Getting Started with Snort 3 Intrusion Policies

Getting Started with Snort 3 Intrusion Policies chapter provides an insight into Intrusion Policy basics. It provides information on creating custom Snort 3 intrusion policy, changing the inspection mode of an intrusion policy, and access control rule configuration to perform intrusion prevention.

Intrusion Policy Basics

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.

At the heart of each intrusion policy are the intrusion rules. 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.

The system delivers several base intrusion policies, which enable you to take advantage of the experience of the Cisco Talos Intelligence Group (Talos). For these policies, Talos sets intrusion and inspector rule states (enabled or disabled), as well as provides the initial configurations for other advanced settings.

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.

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.
- Use Firepower recommendations to associate the operating systems, servers, and client application protocols detected on your network with rules specifically written to protect those assets.

An intrusion policy can drop matching packets and generate intrusion events. To configure an intrusion or preprocessor drop rule, set its state to Block.

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 inspector, the system automatically uses it with its current settings, although the inspector remains disabled in the network analysis policy web interface.

⚠ **Caution** 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.

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.

Note that by default, the system disables intrusion inspection of encrypted payloads. This helps reduce false positives and improve performance when an encrypted connection matches an access control rule that has intrusion inspection configured.

Refer to the video for additional support and information - Snort 3 Intrusion Policy Overview.

Requirements and Prerequisites for Intrusion Policies

Model Support

Threat Defense

Supported Domains

Any

User Roles

- Admin
- Intrusion Admin

Creating a Custom Snort 3 Intrusion Policy

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

Step 2 Click **Create Policy**.

Step 3 Enter a unique **Name** and, optionally, a **Description**.

Step 4 Choose the **Inspection Mode**.

The selected action determines whether intrusion rules block and alert (**Prevention** mode) or only alert (**Detection** mode).

Note Before selecting the prevention mode, you might want block rules to alert only so you can identify rules that cause a lot of false positives.

Step 5 Choose the **Base Policy**.

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

Step 6 Click **Save**.

The new policy has the same settings as its base policy.

What to do next

To customize the policy, see Edit Snort 3 Intrusion Policies, on page 3.

Edit Snort 3 Intrusion Policies

While editing a Snort 3 policy, all the changes are saved instantaneously. No additional action is required to save the changes.

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

Step 2 Ensure the **Intrusion Policies** tab is selected.

Step 3 Click **Snort 3 Version** next to the intrusion policy you want to configure.

Step 4 Edit your policy:

To change the base policy, see Changing the Base Policy of an Intrusion Policy, on page 4.

What to do next

Deploy configuration changes; see Deploy Configuration Changes, on page 6.

Changing the Base Policy of an Intrusion Policy

You can choose a different system-provided or custom policy as your base policy.

You can chain up to five custom policies, with four of the five using one of the other four previously created policies as its base policy; the fifth must use a system-provided policy as its base.

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

Step 2 Click **Edit** (✎) next to the intrusion policy you want to configure.

Step 3 Choose a policy from the **Base Policy** drop-down list.

Step 4 Click **Save**.

What to do next

Deploy configuration changes; see Deploy Configuration Changes, on page 6.

Changing the Inspection Mode of an Intrusion Policy for Both Snort 2 and Snort 3 Versions

You can choose to have a different inspection mode for an existing intrusion policy. The change is applied on the device after a successful deployment. Follow the steps in this topic to change the inspection mode for both Snort 2 and Snort 3 versions of an intrusion policy.

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

Step 2 Click **Edit** (✎) next to the intrusion policy you want to change.

Step 3 Select the **Inspection Mode** that you want to apply to the policy.

Step 4 Click **Save**.

What to do next

Deploy configuration changes; see Deploy Configuration Changes, on page 6.

Managing Intrusion Policies

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

- Number of access control policies and devices are using the intrusion policy to inspect traffic
- In a multidomain deployment, the domain where the policy was created

In a multidomain deployment, the system displays policies created in the current domain, which you can edit. It also displays policies created in ancestor domains, which you cannot edit. To view and edit policies created in a lower domain, switch to that domain.

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

Step 2 Manage your intrusion policy:

- Create — Click **Create Policy**; see Creating a Custom Snort 3 Intrusion Policy , on page 3.
- Delete — Click **Delete** (🗑) next to the policy you want to delete. The system prompts you to confirm and informs you if another user has unsaved changes in the policy. Click **OK** to confirm.

  If the controls are dimmed, the configuration belongs to an ancestor domain, or you do not have permission to modify the configuration.
- Edit intrusion policy details — Click **Edit** (✎) next to the policy you want to edit. You can edit the **Name**, **Inspection Mode**, and the **Base Policy** of the intrusion policy.
- Edit intrusion policy settings — Click **Snort 3 Version**; see Edit Snort 3 Intrusion Policies, on page 3.
- Export — If you want to export an intrusion policy to import on another management center, click Export; see the *Exporting Configurations* topic in the latest version of the *Firepower Management Center Configuration Guide*.
- Deploy — Choose **Deploy** > **Deployment**; see Deploy Configuration Changes, on page 6.
- Report — Click **Report**; see the *Generating Current Policy Reports* topic in the latest version of the *Firepower Management Center Configuration Guide*. Generates wo reports, one for each policy version.

