

CHAPTER 20

Getting Started with Intrusion Policies

Intrusion policies are defined sets of intrusion detection and prevention configurations that inspect traffic for security violations and, in inline deployments, can block or alter malicious traffic. Intrusion policies are invoked by your access control policy and are the system's last line of defense before traffic is allowed to its destination.

Cisco delivers several intrusion policies with the ASA FirePOWER module. By using system-provided policies you can take advantage of the experience of the Cisco Vulnerability Research Team (VRT). For these policies, the VRT sets intrusion and preprocessor rule states (enabled or disabled), as well as provides the initial configurations for other advanced settings. An enabled rule causes the system to generate intrusion events for (and optionally block) traffic matching the rule. Disabling a rule stops processing of the rule.

Tip 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. Understanding Network Analysis and Intrusion Policies, page 12-1 provides an overview of how network analysis and intrusion policies work together to examine your traffic, as well as some basics on using the navigation panel, resolving conflicts, and committing changes.

If you create a custom intrusion policy, you can:

- Tune detection by enabling and disabling rules, as well as by writing and adding your own rules.
- Configure various advanced settings such as external alerting, sensitive data preprocessing, and global rule thresholding.
- Use layers as building blocks to efficiently manage multiple intrusion policies.

When tailoring your intrusion policy, especially when enabling and adding rules, keep in mind that some intrusion rules require that traffic first be decoded or preprocessed in a certain way. Before an intrusion policy examines a packet, the packet is preprocessed according to configurations in a network analysis policy. If you disable a required preprocessor, the system automatically uses it with its current settings, although the preprocessor remains disabled in the network analysis policy user interface.

Note 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. For more information, see Limitations of Custom Policies, page 12-11.

After you configure a custom intrusion policy, you can use it as part of your access control configuration by associating the intrusion policy with one or more access control rules or an access control policy's default action. This forces the system to use the intrusion policy to examine certain allowed traffic before the traffic passes to its final destination. A variable set that you pair with the intrusion policy allows you to accurately reflect your home and external networks and, as appropriate, the servers on your network. For more information, see Controlling Traffic Using Intrusion and File Policies, page 10-1.

This chapter explains how to create a simple custom intrusion policy. The chapter also contains basic information on managing intrusion policies: editing, comparing, and so on. For more information, see:

- Creating a Custom Intrusion Policy, page 20-2
- Managing Intrusion Policies, page 20-3
- Editing Intrusion Policies, page 20-4
- Applying an Intrusion Policy, page 20-8
- Generating a Report of Current Intrusion Settings, page 20-8
- Comparing Two Intrusion Policies or Revisions, page 20-9

Creating a Custom Intrusion Policy

License: Protection

When you create a new intrusion policy you must give it a unique name, specify a base policy, and specify drop behavior.

The base policy defines the intrusion policy's default settings. Modifying a setting in the new policy overrides—but does not change—the settings in the base policy. You can use either a system-provided or custom policy as your base policy. For more information, see Understanding the Base Layer, page 13-2.

The intrusion policy's drop behavior, or **Drop when Inline** setting, determines how the system handles drop rules (intrusion or preprocessor rules whose rule state is set to Drop and Generate Events) and other intrusion policy configurations that affect traffic. You should enable drop behavior in inline deployments when you want to drop or replace malicious packets. Note that in passive deployments, the system cannot affect traffic flow regardless of the drop behavior. For more information, see Setting Drop Behavior in an Inline Deployment, page 20-5.

To create an intrusion policy:

Step 1 Select **Configuration > ASA FirePOWER Configuration > Policies > Intrusion Policy**.

The Intrusion Policy page appears.



Tip You can also import a policy from another ASA FirePOWER module; see Importing and Exporting Configurations, page B-1.

Step 2 Click **Create Policy**.

If you have unsaved changes in another policy, click **Cancel** when prompted to return to the Intrusion Policy page. See Resolving Conflicts and Committing Policy Changes, page 12-15 for information on saving unsaved changes in another policy.

The Create Intrusion Policy pop-up window appears.

Step 3 Give the policy a unique **Name** and, optionally, a **Description**.

Step 4 Specify the initial **Base Policy**.

You can use either a system-provided or custom policy as your base policy.

