cisco Live!

ALL IN

#CiscoLive

The bridge to possible

Snort 3 with the Cisco Secure Firewall

Brave new pig!

Alex Tatistcheff, Technical Marketing Engineer
Cisco Systems

BRKSEC-2484

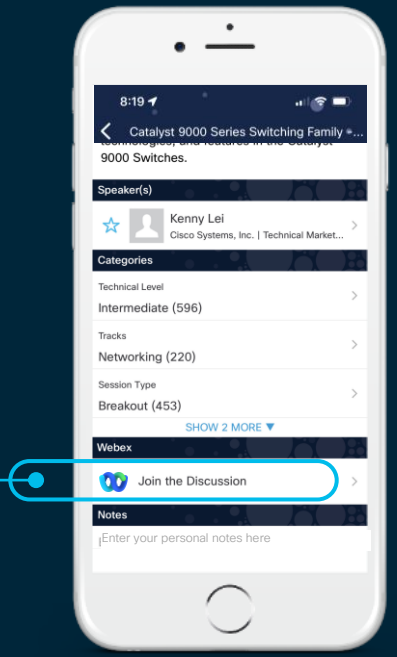
Cisco Webex App

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



https://ciscolive.ciscoevents.com/ciscolivebot/#BRKSEC-2484

Webex spaces will be moderated by the speaker until June 17, 2022.

Agenda

- Snort 2 review
- Snort 3 overview
- Intrusion policy quick look
- Rule Groups
- Rule Recommendations
- Snort 3 rule language

Helpful if you have…

- Familiarity with Secure Firewall (Firepower)
- Experience with Snort 2 Intrusion Policy

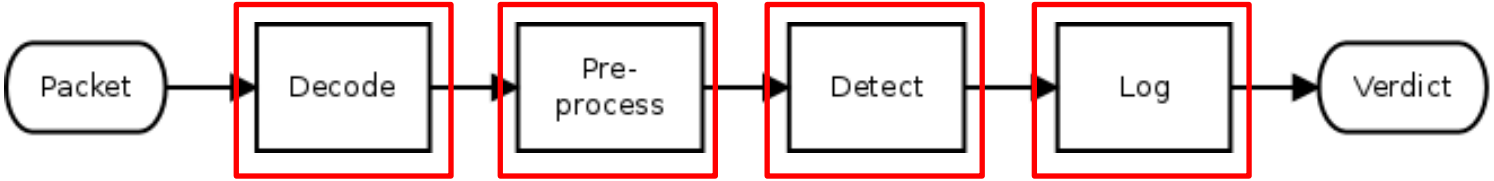
Brand Naming Changes

Firepower Management Center (FMC)	→	Cisco Secure Firewall Management Center (FMC)
Firepower Threat Defense (FTD)	→	Cisco Secure Firewall Threat Defense (FTD)
Adaptive Security Appliance (ASA)	→	Cisco Secure Firewall ASA
Firepower Hardware Appliance	→	Cisco Secure Firewall 3100 Series
Firepower Threat Defense Virtual / NGFWv	→	Cisco Secure Firewall Threat Defense Virtual (FTDv)

Snort 2 Review

Snort 2 Basics

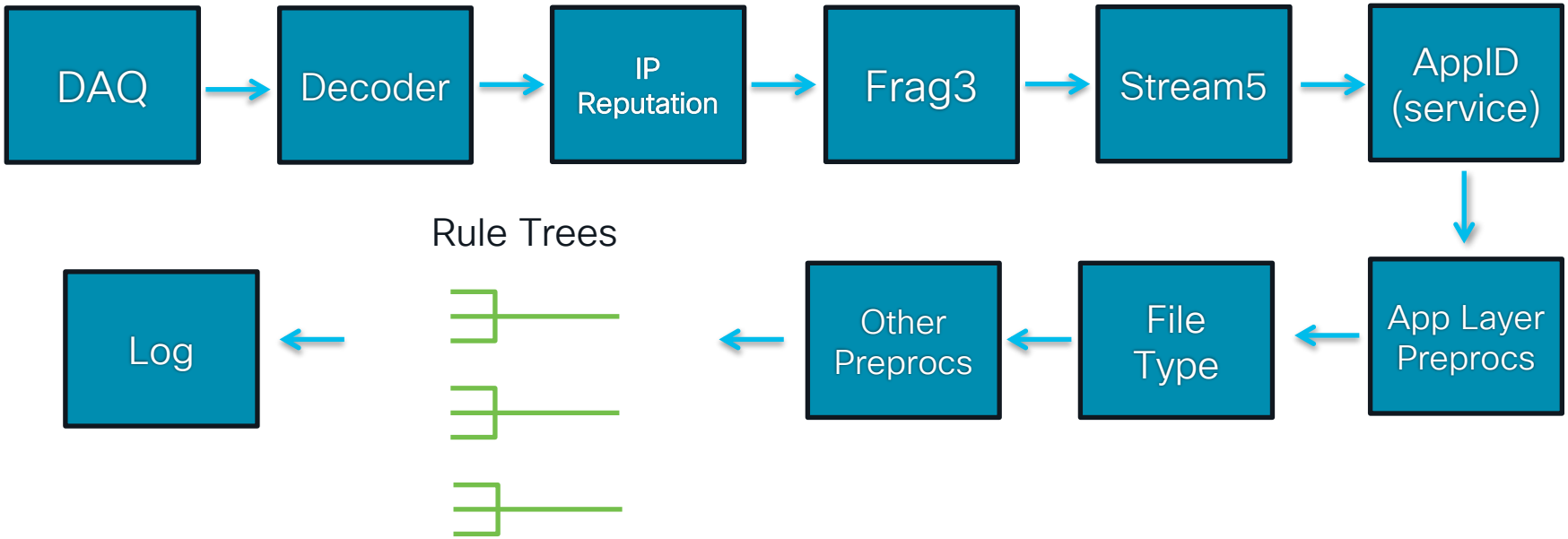
- Four primary components:
  - Sniffer
  - Preprocessors
  - Detection Engine
  - Output/Alerting



Snort 2 Basics

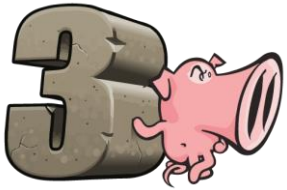
- Preprocessors
  - Present packet data to detection engine
  - Normalize packet data
  - Examples:
    - Fragment reassembly
    - TCP state table
    - TCP stream reassembly
    - Application aware (HTTP, FTP, Telnet, SSH, SSL, SMB, RPC, etc.)
  - Dynamic, new preprocessors can be loaded at startup

Snort Packet Processing Today



Snort 3

Snort 3 Goals/Features



Efficacy

- Modern architecture for viable handling of Snort 2 evasions
- HTTP/2, IoT, multi-session signatures, etc.
- Intelligent traffic normalization to identify obfuscated threats
- Improved rules language allows Talos to provide better protection

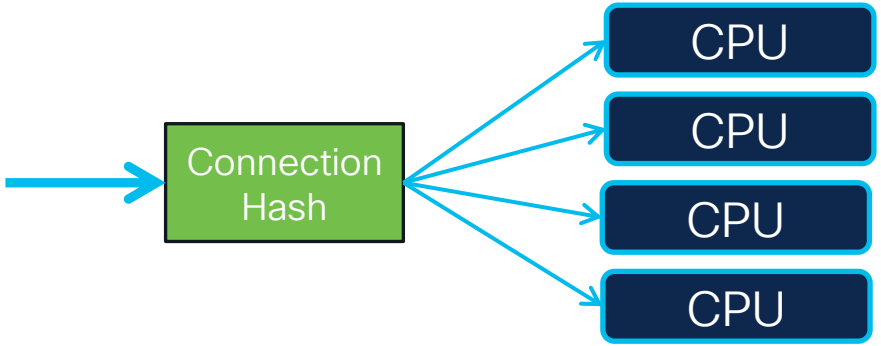
Performance

- Significant performance improvement over Snort 2
- Support for acceleration via Regex offload on next generation platforms
- More efficient memory utilization

Modularity

- Faster time to market with support for new use-cases
- Talos can address 0-day issues with new rule options/inspectors
- Deployable as a cloud service
- Improved maintainability and telemetry

Parallel Processing – Snort 2



Each runs a complete Snort 2 process:

- DAQ
- Configuration
- Preprocessors
- Rule trees

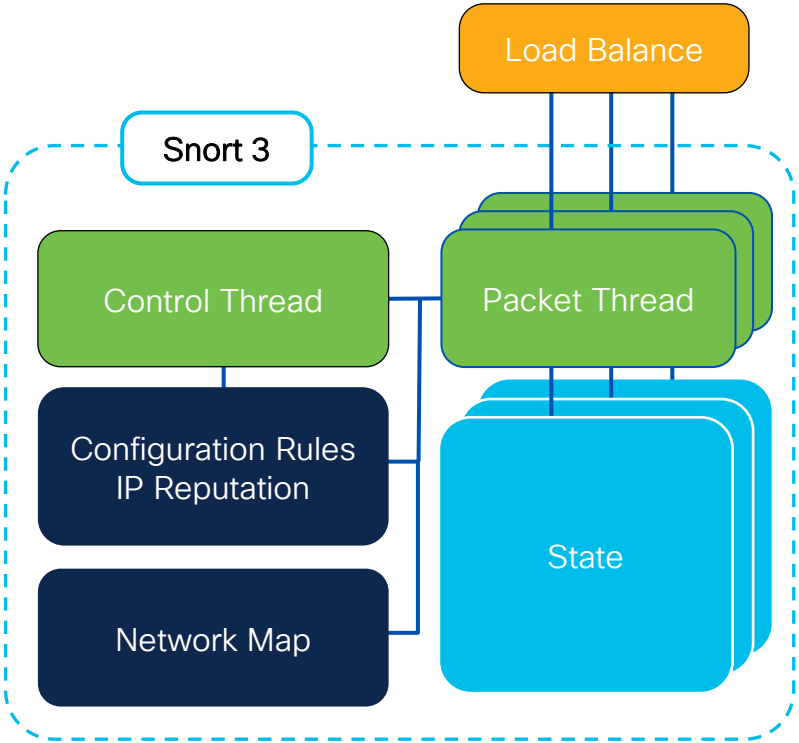
👍 Linear scalability
👎 Duplicated memory structures

