Think Like a TAC Engineer

A guide to Cisco Secure Firewall most common pain points

Ghada Hijazi – Technical Consulting Engineer

BRKSEC-3533

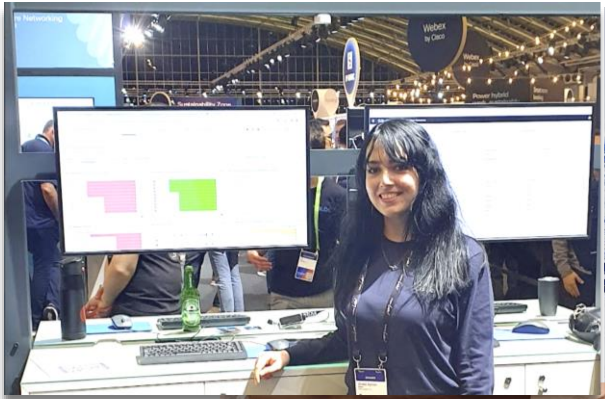
> *“If I had an hour to solve a problem I'd spend 55 minutes thinking about the problem and 5 minutes thinking about solutions.”*

Albert Einstein

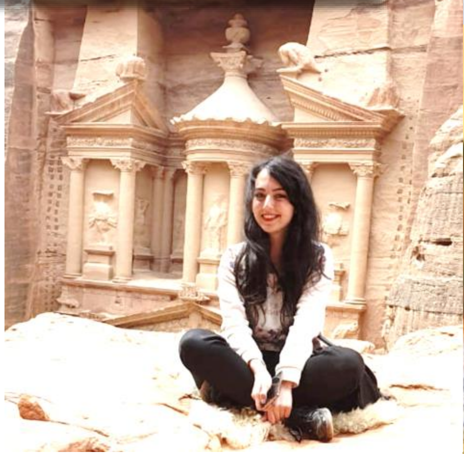
Your Speaker

Ghada Hijazi

- Originally from Jordan
- Based in Poland
- Escalation Engineer CX Security TAC
- 6 Years in Firewall TAC
- 2 Years in Security Professional Services
- Also, into drawing, traveling and books.



CISCO CERTIFIED CCNP SECURITY



SNORT®

Abstract

Tired of struggling with troubleshooting firewall issues that might hinder your daily tasks and activities? Cisco Secure Firewall is one of the most critical security controls in the modern network. Managing and troubleshooting potential issues is critical to ensure a stable and efficient network. The purpose of the session is to familiarize admins with the troubleshooting methodology for the latest, day-to-day, most common Firewall issues. The examples and use cases provided during this session are from real-life customer scenarios that were handled by Cisco TAC. By the end of the session, the attendee will have knowledge of the most recent common issues and should be able to troubleshoot and if possible, fix them before reaching TAC.

Agenda

- Secure Firewall most common pain points
  - Datapath/Connectivity issues:
    - A) Traffic flow
    - B) Troubleshooting tools
  - Upgrade
  - Performance
- Use case
- Wrap-up

Session Goals

- Understand and troubleshoot firewall most common issues.
- Isolate if it is the firewall causing the issue.
- Know when to open a TAC case.
- Become a better troubleshooter!

Before we Go Pact

- Watch out for Hidden Slides. ℹ
- The session will focus on the top case generators faced by TAC.
- This is a technical session, with no commercial or licensing topics.
- This is a troubleshooting session. Detailed configuration can be found in references.
- This is an advanced level session; general knowledge of Secure Firewall is expected.
- Questions at the end of the session.

Webex App

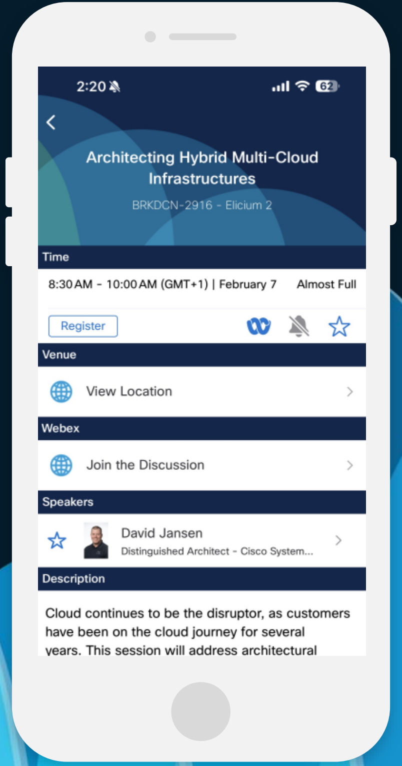
Questions?

Use the Webex app 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 the Webex app or go directly to the Webex space
4. Enter messages/questions in the Webex space

Webex spaces will be moderated by the speaker until February 28, 2025.



Architecting Hybrid Multi-Cloud Infrastructures

BRKDCN-2916 - Elicium 2

Time

8:30 AM - 10:00 AM (GMT+1) | February 7 Almost Full

Venue

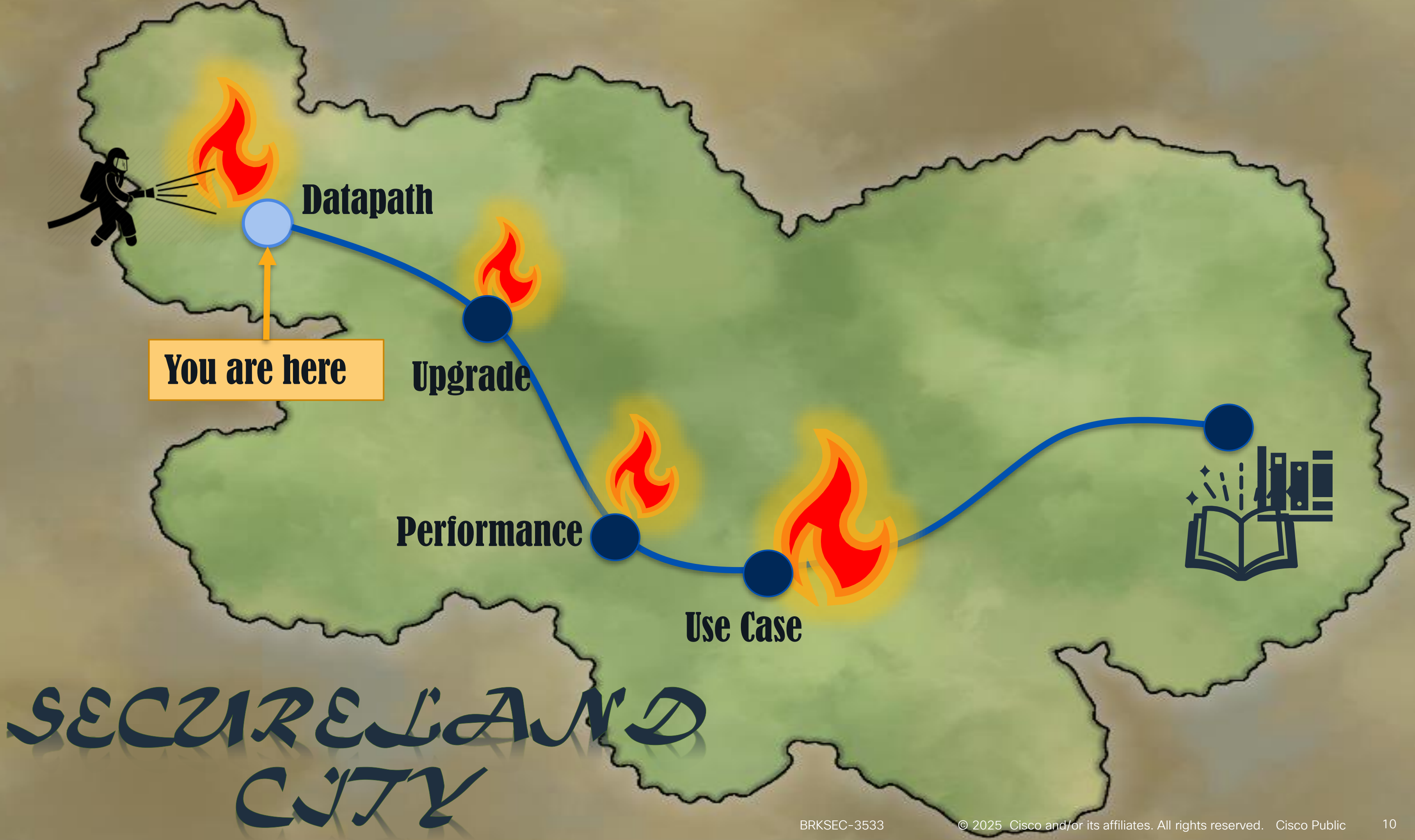
Webex

Speakers

David Jansen
Distinguished Architect - Cisco System...

Description

Cloud continues to be the disruptor, as customers have been on the cloud journey for several years. This session will address architectural

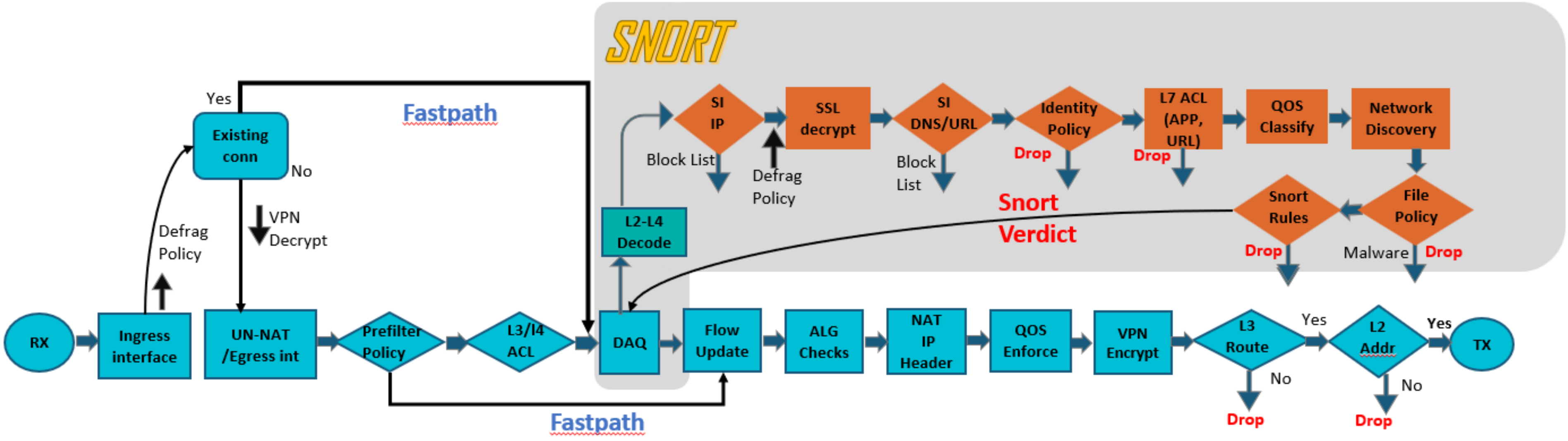

Datapath
You are here
Upgrade
Performance
Use Case
SECURELAND CITY

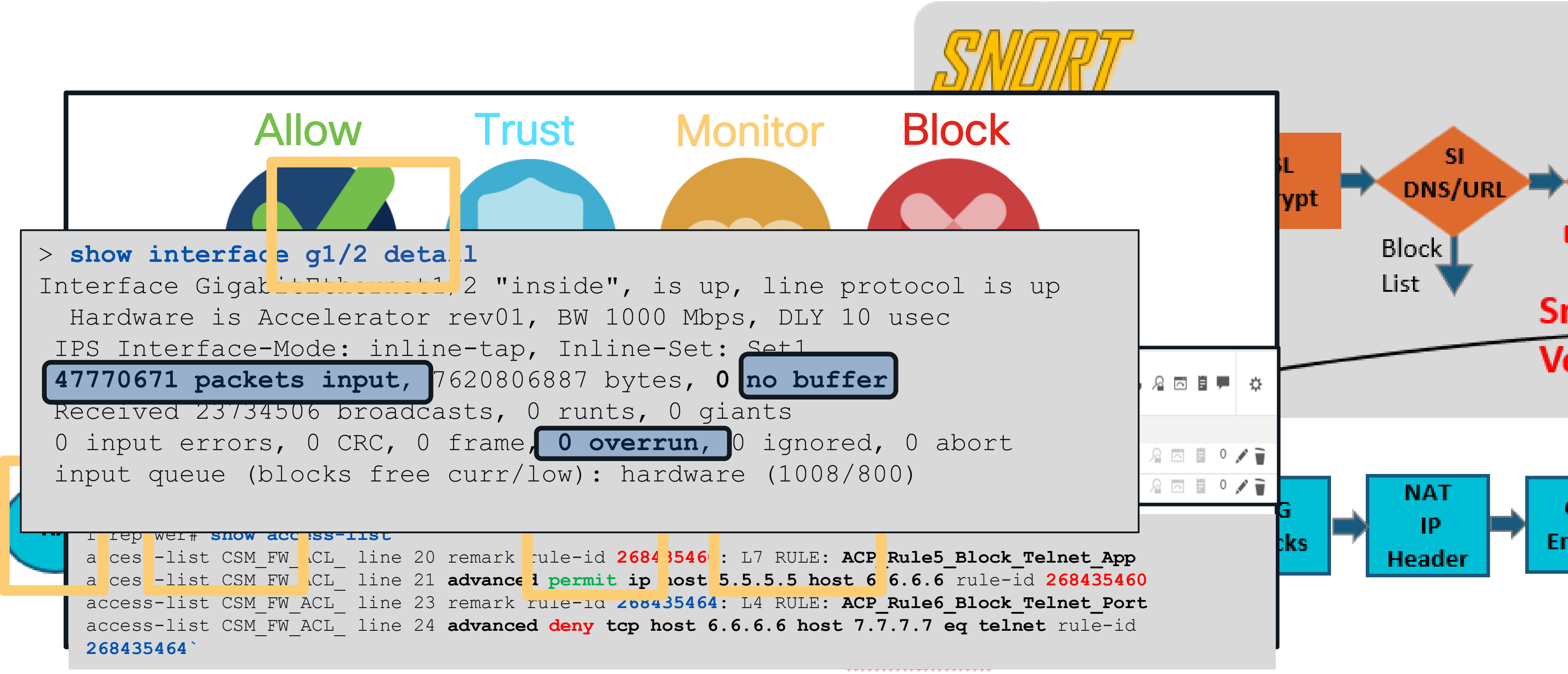
Datapath/Connectivity Issues

Secure Firewall Packet Processing – The Big Picture

Lina Engine

Snort Engine



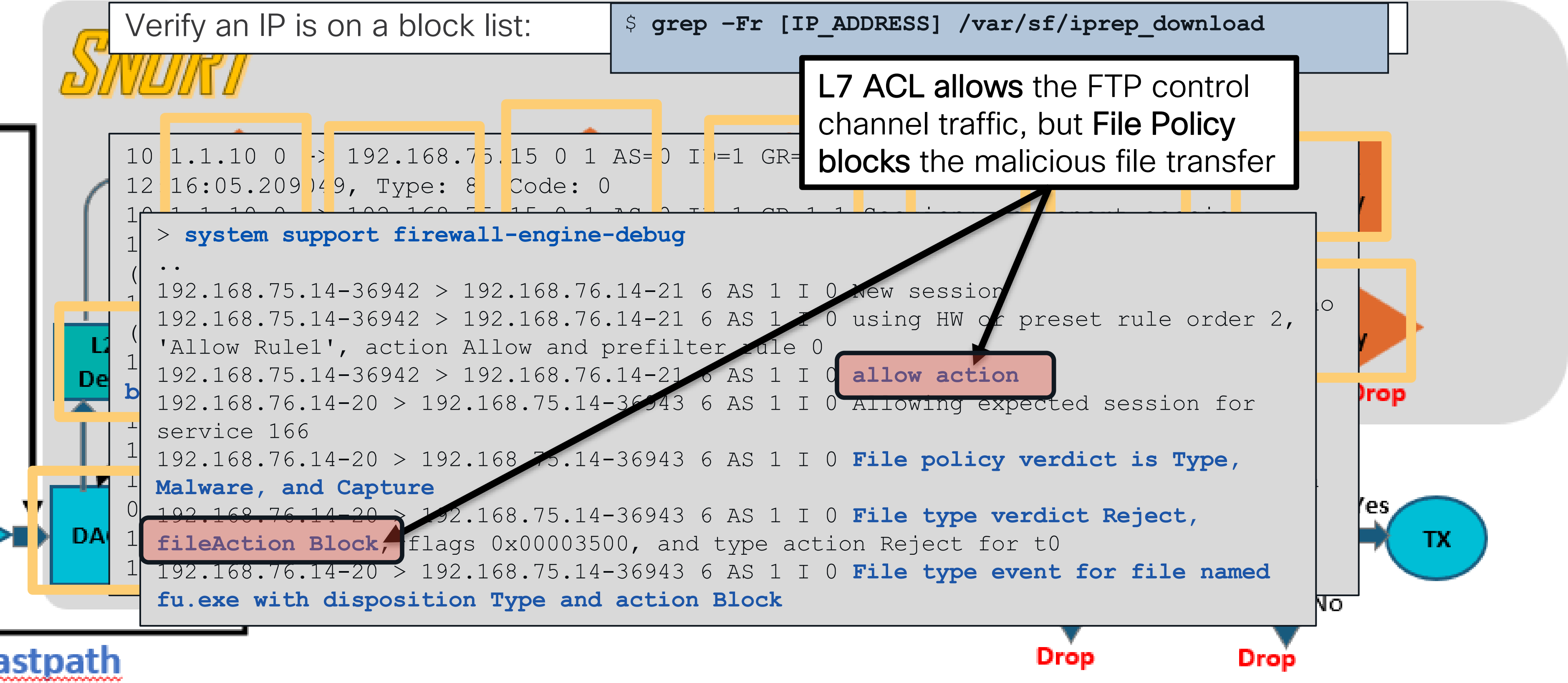


```
> show interface g1/2 detail
Interface GigabitEthernet1/2 "inside", is up, line protocol is up
  Hardware is Accelerator rev01, BW 1000 Mbps, DLY 10 usec
 IPS Interface-Mode: inline-tap, Inline-Set: Set1
 47770671 packets input, 7620806887 bytes, 0 no buffer
 Received 23734506 broadcasts, 0 runts, 0 giants
 0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
 input queue (blocks free curr/low): hardware (1008/800)
```

```
 I rep wer# show access-list
a ces -list CSM_FW_ ACL_ line 20 remark  ule-id 2684 546 : L7 RULE: ACP Rule5_Block_Telnet_App
a ces -list CSM_FW_ ACL_ line 21 advance  permit ip  ost 5.5.5.5 host 6 6.6.6 rule-id 268435460
access-list CSM_FW_ACL_ line 23 remark rule-id 268435464: L4 RULE: ACP_Rule6_Block_Telnet_Port
access-list CSM_FW_ACL_ line 24 advanced deny tcp host 6.6.6.6 host 7.7.7.7 eq telnet rule-id
268435464`
```

Verify an IP is on a block list:

```
$ grep -Fr [IP_ADDRESS] /var/sf/iprep_download
```



```
10 1.1.10 0 -> 192.168.75.15 0 1 AS=0 ID=1 GR=
12:16:05.209049, Type: 8 Code: 0
```

L7 ACL **allows** the FTP control channel traffic, but **File Policy blocks** the malicious file transfer

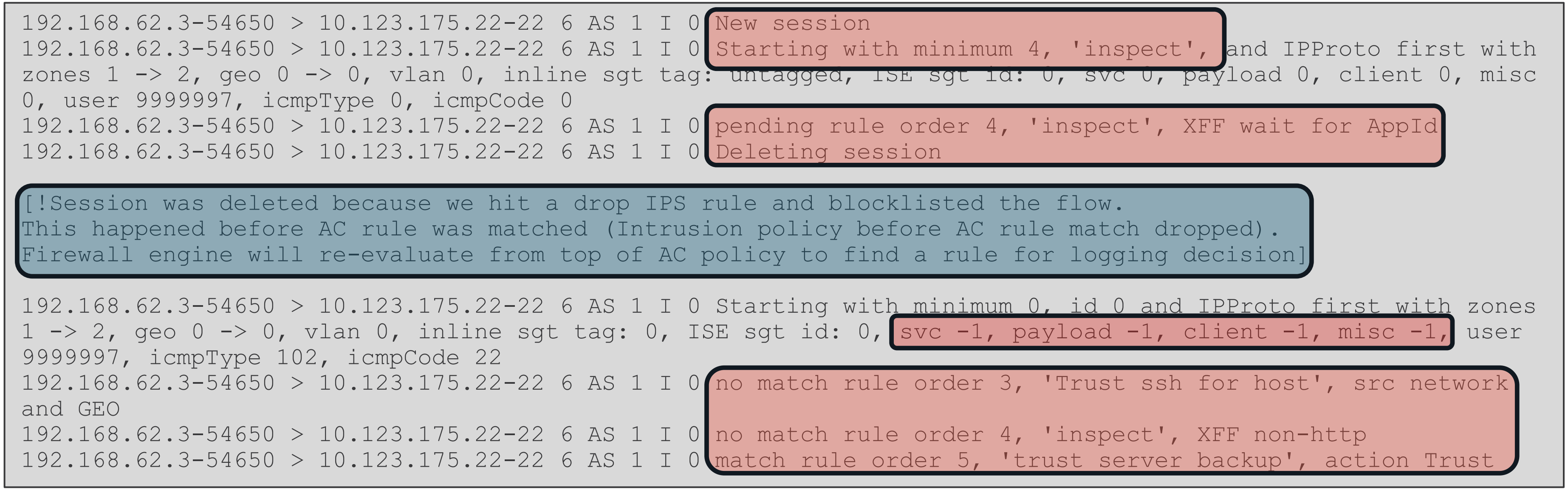
```
> system support firewall-engine-debug
..
192.168.75.14-36942 > 192.168.76.14-21 6 AS 1 I 0 New session
192.168.75.14-36942 > 192.168.76.14-21 6 AS 1 I 0 using HW or preset rule order 2,
'Allow Rule1', action Allow and prefilter rule 0
192.168.75.14-36942 > 192.168.76.14-21 6 AS 1 I 0 allow action
192.168.76.14-20 > 192.168.75.14-36943 6 AS 1 I 0 Allowing expected session for
service 166
192.168.76.14-20 > 192.168.75.14-36943 6 AS 1 I 0 File policy verdict is Type,
Malware, and Capture
192.168.76.14-20 > 192.168.75.14-36943 6 AS 1 I 0 File type verdict Reject,
fileAction Block, flags 0x00003500, and type action Reject for t0
192.168.76.14-20 > 192.168.75.14-36943 6 AS 1 I 0 File type event for file named
fu.exe with disposition Type and action Block
```

Intrusion policy before AC rule match

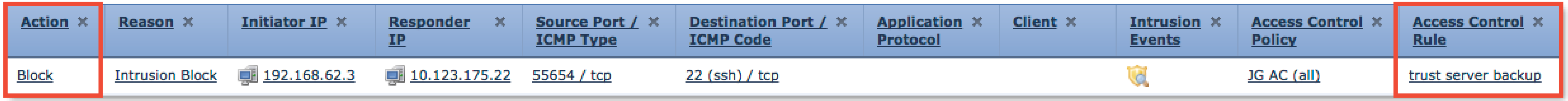
firewall-engine-debug

SSH Connection from 192.168.62.3 to 10.123.175.22

(Blocked/Ended before matching an AC rule)



```
192.168.62.3-54650 > 10.123.175.22-22 6 AS 1 I 0 New session
192.168.62.3-54650 > 10.123.175.22-22 6 AS 1 I 0 Starting with minimum 4, 'inspect', and IPProto first with
zones 1 -> 2, 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
192.168.62.3-54650 > 10.123.175.22-22 6 AS 1 I 0 pending rule order 4, 'inspect', XFF wait for AppId
192.168.62.3-54650 > 10.123.175.22-22 6 AS 1 I 0 Deleting session

[!Session was deleted because we hit a drop IPS rule and blocklisted the flow.
This happened before AC rule was matched (Intrusion policy before AC rule match dropped).
Firewall engine will re-evaluate from top of AC policy to find a rule for logging decision]

192.168.62.3-54650 > 10.123.175.22-22 6 AS 1 I 0 Starting with minimum 0, id 0 and IPProto first with zones
1 -> 2, geo 0 -> 0, vlan 0, inline sgt tag: 0, ISE sgt id: 0, svc -1, payload -1, client -1, misc -1, user
9999997, icmpType 102, icmpCode 22
192.168.62.3-54650 > 10.123.175.22-22 6 AS 1 I 0 no match rule order 3, 'Trust ssh for host', src network
and GEO
192.168.62.3-54650 > 10.123.175.22-22 6 AS 1 I 0 no match rule order 4, 'inspect', XFF non-http
192.168.62.3-54650 > 10.123.175.22-22 6 AS 1 I 0 match rule order 5, 'trust server backup', action Trust
```



Action	Reason	Initiator IP	Responder IP	Source Port / ICMP Type	Destination Port / ICMP Code	Application Protocol	Client	Intrusion Events	Access Control Policy	Access Control Rule
Block	Intrusion Block	192.168.62.3	10.123.175.22	55654 / tcp	22 (ssh) / tcp			🛡	JG AC (all)	trust server backup

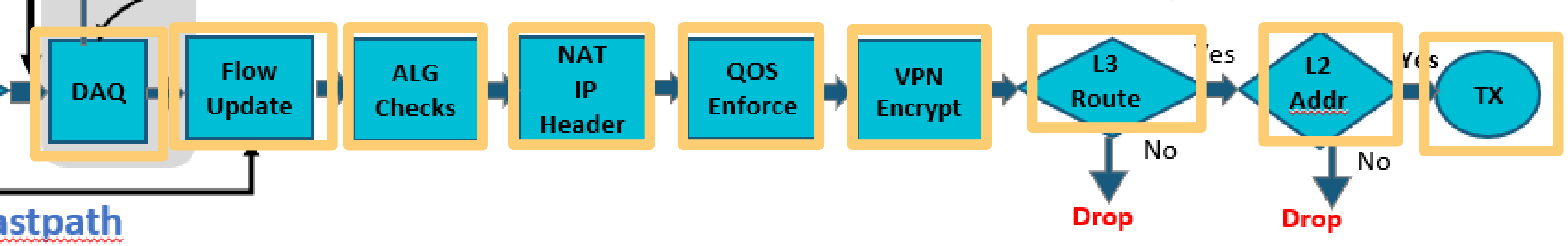
AC Rule has "Trust" action but connection event action shows "Block"

```
> show interface outside
Interface GigabitEthernet0/1 "outside", is up, line protocol is up
         …
         273399 packets output, 115316725 bytes, 80 underruns
         …
         input queue (blocks free curr/low): hardware (485/441)
         output queue (blocks free curr/low): hardware (463/0)
```

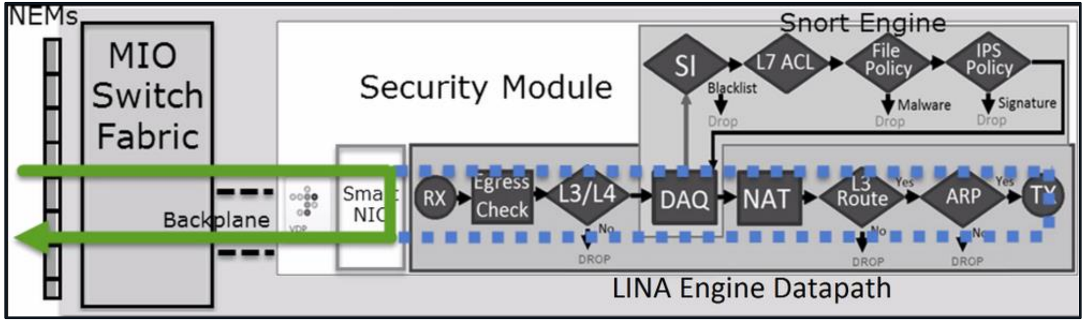
```
.77.40: icmp:
Phase: 16
4980 hits 140
```

```
> show arp
      inside 192.168.75.12 000c.29d0.ebcf 1286
```

```
firepower# show nat detail
[…}
Auto NAT Policies (Section 2)
1 (inside) to (outside) source dynamic science-obj interface
    translate_hits = 37723, untranslate_hits = 0
    Source - Origin: 192.168.0.0/16, Translated: 14.36.103.96/16
```



Packet Processing: Flow Offload

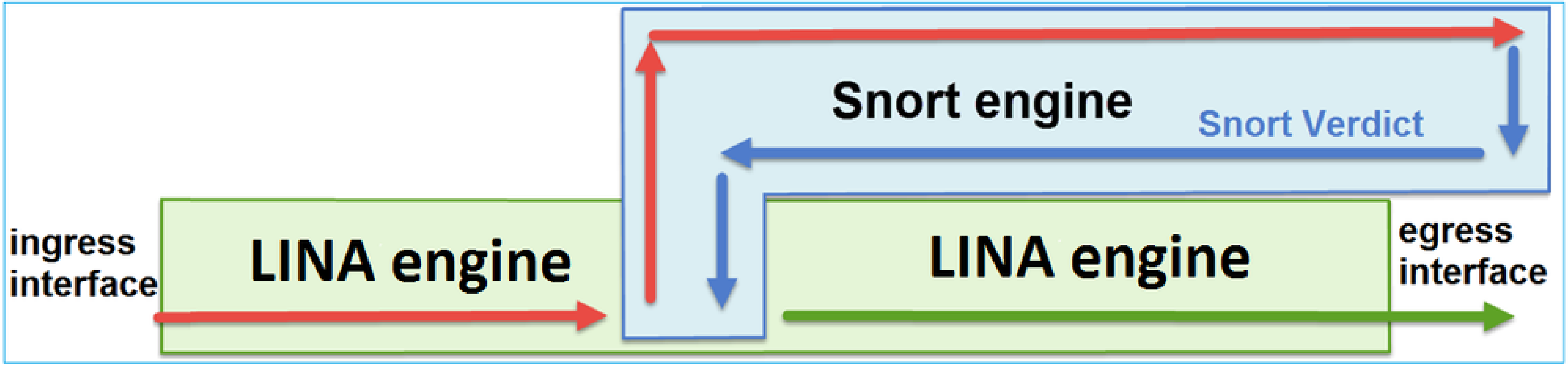


- Bypasses Lina and Snort completely
- L2/L3 re-writing is handled by special network adapter in the security engine blade
- View offloaded flows via the 'show flow-offload flow detail' command in Lina CLI

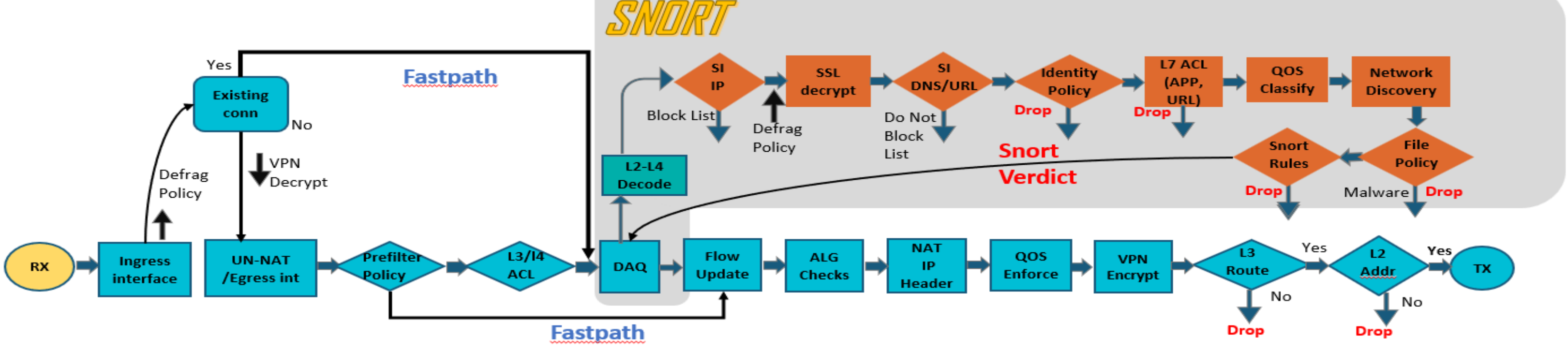
1. Static Flow Offload:
   - Connections that are fastpathed by the prefilter policy.
2. Dynamic Flow Offload:
   - Inspected flows that the inspection engine decides no longer need inspection.

