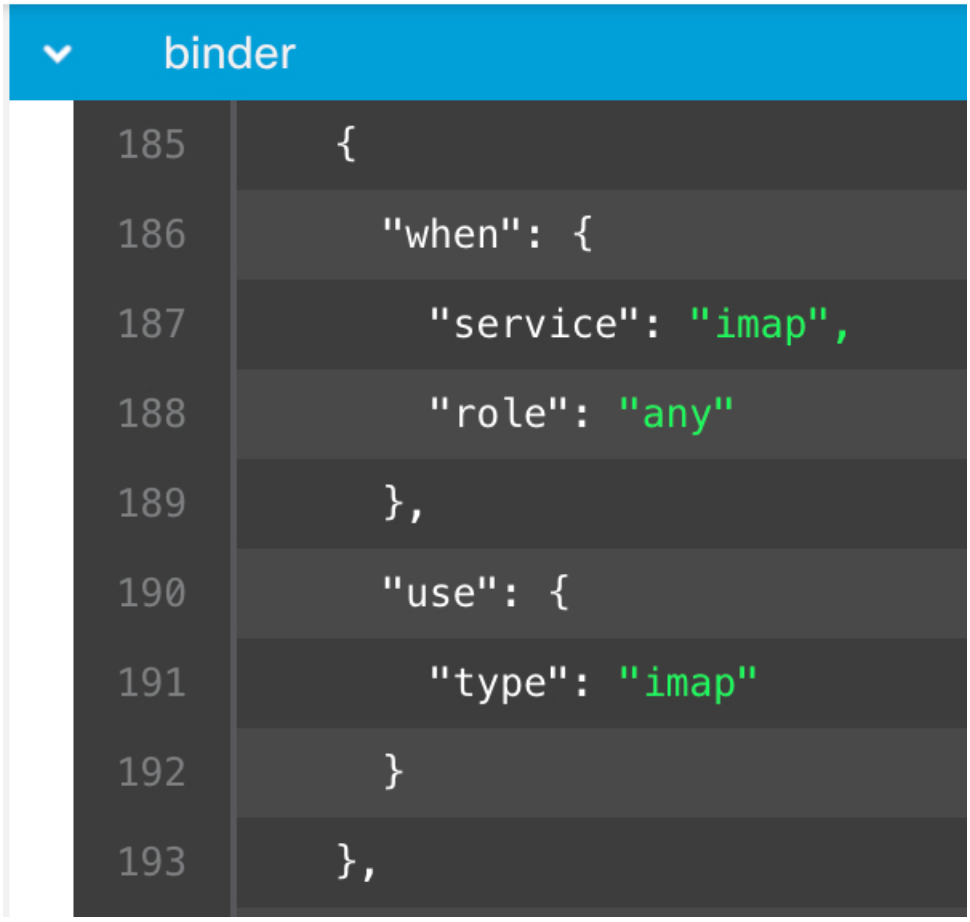
Binder inspector defines the flow when a particular inspector has to be accessed and taken into consideration. When the traffic matches the conditions defined in the binder inspector, only then the values and configurations for that inspector come into effect. For example:

For the *imap* inspector, the binder defines the following condition when it has to be accessed. That is when:

- Service is equal to imap.
- Role is equal to any.

a

If these conditions are met, then use the type imap.



Singleton inspectors

Singleton inspectors contain a single instance. These inspectors do not support adding more instances like multiton inspectors. Settings of a singleton inspector apply to all traffic, not to a specific segment.

For example:

```
{
   "normalizer":{
      "enabled":true,
      "type":"singleton",
      "data":{
         "ip4":{
            "df":true
         }
      }
   }
}
```

Multiton inspectors

Multiton inspectors contain multiple instances which you can configure as needed. These inspectors support configuring settings based on specific conditions, such as network, port, and VLAN. One set of supported settings is called an instance. There is a default instance, and you can also add additional instances based on specific conditions. If the traffic matches that condition, the settings from that instance are applied. Otherwise,

the settings from the default instance are applied. Also, the name of the default instance is the same as the name of the inspector.

For a multiton inspector, when you upload the overridden inspector configuration, you also need to include and define a matching binder condition (conditions under when the inspector has to be accessed or used) for each instance in the JSON file, otherwise, the upload will result in an error. You can also create new instances. Ensure that you include a binder condition for each new instance you create to avoid errors.

For example:

- Multiton inspector where the default instance is modified.

```
{
   "http_inspect":{
      "enabled":true,
      "type":"multiton",
      "instances":[
         {
            "name":"http_inspect",
            "data":{
               "response_depth":5000
            }
         }
      ]
   }
}
```

- Multiton inspector where the default instance and default binder is modified.

```
{
   "http_inspect":{
      "enabled":true,
      "type":"multiton",
      "instances":[
         {
            "name":"http_inspect",
            "data":{
               "response_depth":5000
            }
         }
      ]
   },
   "binder":{
      "type":"binder",
      "enabled":true,
      "rules":[
         {
            "use":{
               "type":"http_inspect"
            },
            "when":{
               "role":"any",
               "ports":"8080",
               "proto":"tcp",
               "service":"http"
            }
         }
      ]
   }
}
```

- Multiton inspector where a custom instance and a custom binder is added.

```
{
   "http_inspect":{
      "enabled":true,
      "type":"multiton",
      "instances":[
         {
            "name":"http_inspect1",
            "data":{
               "response_depth":5000
            }
         }
      ]
   },
   "binder":{
      "type":"binder",
      "enabled":true,
      "rules":[
         {
            "use":{
               "type":"http_inspect",
               "name":"http_inspect1"
            },
            "when":{
               "role":"any",
               "ports":"8080",
               "proto":"tcp",
               "service":"http"
            }
         }
      ]
   }
}
```

Common Industrial Protocol safety

Common Industrial Protocol (CIP) safety is a set of extensions to the CIP that

- enables the safe operation of devices,
- provides fail-safe communication between different nodes on a CIP network, and
- comprises two main components for safety parameter exchange and safety information transmission.

CIP safety protocol components

The CIP safety protocol comprises two main components:

- CIP safety segments—Used in Forward Open messages to exchange safety parameters for the subsequent safety session.
- CIP safety messages—Used to exchange actual safety information.

The CIP inspector detects and identifies:

- CIP as a service and client
- Payloads, such as CIP Read, CIP Admin, CIP Infrastructure, and CIP Write

The CIP inspector can parse the CIP segments and detect the CIP Safety segments in the Forward Open requests.

To test the CIP safety feature, you must enable the CIP inspector. See Detect and block safety segments in CIP packets, on page 10.

Detect and block safety segments in CIP packets

This task enables detection and blocking of CIP safety segments while allowing other CIP packets to pass through.

Use this procedure to detect and block CIP safety segments while allowing other CIP packets:

- Create a custom network analysis policy called **cip_safety**.
- Create access control rules in your access control policy to block CIP safety and to allow all other packets.

To test the CIP safety feature, enable the CIP inspector in the management center and assign it to an access control policy.

Procedure

Step 1 Go to **Policies** > **Security policies** > **Intrusion** > **Network Analysis Policies**.

Step 2 Click the **Snort 3 Version** of the network analysis policy **cip_safety** that you created.

Step 3 Under **Inspectors**, click **CIP** to expand it.

The default configuration appears in the left column and the overridden configuration appears in the right column under the inspector.

Step 4 Under **Overridden Configuration** on the right column, click the **Edit Inspector** icon and change the "enabled" field in **CIP** from false (default) to true.

