
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 Webex App

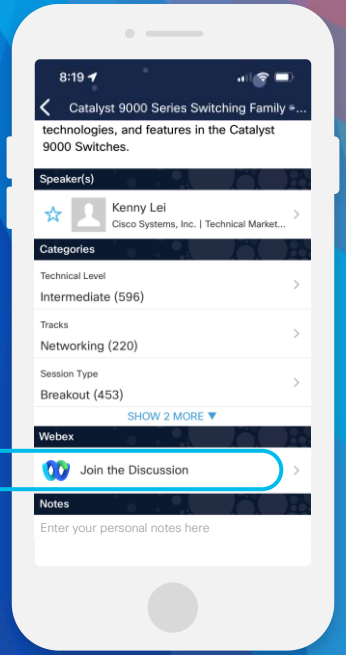
Questions?

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

How

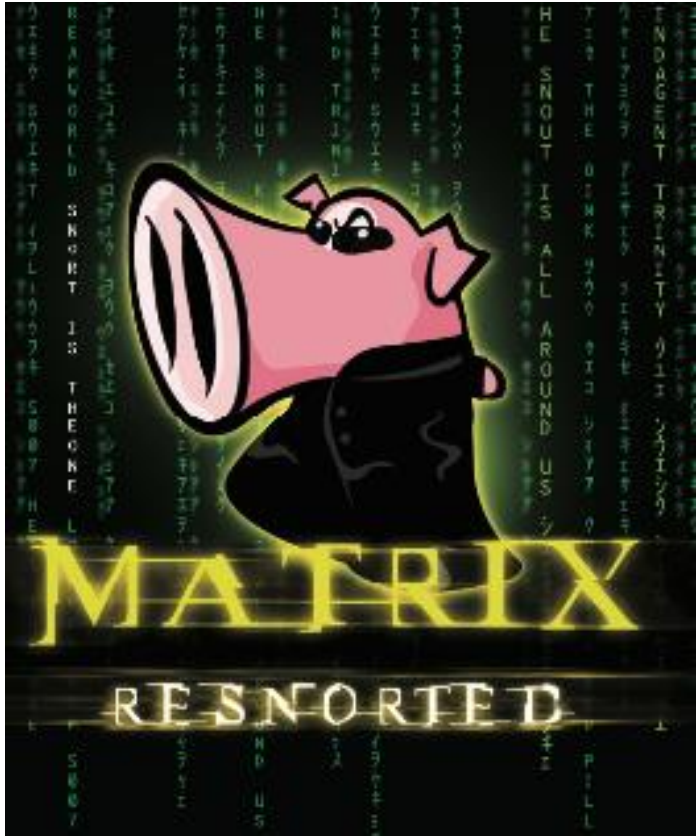
1. Find this session in the Cisco Live Mobile App
2. Click “Join the Discussion”
3. Install the Webex App or go directly to the Webex space
4. Enter messages/questions in the Webex space

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



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

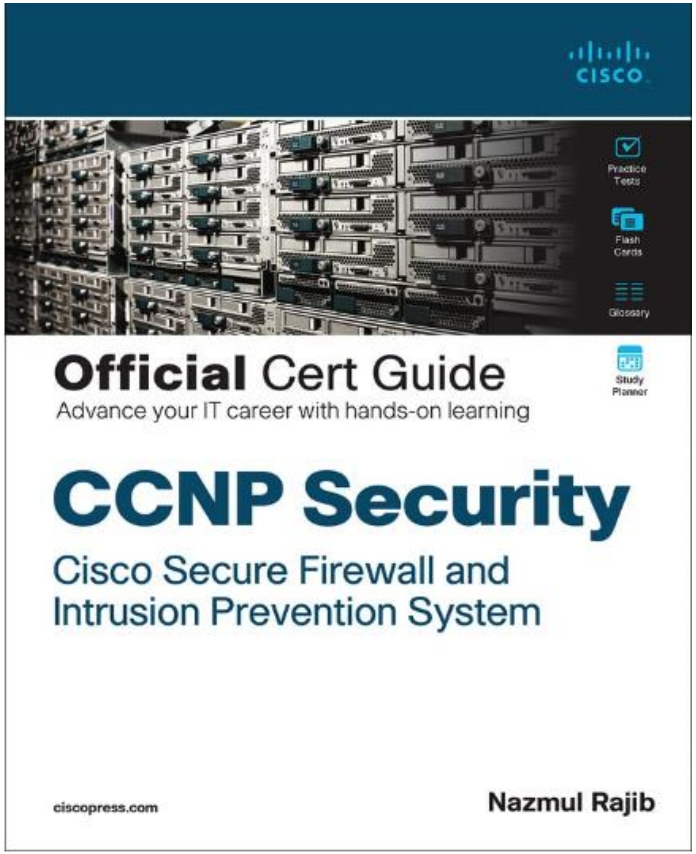
Supplemental Slides In This Presentation!



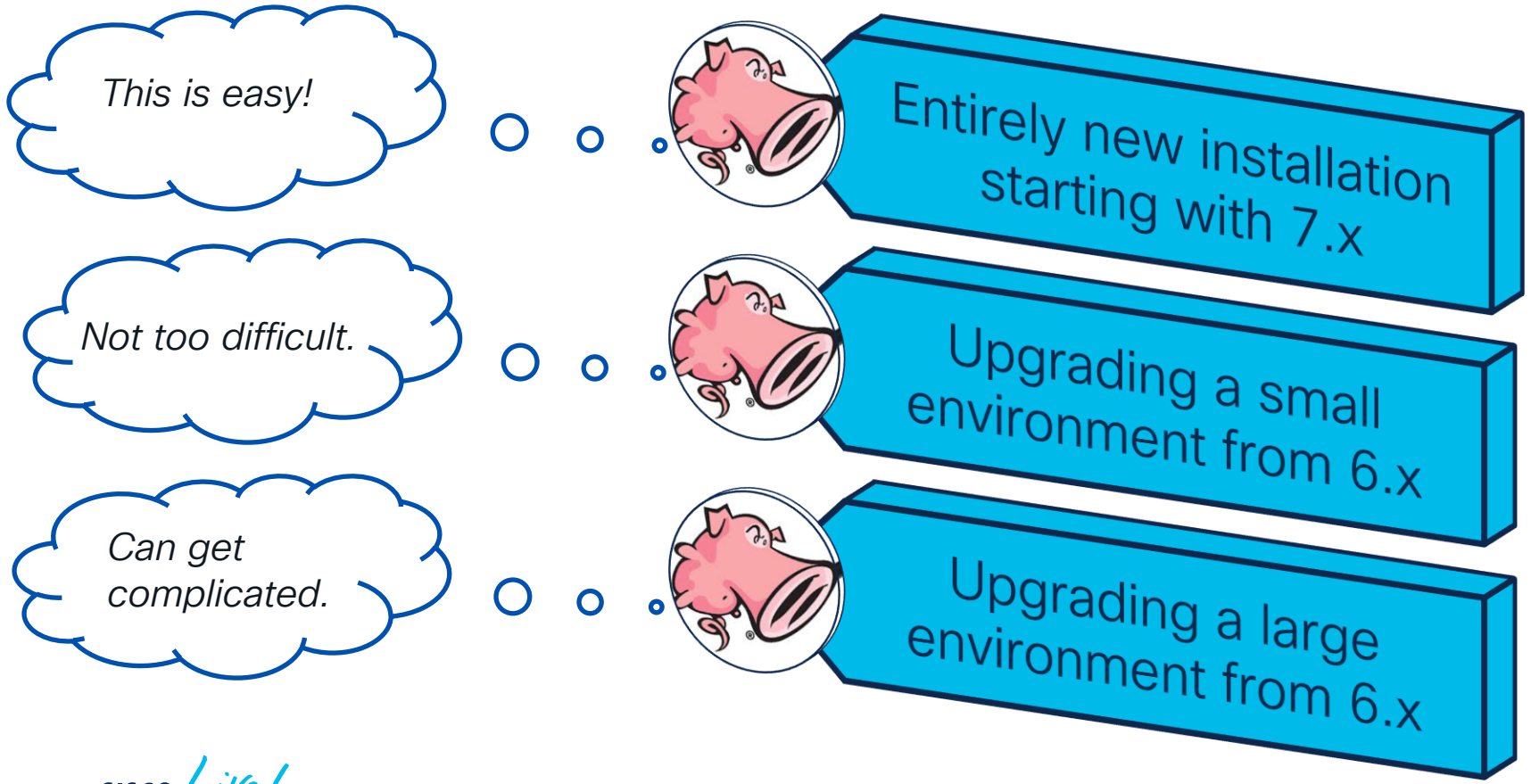
Look for this Snorty Logo!

Lots of additional information available within this presentation document!

Win the newly updated Secure Firewall Guide!



Snort 3 Administrative Expectations



Things To Learn For Mastering Snort 3

Covered in this presentation!

Intrusion Policy Changes

- Firewall Recommendations
- Overrides Vs. Layers
- Sync Tool
- Custom and Pass Rules
- Security Levels
- Rule Actions Vs. States

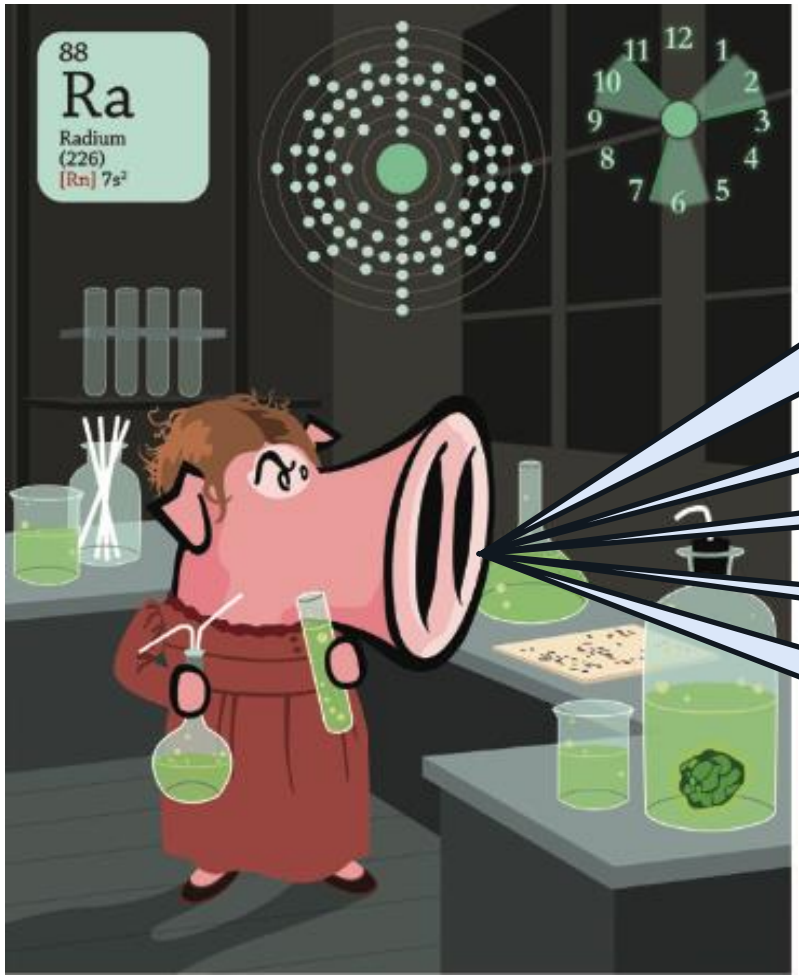
New Snort Features and Tools

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

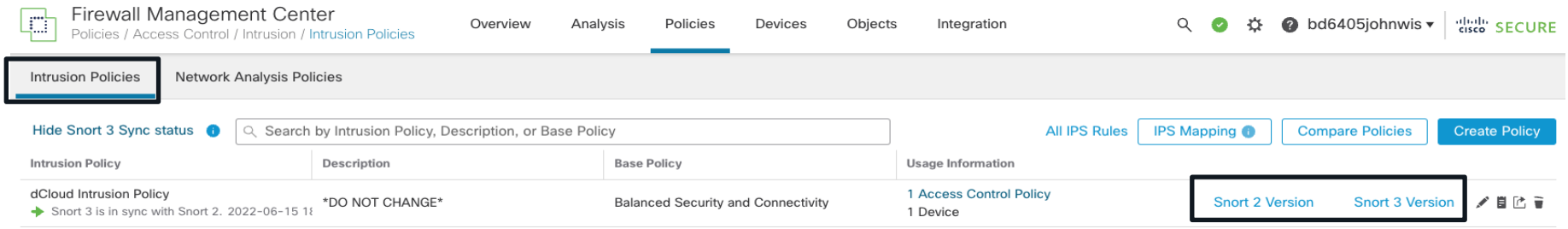
(Primary IPS Policy)

