Use Case - Generate Snort 3 Recommendations In Secure Firewall Management Center

Snort 3 Rule Recommendations

Rule recommendations automatically tune your intrusion policy with rules that are specific to the host environment. You can enable additional rules or tune the current rule set by disabling rules for the vulnerabilities that are not present in your network. For more information, see Overview of Secure Firewall Recommended Rules.

How does it 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. They are:

- 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.

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 large corporate network uses Snort 3 as its primary intrusion detection and prevention system. In a rapidly evolving threat landscape, robust network security measures must be adopted. The security team wants to enhance their incident response capabilities. One of the ways to do that is to generate recommendations or rule sets based on the vulnerabilites detected in the host network. This helps to optimize their intrusion policies, thereby safeguarding the network more effectively.

Best Practices

- You must have 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 an accurate data about applications, services, and vulnerabilities present on your network.
- Devices should have visibility to East-West as well as North-South traffic flows to build an accurate host profile.
- You can create a scheduled task to update recommendations automatically.

Prerequisites

- 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.

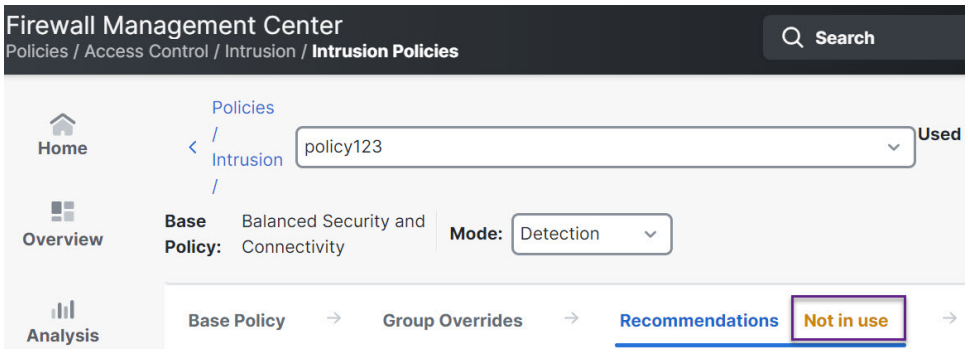
Generate Snort 3 Recommendations

Procedure

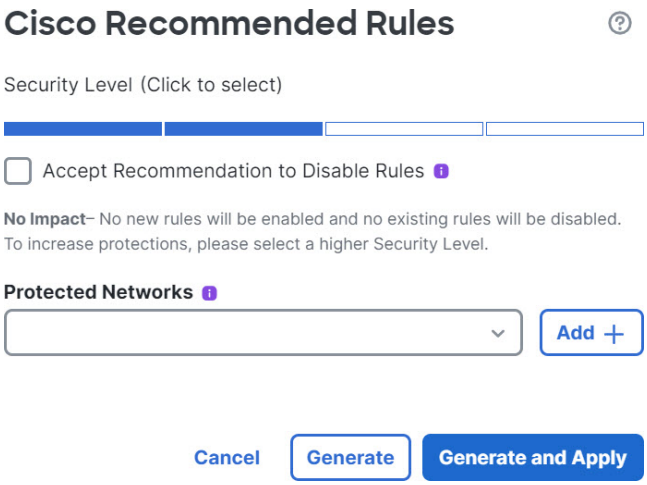
Step 1 Choose **Policies** > **Access Control heading** > **Intrusion**.

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**.

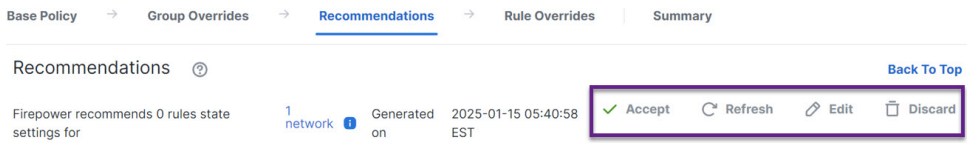
Step 7 Generate and apply recommendations:

- **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)**.

