

The background is a vibrant, abstract graphic. It features a central bright white light source from which numerous colorful rays emanate, creating a sunburst or starburst effect. The rays transition through a spectrum of colors including yellow, orange, red, and various shades of blue and green. Overlaid on this are several large, semi-transparent, wavy shapes in similar color tones, giving the overall image a sense of motion and energy.

cisco *Live!*

Let's go

#CiscoLive



The bridge to possible

Mastering the Snort 3 Upgrade and Configuration in the Cisco Secure Firewall

All while preparing for the SNCF 300-710 exam!

John Wise
Security Education Specialist
BRKCRT-2002

CISCO *Live!*

#CiscoLive

Cisco Webex App

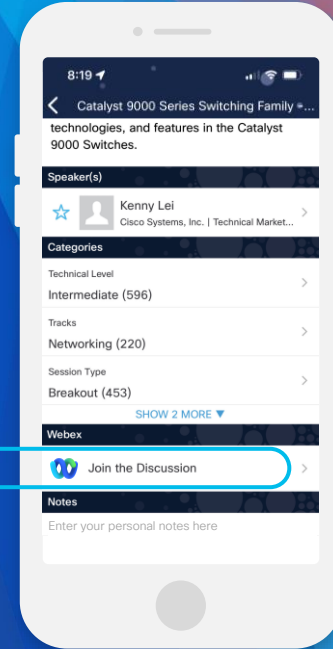
Questions?

Use Cisco Webex App to chat with the speaker after the session

How

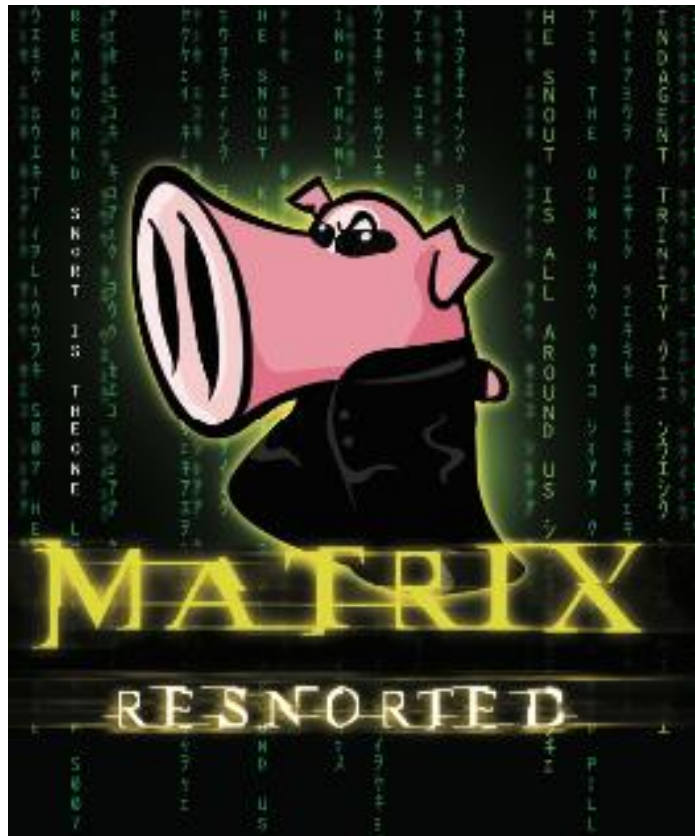
- 1 Find this session in the Cisco Live Mobile App
- 2 Click “Join the Discussion”
- 3 Install the Webex App or go directly to the Webex space
- 4 Enter messages/questions in the Webex space

Webex spaces will be moderated by the speaker until June 9, 2023.



<https://ciscolive.ciscoevents.com/ciscolivebot/#BRKCRT-2002>

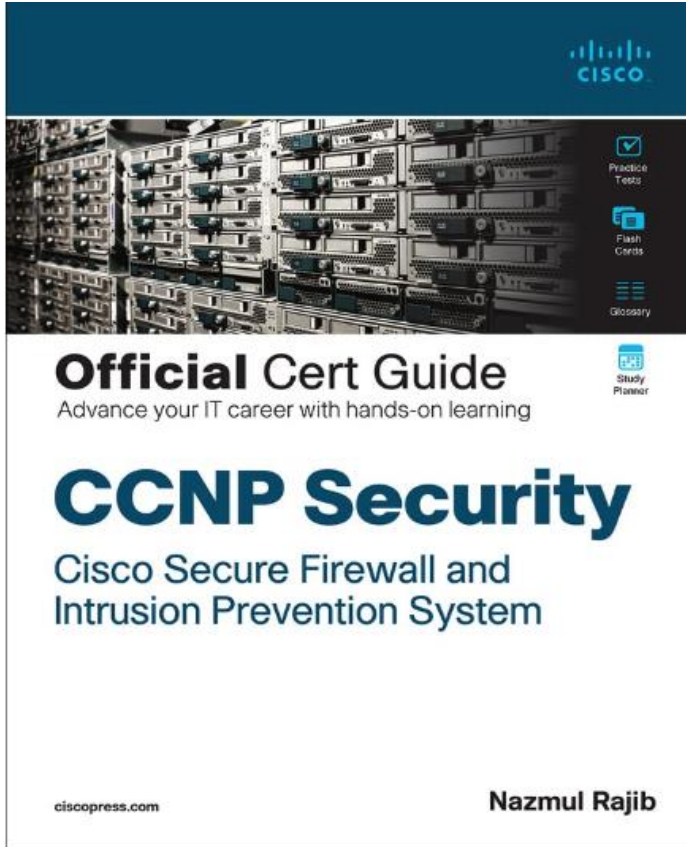
Supplemental Slides In This Presentation!



Look for this Snorty Logo!

Lots of additional information available within this presentation document!

Win the newly updated Secure Firewall Guide!



Snort 3 Administrative Expectations

This is easy!



Entirely new installation
starting with 7.x

Not too difficult.



Upgrading a small
environment from 6.x

*Can get
complicated.*



Upgrading a large
environment from 6.x

Things To Learn For Mastering Snort 3



Covered in this presentation!

Firewall Recommendations

Overrides Vs. Layers

Sync Tool

Intrusion Policy Changes

Custom and Pass Rules

Security Levels

Rule Actions Vs. States

New Snort Features and Tools

Examples:

- Elephant Flow Detection
- Encrypted Visibility Engine

Need to Modify the Network Analysis Policy?

Advanced Manual Configuration

They make it sound so easy! But we have lots of unanswered questions.



Will my admin life become more difficult?

What mistakes could I make?

How does managing Snort 3 compare to Snort 2?

What if I have *both* Snort 2 and Snort 3 firewalls?

What about all the Snort 2 changes I made?

*“How do my administrative tasks
change once I upgrade to Snort 3?”*

You the customer
Company XYZ

Two Policies Manage Snort

Intrusion Policy

(Primary IPS Policy)



Network Analysis
Policy (NAP)

(Optional IPS configuration)



Intrusion Policy

(Intrusion) IPS Policy



Firewall Management Center

Policies / Access Control / Intrusion / [Intrusion Policies](#)

[Overview](#)

[Analysis](#)

[Policies](#)

[Devices](#)

[Objects](#)

[Integration](#)



bd6405johnwis ▾



SECURE

Intrusion Policies

Network Analysis Policies

Hide Snort 3 Sync status ⓘ

Search by Intrusion Policy, Description, or Base Policy

[All IPS Rules](#)

[IPS Mapping ⓘ](#)

[Compare Policies](#)

[Create Policy](#)

Intrusion Policy	Description	Base Policy	Usage Information
dCloud Intrusion Policy ➤ Snort 3 is in sync with Snort 2. 2022-06-15 11	*DO NOT CHANGE*	Balanced Security and Connectivity	1 Access Control Policy 1 Device

[Snort 2 Version](#)

[Snort 3 Version](#)



Both Snort 2 and Snort 3 IPS Policies manage Snort rules.

(Intrusion) IPS Policy



Firewall Management Center

Policies / Access Control / Intrusion / [Intrusion Policies](#)

[Overview](#)

[Analysis](#)

[Policies](#)

[Devices](#)

[Objects](#)

[Integration](#)



bd6405johnwis ▾

SECURE

[Intrusion Policies](#)

[Network Analysis Policies](#)

[Hide Snort 3 Sync status](#) ⓘ

🔍 Search by Intrusion Policy, Description, or Base Policy

[All IPS Rules](#)

[IPS Mapping](#) ⓘ

[Compare Policies](#)

[Create Policy](#)

Intrusion Policy	Description	Base Policy	Usage Information
dCloud Intrusion Policy ➔ Snort 3 is in sync with Snort 2. 2022-06-15 11	*DO NOT CHANGE*	Balanced Security and Connectivity	1 Access Control Policy 1 Device

[Snort 2 Version](#)

[Snort 3 Version](#)



You manage the IPS Policy for Snort 3 differently than Snort 2!

Lots of changes, but easy to learn. We will be exploring these!

Network Analysis Policy (NAP)

Network Analysis Policy (NAP)

The screenshot shows the 'Advanced' tab of a configuration interface. It lists several policy settings:

- SSL Policy Settings**: SSL Policy to use for inspecting encrypted connections. Value: dCloud SSL Policy.
- TLS Server Identity Discovery**: Early application detection and URL categorization. Value: Enabled.
- Prefilter Policy Settings**: Prefilter Policy used before access control. Value: Default Prefilter Policy_1.
- Network Analysis and Intrusion Policies**:
 - Intrusion Policy used before Access Control rule is determined. Value: dCloud Intrusion Policy.
 - Intrusion Policy Variable Set. Value: dCloud_variable_set.
 - Default Network Analysis Policy**. Value: dCloud Network Analysis Policy. This row is highlighted with a blue border.

NAP is enabled in the advanced section of your ACP by default.

NAP manages *critical* Snort engine functions and can be modified for certain deployments.

Snort 2 Versus Snort 3



What an upgrade!!

