CISCO

You make **possible**

Dissecting (FTD) Firepower Threat Defense

Architecture and troubleshooting

Veronika Klauzová
Technical Marketing Engineer

BRKSEC-3455

Barcelona | January 27-31, 2020

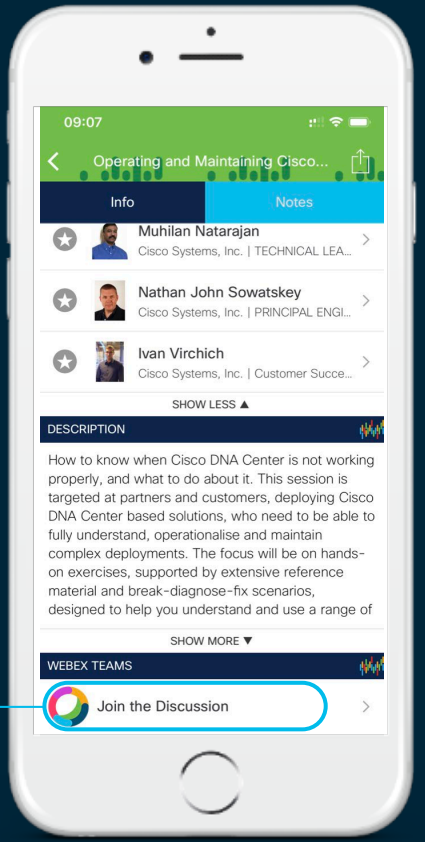
Cisco Webex Teams

Questions?

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

How

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



Agenda

- Introduction
  - Product and software update
- FTD Architecture
- NGFW Rule expansion and optimization
- Policy Deployment Architecture
- Day in the life of packet
  - Troubleshooting tools
  - Data-path and detection engine improvements
- FTD real-world stories
  - User stories

Abstract

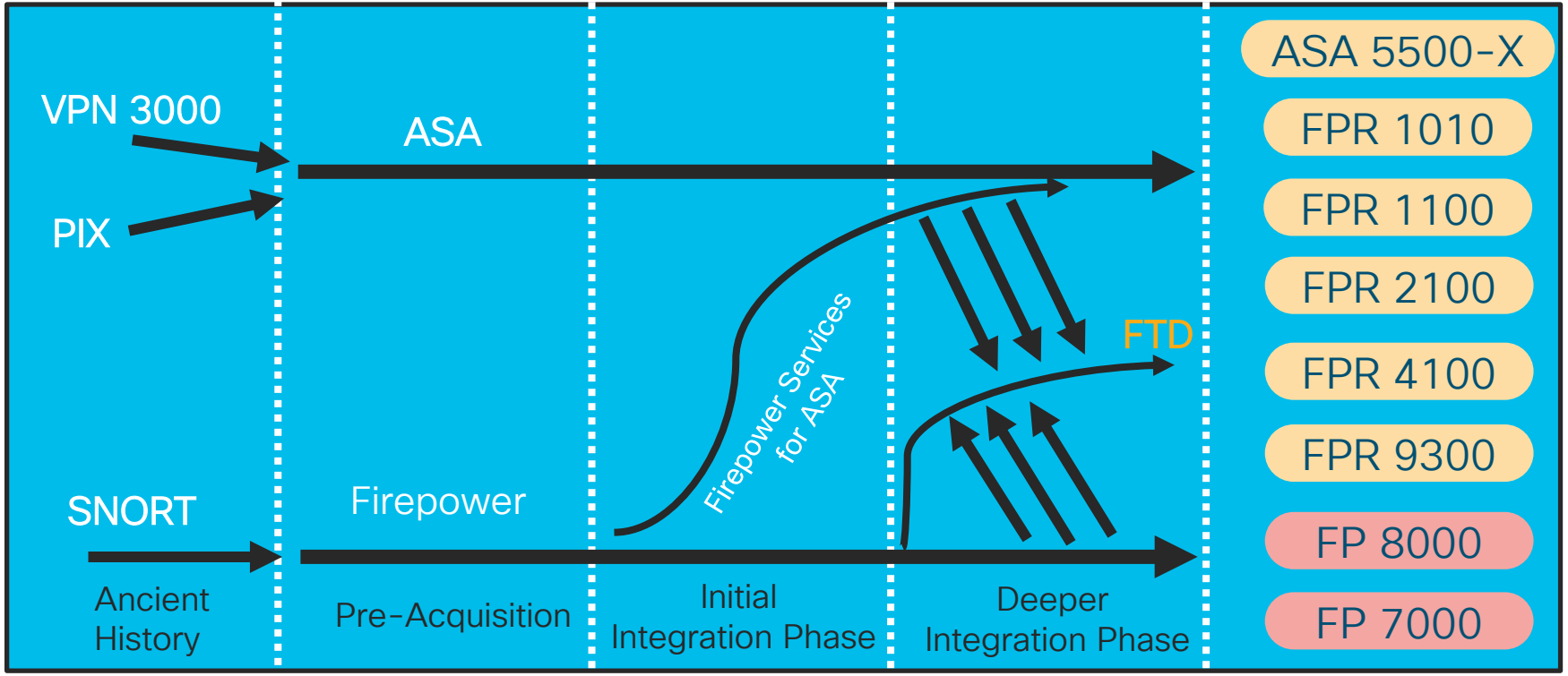
- The session will cover detailed Firepower Threat Defense (FTD) architecture, packet flow processing and troubleshooting. During session we will talk about product and software feature's updates in regards to data-path. In this session we will go through details and explain how to efficiently troubleshoot the NGFW platforms via commonly available tools. Last but not least, we are going to talk about the most interesting user stories that we have seen in real-world and what lessons we have learned.

Your presenter throughout this FTD journey

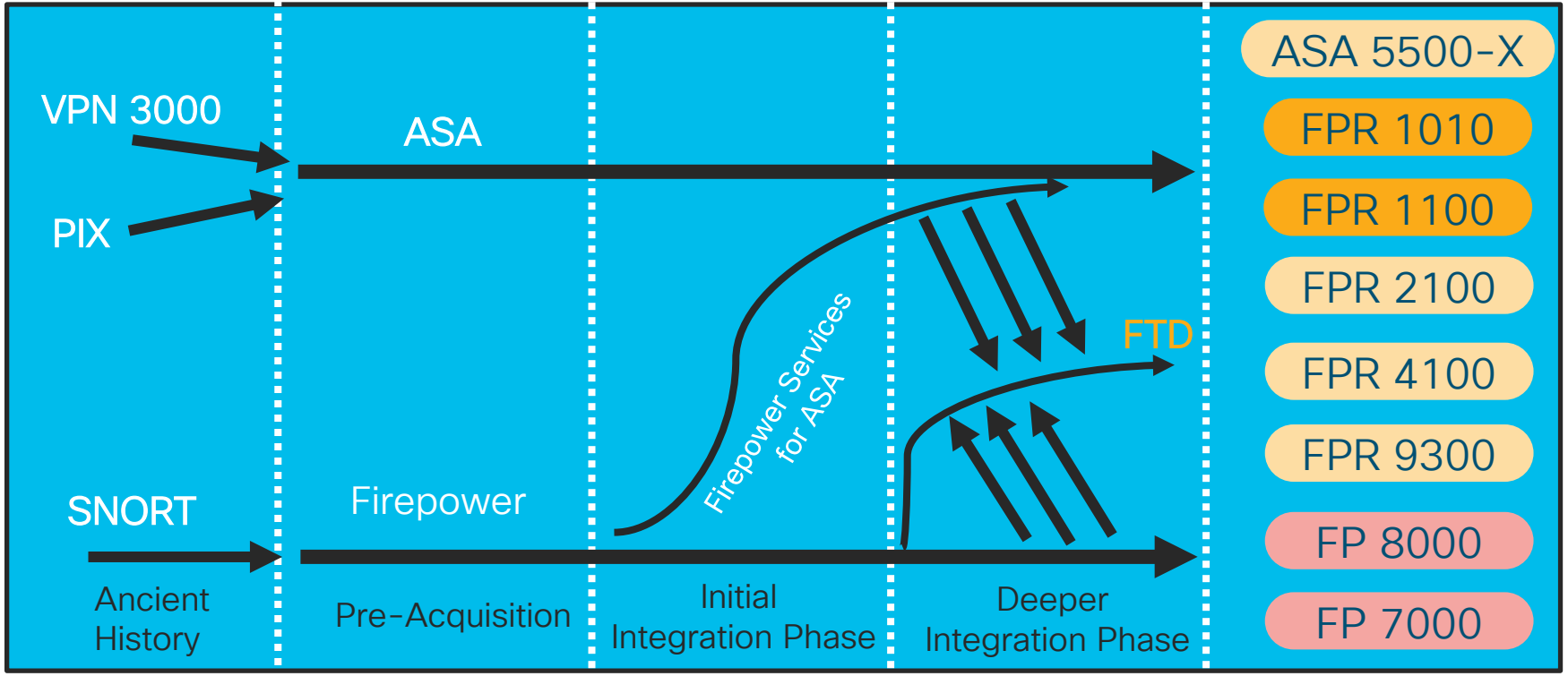
Veronika Klauzová

Product and Software Update

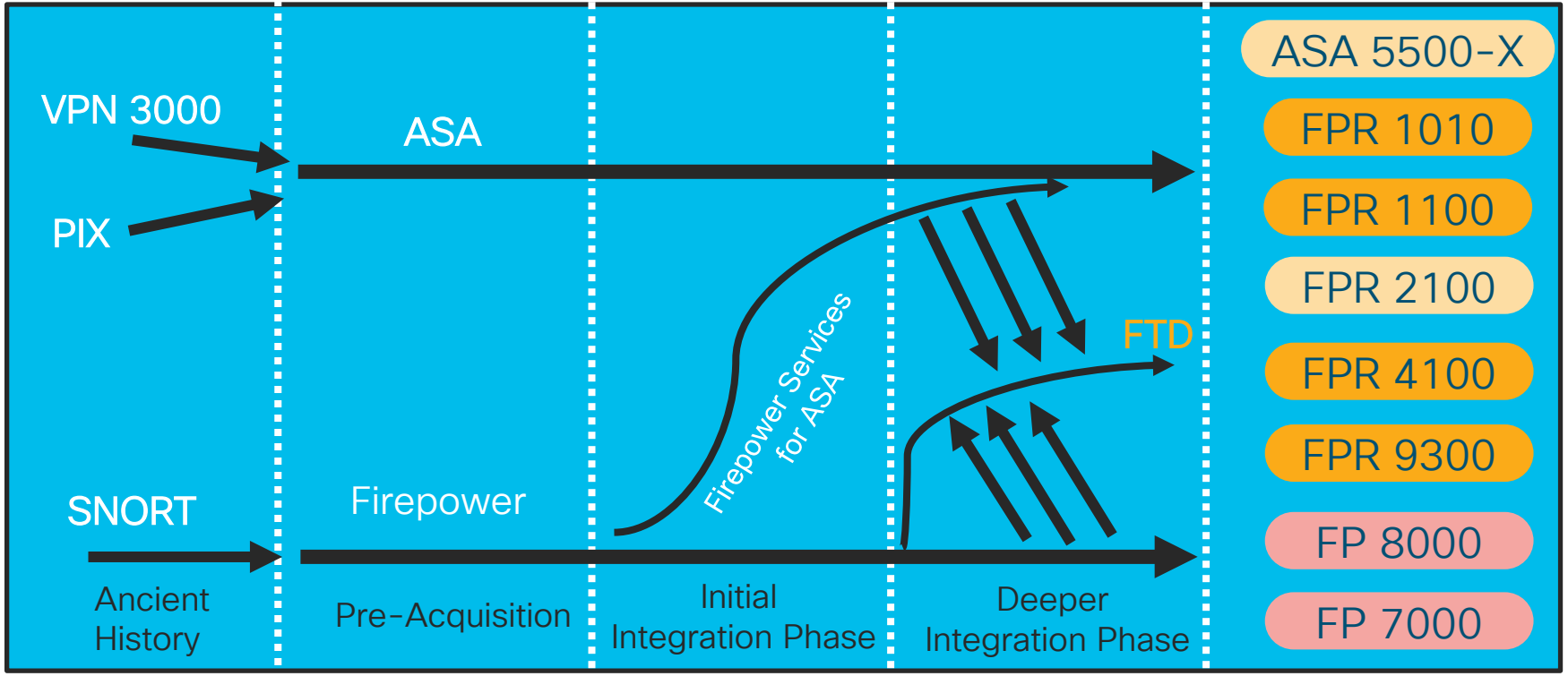
NGFW evolution



NGFW evolution



NGFW evolution



New Hardware – FPR 9300

Current		New Crypto SM's
SM-24	→	**SM-40** (384GB DDR4, 2x 1.6TB SSD)
SM-36	→	**SM-48** (384GB DDR4, 2x 1.6TB SSD)
SM-44	→	**SM-56** (384GB DDR4, 2x1.6TB SSD)

- Improved crypto performance for RAVPN / IPSec and TLS offload
- Allows to configure more instances with multi-instance capability
- Hardware refresh due to UCS M4 EoS, new blades will be M5 based
- All models supported with FTD 6.4 and FXOS 2.6.1

New Hardware – FPR 4100

New platform	Specs
FPR-4115 (PID: FPR4K-SM-24S)	24-core CPU, 192GB DDR4, 1x 400GB SSD
FPR-4125 (PID: FPR4K-SM-32S)	32-core CPU, 192GB DDR4, 1x 800GB SSD
FPR-4145 (PID: FPR4K-SM-44S)	44-core CPU, 384GB DDR4, 1x 800GB SSD

- Increased crypto performance boost (Intel QAT for SSL decrypt)
  - 2-3X better performance than previous generation
- Supported with FTD 6.4, FXOS 2.6.1
- Management options: CDO, FMC, FDM, API's
- UCS M4 refresh to M5, the blade CPU is changed, more memory installed, crypto chips updated

New Hardware – FPR 1000/1100

NEW

FPR 1010	Desktop, 8x1G copper, internal 200GB SSD, 8G DDR4 memory, 4-core CPU
FPR 1120	Rackmount, 8x1G copper & 4x1G SFP, 200GB SSD, 16G DDR4 memory, 12-core CPU
FPR 1140	Rackmount, 8x1G copper & 4x1G SFP, 200GB SSD, 16G DDR4 memory, 16-core CPU
FPR 1150 (New Fall 2019)	Rackmount, 8x1G copper & 2x1G SFP, 2x10GB SFP+, 200GB SSD, 32G DDR4 memory

New Hardware – FPR 1010

- NGFW desktop product
- FTD software version 6.4+ and ASA 9.13.1 in Fall 2019
- **PoE+** and **L2 switch** features available in 6.5 FTD software release
  - Port 7 and 8 are PoE+ ports
- 8x Gigabit Ethernet RJ-45 10/100/1000 BaseT plus management
- Fan less (airflow: side to side)
- Reset button: if pressed for more than 3 seconds the chassis is placed to default state (configuration variables are reset, however files from flash are not removed)

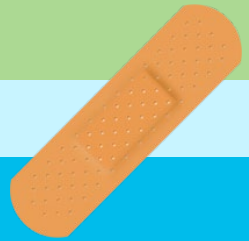
NGFW
HW and SW
Architecture

Firepower Threat Defense

Architecture overview

DETECTION ENGINE (IPS)

Packet Data Transport System (PDTS)

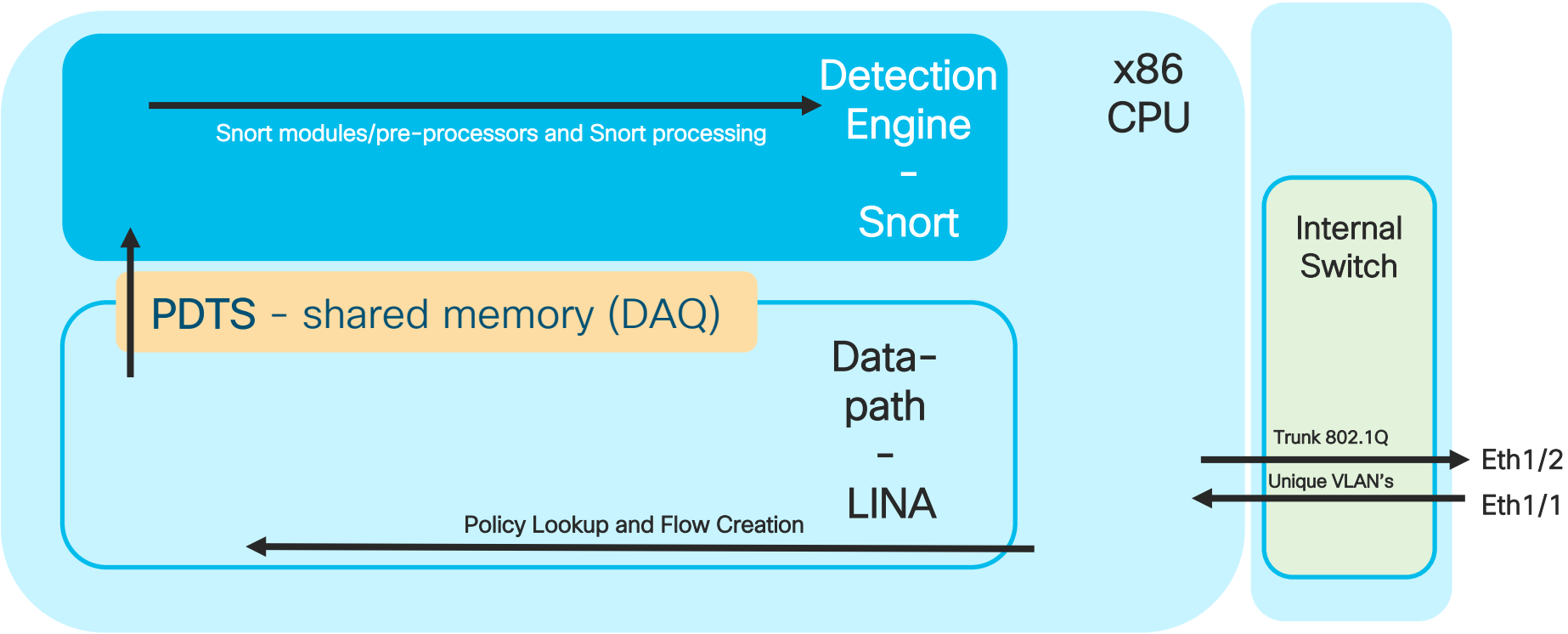


DATA-PATH (FW)

