# Custom Snort 3 Intrusion Policies for Access Control

**Cisco Secure Firewall Management Center**
Updated February 4, 2026

© 2026 Cisco Systems, Inc. All rights reserved.

# Full Cisco Trademarks with Software License

Full Cisco Trademarks with Software License

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

# Topics included


**1 Intrusion Prevention Overview ..... 7**

Intrusion prevention ..... 8
Snort inspection engine ..... 9
Snort 3 ..... 9
Snort 3 multi-process support ..... 11
Multi-layer inspection ..... 12
Header inspection ..... 13
Layer 7 features ..... 13
Example scenarios ..... 13
Encapsulation layer limits and inspection behavior ..... 14
Supported protocols and inspection capabilities of LINA and Snort 3 ..... 14
Guidelines and limitations for network analysis and intrusion policies ..... 15
Prerequisites for network analysis and intrusion policies ..... 16
How policies examine traffic for intrusions ..... 16
Decoding, normalizing, and preprocessing: Network analysis policies ..... 17
Access control rules: Intrusion policy selection ..... 18
Intrusion inspection: Intrusion policies, rules, and variable sets ..... 19
Intrusion event generation ..... 21
System-provided and custom network analysis and intrusion policies ..... 22
System-provided network analysis and intrusion policies ..... 22
Benefits of custom network analysis and intrusion policies ..... 24
Limitations of custom policies ..... 26

**2 Migrate from Snort 2 to Snort 3 ..... 29**

Snort 3 inspection engine ..... 30
Snort 2 versus Snort 3 ..... 30
Migrating from Snort 2 to Snort 3 ..... 30
Prerequisites for migrating from Snort 2 to Snort 3 ..... 31
Enable Snort 3 on an individual device ..... 31
Enable Snort 3 on multiple devices ..... 32
Convert Snort 2 Custom IPS Rules to Snort 3 ..... 33
View Snort 2 and Snort 3 base policy mapping ..... 35
Synchronize Snort 2 rules with Snort 3 ..... 36
Deploy configuration changes ..... 37
Examples for migration ..... 39
Migrate from Snort 2 to Snort 3 ..... 39
Benefits of migrating to snort 3 ..... 40
Sample business scenario ..... 40
Best practices for migrating from Snort 2 to Snort 3 ..... 40

Prerequisites for migration....40
End-to-end migration workflow....41
Enable Snort 3 on Threat Defense device....41
Convert Snort 2 rules of a single intrusion policy to Snort 3....42

**3 Intrusion Policies....49**

Intrusion policies....50
Create a custom snort 3 intrusion policy....51
Edit Snort 3 Intrusion Policies....52
Rule group reporting....55
Rule action logging....56
Change the base policy of an intrusion policy....57
View Snort 2 and Snort 3 base policy mapping....57
Synchronize Snort 2 rules with Snort 3....58
Manage intrusion policies....59
Access control rule configuration to perform intrusion prevention....60
Access control rule configuration and intrusion policies....61
Configure an access control rule to perform intrusion prevention....61
Tune Intrusion Policies using Rules....62
Tuning intrusion rules....62
Intrusion rule types....62
Custom rules in Snort 3....63
View Snort 3 intrusion rules in an intrusion policy....66
Intrusion rule actions....67
Intrusion event notification filters in an intrusion policy....68
Add intrusion rule comments....74
Prepare custom rules for snort 3 conversion....74
Add custom rules to rule groups....76
Add rule groups with custom rules to an intrusion policy....78
Manage custom rules in Snort 3....78
Delete custom rules....79
Delete rule groups....79
Recommended rules....80
Snort 3 rule changes in LSP updates....80
Secure Firewall recommended rules....81
Generate new Secure Firewall recommendations in Snort 3....82
Mitigate threats using MITRE framework in Snort 3 intrusion policies....85
MITRE framework....85
MITRE framework benefits....85
Sample business scenario for MITRE network....86
Prerequisites for MITRE framework....86
View and edit your Snort 3 intrusion policy....86
View intrusion events....91
Additional references....93

**4 Intrusion Prevention Performance Tuning.....95**
Intrusion prevention performance tuning.....96
License requirements for intrusion prevention performance tuning.....96
Requirements and prerequisites for intrusion prevention performance tuning.....97
Limiting pattern matching for intrusions.....97
Regular expression limits overrides for intrusion rules.....98
Override regular expression limits for intrusion rules.....99
Per packet intrusion event generation limits.....99
Limiting intrusion events generated per packet.....100
Packet and intrusion rule latency threshold configuration.....101
Latency-based performance settings.....101
Packet latency thresholding.....102
Rule latency thresholding.....104
Intrusion performance statistic logging configuration.....107
Configure intrusion performance statistic logging.....108

**5 Network Analysis Policies.....111**
Network analysis policies.....112
Manage network analysis policies.....112
Snort 3 definitions and terminologies for network analysis policies.....113
Custom network analysis policy creation for Snort 3.....115
Common Industrial Protocol safety.....119
Detect and block safety segments in CIP packets.....120
Network analysis policy mapping.....120
View network analysis policy mapping.....121
Create a network analysis policy.....121
Modify the network analysis policy.....121
Search for an inspector on the Network Analysis Policy window.....122
Copy the inspector configuration .....123
Customize the network analysis policy.....123
Make inline edit for an inspector to override configuration.....127
Revert unsaved changes during inline edits.....128
View the list of inspectors with overrides.....129
Revert overridden configuration to default configuration.....129
Validate Snort 3 policies.....130
Examples of custom network analysis policy configuration.....133
Network analysis policy settings and cached changes.....144
Generate Snort 3 recommendations.....144
Snort 3 rule recommendations.....144
Benefits.....145
Sample business scenario.....145
Best practices.....145
Prerequisites for generating recommendations.....146

Generate Snort 3 recommendations....146

6 Advanced Access Control settings for Network Analysis and Intrusion Policies...149

Advanced access control settings for network analysis and intrusion policies....150
Advanced access control settings for network analysis and intrusion policies....150
Requirements and prerequisites for advanced access control settings for network analysis and intrusion policies....150
Inspection of packets that pass before traffic is identified....151
Best practices for handling packets that pass before traffic identification....151
Specify a policy to handle packets that pass before traffic identification....152
Advanced settings for network analysis policies....153
Set the default network analysis policy....153
Network analysis rules....154

# 1 Intrusion Prevention Overview

**Topics:**


- Intrusion prevention
- Snort inspection engine
- Snort 3
- Multi-layer inspection
- Guidelines and limitations for network analysis and intrusion policies
- Prerequisites for network analysis and intrusion policies
- How policies examine traffic for intrusions
- System-provided and custom network analysis and intrusion policies


Provides an overview of the Snort inspection engine, and the network analysis and intrusion policies. It provides an insight into system-provided and custom network analysis and intrusion policies, their requirements and prerequisites for these policies.

The Snort inspection engine is an integral part of the Firewall Threat Defense. In most cases, the system-provided policies are all you need. For advanced users with specific needs, you can create custom rules.

> **Note**
>
> To configure custom Snort 2 rules, see Custom Snort 2 Intrusion Policies for Access Control.

# Intrusion prevention

Describes the intrusion detection and prevention feature that uses network analysis and intrusion policies to monitor, analyze, and protect against network threats.

Network analysis and intrusion policies work together as part of the intrusion detection and prevention feature.

- The term 'intrusion detection' generally refers to the process of passively monitoring and analyzing network traffic for potential intrusions and storing attack data for security analysis. This is sometimes referred to as "Intrusion Detection System (IDS)."
- The term 'intrusion prevention' includes the concept of intrusion detection, but adds the ability to block or alter malicious traffic as it travels across your network. This is sometimes referred to as "Intrusion Prevention System (IPS)."
- uses network analysis and intrusion policies working together to provide comprehensive packet inspection and threat protection.

### Intrusion prevention components and operation

In an intrusion prevention deployment, when the system examines packets:

- A **network analysis policy** governs how traffic is *decoded* and *preprocessed* so it can be further evaluated, especially for anomalous traffic that might signal an intrusion attempt.
- An **intrusion policy** uses *intrusion and preprocessor rules* (sometimes referred to collectively as *intrusion rules*) to examine the decoded packets for attacks based on patterns. Intrusion policies are paired with *variable sets*, which allow you to use named values to accurately reflect your network environment.

Both network analysis and intrusion policies are invoked by a parent access control policy, but at different times. As the system analyzes traffic, the network analysis (decoding and preprocessing) phase occurs before and separately from the intrusion prevention (additional preprocessing and intrusion rules) phase. Together, network analysis and intrusion policies provide broad and deep packet inspection. They can help you detect, alert on, and protect against network traffic that could threaten the availability, integrity, and confidentiality of hosts and their data.

The system is delivered with several similarly named network analysis and intrusion policies (for example, Balanced Security and Connectivity) that complement and work with each other. By using system-provided policies, you can take advantage of the experience of the Cisco Talos Intelligence Group (Talos). For these policies, Talos sets intrusion and inspector rule states, as well as provides the initial configurations for inspectors and other advanced settings.

You can also create custom network analysis and intrusion policies. You can tune settings in custom policies to inspect traffic in the way that matters most to you so that you can improve both the performance of your managed devices and your ability to respond effectively to the events they generate.

You create, edit, save, and manage network analysis and intrusion policies using similar policy editors in the web interface. When you are editing either type of policy, a navigation panel appears on the left side of the web interface; the right side displays various configuration pages.

Refer to the videos for additional support and information:

- Snort 3 Condensed Overview
- Snort 3 Extended Overview

**Attention**

Detection mode deprecation: From management center Version 7.4.0, for a network analysis policy (NAP), the Detection inspection mode is deprecated and will be removed in an upcoming release.

The Detection mode was intended to be used as a test mode so that you can enable inspections and see how they behave in your network before setting it to drop traffic, that is, to show traffic that would be dropped.

This behavior is improved where all inspector drops are controlled by the rule state, and you can set each one to generate events. This is done to test them before configuring the rule state to drop traffic. As we now have granular control over traffic drops in Snort 3, the Detection mode only adds more complexity to the product and is not needed, so the detection mode is deprecated.

If you change a NAP in Detection mode to Prevention, the NAP that processes the traffic of intrusion events and have the result "will be dropped" will now be "dropped" and the corresponding traffic will drop the traffic from these events. This is applicable for rules whose GIDs are not 1 or 3. GIDs 1 and 3 are text/compiled rules (typically provided by Talos or from your custom/imported rules) and all other GIDs are inspections for anomalies. These are more uncommon rules to trigger in a network. Changing to Prevention mode is unlikely to have any impact on the traffic. You need to just disable the intrusion rule that is applicable for the dropped traffic and set it to just generate or disable.

We recommend you choose Prevention as the inspection mode, but if you choose Prevention, you cannot revert to Detection mode.

## Snort inspection engine

Describes a traffic analysis component that provides real-time deep packet inspection capabilities.

A Snort inspection engine is an integral traffic analysis component that

- analyzes traffic in real time to provide deep packet inspection,
- operates as part of the Secure Firewall Threat Defense (formerly Firepower Threat Defense) device, and
- enables network analysis and intrusion policies to detect and protect against intrusions.

## Snort 3

Describes the latest version of the Snort inspection engine. This version includes improvements over prior versions.

Snort 3 is a network inspection engine that

- provides vast improvements compared to the earlier version of Snort,
- offers more efficient operation with better performance and scalability, and
- is architecturally redesigned to inspect more traffic with equivalent resources when compared to Snort 2.

### Snort 3 changes and improvements

The older version of Snort is Snort 2, which is no longer supported. Snort 3 provides simplified and flexible insertion of traffic parsers. Snort 3 also provides new rule syntax that makes rule writing easier and shared object rule equivalents visible.

The other significant changes with Snort 3 are:

- Unlike Snort 2, which uses multiple Snort instances, Snort 3 associates multiple threads with a single Snort instance. This uses less memory, improves Snort reload times, and supports more intrusion rules and a larger network map. The number of Snort threads varies by platform and is the same as the number of Snort 2 instances for each platform. Usage is virtually transparent.
- Snort version per Firewall Threat Defense—The Snort inspection engine is Firewall Threat Defense specific and not Secure Firewall Management Center (formerly Firepower Management Center) specific. Firewall Management Center can manage several Firewall Threat Defenses, each with either versions of Snort (Snort 2 and Snort 3). Although the Firewall Management Center's intrusion policies are unique, the system applies Snort 2 or Snort 3 version of an intrusion policy for intrusion protection depending on the device's selected inspection engine.
- Decoder rules—Packet decoder rules fire only in the default intrusion policy. The system ignores decoder rules that you enable in other policies.
- Shared object rules—Snort 3 supports some, but not all, shared object (SO) intrusion rules (rules with a generator ID (GID) of 3). Enabled shared object rules that are not supported do not trigger.
- Multi-layer inspection for Security Intelligence—Snort 3 detects the innermost IP address regardless of the layer.
- Platform support—Snort 3 requires Firewall Threat Defense version 7.0 or later. It is not supported with ASA FirePOWER or NGIPSv.
- Managed Devices—An Firewall Management Center with version 7.0 can simultaneously support versions 6.4, 6.5, 6.6, 6.7, and 7.0 Snort 2 Firewall Threat Defenses, and version 7.0 Snort 3 Firewall Threat Defenses.
- Traffic interruption when switching Snort versions—Switching Snort versions interrupts traffic inspection and a few packets might drop during deployment.
- Unified policies—Irrespective of the underlying Snort engine version that is enabled in the managed Firewall Threat Defenses, the access control policies, intrusion policies, and network analysis policies configured in the Firewall Management Center work seamlessly in applying the policies. All intrusion policies in Firewall Management Center version 7.0 and above have two versions available, Snort 2 version and Snort 3 version. The intrusion policy is unified, which means that it has a common name, base policy, and inspection mode, although there are two versions of the policy (Snort 2 version and Snort 3 version). The Snort 2 and the Snort 3 versions of the intrusion policy can be different in terms of the rule settings. However, when the intrusion policy is applied on a device, the system automatically identifies the Snort version enabled on the device and applies the rule settings configured for that version.
- Lightweight Security Package (LSP)—Replaces the Snort Rule Updates (SRU) for Snort 3 next-generation intrusion rule and configuration updates. Downloading updates downloads both the Snort 3 LSP and the Snort 2 SRU.

  LSP updates provide new and updated intrusion rules and inspector rules, modified states for existing rules, and modified default intrusion policy settings for Firewall Management Center and Firewall Threat Defense versions 7.0 or above. When you upgrade an Firewall Management Center from version 6.7 or lower to 7.0, it supports both LSPs and SRUs. LSP updates may also delete system-provided rules, provide new rule categories and default variables, and modify default variable values. For more information on LSP updates, see the *Update Intrusion Rules* topic in the latest version of the *Firepower Management Center Configuration Guide*.
- Mapping of Snort 2 and Snort 3 rules and presets—Snort 2 and Snort 3 rules are mapped and the mapping is system-provided. However, it is not a one-to-one mapping. The system-provided intrusion base policies are pre-configured for both Snort 2 and Snort 3, and they provide the same intrusion prevention although with different rule sets. The system-provided base policies for Snort 2 and Snort 3 are mapped with each other for the same intrusion prevention settings.
- Synchronizing Snort 2 and Snort 3 rule override—When a Firewall Threat Defense is upgraded to 7.0, you can upgrade the inspection engine of the Firewall Threat Defense to the Snort 3 version. Firewall Management Center maps all the overrides in the existing rules of the Snort 2 version of the intrusion policies to the corresponding Snort 3 rules using the mapping provided by Talos. However, if there are additional overrides performed after the upgrade or if you have installed a new Firewall Threat Defense of version 7.0, they have to be manually synchronized.

- Custom intrusion rules–You can create custom intrusion rules in Snort 3. You can also import the custom intrusion rules that exist for Snort 2 to Snort 3.
- Rule groups–The Firewall Management Center groups all Snort 3 rules into rule groups. Rule groups are logical groups of rules that provide an easy management interface to enhance rule accessibility, rule navigation, and better control over the rule group security level.

  From Firewall Management Center 7.3.0, rule navigation for several levels of rule groups is supported that provides more flexibility and logical grouping of rules. The MITRE framework is added that enables you to navigate through rules using the MITRE framework. MITRE is just another category of rule groups and is a part of Talos rule groups.

  **Note**

  See https://attack.mitre.org for information about MITRE.

  A rule can be part of multiple rule groups, such as multiple MITRE ATT&CK rule groups, a rule category rule group, multiple "asset type" rule groups, a malware campaign, and others. The available rule groups are listed in the intrusion policy editor and can be selected to enhance policies.

  With this multi-level hierarchical structure, you can traverse down to the last element, which is the "leaf rule group." These rule groups contain sets of rules that are related to each other, such as a specific type of vulnerability, a similar target system, or a similar threat category. Rule groups have four security levels associated with them. You can change the security level, add or remove rule groups, and you can change the rule action for rules that match traffic seen on the network. This is done to bring a satisfactory balance between security, performance, and false positive resistance.

## Snort 3 multi-process support

Explains how Snort 3 uses multiple processes to improve performance and resilience on Secure Firewall 6160 and 6170 devices.

Snort 3 multi-process support is a feature that:

- associates multiple threads with two Snort instances on Secure Firewall 6160 and 6170 devices running Secure Firewall version 10.0,
- automatically configures each Snort 3 instance with the threads as required during deployment, and
- results in reduced memory load, reduced lock contention, and shorter core generation times for improved resiliency, performance, and scalability.

### Snort 3 multi-process architecture

Individual Snort 3 instances provide several advantages. Any Snort instance failure results in minimal traffic impact and you can also restart a single Snort process, if required.

Snort threads are distributed over NUMA nodes where each node is considered as an independent processor. This ensures that memory boundaries are maintained. For example, Snort instance 0 uses the memory of node 0, and instance 1 uses the memory of node 1.

The CLI outputs of commands such as **show coredump** and **show perfstats** have been enhanced to display information on both the Snort instances. On the Management Center, navigate to **Troubleshooting > Monitor > Devices** to view the **Overview > Critical Processes** and the **Memory** sections for information on both the Snort instances. If there are any rule profiling errors, the Snort instance number is displayed with the error.

### Disable snort 3 multi-process support

Configure the system to disable Snort 3 multi-process support using the CLI command.

This task disables Snort 3 multi-process support.

Disabling multi-process support is intended for debugging purposes only and requires a manual deployment to take effect.

**Procedure**

1. Use the **configure snort multi-process disable** command to disable Snort 3 multi-process support.

   **Example**

```
> configure snort multi-process disable
----------------------------------------------------------------------
Caution: this command is intended for debugging purposes only.
A deployment is required after enabling/disabling multi-process and will cause
 a Snort
restart and temporary traffic interruption.
----------------------------------------------------------------------
Do you still want to continue?
Please enter 'YES' or 'NO': YES
Please perform a manual deployment to disable multi-process.
```

   **Note**

   This command causes the Snort engine to restart and will also lead to traffic interruption during the next deployment when Snort is changing from the multi-process state to a single-process state.

2. Redeploy the configuration to ensure that the Snort 3 multi-process support is disabled.

## Multi-layer inspection

Provides an overview of the multi-layer inspection feature in Snort 3

The multi-layer inspection feature in Snort 3 enables you to inspect traffic across multiple protocol layers within the same session.

Snort 3 can simultaneously inspect the following layers:

- Network layer (L3): IP addresses, fragmentation
- Transport layer (L4): TCP or UDP ports, flags, session tracking
- Application layer (L7): HTTP, DNS, SMTP, TLS, SIP, and others.
- File and payload layer: File extraction, malware signatures, embedded content

Snort 3 supports decoding for a wide range of protocols. It inspects encapsulated protocols and evaluates packet headers to determine policy actions during advanced threat inspection.

## Header inspection

Describes how header inspection and rule evaluation differ in versions before and after 7.6.4.

### On versions earlier than 7.6.4

For encapsulation protocols not supported by Lina, the system initially matches traffic based on the outer IP header. The subsequent evaluation depends on the rule criteria:

- Rules without Layer 7 (L7) criteria: If the matched rule does not include L7 criteria (such as URL, application ID, or user identity), the system applies the rule based on the outer IP header.
- Rules with Layer 7 (L7) criteria: If the rule includes L7 criteria, the system uses the outer-IP header match as a starting point and then performs an additional evaluation using the innermost header.

This behavior can lead to unexpected results, such as a non-L7 rule matching the outer-IP header taking precedence over a rule matching the inner-IP header located lower in the rule set.

### On version 7.6.4 and later

- Snort 3 always inspects the innermost header for protocols not supported by Lina, regardless of the presence of Layer 7 rules.
- Outer header-based rules alone are not sufficient for policy enforcement for protocols such as VXLAN. Snort 3 disregards connection details for action in such cases, using the actual packet content instead.
- For protocols supported by Lina, policy action continues to be based on the innermost header.
- If you currently manage encapsulated traffic for protocols not supported by Lina (such as VXLAN) using only outer-IP rules, be aware that on version 7.6.4 or later, this traffic will be handled by the default access control rule. In such a scenario, if your default policy action is set to Block, this may result in the traffic being dropped. We recommend that you review and update access control policies to match the inner IP header for such protocols, in addition to any existing outer IP header configurations.

## Layer 7 features

Provides an overview of how Layer 7 features match encapsulated traffic.

For encapsulated traffic in Layer 7 features, only the innermost IP header must be matched in rules. Outer header-only rules will not apply.

## Example scenarios

Describes example scenarios and outcomes for various protocol and rule configurations.

The following table lists examples based on different parameters.

| Protocol | Version | Outer IP rule | Inner IP rule | L7 rule needed | Result |
|---|---|---|---|---|---|
| VXLAN (not supported by LINA) | 7.6.2 | Yes | No | No | Traffic allowed if outer header matches |
| VXLAN (not supported by LINA) | 7.6.4 | No | Yes | No | Traffic allowed if inner header matches |
| GRE (supported by LINA) | 7.6.2 and 7.6.4 | No | Yes | No | Traffic allowed if inner header matches |

| Protocol | Version | Outer IP rule | Inner IP rule | L7 rule needed | Result |
|---|---|---|---|---|---|
| VXLAN + L7 feature | 7.6.2 and 7.6.4 | No | Yes | Yes | Inner header rule required |

**Note**

An outer IP rule matches traffic based on the tunnel endpoints. It evaluates:

- Source IP address of the encapsulating device
- Destination IP address of the encapsulating device

An inner IP rule matches traffic based on the original IP packet inside the tunnel. It evaluates:

- The real client IP address
- The real destination server IP address

## Encapsulation layer limits and inspection behavior

Describes the encapsulation layer decoding limits for Lina and Snort inspection engines.

When managing encapsulated traffic, it is important to understand the processing limits of the system's two primary inspection engines, Lina and Snort.

- LINA: Supports decoding up to 2 layers of encapsulation.
- Snort: Supports decoding up to 255 layers of encapsulation (with a default limit of 40).

## Supported protocols and inspection capabilities of LINA and Snort 3

Supported protocol decoding and inspection capabilities of LINA and Snort 3, including details on encapsulation and tunneling protocols for network security.

### LINA

LINA supports decoding for the following protocols across the Data Link (L2), Network (L3), and Transport (L4) layers.

| Layer | Supported protocols and headers |
|---|---|
| Layer 2 | Cisco MetaData (CMD), IEEE 802.1Q, IEEE 802.1ad (DOT1AD), and Q-in-Q (EtherTypes 0x9100 and 0x9200). Supports up to three levels of VLAN headers. |
| Layer 3 | IPv4, IPv6 |
| Layer 4 | ICMP (v4/v6), ESP, VXLAN, Geneve, GRE, IP-in-IP, and IPv6-in-IPv6. Supports up to 1 level of encapsulation. |

#### GRE-specific support

For GRE traffic, the system supports decoding for the following protocol types:

- Point-to-Point Tunneling Protocol (PPTP)

- Web Cache Communication Protocol (WCCP)

#### ERSPAN handling

The system decodes GRE and ERSPAN (types 1, 2, and 3). To facilitate dispatch layer load-balancing, the system internally skips to the inner headers. Consequently, other modules are unable to inspect ERSPAN headers.

#### Snort 3

While Snort 3 supports a vast array of protocols, the following list highlights common encapsulation and tunneling protocols supported for inspection:

- VXLAN
- GRE
- Teredo
- GTP
- MPLS
- Geneve
- IP-in-IP
  - IPv4-in-IPv4
  - IPv6-in-IPv4
  - IPv4-in-IPv6
  - IPv6-in-IPv6

> **Note**
>
> This list is not exhaustive. Snort 3 is designed to decode a wide range of industry-standard protocols.

## Guidelines and limitations for network analysis and intrusion policies

Consider the feature limitations of Snort 3 for Firewall Management Center-managed Firewall Threat Defense devices when planning your network security deployment.

### Feature Limitations of Snort 3 for Firewall Management Center-Managed Firewall Threat Defense

The table lists the features that are supported on Snort 2 but not supported on Snort 3 for Firewall Management Center-managed Firewall Threat Defense devices.

**Table 1: Feature Limitations of Snort 3**

| Policy/Area | Features not supported |
|---|---|
| Access Control Policy | The following application settings:<br>• Safe Search<br>• YouTube EDU |

| Policy/Area | Features not supported |
|---|---|
| Intrusion Policy | • Global rule thresholding<br>• Logging configuration:<br>  • SNMP<br>• SRU rule updates as Snort 3 supports only LSP rule updates |
| Other features | Event logging with fully qualified domain name (FQDN). |

## Prerequisites for network analysis and intrusion policies

Provides the prerequisites for enabling network analysis and management of intrusion policies.

To allow the Snort inspection engine to process traffic for intrusion and malware analysis, you must have the Intrusion Prevention System (IPS) license enabled for the Firewall Threat Defense device.

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

## How policies examine traffic for intrusions

Describes how the system analyzes traffic through network analysis and intrusion prevention phases in access control deployments.

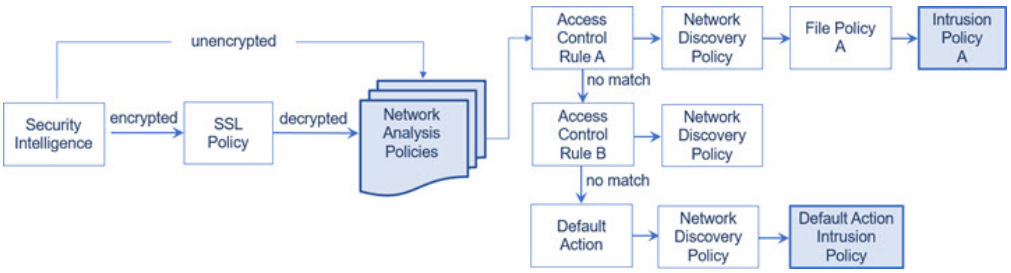
When the system analyzes traffic as part of your access control deployment, the network analysis (decoding and preprocessing) phase occurs before and separately from the intrusion prevention (intrusion rules and advanced settings) phase.

### Summary

The key components involved in examining traffic for intrusions are:

- Security Intelligence: Performs initial traffic filtering and blocking
- SSL policy: Handles encrypted traffic inspection and decryption
- Network analysis policies: Conduct decoding and preprocessing of traffic
- Access control rules: Determine which policies to apply to traffic
- Intrusion policies: Examine traffic for security threats and intrusions
- File policies: Analyze files for malware and threats
- Network discovery policy: Passively inspects packets for network mapping

### Workflow




These stages describe how the system examines traffic for intrusions in an inline deployment:

1. The system processes traffic through multiple policy layers in a specific order, with network analysis and intrusion policy selection phases highlighted in the deployment.

   In an inline deployment (that is, where relevant configurations are deployed to devices using routed, switched, or transparent interfaces, or inline interface pairs), the system can block traffic without further inspection at almost any step in the illustrated process. Security Intelligence, the SSL policy, network analysis policies, file policies, and intrusion policies can all either drop or modify traffic. Only the network discovery policy, which passively inspects packets, cannot affect the flow of traffic.

2. At each step of the process, a packet could cause the system to generate an event. Intrusion and preprocessor events (sometimes referred to collectively as *intrusion events*) are indications that a packet or its contents may represent a security risk.

   **Tip**

   The diagram does not reflect that access control rules handle encrypted traffic when your SSL inspection configuration allows it to pass, or if you do not configure SSL inspection. By default, the system disables intrusion and file inspection of encrypted payloads. This helps reduce false positives and improve performance when an encrypted connection matches an access control rule that has intrusion and file inspection configured.

3. Note that for a single connection, although the system selects a network analysis policy before an access control rule as shown in the diagram, some preprocessing (notably application layer preprocessing) occurs after access control rule selection. This does **not** affect how you configure preprocessing in custom network analysis policies.

## Decoding, normalizing, and preprocessing: Network analysis policies

Describes how network analysis policies decode, normalize, and preprocess traffic before file and intrusion inspection.

Without decoding and preprocessing, the system cannot appropriately evaluate traffic for intrusions because protocol differences would make pattern matching impossible. Network analysis policies govern these traffic-handling tasks

- after traffic is filtered by Security Intelligence,
- after encrypted traffic is decrypted by an optional SSL policy, and
- before traffic can be inspected by file or intrusion policies

A network analysis policy governs packet processing in phases. First the system decodes packets through the first three TCP/IP layers, then continues with normalizing, preprocessing, and detecting protocol anomalies:

- The packet decoder converts packet headers and payloads into a format that can be easily used by the inspectors and later, intrusion rules. Each layer of the TCP/IP stack is decoded in turn, beginning with the data link layer and continuing through the network and transport layers. The packet decoder also detects various anomalous behaviors in packet headers.

- In inline deployments, the inline normalization preprocessor reformats (normalizes) traffic to minimize the chances of attackers evading detection. It prepares packets for examination by other inspectors and intrusion rules, and helps ensure that the packets the system processes are the same as the packets received by the hosts on your network.
- Various network and transport layers inspectors detect attacks that exploit IP fragmentation, perform checksum validation, and perform TCP and UDP session preprocessing.

  Note that some advanced transport and network inspector settings apply globally to all traffic handled by the target devices of an access control policy. You configure these in the access control policy rather than in a network analysis policy.
- Various application-layer protocol decoders normalize specific types of packet data into formats that the intrusion rules engine can analyze. Normalizing application-layer protocol encodings allows the system to effectively apply the same content-related intrusion rules to packets whose data is represented differently, and to obtain meaningful results.
- The Modbus, DNP3, CIP, and s7commplus SCADA inspectors detect traffic anomalies and provide data to intrusion rules. Supervisory Control and Data Acquisition (SCADA) protocols monitor, control, and acquire data from industrial, infrastructure, and facility processes such as manufacturing, production, water treatment, electric power distribution, airport, and shipping systems.
- Several inspectors allow you to detect specific threats, such as Back Orifice, portscans, SYN floods and other rate-based attacks.

  Note that you configure the sensitive data inspector, which detects sensitive data such as credit card numbers and Social Security numbers in ASCII text, in intrusion policies.

> **Note**
>
> When TLS Server Identity is disabled, Snort 3 does not perform SNI mismatch detection. It only evaluates the SNI in the Client Hello packet and bypasses the validation of the certificate's Common Name (CN) in the Server Hello packet.

In a newly created access control policy, one default network analysis policy governs preprocessing for all traffic for all intrusion policies invoked by the same parent access control policy. Initially, the system uses the Balanced Security and Connectivity network analysis policy as the default, but you can change it to another system-provided or custom network analysis policy. In a more complex deployment, advanced users can tailor traffic preprocessing options to specific security zones, networks, and VLANs by assigning different custom network analysis policies to preprocess matching traffic.

> **Note**
>
> For an access control policy with rule action as Trust and a prefilter rule with action as Fastpath with logging options disabled, you will observe that the end-of-flow events are still generated in the system. The events are not visible on the management center event pages.

## Access control rules: Intrusion policy selection

Describes how access control rules evaluate traffic and select intrusion policies for inspection.

Intrusion policy selection is a traffic evaluation process that–

- evaluates traffic after initial preprocessing using access control rules,
- applies matching access control rule to handle traffic through monitor, trust, block, or allow actions,

- inspects allowed traffic for discovery data, malware, prohibited files, and intrusions in that order, and
- handles non-matching traffic using the access control policy's default action.

In most cases, the first access control rule that a packet matches is the rule that handles that traffic; you can monitor, trust, block, or allow matching traffic.

#### Traffic evaluation process

When you allow traffic with an access control rule, the system can inspect the traffic for discovery data, malware, prohibited files, and intrusions, in that order. Traffic not matching any access control rule is handled by the access control policy's default action, which can also inspect for discovery data and intrusions.

> **Note**
>
> All packets, **regardless** of which network analysis policy preprocesses them, are matched to configured access control rules, making them potentially subject to inspection by intrusion policies in top-down order.

The diagram in How policies examine traffic for intrusions on page 16 shows the flow of traffic through a device in an inline, intrusion prevention and AMP for Networks deployment–

- Access Control Rule A allows matching traffic to proceed. The traffic is then inspected for discovery data by the network discovery policy, for prohibited files and malware by File Policy A, and then for intrusions by Intrusion Policy A.
- Access Control Rule B also allows matching traffic. However, in this scenario, the traffic is not inspected for intrusions (or files or malware), so there are no intrusion or file policies associated with the rule. Note that by default, traffic that you allow to proceed is inspected by the network discovery policy; you do not need to configure this.
- In this scenario, the access control policy's default action allows matching traffic. The traffic is then inspected by the network discovery policy, and then by an intrusion policy. You can (but do not have to) use a different intrusion policy when you associate intrusion policies with access control rules or the default action.

The example in the diagram does not include any blocking or trusting rules because the system does not inspect blocked or trusted traffic.

## Intrusion inspection: Intrusion policies, rules, and variable sets

Describes the intrusion prevention system components that inspect traffic for security violations and manage intrusion detection capabilities.

Intrusion inspection is a security mechanism that

- uses intrusion policies to govern how the system inspects traffic for security violations and can block or alter malicious traffic in inline deployments
- employs intrusion and preprocessor rules to analyze network traffic against specified criteria and detect attempts to exploit vulnerabilities, and
- utilizes variable sets to define values commonly used in intrusion rules for identifying source and destination IP addresses and ports.

#### Intrusion and inspector rules

An intrusion rule is a specified set of keywords and arguments that detects attempts to exploit vulnerabilities on your network; the system uses an intrusion rule to analyze network traffic to check if it matches the criteria in the rule. The

system compares packets against the conditions specified in each rule and, if the packet data matches all the conditions specified in a rule, the rule triggers.

The system includes these types of rules created by Cisco Talos Intelligence Group (Talos):

- *shared object intrusion rules*, which are compiled and cannot be modified, except for rule header information such as source and destination ports and IP addresses
- *standard text intrusion rules*, which can be saved and modified as new custom instances of the rule.
- *preprocessor rules*, which are rules associated with inspectors and packet decoder detection options in the network analysis policy. You cannot copy or edit inspector rules. Most inspector rules are disabled by default; you must enable them to use inspectors to generate events and, in an inline deployment, drop offending packets.

When the system processes packets according to an intrusion policy, first a rule optimizer classifies all activated rules in subsets based on criteria such as: transport layer, application protocol, direction to or from the protected network, and so on. Then, the intrusion rules engine selects the appropriate rule subsets to apply to each packet. Finally, a multi-rule search engine performs three different types of searches to determine if the traffic matches the rule:

- The protocol field search looks for matches in particular fields in an application protocol.
- The generic content search looks for ASCII or binary byte matches in the packet payload.
- The packet anomaly search looks for packet headers and payloads that, rather than containing specific content, violate well-established protocols.

In a custom intrusion policy, you can tune detection by enabling and disabling rules, as well as by writing and adding your own standard text rules. You can also use Cisco recommendations to associate the operating systems, servers, and client application protocols detected on your network with rules specifically written to protect those assets.

**Note**

When there are insufficient packets to process specific traffic against a block rule, the system continues to evaluate the remaining traffic against other rules. If any of the remaining traffic matches a rule which is set to block, then the session is blocked. However, if the system analyses the remaining traffic to be passed, then the traffic status shows pending on the rule which is stuck for want of complete packets.

### Variable Sets

Whenever the system uses an intrusion policy to evaluate traffic, it uses an associated *variable set*. Most 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.

The system provides a single default variable set, which is comprised of predefined default variables. Most system-provided shared object rules and standard text rules use these predefined default variables to define networks and port numbers. For example, the majority of the rules use the variable `$HOME_NET` to specify the protected network and the variable `$EXTERNAL_NET` to specify the unprotected (or outside) network. In addition, specialized rules often use other predefined variables. For example, rules that detect exploits against web servers use the `$HTTP_SERVERS` and `$HTTP_PORTS` variables.

**Tip**

Even if you use system-provided intrusion policies, Cisco **strongly** recommends that you modify key default variables in the default set. When you use variables that accurately reflect your network environment, processing is optimized and the system can monitor relevant systems for suspicious activity. Advanced users can create and use custom variable sets for pairing with one or more custom intrusion policies.

