CISCO Live!

#CiscoLive

The bridge to possible

Snort2 to Snort3 Rule Migration

Raghunath Kulkarni – Sr. Technical Leader CX

BRKSEC-2083

Agenda

- Intrusion Basics
- Rule Actions
- Intrusion Policy UI Elements
- Custom Rule Migration
- Rule Recommendations
- Conclusion

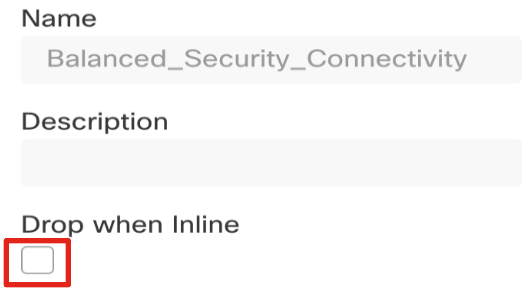
Intrusion Basics

Intrusion Basics

- Intrusion Detection
  - Passively monitor the network traffic
  - Generate alerts for potential intrusion
  - Known as Intrusion Detection Systems (IDS)

- Intrusion Prevention
  - IDS + Ability to block traffic
  - Known as Intrusion Prevention Systems (IPS)

Inspection Modes



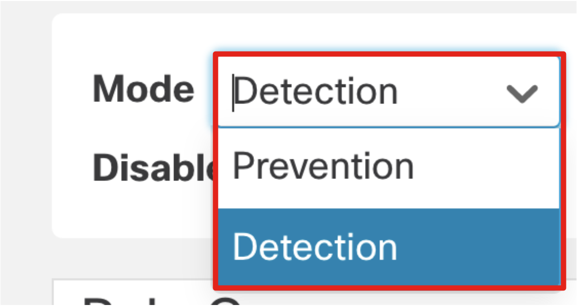
Name

Balanced_Security_Connectivity

Description

Drop when Inline

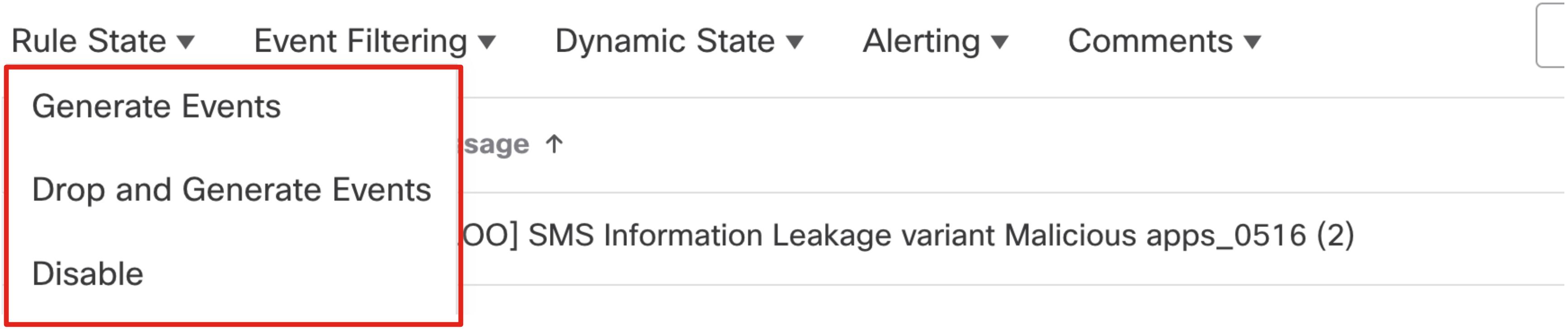
□



Mode: Detection

Rule Actions

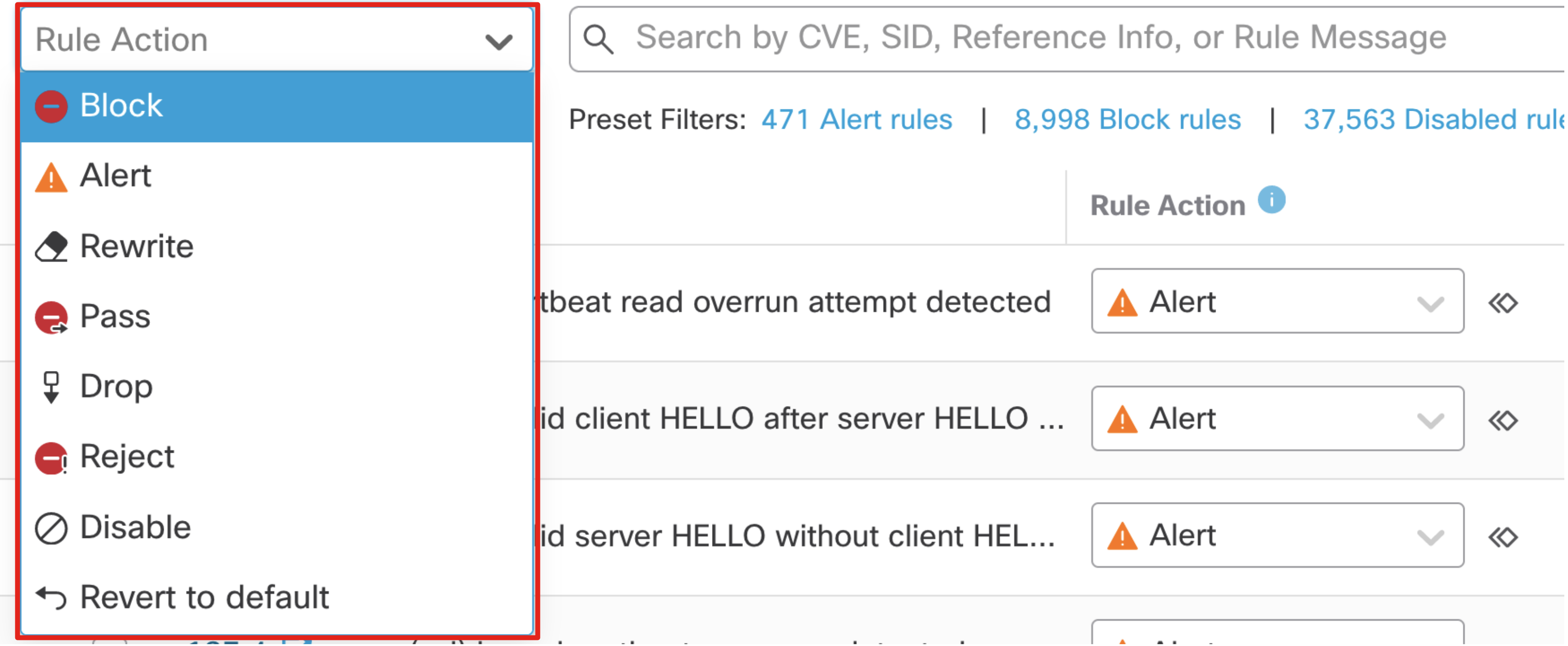
Rule Actions from UI - Snort2 (1/4)



