Tailor Intrusion Protection for Your Network Assets

This chapter provides an insight into Firepower recommended rules and generating and applying Firepower recommended rules.

Snort 3 Rule Changes in LSP Updates

During regular Snort 3 Lightweight Security Package (LSP) updates, an existing system-defined intrusion rule may be replaced with a new intrusion rule. There could be possibilities of a single rule being replaced with multiple rules, or multiple rules being replaced with a single rule. This occurs when better detection is possible for which rules are combined or expanded. For better management, some existing system-defined rules may also be removed as a part of the LSP update.

To get notifications for changes to any *overridden* system-defined rules during LSP updates, ensure that the **Retain user overrides for deleted Snort 3 rules** check box is checked.

To navigate to the **Retain user overrides for deleted Snort 3 rules** check box, click **System** (⚙) > **Configuration** > **Intrusion Policy Preferences**.

By default this check box is checked. When this check box is checked, the system retains the rule overrides in the new replacement rules that are added as a part of the LSP update. The notifications are shown in the **Tasks** tab under the Notifications icon that is located next to **System** (⚙).

Overview of Firepower Recommended Rules

You can use intrusion rule recommendations to target vulnerabilities associated with host assets detected in the network. For example, operating systems, servers, and client application protocols. This allows you to tailor your intrusion policy to the specific needs of your monitored network.

The system makes an individual set of recommendations for each intrusion policy. It typically recommends rule state changes for standard text rules and shared object rules. However, it can also recommend changes for inspector and decoder rules.

When you generate rule state recommendations, you can use the default settings or configure advanced settings. Advanced settings allow you to:

- Redefine which hosts on your network the system monitors for vulnerabilities
- Influence which rules the system recommends based on rule overhead
- Specify whether to generate recommendations to disable rules

You can also choose to use the recommendations immediately or review the recommendations (and affected rules) before accepting them.

Choosing to use recommended rule states adds a read-only Firepower Recommendations layer to your intrusion policy, and subsequently choosing not to use recommended rule states removes the layer.

You can schedule a task to generate recommendations automatically based on the most recently saved configuration settings in your intrusion policy.

The system does not change rule states that you set manually such as:

- Manually setting the states of specified rules *before* you generate recommendations prevents the system from modifying the states of those rules in the future.
- Manually setting the states of specified rules *after* you generate recommendations overrides the recommended states of those rules.

Tip The intrusion policy report can include a list of rules with rule states that differ from the recommended state.

While displaying the recommendation-filtered Rules page, or after accessing the Rules page directly from the navigation panel or the Policy Information page, you can manually set rule states, sort rules, and take any of the other actions available on the Rules page, such as suppressing rules, setting rule thresholds, and so on.

Note The Cisco Talos Intelligence Group (Talos) determines the appropriate state of each rule in the system-provided policies. If you use a system-provided policy as your base policy, and you allow the system to set your rules to the Firepower recommended rule state, the rules in your intrusion policy match the settings recommended for your network assets.

Prerequisites for Network Analysis and Intrusion Policies

To allow the Snort inspection engine to process traffic for intrusion and malware analysis, you must have the IPS license enabled for the FTD device.

You must be an Admin user to manage network analysis, intrusion policies, and perform migration tasks.

Migrating Snort 2 Generated Firepower Recommendations to Snort 3

Starting or stopping use of Firepower recommendations may take several minutes, depending on the size of your network and intrusion rule set.

Firepower recommendations cannot be generated for the Snort 3 version directly. Generate the Firepower recommendations for Snort 2 version of the intrusion policy and then follow the steps that are listed here to migrate the recommended rule settings to Snort 3.

Before you begin

Ensure that hosts are present in the system to generate recommendations.

Procedure

Step 1 Choose **Policies** > **Access Control heading** > **Intrusion**.

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

Step 3 Generate and apply recommendations in the Snort 2 version of the intrusion policy.

See the *Generating and Applying Firepower Recommendations* topic in the latest version of the *Firepower Management Center Configuration Guide*, and perform the steps provided in the topic.

Step 4 Synchronize the Snort 2 rule changes with Snort 3.

For steps, see Synchronize Snort 2 Rules with Snort 3.

Note
During upgrade from pre-7.0 to 7.0 version any existing Snort 2 recommendations will be synched to Snort 3. However, if you generated (not fresh) Snort 2 recommendations after upgrade to 7.0, then **you can synchronize** all these recommendations to Snort 3 version.

What to do next

Deploy configuration changes; see Deploy Configuration Changes.