Caution Do **not** use `Experimental Policy 1` unless instructed to do so by a Cisco representative. Cisco uses this policy for testing.

Step 5 Set the system's drop behavior in an inline deployment:

- To allow intrusion policies to affect traffic and generate events, enable **Drop when Inline**.
- To prevent intrusion policies from affecting traffic while still generating events, disable **Drop when Inline**.

Step 6 Create the policy:

- Click **Create Policy** to create the new policy and return to the Intrusion Policy page. The new policy has the same settings as its base policy.
- Click **Create and Edit Policy** to create the policy and open it for editing in the advanced intrusion policy editor; see Editing Intrusion Policies, page 20-4.

Managing Intrusion Policies

License: Protection

On the Intrusion Policy page (**Configuration > ASA FirePOWER Configuration > Policies > Intrusion Policy**) you can view your current custom intrusion policies, along with the following information:

- the time and date the policy was last modified (in local time)
- whether the **Drop when Inline** setting is enabled, which allows you to drop and modify traffic in an inline deployment
- which access control policies are using the intrusion policy to inspect traffic
- whether a policy has unsaved changes

Options on the Intrusion Policy page allow you to take the actions in the following table.

Table 20-1 Intrusion Policy Management Actions

To...	You can...	See...
create a new intrusion policy	click **Create Policy**.	Creating a Custom Intrusion Policy, page 20-2
edit an existing intrusion policy	click the edit icon ( ).	Editing Intrusion Policies, page 20-4
reapply an intrusion policy	click the apply icon ( ).	Applying an Intrusion Policy, page 20-8
export an intrusion policy to import on another ASA FirePOWER module	click the export icon ( ).	Exporting Configurations, page B-1

Table 20-1 Intrusion Policy Management Actions (continued)

To...	You can...	See...
view a PDF report that lists the current configuration settings in a intrusion policy	click the report icon ( ).	Generating a Report of Current Intrusion Settings, page 20-8
compare the settings of two intrusion policies or two revisions of the same policy	click **Compare Policies**.	Comparing Two Intrusion Policies or Revisions, page 20-9
delete an intrusion policy	click the delete icon ( ), then confirm that you want to delete the policy. You cannot delete an intrusion policy if an access control policy references it.	

Editing Intrusion Policies

License: Protection

When you create a new intrusion policy, it has the same intrusion rule and advanced settings as its base policy. The following table explains the most common actions taken when editing an intrusion policy:

Table 20-2 Intrusion Policy Editing Actions

To...	You can...	See...
specify drop behavior in an inline deployment	select or clear the **Drop when Inline** check box on the Policy Information page.	Setting Drop Behavior in an Inline Deployment, page 20-5
change the base policy	select a base policy from the **Base Policy** drop-down list on the Policy Information page.	Changing the Base Policy, page 13-3
view the settings in the base policy	click **Manage Base Policy** on the Policy Information page	Understanding the Base Layer, page 13-2
display or configure intrusion rules	click **Manage Rules** on the Policy Information page.	Viewing Rules in an Intrusion Policy, page 21-2
display a filtered view of intrusion rules by current rule state and, optionally, configure those rules	on the Policy Information page, click **View** next to the number of rules under **Manage Rules** that are set to Generate Events or to Drop and Generate Events.	Filtering Rules in an Intrusion Policy, page 21-9
enable, disable, or edit advanced settings	click **Advanced Settings** in the navigation panel	Configuring Advanced Settings in an Intrusion Policy, page 20-6
manage policy layers	click **Policy Layers** in the navigation panel	Using Layers in a Network Analysis or Intrusion Policy, page 13-1

When tailoring an intrusion policy, especially when enabling and adding rules, keep in mind that some intrusion rules require that traffic first be decoded or preprocessed in a certain way. Before an intrusion policy examines a packet, the packet is preprocessed according to configurations in a network analysis policy. If you disable a required preprocessor, the system automatically uses it with its current settings, although the preprocessor remains disabled in the network analysis policy user interface.

Note 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. For more information, see Limitations of Custom Policies, page 12-11.

The system caches one intrusion policy. While editing an intrusion 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. In addition to the actions you can perform in the table above, Understanding Network Analysis and Intrusion Policies, page 12-1 provides information on resolving conflicts and committing changes

To edit a intrusion policy:

Step 1 Select **Configuration > ASA FirePOWER Configuration > Policies > Intrusion Policy**.