FXOS

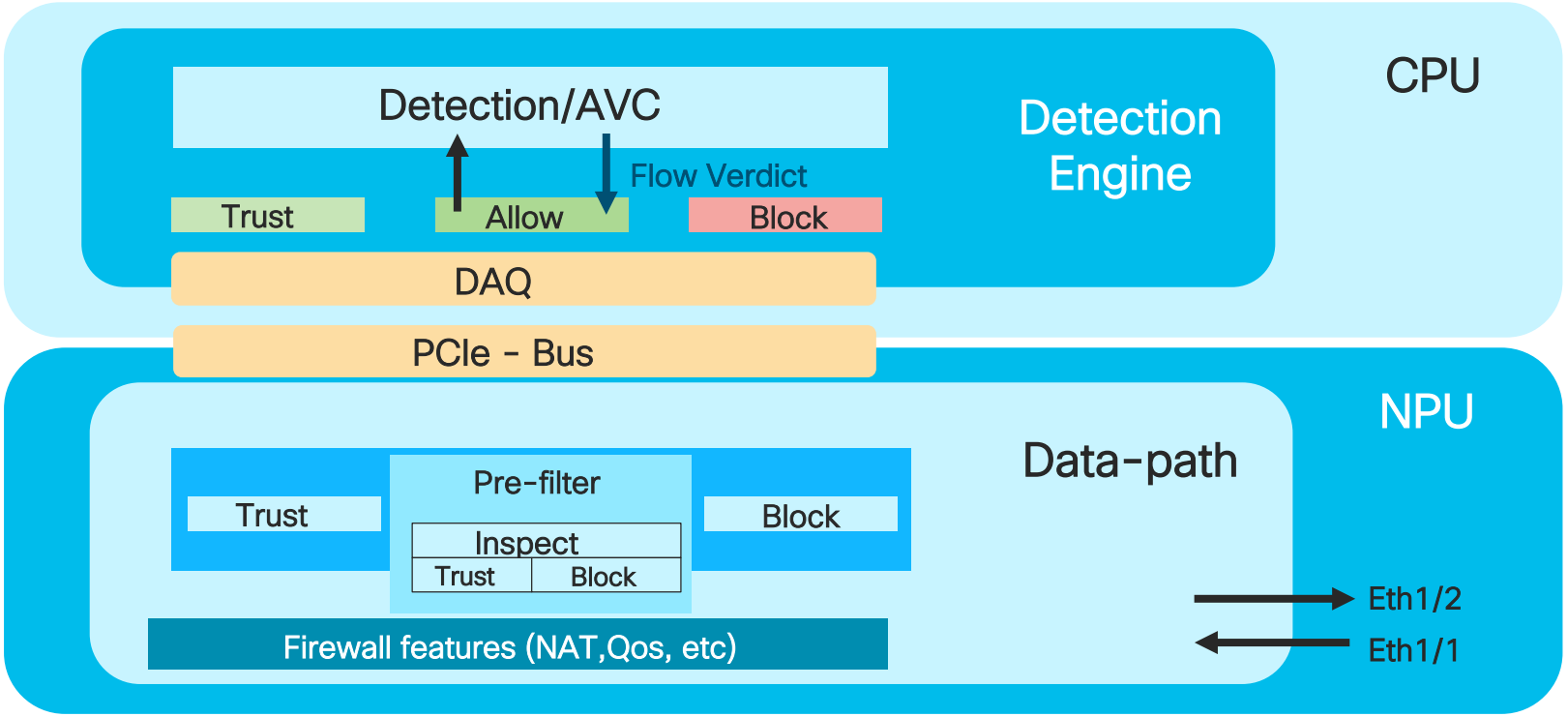
Firepower 1100 series

Architecture overview



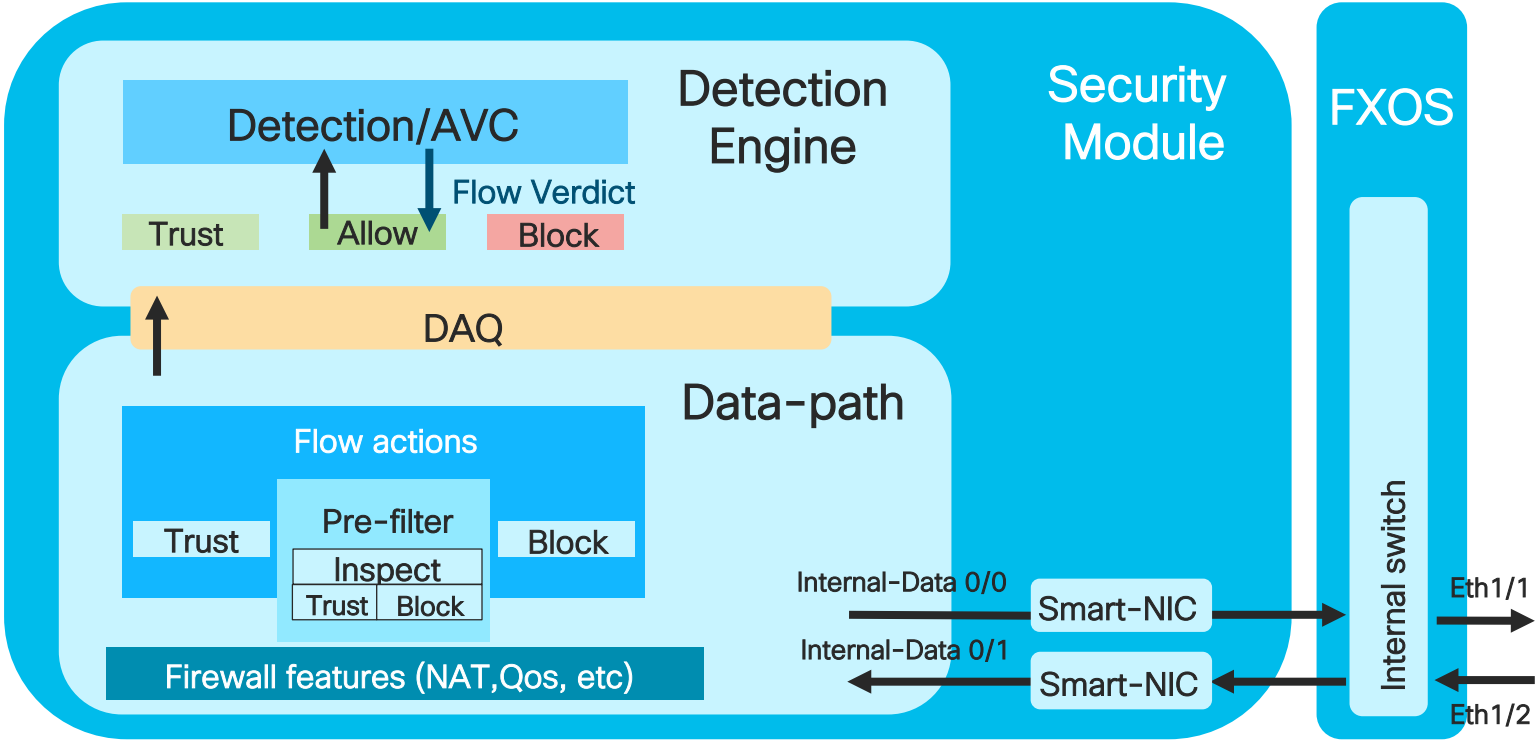
Firepower 2100 platform

Architecture overview



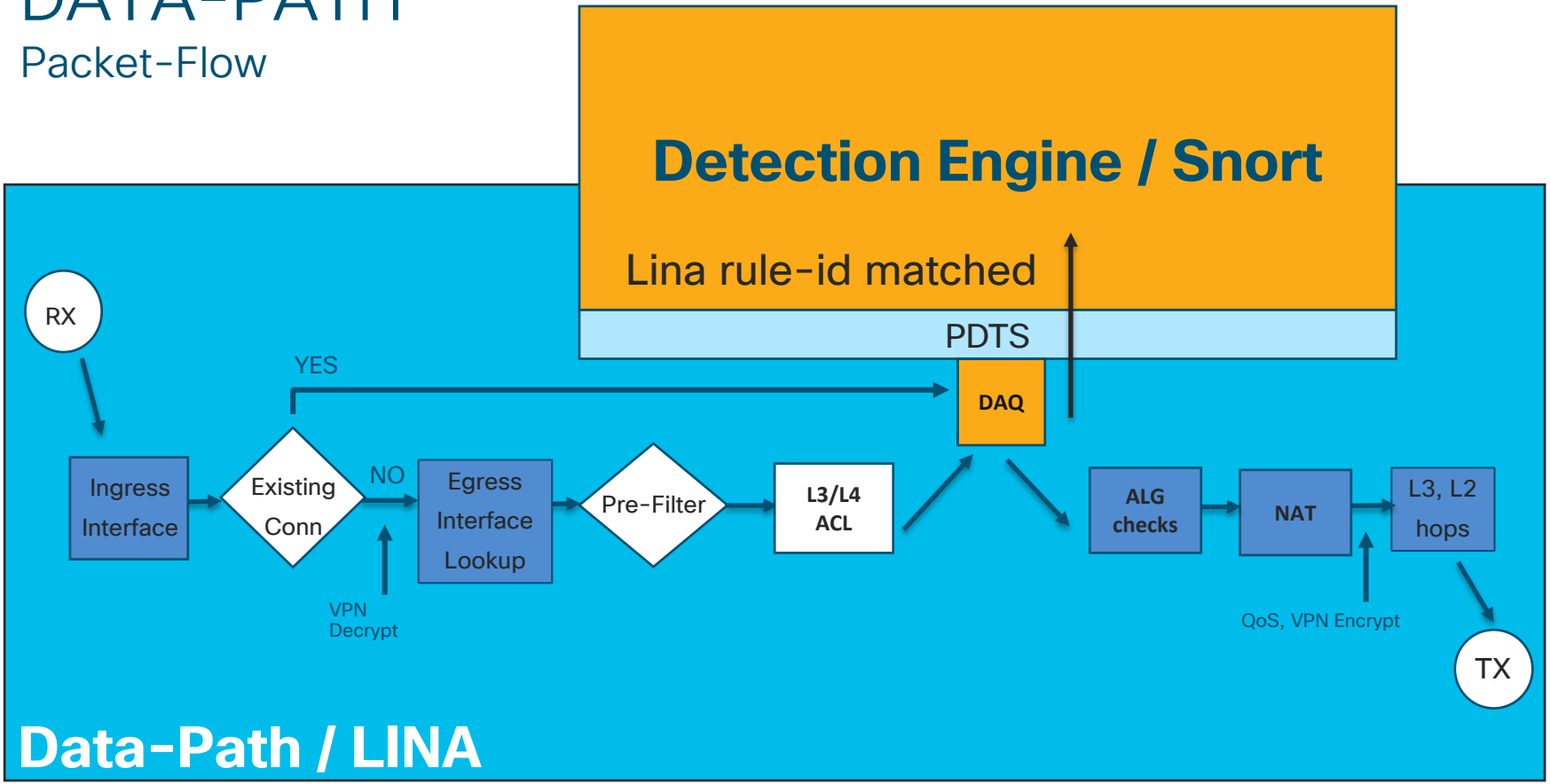
Firepower 4100/9300 platforms

Architecture overview



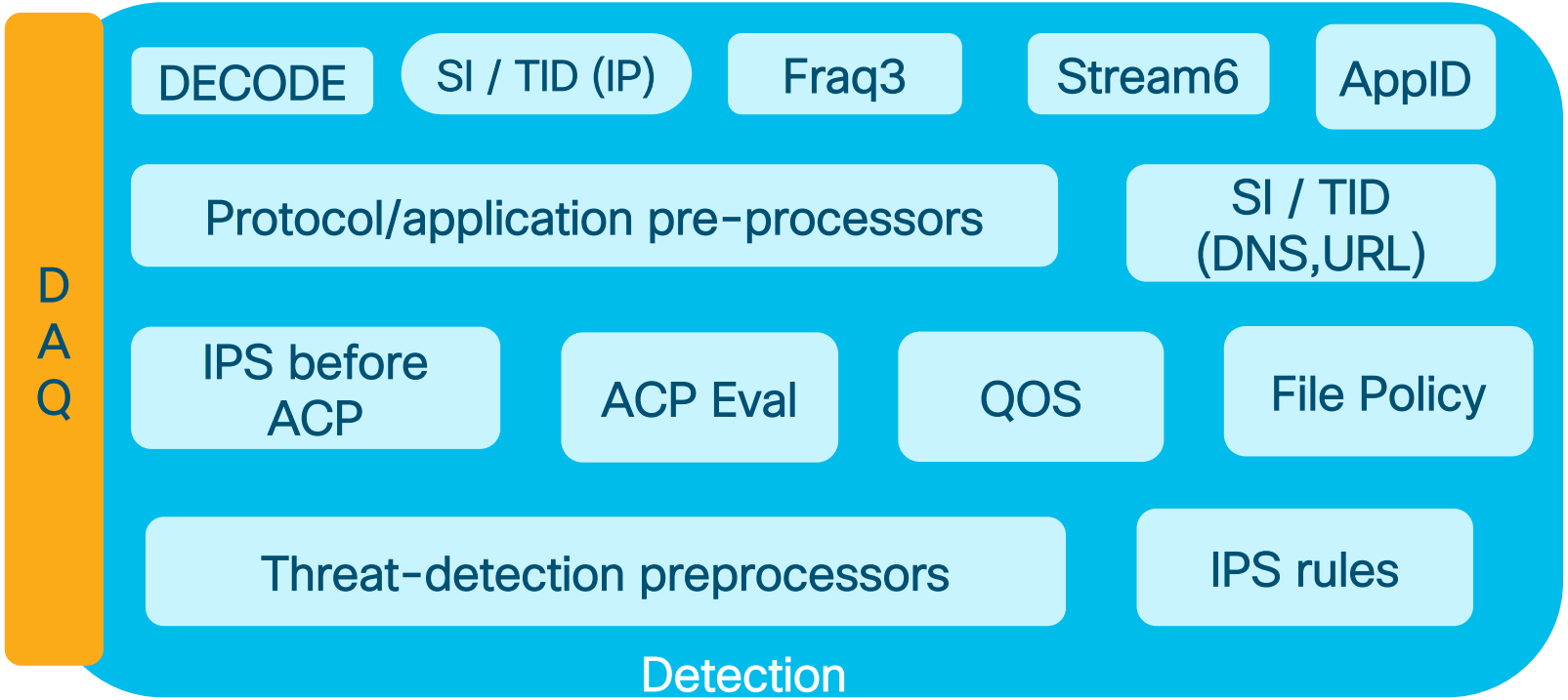
DATA-PATH

Packet-Flow



Detection Engine

Architecture and Packet Flow



Asymmetric traffic handling on FTD

LINA vs. Snort

Asymmetric routing

- TCP connection flow through different routes/directions
- Increases memory usage on Snort

TCP Stream Preprocessor

- Asynchronous Network
  - Instruct Snort to NOT reassemble TCP streams
  - Helps to deal with performance
  - This option does NOT provide better detection – Snort simply can't detect what it doesn't see
  - This configuration option is ignored for FTD routed and transparent interfaces!

Asymmetric traffic handling on FTD

LINA vs. Snort

Why is “Asynchronous Network” preprocessor setting ignored for FTD routed and transparent interfaces ?!?

- Intended for IPS like deployments (inline-sets)
  - Almost all inspection happens in Snort
- NOT supported on transparent/routed interfaces
  - By default LINA DOES have TCP-state bypass disabled hence asymmetric traffic is filtered by LINA
  - If TCP state bypass is enabled (via FlexConfig) on LINA it depends on software version used whether the traffic goes further for deep inspection to Snort or NOT
    - Pre-6.3 releases, traffic will go to Snort
    - To bypass traffic from Snort, user must configure pre-filter rule with fast-path action for asymmetric flows
    - Post-6.3 releases, traffic will NOT go further to Snort for inspection

    Important note: combination of TCP state bypass and Async Network preprocessor is NOT supported!