Parallel Processing – Snort 2

```
root@ftdv2:/home/admin# ps -ef | grep snort
sfsnort   3024  2989  0 Apr09 ?        00:00:21 /ngfw/usr/local/sf/bin/bltd --pid-file=/var/sf/run/bltd.pid
root      7300  2989 54 18:17 ?        00:00:09 /ngfw/var/sf/detection_engines/fb6e9c44-8812-11eb-889e-2b4df1754997/snort
 --daq-dir /ngfw/usr/local/sf/lib/daq -M -Q -G 0 -i SNORT Inspect:Data Plane --daq pdts_sftls --daq-var instance=71 --pid
-path /ngfw/var/sf/detection_engines/fb6e9c44-8812-11eb-889e-2b4df1754997/instance-1 --cs-dir /ngfw/var/sf/detection_engi
nes/fb6e9c44-8812-11eb-889e-2b4df1754997/instance-1 -c /ngfw/var/sf/detection_engines/fb6e9c44-8812-11eb-889e-2b4df175499
7/snort.conf -Z /ngfw/var/sf/detection_engines/fb6e9c44-8812-11eb-889e-2b4df1754997/instance-1/now -z /ngfw/var/sf/detect
ion_engines/fb6e9c44-8812-11eb-889e-2b4df1754997/instance-1/preproc_stats.csv --no-interface-pidfile -l /ngfw/var/sf/dete
ction_engines/fb6e9c44-8812-11eb-889e-2b4df1754997/instance-1 -P 1518
root      7301  2989 55 18:17 ?        00:00:09 /ngfw/var/sf/detection_engines/fb6e9c44-8812-11eb-889e-2b4df1754997/snort
 --daq-dir /ngfw/usr/local/sf/lib/daq -M -Q -G 1 -i SNORT Inspect:Data Plane --daq pdts_sftls --daq-var instance=72 --pid
-path /ngfw/var/sf/detection_engines/fb6e9c44-8812-11eb-889e-2b4df1754997/instance-2 --cs-dir /ngfw/var/sf/detection_engi
nes/fb6e9c44-8812-11eb-889e-2b4df1754997/instance-2 -c /ngfw/var/sf/detection_engines/fb6e9c44-8812-11eb-889e-2b4df175499
7/snort.conf -Z /ngfw/var/sf/detection_engines/fb6e9c44-8812-11eb-889e-2b4df1754997/instance-2/now -z /ngfw/var/sf/detect
ion_engines/fb6e9c44-8812-11eb-889e-2b4df1754997/instance-2/preproc_stats.csv --no-interface-pidfile -l /ngfw/var/sf/dete
ction_engines/fb6e9c44-8812-11eb-889e-2b4df1754997/instance-2 -P 1518 --suppress-config-log
root      7302  2989 55 18:17 ?        00:00:09 /ngfw/var/sf/detection_engines/fb6e9c44-8812-11eb-889e-2b4df1754997/snort
 --daq-dir /ngfw/usr/local/sf/lib/daq -M -Q -G 2 -i SNORT Inspect:Data Plane --daq pdts_sftls --daq-var instance=73 --pid
-path /ngfw/var/sf/detection_engines/fb6e9c44-8812-11eb-889e-2b4df1754997/instance-3 --cs-dir /ngfw/var/sf/detection_engi
nes/fb6e9c44-8812-11eb-889e-2b4df1754997/instance-3 -c /ngfw/var/sf/detection_engines/fb6e9c44-8812-11eb-889e-2b4df175499
7/snort.conf -Z /ngfw/var/sf/detection_engines/fb6e9c44-8812-11eb-889e-2b4df1754997/instance-3/now -z /ngfw/var/sf/detect
ion_engines/fb6e9c44-8812-11eb-889e-2b4df1754997/instance-3/preproc_stats.csv --no-interface-pidfile -l /ngfw/var/sf/dete
ction_engines/fb6e9c44-8812-11eb-889e-2b4df1754997/instance-3 -P 1518 --suppress-config-log
root      7484  3613  0 18:17 pts/0    00:00:00 grep snort
root@ftdv2:/home/admin#
```

Snort 3 Architecture

- Threaded to use multiple cores:
  - 1 control thread (main)
  - N packet threads per process
  - Reloads faster (1 vs N)
- One copy of config and network map:
  - Uses less memory
  - Supports more IPS rules and larger netmap



Inspection Threads – Snort 3

```
root@ftdv2:/home/admin# ps -ef | grep snort
sfsnort   3024  2989  0 Apr09 ?        00:00:21 /ngfw/usr/local/sf/bin/bltd --pid-file=/var/sf/run/bltd.pid
root      3406  2989  1 Apr09 ?        01:14:46 /ngfw/var/sf/detection_engines/fb6e9c44-8812-11eb-889e-2b4df1754997/snort
3 --plugin-path /ngfw/var/sf/detection_engines/fb6e9c44-8812-11eb-889e-2b4df1754997/plugins:/ngfw/var/sf/lsp/active-so_ru
les --daq-dir /ngfw/usr/local/sf/lib/daq3 -M -Q -v -c /ngfw/var/sf/detection_engines/fb6e9c44-8812-11eb-889e-2b4df1754997
/snort3.lua -l /ngfw/var/sf/detection_engines/fb6e9c44-8812-11eb-889e-2b4df1754997 --id-offset 1 --id-subdir --id-zero --
run-prefix instance- --control-socket /ngfw/var/sf/detection_engines/fb6e9c44-8812-11eb-889e-2b4df1754997/snort3.sock --c
reate-pidfile -s 1518 -z 3
root      3469  3406  0 Apr09 ?        00:00:00 /ngfw/usr/local/sf/bin/snort3_crash_handler 5 6 /ngfw/var/common
root      3844  3613  0 18:11 pts/0    00:00:00 grep snort
root@ftdv2:/home/admin#
```

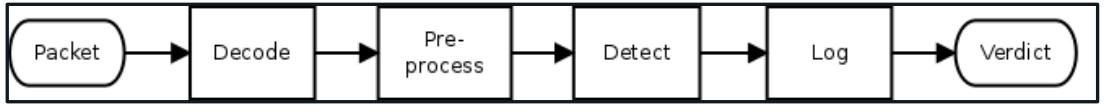
- Single Snort 3 process
- Three inspection threads (-z or --max-packet-threads)

Snort 3 Plugins and Inspectors

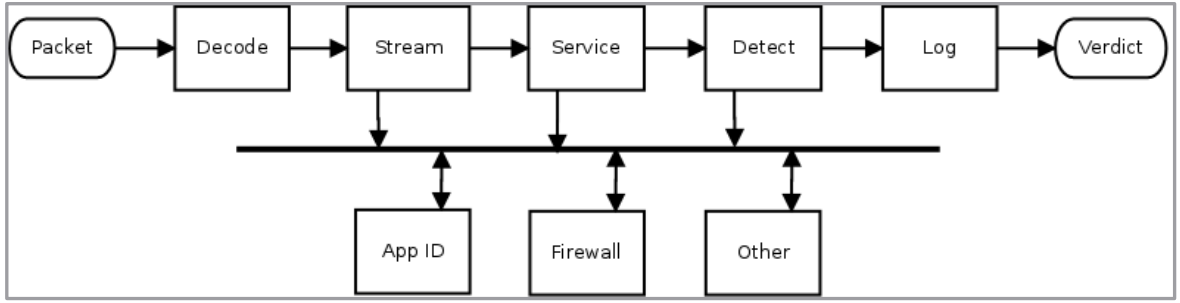
- “Inspectors” are comparable to and replace “preprocessors”
- Each plugin type has a defined purpose and accomplishes most of the processing objectives:
  - **Codec** – to decode and encode packets
  - **Inspector** – like Snort 2 preprocessors, for normalization, etc.
  - **IpsOption** – for detection in Snort rules
  - **IpsAction** – for custom actions
  - **Logger** – for handling events
  - **Multi Pattern Search Engine (MPSE)** – for fast pattern matching
  - **Shared Object (So)** – for dynamic rules

Snort 3 Packet Processing

- Snort 2:



  - Preprocessors use callback functions
  - A later preprocessor (like HTTP) may extract and normalize data that is not used
  - Preprocessors (like AppID) may repeatedly check for available data
- Snort 3 – Parallel Resource Utilization:
  - Uses publish-subscribe model
  - Plugin communication is event driven
  - Subscribers access raw or normalized data as needed
  - JIT buffers



New HTTP Inspector

- HTTP inspection completely new
- Adds HTTP/2 support
- Fully stateful
- JIT buffers
- New rule options
- Flow-based for better evasion resistance
- HTTP Evader
  - 3.0 = 99%

HTTP/2 – Feature and Functional Support

- Previously, HTTP/2 sessions were downgraded to HTTP/1 to support inspection
- Requires SSL Decryption
- Supported in IPS, AppID, Firewall, and File Type Detection
- IPS support:
  - HTTP-based IPS rules trigger for HTTP/1.1 as well as HTTP/2 traffic
  - HTTP/2 Inspector also monitors for specific protocol anomalies, which generate built-in inspector alerts (if enabled)

HTTP/2

Pig vs Pig

Snort 2	Snort 3
Single packet thread	Multiple packet threads
Run to completion	Multiple packets per thread
More monolithic	More plugins
Procedural	Procedural + Event driven
Just-in-Case	Just-in-Time
Text Config	Lua Config
Tricky buffers	Sticky buffers
Intel® CPM	Hyperscan
Packets	PDUs
Deep packet inspection	Deep flow inspection
Ports	Services
<=2 IP layers	<=N IP layers

Snort 3 with Firewall Threat Defense

- Supported on FMC with 7.0 release (6.7 on FDM)
- 7.1 short-term release brought Firepower Recommendations
- 7.2 long-term is latest release
- Both Snort 2 and Snort 3 engines supported on 7.x devices

Intrusion Policy

Policy UI Overview

Firewall Management Center
Policies / Access Control / Intrusion / Intrusion Policies

Overview | Analysis | Policies | Devices | Objects | Integration | Deploy | alext ▾ | 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		
Balanced Intrusion Snort 3 is in sync with Snort 2. 2022	Balanced policy, prevention mode	Balanced Security and Connectivity	*No Access Control Policy* *No Device*	Snort 2 Version	Snort 3 Version
IDS Passive SoC Snort 3 is in sync with Snort 2	Security Over Conn passive devices	Security Over Connectivity	1 Access Control Policy 2 Devices	Snort 2 Version	Snort 3 Version
Secure IPS Snort 3 is out of sync with Snort 2. 2	Extra security, prevention mode	Security Over Connectivity	1 Access Control Policy 2 Devices	Snort 2 Version	Snort 3 Version

One Policy, Two Snort Versions

Firewall Management Center
Policies / Access Control / Intrusion / Intrusion Policies

Overview | Analysis | Policies | Devices | Objects | Integration | Deploy | alext ▾ | cisco 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		
Balanced Intrusion Snort 3 is in sync with Snort 2. 2022	Balanced policy, prevention mode	Balanced Security and Connectivity	*No Access Control Policy* *No Device*	Snort 2 Version	Snort 3 Version
IDS Passive SoC Snort 3 is in sync with Snort 2	Security Over Conn passive devices	Security Over Connectivity	1 Access Control Policy 2 Devices	Snort 2 Version	Snort 3 Version
Secure IPS Snort 3 is out of sync with Snort 2. 2	Extra security, prevention mode	Security Over Connectivity	1 Access Control Policy 2 Devices	Snort 2 Version	Snort 3 Version

One Policy, Two Snort Versions

Firewall Management Center
Policies / Access Control / Intrusion / Intrusion Policies

Deploy alext SECURE

Intrusion Policies | Network Analysis Policies

Hide Snort 3 Sync status | Search by Intrusion Poli | PS Mapping | Compare Policies | Create Policy

Intrusion Policy	Description			
Balanced Intrusion Snort 3 is in sync with Snort 2. 2022	Balanced policy, preventi	Snort 2 Version	Snort 3 Version	
IDS Passive SoC Snort 3 is in sync with Snort 2	Security Over Conn passi	Snort 2 Version	Snort 3 Version	
Secure IPS Snort 3 is out of sync with Snort 2. 2	Extra security, prevention	Snort 2 Version	Snort 3 Version	

Edit Intrusion Policy

Name*

IDS Passive SoC

Description

Security Over Conn passive devices

Inspection Mode

(•) Detection ( ) Prevention

Intrusion rules generate alerts only. A connection that matches a drop rule will generate alert messages, but the connection will not be blocked.