**Important**

If you are creating a custom variable set, do not use a number as the first character in a custom variable set name (for example, 3Snort). This will cause Snort 3 validation to fail when you deploy a configuration to Firewall Threat Defense firewall on the Firewall Management Center.

## Intrusion event generation

Describes how the system identifies possible intrusions and generates events for analysis and response.

Intrusion event generation is a security mechanism that:

- identifies possible intrusions through packet decoding, preprocessing, and rules engine analysis,
- generates *intrusion or preprocessor events* (sometimes collectively called *intrusion events*) when threats are detected, and
- transmits events from managed devices to the Firewall Management Center for aggregated analysis and network asset protection.

### Event composition and data collection

Each intrusion event in the database includes an event header and contains information about the event name and classification; the source and destination IP addresses; ports; the process that generated the event; and the date and time of the event, as well as contextual information about the source of the attack and the target. For packet-based events, the system also logs a copy of the decoded packet header and payload for the packet or packets that triggered the event.

As the database accumulates intrusion events, you can begin your analysis of potential attacks. The system provides you with the tools you need to review intrusion events and evaluate whether they are important in the context of your network environment and your security policies.

### Event generation scenarios

The packet decoder, the preprocessors, and the intrusion rules engine can all cause the system to generate an event. For example:

- If the packet decoder (configured in the network analysis policy) receives an IP packet that is less than 20 bytes, which is the size of an IP datagram without any options or payload, the decoder interprets this as anomalous traffic. If, later, the accompanying decoder rule in the intrusion policy that examines the packet is enabled, the system generates a inspector event.
- If the IP defragmentation preprocessor encounters a series of overlapping IP fragments, the inspector interprets this as a possible attack and, when the accompanying inspector rule is enabled, the system generates a inspector event.
- Within the intrusion rules engine, most standard text rules and shared object rules are written so that they generate intrusion events when triggered by packets.

# System-provided and custom network analysis and intrusion policies

Describes how system-provided and custom network analysis and intrusion policies work together in access control policies to examine and process network traffic for security threats.

Network analysis and intrusion policies are security mechanisms that

- examine traffic through preprocessing and intrusion prevention phases,
- provide system-provided default configurations for immediate deployment, and
- allow custom policy creation for tailored security requirements.

### Default policy behavior in access control deployments

By default, a newly created access control policy invokes system-provided network analysis and intrusion policies to examine traffic.

This diagram shows how a newly created access control policy in an inline, intrusion-prevention deployment initially handles traffic:




The traffic flow demonstrates these characteristics:

- A default network analysis policy governs the preprocessing of *all* traffic handled by the access control policy. Initially, the system-provided *Balanced Security and Connectivity network analysis policy* is the default.
- The default action of the access control policy allows all non-malicious traffic, as determined by the system-provided *Balanced Security and Connectivity intrusion policy*. Because the default action allows traffic to pass, the discovery feature can examine it for host, application, and user data before the intrusion policy can examine and potentially block malicious traffic.
- The policy uses default Security Intelligence options (global Block and Do Not Block lists only), does not decrypt encrypted traffic with an SSL policy, and does not perform special handling and inspection of network traffic using access control rules.

A simple step you can take to tune your intrusion prevention deployment is to use a different set of system-provided network analysis and intrusion policies as your defaults. Cisco delivers several pairs of these policies with the system.

Or, you can tailor your intrusion prevention deployment by creating and using custom policies. You may find that the inspector options, intrusion rule, and other advanced settings configured in those policies do not address the security needs of your network. By tuning your network analysis and intrusion policies, you can control at a very granular level how the system processes and inspects traffic on your network for intrusions.

## System-provided network analysis and intrusion policies

Describes the network analysis and intrusion policies that Cisco delivers with the system.

System-provided network analysis and intrusion policies are security configurations that

- leverage the experience of the Cisco Talos Intelligence Group (Talos) for intrusion and inspector rule states and advanced settings,
- provide starting points for well tuned defensive policies covering common network setups, and
- receive automatic updates through Lightweight Security Package (LSP) releases for new vulnerabilities.

### Key characteristics and usage

No system-provided policy covers every network profile, traffic mix, or defensive posture. Each covers common cases and network setups that provide a starting point for a well-tuned defensive policy. Although you can use system-provided policies as-is, Cisco strongly recommends that you use them as the base for custom policies that you tune to suit your network.

> **Tip**
>
> Even if you use system-provided network analysis and intrusion policies, you should configure the system's intrusion variables to accurately reflect your network environment. At a minimum, modify key default variables in the default set.

As new vulnerabilities become known, Talos releases intrusion rule updates, also known as *Lightweight Security Package* (LSP). These rule updates can modify any system-provided network analysis or intrusion policy, and can provide new and updated intrusion rules and inspector rules, modified states for existing rules, and modified default policy settings. Rule updates may also delete rules from system-provided policies and provide new rule categories, as well as modify the default variable set.

If a rule update affects your deployment, the web interface marks affected intrusion and network analysis policies as out of date, as well as their parent access control policies. You must re-deploy an updated policy for its changes to take effect.

For your convenience, you can configure rule updates to automatically re-deploy affected intrusion policies, either alone or in combination with affected access control policies. This allows you to easily and automatically keep your deployment up-to-date to protect against recently discovered exploits and intrusions.

To ensure up-to-date preprocessing settings, you **must** re-deploy access control policies, which also deploys any associated SSL, network analysis, and file policies that are different from those currently running, and can also update default values for advanced preprocessing and performance options.

Cisco delivers the system-provided network analysis and intrusion policies:

- Balanced Security and Connectivity network analysis and intrusion policies — These policies are built for both speed and detection. Used together, they serve as a good starting point for most organizations and deployment types. The system uses the Balanced Security and Connectivity policies and settings as defaults in most cases.
- Connectivity Over Security network analysis and intrusion policies — These policies are built for organizations where connectivity (being able to get to all resources) takes precedence over network infrastructure security. The intrusion policy enables far fewer rules than those enabled in the Security over Connectivity policy. Only the most critical rules that block traffic are enabled.
- Security Over Connectivity network analysis and intrusion policies — These policies are built for organizations where network infrastructure security takes precedence over user convenience. The intrusion policy enables numerous network anomaly intrusion rules that could alert on or drop legitimate traffic.
- Maximum Detection network analysis and intrusion policies — These policies are built for organizations where network infrastructure security is given even more emphasis than is given by the Security Over Connectivity policies, with the potential for even greater operational impact. For example, the intrusion policy enables rules in a large number of threat categories including malware, exploit kit, old and common vulnerabilities, and known in-the-wild exploits.
- No Rules Active intrusion policy — In the No Rules Active intrusion policy, all intrusion rules, and all advanced settings except intrusion rule thresholds, are disabled. This policy provides a starting point if you want to create your own intrusion policy instead of basing it on the enabled rules in one of the other system-provided policies.

> **Note**
>
> Depending on the system-provided base policy that is selected, the settings of the policy vary. To view the policy settings, click the **Edit** icon next to the policy and then click the **Base Policy** drop-down menu.

## Benefits of custom network analysis and intrusion policies

Explains the advantages of creating customized network analysis and intrusion policies to improve system performance and provide focused security monitoring capabilities.

Custom network analysis and intrusion policies are security configurations that:

- improve system performance in your specific environment,
- provide a focused view of malicious traffic and policy violations occurring on your network, and
- allow granular configuration of how the system processes and inspects network traffic for intrusions.

### Custom policy structure

You may find that the inspector options, intrusion rules, and other advanced settings configured in the system-provided network analysis and intrusion policies do not fully address the security needs of your organization.

All custom policies have a base policy, also called a base layer, which defines the default settings for all configurations in the policy. A layer is a building block that you can use to efficiently manage multiple network analysis or intrusion policies.

In most cases, you base custom policies on system-provided policies, but you can use another custom policy. However, all custom policies have a system-provided policy as the eventual base in a policy chain. Because rule updates can modify system-provided policies, importing a rule update may affect you even if you are using a custom policy as your base. If a rule update affects your deployment, the web interface marks affected policies as out of date.

### Custom network analysis policy benefits

Describes the advantages of creating and using custom network analysis policies for traffic preprocessing optimization.

Custom network analysis policies:

- enable tuning preprocessing to match specific traffic characteristics and monitoring requirements,
- reduce system processing overhead by disabling unnecessary inspectors, and
- allow tailored preprocessing for different security zones, networks, or VLANs in complex deployments.

By default, one network analysis policy preprocesses all unencrypted traffic handled by the access control policy. That means that all packets are decoded and preprocessed according to the same settings, regardless of the intrusion policy (and therefore intrusion rule set) that later examines them.

Initially, the system-provided Balanced Security and Connectivity network analysis policy is the default. A simple way to tune preprocessing is to create and use a custom network analysis policy as the default.

Tuning options available vary by inspector, but some of the ways you can tune inspectors and decoders include:

- You can disable inspectors that do not apply to the traffic you are monitoring. For example, the HTTP Inspect inspector normalizes HTTP traffic. If you are confident that your network does not include any web servers using Microsoft Internet Information Services (IIS), you can disable the inspector option that looks for IIS-specific traffic and thereby reduce system processing overhead.

> **Note**
>
> If you disable an inspector in a custom network analysis policy, but the system needs to use that inspector to later evaluate packets against an enabled intrusion or inspector rule, the system automatically enables and uses the inspector although the inspector remains disabled in the network analysis policy web interface.

- Specify ports, where appropriate, to focus the activity of certain inspectors. For example, you can identify additional ports to monitor for DNS server responses, encrypted SSL sessions, or ports on which you decode telnet, HTTP, and RPC traffic.

If you are an advanced user with a complex deployment, you can create multiple network analysis policies, each tailored to preprocess traffic differently. Then, you can configure the system to use those policies to govern the preprocessing of traffic using different security zones, networks, or VLANs. (Note that ASA FirePOWER modules cannot restrict preprocessing by VLAN.)

> **Note**
>
> Tailoring preprocessing using custom network analysis policies—especially multiple network analysis policies—is an advanced task. Because preprocessing and intrusion inspection are so closely related, you **must** be careful to allow the network analysis and intrusion policies examining a single packet to complement each other.

### Benefits of custom intrusion policies

Describes how custom intrusion policies enable tailored intrusion prevention deployment through rule management and traffic inspection customization.

Custom intrusion policies are security configurations that

- enable tailored traffic inspection through multiple specialized intrusion policies
- manage which intrusion and inspector rules are enabled and how they are configured, and
- allow access control rules to specify which policy inspects which traffic based on multiple criteria.

In a newly created access control policy initially configured to perform intrusion prevention, the default action allows all traffic, but first inspects it with the system-provided Balanced Security and Connectivity intrusion policy. Unless you add access control rules or change the default action, all traffic is inspected by that intrusion policy.

To customize your intrusion prevention deployment, you can create multiple intrusion policies, each tailored to inspect traffic differently. Then, configure an access control policy with rules that specify which policy inspects which traffic. Access control rules can be simple or complex, matching and inspecting traffic using multiple criteria including security zone, network or geographical location, VLAN, port, application, requested URL, or user.

The main function of intrusion policies is to manage which intrusion and inspector rules are enabled and how they are configured, as follows:

- Within each intrusion policy, you should verify that all rules applicable to your environment are enabled, and improve performance by disabling rules that are not applicable to your environment. You can specify which rules should drop or modify malicious packets.
- Cisco recommendations allow you to associate the operating systems, servers, and client application protocols detected on your network with rules specifically written to protect those assets.

- You can modify existing rules and write new standard text rules as needed to catch new exploits or to enforce your security policies.

Other customizations you might make to an intrusion policy include:

- The sensitive data preprocessor detects sensitive data such as credit card numbers and Social Security numbers in ASCII text. Note that other inspectors that detect specific threats (back orifice attacks, several portscan types, and rate-based attacks that attempt to overwhelm your network with excessive traffic) are configured in network analysis policies.
- Global thresholds cause the system to generate events based on how many times traffic matching an intrusion rule originates from or is targeted to a specific address or address range within a specified time period. This helps prevent the system from being overwhelmed with a large number of events.
- Suppressing intrusion event notifications and setting thresholds for individual rules or entire intrusion policies can also prevent the system from being overwhelmed with a large number of events.
- In addition to the various views of intrusion events within the web interface, you can enable logging to syslog facilities or send event data to an SNMP trap server. For each policy, you can specify intrusion event notification limits, set up intrusion event notification to external logging facilities, and configure external responses to intrusion events. Note that in addition to these per-policy alerting configurations, you can globally enable or disable email alerting on intrusion events for each rule or rule group. Your email alert settings are used regardless of which intrusion policy processes a packet.

## Limitations of custom policies

Outlines configuration requirements when using custom network analysis and intrusion policies to ensure proper traffic preprocessing and inspection coordination.

Because preprocessing and intrusion inspection are so closely related, you **must** be careful that your configuration allows the network analysis and intrusion policies processing and examining a single packet to complement each other.

By default, the system uses one network analysis policy to preprocess all traffic handled by managed devices using a single access control policy. This diagram shows how a newly created access control policy in an inline intrusion-prevention deployment initially handles traffic. The preprocessing and intrusion prevention phases are highlighted.




Notice how a default network analysis policy governs the preprocessing of *all* traffic handled by the access control policy. Initially, the system-provided Balanced Security and Connectivity network analysis policy is the default.

You can tune preprocessing by creating and using a custom network analysis policy as the default. However, if you disable a inspector in a custom network analysis policy but the system needs to evaluate preprocessed packets against an enabled intrusion or inspector rule, the system automatically enables and uses the inspector although it remains disabled in the network analysis policy web interface.

**Note**

In order to get the performance benefits of disabling an inspector, you **must** make sure that none of your intrusion policies have enabled rules that require that inspector.

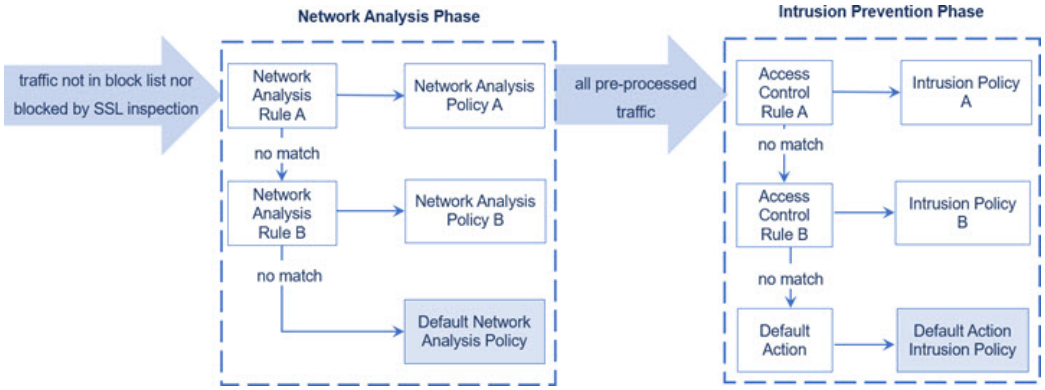
An additional challenge arises if you use multiple custom network analysis policies. For advanced users with complex deployments, you can tailor preprocessing to specific security zones, networks, and VLANs by assigning custom network analysis policies to preprocess matching traffic. (Note that ASA FirePOWER cannot restrict preprocessing by VLAN.) To

accomplish this, you add custom *network analysis rules* to your access control policy. Each rule has an associated network analysis policy that governs the preprocessing of traffic that matches the rule.

> **Tip**
>
> You configure network analysis rules as an advanced setting in an access control policy. Unlike other types of rules, network analysis rules invoke network analysis policies, rather than being contained by them.

The system matches packets to any configured network analysis rules in top-down order by rule number. Traffic that does not match any network analysis rule is preprocessed by the default network analysis policy. While this allows you a great deal of flexibility in preprocessing traffic, keep in mind that all packets, **regardless** of which network analysis policy preprocessed them, are subsequently matched to access control rules—and thus to potential inspection by intrusion policies—in their own process. In other words, preprocessing a packet with a particular network analysis policy does **not** guarantee that the packet will be examined with any particular intrusion policy. You **must** carefully configure your access control policy so it invokes the correct network analysis and intrusion policies to evaluate a particular packet.

The diagram shows in detail how the network analysis policy (preprocessing) selection phase occurs before and separately from the intrusion prevention (rules) phase. For simplicity, the diagram eliminates the discovery and file or malware inspection phases. It also highlights the default network analysis and default-action intrusion policies.




In this scenario, an access control policy is configured with two network analysis rules and a default network analysis policy:

- Network Analysis Rule A preprocesses matching traffic with Network Analysis Policy A. Later, you want this traffic to be inspected by Intrusion Policy A.
- Network Analysis Rule B preprocesses matching traffic with Network Analysis Policy B. Later, you want this traffic to be inspected by Intrusion Policy B.
- All remaining traffic is preprocessed with the default network analysis policy. Later, you want this traffic to be inspected by the intrusion policy associated with the default action of the access control policy.

After the system preprocesses traffic, it can examine the traffic for intrusions. The diagram shows an access control policy with two access control rules and a default action:

- Access Control Rule A allows matching traffic. The traffic is then inspected by Intrusion Policy A.
- Access Control Rule B allows matching traffic. The traffic is then inspected by Intrusion Policy B.
- The default action of the access control policy allows matching traffic. The traffic is then inspected by the default action's intrusion policy.

Each packet's handling is governed by a network analysis policy and intrusion policy pair, but the system does **not** coordinate the pair for you. Consider a scenario where you misconfigure your access control policy so that Network

Analysis Rule A and Access Control Rule A do not process the same traffic. For example, you could intend the paired policies to govern the handling of traffic on a particular security zone, but you mistakenly use different zones in the two rules' conditions. This could cause traffic to be incorrectly preprocessed. For this reason, tailoring preprocessing using network analysis rules and custom policies is an **advanced** task.

Note that for a single connection, although the system selects a network analysis policy before an access control rule, some preprocessing (notably application layer preprocessing) occurs after access control rule selection. This does **not** affect how you configure preprocessing in custom network analysis policies.

# 2 Migrate from Snort 2 to Snort 3

**Topics:**


- Snort 3 inspection engine
- Snort 2 versus Snort 3
- Migrating from Snort 2 to Snort 3
- View Snort 2 and Snort 3 base policy mapping
- Synchronize Snort 2 rules with Snort 3
- Deploy configuration changes
- Examples for migration


Describes how intrusion policies are migrated from Snort 2 to Snort 3. Guides users through enabling Snort 3, converting Snort 2 custom rules, synchronizing rule sets, and deploying configuration changes to leverage Snort 3's enhanced detection and performance capabilities.

Starting with Version 7.0, Snort 3 is the default inspection engine for new Firewall Threat Defense deployments with Firewall Management Center. Snort 3 is required in Version 7.7+. If you are still using the Snort 2 inspection engine, switch to Snort 3 now for improved detection and performance.

Upgrading Firewall Threat Defense to Version 7.2 through 7.6 also upgrades eligible Snort 2 devices to Snort 3. For devices that are ineligible because they use custom intrusion or network analysis policies, manually upgrade to Snort 3 as described here.

Although you can switch individual devices back, you should not. Upgrading Firewall Threat Defense to Version 7.7+ is blocked for Snort 2 devices.

## Snort 3 inspection engine

Describes the default inspection engine for newly registered devices on version 7.0 or later, and the requirements for upgraded devices.

Snort 3 is a network inspection engine that

- serves as the default inspection engine for newly registered Firewall Threat Defense devices on version 7.0 or later,
- requires explicit enablement after upgrading Firewall Threat Defense devices to version 7.0 or later, and
- activates the Snort 3 version of the intrusion policy, which is applied through access control policies, for all traffic passing through the device.

For Firewall Threat Defense devices on version 6.x or earlier, Snort 2 is the default inspection engine.

#### Version switching and rule mapping

You can switch Snort versions when required. Snort 2 and Snort 3 intrusion rules are mapped and the mapping is system-provided. However, you may not find a one-to-one mapping of all the intrusion rules in Snort 2 and Snort 3. If you change the rule action for one rule in Snort 2, that change will not be retained if you switch to Snort 3 without first synchronizing Snort 2 with Snort 3. For more information on synchronization, see Synchronize Snort 2 rules with Snort 3 on page 36.

## Snort 2 versus Snort 3

Provides architectural and inspection engine capability differences between Snort 2 and Snort 3 versions.

Snort 3 has been architecturally redesigned to inspect more traffic with equivalent resources when compared to Snort 2. Snort 3 provides simplified and flexible insertion of traffic parsers. Snort 3 also provides new rule syntax that makes rule writing easier and shared object rule equivalents visible.

This table lists the differences between the Snort 2 and the Snort 3 versions in terms of the inspection engine capabilities.

| Feature | Snort 2 | Snort 3 |
|---|---|---|
| Packet threads | One per process | Any number per process |
| Configuration memory use | Number of processes * *x* GB | *x* gigabytes (GB) in total; more memory available for packets |
| Configuration reload | Slower | Faster; one thread can be pinned to separate cores |
| Rule syntax | Inconsistent and requires line escapes | Uniform system with arbitrary whitespace |
| Rule comments | Comments only | #, #begin and #end marks; C language style |

Additional reference: Differences between Snort 2 and Snort 3 in Firepower.

## Migrating from Snort 2 to Snort 3

Describes the process of switching the inspection engine of the Firewall Threat Defense device from Snort 2 to Snort 3.

Migrating from Snort 2 to Snort 3 requires you to switch the inspection engine of the Firewall Threat Defense device from Snort 2 to Snort 3.

### Summary

Depending on your requirements, go through the stages listed in the workflow to complete the migration of your device from Snort 2 to Snort 3.

### Workflow

These are the stages of migrating from Snort 2 to Snort 3:

1. Enable Snort 3 on the device.
   - Enable Snort 3 on an individual device on page 31
   - Enable Snort 3 on multiple devices on page 32
2. Convert Snort 2 custom rules to Snort 3.
   - Convert all Snort 2 custom rules across all intrusion policies to Snort 3 on page 33
   - Convert Snort 2 custom rules of a single intrusion policy to Snort 3 on page 34
3. Synchronize Snort 2 rules with Snort 3.
   - Synchronize Snort 2 rules with Snort 3 on page 36

## Prerequisites for migrating from Snort 2 to Snort 3

Consider the following recommended prerequisites before migrating your device from Snort 2 to Snort 3.

Consider the recommended prerequisites before migrating your device from Snort 2 to Snort 3.

- Have a working knowledge of Snort. To learn about the Snort 3 architecture, see Snort 3 Adoption.
- Back up your management center. See Backup the Management Center.
- Back up your intrusion policy. See Exporting Configurations.
- Clone your intrusion policy. To do this, you can use an existing policy as the base policy to create a copy of your intrusion policy. In the **Intrusion Policies** page, click **Create Policy** and choose an existing intrusion policy from the **Base Policy** dropdown list.

## Enable Snort 3 on an individual device

Enable Snort 3 inspection engine on a specific device.

Enable Snort 3 on an individual device to take advantage of enhanced security capabilities.

Use this procedure when you need to upgrade a specific device from Snort 2 to Snort 3 inspection engine. The system will automatically convert policy configurations during deployment to ensure compatibility with the selected Snort version.

### Important

During the deployment process, there could be a momentary traffic loss because the current inspection engine needs to be shut down.

**Procedure**

1. Choose **Devices** > **Device Management**.
2. Click the device to go to the device home page.

   > **Note**
   >
   > The device is marked as Snort 2 or Snort 3, showing the current version on the device.

3. Click the **Device** tab.
4. In the Inspection Engine section, click **Upgrade**.

   > **Note**
   >
   > In case you want to disable Snort 3, click **Revert to Snort 2** in the Inspection Engine section.

5. Click **Yes**.

**What to do next**

Deploy the changes on the device. See Deploy configuration changes on page 37.

The system converts your policy configurations during the deployment process to make them compatible with the selected Snort version.

## Enable Snort 3 on multiple devices

Enable Snort 3 on multiple devices.

This task enables Snort 3 on multiple devices to provide enhanced intrusion detection capabilities.

To enable Snort 3 on multiple devices, ensure all the required Firewall Threat Defense devices are on version 7.0 or later.

**Important**

During the deployment process, there could be a momentary traffic loss because the current inspection engine needs to be shut down.

**Procedure**

1. Choose **Devices** > **Device Management**.
2. Select all the devices on which you want to enable or disable Snort 3.

> **Note**
>
> The devices are marked as Snort 2 or Snort 3, showing the current version on the device.

3. Click the **Select Bulk Action** dropdown list and choose **Upgrade to Snort 3**.
4. Click **Yes**.

---

#### What to do next

Deploy the changes on the device. See Deploy configuration changes on page 37.

## Convert Snort 2 Custom IPS Rules to Snort 3

Describes the process of converting custom Snort 2 intrusion prevention system rules to work with Snort 3 detection engines.

Snort 2 to Snort 3 custom IPS rule conversion is a migration process that transforms custom intrusion prevention system rules from Snort 2 format to Snort 3 format.

#### Conversion requirements and resources

If you are using a rule set from a third-party vendor, contact that vendor to confirm that their rules successfully convert to Snort 3 or to obtain a replacement rule set written natively for Snort 3. If you have custom rules that you have written yourself, familiarize yourself with writing Snort 3 rules prior to conversion so that you can update your rules to optimize Snort 3 detection after conversion. See the links to learn more about writing rules in Snort 3.

- https://blog.snort.org/2020/08/how-rules-are-improving-in-snort-3.html
- https://blog.snort.org/2020/10/talos-transition-to-snort-3.html

You can refer to other blogs at https://blog.snort.org/ to learn more about Snort 3 rules.

See these procedures to convert Snort 2 rules to Snort 3 rules using the system-provided tool.

- Convert all Snort 2 custom rules across all intrusion policies to Snort 3 on page 33
- Convert Snort 2 custom rules of a single intrusion policy to Snort 3 on page 34

**Important**

Snort 2 network analysis policy (NAP) settings *cannot* be copied to Snort 3 automatically. NAP settings have to be manually replicated in Snort 3.

#### Convert all Snort 2 custom rules across all intrusion policies to Snort 3

Configure automatic conversion of all Snort 2 custom rules across all intrusion policies to Snort 3 format.

Convert legacy Snort 2 custom rules to the updated Snort 3 format to ensure compatibility with current intrusion detection systems.

This task migrates existing Snort 2 custom rules to Snort 3 format, allowing you to maintain your custom rule configurations while upgrading to the latest intrusion detection engine. You can either import the converted rules directly or download them for review before importing.

**Procedure**

1. Choose **Objects** > **Intrusion Rules**.
2. Click **Snort 3 All Rules** tab.
3. Ensure **All Rules** is selected in the left pane.
4. Click the **Tasks** drop-down list and choose:
   - **Convert Snort 2 rules and import**–To automatically convert all the Snort 2 custom rules across all the intrusion policies to Snort 3 and import them into Firewall Management Center as Snort 3 custom rules.
   - **Convert Snort 2 rules and download**–To automatically convert all the Snort 2 custom rules across all the intrusion policies to Snort 3 and download them into your local system.
5. Click **OK**.

> **Note**
>
> - If you selected **Convert and import** in the previous step, then all the converted rules are saved under a newly created rule group **All Snort 2 Converted Global** under **Local Rules**.
> - If you selected **Convert and download** in the previous step, then save the rules file locally. You can review the converted rules in the downloaded file and later upload them by following the steps in Add custom rules to rule groups on page 76.

Refer to the video Converting Snort 2 Rules to Snort 3 for additional support and information.

**What to do next**

Deploy configuration changes. See Deploy configuration changes on page 37.

**Convert Snort 2 custom rules of a single intrusion policy to Snort 3**

Configure the conversion of Snort 2 custom rules to Snort 3 format for a single intrusion policy.

Convert Snort 2 custom rules in an intrusion policy to Snort 3 format to maintain compatibility with Snort 3 environments.

When migrating to Snort 3, existing Snort 2 custom rules need to be converted to maintain their functionality. This task allows you to convert custom rules for a specific intrusion policy.

**Procedure**

1. Choose **Policies** > **Access Control heading** > **Intrusion**.
2. In the **Intrusion Policies** tab, click **Show Snort 3 Sync status**.
3. Click the **Sync** icon **Snort out-of-Sync** (🔶) of the intrusion policy.

> **Note**
>
> If the Snort 2 and the Snort 3 versions of the intrusion policy are synchronized, then the **Sync** icon is in blue**Snort in-Sync** (). It indicates that there are no custom rules to be converted.

4. Read the summary and click the **Custom Rules** tab.
5. Choose:
   - **Import converted rules to this policy**: To convert the Snort 2 custom rules in the intrusion policy to Snort 3 and import them into Firewall Management Center as Snort 3 custom rules.
   - **Download converted rules**: To convert the Snort 2 custom rules in the intrusion policy to Snort 3 and download them into your local system. You can review the converted rules in the downloaded file and later upload the file by clicking the upload icon.
6. Click **Re-Sync**.

**What to do next**

Deploy configuration changes. See Deploy configuration changes on page 37.

## View Snort 2 and Snort 3 base policy mapping

View the Snort 3 to Snort 2 intrusion policy mapping in the management center.

This task allows you to view the mapping between Snort 3 and Snort 2 intrusion policies.

> **Note**
>
> Snort 2 is not supported on threat defense version 7.7. For information on Snort 2 features that are supported in versions earlier than 7.7, refer to the Firewall Management Center guide that matches your Firewall Threat Defense version.

**Procedure**

1. Choose **Policies** > **Access Control heading** > **Intrusion**.
2. Ensure the **Intrusion Policies** tab is selected.
3. Click **IPS Mapping**.
4. In the **IPS Policy Mapping** dialog box, click **View Mappings** to view the Snort 3 to Snort 2 intrusion policy mapping.
5. Click **OK**.

## Synchronize Snort 2 rules with Snort 3

Configure synchronization to retain Snort 2 version settings and custom rules when moving to Snort 3, ensuring similar coverage between versions.

This task helps ensure that Snort 2 rule override settings and custom rules are replicated on Snort 3, allowing you to start with similar coverage when transitioning between versions.

To ensure that the Snort 2 version settings and custom rules are retained and carried over to Snort 3, the Firewall Management Center provides the synchronization functionality. Synchronization helps Snort 2 rule override settings and custom rules, which you may have altered and added over the last few months or years, to be replicated on the Snort 3 version. This utility helps to synchronize Snort 2 version policy configuration with Snort 3 version to start with similar coverage.

**Note**

Snort 2 is not supported on threat defense Version 7.7. For information on Snort 2 features that are supported in versions earlier than 7.7, refer to the Firewall Management Center guide that matches your Firewall Threat Defense version.

If the Firewall Management Center is upgraded from 6.7 or earlier to 7.0 or later version, the system synchronizes the configuration. If the Firewall Management Center is a fresh 7.0 or later version, you can upgrade to a higher version, and the system will not synchronize any content during upgrade.

Before upgrading a device to Snort 3, if changes are made in Snort 2 version, you can use this utility to have the latest synchronization from Snort 2 version to Snort 3 version so that you start with a similar coverage.

**Note**

When you move to Snort 3, manage the Snort 3 version of the policy independently. Do not use this utility as a regular operation.

**Important**

- Only the Snort 2 rule overrides and custom rules are copied to Snort 3 and not the other way around. You may not find a one-to-one mapping of all the intrusion rules in Snort 2 and Snort 3. Your changes to rule actions for rules that exist in both versions are synchronized when you perform the following procedure.
- Synchronization *does not* migrate the threshold and suppression settings of any custom or system-provided rules from Snort 2 to Snort 3.

### Procedure

1. Choose **Policies** > **Access Control heading** > **Intrusion**.
2. Ensure the **Intrusion Policies** tab is selected.
3. Click **Show Snort 3 Sync status**.

4. Identify the intrusion policy that is out-of-sync.
5. Click the **Sync** icon **Snort out-of-Sync** (🔶).

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

6. Read the summary. Download a copy of the summary if required.
7. Click **Re-Sync**.

> **Note**
>
> - The synchronized settings will be applicable on the Snort 3 intrusion engine only if it is applied on a device, and after a successful deployment.
> - Snort 2 custom rules can be converted to Snort 3 with the system-provided tool. If you have any Snort 2 custom rules, click the Custom Rules tab and follow the on-screen instructions to convert the rules. For more information, see Convert Snort 2 custom rules of a single intrusion policy to Snort 3 on page 34.

---

**What to do next**

Deploy configuration changes. See Deploy configuration changes on page 37.

## Deploy configuration changes

Deploy configuration changes to affected devices after modifying configurations.

Deploy configuration changes to ensure that modifications made to device configurations take effect on the affected devices.

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 to the *Deploy Configuration Changes* topic in the latest version of the *Cisco Secure Firewall Management Center Device 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**

1. On the 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.

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.

     If you select a checkbox next to a device, all changes made to that device and listed for the device, are included in the 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.

3. Click **Deploy**.
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.

Configuration changes are deployed to the selected devices and take effect according to the deployment settings.

**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 Device Configuration Guide*.

# Examples for migration

Describes Snort 2 to Snort 3 migration scenarios and examples.

## Migrate from Snort 2 to Snort 3

Describes the process of transitioning from Snort 2 to Snort 3 to leverage enhanced features and capabilities.

Migrating from Snort 2 to Snort 3

- involves converting and adapting the Snort 2 rules to the Snort 3 rule syntax,
- optimizes the rules for improved detection and performance, and
- allows organizations to leverage the enhanced features and capabilities of Snort 3.

Organizations with Threat Defense devices managed by the Secure Firewall Management Center can opt for a hybrid deployment approach during the migration from Snort 2 to Snort 3. This approach allows for a gradual transition and minimizes potential disruptions, if any.

## Benefits of migrating to snort 3

Describes the advantages of migrating from Snort 2 to Snort 3.

Snort 3 provides

- **Enhanced protocol support**: Snort 3 provides improved protocol support, allowing you to detect and monitor threats across a wide range of modern protocols, including encrypted traffic.
- **Streamlined rule management**: Snort 3 offers a more user-friendly rule language and rule management system, making it easier to create, modify, and manage rules effectively.
- **Improved performance**: Snort 3 has been optimized to handle higher traffic volumes more efficiently, ensuring timely threat detection and reducing the risk of performance bottlenecks.

## Sample business scenario

Describes a typical organizational situation where security analysts and network administrators evaluate migrating from Snort 2 to Snort 3 to enhance network security capabilities.

This sample business scenario is an illustrative situation that

- demonstrates how organizations evaluate network security inspection engine migrations,
- shows the roles and motivations of security analysts and network administrators in technology decisions, and
- highlights the benefits of upgrading from legacy to modern security monitoring solutions.

### Organizational migration scenario

Alice works as a security analyst in a large organization that heavily relies on the Snort inspection engine to monitor and protect their network infrastructure. The organization has been using Snort Version 2 for several years, but they have encountered some limitations and challenges.

Bob, the network administrator, is looking to migrate from Snort 2 to Snort 3 to overcome these issues and enhance his organization's network security capabilities.

This migration will also improve network security monitoring, enhance performance, and streamline rule management.

## Best practices for migrating from Snort 2 to Snort 3

Consider these practices to ensure a successful migration from Snort 2 to Snort 3.

Follow these best practices when migrating from Snort 2 to Snort 3 to ensure data integrity and maintain security coverage.

- Back up your intrusion policy before performing the migration. See the Export Configurations task in the *Cisco Secure Firewall Management Center Administration Guide*.
- Before upgrading a device to Snort 3, if changes are made in Snort 2, use the synchronize utility to include the latest synchronization from Snort 2 to Snort 3 so that you can start with a similar coverage. See Synchronize Snort 2 rules with Snort 3 on page 36.
- Snort 2 custom rules are not automatically converted to Snort 3 and must be manually migrated. See Convert Snort 2 Custom IPS Rules to Snort 3 on page 33.
- Synchronization does not migrate Snort 2 rules with thresholds or suppressions. These rules must be created again in Snort 3.

## Prerequisites for migration

Outlines the essential requirements to prepare for a successful migration process.

Complete these prerequisites before starting the migration process to ensure system readiness and data protection.

- Have a working knowledge of Snort. To learn about the Snort 3 architecture, see Snort 3 Adoption.
- Back up your management center. See Backup the Management Center.
- Back up your intrusion policy. See Exporting Configurations.

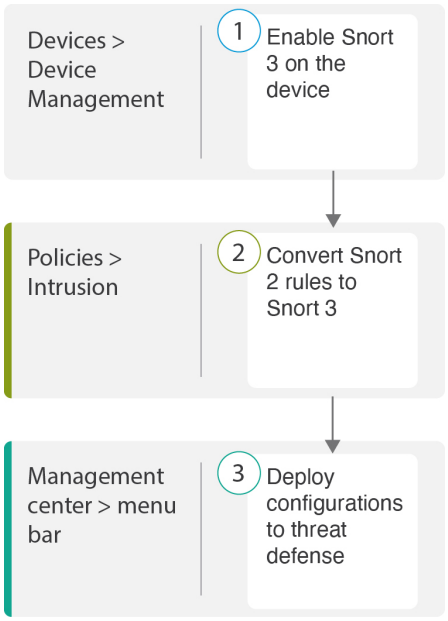
## End-to-end migration workflow

Describes the workflow for migrating Snort 2 to Snort 3 in Secure Firewall Management Center.