OO] SMS Information Leakage variant Malicious apps_0516 (2)

- Generate Events: Detect and Notify through event. Does not drop the offending packet
- Drop & Generate Events: Detect, Drop and notify through event
- Disable: The rule is disabled for evaluation

Rule Actions from UI – Snort3 (2/4)



Rule Action

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

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

Preset Filters: 471 Alert rules | 8,998 Block rules | 37,563 Disabled rul

	Rule Action
tbeat read overrun attempt detected	Alert
id client HELLO after server HELLO ...	Alert
id server HELLO without client HEL...	Alert

Rule Actions from UI – Snort3 (3/4)

- Pass: Stop evaluating subsequent rules against the packet.
- Alert: Generate event only.
- Block: Drop the packet & Block remaining session.
- Drop: Drop the packet only.
- Rewrite: Required if "replace" option is used in signature/rule.
- Reject: Inject TCP RST or ICMP Unreachable
- Disable: The rule is disabled for evaluation.

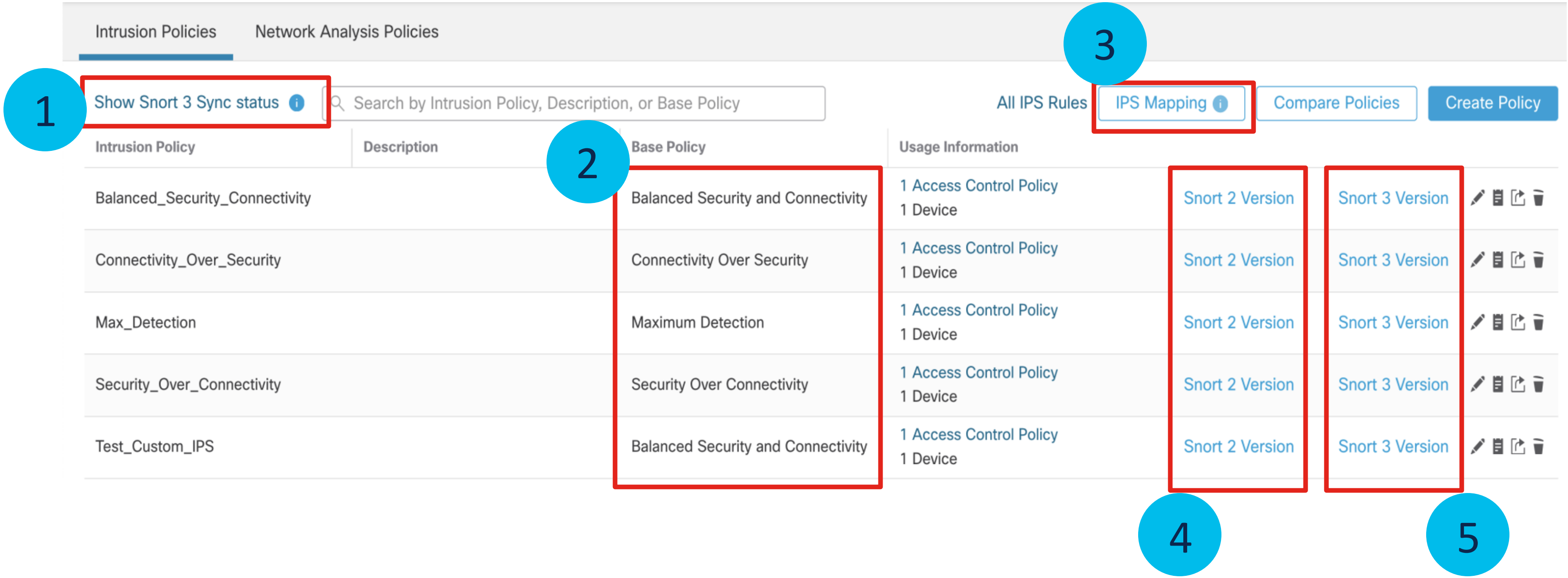
Snort2 vs Snort3 Rule (4/4)

```
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"BLACKLIST URI request for
known malicious URI"; flow:established,to_server; content:"/setup_b.asp?prj="; nocase;
http_uri; content:"&pid="; nocase; http_uri; content:"&mac="; nocase; http_uri;
pcre:"/\/setup_b\.asp\?prj=\d\x26pid=[^\r\n]*\x26mac=/Ui"; metadata:service http;
sid:19626; rev:2;)
```

```
alert http
(
    msg:"BLACKLIST URI request for known malicious URI";
    flow:established,to_server;
    http_uri;
    regex:"/setup_b\.asp\?prj=\d&pid=.*&mac=", nocase, fast_pattern;
    sid:19626; rev:4;
)
```