➢ **Supported by 3100/4100/9300 platforms.**

FTD Packet Processing – The Big Picture

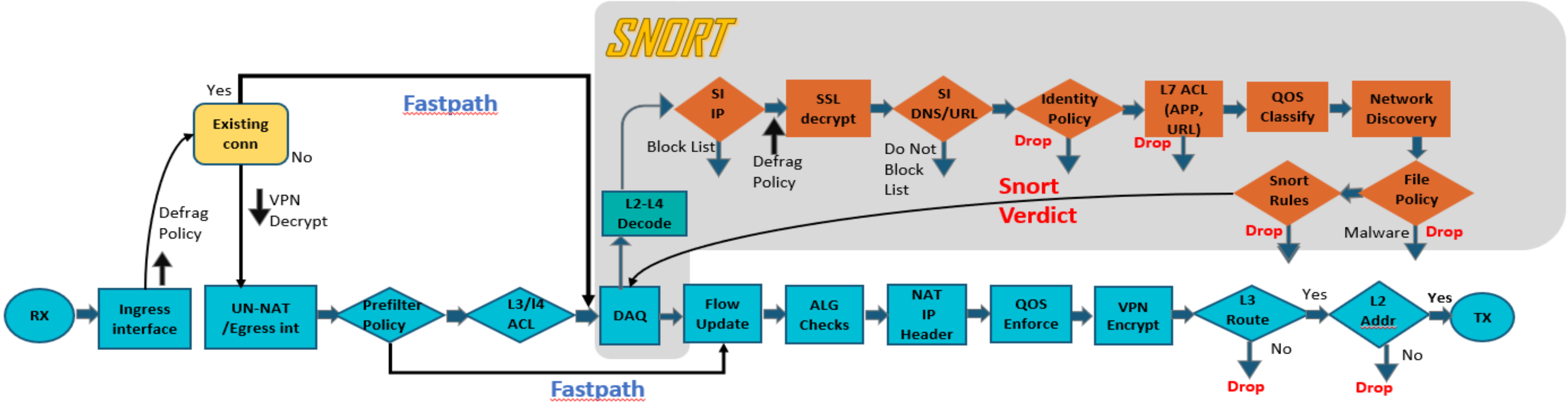


1. Packet enters the ingress interface, and it is handled by the LINA engine
2. If the policy dictates so the packet is inspected by the Snort Engine
3. Snort Engine returns a verdict for the packet
4. Lina Engine drops or forwards the packets based on Snort's verdict



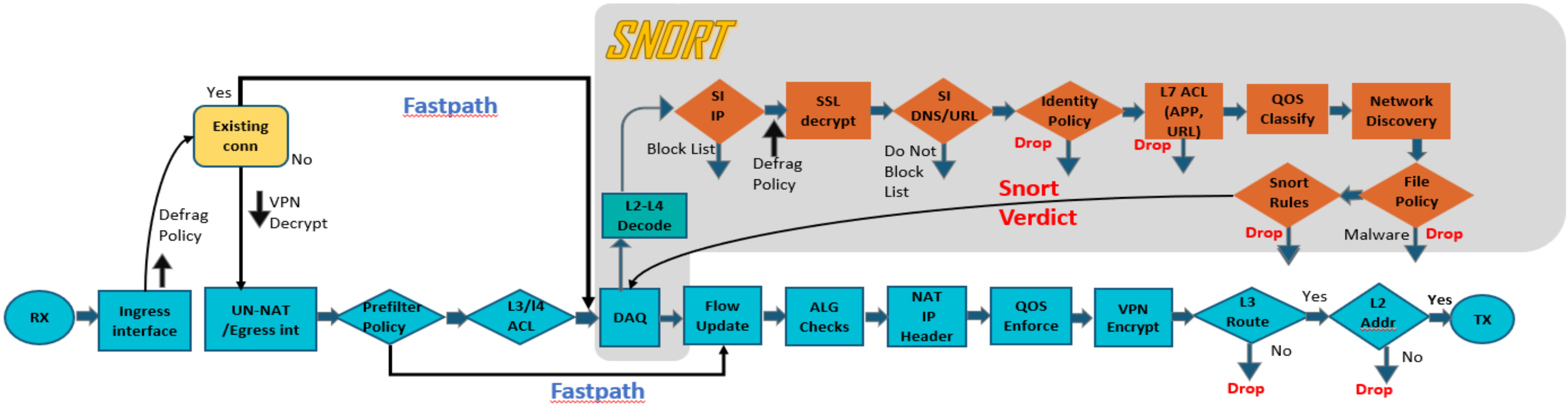
- Packet arrives on ingress interface
- Input counters are incremented by NIC and periodically retrieved by CPU
- Input queue (RX ring) is an indicator of packet load
- Overrun counter indicates packet drops (usually packet bursts)

```
> show interface g1/2 detail
Interface GigabitEthernet1/2 "inside", is up, line protocol is up
  Hardware is Accelerator rev01, BW 1000 Mbps, DLY 10 usec
 IPS Interface-Mode: inline-tap, Inline-Set: Set1
 47770671 packets input, 7620806887 bytes, 0 no buffer
 Received 23734506 broadcasts, 0 runts, 0 giants
 0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
 input queue (blocks free curr/low): hardware (1008/800)
```



- Lina engine checks for existing connections in the connection table.
- If a match is found packet uses Fast Path bypassing basic checks

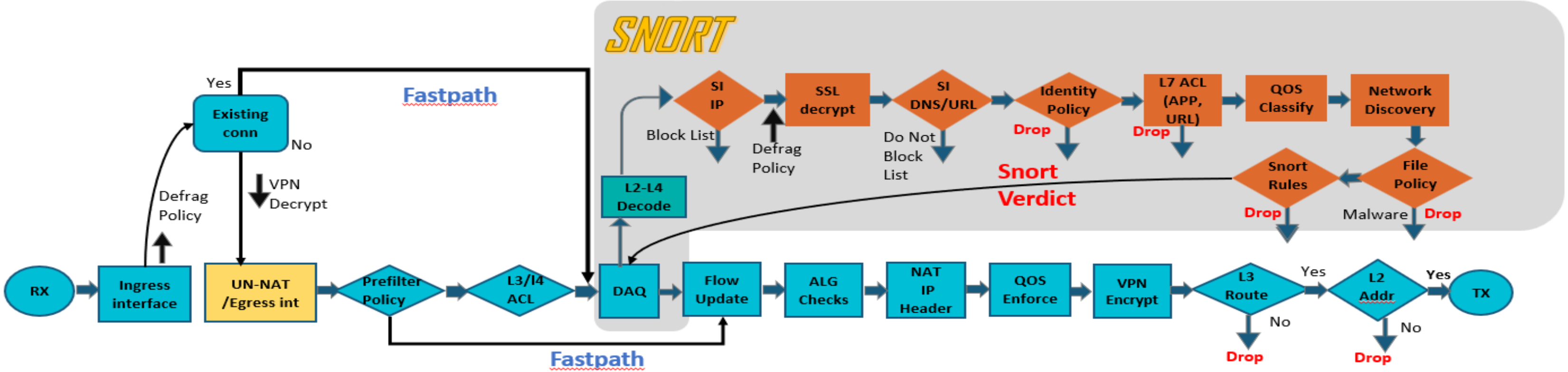
```
firepower# show capture CAPO packet-number 2 trace
2 packets captured
   2: 12:51:51.094691       192.168.76.14 > 192.168.75.14: icmp: echo reply
...
Phase: 3
Type: FLOW-LOOKUP
Result: ALLOW
Config:
Additional Information:
Found flow with id 1541, using existing flow
```



If no existing connection:

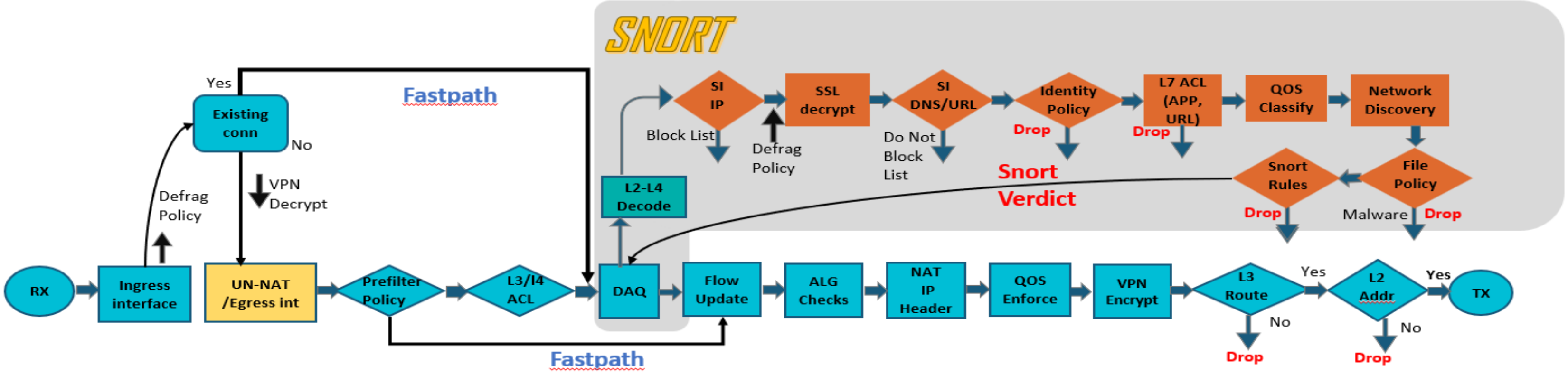
1. TCP SYN or UDP packet, pass to ACL and other policy checks in Session Manager
2. TCP non-SYN packet, drop and log

```
ASA-6-106015: Deny TCP (no connection) from 10.1.1.9/11031 to 198.133.219.25/80 flags PSH ACK  on
interface inside
```



- Egress interface determination
- In case there is Destination NAT (UN-NAT) the egress interface will be determined based on the NAT rule, unless route lookup is preferred (identity NAT)

```
firepower# show capture DMZ packet-number 3 trace detail
Phase: 3
Type: UN-NAT
Subtype: static
Result: ALLOW
Config:
nat (inside,dmz) source static Host-A Host-B
Additional Information:
NAT divert to egress interface inside
Untranslate 192.168.76.100/0 to 192.168.75.14/0
```

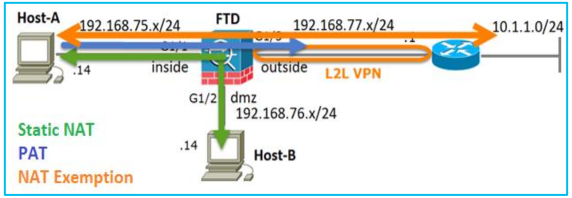


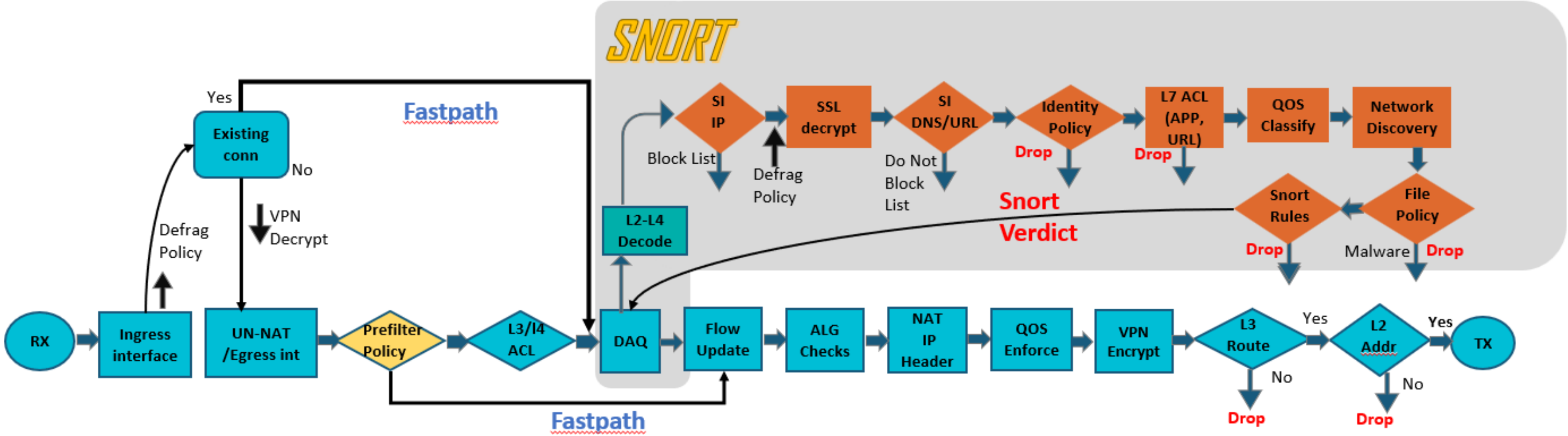
- To verify the NAT applied configuration on Lina engine along with the hit counts:

```
firepower# show nat detail
[…}
Auto NAT Policies (Section 2)
1 (inside) to (outside) source dynamic science-obj interface
    translate_hits = 37723, untranslate_hits = 0
    Source - Origin: 192.168.0.0/16, Translated: 14.36.103.96/16
```

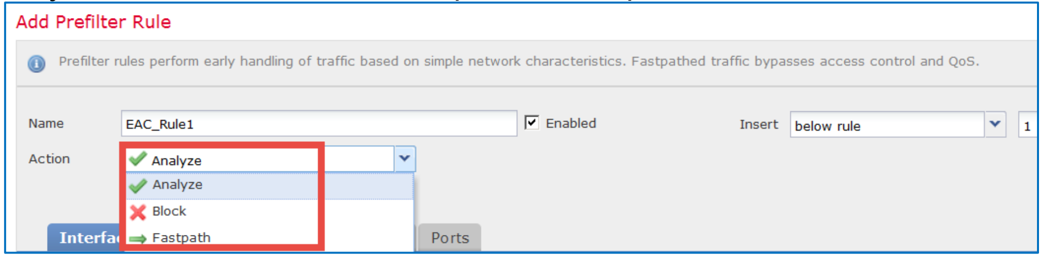
Verifying NAT rules ordering

Is the NAT rule being hit by traffic?





- Early Access Control Rules provide 3 possible actions:



Add Prefilter Rule

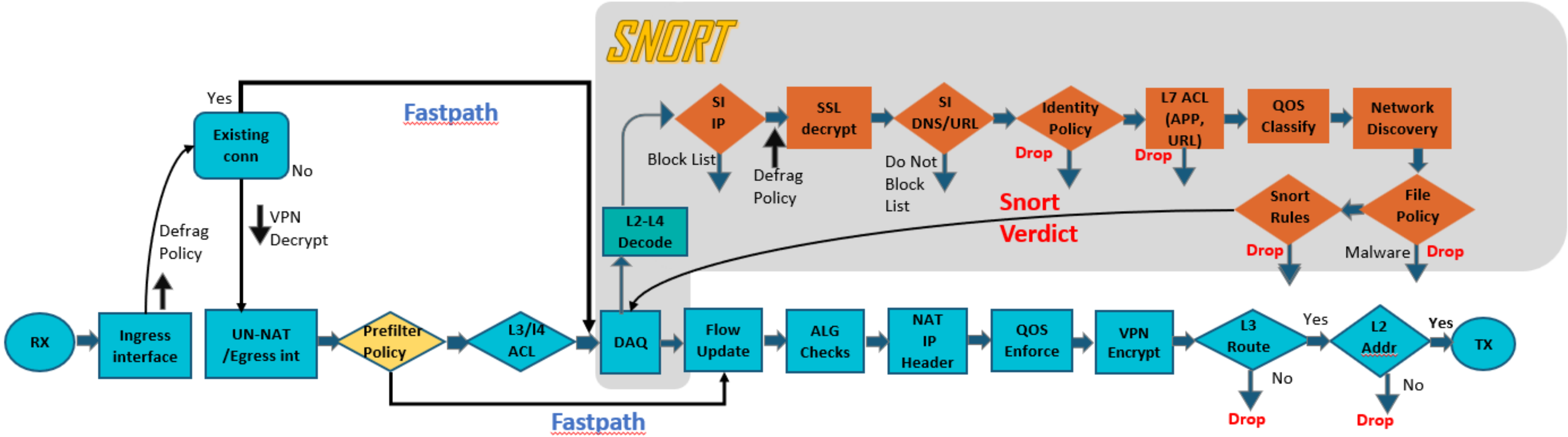
Prefilter rules perform early handling of traffic based on simple network characteristics. Fastpathed traffic bypasses access control and QoS.

Name EAC_Rule1 ☑ Enabled Insert below rule 1

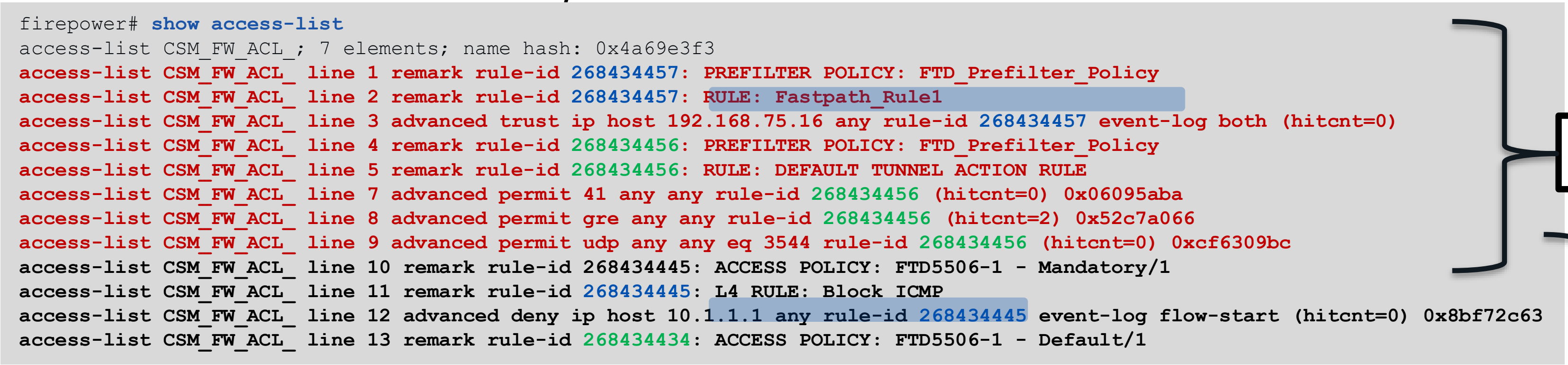
Action ✓ Analyze

Allows a flow to bypass completely the Snort engine.

1. Block – Drops the traffic
2. Fastpath – Allows the traffic and bypasses the Snort Engine
3. Analyze – Sends the traffic to Snort Engine



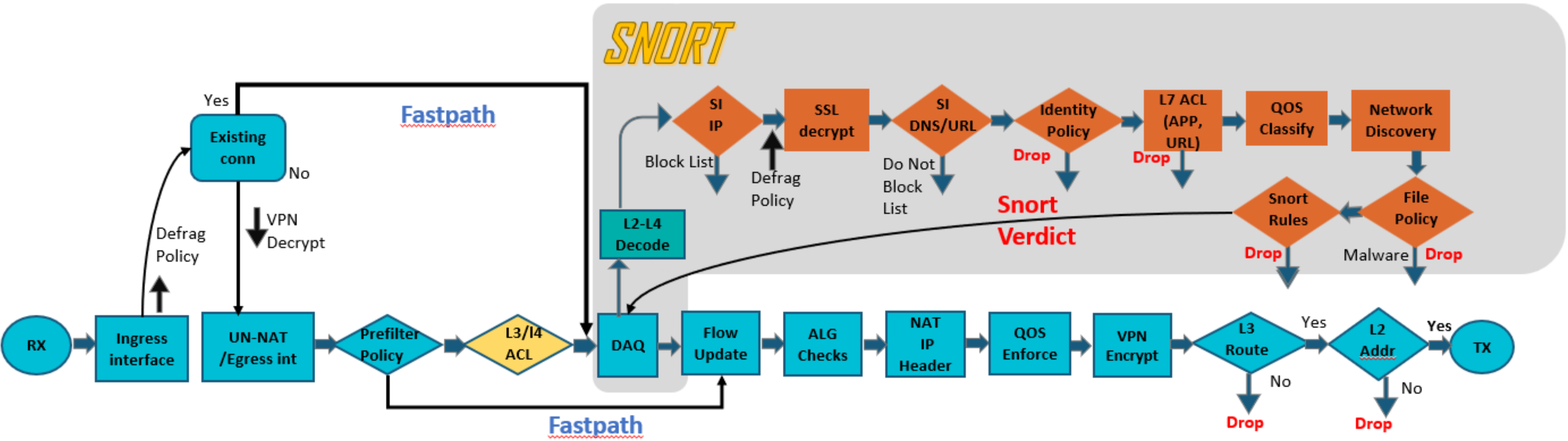
- Prefilter Rules are deployed to Lina as L3/L4 ACEs and are placed **above** the normal L3/L4 ACEs.



```
firepower# show access-list
access-list CSM_FW_ACL_; 7 elements; name hash: 0x4a69e3f3
access-list CSM_FW_ACL_ line 1 remark rule-id 268434457: PREFILTER POLICY: FTD_Prefilter_Policy
access-list CSM_FW_ACL_ line 2 remark rule-id 268434457: RULE: Fastpath_Rule1
access-list CSM_FW_ACL_ line 3 advanced trust ip host 192.168.75.16 any rule-id 268434457 event-log both (hitcnt=0)
access-list CSM_FW_ACL_ line 4 remark rule-id 268434456: PREFILTER POLICY: FTD_Prefilter_Policy
access-list CSM_FW_ACL_ line 5 remark rule-id 268434456: RULE: DEFAULT TUNNEL ACTION RULE
access-list CSM_FW_ACL_ line 7 advanced permit 41 any any rule-id 268434456 (hitcnt=0) 0x06095aba
access-list CSM_FW_ACL_ line 8 advanced permit gre any any rule-id 268434456 (hitcnt=2) 0x52c7a066
access-list CSM_FW_ACL_ line 9 advanced permit udp any any eq 3544 rule-id 268434456 (hitcnt=0) 0xcf6309bc
access-list CSM_FW_ACL_ line 10 remark rule-id 268434445: ACCESS POLICY: FTD5506-1 - Mandatory/1
access-list CSM_FW_ACL_ line 11 remark rule-id 268434445: L4 RULE: Block ICMP
access-list CSM_FW_ACL_ line 12 advanced deny ip host 10.1.1.1 any rule-id 268434445 event-log flow-start (hitcnt=0) 0x8bf72c63
access-list CSM_FW_ACL_ line 13 remark rule-id 268434434: ACCESS POLICY: FTD5506-1 - Default/1
```

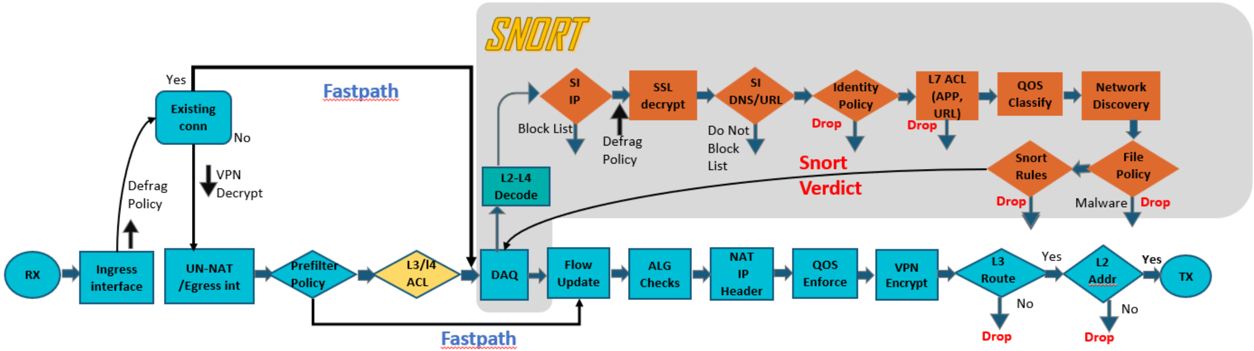
Prefilter Rules

L3/L4 ACEs

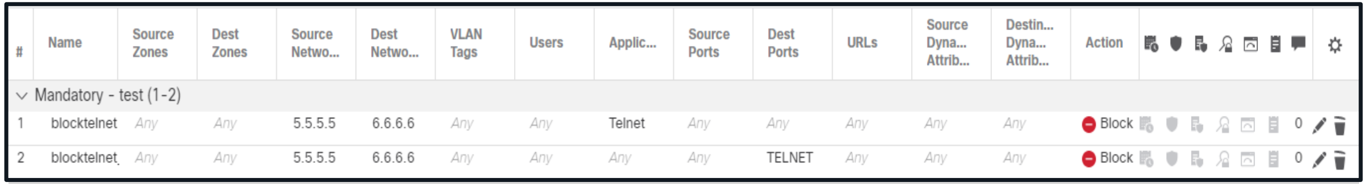


- Access Control Policy (ACP) that is configured on FMC.
- Pushed as a global ACL (CSM_FW_ACL_) to Lina engine and as AC rules in /var/sf/detection_engines/UUID/ngfw.rules file in Snort engine

```
firepower# show run access-list
access-list CSM_FW_ACL_ advanced deny ip host 10.1.1.1 any rule-id 268434445 event-log flow-start
firepower# show run access-group
access-group CSM_FW_ACL_ global
```

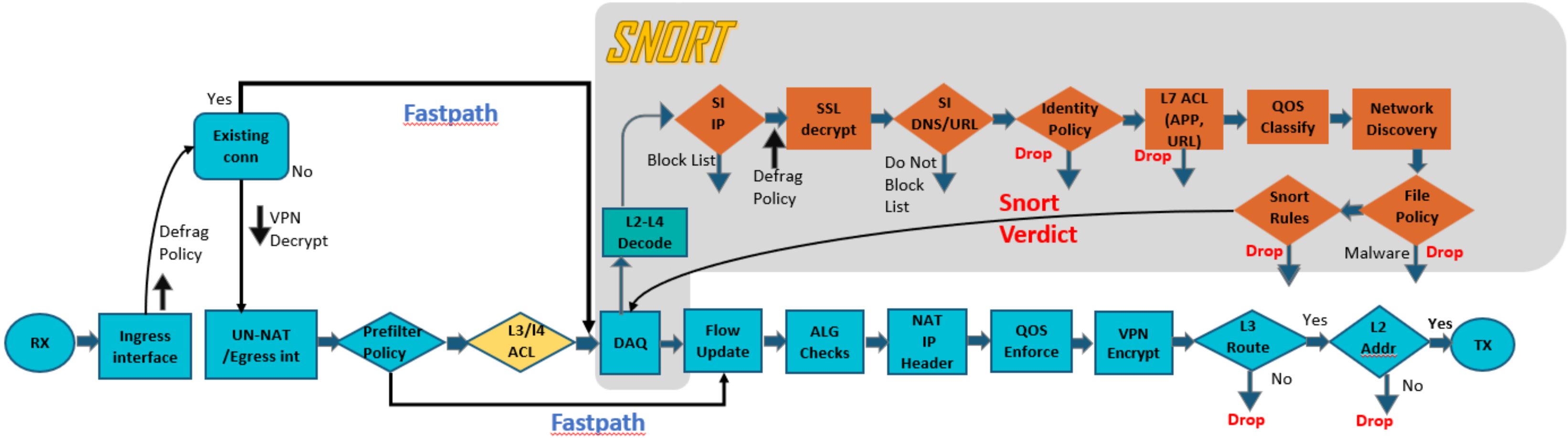


Allow Trust Monitor Block



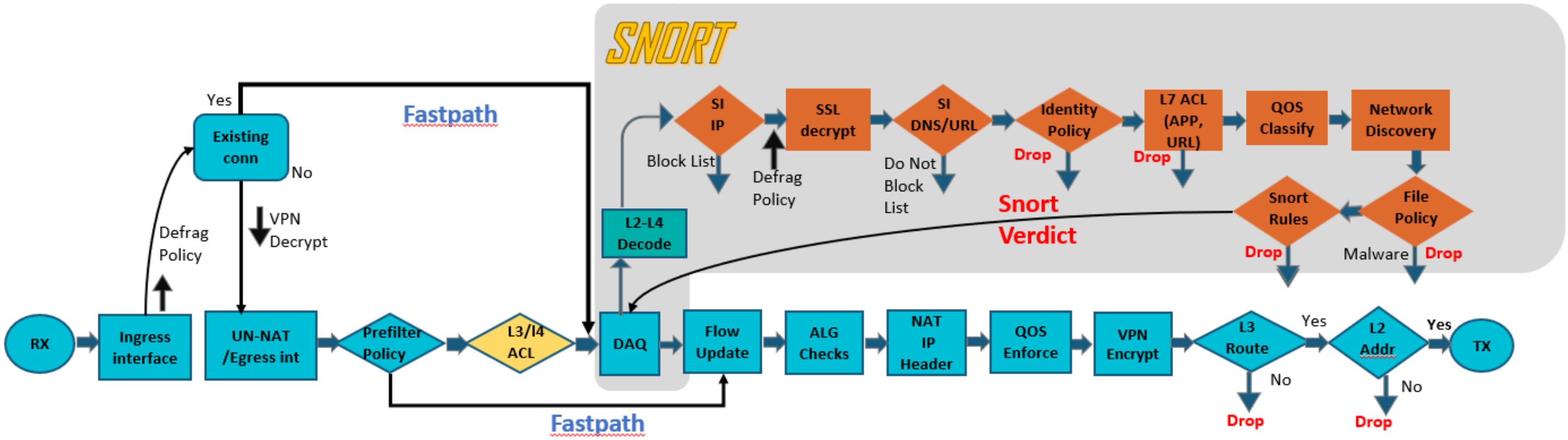
#	Name	Source Zones	Dest Zones	Source Netwo...	Dest Netwo...	VLAN Tags	Users	Applic...	Source Ports	Dest Ports	URLs	Source Dyna... Attrib...	Destin... Dyna... Attrib...	Action		⚙
Mandatory - test (1-2)																
1	blocktelnet	Any	Any	5.5.5.5	6.6.6.6	Any	Any	Telnet	Any	Any	Any	Any	Any	Block	0	
2	blocktelnet	Any	Any	5.5.5.5	6.6.6.6	Any	Any	Any	Any	TELNET	Any	Any	Any	Block	0	

```
firepower# show access-list
access-list CSM_FW_ACL_ line 20 remark rule-id 268435460: L7 RULE: ACP_Rule5_Block_Telnet_App
access-list CSM_FW_ACL_ line 21 advanced permit ip host 5.5.5.5 host 6.6.6.6 rule-id 268435460
access-list CSM_FW_ACL_ line 23 remark rule-id 268435464: L4 RULE: ACP_Rule6_Block_Telnet_Port
access-list CSM_FW_ACL_ line 24 advanced deny tcp host 6.6.6.6 host 7.7.7.7 eq telnet rule-id 268435464
```



- Lina engine will send the packet to Snort engine for a verdict

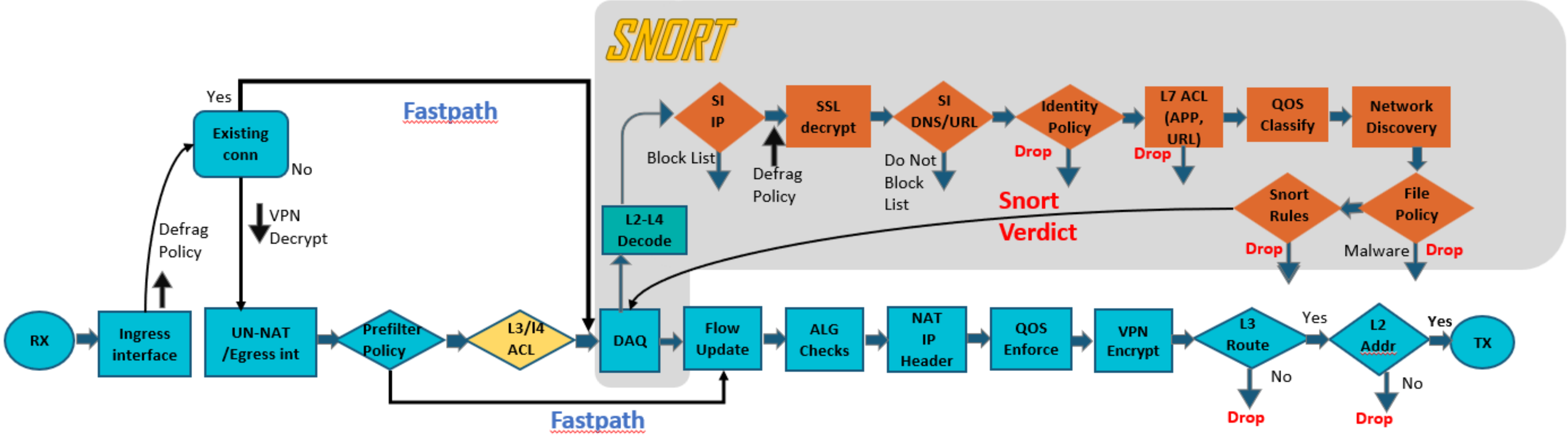
```
> packet-tracer input inside icmp 1.1.1.1 8 0 2.2.2.2

Phase: 2
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group CSM_FW_ACL_ global
access-list CSM_FW_ACL_ advanced permit ip host 1.1.1.1 host 2.2.2.2 rule-id 268435456
access-list CSM_FW_ACL_ remark rule-id 268435456: ACCESS POLICY: FTD5506-1 - Mandatory/1
access-list CSM_FW_ACL_ remark rule-id 268435456: L7 RULE: ACP_Rule1_Allow_ICMP_App
Additional Information:
 This packet will be sent to snort for additional processing where a verdict will be reached
```



Packet-tracer shows that Lina engine will not send any packets to Snort

```
> packet-tracer input inside udp 4.4.4.4 1111 5.5.5.5 53

Phase: 4
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group CSM_FW_ACL_ global
access-list CSM_FW_ACL_ advanced trust udp host 4.4.4.4 host 5.5.5.5 eq domain rule-id 268435477
event-log flow-end
access-list CSM_FW_ACL_ remark rule-id 268435477: ACCESS POLICY: FTD5506-1 - Mandatory/4
access-list CSM_FW_ACL_ remark rule-id 268435477: L4 RULE: ACP_Rule4_Trust DNS Port
Additional Information:
```

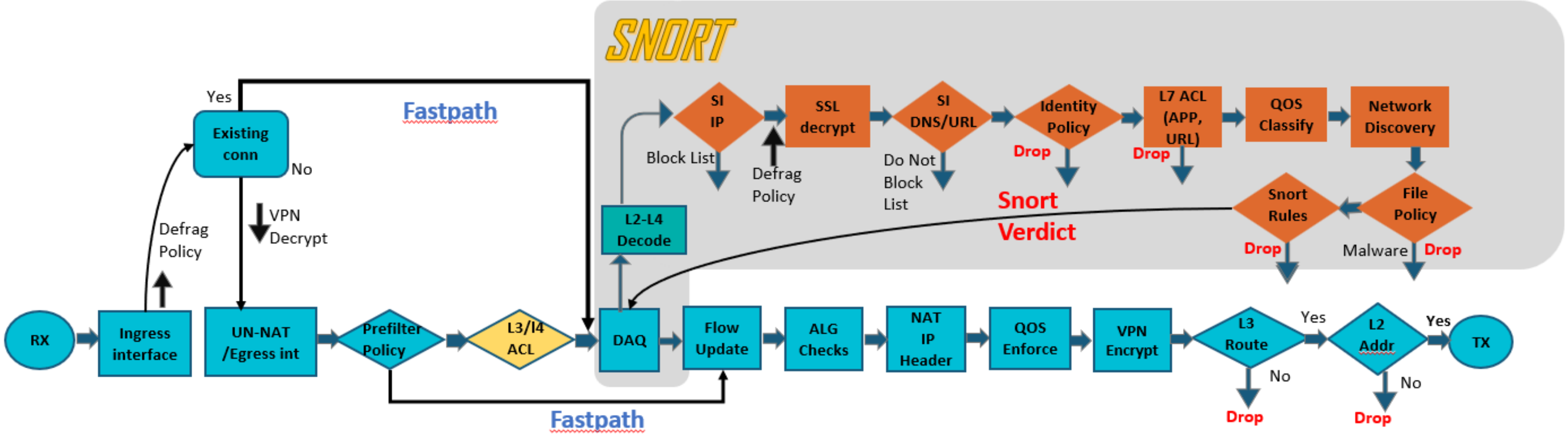
No Additional Information means the packet is not going to be redirected to Snort engine

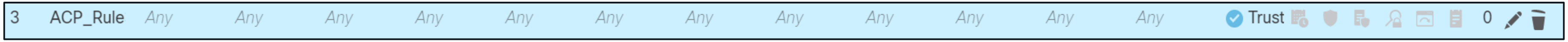


- Tracing real packets shows that no packets are going to be sent to Snort

```
> show capture CAPI packet-number 1 trace
  1: 19:46:23.626386       192.168.75.14.50152 > 192.168.76.14.53:  udp 34

Phase: 4
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group CSM_FW_ACL_ global
access-list CSM_FW_ACL_ advanced trust udp host 192.168.75.14 host 192.168.76.14 eq domain
access-list CSM_FW_ACL_ remark rule-id 268435477: ACCESS POLICY: FTD5506-1 - Mandatory/4
access-list CSM_FW_ACL_ remark rule-id 268435477: L4 RULE: ACP_Rule4_Trust_DNS_Port
Additional Information:
```

```
> show snort statistics

Packet Counters:
  Passed Packets                                  0
  Blocked Packets                                 0
  Injected Packets                                0

Flow Counters:
  Fast-Forwarded Flows                            0
  Blacklisted Flows                               0
  Flows bypassed (Snort Down)                     0
  Flows bypassed (Snort Busy)                     0

Miscellaneous Counters:
  Start-of-Flow events                           23
  End-of-Flow events                             49
```





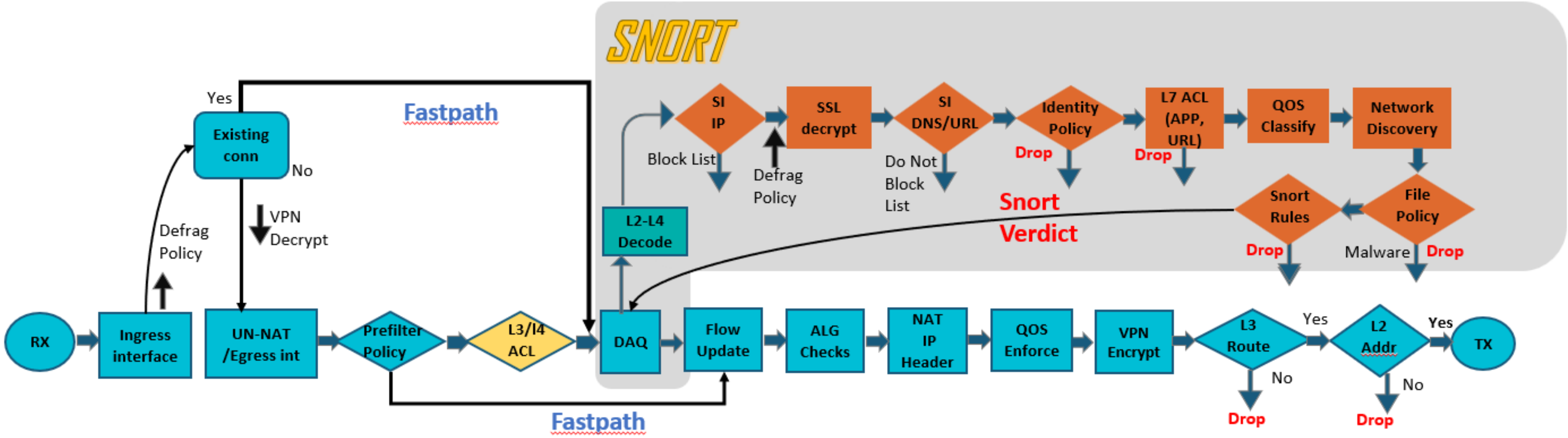
3	ACP_Rule	Any	Any	Any	Any	Any	Any	Any	Any	Any	Any	Any	Any	✓ Trust	0

In case one or more of the following is true the Trust Rule will be pushed to Lina engine as permit action:

- Application is used as a condition and/or SI, QoS, Identity Policy, SSL Policy

```
firepower# show access-list
access-list CSM_FW_ACL_ line 14 remark rule-id 268435458: L7 RULE: ACP_Rule3_Trust_DNS_App
access-list CSM_FW_ACL_ line 15 advanced permit ip host 3.3.3.3 host 4.4.4.4 rule-id 268435458
```

```
root@FTD5506-1:/home/admin# cat /var/sf/detection_engines/27306154-256d-11e6-9fc9-180edde177c5/ngfw.rules
268435458 fastpath any 3.3.3.3 32 any any 4.4.4.4 32 any any any  (appid 617:1)
```



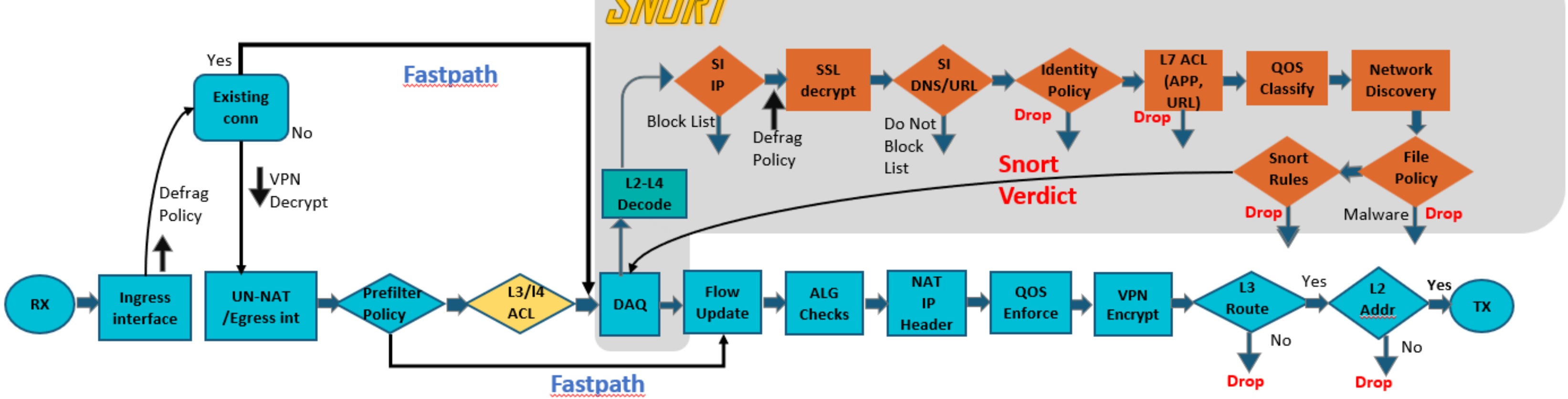
- Tracing real packets shows that the first few packets of the flow are being sent to Snort, but the remaining bypass the Snort engine. Snort statistics also reflect this.