Intrusion Policy Vs. Network Analysis Policy

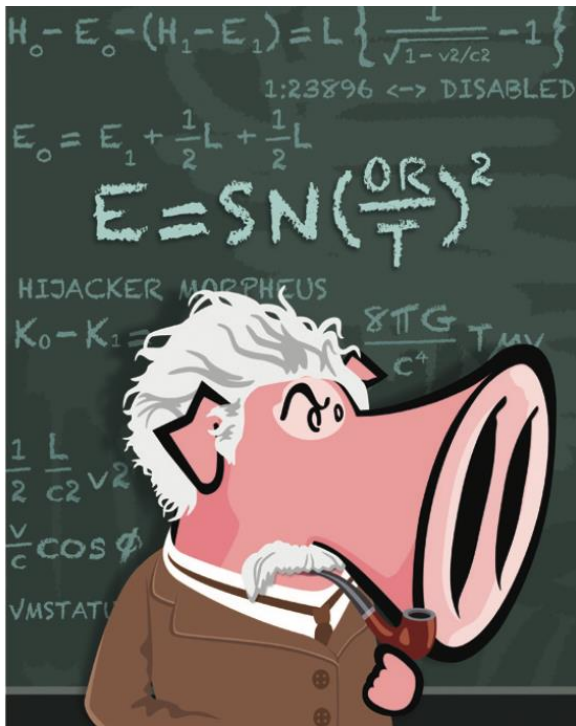
Intrusion Policy is how you manage driving the car.



Network Analysis Policy manages everything under the hood.

Network Analysis Policy in Snort 3

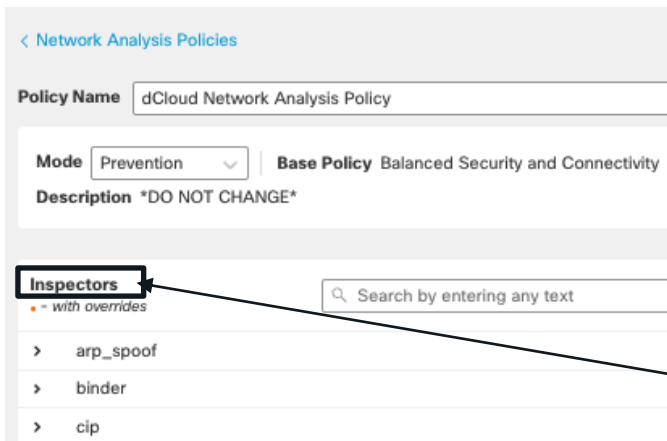
NAP has changed *significantly* in Snort 3!



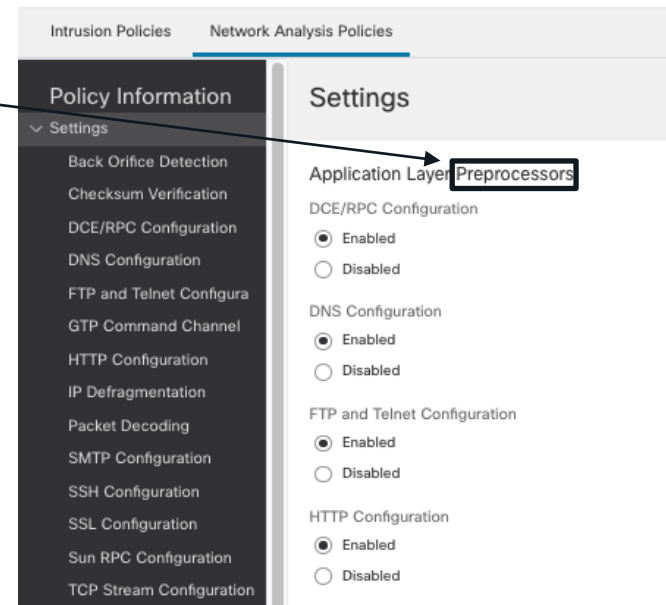
If you have made any changes to preprocessor settings in your Network Analysis Policy in Snort 2, these settings **will not** automatically convert over.

NAP in Snort 2 Vs. Snort 3

Snort 2 NAP manages Snort *Preprocessors*.



In Snort 3 these are called *Inspectors*.



“Great! Overall, just two policies have changed. Managing Snort 3 should not be such a challenge after all!”

You the customer
Company XYZ



*“How challenging will the upgrade
be for me?”*

You the customer
Company XYZ

Can I upgrade to Snort 3?

Starting in 7.0, the firewall runs *either* the Snort 2 or Snort 3 engine.

Upgrades from 6.x:

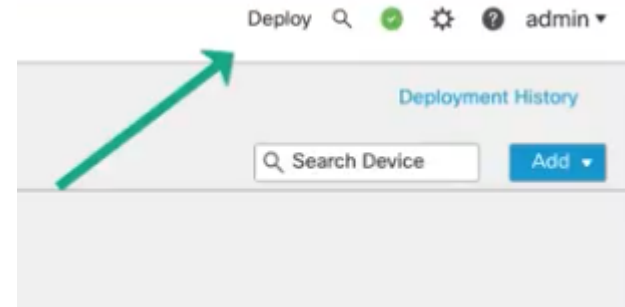
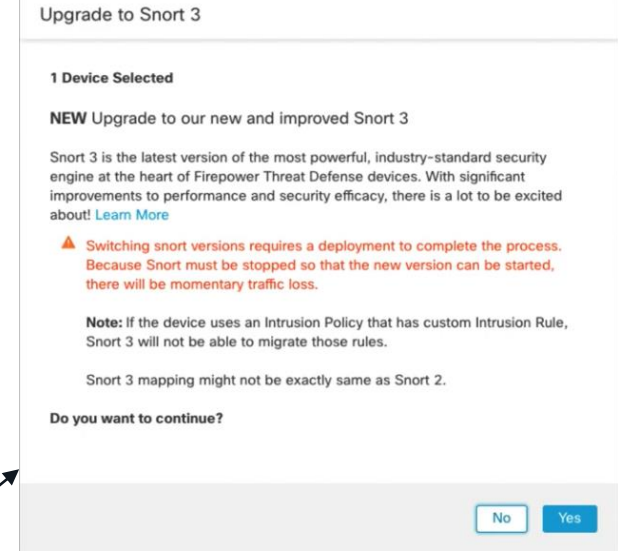
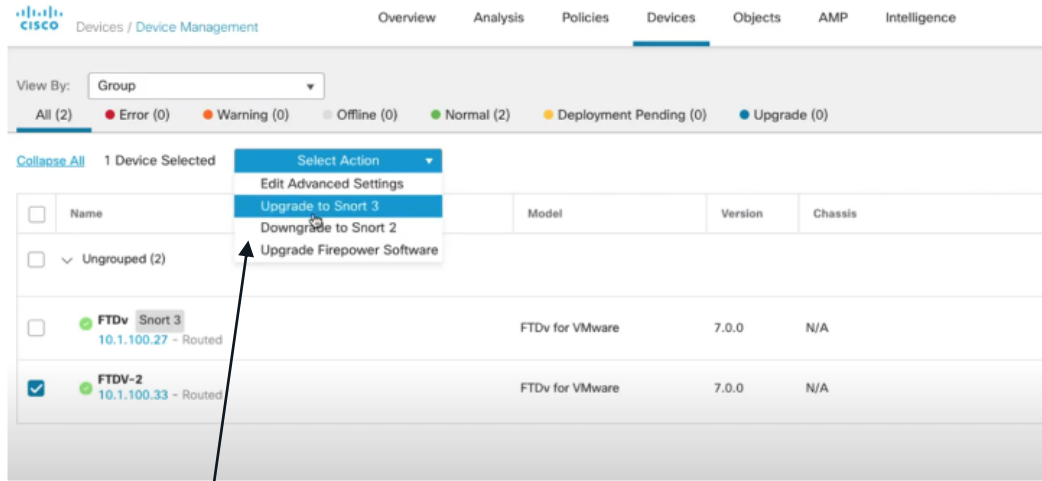
Firewall runs Snort 2 but can easily be **converted** to Snort 3.



OR



How to Upgrade from Snort 2 to Snort 3



1 Select the device you wish to upgrade and select 'Upgrade to Snort 3'.

2 Read the disclaimer!

3 Deploy.

Reverting to Snort 2 from Snort 3



Perform *only* during a maintenance window.

All (1) ● Error (0) ● Warning (0) ● Offline (0) ● Normal (1)

[Collapse All](#) 1 Device Selected

Select Action ▼

- Edit Advanced Settings
- Upgrade to Snort 3
- Downgrade to Snort 2**
- Upgrade Firepower Software