Intrusion Policy UI Elements

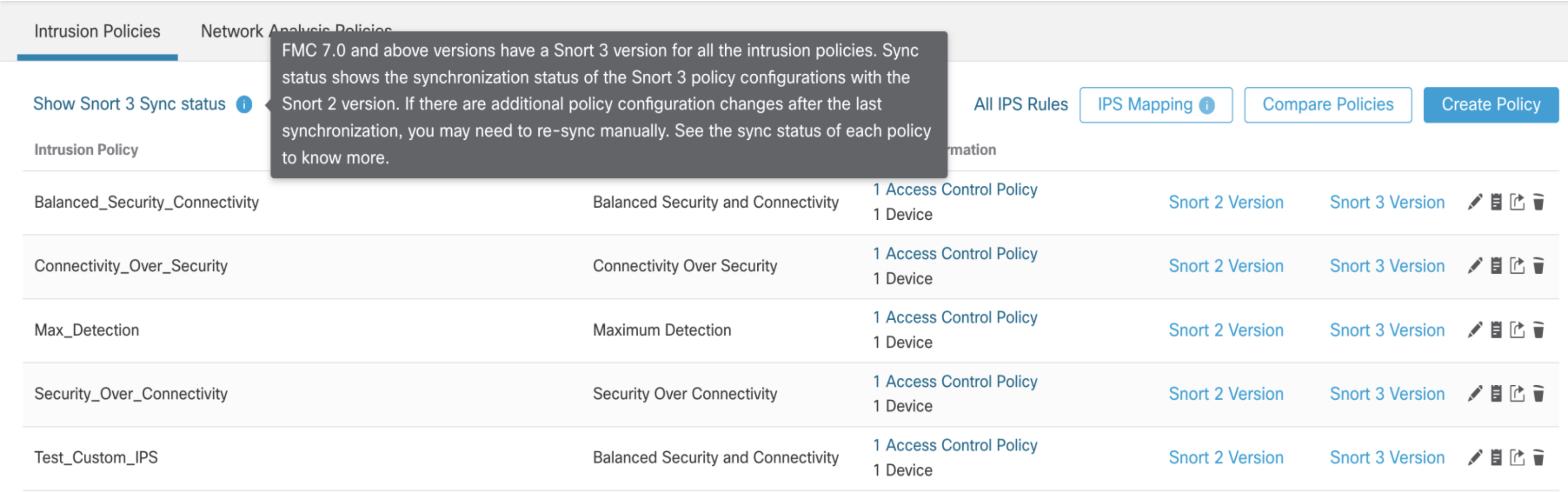
Intrusion Policy UI (1/7)



Intrusion Policy	Description	Base Policy	Usage Information		
Balanced_Security_Connectivity		Balanced Security and Connectivity	1 Access Control Policy 1 Device	Snort 2 Version	Snort 3 Version
Connectivity_Over_Security		Connectivity Over Security	1 Access Control Policy 1 Device	Snort 2 Version	Snort 3 Version
Max_Detection		Maximum Detection	1 Access Control Policy 1 Device	Snort 2 Version	Snort 3 Version
Security_Over_Connectivity		Security Over Connectivity	1 Access Control Policy 1 Device	Snort 2 Version	Snort 3 Version
Test_Custom_IPS		Balanced Security and Connectivity	1 Access Control Policy 1 Device	Snort 2 Version	Snort 3 Version

Intrusion Policy UI (2/7)

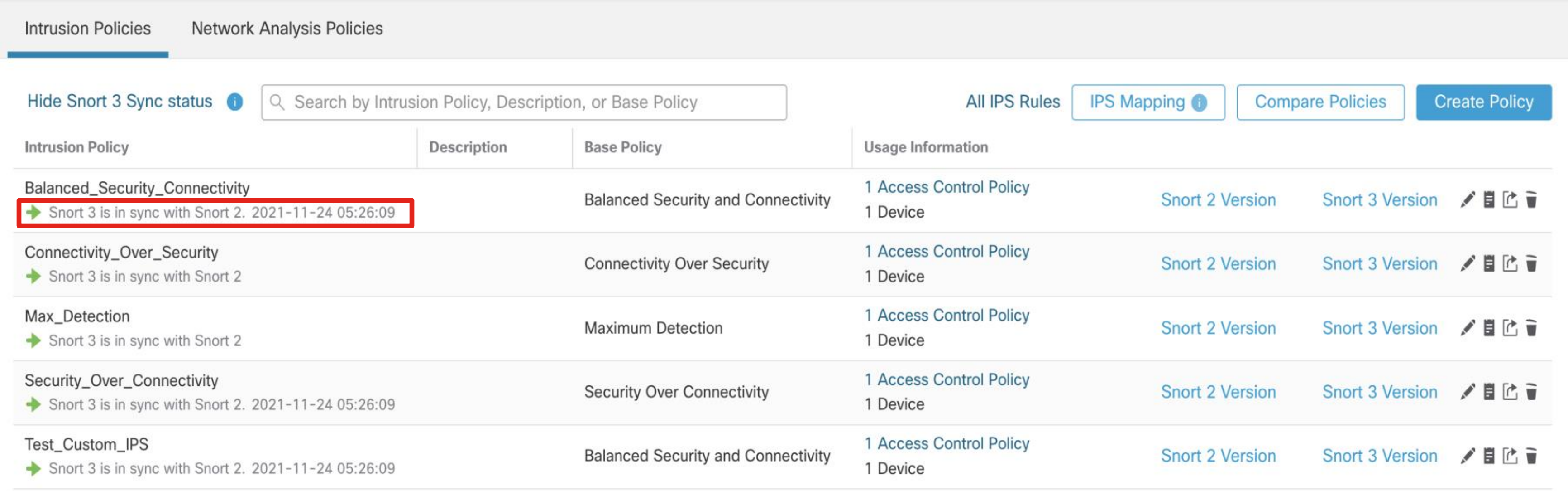
1



FMC 7.0 and above versions have a Snort 3 version for all the intrusion policies. Sync status shows the synchronization status of the Snort 3 policy configurations with the Snort 2 version. If there are additional policy configuration changes after the last synchronization, you may need to re-sync manually. See the sync status of each policy to know more.