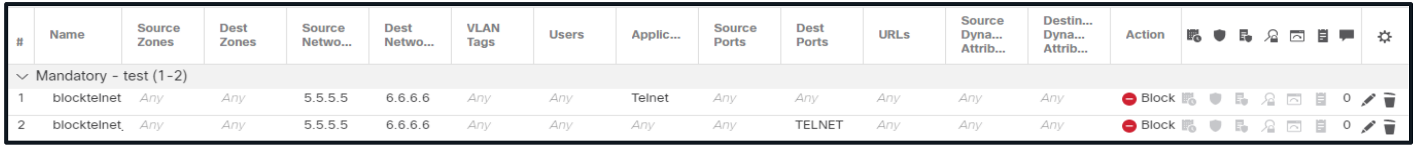
```
> show capture CAPI packet-number 1
Phase: 4
Type: EXTERNAL-INSPECT
Application: 'SNORT Inspect'
Phase: 5
Type: SNORT
Snort Verdict: (pass-packet) allow this packet

> show capture CAPI packet-number 10 trace
Phase: 3
Type: FLOW-LOOKUP
Found flow with id 23429, using existing flow
Phase: 4
Type: SNORT
Snort Verdict: (fast-forward) fast forward this flow
```

Few packets to Snort engine

```
> show snort statistics

Packet Counters:
  Passed Packets                                              2
  Blocked Packets                                             0
  Injected Packets                                            0

Flow Counters:
  Fast-Forwarded Flows                                        7
  Blacklisted Flows                                           0
  Flows bypassed (Snort Down)                                 0
  Flows bypassed (Snort Busy)                                 0
```

The remaining packets bypass the Snort engine

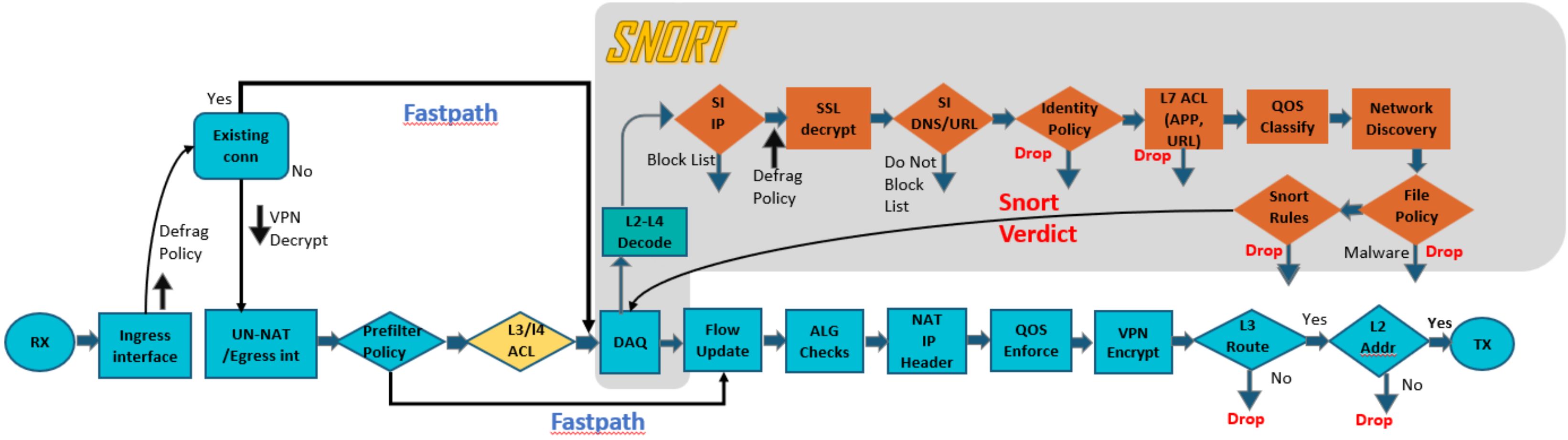




#	Name	Source Zones	Dest Zones	Source Netwo...	Dest Netwo...	VLAN Tags	Users	Applic...	Source Ports	Dest Ports	URLs	Source Dyna... Attrib...	Destin... Dyna... Attrib...	Action		⚙
∨ Mandatory - test (1-2)																
1	blocktelnet	Any	Any	5.5.5.5	6.6.6.6	Any	Any	Telnet	Any	Any	Any	Any	Any	⛔ Block	0	
2	blocktelnet_	Any	Any	5.5.5.5	6.6.6.6	Any	Any	Any	Any	TELNET	Any	Any	Any	⛔ Block	0	

Block Rule will be pushed to Lina engine as a permit or deny action depending on the rule conditions and to Snort engine as deny rule. If both applied, Application takes precedence over Dest Ports.

```
root@FTD5506-1:/home/admin# cat /var/sf/detection_engines/27306154-256d-11e6-9fc9-180edde177c5/ngfw.rules
268435460 deny any 5.5.5.5 32 any any 6.6.6.6 32 any any any  (appid 861:1)
268435464 deny any 6.6.6.6 32 any any 7.7.7.7 32 23 any 6
```



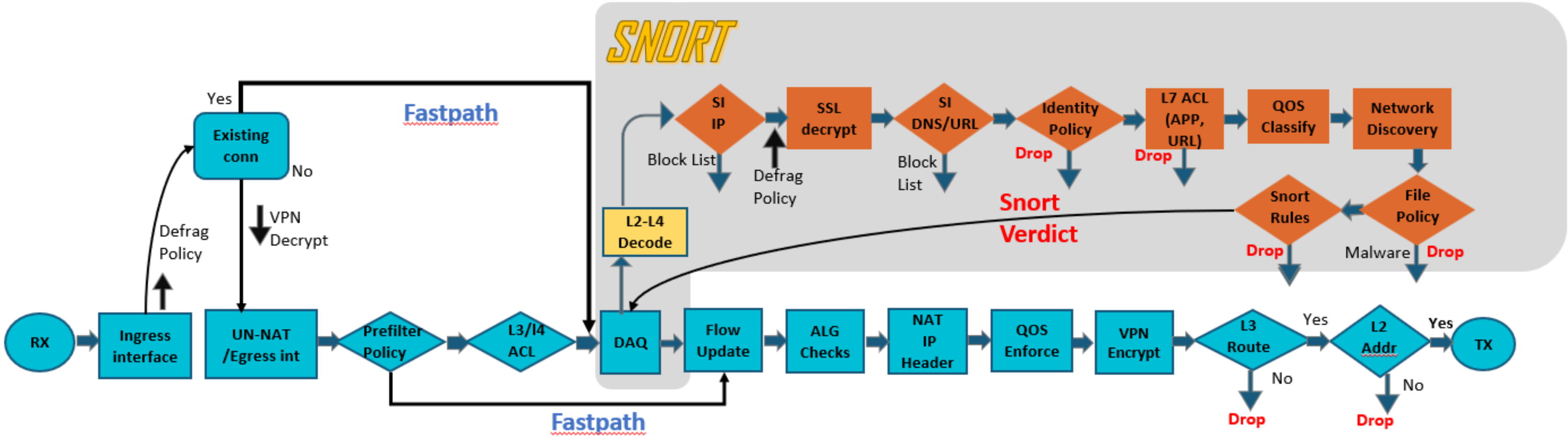
- For Block rule that uses Application the tracing of a real packet shows that the packet is dropped by Lina due to Snort engine verdict

```
firepower# show capture CAPI packet-number 7 trace
   7: 13:42:53.655971       192.168.75.14.36775 > 192.168.76.14.23: P 4147441466:4147441487(21) ack 884051486 win 16695
Type: SNORT
Subtype:
Result: DROP
Additional Information:
Snort Verdict: (black-list) black list this flow
```

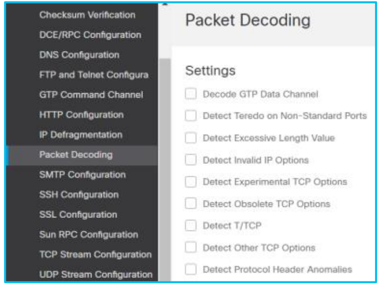
Snort **needs to process few packets** before determines the Application type

- Snort engine debug shows how the verdict was determined

```
> system support firewall-engine-debug
5.5.5.5-36774 > 6.6.6.6-23 6 AS 1 I 0 Starting with minimum 6, 'ACP_Rule5_Block_Telnet_App', and IPProto first with zones
3 -> 1, geo 0(0) -> 0, vlan 0, sgt tag: untagged, svc 861, payload 0, client 2000000861, misc 0, user 9999997, url , xff
5.5.5.5-36774 > 6.6.6.6-23 6 AS 1 I 0 match rule order 5, 'ACP_Rule5_Block_Telnet_App', action Block
5.5.5.5-36774 > 6.6.6.6-23 6 AS 1 I 0 deny action
```



- Packet Decoder – Prepares the packets for preprocessor analysis
- Decoder options that can be applied depend on Secure Firewall interface mode (Routed, inline pair etc)
- L2-L4 Snort Preprocessors are configured under **Policies > Access Control > Access Control > Network Analysis Policy**

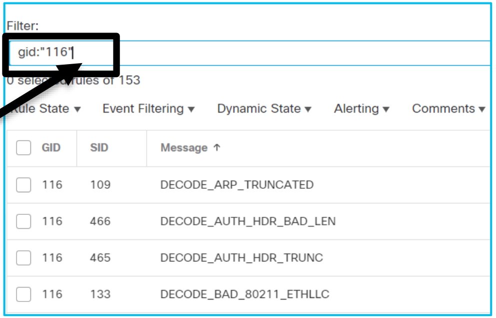


Packet Decoding

Settings

- □ Decode GTP Data Channel
- □ Detect Teredo on Non-Standard Ports
- □ Detect Excessive Length Value
- □ Detect Invalid IP Options
- □ Detect Experimental TCP Options
- □ Detect Obsolete TCP Options
- □ Detect T/TCP
- □ Detect Other TCP Options
- □ Detect Protocol Header Anomalies

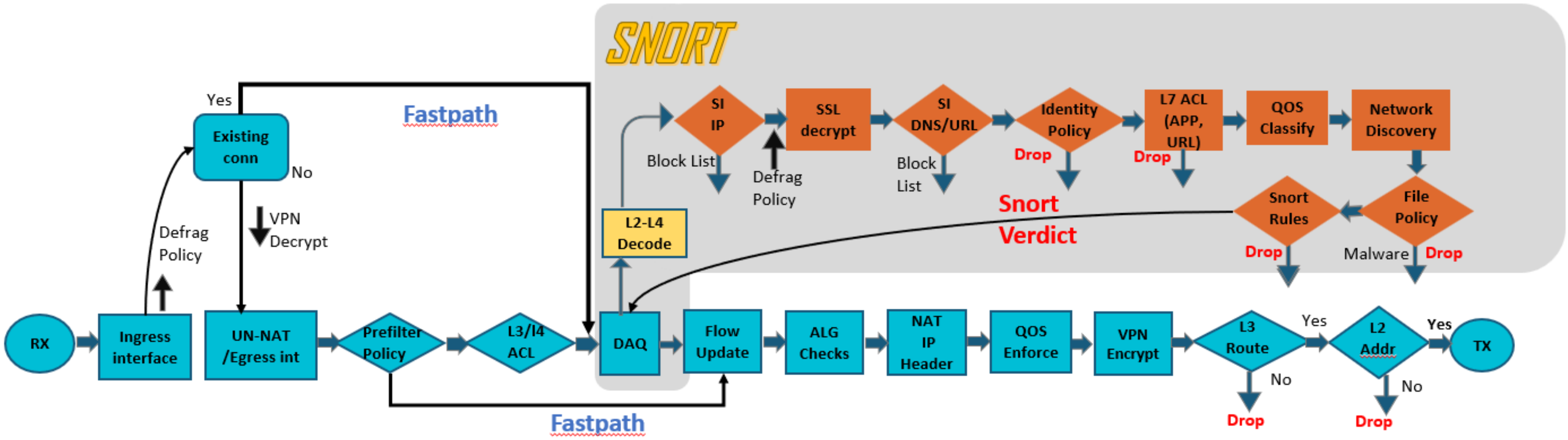
Troubleshooting Tip
You can enable the appropriate Intrusion Rule IDs (**116**:SID) to generate events for Decoder matches



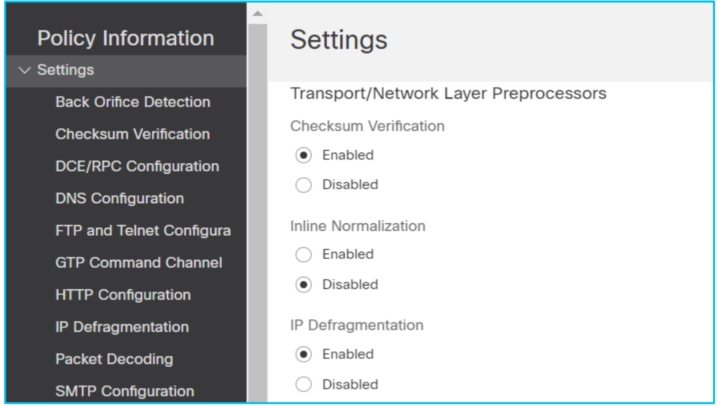
Filter: gid:"116"

0 selected rules of 153

□ GID	SID	Message ↑
□ 116	109	DECODE_ARP_TRUNCATED
□ 116	466	DECODE_AUTH_HDR_BAD_LEN
□ 116	465	DECODE_AUTH_HDR_TRUNC
□ 116	133	DECODE_BAD_80211_ETHLLC



- Secure Firewall Inline pair interface mode handles IP, ICMP, TCP Options using a Snort Preprocessor.



Settings

Transport/Network Layer Preprocessors

Checksum Verification

● Enabled

○ Disabled

Inline Normalization

○ Enabled

● Disabled

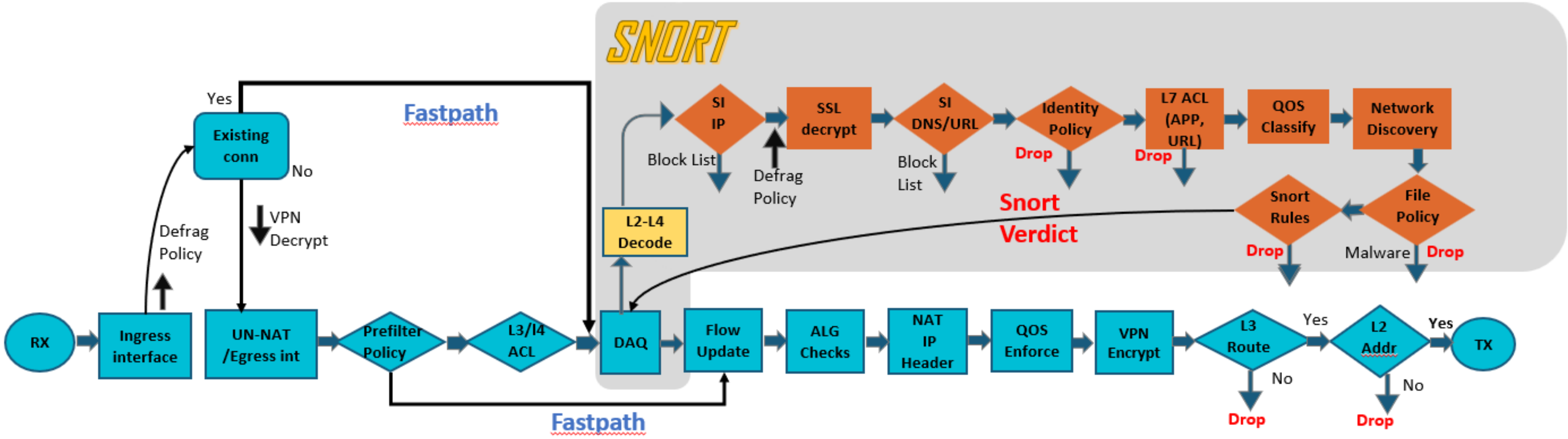
IP Defragmentation

● Enabled

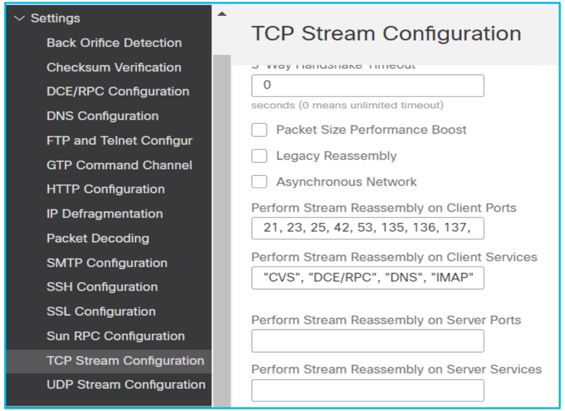
○ Disabled

Troubleshooting Tip

You can enable Intrusion Rule IDs (116:SID and 129:SID) to generate events for Inline Normalizer



- TCP Stream Preprocessor (Stream5) defines how Snort handles TCP streams.
- Similar to Inline Normalizer, the options depend on Secure Firewall interface mode.



TCP Stream Configuration

3-Way Handshake Timeout

0

seconds (0 means unlimited timeout)

□ Packet Size Performance Boost

□ Legacy Reassembly

□ Asynchronous Network

Perform Stream Reassembly on Client Ports

21, 23, 25, 42, 53, 135, 136, 137,

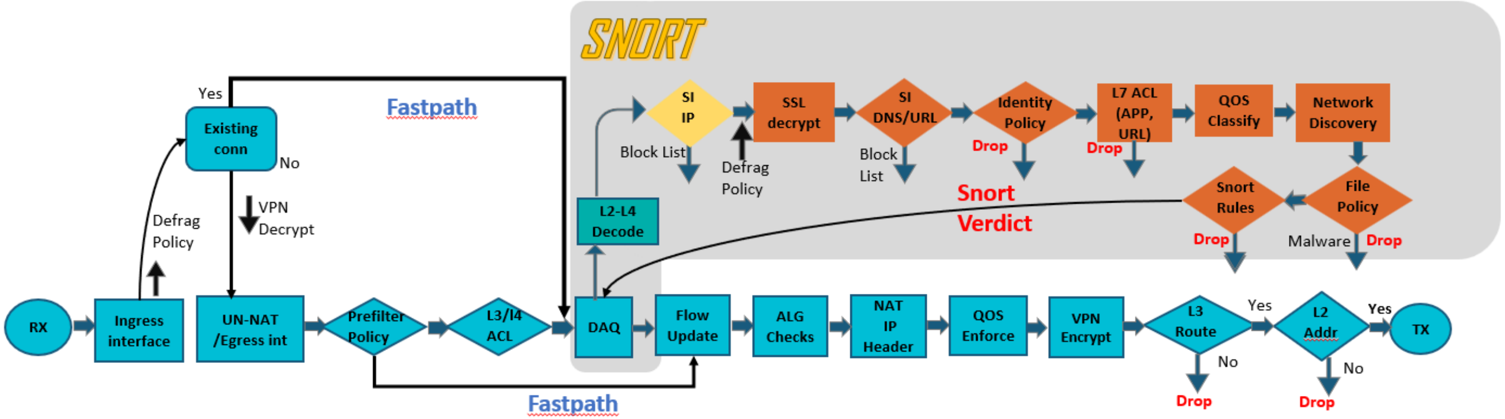
Perform Stream Reassembly on Client Services

"CVS", "DCE/RPC", "DNS", "IMAP"

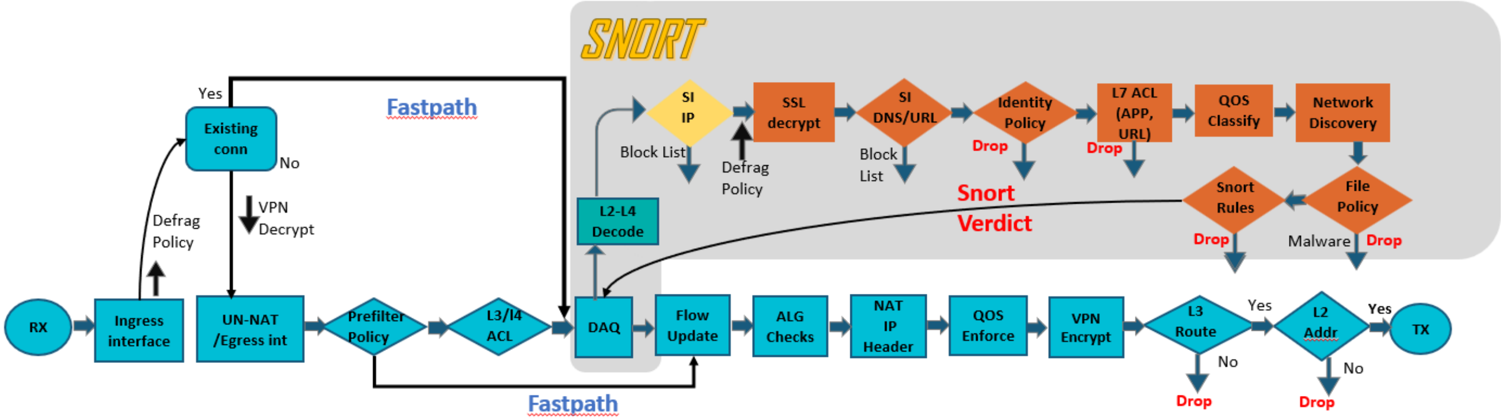
Perform Stream Reassembly on Server Ports

Perform Stream Reassembly on Server Services

Troubleshooting Tip
You can enable Intrusion Rule ID (129:SID) to generate events for TCP Stream Preprocessor



- Security Intelligence (SI) can Blocklist (drop) or Do-Not-Block list (allow) IP addresses early in the packet processing lifetime within the Snort engine
- Do-Not-Block list overwrites the Block-list
- The Blocklist can be populated in 2 ways:
    1. Manually by the Secure Firewall Management Center administrator
    2. Automatically by Intelligence Feed (Talos or custom) or List

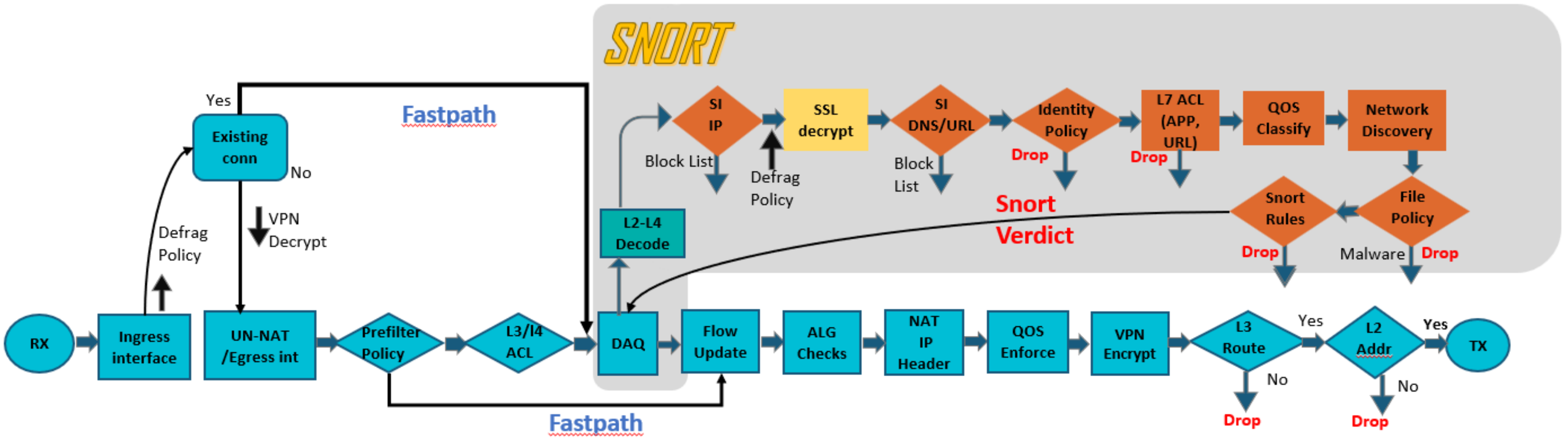


- The files containing the IPs from Talos SI Feed are in /ngfw/var/sf/iprep_download directory

```
root@FTD5506-1:/ngfw/var/sf/iprep_download# ls -alt | grep blf
-rw-r--r--  1 root root 1252278 Jun 12 16:06 3e2af68e-5fc8-4b1c-b5bc-b4e7cab598ba.blf
-rw-r--r--  1 root root  227696 Jun 12 16:05 032ba433-c295-11e4-a919-d4ae5275a468.blf
```

Verify an IP is on a block list:

```
$ grep -Fr [IP_ADDRESS] /var/sf/iprep_download
```

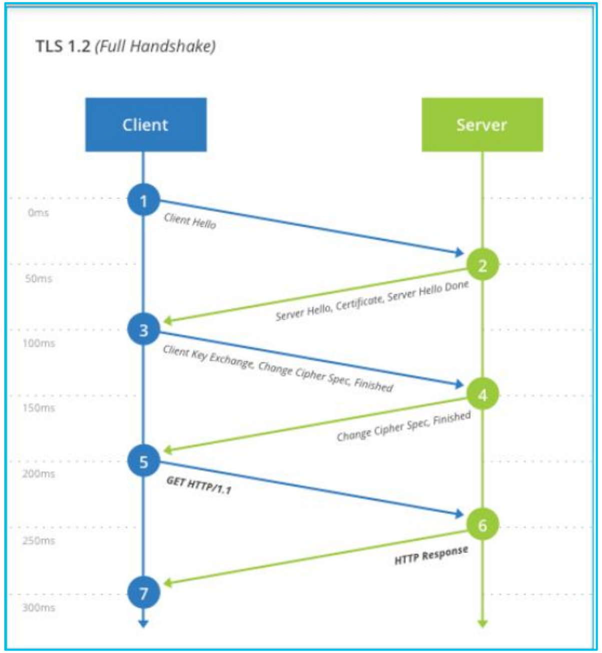


- SSL Inspection Policy controls which traffic will be decrypted by Secure Firewall so that other policies (ACP, File, Snort) can inspect the traffic.
- Can be configured in the Secure Firewall Management Center, under **Policies > SSL.**
- Secure Firewall provides 2 decryption modes:
  1. **Decrypt – Know Key** – SSL/TLS server owned by us
  2. **Decrypt – Resign** – 3rd party SSL/TLS server. Secure Firewall does man-in-the-middle and for that reason requires Internal CA
- SSL Policy is attached to Access Control Policy (ACP)
- Client Hello features (enabled by default) allows Secure Firewall to modify (TLS version, Ciphers) the Client Hello message (**Required** for Safe Search and YouTube EDU)

Want more on SSL Decryption?

BRKSEC-3320

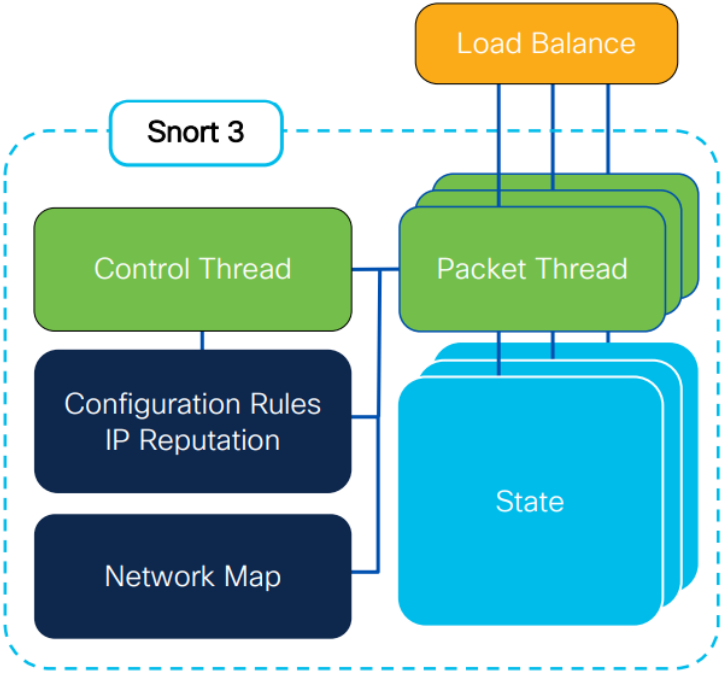
Demystifying TLS Decryption and Encrypted Visibility Engine on Cisco Secure Firewall Threat Defense


TLS 1.2 (Full Handshake)
Client
Server
0ms
50ms
100ms
150ms
200ms
250ms
300ms
1
Client Hello
2
Server Hello, Certificate, Server Hello Done
3
Client Key Exchange, Change Cipher Spec, Finished
4
Change Cipher Spec, Finished
5
GET HTTP/1.1
6
HTTP Response
7

More on Snort3?

BRKSEC-2484

Snort 3 with the Cisco Secure Firewall

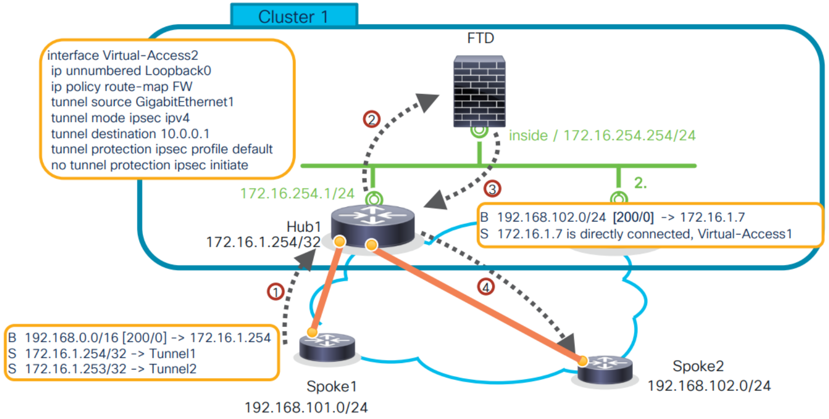


https://www.ciscolive.com/on-demand/on-demand-library.html?search=BRKSEC-2484#/session/1675722392971001tVHi

More on VPN with Cisco Secure Firewall?

BRKSEC-3058

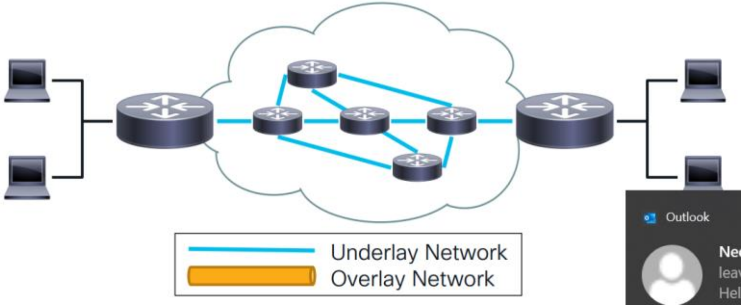
Route based VPNs with Cisco Secure Firewall



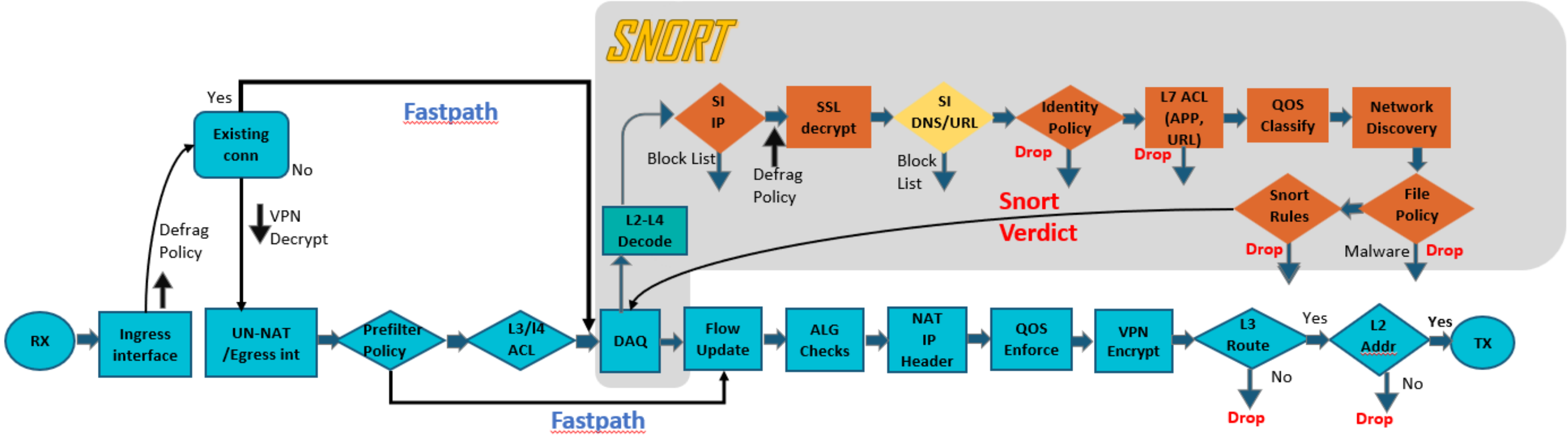
```
interface Virtual-Access2
 ip unnumbered Loopback0
 ip policy route-map FW
 tunnel source GigabitEthernet1
 tunnel mode ipsec ipv4
 tunnel destination 10.0.0.1
 tunnel protection ipsec profile default
 no tunnel protection ipsec initiate
```

```
B  192.168.102.0/24  [200/0]  -> 172.16.1.7
S  172.16.1.7 is directly connected, Virtual-Access1
```

```
B  192.168.0.0/16 [200/0] -> 172.16.1.254
S  172.16.1.254/32 -> Tunnel1
S  172.16.1.253/32 -> Tunnel2
```

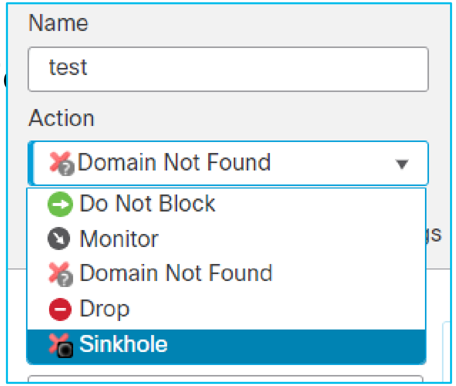


https://www.ciscolive.com/on-demand/on-demand-library.html?search=BRKSEC-3058#/session/1675722394754001t2R3



Security Intelligence (DNS)

- With this feature DNS Requests can get one of the following acti
  1. Do Not Block
  2. Monitor
  3. Domain Not Found (NXDOMAIN)
  4. Drop (drops the DNS query)
  5. Sinkhole (redirection to a local honeypot IP)



Name

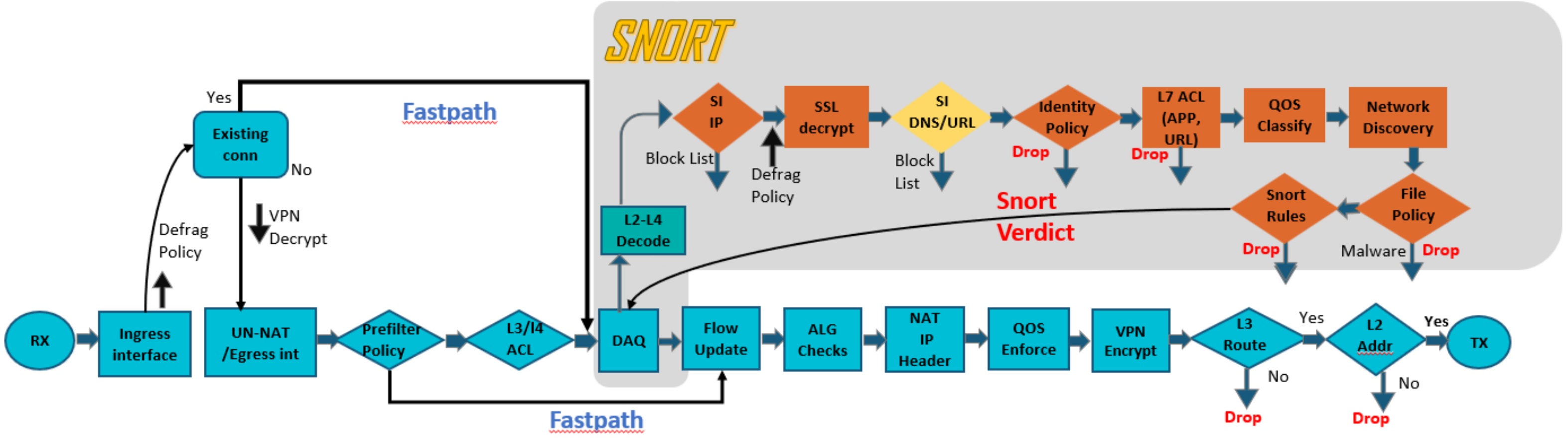
test

Action

Domain Not Found ▾

- Do Not Block
- Monitor
- Domain Not Found
- Drop
- Sinkhole

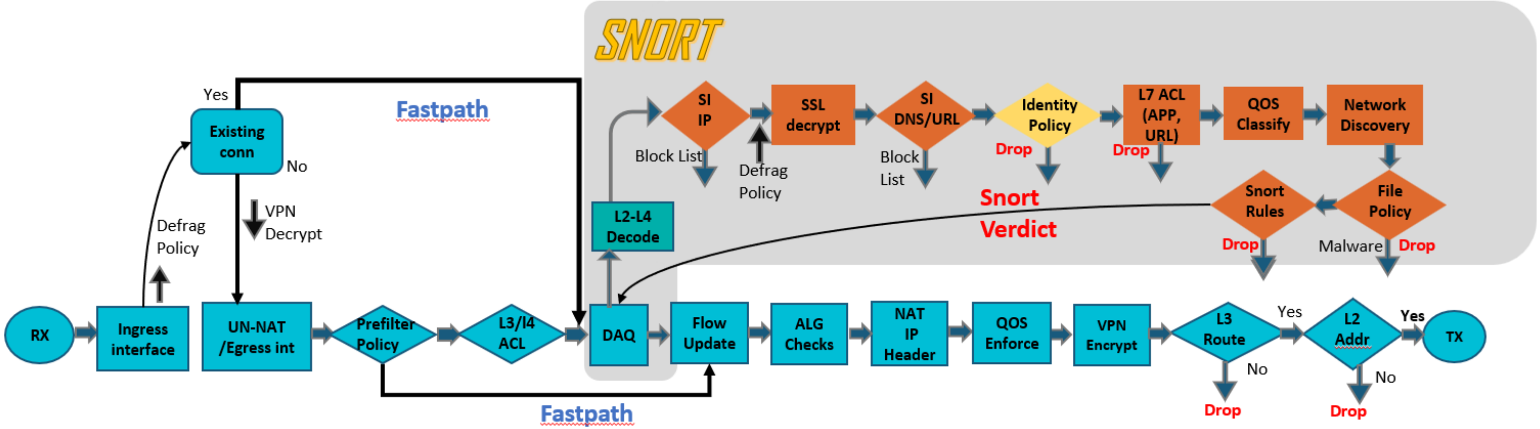
- The DNS lists can be populated manually or automatically (Talos or custom)



Security Intelligence (URL)

- Works similarly to IP Security Intelligence and provides 3 actions
  1. Do-Not-Block list
  2. Block list
  3. (Monitor)

- In case Talos URL Feed is used part of the DB is stored locally and updated daily
- For non-cached URLs a Cloud lookup is done



Identity Policy enables user-based authentication. The user info is obtained in various ways:

1. **Passive Authentication**

- Remote access VPN logins. The following user types are supported for passive identity:

i. User accounts defined in an external authentication server.