### Summary

Depending on your requirements, go through the stages listed in the workflow to complete the migration of your device from Snort 2 to Snort 3.

### Workflow




These are the stages of migrating Snort 2 to Snort 3:

1. Enable Snort 3 on the device. See Enable Snort 3 on Threat Defense device on page 41.
2. Convert Snort 2 rules to Snort 3. See Convert Snort 2 rules of a single intrusion policy to Snort 3 on page 42.
3. Deploy configuration. See Deploy configuration changes on page 37.

## Enable Snort 3 on Threat Defense device

Configure Snort 3 as the inspection engine on your Threat Defense device.

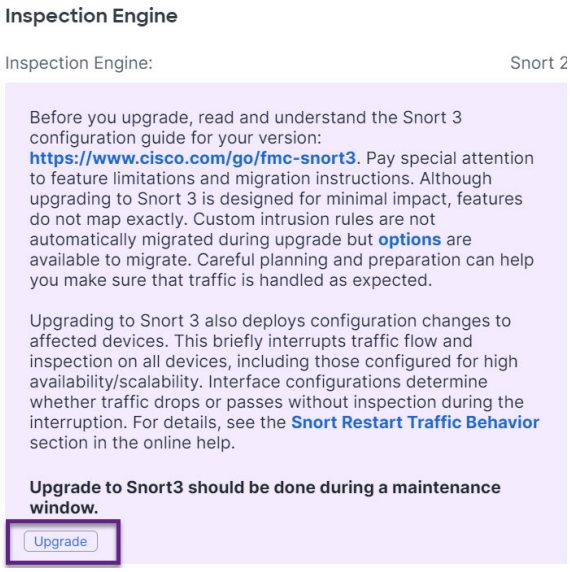
Enable Snort 3 on your Threat Defense device for enhanced security capabilities.

Use this procedure to upgrade from Snort 2 to Snort 3 on your Threat Defense device.

> **Attention**
>
> During the deployment process, there could be a momentary traffic loss because the current inspection engine needs to be shut down.

**Procedure**

1. Choose **Devices** > **Device Management**.
2. Click the corresponding device to go to the device home page.
3. Click the **Device** tab.
4. In the **Inspection Engine** section, click **Upgrade**.




5. Click **Yes**.

**What to do next**

Deploy the changes on the device. See Deploy configuration changes on page 37.

The system converts your policy configurations during the deployment process to make them compatible with the selected Snort version.

## Convert Snort 2 rules of a single intrusion policy to Snort 3

Convert Snort 2 rules to Snort 3 format for a single intrusion policy to ensure compatibility with Snort 3 engines.

This task synchronizes and converts Snort 2 intrusion policy rules to Snort 3 format, ensuring that custom rules, thresholds, and suppressions are properly migrated to maintain security policy effectiveness when using Snort 3 engines.

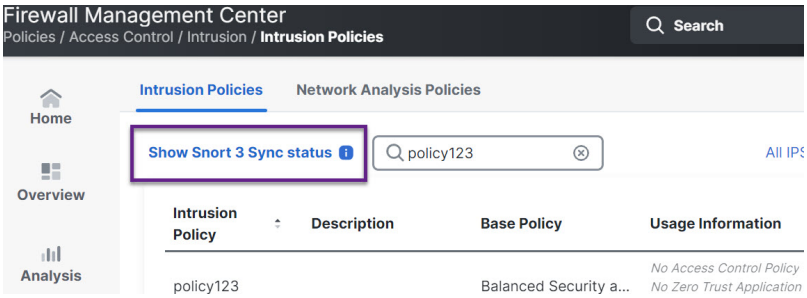
When intrusion policies display an orange arrow indicator, the Snort 2 and Snort 3 versions are not synchronized. The synchronization process uses the snort2Lua tool to convert rules and may require manual intervention for custom rules, thresholds, and suppressions that cannot be automatically migrated.

### Before you begin

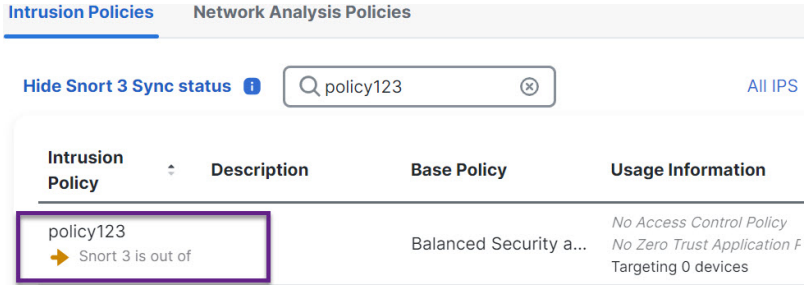
Follow these steps to convert Snort 2 rules of a single intrusion policy to Snort 3:

**Procedure**

1. Choose **Policies** > **Access Control heading** > **Intrusion** > **Intrusion Policies**.
   a) In the **Intrusion Policies** tab, click **Show Snort 3 Sync status**.

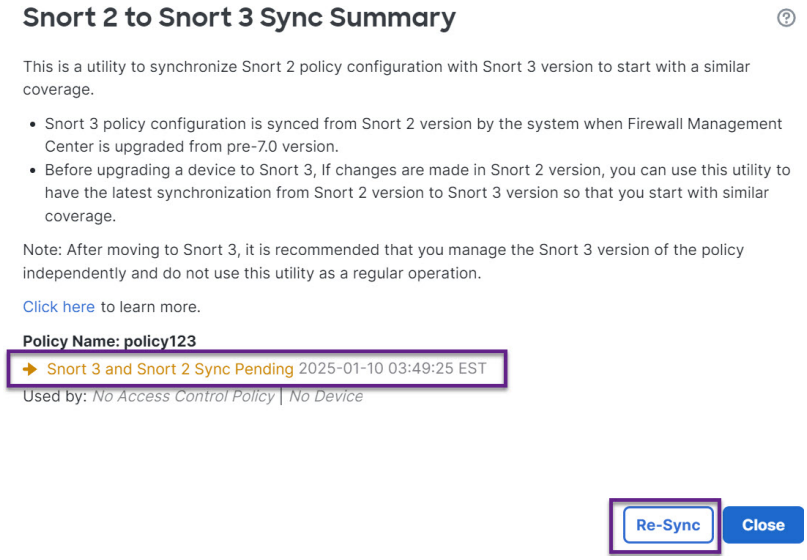



   If your policy displays an orange arrow, it indicates that the Snort 2 and the Snort 3 versions of the intrusion policy are not synchronized.




   b) Click the orange arrow.

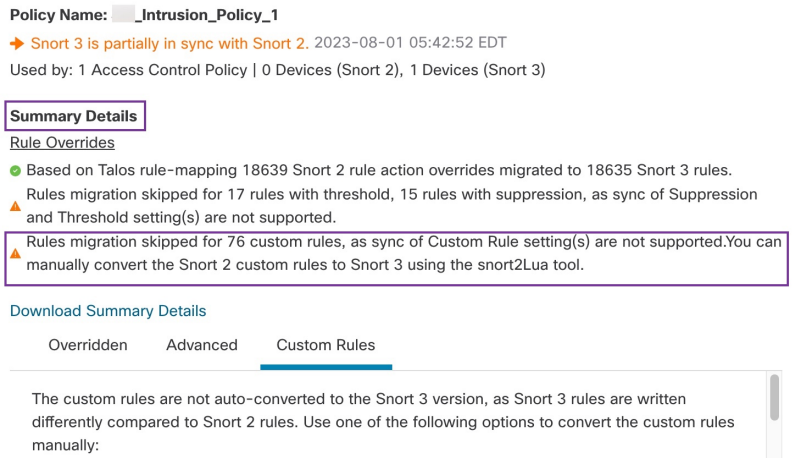
   The **Snort 2 to Snort 3 Sync Summary** page displays that the Snort 2 to Snort 3 sync is pending.



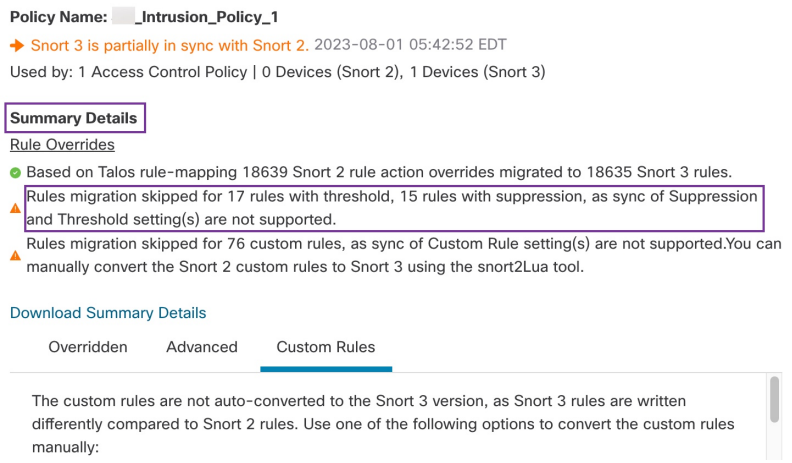

   c) Click **Re-Sync** to start the synchronization.

> **Note**
>
> When you click **Re-Sync**, the snort2Lua tool converts the rules from Snort 2 to Snort 3.

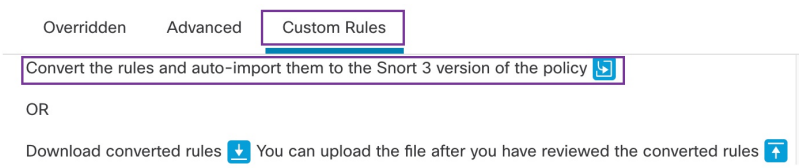
The **Summary Details** section lists the rules that were migrated or skipped. In our use case, there are 76 custom Snort 2 rules, 17 rules with thresholds, and 15 rules with suppression that were skipped during the sync process. To migrate the custom rules, go to the next step.




To migrate rules with thresholds and suppressions, go to Step 6.




2. To migrate the 76 custom rules, perform either one of these steps:
   - In the **Custom Rules** tab, click the **Import** icon to convert and auto-import the local rules to the Snort 3 version of the policy.

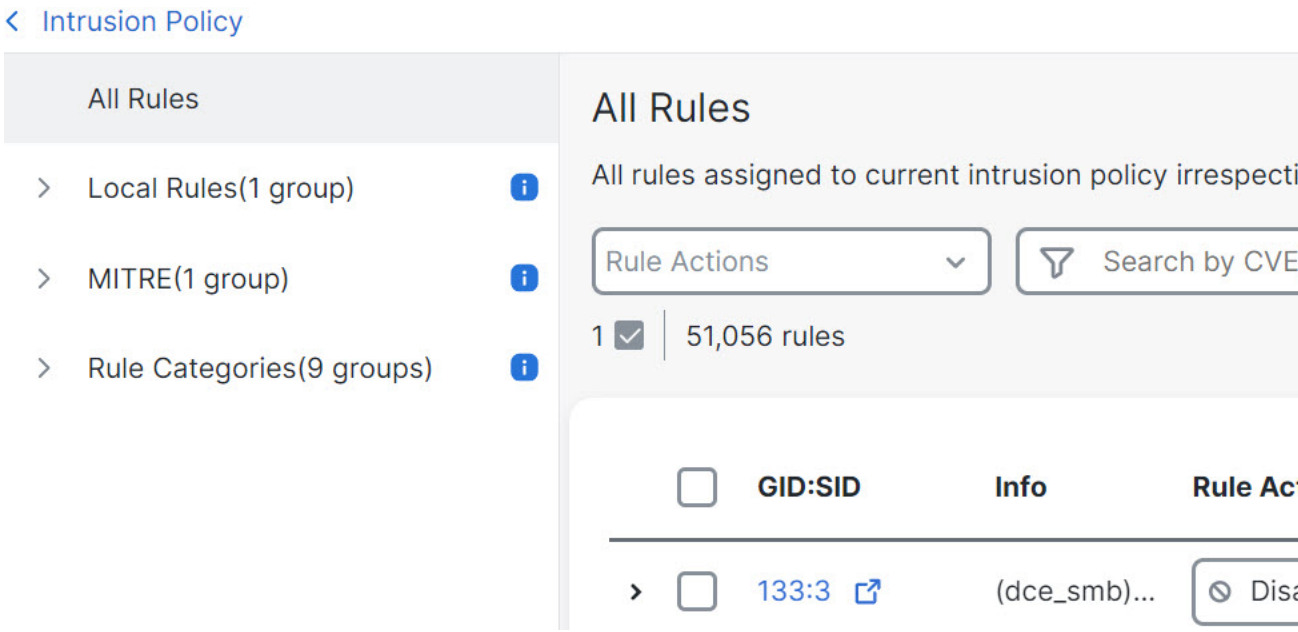



   A confirmation message is displayed after the rules are successfully imported.

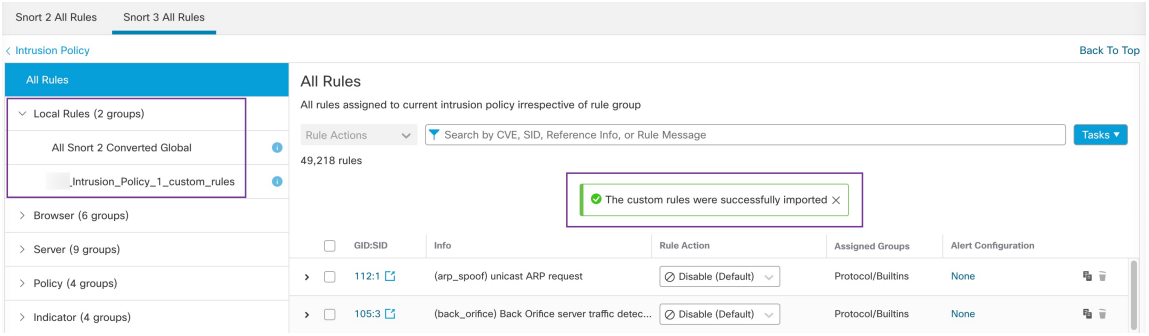
   - Choose **Objects** > **Intrusion Rules** and click **Snort 3 All Rules**.

**a.** Click **Local Rules** in the left panel to check if any rules have been migrated. Notice that no custom rules from Snort 2 have been migrated.

**b.** From the **Tasks** drop-down list, choose **Convert Snort 2 rules and import**.

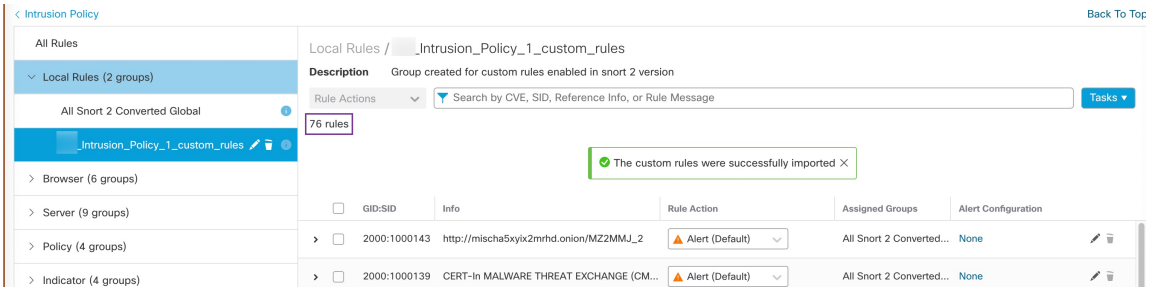



**c.** Click **OK**.




A rule group named (**All Snort 2 Converted Global**) is now created under **Local Rules** in the left panel.

Notice that all 76 custom rules have been migrated, as shown in the following figure.




Alternatively, you can select the **Convert Snort 2 rules and download** in the previous step to save the rules file locally. You can review the converted rules in the downloaded file and later upload them using the **Upload Snort 3 rules** option.

**3.** Click the **Download Summary Details** link to download the rules in .txt format.

This is a sample of the summary that is displayed.

**Example**


```
  "id": "00505691-15DC-0ed3-0000-004294988561",
  "name": "_Intrusion_Policy_1",
  "type": "IntrusionPolicy",
  "syncStatus": {
    "source": {
      "id": "bdce2d6a-1ebe-11ee-8e88-220032eb1fb5",
      "type": "IntrusionPolicy"
    },
    "status": "WARN",
    "description": "Migration is partially successful. Some of the rules are
 not copied to Snort3.",
    "timestamp": 1690883954814,
    "lastUser": {
      "name": "admin"
    },
    "details": [
      {
        "type": "Summary",
        "status": "INFO",
       "description": "Based on Talos rule-mapping 18639 Snort 2 rule action
 overrides migrated to 18635 Snort 3 rules."
      },
      {
        "id":
"1:1000156=alert,1:1000114=alert,1:1000160=alert,1:1000135=alert,1:1000115=alert,1:1000118=alert,

1:1000092=alert,1:1000139=alert,1:1000123=alert,1:1000159=alert,1:1000149=disabled,1:1000167=alert,

1:1000133=alert,1:1000095=alert,1:1000143=alert,1:1000106=alert,1:1000153=alert,1:1000097=alert,1:1000141=alert,

1:1000148=alert,1:1000090=alert,1:1000119=alert,1:1000112=alert,1:1000138=alert,1:1000128=alert,1:1000132=alert,

1:1000134=alert,1:1000145=disabled,1:1000110=disabled,1:1000107=alert,1:1000163=alert,1:1000124=alert,1:1000125=alert,

1:1000094=alert,1:1000113=disabled,1:1000147=alert,1:1000161=alert,1:1000105=disabled,1:1000140=alert,1:1000111=alert,

1:1000102=alert,1:1000129=disabled,1:1000108=alert,1:1000144=disabled,1:1000088=alert,1:1000091=alert,1:1000131=alert,

1:1000157=alert,1:1000120=alert,1:1000126=alert,1:1000165=alert,1:1000146=alert,1:1000162=alert,1:1000116=alert,1:1000142=alert,

1:1000170=disabled,1:1000169=alert,1:1000104=alert,1:1000099=disabled,1:1000171=alert,1:1000093=alert,1:1000087=alert,1:1000100=alert,

1:1000137=alert,1:1000158=alert,1:1000103=alert,1:1000098=alert,1:1000127=disabled,1:1000130=alert,1:1000164=alert,1:1000089=alert,

1:1000109=alert,1:1000136=alert,1:1000117=alert,1:1000166=alert,1:1000168=alert",

        "type": "PolicyInfo",
       "description": "Corresponding Snort 2 policy overridden custom (local)
 rules."
      },
      {
```

```
        "type": "AssignedDevices",
        "status": "INFO",
        "description": "Snort3:0 , Snort2:0"
      },
      {
        "id": "122:6",
        "type": "Threshold",
        "status": "ERROR",
        "description": "PSNG_TCP_FILTERED_DECOY_PORTSCAN"
      },
      {
        "id": "122:15",
        "type": "Threshold",
        "status": "ERROR",
        "description": "PSNG_IP_PORTSWEEP_FILTERED"
       },
      {
        "id": "122:1",
        "type": "Threshold",
        "status": "ERROR",
        "description": "PSNG_TCP_PORTSCAN"
      },
```


4. Click **Close** to close the **Sync Summary** dialog box.
5. To check the rules with status: ERROR, choose **Policies** > **Access Control heading** > **Intrusion** and click the **Snort 2** version of the intrusion policy.
6. Under **Policy Information**, click **Rules** and filter for the rule. For example, enter **PSNG_TCP_PORTSCAN** in the **Filter**field to find the rule.
7. Click **Show Details** to view the detailed version of the rule.
8. Create the rule again in Snort 3 using Snort 3 rule guidelines and save the file as a .txt or .rules file. For more information, see www.snort3.org.
9. Upload the custom rule that you just created locally to the list of all the Snort 3 rules. See Add Custom Rules to Rule Groups.

---

### What to do next

Deploy configuration changes. See Deploy configuration changes on page 37.

# 3 Intrusion Policies

**Topics:**


- Intrusion policies
- Create a custom snort 3 intrusion policy
- Edit Snort 3 Intrusion Policies
- Change the base policy of an intrusion policy
- View Snort 2 and Snort 3 base policy mapping
- Synchronize Snort 2 rules with Snort 3
- Manage intrusion policies
- Access control rule configuration to perform intrusion prevention
- Tune Intrusion Policies using Rules
- Recommended rules
- Mitigate threats using MITRE framework in Snort 3 intrusion policies


Learn how to manage Snort 3 intrusion policies and configure access control rules for effective intrusion detection and prevention.

This chapter provides information on managing Snort 3 intrusion policies and access control rule configurations for intrusion detection and prevention.

# Intrusion policies

Describes defined sets of intrusion detection and prevention configurations that inspect traffic for security violations and can block or alter malicious traffic in inline deployments.

An *intrusion policy* is a defined set of intrusion detection and prevention configurations that

- inspects traffic for security violations,
- can block or alter malicious traffic in inline deployments, and
- serves as 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 Secure Firewall 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.

By default, the system disables intrusion inspection of encrypted payloads. This default reduces false positives and improves performance when an encrypted connection matches an access control rule with intrusion inspection enabled.

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

## Create a custom snort 3 intrusion policy

Configure a custom Snort 3 intrusion policy to define how the system inspects and responds to network intrusions.

Create a custom Snort 3 intrusion policy to tailor intrusion detection and prevention settings to your network security requirements.

Snort 3 intrusion policies define how the system inspects traffic and responds to potential threats. You can create custom policies based on existing system-provided policies or other custom policies to meet specific security needs.

### Before you begin

Follow these steps to create a custom Snort 3 intrusion policy:

#### Procedure

1. Choose **Policies** > **Access Control heading** > **Intrusion**.
2. Click **Create Policy**.
3. Enter a unique **Name** and, optionally, a **Description**.
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 many false positives.

5. Choose the **Base Policy**.

   You can use either a system-provided policy or an existing policy as your base policy.

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 52.

# Edit Snort 3 Intrusion Policies

Edit and configure Snort 3 intrusion policies.

Use this task to understand how to access, modify, and manage Snort 3 intrusion policies in the Firewall Management Center, including editing policy settings, managing rule groups, and applying recommendations to protect your network.

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

**Before you begin**

-

**Procedure**

1. Choose **Policies** > **Access Control heading** > **Intrusion** .
2. Ensure the **Intrusion Policies** tab is selected.
3. Click **Snort 3 Version** next to the intrusion policy you want to configure.
4. Edit your policy:
   - Change the mode–Click the **Mode** drop-down to change the inspection mode.

   > **Caution**
   >
   > The inspection mode is changed only for the Snort 3 version of the policy. The existing inspection mode is retained in the Snort 2 version as is, which means that your Snort 2 and Snort 3 versions of the policy will have different inspection modes. We recommend that you use this option with caution.

   - **Prevention** –Triggered Block rules create an event (alert) and drop the connection.
   - **Detection** –Triggered Block rules create an alert.

     You can choose the detection mode before going for prevention. For example, before choosing the prevention mode, you might want block rules to alert only, so that you can identify rules that cause a lot of false positives.

5. Click the **Base Policy** layer that defines the intrusion policy's default settings.
   - Search rules–Use the search field to filter the display. You can enter the GID, SID, rule message, or reference info. For example, GID:1; SID:9621–to display only rule 1:962, SID:9621,9622,9623–to display multiple rules with different SIDs. You can also click inside the Search text box to choose any of the following options:
     - apply the filters **Action = Alert** , or **Action: Block**
     - apply the **Disabled Rules** filter
     - show **Custom/User Defined Rules**
     - filter by GID, SID, or GID:SID
     - filter by CVE
     - filter by comment
   - View filtered rules–Click any of the **Presets** to view rules that are set to alert, block, disabled, and so on.

Overridden rules indicate the rules where the rule action has been changed from the default action to a different action. Note that, once changed, the rule action status is Overridden even if you change it back to its original default action. However, if you select **Revert to default** from the **Rule Action** drop-down list, the Overridden status is removed.

**Advanced Filters** provides filter options based on the Lightweight Security Package (LSP) releases, Classifications of intrusions, and Microsoft Vulnerabilities.

- View rule documentation–Click the rule ID or the **Rule Documentation** icon to display Talos documentation for the rule.
- View a rule details–Click the **Expand Arrow** (>) icon in a rule row to view the rule details.
- Add rule comments–Click **Comment** (💬) under the Comments column to add comments for a rule.

6. **Group Overrides** –Click the **Group Overrides** layer that lists all the categories of rule groups. The top-level parent rule group with Description, Overrides, Enabled Groups, and other details is displayed. Parent rule groups cannot be updated and are read-only. Only the leaf rule groups can be updated. In each rule group, you can traverse up to the last leaf group. Across each group, you can override, include, and exclude rule groups. In the leaf rule groups, you can:
   - Search rule groups–Use the search field to enter keywords and search for rule groups.
   - In the left panel, you can choose any of the preset filter options to search for rule groups:
     - All–For displaying all rule groups.
     - Excluded–For excluded groups.
     - Included–For included groups.
     - Overridden–For rule group configuration that is overridden.
   - Set the security level for a rule group–Navigate to the required rule group on the left pane and click it. Click **Edit** next to the **Security Level** of the rule group to increase or decrease the security level based on system-defined rule settings.

     In the **Edit Security Level** dialog box, you have the option to click **Revert to Default** , which reverts the changes you made.

     The Firewall Management Center automatically changes the action for the rules of the rule group for the configured security level. In the **Rule Overrides** layer, notice the count of Block Rules and Disabled Rules in the **Presets** every time you change the security level.
   - You can make bulk changes to the security level to change the security level of all rule groups within a particular rule category. Bulk security level applies to rule groups that have more than one rule group. After a bulk update of rule groups, you can still update the security level of any of the associated rule groups within it.

     There can be **mixed** security levels within rule groups; **mixed** indicates that the child groups contain a mix of security levels within the parent rule group.
   - Include or exclude rule groups–The rule groups displayed are the default rule groups associated with the system-provided base intrusion policy. You can include and exclude rule groups from the intrusion policy. An excluded rule group is removed from the intrusion policy and its rules are not applied on the traffic. For information on uploading custom rules in Firewall Management Center , see Add custom rules to rule groups on page 76 .

     To exclude a rule group:

     a. Navigate the Rule Groups pane and choose the rule group that you want to exclude.

     b. Click the **Exclude** hyperlink on the right-pane.

     c. Click **Exclude** .

To include a new rule group or multiple rule groups with the uploaded custom rules or a previously excluded rule group:

a. Click **Add** (+) next to the rule group filter dropdown list.

b. Choose all the rule groups you want to add by checking the check box next to it.

c. Click **Save** .

- For a leaf rule group, click the icon under the **Override** column header to see the rule action trail, which describes the sequence of overridden rule actions that can be assigned due to the base policy and group overrides for an intrusion rule. Rule actions can be obtained from either the base policy configurations or the user group override. The user group override takes the priority between the two; priority refers to the final overridden action that is assigned to the rule group.
- Click the rule count (number) under the **Rule Count** column header to see a summary of rules that are part of the rule group.

7. **Recommendations** –Click the **Recommendations** layer if you want to generate and apply Cisco recommended rules. Recommendations use the host database to enable or disable rules, based on known vulnerabilities.
8. **Rule Overrides** –Click the **Rule Overrides** layer to choose any of the presets to view rules, which are set to alert, block, disabled, overridden, rewrite, pass, drop, or reject.
   - The **Set By** column shows the default set by state (Base Policy) or modified rule state by Group Overrides, Rule Overrides, or Recommendations. The **Set By** column in **All Rules** (in the left pane) shows the trail of rule action override actions based on priority order. The priority order of rule actions is Rule Override > Recommendations > Group Override > Base Policy.
   - Modify **Rule Action** –To modify rule actions, choose either of the following:
     - Bulk edit–Choose one or more rules, then choose the required action from the **Rule Action** drop-down list; and click **Save** .

       **Note**

       Bulk rule action changes are supported only for the first 500 rules.

     - Single rule edit–Choose the action for the rule from the drop-down list in the **Rule Action** column.

   Rule actions are:

   - **Block** – Generates event, blocks current matching packet and all the subsequent packets in this connection.
   - **Alert** – Generates only events for matching packet and does not drop packet or connection.
   - **Disable** –Does not match traffic against this rule. No events are generated.
   - **Revert to default** –Reverts to the system default action.
   - **Pass** – No events are generated, allows packet to pass without further evaluation by any subsequent Snort rules.

> **Note**
>
> The Pass action is available only for custom rules and not for system-provided rules.

- **Drop** – Generates event, drops matching packet and does not block further traffic in this connection.
- **Reject** – Generates event, drops matching packet, blocks further traffic in this connection and sends TCP reset if it is a TCP protocol to source and destination hosts.

  *Behavior of reject in different firewall modes and IP address or source or destination in relation to Client or Server* : Snort sends RST packets to both client and server in cases of routed, inline, and bridged interfaces. Snort sends two RST packets. The RST packet in the client's direction will have the source set to the server's IP and the destination set to client's IP. The RST packet in the server's direction will have the source set to the client's IP and the destination set to the server's IP.
- **Rewrite** – Generates event and overwrites packet contents based on the replace option in the rule.

For IPS rule action logging, see Rule action logging on page 56 .

If there is a **React** rule, it is converted to an alert action.

9. Click the **Summary** layer for a holistic view of the current changes to the policy. The policy summary page contains the following information:
   - Rule distribution of the policy, that is, active rules, disabled rules, and similar categories.
   - Option to export policy and generate report of the intrusion policy.
   - Base policy details.
   - Option to generate recommendations.
   - Group overrides list the groups you have overridden.
   - Rule overrides that shows the list of rules that you have overridden.
   - In the **Summary** layer, click the ? icon to open a pop-up window that explains the Snort layering concepts.

   To change the base policy, see Change the base policy of an intrusion policy on page 57 .

   > **Note**
   >
   > You can navigate to **Objects** > **Intrusion Rules** and click the **Snort 3 All Rules** tab and traverse through all the intrusion rule groups. The parent rule group lists the associated child groups and rule count.

---

**What to do next**

Deploy configuration changes. See Deploy configuration changes on page 37 .

## Rule group reporting

Describes how rule groups are reflected in intrusion events with MITRE tactics and techniques.

Rule group reporting feature reflects rule groups in generated intrusion events, includes MITRE tactics and techniques identification, and provides dedicated columns for both MITRE and non-MITRE rule groups in intrusion event displays.

To view the intrusion events in Firewall Management Center, choose **Analysis** > **Unified Events**. In the **Unified Events** page, explicitly enable the **MITRE ATT&CK** column for rule group reporting.

Alternatively, you can also go to the **Intrusion Events** page to view intrusion events. Choose **Analysis** > **Intrusions** > **Events** to access the **Intrusion Events** page. These fields are added in the **Intrusion Events** page for rule group reporting. Note that you must explicitly enable the mentioned columns:

- MITRE ATT&CK
- Rule Group

For information about these fields, see the section *Intrusion Event Fields* in the *Cisco Secure Firewall Management Center Administration Guide, 7.3*.

## Rule action logging

Lists the events displayed in the Inline Result column for different IPS actions in intrusion event windows.

From Firewall Management Center 7.2.0 onwards, in the **Intrusion Events** window, the event in the **Inline Result** column displays the same name as the IPS action applied to the rule, so that you can see the action that was applied on the traffic matching the rule.

For the IPS actions, the tables show the events that are displayed in the **Inline Result** column of the **Intrusion Events** window and **Action** column for **Intrusion Event Type** in the **Unified Events** window.

| IPS Action for Snort 3 | Inline Result - Firewall Management Center 7.1.0 and earlier | Inline Result -Firewall Management Center 7.2.0 onwards |
|---|---|---|
| Alert | Pass | Alert |
| Block | Dropped/Would Have Dropped/Partially Dropped | Block/Would Block/Partial Block |
| Drop | Dropped/Would have dropped | Drop/Would drop |
| Reject | Dropped/Would have dropped | Reject/Would reject |
| Rewrite | Allow | Rewrite |

**Important**

- In case of a rule without the "Replace" option, the **Rewrite** action is displayed as **Would Rewrite**.
- The **Rewrite** action would also be displayed as **Would Rewrite** if the "Replace" option is specified, but the IPS policy is in Detection mode or the device is in Inline-TAP or Passive mode.

> **Note**
>
> In case of backward compatibility (Firewall Management Center 7.2.0 managing a Firewall Threat Defense 7.1.0 device), the events mentioned are applicable only to the Alert IPS action where **Pass** is displayed as **Alert** for events. For all the other actions, the events for Firewall Management Center 7.1.0 are applicable.

## Change the base policy of an intrusion policy

Configure a different system-provided or custom policy as the base policy for an intrusion policy.

Change the base policy to use a different system-provided or custom policy as the foundation for your intrusion policy configuration.

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.

### Procedure

1. Choose **Policies** > **Access Control heading** > **Intrusion**.
2. Click **Edit** (✎) next to the intrusion policy you want to configure.
3. Choose a policy from the **Base Policy** drop-down list.
4. Click **Save**.

### What to do next

Deploy configuration changes. See Deploy configuration changes on page 37.

## View Snort 2 and Snort 3 base policy mapping

View the Snort 3 to Snort 2 intrusion policy mapping in the management center.

This task allows you to view the mapping between Snort 3 and Snort 2 intrusion policies.

> **Note**
>
> Snort 2 is not supported on threat defense version 7.7. For information on Snort 2 features that are supported in versions earlier than 7.7, refer to the Firewall Management Center guide that matches your Firewall Threat Defense version.

### Procedure

1. Choose **Policies** > **Access Control heading** > **Intrusion**.
2. Ensure the **Intrusion Policies** tab is selected.

3. Click **IPS Mapping**.
4. In the **IPS Policy Mapping** dialog box, click **View Mappings** to view the Snort 3 to Snort 2 intrusion policy mapping.
5. Click **OK**.

## Synchronize Snort 2 rules with Snort 3

Configure synchronization to retain Snort 2 version settings and custom rules when moving to Snort 3, ensuring similar coverage between versions.

This task helps ensure that Snort 2 rule override settings and custom rules are replicated on Snort 3, allowing you to start with similar coverage when transitioning between versions.

To ensure that the Snort 2 version settings and custom rules are retained and carried over to Snort 3, the Firewall Management Center provides the synchronization functionality. Synchronization helps Snort 2 rule override settings and custom rules, which you may have altered and added over the last few months or years, to be replicated on the Snort 3 version. This utility helps to synchronize Snort 2 version policy configuration with Snort 3 version to start with similar coverage.

**Note**

Snort 2 is not supported on threat defense Version 7.7. For information on Snort 2 features that are supported in versions earlier than 7.7, refer to the Firewall Management Center guide that matches your Firewall Threat Defense version.

If the Firewall Management Center is upgraded from 6.7 or earlier to 7.0 or later version, the system synchronizes the configuration. If the Firewall Management Center is a fresh 7.0 or later version, you can upgrade to a higher version, and the system will not synchronize any content during upgrade.

Before upgrading a device to Snort 3, if changes are made in Snort 2 version, you can use this utility to have the latest synchronization from Snort 2 version to Snort 3 version so that you start with a similar coverage.

**Note**

When you move to Snort 3, manage the Snort 3 version of the policy independently. Do not use this utility as a regular operation.

**Important**

- Only the Snort 2 rule overrides and custom rules are copied to Snort 3 and not the other way around. You may not find a one-to-one mapping of all the intrusion rules in Snort 2 and Snort 3. Your changes to rule actions for rules that exist in both versions are synchronized when you perform the following procedure.
- Synchronization *does not* migrate the threshold and suppression settings of any custom or system-provided rules from Snort 2 to Snort 3.

**Procedure**

1. Choose **Policies** > **Access Control heading** > **Intrusion**.
2. Ensure the **Intrusion Policies** tab is selected.
3. Click **Show Snort 3 Sync status**.
4. Identify the intrusion policy that is out-of-sync.
5. Click the **Sync** icon **Snort out-of-Sync** (🔶).

   **Note**

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

6. Read the summary. Download a copy of the summary if required.
7. Click **Re-Sync**.

   **Note**

   - The synchronized settings will be applicable on the Snort 3 intrusion engine only if it is applied on a device, and after a successful deployment.
   - Snort 2 custom rules can be converted to Snort 3 with the system-provided tool. If you have any Snort 2 custom rules, click the Custom Rules tab and follow the on-screen instructions to convert the rules. For more information, see Convert Snort 2 custom rules of a single intrusion policy to Snort 3 on page 34.

**What to do next**

Deploy configuration changes. See Deploy configuration changes on page 37.