Intrusion Policy		rmation		
Balanced_Security_Connectivity	Balanced Security and Connectivity	1 Access Control Policy 1 Device	Snort 2 Version	Snort 3 Version
Connectivity_Over_Security	Connectivity Over Security	1 Access Control Policy 1 Device	Snort 2 Version	Snort 3 Version
Max_Detection	Maximum Detection	1 Access Control Policy 1 Device	Snort 2 Version	Snort 3 Version
Security_Over_Connectivity	Security Over Connectivity	1 Access Control Policy 1 Device	Snort 2 Version	Snort 3 Version
Test_Custom_IPS	Balanced Security and Connectivity	1 Access Control Policy 1 Device	Snort 2 Version	Snort 3 Version

Intrusion Policy UI (3/7)

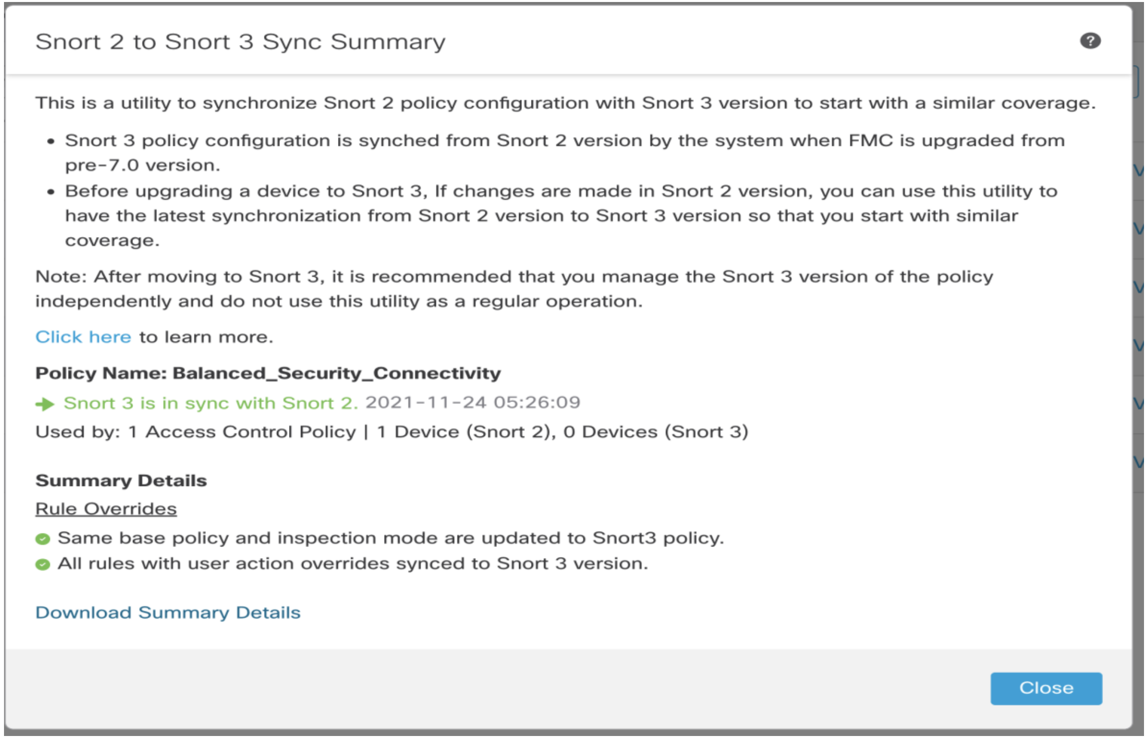


Intrusion Policies   Network Analysis Policies

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_Security_Connectivity ➜ Snort 3 is in sync with Snort 2. 2021-11-24 05:26:09		Balanced Security and Connectivity	1 Access Control Policy 1 Device	Snort 2 Version	Snort 3 Version
Connectivity_Over_Security ➜ Snort 3 is in sync with Snort 2		Connectivity Over Security	1 Access Control Policy 1 Device	Snort 2 Version	Snort 3 Version
Max_Detection ➜ Snort 3 is in sync with Snort 2		Maximum Detection	1 Access Control Policy 1 Device	Snort 2 Version	Snort 3 Version
Security_Over_Connectivity ➜ Snort 3 is in sync with Snort 2. 2021-11-24 05:26:09		Security Over Connectivity	1 Access Control Policy 1 Device	Snort 2 Version	Snort 3 Version
Test_Custom_IPS ➜ Snort 3 is in sync with Snort 2. 2021-11-24 05:26:09		Balanced Security and Connectivity	1 Access Control Policy 1 Device	Snort 2 Version	Snort 3 Version

Intrusion Policy UI (4/7)



Snort 2 to Snort 3 Sync Summary

This is a utility to synchronize Snort 2 policy configuration with Snort 3 version to start with a similar coverage.

- Snort 3 policy configuration is synched from Snort 2 version by the system when FMC is upgraded from pre-7.0 version.
- Before upgrading a device to Snort 3, If changes are made in Snort 2 version, you can use this utility to have the latest synchronization from Snort 2 version to Snort 3 version so that you start with similar coverage.

Note: After moving to Snort 3, it is recommended that you manage the Snort 3 version of the policy independently and do not use this utility as a regular operation.

Click here to learn more.