Step 5 Click **OK** and then click **Save**.

Step 6 To assign the **CIP** inspector to the access control policy, choose **Policies** > **Security policies** > **Access Control**, click **Edit** and choose the **Advanced Settings** option from the **More** drop-down arrow at the end of the packet flow line.

Step 7 Click **Edit** (✎) next to **Network Analysis and Intrusion Policies**.

Step 8 In the **Network Analysis and Intrusion Policies** window, choose the access control policy **cip_safety** that you created from the **Default Network Analysis Policy** drop-down list.

The CIP inspector is now enabled in the management center and you can create the custom access control rules to block CIP safety and to allow all other CIP packets.

Step 9 After you send live traffic containing CIP safety packet flows, go to **Unified Events** to verify that the payload is the expected payload that contains CIP safety packet logs for the detection and block use case as mentioned in this procedure.

CIP is detected as an application protocol and client (see the **Application Protocol** and **Client Application** fields), and **CIP Safety** is shown under the **Web Application** field.

Network analysis policy mapping

Network analysis policy mapping is a correlation mechanism that

- provides mapping information for network analysis policies,
- finds the corresponding Snort 2 version of policies for the Snort 3 version, and
- ensures that the Snort 3 version of policies has its equivalent Snort 2 version.

View network analysis policy mapping

View which Snort 3 network analysis policies are automatically mapped to their Snort 2 equivalent policies in the system.

Network analysis policy mapping allows you to see the relationship between Snort 3 and Snort 2 policies when transitioning between versions or managing both simultaneously.

Procedure

Step 1 Go to **Policies** > **Security policies** > **Intrusion** > **Network Analysis Policies**.

Step 2 Click **NAP Mapping**.

Step 3 Expand the arrow for **View Mappings**.

The Snort 3 network analysis policies that are automatically mapped to a Snort 2 equivalent policy are displayed.

Step 4 Click **OK**.

Create a network analysis policy

Create a new network analysis policy that provides both Snort 2 and Snort 3 versions for network traffic inspection and analysis.

All the existing network analysis policies are available in Firewall Management Center with their corresponding Snort 2 and Snort 3 versions. When you create a new network analysis policy, it is created with both the Snort 2 version and the Snort 3 version.

Procedure

Step 1 Go to **Policies** > **Security policies** > **Intrusion** > **Network Analysis Policies**.

Step 2 Click **Create Policy**.

Step 3 Enter the **Name** and **Description**.

Step 4 Select a **Base Policy** and click **Save**.

The new network analysis policy is created with its corresponding **Snort 2 Version** and **Snort 3 Version**.

Modify the network analysis policy

This task allows you to update the configuration of an existing network analysis policy by modifying its properties such as name, description, or base policy settings.

You can modify the network analysis policy to change its name, description, or the base policy.

Procedure

Step 1 Go to **Policies** > **Security policies** > **Intrusion** > **Network Analysis Policies**.

Step 2 Click **Edit** to change the name, description, inspection mode, or the base policy.

Note If you edit the network analysis policy name, description, base policy, and inspection mode, the edits are applied to both the Snort 2 and Snort 3 versions. If you want to change the inspection mode for a specific version, then you can do that from within the network analysis policy page for that respective version.

Step 3 Click **Save**.

Search for an inspector on the Network Analysis Policy window

This task allows you to quickly locate specific inspectors within the network analysis policy interface by using search functionality.

On the Snort 3 version of the network analysis policy window, you may need to search for an inspector by entering any relevant text in the search bar.

Procedure

Step 1 Go to **Policies** > **Security policies** > **Intrusion** > **Network Analysis Policies**.

Step 2 Go to the **Snort 3 Version** of the network analysis policy.

Step 3 Enter the name of an inspector or any relevant text to search for in the **Search** bar.

All the inspectors matching the text you search for are displayed.

For example, if you enter `pop`, then the pop inspector and the binder inspector are shown as matching results on the screen.

Copy the inspector configuration

This task describes how to copy inspector configurations.

You can copy the inspector configuration for the Snort 3 version of the network analysis policy according to your requirements.

Procedure

Step 1 Go to **Policies** > **Security policies** > **Intrusion** > **Network Analysis Policies**.

Step 2 Go to the **Snort 3 Version** of the network analysis policy.

Step 3 Under **Inspectors**, expand the required inspector for which you want to copy the configuration.

The default configuration is displayed on the left column and the overridden configuration is displayed on the right column under the inspector.

Step 4 Click the **Copy to clipboard** icon to copy the inspector configuration to the clipboard for one or both of these options.

- **Default Configuration** in the left column
- **Overridden Configuration** in the right column

Step 5 Paste the copied inspector configuration to a JSON editor to make any edits you may require.

Related Topics

Customize the network analysis policy, on page 13

Customize the network analysis policy

Customize the network analysis policy to adapt Snort 3 configurations according to your security requirements.

You can customize the Snort 3 version of the network analysis policy according to your requirements.

Procedure

Step 1 Go to **Policies** > **Security policies** > **Intrusion** > **Network Analysis Policies**.

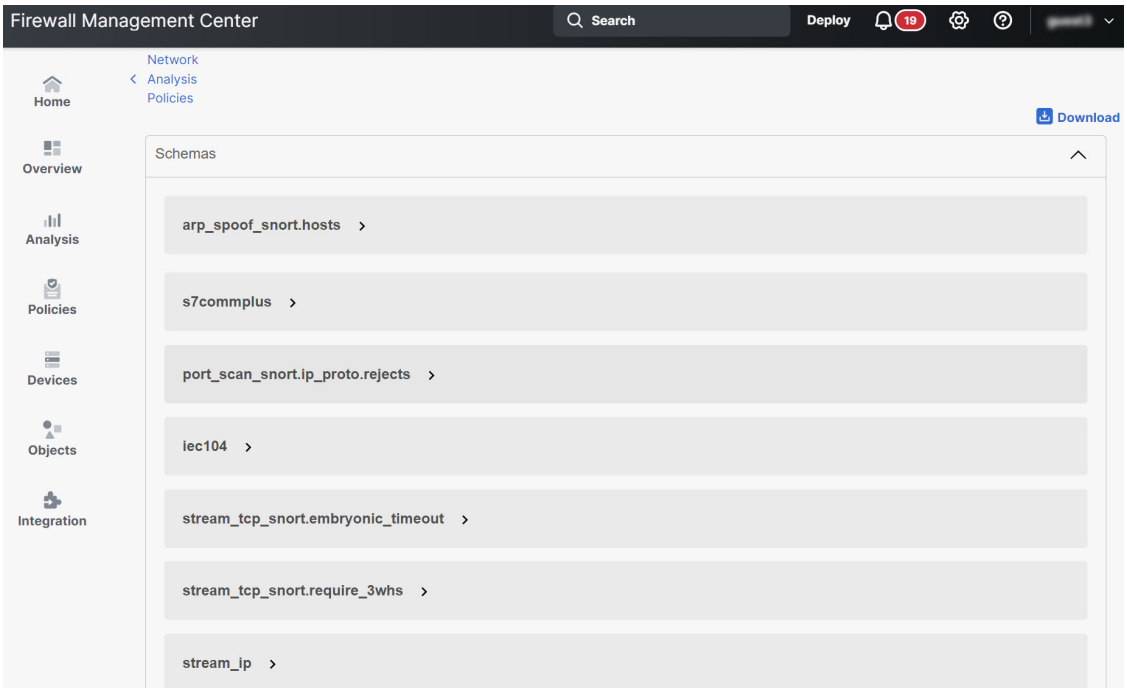
Step 2 Go to the **Snort 3 Version** of the network analysis policy.