☐	Name
☒	Ungrouped (1)
☒	FTDv Snort 3 198.18.133.11 - Routed

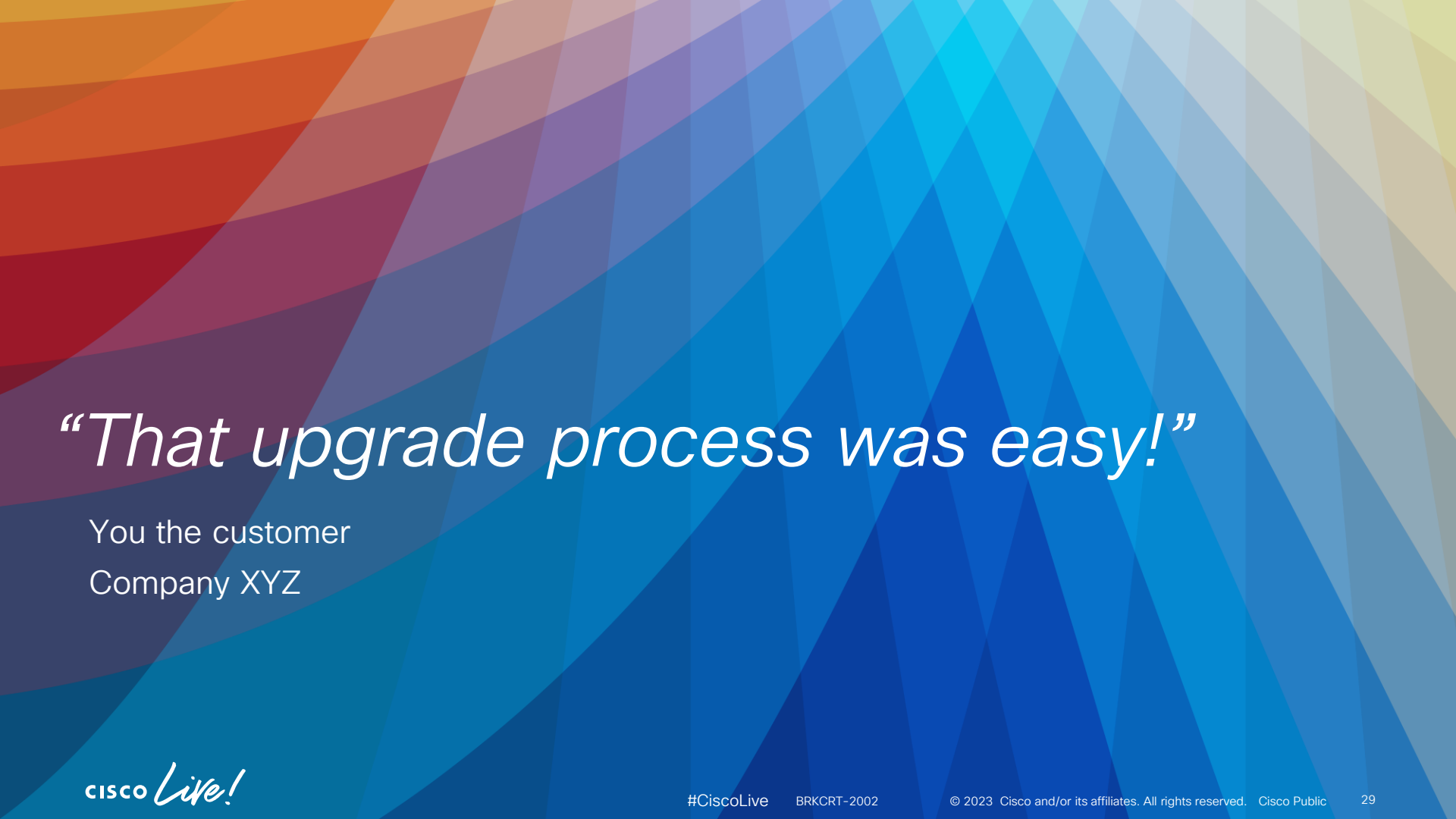
1 Select the device you wish to revert and select 'Downgrade to Snort 2'.

2 Deploy.

Deploy 🔍 🟢 ⚙️ ⓘ admin ▼

Deployment History

🔍 Search Device [Add ▼](#)



“That upgrade process was easy!”

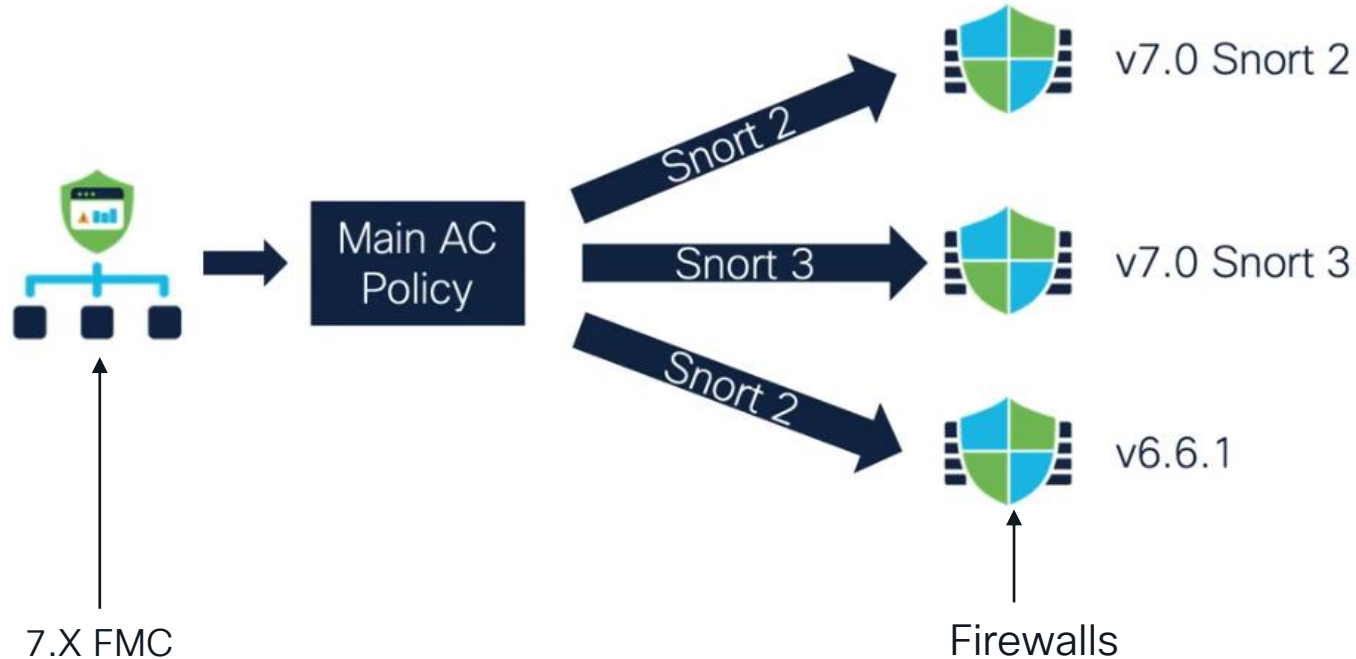
You the customer
Company XYZ



“How does the FMC manage both versions of Snort? Can this get confusing for me?”

You the customer
Company XYZ

Mixing Snort 2 and Snort 3



The FMC Manages all Versions

The 6.x firewall runs only the Snort 2 engine.



OR



The 7.x firewall runs either the Snort 2 or Snort 3 engine.

Management Center (FMC) 7.0 and Later

Starting with FMC 7.0, both policies will be able to manage both Snort 2 and Snort 3 firewalls.

The image displays two screenshots of the Cisco Management Center (FMC) 7.0 and later interface, illustrating the management of Snort 2 and Snort 3 firewalls.

Top Screenshot: Intrusion Policies

- Navigation:** "Intrusion Policies" is selected.
- Search:** "Search by Intrusion Policy, Description, or Base Policy".
- Buttons:** "All IPS Rules", "IPS Mapping", "Compare Policies", "Create Policy".
- Table:**

Intrusion Policy	Description	Base Policy	Usage Information
dCloud Intrusion Policy → Snort 3 is in sync with Snort 2. 2022-06-15 11:00	*DO NOT CHANGE*	Balanced Security and Connectivity	1 Access Control Policy 1 Device
- Actions:** "Snort 2 Version" and "Snort 3 Version" links are highlighted with boxes.

Bottom Screenshot: Network Analysis Policies

- Navigation:** "Network Analysis Policies" is selected.
- Search:** "Filter by Policy Name, Description, or Base Policy".
- Buttons:** "NAP Mapping", "Compare Policies", "Create Policy".
- Table:**

Network Analysis Policy	Description	Base Policy	Usage Information
dCloud Network Analysis Policy	*DO NOT CHANGE*	Balanced Security and Connectivity	1 Access Control Policy 1 Device
- Actions:** "Snort 2 Version" and "Snort 3 Version" links are highlighted with boxes.

Annotations:

- A central text box labeled "Snort 2 ruleset and preprocessors." has arrows pointing to the "Snort 2 Version" links in both screenshots.
- A central text box labeled "Snort 3 ruleset and inspectors" has arrows pointing to the "Snort 3 Version" links in both screenshots.

Ruleset Tied to Snort Version in Each Firewall

All IPS policies have a Snort 2 ruleset and a Snort 3 ruleset starting in 7.x.

CISCO Devices / Device Management

View By: Group
All (1) Error (0) Warning (0)

[Collapse All](#)

☐	Name
☐	Ungrouped (1)
☐	FTDv Snort 3 198.18.133.11 - Routed

The ruleset you use depends on the version of Snort FTD is using.

Ruleset used if FTD is running Snort 2.

Ruleset used if FTD is running Snort 3.

Intrusion Policies Network Analysis Policies

Show Snort 3 Sync status Search by Intrusion Policy, Description, or Base Policy

All IPS Rules IPS Mapping Compare Policies Create Policy

Intrusion Policy	Description	Base Policy	Usage Information	
dCloud Intrusion Policy	*DO NOT CHANGE*	Balanced Security and Connectivity	1 Access Control Policy 1 Device	Snort 2 Version Snort 3 Version
high security networks		Security Over Connectivity	No Access Control Policy No Device	Snort 2 Version Snort 3 Version
Production Network IPS		Balanced Security and Connectivity	No Access Control Policy No Device	Snort 2 Version Snort 3 Version
production networks		Balanced Security and Connectivity	No Access Control Policy No Device	Snort 2 Version Snort 3 Version
wireless networks		Connectivity Over Security	No Access Control Policy No Device	Snort 2 Version Snort 3 Version

“Ok, so I need to plan things carefully when managing environments with firewalls running both versions. We can handle this!”

You the customer
Company XYZ

*“What primary configuration options
will I need to manage in these Snort
rulesets?”*

You the customer
Company XYZ

7.X FMC Available Rules



Snort Rule Version	Rules available to use	FMC Rule actions available	Source	Base Policies
Snort 2	48,818	3	Talos	Identical
Snort 3	48,526	Up to 7	Talos	Identical

(As of SRU
01/20/2023)



Snort 2 and 3 rules cover the same threats/vulnerabilities!