## Manage intrusion policies

Configure intrusion policies through creation, deletion, editing, export, deployment, and reporting functions on the Intrusion Policy window.

This task enables you to perform comprehensive management operations on your intrusion policies including creation, modification, deletion, export, deployment, and reporting.

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

- The number of access control policies and devices using the intrusion policy to inspect traffic.
- Indicates the domain where the policy was created in a multidomain deployment.

> **Note**
>
> Snort 2 is not supported on threat defense version 7.7. For information on Snort 2 features that are supported in versions earlier than 7.7, refer to the Firewall Management Center guide that matches your Firewall Threat Defense version.

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.

**Procedure**

1. Choose **Policies** > **Access Control heading** > **Intrusion**.
2. Manage your intrusion policy:
   - Create – Click **Create Policy**; see Create a custom snort 3 intrusion policy on page 51.
   - 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 52.
   - Export – If you want to export an intrusion policy to import on another Firewall Management Center, click Export; see the *Exporting Configurations* topic in the latest version of the *Cisco Secure Firewall Management Center Configuration Guide*.
   - Deploy – Choose **Deploy** > **Deployment**; see Deploy configuration changes on page 37.
   - Report – Click **Report**; see the *Generating Current Policy Reports* topic in the latest version of the *Cisco Secure Firewall Management Center Configuration Guide*. Generates two reports, one for each policy version.

## Access control rule configuration to perform intrusion prevention

Describes how access control policies can have multiple access control rules associated with intrusion policies to provide different intrusion inspection profiles for different types of network traffic.

An access control rule configuration to perform intrusion prevention is a security mechanism that

- enables multiple access control rules within an access control policy to be associated with intrusion policies,
- permits intrusion inspection for Allow or Interactive Block access control rules to match different intrusion inspection profiles against different types of traffic, and
- evaluates traffic before it reaches its final destination on the network.

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.

#### 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

Describes the relationship between intrusion policies and access control policy configuration on target devices.

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.

## Configure an access control rule to perform intrusion prevention

Configure an access control rule with intrusion prevention to inspect and protect network traffic.

Configure an access control rule to enable intrusion prevention inspection on network traffic, allowing you to detect and prevent malicious activities based on intrusion signatures and policies.

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

Follow these steps to configure an access control rule to perform intrusion prevention:

#### Procedure

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 *Cisco Secure Firewall Management Center Configuration Guide*.
2. Ensure the rule action is set to **Allow**, **Interactive Block**, or **Interactive Block with reset**.
3. Click **Inspection**.
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.
5. If you want to change the variable set associated with the intrusion policy, choose a value from the **Variable Set** drop-down list.
6. Click **Save** to save the rule.
7. Click **Save** to save the policy.

#### What to do next

Deploy configuration changes. See Deploy configuration changes on page 37.

# Tune Intrusion Policies using Rules

Describes how to tune intrusion policies using custom rules in Snort 3, including rule actions, event notification filters, converting Snort 2 rules, and adding rule groups to policies.

This section provides information on custom rules in Snort 3, intrusion rule action, intrusion event notification filters in an intrusion policy, converting Snort 2 custom rules to Snort 3, and adding rule groups with custom rules to an intrusion policy.

## Tuning intrusion rules

Describes how to configure rule states and other settings for shared object rules, standard text rules, and inspector rules.

Tuning intrusion rules is a configuration process that

- enables rule state modification for shared object rules, standard text rules, and inspector rules,
- controls event generation and traffic processing based on rule configuration, and
- allows filtering of rules to display specific subsets for targeted configuration changes.

#### Rule state configuration

You enable a rule by setting its rule state to Alert or to Block. Enabling a rule causes the system to generate events on traffic matching the rule. Disabling a rule stops processing of the rule. You can also set your intrusion policy so that a rule set to Block generates events on, and drops, matching traffic.

You can filter rules to display a subset of rules, enabling you to select the exact set of rules where you want to change rule states or rule settings.

When an intrusion rule or rule argument requires a disabled inspector, the system automatically uses it with its current configuration even though it remains disabled in the web user interface (UI) of the network analysis policy.

> **Note**
>
> We recommend that you do not modify shared object rules and you only enable or disable these rules for your threat defense device. To create custom Snort rules, contact Cisco support.

## Intrusion rule types

Describes the different types of intrusion rules used by the system to detect network vulnerabilities.

An intrusion rule is a specified set of keywords and arguments that the system uses to detect attempts to exploit vulnerabilities in your network. As the system analyzes network traffic, it compares packets against the conditions specified in each rule, and triggers the rule if the data packet meets all the conditions specified in the rule.

- *intrusion rules*, which are subdivided into *shared object rules* and *standard text rules*
- *inspector rules*, which are associated with a detection option of the packet decoder or with one of the inspectors included with the system.

#### Rule type attributes and characteristics

This table summarizes attributes of these rule types:

**Table 2: Intrusion rule types**

| Type | Generator ID (GID) | Snort ID (SID) | Source | Can Copy? | Can Edit? |
|---|---|---|---|---|---|
| shared object rule | 3 | lower than 1,000,000 | Cisco Talos Intelligence Group (Talos) | yes | limited |
| standard text rule | 1 (Global domain or legacy GID) | lower than 1,000,000 | Talos | yes | limited |
| | 1,000-2,000 (descendant domain) | 1,000,000 or higher | Created or imported by user | yes | yes |
| preprocessor rule | decoder- or preprocessor-specific | lower than 1,000,000 | Talos | no | no |
| | | 1,000,000 or higher | Generated by the system during option configuration | no | no |

You cannot save changes to any rule created by Talos, but you can save a copy of a modified rule as a custom rule. You can modify either variables used in the rule or rule header information (such as source and destination ports and IP addresses). In a multidomain deployment, rules created by Talos belong to the Global domain. Administrators in descendant domains can save local copies of the rules, which they can then edit.

For the rules it creates, Talos assigns default rule states in each default intrusion policy. Most preprocessor rules are disabled by default and must be enabled if you want the system to generate events for preprocessor rules and, in an inline deployment, drop offending packets.

## Custom rules in Snort 3

Explains custom intrusion rules in Snort 3 that enable detection of specific network threats and sensitive data through imported rule files and pattern matching.

A custom rule in Snort 3 is an intrusion detection rule that

- enables users to create custom threat detection by importing local rule files with `.txt` or `.rules` extensions,
- belongs to rule groups and can be included in multiple groups simultaneously, and
- receives a unique rule number in `GID:SID:Rev` format with system-generated identifiers.

#### Rule number format

When you create a custom intrusion rule, the system assigns it a unique rule number, which has the format `GID:SID:Rev`. The elements of this number are:

- **GID**–Generator ID. For custom rules, it is not necessary to specify the GID. The system automatically generates the GID based on whether you are in the Global domain or a sub-domain while uploading the rules. For all standard text rules, this value is 2000 for a Global domain.

- **SID**–Snort ID. Indicates whether the rule is a local rule of a system rule. When you create a new rule, assign a unique SID to the rule.

  SID numbers for local rules start at 1,000,000, and the SID for each new local rule is incremented by one.

- **Rev**–The revision number. For a new rule, the revision number is one. Each time you modify a custom rule the revision number should be incremented by one.

In a custom standard text rule, you set the rule header settings and the rule keywords and arguments. You can use the rule header settings to focus the rule to only match traffic using a specific protocol and traveling to or from specific IP addresses or ports.

To check whether a SID is enabled or disabled, verify the entries in the snort.lua file located in the `./file-contents/ngfw/var/sf/detection_engines/<ID>/IPS/<ID>` directory.

- If the SID is disabled by default, no entry will be present in the file.
- If the SID is manually enabled, you will see an entry with **enable:yes**.
- If the SID is disabled after being manually enabled, the entry remains in the file and will display **enable:no**.

**Note**

- Snort 3 custom rules cannot be edited. Ensure that custom rules have a valid classification message for `classtype` within the rule text. If you import a rule without a classification or with an incorrect classification, delete and recreate the rule.
- You can create custom intrusion rules using Snort 3. However, support for tuning and troubleshooting these rules is currently not available.
- The *classtype* in a Snort rule assigns a classification to the rule indicating the type of attack that is associated with an event. A priority level of 1-4 is also associated with each *classtype*. However, the priority level for certain *classtypes* on the Threat Defense device do not match the open-source Snort *classtype* priority levels that are mentioned in the Snort documentation. For example, *tcp-connection* has a priority of 4 in open-source Snort while a priority of 3 is assigned to it on the Threat Defense device.

### Sensitive data detection

Sensitive data such as social security numbers, credit card numbers, emails, and so on may be leaked onto the internet, intentionally or accidentally. Sensitive data detection is used to detect and generate events on possible sensitive data leakage. Events are generated only when a significant amount of Personally Identifiable Information (PII) is transferred. Sensitive data detection can mask PII in the output of events.

Use the `sd_pattern` IPS option to detect and filter PII. This information includes credit card numbers, U.S. Social Security numbers, phone numbers, and email addresses. A regular expression (regex) syntax is available for defining your own PII.

The sd_pattern option has the following settings:

- Pattern–An implicit, required setting that specifies the regular expression to look for in the PDU. The regex must be written in PCRE syntax.
- Threshold–An explicit, optional setting that specifies the number of matches in the PDU required to generate an event.

  The `sd_pattern` as IPS rule option is available in Snort with no requirements for additional inspectors. The syntax for the rule option is:

  ```
  sd_pattern: "<pattern>"[, threshold <count>];
  ```

For example:

```
sd_pattern:"credit_card", threshold 2;
```

There are five built-in patterns for sensitive data. To use the built-in patterns in the "pattern" setting, you must specify the name of the PII type that needs to be matched and the necessary regex is substituted for it. The PII name and regex mappings or patterns are described here:

**Table 3: Built-in patterns**

| PII Name | Pattern |
|---|---|
| credit_card | `\d{4}\D?\d{4}\D?\d{2}\D?\d{2}\D?\d{3,4}` |
| us_social | `[0-8]\d{2}-\d{2}-\d{4}` |
| us_social_nodashes | `[0-8]\d{8}` |
| Email | `[a-zA-Z0-9!#$%&'*+\/=?^_`{\|}~-]+(?:\.[a-zA-Z0-9!#$%&'*+\/=?^_`{\|}~-]+)*@(?:[a-zA-Z0-9](?:[a-zA-Z0-9-]*[a-zA-Z0-9])?\.)+[a-zA-Z0-9](?:[a-zA-Z0-9-]*[a-zA-Z0-9])?` |
| us_phone | `(?:\+?1[-\.\s]?)?\(?([2-9][0-8]\d)\)?[-\.\s]([2-9]\d{2})[-\.\s](\d{4})` |

Masking for data matching these patterns only work with system-provided rules or built-in patterns for Credit Cards, U.S. Social Security numbers, emails, and U.S. phone numbers. Masking does not work for custom rules or user-defined PII patterns. Rules are available in the Lightweight Security Package (LSP) for sensitive data, gid:13. By default, they are not enabled in any system-provided policy.

The sensitive data rules in LSP cover all built-in patterns and have the following threshold values:

- credit_card: 2
- us_social: 2
- us_social_nodashes: 20
- email: 20
- us_phone: 20

You can use the sd_pattern option to create custom rules and modify existing rules. To do this, use the Snort 3 intrusion policy interface.

An example of a rule with sd_pattern with a custom pattern and threshold:

*alert tcp (sid: 1000000001; sd_pattern:"[\w-\.]+@([\w-]+\.)+[\w-]{2,4}",threshold 4; msg: "email, threshold 4")*

**Examples**

An example of custom rules using sensitive data detection:

Rule with built-in pattern

```
alert tcp (
        msg:"SENSITIVE-DATA Email";
        flow:only_stream;
        pkt_data;
```

```
        sd_pattern:"email", threshold 5;
        service:http, smtp, ftp-data, imap, pop3;
        gid:2000;
        sid:1000001;
)
```

Rule with custom pattern

```
alert tcp (
        msg:"SENSITIVE-DATA US phone numbers";
        flow:only_stream;
        file_data;
       sd_pattern:"+?3?8?(0[\s\.-]\d{2}[\s\.-]\d{3}[\s\.-]\d{2}[\s\.-]\d{2})",
 threshold 2;
        service:http, smtp, ftp-data, imap, pop3;
        gid:2000;
        sid:1000002;
)
```

Here are some more examples of complete Snort IPS rules with built-in sensitive data patterns:

- alert tcp ( sid:1; msg:"Credit Card"; sd_pattern:"credit_card", threshold 2; )
- alert tcp ( sid:2; msg:"US Social Number"; sd_pattern:"us_social", threshold 2; )
- alert tcp ( sid:3; msg:"US Social Number No Dashes"; sd_pattern:"us_social_nodashes", threshold 2; )
- alert tcp ( sid:4; msg:"US Phone Number"; sd_pattern:"us_phone", threshold 2; )
- alert tcp ( sid:5; msg:"Email"; sd_pattern:"email", threshold 2; )

Disabling data masking is not supported in the Secure Firewall Management Center, and Secure Firewall Device Manager.

For information on how to add custom rules to rule groups, see Add custom rules to rule groups on page 76.

## View Snort 3 intrusion rules in an intrusion policy

View Snort 3 intrusion rules in an intrusion policy and adjust how rules are displayed.

This task allows you to view and interact with Snort 3 intrusion rules within an intrusion policy, enabling you to manage rule display settings and access detailed rule information.

You can adjust how rules are displayed in the intrusion policy. You can also display the details for a specific rule to see rule settings, rule documentation, and other rule specifics.

### Procedure

1. Choose **Policies** > **Access Control heading** > **Intrusion**.
2. Click **Snort 3 Version** next to the policy.
3. While viewing the rules, you can:
   - Filter the rules.
   - Choose a rule group to see rules related to that group.
   - View an intrusion rule's details.
   - View rule comments.
   - View rule documentation.

   See Edit Snort 3 Intrusion Policies on page 52 for details on performing these tasks.

# Intrusion rule actions

Describes how intrusion rule actions control rule behavior within intrusion policies and specify system responses to monitored conditions.

An intrusion rule action is a policy configuration mechanism that

- enables or disables rules within individual intrusion policies,
- specifies which action the system takes if monitored conditions trigger the rule, and
- inherits default actions from the base policy used during intrusion policy creation.

### Default action behavior

The Cisco Talos Intelligence Group (Talos) sets the default action of each intrusion and inspector rule in each default policy. For example, a rule may be enabled in the Security over Connectivity default policy and disabled in the Connectivity over Security default policy. Talos sometimes uses a rule update to change the default action of one or more rules in a default policy. If you allow rule updates to update your base policy, you also allow the rule update to change the default action of a rule in your policy when the default action changes in the default policy you used to create your policy (or in the default policy it is based on). Note, however, that if you have changed the rule action, the rule update does not override your change.

When you create an intrusion rule, it inherits the default actions of the rules in the default policy you use to create your policy.

### Intrusion rule action options

Lists the available rule action values that can be set in an intrusion policy.

In an intrusion policy, you can set a rule's action to specific values that determine how the system responds to matching traffic.

#### Alert

You want the system to detect a specific intrusion attempt and generate an intrusion event when it finds matching traffic. When a malicious packet crosses your network and triggers the rule, the packet is sent to its destination and the system generates an intrusion event. The malicious packet reaches its target, but you are notified through the event logging.

#### Block

You want the system to detect a specific intrusion attempt, drop the packet containing the attack, and generate an intrusion event when it finds matching traffic. The malicious packet never reaches its target, and you are notified through the event logging.

#### Disable

You do not want the system to evaluate matching traffic.

**Note**

Choosing either the **Alert** or **Block** options enables the rule. Choosing **Disable** disables the rule.

We strongly recommend that you **do not** enable all the intrusion rules in an intrusion policy. The performance of your managed device is likely to degrade if all rules are enabled. Instead, tune your rule set to match your network environment as closely as possible.

#### Set intrusion rule action

Configure intrusion rule actions for specific policies in the Secure Firewall Management Center.

Set intrusion rule actions to control how the system responds to detected threats, allowing you to configure rules to alert on or block specific intrusion attempts.

Intrusion rule actions are policy-specific.

#### Procedure

1. Choose **Policies** > **Access Control heading** > **Intrusion**.
2. Click **Snort 3 Version** next to the policy you want to edit.

   **Tip**

   This page shows the total number of:

   - disabled rules
   - enabled rules set to Alert
   - enabled rules set to Block
   - overridden rules

3. Choose the rule or rules where you want to set the rule action.
4. Choose one of the rule actions from the **Rule Action** drop-down list. See Edit Snort 3 Intrusion Policies on page 52 for more information about the different rule actions.
5. Click **Save**.

#### What to do next

Deploy configuration changes. See Deploy configuration changes on page 37.

## Intrusion event notification filters in an intrusion policy

Explains how intrusion event notification filters in an intrusion policy manage event importance based on frequency and network addresses.

An intrusion event notification filter in an intrusion policy is a security mechanism that

- determines event importance based on frequency of occurrence or source and destination IP addresses,
- allows administrators to specify thresholds for when events require attention, and
- prevents system overwhelm by limiting notifications for widespread attacks.

### Event notification filtering scenarios

The importance of an intrusion event can be based on frequency of occurrence, or on source or destination IP address. In some cases you may not care about an event until it has occurred a certain number of times. For example, you may not be concerned if someone attempts to log into a server until they fail a certain number of times. In other cases, you may only need to see a few occurrences to know there is a widespread problem. For example, if a DoS attack is launched against your web server, you may only need to see a few occurrences of an intrusion event to know that you need to address the situation. Your system is overwhelmed when it receives hundreds of the same event.

### Intrusion event thresholds

Describes configuration settings that limit event logging frequency for intrusion detection rules.

An intrusion event threshold is a configuration setting that

- limits the number of times the system logs and displays an intrusion event based on how many times the event is generated within a specified time period,
- prevents you from being overwhelmed with a large number of identical events, and
- can be set per shared object rule, standard text rule, or inspector rule.

### Set intrusion event thresholds

Provides the thresholding options, IP tracking options, and instance/time parameters for configuring intrusion event thresholds.

To set a threshold, first specify the thresholding type.

**Table 4: Thresholding options**

| Option | Description |
|---|---|
| Limit | Logs and displays events for the specified number of packets (specified by the Count argument) that trigger the rule during the specified time period. For example, if you set the type to **Limit**, the **Count** to `10`, and the **Seconds** to `60`, and 14 packets trigger the rule, the system stops logging events for the rule after displaying the first 10 that occur within the same minute. |
| Threshold | Logs and displays a single event when the specified number of packets (specified by the Count argument) trigger the rule during the specified time period. Note that the counter for the time restarts after you hit the threshold count of events and the system logs that event. For example, you set the type to **Threshold**, **Count** to `10`, and **Seconds** to `60`, and the rule triggers 10 times by second 33. The system generates one event, then resets the Seconds and Count counters to 0. The rule then triggers another 10 times in the next 25 seconds. Because the counters reset to 0 at second 33, the system logs another event. |

| Option | Description |
|---|---|
| Both | Logs and displays an event once per specified time period, after the specified number (count) of packets trigger the rule. For example, if you set the type to **Both**, **Count** to two, and **Seconds** to `10`, these event counts result:<br>• If the rule is triggered once in 10 seconds, the system does not generate any events (the threshold is not met)<br>• If the rule is triggered twice in 10 seconds, the system generates one event (the threshold is met when the rule triggers the second time)<br>• If the rule is triggered four times in 10 seconds, the system generates one event (the threshold is met when the rule triggers the second time, and subsequent events are ignored) |

Secondly, specify tracking, which determines whether the event threshold is calculated per source or destination IP address.

**Table 5: Thresholding IP options**

| Option | Description |
|---|---|
| Source | Calculates event instance count per source IP address. |
| Destination | Calculates event instance count per destination IP address. |

Finally, specify the number of instances and time period that define the threshold.

**Table 6: Thresholding Instance/Time options**

| Option | Description |
|---|---|
| Count | The number of event instances per specified time period per tracking IP address required to meet the threshold. |
| Seconds | The number of seconds that elapse before the count resets. If you set the threshold type to **limit**, the tracking to **Source IP**, the **count** to `10`, and the **seconds** to `10`, the system logs and displays the first 10 events that occur in 10 seconds from a given source port. If only 7 events occur in the first 10 seconds, the system logs and displays those; if 40 events occur in the first 10 seconds, the system logs and displays 10, then begins counting again when the 10-second time period elapses. |

You can use intrusion event thresholding alone or combine it with rate-based attack prevention, the `detection_filter` keyword, or intrusion event suppression.

**Tip**

You can also add thresholds from within the packet view of an intrusion event.

**Set threshold for an intrusion rule in snort 3**

Configure a threshold for an intrusion rule from the Rule Detail window to control alert frequency and timing.

Set a threshold for an intrusion rule to control when and how often alerts are generated based on event instances within a specified time period.

You can set a single threshold for a rule from the Rule Detail window. Adding a threshold overwrites any existing threshold for the rule. The threshold you set for an intrusion rule is applied to each packet thread. However, the configuration is fully applied only within the context of a unique flow. You might see more alerts on different network flows, but you will not see fewer alerts than the configured number.

**Procedure**

1. Choose **Objects** > **Intrusion Rules**.
2. Click **Snort 3 All Rules** tab. From an intrusion rule's Alert Configuration column, click the **None** link.
3. Click **Edit** (✎).
4. In the Alert Configuration window, click the **Threshold** tab.
5. From the **Type** drop-down list, choose the type of threshold you want to set:
   - Choose **Limit** to limit notification to the specified number of event instances per time period.
   - Choose **Threshold** to provide notification for each specified number of event instances per time period.
   - Choose **Both** to provide notification once per time period after a specified number of event instances.
6. Choose **Source** or **Destination** in the **Track By** field to indicate whether you want the event instances tracked by source or destination IP address.
7. Enter the number of event instances you want to use as your threshold in the **Count** field.
8. Enter a number that specifies the time period, in seconds, for which event instances are tracked in the **Seconds** field.
9. Click **Save**.

   Refer to the video Snort 3 Suppression and Threshold for additional support and information.

**What to do next**

Deploy configuration changes. See Deploy configuration changes on page 37.

**View and delete intrusion event thresholds**

Configure the removal of intrusion event threshold settings for rules in the Snort 3 All Rules environment.

This task allows you to view existing threshold settings for intrusion rules and delete them when they are no longer appropriate for your system configuration.

To view or delete an existing threshold setting for a rule, use the Rules Details view to display the configured settings for a threshold and see if they are appropriate for your system. If they are not, you can add a new threshold to overwrite the existing values.

**Procedure**

1. Choose **Objects** > **Intrusion Rules**.
2. Click **Snort 3 All Rules** tab.
3. Choose the rule with a configured threshold as shown in the **Alert Configuration** column (the **Alert Configuration** column displays **Threshold** as a link for the rule).
4. To remove the threshold for the rule, click **Threshold** link in the **Alert Configuration** column.
5. Click **Edit** (✎).

6. Click **Threshold** tab.
7. Click **Reset**.
8. Click **Save**.

---

### What to do next

Deploy configuration changes. See Deploy configuration changes on page 37.

### Intrusion policy suppression configuration

Describes how intrusion policy suppression configuration eliminates false positive event notifications from specific IP addresses or ranges.

Intrusion policy suppression configuration is a security mechanism that

- suppresses intrusion event notification when a specific IP address or range of IP addresses triggers a specific rule or inspector,
- eliminates false positives by allowing rules to trigger for all packets while only showing events for legitimate attacks, and
- is useful for scenarios such as mail servers that transmit packets resembling specific exploits.

### Mail server suppression example

If you have a mail server that transmits packets that look like a specific exploit, you might suppress event notification for that event when it is triggered by your mail server. The rule triggers for all packets, but you only see events for legitimate attacks.

### Intrusion policy suppression types

Lists the available intrusion event suppression configurations and their usage options.

You can use intrusion event suppression alone or in any combination with rate-based attack prevention, the `detection_filter` keyword, or intrusion event thresholding.

> **Tip**
>
> You can add suppressions from within the packet view of an intrusion event. You can also access suppression settings by using the **Alert Configuration** column on the intrusion rules editor page (**Objects** > **Intrusion Rules**, click **Snort 3 All Rules**).

### Set suppression for an intrusion rule in Snort 3

Configure suppression settings for intrusion rules to prevent events from being generated by packets from specific source or destination IP addresses.

This task allows you to configure one or more suppressions for a rule in your intrusion policy to reduce false positives and focus on relevant security events.

You can set one or more suppressions for a rule in your intrusion policy.

#### Before you begin

Ensure you create the required network objects to be added for source or destination suppression.

Follow these steps to set suppression for an intrusion rule in Snort 3:

### Procedure

1. Choose **Objects** > **Intrusion Rules**.
2. Click **Snort 3 All Rules** tab.
3. Click the **None** link in the Alert Configuration column for the intrusion rule.
4. Click **Edit** ( ).
5. From the **Suppressions** tab, click the add icon **Add** ( ) next to any of these options:
   - Choose **Source Networks** to suppress events generated by packets originating from a specified source IP address.
   - Choose **Destination Networks** to suppress events generated by packets going to a specified destination IP address.
6. Select any of the preset networks in the **Network** drop-down list.
7. Click **Save**.
8. (Optional) Repeat steps 5, 6, and 7 if needed.
9. Click **Save** in the Alert Configuration window.

### What to do next

Deploy configuration changes. See Deploy configuration changes on page 37.

### View and delete suppression conditions

Configure suppression conditions by viewing existing conditions and removing unwanted suppressions from intrusion rules.

View or delete existing suppression conditions to manage event notifications for specific network conditions.

You may want to view or delete an existing suppression condition. For example, you can suppress event notification for packets originating from a mail server IP address because the mail server normally transmits packets that look like exploits. If you then decommission that mail server and reassign the IP address to another host, you should delete the suppression conditions for that source IP address.

### Procedure

1. Choose **Objects** > **Intrusion Rules**.
2. Click **Snort 3 All Rules** tab.
3. Choose the rule for which you want to view or delete suppressions.
4. Click **Suppression** in the **Alert Configuration** column.
5. Click **Edit** ( ).
6. Click **Suppressions** tab.
7. Remove the suppression by clicking **Clear** ( ) next to the suppression.
8. Click **Save**.

### What to do next

Deploy configuration changes. See Deploy configuration changes on page 37.

## Add intrusion rule comments

Configure comments for rules in your intrusion policy to add policy-specific notes that are not visible in other intrusion policies.

Add comments to rules in your intrusion policy for documentation and management purposes.

You can add comments to rules in your intrusion policy. Comments added this way are specific to the policy. Comments you add to a rule in one intrusion policy are not visible in other intrusion policies.

### Procedure

1. Choose **Policies** > **Access Control heading** > **Intrusion**.
2. Click **Snort 3 Version** next to the policy you want to edit.
3. In the right side of the page where all the rules are listed, choose the rule where you want to add a comment.
4. Click **Comment** ( ) under the **Comments** column.
5. In the **Comments** field, enter the rule comment.
6. Click **Add Comment**.
7. Click **Save**.

   The system displays a **Comment** ( ) next to the rule in the Comments column.

### What to do next

Deploy configuration changes. See Deploy configuration changes on page 37.

## Prepare custom rules for snort 3 conversion

Consider preparing custom rule management for Snort 3 before converting from Snort 2.

Before converting from Snort 2 to Snort 3, make sure you are prepared to manage your custom rule set for Snort 3.

- If you are using a rule set from a third-party vendor, contact that vendor to confirm that their rules will successfully convert to Snort 3 or to obtain a replacement rule set written natively for Snort 3.
- If you have custom rules that you have written yourself, familiarize yourself with writing Snort 3 rules before converting, so you can update your rules to optimize Snort 3 detection after conversion.

Learn more about writing rules in Snort 3:

- https://blog.snort.org/2020/08/how-rules-are-improving-in-snort-3.html
- https://blog.snort.org/2020/10/talos-transition-to-snort-3.html

You can refer to other blogs at https://blog.snort.org/ to learn more about Snort 3 rules.

**Important**

Snort 2 network analysis policy (NAP) settings *cannot* be copied to Snort 3 automatically. NAP settings must be manually replicated in Snort 3.

**Note**

Snort 2 is not supported on threat defense version 7.7. For information on Snort 2 features that are supported in versions earlier than 7.7, refer to the Firewall Management Center guide that matches your Firewall Threat Defense version.

### Convert all Snort 2 custom rules across all intrusion policies to Snort 3

Configure automatic conversion of all Snort 2 custom rules across all intrusion policies to Snort 3 format.

Convert legacy Snort 2 custom rules to the updated Snort 3 format to ensure compatibility with current intrusion detection systems.

This task migrates existing Snort 2 custom rules to Snort 3 format, allowing you to maintain your custom rule configurations while upgrading to the latest intrusion detection engine. You can either import the converted rules directly or download them for review before importing.

#### Procedure

1. Choose **Objects** > **Intrusion Rules**.
2. Click **Snort 3 All Rules** tab.
3. Ensure **All Rules** is selected in the left pane.
4. Click the **Tasks** drop-down list and choose:
   - **Convert Snort 2 rules and import**–To automatically convert all the Snort 2 custom rules across all the intrusion policies to Snort 3 and import them into Firewall Management Center as Snort 3 custom rules.
   - **Convert Snort 2 rules and download**–To automatically convert all the Snort 2 custom rules across all the intrusion policies to Snort 3 and download them into your local system.
5. Click **OK**.

   **Note**

   - If you selected **Convert and import** in the previous step, then all the converted rules are saved under a newly created rule group **All Snort 2 Converted Global** under **Local Rules**.
   - If you selected **Convert and download** in the previous step, then save the rules file locally. You can review the converted rules in the downloaded file and later upload them by following the steps in Add custom rules to rule groups on page 76.

   Refer to the video Converting Snort 2 Rules to Snort 3 for additional support and information.

#### What to do next

Deploy configuration changes. See Deploy configuration changes on page 37.

### Convert Snort 2 custom rules of a single intrusion policy to Snort 3

Configure the conversion of Snort 2 custom rules to Snort 3 format for a single intrusion policy.

Convert Snort 2 custom rules in an intrusion policy to Snort 3 format to maintain compatibility with Snort 3 environments.

When migrating to Snort 3, existing Snort 2 custom rules need to be converted to maintain their functionality. This task allows you to convert custom rules for a specific intrusion policy.

#### Procedure

1. Choose **Policies** > **Access Control heading** > **Intrusion**.
2. In the **Intrusion Policies** tab, click **Show Snort 3 Sync status**.
3. Click the **Sync** icon **Snort out-of-Sync** (🔶) of the intrusion policy.

   **Note**

   If the Snort 2 and the Snort 3 versions of the intrusion policy are synchronized, then the **Sync** icon is in blue**Snort in-Sync** (🔷). It indicates that there are no custom rules to be converted.

4. Read the summary and click the **Custom Rules** tab.
5. Choose:
   - **Import converted rules to this policy**: To convert the Snort 2 custom rules in the intrusion policy to Snort 3 and import them into Firewall Management Center as Snort 3 custom rules.
   - **Download converted rules**: To convert the Snort 2 custom rules in the intrusion policy to Snort 3 and download them into your local system. You can review the converted rules in the downloaded file and later upload the file by clicking the upload icon.
6. Click **Re-Sync**.

#### What to do next

Deploy configuration changes. See Deploy configuration changes on page 37.

## Add custom rules to rule groups

Upload custom rules to the Firewall Management Center and associate them with rule groups.

Upload custom rules to add locally created Snort 3 rules to the list of all available rules in the system.

Uploading custom rules in the Firewall Management Center adds the custom rules that you have created locally to the list of all the Snort 3 rules.

#### Procedure

1. Choose **Objects** > **Intrusion Rules**.
2. Click **Snort 3 All Rules** tab.
3. Click the **Tasks** drop-down list.
4. Click **Upload Snort 3 Rules**.

5. Drag and drop the `.txt` or `.rules` file that contains the Snort 3 custom rules that you have created.
6. Click **OK**.

> **Note**
>
> If there are any errors in the selected file, then you cannot proceed further. You can download the error file and **Replace File** link to upload version 2 of the file, after fixing the errors.

7. Associate rules to a rule group to add the new rules to that group.

   You can also create a new custom rule group (by clicking the **Create New Custom Rule Group** link) and then add the rules to the new group.

> **Note**
>
> If there are no existing local rule groups, then proceed by clicking **Create New Custom Rule Group to proceed**. Enter a **Name** for the new rule group and click **Save**.

8. Choose either of these options:
   - **Merge Rules** to merge the new rules that you are adding with the existing rules in the rule group.
   - **Replace all rules in the group with file contents** to replace all the existing rules with the new rules that you are adding.

> **Note**
>
> If you chose more than one rule group in the previous step, then only the **Merge Rules** option is available.

9. Click **Next**.

   Review the summary to know the new rule IDs that are being added and optionally download it.

10. Click **Finish**.

---

**Important**

All uploaded rules are disabled by default. Change their state as needed to ensure the rules are active.

### What to do next

- Uploading custom rules in the Firewall Management Center adds the custom rules that you have created to the list of all the Snort 3 rules. To enforce these custom rules on the traffic, add and enable these rules in the required intrusion policies. For information on adding rule groups with custom rules to an intrusion policy, see Add rule groups with custom rules to an intrusion policy on page 78. For information on enabling custom rules, see Manage custom rules in Snort 3 on page 78.

- Deploy configuration changes. See Deploy configuration changes on page 37.

## Add rule groups with custom rules to an intrusion policy

Configure an intrusion policy to enforce custom rules by adding uploaded rule groups to the policy.

Enable custom rules in an intrusion policy to enforce these rules on network traffic.

Custom rules that are uploaded in the system have to be enabled in an intrusion policy to enforce those rules on the traffic. After uploading custom rules on Firewall Management Center, add the rule group with the new custom rules in the intrusion policy.

### Procedure

1. Choose **Policies** > **Access Control heading** > **Intrusion**.
2. In the **Intrusion Policies** tab, click the **Snort 3 Version** of the intrusion policy.
3. Click **Add** (+) next to the Rule Groups search bar.
4. In the **Add Rule Groups** window, click the **Expand Arrow** (>) icon next to a rule group to expand the local rule group.
5. Check the check box next to the uploaded custom rules group.
6. Click **Save**.

### What to do next

Deploy configuration changes. See Deploy configuration changes on page 37.

## Manage custom rules in Snort 3

Configure custom rules in Snort 3 by adding uploaded rules to intrusion policies and enabling them to enforce traffic monitoring across all policies or selectively on individual policies.

This task enables uploaded custom rules in intrusion policies to enforce rule monitoring on network traffic.

Custom rules that are uploaded in the system have to be added to an intrusion policy and enabled to enforce those rules on the traffic. You can enable the uploaded custom rules across all policies or selectively on individual policies.

### Before you begin

Follow these steps to enable custom rules in one or many intrusion policies:

### Procedure

1. Choose **Objects** > **Intrusion Rules**.
2. Click **Snort 3 All Rules** tab.
3. Expand **Local Rules** and select the required rule group.
4. Select the rules by checking the check boxes next to them.
5. Select **Per Intrusion Policy** from the **Rule Actions** drop-down list.
6. Choose:
   - **All Policies** to have the same rule actions for all the rules to be added.
   - **Per Intrusion Policy** to have different rule actions for each intrusion policy.

7. Set the rule actions:
   - If you selected All Policies in the previous step, then select the required rule action from the **Select Override state** drop-down list.
   - If you selected Per Intrusion Policy in the previous step, then select the **Rule Action** against the policy name. To add more policies, click **Add Another**.
8. Optionally, add a comment in the **Comments** text box.
9. Click **Save**.

#### What to do next

Deploy configuration changes. See Deploy configuration changes on page 37.

## Delete custom rules

Configure the deletion of custom rules from the Snort 3 All Rules section.

Delete custom rules that are no longer needed from your intrusion rule configuration to maintain an organized and efficient rule set.

Use this procedure when you need to remove custom rules from the Local Rules section in the Snort 3 All Rules interface. Before deletion, all rules must be disabled to prevent configuration conflicts.

#### Procedure

1. Choose **Objects** > **Intrusion Rules**.
2. Click **Snort 3 All Rules** tab.
3. Expand **Local Rules** in the left pane.
4. Check the check boxes of the rules you want to delete.
5. Ensure that the rule action for all the rules that you select is **Disable**.

   If required, follow these steps to disable the rule action for multiple selected rules:

   a) From the **Rule Actions** drop-down box, select **Per Intrusion Policy**.
   b) Select **All Policies** radio button.
   c) Select **Disable** from the **Select Override state** drop-down list.
   d) Click **Save**.
   e) Check the check boxes of the rules you want to delete.
6. From the **Rule Actions** drop-down list, select **Delete**.
7. Click **Delete** in the Delete Rules pop-up window.

#### What to do next

Deploy configuration changes. See Deploy configuration changes on page 37.

