



# Mitigate Threats Using MITRE Framework in Snort 3 Intrusion Policies

---

- [About MITRE Framework, on page 1](#)
- [Benefits of MITRE Framework, on page 2](#)
- [Prerequisites, on page 2](#)
- [Sample Business Scenario, on page 2](#)
- [View and Edit Your Snort 3 Intrusion Policy, on page 2](#)
- [View Intrusion Events, on page 7](#)
- [Additional References, on page 9](#)

## About MITRE Framework

The MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) Framework is an extensive knowledge base and methodology that provides insights into the tactics, techniques, and procedures (TTPs) distributed by threat actors aiming to harm systems. ATT&CK is compiled into matrices that each represent operating systems or a particular platform. Each stage of an attack, which is known as "tactics", is mapped to the specific methods used to achieve those stages, which are known as "techniques."



---

**Note** See <https://attack.mitre.org> for information about MITRE.

---

Each technique in the ATT&CK framework is accompanied with information about the technique, associated procedures, probable defenses and detections, and real-world examples. The MITRE ATT&CK framework also incorporates groups to refer to threat groups, activity groups, or threat actors based on the set of tactics and techniques they employ. Usage of groups in the framework helps categorize and document behaviors.

The MITRE framework enables you to navigate through your intrusion rules. MITRE is just another category of rule groups and is part of the Talos rule groups. In your Snort 3 intrusion policy, you can navigate through several levels of rule groups that provide more flexibility and logical grouping of rules.

## Benefits of MITRE Framework

- MITRE Tactics, Techniques, and Procedures (TTPs) are added to intrusion events that enables administrators to act on traffic based on the MITRE ATT&CK (Adversary Tactics Techniques and Common Knowledge) framework. This enables administrators to view and handle traffic with more granularity, and they can group rules by vulnerability type, target system, or threat category.
- You can organize intrusion rules according to the MITRE ATT&CK framework. This allows you to customize policies according to specific attacker tactics and techniques.

## Prerequisites

- You must be running management center 7.3.0 or later with managed devices 7.3.0 or later using Snort 3.
- You must have at least one intrusion policy. See [Create a Custom Snort 3 Intrusion Policy](#).

## Sample Business Scenario

A large corporate network uses Snort 3 as its primary intrusion detection and prevention system. In a rapidly evolving threat landscape, adoption of robust network security measures is necessary and important. Network administrators need to know if the configured policies are finding traffic of interest and if they are observing a known attack group.

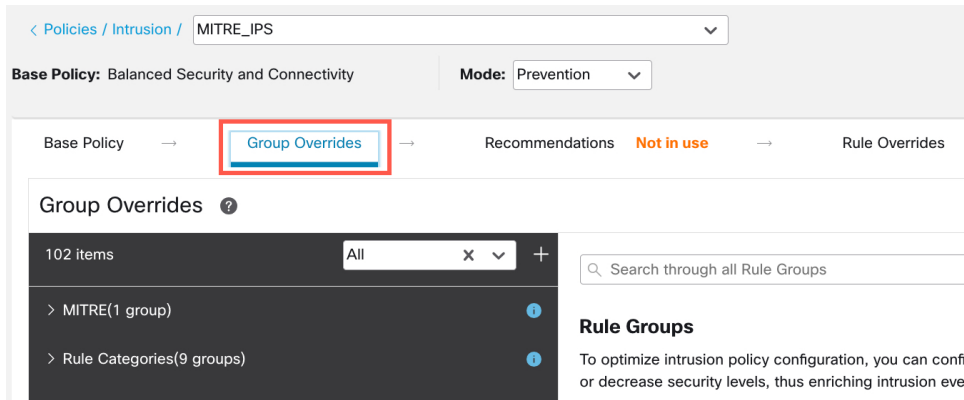
As an example, you may want to know if adversaries are attempting to take advantage of a weakness in your systems or applications to cause unintended or unanticipated behavior. The weakness in the system can be a bug, a glitch, or a design vulnerability. The applications may be websites, databases, standard services, such as SMB or SSH, network device administration and management protocols, or applications, such as web servers and related services.

The insights provided by the MITRE framework enables the administrators a more precise opportunity to specify protection for specific assets and protect themselves from specific threat groups.