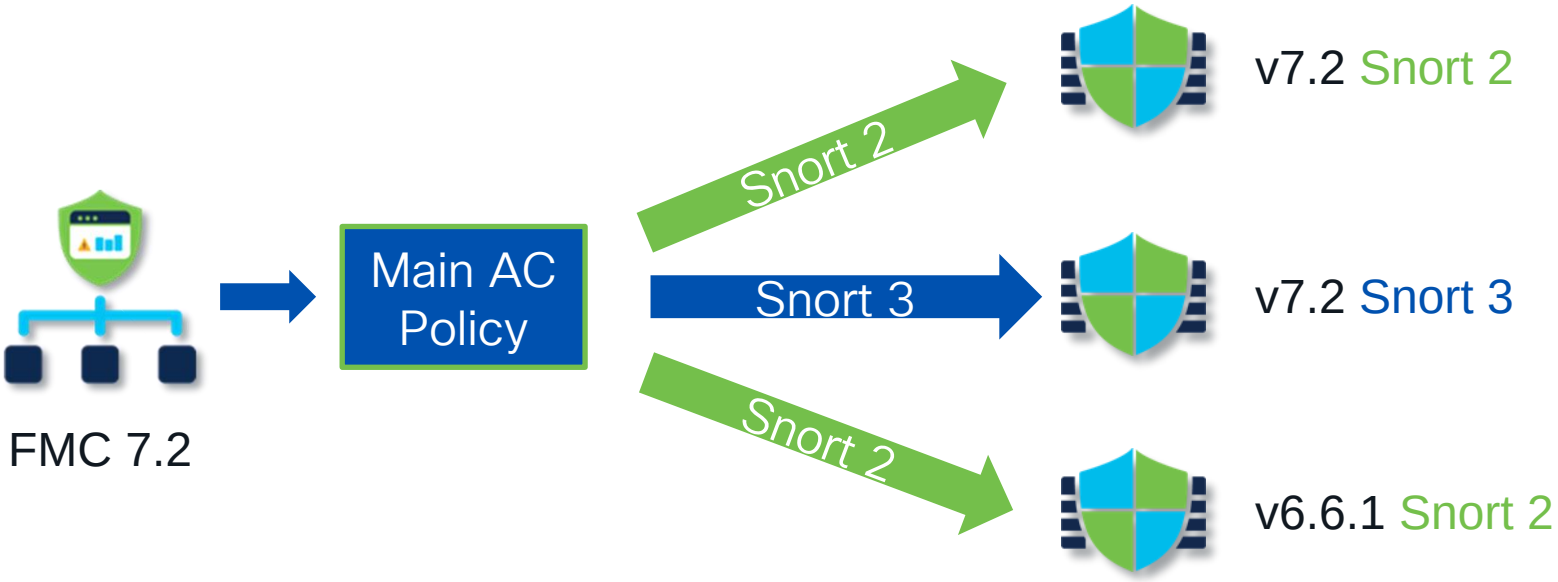
Base Policy

Security Over Connectivity

Cancel | Save

Hybrid Policy Deployment Example

Ensure Snort 2/3 policies provide the same protection



Rule Group Security Levels

Snort 3 Rule Groups

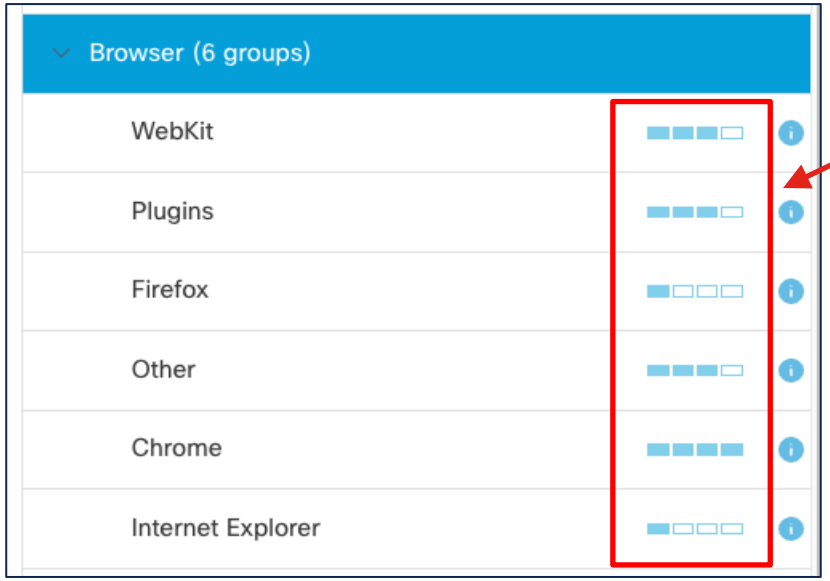
What are they?

New rule groupings in Snort 3

”Big Deal” you say...

Snort 3 Rule Groups

What do they offer?



Security Level

- Can be set an a per group basis
- Equates to Talos policy
- Snort 2 offers this only in the base policy

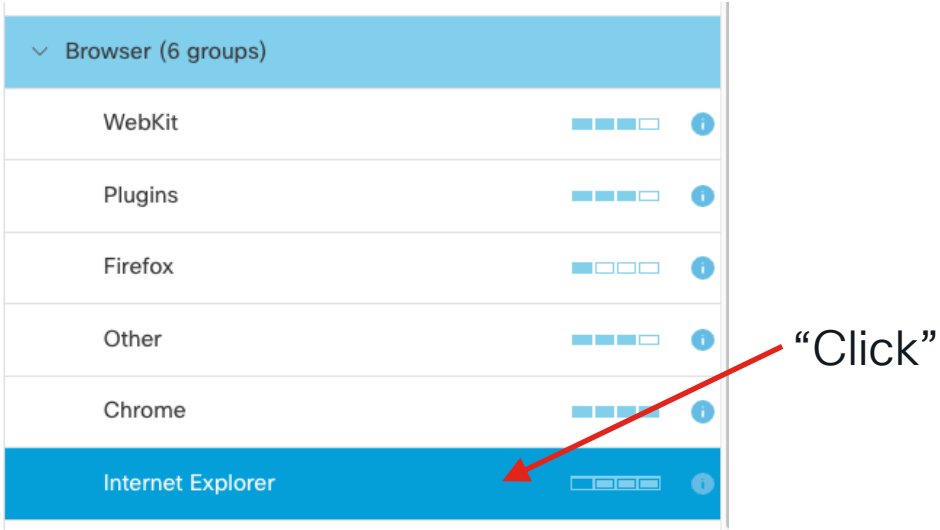
Snort 3 Rule Groups

- Security Level equates to policy
    - **Level 1** – Connectivity Over Security
    - **Level 2** – Balanced Security and Connectivity
    - **Level 3** – Security Over Connectivity
    - **Level 4** – Maximum Detection

Snort 3 Rule Groups

How do I use them?

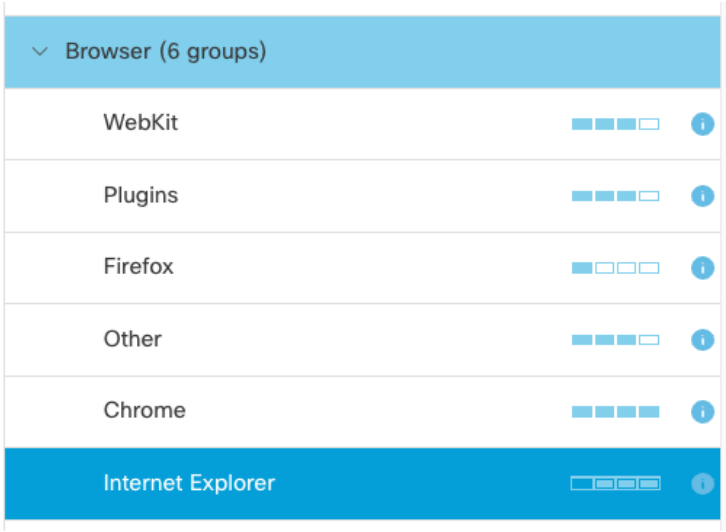
1. Select a Group

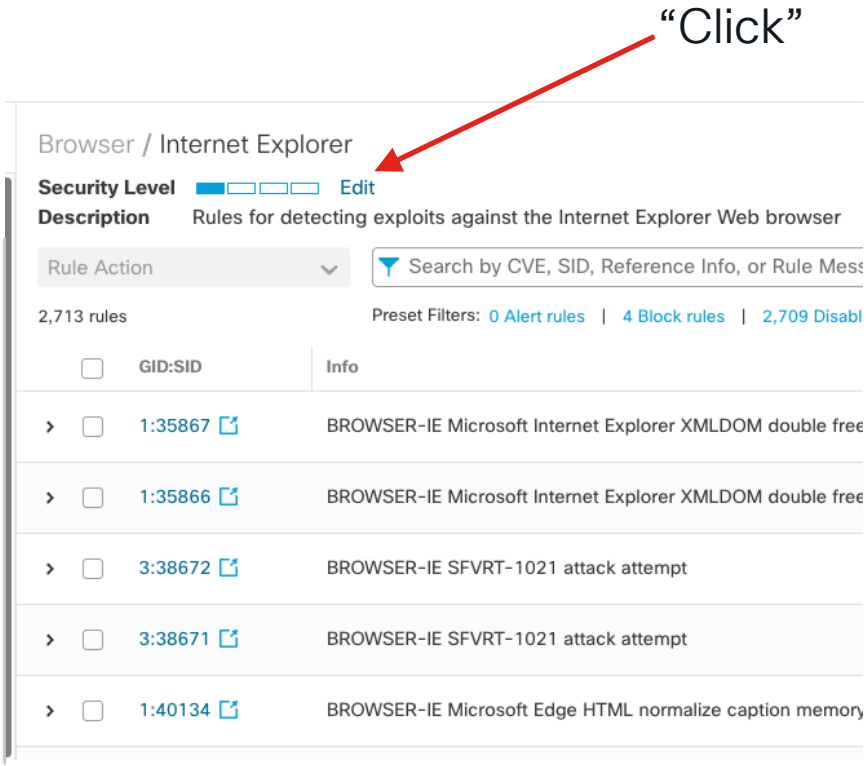


Snort 3 Rule Groups

How do I use them?

2. Edit the Security Level





Snort 3 Rule Groups

How do I use them?

2. Edit the Security Level

Select Level

Browser (6 groups)
WebKit
Plugins
Firefox
Other
Chrome
Internet Explorer

Edit Security Level

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

Cancel Save

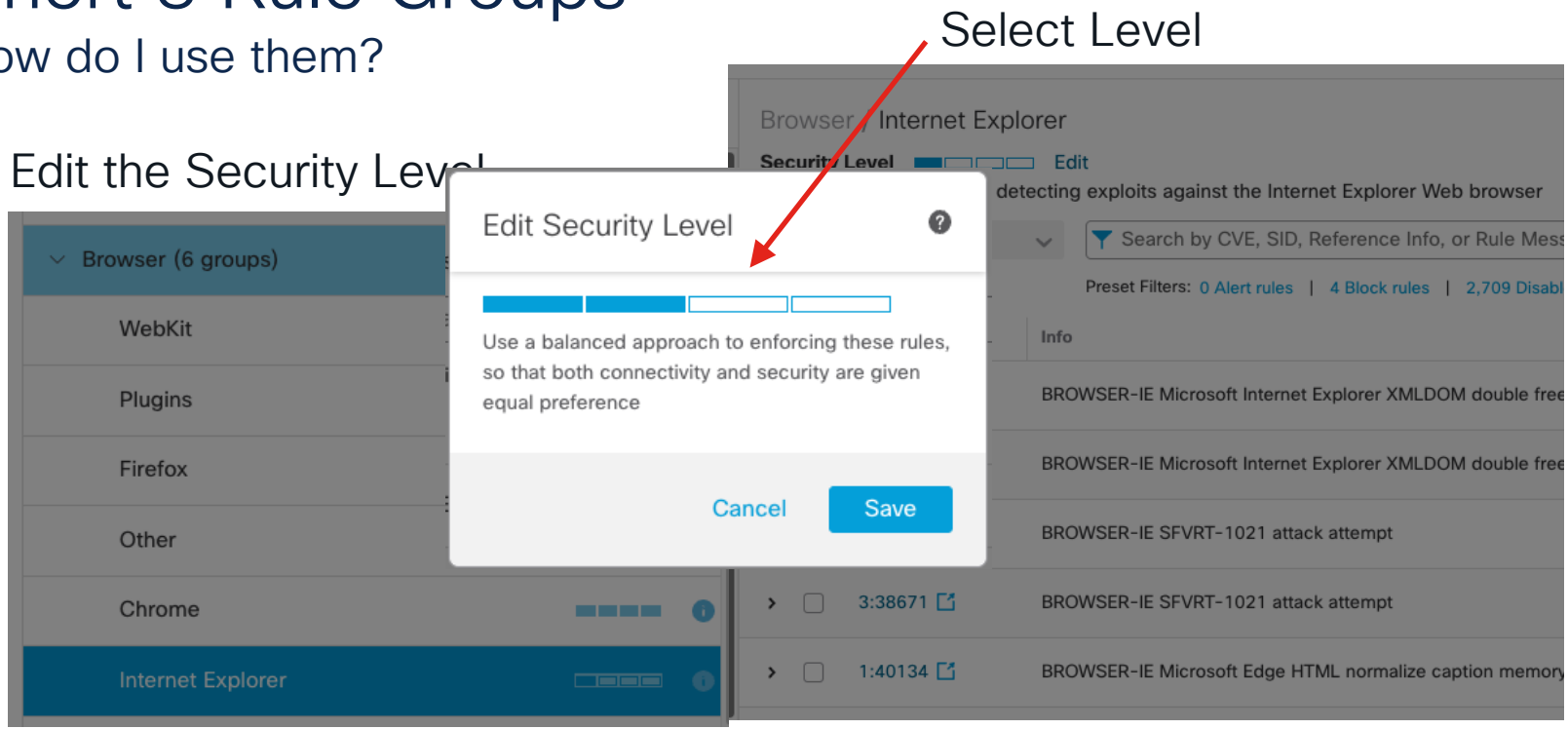
Browser / Internet Explorer
Security Level Edit
detecting exploits against the Internet Explorer Web browser
Search by CVE, SID, Reference Info, or Rule Mess
Preset Filters: 0 Alert rules | 4 Block rules | 2,709 Disabl

	Info
	BROWSER-IE Microsoft Internet Explorer XMLDOM double free
	BROWSER-IE Microsoft Internet Explorer XMLDOM double free
	BROWSER-IE SFVRT-1021 attack attempt
3:38671	BROWSER-IE SFVRT-1021 attack attempt
1:40134	BROWSER-IE Microsoft Edge HTML normalize caption memory

Snort 3 Rule Groups

How do I use them?