Network Analysis Policy (NAP)

(Optional IPS configuration)

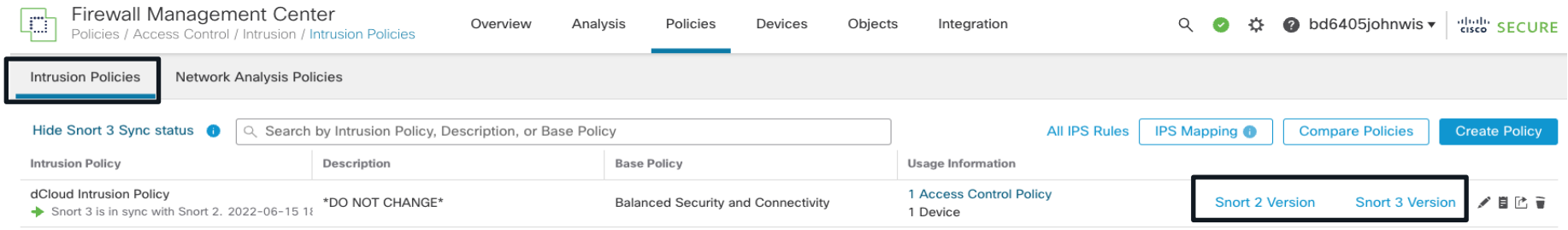
Intrusion Policy

(Intrusion) IPS Policy



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

(Intrusion) IPS Policy

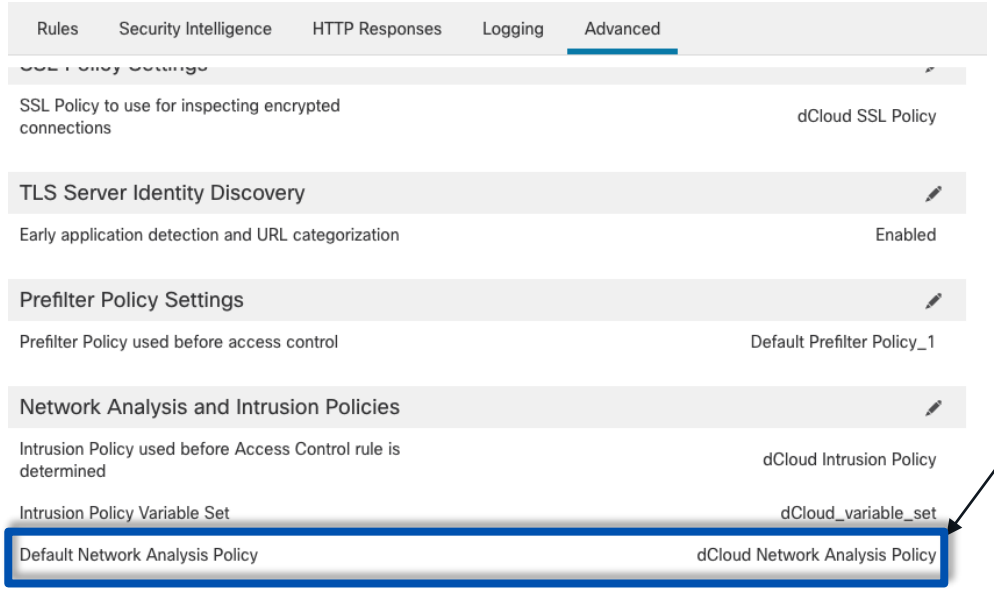


You manage the IPS Policy for Snort 3 differently than Snort 2!

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

Network Analysis Policy (NAP)

Network Analysis Policy (NAP)



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!!

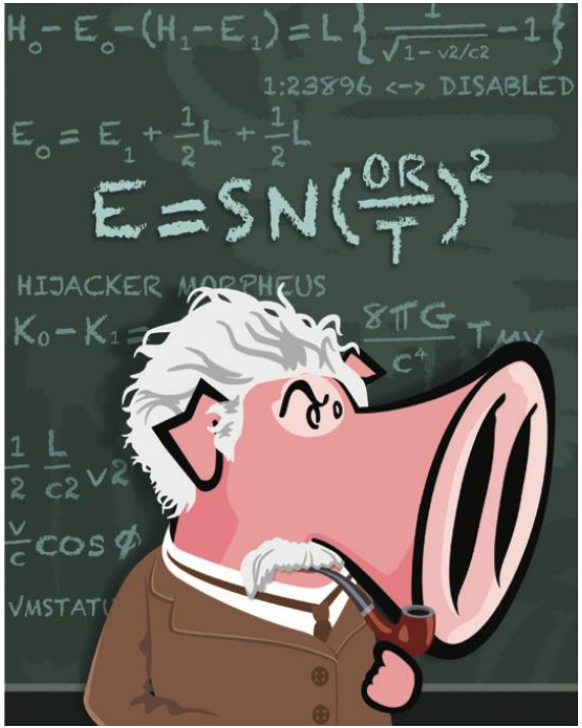
Intrusion Policy Vs. Network Analysis Policy

Intrusion Policy is how you manage *driving* the car.

Network Analysis Policy manages everything *under the hood*.

Network Analysis Policy in Snort 3

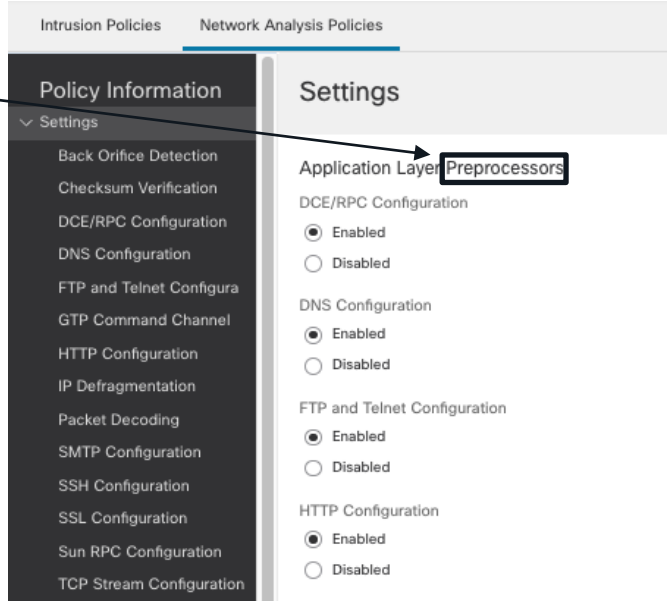
NAP has changed *significantly* in Snort 3!

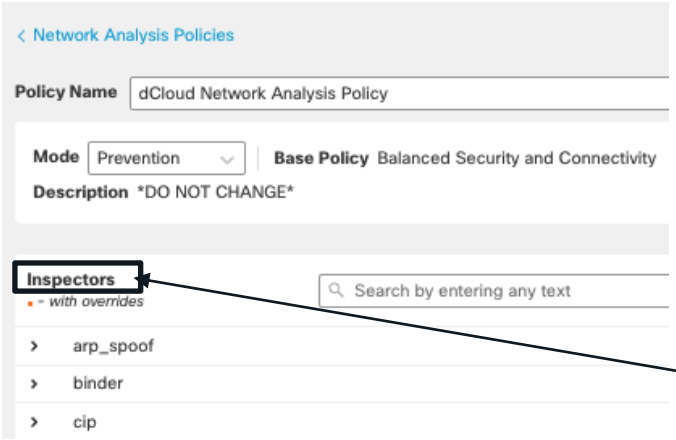


If you have made any changes to preprocessor settings in your Network Analysis Policy in Snort 2, these settings **will not** automatically convert over.

NAP in Snort 2 Vs. Snort 3

Snort 2 NAP manages Snort *Preprocessors.*





In Snort 3 these are called *Inspectors.*

“Great! Overall, just two polices 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:

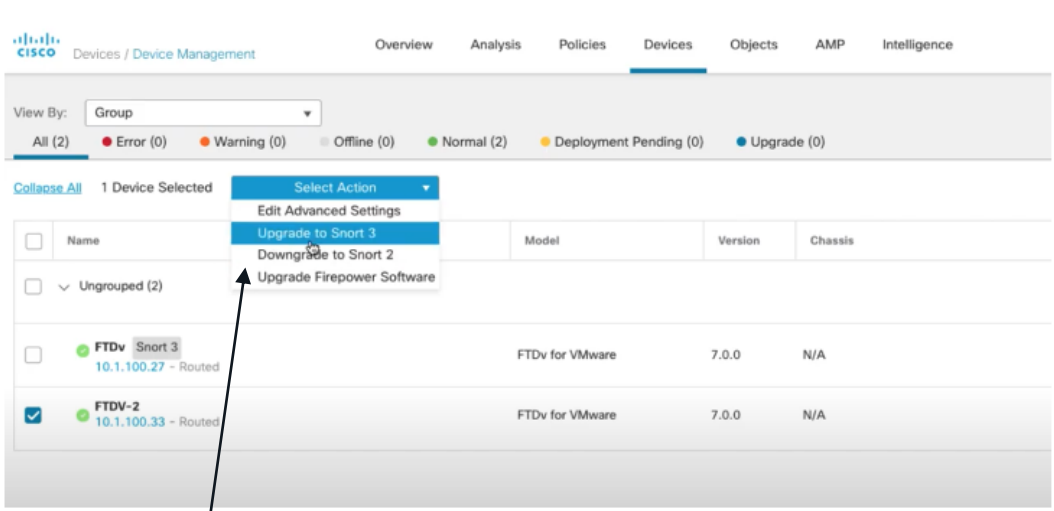
Firewall runs Snort 2 but can easily be **converted** to Snort 3.

New installs of 7.x:

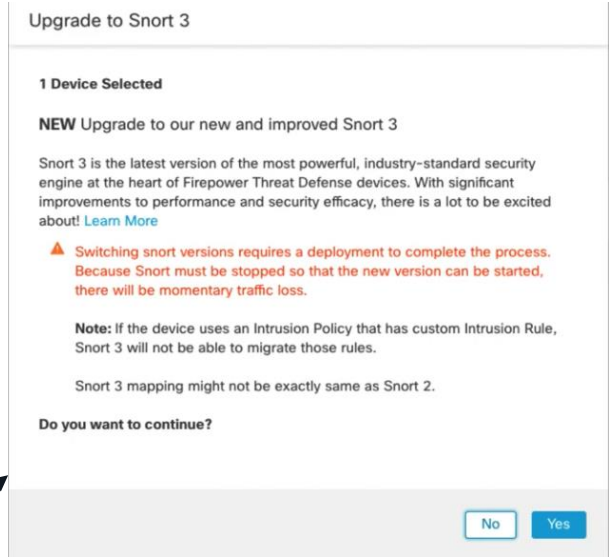
Firewall runs Snort 3 by default.