## Delete rule groups

Remove unwanted rule groups from your intrusion detection configuration.

Delete rule groups to remove unwanted or obsolete intrusion detection rules from your system configuration and maintain an organized rule structure.

Before deleting a rule group, you must exclude it from all intrusion policies and disable all rules within the group to prevent system conflicts.

### Before you begin

Exclude the rule group you want to delete from all intrusion policies where you have included it. For steps on excluding a rule group from an intrusion policy, see Edit Snort 3 Intrusion Policies on page 52.

Follow these steps to delete rule groups:

#### Procedure

1. Choose **Objects** > **Intrusion Rules**.
2. Click **Snort 3 All Rules** tab.
3. Expand **Local Rules** in the left pane.
4. Select the rule group to be deleted.
5. Ensure the rule action for all the rules in the group is set to **Disable** before proceeding.

   If the rule action for any of the rules is anything other than **Disable**, then you cannot delete the rule group. If required, follow the steps below to disable the rule action for all the rules:

   a) Check the check box below the **Rule Actions** drop-down list to select all the rules in the group.
   b) From the **Rule Actions** drop-down box, select **Per Intrusion Policy**.
   c) Select **All Policies** radio button.
   d) Select **Disable** from the **Select Override state** drop-down list.
   e) Click **Save**.
6. Click the **Delete** ( ) next to the rule group.
7. Click **OK** in the Delete Rule Group pop-up window.

#### What to do next

Deploy configuration changes. See Deploy configuration changes on page 37.

## Recommended rules

Describes the Secure Firewall recommended rules and explains how to generate and apply these rules to enhance security policy effectiveness.

This section provides an insight into Secure Firewall recommended rules and generating and applying Secure Firewall recommended rules.

### Snort 3 rule changes in LSP updates

Describes how system-defined intrusion rules may be replaced, combined, or removed during Snort 3 Lightweight Security Package updates to improve detection capabilities.

Snort 3 rule changes in LSP updates are modifications to system-defined intrusion rules that

- replace existing rules with new rules for better detection capabilities,
- combine multiple rules into a single rule or expand a single rule into multiple rules when better detection is possible, and
- remove existing system-defined rules for better management as 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** (⚙).

## Secure Firewall recommended rules

Explains intrusion rule recommendations that target vulnerabilities associated with detected host assets in the network.

Secure Firewall recommended rules are intrusion rule recommendations that

- target vulnerabilities associated with host assets detected in the network, such as operating systems, servers, and client application protocols,
- allow you to tailor your intrusion policy to the specific needs of your monitored network, and
- provide individual recommendations for each intrusion policy. These typically apply to standard text rules and shared object rules, but recommendations can also include inspector and decoder rules.

### Rule recommendation configuration options

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 Secure Firewall 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 Secure Firewall recommended rule state, the rules in your intrusion policy match the settings recommended for your network assets.

## Generate new Secure Firewall recommendations in Snort 3

Configure new recommended rule settings in Snort 3 for Secure Firewall recommendations by generating and applying recommendations to the intrusion policy.

Generate Secure Firewall recommendations to create new recommended rule settings in Snort 3.

Generate the Secure Firewall recommendations for the intrusion policy and then follow the steps that are listed here to create new recommended rule settings in Snort 3. Rule overheads are interpreted as **security levels** based on the threshold policies you select in Snort 3. The recommended action depends on the selected security level. If it is higher than the base policy, the recommendation includes actions beyond only generating events.

Prior to setting the Secure Firewall 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 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, these are the recommended actions:

- Set recommendations to the next highest security level, and clear the option to disable rules.
- Set recommendations to the next highest security level, and select the option to disable rules.
- Set recommendations to the current security level, and select the option to disable rules.

### Before you begin

Secure Firewall recommendations have the following requirements:

- 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

Follow these steps to generate new Secure Firewall recommendations in Snort 3:

**Procedure**

1. Choose **Policies** > **Access Control heading** > **Intrusion**.
2. Click the **Snort 3 Version** button of the intrusion policy.
3. Click the **Recommendations (Not in Use)** layer to configure the rule recommendations. Click **Start**.

   In the Secure Firewall Rule Recommendations window you can set the following:

   - **Security Level**: Click to select the security level. Optionally, you can check the **Accept Recommendation to Disable Rules** checkbox to disable rules that are not enabled at the input security level and in protected networks. Only enable this option if you need to trim your rule set due to a high number of alerts or to improve inspection performance. The security levels are:
     - Security level 1: Connectivity Over Security

       **No Impact**–No new rules are enabled and no existing rules are disabled. To increase the protection, select a higher security level.

       **Lower Security** (checkbox is checked)–All rules are disabled except for the rules in the Connectivity Over Security ruleset that match potential vulnerabilities on discovered hosts. It is recommended instead to adjust the Base Policy.

     - Security level 2: Balanced Security Over Connectivity

       **No Impact**–No new rules are enabled and no existing rules are disabled. To increase the protection, select a higher security level.

       **Higher Efficiency**(checkbox is checked)–Keeps existing rules that match potential vulnerabilities on discovered hosts and disables rules for vulnerabilities not found on the network.

     - Security level 3: Security Over Connectivity

       **Increased Security**–Enables additional rules that match potential vulnerabilities on discovered hosts based on the Maximum Detection ruleset.

       **Focused Security**(checkbox is checked)–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 4 : Maximum Detection

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

       **Focused Security** (checkbox is checked)–Enables additional rules that match vulnerabilities on discovered hosts based on the Maximum Detection ruleset, while disabling existing rules that do not match potential vulnerabilities on discovered hosts.

       > **Note**
       >
       > Maximum Detection enables a very high number of rules and may impact performance. We recommend you to review and test this setting before deploying into a production environment.

   - **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 or 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 Secure Firewall Management Center Device Configuration guide*.

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

4. 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 (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 new recommendations.
5. You can verify the recommendations and choose to apply them.
   - **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, Firewall 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 on page 37.

# Mitigate threats using MITRE framework in Snort 3 intrusion policies

Describes how to use the MITRE ATT&CK framework within Snort 3 intrusion policies to identify, categorize, and mitigate security threats based on known adversary tactics and techniques.

This section describes how to use the MITRE ATT&CK framework in Snort 3 intrusion policies to identify attack tactics and techniques, review rule coverage, and improve threat mitigation.

## MITRE framework

Describes a comprehensive knowledge base that outlines tactics, techniques, and procedures used by threat actors to compromise systems.

The MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) framework is a comprehensive knowledge base that

- provides insights into the tactics, techniques, and procedures (TTPs) distributed by threat actors aiming to harm systems,
- incorporates groups to refer to threat groups, activity groups, or threat actors based on the set of tactics and techniques they employ, and
- is compiled as matrices, with each matrix representing an operating system or a particular platform.

Each technique includes information about execution, procedures, defenses, detections, and real-world examples.

> **Note**
>
> See https://attack.MITRE.org for additional information about MITRE ATT&CK.

The management center uses the MITRE ATT&CK Framework to enhance threat detection and response, incorporating these capabilities:

- Intrusion events include TTPs, allowing administrators to manage traffic with greater granularity by grouping rules according to vulnerability type, target system, or threat category.
- Select malware events use TTPs, enhancing the ability to detect and respond to threats.
- Unified and Classic Event Viewers display tactics, techniques, attack lifecycle graphs, and contextual enrichments from the Talos taxonomy. These enrichments include MITRE tags and a hierarchical view of associated tactics, techniques, and sub-techniques. You can also filter events using MITRE identifiers.

## MITRE framework benefits

Explains the advantages of implementing MITRE framework for intrusion detection and policy management.

MITRE framework provides security advantages that

- enable administrators to act on traffic based on MITRE Tactics, Techniques, and Procedures (TTPs) added to intrusion events,
- allow viewing and handling traffic with more granularity through grouping rules by vulnerability type, target system, or threat category, and
- provide the ability to organize intrusion rules according to the MITRE ATT&CK framework for customized policies based on specific attacker tactics and techniques.

## Sample business scenario for MITRE network

Describes how a large corporate network uses Snort 3 as its primary intrusion detection and prevention system with MITRE framework insights for enhanced threat protection.

A sample business scenario for MITRE network is a security implementation example that

- uses Snort 3 as the primary intrusion detection and prevention system for a large corporate network,
- addresses the need for robust network security measures in a rapidly evolving threat landscape, and
- enables network administrators to determine if configured policies are finding traffic of interest and tracking known attack groups.

### Network security considerations

Network administrators need to know if adversaries are attempting to take advantage of weaknesses in their systems or applications to cause 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 Server Message Block (SMB) or Secure Shell (SSH), network device administration and management protocols or applications, such as web servers and related services.

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

## Prerequisites for MITRE framework

Outlines the system and configuration requirements that must be met before implementing the MITRE framework.

Ensure that your system meets these requirements before implementing the MITRE framework:

- You must be running Secure Firewall Management Center and Secure Firewall Threat Defense Version 7.3.0 or later with Snort 3.
- You must have at least one intrusion policy. See Create a custom snort 3 intrusion policy on page 51.

## View and edit your Snort 3 intrusion policy

Configure your Snort 3 intrusion policy by viewing and editing rule groups, security levels, and recommendations to customize threat detection settings.

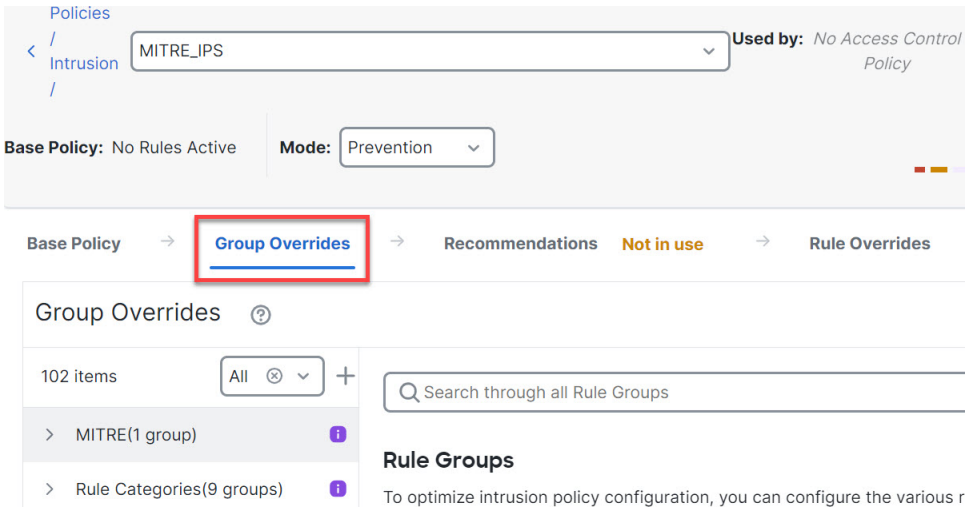
This task allows you to customize your Snort 3 intrusion policy by modifying rule groups, security levels, and accessing Cisco-recommended rules to enhance threat detection capabilities.

Snort 3 intrusion policies use a hierarchical rule group structure organized by the MITRE framework. You can drill down to specific rule categories and modify security levels for bulk changes or individual rule actions. The policy editor provides multiple layers, including Group Overrides, Rule Overrides, Recommendations, and Summary views.

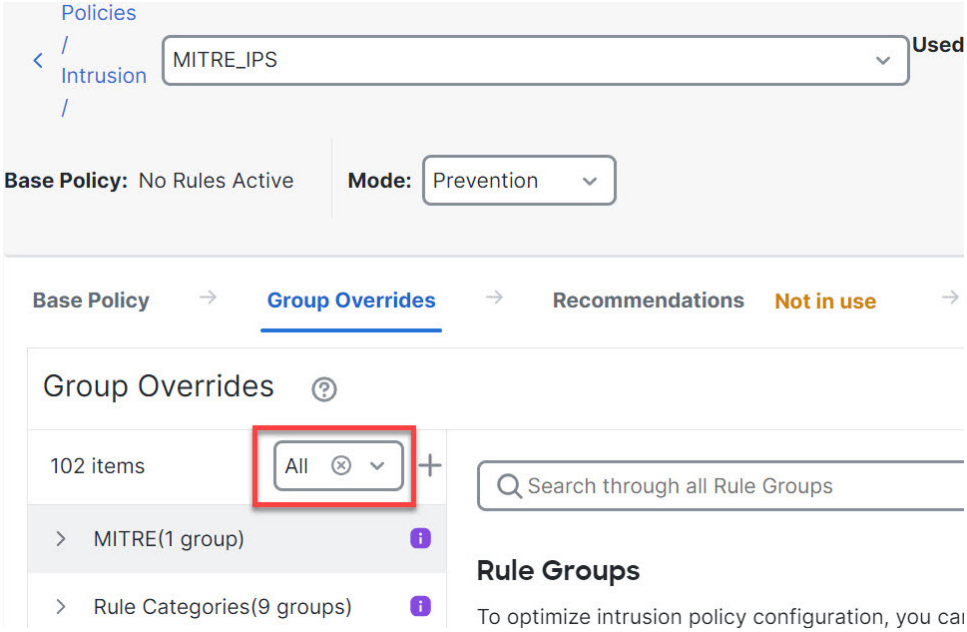
### Procedure

1. Choose **Policies** > **Access Control heading** > **Intrusion**.
2. Ensure that the **Intrusion Policies** tab is chosen.
   a) Click **Snort 3 Version** next to the intrusion policy that you want to view or edit.
   b) Close the Snort helper guide that is displayed.
3. Click the **Group Overrides** layer.

   This layer lists all the categories of rule groups, in a hierarchical structure. You can drill down to the final leaf rule group under each rule group.

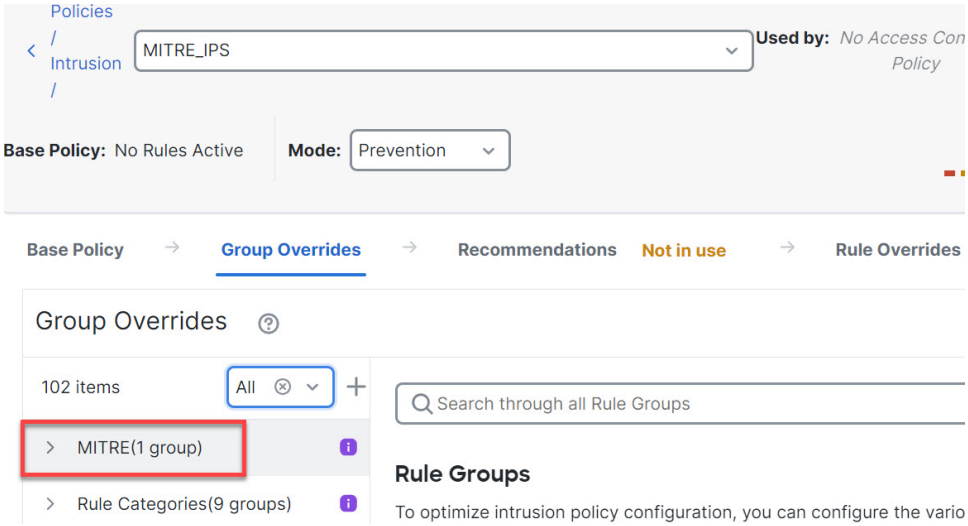



a) Under **Group Overrides**, ensure that **All** is chosen in the drop-down list, so that all the rule groups for the corresponding intrusion policy are visible in the left pane.

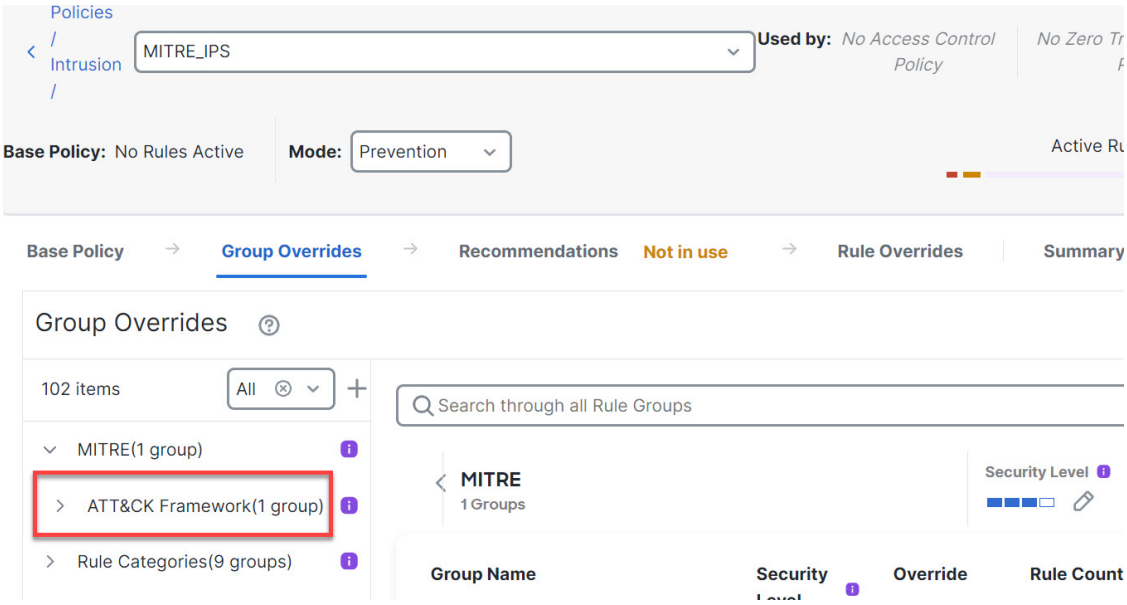



4. Click **MITRE** in the left pane.

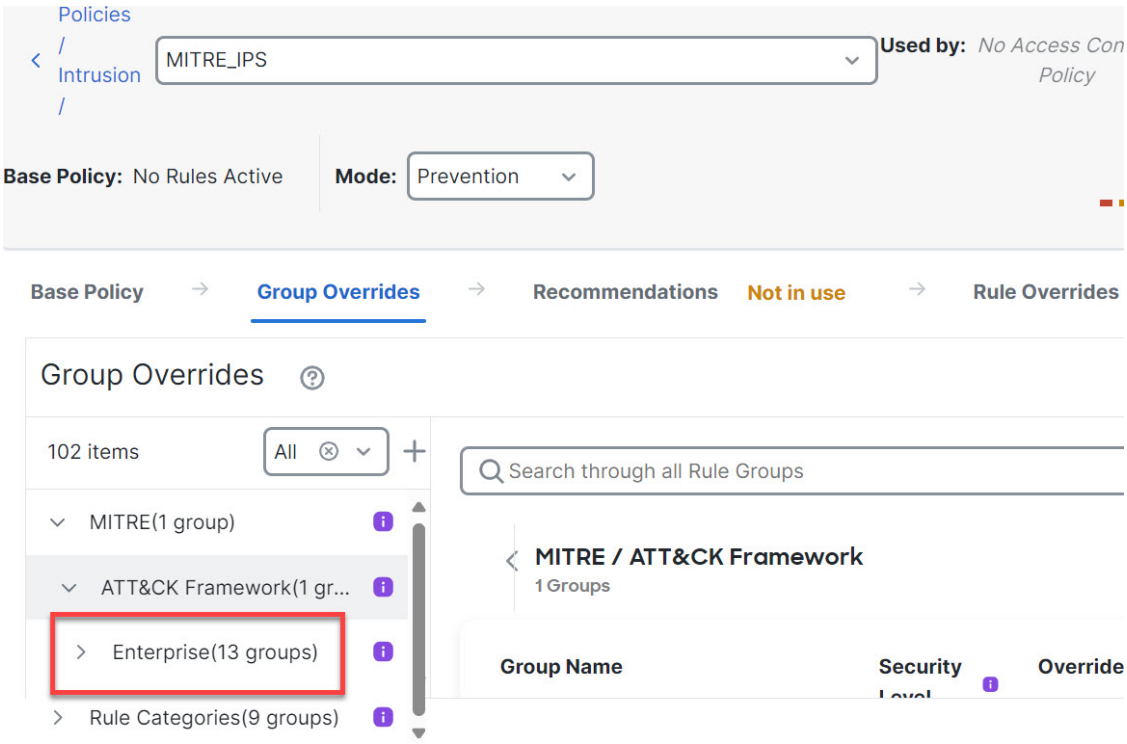
> **Note**
>
> Depending on your specific requirements, you can choose the **Rule Categories** rule group or any other rule group and subrule groups under it. All the rule groups use the MITRE framework.



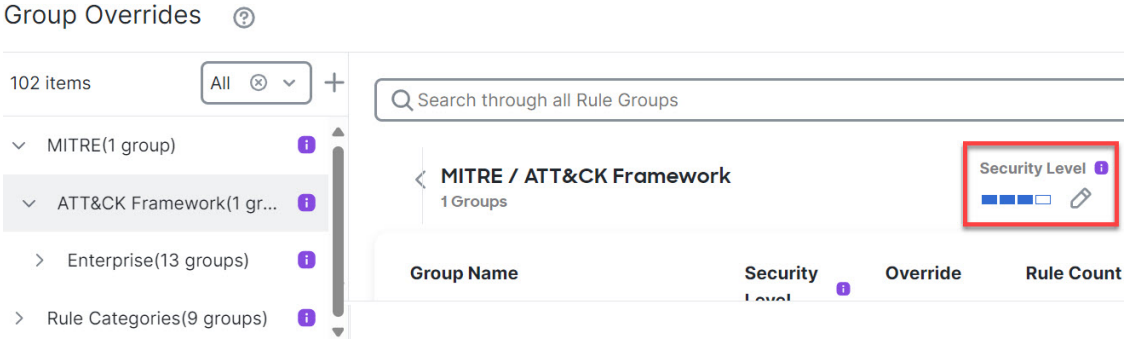

a) Under **MITRE**, click **ATT&CK Framework** to drill down.



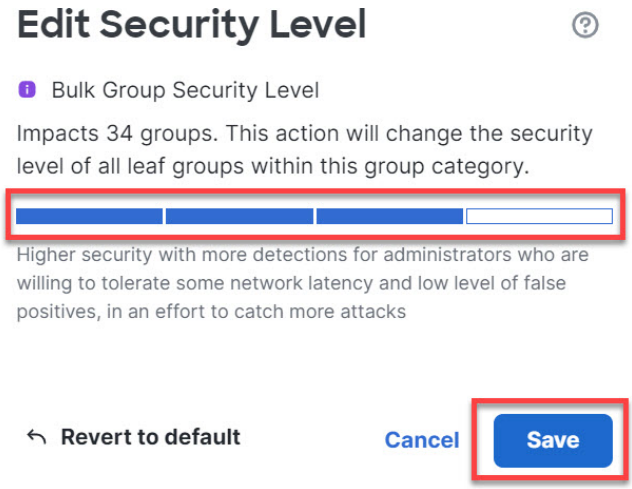

b) Under **ATT&CK Framework**, click **Enterprise** to expand it.




c) Click the **Edit** (✎) icon next to the **Security Level** of the rule group to make bulk changes to all associated rule group security levels under the **Enterprise** rule group category.

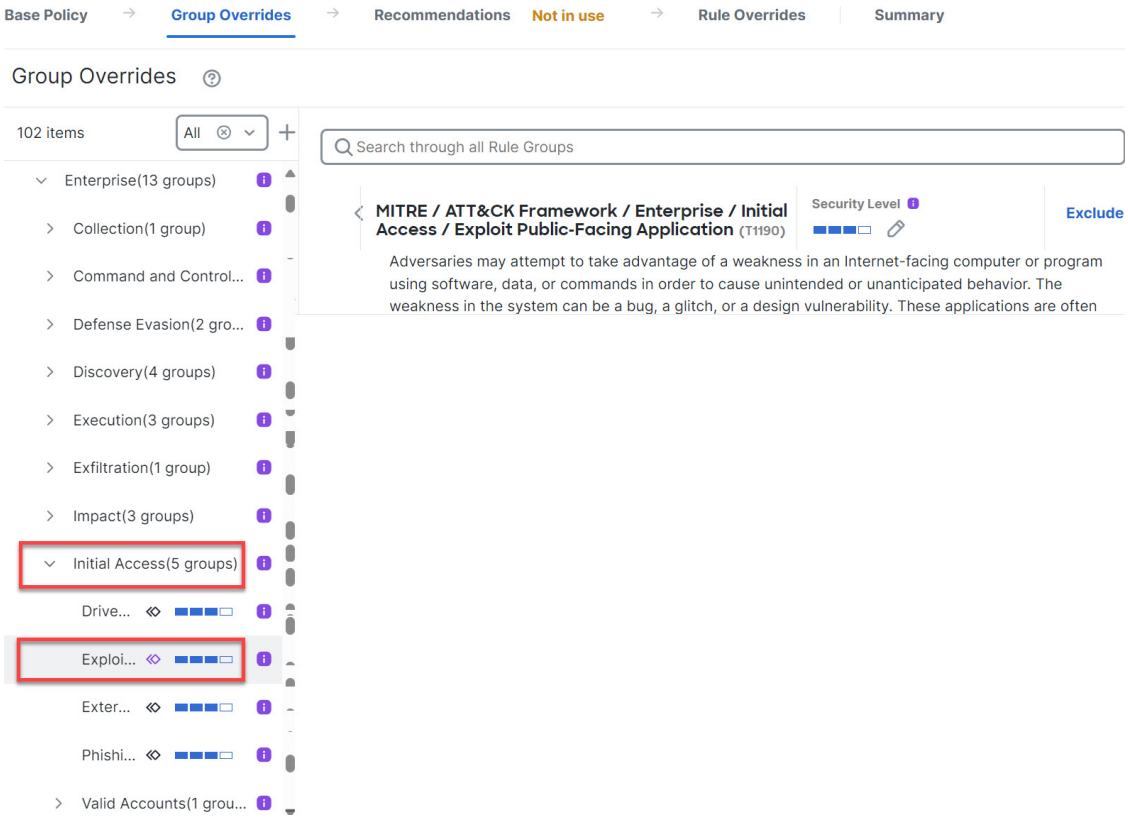



d) In the **Edit Security Level** window, choose a **Security Level** (in this example, **3**), and click **Save**.

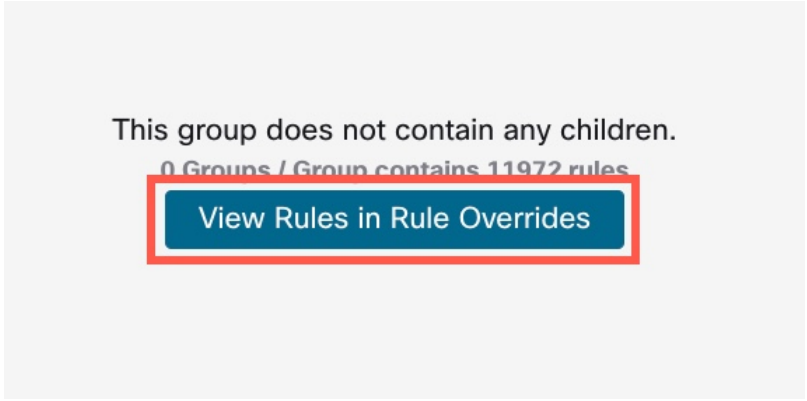



5. Under **Enterprise**, click **Initial Access** to expand it.

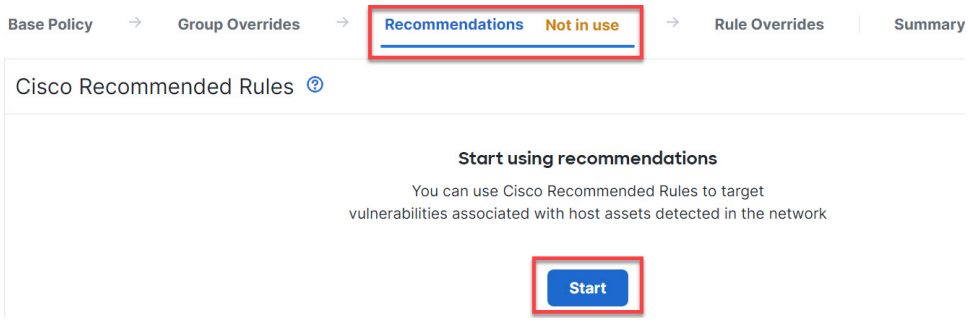
6. Under **Initial Access**, click **Exploit Public-Facing Application**, which is the last leaf group.



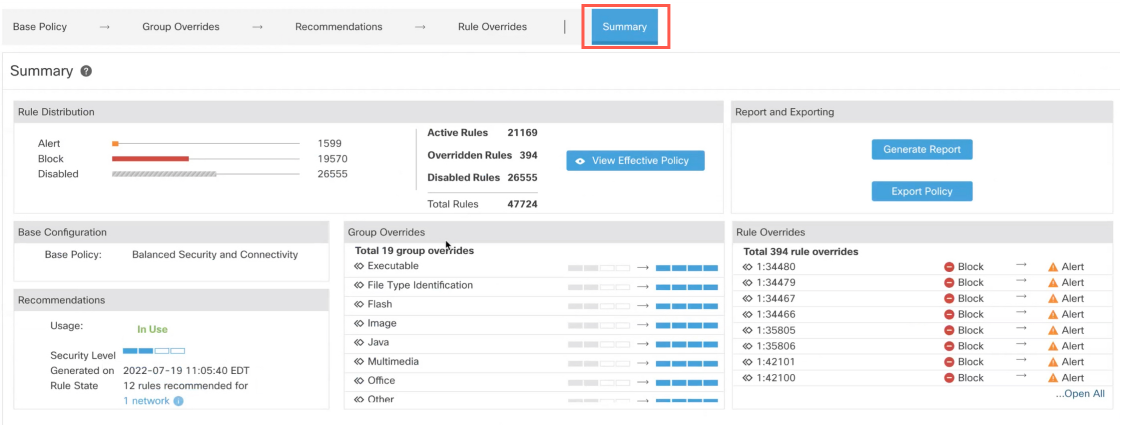

7. Click **View Rules in Rule Overrides** to view the available rules, their details, and actions. You can change the rule actions for one or multiple rules in the **Rule Overrides** layer.




8. Click the **Recommendations** layer and then click **Start** to start using Cisco-recommended rules. You can use the intrusion rule recommendations to target the vulnerabilities that are associated with the host assets detected in the network. For more information, see Generate new Secure Firewall recommendations in Snort 3 on page 82.



9. 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 additional details 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 on page 37.

## View intrusion events

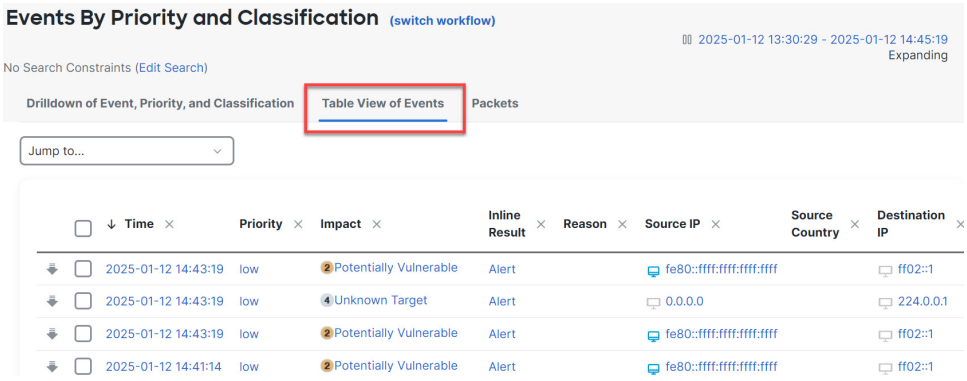
Configure the viewing of MITRE techniques and rule groups in intrusion events on the Classic Event Viewer and Unified Event Viewer pages.

This task allows you to view MITRE ATT&CK techniques and rule groups associated with intrusion events, providing security context and attack pattern mapping for better threat analysis.

You can view the MITRE ATT&CK techniques and rule groups in the intrusion events on the **Classic Event Viewer** and **Unified Event Viewer** pages. 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).

### Procedure

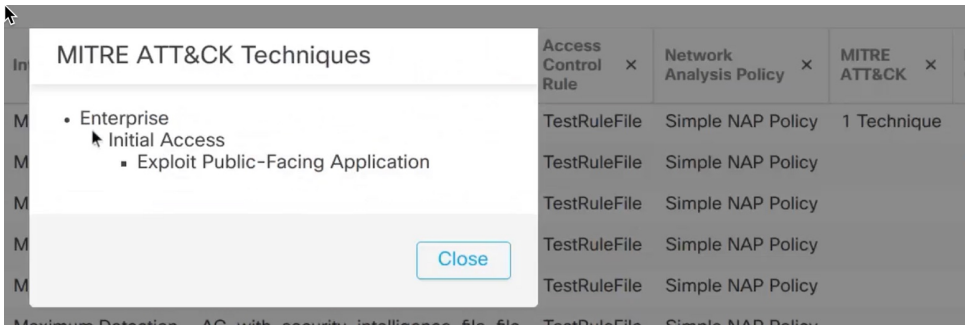
1. Click **Analysis** and select **Events** under **Intrusions**.
2. Click the **Table View of Events** tab.



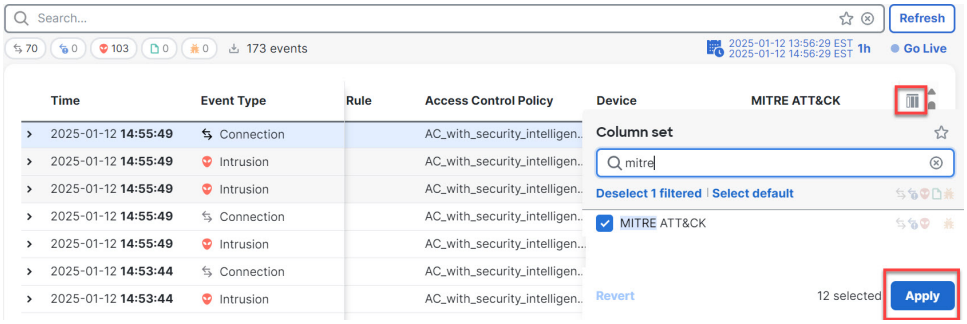

3. Under **MITRE ATT&CK**, you can see the techniques for an intrusion event. Click **1 Technique** to view the MITRE ATT&CK techniques.



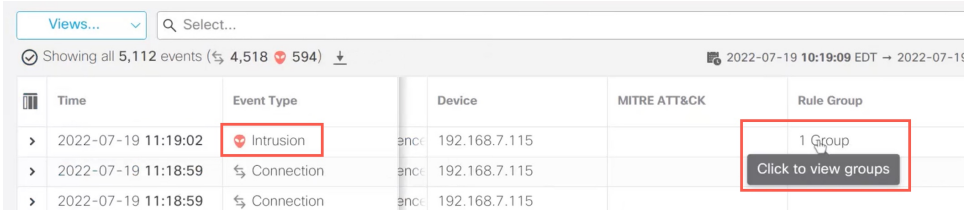

In this example, **Exploit Public-Facing Application** is the technique.



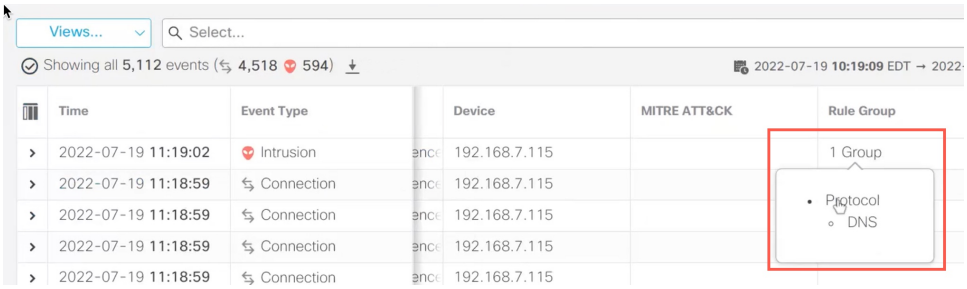

4. Click **Close**.
5. Click **Analysis** and select **Unified Events**.
6. If not enabled, click the column selector icon to enable the **MITRE ATT&CK** and **Rule Group** columns.



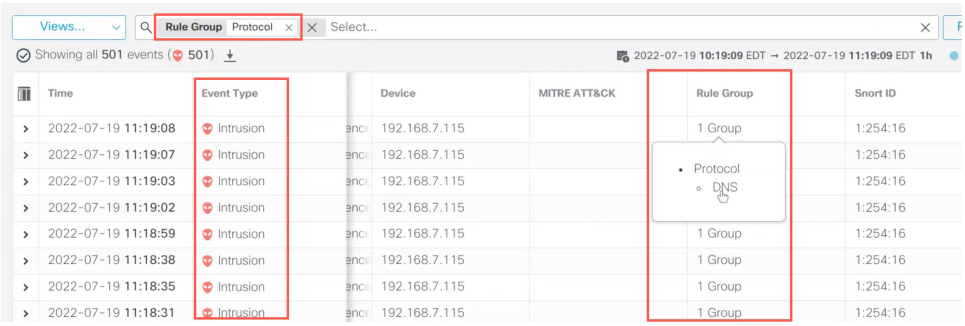

7. In this example, the intrusion event is triggered by an event that is mapped to one rule group. Click **1 Group** under the **Rule Group** column.