Access Control Rule Configuration to Perform Intrusion Prevention

An access control policy can have multiple access control rules associated with intrusion policies. You can configure intrusion inspection for any Allow or Interactive Block access control rule, which permits you to match different intrusion inspection profiles against different types of traffic on your network before it reaches its final destination.

Whenever the system uses an intrusion policy to evaluate traffic, it uses an associated *variable set*. Variables in a set represent values commonly used in intrusion rules to identify source and destination IP addresses and ports. You can also use variables in intrusion policies to represent IP addresses in rule suppressions and dynamic rule states.

Tip Even if you use system-provided intrusion policies, Cisco **strongly** recommends you configure the system's intrusion variables to accurately reflect your network environment. At a minimum, modify default variables in the default set.

Understanding System-Provided and Custom Intrusion Policies

Cisco delivers several intrusion policies with the system. By using system-provided intrusion policies, you can take advantage of the experience of the Cisco Talos Intelligence Group (Talos). For these policies, Talos sets intrusion and preprocessor rule states, as well as provides the initial configurations for advanced settings. You can use system-provided policies as-is, or you can use them as the base for custom policies. Building custom policies can improve the performance of the system in your environment and provide a focused view of the malicious traffic and policy violations occurring on your network.

Connection and Intrusion Event Logging

When an intrusion policy invoked by an access control rule detects an intrusion and generates an intrusion event, it saves that event to the Management Center. The system also automatically logs the end of the connection where the intrusion occurred to the Management Center database, regardless of the logging configuration of the access control rule.

Access Control Rule Configuration and Intrusion Policies

The number of unique intrusion policies you can use in a single access control policy depends on the model of the target devices; more powerful devices can handle more. Every unique **pair** of intrusion policy and variable set counts as one policy. Although you can associate a different intrusion policy-variable set pair with each Allow and Interactive Block rule (as well as with the default action), you cannot deploy an access control policy if the target devices have insufficient resources to perform inspection as configured.

Configuring an Access Control Rule to Perform Intrusion Prevention

You must be an Admin, Access Admin, or Network Admin to perform this task.

Step 1 In the access control policy editor, create a new rule or edit an existing rule; see the *Access Control Rule Components* topic in the latest version of the *Firepower Management Center Configuration Guide*.

Step 2 Ensure the rule action is set to **Allow**, **Interactive Block**, or **Interactive Block with reset**.

Step 3 Click **Inspection**.

Step 4 Choose a system-provided or a custom intrusion policy, or choose **None** to disable intrusion inspection for traffic that matches the access control rule.

Step 5 If you want to change the variable set associated with the intrusion policy, choose a value from the **Variable Set** drop-down list.

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

Step 7 Click **Save** to save the policy.

What to do next

Deploy configuration changes; see Deploy Configuration Changes, on page 6.

Deploy Configuration Changes

After you change configurations, deploy them to the affected devices.

Note This topic covers the basic steps to deploy configuration changes. We *strongly* recommend that you refer the *Deploy Configuration Changes* topic in the latest version of the *Firepower Management Center Configuration Guide* to understand the prerequisites and the implications of deploying the changes before proceeding with the steps.

Caution When you deploy, resource demands may result in a small number of packets dropping without inspection. Additionally, deploying some configurations restarts the Snort process, which interrupts traffic inspection. Whether traffic drops during this interruption or passes without further inspection depends on how the target device handles traffic.

Step 1 On the Secure Firewall Management Center menu bar, click **Deploy** and then select **Deployment**.

The GUI page lists the devices with out-of-date configurations having the pending status.

- The **Modified By** column lists the users who have modified the policies or objects. On expanding the device listing, you can view the users who have modified the policies against each policy listing.

  Note Usernames are not provided for deleted policies and objects.

- The **Inspect Interruption** column indicates if traffic inspection interruption may be caused in the device during deployment.

  If the entry is blank in this column for a device, then it indicates that there will be no traffic inspection interruptions on that device during deployment.

- The **Last Modified Time** column specifies when you last made the configuration changes.
- The **Preview** column allows you to preview the changes for the next deployment.
- The **Status** column provides the status for each deployment.

Step 2 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 the changes for the device, which are listed under the device, are pushed for deployment. However, you can use **Policy selection** ( ) to select individual policies or specific configurations to deploy while withholding the remaining changes without deploying them.

  Note
  - When the status in the **Inspect Interruption** column indicates (Yes) that deploying will interrupt inspection, and perhaps traffic, on a threat defense device, the expanded list indicates the specific configurations causing the interruption with the **Inspect Interruption** ( ).
  - When there are changes to interface groups, security zones, or objects, the impacted devices are shown as out-of-date on the management center. To ensure that these changes take effect, the policies with these interface groups, security zones, or objects, also need to be deployed along with these changes. The impacted policies are shown as out-of-date on the Preview page on the management center.

Step 3 Click **Deploy**.

Step 4 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.

You have the following choices:

- Deploy—Continue deploying without resolving warning conditions. You cannot proceed if the system identifies errors.
- Close—Exit without deploying. Resolve the error and warning conditions, and attempt to deploy the configuration again.

What to do next

During deployment, if there is a deployment failure due to any reason, there is a possibility that the failure may impact traffic. However, it depends on certain conditions. If there are specific configuration changes in the deployment, the deployment failure may lead to traffic being interrupted. For details, see *Deploy Configuration Changes* topic in the latest version of the *Firepower Management Center Configuration Guide*.