OR

How to Upgrade from Snort 2 to Snort 3

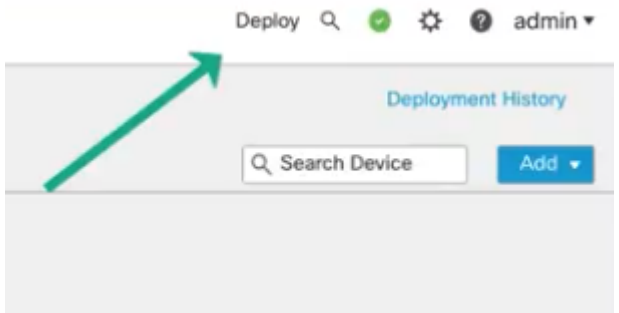


1 Select the device you wish to upgrade and select 'Upgrade to Snort 3'.

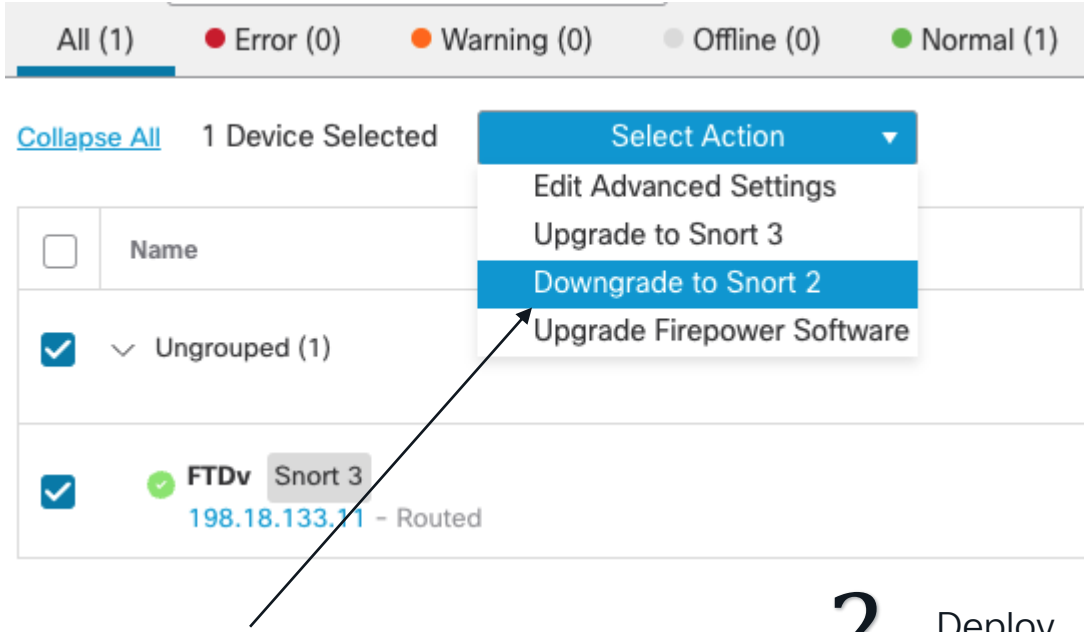


2 Read the disclaimer!

3 Deploy.



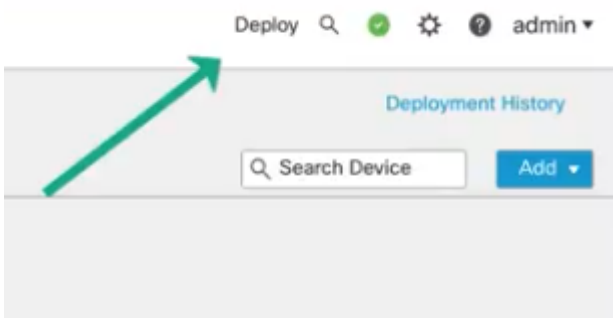
Reverting to Snort 2 from Snort 3



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

Perform *only* during a maintenance window.

2 Deploy.



“That upgrade process was easy!”

You the customer

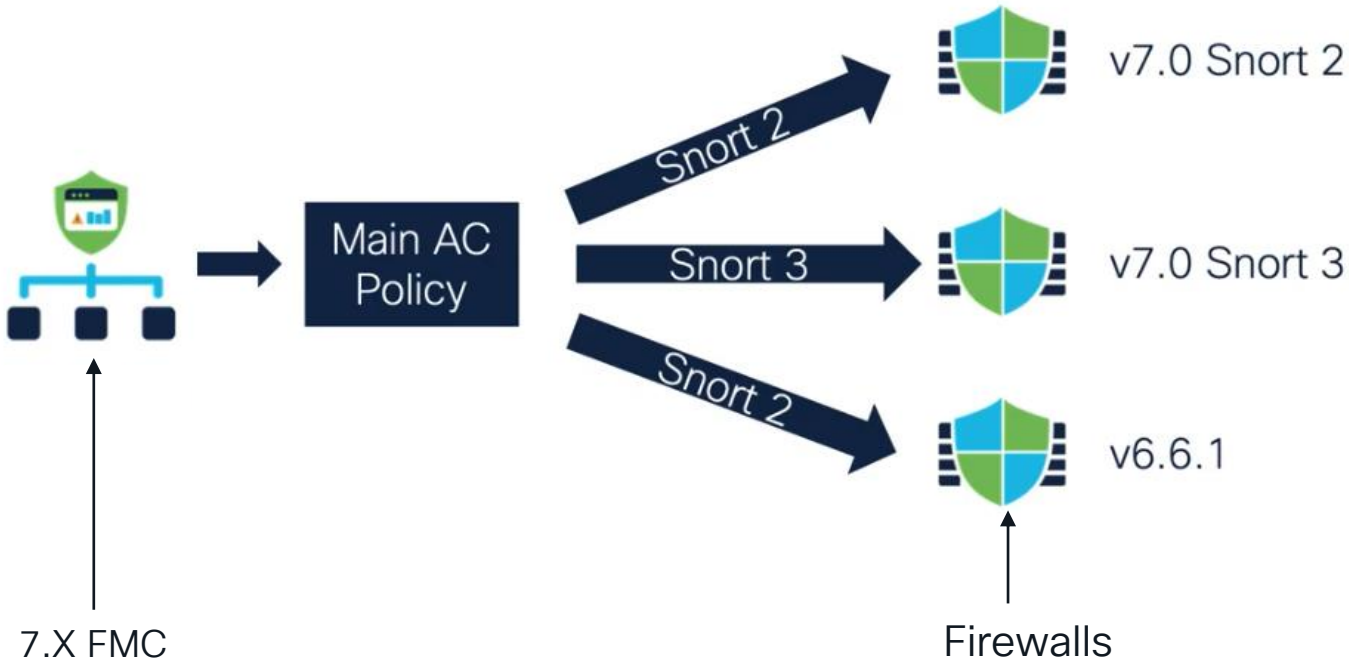
Company XYZ

“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



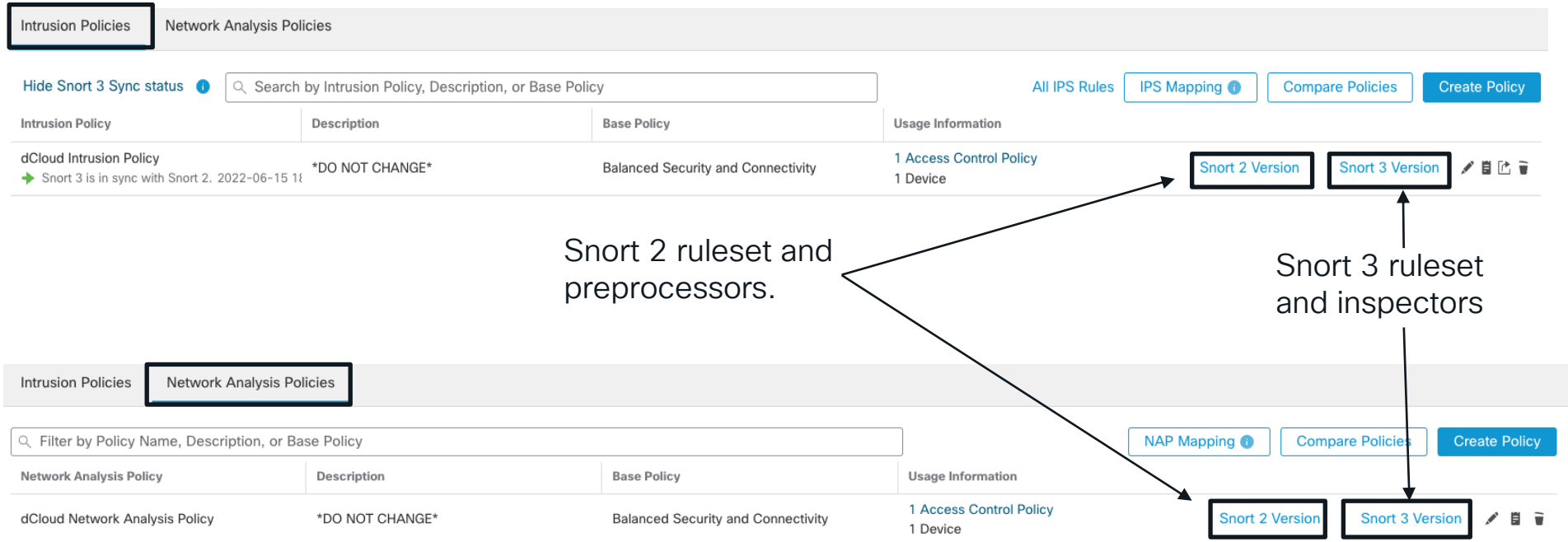
The FMC Manages all Versions

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

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

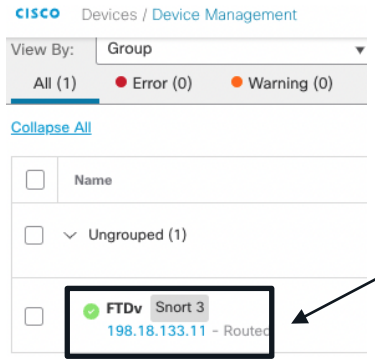
Management Center (FMC) 7.0 and Later

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



Ruleset Tied to Snort Version in Each Firewall

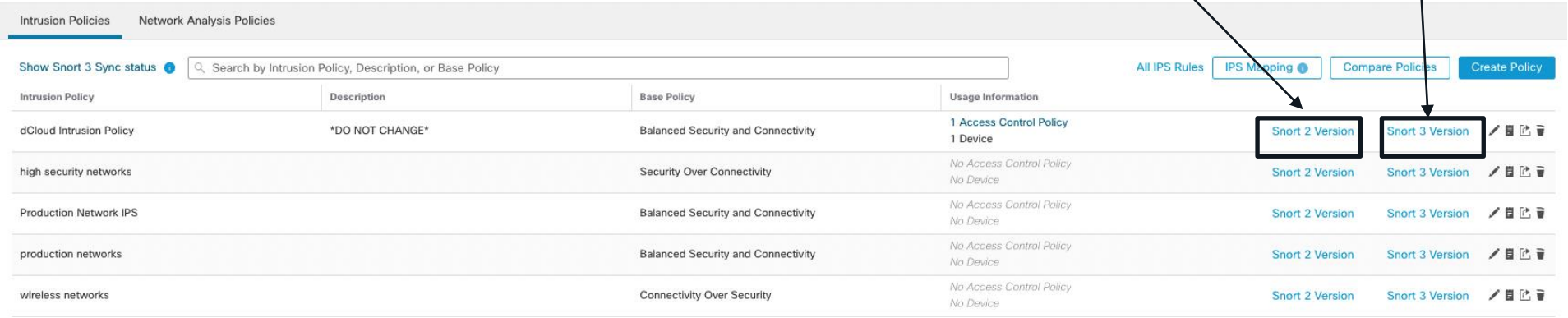
All IPS policies have a Snort 2 ruleset and a Snort 3 ruleset starting in 7.x.



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.



“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

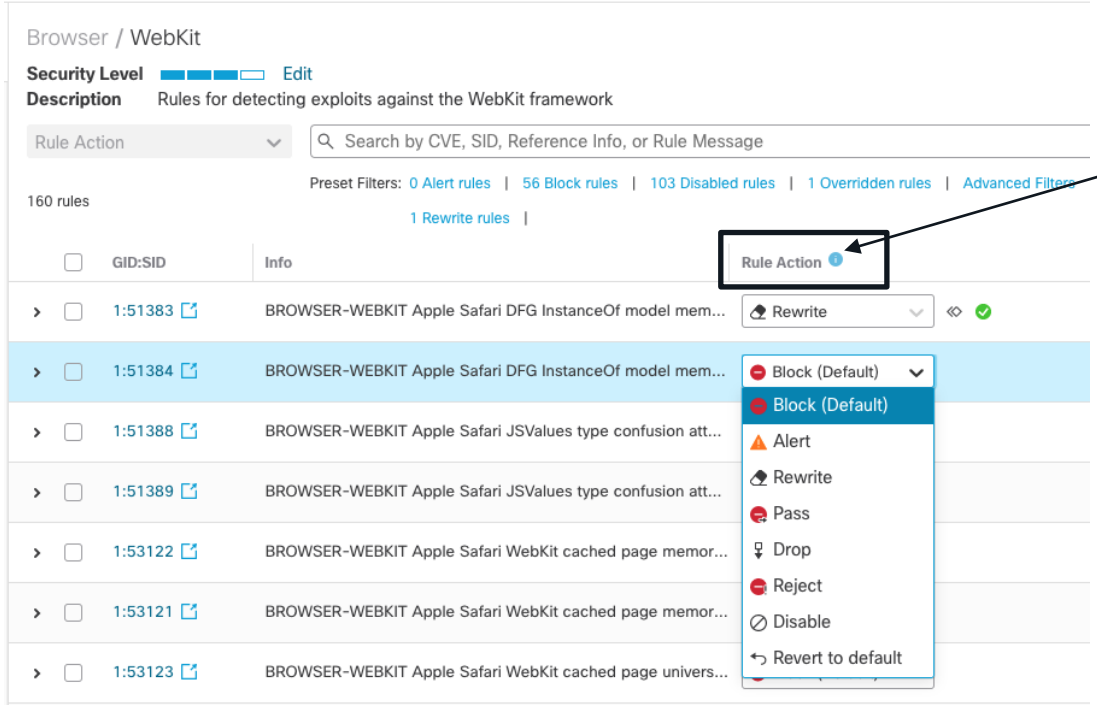
7.X FMC Available Rules

Snort Rule Version	Rules available to use	FMC Rule actions available	Source	Base Polices
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!

