Tailoring Intrusion Protection to Your Network Assets

Tailoring Intrusion Protection to Your Network Assets 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 intrusion rule (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 would occur in case where 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. As a system 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 **Cog** ( ).

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

About 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 either to use the recommendations immediately or to 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:

- 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 by Cisco for your network assets.

Generating New Firepower Recommendations to Snort 3

Generate the Firepower recommendations for the intrusion policy and then follow the steps that are listed here to create new recommended rule settings to Snort 3. Rule overheads are interpreted as **security levels** based on the threshold policies selected by you in Snort 3. Recommended action is based on the selected security level and if it is higher than the base policy, then recommendation is not just limited to generating the events.

Prior to setting the Firepower recommendations you should ask which of the three points listed below closely matches the goal:

- Increased Protection - Enable additional rules based on vulnerabilities found in the host database and do not automatically disable any rules. This will likely result in a larger rule set.
- Focused Protection - Enable additional rules based and disable existing rules based on vulnerabilities found in the host database. This can increase or decrease the number of rules depending on vulnerabilities discovered.
- Higher Efficiency - Use the currently enabled rule set and disable any rules for vulnerabilities not found in the host database. This will likely result in a smaller enabled rule set.

Based on the response, the recommendation actions are as follows:

- Set recommendations to the next highest security level, and uncheck the disable rules.
- Set recommendations to the next highest security level, and check the disable rules.
- Set recommendations to the current security level, and check the disable rules.

Before you begin

Firepower recommendations have the following requirements:

- Threat Defense License—Threat
- Classic License—Protection
- User Roles—Admin or Intrusion Admin
- Ensure that hosts are present in the system to generate recommendations.
- Protected networks configured for recommendations should map to the hosts present in system

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

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

Step 3 Click **Recommendations** from the left panel to configure the rule recommendations.

In the Firepower Rule Recommendations window you can set the following:

- **Security Level**: Select the security levels in combination with either selecting the checkbox or not:
  - Security Level matches the Base Policy or lower than the Base Policy and disable checkbox is unchecked.

    No Impact - No new rules will be enabled and no existing rules will be disabled. To increase the protection, select a higher security level.
  - Security level matches Base Policy and disable checkbox is checked.

    Higher Efficiency - Keeps existing rules that match potential vulnerabilities on discovered hosts and disables rules for vulnerabilities not found on the network.
  - Security level higher than the Base Policy (not maximum detection) and disable checkbox is unchecked.

    Increased Security - Enables additional rules that match potential vulnerabilities on discovered hosts based on the Security Over Connectivity ruleset.

- Security Level higher than the Base Policy (not maximum detection) and disable checkbox is checked.

  Focused Security - Enables additional rules that match vulnerabilities on discovered hosts based on the Security Over Connectivity ruleset, while disabling existing rules that do not match potential vulnerabilities on discovered hosts.

- Security Level increased to Maximum Detection (with lower Base Policy) and disable checkbox is unchecked or checked.

  Increased Protection - Enables a very high number of rules and may impact performance. It is recommended to review and test this setting before deploying into a production environment.

- Security Level lower than Base Policy and disable checkbox is checked.

  Lower Security - All rules will be disabled except for rules in the Connectivity Over Security ruleset which match potential vulnerabilities on discovered hosts. It is recommended instead of adjusting the Base Policy.

- **Protected Networks**: Specifies the monitored networks or individual hosts to examine for recommendations. You can select one or more system or custom defined network objects from the drop-down list. By default, any IPv4 and any IPv6 networks are selected, if no selection is done.

  Important The Secure Firewall Rule Recommendations depend on network discovery. Protected Networks apply to any hosts discovered within the ranges configured in your Network Discovery policy. For more information, see the chapter Network Discovery Policies in the *Cisco Firepower Management Center Device Configuration guide*.

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

- **Accept Recommendations to Disable Rules**: Specifies whether the system disables intrusion rules that are based on Firepower recommendations.

Step 4 Generate and apply recommendations:

- **Generate**: Generates the recommendations for an Intrusion policy. Generate action lists the rules under Recommended Rules (Not in use).
- **Generate and Apply**: Generates and Applies the recommendations for an Intrusion policy. Generate and Apply action lists the rules under Recommended Rules (In use).

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

Step 5 You can verify the recommendations and then choose to 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** - It opens the Recommendations dialog box, you can provide the recommendation input values and then generate the recommendations.
- **Remove All** - Revert or remove the applied recommended rules from the policy and also removes the recommendation tab.

Under **All Rules**, there is a Recommended Rules section which displays the recommended rules.

Note Final action for an Intrusion rule is applied based on the rule action priority order and following is the rule action priority order:

Rule Override > Generated Recommendations > Group Override > Base Policy Default Action

For enabled recommendations, management center considers the current state: group overrides, base policy, and recommendation configurations and priority order of actions is:

pass > block > reject > drop > rewrite > alert

What to do next

Deploy configuration changes; see Deploy Configuration Changes.

Generating Firepower Recommendations to Snort 3: Upgrade Scenarios

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

Generate the Firepower recommendations for the intrusion policy. Follow the steps that are listed for the upgrade scenarios recommended rule settings to Snort 3.

Before you begin

Firepower recommendations have the following requirements:

- Threat Defense License—Threat
- Classic License—Protection
- User Roles—Admin or Intrusion Admin
- Ensure that hosts are present in the system to generate recommendations.
- Protected networks configured for recommendations should map to the hosts present in system

Step 1 **Considering an Upgrade Scenario 1:** Upgrade from 6.5+ to 7.1 - Considering no changes are in 7.0

Step 2 Snort 3 Recommendations are generated in 7.1 using existing Snort 2 recommendations configurations.

Step 3 Displays the Snort 2 to Snort 3 Sync summary details:

- Recommendations generated for Snort 3 version of the following Intrusion policy.
- Same base policy and inspection mode are updated to Snort 3 policy.

You can also download the summary details.

Step 4 **Considering an Upgrade Scenario 2:** Upgrade from 6.5+ to 7.0 to 7.1 - First upgrading to 7.0:

Step 5 Choose **Policies** > **Intrusion** and identify the intrusion policy that is out-of-sync.

Step 6 Click the **Sync** icon ( ).

Note If the Snort 2 and the Snort 3 versions of the intrusion policy are synchronized, then the **Sync** icon is in green ( ).

During upgrade from pre-7.0 to 7.0, any existing Snort 2 recommendations will be synched to Snort 3. However, if you have generated Snort 2 recommendations after upgrade to 7.0, **then you can sync** all these recommendations to Snort 3 version.

Step 7 Read through the summary and download a copy of the summary if required.

Step 8 Considering there are no recommendations in 7.0 and Snort 2 recommendations are migrated as the rule overrides in 7.0.

Step 9 Displays the Migrated Overrides details:

- This policy had Snort 2 recommendations that are migrated as overrides, in previous upgrade. Select **Snort 3** version to generate recommendations for Snort 3.

  Prior to generating Snort 3 recommendations, click **View** to view the overrides or click **Remove** to remove the overrides or click **Ignore and Generate** to ignore the overrides and generate the recommendations.

- Same base policy and inspection mode are updated to Snort 3 policy.

You can also download the summary details.

Step 10 **Upgrade from 7.0 to 7.1**:

Step 11 For a 7.0 management center with Snort 2 Rule Recommendations, after upgrade to 7.1, you will be notified with a sync summary message.

What to do next

Deploy configuration changes; see Deploy Configuration Changes.