Snort Rule Action Options

Browser / WebKit

Security Level ■■■■■ Edit

Description Rules for detecting exploits against the WebKit framework

Rule Action ▼

Preset Filters: 0 Alert rules | 56 Block rules | 103 Disabled rules | 1 Overridden rules | [Advanced Filters](#)

160 rules

[1 Rewrite rules](#) |

☐	GID:SID	Info	Rule Action
> ☐	1:51383 🔗	BROWSER-WEBKIT Apple Safari DFG InstanceOf model mem...	Rewrite ▼ ↔ ✔
> ☐	1:51384 🔗	BROWSER-WEBKIT Apple Safari DFG InstanceOf model mem...	Block (Default) ▼ Block (Default) Alert Rewrite Pass Drop Reject Disable Revert to default
> ☐	1:51388 🔗	BROWSER-WEBKIT Apple Safari JSValues type confusion att...	
> ☐	1:51389 🔗	BROWSER-WEBKIT Apple Safari JSValues type confusion att...	
> ☐	1:53122 🔗	BROWSER-WEBKIT Apple Safari WebKit cached page memor...	
> ☐	1:53121 🔗	BROWSER-WEBKIT Apple Safari WebKit cached page memor...	
> ☐	1:53123 🔗	BROWSER-WEBKIT Apple Safari WebKit cached page univers...	

All Snort rules have an *action*.

The action tells FTD what to do *when the rule matches a packet*.

Snort 2 'Actions' Are Called 'Rule States'

Intrusion Policies Network Analysis Policies

Policy Information

Rules

Firepower Recommendations

> Advanced Settings

> Policy Layers

Rules

Rule Configuration

Rule Content

Category

app-detect

browser-chrome

browser-firefox

browser-ie

browser-other

browser-plugins

browser-webkit

content-replace

decoder

exploit-kit

file-executable

Filter:

1 selected rule of 46669

Rule State ▼ Event Filtering ▼ Dynamic State ▼ Alerting ▼ Comments ▼

Generate Events

Drop and Generate Events

Disable

1 28071 APP-DETECT 360.cn SafeGuard local HTTP management console access attempt

1 28068 APP-DETECT 360.cn Safeguard runtime outbound communication

Disable – Rule is not enabled.

Drop and Generate Events – Generate an event and drop the packet and all subsequent packets in this connection.

Generate Events – Generate an event only.

Snort 3 Rule Action Options

Snort 3 action is configured by changing the rule **action**.

The screenshot shows the 'Rules' configuration page in the Snort 3 interface. The left sidebar contains 'Policy Information', 'Rules', 'Firepower Recommendations', 'Advanced Settings', and 'Policy Layers'. The main area is titled 'Rules' and includes a 'Filter:' field and a 'Category' dropdown. Below this, a table lists rules. The 'Rule State' dropdown for the first rule is highlighted with a red box, and an arrow points from the text 'Snort 2 action is configured by changing the rule **state**.' below to it.

Rule State	Event Filtering	Dynamic State	Alerting	Comments
Generate Events				
Drop and Generate Events				
Disable				
☐ 1	28071	APP-DETECT 360.cn SafeGuard local HTTP management console access attempt		
☐ 1	28068	APP-DETECT 360.cn Safeguard runtime outbound communication		

Snort 2 action is configured by changing the rule **state**.

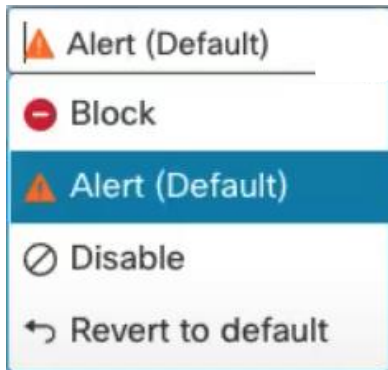
The screenshot shows the 'Rule Action' dropdown menu. The 'Block' option is selected and highlighted with a blue bar. Other options include Alert, Rewrite, Pass, Drop, Reject, Disable, and Revert to default.

- Block
- Alert
- Rewrite
- Pass
- Drop
- Reject
- Disable
- Revert to default

Snort 3 Rule Actions 7.x

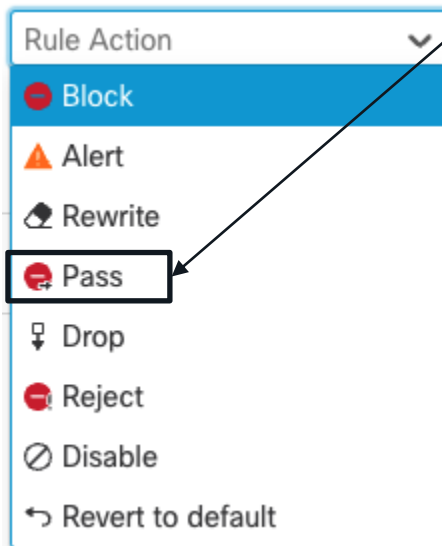
7.0

Same options as Snort 2 but with different names.



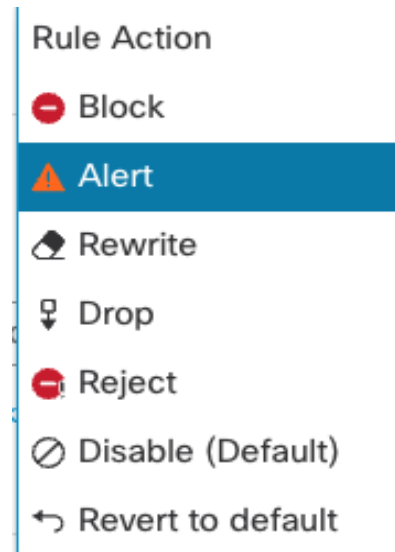
7.1

Four new rule actions available.



7.2

Pass rule action no longer available except for *custom pass rules*.



Talos Rule Action Options

Snort Rule version	Rule action name	Action option to not utilize the rule	Generate an Intrusion Event and drop the packet and all subsequent packets in this connection	Generate an Intrusion Event only
Snort 2	Rule State	Disable	Drop and Generate Events	Generate Events
Snort 3	Rule Action	⊘ Disable	⊘ Block	⚠ Alert



New Custom Snort Rule Actions For Snort 3

- **Drop:** Drop packet only, do not block entire connection/flow.
Important! The effect of this rule action is different than the 'Drop and Generate' rule state in Snort 2.
- **Reject:** Block the packet and send a TCP reset if the protocol is TCP or an ICMP port unreachable message if the protocol is UDP.
- **Rewrite:** Replace packet contents.



These actions are not currently used in the Talos rules, and it would be highly unlikely you would ever use these actions.

Snort Rules Drop Action Warning!

The "*drop*" action is *not commonly used*!

Action: **drop**

Snort 2 Equivalent: **none**

Description: Packets matching a `drop` rule are dropped however the connection they are a part of is not blocked. Use this to drop **ONLY** the offending packet.

Example:

```
drop tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (  
msg:"SERVER-APACHE Apache Struts allowStaticMethodAccess  
invocation attempt"; flow:to_server,established; http_uri;  
content:".action?",nocase;  
content:"allowStaticMethodAccess",distance 0,nocase;  
sid:21073; rev:7; )
```



Important! This is not the same as ***Drop and Generate*** in Snort 2.

In Snort 3 ***Drop and Generate*** is equivalent is ***Block***.

'Block' is the New 'Drop and Generate'

Snort Rule version	Rule action name	Action option to not utilize the rule	Generate an Intrusion Event and drop the packet and all subsequent packets in this connection	Generate an Intrusion Event only
Snort 2	Rule State	Disable	Drop and Generate Events	Generate Events
Snort 3	Rule Action	⊘ Disable	🛑 Block	⚠ Alert



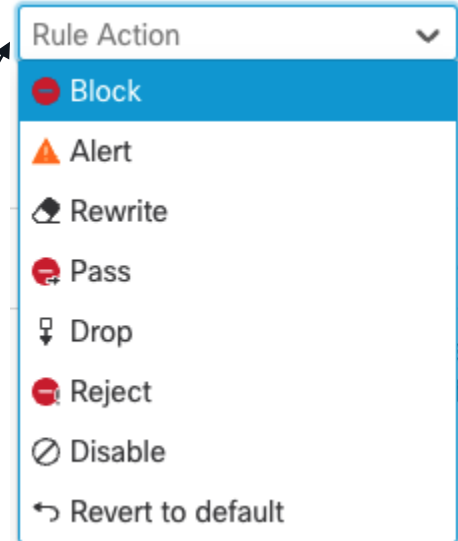
Do not accidentally use the 'Drop' action!

Open-Source Snort Action Vs FTD Snort Action

Open-Source Snort rules specify the action *in the rule*.

`block tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (`
`msg:"SERVER-APACHE Apache Struts allowStaticMethodAccess`
`invocation attempt"; flow:to_server,established; http_uri;`
`content:".action?",nocase;`
`content:"allowStaticMethodAccess",distance 0,nocase;`
`sid:21073; rev:7; )`

FTD Snort Rules specify the action *in the GUI*.



'Alert' Action in Rule Syntax

☐	GID:SID	Info	Rule Action 1	Assigned Groups
> ☐	133:6 🔗	(dce_smb) SMB - bad byte count	⚠️ Alert ↔️ ✅	Protocol/Builtins 📄 💬
> ☐	133:7 🔗	(dce_smb) SMB - bad format type	⚠️ Alert ↔️	Protocol/Builtins 📄 💬
> ☐	133:2 🔗	(dce_smb) SMB - bad NetBIOS session service sessio...	⚠️ Alert ↔️ ✅	Protocol/Builtins 📄 💬
▼ ☐	133:8 🔗	(dce_smb) SMB - bad offset	🛑 Block ↔️ ✅	Protocol/Builtins 📄 💬
alert gid:133; sid:8; rev:2; msg:"(dce_smb) SMB - bad offset"; metadata: policy max-detect-ips drop, rule-type preproc; reference:url,msdn.microsoft.com/en-us/library/cc201989.aspx; service:dcerpc; classtype:bad-unknown;)				

All Talos rules contain the *alert* action in the rule syntax.

'Alert' in the rule syntax does not specify anything unique in the FMC.