Tuning NGFW Rule Set from Security and Performance Aspects

Rule Expansion Example

Rules | Security Intelligence | HTTP Responses | Logging | Advanced Settings

Filter by Device | Search Rules

Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Applicat...	Source Ports
▼ Mandatory - empty (1-1)								
AC rule expansion example	Any	Any	1.1.1.1 2.2.2.2	3.3.3.3 4.4.4.4	Any	Any	Any	Any

FMC UI Rule definition

```
# show access-list
access-list CSM_FW_ACL_ line 10 advanced permit ip object-group FMC_INLINE_src_rule_268434433 object-group
FMC_INLINE_dst_rule_26843                4433 rule-id 268434433 (hitcnt=0) 0xfeb692b0

  access-list CSM_FW_ACL_ line 10 advanced permit ip host 1.1.1.1 host 3.3.3.3 rule-id 268434433 (hitcnt=0) 0xa866baa3
  access-list CSM_FW_ACL_ line 10 advanced permit ip host 1.1.1.1 host 4.4.4.4 rule-id 268434433 (hitcnt=0) 0x1f2904fd
  access-list CSM_FW_ACL_ line 10 advanced permit ip host 2.2.2.2 host 3.3.3.3 rule-id 268434433 (hitcnt=0) 0x7cbde7d7
  access-list CSM_FW_ACL_ line 10 advanced permit ip host 2.2.2.2 host 4.4.4.4 rule-id 268434433 (hitcnt=0) 0x64d8a459
```

4 elements

FTD CLI Rule representation

Access Control Rule Sizing Guidelines NOT hardcoded limits!

Platform	Max Recommended AC element count (LINA Engine)
ASA 5506-X	12,500
ASA 5508-X	50,000
ASA 5516-X	125,000
ASA 5525-X	150,000
ASA 5545-X	250,000
ASA 5555-X	250,000

Platform	Max Recommended AC element count (LINA Engine)
FPR 1010 (NEW)	15,000
FPR 1020 (NEW)	125,000
FPR 1040 (NEW)	150,000
FPR 1050 (NEW)	250,000
FPR 2110	50,000
FPR 2120	75,000
FPR 2130	300,000
FPR 2140	375,000

Access Control Rule Sizing Guidelines NOT hardcoded limits!

Platform	Max Recommended AC element count (LINA Engine)
FPR 4110	2,250,000
FPR 4120	2,250,000
FPR 4140	2,250,000
FPR 4150	300,000,000
FPR 4115 (New)	2,500,000
FPR 4125 (New)	2,750,000
FPR 4145 (New)	3,000,000

Platform	Max Recommended AC element count (LINA Engine)
FPR 9300 SM-24	2,250,000
FPR 9300 SM-36	2,250,000
FPR 9300 SM-44	3,000,000
FPR 9300 SM-40 (New)	6,000,000
FPR 9300 SM-48 (New)	6,000,000
FPR 9300 SM-56 (New)	6,000,000

Total Number of Access Control Elements

```
> expert
$ sudo su
# perl /var/opt/CSCOpx/bin/access_rule_expansion_count.pl

  Cisco Firepower Management Center 2000 - v6.5.0.2 - (build 57)
  Access Control Rule Expansion Computer

  Enter FTD UUID or Name:
  > FTD-Veronika-Home-Office-shelf-1
```

AC Rule Expansion "FMC Built-In" Calculator

Introduced in 6.5 release
-
Available in FMC CLI

FMC:
Devices > Device Management > Edit device > Navigate to Device tab

https://netsec-fmc.cisco.com/ddd/#NGFWDevice;id=0ed8d092-35e4-11ea-a3f3-ad2ea926233e

Device UUID

Access Control Rule Element Count "Calculator"

Prior Policy Deployment

```
Enter FTD UUID or Name:
  > FTD-Veronika-Home-Office-shelf-1
..........
 Access Control Policy:
   UUID: 005056B2-93AB-0ed3-0000-004294967299
   Name: Policy-3
.......... (output omitted)
-------------------------------------------------------------------------------------------------------------
| UUID                                | NAME                                |                COUNT |
-------------------------------------------------------------------------------------------------------------
| 005056B2-93AB-0ed3-0000-000268436484 | ACP_Rule_22131 |                    4 |
| 005056B2-93AB-0ed3-0000-000268436483 | ACP_Rule_22130 |                    4 |
-------------------------------------------------------------------------------------------------
| TOTAL: 8
-------------------------------------------------------------------------------------------------
| Access Rule Elements Count on FTD: 14
```

AC element expansion count for specific rule

Sum of expanded AC elements for all AC rules

Total amount of expanded rules includes
Default set of FTD rules (Pre-Filter) + Default AC rule

Default FTD Rule Set

```
> show access-list

access-list CSM_FW_ACL_; 6 elements; name hash: 0x4a69e3f3

access-list CSM_FW_ACL_ line 1 remark rule-id 9998: PREFILTER POLICY: Default Tunnel and
Priority Policy
access-list CSM_FW_ACL_ line 2 remark rule-id 9998: RULE: DEFAULT TUNNEL ACTION RULE
access-list CSM_FW_ACL_ line 3 advanced permit ipinip any any rule-id 9998 (hitcnt=0) 0xf5b597d6
access-list CSM_FW_ACL_ line 4 advanced permit udp any eq 3544 any range 1025 65535 rule-id 9998
(hitcnt=0) 0x46d7839e
access-list CSM_FW_ACL_ line 5 advanced permit udp any range 1025 65535 any eq 3544 rule-id 9998
(hitcnt=0) 0xaf1d5aa5
access-list CSM_FW_ACL_ line 6 advanced permit 41 any any rule-id 9998 (hitcnt=0) 0x06095aba
access-list CSM_FW_ACL_ line 7 advanced permit gre any any rule-id 9998 (hitcnt=0) 0x52c7a066

access-list CSM_FW_ACL_ line 8 remark rule-id 268434432: ACCESS POLICY: empty - Default
access-list CSM_FW_ACL_ line 9 remark rule-id 268434432: L4 RULE: DEFAULT ACTION RULE
access-list CSM_FW_ACL_ line 10 advanced deny ip any any rule-id 268434432 (hitcnt=0) 0x97aa021a
```

Tuning NGFW Rule Set from Security and Performance Aspects

Pre-filter rules

- Allowing traffic based on IP/Port should come in early packet flow stages for trusted applications (backup)
- Processing traffic in hardware
- Recommended for highly trusted traffic over Trust

Security Intelligence / Threat Intelligence Director

- Backlisting traffic based on IP should come in early packet flow stages

Trust rules

- At the beginning of AC policy after the Block rules

L3/L4 rules

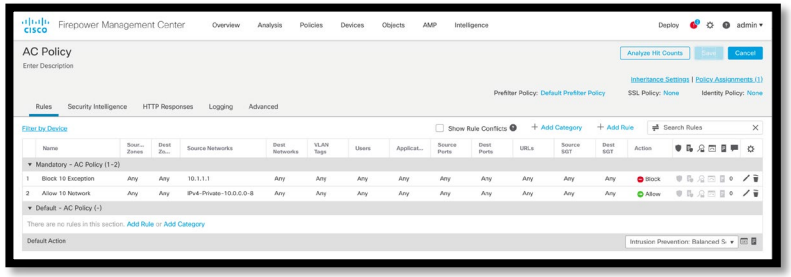
- Rules with IP and port information
- Recommended to place specific rules prior general rules

L7 rules

- URL, Geo location, Application detectors

Processing from top to bottom

- Access Control Policy
  - "Heart" of all Security policies
  - Defines how traffic is allowed, blocked, inspected and logged based on rule definition and it's order!



- TIPS
  - Avoid rule conflicts (shadowing rules)
  - Tune logging (only for critical traffic flows)
  - Build rule set "right way"
    - to avoid rule expansion, incorrect rule handling, etc.

Overlapping NGFW Rules a.k.a **Rule Shadowing**

shadow rules example

Enter Description

Analyze Hit Counts | Save | Cancel

Inheritance Settings | Policy Assignments (1)

Rules | Security Intelligence | HTTP Responses | Logging | Advanced Settings

Prefilter Policy: Default Prefilter Policy | SSL Policy: None | Identity Policy: None

Filter by Device | Search Rules | Show Rule Conflicts | + Add Category | + Add Rule

#	Name	Source Networks	Dest Networks	Applications	URLs	Source SGT	Dest SGT	Action
▼ Mandatory - shadow rules example (1-5)								
1	log everything	Any	Any	Any	Any (Except Uncategorized) (Re	Any	Any	Monitor
2	DST SGT	Any	Any	Any	Any	Employees	Network_Services	Trust
3	proffesors	10.0.0.0/8	Any	Any	Any	Any	Any	Allow
4	block Facebook	Any	Any	Facebook	Any	Any	Any	Block with reset
5	students	10.8.0.0/16	Any	Any	Any	Any	Any	Block

Disabled
By default

shadow rules example

Enter Description

Show Warnings | Analyze Hit

Inheritance

Rules | Security Intelligence | HTTP Responses | Logging | Advanced Settings

Prefilter Policy: Default Prefilter Policy | SSL Policy:

Filter by Device | Search Rules | Show Rule Conflicts

#	Name	Source Networks	Action
▼ Mandatory - shadow rules example (1-5)			
1	log everything	Any	Monitor
2	DST SGT	Any	Trust
3	proffesors	10.0.0.0/8	Allow
4	block Facebook	Any	Block with reset
5	students	10.8.0.0/16	Block
▼ Default - shadow rules example (-)			

Policy Warnings

Rule Warnings (1)

Search

Rule Name	Message
students	Warning: This rule is preempted by rule 3: proffesors

Enabled
Manually

Access Control Rule Optimization

Object Group Search (OGS) and Access Control Expansion

Upcoming Release

- Object Group Search (**OGS**) is **Access Control List optimization** feature.
- OGS **installs ONLY 1 Access Control Rule** instead of multiple Access Control Element entries that are multiplier of source and destination individual elements.
- **Saves** significant amount of **memory resources**.
- When OGS is enabled, **policy deployment time** is **faster**.
- **FMC** provides **health warning** when **number of Access Control Entries (ACE's)** reaches the limit of recommended entries per platform basis and suggest to enable OGS.

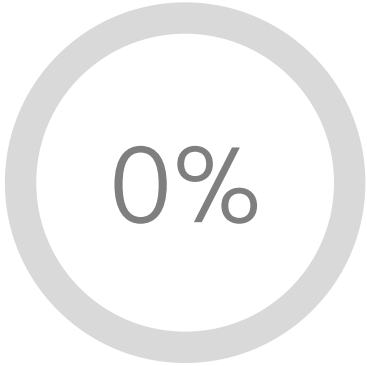
Access Control Rule Optimization

Benefits of Object Group Search (OGS)

Upcoming Release

Memory usage reduction

Deploy Time Reduction



No CPU impact during and after policy deployment

Rule Expansion with OGS disabled

```
# show run object-group-search
#
# show access-list
access-list CSM_FW_ACL_ line 10 advanced permit ip object-group FMC_INLINE_src_rule_268434433 object-group
FMC_INLINE_dst_rule_26843                4433 rule-id 268434433 (hitcnt=0) 0xfeb692b0

  access-list CSM_FW_ACL_ line 10 advanced permit ip host 1.1.1.1 host 3.3.3.3 rule-id 268434433 (hitcnt=0) 0xa866baa3
  access-list CSM_FW_ACL_ line 10 advanced permit ip host 1.1.1.1 host 4.4.4.4 rule-id 268434433 (hitcnt=0) 0x1f2904fd
  access-list CSM_FW_ACL_ line 10 advanced permit ip host 2.2.2.2 host 3.3.3.3 rule-id 268434433 (hitcnt=0) 0x7cbde7d7
  access-list CSM_FW_ACL_ line 10 advanced permit ip host 2.2.2.2 host 4.4.4.4 rule-id 268434433 (hitcnt=0) 0x64d8a459
```

4 elements

Rule Expansion with OGS enabled

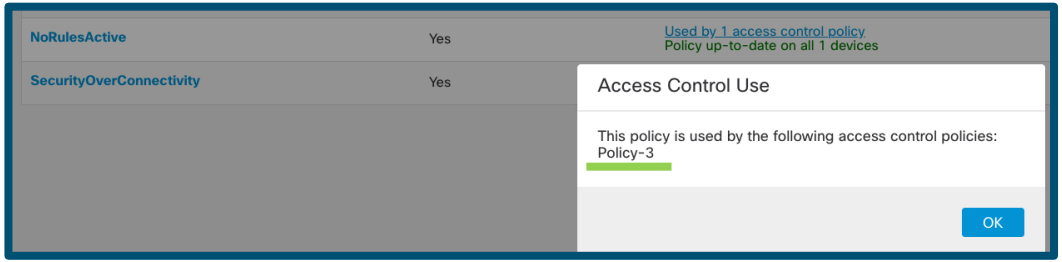
```
# show run object-group-search
object-group-search access-control
#
# show access-list
access-list CSM_FW_ACL_ line 10 advanced permit ip object-group FMC_INLINE_src_rule_268434433 object-group
FMC_INLINE_dst_rule_268434433 rule-id 268434433 (hitcnt=0) 0xfeb692b0

  access-list CSM_FW_ACL_ line 10 advanced permit ip v4-object-group FMC_INLINE_src_rule_268434433(2147483648) v4-object-group
FMC_INLINE_dst_rule_268434433(2147483649) rule-id 268434433 (hitcnt=0) 0xe88cf0c7
```

1 element

Where is my IPS policy being used?!?

Intrusion Policy	Drop when Inline	Status	Last Modified
BalancedSecurityConnectivity	Yes	Used by 1 access control policy Policy up-to-date on all 1 devices	2020-01-20 11:34:19 Modified by "admin"
ConnectivityOverSecurity	Yes	Used by 2 access control policies Policy up-to-date on all 2 devices	2020-01-20 11:35:07 Modified by "admin"
IPS-custom	Yes	Used by 2 access control policies Policy up-to-date on all 2 devices	2020-01-15 15:09:00 Modified by "admin"
MaximumDetection	Yes	No access control policies use this policy Policy not applied on any devices	2020-01-20 11:35:45 Modified by "admin"
NoRulesActive	Yes	Used by 1 access control policy Policy up-to-date on all 1 devices	2020-01-20 11:37:08 Modified by "admin"
SecurityOverConnectivity	Yes	No access control policies use this policy Policy not applied on any devices	2020-01-20 11:37:44 Modified by "admin"

- IPS Policy with baseline ”No Rules Active” is NOT allowed per company policy
  - It was used only for temporary troubleshooting use case and has been forgotten to be removed/replaced
- How to figure out where this IPS policy is used?



Where is my IPS policy being used?!?

Policy-3

Policy with 50

Analyze Hit Counts | Save | Cancel

Inheritance Settings | Policy Assignments (1)

Rules | Security Intelligence | HTTP Responses | Logging | Advanced Settings

Prefilter Policy: Default Prefilter Policy | SSL Policy: None | Identity Policy: None

Filter by Device | Search Rules | Show Rule Conflicts | + Add Category | + Add Rule

	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Applicat...	Source Ports	Dest Por...	URLs	Source SGT	Dest SGT	Action
▼ Mandatory - Policy-3 (-)														
There are no rules in this section. Add Rule or Add Category														
▼ Default - Policy-3 (1-500)														
1	Application_R	Any	Any	PolicyACPOt	PolicyACPOt	Any	Any	Business Rel	Any	Any	Any	Any	Any	Trust
2	Application_R	Any	Any	PolicyACPOt	PolicyACPOt	Any	Any	Categories: /	Any	Any	Any	Any	Any	Interact
3	Application_R	Any	Any	PolicyACPOt	PolicyACPOt	Any	Any	Categories: /	Any	Any	Any	Any	Any	Allow
4	Application_R	Any	Any	PolicyACPOt	PolicyACPOt	Any	Any	Tags: adds/ir	Any	Any	Any	Any	Any	Interact
5	Application_R	Any	Any	PolicyACPOt	PolicyACPOt	Any	Any	Categories: /	Any	Any	Any	Any	Any	Block
6	Application_R	Any	Any	PolicyACPOt	PolicyACPOt	Any	Any	Risks: Very H	Any	Any	Any	Any	Any	Interact
7	Application_R	Any	Any	PolicyACPOt	PolicyACPOt	Any	Any	Categories: /	Any	Any	Any	Any	Any	Trust
8	Application_R	Any	Any	PolicyACPOt	PolicyACPOt	Any	Any	Tags: adds/ir	Any	Any	Any	Any	Any	Interact
9	Application_R	Any	Any	PolicyACPOt	PolicyACPOt	Any	Any	Ty						

1 Row Selected

Displaying 1 - 98 of 500 rules | Page 1 of 6

Where is my IPS policy being used?!?