8. You can view **Protocol**, which is the parent rule group, and the DNS rule group under it. Choose **Protocol** > **DNS** to search for all the intrusion events that have at least one rule group.



The search results are displayed.




## Additional references

Lists additional reference sources for intrusion policies in Snort 3, including MITRE framework information that provides context and classification details for malware events and security incidents.

This reference provides links to additional documentation and resources for intrusion policies in Snort 3 and MITRE framework information for malware event classification.

- Intrusion Policy in Snort 3
- Edit Snort 3 Intrusion Policies on page 52
- MITRE Information in Malware Events

# 4 Intrusion Prevention Performance Tuning

**Topics:**


- Intrusion prevention performance tuning
- License requirements for intrusion prevention performance tuning
- Requirements and prerequisites for intrusion prevention performance tuning
- Limiting pattern matching for intrusions
- Regular expression limits overrides for intrusion rules
- Override regular expression limits for intrusion rules
- Per packet intrusion event generation limits
- Limiting intrusion events generated per packet
- Packet and intrusion rule latency threshold configuration
- Intrusion performance statistic logging configuration
- Configure intrusion performance statistic logging


Identifies techniques and best practices for optimizing intrusion prevention system performance.

This chapter explains how to refine intrusion prevention performance.

# Intrusion prevention performance tuning

Describes features for improving system performance while analyzing traffic for attempted intrusions.

Intrusion prevention performance tuning is a system optimization mechanism that

- improves performance while analyzing traffic for attempted intrusions,
- applies settings on a per-access control policy basis to all intrusion policies invoked by that parent access control policy, and
- balances security with the need to maintain device latency at an acceptable level.

### Performance tuning features

Cisco provides several features for improving the performance of your system as it analyzes traffic for attempted intrusions. You can:

- specify the number of packets to allow in the event queue. You can also, before and after stream reassembly, enable or disable inspection of packets that will be rebuilt into larger streams.
- override default match and recursion limits on PCRE that are used in intrusion rules to examine packet payload content.
- elect to have the rules engine log more than one event per packet or packet stream when multiple events are generated, allowing you to collect information beyond the reported event.
- balance security with the need to maintain device latency at an acceptable level with packet and rule latency thresholding.
- configure the basic parameters of how devices monitor and report their own performance. This allows you to specify the intervals at which the system updates performance statistics on your devices.

> **Note**
>
> Snort 2 is not supported on threat defense version 7.7. For information on Snort 2 features that are supported in versions earlier than 7.7, refer to the Firewall Management Center guide that matches your Firewall Threat Defense version.

# License requirements for intrusion prevention performance tuning

Lists the licensing prerequisites and requirements needed to enable and configure intrusion prevention performance tuning features on Cisco Secure Firewall devices.

This reference provides licensing information required for implementing intrusion prevention performance tuning on Cisco Secure Firewall devices, covering both Threat Defense and Classic licensing models.

### Threat Defense License

IPS

# Requirements and prerequisites for intrusion prevention performance tuning

Lists the system requirements and prerequisite configurations needed before implementing intrusion prevention performance tuning on Cisco Secure Firewall devices.

This reference provides the system requirements and prerequisite configurations needed before implementing intrusion prevention performance tuning on Cisco Secure Firewall devices.

**Model support**

Any

**Supported domains**

Any

**User roles**

- Admin
- Access Admin
- Network Admin

# Limiting pattern matching for intrusions

Configure pattern matching limits to optimize intrusion detection performance by controlling the maximum number of pattern states analyzed per packet and managing content checks on reassembled traffic.

Limit pattern matching for intrusions to optimize system performance by controlling how many pattern states are analyzed per packet and managing content inspection before and after stream reassembly.

Pattern matching limits help balance security effectiveness with system performance. When processing high volumes of traffic, limiting the number of pattern states analyzed per packet can prevent performance degradation while maintaining essential intrusion detection capabilities.

## Before you begin

Follow these steps to limit pattern matching for intrusions:

**Procedure**

1. In the access control policy editor, click **Advanced** (**Policies** > **Access Control heading** > **Access Control**, click **Edit** and then click **Advanced Settings**).

   In the new UI, select **Advanced Settings** from the drop-down arrow at the end of the packet flow line.

2. Click **Edit** (✎) next to **Performance Settings**.

   If **View** (👁) appears instead, settings are inherited from an ancestor policy, or you do not have permission to modify the settings. If the configuration is unlocked, uncheck **Inherit from base policy** to enable editing.

3. Click **Pattern Matching Limits** in the **Performance Settings** pop-up window.
4. Enter a value for the maximum number of events to queue in the **Maximum Pattern States to Analyze Per Packet** field.

5. To disable the inspection of packets that will be rebuilt into larger streams of data before and after stream reassembly in Snort 2, check the **Disable Content Checks on Traffic Subject to Future Reassembly** check box. Inspection before and after reassembly requires more processing overhead and may decrease performance.

   **Important**

   In Snort 3, the **Disable Content Checks on Traffic Subject to Future Reassembly** check box settings are:

   - Checked–Indicates detecting TCP payload before reassembly. It includes inspection of packets before and after stream reassembly. This process requires more processing overhead and may decrease performance.
   - Unchecked–Indicates detecting TCP payload after reassembly.

6. Click **OK**.
7. Click **Save** to save the policy.

**What to do next**

- Deploy configuration changes.

## Regular expression limits overrides for intrusion rules

Describes how to override default regular expression limits for intrusion rules to balance improved detection with system performance.

The default regular expression limits ensure a minimum level of performance. Overriding these limits could increase security, but could also significantly impact performance by permitting packet evaluation against inefficient regular expressions.

> ⚠ **Caution**
>
> Do not override default PCRE limits unless you are an experienced intrusion rule writer with knowledge of the impact of degenerative patterns.

**Table 7: Regular expression constraint options**

| Option | Description |
|---|---|
| Match Limit State | Specifies whether to override **Match Limit**. You have these options:<br>• select **Default** to use the value configured for **Match Limit**<br>• select **Unlimited** to permit an unlimited number of attempts<br>• select **Custom** to specify either a limit of 1 or greater for **Match Limit**, or to specify 0 to completely disable PCRE match evaluations |
| Match Limit | Specifies the number of times to attempt to match a pattern defined in a PCRE regular expression. |

| Option | Description |
|---|---|
| Match Recursion Limit State | Specifies whether to override **Match Recursion Limit**. You have these options:<br>• select **Default** to use the value configured for **Match Recursion Limit**<br>• select **Unlimited** to permit an unlimited number of recursions<br>• select **Custom** to specify either a limit of 1 or greater for **Match Recursion Limit**, or to specify 0 to completely disable PCRE recursions<br><br>Note that for **Match Recursion Limit** to be meaningful, it must be smaller than **Match Limit**. |
| Match Recursion Limit | Specifies the number of recursions when evaluating a PCRE regular expression against the packet payload. |

## Override regular expression limits for intrusion rules

Override regular expression limits for intrusion rules to optimize performance.

Override the default regular expression limits to customize performance settings for intrusion rules according to your network requirements.

Regular expression limits control the processing of pattern matching in intrusion rules. Modifying these limits can help optimize performance based on your specific environment and traffic patterns.

### Procedure

1. In the access control policy editor, click **Advanced**.

   In the new UI, select **Advanced Settings** from the drop-down arrow at the end of the packet flow line.
2. Click **Edit** (✎) next to **Performance Settings**.

   If **View** (👁) appears instead, settings are inherited from an ancestor policy, or you do not have permission to modify the settings. If the configuration is unlocked, uncheck **Inherit from base policy** to enable editing.
3. Click **Regular Expression Limits** in the **Performance Settings** pop-up window.
4. You can modify any of the options as described in Regular expression limits overrides for intrusion rules on page 98.
5. Click **OK**.
6. Click **Save** to save the policy.

### What to do next

- Deploy configuration changes.

## Per packet intrusion event generation limits

Lists the configuration options for controlling intrusion event logging limits when the rules engine evaluates traffic.

When the intrusion rules engine evaluates traffic against rules, it places the events generated for a given packet or packet stream in an event queue, then reports the top events in the queue to the user interface. When configuring the intrusion

event logging limits, you can specify how many events can be placed in the queue and how many are logged, and select the criteria for determining event order within the queue.

**Table 8: Intrusion event logging limits options**

| Option | Description |
|---|---|
| Maximum events stored per packet | The maximum number of events that can be stored for a given packet or packet stream. |
| Maximum events logged per packet | The number of events logged for a given packet or packet stream. This cannot exceed the **Maximum Events Stored Per Packet** value. |
| Prioritize event logging by | The value used to determine event ordering within the event queue. The highest ordered event is reported through the user interface. You can select from:<br>• `priority`, which orders events in the queue by the event priority.<br>• `content_length`, which orders events by the longest identified content match. When events are ordered by content length, rule events always take precedence over decoder and preprocessor events. |

## Limiting intrusion events generated per packet

Configure the intrusion event logging limits to control the number of intrusion events generated per packet.

This task allows you to control the number of intrusion events generated per packet by configuring intrusion event logging limits in the access control policy performance settings.

Use this task when you need to manage intrusion detection system performance by limiting the number of events generated for each packet processed by the firewall.

### Procedure

1. In the access control policy editor, click **Advanced**.

   In the new UI, select **Advanced Settings** from the drop-down arrow at the end of the packet flow line.
2. Click **Edit** (✎) next to **Performance Settings**.

   If **View** (👁) appears instead, settings are inherited from an ancestor policy, or you do not have permission to modify the settings. If the configuration is unlocked, uncheck **Inherit from base policy** to enable editing.
3. Click **Intrusion Event Logging Limits** in the **Performance Settings** pop-up window.
4. You can modify any of the options in Per packet intrusion event generation limits on page 99.
5. Click **OK**.
6. Click **Save** to save the policy.

### What to do next

- Deploy configuration changes.

# Packet and intrusion rule latency threshold configuration

Describes latency-based settings that use thresholding to manage packet and rule processing performance in access control policies.

Packet and intrusion rule latency threshold configuration is a performance management mechanism that

- uses thresholding to manage packet and rule processing performance in access control policies,
- measures elapsed time for packet and rule processing operations, and
- implements protective actions when configurable time thresholds are exceeded.

### Processing mechanisms

This configuration includes two distinct processing mechanisms:

- **Packet latency thresholding**: Measures the total elapsed time taken to process a packet by applicable decoders, preprocessors, and rules, and ceases inspection of the packet if the processing time exceeds a configurable threshold.
- **Rule latency thresholding**: Measures the elapsed time each rule takes to process an individual packet, suspends the violating rule along with a group of related rules for a specified time if the processing time exceeds the rule latency threshold a configurable consecutive number of times, and restores the rules when the suspension expires.

> **Note**
>
> Snort 2 is not supported on Threat Defense version 7.7. For information on Snort 2 features that are supported in versions earlier than 7.7, refer to the Firewall Management Center guide that matches your Firewall Threat Defense version.

## Latency-based performance settings

Describes the configuration mechanism that determines system latency thresholds based on network analysis policy security levels and intrusion rule updates.

Latency-based performance settings are a system configuration mechanism that

- takes performance settings from the latest intrusion rule update deployed on the system,
- applies settings based on the security level of the network analysis policy (NAP) associated with the access control policy, and
- evaluates the most secure network analysis policy among custom rules when multiple policies are configured.

### Policy evaluation logic

The latency settings that are actually applied depend on the security level of the network analysis policy (NAP) associated with the access control policy. Generally, this is the default NAP policy. However, if custom network analysis rules are configured, and if any of these specify a NAP policy that is more secure than the default NAP policy, then latency settings are based on the most secure NAP policy among the custom rules. If the default NAP policy or any custom rules invoke a custom NAP policy, then the security level used in the evaluation is the system-provided base policy on which each custom NAP policy is based.

This policy evaluation logic applies regardless of whether the effective threshold and network analysis configurations are inherited or configured directly in the policy.

## Packet latency thresholding

Describes a software-based latency implementation that measures elapsed time to improve system performance by stopping inspection of packets that require excessive processing time.

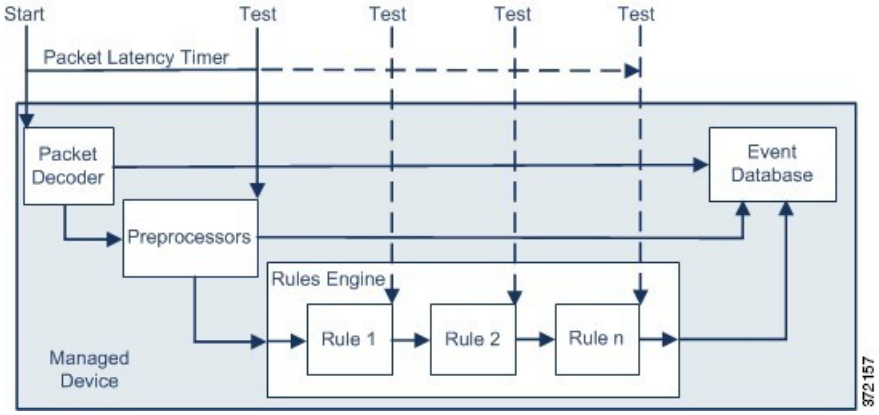
Packet latency thresholding is a software-based latency implementation that

- measures elapsed time, not just processing time, to more accurately reflect the actual time required for the rule to process a packet,
- does not enforce strict timing, and
- can improve system performance by stopping inspection of packets that require excessive processing time.

### Packet latency thresholding operation

A timer starts for each packet when decoder processing begins. Timing continues either until all processing ends for the packet or until the processing time exceeds the threshold at a timing test point.

The trade-off for the performance and latency benefits derived from latency thresholding is that uninspected packets could contain attacks.




Packet latency timing is tested at these test points:

- after the completion of all decoder and preprocessor processing and before rule processing begins
- after processing by each rule

If the processing time exceeds the threshold at any test point, packet inspection ceases.

> **Tip**
>
> Total packet processing time does not include routine TCP stream or IP fragment reassembly times.

Packet latency thresholding has no effect on events triggered by a decoder, preprocessor, or rule processing the packet. Any applicable decoder, preprocessor, or rule triggers normally until a packet is fully processed, or until packet processing ends because the latency threshold is exceeded, whichever comes first. If a drop rule detects an intrusion in an inline deployment, the drop rule triggers an event and the packet is dropped.

> **Note**
>
> No packets are evaluated against rules after processing for that packet ceases because of a packet latency threshold violation. A rule that would have triggered an event cannot trigger that event, and for drop rules, cannot drop the packet.

Packet latency thresholding can improve system performance in both passive and inline deployments, and can reduce latency in inline deployments, by stopping inspection of packets that require excessive processing time. These performance benefits might occur when, for example:

- for both passive and inline deployments, sequential inspection of a packet by multiple rules requires an excessive amount of time
- for inline deployments, a period of poor network performance, such as when someone downloads an extremely large file, slows packet processing

In a passive deployment, stopping the processing of packets might not contribute to restoring network performance because processing simply moves to the next packet.

### Packet latency thresholding notes

Provides guidance on configuring packet latency thresholds and performance settings for packet inspection.

By default, the latency-based performance settings for packet handling are disabled. You may choose to enable it. However, Cisco recommends that you do not change the default value for the threshold setting. The information in this section applies only if you choose to specify custom values.

### Enable packet latency thresholding

Configure packet latency thresholding to optimize network performance.

Enable packet latency thresholding to monitor and manage packet processing delays, which helps optimize network performance and identify potential bottlenecks.

Packet latency thresholding allows you to set performance parameters for packet processing. This feature is useful for monitoring network performance and ensuring optimal packet flow through the system.

### Procedure

1. In the access control policy editor, click **Advanced**.

   In the new UI, select **Advanced Settings** from the drop-down arrow at the end of the packet flow line.
2. Click **Edit** (✎) next to **Latency-Based Performance Settings**.

   If **View** (👁) appears instead, settings are inherited from an ancestor policy, or you do not have permission to modify the settings.
3. Click **Packet Handling** in the **Latency-Based Performance Settings** pop-up window.
4. Check the **Enabled** check box.
5. Click **OK**.
6. Click **Save** to save the policy.

#### What to do next

- Deploy configuration changes.

#### Configure packet latency thresholding

Configure packet latency thresholding to enable latency-based performance settings for packet handling.

This task enables you to configure packet latency thresholding for latency-based performance settings.

By default, the latency-based performance settings for packet handling is disabled. You may choose to enable it. However, Cisco recommends that you do not change the default value for the threshold setting.

#### Procedure

1. In the access control policy editor, click **Advanced**.

   In the new UI, select **Advanced Settings** from the drop-down arrow at the end of the packet flow line.
2. Click **Edit** (✎) next to **Latency-Based Performance Settings**.

   **System** (⚙) > **Monitoring** > **Statistics**
3. If the configuration is unlocked, uncheck **Inherit from base policy** to enable editing.
4. Click **Packet Handling** in the **Latency-Based Performance Settings** pop-up window.

   By default, **Installed Rule Update** is selected. We recommend using this default.

   The values displayed do not reflect the automated settings.
5. If you choose to specify custom values:
   - Check the **Enabled** check box, and see Packet latency thresholding notes on page 103 for recommended minimum **Threshold** settings.
   - You must specify custom values in both the packet handling tab and the rule handling tab.
6. Click **OK**.
7. Click **Save** to save the policy.

#### What to do next

- Deploy configuration changes.

## Rule latency thresholding

Describes a performance optimization feature that measures elapsed time to improve system performance by suspending rules that exceed processing time thresholds.

Rule latency thresholding is a software-based latency implementation that

- measures elapsed time, not just processing time, to more accurately reflect the actual time required for the rule to process a packet,
- does not enforce strict timing, and
- temporarily suspends rules that exceed specified processing time thresholds to improve system performance.

### Rule latency thresholding operations

A timer measures the processing time each time a packet is processed against a group of rules. Any time the rule processing time exceeds a specified rule latency threshold, the system increments a counter. If the number of consecutive threshold violations reaches a specified number, the system takes these actions:

- suspends the rules for the specified period
- triggers an event indicating the rules have been suspended
- re-enables the rules when the suspension expires
- triggers an event indicating the rules have been re-enabled

The system zeroes the counter when the group of rules has been suspended, or when rule violations are not consecutive. Permitting some consecutive violations before suspending rules lets you ignore occasional rule violations that might have negligible impact on performance and focus instead on the more significant impact of rules that repeatedly exceed the rule latency threshold.

The trade-off for the performance and latency benefits derived from latency thresholding is that uninspected packets could contain attacks.

Rule latency thresholding has no effect on intrusion events triggered by the rules processing the packet. A rule triggers an event for any intrusion detected in the packet, regardless of whether the rule processing time exceeds the threshold. If the rule detecting the intrusion is a drop rule in an inline deployment, the packet is dropped. When a drop rule detects an intrusion in a packet that results in the rule being suspended, the drop rule triggers an intrusion event, the packet is dropped, and that rule and all related rules are suspended.

> **Note**
>
> Packets are not evaluated against suspended rules. A suspended rule that would have triggered an event cannot trigger that event and, for drop rules, cannot drop the packet.

Rule latency thresholding can improve system performance in both passive and inline deployments, and can reduce latency in inline deployments, by suspending rules that take the most time to process packets. Packets are not evaluated again against suspended rules until a configurable time expires, giving the overloaded device time to recover. These performance benefits might occur when:

- hastily written, largely untested rules require an excessive amount of processing time
- a period of poor network performance, such as when someone downloads an extremely large file, causes slow packet inspection

### Rule latency thresholding examples

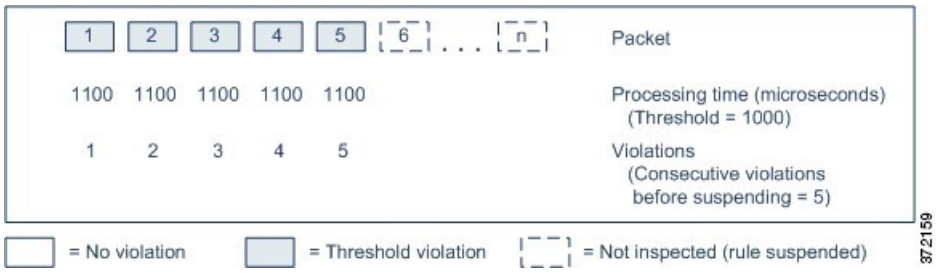
This example shows five consecutive rule processing times that do not result in rule suspension.




In this example, the time required to process each of the first three packets violates the rule latency threshold of 1000 microseconds, and the violations counter increments with each violation. Processing of the fourth packet does not violate

the threshold, and the violations counter resets to zero. The fifth packet violates the threshold and the violations counter restarts at one.

This example shows five consecutive rule processing times that do result in rule suspension.




In the second example, the time required to process each of the five packets violates the rule latency threshold of 1000 microseconds. The group of rules is suspended because the rule processing time of 1100 microseconds for each packet violates the threshold of 1000 microseconds for the specified five consecutive violations. Any subsequent packets, represented in the figure as packets 6 through n, are not examined against suspended rules until the suspension expires. If more packets occur after the rules are re-enabled, the violations counter begins again at zero.

### Rule latency thresholding notes

Provides configuration options and guidance for rule latency thresholding performance settings.

Rule latency thresholding suspends rules for the time specified by **Suspension Time** when the time rules take to process a packet exceeds **Threshold** for the consecutive number of times specified by **Consecutive Threshold Violations Before Suspending Rule**.

By default, latency-based performance settings for both packet and rule handling are automatically populated by the latest deployed intrusion rule update, and we recommend that you do not change the default.

The information in this topic applies only if you choose to specify custom values.

You can enable rule 134:1 to generate an event when rules are suspended, and rule 134:2 to generate an event when suspended rules are enabled.

**Table 9: Rule latency thresholding options**

| Option | Description |
|---|---|
| Threshold | Specifies the time in microseconds that rules should not exceed when examining a packet. |
| Consecutive Threshold Violations Before Suspending Rule | Specifies the consecutive number of times rules can take longer than the time set for **Threshold** to inspect packets before rules are suspended. |
| Suspension Time | Specifies the number of seconds to suspend a group of rules. |

### Configure rule latency thresholding

Configure rule latency thresholding to customize performance settings for latency-based rule handling in access control policies.

Configure rule latency thresholding to customize how the system handles rules when latency conditions are detected, improving overall performance and system responsiveness.

By default, latency-based performance settings for both packet and rule handling are automatically populated by the latest deployed intrusion rule update, and we recommend that you do not change the default.

**Procedure**

1. In the access control policy editor, click **Advanced**.

   In the new UI, select **Advanced Settings** from the drop-down arrow at the end of the packet flow line.

2. Click **Edit** (✎) next to **Latency-Based Performance Settings**.

   If **View** (👁) appears instead, settings are inherited from an ancestor policy, or you do not have permission to modify the settings. If the configuration is unlocked, uncheck **Inherit from base policy** to enable editing.

3. Click **Rule Handling** in the **Latency-Based Performance Settings** pop-up window.

   By default, **Installed Rule Update** is selected. We recommend using this default.

   The values displayed do not reflect the automated settings.

4. If you choose to specify custom values:
   - You can configure any of the options in Rule latency thresholding notes on page 106.
   - You must specify custom values in both the packet handling tab and the rule handling tab.

5. Click **OK**.
6. Click **Save** to save the policy.

**What to do next**

- If you want to generate events, enable latency rules 134:1 and 134:2.
- Deploy configuration changes.

## Intrusion performance statistic logging configuration

Lists the configuration options for intrusion performance statistic logging settings and troubleshooting options.

This reference provides information about intrusion performance statistic logging configuration options, including sample time settings, minimum packet requirements, and troubleshooting options for logging session and protocol distribution data.

### Sample time (seconds) and minimum number of packets

When the number of seconds specified elapses between performance statistics updates, the system verifies it has analyzed the specified number of packets. If it has, the system updates performance statistics. Otherwise, the system waits until it analyzes the specified number of packets.

> **Caution**
>
> Configuring a very low value, such as one second, for the sample time can greatly impact the device. The device may experience disk space issues, and its operation may be affected by the volume of performance statistics logged. To avoid these issues, do not set a very low value.

#### Troubleshooting options: log session/protocol distribution

Support might ask you during a troubleshooting call to log protocol distribution, packet length, and port statistics.

> **Caution**
>
> Do not enable **Log Session/Protocol Distribution** unless instructed to by Support. Note that for Classic devices only, enabling or disabling **Log Session/Protocol Distribution** restarts the Snort process when you deploy configuration changes, temporarily interrupting traffic inspection. Whether traffic drops during this interruption or passes without further inspection depends on how the assigned device handles traffic.

#### Troubleshooting options: summary

Support might ask you during a troubleshooting call to configure the system to calculate the performance statistics only when the Snort process is shut down or restarted. To enable this option, you must also enable the **Log Session/Protocol Distribution** troubleshooting option.

> **Caution**
>
> Do not enable **Summary** unless instructed to do so by Support.

## Configure intrusion performance statistic logging

Configure intrusion performance statistic logging to customize sampling parameters and troubleshoot options for monitoring device performance.

Configure intrusion performance statistic logging to customize how the system samples and logs performance statistics for monitoring and troubleshooting purposes.

Performance statistics logging allows you to monitor device performance by sampling statistics at defined intervals. Proper configuration ensures optimal device performance while providing necessary monitoring data.

#### Procedure

1. In the access control policy editor, click **Advanced**, then click **Edit** (✎) next to **Performance Settings**.

   In the new UI, select **Advanced Settings** from the drop-down arrow at the end of the packet flow line.

   If **View** (👁) appears instead, settings are inherited from an ancestor policy, or you do not have permission to modify the settings. If the configuration is unlocked, uncheck **Inherit from base policy** to enable editing.

2. Click **Performance Statistics** in the pop-up window that appears.
3. Modify the **Sample time** or **Minimum number of packets** as described in Intrusion performance statistic logging configuration on page 107.

> **Caution**
>
> Configuring a very low value, such as one second, for the **Sample time** can greatly impact the device. The device may experience disk space issues, and its operation may be affected by the volume of performance statistics logged. To avoid these issues, do not set a very low value.

4. Optionally, expand the **Troubleshoot Options** section and modify those options only if asked to do so by Support.
5. Click **OK**.

---

### What to do next

- Deploy configuration changes.

# 5 Network Analysis Policies

**Topics:**


- Network analysis policies
- Manage network analysis policies
- Snort 3 definitions and terminologies for network analysis policies
- Custom network analysis policy creation for Snort 3
- Network analysis policy settings and cached changes
- Generate Snort 3 recommendations


Provides an overview of network analysis policies, including prerequisites, creation, and settings management.

This chapter provides an insight into network analysis policy basics, prerequisites, and how to manage network analysis policies. It also provides information on custom network analysis policy creation and network analysis policy settings.

# Network analysis policies

Describes traffic preprocessing policies that govern security and connectivity options in access control systems.

A *network analysis policy* is a traffic preprocessing configuration that

- governs many traffic preprocessing options and is invoked by advanced settings in your access control policy,
- performs preprocessing after Security Intelligence matching and SSL decryption, and
- completes processing before intrusion or file inspection begins.

### Default and custom network analysis policies

By default, the system uses the *Balanced Security and Connectivity* network analysis policy to preprocess all traffic handled by an access control policy. However, you can choose a different default network analysis policy to perform this preprocessing. For your convenience, the system provides a choice of several non-modifiable network analysis policies, which are tuned for a specific balance of security and connectivity by the Talos Intelligence Group. You can also create a custom network analysis policy with custom preprocessing settings.

**Note**

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. Network analysis and intrusion policies work together to examine your traffic.

You can also tailor traffic preprocessing options to specific security zones, networks, and VLANs by creating multiple custom network analysis policies, then assigning them to preprocess different traffic.

# Manage network analysis policies

Configure network analysis policy management by accessing, creating, editing, deleting, or generating reports for policies in the management center.

This task allows you to perform various management operations on network analysis policies, including creation, editing, deletion, comparison, and report generation.

Under your user name in the toolbar, the system displays a tree of available domains. To switch domains, choose the domain you want to access.

> **Note**
>
> Snort 2 is not supported on threat defense version 7.7. For information on Snort 2 features that are supported in versions earlier than 7.7, refer to the management center guide that matches your threat defense version.

**Procedure**

1. Choose one of these paths to access the network analysis policy.
   - **Policies** > **Access Control heading** > **Access Control**, and then click **Network Analysis Policy**
   - **Policies** > **Access Control heading** > **Intrusion**, and then click **Network Analysis Policies**

   > **Note**
   >
   > If your custom user role limits access to the first path listed here, use the second path to access the policy.

2. Manage your network analysis policy:
   - Create–If you want to create a new network analysis policy, click **Create Policy**.

     Two versions of the network analysis policy are created, a **Snort 2 Version** and a **Snort 3 Version**.
     - For the Snort 2 version, see *Custom Network Analysis Policy Creation for Snort 2* in the *Cisco Secure Firewall Management Center Configuration Guide*.
     - For the Snort 3 version, see Custom network analysis policy creation for Snort 3 on page 115.
   - Delete–If you want to delete a network analysis policy, click the **Delete** icon, then confirm that you want to delete the policy. You cannot delete a network analysis policy if an access control policy references it.

     If the controls are dimmed, the configuration belongs to an ancestor domain, or you do not have permission to modify the configuration.
   - Edit–If you want to edit an existing network analysis policy, click the **Edit** icon.

     If **View** ( ) appears instead, the configuration belongs to an ancestor domain, or you do not have permission to modify the configuration.
   - Report–Click the **Report** icon; see *Generating Current Policy Reports* in the *Cisco Secure Firewall Management Center Configuration Guide*.

## Snort 3 definitions and terminologies for network analysis policies

Lists the Snort 3 concepts and terms used in the Network Analysis Policy.

This table lists the Snort 3 concepts and terms used in the Network Analysis Policy.

**Table 10: Snort 3 definitions and terminologies for network analysis policy**

| Term | Description |
|---|---|
| Inspectors | Inspectors are plugins that process packets (similar to the Snort 2 preprocessor). |
| Binder inspector | The binder inspector defines the flow when a particular inspector must be accessed and considered.<br>When the traffic matches the conditions defined in the binder inspector, only then do the values and configurations for that inspector come into effect.<br>For more information, see *Binder Inspector* in Custom network analysis policy creation for Snort 3 on page 115. |
| Singleton inspectors | Singleton inspectors contain one instance. These inspectors do not support adding more instances like multiton inspectors. Settings for a singleton inspector apply to all traffic that matches the inspector, not just a specific traffic segment.<br>For more information, see *Singleton Inspectors* in Custom network analysis policy creation for Snort 3 on page 115. |
| Multiton inspectors | Multiton inspectors contain multiple instances which you can configure as needed. These inspectors support configuring settings based on specific conditions, such as network, port, and VLAN. One set of supported settings is called an instance.<br>For more information, see *Multiton Inspectors* in Custom network analysis policy creation for Snort 3 on page 115. |
| Schema | The schema file is based on the OpenAPI JSON specification, and it validates the content that you upload or download. You can download the schema file and open it using any third-party JSON editor, such as Swagger editor. The schema file helps you to identify what parameters can be configured for inspectors with their corresponding allowed values, range, and accepted patterns to be used.<br>For more information, see Customize the network analysis policy on page 123. |
| Sample file | It is a pre-existing template that contains example configurations to help you with configuring the inspectors.<br>You can refer to the example configurations included in the sample file and make any changes you require.<br>For more information, see Customize the network analysis policy on page 123. |

| Term | Description |
| --- | --- |
| Full configuration | You can download the entire inspector configurations in a single file.<br><br>All information regarding the inspector configuration is available in this file.<br><br>The full configuration is a merged configuration of the default configuration (provided as part of the LSP updates by Cisco Talos) and the custom NAP inspector configurations.<br><br>For more information, see Customize the network analysis policy on page 123. |
| Overridden configuration | In the **Snort 3 Version** of the network analysis policy page:<br><br>• Under **Actions** > **Upload**, you can click **Overridden Configuration** to upload the JSON file that contains the overridden configuration.<br><br>• Under **Actions** > **Download**, you can click **Overridden Configuration** to download the inspector configuration that has been overridden.<br><br>If you have not overridden any inspector configuration, then this option is disabled. When you override the inspector configuration, then this option is enabled automatically to allow you to download.<br><br>For more information, see Customize the network analysis policy on page 123. |

**Related concepts**

Custom network analysis policy creation for Snort 3 on page 115

Describes the process and components involved in creating customized network analysis policies for Snort 3 environments.

Network analysis policy mapping on page 120

Describes the mapping information provided by Cisco Talos for network analysis policies.

**Related tasks**

Customize the network analysis policy on page 123

Configure the Snort 3 version of the network analysis policy to meet your specific requirements.

## Custom network analysis policy creation for Snort 3

Describes the process and components involved in creating customized network analysis policies for Snort 3 environments.

A custom network analysis policy creation for Snort 3 is a data-driven configuration process that

- enables advanced users to customize the default network analysis policy for specific network requirements or to optimize performance, and
- utilizes JSON and JSON Schema based on the OpenAPI specification to configure inspectors and settings.

### Network analysis policy customization overview

The default network analysis policy is tuned for typical network requirements and optimal performance. In most situations, you do not need to customize the policy. However, when you have a specific network requirement or when you are facing performance issues, the default network analysis policy can be customized. Note that customizing the network analysis policy is an advanced configuration that should only be done by advanced users or Cisco Support.

In Snort 3, the list of inspectors and settings are not in a one-to-one mapping with the Snort 2 list of preprocessors and settings. The number of inspectors and settings available in Firewall Management Center forms a subset of those that Snort 3 supports. See https://snort.org/snort3 for more information on Snort 3. See https://www.cisco.com/go/snort3-inspectors for more information on the inspectors available in Firewall Management Center.

**Note**

- While upgrading the Firewall Management Center to the 7.0 release, the changes that were done in the Snort 2 version of the network analysis policy are not migrated to Snort 3 after the upgrade.
- Unlike the intrusion policy, there is no option to synchronize Snort 2 network analysis policy settings to Snort 3.

### Default inspector updates

Lightweight Security Package (LSP) updates may contain new inspectors or modifications to integer ranges for existing inspector configurations. After you install an LSP, new inspectors or updated ranges will be available under **Inspectors** in the **Snort 3 Version** of your network analysis policy.

### Binder inspector

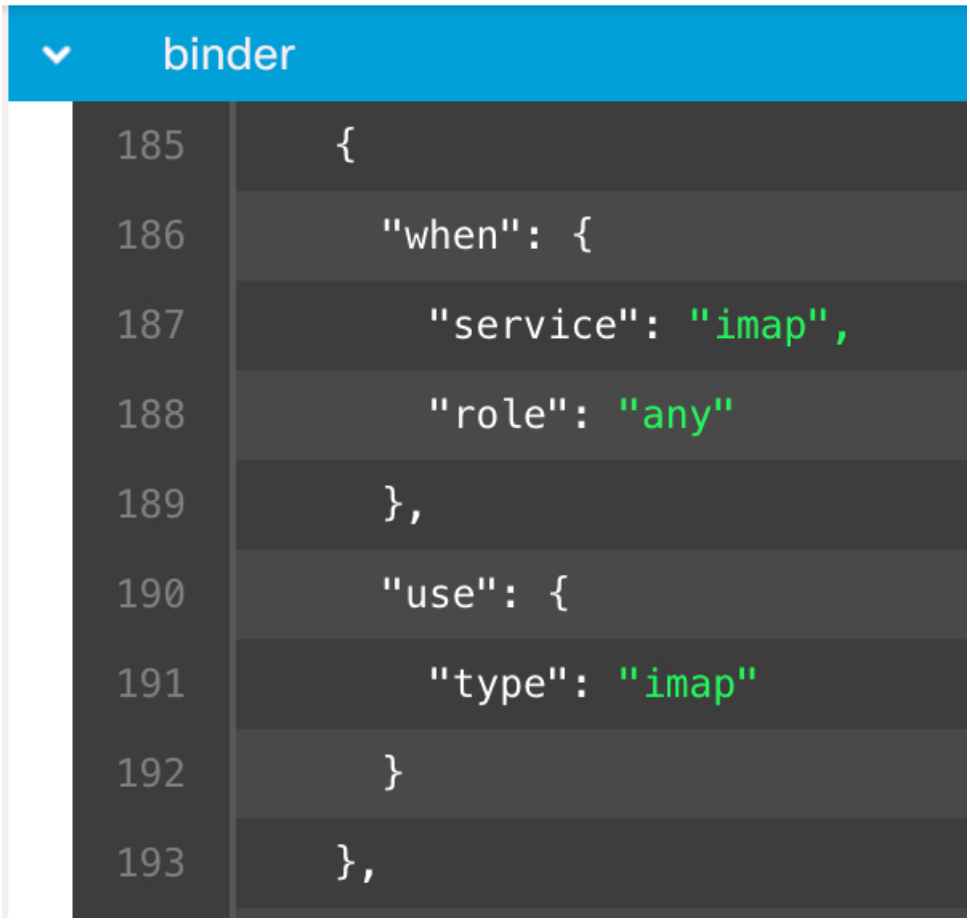
Binder inspector defines the flow when a particular inspector has to be accessed and taken into consideration. When the traffic matches the conditions defined in the binder inspector, only then the values and configurations for that inspector come into effect. For example:

For the *imap* inspector, the binder defines the following condition when it has to be accessed. That is when:

- Service is equal to imap.
- Role is equal to any.

a

If these conditions are met, then use the type imap.