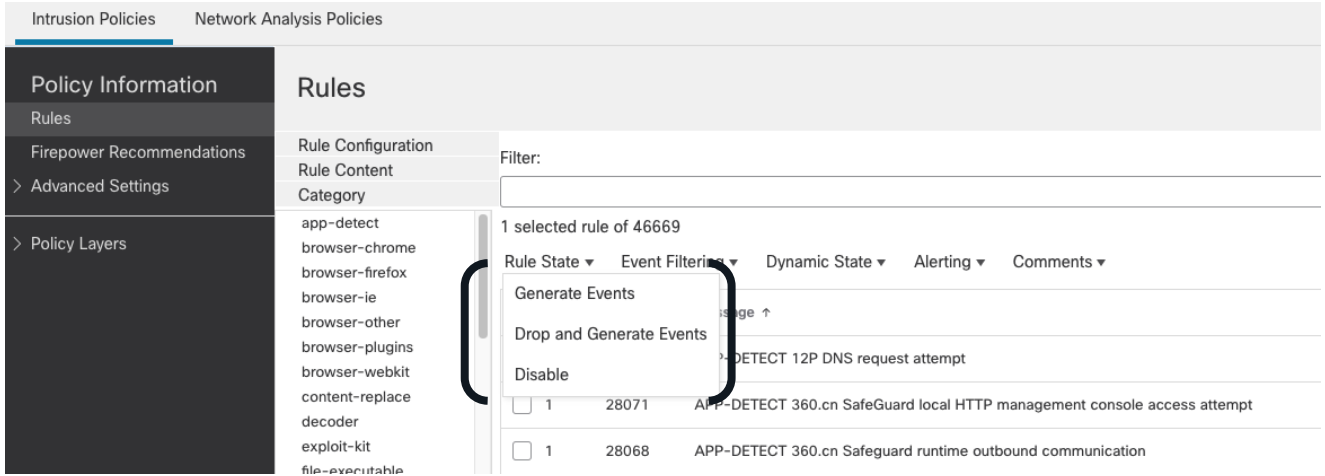
Snort Rule Action Options



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’



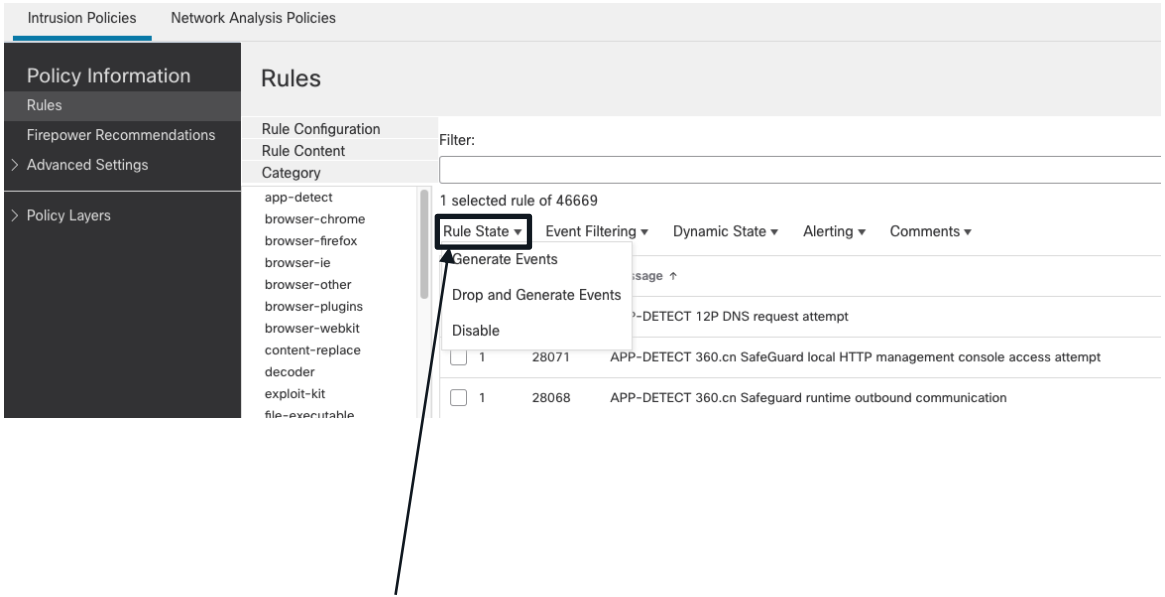
Disable – Rule is not enabled.

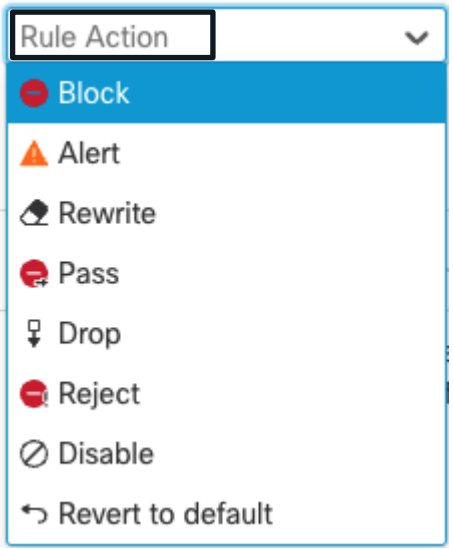
Drop and Generate Events – Generate an event and drop the packet and all subsequent packets in this connection.

Generate Events – Generate an event only.

Snort 3 Rule Action Options

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



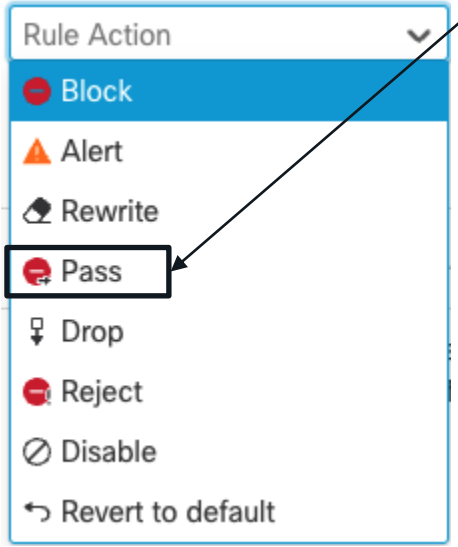


Snort 2 action is configured by changing the rule ***state***.

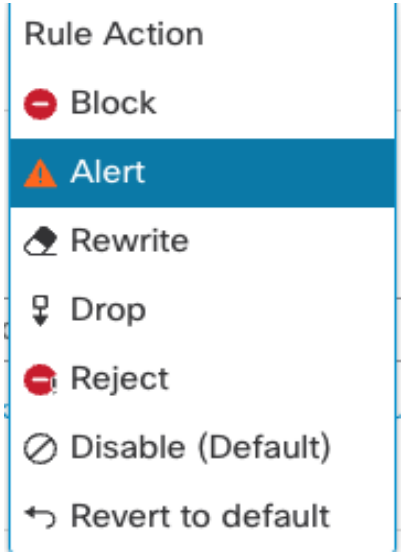
Snort 3 Rule Actions 7.x

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

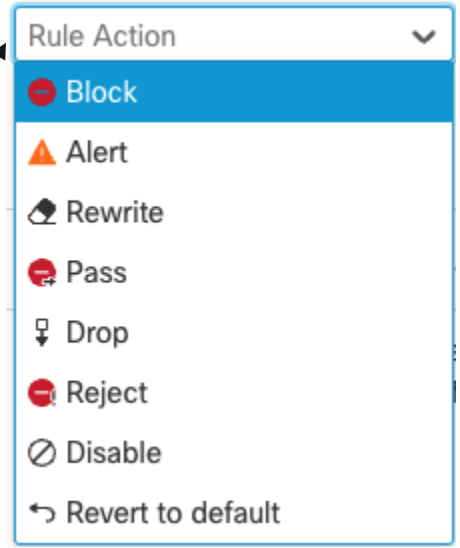
Do not accidently use the ‘Drop’ action!