Policy-3

Policy with 500

Analyze Hit Counts | Save | Cancel

Inheritance Settings | Policy Assignments (1)

Rules | Security Intelligence | HTTP Responses | Logging | Advanced Settings

Prefilter Policy: Default Prefilter Policy | SSL Policy: None | Identity Policy: None

Filter by Device | Search Rules | Show Rule Conflicts | + Add Category | + Add Rule

	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Applicat...	Source Ports	Dest Por...	URLs	Source SGT	Dest SGT	Action
▼ Mandatory - Policy-3 (-)														
There are no rules in this section. Add Rule or Add Category														
▼ Default - Policy-3 (1-500)														
1	Application_R	Any	Any	PolicyACPOt	PolicyACPOt	Any	Any	Business Rel	Any	Any	Any	Any	Any	Trust
2	Application_R	Any	Any	PolicyACPOt	PolicyACPOt	Any	Any	Categories: /	Any	Any	Any	Any	Any	Interact
3	Application_R	Any	Any	PolicyACPOt	PolicyACPOt	Any	Any	Categories: /	Any	Any	Any	Any	Any	Allow
4	Application_R	Any	Any	PolicyACPOt	PolicyACPOt	Any	Any	Tags: adds/ir	Any	Any	Any	Any	Any	Interact
5	Application_R	Any	Any	PolicyACPOt	PolicyACPOt	Any	Any	Categories: /	Any	Any	Any	Any	Any	Block
6	Application_R	Any	Any	PolicyACPOt	PolicyACPOt	Any	Any	Risks: Very H	Any	Any	Any	Any	Any	Interact
7	Application_R	Any	Any	PolicyACPOt	PolicyACPOt	Any	Any	Categories: /	Any	Any	Any	Any	Any	Trust
8	Application_R	Any	Any	PolicyACPOt	PolicyACPOt	Any	Any	Tags: adds/ir	Any	Any	Any	Any	Any	Interact
9	Application_R	Any	Any	PolicyACPOt	PolicyACPOt	Any	Any	Ty						

1 Row Selected

Displaying 1 - 98 of 500 rules | Page 1 of 6

Where is my IPS policy being used?!?

Policy-3

Policy with 50

Analyze Hit Counts | Save | Cancel

Inheritance Settings | Policy Assignments (1)

Rules | Security Intelligence | HTTP Re

SSL Policy: None | Identity Policy: None

Filter by Device | Search Rules

+ Add Category | + Add Rule

Name | Source Zones | Dest Zones | Action

Mandatory - Policy-3 (-)

There are no rules in this section. Add Rule or Ad

Default - Policy-3 (1-500)

1	Application_R	Any	Any										Trust	0
2	Application_R	Any	Any										Interact	0
3	Application_R	Any	Any										Allow	0
4	Application_R	Any	Any										Interact	0
5	Application_R	Any	Any										Block	0
6	Application_R	Any	Any										Interact	0
7	Application_R	Any	Any	PolicyACPOt	PolicyACPOt	Any	Any	Categories: /	Any	Any	Any	Any	Trust	0
8	Application_R	Any	Any	PolicyACPOt	PolicyACPOt	Any	Any	Tags: adds/ir	Any	Any			Interact	0
9	Application_R	Any	Any	PolicyACPOt	PolicyACPOt	Any	Any							0

1 Row Selected

Displaying 1 - 98 of 500 rules | Page 1 of 6

Policy Assignments

Targeted Devices

Select devices to which you want to apply this policy.

Available Devices

Search by name or value

FTD-Veronika-Hom...

Add to Policy

Selected Devices

FTD-Veronika-Hom...

Impacted Devices

Cancel | OK

Where is my IPS policy being used?!?

```
> show access-control-config
====================[ Policy-3 ]====================
Description                 : Policy with 500 rules
Default Action              : Allow
Default Policy              : Balanced Security and Connectivity

… (output omitted)

-----------[ Rule: Application_Rule_12 ]------------
    Action                  : Allow
    Intrusion Policy        : Security Over Connectivity
      ISE Metadata            :

    Source Networks         : PolicyACPObject-3-Network-20-XYZ (26.228.125.211)
    Destination Networks    : PolicyACPObject-3-Network-21-XYZ (64.75.150.4)
    Application             : Risk: Critical
    Logging Configuration
    DC                      : Disabled
      Beginning             : Disabled
      End                   : Disabled
      Files                 : Disabled
    Safe Search             : No
    Rule Hits               : 0

… (output omitted)
```

Where is my IPS policy being used?!?

Option 1

```
> expert
$ sudo su
# sfcli.pl show firewall | grep "Rule:\|Intrusion Policy" | grep "NoRulesActive" -B 1
------------[ Rule: Basic 5 Tuple_302 ]-------------
   Intrusion Policy      : NoRulesActive
#
```

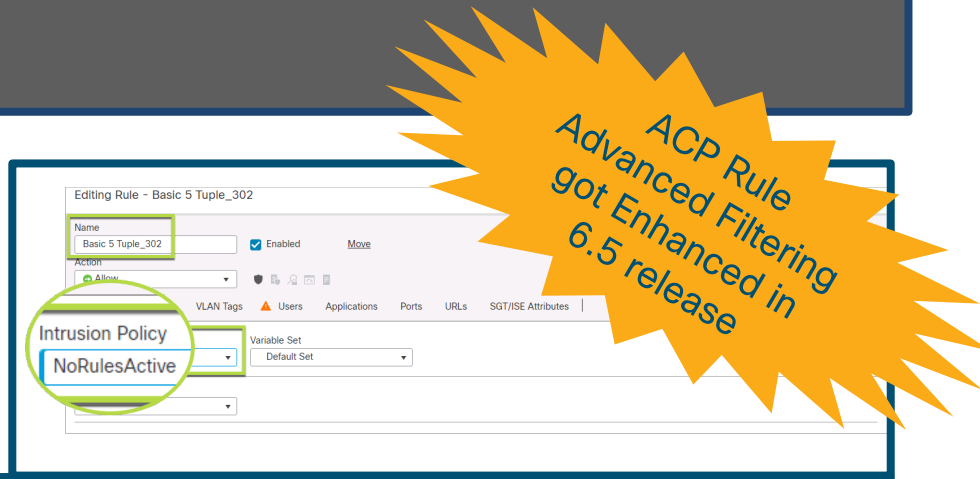
ACP Advanced Filtering

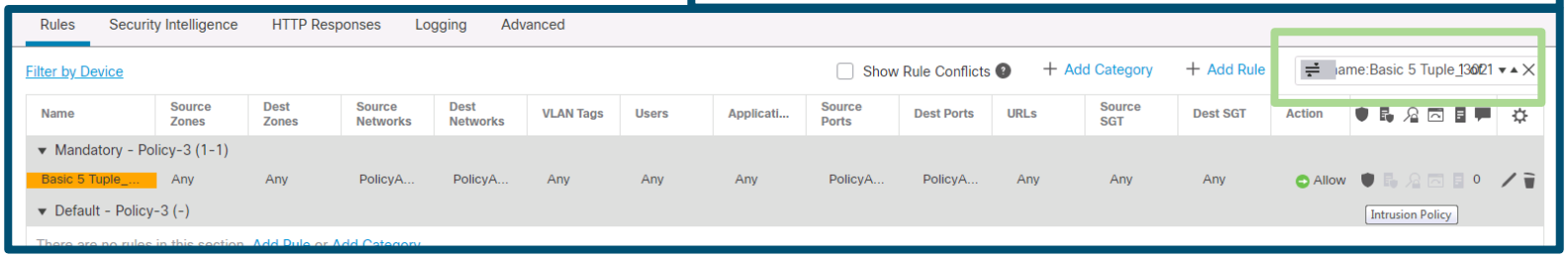
Find the ACP rule named “Basic 5 Tuple_302” in column Name

- name:Basic 5 Tuple_302

Use Toggle button – Show Only Rules Matching Filter Criteria

- Useful in the network environments with large NGFW rule set





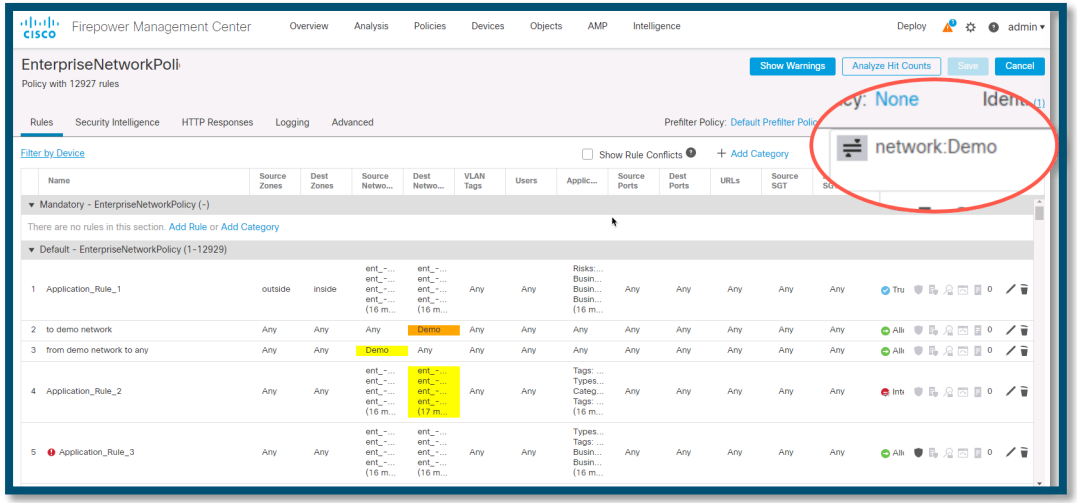
Where is my IPS policy being used?!?

Option 2

```
$ python3 acp-rule-to-ips-policy-association.py
AC rule name: rule with IPS Connectivity
IPS policy: Connectivity Over Security

AC rule name: rule with IPS NoActiveRules
IPS policy: NoRulesActive
```

- Script returns AC rule name and IPS policy that is associated with the rule
  - Written in Python scripting language
  - Leverage FMC API call to extract Access Control Rules details
- Illustrative above-mentioned basic Python script can be downloaded HERE

Finding the AC Rule in large rule set using TAGs



ACP Rule Advanced Filtering got Enhanced in 6.5 release

Column Name	Filter TAG
ACP rule name	name
Source/Destination Port	port
Source/Destination Network	network
URLs	url
Applications	app
Source/Destination zones	sz
VLAN TAGs	vlan

Policy Deployment

History, Architecture and latest improvements!

Policy Deployment Improvements in 6.2.3

FMC: LINA_ONLY delta deploy and elastic timeout

Pre-6.2.3 behavior

- FTD device timeout set to 35 minutes by default, FMC timeout is 45 minutes, delta LINA CLI written to XML
- Policy deployment timeout after default 35 minutes regardless whether the transfer is in progress or not

Post-6.2.3 behavior

- FTD device starts using a new feature called 'Elastic timeout'
  - Timeout value is automatically adjusted based on deployment file transfer progress
  - Timeout invoked only during inactivity time meaning no file copy in progress
- Serviceability enhancements
  - Updated details of error messages and troubleshooting details in FMC UI
  - Added indicator of policy deployment progress
  - Transcript record shown after FW-related changes when deployment is completed
- 5-tuple FW policy deployment delta changes are written to file that is directly applied to running-configuration for better performance

Use cases resolved

- Helpful in environments with low bandwidth such us satellite links where deployment takes over 35 minutes, which could be in previous release be interrupted by default timeout.
- Addresses scenarios where policy deployment unexpectedly hangs for unknown reasons

Policy Deployment Improvements in 6.3

FMC: Delta deployments
FDM: LINA_ONLY deployments, discard configuration changes

Pre-6.3 behavior

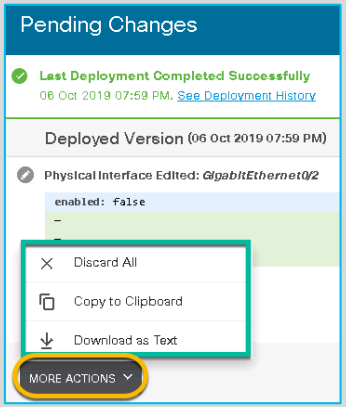
- Missing capability to review pre and post deployment changes and discard pending changes that user does not want to deploy. Users are unable to backup and restore device configuration, that is necessary for example after software reimage process.

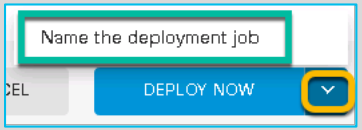
Post-6.3 behavior

- FDM: Change management
  - Review, copy, download, rollback and audit of changes
    - Configuration is stored in YML format
  - Deployment history
  - Download device configuration in JSON format
  - Sensitive data sanitized
  - Audit events have filtering options per specific period of the time
  - Related API: ‘pendingchanges’, ‘auditevents’, ‘exportconfig’, ‘exportconfigjob’, ‘downloadconfig’

Use cases resolved

- Requirement for audit of deployment changes





Policy Deployment Improvements in 6.4

FMC: Enhanced deploy framework

FDM: Delta deployments

Pre-6.3 behavior

- Potential temporary network disruption on policy deployment failure when config rollback mechanism kick-in
  - Rollback reverts full configuration: ‘clear configure all’ and ’copy startup-config running-config’
  - That clears all connection state table and shutdown the interfaces

Post-6.3 behavior

- Reduce traffic drops during LINA rollback
  - LINA performs configuration validation without affecting traffic
  - Configuration is reverted on failure only on last configuration changes that were pushed to device
- Performance improvements
- Framework provides better code readability, allowing easy of plugging in a new additional functions
- Caching mechanism was added that avoids export of unchanged configuration again
  - Device applies only changed configuration

Use cases resolved

- Minimizes network traffic interruptions during policy deployment rollback that can kick-in on failure introduced by typo in FlexConfig for example.

Policy Deployment Improvements in 6.5

FDM: Snort Delta Deployments

Pre-6.5 behavior

- All rules regardless of configuration change were entirely reconstructed due to which the policy deployment taken longer time

Post-6.5 behavior

- Snort delta deployments are faster during incremental policy rule modifications
- Enhancement optimizes process of generating AC rules that are:
    - Modified
    - Added
    - Deleted
- Only adjusted rules are reconstructed in backend instead of whole AC rule set
- Full configuration deployment performs as in previous releases

Post-6.5 behavior

- Modification of AC rules and their subsequent deployments are done quicker.

Policy Deployment Improvements in 6.5

FTD: HA/Cluster policy deployment file copy transfer between units

Pre-6.5 behavior

- Policy deployment bundle package is transferred between HA Active and Standby or Cluster Master and Slave units by leveraging an internal LINA based file copy mechanism.
    - File is copied via 'push' method by Active unit to Standby
- The old policy deploy file copy mechanism causes the policy deployment to take significant amount of the time, which results into bad customer experience.

Post-6.5 behavior

- Policy deployment bundle package is transferred between HA Active and Standby or Cluster Master and Slave units by leveraging a new copy file mechanism (r-sync).
    - File is copied via 'pull' method by Standby unit from Active
- The changes are reflected when all devices in HA or Cluster are running 6.5 release

Use cases resolved

- Policy deployments towards HA/Clustering units in network environments with saturated state sharing load links or the links with lower speeds

Policy deployment

Architectural enhancements

6.2.3

FMC: LINA_ONLY deployment

- 5-tuple FW rules

FTD: Elastic timeout

6.3

FMC: Delta deployments

FDM: LINA_ONLY deployment

- 5-tuple FW rules

FDM: discard configuration changes

6.4

FMC: Enhanced deploy framework

FDM: Delta deployments

6.5

FMC: changed file copy mechanism for file copy between HA Active/Standby nodes and Cluster Master/Slave units (r-sync)