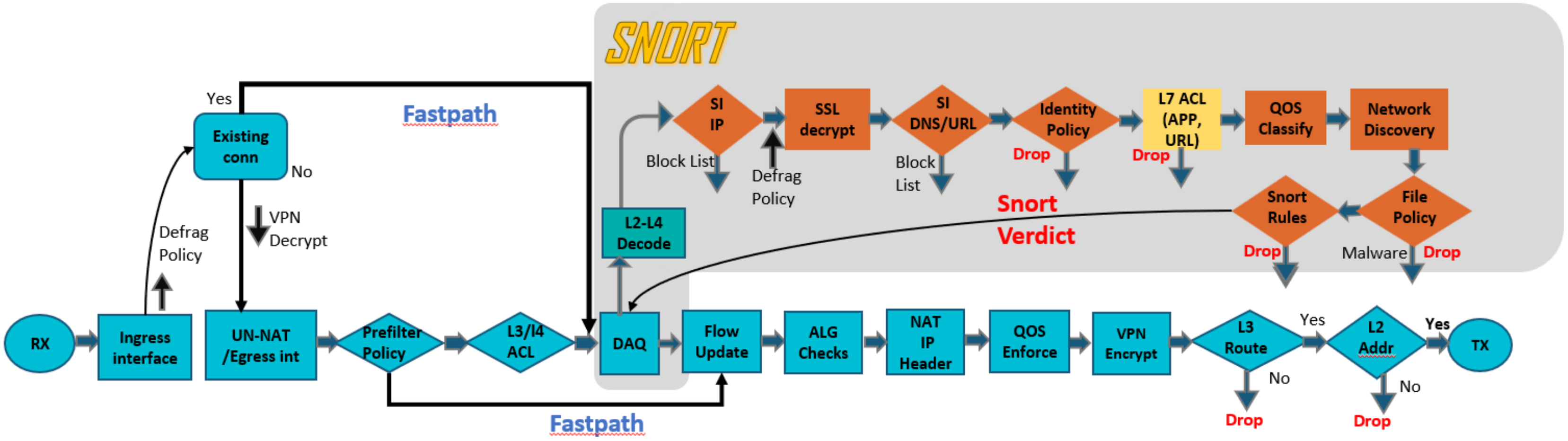
ii. Local user accounts that are defined in the FDM.

- Cisco Identity Services Engine (ISE); Cisco Identity Services Engine Passive Identity Connector (ISE PIC).

2. **Active Authentication**

   - Captive Portal

Basic, NTLM, Kerberos

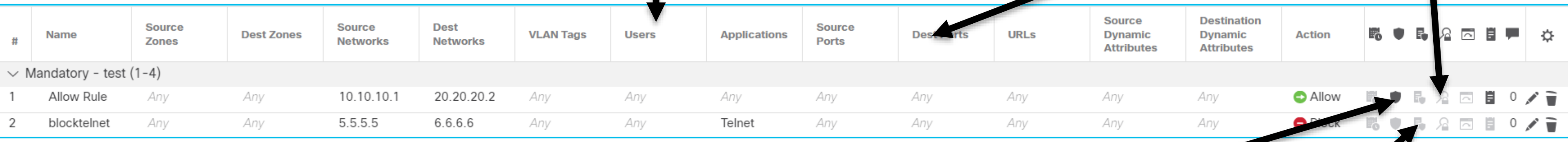


L7 ACL can do among others:

User-based rules

Application filtering

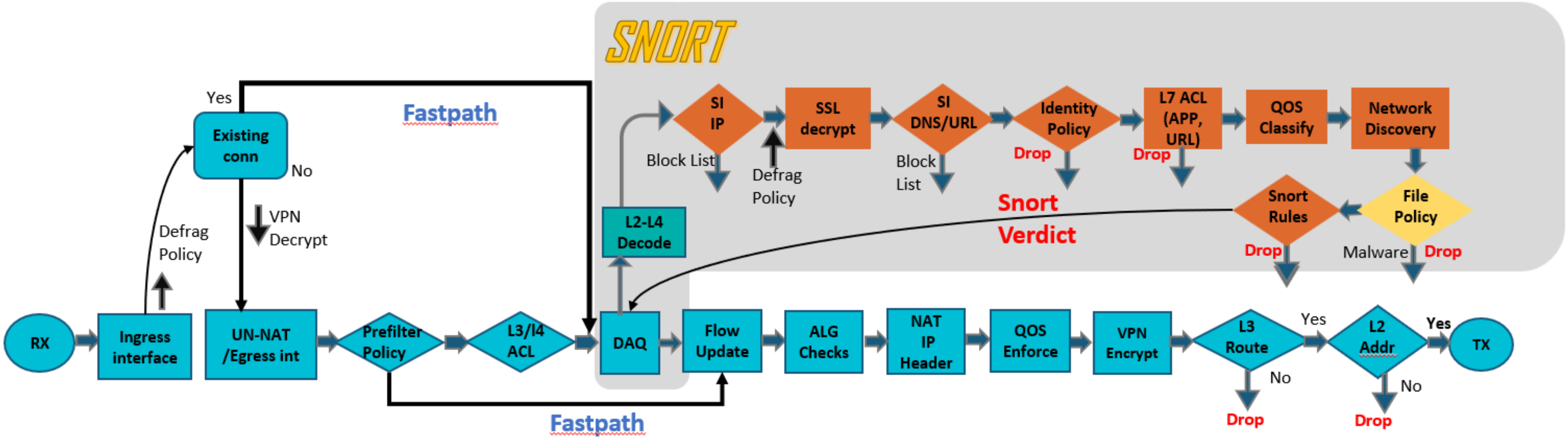
SafeSearch



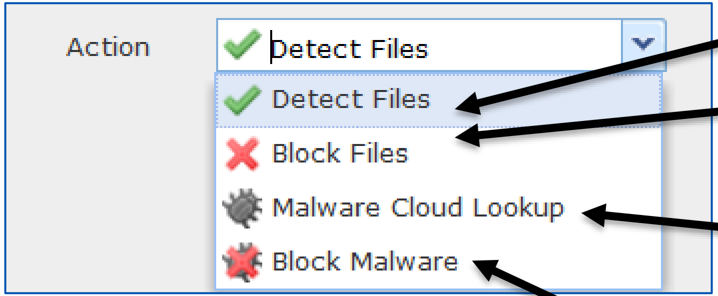
#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Applications	Source Ports	Dest Ports	URLs	Source Dynamic Attributes	Destination Dynamic Attributes	Action		
Mandatory - test (1-4)																
1	Allow Rule	Any	Any	10.10.10.1	20.20.20.2	Any	Any	Any	Any	Any	Any	Any	Any	Allow	0	
2	blocktelnet	Any	Any	5.5.5.5	6.6.6.6	Any	Any	Telnet	Any	Any	Any	Any	Any	Block	0	

Forward to Intrusion Policy

Forward to File Policy



- File Policy provides few different functionalities:



Action: Detect Files

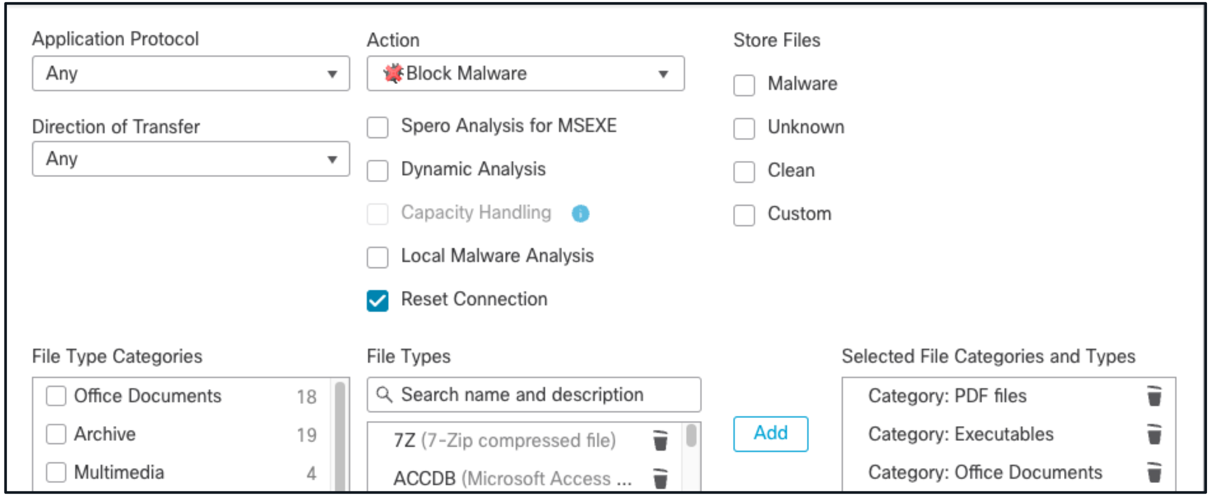
Detect Files = Checks first 1460 Bytes of a file, determines the type and **generates a log**

Block Files = Blocks the file based on first 1460 Bytes

Malware Cloud Lookup = Sends the SHA-256 hash of a file to the cloud for analysis and depending on the answer **generates a log if the file is bad**. Optionally, Local Analysis can analyze the file and Dynamic Analysis Capable files can be sent to cloud for Dynamic Analysis and/or SPERO analysis

Block Malware = Sends the SHA-256 hash of a file to the cloud for analysis and depending on the **answer blocks it if the file is bad**. Optionally, Local Analysis **can block** the file and/or Dynamic Analysis Capable files can be sent to cloud for Dynamic Analysis and/or SPERO analysis.

Packet Processing: Access Control with File Policy



Application Protocol: Any ▾

Direction of Transfer: Any ▾

Action: Block Malware ▾

□ Spero Analysis for MSEXE

□ Dynamic Analysis

□ Capacity Handling

□ Local Malware Analysis

☑ Reset Connection

Store Files

□ Malware

□ Unknown

□ Clean

□ Custom

File Type Categories

□ Office Documents	18
□ Archive	19
□ Multimedia	4

File Types

Search name and description

7Z (7-Zip compressed file)

ACCDB (Microsoft Access ...

Add

Selected File Categories and Types

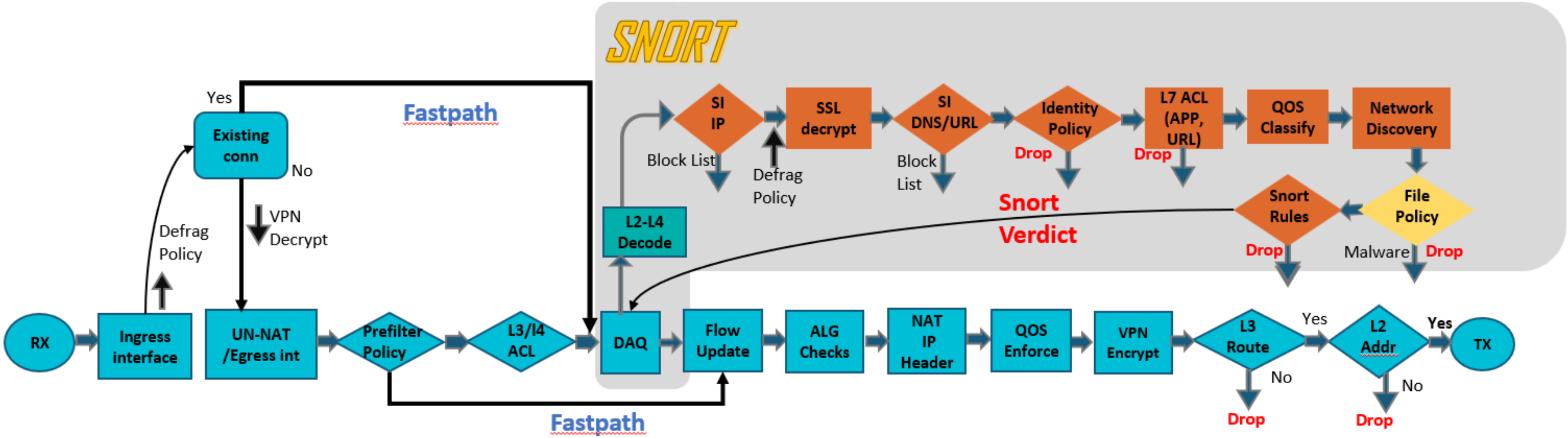
Category: PDF files

Category: Executables

Category: Office Documents

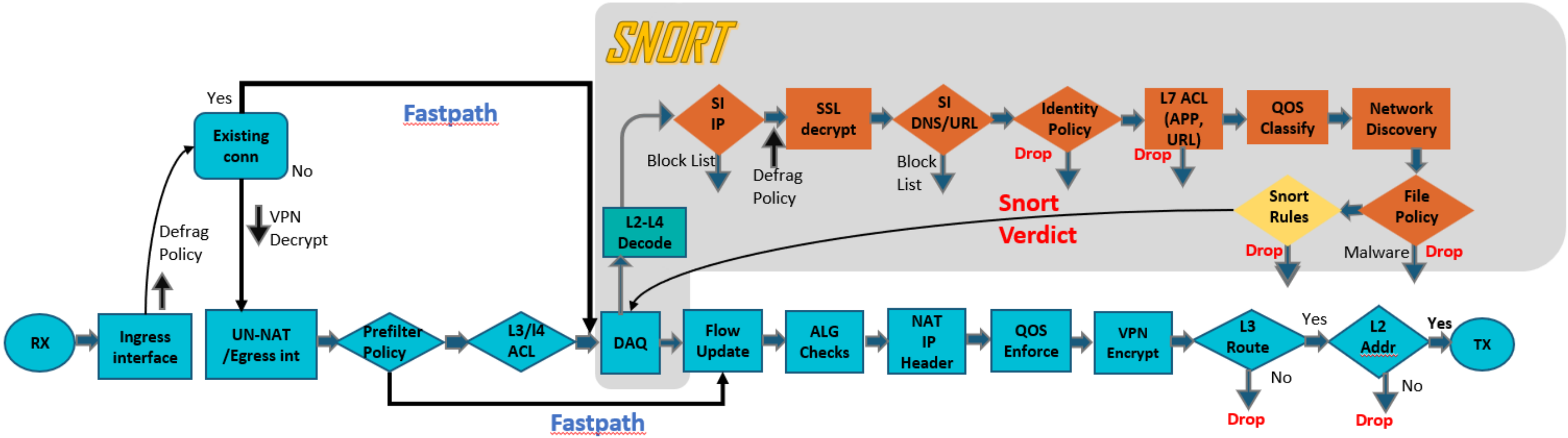
- Like Intrusion Policies, a **File Policy** is tied to an Access Control Rule
- Checks files by looking at the SHA256 hash to compare against known malware hashes
- Can submit unknown files to the AMP cloud or Secure Malware Analytics (SMA) appliance

```
> system support firewall-engine-debug
10.1.1.2-16969 > 10.9.9.9-80 6 AS 0 I 1 File malware event for
275a021bbfb6489e54d471899f7db9d1663fc695ec2fe2a2c4538aabf651fd0f named eicar.com with
disposition Malware and action Block Malware
```



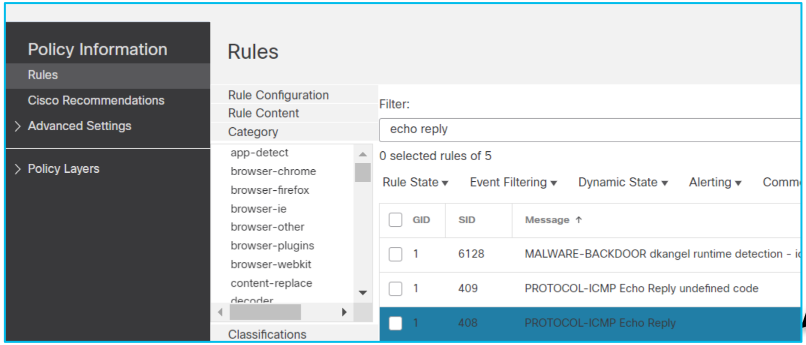
If File Policy doesn't work properly:

- Check that Malware license is installed on FMC and applied on Secure Firewall
- Make sure the File Policy is attached to the Access Control Policy
- Make sure the File Policy has proper Actions configured
- Check connectivity between FMC and Cloud (US or Europe cloud)
- If the file is too large (over about 100Mb), or too small (approximately 6K), it will not be sent for dynamic analysis, static analysis or file pre-classification



- Intrusion Policy (Snort Rules)

(Policies > Access Control > Intrusion)



Policy Information
- Rules
- Cisco Recommendations
- > Advanced Settings
- > Policy Layers

Rules

Rule Configuration
Rule Content
Category
app-detect
browser-chrome
browser-firefox
browser-ie
browser-other
browser-plugins
browser-webkit
content-replace
decoder
Classifications

Filter: echo reply

0 selected rules of 5

Rule State ▾ Event Filtering ▾ Dynamic State ▾ Alerting ▾ Comm

□	GID	SID	Message ↑
□	1	6128	MALWARE-BACKDOOR dkangel runtime detection - i
□	1	409	PROTOCOL-ICMP Echo Reply undefined code
□	1	408	PROTOCOL-ICMP Echo Reply

Tip – You can enable Snort Signature **GID=1, SID=408** (PROTOCOL-ICMP Echo Reply) to block ICMP echo replies and test the above

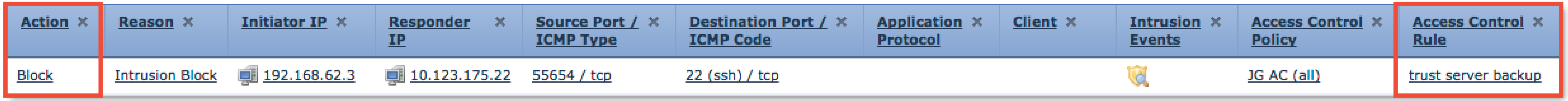
Packet Processing: Rule Evaluation

firewall-engine-debug

SSH Connection from 192.168.62.3 to 10.123.175.22

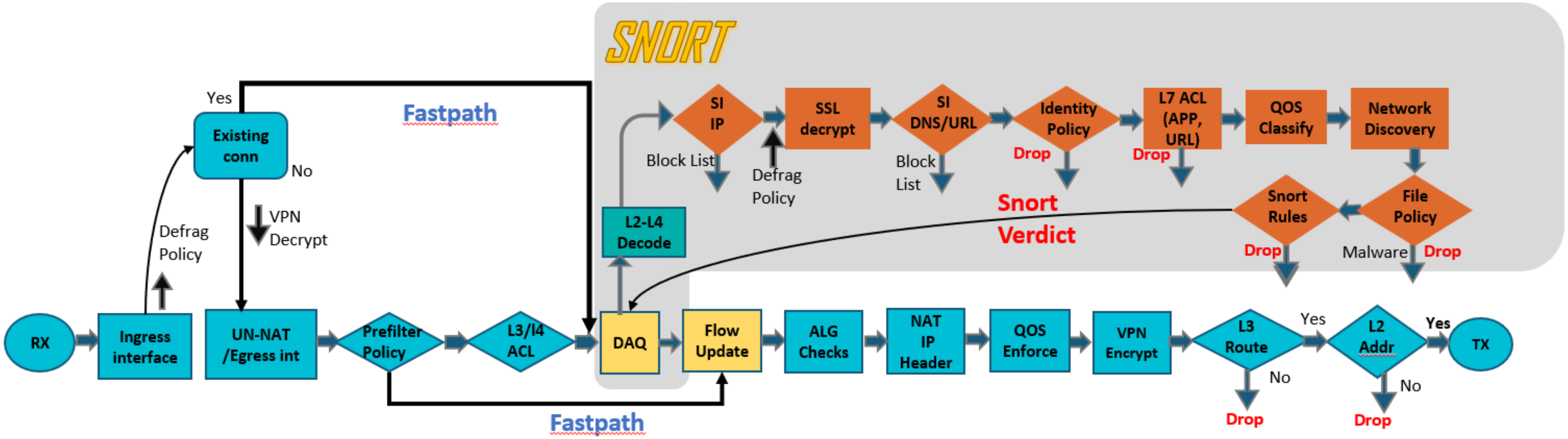
(Blocked/Ended before matching an AC rule)

```
192.168.62.3-54650 > 10.123.175.22-22 6 AS 1 I 0 New session
192.168.62.3-54650 > 10.123.175.22-22 6 AS 1 I 0 Starting with minimum 4, 'inspect', and IPProto first with
zones 1 -> 2, 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
192.168.62.3-54650 > 10.123.175.22-22 6 AS 1 I 0 pending rule order 4, 'inspect', XFF wait for AppId
192.168.62.3-54650 > 10.123.175.22-22 6 AS 1 I 0 Deleting session

[!Session was deleted because we hit a drop IPS rule and blocklisted the flow.
This happened before AC rule was matched (Intrusion policy before AC rule match dropped).
Firewall engine will re-evaluate from top of AC policy to find a rule for logging decision]

192.168.62.3-54650 > 10.123.175.22-22 6 AS 1 I 0 Starting with minimum 0, id 0 and IPProto first with zones
1 -> 2, geo 0 -> 0, vlan 0, inline sgt tag: 0, ISE sgt id: 0, svc -1, payload -1, client -1, misc -1, user
9999997, icmpType 102, icmpCode 22
192.168.62.3-54650 > 10.123.175.22-22 6 AS 1 I 0 no match rule order 3, 'Trust ssh for host', src network
and GEO
192.168.62.3-54650 > 10.123.175.22-22 6 AS 1 I 0 no match rule order 4, 'inspect', XFF non-http
192.168.62.3-54650 > 10.123.175.22-22 6 AS 1 I 0 match rule order 5, 'trust server backup', action Trust
```



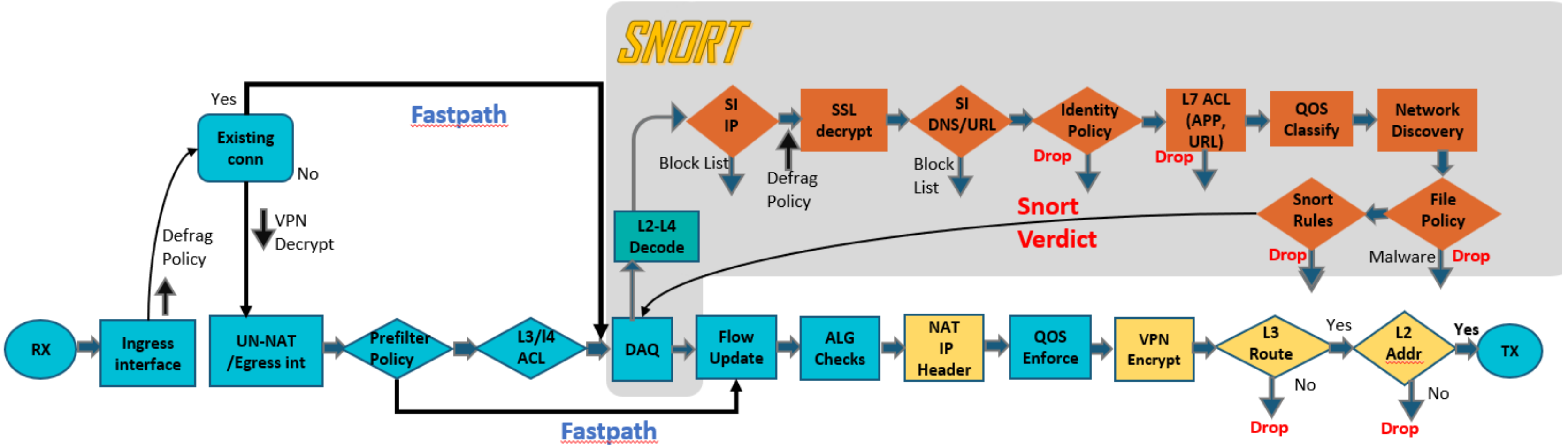
Action	Reason	Initiator IP	Responder IP	Source Port / ICMP Type	Destination Port / ICMP Code	Application Protocol	Client	Intrusion Events	Access Control Policy	Access Control Rule
Block	Intrusion Block	192.168.62.3	10.123.175.22	55654 / tcp	22 (ssh) / tcp				JG AC (all)	trust server backup

AC Rule has “Trust” action but connection event action shows “Block”



- At this point the Snort Engine returns to Lina Data Path through the DAQ and PDTS framework a verdict (Pass, Block-list (Block), Fast-Forward etc)
- Note: It is extremely rare for any packets to be dropped at this stage.
- Depending on the verdict the Lina engine will update the Flow accordingly (terminate or proceed with further checks)

```
> show logging | include connection
Jun 13 2022 13:32:49: %FTD-6-302021: Teardown ICMP connection for faddr 192.168.76.14/0 gaddr 192.168.75.14/0 laddr
192.168.75.14/0
Jun 13 2022 13:33:00: %FTD-6-302016: Teardown UDP connection 357875 for inside:192.168.75.14/60131 to dmz:192.168.76.14/53
duration 0:02:01 bytes 43

> show conn address 192.168.75.179
UDP outside  192.168.75.179:138 inside  192.168.75.255:138, idle 0:00:19, bytes 35306, flags - N
UDP outside  192.168.75.179:137 inside  192.168.75.255:137, idle 0:00:19, bytes 6350, flags - N
```

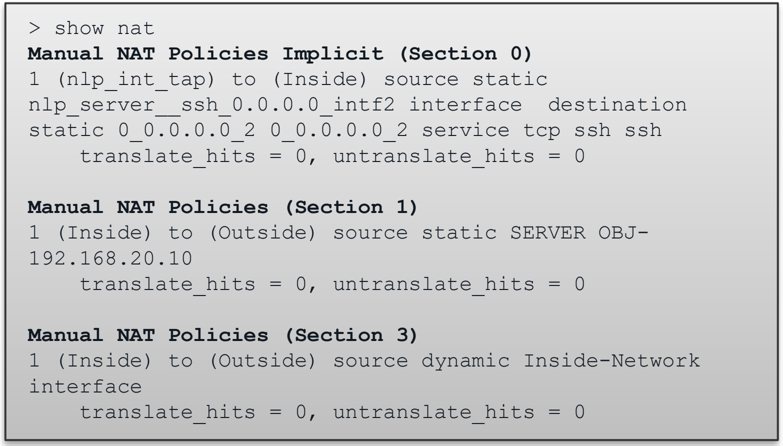


The remaining checks on Lina engine are the same as on classic ASA

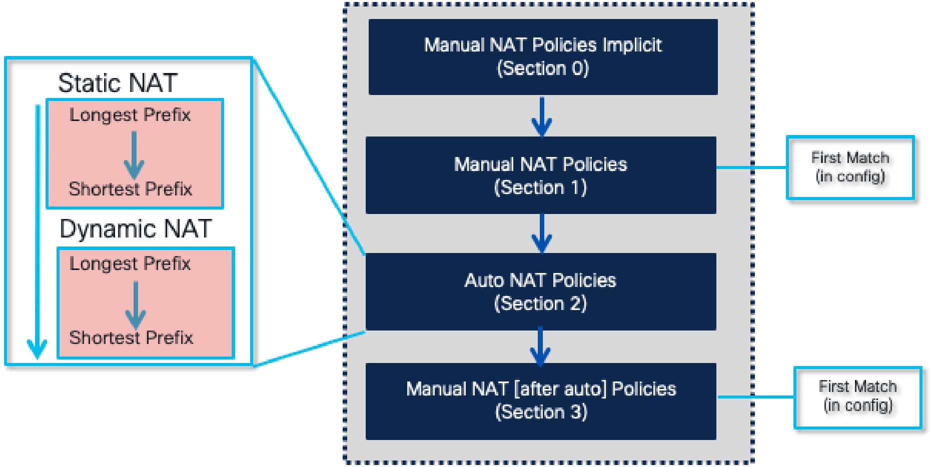
- NAT IP header
- VPN Encrypt
- L3 Route
- L2 Resolution of next hop

NAT Order of Operation

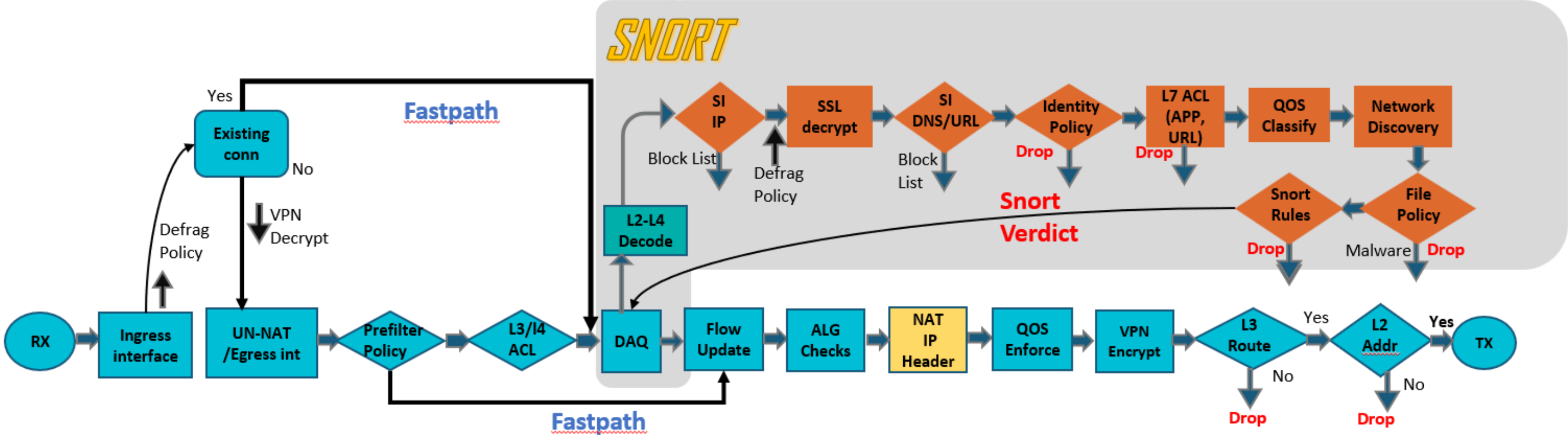
- In Secure Firewall version 7.0, a new section, Section 0, is added to the NAT table for all implicit NAT rules for NLP applications (sftunnel, SSH, SNMP, HTTP)



```
> show nat
Manual NAT Policies Implicit (Section 0)
1 (nlp_int_tap) to (Inside) source static
nlp_server__ssh_0.0.0.0_intf2 interface  destination
static 0_0.0.0.0_2 0_0.0.0.0_2 service tcp ssh ssh
    translate_hits = 0, untranslate_hits = 0

Manual NAT Policies (Section 1)
1 (Inside) to (Outside) source static SERVER OBJ-
192.168.20.10
    translate_hits = 0, untranslate_hits = 0

Manual NAT Policies (Section 3)
1 (Inside) to (Outside) source dynamic Inside-Network
interface
    translate_hits = 0, untranslate_hits = 0
```

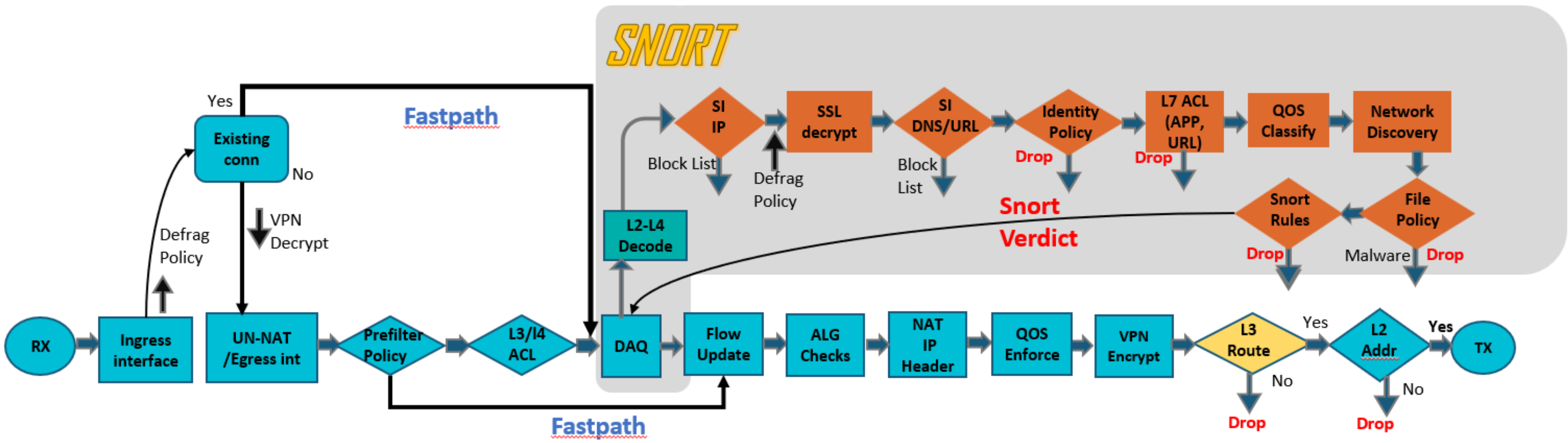


Static NAT
Longest Prefix
Shortest Prefix
Dynamic NAT
Longest Prefix
Shortest Prefix
Manual NAT Policies Implicit (Section 0)
Manual NAT Policies (Section 1)
First Match (in config)
Auto NAT Policies (Section 2)
Manual NAT [after auto] Policies (Section 3)
First Match (in config)



- Here is where the actual NAT is happening
- The source/destination IP addresses and Ports (in case of PAT) are rewritten

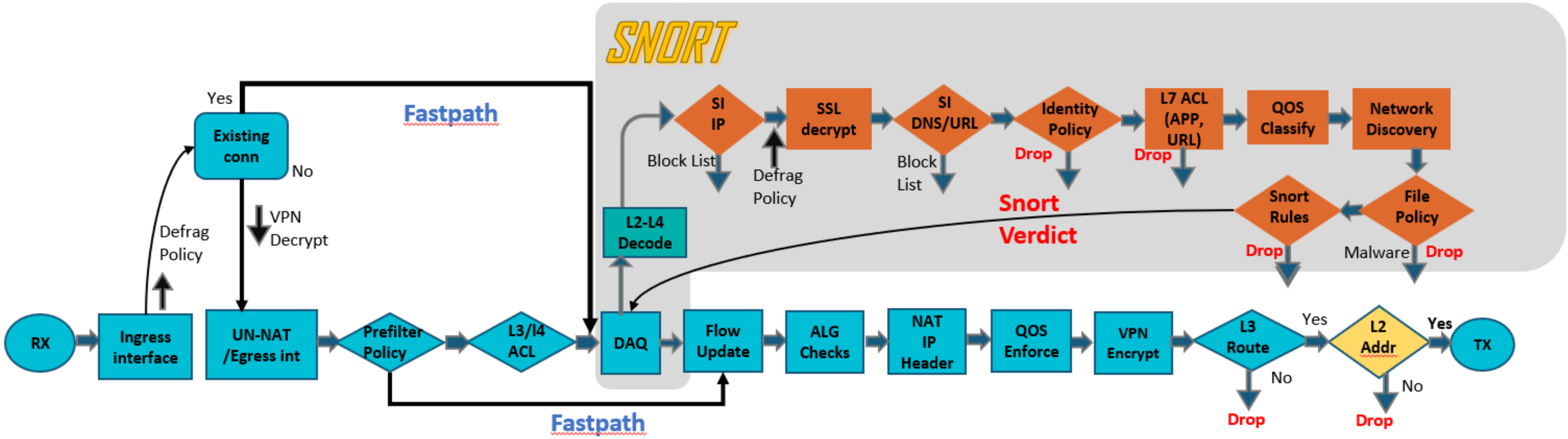
```
> show capture CAPI packet-number 1 trace
   1: 18:54:43.658001  192.168.75.14 > 192.168.77.1: icmp: echo request
..
Phase: 6
Type: NAT
Subtype:
Result: ALLOW
Config:
nat (inside,outside) source dynamic Net_192.168.75.0_24bits interface
Additional Information:
Dynamic translate 192.168.75.14/1 to 192.168.77.6/1
```