Open-Source Snort Action Vs FTD Snort Action

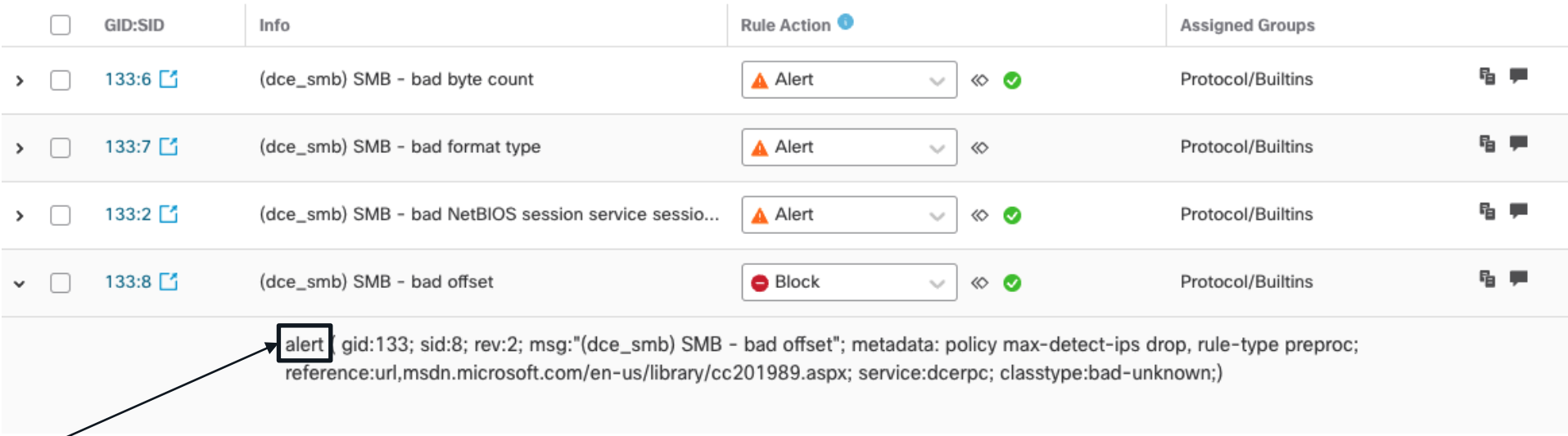
Open-Source Snort rules specify the action *in the rule*.

```
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



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

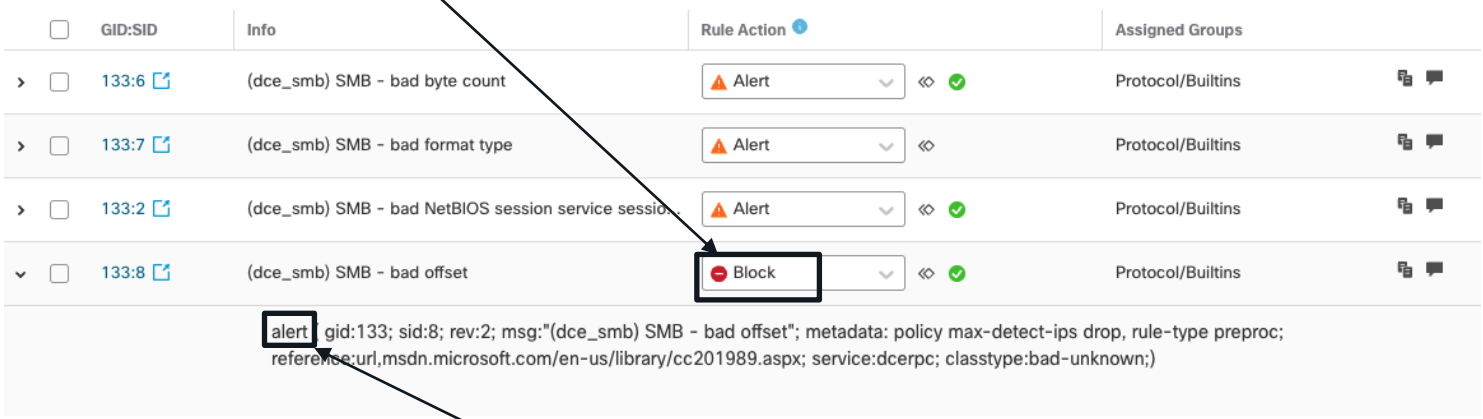
alert (gid:133; sid:8; rev:2; msg:"(dce_smb) SMB - bad offset"; metadata: policy max-detect-ips drop, rule-type preproc; reference:url,msdn.microsoft.com/en-us/library/cc201989.aspx; service:dcerpc; classtype:bad-unknown;)

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.



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!

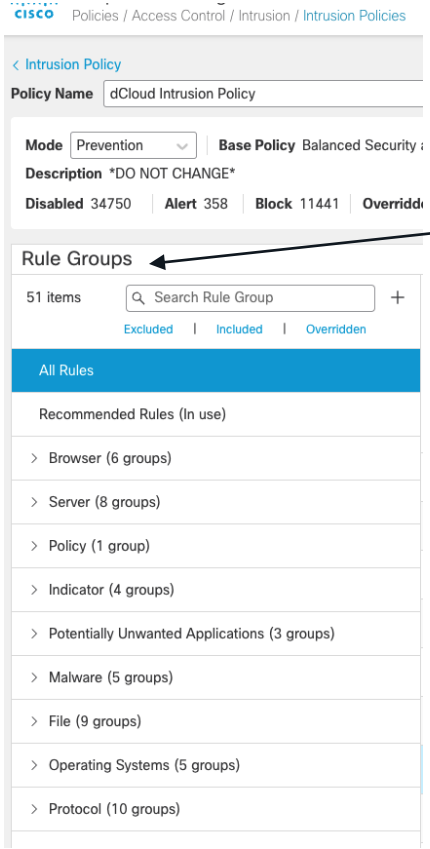
700 rules enabled

10,000 rules enabled

21,000 rules enabled

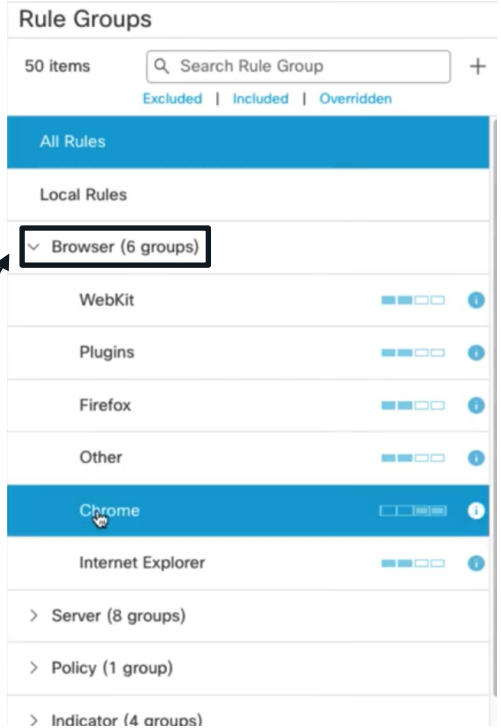
Connectivity over Security	Balanced Security and Connectivity	Security over Connectivity

Snort 3 Rules are Organized by Groups



Each Intrusion Policy has approx. 55 groups.

Rule groups have a high-level category.

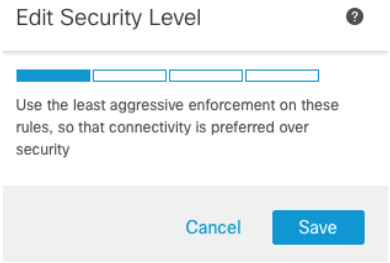


TIP

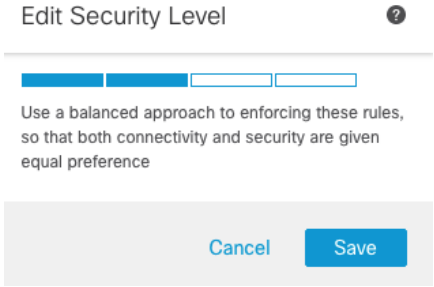
Remember Snort 2 and Snort 3 have mostly the *same rules*, so category and group are just different ways to organize and manage these rules.

Snort Rule Group Security Level

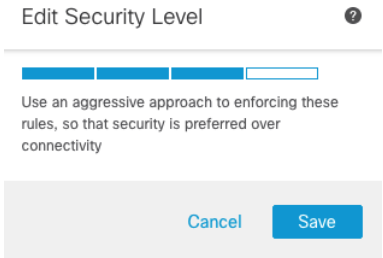
Connectivity over Security



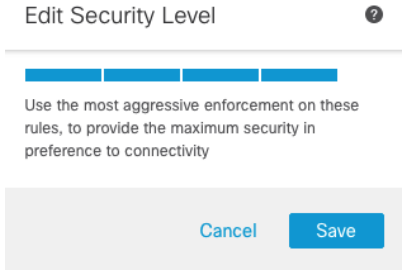
Balanced Security and Connectivity



Security over Connectivity



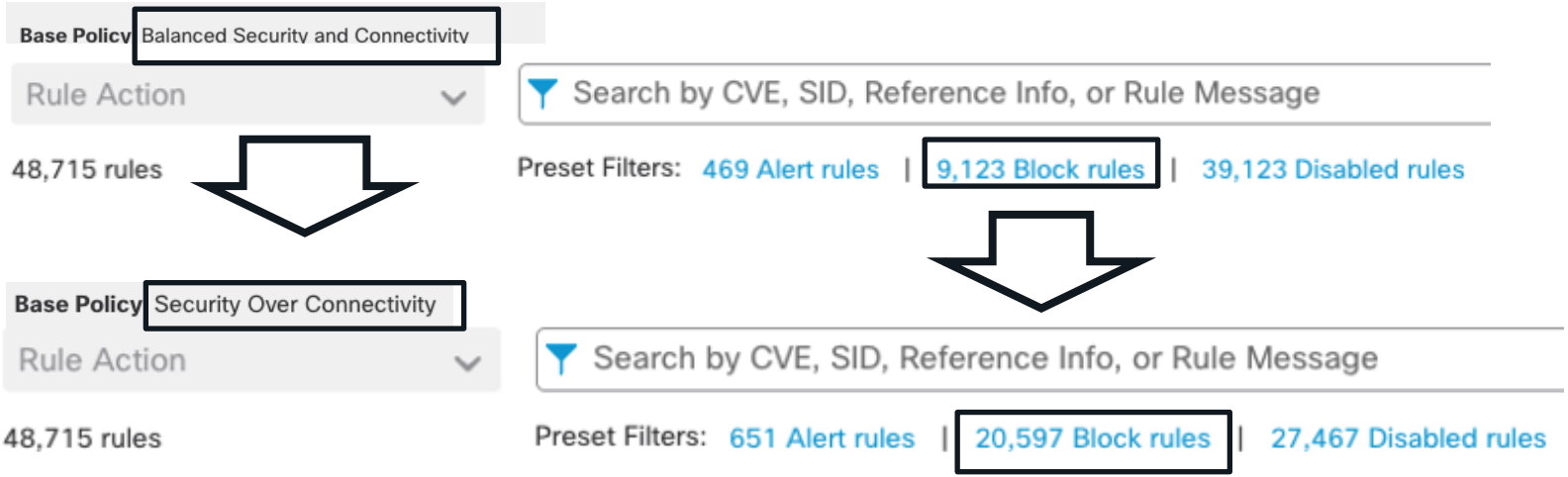
Maximum Detection



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

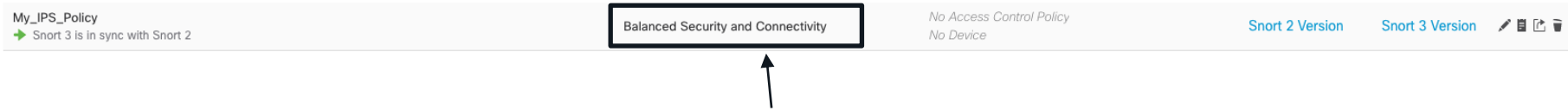
Increasing Security in a Snort 2 IPS Policy

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



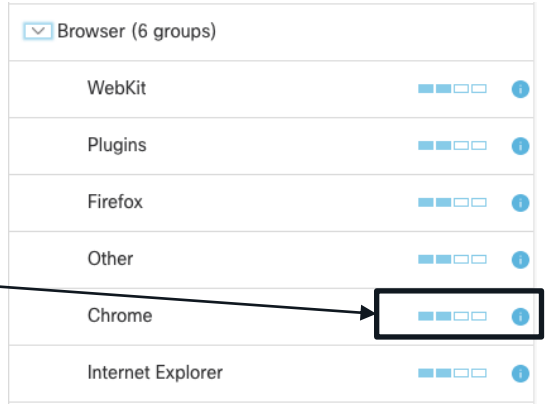
This change enables over 10,000 additional rules! This is a significant increase.

Snort 3 Rule Security Levels

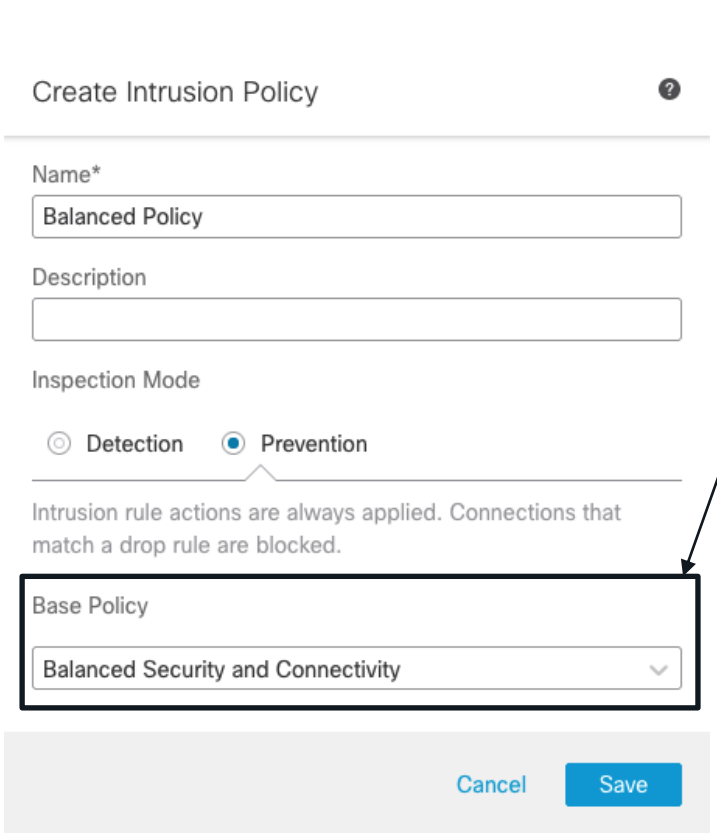


The *Base policy* for all IPS policies sets the *security level* for *all the rules* within the same IPS policy.

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