Policy Name: Balanced_Security_Connectivity

➜ Snort 3 is in sync with Snort 2. 2021-11-24 05:26:09

Used by: 1 Access Control Policy | 1 Device (Snort 2), 0 Devices (Snort 3)

Summary Details

Rule Overrides

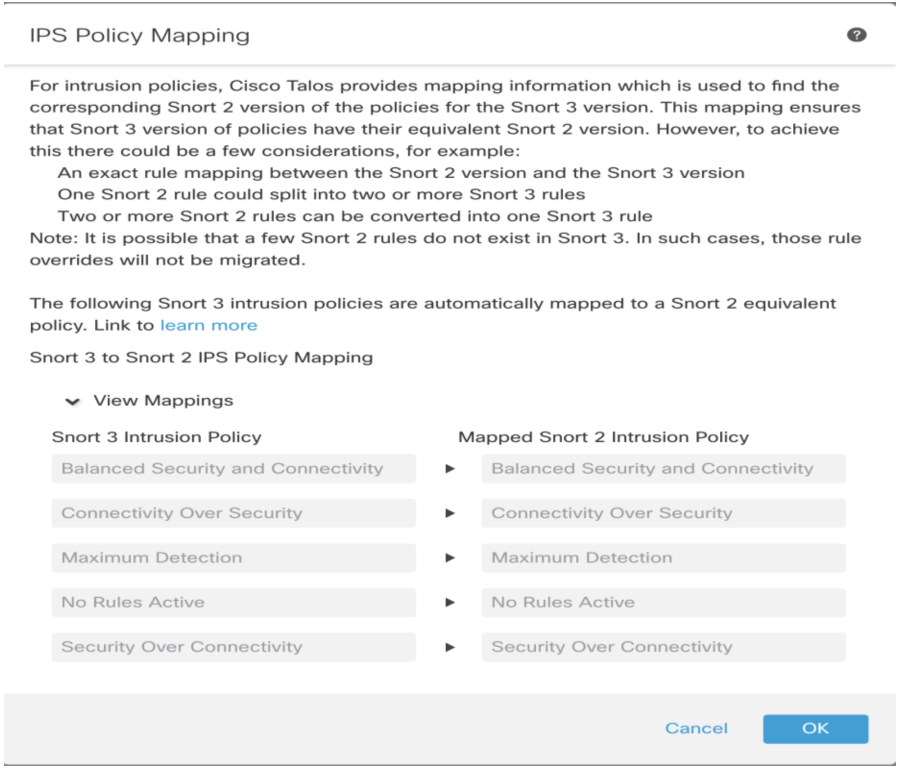
✓ Same base policy and inspection mode are updated to Snort3 policy.

✓ All rules with user action overrides synced to Snort 3 version.

Download Summary Details

Intrusion Policy UI (5/7)

2 3



IPS Policy Mapping

For intrusion policies, Cisco Talos provides mapping information which is used to find the corresponding Snort 2 version of the policies for the Snort 3 version. This mapping ensures that Snort 3 version of policies have their equivalent Snort 2 version. However, to achieve this there could be a few considerations, for example:

An exact rule mapping between the Snort 2 version and the Snort 3 version
One Snort 2 rule could split into two or more Snort 3 rules
Two or more Snort 2 rules can be converted into one Snort 3 rule

Note: It is possible that a few Snort 2 rules do not exist in Snort 3. In such cases, those rule overrides will not be migrated.

The following Snort 3 intrusion policies are automatically mapped to a Snort 2 equivalent policy. Link to learn more