### Singleton inspectors

Singleton inspectors contain a single instance. These inspectors do not support adding more instances like multiton inspectors. Settings of a singleton inspector apply to all traffic, not to a specific segment.

For example:

```
{
   "normalizer":{
      "enabled":true,
      "type":"singleton",
      "data":{
         "ip4":{
            "df":true
         }
      }
   }
}
```

### Multiton inspectors

Multiton inspectors contain multiple instances which you can configure as needed. These inspectors support configuring settings based on specific conditions, such as network, port, and VLAN. One set of supported settings is called an instance. There is a default instance, and you can also add additional instances based on specific conditions. If the traffic matches that condition, the settings from that instance are applied. Otherwise, the settings from the default instance are applied. Also, the name of the default instance is the same as the name of the inspector.

For a multiton inspector, when you upload the overridden inspector configuration, you also need to include and define a matching binder condition (conditions under when the inspector has to be accessed or used) for each instance in the JSON file, otherwise, the upload will result in an error. You can also create new instances. Ensure that you include a binder condition for each new instance you create to avoid errors.

For example:

- Multiton inspector where the default instance is modified.

```
{
   "http_inspect":{
      "enabled":true,
      "type":"multiton",
      "instances":[
         {
            "name":"http_inspect",
            "data":{
               "response_depth":5000
            }
         }
      ]
   }
}
```

- Multiton inspector where the default instance and default binder is modified.

```
{
   "http_inspect":{
      "enabled":true,
      "type":"multiton",
      "instances":[
         {
            "name":"http_inspect",
            "data":{
               "response_depth":5000
            }
         }
      ]
   },
   "binder":{
      "type":"binder",
      "enabled":true,
      "rules":[
         {
            "use":{
               "type":"http_inspect"
            },
            "when":{
               "role":"any",
               "ports":"8080",
               "proto":"tcp",
               "service":"http"
            }
         }
      ]
   }
}
```

- Multiton inspector where a custom instance and a custom binder is added.

```
{
   "http_inspect":{
```

```
      "enabled":true,
      "type":"multiton",
      "instances":[
         {
            "name":"http_inspect1",
            "data":{
               "response_depth":5000
            }
         }
      ]
   },
   "binder":{
      "type":"binder",
      "enabled":true,
      "rules":[
         {
            "use":{
               "type":"http_inspect",
               "name":"http_inspect1"
            },
            "when":{
               "role":"any",
               "ports":"8080",
               "proto":"tcp",
               "service":"http"
            }
         }
      ]
   }
}
```

## Common Industrial Protocol safety

Describes a set of extensions to the Common Industrial Protocol (CIP) that enables the safe operation of devices and provides fail-safe communication between different nodes on a CIP network.

Common Industrial Protocol (CIP) safety is a set of extensions to the CIP that

- enables the safe operation of devices,
- provides fail-safe communication between different nodes on a CIP network, and
- comprises two main components for safety parameter exchange and safety information transmission.

### CIP safety protocol components

The CIP safety protocol comprises two main components:

- CIP safety segments–Used in Forward Open messages to exchange safety parameters for the subsequent safety session.
- CIP safety messages–Used to exchange actual safety information.

The CIP inspector detects and identifies:

- CIP as a service and client
- Payloads, such as CIP Read, CIP Admin, CIP Infrastructure, and CIP Write

The CIP inspector can parse the CIP segments and detect the CIP Safety segments in the Forward Open requests.

To test the CIP safety feature, you must enable the CIP inspector. See Detect and block safety segments in CIP packets on page 120.

## Detect and block safety segments in CIP packets

Configure the CIP inspector to detect and block safety segments in CIP packets while allowing other CIP packets.

This task enables detection and blocking of CIP safety segments while allowing other CIP packets to pass through.

Use this procedure to detect and block CIP safety segments while allowing other CIP packets:

- Create a custom network analysis policy called **cip_safety**.
- Create access control rules in your access control policy to block CIP safety and to allow all other packets.

To test the CIP safety feature, enable the CIP inspector in the management center and assign it to an access control policy.

### Procedure

1. Go to **Policies** > **Access Control heading** > **Intrusion** > **Network Analysis Policies**.
2. Click the **Snort 3 Version** of the network analysis policy **cip_safety** that you created.
3. Under **Inspectors**, click **CIP** to expand it.

   The default configuration appears in the left column and the overridden configuration appears in the right column under the inspector.
4. Under **Overridden Configuration** on the right column, click the **Edit Inspector** icon and change the "enabled" field in **CIP** from false (default) to true.
5. Click **OK** and then click **Save**.
6. To assign the **CIP** inspector to the access control policy, choose **Policies** > **Access Control heading** > **Access Control**, click **Edit** and choose the **Advanced Settings** option from the **More** drop-down arrow at the end of the packet flow line.
7. Click **Edit** (✎) next to **Network Analysis and Intrusion Policies**.
8. In the **Network Analysis and Intrusion Policies** window, choose the access control policy **cip_safety** that you created from the **Default Network Analysis Policy** drop-down list.

   The CIP inspector is now enabled in the management center and you can create the custom access control rules to block CIP safety and to allow all other CIP packets.
9. After you send live traffic containing CIP safety packet flows, go to **Unified Events** to verify that the payload is the expected payload that contains CIP safety packet logs for the detection and block use case as mentioned in this procedure.

   **CIP** is detected as an application protocol and client (see the **Application Protocol** and **Client Application** fields), and **CIP Safety** is shown under the **Web Application** field.

## Network analysis policy mapping

Describes the mapping information provided by Cisco Talos for network analysis policies.

Network analysis policy mapping is a correlation mechanism that

- provides mapping information for network analysis policies,
- finds the corresponding Snort 2 version of policies for the Snort 3 version, and

- ensures that the Snort 3 version of policies has its equivalent Snort 2 version.

## View network analysis policy mapping

View the automatic mapping between Snort 3 and Snort 2 network analysis policies in the management interface.

View which Snort 3 network analysis policies are automatically mapped to their Snort 2 equivalent policies in the system.

Network analysis policy mapping allows you to see the relationship between Snort 3 and Snort 2 policies when transitioning between versions or managing both simultaneously.

**Procedure**

1. Go to **Policies** > **Access Control heading** > **Intrusion** > **Network Analysis Policies**.
2. Click **NAP Mapping**.
3. Expand the arrow for **View Mappings**.

   The Snort 3 network analysis policies that are automatically mapped to a Snort 2 equivalent policy are displayed.
4. Click **OK**.

## Create a network analysis policy

Create a network analysis policy with both Snort 2 and Snort 3 versions for network inspection.

Create a new network analysis policy that provides both Snort 2 and Snort 3 versions for network traffic inspection and analysis.

All the existing network analysis policies are available in Firewall Management Center with their corresponding Snort 2 and Snort 3 versions. When you create a new network analysis policy, it is created with both the Snort 2 version and the Snort 3 version.

**Procedure**

1. Go to **Policies** > **Access Control heading** > **Intrusion** > **Network Analysis Policies**.
2. Click **Create Policy**.
3. Enter the **Name** and **Description**.
4. Select a **Base Policy** and click **Save**.

The new network analysis policy is created with its corresponding **Snort 2 Version** and **Snort 3 Version**.

## Modify the network analysis policy

Configure the network analysis policy to change its name, description, or the base policy.

This task allows you to update the configuration of an existing network analysis policy by modifying its properties such as name, description, or base policy settings.

You can modify the network analysis policy to change its name, description, or the base policy.

**Procedure**

1. Go to **Policies** > **Access Control heading** > **Intrusion** > **Network Analysis Policies**.

2. Click **Edit** to change the name, description, inspection mode, or the base policy.

> **Attention**
>
> **Detection mode deprecation:** From management center 7.4.0 onwards, for a network analysis policy (NAP), the **Detection** inspection mode is deprecated and will be removed in an upcoming release.
>
> The **Detection** mode was intended to be used as a test mode so that you can enable inspections and see how they behave in your network before setting it to drop traffic, that is, to show traffic that would be dropped.
>
> This behavior is improved where all inspector drops are controlled by the rule state, and you can set each one to generate events. This is done to test them before configuring the rule state to drop traffic. As we now have granular control over traffic drops in Snort 3, the **Detection** mode only adds more complexity to the product and is not needed, so the detection mode is deprecated.
>
> If you change a NAP in **Detection** mode to **Prevention**, the NAP that processes the traffic of intrusion events and have the result "will be dropped" will now be "dropped" and the corresponding traffic will drop the traffic from these events. This is applicable for rules whose GIDs are not 1 or 3. GIDs 1 and 3 are text/compiled rules (typically provided by Talos or from your custom/imported rules) and all other GIDs are inspections for anomalies. These are more uncommon rules to trigger in a network. Changing to **Prevention** mode is unlikely to have any impact on the traffic. You need to just disable the intrusion rule that is applicable for the dropped traffic and set it to just generate or disable.
>
> We recommend you choose **Prevention** as the inspection mode, but if you choose **Prevention**, you cannot revert to **Detection** mode.

> **Note**
>
> If you edit the network analysis policy name, description, base policy, and inspection mode, the edits are applied to both the Snort 2 and Snort 3 versions. If you want to change the inspection mode for a specific version, then you can do that from within the network analysis policy page for that respective version.

3. Click **Save**.

## Search for an inspector on the Network Analysis Policy window

Configure inspector search functionality within the Snort 3 version on the network analysis policy window.

This task allows you to quickly locate specific inspectors within the network analysis policy interface by using search functionality.

On the Snort 3 version of the network analysis policy window, you may need to search for an inspector by entering any relevant text in the search bar.

### Procedure

1. Go to **Policies** > **Access Control heading** > **Intrusion** > **Network Analysis Policies**.
2. Go to the **Snort 3 Version** of the network analysis policy.
3. Enter the name of an inspector or any relevant text to search for in the **Search** bar.

All the inspectors matching the text you search for are displayed.

For example, if you enter `pop`, then the pop inspector and the binder inspector are shown as matching results on the screen.

## Copy the inspector configuration

Configure inspector settings by copying the configuration for the Snort 3 version of the network analysis policy.

This task describes how to copy inspector configurations.

You can copy the inspector configuration for the Snort 3 version of the network analysis policy according to your requirements.

**Procedure**

1. Go to **Policies** > **Access Control heading** > **Intrusion** > **Network Analysis Policies**.
2. Go to the **Snort 3 Version** of the network analysis policy.
3. Under **Inspectors**, expand the required inspector for which you want to copy the configuration.

   The default configuration is displayed on the left column and the overridden configuration is displayed on the right column under the inspector.
4. Click the **Copy to clipboard** icon to copy the inspector configuration to the clipboard for one or both of these options.
   - **Default Configuration** in the left column
   - **Overridden Configuration** in the right column
5. Paste the copied inspector configuration to a JSON editor to make any edits you may require.

**Related tasks**

Customize the network analysis policy on page 123

Configure the Snort 3 version of the network analysis policy to meet your specific requirements.

## Customize the network analysis policy

Configure the Snort 3 version of the network analysis policy to meet your specific requirements.

Customize the network analysis policy to adapt Snort 3 configurations according to your security requirements.

You can customize the Snort 3 version of the network analysis policy according to your requirements.

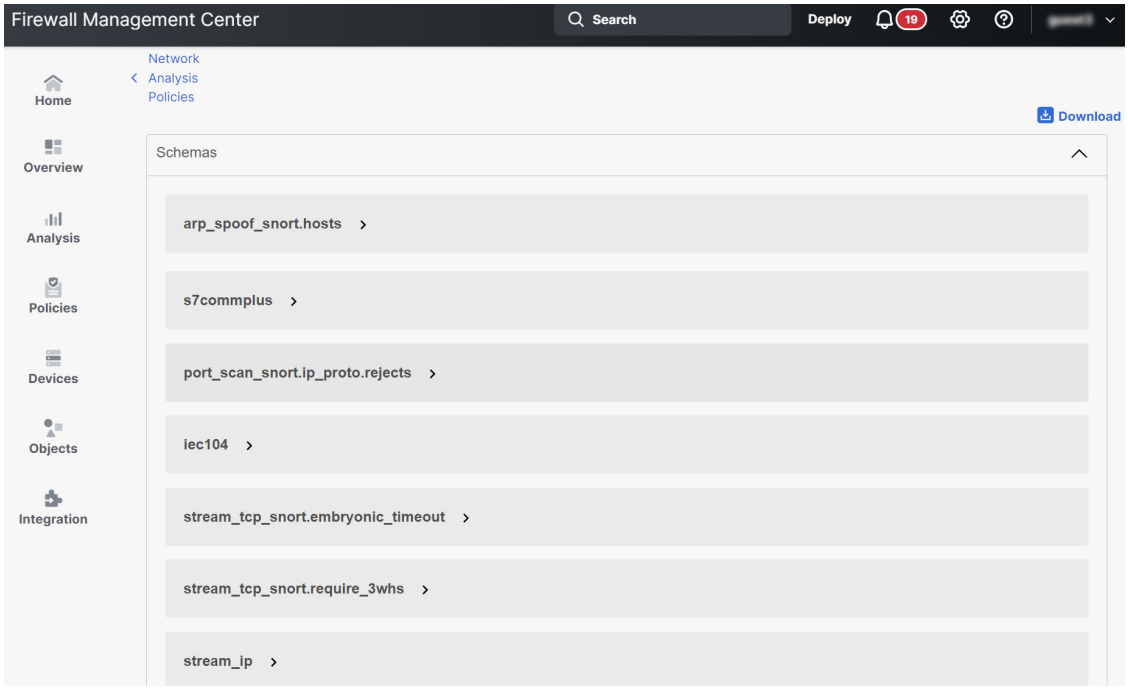
**Procedure**

1. Go to **Policies** > **Access Control heading** > **Intrusion** > **Network Analysis Policies**.
2. Go to the **Snort 3 Version** of the network analysis policy.
3. Click the **Actions** dropdown menu.

   The following options are displayed:
   - View Schema
   - Download Schema / Download Sample File / Template

- Download Full Configuration
- Download Overridden Configuration
- Upload Overridden Configuration

4. Click **View Schema** to open the schema file directly in a browser.




5. You can download the schema file, sample file / template, full configuration, or overridden configuration as needed.

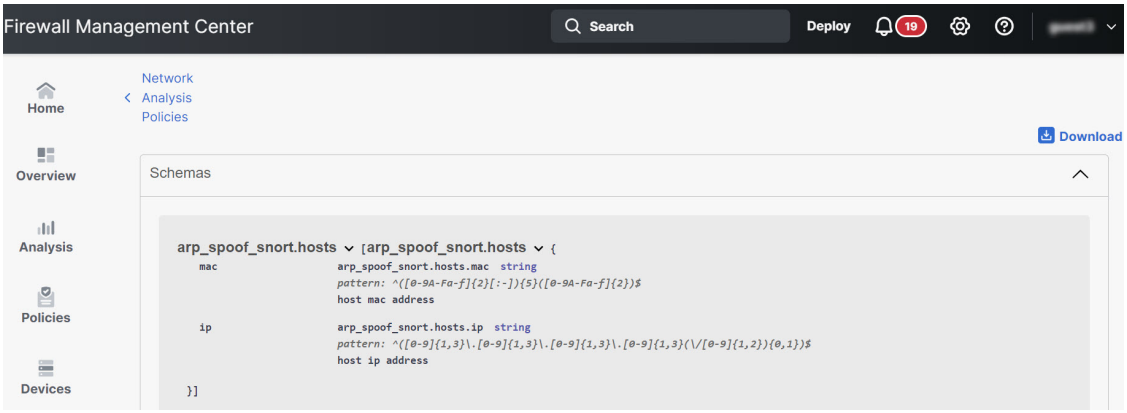
   These options provide you an insight about the allowed values, range, and patterns, existing and default inspector configurations, and overridden inspector configurations.

   a) Click **Download Schema** to download the schema file.

      The schema file validates the content that you upload or download. You can download the schema file and open it using any third-party JSON editor. The schema file helps you identify which parameters can be configured for inspectors, along with their allowed values, ranges, and accepted patterns.

      For example, for the *arp_spoof_snort* inspector, you can configure the hosts. The hosts include the *mac* and *ip* address values. The schema file shows the following accepted pattern for these values.

      - **mac** - `pattern: ^([0-9A-Fa-f]{2}[:-]){5}([0-9A-Fa-f]{2})$`
      - **ip** - `pattern: ^([0-9]{1,3}.[0-9]{1,3}.[0-9]{1,3}.[0-9]{1,3}(/[0-9]{1,2}){0,1})$`




You must provide the values, range, patterns according to the accepted ones in the schema file to be able to successfully override the inspector configuration, otherwise, you get an error message.

b) Click **Download Sample File / Template** to use a pre-existing template that contains example configurations to help you with configuring the inspectors.

You can refer to the example configurations included in the sample file and make any changes that you may require.

c) Click **Download Full Configuration** to download the entire inspector configurations in a single JSON file.

You can download the full configuration to find the information you need, rather than expanding the inspectors separately. This file contains all information about the inspector configuration.

d) Click **Download Overridden Configuration** to download the inspector configuration that has been overridden.

**6.** To override the existing configuration, follow these steps.

You can choose to override an inspector configuration using these ways.

- Make inline edits for an inspector directly on the Firewall Management Center. See the topic **Make Inline Edit for an Inspector to Override Configuration** in the **Getting Started with Network Analysis Policies** chapter of the *Cisco Secure Firewall Management Center Snort 3 Configuration Guide*.
- Continue to follow the current procedure of using the **Actions** dropdown menu to upload the overridden configuration file.

If you chose to make inline edits directly in the Firewall Management Center, then you do not need to complete this procedure any further. Otherwise, you must complete this procedure completely.

a) Under **Inspectors**, expand the required inspector for which you want to override the default configuration.

The default configuration is displayed on the left column and the overridden configuration is displayed on the right column under the inspector.

You may need to search for an inspector by entering any relevant text in in the search bar.

b) Click the **Copy to clipboard** icon to copy the default inspector configuration to the clipboard.

c) Create a JSON file and paste the default configuration in it.

d) Keep the inspector configuration that you want to override, and remove all other configuration and instances from the JSON file.

You can also use the **Sample File / Template** to understand how to override the default configuration. This is a sample file that includes JSON snippets explaining how you can customize the network analysis policy for Snort 3.

e) Make changes to the inspector configuration as needed.

Validate the changes and make sure they conform to the schema file. For multiton inspectors, make sure that the binder conditions for all instances are included in the JSON file. See *Multiton Inspectors* in the topic **Custom**

**Network Analysis Policy Creation for Snort 3** in the *Cisco Secure Firewall Management Center Snort 3 Configuration Guide* for more information.

f) If you are copying any further default inspector configurations, add the inspector configuration to the existing file that contains the overridden configuration.

> **Note**
>
> The copied inspector configuration must comply with the JSON standards.

g) Save the overridden configuration file to your system.

7. From the **Actions** dropdown menu, choose Upload Overridden Configuration to upload the JSON file that contains the overridden configuration.

> **Caution**
>
> Upload only the changes that you require. You should not upload the entire configuration as it makes the overrides sticky in nature and therefore, any subsequent changes to the default configuration as part of the LSP updates would not be applied.

You can drag and drop a file or click to browse to the JSON file saved in your system that contains the overridden inspector configuration.

- **Merge inspector overrides** – Content in the uploaded file is merged with the existing configuration if there is no common inspector. If there are common inspectors, then the content in the uploaded file (for common inspectors) takes precedence over the previous content, and it replaces the previous configuration for those inspectors.
- **Replace inspector overrides** – Removes all previous overrides and replaces them with the new content in the uploaded file.

> **Attention**
>
> Choosing this option deletes all the previous overrides. Review your choice carefully before using this option to override the configuration.

If any error occurs while uploading the overridden inspectors, you see the error in the **Upload Overridden Configuration File** pop-up window. You can also download the file with the error, fix the error, and reupload the file.

8. In the **Upload Overridden Configuration File** pop-up window, click **Import** to upload the overridden inspector configuration.

After you upload the overridden inspector configuration, you will see an orange icon next to the inspector that signifies that it is an overridden inspector.

Also, the **Overridden Configuration** column under the inspector shows the overridden value.

You can also view all the overridden inspectors using the **Show Overrides Only** checkbox adjacent to the Search bar.

> **Note**
>
> Make sure that you always download the overridden configuration, open the JSON file, and append any new changes/overrides to the inspector configurations to this file. This action is needed so that you do not lose the old overridden configurations.

9. (Optional) Take a backup of the overridden configuration file on your system before making any new inspector configuration changes.

> **Tip**
>
> We recommend that you take a backup from time to time as you override the inspector configuration.

## Make inline edit for an inspector to override configuration

Configure inline edits for inspector configurations to override default settings in Snort 3 network analysis policies.

This task allows you to make inline edits for inspector configurations to override the default configuration according to your requirements in the Snort 3 version of the network analysis policy.

For the Snort 3 version of the network analysis policy, you can make an inline edit for the inspector configuration to override the configuration according to your requirements.

Alternatively, you can also use the **Actions** drop-down menu to upload the overridden configuration file. See Customize the network analysis policy on page 123 for more information.

### Procedure

1. Go to **Policies** > **Access Control heading** > **Intrusion** > **Network Analysis Policies**.
2. Go to the **Snort 3 Version** of the network analysis policy.
3. Under **Inspectors**, expand the required inspector for which you want to override the default setting.

   The default configuration is displayed on the left column and the overridden configuration is displayed on the right column under the inspector.

4. Under the **Overridden Configuration** in the right column, click **Edit Inspector** (Pencil) icon to make changes to the inspector configuration.

   The Override Configuration pop-up appears where you can make the required edits.

**Note**

- Make sure that you keep only those settings that you want to override. If you leave a setting with the same value, that field becomes sticky. This means if that setting is changed in the future by Talos, the current value will be retained.
- If you are adding or deleting any custom instance, make sure that you add or delete a binder rule for that instance in the binder inspector as well.

5. Click **OK**.

   If there are any errors according to the JSON standards, it shows you an error message.

6. Click **Save** to save the changes.

   If the changes conform to the OpenAPI schema specification, the Firewall Management Center allows you to save the configuration, otherwise, the **Error saving overridden configuration** pop-up appears that shows the errors. You can also download the file with the errors.

**Related tasks**

Customize the network analysis policy on page 123

Configure the Snort 3 version of the network analysis policy to meet your specific requirements.

Revert unsaved changes during inline edits on page 128

Configure the network analysis policy to revert any unsaved changes made during inline edits to override inspector configuration.

Revert overridden configuration to default configuration on page 129

Configure an inspector to revert any overridden settings back to the default network analysis policy configuration.

**Related reference**

Examples of custom network analysis policy configuration on page 133

Provides JSON examples for customizing Snort 3 network analysis policy inspector settings and override configurations.

## Revert unsaved changes during inline edits

Configure the network analysis policy to revert any unsaved changes made during inline edits to override inspector configuration.

This task allows you to revert any unsaved changes made during inline edits to override the configuration for an inspector, returning to the most recently saved value.

While making inline edits to override the configuration for an inspector , you can revert any unsaved changes. Note that this action reverts all unsaved changes to the most recently saved value, but does not revert the configuration to the default configuration for an inspector.

**Procedure**

1. Go to **Policies** > **Access Control heading** > **Intrusion** > **Network Analysis Policies**.
2. Go to the **Snort 3 Version** of the network analysis policy.

3. Under **Inspectors**, expand the required inspector for which you want to revert the unsaved changes.

   The default configuration is displayed in the left column and the overridden configuration is displayed in the right column under the inspector.

4. Under the **Overridden Configuration** on the right column, click the **Cross** ✕ icon to revert any unsaved changes for the inspector.

   Alternatively, you can click **Cancel** to cancel the changes.

   If you do not have any unsaved changes to the inspector configuration, then this option is not visible.

**Related tasks**

Revert overridden configuration to default configuration on page 129

Configure an inspector to revert any overridden settings back to the default network analysis policy configuration.

Make inline edit for an inspector to override configuration on page 127

Configure inline edits for inspector configurations to override default settings in Snort 3 network analysis policies.

## View the list of inspectors with overrides

View a list of all overridden inspectors in the network analysis policy.

This task enables you to identify and review all inspectors that have been overridden in your network analysis policy configuration.

You can view a list of all the overridden inspectors.

**Procedure**

1. Go to **Policies** > **Access Control heading** > **Intrusion** > **Network Analysis Policies**.
2. Go to the **Snort 3 Version** of the network analysis policy.
3. Check the **Show Overrides Only** checkbox adjacent to the Search bar to view the list of overridden inspectors.

   All the overridden inspectors are shown with an orange icon next to their names to help you identify them.

**Related tasks**

Search for an inspector on the Network Analysis Policy window on page 122

Configure inspector search functionality within the Snort 3 version on the network analysis policy window.

Make inline edit for an inspector to override configuration on page 127

Configure inline edits for inspector configurations to override default settings in Snort 3 network analysis policies.

Customize the network analysis policy on page 123

Configure the Snort 3 version of the network analysis policy to meet your specific requirements.

## Revert overridden configuration to default configuration

Configure an inspector to revert any overridden settings back to the default network analysis policy configuration.

Revert any changes that you made to override the default configuration for an inspector, restoring the original default settings.

You can revert any changes that you made to override the default configuration for an inspector. This action reverts the overridden configuration to the default configuration for an inspector.

**Procedure**

1. Go to **Policies** > **Access Control heading** > **Intrusion** > **Network Analysis Policies**.
2. Go to the **Snort 3 Version** of the network analysis policy.
3. Under **Inspectors**, expand the required inspector for which you want to revert the overridden configuration.

   The overridden inspectors are shown with the orange icon next to their name.

   The default configuration is displayed on the left column and the overridden configuration is displayed on the right column under the inspector. Under the **Overridden Configuration** on the right column, click **Revert to default configuration** (back arrow) icon to revert the overridden configuration for the inspector to the default configuration.

   If you did not make any changes to the default configuration for the inspector, then this option is disabled.
4. Click **Revert** to confirm the decision.
5. Click **Save** to save the changes.

   If you do not want to save the changes, you can click **Cancel** or the **Cross** ✕ icon.

**Related tasks**

Revert unsaved changes during inline edits on page 128

Configure the network analysis policy to revert any unsaved changes made during inline edits to override inspector configuration.

Customize the network analysis policy on page 123

Configure the Snort 3 version of the network analysis policy to meet your specific requirements.

Make inline edit for an inspector to override configuration on page 127

Configure inline edits for inspector configurations to override default settings in Snort 3 network analysis policies.

**Related reference**

Examples of custom network analysis policy configuration on page 133

Provides JSON examples for customizing Snort 3 network analysis policy inspector settings and override configurations.

## Validate Snort 3 policies

Configure validation for Snort 3 policies by overriding network analysis policy (NAP) configurations, associating NAP policies to access control policies, and deploying them on devices.

This task validates Snort 3 policies to ensure they work correctly with current and previous device versions, handling version-specific configurations and inspector settings.

To validate the Snort 3 policies, here is a list of basic information that you can make note of:

- Current version of the Firewall Management Center can manage multiple Firewall Threat Defense versions.
- Current version of Firewall Management Center supports network analysis policy (NAP) configurations which are not applicable to previous version of Firewall Threat Defense devices.
- Current NAP Policy and validations will work based on the current version support.
- Changes may include content which is not valid for previous versions of Firewall Threat Defenses.

- Policy configuration changes are accepted if they are valid for the current version and performed using the current Snort 3 binary and NAP schema.
- For previous version Firewall Threat Defenses, validation is performed during deployment using NAP schema and Snort 3 binary for that specific version. If there is any configuration which is not applicable for the given version, the user is informed or warned that the configuration not supported on the given version will not be deployed, while the remaining configuration will be deployed.

In this procedure, when we associate the NAP policy to an Access Control Policy and deploy it on a device, for example any inspector like rate filter configuration is applied to validate the Snort 3 policies.

**Procedure**

1. **Steps to Override NAP Policy Configuration:** Under **Inspectors** in the **Snort 3 Version** of the network analysis policy, expand the required inspector for which you want to override the default setting.

   The default configuration is displayed on the left column and the overridden configuration is displayed on the right column under the inspector.

   a) Under the **Overridden Configuration** on the right column, click **Edit Inspector** (Pencil) icon to make changes to any inspector like rate_filter.

      The Override Configuration pop-up appears where you can make the required edits to the rate_filter inspector. Click **OK**.

   b) Click **Save** to save the changes.

      Alternatively, you can use the **Actions** dropdown menu to upload the overridden configuration file.

2. Click the **Actions** dropdown menu in the **Snort 3 Version** of the network analysis policy.
3. Under **Upload**, you can click **Overridden Configuration** to upload the JSON file that contains the overridden configuration.

   > ⚠ **Caution**
   >
   > Upload only the changes that you require. You should not upload the entire configuration as it causes the overrides to remain persistent, so any subsequent changes to the default configuration from LSP updates will not be applied.

   You can drag and drop a file or click to browse to the JSON file saved in your system that contains the overridden inspector configuration.

   - **Merge inspector overrides**: Content in the uploaded file is merged with the existing configuration if there is no common inspector. If there are common inspectors, then the content in the uploaded file (for common inspectors) takes precedence over the previous content, and it replaces the previous configuration for those inspectors.
   - **Replace inspector overrides**: Removes all previous overrides and replaces them with the new content in the uploaded file.

> **Note**
>
> As choosing this option deletes all the previous overrides, make an informed decision before overriding the configuration using this option.

If any error occurs while uploading the overridden inspectors, you see the error on the **Upload Overridden Configuration File** pop-up window. You can also download the file with the error, then fix the error and reupload the file.

4. **Steps to Associate NAP Policy to Access Control Policy:** In the access control policy editor, click **Advanced**, then click **Edit** next to the Network Analysis and Intrusion Policies section.
   a) From the **Default Network Analysis Policy** drop-down list, select a default network analysis policy.

      If you choose a user-created policy, you can click **Edit** to edit the policy in a new window. You cannot edit system-provided policies.

   b) Click **OK** and then click **Save** to save the policy.
5. Alternatively, in the access control policy editor, click **Advanced**, then click **Edit** next to the Network Analysis and Intrusion Policies section.
   a) Click **Add Rule**.
   b) Configure the rule's conditions by clicking the options you want to add.
   c) Click **Network Analysis** and choose the **Network Analysis Policy** you want to use to preprocess the traffic matching this rule.
   d) Click **Add**.
6. **Deployment:** On the Firewall Management Center menu bar, click **Deploy** and then select **Deployment**.
7. 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 changes for that device listed under it are pushed for deployment. Alternatively, you can use the **Policy Selection** to select individual policies or configurations to deploy, withholding the rest.

   Optionally, use **Show or Hide Policy** to selectively view or hide the associated unmodified policies.
8. Click **Deploy**.
9. 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.

> **Note**
>
> It displays a warning that Snort 3 network analysis policy contains inspectors or attributes not valid for this Firewall Threat Defense version. Invalid settings will be skipped during deployment. Invalid inspectors are: ["rate_filter"] only for devices lower than 7.1 version.

## Examples of custom network analysis policy configuration

Provides JSON examples for customizing Snort 3 network analysis policy inspector settings and override configurations.

This is a sample file that includes JSON snippets explaining how you can customize the network analysis policy for Snort 3. You can choose to override an inspector configuration using the following ways:

- Make inline edits for an inspector directly on the Firewall Management Center. See Make inline edit for an inspector to override configuration on page 127.
- Use the **Actions** drop-down menu to upload the overridden configuration file. See Customize the network analysis policy on page 123.

Before you choose any of these options, review all the details and examples to help you define the network analysis policy overrides successfully. To avoid risks and errors, read and understand the scenarios provided here.

If you choose to override an inspector configuration from the **Actions** drop-down menu, you need to construct a JSON file for the network analysis policy overrides and upload the file.

For overriding an inspector configuration in the network analysis policy, you must upload only the changes that you require. You should not upload the entire configuration because it makes the overrides sticky in nature and therefore, any subsequent changes to the default values or configuration as part of the LSP updates would not be applied.

Here are the examples for various scenarios:

### Enabling a Singleton Inspector when the Default State in the Base Policy is Disabled

```
{
  "rate_filter": {
    "enabled": true,
    "type": "singleton",
    "data": []
  }
}
```

### Disabling a Singleton Inspector when the Default State in the Base Policy is Enabled

```
{
  "rate_filter": {
    "enabled": false,
    "type": "singleton",
    "data": []
  }
}
```

### Enabling a Multiton Inspector when the Default State in the Base Policy is Disabled

```
{
  "ssh": {
    "enabled": true,
    "type": "multiton",
    "instances": []
  }
}
```

**Disabling a Multiton Inspector when the Default State in the Base Policy is Enabled**

```
{
  "ssh": {
    "enabled": false,
    "type": "multiton",
    "instances": []
  },
  "iec104": {
    "type": "multiton",
    "enabled": false,
    "instances": []
  }
}
```

**Overriding the Default Value of Specific Setting(s) for Singleton Inspector**

```
{
  "normalizer": {
    "enabled": true,
    "type": "singleton",
    "data": {
      "tcp": {
        "block": true
      },
      "ip6": true
    }
  }
}
```

**Overriding Specific Setting(s) of a Default Instance (where Instance Name Matches with Inspector Type) in Multiton Inspector**

```
{
  "http_inspect": {
    "enabled": true,
    "type": "multiton",
    "instances": [
      {
        "data": {
          "unzip": false
        },
        "name": "http_inspect"
      }
    ]
  }
}
```

**Adding Binder Rule for a Default Instance with Required Changes**

> **Note**
>
> Default binder rules cannot be edited; they are always appended at the end.

```
{
  "binder": {
    "enabled": true,
    "type": "binder",
    "rules": [
      {
        "use": {
          "type": "http_inspect"
        },
        "when": {
          "role": "server",
          "service": "http",
          "dst_nets": "10.1.1.0/24"
        }
      }
    ]
  }
}
```

**Adding a New Custom Instance**

> **Note**
>
> Corresponding binder rule entry must be defined in the binder inspector.

```
{
  "telnet": {
    "enabled": true,
    "type": "multiton",
    "instances": [
      {
        "name": "telnet_my_instance",
        "data": {
          "encrypted_traffic": true
        }
      }
    ]
  },
  "binder": {
    "enabled": true,
    "type": "binder",
    "rules": [
      {
        "when": {
          "role": "any",
          "service": "telnet"
        },
```

```
        "use": {
          "type": "telnet",
          "name": "telnet_my_instance"
        }
      }
    ]
  }
}
```

**Overriding a Singleton Instance, Multiton Default Instance, and Creating a New Multiton Instance in a Single JSON Override**

Example to show the following in a single JSON override:

- Overriding a Singleton instance (**`normalizer`** inspector)
- Overriding a Multiton default instance (**`http_inspect`** inspector)
- Creating a new Multiton instance (**`telnet`** inspector)

```
{
  "normalizer": {
    "enabled": true,
    "type": "singleton",
    "data": {
      "tcp": {
        "block": true
      },
      "ip6": true
    }
  },
  "http_inspect": {
    "enabled": true,
    "type": "multiton",
    "instances": [
      {
        "data": {
          "unzip": false,
          "xff_headers": "x-forwarded-for true-client-ip
x-another-forwarding-header"
        },
        "name": "http_inspect"
      }
    ]
  },
  "telnet": {
    "enabled": true,
    "type": "multiton",
    "instances": [
      {
        "name": "telnet_my_instance",
        "data": {
          "encrypted_traffic": true
        }
      }
    ]
  },
  "binder": {
    "enabled": true,
    "type": "binder",
    "rules": [
```

```
      {
        "when": {
          "role": "any",
          "service": "telnet"
        },
        "use": {
          "type": "telnet",
          "name": "telnet_my_instance"
        }
      },
      {
        "use": {
          "type": "http_inspect"
        },
        "when": {
          "role": "server",
          "service": "http",
          "dst_nets": "10.1.1.0/24"
        }
      }
    ]
  }
}
```

**Note**

You do not need to provide the **name** attribute for the default instance in binder rules.