Step 3 Click the **Actions** dropdown menu.

The following options are displayed:

- View Schema
- Download Schema / Download Sample File / Template
- Download Full Configuration
- Download Overridden Configuration
- Upload Overridden Configuration

Step 4 Click **View Schema** to open the schema file directly in a browser.



Step 5 You can download the schema file, sample file / template, full configuration, or overridden configuration as needed.

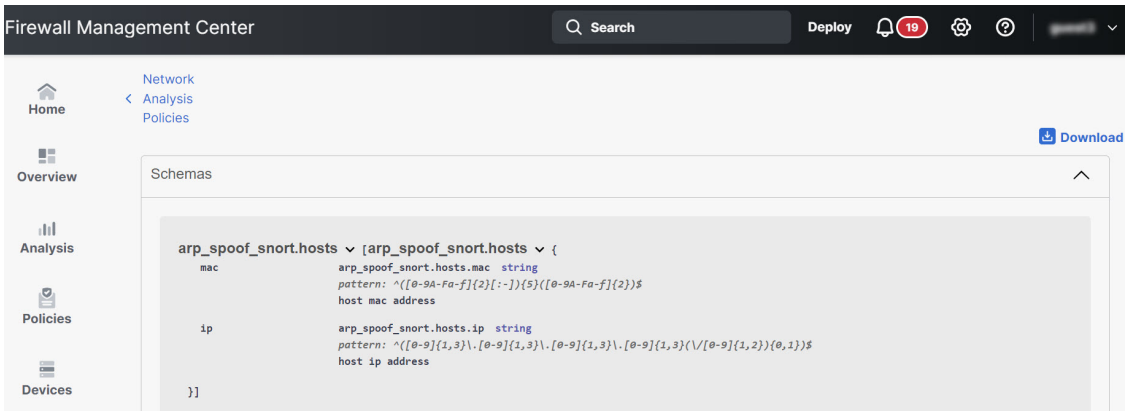
These options provide you an insight about the allowed values, range, and patterns, existing and default inspector configurations, and overridden inspector configurations.

a) Click **Download Schema** to download the schema file.

The schema file validates the content that you upload or download. You can download the schema file and open it using any third-party JSON editor. The schema file helps you identify which parameters can be configured for inspectors, along with their allowed values, ranges, and accepted patterns.

For example, for the *arp_spoof_snort* inspector, you can configure the hosts. The hosts include the *mac* and *ip* address values. The schema file shows the following accepted pattern for these values.

- **mac** – `pattern: ^([0-9A-Fa-f]{2}[:-]){5}([0-9A-Fa-f]{2})$`
- **ip** – `pattern: ^([0-9]{1,3}.[0-9]{1,3}.[0-9]{1,3}.[0-9]{1,3}(/[0-9]{1,2}){0,1})$`



You must provide the values, range, patterns according to the accepted ones in the schema file to be able to successfully override the inspector configuration, otherwise, you get an error message.

b) Click **Download Sample File / Template** to use a pre-existing template that contains example configurations to help you with configuring the inspectors.

You can refer to the example configurations included in the sample file and make any changes that you may require.

c) Click **Download Full Configuration** to download the entire inspector configurations in a single JSON file.

You can download the full configuration to find the information you need, rather than expanding the inspectors separately. This file contains all information about the inspector configuration.

d) Click **Download Overridden Configuration** to download the inspector configuration that has been overridden.

Step 6 To override the existing configuration, follow these steps.

You can choose to override an inspector configuration using these ways.

- Make inline edits for an inspector directly on the Firewall Management Center. See the topic **Make Inline Edit for an Inspector to Override Configuration** in the **Getting Started with Network Analysis Policies** chapter of the *Cisco Secure Firewall Management Center Snort 3 Configuration Guide*.
- Continue to follow the current procedure of using the **Actions** dropdown menu to upload the overridden configuration file.

If you chose to make inline edits directly in the Firewall Management Center, then you do not need to complete this procedure any further. Otherwise, you must complete this procedure completely.

a) Under **Inspectors**, expand the required inspector for which you want to override the default configuration.

The default configuration is displayed on the left column and the overridden configuration is displayed on the right column under the inspector.

You may need to search for an inspector by entering any relevant text in in the search bar.

b) Click the **Copy to clipboard** icon to copy the default inspector configuration to the clipboard.
c) Create a JSON file and paste the default configuration in it.
d) Keep the inspector configuration that you want to override, and remove all other configuration and instances from the JSON file.

You can also use the **Sample File / Template** to understand how to override the default configuration. This is a sample file that includes JSON snippets explaining how you can customize the network analysis policy for Snort 3.

e) Make changes to the inspector configuration as needed.

Validate the changes and make sure they conform to the schema file. For multiton inspectors, make sure that the binder conditions for all instances are included in the JSON file. See *Multiton Inspectors* in the topic **Custom Network Analysis Policy Creation for Snort 3** in the *Cisco Secure Firewall Management Center Snort 3 Configuration Guide* for more information.

f) If you are copying any further default inspector configurations, add the inspector configuration to the existing file that contains the overridden configuration.



Note The copied inspector configuration must comply with the JSON standards.

g) Save the overridden configuration file to your system.

Step 7 From the **Actions** dropdown menu, choose Upload Overridden Configuration to upload the JSON file that contains the overridden configuration.



Caution Upload only the changes that you require. You should not upload the entire configuration as it makes the overrides sticky in nature and therefore, any subsequent changes to the default configuration as part of the LSP updates would not be applied.

You can drag and drop a file or click to browse to the JSON file saved in your system that contains the overridden inspector configuration.

- **Merge inspector overrides** – Content in the uploaded file is merged with the existing configuration if there is no common inspector. If there are common inspectors, then the content in the uploaded file (for common inspectors) takes precedence over the previous content, and it replaces the previous configuration for those inspectors.
- **Replace inspector overrides** – Removes all previous overrides and replaces them with the new content in the uploaded file.



Attention Choosing this option deletes all the previous overrides. Review your choice carefully before using this option to override the configuration.

If any error occurs while uploading the overridden inspectors, you see the error in the **Upload Overridden Configuration File** pop-up window. You can also download the file with the error, fix the error, and reupload the file.

Step 8 In the **Upload Overridden Configuration File** pop-up window, click **Import** to upload the overridden inspector configuration.

After you upload the overridden inspector configuration, you will see an orange icon next to the inspector that signifies that it is an overridden inspector.

Also, the **Overridden Configuration** column under the inspector shows the overridden value.

You can also view all the overridden inspectors using the **Show Overrides Only** checkbox adjacent to the Search bar.

Note Make sure that you always download the overridden configuration, open the JSON file, and append any new changes/overrides to the inspector configurations to this file. This action is needed so that you do not lose the old overridden configurations.

Step 9 (Optional) Take a backup of the overridden configuration file on your system before making any new inspector configuration changes.

Tip We recommend that you take a backup from time to time as you override the inspector configuration.

Make inline edit for an inspector to override configuration

This task allows you to make inline edits for inspector configurations to override the default configuration according to your requirements in the Snort 3 version of the network analysis policy.

For the Snort 3 version of the network analysis policy, you can make an inline edit for the inspector configuration to override the configuration according to your requirements.

Alternatively, you can also use the **Actions** drop-down menu to upload the overridden configuration file. See Customize the network analysis policy, on page 13 for more information.