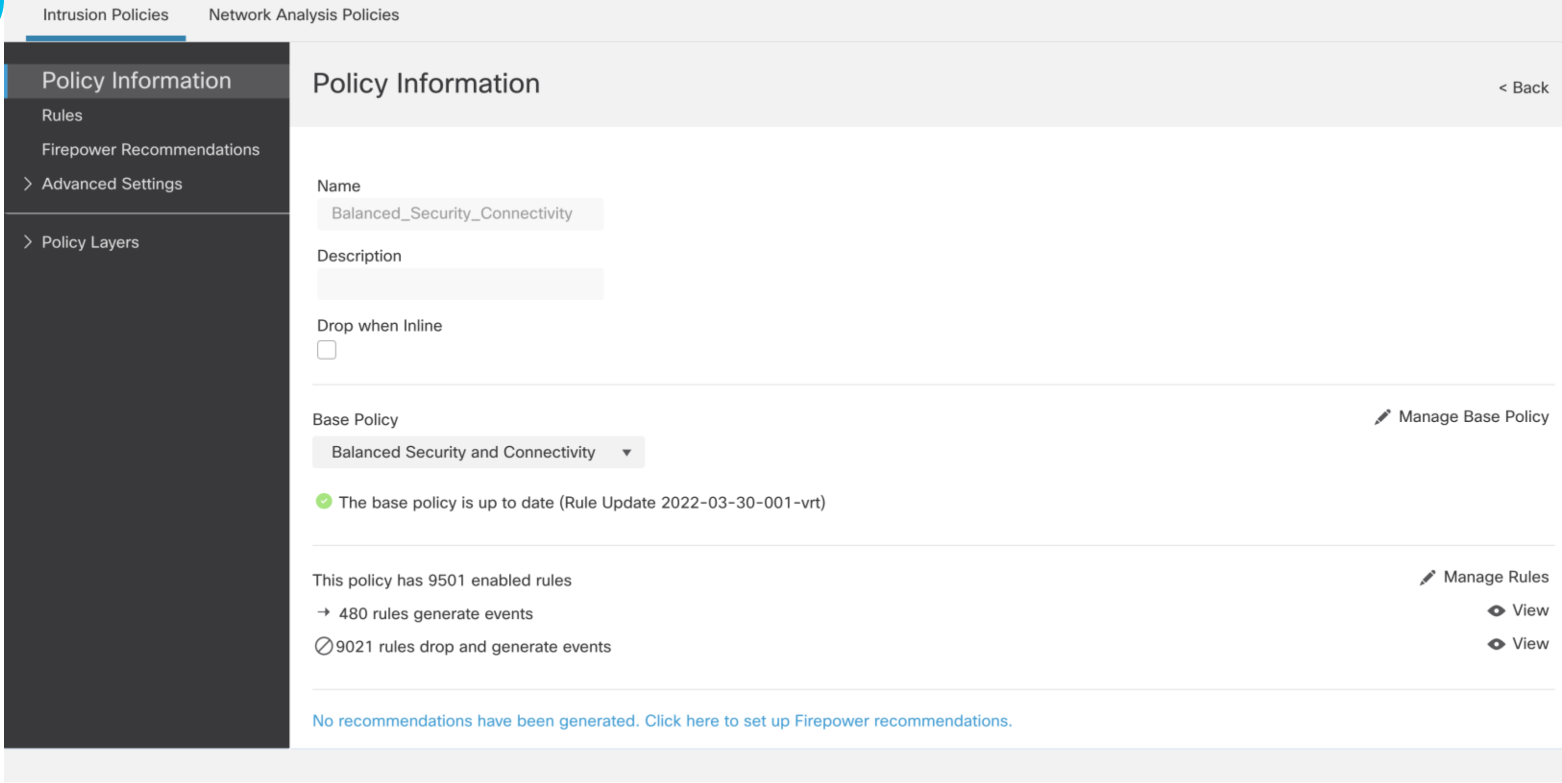
Snort 3 to Snort 2 IPS Policy Mapping

View Mappings

Snort 3 Intrusion Policy		Mapped Snort 2 Intrusion Policy
Balanced Security and Connectivity	▶	Balanced Security and Connectivity
Connectivity Over Security	▶	Connectivity Over Security
Maximum Detection	▶	Maximum Detection
No Rules Active	▶	No Rules Active
Security Over Connectivity	▶	Security Over Connectivity

Intrusion Policy UI (6/7)

4



Policy Information

Name

Balanced_Security_Connectivity

Description

Drop when Inline

□

Base Policy

Balanced Security and Connectivity ▼

Manage Base Policy

✓ The base policy is up to date (Rule Update 2022-03-30-001-vrt)

This policy has 9501 enabled rules

Manage Rules

→ 480 rules generate events

View

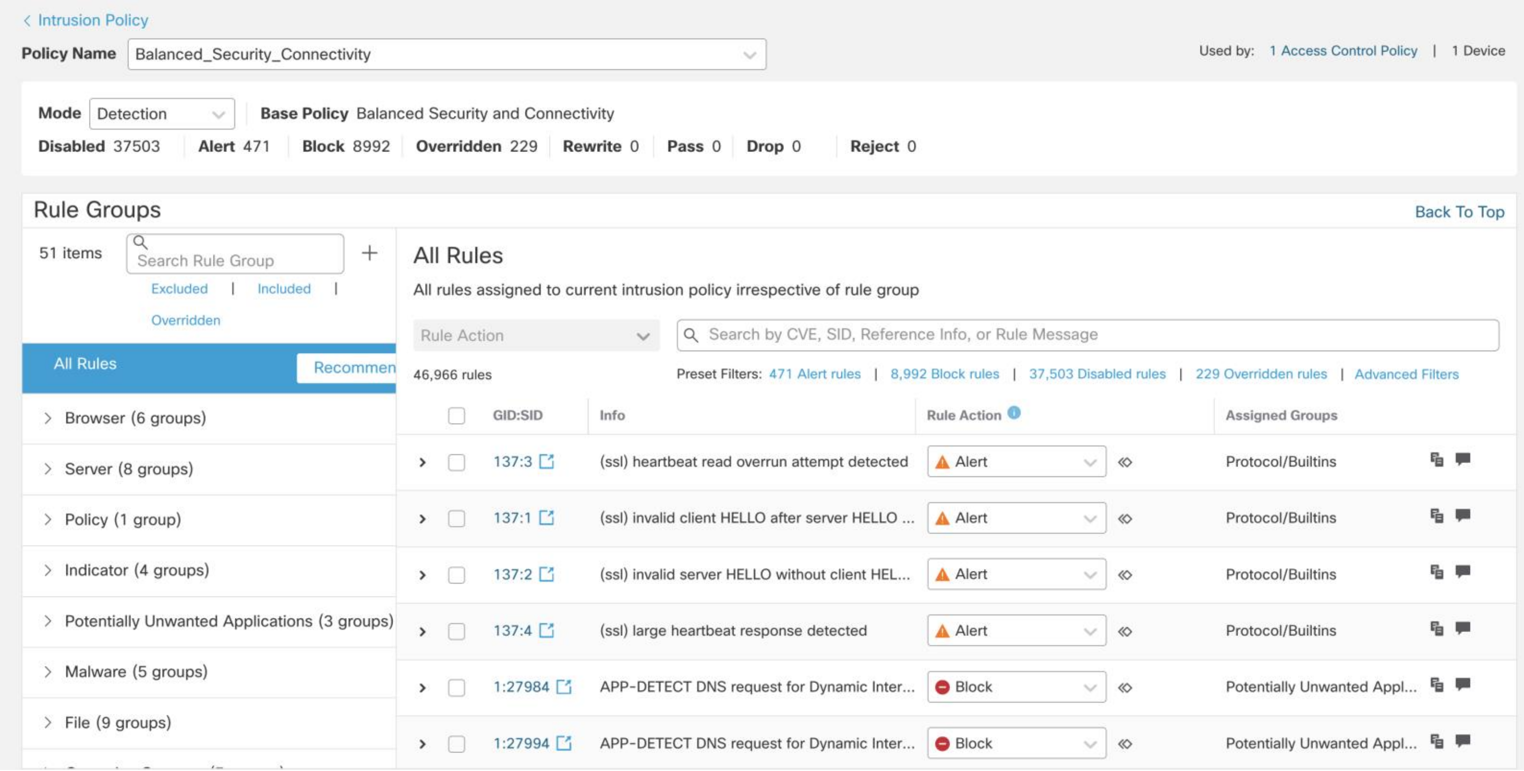
⊘ 9021 rules drop and generate events

View

No recommendations have been generated. Click here to set up Firepower recommendations.