Pork Quiz!



Rule action set to *Block* by the administrator.

☐	GID:SID	Info	Rule Action	Assigned Groups
> ☐	133:6	(dce_smb) SMB - bad byte count	Alert	Protocol/Builtins
> ☐	133:7	(dce_smb) SMB - bad format type	Alert	Protocol/Builtins
> ☐	133:2	(dce_smb) SMB - bad NetBIOS session service sessio...	Alert	Protocol/Builtins
▼ ☐	133:8	(dce_smb) SMB - bad offset	Block	Protocol/Builtins

alert (gid:133; sid:8; rev:2; msg:"(dce_smb) SMB - bad offset"; metadata: policy max-detect-ips drop, rule-type preproc; reference:url,msdn.microsoft.com/en-us/library/cc201989.aspx; service:dcerpc; classtype:bad-unknown;)

The rule syntax specifies the action of *alert*.

Will this rule block the packet or only alert?

FTD Rule Action Configuration

Rule action set to *Block* by the administrator.

☐	GID:SID	Info	Rule Action		Assigned Groups
> ☐	133:6	(dce_smb) SMB - bad byte count	Alert	<> ✓	Protocol/Builtins
> ☐	133:7	(dce_smb) SMB - bad format type	Alert	<>	Protocol/Builtins
> ☐	133:2	(dce_smb) SMB - bad NetBIOS session service session	Alert	<> ✓	Protocol/Builtins
▼ ☐	133:8	(dce_smb) SMB - bad offset	Block	<> ✓	Protocol/Builtins

alert gid:133; sid:8; rev:2; msg:"(dce_smb) SMB - bad offset"; metadata: policy max-detect-ips drop, rule-type preproc; reference:url,msdn.microsoft.com/en-us/library/cc201989.aspx; service:dcerpc; classtype:bad-unknown;)

Notice the rule syntax remains *alert*.

“Ok got it! So even though there are a few new actions available in Snort 3 it’s unlikely I would ever use them. So not much has changed for my decision-making processes for the rule actions!”

You the customer
Company XYZ

*“How are rules organized in Snort 3?
I heard you now have greater
flexibility in changing rule states per
category? How does this relate to
Base Polices?”*

You the customer
Company XYZ

Snort 3 Security Levels

Talos Managed Base Policy

In most networks
use this one!



Warning! **Maximum Detection** base policy not typically used in production. It enables almost 40,000 rules!

*700 rules
enabled*

*10,000 rules
enabled*

*21,000 rules
enabled*

Connectivity
over
Security

Balanced Security
and
Connectivity

Security
over
Connectivity



Snort 3 Rules are Organized by Groups

cisco Policies / Access Control / Intrusion / Intrusion Policies

< Intrusion Policy

Policy Name dCloud Intrusion Policy

Mode Prevention Base Policy Balanced Security

Description *DO NOT CHANGE*

Disabled 34750 Alert 358 Block 11441 Override

Rule Groups

51 items Search Rule Group +

Excluded Included Overridden

All Rules

Recommended Rules (In use)

- > Browser (6 groups)
- > Server (8 groups)
- > Policy (1 group)
- > Indicator (4 groups)
- > Potentially Unwanted Applications (3 groups)
- > Malware (5 groups)
- > File (9 groups)
- > Operating Systems (5 groups)
- > Protocol (10 groups)

Each Intrusion Policy has approx. 55 groups.

Rule groups have a high-level category.



Remember Snort 2 and Snort 3 have mostly the *same rules*, so category and group are just different ways to organize and manage these rules.

Rule Groups

50 items Search Rule Group +

Excluded Included Overridden

All Rules

Local Rules

- Browser (6 groups)
- WebKit
- Plugins
- Firefox
- Other
- Chrome
- Internet Explorer
- > Server (8 groups)
- > Policy (1 group)
- > Indicator (4 groups)

Snort Rule Group Security Level

Connectivity over Security

Edit Security Level ?



Use the least aggressive enforcement on these rules, so that connectivity is preferred over security

Cancel

Save

Security over Connectivity

Edit Security Level ?



Use an aggressive approach to enforcing these rules, so that security is preferred over connectivity

Cancel

Save

Balanced Security and Connectivity

Edit Security Level ?



Use a balanced approach to enforcing these rules, so that both connectivity and security are given equal preference

Cancel

Save

Maximum Detection



Edit Security Level ?



Use the most aggressive enforcement on these rules, to provide the maximum security in preference to connectivity

Cancel

Save

Security Levels
allow you to
change the *base policy* of these
groups!

Increasing Security in a Snort 2 IPS Policy

In Snort 2, changing security in an IPS Policy would require changing the *base policy*.

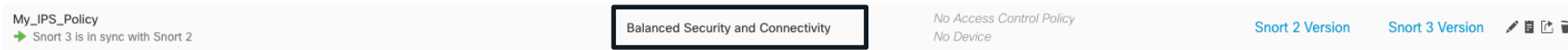
The image shows a comparison of two Snort 2 IPS policies. The top policy, 'Balanced Security and Connectivity', has 48,715 rules and 9,123 block rules. The bottom policy, 'Security Over Connectivity', has 48,715 rules and 20,597 block rules. Arrows indicate the transition from the top policy to the bottom one. The 'Block rules' counts are highlighted with boxes.

Policy	Base Policy	Rule Action	48,715 rules	Preset Filters
Top	Balanced Security and Connectivity	Rule Action	48,715 rules	469 Alert rules 9,123 Block rules 39,123 Disabled rules
Bottom	Security Over Connectivity	Rule Action	48,715 rules	651 Alert rules 20,597 Block rules 27,467 Disabled rules



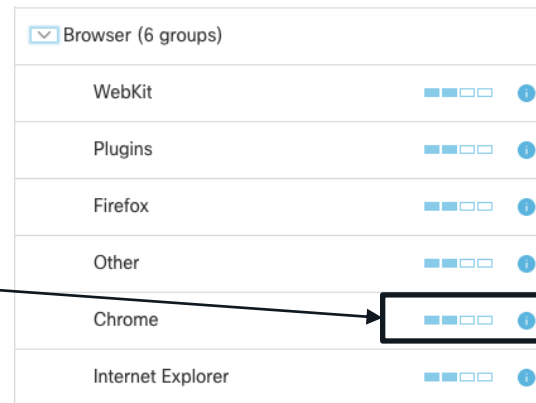
This change enables over 10,000 additional rules! This is a significant increase.

Snort 3 Rule Security Levels



The *Base policy* for all IPS policies sets the *security level* for *all the rules* within the same IPS policy.

The *security level* allows you to change this *per group*.



Utilizing Security Levels

Create Intrusion Policy

Name*

Balanced Policy

Description

Inspection Mode



Detection



Prevention

Intrusion rule actions are always applied. Connections that match a drop rule are blocked.

Base Policy

Balanced Security and Connectivity

Cancel

Save

1'st

Create intrusion policy and specify base policy.

Now All 50+ groups will be set to the 'Balanced' security level.

Browser (6 groups)

WebKit



Plugins



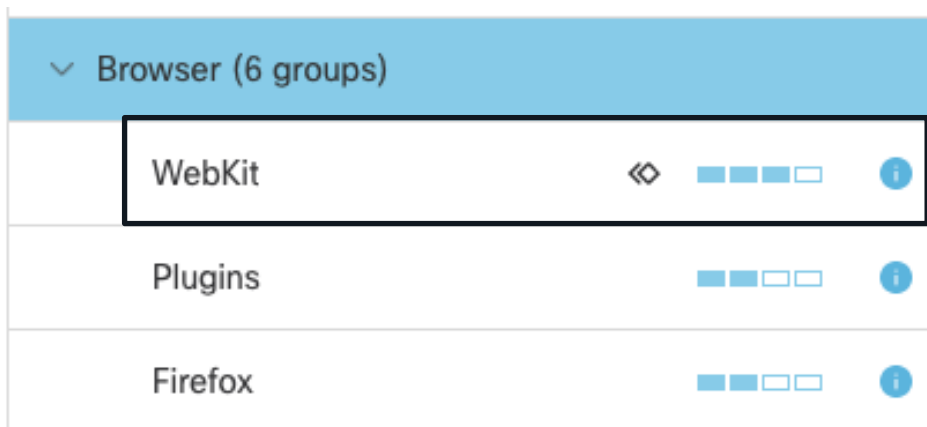
Firefox



Utilizing Security Levels

2'nd

Now *increase* or *decrease* security level (base policy) based on the groups.



WebKit has been increased to 'Security Over Connectivity'.

Another Example!

Balanced as the Base Policy.

Now, any *Chrome* group changes Talos makes is automatically using the *Security over Connectivity* policy.

Browser / Chrome

Security Level  Edit

Description Rules for detecting exploits against the Chrome Web browser

Rule Action 

 Search by CVE, SID, Reference Info, or Rule Message

179 rules

Preset Filters: [0 Alert rules](#) | [20 Block rules](#) | [159 Disabled rules](#) | [0 Overridden rules](#) | [Advanced Filters](#)

20 rules set to block

Browser/Chrome changed to Security Level 

Browser / Chrome

Security Level  Edit

Description Rules for detecting exploits against the Chrome Web browser

Rule Action 

 Search by CVE, SID, Reference Info, or Rule Message

179 rules

Preset Filters: [0 Alert rules](#) | [103 Block rules](#) | [76 Disabled rules](#) | [0 Overridden rules](#) | [Advanced Filters](#)

Now 103 rules set to block

“The new security levels sure make it easy to configure different levels of security for only applicable parts of my network. Great feature!”

You the customer
Company XYZ



“What about Firewall/Firepower Recommendations?”