FDM: Snort delta deployment

Upcoming Release

FMC: Delta preview changes

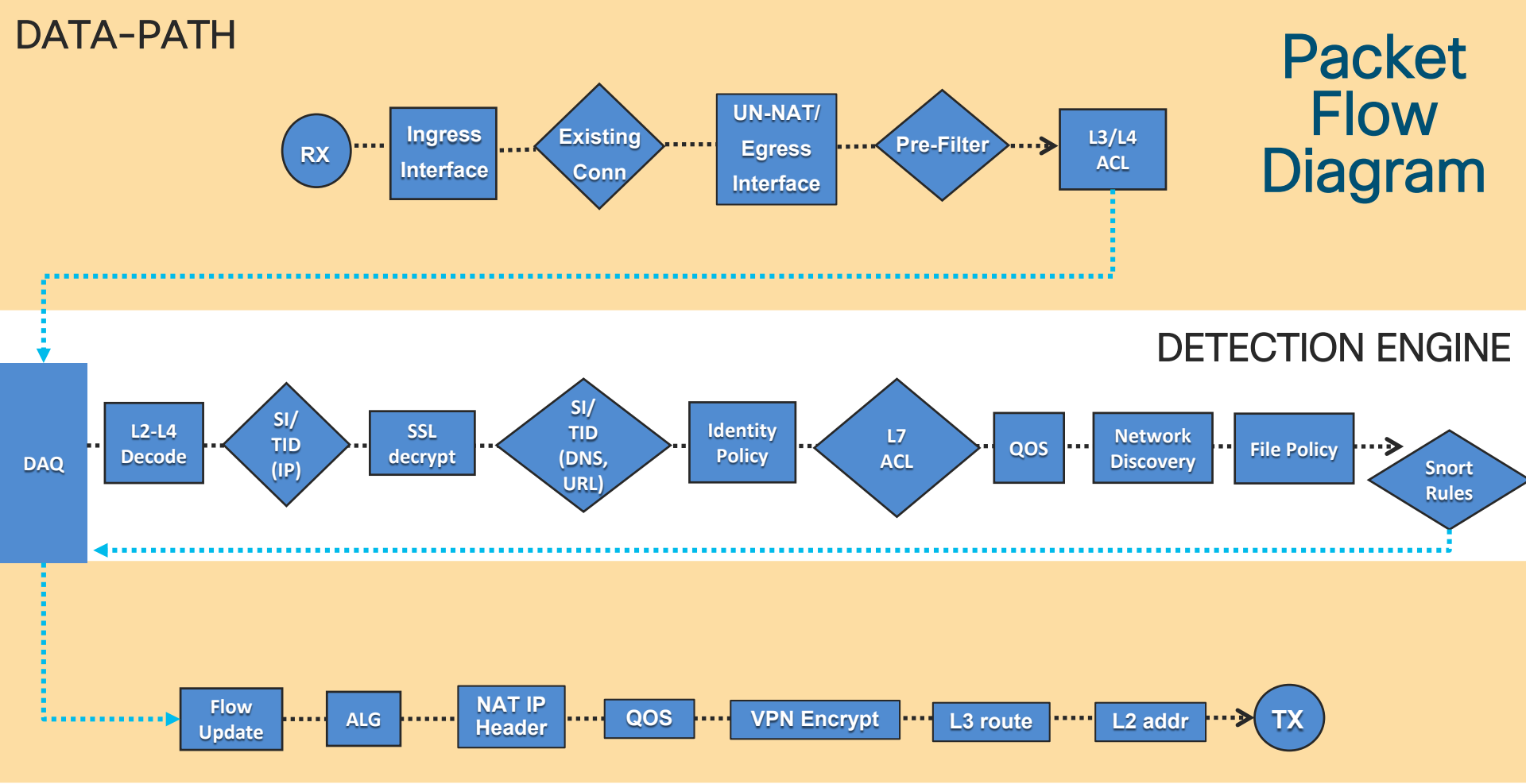
FMC: Selective deployment

FMC: Policy deployment time estimate

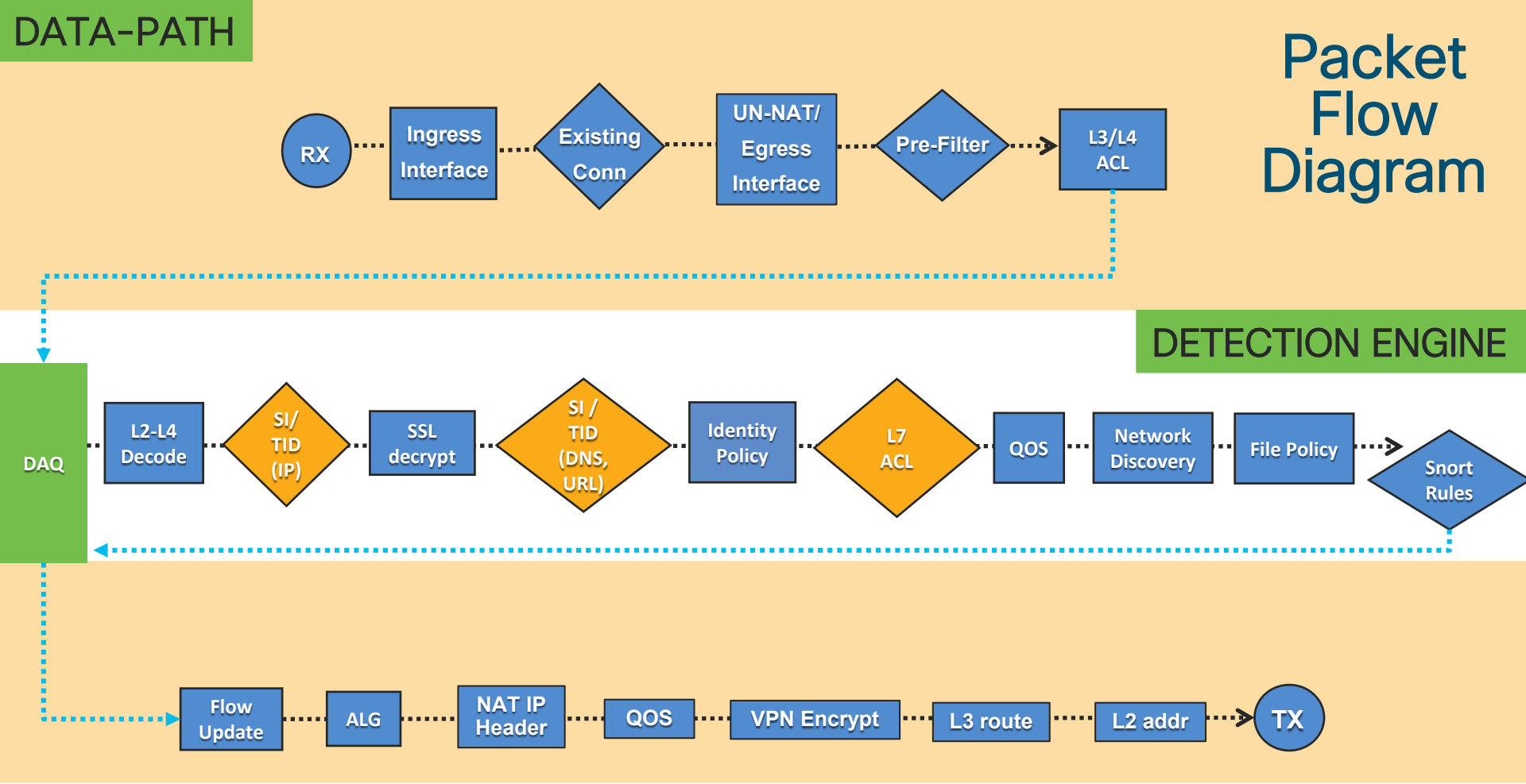
FMC: Policy Deployment History

Day in the Life of Packet

Packet Flow Diagram



Packet Flow Diagram



User story: Security Intelligence

Some websites categorized as malicious are not blocked

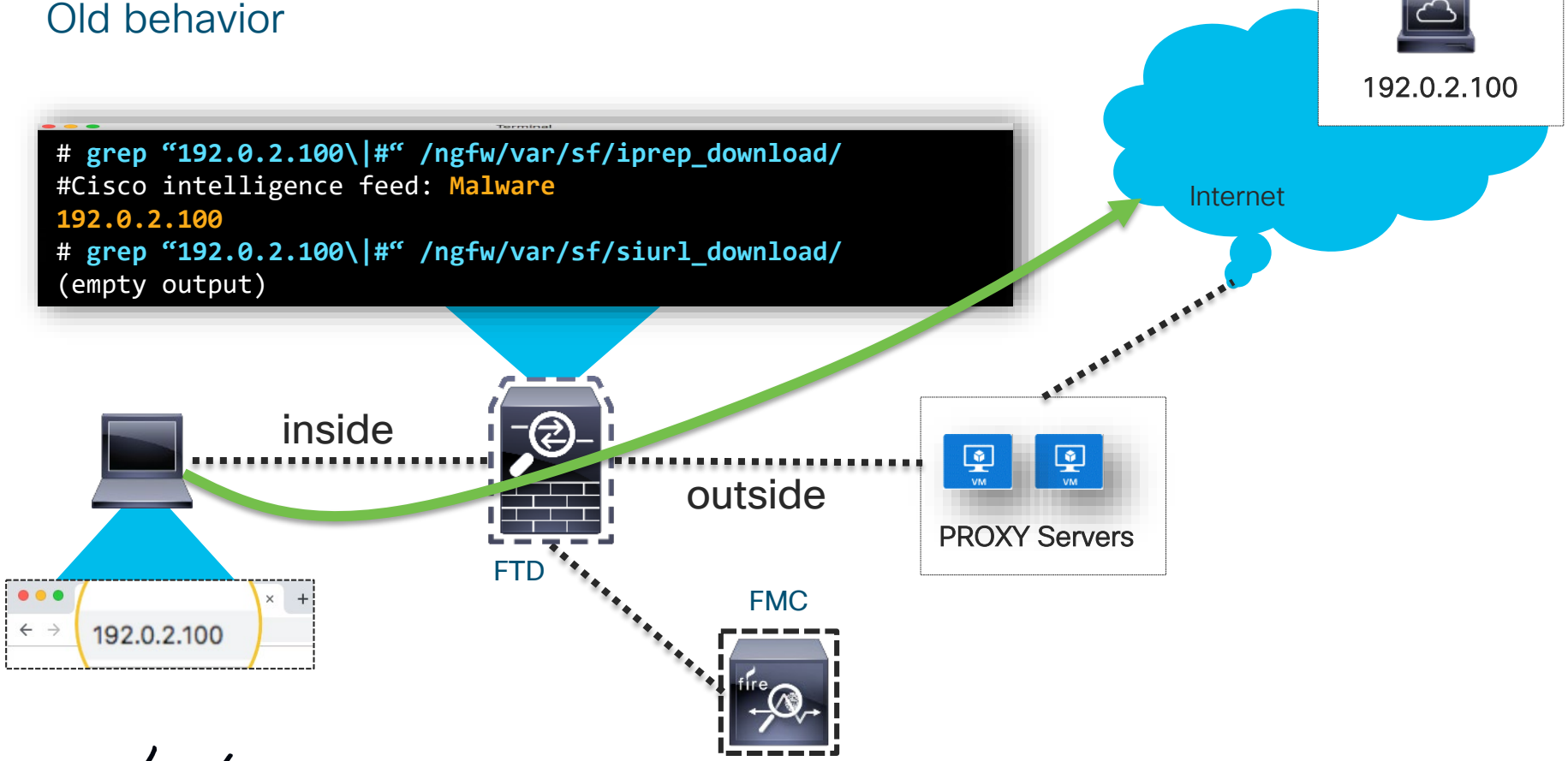
Description

- User attempts to access malicious website using IP address instead of domain name
- This traffic is being blocked only when the user traffic is not being redirected via the proxy

User story: Security Intelligence

Old behavior

```
# grep "192.0.2.100\|#" /ngfw/var/sf/iprep_download/
#Cisco intelligence feed: Malware
192.0.2.100
# grep "192.0.2.100\|#" /ngfw/var/sf/siurl_download/
(empty output)
```



User story: Security Intelligence

Old behavior

Overview | Analysis | Policies | Devices

Context Explorer | Connections ▸ Events

Connection Events (switch workflow)

	Initiator IP	Responder IP	Security Intelligence Category	Source Port / ICMP Type	Destination Port / ICMP Code
Allow	192.168.10.200	64.103.36.133		54909 / tcp	80 (http) / tcp

CLIENT IP

PROXY SERVER IP

Responder IP address is Proxy server IP, which is not in SI (IP) feed list

Internet

192.0.2.100

inside

outside

FTD

FMC

PROXY Servers
64.103.36.133

192.0.2.100

User story: Security Intelligence

... in more secure way!

```
# grep "192.0.2.100\|#" /ngfw/var/sf/iprep_download/
#Cisco intelligence feed: Malware
192.0.2.100
# grep "192.0.2.100\|#" /ngfw/var/sf/siurl_download/
#Cisco DNS and URL intelligence feed: URL Malware
192.0.2.100
```

IP feed list

URL feed list

192.0.2.100

inside

outside

Traffic blocked!

FTD

FMC

PROXY Servers
64.103.36.133

192.0.2.100

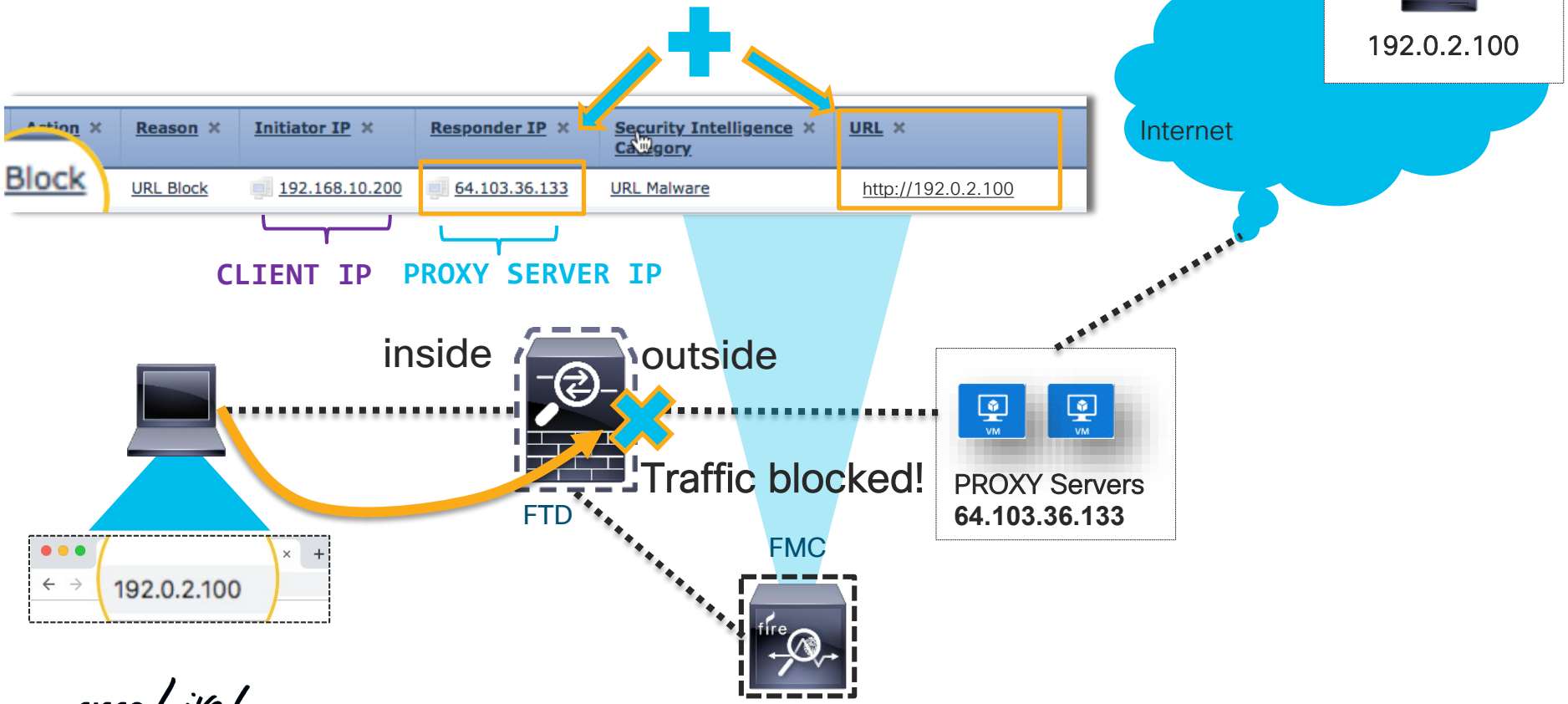
6.5 – URL and IP feed list is cross checked in memory

User story: Security Intelligence

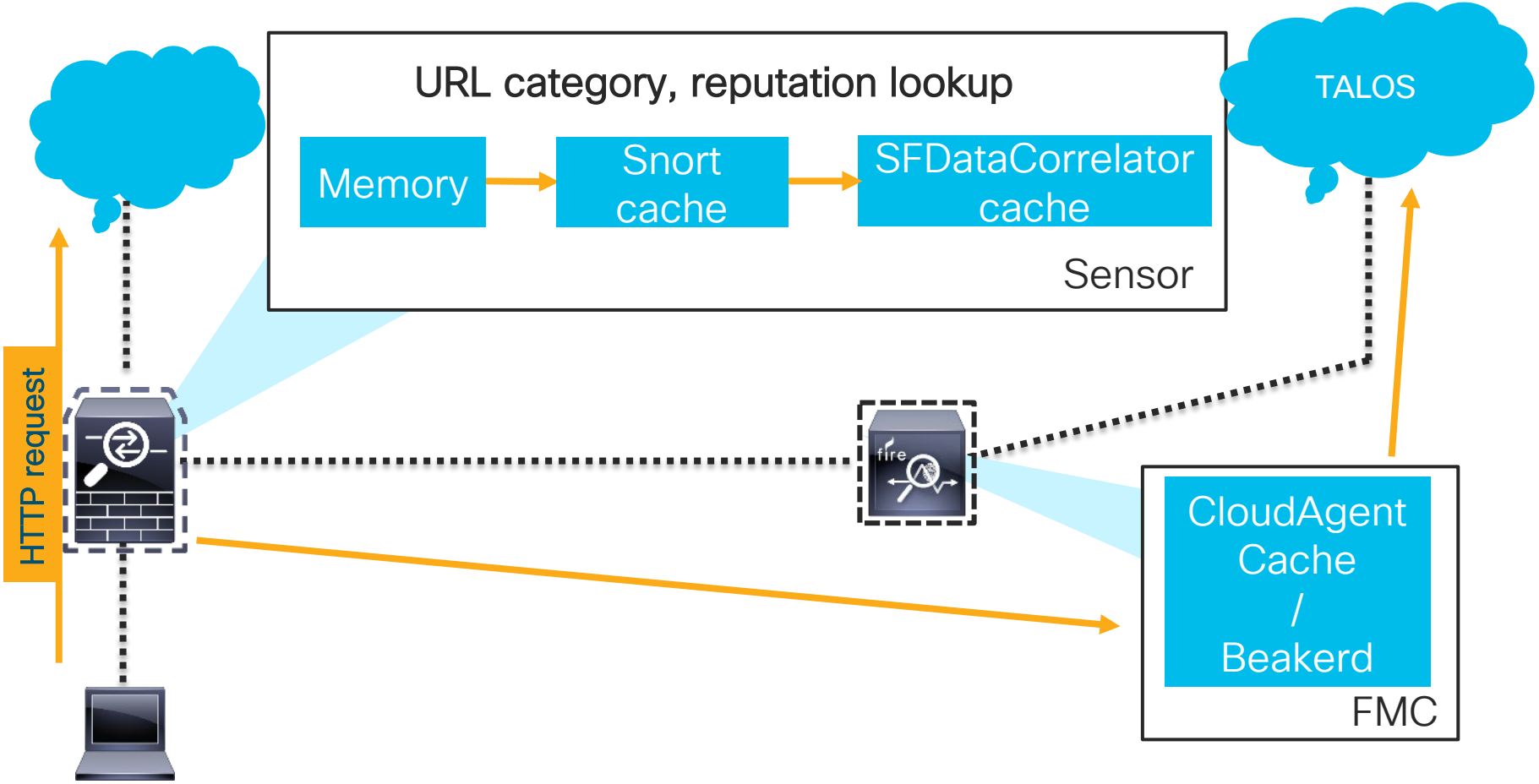
... in more secure way!