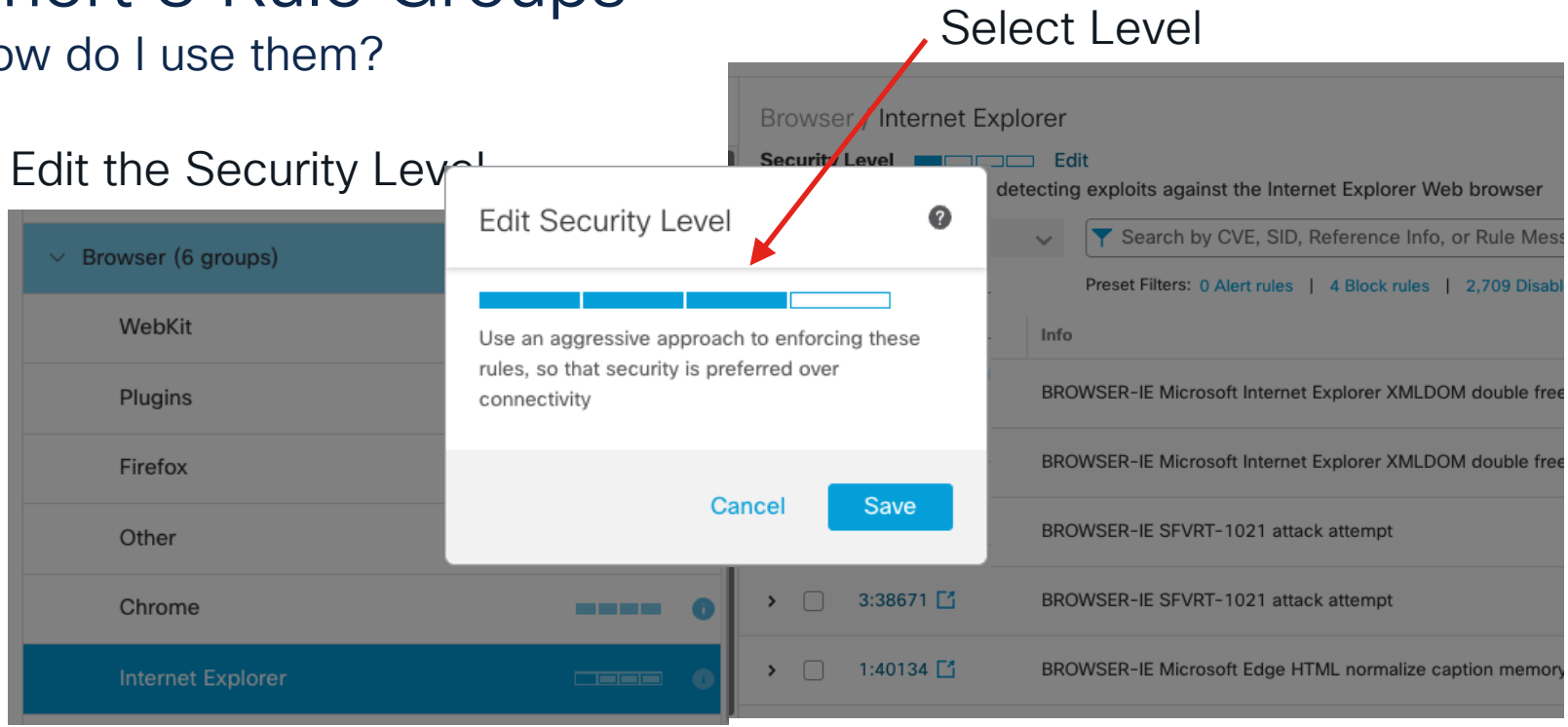
2. Edit the Security Level



Snort 3 Rule Groups

How do I use them?

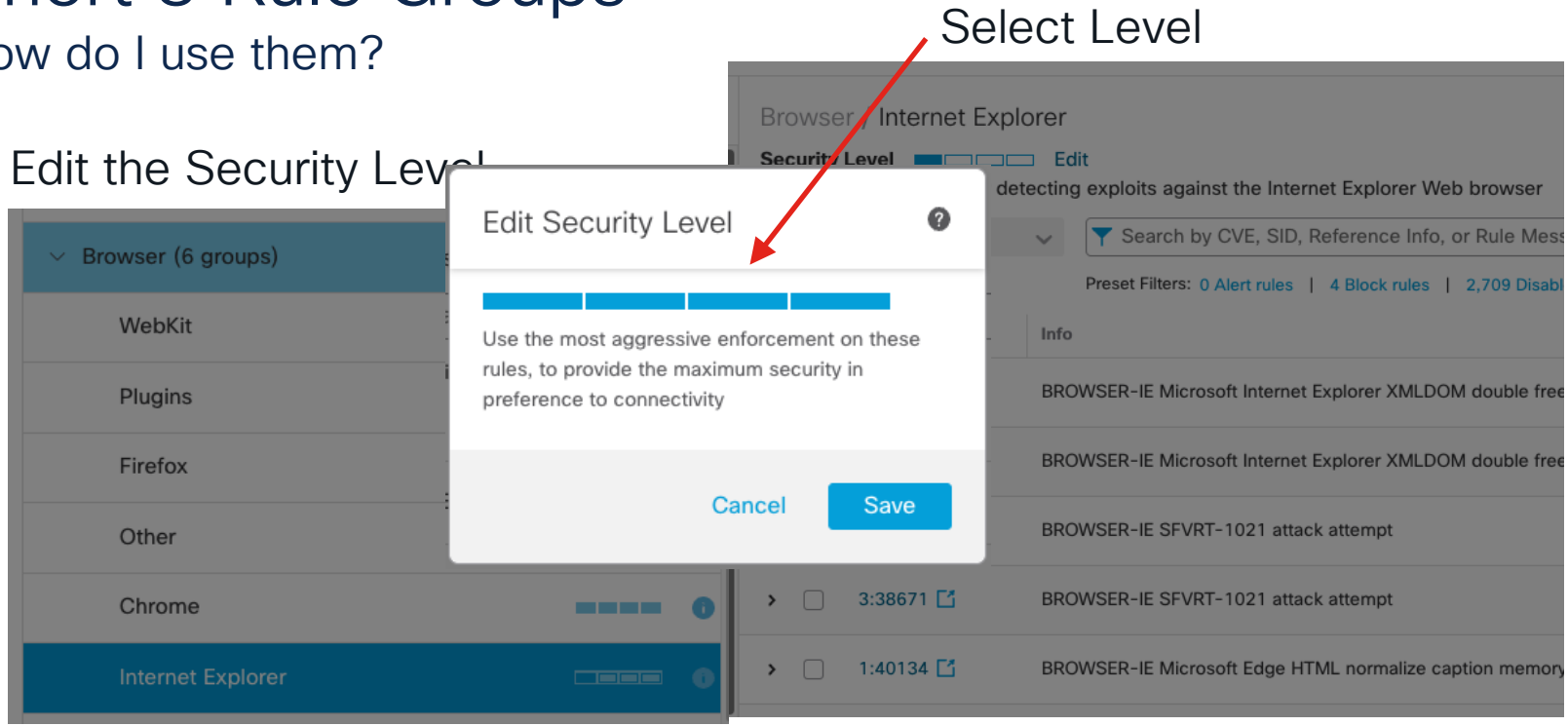
2. Edit the Security Level



Snort 3 Rule Groups

How do I use them?

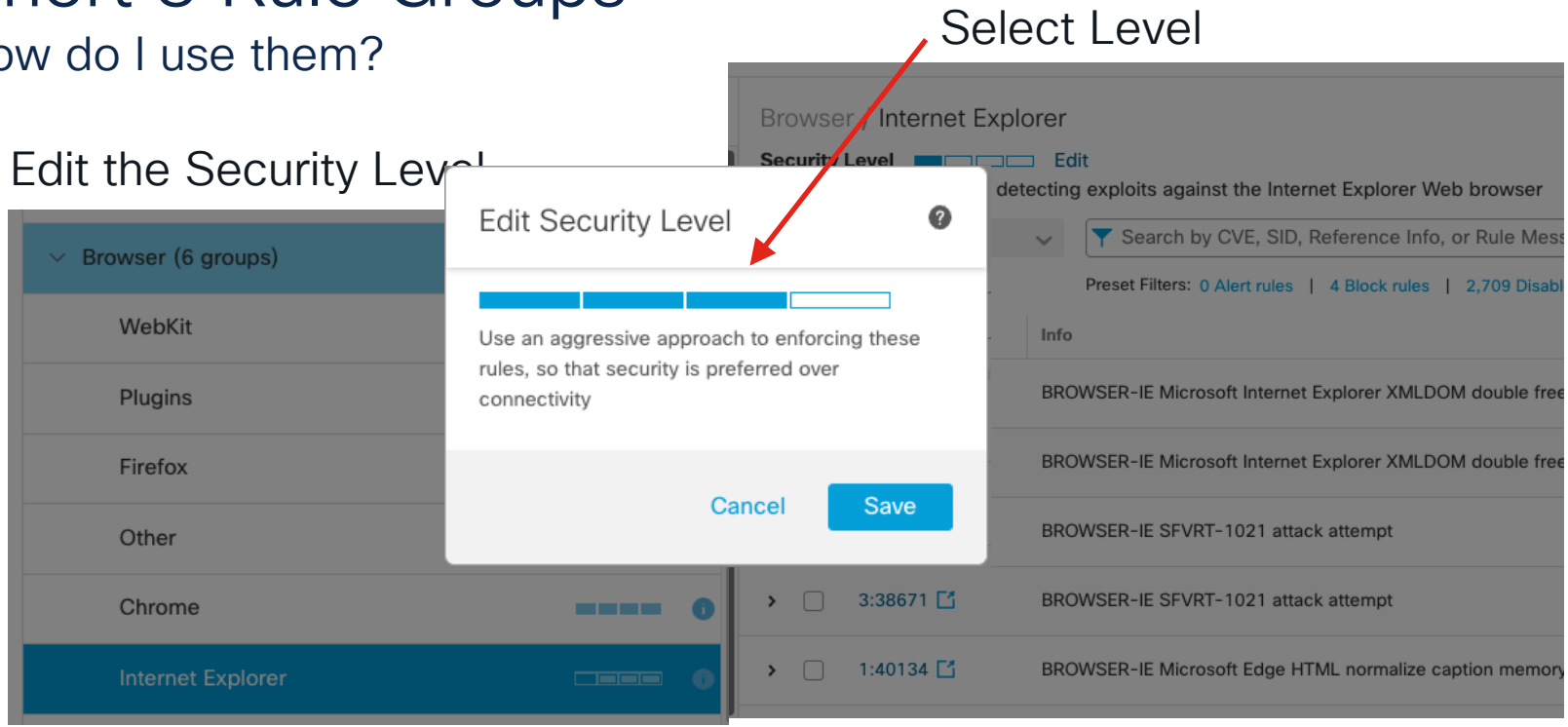
2. Edit the Security Level



Snort 3 Rule Groups

How do I use them?