You the customer
Company XYZ

Secure Firewall Recommendations

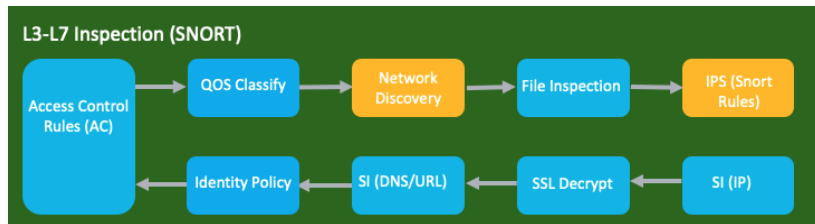
Secure Firewall Recommendations



Network Discovery for *hosts* must be enabled and working as expected for this feature to function.



L3-L7 Inspection
(SNORT)



Add Rule

Discover ☒ Hosts ☐ Users ☒ Applications

Secure Firewall Recommendations

Recommendations will recommend to change the rule action to:



Block



Alert



If the vulnerability is seen in the network.



Disable



If the vulnerability is NOT seen in the network.

Secure Firewall Recommendation Example

Network Discovery discovered a Windows 10 host that has vuln cve:2013-1690.

The disabled Snort rule addressing this vulnerability will be recommended to be enabled.

Host Profile Vulnerability

Vulnerability the rule is protecting against

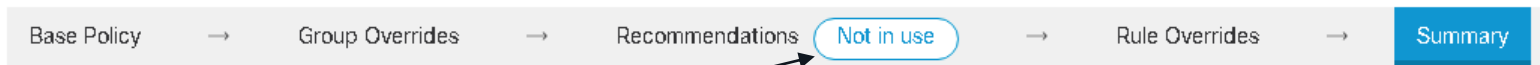
Vulnerabilities (362)

Edit Vulnerabilities

Name	Remote	Component	Port
Adobe Acrobat, Reader, and Flash Player Remote Code Execution Vulnerability	Yes	Mac OSX 10.5, 10.6, 10.14, Server 10.5, Server 10.6, Server 10.14	
Adobe Flash Player and AIR 'intf_count' Integer Overflow Vulnerability	Yes	Mac OSX 10.5, 10.6, 10.14, Server 10.5, Server 10.6, Server 10.14	

```
rule alert tcp $EXTERNAL_NET any -> $SMTP_SERVERS 25 (msg:"BROWSER-FIREFOX Mozilla Firefox 17 onreadystatechange memory corruption attempt"; flow:to_server,established; file_data;; content:"document.onreadystatechange"; content:"window.parent.ames[0].frameElement.ownerDocument.write("; fast_pattern:only; metadata:policy balanced-ips drop, policy max-detect-ips drop, policy security-ips drop, service smtp; reference:cve,2013-1690; reference:url,pastebin.mozilla.org/2777139; classtype:attempted-user; sid:33089; rev:5; gid:1; )
```

Enabling Rule Recommendations



Select here.

Security Level will default to the security level of your base policy.

Secure Firewall Rule Recommendations

Security Level (Click tiles to select size)

☐ Accept Recommendation to Disable Rules

No Impact– No new rules will be enabled and no existing rules will be disabled. To increase protections, please select a higher Security Level.

Protected Networks

Add +

Cancel

Generate

Generate and Apply

Enabling Rule Recommendation Settings

Security Level can be *adjusted* to match your security approach.



Select here to allow the tool to disable already enabled rules. Use with caution!

Secure Firewall Rule Recommendations



Security Level (Click tiles to select size)



☐ Accept Recommendation to Disable Rules 

No Impact– No new rules will be enabled and no existing rules will be disabled. To increase protections, please select a higher Security Level.

Protected Networks 



Add +

Cancel

Generate

Generate and Apply

Specify the networks in the “*Network map*” you wish to use the discovered data from to make the rule recommendations.

Rule Recommendations Security Level

Connectivity over Security

Edit Security Level ?



Use the least aggressive enforcement on these rules, so that connectivity is preferred over security

Cancel

Save

Balanced Security and Connectivity

Edit Security Level ?



Use a balanced approach to enforcing these rules, so that both connectivity and security are given equal preference

Cancel

Save

Security level for recommendations *is the same* as the security level for rule groups.

Security over Connectivity

Edit Security Level ?



Use an aggressive approach to enforcing these rules, so that security is preferred over connectivity

Cancel

Save

Maximum Detection

Edit Security Level ?



Use the most aggressive enforcement on these rules, to provide the maximum security in preference to connectivity

Cancel

Save

Increased Security Rule Recommendations

Secure Firewall Rule Recommendations ⓘ ✕

Security Level (Click tiles to select size)

☐ Accept Recommendation to Disable Rules ⓘ

No Impact - No new rules will be enabled and no existing rules will be disabled. To increase protections, please select a higher Security Level.

Protected Networks ⓘ

Add +

Cancel Generate Generate and Apply



Secure Firewall Rule Recommendations ⓘ ✕

Security Level (Click tiles to select size)

☐ Accept Recommendation to Disable Rules ⓘ

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

Protected Networks ⓘ

Add +

Cancel Generate Generate and Apply



Move the security level higher

The result: Enable additional rules for vulnerabilities seen on the hosts based on the the higher security level's ruleset.

Focused Security Rule Recommendations

Secure Firewall Rule Recommendations ⓘ ✕

Security Level (Click tiles to select size)

☐ Accept Recommendation to Disable Rules ⓘ

No Impact- No new rules will be enabled and no existing rules will be disabled. To increase protections, please select a higher Security Level.

Protected Networks ⓘ

Add +

Cancel Generate Generate and Apply



Secure Firewall Rule Recommendations ⓘ ✕

Security Level (Click tiles to select size)

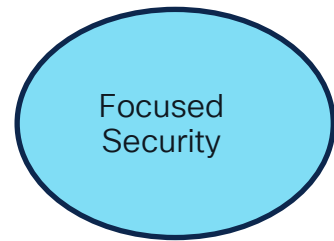
☒ Accept Recommendation to Disable Rules ⓘ

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

Protected Networks ⓘ

Add +

Cancel Generate Generate and Apply



Enable the “Disable Rules” option and move the security level one higher.

The result: Enable additional rules for vulnerabilities seen on the hosts based on the higher security level's ruleset and disable others that do not.

Only Disable Rules Option

Secure Firewall Rule Recommendations ⓘ ✕

Security Level (Click tiles to select size)

☐ Accept Recommendation to Disable Rules ⓘ

No Impact - No new rules will be enabled and no existing rules will be disabled. To increase protections, please select a higher Security Level.

Protected Networks ⓘ

Add +

Cancel Generate Generate and Apply

Enable the “Disable Rules” option.



Secure Firewall Rule Recommendations ⓘ ✕

Security Level (Click tiles to select size)

☒ Accept Recommendation to Disable Rules ⓘ

Higher Efficiency - Keeps existing rules that match potential vulnerabilities on discovered hosts and disables rules for vulnerabilities not found on the network.

Protected Networks ⓘ

Add +

Cancel Generate Generate and Apply



The result: Keep existing rules enabled that match vulnerabilities seen on the hosts but disable others that do not.

Maximum Detection Security Level

Not Typically
Recommended!



Secure Firewall Rule Recommendations ⓘ ✕

Security Level (Click tiles to select size)

☐ Accept Recommendation to Disable Rules ⓘ

No Impact- No new rules will be enabled and no existing rules will be disabled. To increase protections, please select a higher Security Level.

Protected Networks ⓘ

Cancel Generate Generate and Apply



Secure Firewall Rule Recommendations ⓘ ✕

Security Level (Click tiles to select size)

☒ Accept Recommendation to Disable Rules ⓘ

Focused Security- 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.

▲ 'Maximum Detection' enables a very high number of rules and may impact performance. It is recommended to review and test this setting before deploying into a production environment.

Protected Networks ⓘ

Cancel Generate Generate and Apply

Enable the “Disable Rules” option and move the security level to the highest setting: “Maximum Detection” .

The result: Enable additional rules for vulnerabilities seen on the hosts based on the Maximum Detection security level and disable others that do not. Likely to significantly impact performance.

The Safest Option

Secure Firewall Rule Recommendations ⓘ ✕

Security Level (Click tiles to select size)

☐ Accept Recommendation to Disable Rules ⓘ

No Impact - No new rules will be enabled and no existing rules will be disabled. To increase protections, please select a higher Security Level.

Protected Networks ⓘ

Add +

Cancel Generate Generate and Apply



Secure Firewall Rule Recommendations ⓘ ✕

Security Level (Click tiles to select size)

☐ Accept Recommendation to Disable Rules ⓘ

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

Protected Networks ⓘ

Add +

Cancel Generate Generate and Apply



Move the security level higher

The result: Enable additional rules for vulnerabilities seen on the hosts based on the the higher security level's ruleset.

Generate and Apply

Secure Firewall Rule Recommendations ⓘ ✕

Security Level (Click tiles to select size)

☒ Accept Recommendation to Disable Rules ⓘ

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

Protected Networks ⓘ

Add +

Cancel Generate Generate and Apply

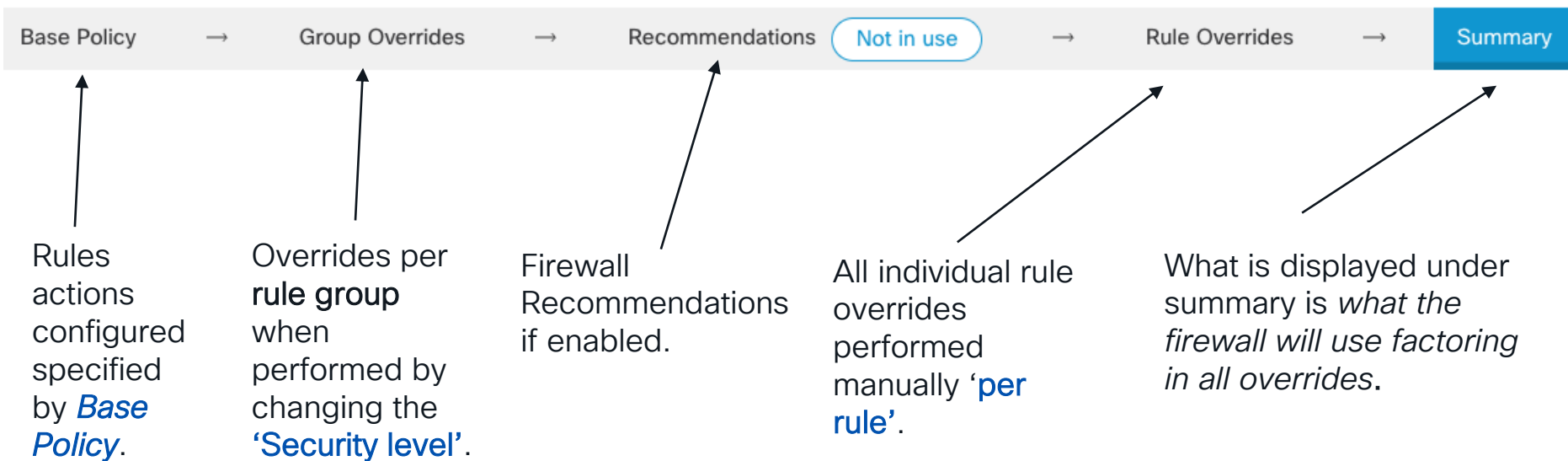
Generate will only generate the recommendations but will not make the changes.