Procedure

Step 1 Go to **Policies** > **Security policies** > **Intrusion** > **Network Analysis Policies**.

Step 2 Go to the **Snort 3 Version** of the network analysis policy.

Step 3 Under **Inspectors**, expand the required inspector for which you want to override the default setting.

The default configuration is displayed on the left column and the overridden configuration is displayed on the right column under the inspector.

Step 4 Under the **Overridden Configuration** in the right column, click **Edit Inspector** (Pencil) icon to make changes to the inspector configuration.

The Override Configuration pop-up appears where you can make the required edits.

Note

- Make sure that you keep only those settings that you want to override. If you leave a setting with the same value, that field becomes sticky. This means if that setting is changed in the future by Talos, the current value will be retained.
- If you are adding or deleting any custom instance, make sure that you add or delete a binder rule for that instance in the binder inspector as well.

Step 5 Click **OK**.

If there are any errors according to the JSON standards, it shows you an error message.

Step 6 Click **Save** to save the changes.

If the changes conform to the OpenAPI schema specification, the Firewall Management Center allows you to save the configuration, otherwise, the **Error saving overridden configuration** pop-up appears that shows the errors. You can also download the file with the errors.

Related Topics

Customize the network analysis policy, on page 13
Revert unsaved changes during inline edits, on page 18
Revert overridden configuration to default configuration, on page 19
Examples of custom network analysis policy configuration, on page 22

Revert unsaved changes during inline edits

This task allows you to revert any unsaved changes made during inline edits to override the configuration for an inspector, returning to the most recently saved value.

While making inline edits to override the configuration for an inspector , you can revert any unsaved changes. Note that this action reverts all unsaved changes to the most recently saved value, but does not revert the configuration to the default configuration for an inspector.

Procedure

Step 1 Go to **Policies** > **Security policies** > **Intrusion** > **Network Analysis Policies**.

Step 2 Go to the **Snort 3 Version** of the network analysis policy.

Step 3 Under **Inspectors**, expand the required inspector for which you want to revert the unsaved changes.

The default configuration is displayed in the left column and the overridden configuration is displayed in the right column under the inspector.

Step 4 Under the **Overridden Configuration** on the right column, click the **Cross** ✕ icon to revert any unsaved changes for the inspector.

Alternatively, you can click **Cancel** to cancel the changes.

If you do not have any unsaved changes to the inspector configuration, then this option is not visible.

Related Topics

Revert overridden configuration to default configuration, on page 19
Make inline edit for an inspector to override configuration, on page 17

View the list of inspectors with overrides

This task enables you to identify and review all inspectors that have been overridden in your network analysis policy configuration.

You can view a list of all the overridden inspectors.

Procedure

Step 1 Go to **Policies** > **Security policies** > **Intrusion** > **Network Analysis Policies**.

Step 2 Go to the **Snort 3 Version** of the network analysis policy.

Step 3 Check the **Show Overrides Only** checkbox adjacent to the Search bar to view the list of overridden inspectors.

All the overridden inspectors are shown with an orange icon next to their names to help you identify them.

Related Topics

Search for an inspector on the Network Analysis Policy window, on page 12
Make inline edit for an inspector to override configuration, on page 17
Customize the network analysis policy, on page 13

Revert overridden configuration to default configuration

Revert any changes that you made to override the default configuration for an inspector, restoring the original default settings.

You can revert any changes that you made to override the default configuration for an inspector. This action reverts the overridden configuration to the default configuration for an inspector.

Procedure

Step 1 Go to **Policies** > **Security policies** > **Intrusion** > **Network Analysis Policies**.

Step 2 Go to the **Snort 3 Version** of the network analysis policy.

Step 3 Under **Inspectors**, expand the required inspector for which you want to revert the overridden configuration.

The overridden inspectors are shown with the orange icon next to their name.

The default configuration is displayed on the left column and the overridden configuration is displayed on the right column under the inspector. Under the **Overridden Configuration** on the right column, click **Revert**

to default configuration (back arrow) icon to revert the overridden configuration for the inspector to the default configuration.

If you did not make any changes to the default configuration for the inspector, then this option is disabled.

Step 4 Click **Revert** to confirm the decision.

Step 5 Click **Save** to save the changes.

If you do not want to save the changes, you can click **Cancel** or the **Cross** ✕ icon.

Related Topics

Revert unsaved changes during inline edits, on page 18
Customize the network analysis policy, on page 13
Make inline edit for an inspector to override configuration, on page 17
Examples of custom network analysis policy configuration, on page 22

Validate Snort 3 policies

This task validates Snort 3 policies to ensure they work correctly with current and previous device versions, handling version-specific configurations and inspector settings.

To validate the Snort 3 policies, here is a list of basic information that you can make note of:

- Current version of the Cloud-Delivered Firewall Management Center can manage multiple Firewall Threat Defense versions.
- Current version of Cloud-Delivered Firewall Management Center supports network analysis policy (NAP) configurations which are not applicable to previous version of Firewall Threat Defense devices.
- Current NAP Policy and validations will work based on the current version support.
- Changes may include content which is not valid for previous versions of Firewall Threat Defenses.
- Policy configuration changes are accepted if they are valid for the current version and performed using the current Snort 3 binary and NAP schema.
- For previous version Firewall Threat Defenses, validation is performed during deployment using NAP schema and Snort 3 binary for that specific version. If there is any configuration which is not applicable for the given version, the user is informed or warned that the configuration not supported on the given version will not be deployed, while the remaining configuration will be deployed.

In this procedure, when we associate the NAP policy to an Access Control Policy and deploy it on a device, for example any inspector like rate filter configuration is applied to validate the Snort 3 policies.

Procedure

Step 1 **Steps to Override NAP Policy Configuration:** Under **Inspectors** in the **Snort 3 Version** of the network analysis policy, expand the required inspector for which you want to override the default setting.

The default configuration is displayed on the left column and the overridden configuration is displayed on the right column under the inspector.

a) Under the **Overridden Configuration** on the right column, click **Edit Inspector** (Pencil) icon to make changes to any inspector like rate_filter.

The Override Configuration pop-up appears where you can make the required edits to the rate_filter inspector. Click **OK**.

b) Click **Save** to save the changes.

Alternatively, you can use the **Actions** dropdown menu to upload the overridden configuration file.

Step 2 Click the **Actions** dropdown menu in the **Snort 3 Version** of the network analysis policy.

Step 3 Under **Upload**, you can click **Overridden Configuration** to upload the JSON file that contains the overridden configuration.



Caution Upload only the changes that you require. You should not upload the entire configuration as it causes the overrides to remain persistent, so any subsequent changes to the default configuration from LSP updates will not be applied.

You can drag and drop a file or click to browse to the JSON file saved in your system that contains the overridden inspector configuration.

- **Merge inspector overrides**: Content in the uploaded file is merged with the existing configuration if there is no common inspector. If there are common inspectors, then the content in the uploaded file (for common inspectors) takes precedence over the previous content, and it replaces the previous configuration for those inspectors.
- **Replace inspector overrides**: Removes all previous overrides and replaces them with the new content in the uploaded file.



Note As choosing this option deletes all the previous overrides, make an informed decision before overriding the configuration using this option.

If any error occurs while uploading the overridden inspectors, you see the error on the **Upload Overridden Configuration File** pop-up window. You can also download the file with the error, then fix the error and reupload the file.