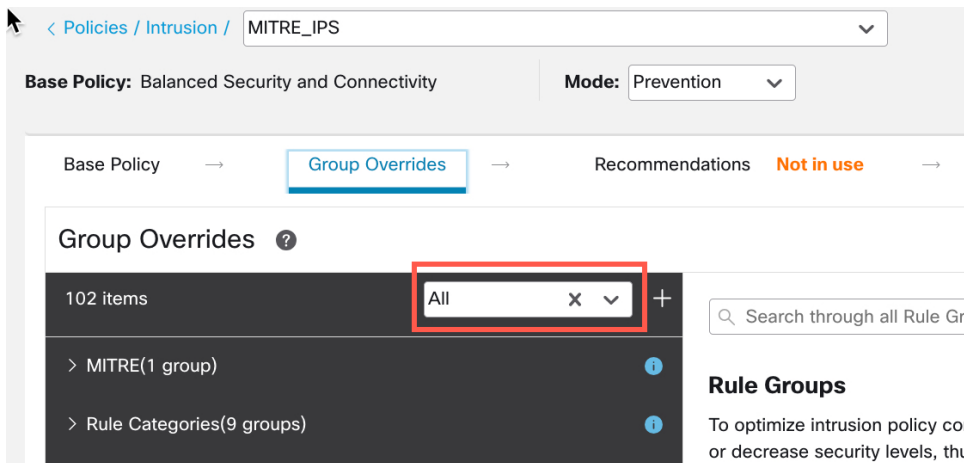
## View and Edit Your Snort 3 Intrusion Policy

- 
- Step 1** Choose **Policies > Intrusion**.
  - Step 2** Ensure that the **Intrusion Policies** tab is chosen.
  - Step 3** Click **Snort 3 Version** next to the intrusion policy that you want to view or edit.
  - Step 4** Close the Snort helper guide that pops up.
  - Step 5** Click the **Group Overrides** layer.

The **Group Overrides** layer lists all the categories of rule groups in a hierarchical structure. You can traverse to the last leaf rule group in each rule group.

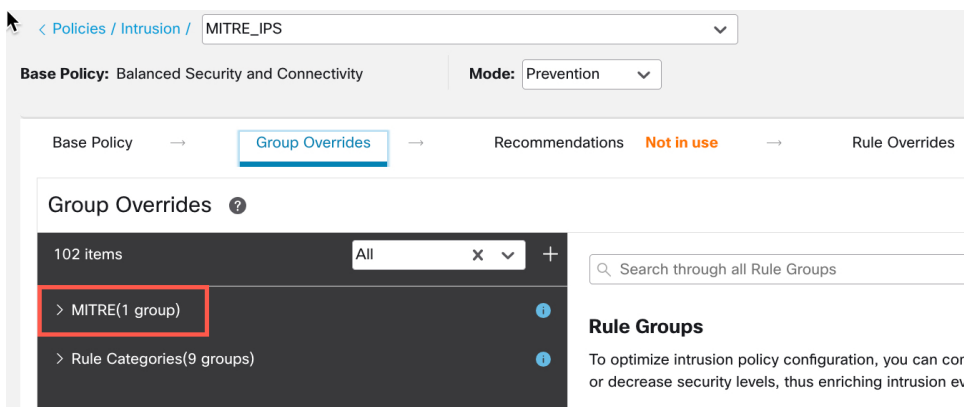


**Step 6** Under **Group Overrides**, ensure that **All** is chosen in the drop-down list, so that all the rule groups for the intrusion policy are visible in the left pane.



**Step 7** Click **MITRE** in the left pane.

**Note** For this example, we have chosen MITRE, but depending on your specific requirements, you can choose the **Rule Categories** rule group or any other rule group and subsequent rule groups under it. All the rule groups use the MITRE framework.



**Step 8** Under **MITRE**, click **ATT&CK Framework** to expand it.

The screenshot shows the 'Group Overrides' section for the 'MITRE\_IPS' policy. The 'Base Policy' is 'Balanced Security and Connectivity' and the 'Mode' is 'Prevention'. The 'Group Overrides' section is active, showing a list of 102 items. The 'MITRE(1 group)' is expanded, and the 'ATT&CK Framework(1 group)' is highlighted with a red box. The 'Rule Categories(9 groups)' is also visible.