Generate and apply will generate the recommendations and uses them in the IPS policy.



It is best practice to first generate the recommendations and go through the changes **before applying**.

Overrides – IPS Policy Flow



“Nice! Ok so I will be sure to ensure my Network Discovery Policy is enabled and working correctly and then use the recommendations feature!”

You the customer
Company XYZ

“Sounds like overall managing Snort 3 with the IPS policy is not so difficult! Where should I go next on my journey to becoming a true Snort 3 guru in FTD?”

You the customer
Company XYZ



What's next for us to learn?

- Custom/Pass Rules, Sync, and Alerting (Included within this presentation).
- If using 'Firewall Recommendations' ensure 'Network Discovery' is configured correctly!

*How? Slides included within this presentation **and** please watch the Cisco Live replay videos sessions BRKCRT-2001 and BRKCRT-2466.*

- Snort 3 Network Analysis Policy (applicable if you currently use or need to use a modified NAP Policy).

Official Cisco Documentation

 Docs YouTube Channel DevNet Application Detectors Cisco Defense Orchestrator Docs Additional Firewall Learning

v7.2 Home Guides

GETTING STARTED

Secure Firewall

Smart Licensing

Cloud-delivered Firewall Management Center

RELEASE 7.2 FEATURES

EIGRP FMC Configuration

Elephant Flow Detection

Encrypted Visibility Engine

HA and Cluster Upgrade Workflow

Policy-Based Routing with Path Monitoring

Port Scan Detection

Umbrella Connector

Virtual Firewall Clustering

VPN Certificate and SAML Authentication

VXLAN and GENEVE Support

Secure Firewall

An introduction to the Cisco Secure Firewall solutions



To unify and simplify our broad security products portfolio, we've renamed our offerings Cisco Secure. Cisco Secure is built on the principle of better security, not more. It delivers a streamlined, customer-centric approach to security that ensures it's easy to deploy, easy to manage, and easy to use - and that it all works together.

Secure Firewall

New! Starting point for all things Cisco Secure Firewall!

<https://secure.cisco.com/secure-firewall/docs>

Management Center Administration Guide



Management Center-specific guide.

Cisco Secure Firewall Management Center Administration Guide, 7.3

<https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/management-center/admin/730/management-center-admin-73.html>

Firewall *Device* Configuration Guide



Cisco Secure Firewall Management Center Device Configuration Guide, 7.3

Primary guide for the Cisco Secure Firewall.

Approx. 2400 pages!

Snort 2 configuration.

<https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/management-center/device-config/730/management-center-device-config-73.html>

Snort 3 Configuration Guide

... / Cisco Secure Firewall Management Center / Configuration Guides /

Cisco Secure Firewall Management Center Snort 3 Configuration Guide, Version 7.3

 Find Matches in This Book

Book Table of Contents

[An Overview of Network Analysis and Intrusion Policies](#)

[Migrate from Snort 2 to Snort 3](#)

> [Intrusion Detection and Prevention in Snort 3](#)

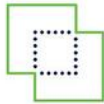
> [Advanced Network Analysis in Snort 3](#)

All things Snort 3.

Does NOT cover Snort 2!

<https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/management-center/snort/730/snort3-configuration-guide-v73.pdf>

Cisco Secure Firewall YouTube Channel



Cisco Secure Firewall

@CiscoNetSec 5.06K subscribers 221 videos

Welcome to Cisco Secure Firewall Channel. >

Subscribe

HOME

VIDEOS

LIVE

PLAYLISTS

COMMUNITY

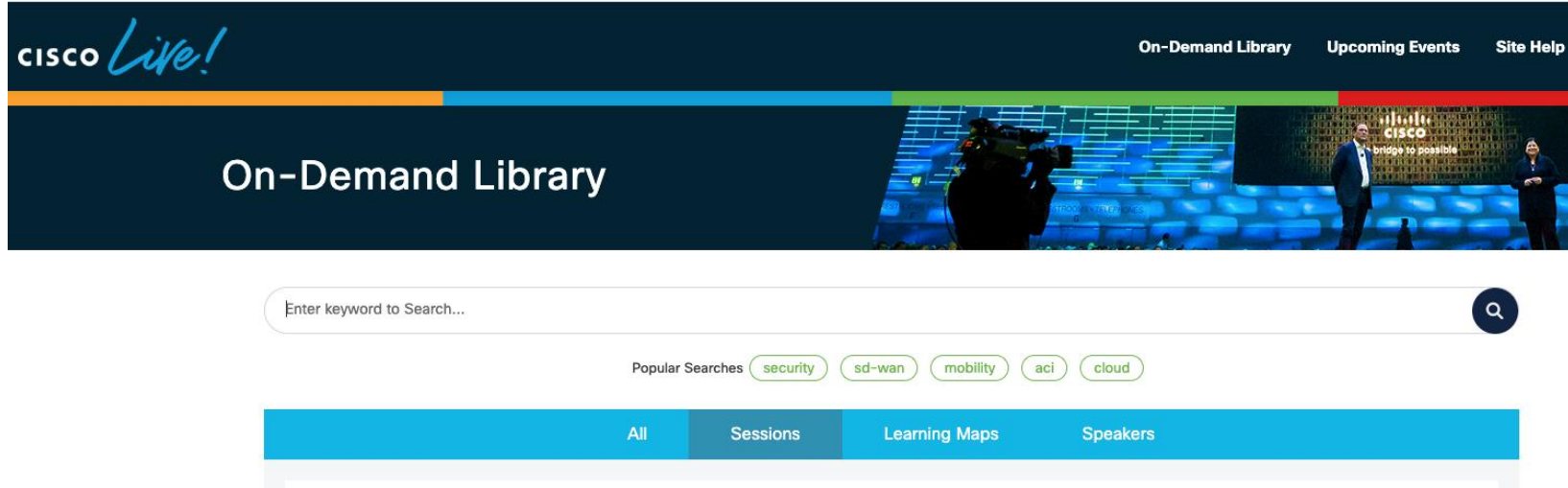
CHANNELS

ABOUT

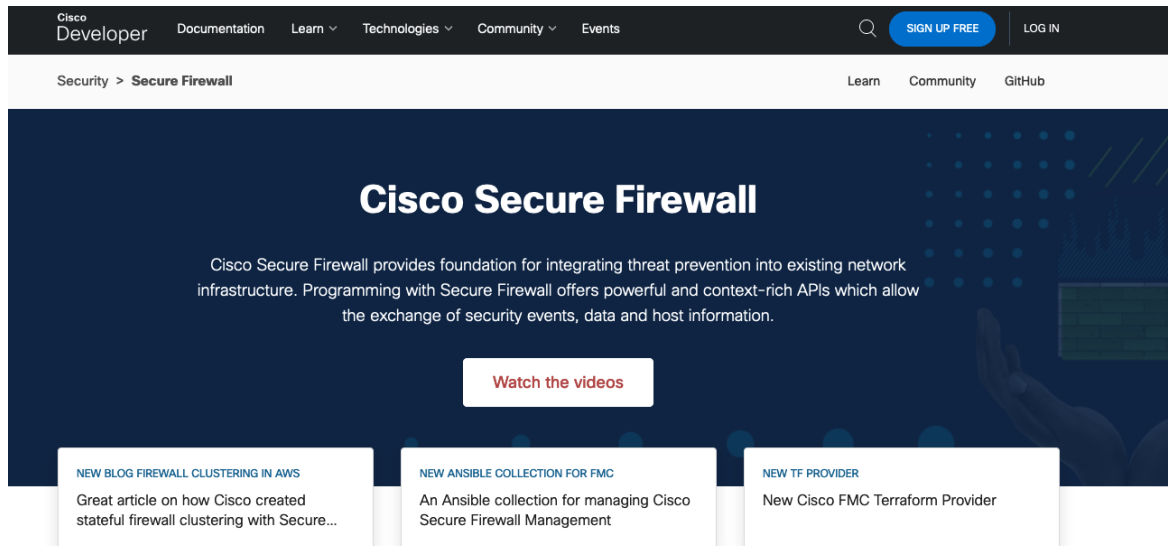


<https://www.youtube.com/c/CiscoNetSec>

Cisco Live On-Demand Library



<https://www.ciscolive.com/on-demand/on-demand-library.html>



The screenshot shows the Cisco Developer website's 'Secure Firewall' page. The header includes the 'Cisco Developer' logo, navigation links for 'Documentation', 'Learn', 'Technologies', 'Community', and 'Events', a search icon, and buttons for 'SIGN UP FREE' and 'LOG IN'. Below the header, a breadcrumb trail shows 'Security > Secure Firewall', and links for 'Learn', 'Community', and 'GitHub' are present. The main content area features a large dark blue banner with the title 'Cisco Secure Firewall' and a descriptive paragraph about its role in threat prevention. A 'Watch the videos' button is centered below the text. At the bottom, three white boxes highlight recent content: a blog on AWS firewall clustering, an Ansible collection for FMC, and a new Terraform provider for FMC.