Step 4 **Steps to Associate NAP Policy to Access Control Policy:** In the access control policy editor, click **Advanced**, then click **Edit** next to the Network Analysis and Intrusion Policies section.

a) From the **Default Network Analysis Policy** drop-down list, select a default network analysis policy.

If you choose a user-created policy, you can click **Edit** to edit the policy in a new window. You cannot edit system-provided policies.

b) Click **OK** and then click **Save** to save the policy.

Step 5 Alternatively, in the access control policy editor, click **Advanced**, then click **Edit** next to the Network Analysis and Intrusion Policies section.

a) Click **Add Rule**.

b) Configure the rule's conditions by clicking the options you want to add.

c) Click **Network Analysis** and choose the **Network Analysis Policy** you want to use to preprocess the traffic matching this rule.
d) Click **Add**.

Step 6 **Deployment:** On the Cloud-Delivered Firewall Management Center menu bar, click **Deploy** and then select **Deployment**.

Step 7 Identify and choose the devices on which you want to deploy configuration changes.

- Search: Search for the device name, type, domain, group, or status in the search box.
- Expand: Click **Expand Arrow** to view device-specific configuration changes to be deployed.

  By selecting the device check box, all changes for that device listed under it are pushed for deployment. Alternatively, you can use the **Policy Selection** to select individual policies or configurations to deploy, withholding the rest.

  Optionally, use **Show or Hide Policy** to selectively view or hide the associated unmodified policies.

Step 8 Click **Deploy**.

Step 9 If the system identifies errors or warnings in the changes to be deployed, it displays them in the **Validation Messages** window. To view complete details, click the arrow icon before the warnings or errors.

Note It displays a warning that Snort 3 network analysis policy contains inspectors or attributes not valid for this Firewall Threat Defense version. Invalid settings will be skipped during deployment. Invalid inspectors are: ["rate_filter"] only for devices lower than 7.1 version.

Examples of custom network analysis policy configuration

This is a sample file that includes JSON snippets explaining how you can customize the network analysis policy for Snort 3. You can choose to override an inspector configuration using the following ways:

- Make inline edits for an inspector directly on the Firewall Management Center. See Make inline edit for an inspector to override configuration, on page 17.
- Use the **Actions** drop-down menu to upload the overridden configuration file. See Customize the network analysis policy, on page 13.

Before you choose any of these options, review all the details and examples to help you define the network analysis policy overrides successfully. To avoid risks and errors, read and understand the scenarios provided here.

If you choose to override an inspector configuration from the **Actions** drop-down menu, you need to construct a JSON file for the network analysis policy overrides and upload the file.

For overriding an inspector configuration in the network analysis policy, you must upload only the changes that you require. You should not upload the entire configuration because it makes the overrides sticky in nature and therefore, any subsequent changes to the default values or configuration as part of the LSP updates would not be applied.

Here are the examples for various scenarios:

Enabling a Singleton Inspector when the Default State in the Base Policy is Disabled

```
{
  "rate_filter": {
    "enabled": true,
    "type": "singleton",
    "data": []
  }
}
```

Disabling a Singleton Inspector when the Default State in the Base Policy is Enabled

```
{
  "rate_filter": {
    "enabled": false,
    "type": "singleton",
    "data": []
  }
}
```

Enabling a Multiton Inspector when the Default State in the Base Policy is Disabled

```
{
  "ssh": {
    "enabled": true,
    "type": "multiton",
    "instances": []
  }
}
```

Disabling a Multiton Inspector when the Default State in the Base Policy is Enabled

```
{
  "ssh": {
    "enabled": false,
    "type": "multiton",
    "instances": []
  },
  "iec104": {
    "type": "multiton",
    "enabled": false,
    "instances": []
  }
}
```

Overriding the Default Value of Specific Setting(s) for Singleton Inspector

```
{
  "normalizer": {
    "enabled": true,
    "type": "singleton",
    "data": {
      "tcp": {
        "block": true
      },
      "ip6": true
    }
  }
}
```

Overriding Specific Setting(s) of a Default Instance (where Instance Name Matches with Inspector Type) in Multiton Inspector

```
{
  "http_inspect": {
    "enabled": true,
    "type": "multiton",
    "instances": [
      {
        "data": {
          "unzip": false
        },
        "name": "http_inspect"
      }
    ]
  }
}
```

Adding Binder Rule for a Default Instance with Required Changes



Note Default binder rules cannot be edited; they are always appended at the end.

```
{
  "binder": {
    "enabled": true,
    "type": "binder",
    "rules": [
      {
        "use": {
          "type": "http_inspect"
        },
        "when": {
          "role": "server",
          "service": "http",
          "dst_nets": "10.1.1.0/24"
        }
      }
    ]
  }
}
```

Adding a New Custom Instance



Note Corresponding binder rule entry must be defined in the binder inspector.

```
{
  "telnet": {
    "enabled": true,
    "type": "multiton",
    "instances": [
      {
        "name": "telnet_my_instance",
        "data": {
          "encrypted_traffic": true
        }
      }
```

```
    ]
  },
  "binder": {
    "enabled": true,
    "type": "binder",
    "rules": [
      {
        "when": {
          "role": "any",
          "service": "telnet"
        },
        "use": {
          "type": "telnet",
          "name": "telnet_my_instance"
        }
      }
    ]
  }
}
```

Overriding a Singleton Instance, Multiton Default Instance, and Creating a New Multiton Instance in a Single JSON Override

Example to show the following in a single JSON override:

- Overriding a Singleton instance (**`normalizer`** inspector)
- Overriding a Multiton default instance (**`http_inspect`** inspector)
- Creating a new Multiton instance (**`telnet`** inspector)

```
{
  "normalizer": {
    "enabled": true,
    "type": "singleton",
    "data": {
      "tcp": {
        "block": true
      },
      "ip6": true
    }
  },
  "http_inspect": {
    "enabled": true,
    "type": "multiton",
    "instances": [
      {
        "data": {
          "unzip": false,
          "xff_headers": "x-forwarded-for true-client-ip x-another-forwarding-header"
        },
        "name": "http_inspect"
      }
    ]
  },
  "telnet": {
    "enabled": true,
    "type": "multiton",
    "instances": [
      {
        "name": "telnet_my_instance",
        "data": {
          "encrypted_traffic": true
```

```
        }
      }
    ]
  },
  "binder": {
    "enabled": true,
    "type": "binder",
    "rules": [
      {
        "when": {
          "role": "any",
          "service": "telnet"
        },
        "use": {
          "type": "telnet",
          "name": "telnet_my_instance"
        }
      },
      {
        "use": {
          "type": "http_inspect"
        },
        "when": {
          "role": "server",
          "service": "http",
          "dst_nets": "10.1.1.0/24"
        }
      }
    ]
  }
}
```



Note You do not need to provide the **name** attribute for the default instance in binder rules.

Configuring arp_spoof

Example for configuring **arp_spoof**:

The **arp_spoof** inspector does not have any default configurations for any attributes. This demonstrates the case where you can provide the overrides.

```
{
  "arp_spoof": {
    "type": "singleton",
    "data": {
      "hosts": [
        {
          "ip": "1.1.1.1",
          "mac": "ff:0f:f1:0f:0f:ff"
        },
        {
          "ip": "2.2.2.2",
          "mac": "ff:0f:f2:0f:0f:ff"
        }
      ]
    },
    "enabled": true
  }
}
```

Configuring rate_filter

```
{
  "rate_filter": {
    "data": [
      {
        "apply_to": "[10.1.2.100, 10.1.2.101]",
        "count": 5,
        "gid": 135,
        "new_action": "alert",
        "seconds": 1,
        "sid": 1,
        "timeout": 5,
        "track": "by_src"
      }
    ],
    "enabled": true,
    "type": "singleton"
  }
}
```

Configuring Binder Rules when Multi-Hierarchy Network Analysis Policy is Used

This example illustrates adding a new custom instance in child policy and the way binder rules should be written. Binder rules are defined as a list and therefore, it is important to pick up the rules defined in the parent policy and build the new rules on top of it as rules will not be merged automatically. The binder rules available in child policy are a source of truth in totality.