Action	Reason	Initiator IP	Responder IP	Security Intelligence Category	URL
Block	URL Block	192.168.10.200	64.103.36.133	URL Malware	http://192.0.2.100

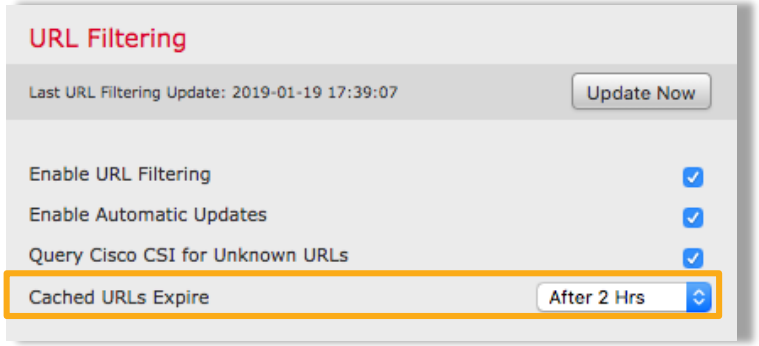
CLIENT IP PROXY SERVER IP



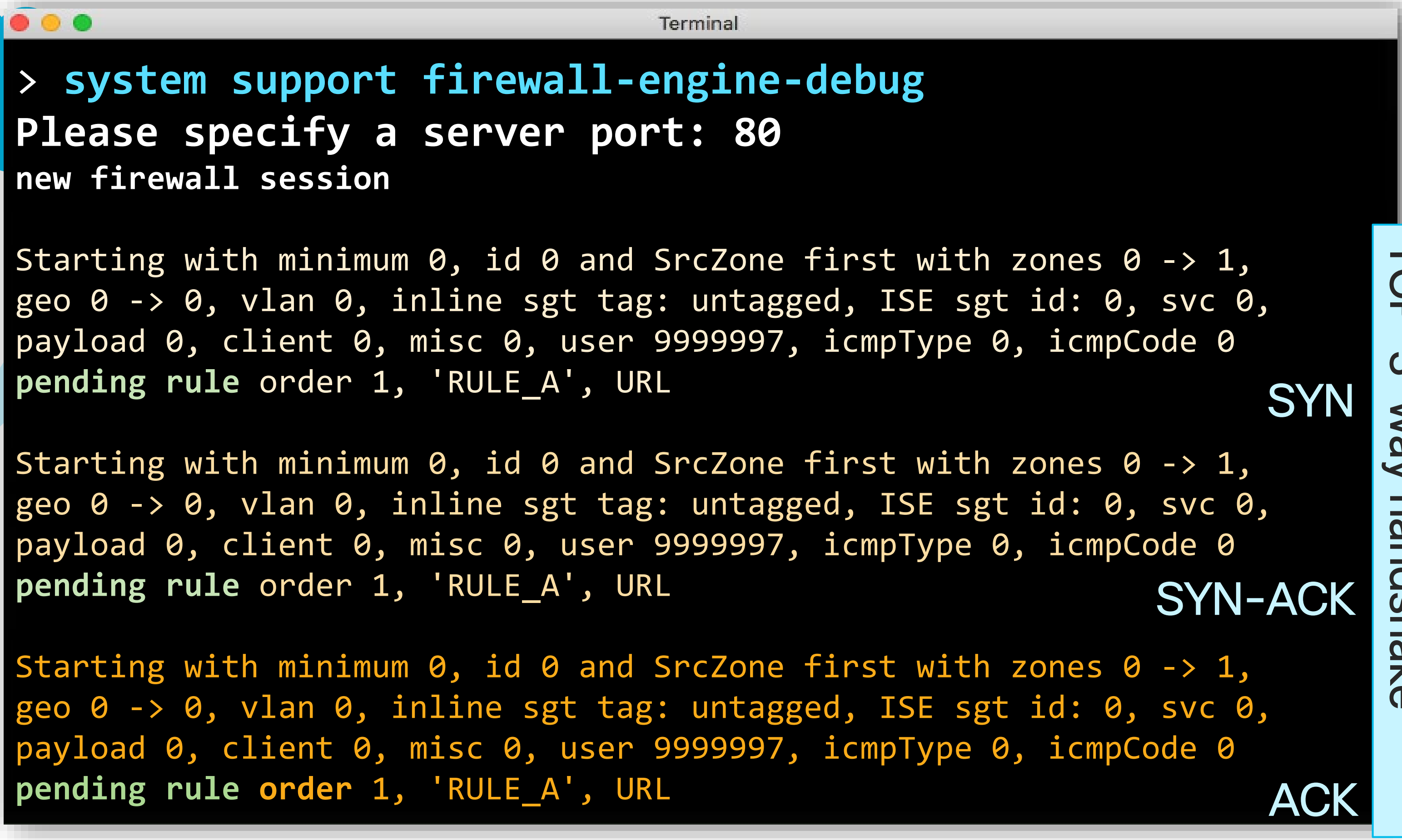
URL Cloud Lookup Process



FTD URL TTL Cache



- Prerequisites
- FMC and sensor (inline) >= 6.3
- Sensor has URL filtering license
- Access Control Policy Rule with URL category/reputation level
  - Rule A => any/…/any/Social Networking/…/Block
- FMC: System > Integration > Cisco CSI
  - Enable URL filtering
  - Query Cisco CSI for unknown URL's



```
> system support firewall-engine-debug
Please specify a server port: 80
new firewall session

Starting with minimum 0, id 0 and SrcZone first with zones 0 -> 1,
geo 0 -> 0, vlan 0, inline sgt tag: untagged, ISE sgt id: 0, svc 0,
payload 0, client 0, misc 0, user 9999997, icmpType 0, icmpCode 0
pending rule order 1, 'RULE_A', URL

Starting with minimum 0, id 0 and SrcZone first with zones 0 -> 1,
geo 0 -> 0, vlan 0, inline sgt tag: untagged, ISE sgt id: 0, svc 0,
payload 0, client 0, misc 0, user 9999997, icmpType 0, icmpCode 0
pending rule order 1, 'RULE_A', URL

Starting with minimum 0, id 0 and SrcZone first with zones 0 -> 1,
geo 0 -> 0, vlan 0, inline sgt tag: untagged, ISE sgt id: 0, svc 0,
payload 0, client 0, misc 0, user 9999997, icmpType 0, icmpCode 0
pending rule order 1, 'RULE_A', URL
```

SYN

SYN-ACK

ACK

TCP-3-way handshake

Terminal

```
 Starting with minimum 0, id 0 and SrcZone first with zones 0 -> 1, geo
0(0) -> 0, vlan 0, inline sgt tag: untagged, ISE sgt id: 0, svc 1122,
payload 0, client 1                                  9999997, url www.example.com, xff

:                                  LData:  www.example.com found in cache, index: 96,
r

: DataMessaging_GetURLData: Cache hit url www.example.com category 12,
returning URL_SFTYPE

 rule order 1, 'RULE_A', URL Lookup Success: www.example.com waited: 0ms

 no match rule order 1, 'RULE_A', url=(www.example.com) c=12 r=96

 match rule order 2, id 268434432 action Allow

 allow action
```

URL identified

Entry in CACHE

Immediate results

Getting info from the CACHE

Stale URL information

Terminal

```
> system support firewall-engine-debug
Please specify a server port: 80
new firewall session

Starting with minimum 0, id 0 and SrcZone first with zones 0 -> 1, geo 0
-> 0, vlan 0, inline sgt tag: untagged, ISE sgt id: 0, svc 0, payload 0,
client 0, misc 0, user 9999997, icmpType 0, icmpCode 0
 pending rule order 1, 'RULE_A', URL

 Starting with minimum 0, id 0 and SrcZone first with zones 0 -> 1, geo 0
-> 0, vlan 0, inline sgt tag: untagged, ISE sgt id: 0, svc 0, payload 0,
client 0, misc 0, user 9999997, icmpType 0, icmpCode 0
 pending rule order 1, 'RULE_A', URL

 Starting with minimum 0, id 0 and SrcZone first with zones 0 -> 1, geo 0
-> 0, vlan 0, inline sgt tag: untagged, ISE sgt id: 0, svc 0, payload 0,
client 0, misc 0, user 9999997, icmpType 0, icmpCode 0
 pending rule order 1, 'RULE_A', URL
```

TCP 3-way handshake

Terminal

```
 Starting with minimum 0, id 0 and SrcZone first with zones 0 -> 1, geo
0(0) -> 0, vlan 0, inline sgt tag: untagged, ISE sgt id: 0, svc 1122,
payload 0, client 1296, misc 0, user 9999997, url www.example.com, xff


: DataMessaging_GetURLData: www.example.com found in cache, index: 96,
rval: 59
: DataMessaging_GetURLData: Cache hit url www.example.com category 12,
returning URL_SFTYPE

: DataMessaging_GetURLData: Current category is stale for url
www.whateverworks.com, cache entry times out every 7200 sec
: DataMessaging_GetURLData: Adding url www.example.com to queue
: DataMessaging_GetURLData: Successfully added to queue

rule order 1, 'RULE_A', URL Lookup Success: www.example.com waited: 0ms
 no match rule order 1, 'RULE_A', url=(www.example.com) c=12 r=96
 match rule order 2, id 268434432 action Allow
 allow action
```

FOUND STALE INFO

FTD URL TTL Cache

- URL cache is not lost upon process restart
  - Information is being written to the disk

```
# cat /etc/sf/url_cache_seed_file.fmc
www.example.com,1548115153,96,1,12,4
```

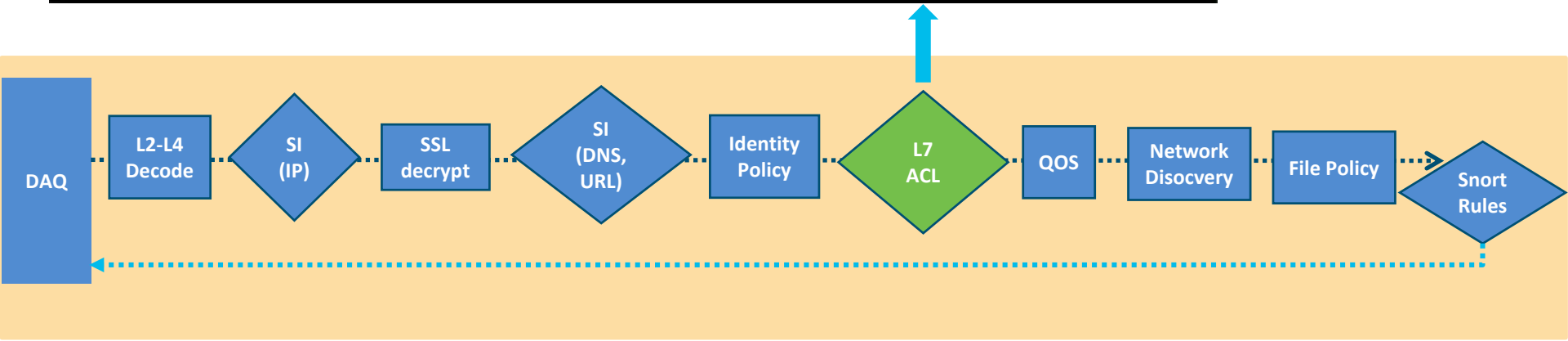
```
# cat /etc/sf/url_cache_seed_file.sensor
www.example.com:443,1548115153,96,1,12,4
```

```
$date -d@1548115153
```

Detection Debugging Tools

Terminal

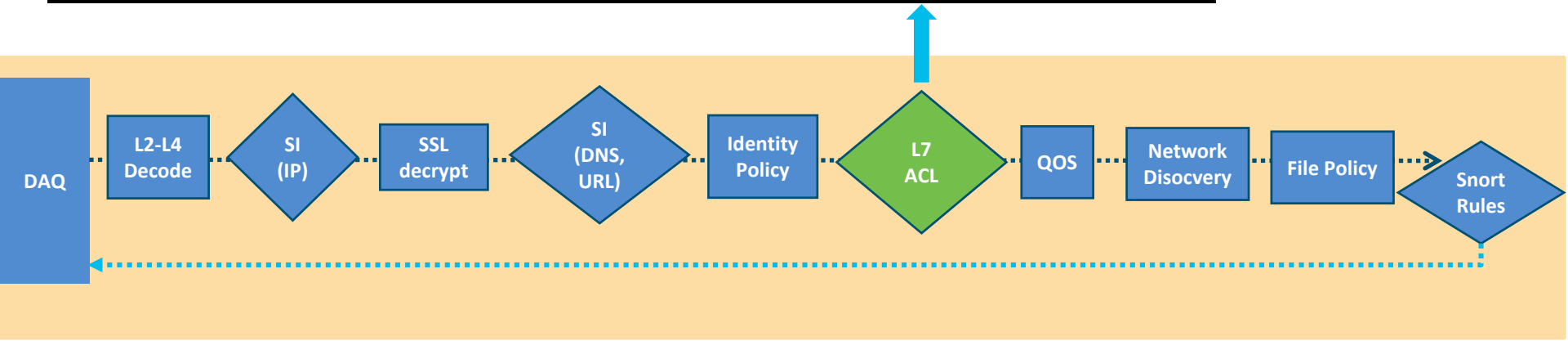
```
> system support firewall-engine-debug
192.168.10.200-58590 > 64.103.36.133-80 6 AS 1 I 1 rule order 3, id 268434436
URL Match Pending: www.example.com:443 waited: 0ms

# grep NGFWDbg /ngfw/var/log/messages
Jan 20 14:58:04 firepower SF-IMS[3371]: NGFWDbg 192.168.10.200-
58590 > 64.103.36.133-80 6 AS 1 I 1 rule order 3, id 268434436 URL
Match Pending: www.example.com:443 waited: 0ms
```



Detection Debugging Tools

Terminal

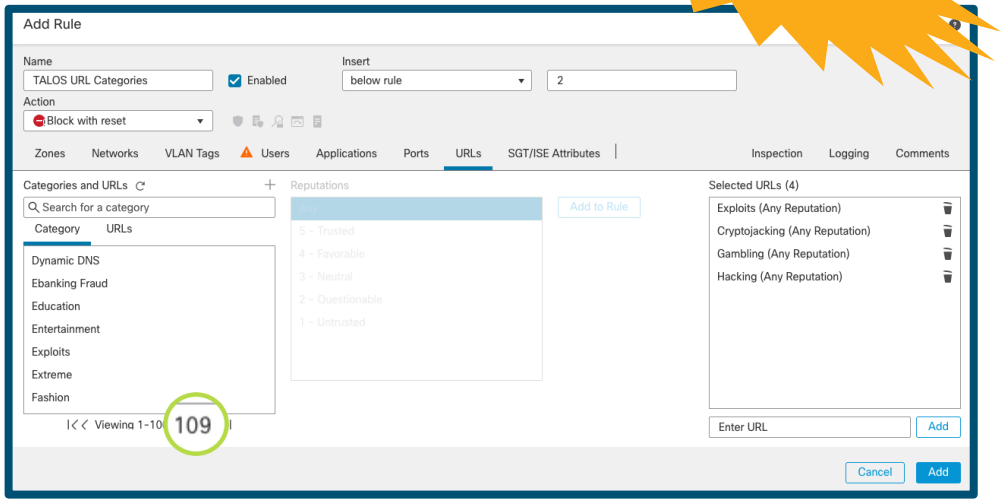
```
> system support firewall-engine-debug
192.168.10.200-58590 > 64.103.36.133-80 6 AS 1 I 1 rule order 3, id 268434436
URL Match Pending: www.example.com:443 waited: 0ms

# grep NGFWDbg /ngfw/var/log/messages
Jan 20 14:58:04 firepower SF-IMS[3371]: NGFWDbg 192.168.10.200-
58590 > 64.103.36.133-80 6 AS 1 I 1 rule order 3, id 268434436 URL
Match Pending: www.example.com:443 waited: 0ms
```



New Web Category Filtering Engine - TALOS

- URL Engine on NGFW is aligned with other Cisco Products like WSA
  - Use Cisco Talos Database
- Benefits
  - More URL categories compared to previous engine (Bright Cloud)
  - Better miscategorization dispute mechanism
  - Support for category changes