Cisco Developer Documentation Learn Technologies Community Events SIGN UP FREE LOG IN

Security > Secure Firewall Learn Community GitHub

Cisco Secure Firewall

Cisco Secure Firewall provides foundation for integrating threat prevention into existing network infrastructure. Programming with Secure Firewall offers powerful and context-rich APIs which allow the exchange of security events, data and host information.

Watch the videos

NEW BLOG FIREWALL CLUSTERING IN AWS
Great article on how Cisco created stateful firewall clustering with Secure...

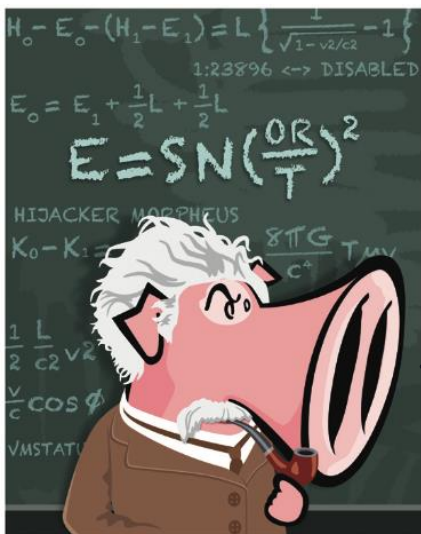
NEW ANSIBLE COLLECTION FOR FMC
An Ansible collection for managing Cisco Secure Firewall Management

NEW TF PROVIDER
New Cisco FMC Terraform Provider

<https://developer.cisco.com/secure-firewall>

Securing Networks with Cisco Firepower

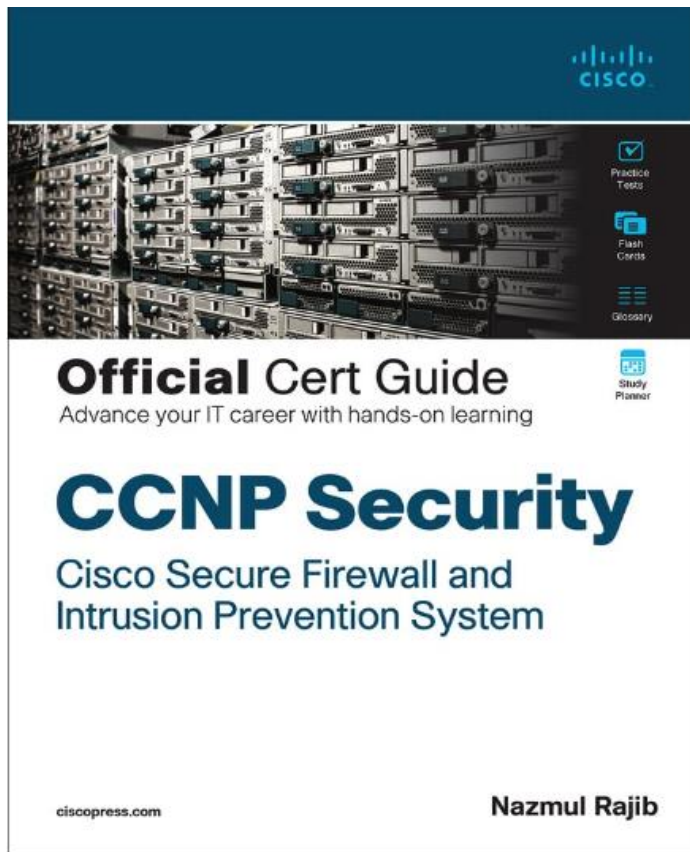
Languages: English



*Ask me about our 5-day
Secure Firewall training
offerings!*



Who Wins the CCNP Security Book?



Security

Secure Firewall

Learn how Cisco Secure Firewall keeps businesses moving while keeping it secure. They offer deep visibility using built-in advanced security features like Cisco Secure IPS and Cisco Secure Endpoint to detect and stop advanced threats fast.

START

Monday, June 5 | 9:30 a.m.

BRKSEC-1026

Strengthening the First Line of Defense using Cisco Secure Firewall and Cisco Umbrella

Monday, June 5 | 10:30 a.m.

BRKSEC-1138

Security Management from Anywhere: Cisco Defense Orchestrator & Security Analytics and Logging

Tuesday, June 6 | 1:00 p.m.

BRKSEC-3058

Route based VPNs with Cisco Secure Firewall

Tuesday, June 6 | 2:30 p.m.

BRKSEC-2093

Hardening the Secure Firewall

Tuesday, June 6 | 3:00 p.m.

BRKSEC-3320

Demystifying TLS, QUIC and Encrypted Visibility Engine on Secure Firewall

FINISH

Wednesday, June 7 | 1:00 p.m.

BRKSEC-2123

Solving the Segmentation Puzzle! Secure Workload and Secure Firewall Integration

Thursday, June 8 | 8:00 a.m.

BRKSEC-2086

Implement Direct Internet Access with Secure Firewall Threat Defense

Thursday, June 8 | 8:30 a.m.

BRKSEC-2236

Keeping Up on Network Security with Cisco Secure Firewall

Thursday, June 8 | 10:30 a.m.

BRKSEC-2828

Secure Firewall in the DC and Enterprise - Deployment Tips and New Features

Thursday, June 8 | 1:00 p.m.

BRKSEC-3023

Secure your multi-cloud infrastructure using Cisco Secure Firewall Virtual



Las Vegas, NV | June 4-8, 2023

If you are unable to attend a live session, you can watch it in the On-Demand Library after the event.

BRKCR-2002

tes. All rights reserved. Cisco Public

173

Fill out your session surveys!



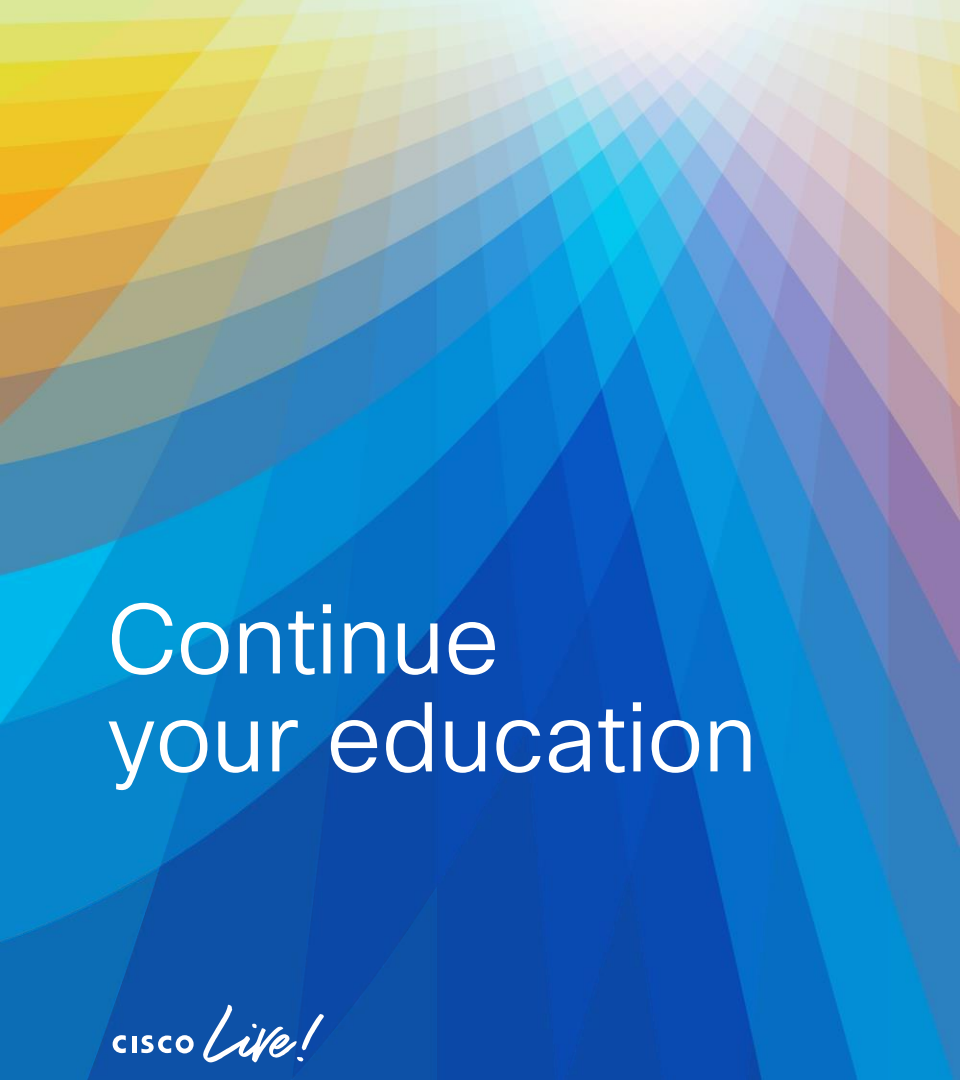
Attendees who fill out a minimum of four session surveys and the overall event survey will get **Cisco Live-branded socks** (while supplies last)!



Attendees will also earn 100 points in the **Cisco Live Game** for every survey completed.



These points help you get on the leaderboard and increase your chances of winning daily and grand prizes



Continue your education

CISCO *Live!*

- Visit the Cisco Showcase for related demos
- Book your one-on-one Meet the Engineer meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand



The bridge to possible

Thank you

CISCO *Live!*

#CiscoLive

The background is a vibrant, abstract graphic. It features a central bright white light source from which numerous colorful rays emanate, creating a sunburst or starburst effect. The rays transition through a spectrum of colors: yellow, orange, red, pink, purple, blue, and green. Overlaid on this are several large, semi-transparent, wavy shapes in shades of orange, red, and yellow, giving the impression of clouds or flowing liquid. The overall composition is dynamic and energetic.

cisco *Live!*

Let's go

#CiscoLive