On the Firewall Threat Defense, the default Cisco Talos policy rules are appended on these user-defined overrides.

Parent Policy:

We have defined a custom instance by the name **`telnet_parent_instance`** and the corresponding binder rule.

```
{
  "telnet": {
    "type": "multiton",
    "instances": [
      {
        "data": {
          "normalize": true,
          "encrypted_traffic": true
        },
        "name": "telnet_parent_instance"
      }
    ],
    "enabled": true
  },
  "binder": {
    "enabled": true,
    "type": "binder",
    "rules": [
      {
        "when": {
          "role": "any",
          "service": "telnet"
        },
        "use": {
          "type": "telnet",
          "name": "telnet_parent_instance"
        }
```

```
      }
    ]
  }
}
```

Child Policy:

This network analysis policy has the aforementioned policy as its base policy. We have defined a custom instance by the name **`telnet_child_instance`** and have also defined the binder rules for this instance. The binder rules from parent policy need to be copied here, and then child policy binder rules can be prepended or appended on top of it based on the nature of the rule.

```
{
  "telnet": {
    "type": "multiton",
    "instances": [
      {
        "data": {
          "normalize": true,
          "encrypted_traffic": false
        },
        "name": "telnet_child_instance"
      }
    ],
    "enabled": true
  },
  "binder": {
    "enabled": true,
    "type": "binder",
    "rules": [
      {
        "when": {
          "role": "any",
          "service": "telnet",
          "nets": "10.2.2.0/24"
        },
        "use": {
          "type": "telnet",
          "name": "telnet_child_instance"
        }
      },
      {
        "when": {
          "role": "any",
          "service": "telnet"
        },
        "use": {
          "type": "telnet",
          "name": "telnet_parent_instance"
        }
      }
    ]
  }
}
```

Configuring List Inspector Attribute in General

While changing overrides for any attribute of type list, it is important to pass the full contents rather than partial override. This means if a base policy attributes are defined as:

```
{
  "list-attribute": [
    {
      "entry1": {
```

```
        "key1": "value1"
      }
    },
    {
      "entry2": {
        "key2": "value2"
      }
    }
  ]
}
```

If you want to modify **value1** to **value1-new**, the override payload must look like the following:

Correct Way:

```
{
  "list-attribute": [
    {
      "entry1": {
        "key1": "value1-new"
      }
    },
    {
      "entry2": {
        "key2": "value2"
      }
    }
  ]
}
```

Incorrect Way:

```
{
  "list-attribute": [
    {
      "entry1": {
        "key1": "value1-new"
      }
    }
  ]
}
```

You can understand this configuration by taking the trimmed values of the **alt_max_command_line_len** attribute in the **smtp** inspector. Suppose the default (base) policy configuration for **smtp** inspector is as follows:

```
{
  "smtp": {
    "type": "multiton",
    "instances": [
      {
        "name": "smtp",
        "data": {
          "decompress_zip": false,
          "normalize_cmds": "ATRN AUTH BDAT CHUNKING DATA DEBUG EHLO
           EMAL ESAM ESND ESOM ETRN EVFY EXPN HELO HELP IDENT MAIL
           NOOP ONEX QUEU QUIT RCPT RSET SAML SEND SOML STARTTLS TICK
           TIME TURN TURNME VERB VRFY X-ADAT XADR XAUTH XCIR X-DRCP X-
           ERCP XEXCH50 X-EXCH50 X-EXPS XGEN XLICENSE X-LINK2STATE XQUE
           XSTA XTRN XUSR",
          "ignore_data": false,
          "max_command_line_len": 512,
          "max_header_line_len": 1000,
          "log_rcptto": false,
          "decompress_swf": false,
```

```
            "max_response_line_len": 512,
            "b64_decode_depth": -1,
            "max_auth_command_line_len": 1000,
            "log_email_hdrs": false,
            "xlink2state": "alert",
            "binary_data_cmds": "BDAT XEXCH50",
            "auth_cmds": "AUTH XAUTH X-EXPS",
            "log_filename": false,
            "uu_decode_depth": -1,
            "ignore_tls_data": false,
            "data_cmds": "DATA",
            "bitenc_decode_depth": -1,
            "alt_max_command_line_len": [
              {
                "length": 255,
                "command": "ATRN"
              },
              {
                "command": "AUTH",
                "length": 246
              },
              {
                "length": 255,
                "command": "BDAT"
              },
              {
                "length": 246,
                "command": "DATA"
              }
            ],
            "log_mailfrom": false,
            "decompress_pdf": false,
            "normalize": "none",
            "email_hdrs_log_depth": 1464,
            "valid_cmds": "ATRN AUTH BDAT CHUNKING DATA DEBUG EHLO
             EMAL ESAM ESND ESOM ETRN EVFY EXPN HELO HELP IDENT MAIL
             NOOP ONEX QUEU QUIT RCPT RSET SAML SEND SOML STARTTLS TICK
             TIME TURN TURNME VERB VRFY X-ADAT XADR XAUTH XCIR X-DRCP X-
             ERCP XEXCH50 X-EXCH50 X-EXPS XGEN XLICENSE X-LINK2STATE XQUE
             XSTA XTRN XUSR",
            "qp_decode_depth": -1
          }
        }
    ],
    "enabled": true
  }
}
```

Now, if you want to add two more objects to the **alt_max_command_line_len** list:

```
{
    "length": 246,
    "command": "XEXCH50"
},
{
    "length": 246,
    "command": "X-EXPS"
}
```

Then the custom network analysis policy override JSON would look like the following:

```
{
  "smtp": {
    "type": "multiton",
    "instances": [
```

```
      {
        "name": "smtp",
        "data": {
          "alt_max_command_line_len": [
            {
              "length": 255,
              "command": "ATRN"
            },
            {
              "command": "AUTH",
              "length": 246
            },
            {
              "length": 255,
              "command": "BDAT"
            },
            {
              "length": 246,
              "command": "DATA"
            },
            {
              "length": 246,
              "command": "XEXCH50"
            },
            {
              "length": 246,
              "command": "X-EXPS"
            }
          ]
        }
      }
    ],
    "enabled": true
  }
}
```

Configuring Overrides when Multi-Hierarchy Network Analysis Policy is used in Multiton Inspector

This example illustrates overriding attributes in child policy and how the merged configuration will be used in the child policy for any instance. Any overrides defined in the child policy will be merged with the parent policy. Thus, if attribute1 and attribute2 are overridden in parent policy and attribute2 and attribute3 are overridden in the child policy, the merged configurations are for child policy. This means that attribute1 (defined in parent policy), attribute2 (defined in child policy), and attribute3 (defined in child policy) will be configured on the device.