The Intrusion Policy page appears.

Step 2 Click the edit icon ( ) next to the intrusion policy you want to configure.

The intrusion policy editor appears, focused on the Policy Information page and with a navigation panel on the left.

Step 3 Edit your policy. Take any of the actions summarized above.

Step 4 Save your policy, continue editing, discard your changes, or exit while leaving your changes in the system cache. For more information, see Resolving Conflicts and Committing Policy Changes, page 12-15.

Setting Drop Behavior in an Inline Deployment

License: Protection

In an inline deployment, an intrusion policy can block and modify traffic:

- *Drop rules* can drop matching packets and generate intrusion events. To configure an intrusion or preprocessor drop rule, set its state to Drop and Generate Events; see Setting Rule States, page 21-19.
- Intrusion rules can use the `replace` keyword to replace malicious content; see Replacing Content in Inline Deployments, page 24-29.

For intrusion rules to affect traffic, you must correctly configure drop rules and rules that replace content, as well as correctly deploy the system inline. Finally, you must enable the intrusion policy's *drop behavior*, or **Drop when Inline** setting.

Note To block the transfer of malware files over FTP, you must not only correctly configure network-based advanced malware protection (AMP), but also enable **Drop when Inline** in your access control policy's default intrusion policy. To determine or change the default intrusion policy, see Setting the Default Intrusion Policy for Access Control, page 14-1.

If you want to assess how your configuration would function in an inline deployment without actually affecting traffic, you can disable drop behavior. In this case, the system generates intrusion events but does not drop packets that trigger drop rules. When you are satisfied with the results, you can enable drop behavior.

Note that in passive deployments the system cannot affect traffic regardless of the drop behavior. In other words, in a passive deployment, rules set to Drop and Generate Events behave identically to rules set to Generate Events—the system generates intrusion events but cannot drop packets.

When you view intrusion events, workflows can include the *inline result*, which indicates whether traffic was actually dropped, or whether it only would have dropped. When a packet matches a drop rule, the inline result is:

- `Dropped`, for packets dropped by a correctly configured inline deployment with drop behavior enabled
- `Would have dropped`, for packets that were not dropped either because your device is deployed passively or because drop behavior is disabled. Note that the inline result is always `Would have dropped` for packets seen while the system is pruning, regardless of deployment.

To set the drop behavior of an intrusion policy in an inline deployment:

Step 1 Select **Configuration > ASA FirePOWER Configuration > Policies > Intrusion Policy**.

The Intrusion Policy page appears.

Step 2 Click the edit icon ( ) next to the policy you want to edit.

The Policy Information page appears.

Step 3 Set the policy's drop behavior:

- To allow intrusion rules to affect traffic and generate events, enable **Drop when Inline**.
- To prevent intrusion rules from affecting traffic while still generating events, disable **Drop when Inline**.

Step 4 Save your policy, continue editing, discard your changes, or exit while leaving your changes in the system cache. For more information, see Resolving Conflicts and Committing Policy Changes, page 12-15.

Configuring Advanced Settings in an Intrusion Policy

License: Protection

An intrusion policy's *advanced settings* require specific expertise to configure. The base policy for your intrusion policy determines which advanced settings are enabled by default and the default configuration for each.

When you select **Advanced Settings** in the navigation panel of an intrusion policy, the policy lists its advanced settings by type. On the Advanced Settings page, you can enable or disable advanced settings in your intrusion policy, as well as access advanced setting configuration pages.

An advanced setting must be enabled for you to configure it. When you enable an advanced setting, a sublink to the configuration page for the advanced setting appears beneath the **Advanced Settings** link in the navigation panel, and an **Edit** link to the configuration page appears next to the advanced setting on the Advanced Settings page.



Tip To revert an advanced setting's configuration to the settings in the base policy, click **Revert to Defaults** on the configuration page for the advanced setting. When prompted, confirm that you want to revert.

When you disable an advanced setting, the sublink and **Edit** link no longer appear, but your configurations are retained. Note that some intrusion policy configurations (sensitive data rules, SNMP alerts for intrusion rules) require enabled and correctly configured advanced settings. You cannot save an intrusion policy misconfigured in this way; see Resolving Conflicts and Committing Policy Changes, page 12-15.