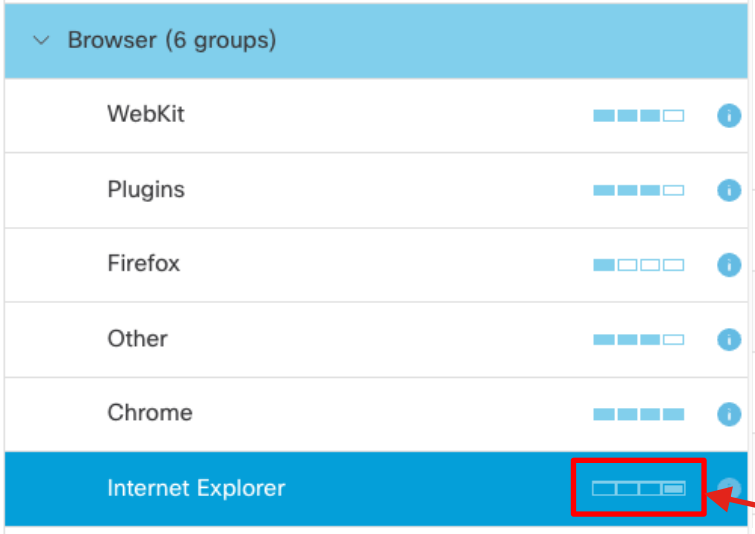
2. Edit the Security Level

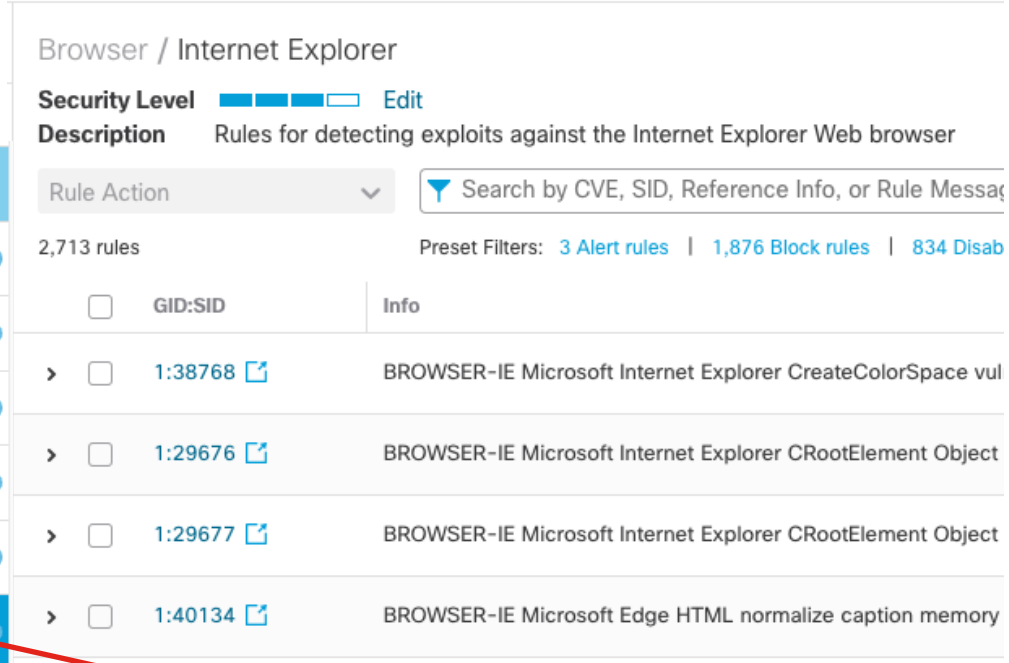


Snort 3 Rule Groups

How do I use them?

3. Save the Security Level





Customized security level

Snort 3 Rule Groups

What problem does this solve?

- No need to set individual rule states
- Rules maintained by Talos
- New updates (LSP) will leverage your customized Group Security Level
- No need to constantly “tweak” your rule set

Recommended Rules
(f.k.a. Firepower Recommendations)

Rule Recommendations

What are they?

- Self-tuning rule set
- Snort rules enabled/disabled based on host data in the network map
- Network Discovery maintains host database based on passive traffic analysis
- Hosts have various attributes:
  - Operating System
  - Services
  - Applications (client)
  - Listening ports
  - Vulnerabilities

Various Snort rules written for these

- Recommendations maps Snort rules to host vulnerabilities

Rule Recommendations

Changes from Snort 2

- No rule overhead
- Security Level based on Talos base policies
- Recommended rule action derived from Security Level

Snort 3 Rule Recommendations

7.1 Release

Rule Groups

65 items | Search Rule Group | +

Excluded | Included | Overridden

All Rules | Recommendations

- Browser (6 groups)
- Server (9 groups)
- Policy (4 groups)
- Indicator (4 groups)
- Potentially Unwanted Applications (5 groups)
- Malware (5 groups)

All Rules

All rules assigned to current intrusion policy irrespective of rule group

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

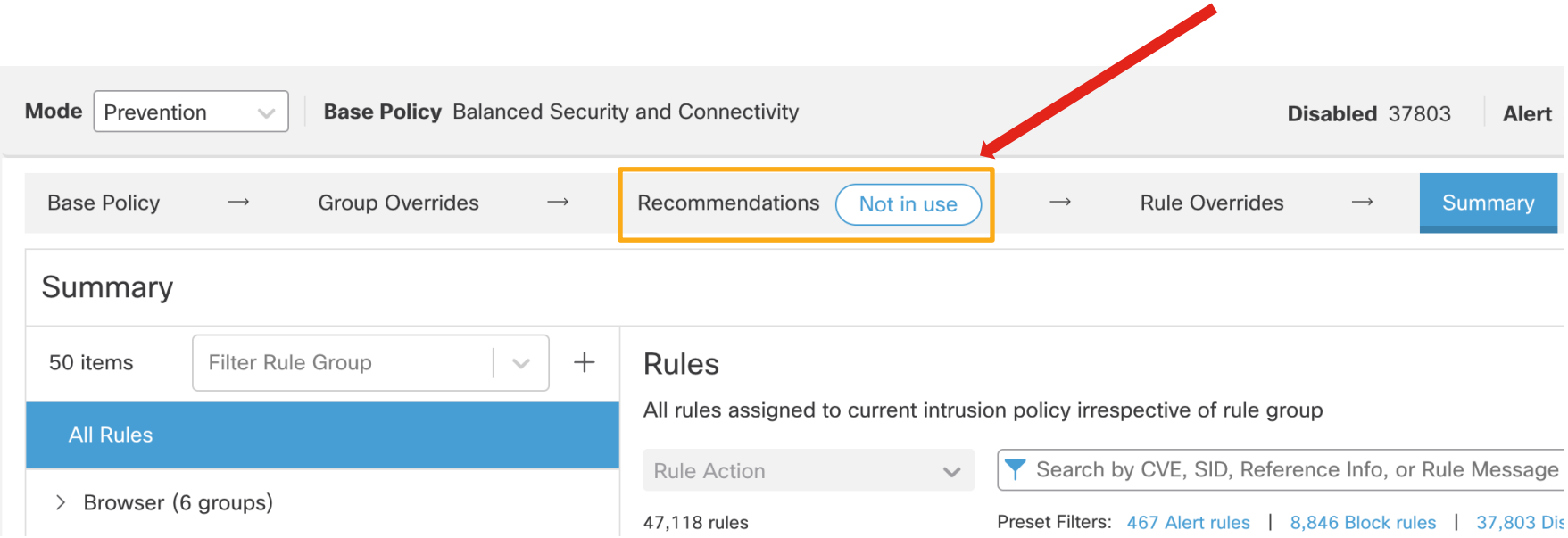
45,468 rules

Preset Filters: 1,322 Alert rules | 34,830 Block rules | 9,316 Disabled rules | 0 Overridden rules | 0 Rewrite rules | 0 Pass rules | 0 Drop rules | 0 Reject rules

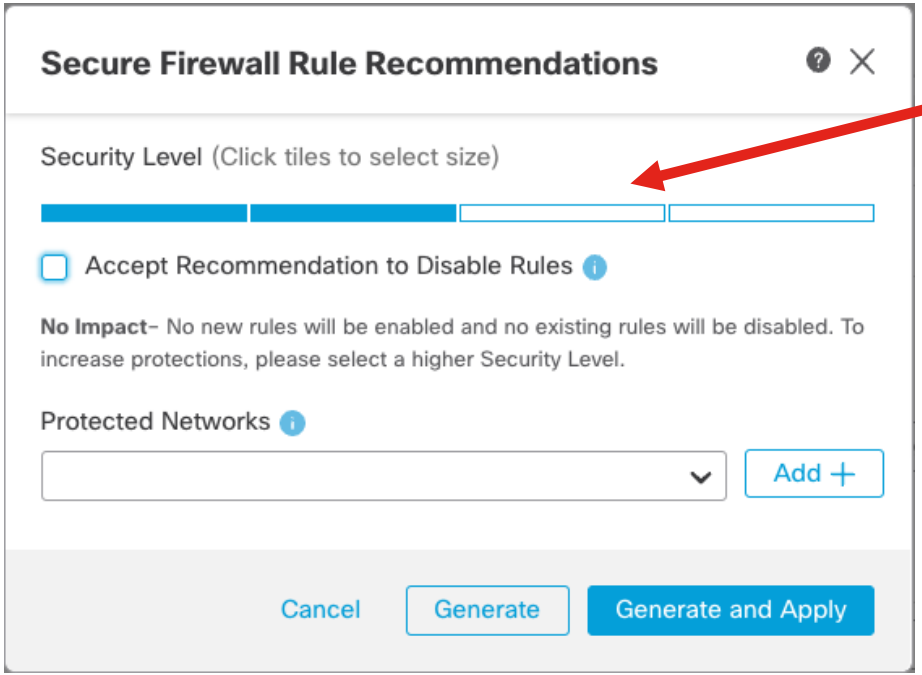
GID:SID	Info	Rule Action
1:23616	APP-DETECT Amazon Kindle 3.0 User-Agent string requested	Alert (Default)
1:13898	APP-DETECT Apple iTunes client request for server info	Alert (Default)
1:50870	APP-DETECT Quagga password challenge detected	Alert (Default)
1:15468	BROWSER-IE Apple Safari-Internet Explorer SearchPath blende...	Alert (Default)

Snort 3 Rule Recommendations

7.2 Release



Recommendations Security Level



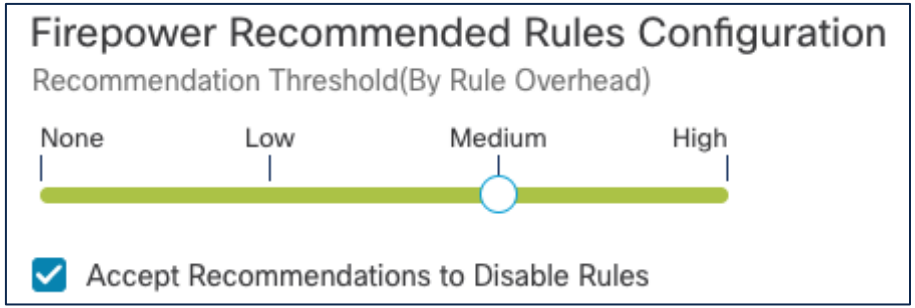
Security Level

Recommendations Security Level

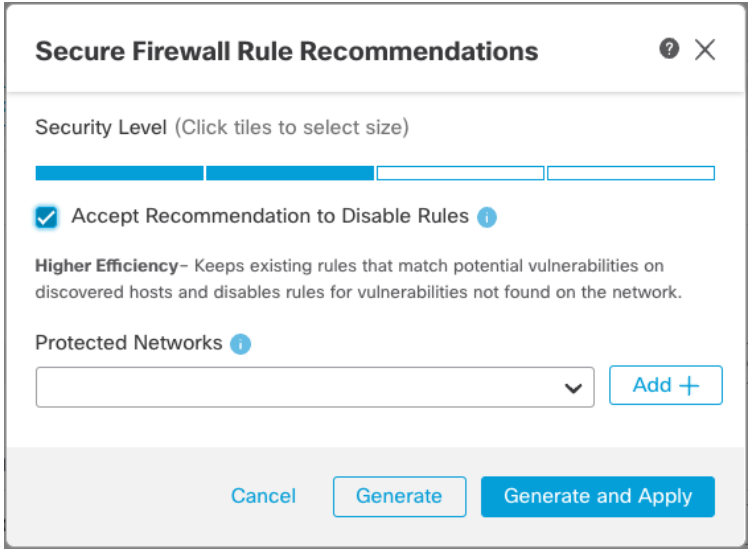
Consider enabled rules from:

- **Level 1** - Connectivity Over Security
- **Level 2** - Balanced Security and Connectivity
- **Level 3** - Security Over Connectivity
- **Level 4** - Maximum Detection

Snort 2 vs. Snort 3



=

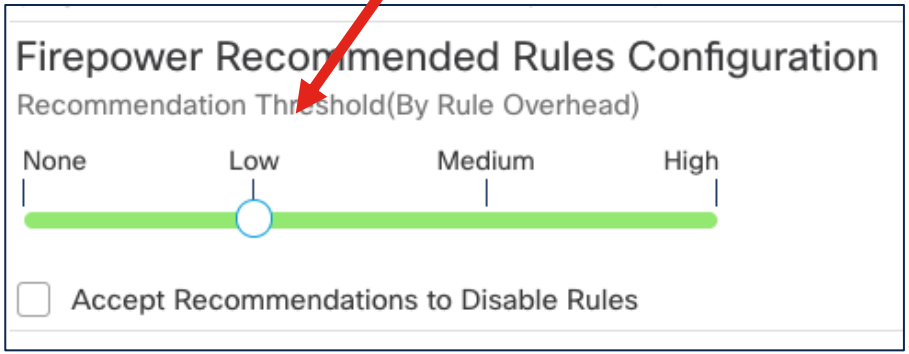


Snort 2

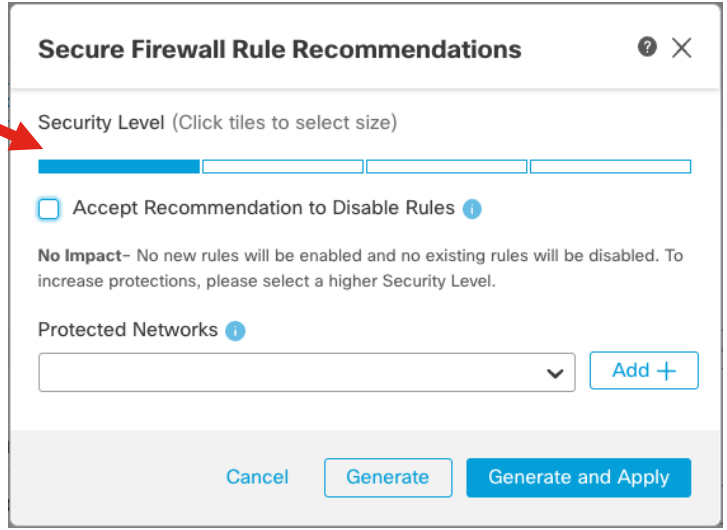
Snort 3

Snort 2 vs. Snort 3

Connectivity (Security Level 1)



=

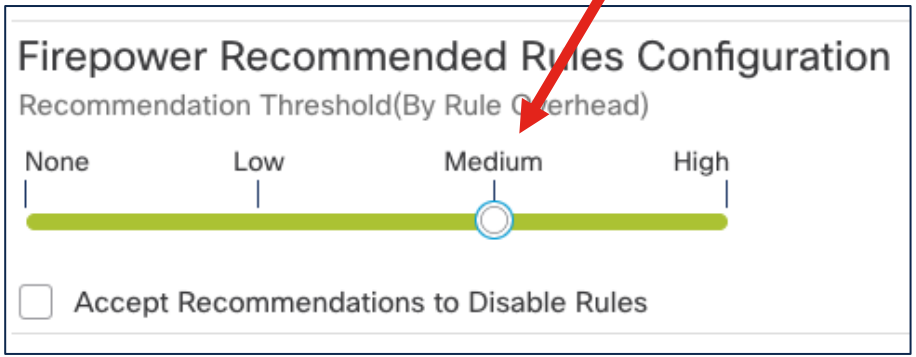


Snort 2

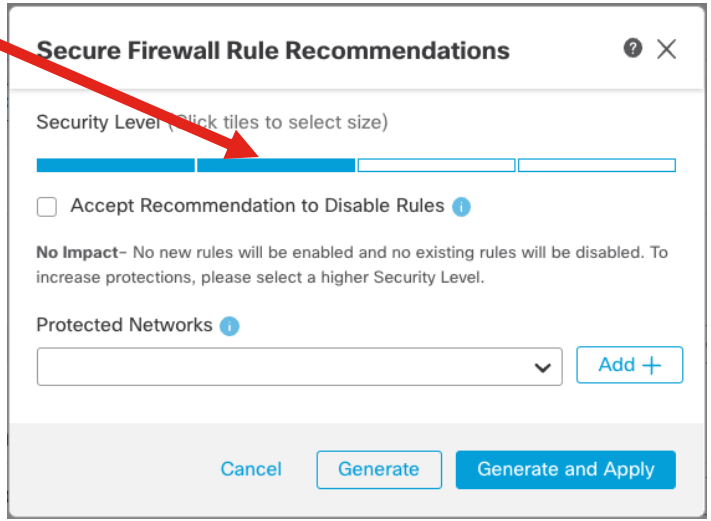
Snort 3

Snort 2 vs. Snort 3

Balanced (Security Level 2)



=

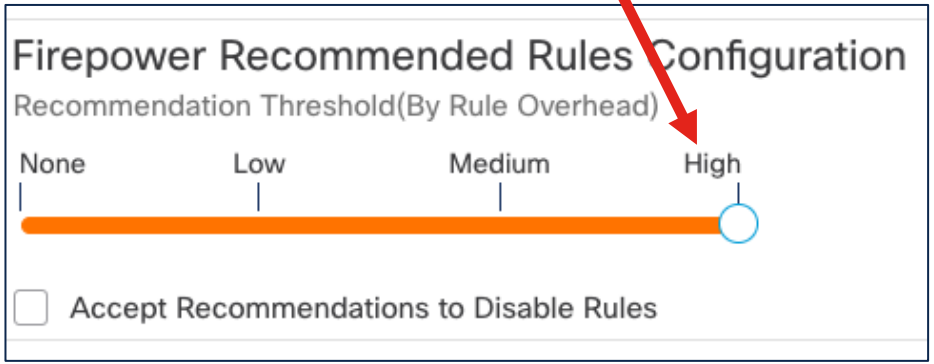


Snort 2

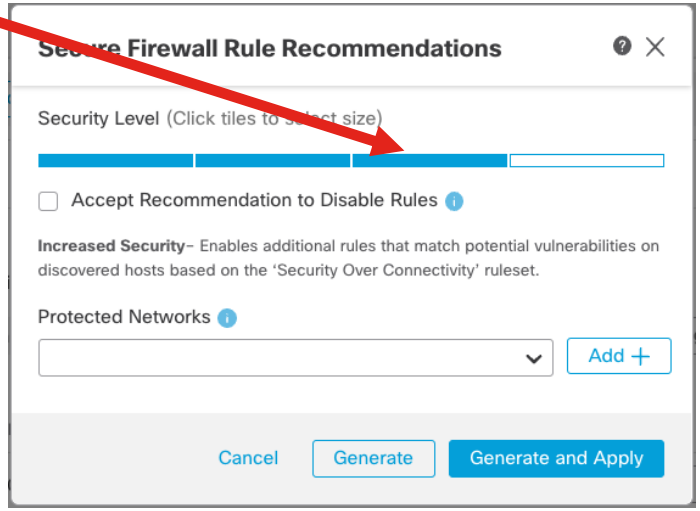
Snort 3

Snort 2 vs. Snort 3

Security Over Connectivity (Security Level 3)



=



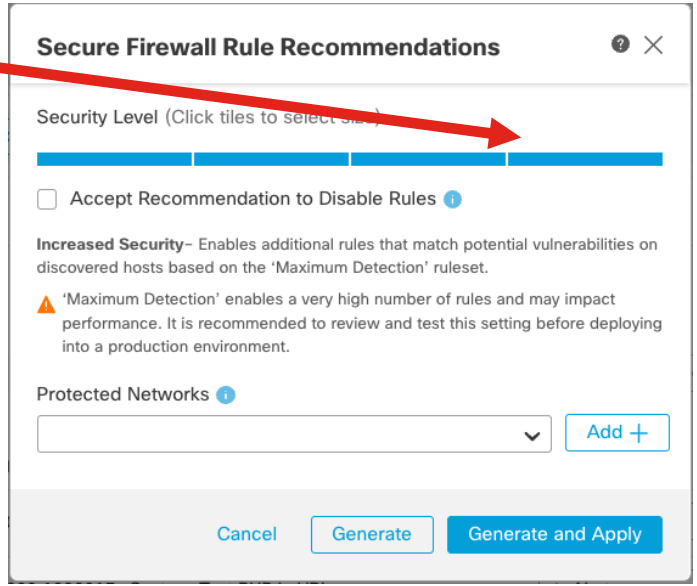
Snort 2

Snort 3

Snort 2 vs. Snort 3

Maximum Detection (Security Level 4)