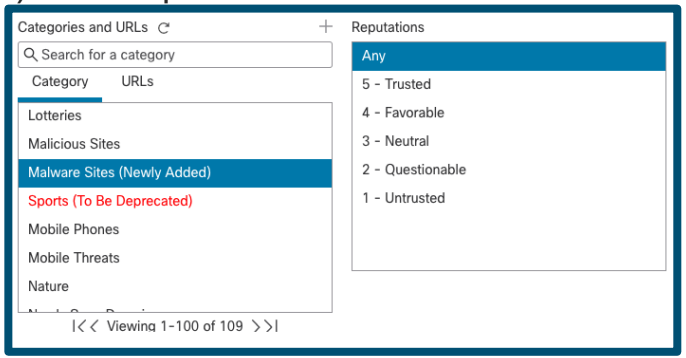
Changes in 6.5 release



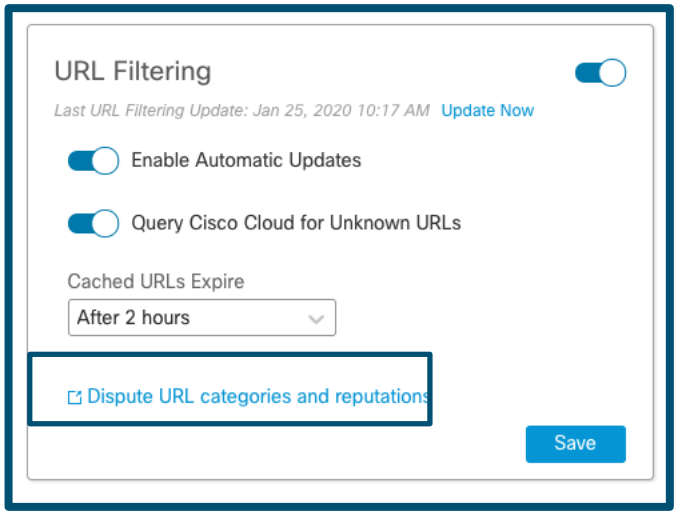
New Web Category Filtering Engine - TALOS

Changes in 6.5 release
FMC / FDM

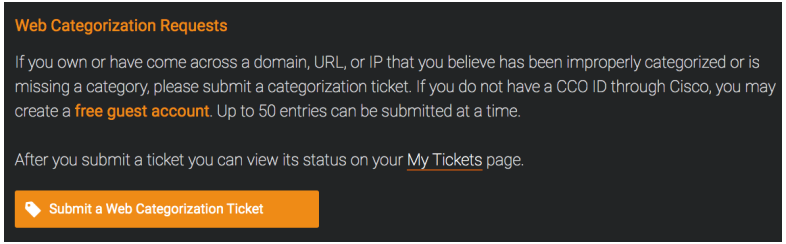
- URL categories can be added/removed over time
- User will learn about Web Category changes via System Notification Warnings
  - Available In AC, SSL and QOS policies
    - The rule contains deprecated URL categories
    - The rule contains to be deprecated URL categories
    - The rule contains newly added URL categories
- Save and deploy of policy (manual or scheduled) is not possible when the rule includes deprecated URL category



New Web Category Filtering Engine - TALOS

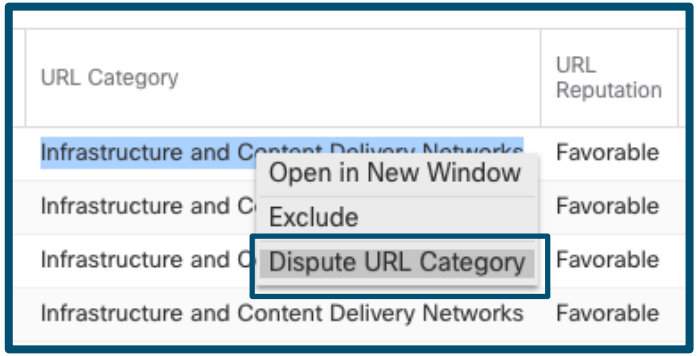


System > Integration > Cloud Services



Changes in 6.5 release
FMC / FDM

Analysis > Connection Events



Snort-preserve
&
mid-stream handling

Snort Reload / Restart

How to confirm?

```
# grep ”RELOAD snort\|RESTART snort”  /ngfw/log/action_queue.log
Dec 21 02:53:16 firepower policy_apply.pl[4451]: RELOAD snort at
/ngfw/var/cisco/deploy/sandbox/exporter-pkg/code/SF/NGFW/PolicyApply.pm line 1518
Dec 21 03:43:44 firepower policy_apply.pl[18318]: RESTART snort at
/ngfw/var/cisco/deploy/sandbox/exporter-pkg/code/SF/NGFW/PolicyApply.pm line 1518
```

```
# grep -i "Reload" /ngfw/var/log/messages*
Dec 22 10:14:31 ciscoasa SF-IMS[8994]: --== Reloading Snort ==--
Dec 22 10:14:52 ciscoasa SF-IMS[8994]: --== Reload Complete ==-
```

reload took 21sec

Snort Reload / Restart

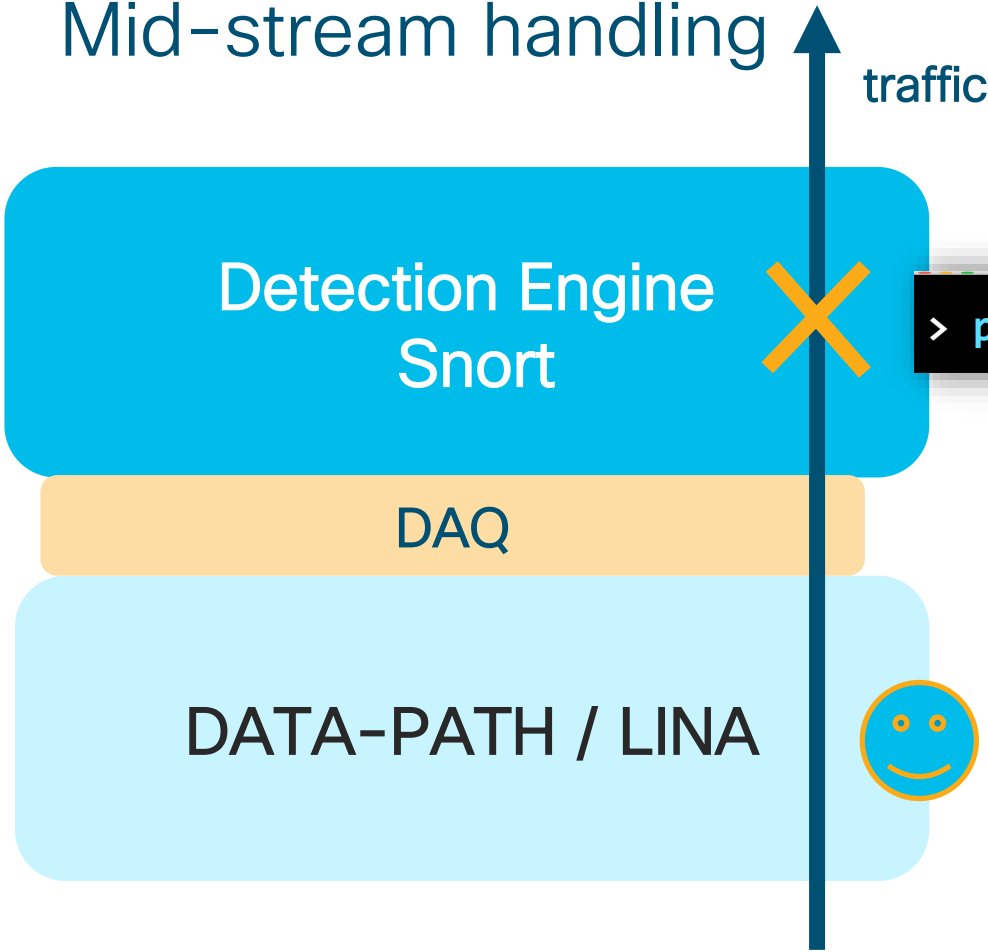
How to confirm?

```
# while true; do ASALinaCliUtilShow "conn address 10.10.2.1" | grep
outside;  sleep 1; done
TCP outside  10.10.2.1:8080 inside  192.168.10.1:39703, idle 0:00:03,
bytes 6848, flags UIO N1
TCP outside  10.10.2.1:8080 inside  192.168.10.1:39703, idle 0:00:01,
bytes 8848, flags UIO N2
```

```
# pmtool restartbytype snort
```

```
> configure snort preserve-connection disable/enable
```

Mid-stream handling

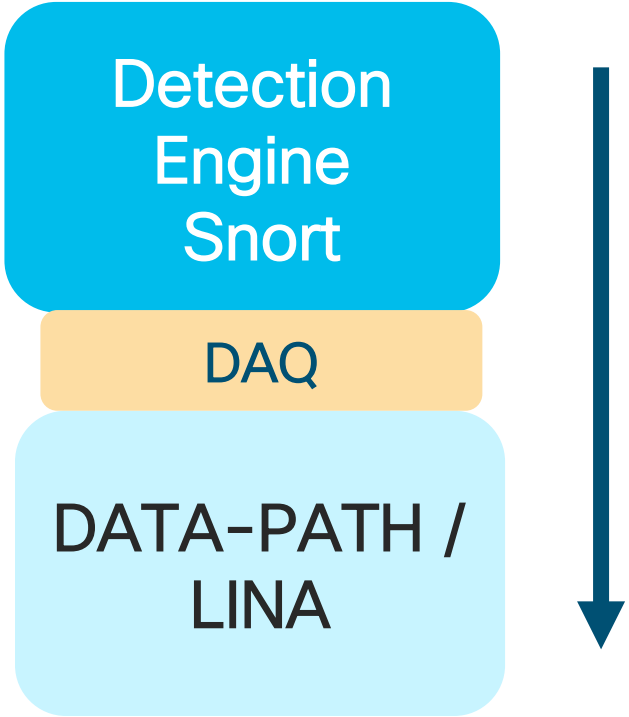



```
> pmtool restartbytype DetectionEngine
```

Common issues:

- incorrect rule match
- traffic can be blacklisted

Mid-stream handling



When an AC rule is matched in SNORT, it will send following data to DAQ:

Rule-id	AC rule that flow matched
Revision-id	current revision ID at the time of rule match
Rule-action	rule action from Snort
Flags (EoF)	if “log at the end of the connection” is set for an AC rule

DAQ will send above data to LINA.

Terminal

```
> system support trace

match rule order 4, id 268434432 action Allow

MidRecovery data sent for rule id: 268434432,rule_action:2,
rev id:2675917916, rule_match flag:0x0

allow action
```

SNORT sends mid-recovery data to LINA via DAQ

Terminal

```
> system support diagnostic-cli
# debug snort generic
# debug snort events
# debug pdts
Data received from upper layer:
   Rule ID:      268434432
   Rule Action:  -1619049380
   Rev ID:       2
   Flags:        0x0

Data stored in conn meta:
 Rule ID:       268434432
 Rule Action:   2
 Rev ID:        -1619049380
 Flags:         0x4
```

LINA debugs

Data received from **SNORT** over **DAQ** to **LINA** as CONNECTION METADATA

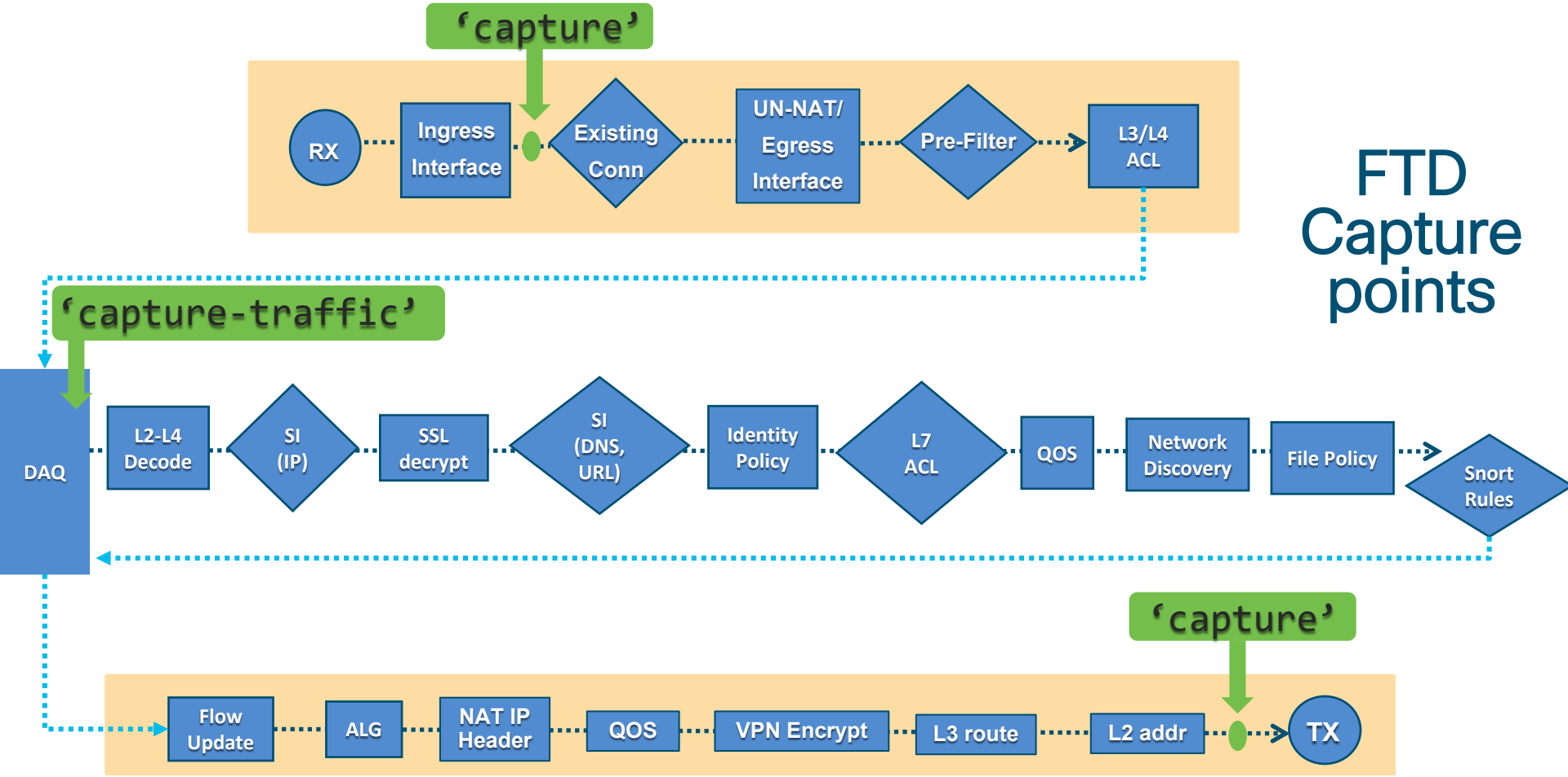
Terminal

```
> system support trace

AppID: serviceunknown(0), applicationunknown(0)

MidRecovery data queried. Got session type 2, ruleid:
268434432, rule_action:2, revid:2675917916,ruleMatchflag:0x4

Using HW or preset rule order 4, ,‘Test Rule‘,actionAllow
```

SNORT query mid-recovery LINA via DAQ

Capture-points
&
Tools

FTD Capture points



Data-Path Packet Captures

Data-path captures

History overview

CLISH – converged CLI

```
> capture IN interface inside match ip host 1.1.1.1 host 2.2.2.2
> system support diagnostic-cli
> enable
# capture IN interface inside match ip host 1.1.1.1 host 2.2.2.2
```

Diagnostic-CLI

- FTD Data-path capture is the same as on the ASA platforms
- Initially supported in FTD Diagnostic CLI only, in post 6.1 releases the tool was added into converged CLI that is called CLISH

Working with FTD packet captures:
https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/212474-working-with-firepower-threat-defense-f.html

Data-path captures

Pre-6.3 behavior

- Buffer size up to 32MB
- Possibility to view captures live: **show capture <name>**
- Classic capture allows you to trace captures up to 1000 packets:

 # capture <name> trace trace-count 1000

```
# capture in type raw-data buffer 33554432 interface inside-
linux circular-buffer match tcp any any eq 443

# copy /noconfirm /pcap capture:/in disk0:/in.pcap
```

Data-path captures

Exporting captures each 1 minute

```
# vim /ngfw/var/common/capture.sh
/usr/local/sf/bin/sfcli.pl converged_cmd converged_cli_util 'copy
/noconfirm /pcap capture:INSIDE disk0:temp.pcap' && mv
/mnt/disk0/temp.pcap /ngfw/var/common/rolling-pcap-$(date '+%Y-%m-%d-
%T').pcap
:wq!

# ln -s /ngfw/usr/bin/vi /bin/vi

# crontab -e
* * * * *     bash /ngfw/var/common/capture.sh
:wq!
```

Data-path captures

Exporting captures each 1 minute

Terminal

```
# crontab -l
* * * * *
```

minute

hour

day (month)

month

day (week)

```
bash /ngfw/var/common/capture.sh
```

various examples

https://crontab.guru/examples.html

Data-path captures

Exporting captures each 1 minute

Terminal

```
# ls -la /ngfw/var/common/ | grep -i pcap

-rwxr-xr-x  1 root root          9644 Jan 12 18:55 rolling-pcap-2019-
01-12-18:55:14.pcap
-rwxr-xr-x  1 root root          9644 Jan 12 18:56 rolling-pcap-2019-
01-12-18:56:01.pcap
-rwxr-xr-x  1 root root         82143 Jan 12 18:57 rolling-pcap-
2019-01-12-18:57:02.pcap
-rwxr-xr-x  1 root root         93544 Jan 12 18:58 rolling-pcap-
2019-01-12-18:58:01.pcap
…
```

Data-path captures

Exporting captures each 1 minute

Terminal

```
! Pushed to FTD via FlexConfig object
# sh run event
event manager applet EEM_TAC
 event timer watchdog time 60
 action 1 cli command "show asp drop"
 action 2 cli command "sh conn"
 action 3 cli command "copy /noconfirm /pcap capture:INSIDE
disk0:/in.pcap"
 output file append disk0:EEM_TAC
```

Data-path captures

Exporting captures each 1 minute

Terminal

```
# show event manager
event manager applet EEM_TAC, hits 4, last 2019/01/12 19:16:02
  last file disk0:/EEM_TAC
  event watchdog 60 secs, left 55 secs, hits 4, last 2019/01/12
19:16:02
  action 1 cli command "show asp drop", hits 4, last 2019/01/12
19:16:02
  action 2 cli command "sh conn", hits 4, last 2019/01/12 19:16:02
  action 3 cli command "copy /noconfirm /pcap capture:INSIDE
disk0:/in.pcap", hits 4, last 2019/01/12 19:16:02

# ls /mnt/disk0/ -la | grep pcap
-rwxr-xr-x 1 root root  9644 Jan 12 19:16 in.pcap
```

6.3 release introduces extended capture size up to 10 000MB

Terminal

```
# capture <NAME> interface <NAMEIF> ?
  buffer              Configure size of capture buffer, default is 512 KB
  circular-buffer     Overwrite buffer from beginning when full, default
is
                      non-circular
file-size           Configure size of capture file in MB (32 - 10000)

# capture INSIDE interface INTERNAL-INT file-size 10000

# show disk0:
408439725  24          Dec 28 2018 10:05:12  INSIDE.pcap

# copy /noconfirm disk0:INSIDE.pcap scp://admin@10.10.10.100
```

Caution: multiple captures with file-size option can starve the processor!