Modifying the configuration of an advanced setting requires an understanding of the configuration you are modifying and its potential impact on your network. The following sections provide links to specific configuration details for each advanced setting.

Specific Threat Detection

The sensitive data preprocessor detects sensitive data such as credit card numbers and Social Security numbers in ASCII text. For information on configuring this preprocessor, see Detecting Sensitive Data, page 22-19.

Note that other preprocessors that detect specific threats (back orifice attacks, several portscan types, and rate-based attacks that attempt to overwhelm your network with excessive traffic) are configured in network analysis policies. For more information, see Detecting Specific Threats, page 22-1.

Intrusion Rule Thresholds

Global rule thresholding can prevent your system from being overwhelmed with a large number of events by allowing you to use thresholds to limit the number of times the system logs and displays intrusion events. For more information, see Globally Limiting Intrusion Event Logging, page 23-1.

External Responses

In addition to the various views of intrusion events within the user interface, you can enable logging to system log (syslog) facilities or send event data to an SNMP trap server. Per policy, you can specify intrusion event notification limits, set up intrusion event notification to external logging facilities, and configure external responses to intrusion events. For more information, see:

- Configuring SNMP Responses, page 30-3
- Configuring Syslog Responses, page 30-6

Applying an Intrusion Policy

License: Protection

After you apply an intrusion policy using access control (see Deploying Configuration Changes, page 4-11), you can reapply the intrusion policy at any time. This allows you to implement intrusion policy changes on your monitored network without reapplying the access control policy. While reapplying, you can also view a comparison report to review the changes made since the last time the intrusion policy was applied.

Note the following when reapplying intrusion policies:

- You can schedule intrusion policy reapply tasks to recur on a regular basis; see Automating Applying an Intrusion Policy, page 33-4.
- When you import a rule update, you can automatically apply intrusion policies after the import completes. If you do not enable this option, you must manually reapply the policies changed by the rule update. See Importing Rule Updates and Local Rule Files, page 37-9 for more information.

To reapply an intrusion policy:

Step 1 Select **Configuration > ASA FirePOWER Configuration > Policies > Intrusion Policy**.

The Intrusion Policy page appears.

Step 2 Click the apply icon ( ) next to the policy you want to reapply.

The Reapply Intrusion Policy window appears.

Step 3 Click **Reapply**.

The policy is reapplied. You can monitor the status of the apply using the task queue (**Monitoring > ASA FirePOWER Monitoring > Task Status**). See Viewing the Task Queue, page C-1 for more information.

Generating a Report of Current Intrusion Settings

License: Protection

An intrusion policy report is a record of the policy configuration at a specific point in time. The system combines the settings in the base policy with the settings of the policy layers, and makes no distinction between which settings originated in the base policy or policy layer.

You can use the report, which contains the following information, for auditing purposes or to inspect the current configuration.

Table 20-3 Intrusion Policy Report Sections

Section	Description
Policy Information	Provides the name and description of the intrusion policy, the name of the user who last modified the policy, and the date and time the policy was last modified. Also indicates whether dropping packets in an inline deployment is enabled or disabled, the current rule update version, and whether the base policy is locked to the current rule update.

Table 20-3 Intrusion Policy Report Sections (continued)

Section	Description
Advanced Settings	Lists all enabled intrusion policy advanced settings and their configurations.
Rules	Provides a list of all enabled rules and their actions.

You can also generate a comparison report that compares two intrusion policies, or two revisions of the same policy. For more information, see Comparing Two Intrusion Policies or Revisions, page 20-9.

To view an intrusion policy report:

Step 1 Select **Configuration > ASA FirePOWER Configuration > Policies > Intrusion Policy**.

The Intrusion Policy page appears.

Step 2 Click the report icon ( ) next to the intrusion policy for which you want to generate a report. Remember to commit any potential changes before you generate an intrusion policy report; only committed changes appear in the report.

The system generates the intrusion policy report. You are prompted to save the report to your computer.