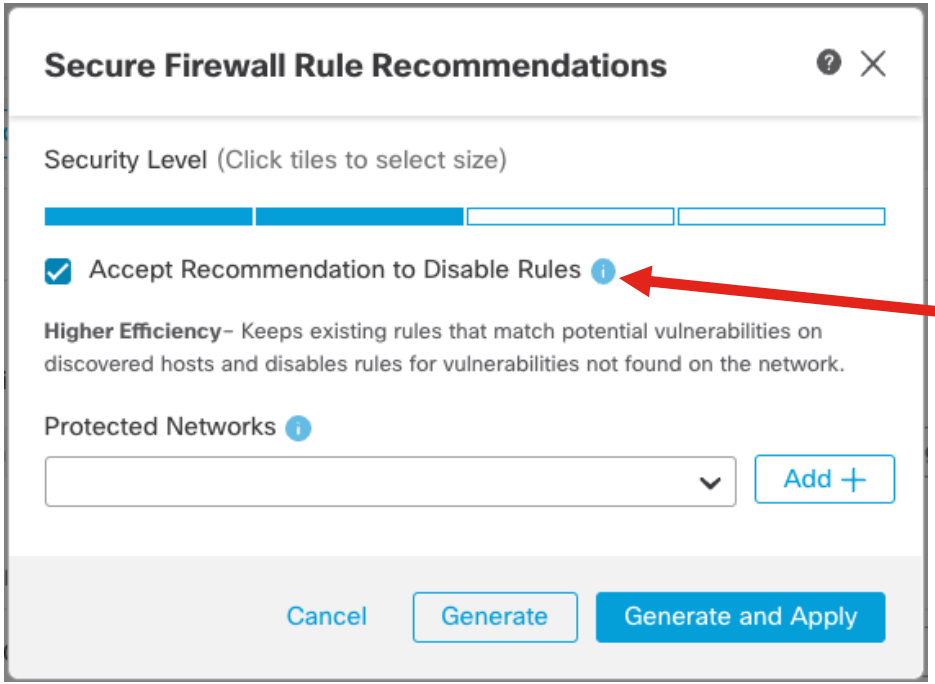
=



Snort 2

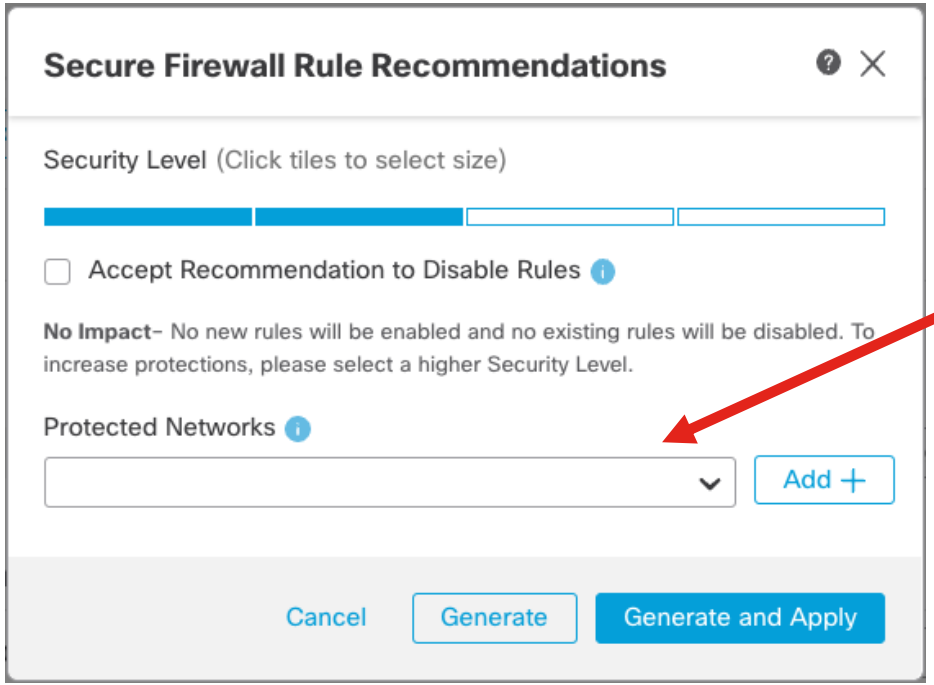
Snort 3

Disable Rules



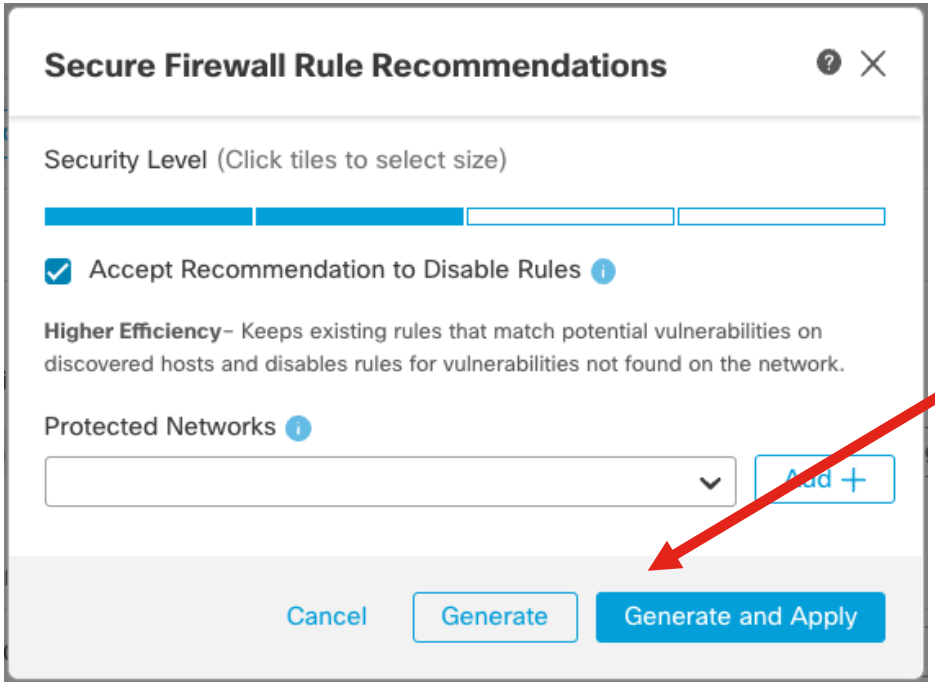
Disable rules designed for vulnerabilities not found in network map

Protected Networks



Blank defaults to any-ipv4 and any-ipv6 (all hosts)

Update Policy with Recommendations



After configuring, click Generate or Generate and Apply

Snort 3 Rule Recommendations - Actions

Firewall Management Center
Policies / Access Control / Intrusion / Intrusion Policies

Overview | Analysis | Policies | Devices | Objects | Integration | Deploy | alext | SECURE

Policies / Intrusion / Balanced Intrusion

Mode Prevention | Base Policy Balanced Security and Connectivity
Description Balanced policy, prevention mode
Disabled 37773 | Alert 470 | Block 8846 | Overridden 3 | Rewrite 0 | Pass 0 | Drop 0 | Reject 0

Base Policy → Group Overrides → Recommendations → Rule Overrides → Summary

Select layer

Additional controls

Recommendations

Recommended Rules (Not in use)

Recommended Rules

Accept | Refresh | Edit | Discard

Firepower recommends 13,325 rules state settings for 2 networks | Generated on 2022-04-13 10:11:32 MDT

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

13,325 rules | Preset Filters: 294 Alert rules | 13,031 Block rules | 0 Disabled rules | 1 Overridden rules | New recommendations

GID:SID	Info	Rule Action	Assigned Groups
1:27766	BROWSER-PLUGINS Oracle Java Security Sli...	Alert	Browser/Plugins
1:27110	EXPLOIT-KIT Blackholev2/Cool exploit kit out...	Alert	Malware/Exploit Kit
1:30970	EXPLOIT-KIT CritX exploit kit outbound reque...	Alert	Malware/Exploit Kit
1:30969	EXPLOIT-KIT CritX exploit kit outbound reque...	Alert	Malware/Exploit Kit
1:30972	EXPLOIT-KIT CritX exploit kit outbound reque...	Alert	Malware/Exploit Kit
1:30971	EXPLOIT-KIT CritX exploit kit outbound reque...	Alert	Malware/Exploit Kit
1:32555	EXPLOIT-KIT Hellspawn exploit kit outbound ...	Alert	Malware/Exploit Kit
1:28796	EXPLOIT-KIT iFRAMEr successful cnt.php red...	Alert	Malware/Exploit Kit

Snort 3 Rule Recommendations - Actions

- Accept - Implements the previously generated recommendations layer*
- Refresh - Regenerates and updates the rule recommendations
- Edit - Allows the user to change the recommendation configuration
- Discard - Removes the recommendations layer

* Does not appear if you selected Generate and Apply

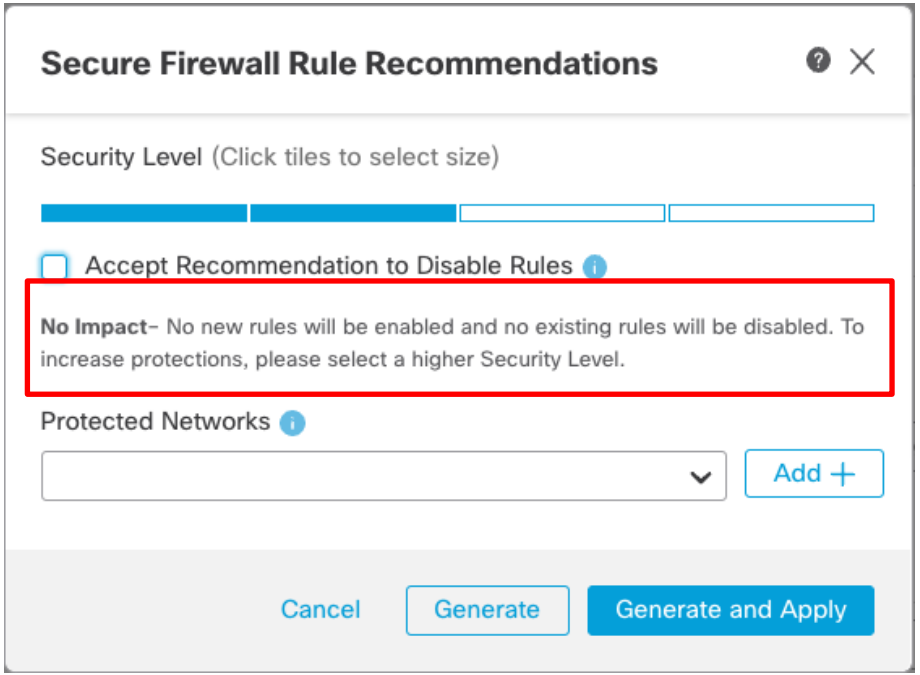
Goals

Why might you use Recommendations?

- Increased Protection – Expand my current rule set to address more threats/vulns
- Focused Protection – Trim the fat from my rule set while at the same time addressing additional threats
- High Efficiency – Performance is my key concern, I need to reduce the enabled rule count in an intelligent manner

Recommended Rules

Messages you might see



Recommended Rules

Messages you might see

Accept Recommendation to Disable Rules

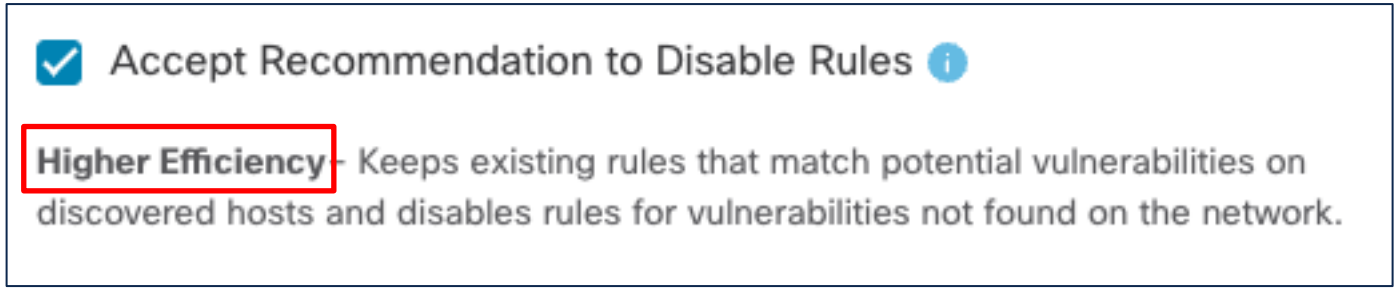
No Impact - No new rules will be enabled and no existing rules will be disabled. To increase protections, please select a higher Security Level.

You would see this if:

- Security level selected is the same as your base policy
- Disable is not checked

Recommended Rules

Messages you might see

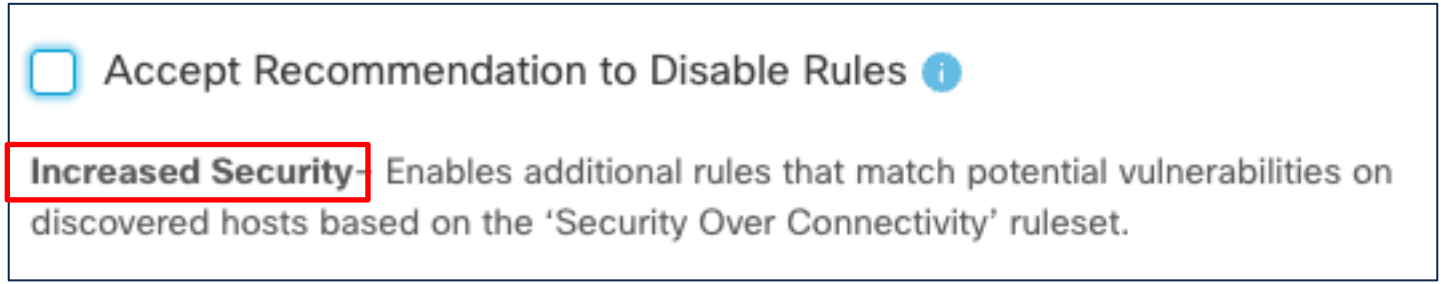


You would see this if:

- Security level selected is the same as your base policy
- Disable is checked

Recommended Rules

Messages you might see

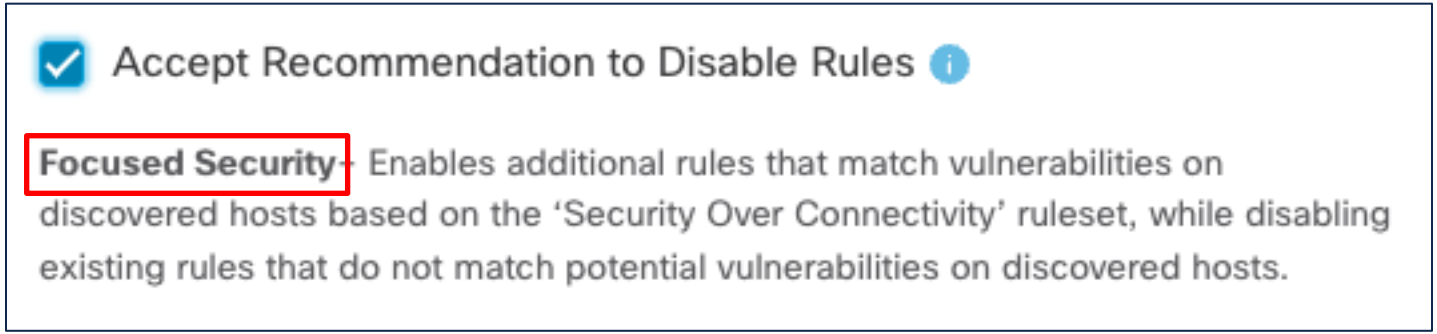


You would see this if:

- Security level selected is higher than your base policy
- Disable is not checked

Recommended Rules

Messages you might see

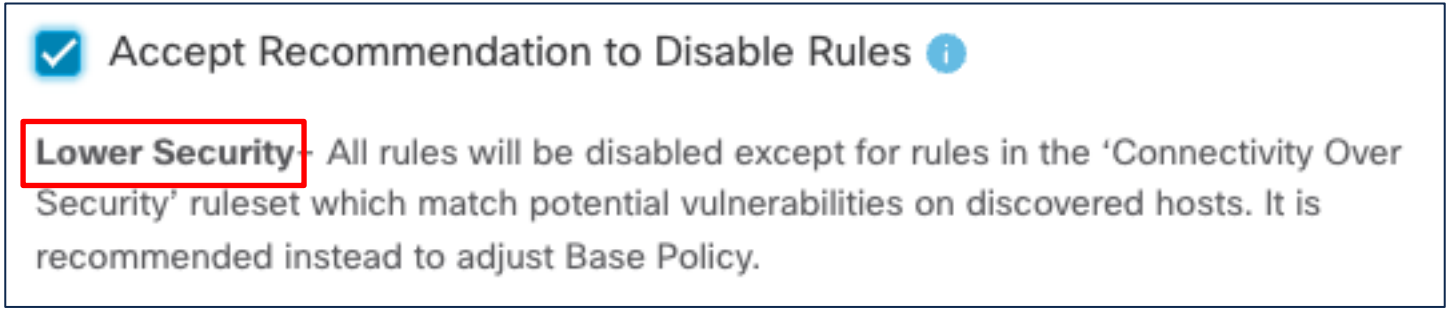


You would see this if:

- Security level selected is higher than your base policy
- Disable is checked

Recommended Rules

Messages you might see



You would see this if:

- Security level selected is lower than your base policy
- Disable is checked

Recommended Rules

Note: Policy delta messages only apply if using a Talos base policy. They might be incorrect if using a custom base policy.

Recommended Rules

Baseline policy rule counts*

Policy - Sec Level	Block	Alert	Total
Conn over Sec - 1	446	110	556
Balanced - 2	8,845	469	9,314
Sec over Conn - 3	19,473	648	20,121
Max Detect - 4	36,408	1,328	37,736

*LSP: 20220412-1306

What to Expect?

Lab network results – your mileage will vary

Block	Alert	Total	Setting
8,845	469	9,314	Starting policy*
5,783	233	6,016	Higher Efficiency
16,508	533	17,041	Increased Security
12,999	296	13,295	Focused Security
343	50	393	Lower Security

*Balanced – Security Level 2

Before Taking the Plunge

Important considerations prior to implementing

- Accurate host data is key to the operation of this feature
- You must have quality discovery data
- To build an accurate host profile, devices should have visibility to East/West as well as North/South flows

Rules Language

Snort 3 Change Summary

- Snort 3 rules are easier to read, write, and verify
- Consistent use of , and ;
- Use service matching criteria
- Header nets and ports optional
- Additional rule actions
- More sticky buffers
- New buffers and other rule options
- snort2lua converts 2.9 rules to 3.x format to ease adoption

Inconsistent syntax

Comma and Semicolon

Snort 2:

```
flow:to_server, established;
byte_test:1,!,!128,4,relative;
content:"evil"; offset:5; depth:4; nocase; http_uri;
```

- Sometimes parameters are comma separated
- Sometimes they use semicolons

Consistent syntax

Comma and Semicolon

Snort 3:

```
flow:to_server, established;
byte_test:1,&,128,4,relative;
content:"evil", offset 5, depth 4, nocase;
```

- Comma always used for parameters
- Semicolon always separates keywords
- Colon used only for keyword rather than within parameter

Rule Header

Traditional header still supported

```
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any
(msg:"Snort 2 vs. evil"; flow:to_client,established;
content:"evil"; nocase; metadata: service http;
classtype:attempted-user; sid:1000000;)
```

Protocol

Rule Header

Traditional header still supported

```
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any
(msg:”Snort 2 vs. evil"; flow:to_client,established;
content:"evil"; nocase; metadata: service http;
classtype:attempted-user; sid:1000000;)
```

IP address

Rule Header

Traditional header still supported

```
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any
(msg:”Snort 2 vs. evil"; flow:to_client,established;
content:"evil"; nocase; metadata: service http;
classtype:attempted-user; sid:1000000;)
```

Port

Rule Header

Header IP/ports are now optional

```
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any
(msg:”Snort 2 vs. evil"; flow:to_client,established;
content:"evil"; nocase; metadata: service http;
classtype:attempted-user; sid:1000000;)
```

```
alert http
(msg:”Snort 3 Evil HTTP";
flow:to_client,established;
content:"evil",nocase;
classtype:attempted-user; sid:1000000;)
```

Rule Actions

- `Pass` – Stop evaluating subsequent rules against packet
- `Alert` – generate event only
- `Block` – drop packet, block remaining session
- `Drop` – drop packet only
- `Rewrite` – required if “replace” option is used
- `Reject` – inject TCP RST or ICMP unreachable
- `React` – send HTML block response page

Sticky Buffers

- http_uri
- http_raw_uri
- http_header
- http_raw_header
- http_trailer
- http_raw_trailer
- http_cookie
- http_raw_cookie
- http_true_ip
- http_client_body
- http_raw_body
- http_method
- http_stat_code
- http_stat_msg
- http_version
- http2_frame_header
- file_data*
- script_data
- pkt_data*
- raw_data

* Snort 2 sticky keywords

Narrowing the Search

- Some sticky buffers have additional options
- Improves speed and accuracy
- `http_header: field content-language;`
  - Narrows search to the Content-Language field of the header
  - Any header field can be used
- `http_uri: path;`
  - Narrows search to just path portion of the URI

Rem Keyword

Comments within rules

```
alert tcp $EXTERNAL_NET any -> $SMTP_SERVERS 25
( msg:"BROWSER-FIREFOX Mozilla Firefox
Array.prototype.pop type confusion attempt";
flow:to_server,established;
file_data;
content:"={}|3B|";
rem:“Put comments in the rule anywhere”;
content:".__proto__=[",distance 0;
content:".__proto__=",distance 0;
content:".pop()|3B|";
service:smtp;
classtype:attempted-user; sid:57181; rev:1; )
```

Appids Keyword

Thousands of applications now available in Snort rules

```
alert tcp $HOME_NET any -> $EXTERNAL_NET any
( msg:"Alert on the Googles";
appids:”Google,Google Drive,Google App Engine”;
sid:1100003;
rev: 1;)
```

More Keyword Examples

- Hyperscan enabled pcre:
  - `regex`
- Sensitive Data Filtering:
  - `sd_pattern`
- IEC104 Inspector:
  - `iec104_apci_type`
  - `iec104_asdu_func`

Additional Information

- Secure Firewall YouTube Channel
  - https://www.youtube.com/cisco-netsec
- Secure Firewall Essentials Hub
  - https://secure.cisco.com/secure-firewall
- Snort.org
  - https://www.snort.org/

Cisco Security Beta Programs

Sign-Up Now:
http://cs.co/clive-security-beta

"I've been involved in many beta programs…I must say that this one has been the best organized. This beta takes a very active, hands-on approach."
Higher-Ed Beta Customer

Early Feedback Programs

Beta Software Access

Product Training

Influence Product Roadmap

CISCO SECURE

Security Reference Architecture

TALOS — Threat Intelligence | Malware Analytics | Actionable Intelligence | Unmatched Visibility | Collective Responses

Security Operations

SECURE X (XDR)

- Managed Detection and Response Services
- Security, Orchestration, Automation and Response
- Incident Response and Remediation Services
- Threat Visibility & Hunting
- Device Insights
- Kenna Vuln Mgmt
- Secure Cloud Insights
- 3rd Party Integrations

User/Device Security

ZERO TRUST

Adaptive MFA | Passwordless | Trust

Duo Secure Access

Secure E-mail

SASE/REMOTE WORKER

Unified Client | EDR | Cloud Managed

Cisco Secure Client

- VPN
- Posture
- Telemetry
- Threat
- Query

ThousandEyes (Visibility)

Device Mgmt: Meraki SM OS, App Control

Network Security

Cloud Edge

SECURE ACCESS SERVICE EDGE (SASE) | **ZERO TRUST**

Threat Protection | Secure Access Control | Managed Remote Access

PRIVATE CLOUD EDGE (MSP or CUSTOMER)

Reliable | Scalable | Flexible

Umbrella/Duo

- ZTNA
- DNS-layer security
- Secure web gateway
- L7 firewall + IPS
- Cloud access security broker/ shadow IT
- RAaaS
- SSL decryption
- Remote browser Isolation
- Data loss prevention
- Cloud malware detection

SDWAN

- Meraki SDWAN
- SDWAN by Viptela
- Secure Firewall
- ThousandEyes
- Cloud DDoS,WAF

On-Premises

SASE/SDWAN

Scalable | Flexible | Visibility | Comprehensive Security

Network Edge

- Meraki SDWAN
- SDWAN by Viptela
- Secure Firewall
- ThousandEyes

IoT/OT SECURITY

Secure Critical Infrastructure | Unified IT and OT

- Industrial Router
- Industrial Firewall
- Industrial Switch/AP
- Cyber Vision
- ISE TrustSec

ZERO TRUST

Segmentation | Identity and Context | Profiling | Containment | Encrypted Visibility

- Security Analytics and Logging
- Secure Firewall
- DuoCloud SSO+IDP
- Network Gateway
- Secure DDoS
- Meraki Full Stack
- Secure Network Analytics
- Secure Web Appliance
- ISE TrustSec
- Cisco DNA Center

Application Security

ZERO TRUST

Policy | API Security
Application Segmentation
Run-time Application Security

Application Security Stack

- Cloud Native Security
- APIC
- Secure Workload
- Secure Application by AppDynamics

App Observability | Detection | Response

- Hybrid Private
- Public Cloud
- Secure Cloud Analytics
- Secure Firewall
- ThousandEyes
- Secure DDoS, WAF/Bot

Cisco Learning and Certifications

From technology training and team development to Cisco certifications and learning plans, let us help you empower your business and career. www.cisco.com/go/certs

Pay for Learning with Cisco Learning Credits

(CLCs) are prepaid training vouchers redeemed directly with Cisco.

Learn

Cisco U.
IT learning hub that guides teams and learners toward their goals

Cisco Digital Learning
Subscription-based product, technology, and certification training

Cisco Modeling Labs
Network simulation platform for design, testing, and troubleshooting

Cisco Learning Network
Resource community portal for certifications and learning

Train

Cisco Training Bootcamps
Intensive team & individual automation and technology training programs

Cisco Learning Partner Program
Authorized training partners supporting Cisco technology and career certifications

Cisco Instructor-led and Virtual Instructor-led training
Accelerated curriculum of product, technology, and certification courses

Certify

Cisco Certifications and Specialist Certifications
Award-winning certification program empowers students and IT Professionals to advance their technical careers

Cisco Guided Study Groups
180-day certification prep program with learning and support

Cisco Continuing Education Program
Recertification training options for Cisco certified individuals

Here at the event? Visit us at **The Learning and Certifications lounge at the World of Solutions**

Technical Session Surveys

- Attendees who fill out a minimum of four session surveys and the overall event survey will get Cisco Live branded socks!
- 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

Thank you

cisco Live!

ALL IN

#CiscoLive