Parent Policy:

Here we have defined a custom instance by the name **`telnet_parent_instance`** and overridden 2 attributes namely, **`normalize`** and **`encrypted_traffic`** in the custom instance.

```
{
  "telnet": {
    "type": "multiton",
    "instances": [
      {
        "data": {
          "normalize": true,
          "encrypted_traffic": false
        },
        "name": "telnet_parent_instance"
      }
    ],
    "enabled": true
```

```
  },
  "binder": {
    "enabled": true,
    "type": "binder",
    "rules": [
      {
        "when": {
          "role": "any",
          "service": "telnet"
        },
        "use": {
          "type": "telnet",
          "name": "telnet_parent_instance"
        }
      }
    ]
  }
}
```

Child Policy:

This network analysis policy has the aforementioned policy as its base policy. We have overridden attribute **`encrypted_traffic`** from parent policy and also overridden new attribute **`ayt_attack_thresh`**.

```
{
  "telnet": {
    "type": "multiton",
    "instances": [
      {
        "data": {
          "encrypted_traffic": true,
          "ayt_attack_thresh": 1
        },
        "name": "telnet_parent_instance"
      }
    ],
    "enabled": true
  }
}
```

With the above policy JSON, when you deploy the network analysis policy the following merged JSON will be configured on the device.

```
{
  "telnet": {
    "type": "multiton",
    "instances": [
      {
        "data": {
          "normalize": true,
          "encrypted_traffic": true,
          "ayt_attack_thresh": 1
        },
        "name": "telnet_parent_instance"
      }
    ],
    "enabled": true
  },
  "binder": {
    "enabled": true,
    "type": "binder",
    "rules": [
      {
        "when": {
          "role": "any",
```

```
          "service": "telnet"
        },
        "use": {
          "type": "telnet",
          "name": "telnet_parent_instance"
        }
      }
    ]
  }
}
```

This example illustrates details for the custom network analysis policy. The same behavior is also exhibited in the default instance. Also, a similar merging would be done for Singleton inspectors.

Removing all the Inspector Overrides for the Network Analysis Policy

Whenever you want to remove all the overrides for a specific network analysis policy, you can upload an empty JSON. While uploading the overrides, choose the option **Replace inspector overrides**.

Network analysis policy settings and cached changes

When you create a new network analysis policy, it has the same settings as its base policy.

When tailoring a network analysis policy, especially when disabling inspectors, keep in mind that some inspectors and intrusion rules require that traffic first be decoded or preprocessed in a certain way. If you disable a required inspector, the system automatically uses it with its current settings, although the inspector remains disabled in the network analysis policy web interface.

Because preprocessing and intrusion inspection are so closely related, the network analysis and intrusion policies examining a single packet **must** complement each other. Tailoring preprocessing, especially using multiple custom network analysis policies, is an **advanced** task.

The system caches one network analysis policy per user. While editing a network analysis policy, if you select any menu or other path to another page, your changes stay in the system cache even if you leave the page.

Generate Snort 3 recommendations

Snort 3 rule recommendations

Snort 3 rule recommendations are a security tuning feature that

- automatically tune your intrusion policy with rules specific to the host environment,
- enable additional rules or tune the current rule set by disabling rules for vulnerabilities not present in your network, and
- use the host database to determine rules that apply to your environment.

How rule recommendations work

The management center builds a database of hosts on your network with details such as the IP address, hostname, operating system, services, users, and client applications through passive discovery. Based on this

information, the system maps vulnerabilities to each discovered host. The recommendations feature uses this host database to determine the rules that apply to your environment.

In Snort 3, there are four security levels, each corresponding to a specific Talos policy:

- Level 1–Connectivity Over Security
- Level 2–Balanced Security and Connectivity
- Level 3–Security Over Connectivity
- Level 4–Maximum Detection

Check the **Accept Recommendations to Disable Rules** check box to disable rules for vulnerabilities not found on the hosts in your network. Check this option only if you have to trim your rule set because of a high number of alerts, or to improve inspection performance.

For more information, see Secure Firewall recommended rules.

Benefits

- By configuring recommendations, you can tailor your intrusion policy to detect specific types of threats more effectively using rules that are specific to the host environment.
- Recommendations contribute to a more efficient and effective incident response process by reducing false positives and false negatives.

Sample business scenario

A sample business scenario is a network security implementation that demonstrates how a large corporate network uses Snort 3 as its primary intrusion detection and prevention system to enhance incident response capabilities through vulnerability-based rule generation and intrusion policy optimization.

Business scenario details

In this scenario, a large corporate network adopts robust network security measures in a rapidly evolving threat landscape. The security team wants to enhance their incident response capabilities by generating recommendations or rule sets based on the vulnerabilities detected in the host network. This helps to optimize their intrusion policies, thereby safeguarding the network more effectively.

Best practices

- You must have high-quality, accurate host data.

  Because of the passive nature of network discovery, your threat defense devices must be positioned as close as possible to your protected hosts. This allows the threat defense devices to watch network traffic to and from these hosts, giving you accurate data about applications, services, and vulnerabilities on your network.

- Devices should have visibility to east–west traffic flows as well as north–south traffic flows to build an accurate host profile.
- You can create a scheduled task to update recommendations automatically.

Prerequisites for generating recommendations

- Ensure that hosts are present in the system to generate recommendations.
- Protected networks configured for recommendations should map to the hosts present in the system.

Generate Snort 3 recommendations

Generate and apply Snort 3 rule recommendations to optimize your intrusion policy based on your network configuration and security requirements.

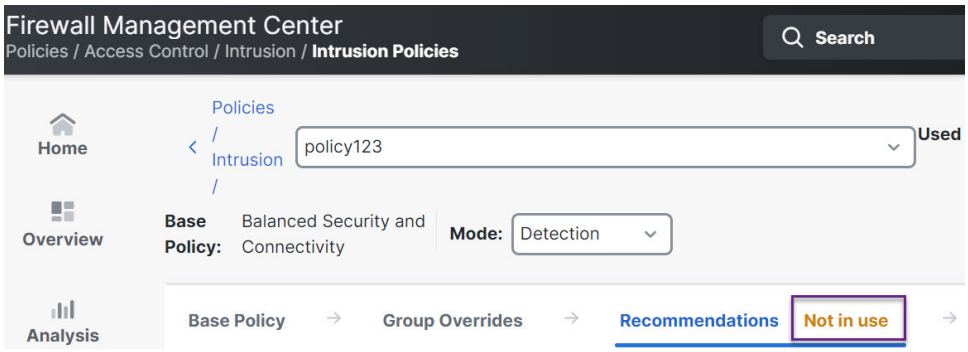
Snort 3 recommendations help you configure intrusion policies with rules that are tailored to your network environment. The system analyzes your protected networks and suggests appropriate security levels and rule configurations.

Procedure

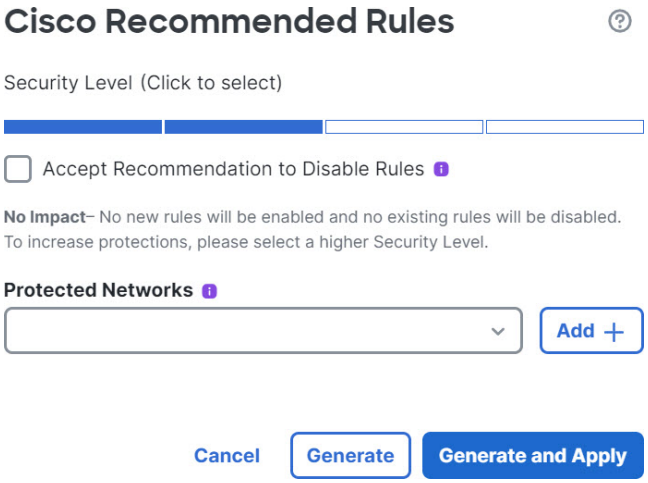
Step 1 Choose **Policies** > **Security policies** > **Intrusion**.