### Configuring arp_spoof

Example for configuring **arp_spoof**:

The **arp_spoof** inspector does not have any default configurations for any attributes. This demonstrates the case where you can provide the overrides.

```
{
  "arp_spoof": {
    "type": "singleton",
    "data": {
      "hosts": [
        {
          "ip": "1.1.1.1",
          "mac": "ff:0f:f1:0f:0f:ff"
        },
        {
          "ip": "2.2.2.2",
          "mac": "ff:0f:f2:0f:0f:ff"
        }
      ]
    },
    "enabled": true
  }
}
```

**Configuring rate_filter**

```
{
  "rate_filter": {
    "data": [
      {
        "apply_to": "[10.1.2.100, 10.1.2.101]",
        "count": 5,
        "gid": 135,
        "new_action": "alert",
        "seconds": 1,
        "sid": 1,
        "timeout": 5,
        "track": "by_src"
      }
    ],
    "enabled": true,
    "type": "singleton"
  }
}
```

**Configuring Binder Rules when Multi-Hierarchy Network Analysis Policy is Used**

This example illustrates adding a new custom instance in child policy and the way binder rules should be written. Binder rules are defined as a list and therefore, it is important to pick up the rules defined in the parent policy and build the new rules on top of it as rules will not be merged automatically. The binder rules available in child policy are a source of truth in totality.

On the Firewall Threat Defense, the default Cisco Talos policy rules are appended on these user-defined overrides.

**Parent Policy**:

We have defined a custom instance by the name **`telnet_parent_instance`** and the corresponding binder rule.

```
{
  "telnet": {
    "type": "multiton",
    "instances": [
      {
        "data": {
          "normalize": true,
          "encrypted_traffic": true
        },
        "name": "telnet_parent_instance"
      }
    ],
    "enabled": true
  },
  "binder": {
    "enabled": true,
    "type": "binder",
    "rules": [
      {
        "when": {
          "role": "any",
          "service": "telnet"
        },
        "use": {
          "type": "telnet",
          "name": "telnet_parent_instance"
        }
      }
```

```
    ]
  }
}
```

**Child Policy**:

This network analysis policy has the aforementioned policy as its base policy. We have defined a custom instance by the name **`telnet_child_instance`** and have also defined the binder rules for this instance. The binder rules from parent policy need to be copied here, and then child policy binder rules can be prepended or appended on top of it based on the nature of the rule.

```
{
  "telnet": {
    "type": "multiton",
    "instances": [
      {
        "data": {
          "normalize": true,
          "encrypted_traffic": false
        },
        "name": "telnet_child_instance"
      }
    ],
    "enabled": true
  },
  "binder": {
    "enabled": true,
    "type": "binder",
    "rules": [
      {
        "when": {
          "role": "any",
          "service": "telnet",
          "nets": "10.2.2.0/24"
        },
        "use": {
          "type": "telnet",
          "name": "telnet_child_instance"
        }
      },
      {
        "when": {
          "role": "any",
          "service": "telnet"
        },
        "use": {
          "type": "telnet",
          "name": "telnet_parent_instance"
        }
      }
    ]
  }
}
```

### Configuring List Inspector Attribute in General

While changing overrides for any attribute of type list, it is important to pass the full contents rather than partial override. This means if a base policy attributes are defined as:

```
{
  "list-attribute": [
```

```
    {
      "entry1": {
        "key1": "value1"
      }
    },
    {
      "entry2": {
        "key2": "value2"
      }
    }
  ]
}
```

If you want to modify **value1** to **value1-new**, the override payload must look like the following:

Correct Way:

```
{
  "list-attribute": [
    {
      "entry1": {
        "key1": "value1-new"
      }
    },
    {
      "entry2": {
        "key2": "value2"
      }
    }
  ]
}
```

Incorrect Way:

```
{
  "list-attribute": [
    {
      "entry1": {
        "key1": "value1-new"
      }
    }
  ]
}
```

You can understand this configuration by taking the trimmed values of the **alt_max_command_line_len** attribute in the **smtp** inspector. Suppose the default (base) policy configuration for **smtp** inspector is as follows:

```
{
  "smtp": {
    "type": "multiton",
    "instances": [
      {
        "name": "smtp",
        "data": {
          "decompress_zip": false,
          "normalize_cmds": "ATRN AUTH BDAT CHUNKING DATA DEBUG EHLO
           EMAL ESAM ESND ESOM ETRN EVFY EXPN HELO HELP IDENT MAIL
           NOOP ONEX QUEU QUIT RCPT RSET SAML SEND SOML STARTTLS TICK
           TIME TURN TURNME VERB VRFY X-ADAT XADR XAUTH XCIR X-DRCP X-
           ERCP XEXCH50 X-EXCH50 X-EXPS XGEN XLICENSE X-LINK2STATE XQUE
           XSTA XTRN XUSR",
```

```
          "ignore_data": false,
          "max_command_line_len": 512,
          "max_header_line_len": 1000,
          "log_rcptto": false,
          "decompress_swf": false,
          "max_response_line_len": 512,
          "b64_decode_depth": -1,
          "max_auth_command_line_len": 1000,
          "log_email_hdrs": false,
          "xlink2state": "alert",
          "binary_data_cmds": "BDAT XEXCH50",
          "auth_cmds": "AUTH XAUTH X-EXPS",
          "log_filename": false,
          "uu_decode_depth": -1,
          "ignore_tls_data": false,
          "data_cmds": "DATA",
          "bitenc_decode_depth": -1,
          "alt_max_command_line_len": [
            {
              "length": 255,
              "command": "ATRN"
            },
            {
              "command": "AUTH",
              "length": 246
            },
            {
              "length": 255,
              "command": "BDAT"
            },
            {
              "length": 246,
              "command": "DATA"
            }
          ],
          "log_mailfrom": false,
          "decompress_pdf": false,
          "normalize": "none",
          "email_hdrs_log_depth": 1464,
          "valid_cmds": "ATRN AUTH BDAT CHUNKING DATA DEBUG EHLO
           EMAL ESAM ESND ESOM ETRN EVFY EXPN HELO HELP IDENT MAIL
           NOOP ONEX QUEU QUIT RCPT RSET SAML SEND SOML STARTTLS TICK
           TIME TURN TURNME VERB VRFY X-ADAT XADR XAUTH XCIR X-DRCP X-
           ERCP XEXCH50 X-EXCH50 X-EXPS XGEN XLICENSE X-LINK2STATE XQUE
           XSTA XTRN XUSR",
          "qp_decode_depth": -1
        }
      }
    ],
    "enabled": true
  }
}
```

Now, if you want to add two more objects to the **alt_max_command_line_len** list:

```
{
    "length": 246,
    "command": "XEXCH50"
},
{
    "length": 246,
```

```
    "command": "X-EXPS"
}
```

Then the custom network analysis policy override JSON would look like the following:

```
{
  "smtp": {
    "type": "multiton",
    "instances": [
      {
        "name": "smtp",
        "data": {
          "alt_max_command_line_len": [
            {
              "length": 255,
              "command": "ATRN"
            },
            {
              "command": "AUTH",
              "length": 246
            },
            {
              "length": 255,
              "command": "BDAT"
            },
            {
              "length": 246,
              "command": "DATA"
            },
            {
              "length": 246,
              "command": "XEXCH50"
            },
            {
              "length": 246,
              "command": "X-EXPS"
            }
          ]
        }
      }
    ],
    "enabled": true
  }
}
```

**Configuring Overrides when Multi-Hierarchy Network Analysis Policy is used in Multiton Inspector**

This example illustrates overriding attributes in child policy and how the merged configuration will be used in the child policy for any instance. Any overrides defined in the child policy will be merged with the parent policy. Thus, if attribute1 and attribute2 are overridden in parent policy and attribute2 and attribute3 are overridden in the child policy, the merged configurations are for child policy. This means that attribute1 (defined in parent policy), attribute2 (defined in child policy), and attribute3 (defined in child policy) will be configured on the device.

**Parent Policy**:

Here we have defined a custom instance by the name **`telnet_parent_instance`** and overridden 2 attributes namely, **`normalize`** and **`encrypted_traffic`** in the custom instance.

```
{
  "telnet": {
    "type": "multiton",
```

```
    "instances": [
      {
        "data": {
          "normalize": true,
          "encrypted_traffic": false
        },
        "name": "telnet_parent_instance"
      }
    ],
    "enabled": true
  },
  "binder": {
    "enabled": true,
    "type": "binder",
    "rules": [
      {
        "when": {
          "role": "any",
          "service": "telnet"
        },
        "use": {
          "type": "telnet",
          "name": "telnet_parent_instance"
        }
      }
    ]
  }
}
```

**Child Policy**:

This network analysis policy has the aforementioned policy as its base policy. We have overridden attribute **`encrypted_traffic`** from parent policy and also overridden new attribute **`ayt_attack_thresh`**.

```
{
  "telnet": {
    "type": "multiton",
    "instances": [
      {
        "data": {
          "encrypted_traffic": true,
          "ayt_attack_thresh": 1
        },
        "name": "telnet_parent_instance"
      }
    ],
    "enabled": true
  }
}
```

With the above policy JSON, when you deploy the network analysis policy the following merged JSON will be configured on the device.

```
{
  "telnet": {
    "type": "multiton",
    "instances": [
      {
        "data": {
          "normalize": true,
          "encrypted_traffic": true,
          "ayt_attack_thresh": 1
```

```
        },
        "name": "telnet_parent_instance"
      }
    ],
    "enabled": true
  },
  "binder": {
    "enabled": true,
    "type": "binder",
    "rules": [
      {
        "when": {
          "role": "any",
          "service": "telnet"
        },
        "use": {
          "type": "telnet",
          "name": "telnet_parent_instance"
        }
      }
    ]
  }
}
```

This example illustrates details for the custom network analysis policy. The same behavior is also exhibited in the default instance. Also, a similar merging would be done for Singleton inspectors.

#### Removing all the Inspector Overrides for the Network Analysis Policy

Whenever you want to remove all the overrides for a specific network analysis policy, you can upload an empty JSON. While uploading the overrides, choose the option **Replace inspector overrides**.

## Network analysis policy settings and cached changes

Describes network analysis policy configuration behavior and system caching mechanisms for policy modifications.

When you create a new network analysis policy, it has the same settings as its base policy.

When tailoring a network analysis policy, especially when disabling inspectors, keep in mind that some inspectors and intrusion rules require that traffic first be decoded or preprocessed in a certain way. 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.

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.

The system caches one network analysis policy per user. While editing a network analysis policy, if you select any menu or other path to another page, your changes stay in the system cache even if you leave the page.

## Generate Snort 3 recommendations

Describes how to generate Snort 3 recommendations for optimizing intrusion detection and prevention based on network traffic analysis and security requirements.

### Snort 3 rule recommendations

Explains how Snort 3 rule recommendations automatically tune intrusion policies with rules specific to host environments.

Snort 3 rule recommendations are a security tuning feature that

- automatically tune your intrusion policy with rules specific to the host environment,
- enable additional rules or tune the current rule set by disabling rules for vulnerabilities not present in your network, and
- use the host database to determine rules that apply to your environment.

#### How rule recommendations 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:

- 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.

For more information, see Secure Firewall recommended rules on page 81.

## Benefits

Describes the advantages of configuring recommendations for intrusion policy detection.

- 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

Describes a large corporate network that uses Snort 3 as its primary intrusion detection and prevention system to enhance incident response capabilities.

A sample business scenario is a network security implementation that demonstrates how a large corporate network uses Snort 3 as its primary intrusion detection and prevention system to enhance incident response capabilities through vulnerability-based rule generation and intrusion policy optimization.

#### Business scenario details

In this scenario, a large corporate network adopts robust network security measures in a rapidly evolving threat landscape. The security team wants to enhance their incident response capabilities by generating recommendations or rule sets based on the vulnerabilities detected in the host network. This helps to optimize their intrusion policies, thereby safeguarding the network more effectively.

## Best practices

Consider these best practices to ensure effective intrusion detection and prevention.

- You must have high-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 accurate data about applications, services, and vulnerabilities on your network.

- Devices should have visibility to east-west traffic flows as well as north-south traffic flows to build an accurate host profile.
- You can create a scheduled task to update recommendations automatically.

## Prerequisites for generating recommendations

Outlines the requirements for generating recommendations, including the presence of hosts in the system and proper mapping between protected networks and existing hosts.

- 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

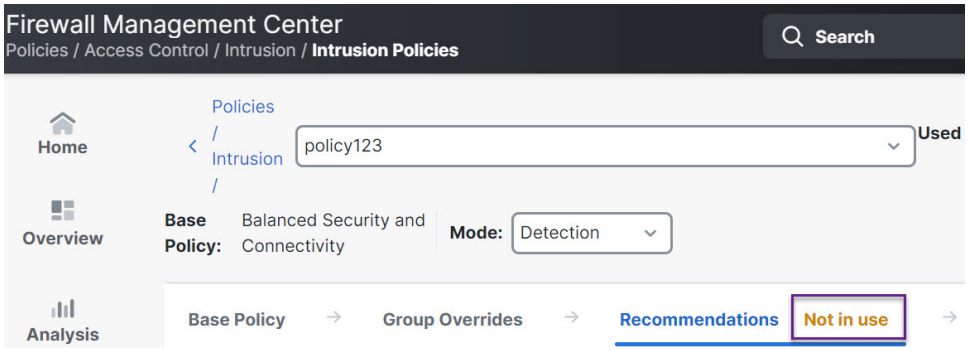
Configure Snort 3 rule recommendations to optimize your intrusion policy with recommended security levels and rule settings.

Generate and apply Snort 3 rule recommendations to optimize your intrusion policy based on your network configuration and security requirements.

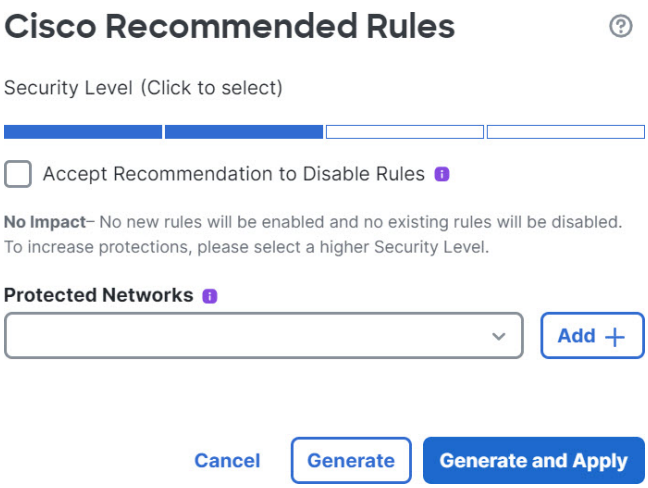
Snort 3 recommendations help you configure intrusion policies with rules that are tailored to your network environment. The system analyzes your protected networks and suggests appropriate security levels and rule configurations.

### Procedure

1. Choose **Policies** > **Access Control heading** > **Intrusion**.
2. Click the **Snort 3 Version** button of the corresponding intrusion policy.
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.

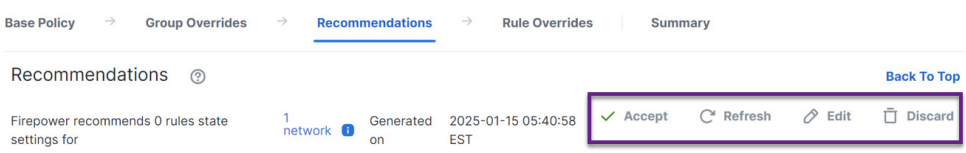



4. Click to select the security level.
5. (Optional) Check the **Accept Recommendation to Disable Rules** check box to disable the rules written for vulnerabilities not found on the hosts in your network.

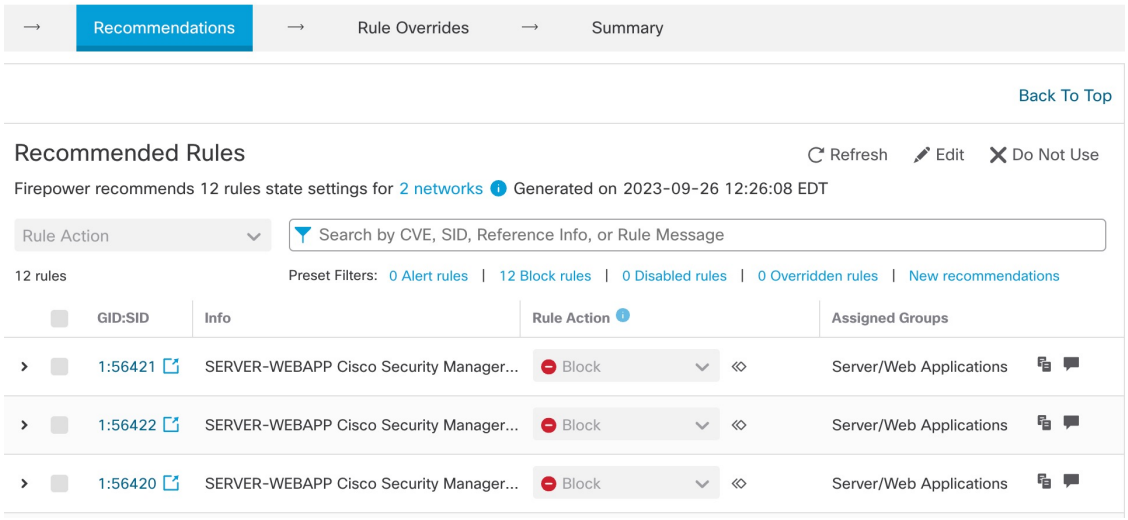
   Use this option, only if you have to trim your rule set because of a high number of alerts or to improve inspection performance.
6. From the **Protected Networks** drop-down list, choose the network objects that must be examined by the recommendations. By default, any IPv4 or IPv6 networks are selected if you do not make a selection.

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

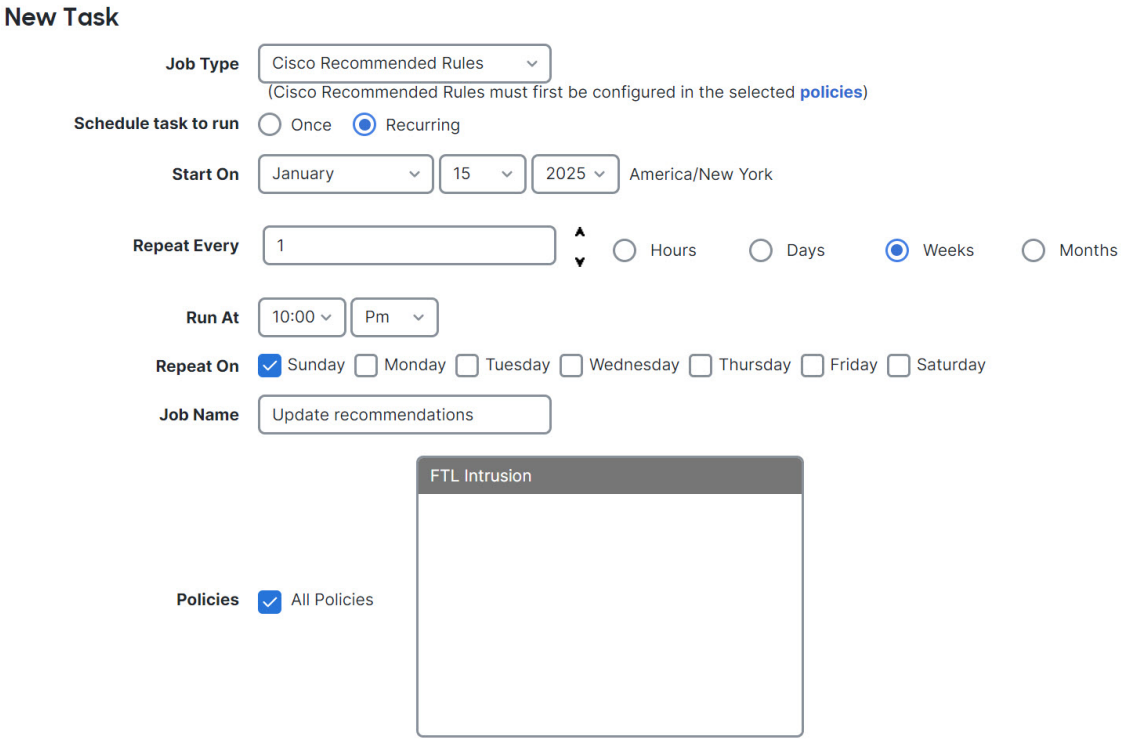
   Recommendations are generated successfully. A new recommendation tab appears with all the recommended rules and their corresponding recommended actions. Rule action preset filters are also available for this tab, in addition to new recommendations.
8. Verify the recommendations and then apply them accordingly:
   - **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.




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. Refer to Deploy configuration changes on page 37.

# 6 Advanced Access Control settings for Network Analysis and Intrusion Policies

**Topics:**


- Advanced access control settings for network analysis and intrusion policies
- Advanced access control settings for network analysis and intrusion policies
- Requirements and prerequisites for advanced access control settings for network analysis and intrusion policies
- Inspection of packets that pass before traffic is identified
- Advanced settings for network analysis policies


Learn about configuring advanced settings for network analysis and intrusion policies.

This chapter describes how to configure advanced settings for network analysis and intrusion policies.

## Advanced access control settings for network analysis and intrusion policies

Describes advanced configuration options in access control policies that govern intrusion detection and prevention.

Advanced access control settings are intrusion detection and prevention configurations that

- require specific expertise to configure,
- typically require little or no modification, and
- are not common to every deployment.

**Version compatibility**

**Note**

Snort 2 is not supported on Threat Defense version 7.7. For information on Snort 2 features that are supported in versions earlier than 7.7, refer to the Firewall Management Center guide that matches your Firewall Threat Defense version.

## Advanced access control settings for network analysis and intrusion policies

Describes advanced configuration options in access control policies that govern intrusion detection and prevention.

Advanced access control settings are intrusion detection and prevention configurations that

- require specific expertise to configure,
- typically require little or no modification, and
- are not common to every deployment.

**Version compatibility**

**Note**

Snort 2 is not supported on Threat Defense version 7.7. For information on Snort 2 features that are supported in versions earlier than 7.7, refer to the Firewall Management Center guide that matches your Firewall Threat Defense version.

## Requirements and prerequisites for advanced access control settings for network analysis and intrusion policies

Lists the system requirements, software prerequisites, and configuration dependencies needed to implement advanced access control settings for network analysis and intrusion detection policies in Cisco Secure Firewall environments.

This reference provides the system requirements, software prerequisites, and configuration dependencies needed to implement advanced access control settings for network analysis and intrusion detection policies in Cisco Secure Firewall environments.

**Model support**

Any.

**Supported domains**

Any

**User roles**

- Admin
- Access Admin
- Network Admin

# Inspection of packets that pass before traffic is identified

Describes the inspection process for packets that pass before the system can identify traffic and determine which access control rule applies.

Inspection of packets that pass before traffic is identified is a network security process that

- allows a few packets to pass initially for connection establishment and traffic identification,
- enables features like URL filtering, application detection, rate limiting, and Intelligent Application Bypass to function properly, and
- requires explicit configuration in access control policies to inspect, prevent, and generate events for these initial packets.

**Configuration requirements**

You must explicitly configure your access control policy to inspect these packets, prevent them from reaching their destination, and generate any events.

As soon as the system identifies the access control rule or default action that should handle the connection, the remaining packets in the connection are handled and inspected accordingly.

## Best practices for handling packets that pass before traffic identification

Consider these guidelines when configuring intrusion policy settings for packets that arrive before access control rules are determined.

The default action specified for an access control policy is NOT applied to these packets.

Use these guidelines to choose a value for the **Intrusion Policy used before Access Control rule is determined** setting in the Advanced settings of the access control policy.

- You can choose a system-created or custom intrusion policy. For example, you can choose **Balanced Security and Connectivity**.
- For performance reasons, unless you have good reason to do otherwise, this setting should match the default action set for your access control policy.

- If your system does NOT perform intrusion inspection (for example, in a discovery-only deployment), select **No Rules Active**. The system will NOT inspect these initial packets, and they will be allowed to pass.
- By default, this setting uses the default variable set. Ensure that this is suitable for your purposes. For information, see Variable sets.
- The network analysis policy associated with the first matching network analysis rule preprocesses traffic for the policy you select. If there are no network analysis rules, or none match, the default network analysis policy is used.

## Specify a policy to handle packets that pass before traffic identification

Configure an intrusion policy to handle packets that pass before traffic identification is completed.

This task explains how to specify the system's behavior for network traffic during the period before traffic identification is complete.

**Note**

This setting is sometimes referred to as the *default intrusion policy*. (This is distinct from the default action for an access control policy.)

**Caution**

Changing the total number of intrusion policies used by an access control policy restarts the Snort process when you deploy configuration changes, temporarily interrupting traffic inspection. Whether traffic drops during this interruption or passes without further inspection depends on how the assigned device handles traffic. You can add an intrusion policy that is not currently used or remove the last instance of an intrusion policy. Intrusion policies are used in access control rules, as the default action, or as the default intrusion policy.

### Before you begin

Review best practices for these settings. See Best practices for handling packets that pass before traffic identification on page 151.

Follow these steps to specify a policy to handle packets that pass before traffic identification:

#### Procedure

1. In the access control policy editor, click **Advanced**, then click **Edit** (✎) next to the **Network Analysis** and **Intrusion Policies** section.

   If **View** (👁) appears instead, settings are inherited from an ancestor policy, or you do not have permission to modify the settings. If the configuration is unlocked, uncheck **Inherit from base policy** to enable editing.

2. Select an intrusion policy from the **Intrusion Policy used before Access Control rule is determined** drop-down list.

   If you choose a user-created policy, you can click **Edit** (✎) to edit the policy in a new window. You cannot edit system-provided policies.

3. Optionally, select a different variable set from the **Intrusion Policy Variable Set** drop-down list. You can also select **Edit** (✎) next to the variable set to create and edit variable sets. If you do not change the variable set, the system uses a default set.
4. Click **OK**.
5. Click **Save** to save the policy.

---

**What to do next**

- Deploy configuration changes.

# Advanced settings for network analysis policies

Describes advanced configuration options for network analysis policies that enable customized traffic preprocessing through multiple policies and network analysis rules.

A *network analysis policy* is a traffic preprocessing configuration that governs how traffic is decoded and preprocessed so that it can be further evaluated, especially for anomalous traffic that might signal an intrusion attempt.

**Advanced configuration concepts**

This traffic preprocessing occurs after Security Intelligence matching and traffic decryption, but before intrusion policies inspect packets in detail. By default, the system-provided Balanced Security and Connectivity network analysis policy is the default network analysis policy.

> **Tip**
>
> The system-provided 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.

A simple way to tune preprocessing is to create and use a custom network analysis policy as the default. If you are an advanced user with a complex deployment, you can create multiple network analysis policies, each tailored to preprocess traffic differently. Then, you can configure the system to use those policies to govern the preprocessing of traffic using different security zones, networks, or VLANs.

To accomplish this, you add custom *network analysis rules* to your access control policy. A network analysis rule is simply a set of configurations and conditions that specifies how you preprocess traffic that matches those qualifications. You create and edit network analysis rules in the advanced options in an existing access control policy. Each rule belongs to only one policy.

Each rule has:

- a set of rule conditions that identifies the specific traffic you want to preprocess
- an associated network analysis policy that you want to use to preprocess traffic that meets all the rules' conditions

When it is time for the system to preprocess traffic, it matches packets to network analysis rules in top-down order by rule number. Traffic that does not match any network analysis rules is preprocessed by the default network analysis policy.

## Set the default network analysis policy

Configure the default network analysis policy for an access control policy to establish preprocessing behavior.

Setting a default network analysis policy establishes the baseline preprocessing behavior for network traffic analysis within your access control policy.

You can choose a system- or user-created policy.

> **Note**
>
> If you disable a preprocessor but the system needs to evaluate preprocessed packets against an enabled intrusion or preprocessor rule, the system automatically enables and uses the preprocessor although it remains disabled in the network analysis policy web interface. Tailoring preprocessing, especially using multiple custom network analysis policies, is an **advanced** task. Because preprocessing and intrusion inspection are so closely related, you **must** be careful that you allow the network analysis and intrusion policies examining a single packet to complement each other.

**Procedure**

1. In the access control policy editor, click **Advanced**, then click **Edit** (✎) next to the Network Analysis and Intrusion Policies section.

   If **View** (👁) appears instead, settings are inherited from an ancestor policy, or you do not have permission to modify the settings. If the configuration is unlocked, uncheck **Inherit from base policy** to enable editing.

2. From the **Default Network Analysis Policy** drop-down list, select a default network analysis policy.

   If you choose a user-created policy, you can click **Edit** (✎) to edit the policy in a new window. You cannot edit system-provided policies.

   > **Caution**
   >
   > Changing the total number of network analysis policies used by an access control policy restarts the Snort process when you deploy configuration changes, temporarily interrupting traffic inspection. Whether traffic drops during this interruption or passes without further inspection depends on how the assigned device handles traffic. You change the total number of network analysis policies by adding a policy that is not currently used, or by removing the last instance of a network analysis policy. You can use a network analysis policy with network analysis rules or as the default network analysis policy.

3. Click **OK**.
4. Click **Save** to save the policy.

**What to do next**

- Deploy configuration changes.

## Network analysis rules

Explains how network analysis rules tailor preprocessing configurations to network traffic within access control policy advanced settings.

A network analysis rule is a preprocessing configuration component that

- tailors preprocessing configurations to network traffic within access control policy advanced settings,
- matches packets in top-down order by ascending rule number, starting at 1, and
- preprocesses traffic according to the first rule where all conditions match.

### Network analysis rule conditions and matching

You can add zone, network, and VLAN tag conditions to a rule. If you do not configure a particular condition for a rule, the system does not match traffic based on that criterion. For example, a rule with a network condition but no zone condition evaluates traffic based on its source or destination IP address, regardless of its ingress or egress interface. Traffic that does not match any network analysis rules is preprocessed by the default network analysis policy.

### Network analysis policy rule conditions

Explains rule conditions that enable you to fine-tune your network analysis policy to target the users and networks you want to control.

Network analysis policy rule conditions are configuration parameters that enable you to fine-tune your network analysis policy to target the users and networks you want to control.

### Security zone rule conditions

Describes how to use security zones and zone conditions to control or decrypt network traffic by grouping interfaces and specifying matching criteria for source and destination zones across devices.

A security zone rule condition is a network traffic control mechanism that

- segments your network to help you manage, classify, and decrypt traffic flow by grouping interfaces across multiple devices,
- controls or decrypts traffic by its source and destination security zones, and
- requires all interfaces in a zone to be of the same type (all inline, passive, switched, or routed).

### Zone condition traffic matching

If you add both source and destination zones to a zone condition, matching traffic must originate from an interface in one of the source zones and leave through an interface in one of the destination zones.

All zones used in a zone condition must be of the same type. Because devices deployed passively do not transmit traffic, you cannot use a zone with passive interfaces as a destination zone.

Minimize the number of matching criteria whenever possible, especially those for security zones, network objects, and port objects. When you specify multiple criteria, the system must match against *every* combination of the contents of the criteria you specify.

**Tip**

Constraining rules by zone is one of the best ways to improve system performance. If a rule does not apply to traffic through any of device's interfaces, that rule does not affect that device's performance.

*Security zone conditions in multidomain environments*

Explains how to configure a security zone condition in a multidomain environment to control only the interfaces visible within your domain, even if the zone itself spans multiple domains.

In a multidomain deployment, a zone created in an ancestor domain can contain interfaces that reside on devices in different domains. When you configure a zone condition in an descendant domain, your configurations apply to only the interfaces you can see.

### Network rule conditions

Explains how to create and apply network conditions that control or decrypt traffic based on source and destination IP addresses, using either predefined objects or manual entry of IP addresses and address blocks.

A network condition is a traffic matching criterion that

- controls or decrypts traffic based on source and destination IP addresses using inner packet headers,
- enables administrators to specify exact IP addresses or blocks for granular policy enforcement, and
- can be built using predefined network objects or by manually entering IP addresses or address blocks.

### Network rule condition restrictions

Minimize the number of matching criteria whenever possible, especially those for security zones, network objects, and port objects. When you specify multiple criteria, the system must match against *every* combination of the contents of the criteria you specify.

> **Note**
>
> You *cannot* use FDQN network objects in identity rules.

### VLAN tag rule conditions

Explains the VLAN match conditions in access control and other policy rules.

VLAN tags rule conditions are filtering mechanisms that

- control VLAN-tagged traffic, including Q-in-Q (stacked VLAN) traffic
- use the innermost VLAN tag to filter VLAN traffic, with the exception of prefilter policy which uses the outermost VLAN tag, and
- apply only to inline sets and do not match traffic on firewall interfaces.

### VLAN tag rule conditions configuration details

> **Note**
>
> VLAN tags in access rules only apply to inline sets. Access rules with VLAN tags do not match traffic on firewall interfaces.

The system uses the innermost VLAN tag to filter VLAN traffic, with the exception of the prefilter policy, which uses the outermost VLAN tag in its rules.

Note this Q-in-Q support:

- Firewall Threat Defense on Firepower 4100/9300—Does not support Q-in-Q (supports only one VLAN tag).
- Firewall Threat Defense on all other models:

- Inline sets and passive interfaces–Supports Q-in-Q, up to 2 VLAN tags.
- Firewall interfaces–Does not support Q-in-Q (supports only one VLAN tag).

You can use predefined objects to build VLAN conditions, or manually enter any VLAN tag from 1 to 4094. Use a hyphen to specify a range of VLAN tags.

In a cluster, if you encounter problems with VLAN matching, edit the access control policy advanced options, Transport/Network Preprocessor Settings, and select the **Ignore the VLAN header when tracking connections** option.

#### Configure network analysis rules

Configure custom network analysis rules to define which network analysis policy preprocesses traffic that matches specific conditions in your access control policy.

Network analysis rules allow you to specify which network analysis policy should preprocess traffic that matches specific conditions, providing granular control over traffic inspection before intrusion detection.

Network analysis rules are configured within the advanced settings of an access control policy. You can create custom rules to apply different network analysis policies based on traffic conditions such as source, destination, ports, or applications.

### Before you begin

Follow these steps to configure network analysis rules:

#### Procedure

1. In the access control policy editor, click **Advanced**, then click **Edit** (✎) next to the Network Analysis and Intrusion Policies section.

   If **View** (👁) appears instead, settings are inherited from an ancestor policy, or you do not have permission to modify the settings.If the configuration is unlocked, uncheck **Inherit from base policy** to enable editing.

   > **Tip**
   >
   > Click **Network Analysis Policy List** to view and edit existing custom network analysis policies.

2. Next to **Network Analysis Rules**, click the statement that indicates how many custom rules you have.
3. Click **Add Rule**.
4. Configure the rule's conditions by clicking the conditions you want to add.
5. Click **Network Analysis** and choose the **Network Analysis Policy** you want to use to preprocess the traffic matching this rule.

   Click **Edit** (✎) to edit a custom policy in a new window. You cannot edit system-provided policies.

> **Caution**
>
> Changing the total number of network analysis policies used by an access control policy restarts the Snort process when you deploy configuration changes, temporarily interrupting traffic inspection. Whether traffic drops during this interruption or passes without further inspection depends on how the assigned device handles traffic.You change the total number of network analysis policies by adding a policy that is not currently used, or by removing the last instance of a network analysis policy. You can use a network analysis policy with network analysis rules or as the default network analysis policy.

6. Click **Add**.

### What to do next

- Deploy configuration changes.

### Manage network analysis rules

Configure network analysis rules to specify how traffic preprocessing is handled based on defined conditions and configurations.

Network analysis rules allow you to control how traffic preprocessing occurs by defining specific conditions and configurations that determine traffic handling methods.

A network analysis rule is simply a set of configurations and conditions that specifies how you preprocess traffic that matches those qualifications. You create and edit network analysis rules in the advanced options in an existing access control policy. Each rule belongs to only one policy.

### Procedure

1. In the access control policy editor, click **Advanced**, then click **Edit** (✎) next to the Intrusion and Network Analysis Policies section.

   If **View** (👁) appears instead, settings are inherited from an ancestor policy, or you do not have permission to modify the settings.If the configuration is unlocked, uncheck **Inherit from base policy** to enable editing.
2. Next to **Network Analysis Rules**, click the statement that indicates how many custom rules you have.
3. Edit your custom rules. You have the following options:
   - To edit a rule's conditions, or change the network analysis policy invoked by the rule, click **Edit** (✎) next to the rule.
   - To change a rule's order of evaluation, click and drag the rule to the correct location. To select multiple rules, use the Shift and Ctrl keys.
   - To delete a rule, click **Delete** (🗑) next to the rule.

> **Tip**
>
> Right-click a rule to display a context menu that lets you cut, copy, paste, edit, delete, or add new network analysis rules.

4. Click **OK**.
5. Click **Save** to save the policy.

---

### What to do next

- Deploy configuration changes.