- Based on the outcome of the UN-NAT/Egress interface determination the **'out'** entries of the ASP routing table will be checked to determine the next hop IP

```
firepower# show asp table routing
route table timestamp: 449
in   192.168.75.0    255.255.255.0   inside
in   192.168.76.0    255.255.255.0   dmz
in   192.168.77.0    255.255.255.0   outside
in   5.5.5.5         255.255.255.255 via 192.168.77.1, outside
out  255.255.255.255 255.255.255.255 outside
out  5.5.5.5         255.255.255.255 via 192.168.77.1, outside
out  10.1.1.0        255.255.255.0   via 192.168.77.1, outside
```

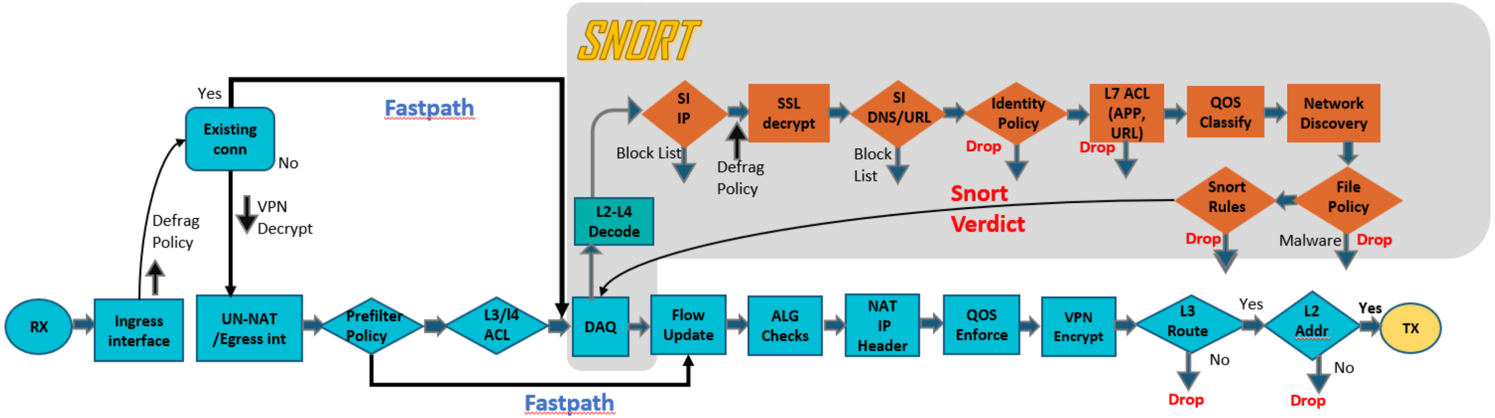
```
> show capture CAPI packet-number 3 trace
3: 09:11:54.814395 192.168.75.39 > 192.168.77.40: icmp: echo request
..
Phase: 15
Type: ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
found next-hop 192.168.77.40 using egress ifc  outside
```



- Based on the outcome of the L3 Route Next Hop determination the local ARP table is being checked for an entry

```
> show arp
        inside 192.168.75.14 000c.2930.2b78 8
        inside 192.168.75.12 000c.29d0.ebcf 1286
        inside 192.168.75.39 0004.deab.681b 3923
        inside 192.168.75.122 000c.29ec.80e1 12451
        dmz 192.168.76.14 000c.2998.3fec 55
        dmz 192.168.76.1 c84c.758d.4981 3413
        dmz 192.168.76.39 0004.deab.681a 3743
        outside 192.168.77.23 6c41.6aa1.2bf5 1305
        outside 192.168.77.40 c84c.758d.4980 4613
```

```
> show capture CAPI packet-number 3 trace
3: 09:11:54.814395 192.168.75.39 > 192.168.77.40: icmp: echo request
..
Phase: 16
Type: ADJACENCY-LOOKUP
Subtype: next-hop and adjacency
Result: ALLOW
Config:
Additional Information:
adjacency Active
next-hop mac address c84c.758d.4980 hits 140
```



- Packet is transmitted on wire
- Interface counters will increment on interface
- **Underrun** counter may indicate drops due to egress interface oversubscription
  - TX ring is full

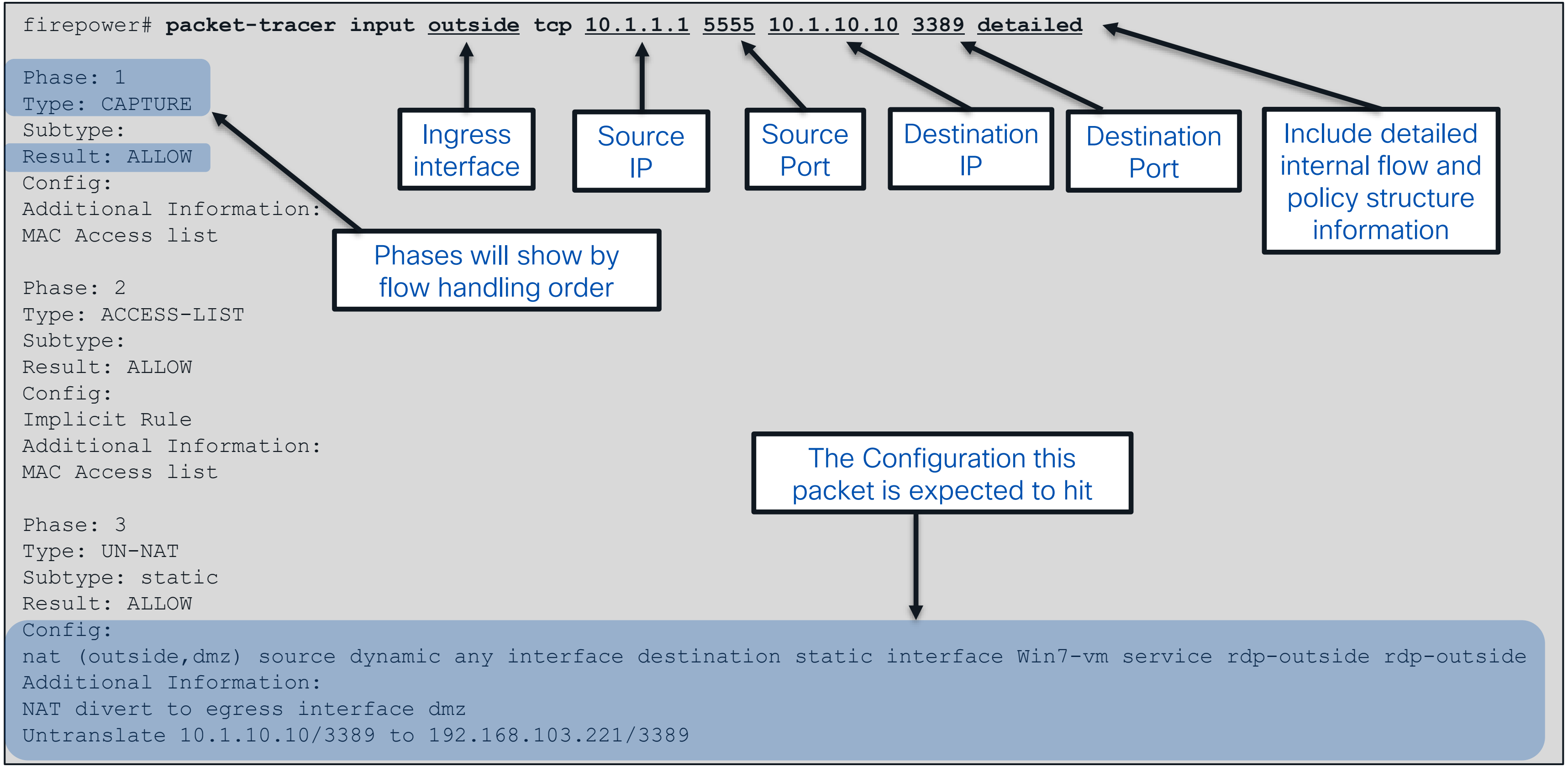
```
> show interface outside
Interface GigabitEthernet0/1 "outside", is up, line protocol is up
        …
        273399 packets output, 115316725 bytes, 80 underruns
        …
        input queue (blocks free curr/low): hardware (485/441)
        output queue (blocks free curr/low): hardware (463/0)
```

You have connectivity issues, now What?

1) Understand the topology.
2) Understand the packet flow.
3) Simultaneously collect at the time of the issue:
   - Packet Tracer
   - Captures: ASP drops, Capture with Trace
   - System support Trace (firewall engine debug)
   - Check connection events
   - Syslogs

Note:
Troubleshooting file/show tech need to be collected before rebooting the device.

Packet Tracer



```
firepower# packet-tracer input outside tcp 10.1.1.1 5555 10.1.10.10 3389 detailed

Phase: 1
Type: CAPTURE
Subtype:
Result: ALLOW
Config:
Additional Information:
MAC Access list

Phase: 2
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
MAC Access list

Phase: 3
Type: UN-NAT
Subtype: static
Result: ALLOW
Config:
nat (outside,dmz) source dynamic any interface destination static interface Win7-vm service rdp-outside rdp-outside
Additional Information:
NAT divert to egress interface dmz
Untranslate 10.1.10.10/3389 to 192.168.103.221/3389
```

Ingress interface
Source IP
Source Port
Destination IP
Destination Port
Include detailed internal flow and policy structure information
Phases will show by flow handling order
The Configuration this packet is expected to hit

Packet Tracer Sample Output

```
Phase: 4
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group outside_in in interface outside
access-list outside_in extended permit tcp any any eq 3389
Additional Information:
……
Phase: 12
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 16538274, packet dispatched to next module

Result:
input-interface: outside
input-status: up
input-line-status: up
output-interface: dmz
output-status: up
output-line-status: up
Action: allow
```

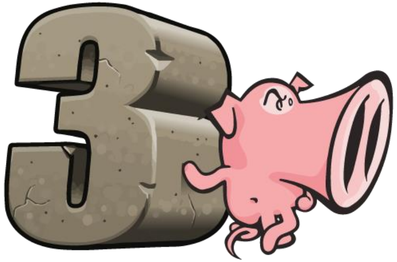
Focus on the end result

Packet Tracer Enhancements 7.1

- Improved navigation helps easy access to the Packet Tracer tool in UI.
- Tabs support running multiple packets.
- PCAP file as input support to replay and trace an entire flow traces in parallel across managed devices

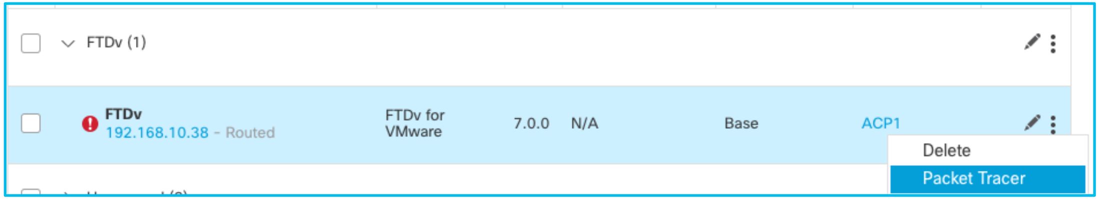
PCAP Replay Capability → Such tracing of packets gives us a good insight into various NGFW capabilities; especially L4-L7 rule validations.

- REST API support.
- Detailed Snort 3 Phases



FMC 7.1 Enhancement – Packet Tracer in FMC GUI

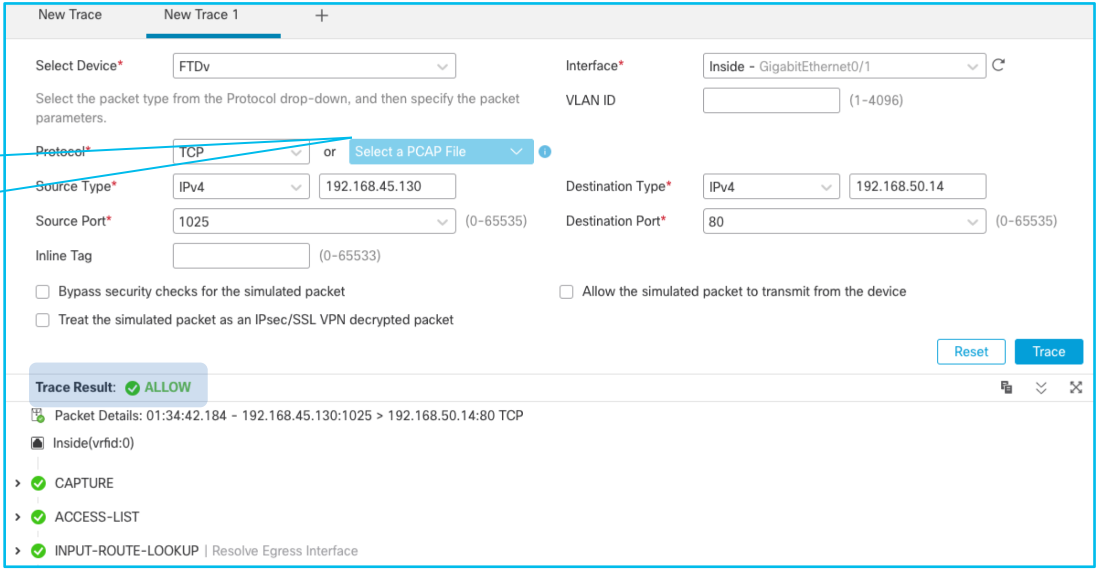
1 From Device Menu



FTDv (1)

FTDv 192.168.10.38 - Routed	FTDv for VMware	7.0.0	N/A	Base	ACP1	

2 Define Simulated packet



Select Device*: FTDv

Interface*: Inside - GigabitEthernet0/1

Select the packet type from the Protocol drop-down, and then specify the packet parameters.

VLAN ID: (1-4096)

Protocol*: TCP or Select a PCAP File

Source Type*: IPv4 192.168.45.130

Destination Type*: IPv4 192.168.50.14

Source Port*: 1025 (0-65535)

Destination Port*: 80 (0-65535)

Inline Tag: (0-65533)

☐ Bypass security checks for the simulated packet

☐ Allow the simulated packet to transmit from the device

☐ Treat the simulated packet as an IPsec/SSL VPN decrypted packet

3 Resulting action

Trace Result: ✓ ALLOW

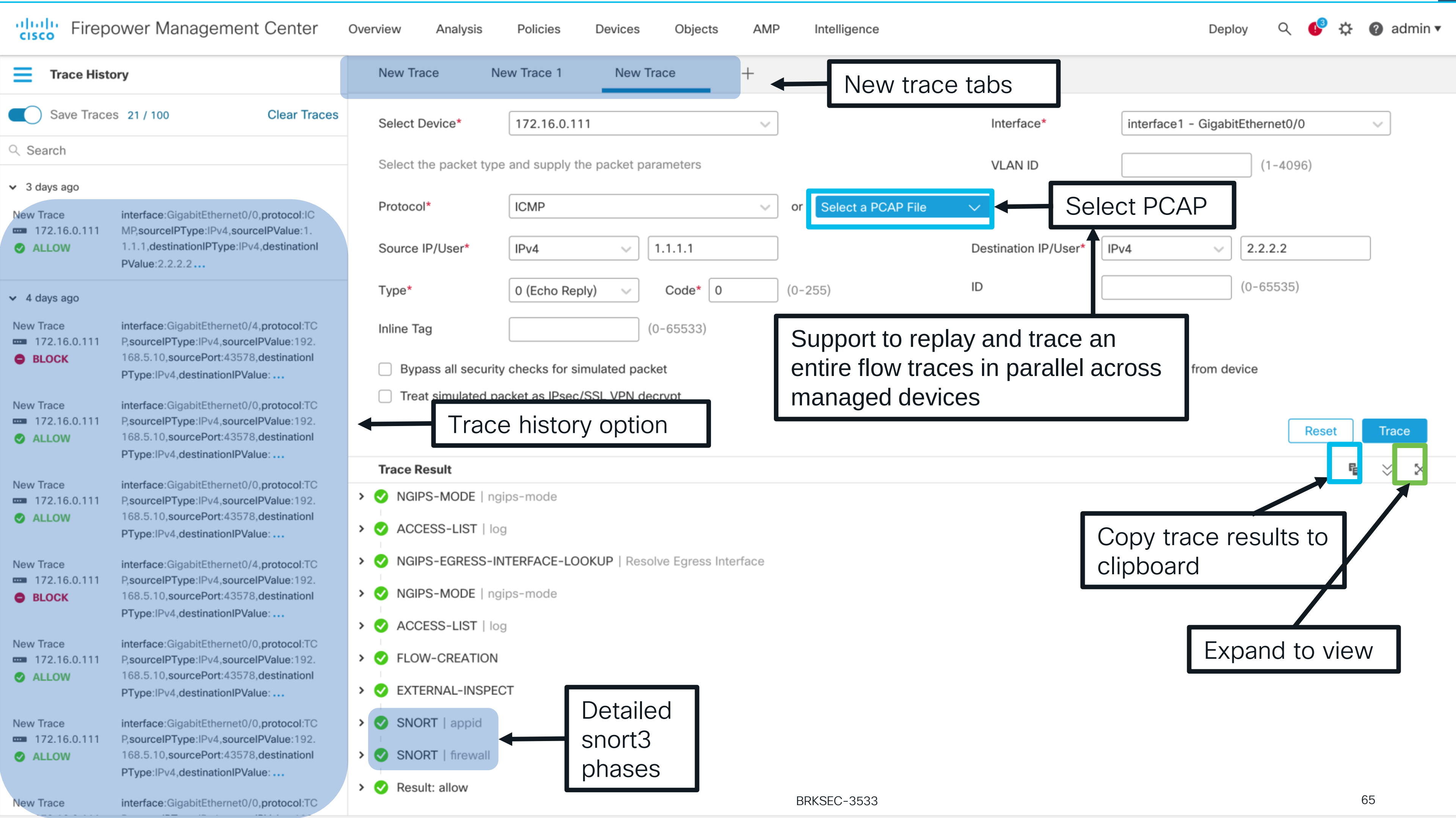
Packet Details: 01:34:42.184 - 192.168.45.130:1025 > 192.168.50.14:80 TCP

Inside(vrfid:0)

› ✓ CAPTURE

› ✓ ACCESS-LIST

› ✓ INPUT-ROUTE-LOOKUP | Resolve Egress Interface



New trace tabs

Save Traces 21 / 100 Clear Traces

Search

3 days ago

New Trace
172.16.0.111
ALLOW
interface:GigabitEthernet0/0,protocol:ICMP,sourceIPType:IPv4,sourceIPValue:1.1.1.1,destinationIPType:IPv4,destinationIPValue:2.2.2.2...

4 days ago

New Trace
172.16.0.111
BLOCK
interface:GigabitEthernet0/4,protocol:TCP,sourceIPType:IPv4,sourceIPValue:192.168.5.10,sourcePort:43578,destinationIPType:IPv4,destinationIPValue:...

New Trace
172.16.0.111
ALLOW
interface:GigabitEthernet0/0,protocol:TCP,sourceIPType:IPv4,sourceIPValue:192.168.5.10,sourcePort:43578,destinationIPType:IPv4,destinationIPValue:...

New Trace
172.16.0.111
ALLOW
interface:GigabitEthernet0/0,protocol:TCP,sourceIPType:IPv4,sourceIPValue:192.168.5.10,sourcePort:43578,destinationIPType:IPv4,destinationIPValue:...

New Trace
172.16.0.111
BLOCK
interface:GigabitEthernet0/4,protocol:TCP,sourceIPType:IPv4,sourceIPValue:192.168.5.10,sourcePort:43578,destinationIPType:IPv4,destinationIPValue:...

New Trace
172.16.0.111
ALLOW
interface:GigabitEthernet0/0,protocol:TCP,sourceIPType:IPv4,sourceIPValue:192.168.5.10,sourcePort:43578,destinationIPType:IPv4,destinationIPValue:...

New Trace
172.16.0.111
ALLOW
interface:GigabitEthernet0/0,protocol:TCP,sourceIPType:IPv4,sourceIPValue:192.168.5.10,sourcePort:43578,destinationIPType:IPv4,destinationIPValue:...

New Trace
interface:GigabitEthernet0/0,protocol:TC

Select Device* 172.16.0.111

Interface* interface1 - GigabitEthernet0/0

Select the packet type and supply the packet parameters

VLAN ID (1-4096)

Protocol* ICMP or Select a PCAP File

Select PCAP

Source IP/User* IPv4 1.1.1.1

Destination IP/User* IPv4 2.2.2.2

Type* 0 (Echo Reply) Code* 0 (0-255)

ID (0-65535)

Inline Tag (0-65533)

☐ Bypass all security checks for simulated packet

☐ Treat simulated packet as IPsec/SSL VPN decrypt

from device

Support to replay and trace an entire flow traces in parallel across managed devices

Trace history option

Trace Result

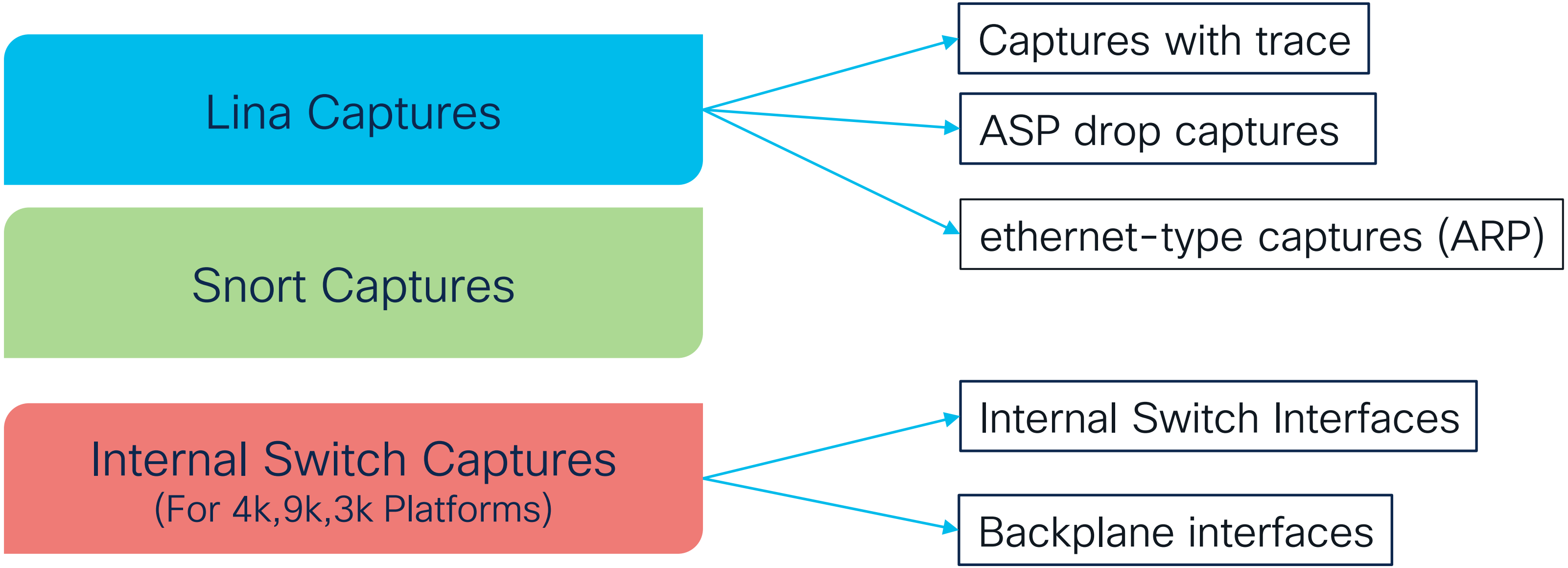
- NGIPS-MODE | ngips-mode
- ACCESS-LIST | log
- NGIPS-EGRESS-INTERFACE-LOOKUP | Resolve Egress Interface
- NGIPS-MODE | ngips-mode
- ACCESS-LIST | log
- FLOW-CREATION
- EXTERNAL-INSPECT
- SNORT | appid
- SNORT | firewall
- Result: allow

Detailed snort3 phases

Copy trace results to clipboard

Expand to view

Captures



Lina Captures

Captures with trace

ASP drop captures

ethernet-type captures (ARP)

Snort Captures

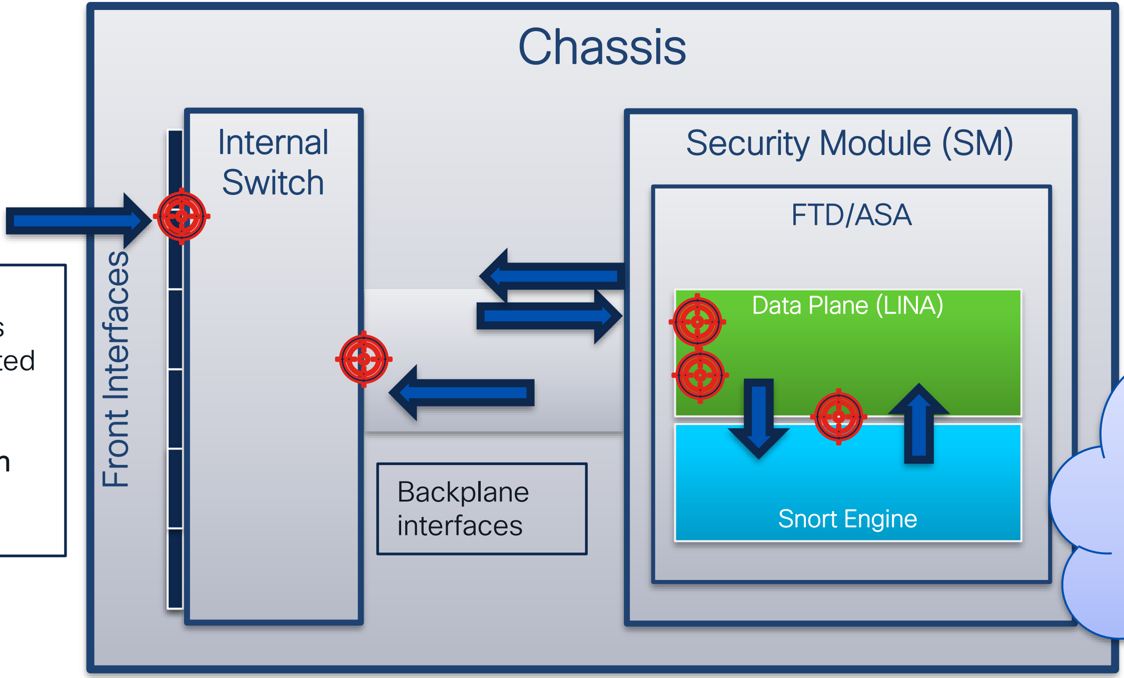
Internal Switch Captures
(For 4k,9k,3k Platforms)

Internal Switch Interfaces

Backplane interfaces

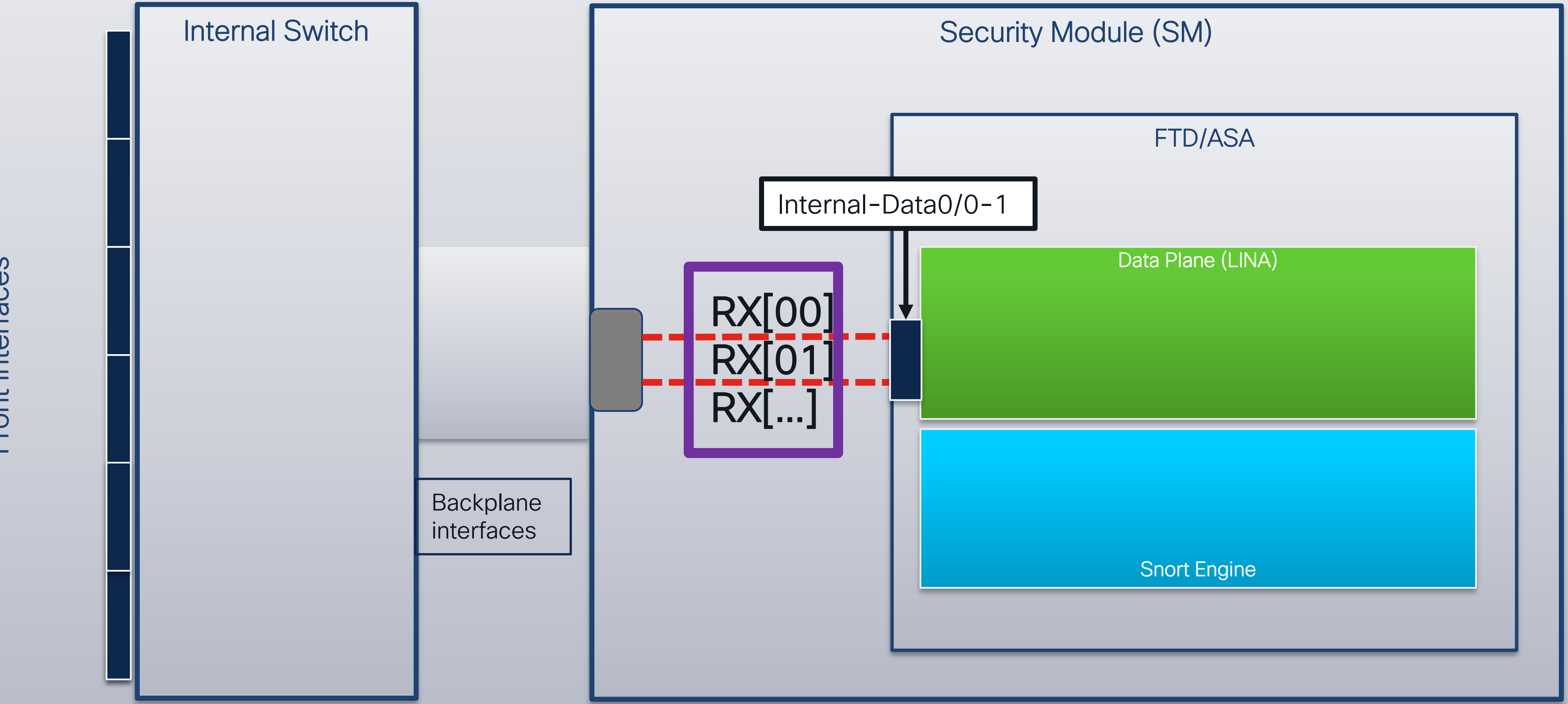
Capture Points For 41xx, 42xx, 93xx and 31xx devices

For the internal switch, captures are only supported in the **ingress** direction **(Egress direction capture is not possible**)

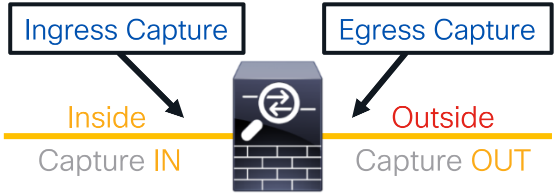


1100/2100 platforms do not officially support internal switch captures

Chassis


Front Interfaces
Internal Switch
Backplane interfaces
Security Module (SM)
FTD/ASA
Internal-Data0/0-1
RX[00]
RX[01]
RX[...]
Data Plane (LINA)
Snort Engine

Lina Captures



Main capture points:

Ingress Interface

Egress Interface

ASP Interface

```
> capture CAPI interface INSIDE match icmp host 192.168.103.1 host 192.168.101.1
```

Interface

Protocol

Source IP

Destination IP

To verify

```
> Show capture CAPI
```

ASP drops captures

```
> capture ASP type asp-drop all
```

```
> Show capture asp | i "ip address"
```

ARP Captures

```
> capture ARP ethernet-type arp interface OUTSIDE
```

```
> Show capture ARP
```

Lina Capture

- Apply capture under unique name to ingress and egress interfaces
- Define the traffic that you want to capture, use pre-NAT information for source IP and post-NAT for destination IP

```
firepower# capture OUT interface outside match ip any host 172.18.124.1
firepower# capture IN interface inside match ip any host 172.18.124.1
firepower# show capture IN

4 packets captured

   1: 10:51:26.139046       802.1Q vlan#10 P0 172.18.254.46 > 172.18.124.1: icmp: echo request
   2: 10:51:26.139503       802.1Q vlan#10 P0 172.18.124.1 > 172.18.254.46: icmp: echo reply
   3: 10:51:27.140739       802.1Q vlan#10 P0 172.18.254.46 > 172.18.124.1: icmp: echo request
   4: 10:51:27.141182       802.1Q vlan#10 P0 172.18.124.1 > 172.18.254.46: icmp: echo reply
4 packets shown

firepower# no capture IN
```

Unlike ACL, match covers both directions of the flow

Remember to remove the captures when done with troubleshooting

Lina Captures (continued)

- Captures can be exported to PCAP format to an external server:

```
copy /pcap capture:CAPI tftp://192.168.78.73
```

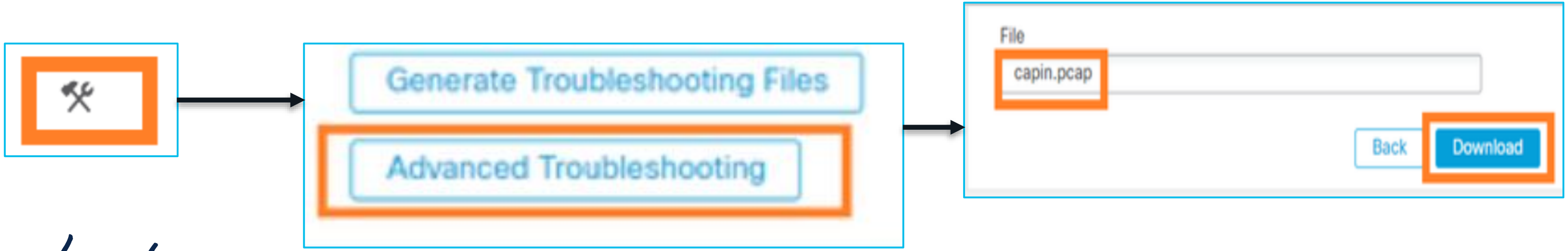
- Collect PCAP from FMC GUI:

```
copy /pcap capture:capin disk0:capin.pcap
```

From Secure Firewall expert mode (after using “sudo su –”):

```
root@firepower:/mnt/disk0# cp capin.pcap /ngfw/var/common
```

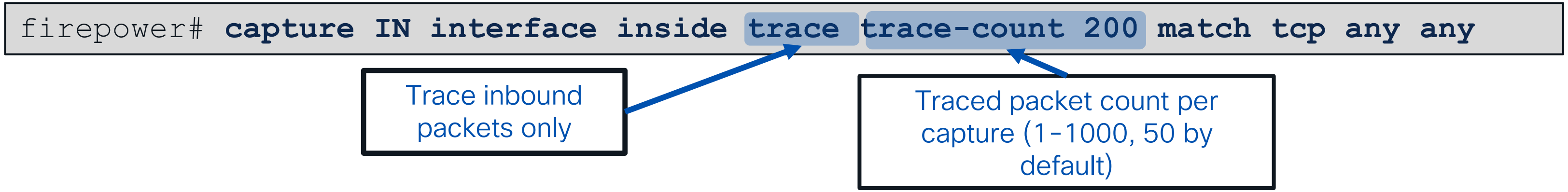
From FMC GUI, navigate to **Devices** > **Device Management.** Locate the Secure Firewall device and select the Troubleshoot icon:



File: capin.pcap

Packet Capture w/ Trace

- Enable packet tracer within an internal packet capture



```
firepower# capture IN interface inside trace trace-count 200 match tcp any any
```

Trace inbound packets only

Traced packet count per capture (1-1000, 50 by default)

- Find the packet that you want to trace in the capture

```
firepower# show capture inside
  68 packets captured
  1: 15:22:47.581116 10.1.1.2.31746 > 198.133.219.25.80: S
  2: 15:22:47.583465 198.133.219.25.80 > 10.1.1.2.31746: S ack
  3: 15:22:47.585052 10.1.1.2.31746 > 198.133.219.25.80: . ack
  4: 15:22:49.223728 10.1.1.2.31746 > 198.133.219.25.80: P ack
  5: 15:22:49.223758 198.133.219.25.80 > 10.1.1.2.31746: . Ack
     ...
```

- Select that packet to show the tracer results

```
firepower# show capture inside trace packet-number 4
```

Cool Tips from TAC

New option captures packets that match the criteria after decryption

- You can now capture traffic post-decryption across a VPN tunnel w/ Secure Firewall as VPN endpoint:

```
firepower# capture OUT interface outside trace include-decrypted match tcp any any
```

- You can use headers-only option or set the buffer for the captures when there is high traffic rate:

```
firepower# Capture capin interface inside headers-only buffer 10000000
```

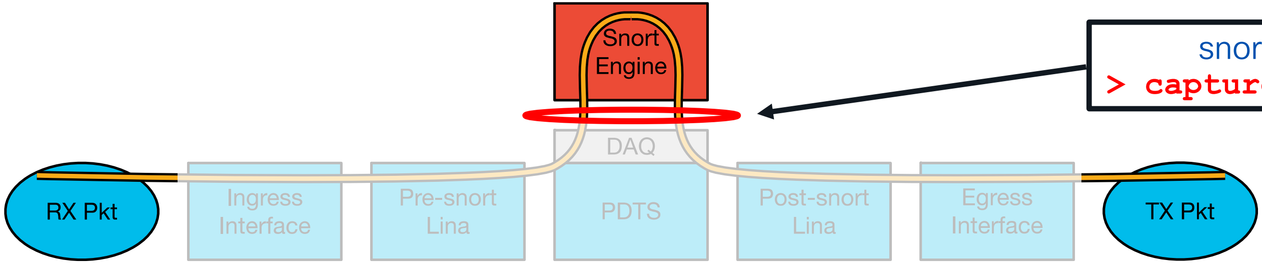
- Transmit packet tracer simulated packet to destination.