**Step 9** Under **ATT&CK Framework**, click **Enterprise** to expand it.

The screenshot shows the 'Group Overrides' section for the 'MITRE\_IPS' policy. The 'Base Policy' is 'Balanced Security and Connectivity' and the 'Mode' is 'Prevention'. The 'Group Overrides' section is active, showing a list of 102 items. The 'MITRE(1 group)' is expanded, and the 'ATT&CK Framework(1 group)' is expanded. The 'Enterprise(13 groups)' is highlighted with a red box. The 'Rule Categories(9 groups)' is also visible.

**Step 10** Click **Edit** (✎) next to the Security Level of the rule group to make bulk changes to the security level for all the associated rule groups under the **Enterprise** rule group category.

The screenshot shows the 'Group Overrides' section for the 'MITRE\_IPS' policy. The 'Base Policy' is 'Balanced Security and Connectivity' and the 'Mode' is 'Prevention'. The 'Group Overrides' section is active, showing a list of 102 items. The 'MITRE(1 group)' is expanded, and the 'ATT&CK Framework(1 group)' is expanded. The 'Enterprise(13 groups)' is expanded, and the 'Enterprise' rule group is selected. The 'Security Level' is highlighted with a red box.

**Step 11** As an example, choose security level 3 in the **Edit Security Level** window and click **Save**.

## Edit Security Level ?

**Bulk Group Security Level**

Impacts 34 groups. This action will change the security level of all leaf groups within this group category.

Higher security with more detections for administrators who are willing to tolerate some network latency and low level of false positives, in an effort to catch more attacks

**Step 12** Under **Enterprise**, click **Initial Access** to expand it.

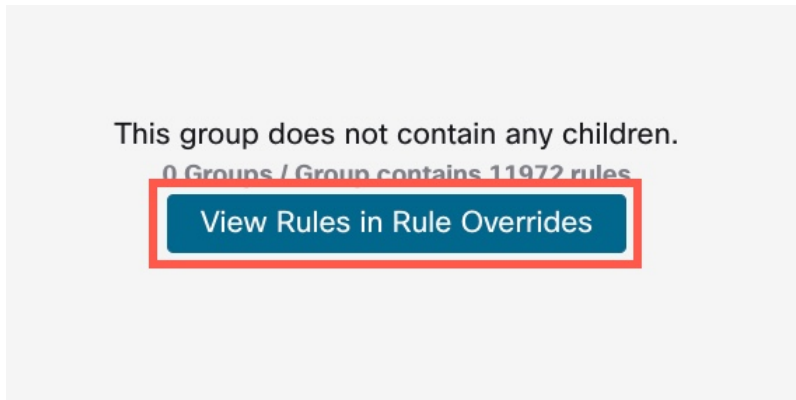
**Step 13** Under **Initial Access**, click **Exploit Public-Facing Application**, which is the last leaf group.

**Figure 1: MITRE Tactics and Techniques**

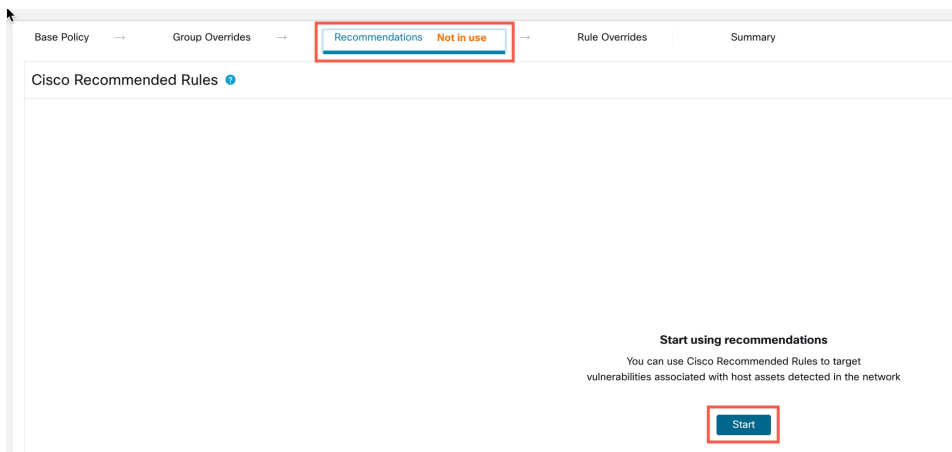
The screenshot displays the 'Group Overrides' section for the 'MITRE / ATT&CK Framework / Enterprise / Initial Access' group. The left sidebar shows a tree view of groups, with 'Initial Access (5 groups)' expanded and 'Exploit Public-Facing Application' selected. The main panel shows a table of rules with their security levels and override options.