Utilizing Security Levels



1'st

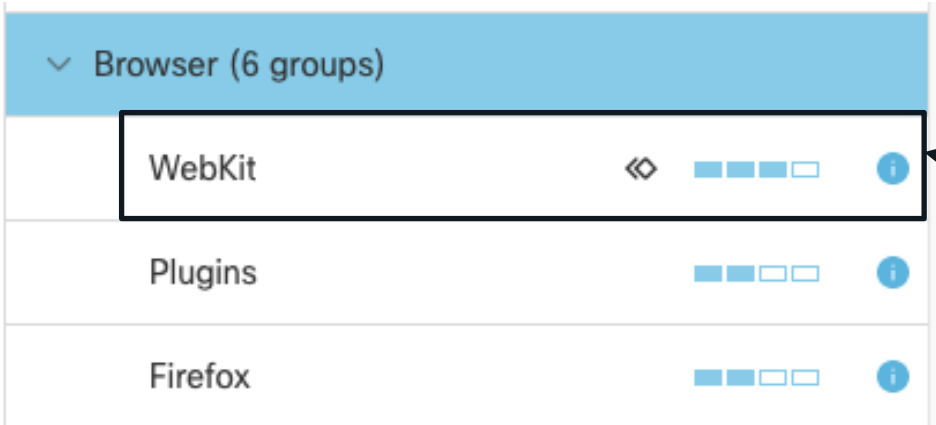
Create intrusion policy and specify base policy.

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

Utilizing Security Levels

2’nd

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

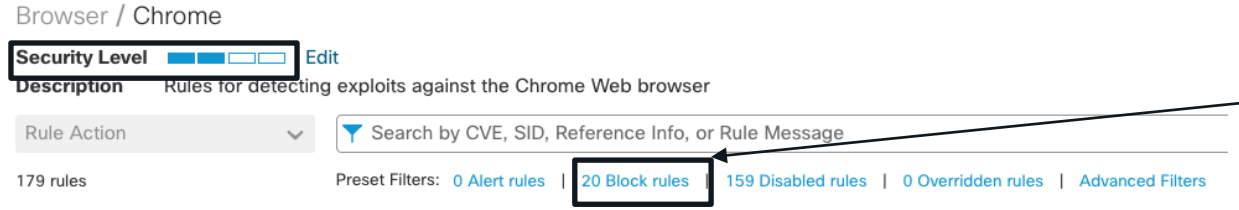


WebKit has been increased to ‘Security Over Connectivity’.

Another Example!

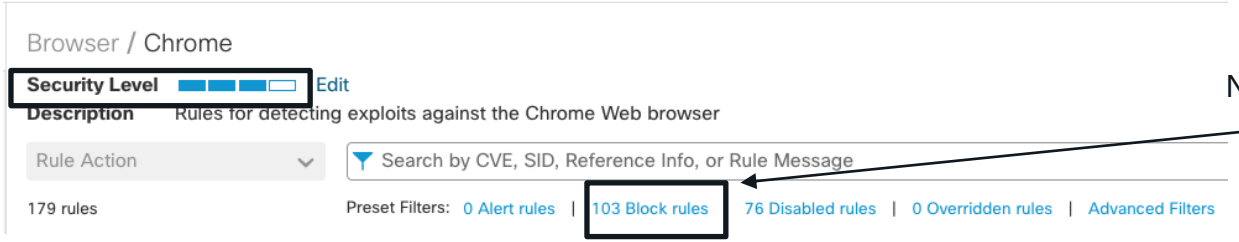
Balanced as the Base Policy.

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



20 rules set to block

Browser/Chrome changed to **Security Level**



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

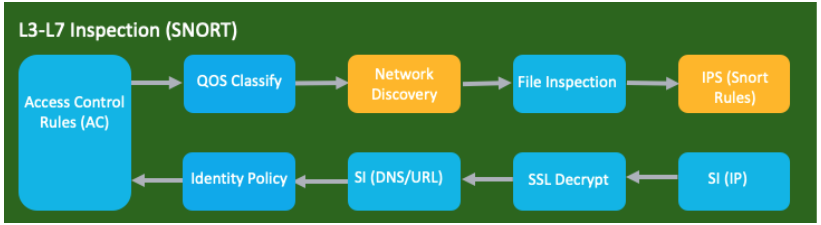
Company XYZ

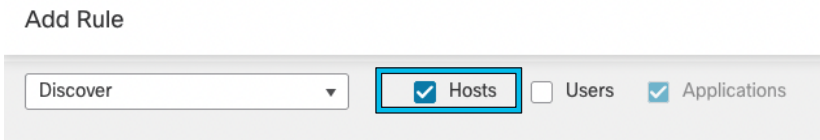
Secure Firewall Recommendations

Secure Firewall Recommendations

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

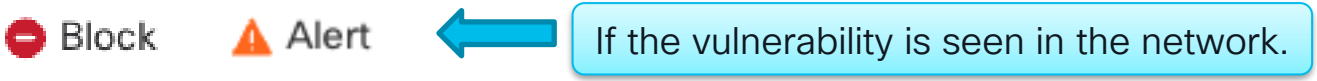
L3-L7 Inspection (SNORT)

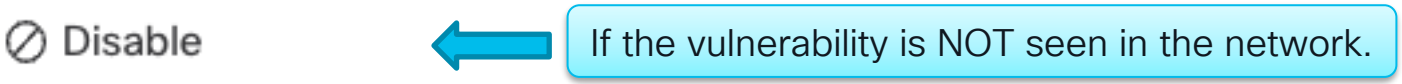




Secure Firewall Recommendations

Recommendations will recommend to change the rule action to:





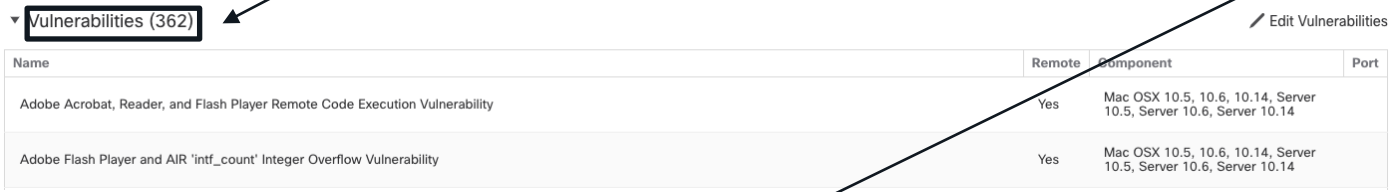
Secure Firewall Recommendation Example

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

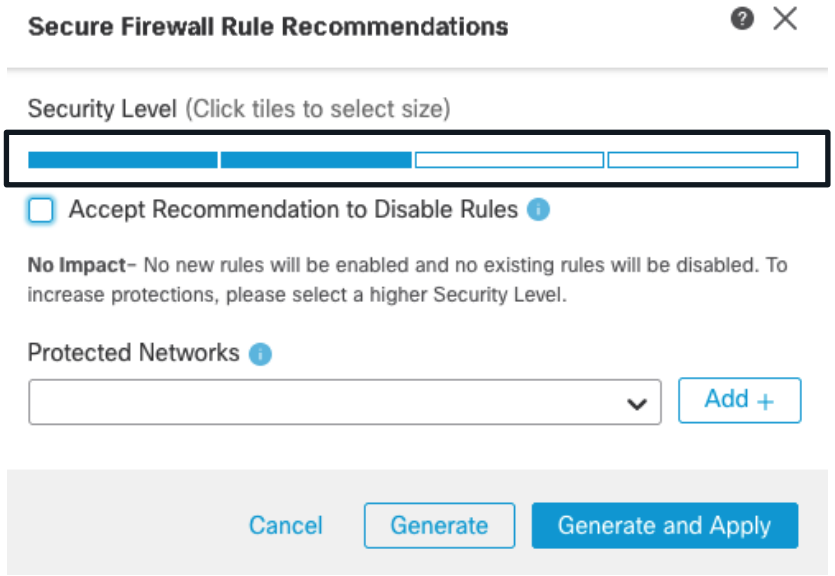


rule alert tcp $EXTERNAL_NET any -> $SMTP_SERVERS 25 (msg:"BROWSER-FIREFOX Mozilla Firefox 17 onreadystatechange memory corruption attempt"; flow:to_server,established; file_data:; content:"document.onreadystatechange"; content:"window.parent.frames[0].frameElement.ownerDocument.write("; fast_pattern:only; 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.

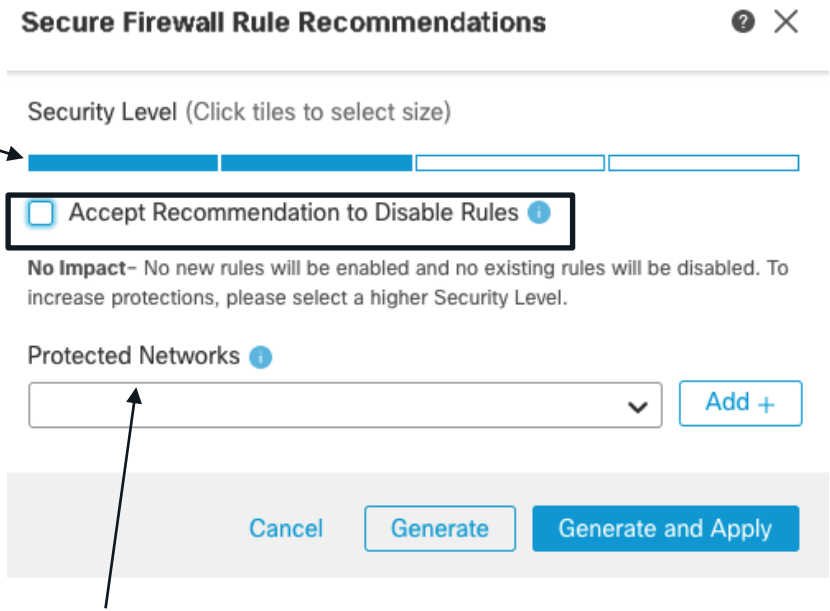
Security Level will default to the security level of your base policy.



Enabling Rule Recommendation Settings

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

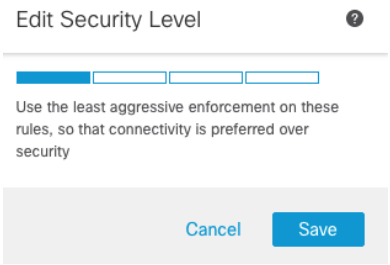
Select here to allow the tool to disable already enabled rules. Use with caution!



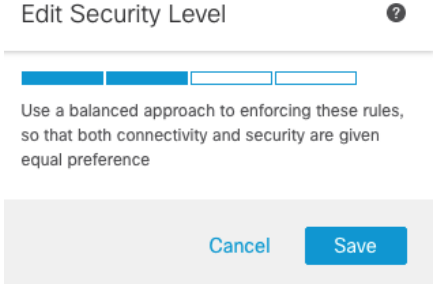