Intrusion Policy UI (7/7)

5



< Intrusion Policy

Policy Name Balanced_Security_Connectivity

Used by: 1 Access Control Policy | 1 Device

Mode Detection **Base Policy** Balanced Security and Connectivity

Disabled 37503 **Alert** 471 **Block** 8992 **Overridden** 229 **Rewrite** 0 **Pass** 0 **Drop** 0 **Reject** 0

Rule Groups

Back To Top

51 items

Search Rule Group

Excluded | Included | Overridden

- All Rules
- Recommen
- Browser (6 groups)
- Server (8 groups)
- Policy (1 group)
- Indicator (4 groups)
- Potentially Unwanted Applications (3 groups)
- Malware (5 groups)
- File (9 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

46,966 rules

Preset Filters: 471 Alert rules | 8,992 Block rules | 37,503 Disabled rules | 229 Overridden rules | Advanced Filters

GID:SID	Info	Rule Action	Assigned Groups
137:3	(ssl) heartbeat read overrun attempt detected	Alert	Protocol/Builtins
137:1	(ssl) invalid client HELLO after server HELLO ...	Alert	Protocol/Builtins
137:2	(ssl) invalid server HELLO without client HEL...	Alert	Protocol/Builtins
137:4	(ssl) large heartbeat response detected	Alert	Protocol/Builtins
1:27984	APP-DETECT DNS request for Dynamic Inter...	Block	Potentially Unwanted Appl...
1:27994	APP-DETECT DNS request for Dynamic Inter...	Block	Potentially Unwanted Appl...

Surprised

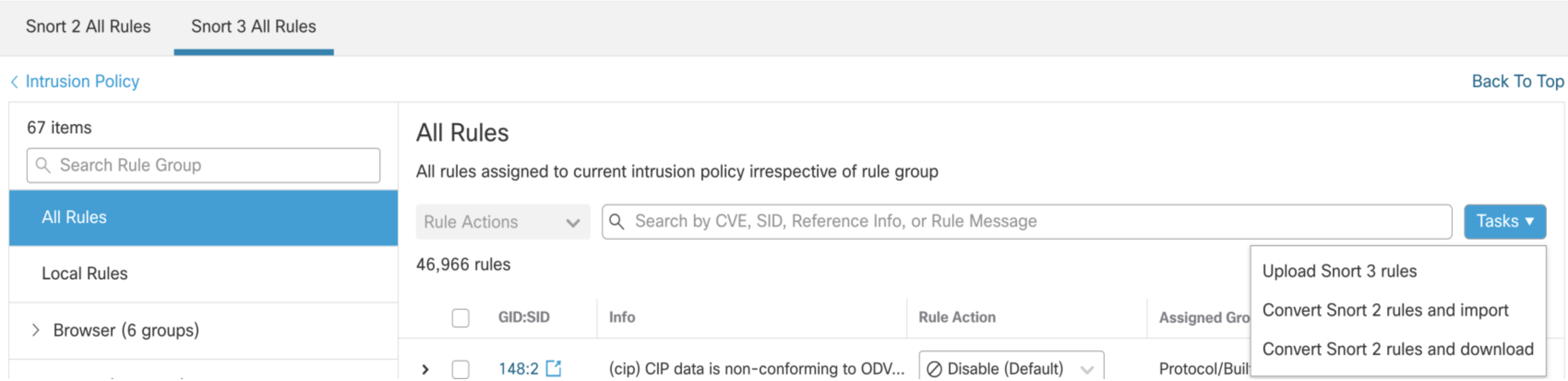
- Why is the sync shown only for some policies?

- Why is the sync date not current?

- Why do we maintain snort2 and snort3 version of IPS policies?

Custom Rules

Custom Rules Migration (1/2)



Snort 2 All Rules | Snort 3 All Rules

< Intrusion Policy

Back To Top

67 items

Search Rule Group

All Rules

Local Rules

> Browser (6 groups)

All Rules

All rules assigned to current intrusion policy irrespective of rule group

Rule Actions

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

Tasks ▾

- Upload Snort 3 rules
- Convert Snort 2 rules and import
- Convert Snort 2 rules and download

46,966 rules

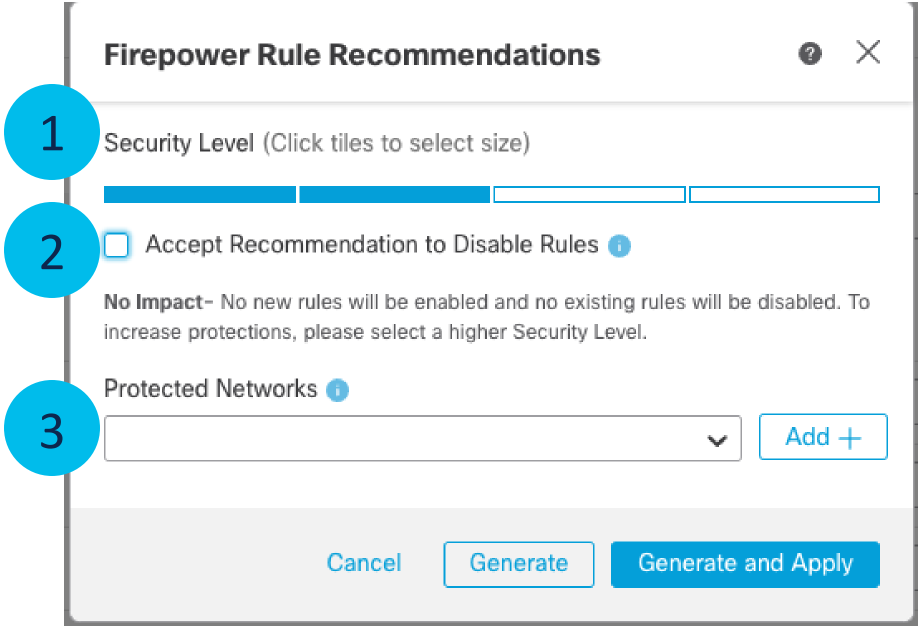
□	GID:SID	Info	Rule Action	Assigned Gro
> □	148:2	(cip) CIP data is non-conforming to ODV...	⊘ Disable (Default)	Protocol/Buil