Group Name	Security Level	Override
<b>Drive-by Compromise</b> (T1189) Adversaries may gain access to a system through a user visiting a website over the normal course ...	Security Level	Override
<b>Exploit Public-Facing Application</b> (T1190) Adversaries may attempt to take advantage of a weakness in an Internet-facing computer or progr...	Security Level	Override
<b>External Remote Services</b> (T1133) Adversaries may leverage external-facing remote services to initially access and/or persist within a...	Security Level	Override
<b>Phishing</b> (T1566) Adversaries may send phishing messages to gain access to victim systems. All forms of phishing a...	Security Level	Override
<b>Valid Accounts</b> (T1078) Adversaries may obtain and abuse credentials of existing accounts as a means of gaining Initial Ac...	Security Level	Override

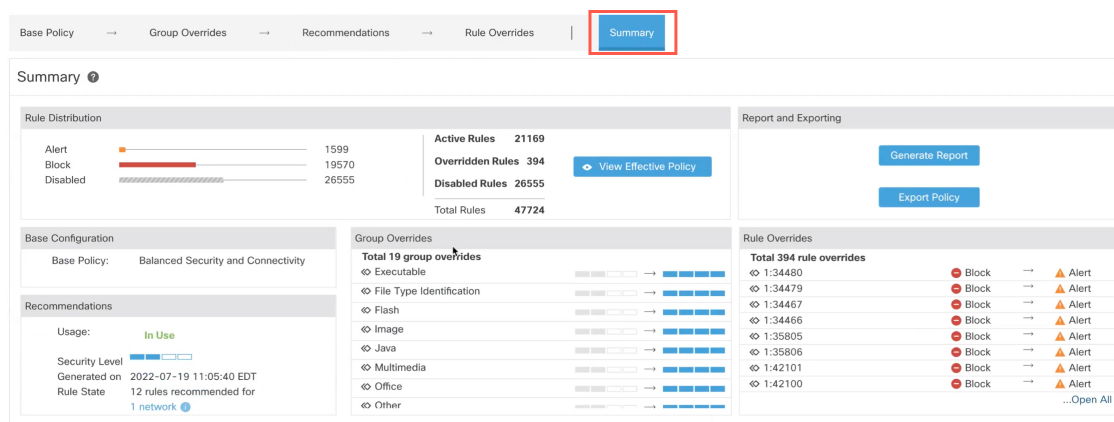
**Step 14** Click the **View Rules in Rule Overrides** button to view the different rules, rule details, rule actions, and so on, for the different rules. You can change the rule actions for one or multiple rules in the **Rule Overrides** layer.

**Step 15**

Click the **Recommendations** layer and then click **Start** to start using Cisco recommended rules. You can use the intrusion rule recommendations to target vulnerabilities that are associated with host assets detected in the network. For more information, see [Generate New Secure Firewall Recommendations in Snort 3](#).

**Step 16**

Click the **Summary** layer for a holistic view of the current changes to the policy. Based on the rule overrides, security level changes, and generation of Cisco recommended rules, you can view the rule distribution of the policy, group overrides, rule overrides, rule recommendations, and so on, to verify your changes.



### What to do next

Deploy your intrusion policy to detect and log events that are triggered by the Snort rules. See [Deploy Configuration Changes](#).

## View Intrusion Events

You can view the MITRE ATT&CK techniques and rule groups in the intrusion events in the Classic Event Viewer and Unified Event Viewer. Talos provides mappings from Snort rules (GID:SID) to MITRE ATT&CK techniques and rule groups. These mappings are installed as part of the Lightweight Security Package (LSP).

**Step 1** Click **Analysis > Intrusions > Events**.

**Step 2** Click the **Table View of Events** tab.

Events By Priority and Classification (switch workflow) 2022-07-19 09:05:58 - 2022-07-19 09:05:58

No Search Constraints [\(Edit Search\)](#)

Drilldown of Event, Priority, and Classification Table View of Events Packets

Jump to...