Specify the networks in the "*Network map*" you wish to use the discovered data from to make the rule recommendations.

Rule Recommendations Security Level

Connectivity over Security

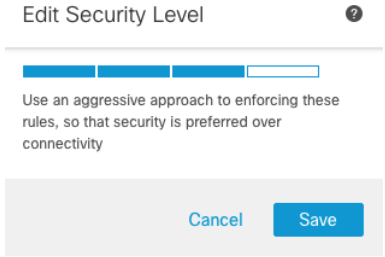


Balanced Security and Connectivity

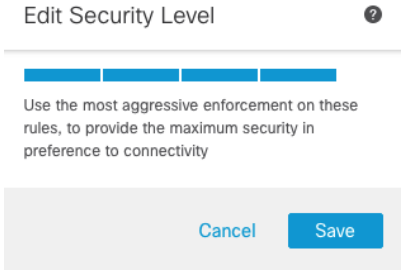


Security level for recommendations *is the same* as the security level for rule groups.

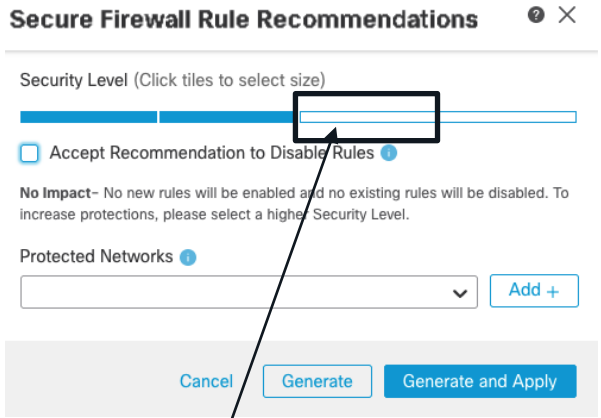
Security over Connectivity



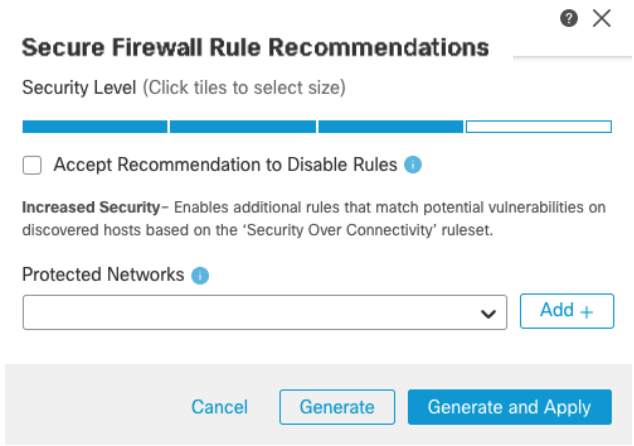
Maximum Detection



Increased Security Rule Recommendations



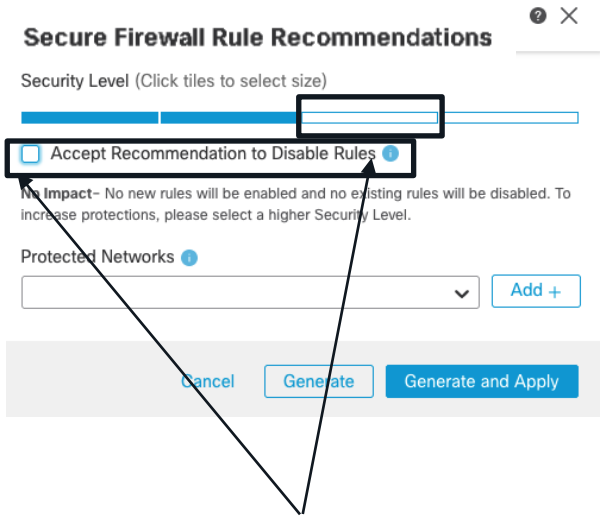
Move the security level higher

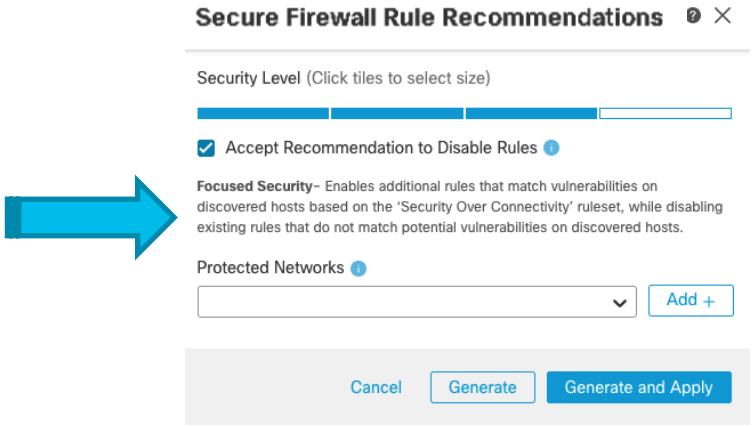


Increased Security

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

Focused Security Rule Recommendations



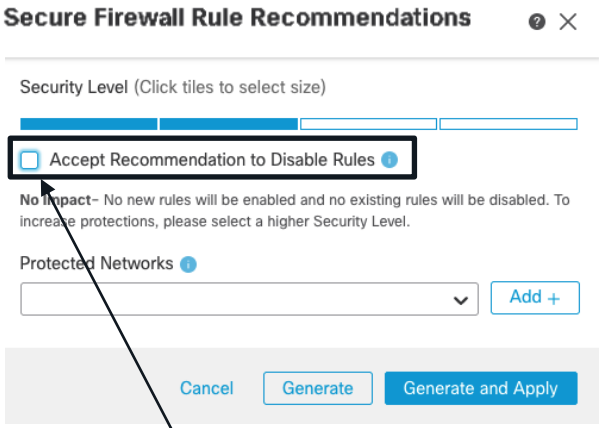


Focused Security

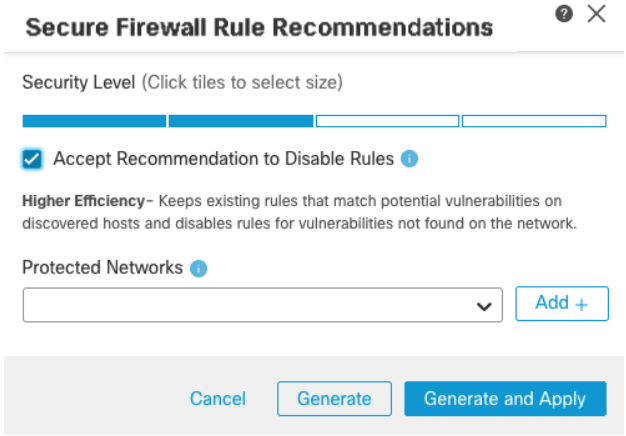
Enable the "*Disable Rules*" option *and* move the security level one higher.

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



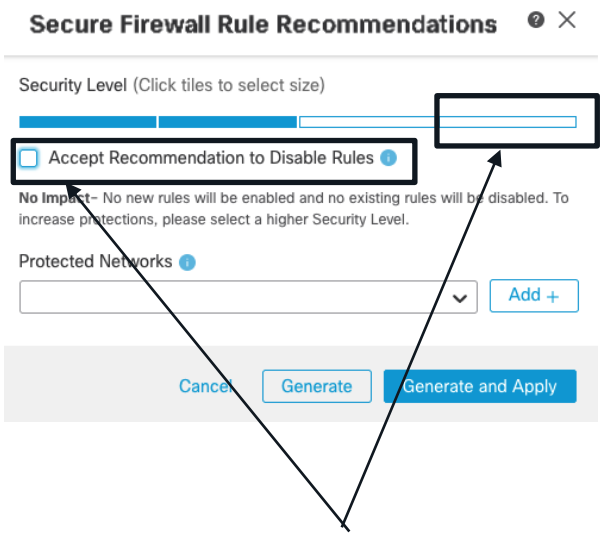
Enable the "*Disable Rules*" option.

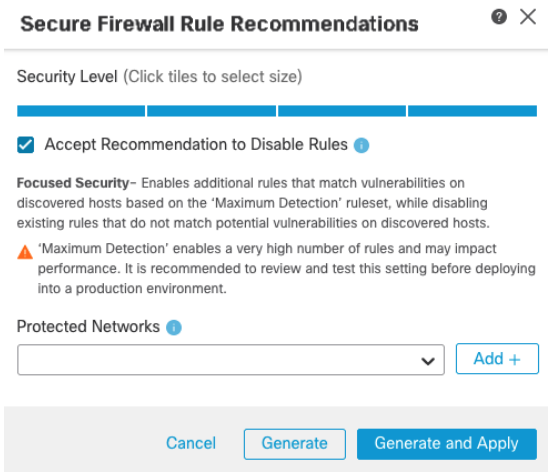


The result: Keep existing rules enabled that match vulnerabilities seen on the hosts but disable others that do not.

Maximum Detection Security Level

Not Typically Recommended!

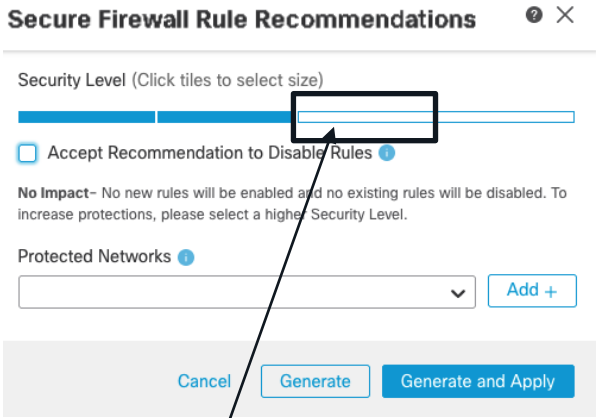




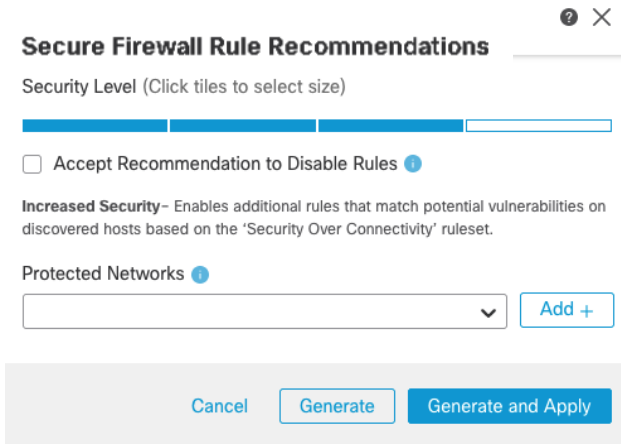
Enable the "*Disable Rules*" option *and* move the security level to *the* highest setting*: "Maximum Detection"* .

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

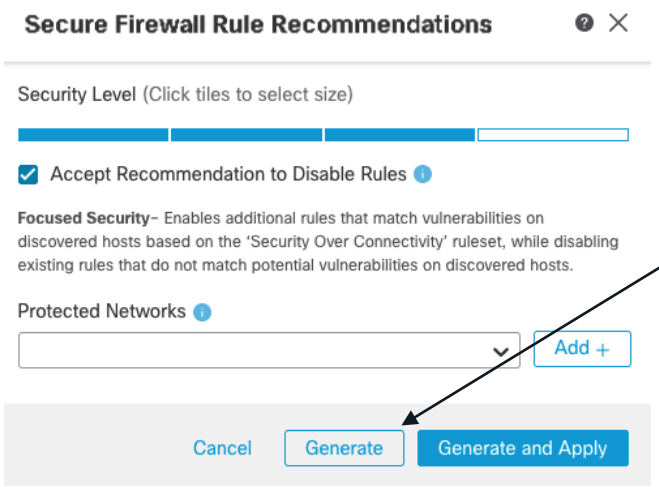


Move the security level higher



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

Generate and Apply



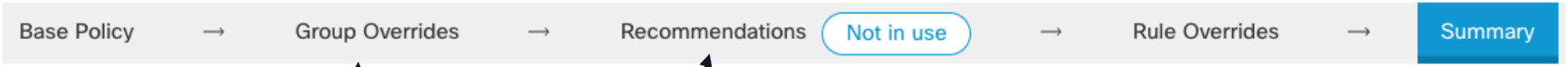
Generate will only generate the recommendations but will not make the changes.

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

TIP

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

Overrides – IPS Policy Flow



Rules actions configured specified by *Base Policy*.