New packet-tracer option to allow egress of simulated packets

```
firepower#  packet-tracer input inside tcp 10.1.1.20 10000 10.1.2.100 80 transmit detailed
firepower#  sh cap capout
1 packet captured
   1: 12:08:30.837709       10.1.1.20.10000 > 10.1.2.100.80: S 1119191062:1119191062(0) win
```

cisco Live!

Snort-side captures



snort side
> capture-traffic

```
> 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: -w SNORTCAP.pcap -c 1000 host 192.168.1.2 and port 80
```

Filter Options

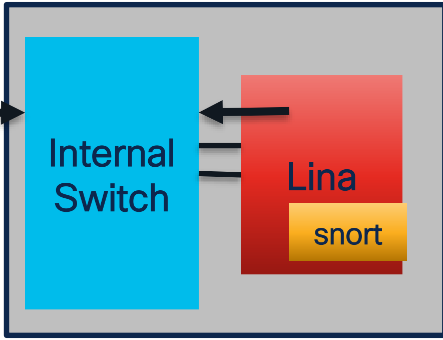
> capture-traffic
PCAPs are written to:
/ngfw/var/common/

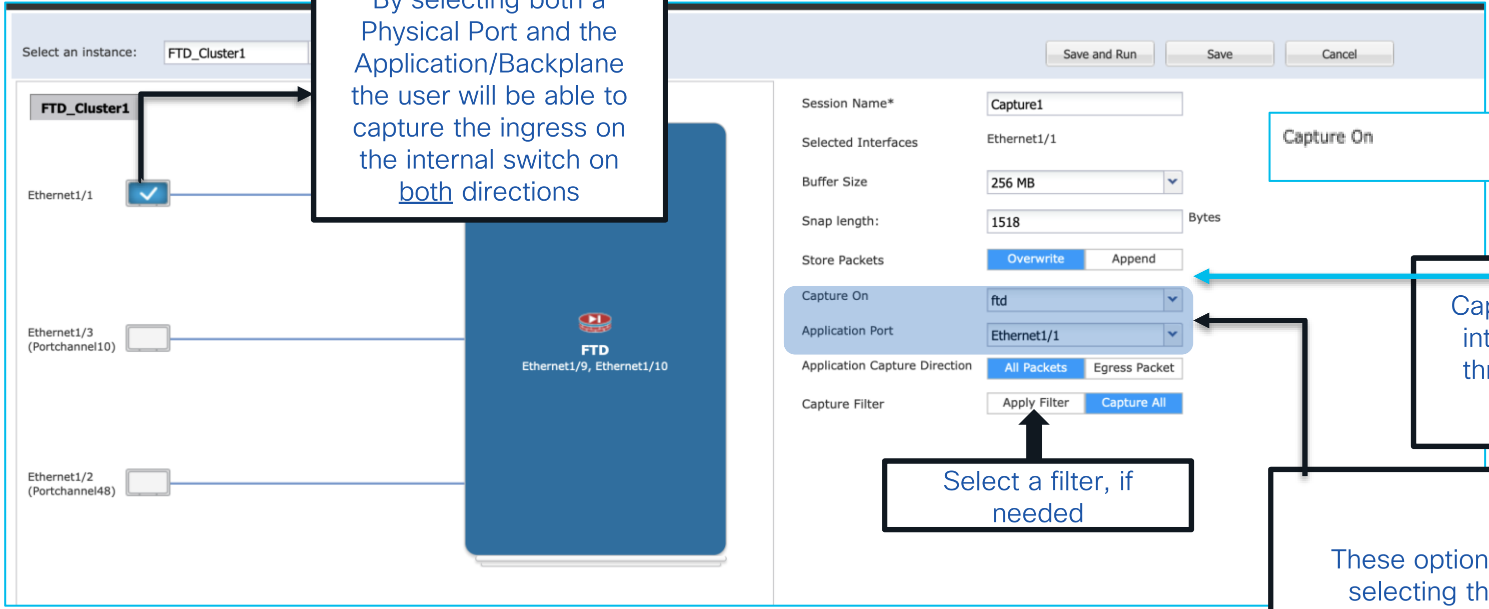
tcpdump -w FILE.pcap
Write the capture to file

TCPdump like format (BPF)

Internal Switch Captures
(for 41xx, 93xx)

- Internal switch captures can be only taken in the ingress direction of the internal switch
- From chassis FCM : **Tools** > **Packet Capture** > **Capture session**





FTD_Cluster1
Ethernet1/1
Ethernet1/3 (Portchannel10)
Ethernet1/2 (Portchannel48)
FTD
Ethernet1/9, Ethernet1/10
Save and Run
Save
Cancel

Select an instance: FTD_Cluster1

Session Name* Capture1

Selected Interfaces Ethernet1/1

Buffer Size 256 MB

Snap length: 1518 Bytes

Store Packets [✓ Overwrite] Append

Capture On ftd

Application Port Ethernet1/1

Application Capture Direction [✓ All Packets] Egress Packet

Capture Filter Apply Filter [✓ Capture All]

Capture On All Backplane Ports

By selecting both a Physical Port and the Application/Backplane the user will be able to capture the ingress on the internal switch on both directions

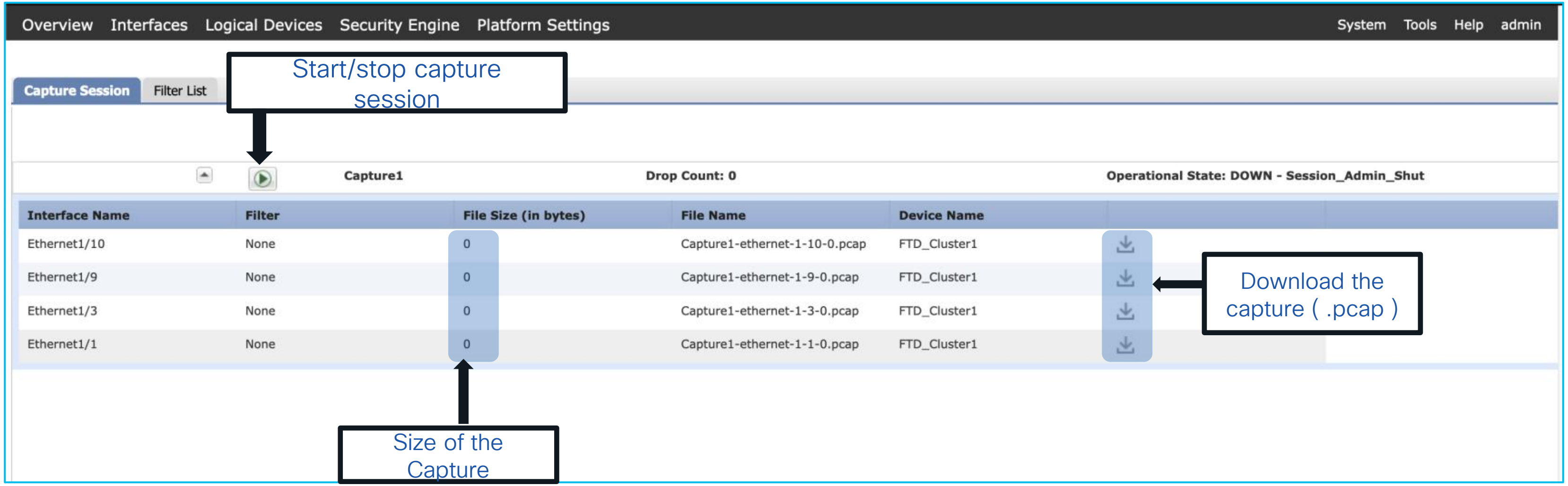
Capture all traffic coming into the internal switch through the Backplane interfaces

Select a filter, if needed

These options appear after selecting the application

FXOS Level Captures (for 41xx and 93xx)

Session Dashboard – Session created



Start/stop capture session

Capture1 Drop Count: 0 Operational State: DOWN - Session_Admin_Shut

Interface Name	Filter	File Size (in bytes)	File Name	Device Name
Ethernet1/10	None	0	Capture1-ethernet-1-10-0.pcap	FTD_Cluster1
Ethernet1/9	None	0	Capture1-ethernet-1-9-0.pcap	FTD_Cluster1
Ethernet1/3	None	0	Capture1-ethernet-1-3-0.pcap	FTD_Cluster1
Ethernet1/1	None	0	Capture1-ethernet-1-1-0.pcap	FTD_Cluster1

Download the capture (.pcap)

Size of the Capture

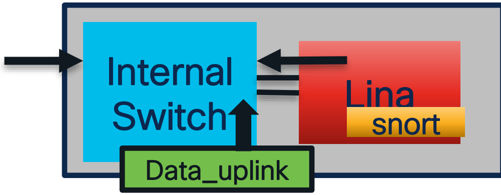
On this example ‘All Backplane Interfaces’ option was selected.

FXOS Level Captures (for 41xx and 93xx)

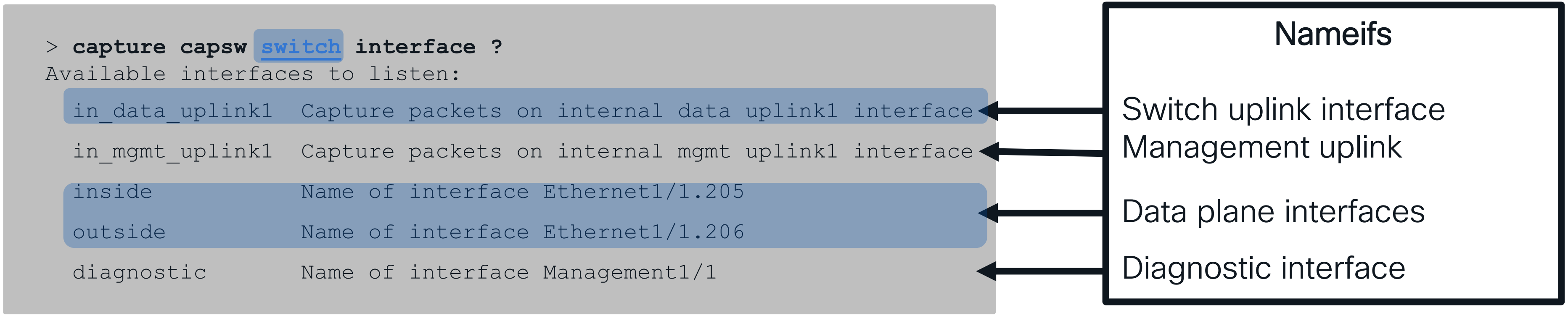
Troubleshooting tips

- Application-level captures do not provide full visibility to the packet path within the chassis. For better visibility consider taking simultaneous chassis and application-level captures.
- Use the filter !vntag on Wireshark to display only packets without the VN-tag. This is useful to hide VN-tagged packets in the front interface packet capture files (eliminate the packet duplication)
- In backplane captures use wireshark filter “frame.number & 1” to remove duplicates

Captures on 31xx and 42xx Platforms



- Internal switch packet capture configuration is unified with existing ASA/Secure Firewall Command-Line Interface (CLI) data plane packet capture configuration.
- Internal switch capture configuration accept ingress interface **nameif**:



```
> capture capsw switch interface ?
Available interfaces to listen:
  in_data_uplink1   Capture packets on internal data uplink1 interface
  in_mgmt_uplink1   Capture packets on internal mgmt uplink1 interface
  inside            Name of interface Ethernet1/1.205
  outside           Name of interface Ethernet1/1.206
  diagnostic        Name of interface Management1/1
```

Nameifs

Switch uplink interface

Management uplink

Data plane interfaces

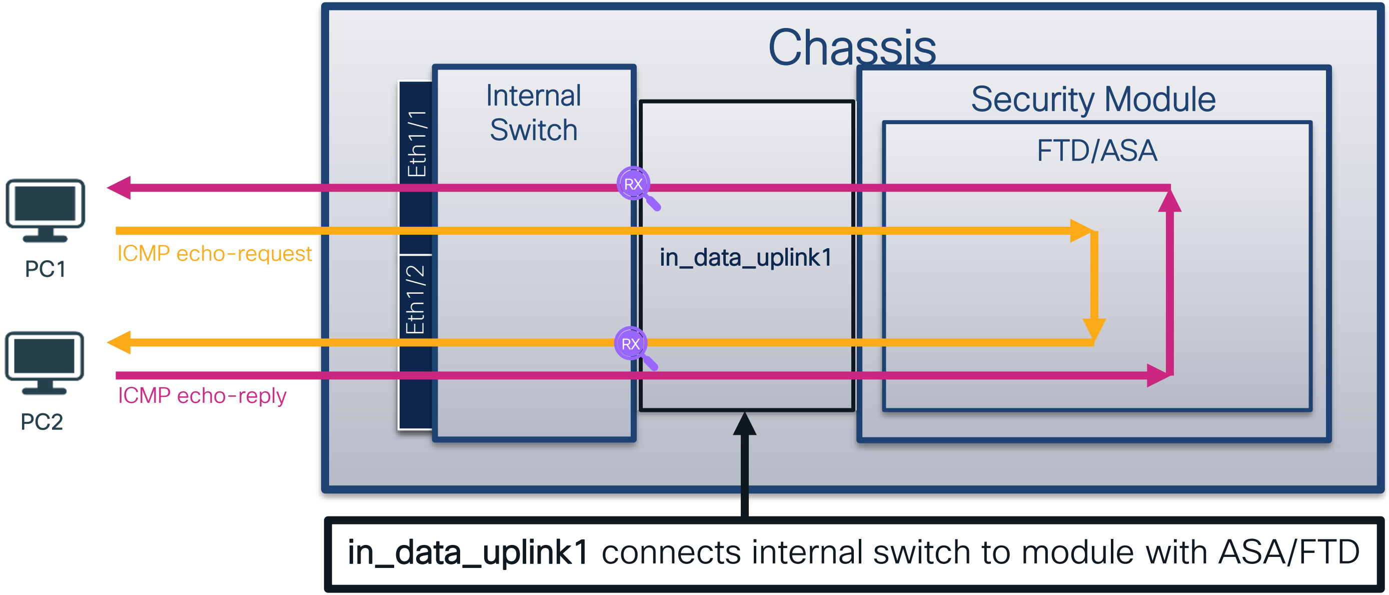
Diagnostic interface

in_data_uplink1 connects internal switch to module with ASA/FTD
in_mgmt_uplink1 connects chassis mgmt interface to ASA/FTD

Secure Firewall 3100 Troubleshooting

Internal Switch Packet Capture Configuration

Ingress interface > EtherType > Match conditions > Other parameters > Enable

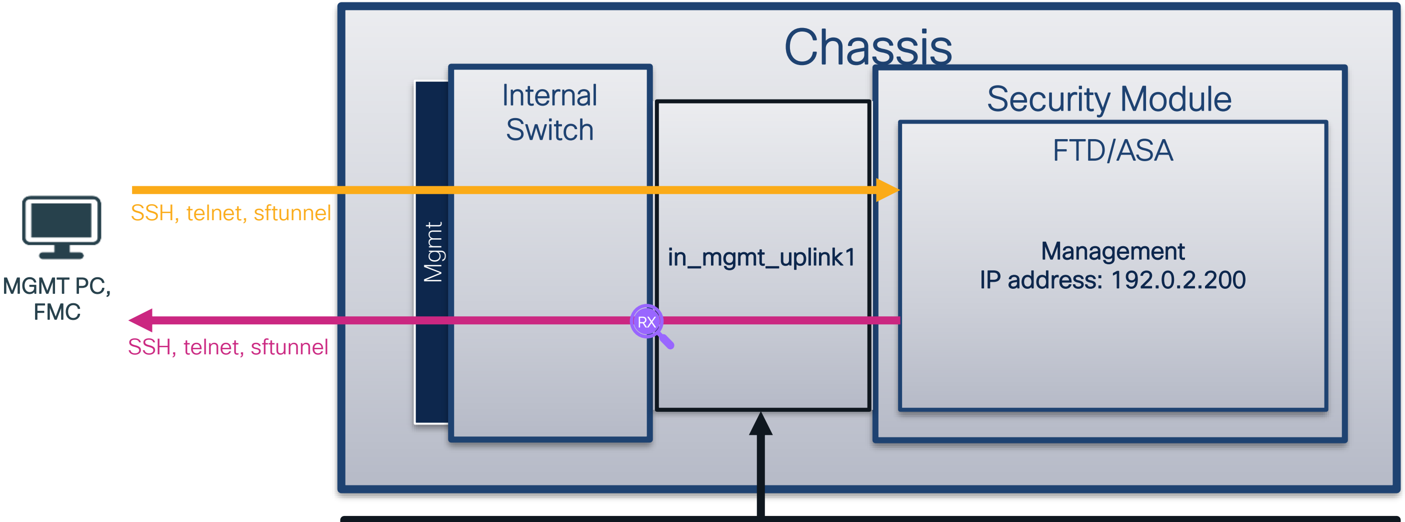


in_data_uplink1 connects internal switch to module with ASA/FTD

Secure Firewall 3100 Troubleshooting

Internal Switch Packet Capture Configuration

Ingress interface > EtherType > Match conditions > Other parameters > Enable



in_mgmt_uplink1 connects chassis mgmt interface to ASA/FTD

Secure Firewall 3100 Troubleshooting

Internal Switch Packet Capture File Collection

Use the **copy** command in diagnostic CLI to upload switch packet capture files:

```
> system support diagnostic-cli
Attaching to Diagnostic CLI ... Click 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.

firepower> enable
Password: <-- Enter
firepower#

firepower# copy flash:/packet-capture/sess-1-capsw-ethernet-1-1-0.pcap tftp://198.51.100.10/
Source filename [/packet-capture/sess-1-capsw-ethernet-1-1-0.pcap]?
Destination filename [sess-1-capsw-ethernet-1-1-0.pcap]?
Copy in progress...C
139826 bytes copied in 0.532 secs
```

Secure Firewall 3100 Troubleshooting

Internal Switch Packet Capture File Collection

Steps to collect switch capture files from FMC:

1. Use the **capture <name> switch stop** to stop the capture on CLI.
2. Go to **expert** mode and copy capture file to **/ngfw/var/common**:

```
> expert
admin@firepower:~$ sudo cp /mnt/disk0/packet-capture/sess-1-capsw-ethernet-1-1-0.pcap /ngfw/var/common/
Password:
admin@firepower:~$ ls -l /ngfw/var/common/sess*
-rwxr-xr-x 1 root admin 139826 Aug  7 20:14 /ngfw/var/common/sess-1-capsw-ethernet-1-1-0.pcap
```

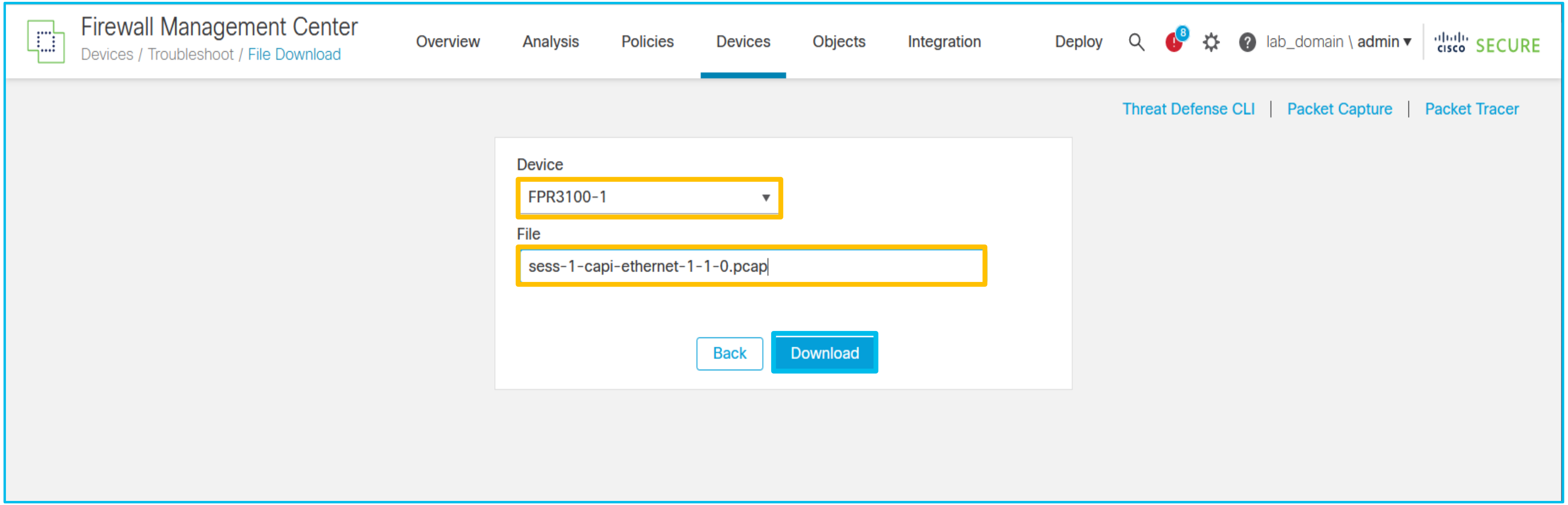
3. On FMC, navigate to **Devices > File Download.**

Secure Firewall 3100 Troubleshooting

Internal Switch Capture File Collection

Steps to collect switch capture files from FMC:

4. Choose FTD, provide filename and press **Download**:



Firewall Management Center
Devices / Troubleshoot / File Download
Overview
Analysis
Policies
Devices
Objects
Integration
Deploy
lab_domain \ admin
SECURE
Threat Defense CLI | Packet Capture | Packet Tracer
Back
Download

Device: FPR3100-1

File: sess-1-capi-ethernet-1-1-0.pcap

Secure Firewall 3100 Troubleshooting

System Support Trace (Snort)

```
> system support trace

Please specify an IP protocol: tcp
Please specify a client IP address: 192.168.1.40
Please specify a client port:
Please specify a server IP address: 192.168.2.40
Please specify a server port:
Enable firewall-engine-debug too? [n]: y

192.168.2.40-80 - 192.168.1.40-32791 6 Packet: TCP, ACK, seq 2620409314, ack 3700371681
192.168.1.40-32791 > 192.168.2.40-80 6 AS 1 I 0 Starting with minimum 2, 'Rule1', and SrcZone first
 with zones -1 -> -1, geo 0(0) -> 0, vlan 0, inline sgt tag: untagged, ISE sgt id: 0, svc 676,
payload 0, client 686, misc 0, user 9999997, url http://192.168.2.40/128k.html, xff
192.168.1.40-32791 > 192.168.2.40-80 6 Firewall: starting rule matching, zone -1 -> -1, geo 0(0) ->
 0, vlan 0, sgt 65535, user 9999997, url http://192.168.2.40/128k.html
192.168.1.40-32791 > 192.168.2.40-80 6 AS 1 I 0 match rule order 2, 'Rule1', action Block
192.168.1.40-32791 > 192.168.2.40-80 6 AS 1 I 0 deny action
192.168.1.40-32791 > 192.168.2.40-80 6 Firewall: block rule, 'Rule1', drop
192.168.1.40-32791 > 192.168.2.40-80 6 Snort: processed decoder alerts or actions queue, drop
192.168.1.40-32791 > 192.168.2.40-80 6 AS 1 I 0 Deleting session
192.168.1.40-32791 > 192.168.2.40-80 6 NAP id 1, IPS id 0, Verdict BLOCKLIST
192.168.1.40-32791 > 192.168.2.40-80 6 ===> Blocked by Firewall
```

Leave a field blank for "any"

Match rule and action

Snort verdict sent to DAQ/PDTS

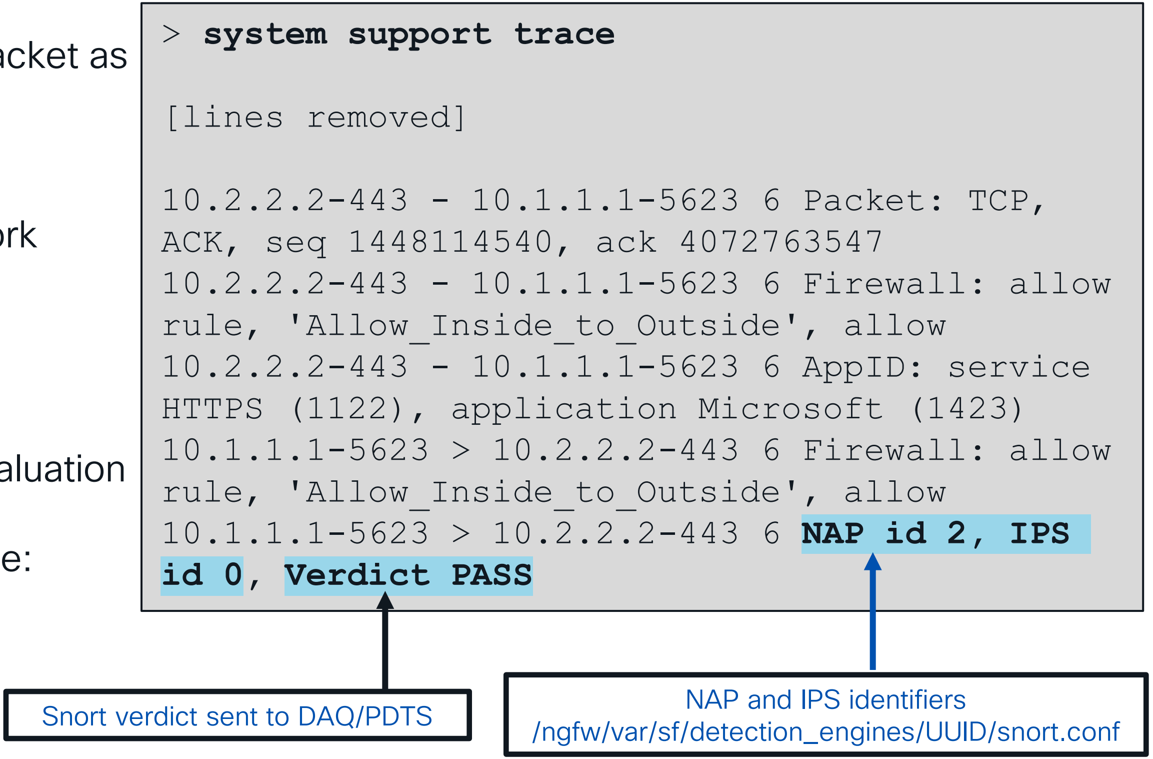
System Support Trace (Snort)

> system support trace

- Shows the Snort verdict for each packet as it is sent to DAQ and seen in LINA.
- Recommended to optionally enable firewall-engine-debug in parallel.
- Shows preprocessor impact (Network Analysis Policy).

>firewall engine debug

- Shows Snort access control rule evaluation
- Indicates which rule a flow matches
- Debug is written to messages log file:
  grep -i ngfw/var/log/messages



```
> system support trace

[lines removed]

10.2.2.2-443 - 10.1.1.1-5623 6 Packet: TCP,
ACK, seq 1448114540, ack 4072763547
10.2.2.2-443 - 10.1.1.1-5623 6 Firewall: allow
rule, 'Allow_Inside_to_Outside', allow
10.2.2.2-443 - 10.1.1.1-5623 6 AppID: service
HTTPS (1122), application Microsoft (1423)
10.1.1.1-5623 > 10.2.2.2-443 6 Firewall: allow
rule, 'Allow_Inside_to_Outside', allow
10.1.1.1-5623 > 10.2.2.2-443 6 NAP id 2, IPS
id 0, Verdict PASS
```

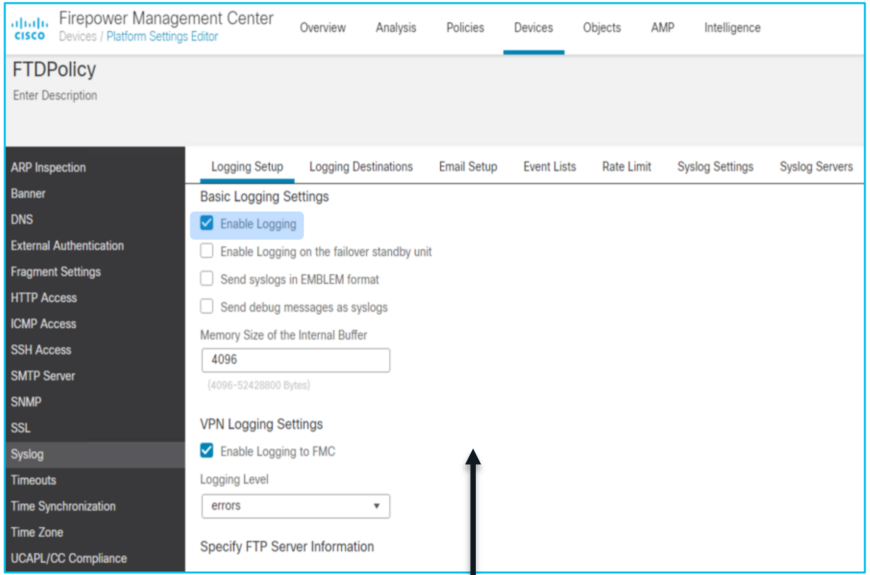
Snort verdict sent to DAQ/PDTS

NAP and IPS identifiers
/ngfw/var/sf/detection_engines/UUID/snort.conf

Syslogs

- Record connections to and through the firewall
- Syslogs that can be generated from Lina:
  - Health of Lina’s resources and processes.
  - Performance: Lina CPU, memory, block depletion.
  - Failover events.
  - Connections builds/teardowns and NAT translation.

- On Snort, Connection/Unified Events can as well be sent as syslogs.



FTDPolicy

Enter Description

Basic Logging Settings

☑ Enable Logging

□ Enable Logging on the failover standby unit

□ Send syslogs in EMBLEM format

□ Send debug messages as syslogs

Memory Size of the Internal Buffer

4096

(4096-52428800 Bytes)

VPN Logging Settings

☑ Enable Logging to FMC

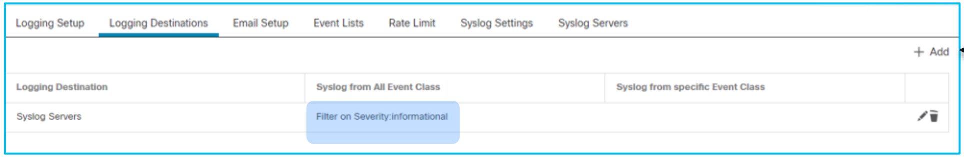
Logging Level

errors

Specify FTP Server Information

Syslogs are configure from the FTD Platform settings

Syslog's Configuration

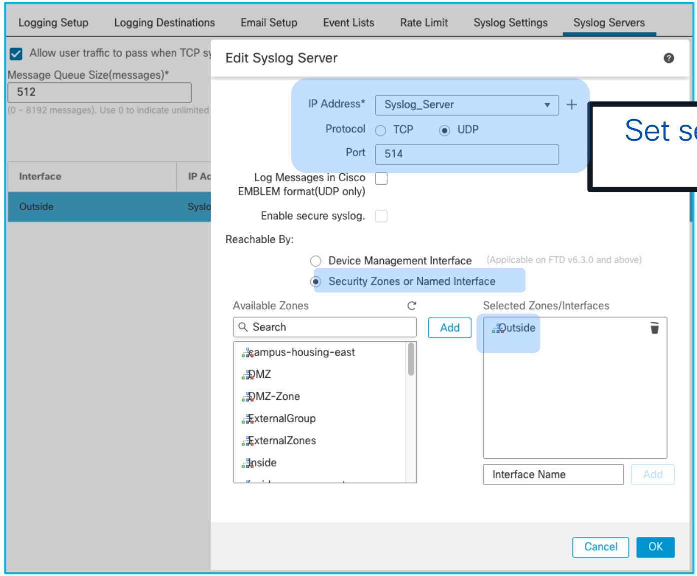


Logging Setup | Logging Destinations | Email Setup | Event Lists | Rate Limit | Syslog Settings | Syslog Servers

＋ Add

Logging Destination	Syslog from All Event Class	Syslog from specific Event Class
Syslog Servers	Filter on Severity:informational	

Syslog Server as logging destination



Logging Setup | Logging Destinations | Email Setup | Event Lists | Rate Limit | Syslog Settings | Syslog Servers

☑ Allow user traffic to pass when TCP sy

Message Queue Size(messages)*: 512

(0 - 8192 messages). Use 0 to indicate unlimited

Interface	IP Ac
Outside	Syslo

Edit Syslog Server

IP Address*: Syslog_Server

Protocol: ○ TCP ● UDP

Port: 514

Log Messages in Cisco EMBLEM format(UDP only): □

Enable secure syslog.: □

Reachable By:

○ Device Management Interface (Applicable on FTD v6.3.0 and above)

● Security Zones or Named Interface

Available Zones: campus-housing-east, DMZ, DMZ-Zone, ExternalGroup, ExternalZones, Inside

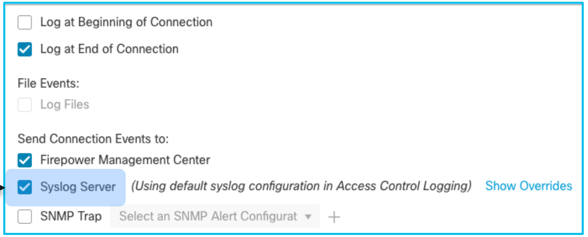
Selected Zones/Interfaces: Outside

Set server IP, port and interface

```
firepower# show run logging
logging enable
logging trap informational
logging host outside 10.1.0.1
```

Verify configuration from Lina

Set connection events to be sent to the syslog server from Access Control Policy logging



□ Log at Beginning of Connection

☑ Log at End of Connection

File Events:

□ Log Files

Send Connection Events to:

☑ Firepower Management Center

☑ Syslog Server *(Using default syslog configuration in Access Control Logging)* Show Overrides

□ SNMP Trap Select an SNMP Alert Configurat

How do Syslogs Look Like?