<input type="checkbox"/>	Time	Priority	Impact	Inline Result	Reason	Source IP	Source Country	Destination IP
▼	2022-07-19 11:17:10	high	2	Would block	Interface in Passive or Tap mode	192.168.0.227		146.112.255.69
▼	2022-07-19 11:17:06	medium	2	Would block	Interface in Passive or Tap mode	192.168.3.254		192.168.4.106
▼	2022-07-19 11:17:06	medium	3	Would block	Interface in Passive or Tap mode	54.68.177.240	USA	192.168.7.214
▼	2022-07-19 11:17:05	medium	2	Would block	Interface in Passive or Tap mode	192.168.3.254		192.168.7.241

**Step 3** In the **MITRE ATT&CK** column header, you can see the techniques for an intrusion event.

Access Control Policy	Access Control Rule	Network Analysis Policy	MITRE ATT&CK	Rule Group
AC_with_security_intelligence_file_file	TestRuleFile	Simple NAP Policy	1 Technique	1 Group
AC_with_security_intelligence_file_file	TestRuleFile	Simple NAP Policy		1 Group
AC_with_security_intelligence_file_file	TestRuleFile	Simple NAP Policy		1 Group
AC_with_security_intelligence_file_file	TestRuleFile	Simple NAP Policy		1 Group

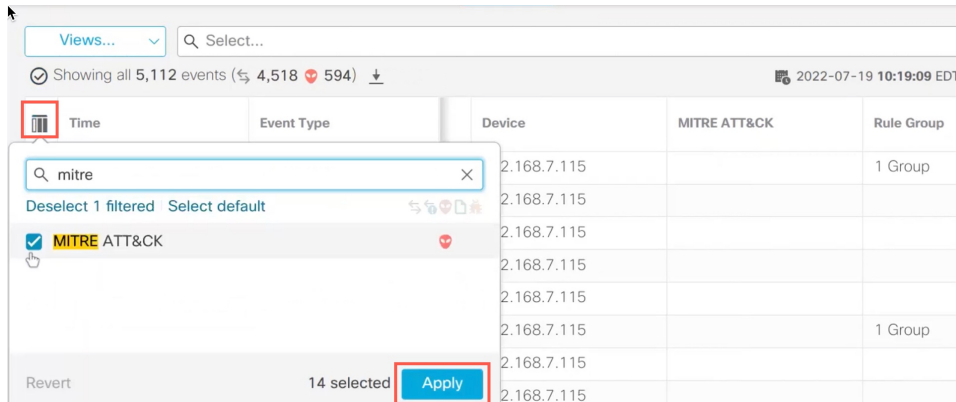
**Step 4** Click **1 Technique** to view the MITRE ATT&CK Techniques, as shown in the following figure. In this example, **Exploit Public-Facing Application** is the technique.

MITRE ATT&CK Techniques	Access Control Rule	Network Analysis Policy	MITRE ATT&CK
<ul style="list-style-type: none"> <li>• Enterprise               <ul style="list-style-type: none"> <li>• Initial Access                   <ul style="list-style-type: none"> <li>• Exploit Public-Facing Application</li> </ul> </li> </ul> </li> </ul>	TestRuleFile	Simple NAP Policy	1 Technique
	TestRuleFile	Simple NAP Policy	
	TestRuleFile	Simple NAP Policy	
	TestRuleFile	Simple NAP Policy	
	TestRuleFile	Simple NAP Policy	

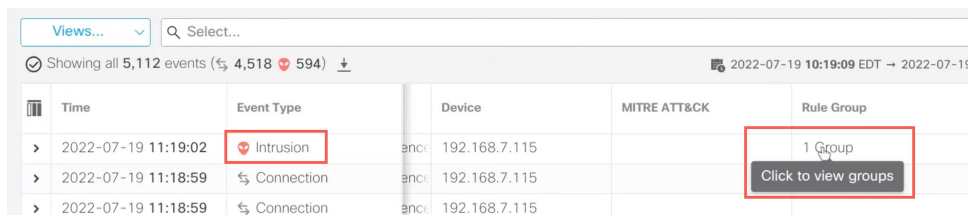
**Step 5** Click **Close**.