Overrides per **rule group** when performed by changing the 'Security level'.

Firewall Recommendations if enabled.

All individual rule overrides performed manually 'per rule'.

What is displayed under summary is *what the firewall will use factoring in all overrides*.

“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

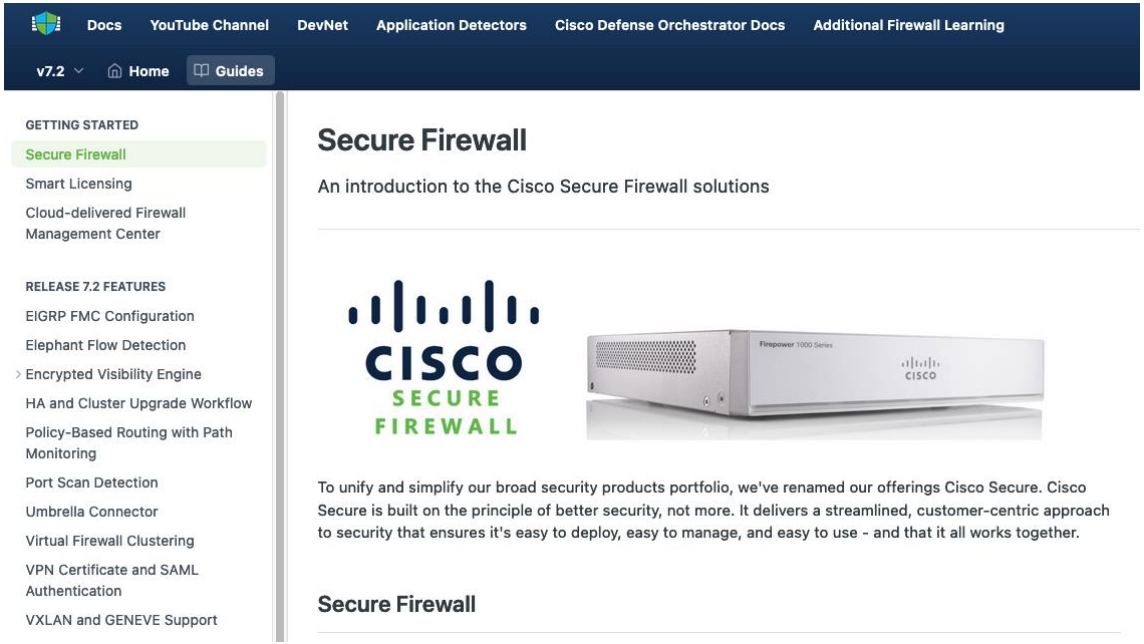
What's next for us to learn?

- 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



New! Starting point for all things Cisco Secure Firewall!

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

Management Center Administration Guide

Cisco Secure Firewall Management Center Administration Guide, 7.3

Management Center-specific guide.

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

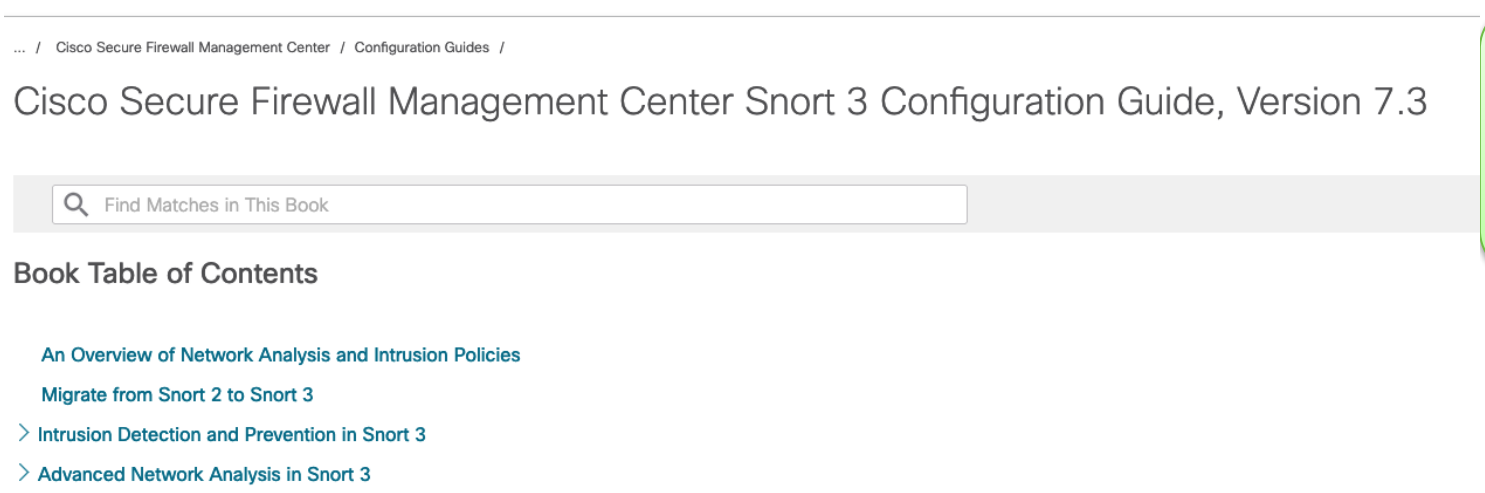
Primary guide for the Cisco Secure Firewall.

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



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

NetSec Community

Cisco Secure Firewall

@CiscoNetSec 5.06K subscribers 221 videos

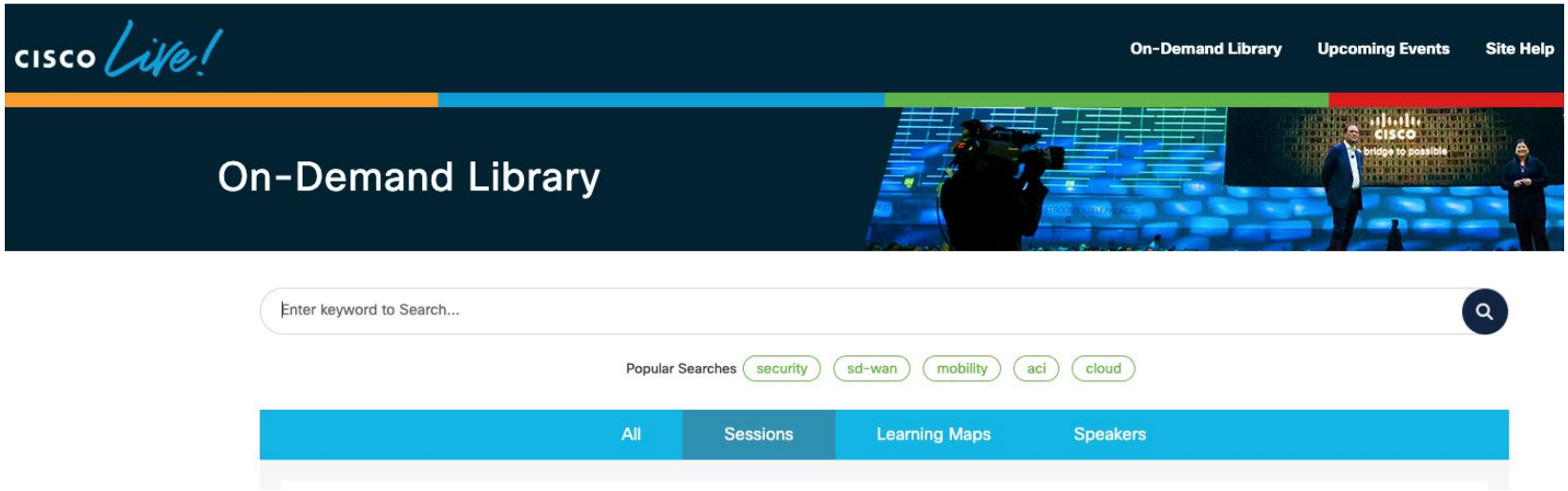
Welcome to Cisco Secure Firewall Channel.

Subscribe

HOME VIDEOS LIVE PLAYLISTS COMMUNITY CHANNELS ABOUT

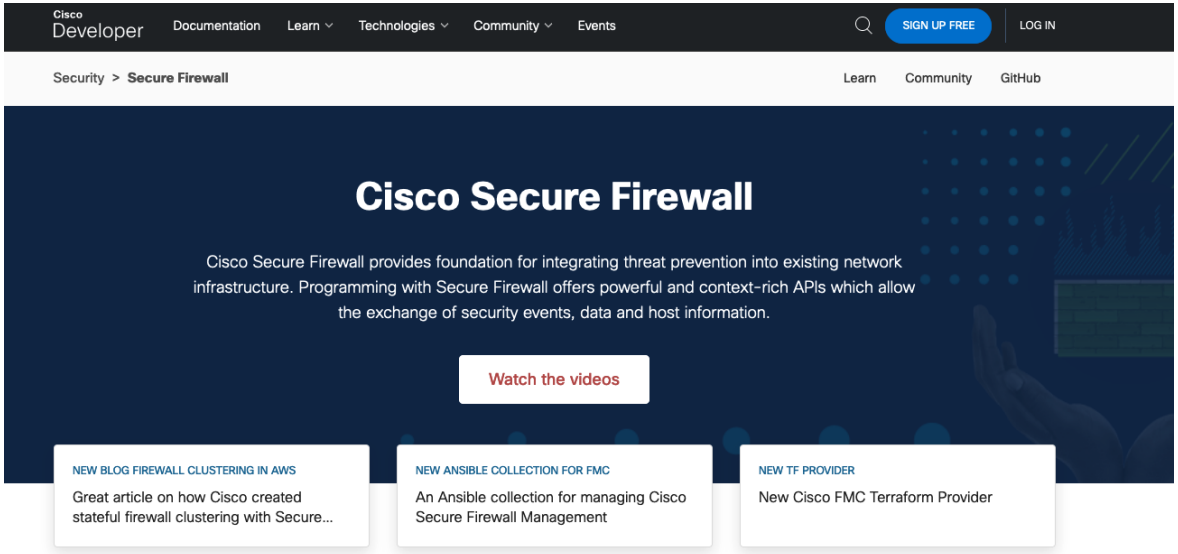
https://www.youtube.com/c/CiscoNetSec

Cisco Live On-Demand Library



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

DevNet

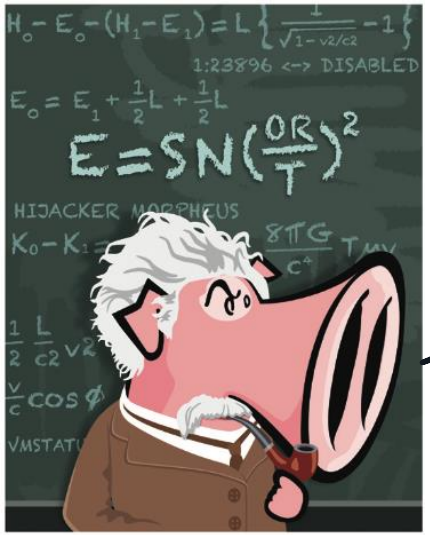


https://developer.cisco.com/secure-firewall

300-710 SNCF

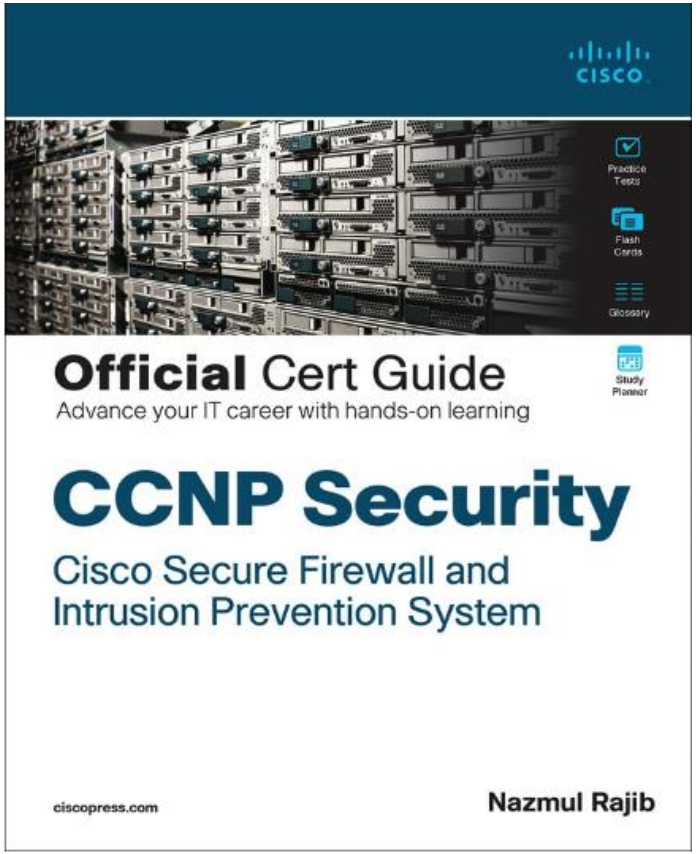
Securing Networks with Cisco Firepower

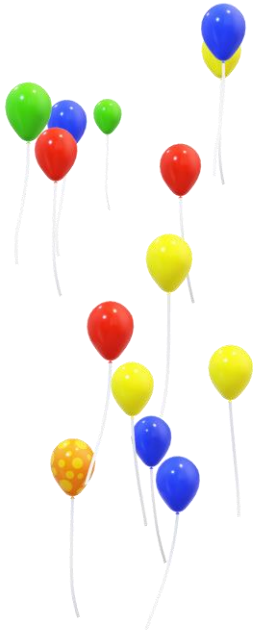
Duration: 90 minutes
Languages: English



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

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.
FINISH
BRKSEC-3023
Secure your multi-cloud infrastructure using Cisco Secure Firewall Virtual

If you are unable to attend a live session, you can watch it in the On-Demand Library after the event.
BRKCRT-2002

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

- 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!
Let's go
#CiscoLive