Connection Events Syslogs

```
May 24 21:30:17 FPR4100 SFIMS: Protocol: TCP, SrcIP: 10.1.1.20, OriginalClientIP: ::, DstIP:
172.18.124.145, SrcPort: 50072, DstPort: 21, TCPFlags: 0x0, DE: Primary Detection Engine (51a7d9fa-2943-
11e7-80c4-bd73daa17015), Policy: 4120_Access_Policy, ConnectType: Start, AccessControlRuleName:
Allow_Hosts, AccessControlRuleAction: Allow, UserName: No Authentication Required, InitiatorPackets: 2,
ResponderPackets: 1, InitiatorBytes: 148, ResponderBytes: 78, DNSResponseType: No Error, Sinkhole: Unknown,
URLCategory: Unknown, URLReputation: Risk unknown
```

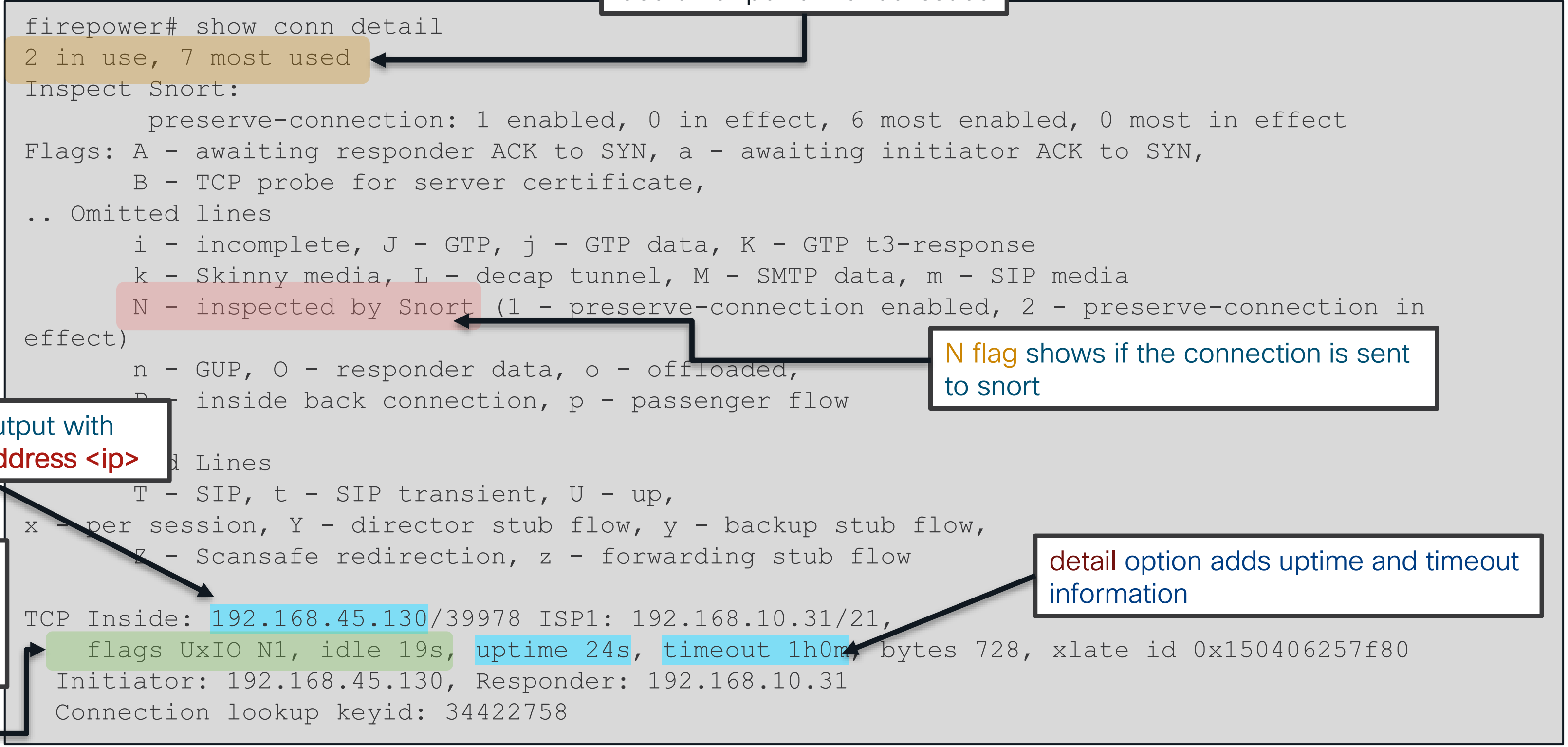
Lina Syslogs

```
%FTD-6-302013: Built inbound TCP connection 14704 for inside:10.1.1.20/50072 (10.2.104.80/50072) to
outside:172.18.124.145/21 (172.18.124.145/21)
```

Show Commands

Connection Table

Make sure to use "`terminal pager 24`"



```
firepower# show conn detail
2 in use, 7 most used
Inspect Snort:
        preserve-connection: 1 enabled, 0 in effect, 6 most enabled, 0 most in effect
Flags: A - awaiting responder ACK to SYN, a - awaiting initiator ACK to SYN,
       B - TCP probe for server certificate,
.. Omitted lines
       i - incomplete, J - GTP, j - GTP data, K - GTP t3-response
       k - Skinny media, L - decap tunnel, M - SMTP data, m - SIP media
       N - inspected by Snort (1 - preserve-connection enabled, 2 - preserve-connection in
effect)
       n - GUP, O - responder data, o - offloaded,
       P - inside back connection, p - passenger flow

          d Lines
       T - SIP, t - SIP transient, U - up,
x - per session, Y - director stub flow, y - backup stub flow,
       Z - Scansafe redirection, z - forwarding stub flow

TCP Inside: 192.168.45.130/39978 ISP1: 192.168.10.31/21,
  flags UxIO N1, idle 19s, uptime 24s, timeout 1h0m, bytes 728, xlate id 0x150406257f80
  Initiator: 192.168.45.130, Responder: 192.168.10.31
  Connection lookup keyid: 34422758
```

Connection count
Useful for performance issues

N flag shows if the connection is sent to snort

Filter the output with
show conn address <ip>

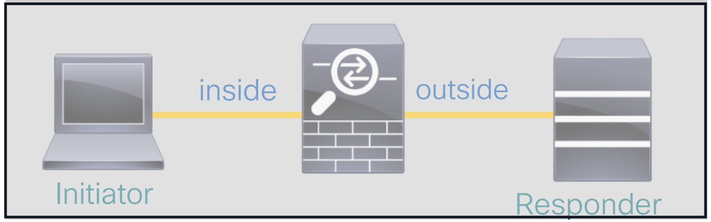
Conn flags indicate the connection state

detail option adds uptime and timeout information

TCP Connection Flags in FTD

TCP Connection

TCP Flags		Conn Flags
SYN	→	aA N1
SYN+ACK	←	a N1
ACK	→	U N1
Initiator data	←	UI N1
Responder data	→	UIO N1
FIN	→	UFIO N1
FIN+ACK	←	UfFRIO N1
ACK	→	~~UfFRrIO~~



a	Awaitting initiator ACK to SYN
A	Awaitting responder ACK to SYN
U	Up – 3way Handshake complete
I	Received Initiator Data
O	Received Responder Data
F	Received Initiator FIN
f	Received Responder FIN
R	Received Initiator ACK to FIN
N1	Inspected by Snort

Show Commands

Accelerated Security Path (ASP)

- Packets and flows dropped in the ASP will increment a counter
- See command reference under **show asp drop** for full list of counters
- Clear the counters using **clear asp drop**

```
> show asp drop

Frame drop:
   Invalid encapsulation (invalid-encap)                     10897
   Invalid tcp length (invalid-tcp-hdr-length)                9382
   Invalid udp length (invalid-udp-length)                      10
   No valid adjacency (no-adjacency)                          5594
   No route to host (no-route)                                1009
   Reverse-path verify failed (rpf-violated)                    15
   Flow is denied by access rule (acl-drop)               25247101
   First TCP packet not SYN (tcp-not-syn)                    36888
   Bad TCP Checksum (bad-tcp-cksum)                            893

…
```

Troubleshooting Tip

!

Clear ASP drop

Show asp drop

(before and after the issue happen)

Show Commands

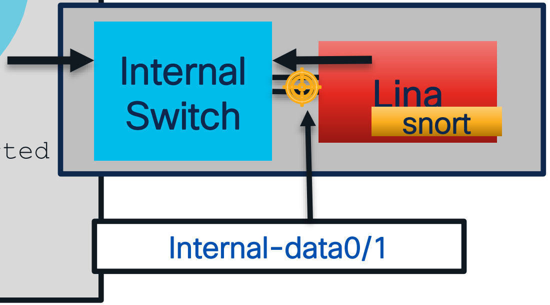
Interface Counters (show interface)

- Useful to spot traffic bursts, overruns, and other errors.
- Can be cleared using clear interface

Oversubscription may result in packet drops at the RX ring level before reaching the data plane.

The no buffer counter under Internal-Data0/1 interface may increase → In this case, packets will not be captured at the Lina level.

```
> show interface detail
Interface Internal-Data0/1 "", is up, line protocol is up
  Hardware is , BW 25000 Mbps, DLY 10 usec
        (Full-duplex), (25000 Mbps)
        Input flow control is unsupported, output flow control is unsupported
        MAC address 0000.0041.0004, MTU not set
        IP address unassigned
        17400454 packets input, 10426020714 bytes, 4736 no buffer
```



Show Commands

```
> show snort statistics

Packet Counters:
  Passed Packets                                62501
  Blocked Packets                               2339
  Injected Packets                              5739
  Packets bypassed (Snort Down)                 5678
  Packets bypassed (Snort Busy)                 0
```

Snort related Stats

Xlate Table displays information about NAT translations through FTD

Output can be filtered to **local** or **global IP**

Depleted NAT/PAT pools may cause connectivity issues

```
firepower# show xlate local 10.2.1.2
5014 in use, 5772 most used
TCP PAT from inside:192.168.103.220/57762 to outside:10.2.1.2/43756 flags ri
idle 0:00:00 timeout 0:00:30
```

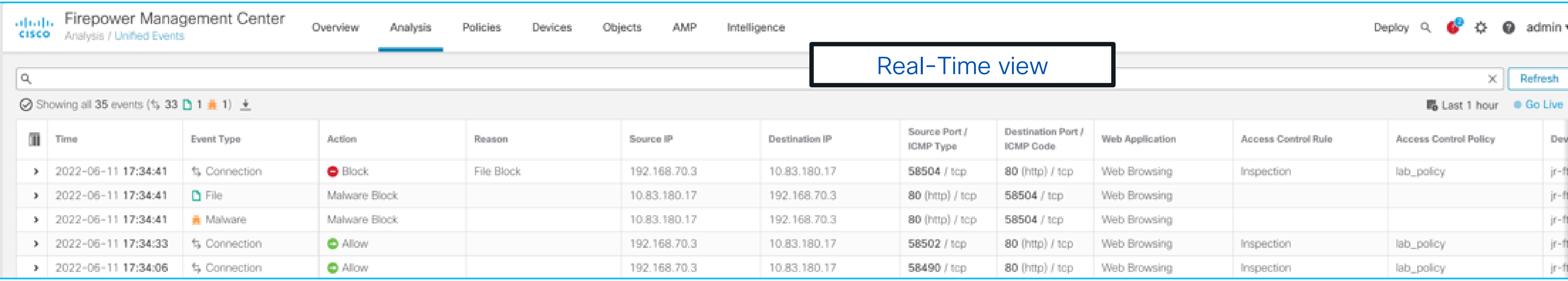
```
firepower# show nat pool
…
TCP PAT pool outside, address 10.2.1.2, range 1024-65535, allocated 64102
```

Events

Connection events can be exported into reports (PDF, Excel) → Useful for sending to TAC.

- Unified event viewer is added starting from version 7.x

View and work with multiple event types (connection, intrusion, file, malware, and some security intelligence events) in a single table.

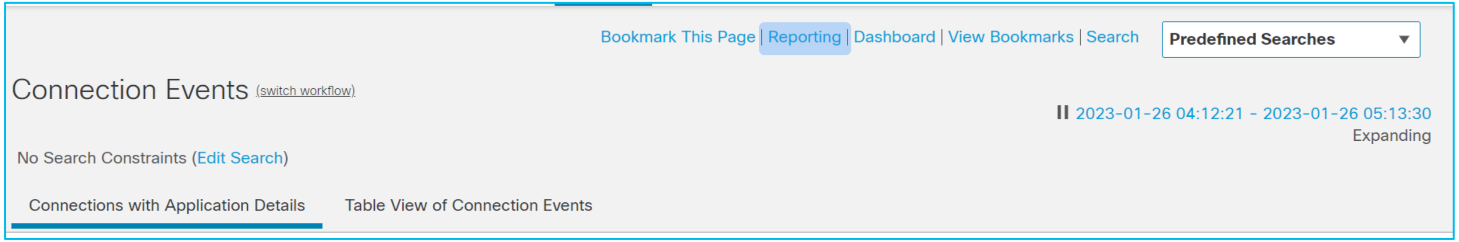


Real-Time view

Showing all 35 events (33 1 1)

	Time	Event Type	Action	Reason	Source IP	Destination IP	Source Port / ICMP Type	Destination Port / ICMP Code	Web Application	Access Control Rule	Access Control Policy	Dev
›	2022-06-11 17:34:41	Connection	Block	File Block	192.168.70.3	10.83.180.17	58504 / tcp	80 (http) / tcp	Web Browsing	Inspection	lab_policy	jr-f
›	2022-06-11 17:34:41	File	Malware Block		10.83.180.17	192.168.70.3	80 (http) / tcp	58504 / tcp	Web Browsing			jr-f
›	2022-06-11 17:34:41	Malware	Malware Block		10.83.180.17	192.168.70.3	80 (http) / tcp	58504 / tcp	Web Browsing			jr-f
›	2022-06-11 17:34:33	Connection	Allow		192.168.70.3	10.83.180.17	58502 / tcp	80 (http) / tcp	Web Browsing	Inspection	lab_policy	jr-f
›	2022-06-11 17:34:06	Connection	Allow		192.168.70.3	10.83.180.17	58490 / tcp	80 (http) / tcp	Web Browsing	Inspection	lab_policy	jr-f

Connection Events – Report Generation

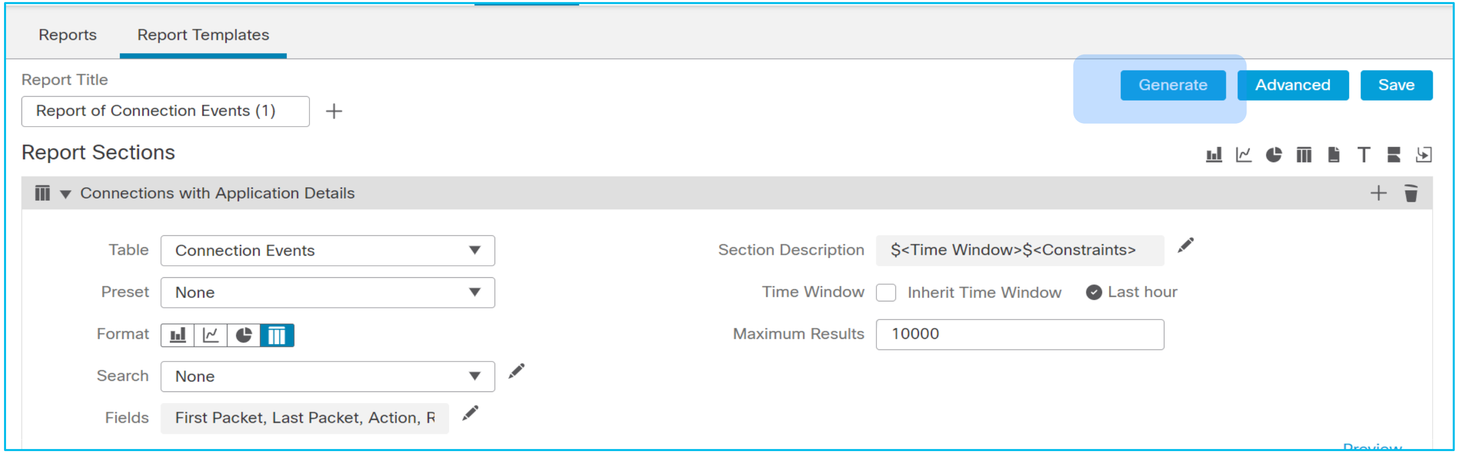

Bookmark This Page | Reporting | Dashboard | View Bookmarks | Search
Predefined Searches ▼

Connection Events (switch workflow)

❚❚ 2023-01-26 04:12:21 - 2023-01-26 05:13:30
Expanding

No Search Constraints (Edit Search)

Connections with Application Details
Table View of Connection Events



Report Title: Report of Connection Events (1)

Table: Connection Events ▼

Preset: None ▼

Format

Search: None ▼

Fields: First Packet, Last Packet, Action, R

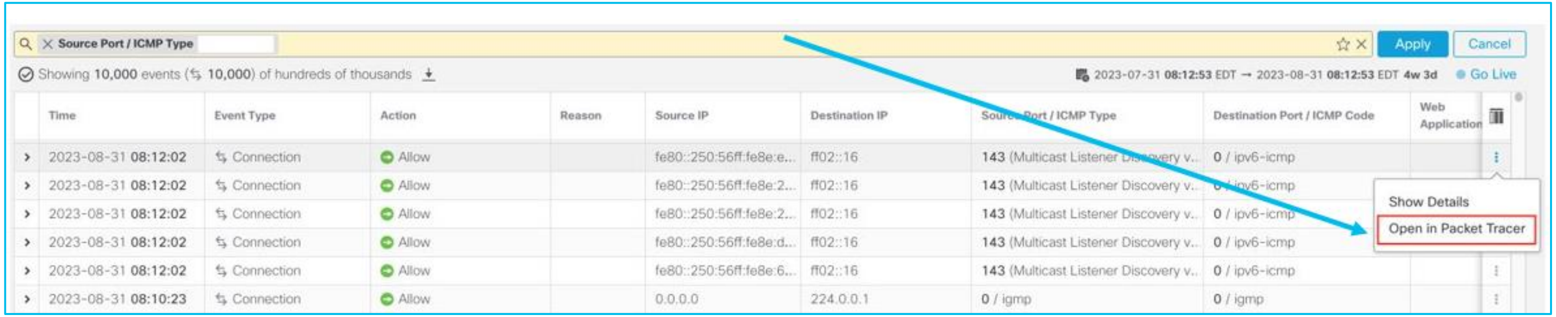
Section Description: $<Time Window>$<Constraints>

Time Window: □ Inherit Time Window ● Last hour

Maximum Results: 10000

7.4.1 Event Data in Packet Tracer

Loads connection details into Packet Tracer to simplify capture sessions

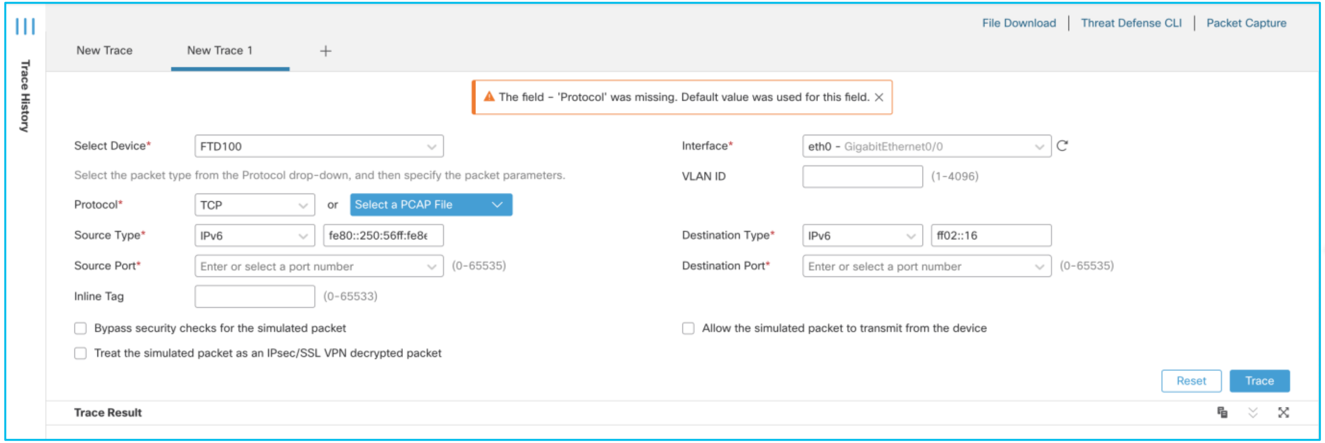


Source Port / ICMP Type

Showing 10,000 events (⇆ 10,000) of hundreds of thousands

2023-07-31 08:12:53 EDT → 2023-08-31 08:12:53 EDT 4w 3d

	Time	Event Type	Action	Reason	Source IP	Destination IP	Source Port / ICMP Type	Destination Port / ICMP Code	Web Application
›	2023-08-31 08:12:02	⇆ Connection	Allow		fe80::250:56ff:fe8e:e...	ff02::16	143 (Multicast Listener Discovery v...	0 / ipv6-icmp	
›	2023-08-31 08:12:02	⇆ Connection	Allow		fe80::250:56ff:fe8e:2...	ff02::16	143 (Multicast Listener Discovery v...	0 / ipv6-icmp	
›	2023-08-31 08:12:02	⇆ Connection	Allow		fe80::250:56ff:fe8e:2...	ff02::16	143 (Multicast Listener Discovery v...	0 / ipv6-icmp	
›	2023-08-31 08:12:02	⇆ Connection	Allow		fe80::250:56ff:fe8e:d...	ff02::16	143 (Multicast Listener Discovery v...	0 / ipv6-icmp	
›	2023-08-31 08:12:02	⇆ Connection	Allow		fe80::250:56ff:fe8e:6...	ff02::16	143 (Multicast Listener Discovery v...	0 / ipv6-icmp	
›	2023-08-31 08:10:23	⇆ Connection	Allow		0.0.0.0	224.0.0.1	0 / igmp	0 / igmp	



⚠ The field – 'Protocol' was missing. Default value was used for this field. ✕

Select Device*: FTD100

Interface*: eth0 – GigabitEthernet0/0

Select the packet type from the Protocol drop-down, and then specify the packet parameters.

VLAN ID: (1-4096)

Protocol*: TCP or Select a PCAP File

Source Type*: IPv6 fe80::250:56ff:fe8e

Destination Type*: IPv6 ff02::16

Source Port*: Enter or select a port number (0-65535)

Destination Port*: Enter or select a port number (0-65535)

Inline Tag: (0-65533)

☐ Bypass security checks for the simulated packet

☐ Allow the simulated packet to transmit from the device

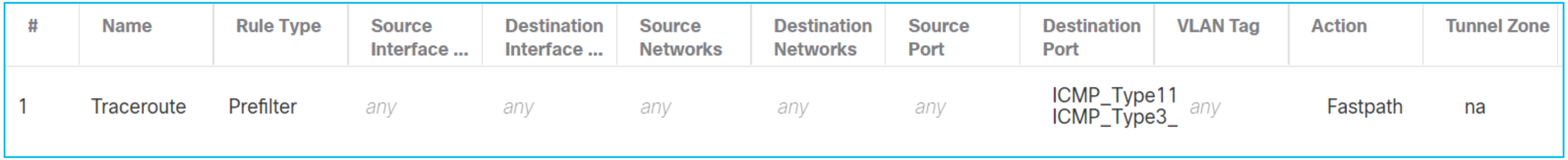
☐ Treat the simulated packet as an IPsec/SSL VPN decrypted packet

The data in the input fields is populated with data provided by the event in the Unified Event Viewer.

How to isolate if firewall is causing the issue?

- How to isolate if the issue is caused by snort?

Use prefilter policy with Fastpath action → If traffic is prefiltered and the issue is still happening, then the issue is not related to the snort side.

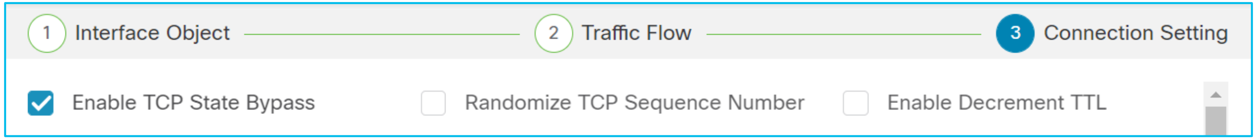


#	Name	Rule Type	Source Interface ...	Destination Interface ...	Source Networks	Destination Networks	Source Port	Destination Port	VLAN Tag	Action	Tunnel Zone
1	Traceroute	Prefilter	*any*	*any*	*any*	*any*	*any*	ICMP_Type11 ICMP_Type3_	*any*	Fastpath	na

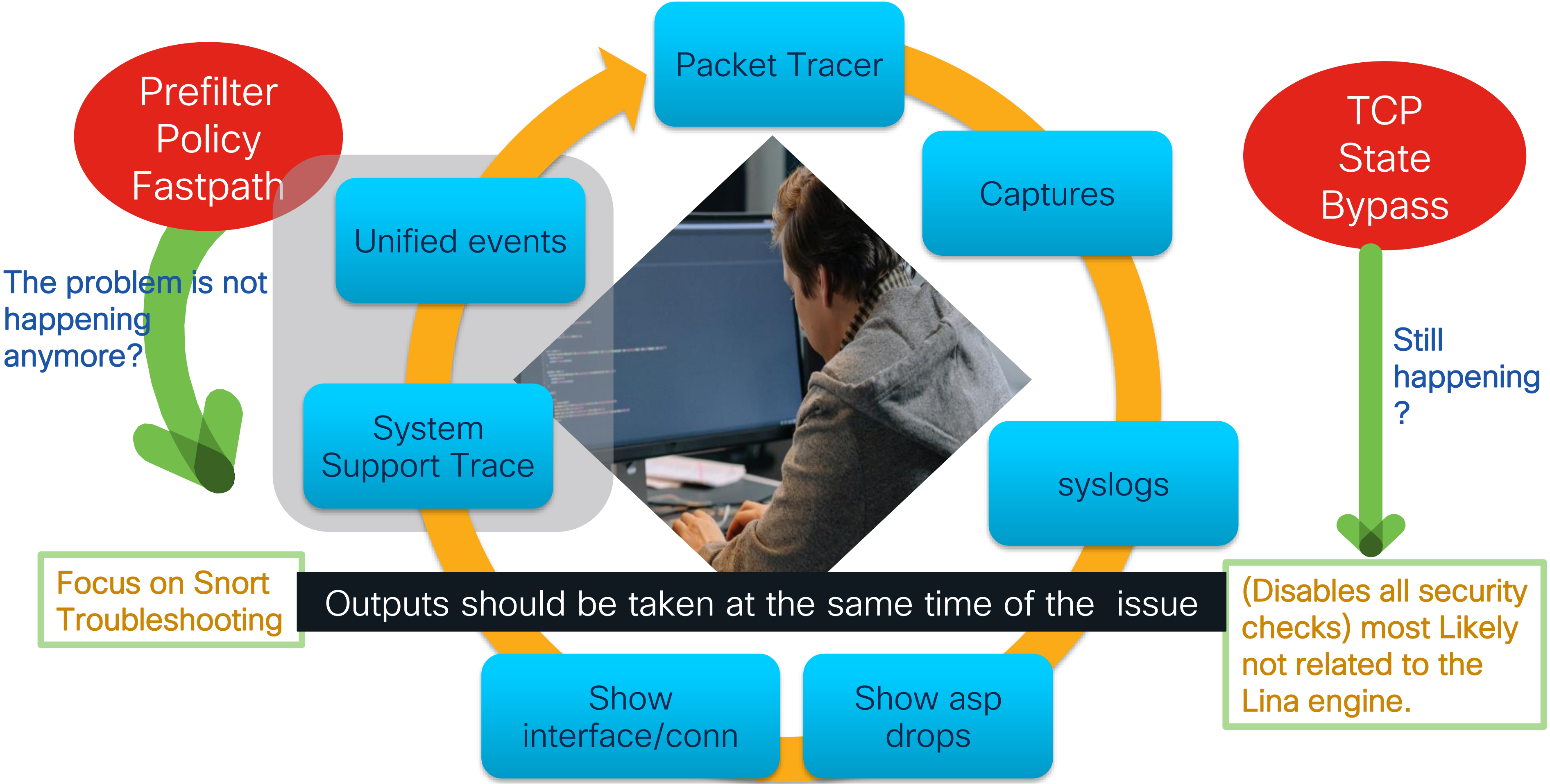
- How to bypass security checks on Lina?

TCP state bypass → Connections are not inspected by any inspection engines, and they bypass all TCP state checking and TCP normalization (use with caution).

Policies > Access Control > Access Control > edit the access control policy > Advanced > Threat Defense Service Policy.



☑ Enable TCP State Bypass □ Randomize TCP Sequence Number □ Enable Decrement TTL



Prefilter Policy Fastpath

The problem is not happening anymore?

Focus on Snort Troubleshooting

Packet Tracer

Captures

syslogs

Show asp drops

Show interface/conn

System Support Trace

Unified events

Outputs should be taken at the same time of the issue

TCP State Bypass

Still happening ?

(Disables all security checks) most Likely not related to the Lina engine.

~~Datapath~~
You are here
Upgrade
Performance
Use Case
SECURELAND CITY

Upgrade

Upgrade Failure

General Troubleshooting

- File copied to FTD?

```
admin@firepower:/ngfw/var/sf/updates$ ls -ls
total 1083648
1083644 -rw-r--r-- 1 www  www  1109647360 Sep 30 22:06 Cisco_FTD_Upgrade-7.1.0-90.sh.REL.tar
```

- Upgrade running?

```
admin@firepower:/ngfw/var/sf/updates$ ps aux | grep install
root      25389  0.0  0.2  88976 70908 ?        S    22:23   0:00 /usr/bin/perl /usr/local/sf/bin/install_update.pl
/var/sf/updates/Cisco_FTD_Upgrade-7.1.0-90.sh.REL.tar --detach --auto_upgrade_cancel true
admin     29100  0.0  0.0   2796   784 pts/0    S+   22:25   0:00 grep install
```

- Check Upgrade log folder and related upgrade logs files:

```
admin@firepower:/ngfw/var/log/sf$ ls -ls
total 488
  4 drwxr-xr-x 4 root root   4096 Sep 30 22:25
Cisco_FTD_Upgrade-7.1.0
```

Monitor the upgrade process:

/ngfw/var/log/sf/update.status
/ngfw/var/log/sf/Cisco_FTD_Upgrade-x.x.x/upgrade_status.log
/ngfw/var/log/sf/Cisco_FTD_Upgrade-x.x.x/status.log
/ngfw/var/log/sf/Cisco_FTD_Upgrade-x.x.x/main_upgrade_script.log

Troubleshoot Firewall Upgrade Issues

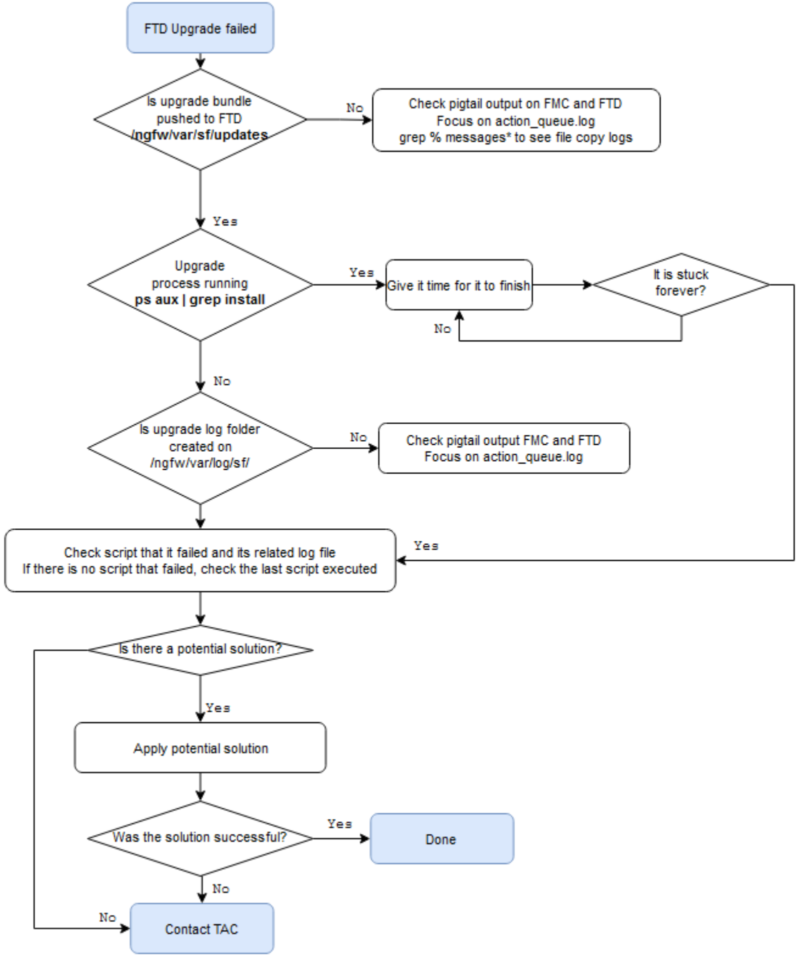
Notes About Upgrade log Files

File	Notes
/ngfw/var/log/sf/update.status	• It has timestamps • The file is automatically deleted once the upgrade is done
upgrade_status.log	• It has timestamps • It has percentages
status.log	• It has percentages • It mentions time to reboot
main_upgrade_script.log	• Each script begin/end timestamps

Upgrade Failure

General Troubleshooting

For your reference



FTD Upgrade failed
Is upgrade bundle pushed to FTD /ngfw/var/sf/updates
No
Check pigtail output on FMC and FTD
Focus on action_queue.log
grep % messages* to see file copy logs
Yes
Upgrade process running
ps aux | grep install
Yes
Give it time for it to finish
It is stuck forever?
No
No
Is upgrade log folder created on /ngfw/var/log/sf/
No
Check pigtail output FMC and FTD
Focus on action_queue.log
Yes
Check script that it failed and its related log file
If there is no script that failed, check the last script executed
Is there a potential solution?
Yes
Apply potential solution
Was the solution successful?
Yes
Done
No
No
Contact TAC

Troubleshoot Firewall Upgrade Issues

Common Failure Reasons

1. Pending deploy/changes.
2. Pending registration to FMC.
3. Not enough space in disk.
4. HA issues.

Troubleshooting Steps

- Symptoms

From status.log file:

```
ui:[15%] Running script 200_pre/006_check_snort.sh...
ui:[15%] Fatal error: Error running script
200_pre/006_check_snort.sh
```

Inside 006_check_snort.sh :

```
Entering 200_pre/006_check_snort.sh...
Snort build is too old.
Please apply AC Policy from FMC before attempting upgrade.
```

- Solution

Deploy pending policy

Troubleshoot Firewall Upgrade Issues

Common Failure Reasons

1. Pending deploy/changes.
2. **Pending registration to FMC.**
3. Not enough space in disk.
4. HA issues.

Troubleshooting Steps

- Symptoms

From /ngfw/var/log/action_queue.log file:

```
Jan 28 09:46:24 firepower
ActionQueueScrape.pl[5423]: Update Unable to
Execute : Peer registration in progress.
Please retry in a few moments.
```

- Solution

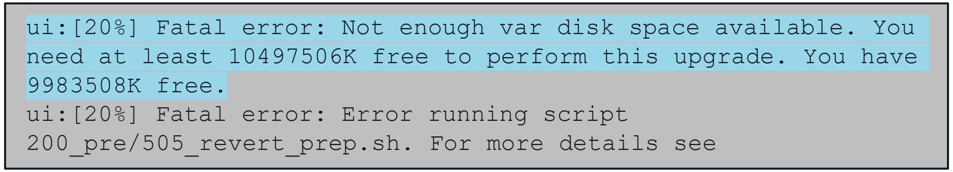
Solve registration issues before trying the upgrade again.

Troubleshoot Firewall Upgrade Issues

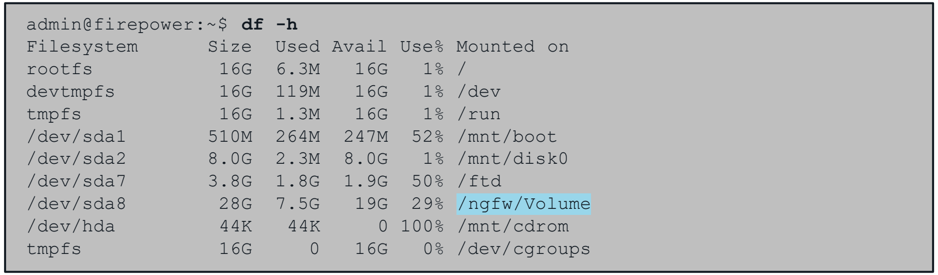
Common Failure Reasons

1. Pending deploy/changes.
2. Pending registration to FMC.
3. Not enough space in disk.
4. HA is

old backup files, update files, patch files, troubleshoot and core files under /ngfw/var/common/. And /ngfw/var/sf/



```
ui:[20%] Fatal error: Not enough var disk space available. You
need at least 10497506K free to perform this upgrade. You have
9983508K free.
ui:[20%] Fatal error: Error running script
200_pre/505_revert_prep.sh. For more details see
```



```
admin@firepower:~$ df -h
Filesystem        Size  Used Avail  Use% Mounted on
rootfs             16G  6.3M   16G    1% /
devtmpfs           16G  119M   16G    1% /dev
tmpfs              16G  1.3M   16G    1% /run
/dev/sda1         510M  264M  247M   52% /mnt/boot
/dev/sda2         8.0G  2.3M  8.0G    1% /mnt/disk0
/dev/sda7         3.8G  1.8G  1.9G   50% /ftd
/dev/sda8          28G  7.5G   19G   29% /ngfw/Volume
/dev/hda           44K   44K     0  100% /mnt/cdrom
tmpfs              16G     0   16G    0% /dev/cgroups
```

- **Useful commands:**

`show disk-manager` → CLISH Mode

`df -h` > Expert mode

`find /ngfw -type f -exec du -Sh {} + | sort -rh | head -n 15` → Expert Mode

- **Solution:**

Remove old and unnecessary files

! Note: Be very careful when removing files/folders on Secure Firewall.