Custom Rules Migration (2/2)

NEW
FIREWALL THREAT DEFENSE 7.0
COVERTING SNORT 2 RULES TO SNORT 3
CISCO
SECURE

Rule Recommendations

Rule Recommendations (1/4)



Firepower Rule Recommendations

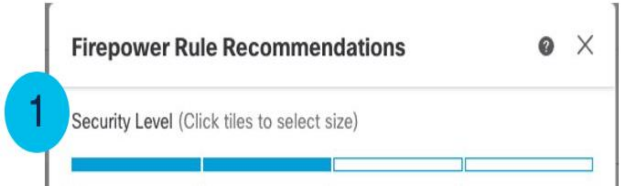
1 Security Level (Click tiles to select size)

2 □ 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.

3 Protected Networks

Rule Recommendations (2/4)

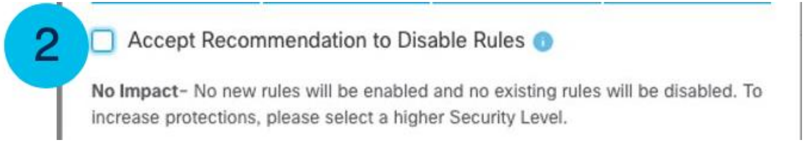


Firepower Rule Recommendations

Security Level (Click tiles to select size)

Lower Security	Disables all rules except ones in CoS that matches potential vulnerabilities from discovered hosts.
Higher Efficiency	Keep existing & Disable rules for vulnerabilities not applicable on discovered hosts.
Focused Security (1)	Increased security enables rules for vulnerabilities based on SoC on discovered hosts.
Focused Security (2)	Increased protection enables rules based on MD for discovered host. *May impact performance.

Rule Recommendations (3/4)

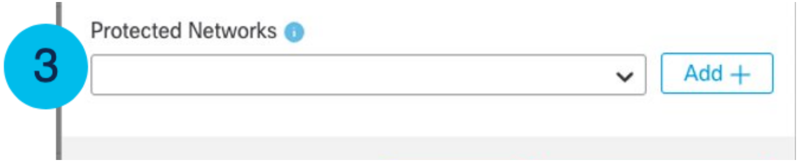


□ Accept Recommendation to Disable Rules

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

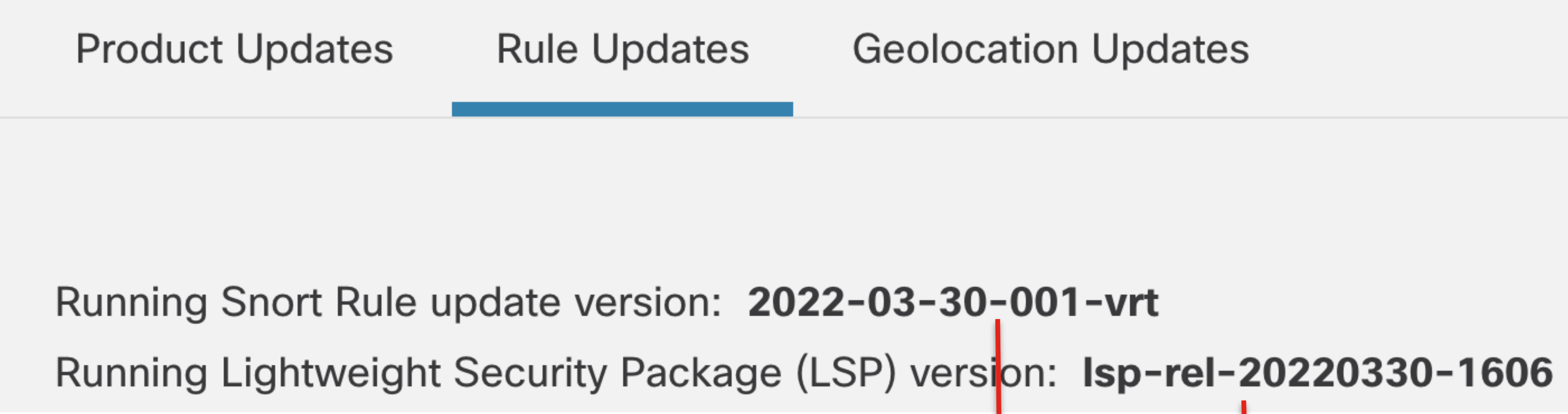
- Security Level matches the base policy or lower
- Accept Recommendation is disabled.
- No changes to existing rules

Rule Recommendations (4/4)



- Specify networks to monitor.
- Default value is Any (IPv4 + IPv6).
- Custom network objects can be chosen.

Intrusion Rule Updates



Running Snort Rule update version: **2022-03-30-001-vrt**

Running Lightweight Security Package (LSP) version: **lsp-rel-20220330-1606**

Snort2

Snort3

Conclusion

1. Exact rule mapping might not exist.
2. Migration is one way. (Snort2 to Snort3, not other way)
3. Synchronization does not migrate thresholds/suppressions.
4. Local rules to be migrated manually through built in tool.
5. Recommendations are not migrated

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!

#CiscoLive