Snort Packet Captures

Detection engine captures

Rolling packet capture

```
Terminal
# /usr/local/sf/bin/sfcli.pl capture traffic
Selecting the inline set
-s 0 -C 500 -W 20 -w rollingcapture.pcap
CTRL + z
# bg
# disown
```

- CTRL + z → suspend a current foreground job (capture-traffic)
- # bg → to start a stopped process in background
- # disown → instruct shell to not terminate a process after exiting the terminal session

Series-3 (7000/8000)

... momentarily network outage, why?

Detection engine captures

Rolling packet captures procedure

```
> capture-traffic
Please choose domain to capture traffic from:
  0 - br1
  1 - Router
Selection? 1
Please specify tcpdump options desired.
(or enter '?' for a list of supported options)
Options: -s 0 -C 500 -W 20 -w rolling-capture.pcap
```

FXOS
Packet Captures

FXOS captures

Control Plane

```
# ethanalyzer local interface mgmt capture-filter "icmp" limit-captured-frames 50
 Capturing on eth0 wireshark-broadcom-rcpu-dissector: ethertype=0xde08, devicetype=0x0
2018-12-18 10:05:05.535698 10.10.10.100 -> 192.168.10.1 ICMP Echo (ping) request
2018-12-18 10:05:06.546796 10.10.10.100 -> 192.168.10.1 ICMP Echo (ping) request
```

TIPS

Upgrade FXOS captures are **bidirectional** starting from FXOS version **2.3.1.97+**

```
2018-12-18 10:05:05.535698 10.10.10.100 -> 192.168.10.1 ICMP Echo (ping) request
2018-12-18 10:05:05.556851 192.168.10.1 -> 10.10.10.100 ICMP Echo (ping) reply
```


User Story: Disk and Logging

FMC: “Frequent drain of Connection Events”

Description

- FMC generate critical health alert for disk usage because of frequent drain of connection events
- Access Control Policy Rules has been tuned, logging optimized
- Error message still does not get cleared

User Story: Disk and Logging

Access Control Policy tuning based on logging hit counters

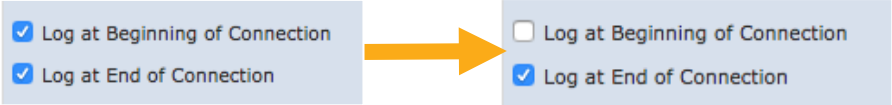
Terminal

```
> show access-control-config
> pmtool restartbytype DetectionEngine
# /usr/local/sf/bin/sfcli.pl show firewall | grep "Rule\:\|Rule Hits"

Rule Hits                    : 0
------------------[ Rule: bypass ]------------------
    Rule Hits                : 0
------[ Rule: block all social media URL cat ]------
    Rule Hits                : 0
```


User Story: Disk and Logging

Access Control Policy logging hit counters

```
# /usr/local/sf/bin/sfcli.pl show firewall | grep "Rule\:\|Rule Hits"
Rule Hits                    : 45
------------------[ Rule: bypass ]------------------
    Rule Hits                : 100216
------[ Rule: block all social media URL cat ]------
    Rule Hits                : 125
```



User Story: Disk and Logging

Access Control Policy logging hit counters

FMC 6.4

Hit Count

192.168.0.12 | Fetch Current Hit Count | Last Fetched :2018-11-15 14:38:40 (3 minute(s) ago)

Clear Hit Count | Filter Rules | Show Zero Hit Count Rules

#	Rule Name	Policy Name	Hit Count	Last Hit Time
4	Rule 03	Global AC Policy	96	2018-11-02 06:08:08
2	Rule 01	Global AC Policy	41	2018-11-02 06:08:04
5	Rule 04	Global AC Policy	23	2018-11-02 06:08:10
3	Rule 02	Global AC Policy	15	2018-11-02 06:08:06
1	vreyGrule	Global AC Policy	0	
6	any-any-block	Global AC Policy	0	

Displaying 1-7 of 7 rows | Page 1 of 1

Generate PDF | Close

Sort Ascending
Sort Descending
Columns
Rule Name
Policy Name
First Hit Time

Deploy | Show | Inherit | Displaying 1 - 6 of 6 rules

Analysis > Access Control Policy > Edit Policy > Analyze Hit Count

User Story: Disk and Logging

Access Control Policy logging hit counters

FTD 6.4

```
> show rule hits

RuleID                  Hit Count           First Hit Time(UTC)     Last Hit
Time(UTC)
-----------------------------------------------------------------------------
268436981               2                   22:02:00 Apr 25 2019     22:02:02
Apr 25 2019
268436925               2                   22:01:53 Apr 25 2019     22:04:51
Apr 25 2019
```


User Story: Disk and Logging

FMC “Frequent drain of connection events” health alert

TIPS

Configure logging system to write into SSD instead of RAMDISK:

```
> configure log-events-to-ramdisk disable
Now logging connection events to SSD.
Task inserted into queue and Snort will restart.
```

Live monitoring of silo’s file size growth:

```
# watch 'sudo /usr/local/sf/bin/sfcli.pl showdiskmanager system'
```

Verification, whether we are logging into SSD or RAMDISK:

```
> show log-events-to-ramdisk
Logging connection events to SSD.
```

```
> show log-events-to-ramdisk
Logging connection events to RAM Disk.
```

Note, **virtual appliances** does **not support** this configuration option.

User Story

Intermittent connectivity issue

Description

- Network down situation every evening hours
- Device is no accessible during time of the issue
- Network operation is restored without human intervention after certain period of the time
- There is no reboot scheduled

User Story

Intermittent connectivity issue

✔ Generate Troubleshooting Files

Generate troubleshooting files for firepower.servertest.com.
Click to retrieve generated files.

Terminal

```
Jan 23 19:28:53 firepower init: Id "ftd1" respawning too fast
Jan 23 19:30:01 firepower crond[5358]: pam_unix(crond:session)
Jan 23 19:30:01 firepower CROND[5358]: pam_unix(crond:session)
Jan 23 19:32:45 firepower SF-IMS[3685]: [3714] sfmgr:sfmanager
Jan 23 19:53:20 firepower SF-IMS[2781]: [2781] pm:process

# uptime
 19:57:22 up 4 min,  1 user,  load average: 0.38, 0.47, 0.23
```

User Story

Hardware error on LCD screen

Description

"**HARDWARE ERROR**" message displayed

on the LCD panel screen

of Firepower Sensor

Closure

What is current FTD suggested release and why?

FTD **6.4.0.7** is the suggested release for customers looking for reliability and stability

High-Value Features

- Hit counts for ACL and Pre-filter
- Multi-Instance
- SSL Hardware Acceleration
- Integration with CTR and Splunk
- FMCv on Azure
- RA VPN + S2S enhancements
- API enhancements FMC/FDM
- Scheduling backups of managed devices

Eliminates challenges

- Improved deploy times

Around 48% faster than 6.2.3

Around 20% faster than 6.3.0

Strongest FTD release

- > 20K downloads
- > 6.5k unique customers and partners
- Lowest amount of customer found defects

Useful references

- Voice of the Security TME

  https://www.youtube.com/channel/UC7rdKaO-3UPPXmkJkI6wgcg

- Clarifying the Firepower Threat Defense LINA process CPU utilization

  https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/200950-Clarifying-the-Firepower-Threat-Defense.html

- Snort Restart Traffic behavior

  https://www.cisco.com/c/en/us/td/docs/security/firepower/630/configuration/guide/fpmc-config-guide-v63/policy_management.html#concept_uc1_gtq_ty – 6.3 release

  https://www.cisco.com/c/en/us/td/docs/security/firepower/640/configuration/guide/fpmc-config-guide-v64/policy_management.html#concept_33516C5D6B574B6888B1A05F956ABDF9 – 6.4 release

- TAC documents

  https://www.cisco.com/c/en/us/support/docs/security/firesight-management-center/118889-technote-firesight-00.html

Useful references

- **Hardening FTD/FMC**

  https://www.cisco.com/c/en/us/td/docs/security/firepower/640/hardening/ftd/FTD_Hardening_Guide_v64.html

- Configuration has added "**Best Practices**" sections on various functionalities like
  - Access Rule Creation
  - Intrusion Policy
  - NAP Policy

- **NGFW Policy Order of Operations**

  https://www.cisco.com/c/dam/en/us/td/docs/security/firepower/Self-Help/NGFW_Policy_Order_of_Operations.pdf

- **Rule Expansion**

  https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/200522-Understand-the-Rule-Expansion-on-FirePOW.html

Useful references – NGFW White Papers

NEW & Recommended!

https://www.cisco.com/c/en/us/products/security/firepower-ngfw/white-paper-listing.html

Products & Services / Security /

White Papers

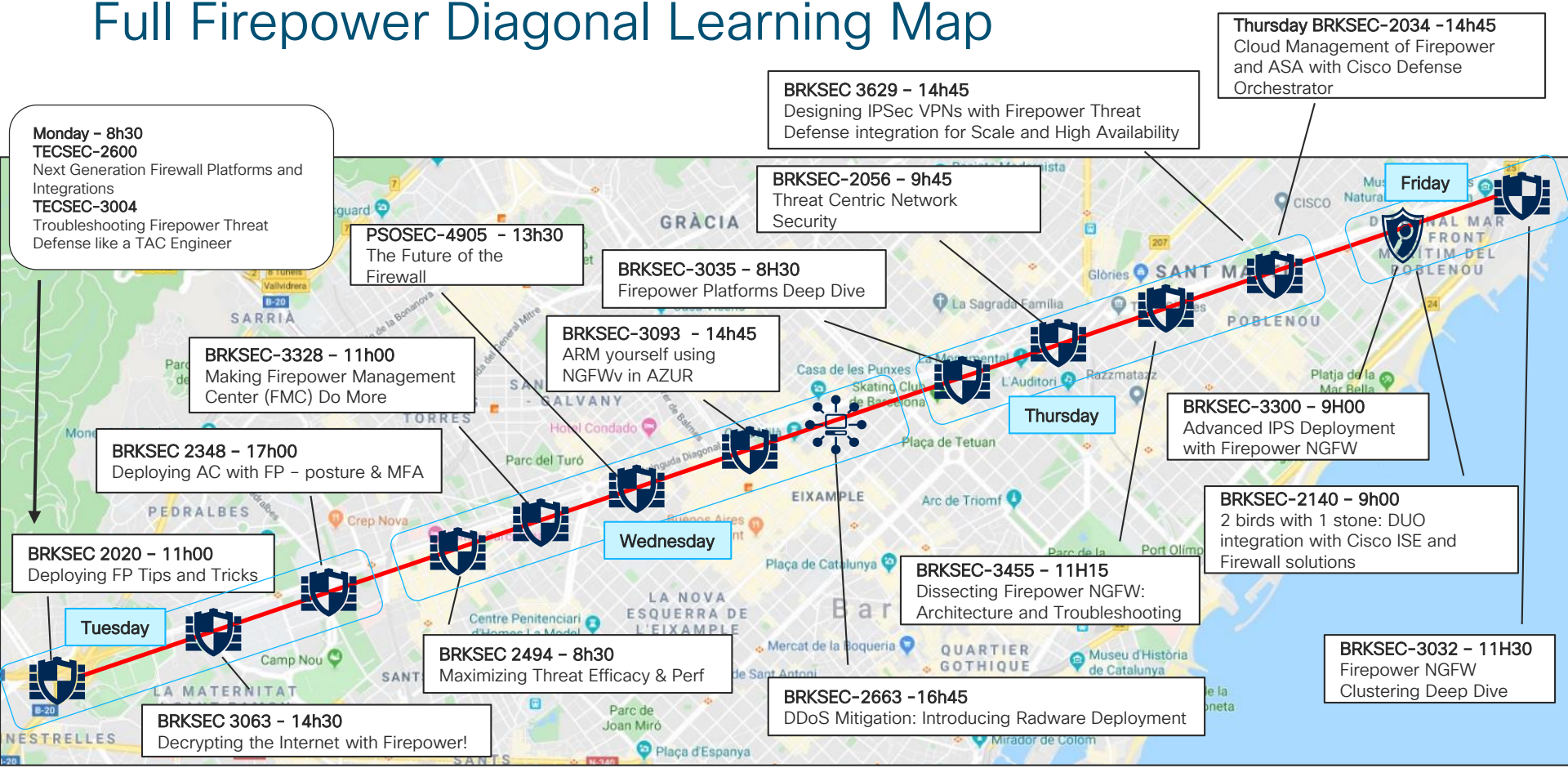
Cisco (NGFWv) and (ASAv) in Public Cloud (Azure and AWS) White Paper

Cisco Firepower Threat Defense (FTD) SNMP Monitoring White Paper UPDATED

Cisco Firepower Threat Defense Multi-Instance Capability on Cisco Firepower 4100 and 9300 Series Appliances White Paper NEW

Identity Awareness and Control on Cisco Firepower NGFW Guide NEW

Full Firepower Diagonal Learning Map



#CLEUR NGFW related session

BRKSEC-2034

Cloud Management of Firepower and ASA with Cisco Defense Orchestrator

14:45
Thursday

BRKSEC-3032

Firepower NGFW Clustering Deep Dive

11:30
Friday

BRKSEC-3300

Advanced IPS Deployment with Firepower NGFW

9:00
Friday

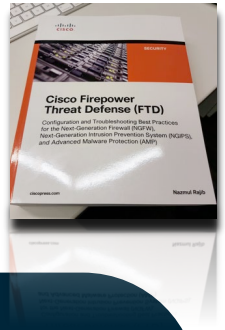
https://ciscolive.cisco.com/on-demand-library/

Complete your online session survey

- Please complete your session survey after each session. Your feedback is very important.
- Complete a minimum of 4 session surveys and the Overall Conference survey (starting on Thursday) to receive your Cisco Live t-shirt.
- All surveys can be taken in the Cisco Events Mobile App or by logging in to the Content Catalog on ciscolive.com/emea.

Cisco Live sessions will be available for viewing on demand after the event at ciscolive.com.

Continue your education

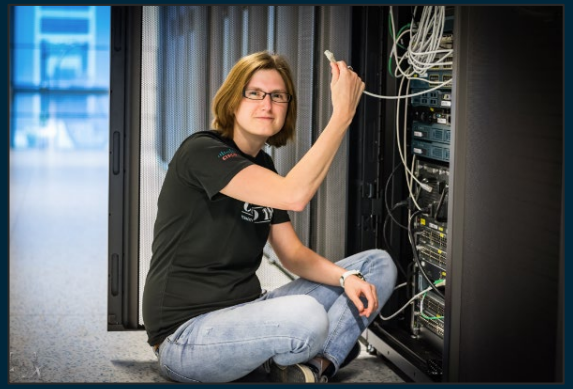


Demos in the Cisco campus

Walk-in labs

Meet the engineer 1:1 meetings

Related sessions



Thank you

CISCO

You make **possible**