**Step 6** Click **Analysis > Unified Events**.

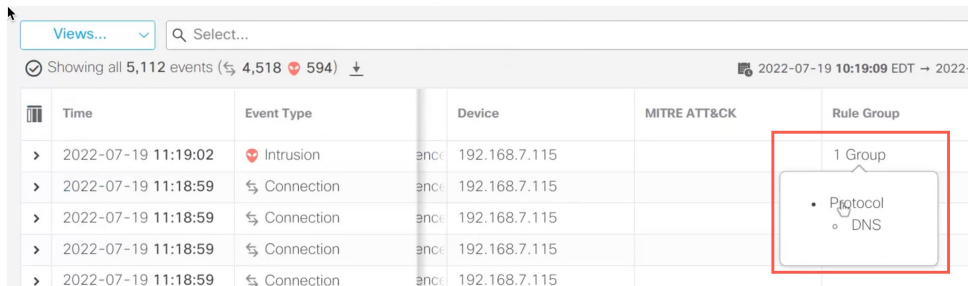
**Step 7** If not already enabled, click the column selector icon to enable the **MITRE ATT&CK** and **Rule Group** columns.



**Step 8** As shown in the example here, the intrusion event was triggered by an event that is mapped to one rule group. Click **1 Group** under the **Rule Group** column.

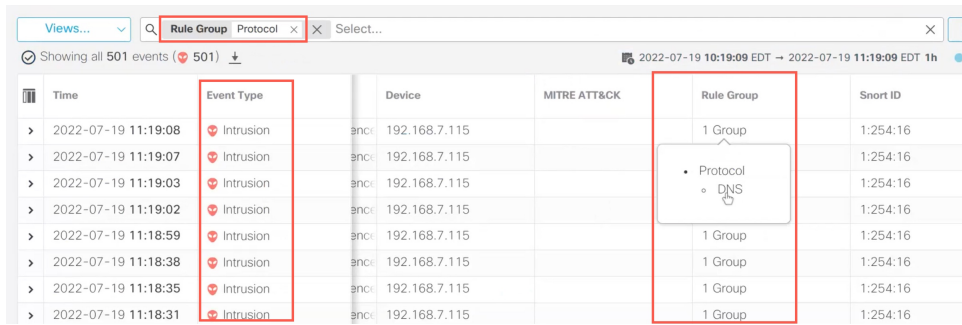


**Step 9** As an example, you can view Protocol, which is the parent rule group, and DNS rule group under it.



**Step 10** You can click **Protocol** to search for all the intrusion events that have at least one rule group, that is Protocol > DNS. The search results are displayed, as shown in the example below.





The screenshot displays a Snort 3 event log interface. At the top, there is a search bar with the text 'Rule Group: Protocol' and a dropdown menu. Below the search bar, it indicates 'Showing all 501 events (501)'. The main table has columns for Time, Event Type, Device, MITRE ATT&CK, Rule Group, and Snort ID. The 'Event Type' column is highlighted in red. A dropdown menu is open for the 'Rule Group' column, showing a tree structure with 'Protocol' and 'DNS' as sub-items. The table contains several rows of intrusion events, all with 'Intrusion' as the event type and '192.168.7.115' as the device.

Time	Event Type	Device	MITRE ATT&CK	Rule Group	Snort ID
> 2022-07-19 11:19:08	Intrusion	enc01 192.168.7.115		1 Group	1:254:16
> 2022-07-19 11:19:07	Intrusion	enc01 192.168.7.115		1 Group	1:254:16
> 2022-07-19 11:19:03	Intrusion	enc01 192.168.7.115		1 Group	1:254:16
> 2022-07-19 11:19:02	Intrusion	enc01 192.168.7.115		1 Group	1:254:16
> 2022-07-19 11:18:59	Intrusion	enc01 192.168.7.115		1 Group	1:254:16
> 2022-07-19 11:18:38	Intrusion	enc01 192.168.7.115		1 Group	1:254:16
> 2022-07-19 11:18:35	Intrusion	enc01 192.168.7.115		1 Group	1:254:16
> 2022-07-19 11:18:31	Intrusion	enc01 192.168.7.115		1 Group	1:254:16

## Additional References

- [Intrusion Policy in Snort 3](#)
- [Edit Snort 3 Intrusion Policies](#)
- [MITRE Information in Malware Events](#)