Step 2 Click the **Snort 3 Version** button of the corresponding intrusion policy.

Step 3 Click the **Recommendations (Not in Use)** layer to configure the rule recommendations.



In the **Cisco Recommended Rules** window, you can set the security level.



Step 4 Click to select the security level.

Step 5 (Optional) Check the **Accept Recommendation to Disable Rules** check box to disable the rules written for vulnerabilities not found on the hosts in your network.

Use this option, only if you have to trim your rule set because of a high number of alerts or to improve inspection performance.

Step 6 From the **Protected Networks** drop-down list, choose the network objects that must be examined by the recommendations. By default, any IPv4 or IPv6 networks are selected if you do not make a selection.

Click **Add +** to create a new network object of type **Host** or **Network** and click **Save**.

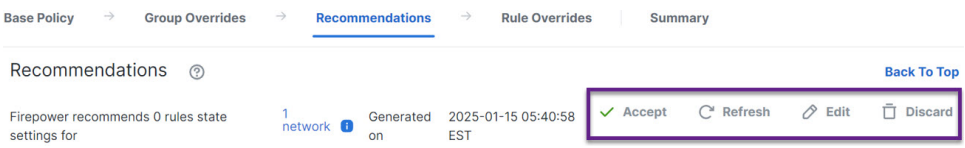
Step 7 Generate and apply recommendations:

- **Generate**—Generates the recommendations for an intrusion policy. This action lists the rules under **Recommended Rules (Not in use)**.
- **Generate and Apply**—Generates and applies the recommendations for an intrusion policy. This action lists the rules under **Recommended Rules (Not in use)**.

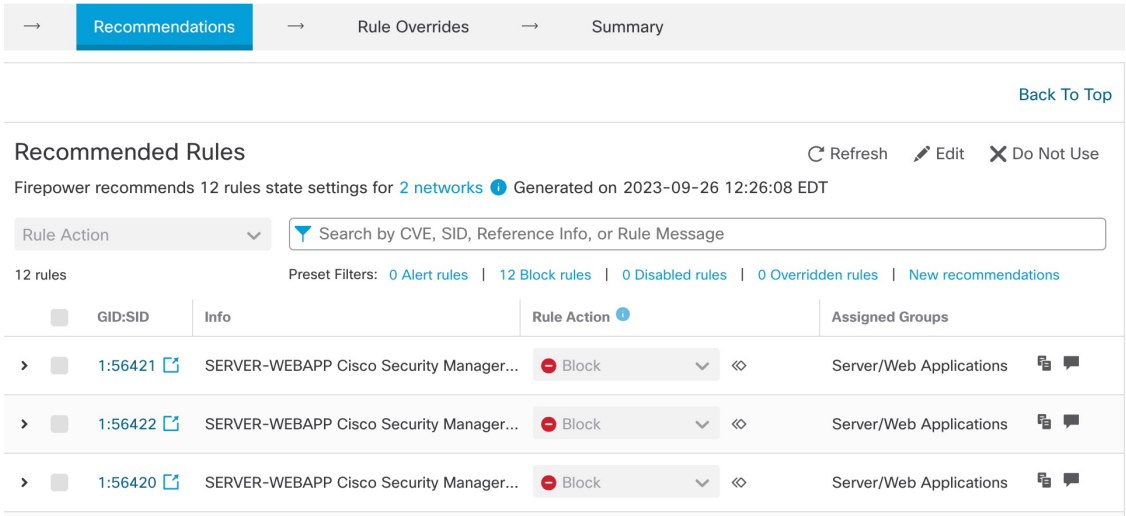
Recommendations are generated successfully. A new recommendation tab appears with all the recommended rules and their corresponding recommended actions. Rule action preset filters are also available for this tab, in addition to new recommendations.

Step 8 Verify the recommendations and then apply them accordingly:

- **Accept**—Applies the previously generated recommendations for an intrusion policy.
- **Refresh**—Regenerates and updates the rule recommendations for an intrusion policy.
- **Edit**—Opens the **Recommendations** dialog box where you can provide the recommendation input values and then generate the recommendations.
- **Discard**—Either reverts or removes the applied recommended rules from the policy; also removes the **Recommendations** tab.



Under **All Rules**, the Recommended Rules section displays the recommended rules.



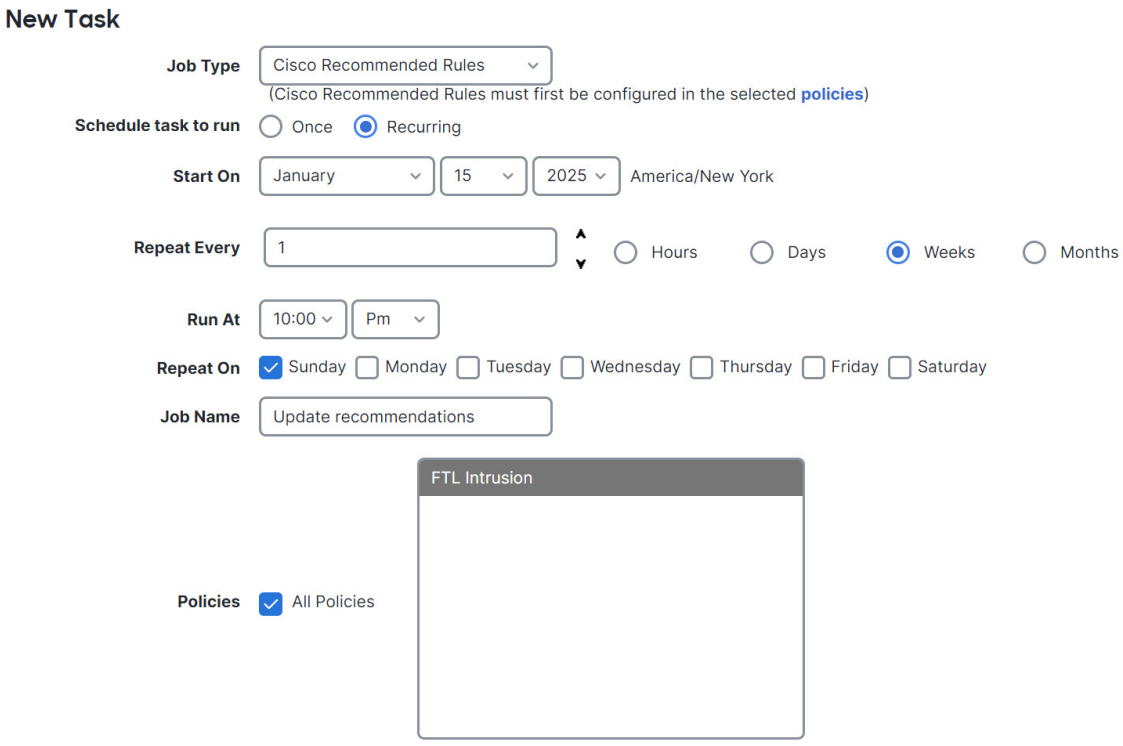
Step 9 To effectively use recommendations, they must be updated periodically. Follow these steps:

a. Choose **Administration** > **Advanced** > **Scheduling**.

b. Click **Add Task**.

c. Choose **Cisco Recommended Rules** from the **Job Type** drop-down list.

d. Update the required fields, as needed.



e. Click **Save**.

What to do next

Deploy configuration changes. Refer to Deploy configuration changes.