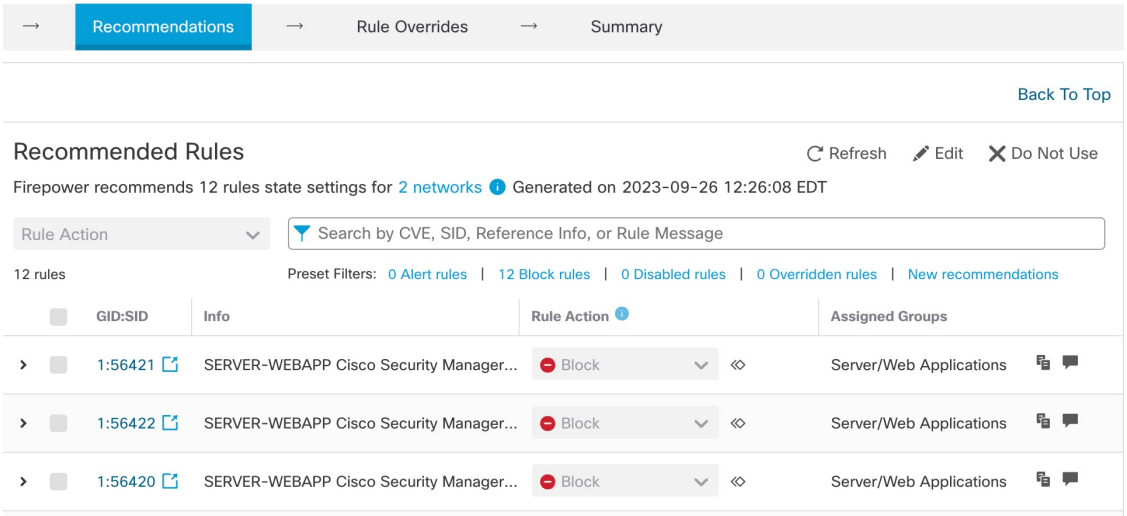
Recommendations are generated successfully. A new recommendation tab appears with all the recommended rules and their corresponding recommended actions. Rule action preset filters are also available for this tab, in addition to new recommendations.

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.



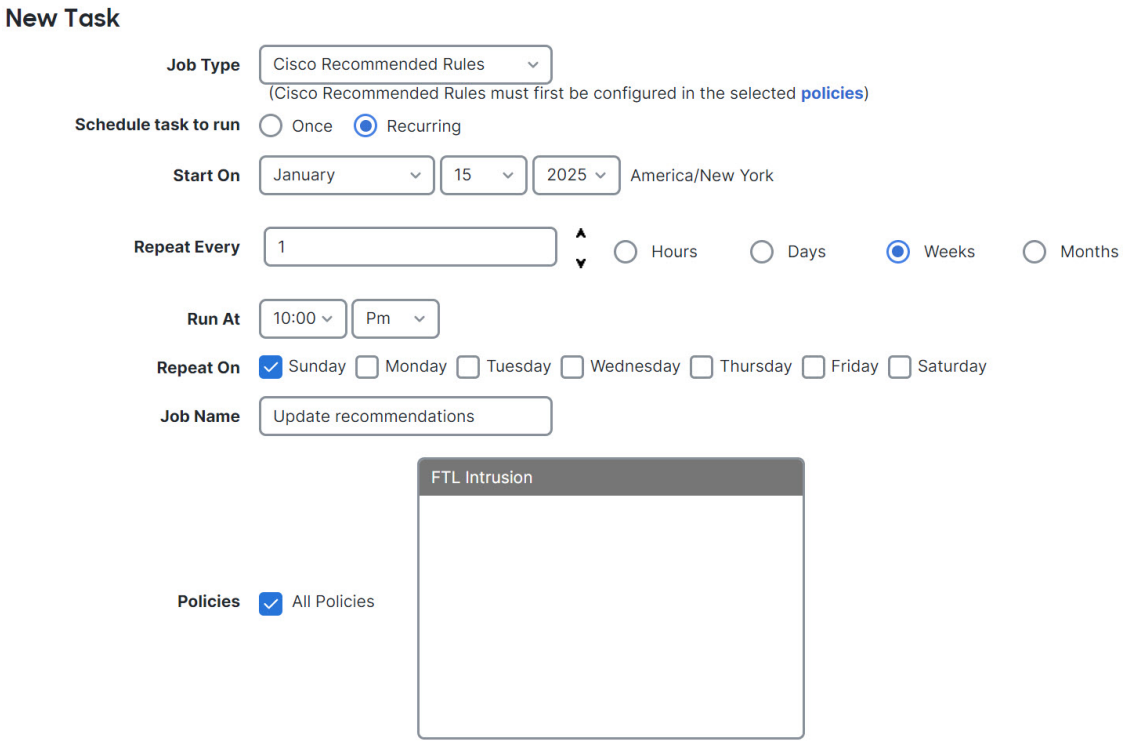
Step 9 To effectively use recommendations, they must be updated periodically. Follow these steps:

a. Choose **System** (⚙) > **Tools** > **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. See Deploy Configuration Changes.

Deploy Configuration Changes

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

Note This topic covers the basic steps involved in deploying configuration changes. We *strongly* recommend that you refer the *Deploy Configuration Changes* topic in the latest version of the *Cisco Secure Firewall Management Center Configuration Guide* to understand the prerequisites and 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.

Procedure

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

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

- The **Modified By** column lists the users who have modified the policies or objects. Expand the device listing to view the users who have modified the policies for each policy listing.

  Note
  Usernames are not provided for deleted policies and objects.

- The **Inspect Interruption** column indicates if traffic inspection interruption might occur in the device during deployment.

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

- The **Last Modified Time** column specifies the last time you made 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.

  When you check a check box adjacent to a device, all the changes made to the device and 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 Firewall 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 Firewall 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 Firewall 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, 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 the Deploy Configuration Changes topic in the latest version of the *Cisco Secure Firewall Management Center Configuration Guide*.