Comparing Two Intrusion Policies or Revisions

License: Protection

To review policy changes for compliance with your organization's standards or to optimize system performance, you can examine the differences between two intrusion policies. You can compare any two intrusion policies or two revisions of the same intrusion policy, for the intrusion policies you can access. Optionally, after you compare, you can then generate a PDF report to record the differences between the two policies or policy revisions.

There are two tools you can use to compare intrusion policies:

- The comparison view displays only the differences between two intrusion policies or intrusion policy revisions in a side-by-side format; the name of each policy appears in the title bar on the left and right sides of the comparison view.

  You can use this to view and navigate both policy revisions on the user interface, with their differences highlighted.

- The comparison report creates a record of only the differences between two intrusion policies or intrusion policy revisions in a format similar to the intrusion policy report, but in PDF format.

  You can use this to save, copy, print and share your policy comparisons for further examination.

For more information on understanding and using the intrusion policy comparison tools, see:

- Using the Intrusion Policy Comparison View, page 20-9
- Using the Intrusion Policy Comparison Report, page 20-10

Using the Intrusion Policy Comparison View

License: Protection

The comparison view displays both intrusion policies or policy revisions in a side-by-side format, with each policy or policy revision identified by name in the title bar on the left and right sides of the comparison view. The time of last modification and the last user to modify are displayed to the right of the policy name. Note that the Intrusion Policy page displays the time a policy was last modified in local time, but the intrusion policy report lists the time modified in UTC. Differences between the two intrusion policies or policy revisions are highlighted:

- Blue indicates that the highlighted setting is different in the two policies or policy revisions, and the difference is noted in red text.
- Green indicates that the highlighted setting appears in one policy or policy revision but not the other.

You can perform any of the actions described in the following table.

Table 20-4 Intrusion Policy Comparison View Actions

To...	You can...
navigate individually through changes	click **Previous** or **Next** above the title bar. The double-arrow icon ( ) centered between the left and right sides moves, and the **Difference** number adjusts to identify which difference you are viewing.
generate a new intrusion policy comparison view	click **New Comparison**. The **Select Comparison** window appears. See Using the Intrusion Policy Comparison Report for more information.
generate an intrusion policy comparison report	click **Comparison Report**. The policy comparison report creates a PDF that lists only the differences between the two policies or policy revisions.

Using the Intrusion Policy Comparison Report

License: Protection

An intrusion policy comparison report is a record of all differences between two intrusion policies or two revisions of the same intrusion policy identified by the intrusion policy comparison view, presented as a PDF. You can use this report to further examine the differences between two intrusion policy configurations and to save and disseminate your findings.

You can generate an intrusion policy comparison report from the comparison view for any intrusion policies to which you have access. Remember to commit any potential changes before you generate an intrusion policy report; only committed changes appear in the report.

The format of the intrusion policy comparison report is the same as the intrusion policy report with one exception: the intrusion policy report contains all settings in the intrusion policy, and the intrusion policy comparison report lists only those settings which differ between the policies.

Depending on your configuration, an intrusion policy comparison report can contain one or more sections as described in the Intrusion Policy Report Sections table.

Tip You can use a similar procedure to compare access control, network analysis, file, or system policies.

To compare two intrusion policies or two revisions of the same policy:

Step 1 Select **Configuration > ASA FirePOWER Configuration > Policies > Intrusion Policy**.

The Intrusion Policy page appears.

Step 2 Click **Compare Policies**.

The Select Comparison window appears.

Step 3 From the **Compare Against** drop-down list, select the type of comparison you want to make:

- To compare two different policies, select **Other Policy**.
- To compare two revisions of the same policy, select **Other Revision**.

Remember to commit any changes before you generate an intrusion policy report; only committed changes appear in the report.

Step 4 Depending on the comparison type you selected, you have the following choices:

- If you are comparing two different policies, select the policies you want to compare from the **Policy A** and **Policy B** drop-down lists.
- If you are comparing two revisions of the same policy, select the policy from the **Policy** drop-down list, then select the revisions you want to compare from the **Revision A** and **Revision B** drop-down lists.

Step 5 Click **OK** to display the intrusion policy comparison view.

The comparison view appears.

Step 6 Click **Comparison Report** to generate the intrusion policy comparison report.

Step 7 The intrusion policy report appears. You are prompted to save the report to your computer.