Troubleshoot Firewall Upgrade Issues

Common Failure Reasons

1. Pending deploy/changes.
2. Pending registration to FMC.
3. Not enough space in disk.
4. HA issues

Troubleshooting Steps

- Symptoms

```
****** TIMESTAMP:Fri Mar  4 03:57:59 UTC 2022
PERCENT: 8%  MESSAGE:Fatal error: Failure to
enter maintenance mode: rc=2, error=:Peer device
is not in active failover-state. Upgrade cannot
continue, as it would result in traffic loss.
This happens if the peer device is not
reachable, or is in disabled or failed state….
```

- Commands to Troubleshoot:

➢ **`show failover`**

➢ **`show failover history`**

➢ **`show failover state`**

Troubleshoot Firewall Upgrade Issues

~~Datapath~~
~~Upgrade~~
Performance
You are here
Use Case
SECURELAND CITY

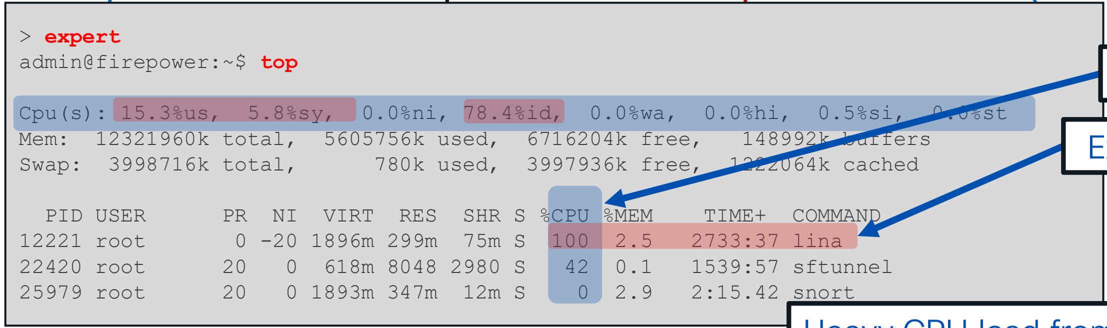
Performance

Alerts about High CPU do not necessarily indicate a problem unless there is also latency and/or packet loss

CPU Issues

Secure Firewall provides 2 levels of CPU usage:

- System Level: Expert Mode Top Command (> Show CPU system)



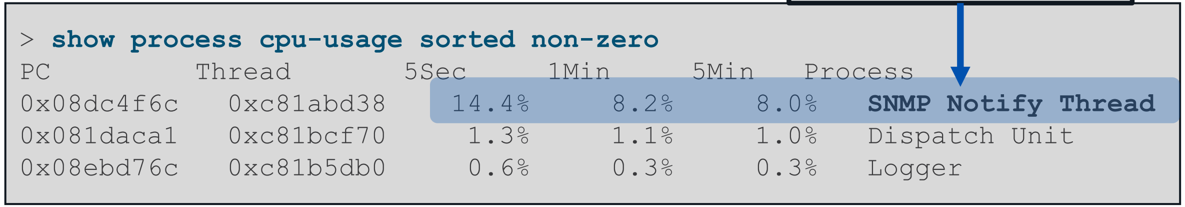
```
> expert
admin@firepower:~$ top

Cpu(s): 15.3%us,  5.8%sy,  0.0%ni, 78.4%id,  0.0%wa,  0.0%hi,  0.5%si,  0.0%st
Mem:  12321960k total,  5605756k used,  6716204k free,   148992k buffers
Swap:  3998716k total,      780k used,  3997936k free,  1222064k cached

  PID USER      PR  NI  VIRT  RES  SHR S %CPU %MEM    TIME+  COMMAND
12221 root       0 -20 1896m 299m  75m S  100  2.5  2733:37 lina
22420 root      20   0  618m 8048 2980 S   42  0.1  1539:57 sftunnel
25979 root      20   0 1893m 347m  12m S    0  2.9  2:15.42 snort
```

Usage per process

Expected! Disregard this

Heavy CPU load from SNMP traps.

- LINA engine level



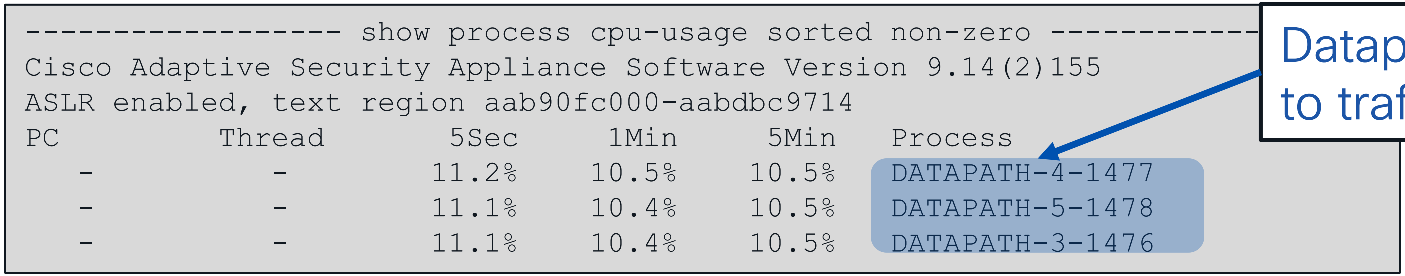
```
> show process cpu-usage sorted non-zero
PC          Thread          5Sec      1Min      5Min     Process
0x08dc4f6c  0xc81abd38     14.4%      8.2%      8.0%    SNMP Notify Thread
0x081daca1  0xc81bcf70      1.3%      1.1%      1.0%    Dispatch Unit
0x08ebd76c  0xc81b5db0      0.6%      0.3%      0.3%    Logger
```

Useful commands

```
Show cpu
Show process
Show perfmon
Show conn count
```

- Baseline average CPU usage. Monitor CPU usage based on that.
- For Oversubscription, Determine Packet size and calculate throughput.

High CPU Usage on Lina Possible Reasons



```
------------------ show process cpu-usage sorted non-zero ------------
Cisco Adaptive Security Appliance Software Version 9.14(2)155
ASLR enabled, text region aab90fc000-aabdbc9714
PC         Thread       5Sec     1Min     5Min   Process
   -          -        11.2%    10.5%    10.5%   DATAPATH-4-1477
   -          -        11.1%    10.4%    10.5%   DATAPATH-5-1478
   -          -        11.1%    10.4%    10.5%   DATAPATH-3-1476
```

Datapath is related to traffic

Show conn

Oversubscription

- Use “show traffic”
- Calculate Throughput
- Check for overruns and interface errors

Routing Loops

- “show traffic” and compare interface counters.
- Captures (Check MAC address)
- Syslogs

Other Causes

- Host with a high number of connections
- Excessive logging
- Captures left on the device at a high rate.
- Lina L7 inspection
- VPN Traffic Overload

Lina L7 inspections

- FTD has L7 inspections at LINA level for specific protocols like:
  - FTP, H323, RTSP, SQLNET, SIP, NETBIOS, etc.

- Misconfiguration of class-maps in service-policy can lead to more than usual traffic being inspected erroneously causing high CPU.

```
firepower# show service-policy

Global policy:
  Service-policy: global_policy
    Class-map: inspection_default
      Inspect: dns preset_dns_map, packet 0, lock fail 0, drop 0, reset-drop 0, 5-min-pkt-rate 0 pkts/sec, v6-fail-close 0 sctp-drop-override 0
      Inspect: ftp, packet 185775370, lock fail 4983, drop 87526, reset-drop 8375, 5-min-pkt-rate 24905 pkts/sec, v6-fail-close 0 sctp-drop-override 0
      Inspect: h323 h225 _default_h323_map, packet 0, lock fail 0, drop 0, reset-drop 0, 5-min-pkt-rate 0 pkts/sec, v6-fail-close 0 sctp-drop-override 0
               tcp-proxy: bytes in buffer 0, bytes dropped 0
      Inspect: h323 ras _default_h323_map, packet 0, lock fail 0, drop 0, reset-drop 0, 5-min-pkt-rate 0 pkts/sec, v6-fail-close 0 sctp-drop-override 0
      Inspect: rsh, packet 0, lock fail 0, drop 0, reset-drop 0, 5-min-pkt-rate 0 pkts/sec, v6-fail-close 0 sctp-drop-override 0
      Inspect: rtsp, packet 0, lock fail 0, drop 0, reset-drop 0, 5-min-pkt-rate 0 pkts/sec, v6-fail-close 0 sctp-drop-override 0
               tcp-proxy: bytes in buffer 0, bytes dropped 0
      Inspect: sqlnet, packet 0, lock fail 0, drop 0, reset-drop 0, 5-min-pkt-rate 0 pkts/sec, v6-fail-close 0 sctp-drop-override 0
      Inspect: skinny, packet 0, lock fail 0, drop 0, reset-drop 0, 5-min-pkt-rate 0 pkts/sec, v6-fail-close 0 sctp-drop-override 0
               tcp-proxy: bytes in buffer 0, bytes dropped 0
      Inspect: sunrpc, packet 0, lock fail 0, drop 0, reset-drop 0, 5-min-pkt-rate 0 pkts/sec, v6-fail-close 0 sctp-drop-override 0
               tcp-proxy: bytes in buffer 0, bytes dropped 0
      Inspect: sip , packet 0, lock fail 0, drop 0, reset-drop 0, 5-min-pkt-rate 0 pkts/sec, v6-fail-close 0 sctp-drop-override 0
               tcp-proxy: bytes in buffer 0, bytes dropped 0
      Inspect: icmp, packet 258863783, lock fail 0, drop 0, reset-drop 0, 5-min-pkt-rate 0 pkts/sec, v6-fail-close 0 sctp-drop-override 0
      Inspect: icmp error, packet 78, lock fail 0, drop 0, reset-drop 0, 5-min-pkt-rate 0 pkts/sec, v6-fail-close 0 sctp-drop-override 0
Class-map: class_snmp
      Inspect: snmp, packet 3336, lock fail 0, drop 0, reset-drop 0, 5-min-pkt-rate 0 pkts/sec, v6-fail-close 0 sctp-drop-override 0
    Class-map: class-default
```

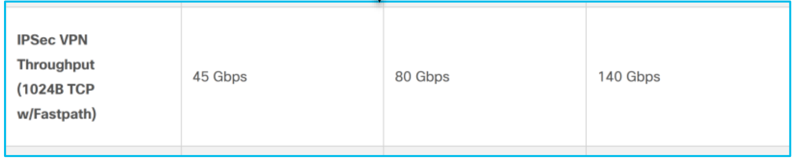
VPN Traffic Overload

- Check how many sessions and connections are related to VPN users.
- Use crypto accelerator statistics to calculate amount of VPN traffic.

```
firepower# show conn count

69125 in use, 72657 most used

firepower# sh conn | count 10.59.17
Number of lines which match regexp = 10975
firepower# sh conn | count 10.59.18
Number of lines which match regexp = 49691
firepower# sh conn | count 10.59.19
Number of lines which match regexp = 6976
```

Filter using the different Secure Client pools

Compare with the official Platform Datasheets on Cisco Website



IPSec VPN Throughput (1024B TCP w/Fastpath)	45 Gbps	80 Gbps	140 Gbps

```
firepower# show crypto accelerator statistics

Crypto Accelerator Status
-------------------------
[Capability]
   Supports hardware crypto: True
   Supports modular hardware crypto: False
   Max accelerators: 2
   Max crypto throughput: 1000 Mbps
   Max crypto connections: 5000
[Global Statistics]
   Number of active accelerators: 2
   Number of non-operational accelerators: 0
   Input packets: 257353
   Input bytes: 27173022
   Output packets: 2740
   Output error packets: 0
   Output bytes: 57793
[…]
```

(27173022 + 57793) x 8 =
217846520 ~ 217 Mbps
VPN traffic

High CPU Usage on Snort

Possible high CPU reasons

- Asymmetric Traffic
- Elephant flows
- SSL Decryption
- Connection logging
- Non-Default and poorly-written Snort rules

Suggestions

- Intelligent Application Bypass (IAB)

Note: For snort3, IAB is deprecated, use **Elephant Flow Settings**.

- Trusted Large (Elephant) flows can be bypassed
- Configuration tuning

Configuration Tuning.

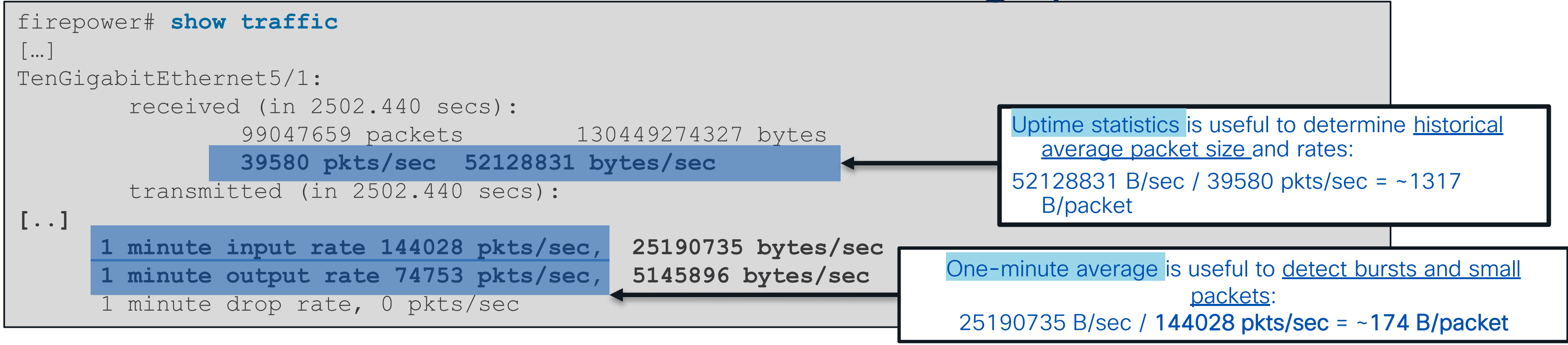
- Adjust policies, enable and disable features, measure how this affect CPU usage.
- Follow best practice regarding connection logging. For example, Make sure that Access Control Rules with "Allow" and "Trust" as the action only have logging enabled for the beginning OR end of connection, rather than beginning AND end.

- Note that logging at the end of the connection will contain more data than logging at the beginning. Logging the beginning of an allowed or trusted connection is typically only used for troubleshooting purposes.

- Avoid double inspection (inspecting the same traffic twice).

- An efficient ordering of the rules, such as placing block rules at the top of the access control policy.

Calculate Packet Size and Throughput



```
firepower# show traffic
[…]
TenGigabitEthernet5/1:
        received (in 2502.440 secs):
                99047659 packets         130449274327 bytes
                39580 pkts/sec   52128831 bytes/sec
        transmitted (in 2502.440 secs):
[..]
     1 minute input rate 144028 pkts/sec,  25190735 bytes/sec
     1 minute output rate 74753 pkts/sec,  5145896 bytes/sec
     1 minute drop rate, 0 pkts/sec
```

Uptime statistics is useful to determine historical average packet size and rates:
52128831 B/sec / 39580 pkts/sec = ~1317 B/packet

One-minute average is useful to detect bursts and small packets:
25190735 B/sec / **144028 pkts/sec** = ~**174 B/packet**

Throughput (Mbit/sec) = ((1 minute input [OR OUTPUT] int1 rate + same for int2 + ...etc) *8) / 1000000

Posted throughput ratings for the Firepower appliances in the Datasheets are usually rated at 1024 bytes **Smaller packets** results in **more processing**.

Asymmetric Traffic and SYN Flood

- Inside **/ngfw/var/sf/detection_engines/<UUID_of_Primary_DE>** directory

```
for i in `ls | grep instance-`; do echo $i; perfstats -q < $i/now | egrep
"Syns/Sec:|SynAcks/Sec:|New Sessions Cached/Sec:"; done;

 instance-1

                         Syns/Sec:      77216.4        210.0      99843.6

                      SynAcks/Sec:         32.3          1.7         99.1

             New Sessions Cached/Sec:      33.7          3.0         97.5
```

SYN /SYN ACK Ratio

# ratio is far from 1:1

- From **/ngfw/var/log/messages**

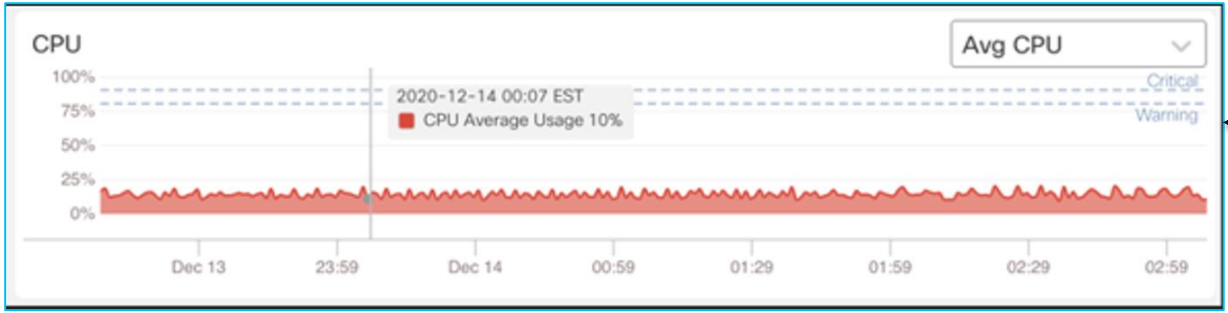
```
S5: Session exceeded configured max segs to queue xxxxx using xxxxx bytes
S5: Pruned session from cache that was using xxxxx bytes
```

Recommended Action:

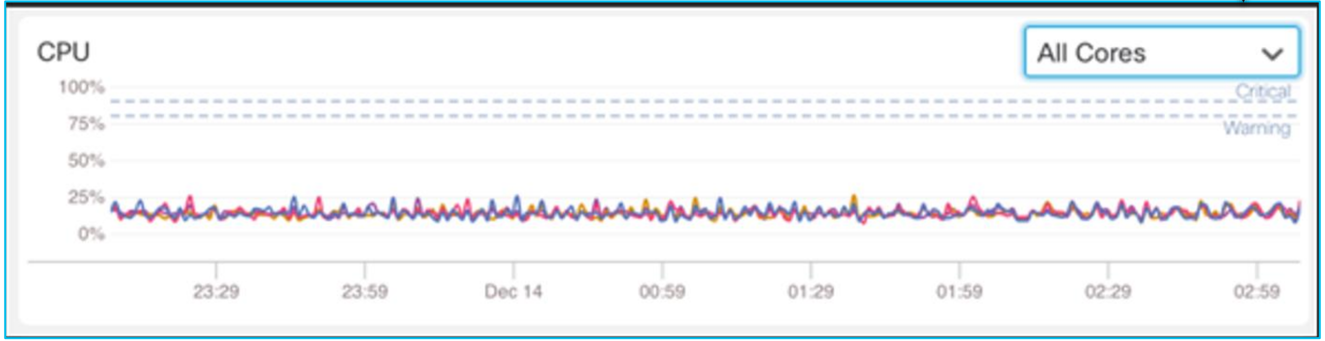
- Trust Asynchronous traffic
- Fix the network
- Enable Asynchronous Network in NAP*

*This is only to help with performance, but it will make inspection less secure because snort will not do any re-assembly on packets

CPU Monitoring – FMC Dashboard



CPU Panel shows: **Average CPU** **All Cores**



Elephant Flow Visibility

What is Elephant Flow ?

- Typically, traffic like database backups, database replication, etc.)

Why it could be a problem?

- Can overload a single SNORT instance

7.1 Release: Basic Detection Capabilities:

1. Identify elephant flows
2. Health monitoring dashboard provides correlation of CPU spikes with elephant flow
3. Easier to troubleshoot performance issues.

7.2 Release: Improved Detection and Remediation

1. Detection
   I. Per Flow CPU Utilization in a fixed time duration
   II. Percentage of packets dropped by Snort
2. Remediation
   I. Bypass inspection
   II. Throttle flows

Bypass and throttle not supported on Firepower 2100 series

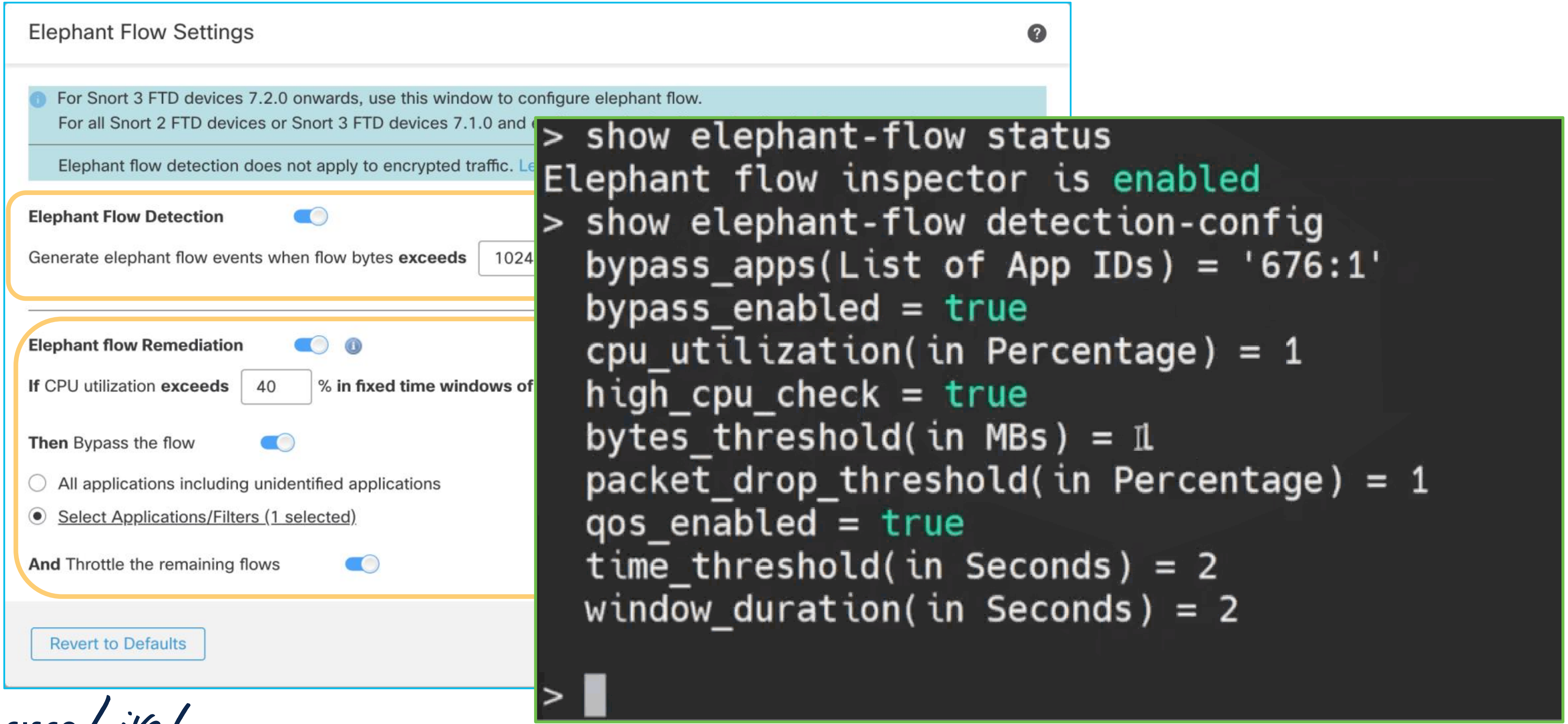
Elephant Flows Overview

- Supported with Snort 3 only
  - Configurable through FMC GUI and API
- Improve Detection Method added two new parameters to find elephant flows
  - Per Flow CPU Utilization in a fixed time duration
  - Percentage of packets dropped by Snort
- Remediation – act on detected elephant flows
- Bypass inspection – set flag to bypass flow from Snort
  - Throttle flow – apply rate-limit to the flow and continue inspecting
  - Snort sends Verdict (QoS flow with 10% less flow rate) to data plane

Bypass and throttle not supported on Firepower 2100 series

Secure Firewall CLI Commands (Secure Firewall Version 7.2)

Feature is configured in **ACP Advanced** tab in Elephant Flow section



Elephant Flow Settings

For Snort 3 FTD devices 7.2.0 onwards, use this window to configure elephant flow.
For all Snort 2 FTD devices or Snort 3 FTD devices 7.1.0 and

Elephant flow detection does not apply to encrypted traffic. Le

Elephant Flow Detection

Generate elephant flow events when flow bytes **exceeds** 1024

Elephant flow Remediation

If CPU utilization **exceeds** 40 **% in fixed time windows of**

Then Bypass the flow

○ All applications including unidentified applications

● Select Applications/Filters (1 selected)

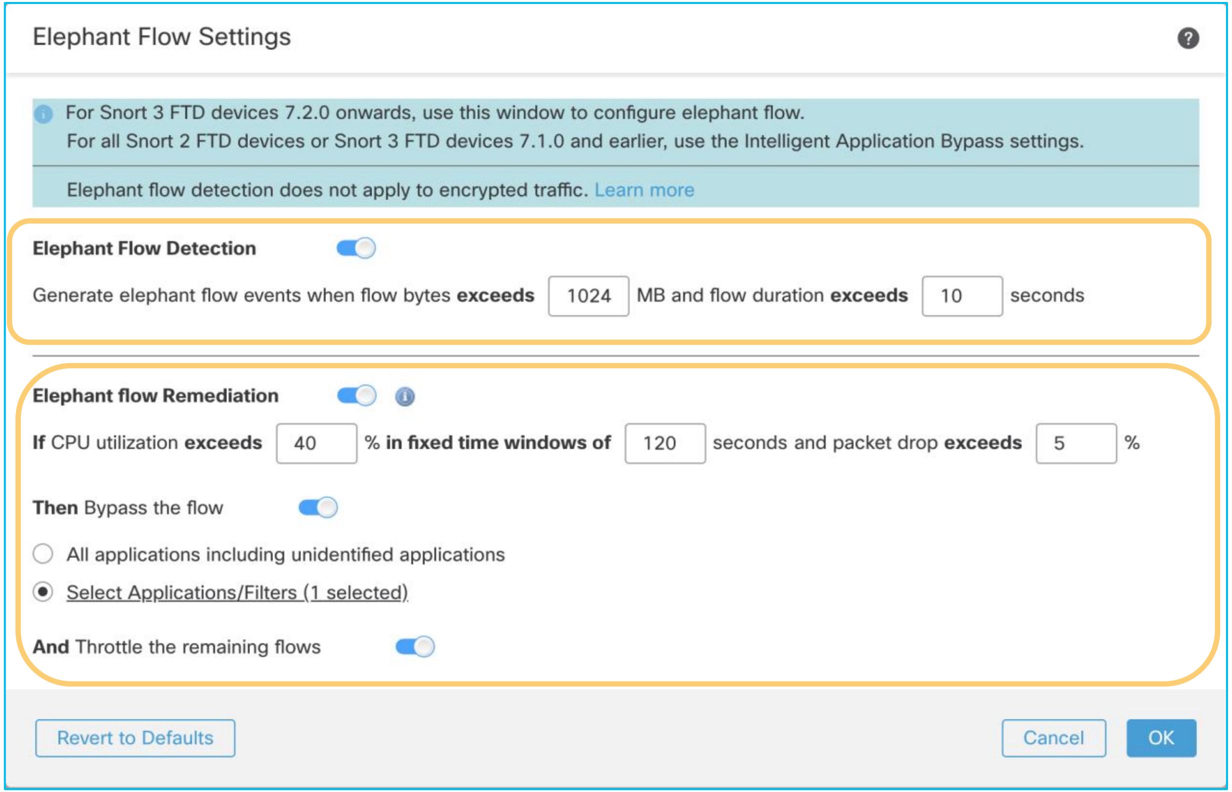
And Throttle the remaining flows

Revert to Defaults

```
> show elephant-flow status
Elephant flow inspector is enabled
> show elephant-flow detection-config
  bypass_apps(List of App IDs) = '676:1'
  bypass_enabled = true
  cpu_utilization(in Percentage) = 1
  high_cpu_check = true
  bytes_threshold(in MBs) = 1
  packet_drop_threshold(in Percentage) = 1
  qos_enabled = true
  time_threshold(in Seconds) = 2
  window_duration(in Seconds) = 2

>
```

Secure Firewall CLI Commands (Secure Firewall Version 7.2)

Feature is configured in **ACP Advanced** tab in Elephant Flow section



Elephant Flow Settings

For Snort 3 FTD devices 7.2.0 onwards, use this window to configure elephant flow.
For all Snort 2 FTD devices or Snort 3 FTD devices 7.1.0 and earlier, use the Intelligent Application Bypass settings.

Elephant flow detection does not apply to encrypted traffic. Learn more

Elephant Flow Detection ●

Generate elephant flow events when flow bytes **exceeds** 1024 MB and flow duration **exceeds** 10 seconds

Elephant flow Remediation ●

If CPU utilization **exceeds** 40 **% in fixed time windows of** 120 seconds and packet drop **exceeds** 5 %

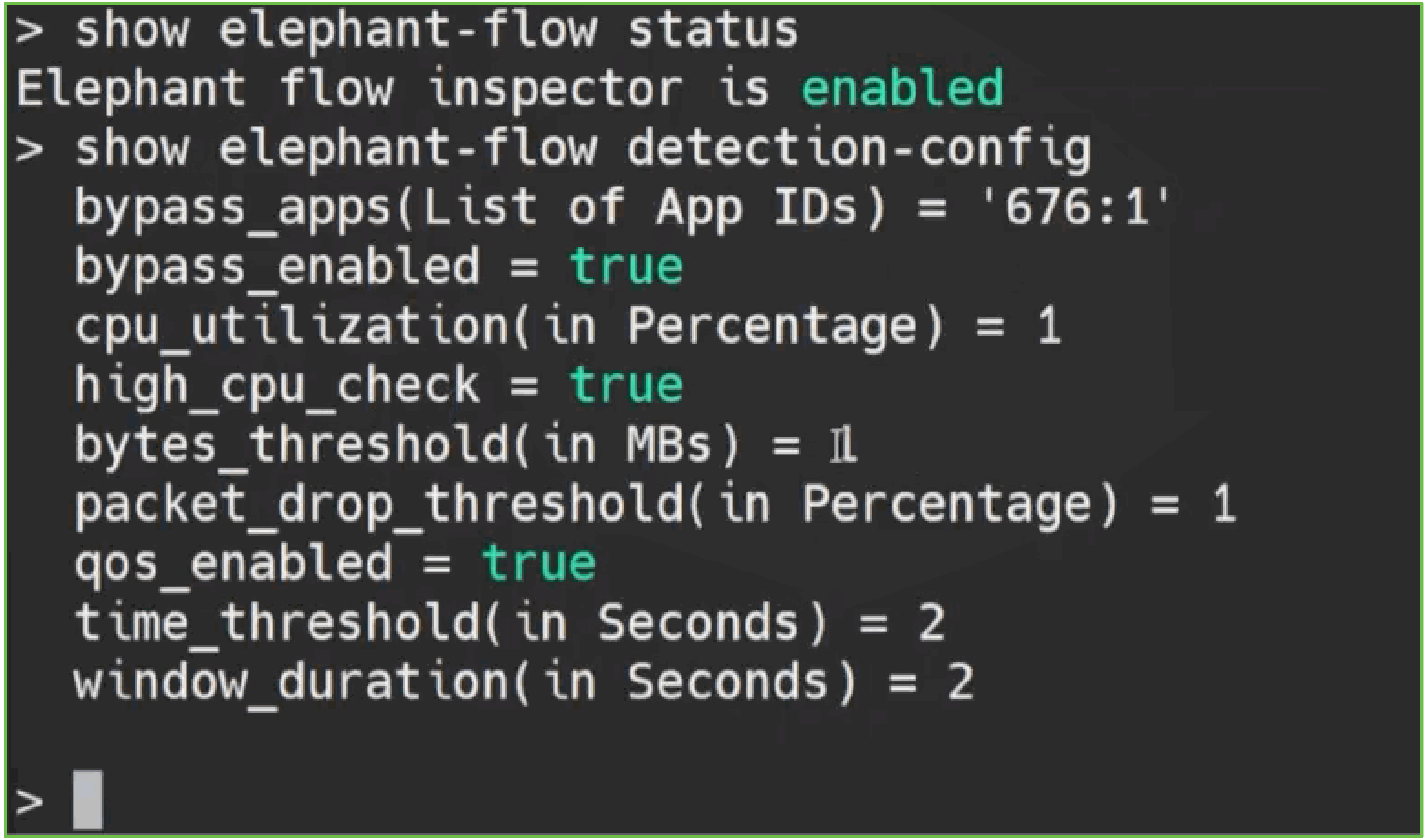
Then Bypass the flow ●

○ All applications including unidentified applications

● Select Applications/Filters (1 selected)

And Throttle the remaining flows ●

Secure Firewall CLI Commands (Secure Firewall Version 7.2)



```
> show elephant-flow status
Elephant flow inspector is enabled
> show elephant-flow detection-config
  bypass_apps(List of App IDs) = '676:1'
  bypass_enabled = true
  cpu_utilization(in Percentage) = 1
  high_cpu_check = true
  bytes_threshold(in MBs) = 1
  packet_drop_threshold(in Percentage) = 1
  qos_enabled = true
  time_threshold(in Seconds) = 2
  window_duration(in Seconds) = 2


>
```

Secure Firewall CLI Commands (Secure Firewall Version 7.1)

Command to tune elephant flow detection parameters

```
> system support elephant-flow-detection
 disable Disable elephant-flow-detection
 enable Enable elephant-flow-detection
 time-threshold Time threshold (in seconds) to detect elephant flow
 bytes-threshold Bytes threshold (in MB) to detect elephant flow
```

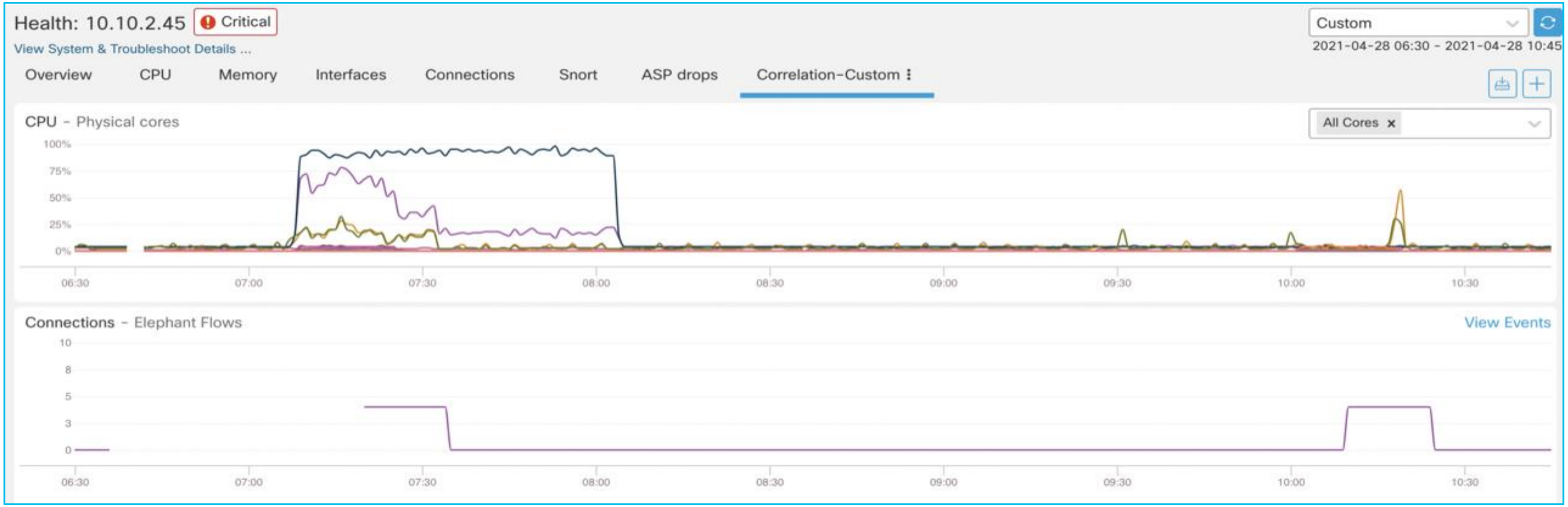
Command to display the threshold values

```
> show elephant-flow detection-config
bytes_threshold = 1024,
time_threshold = 10
```

Command to display the feature status

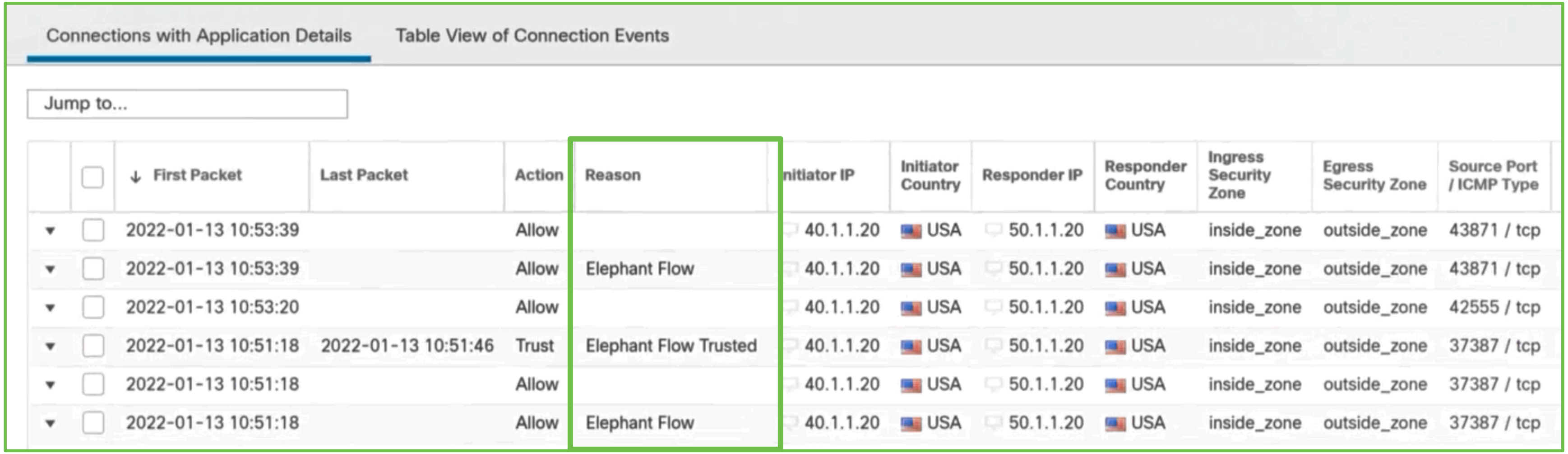
```
> show elephant-flow status
Elephant flow inspector is enabled
```

Detecting and Identifying Elephant Flows



Health Dashboard showing Correlation of Elephant flows with system parameters, showing the CPU spike.

Detecting and Identifying Elephant Flows



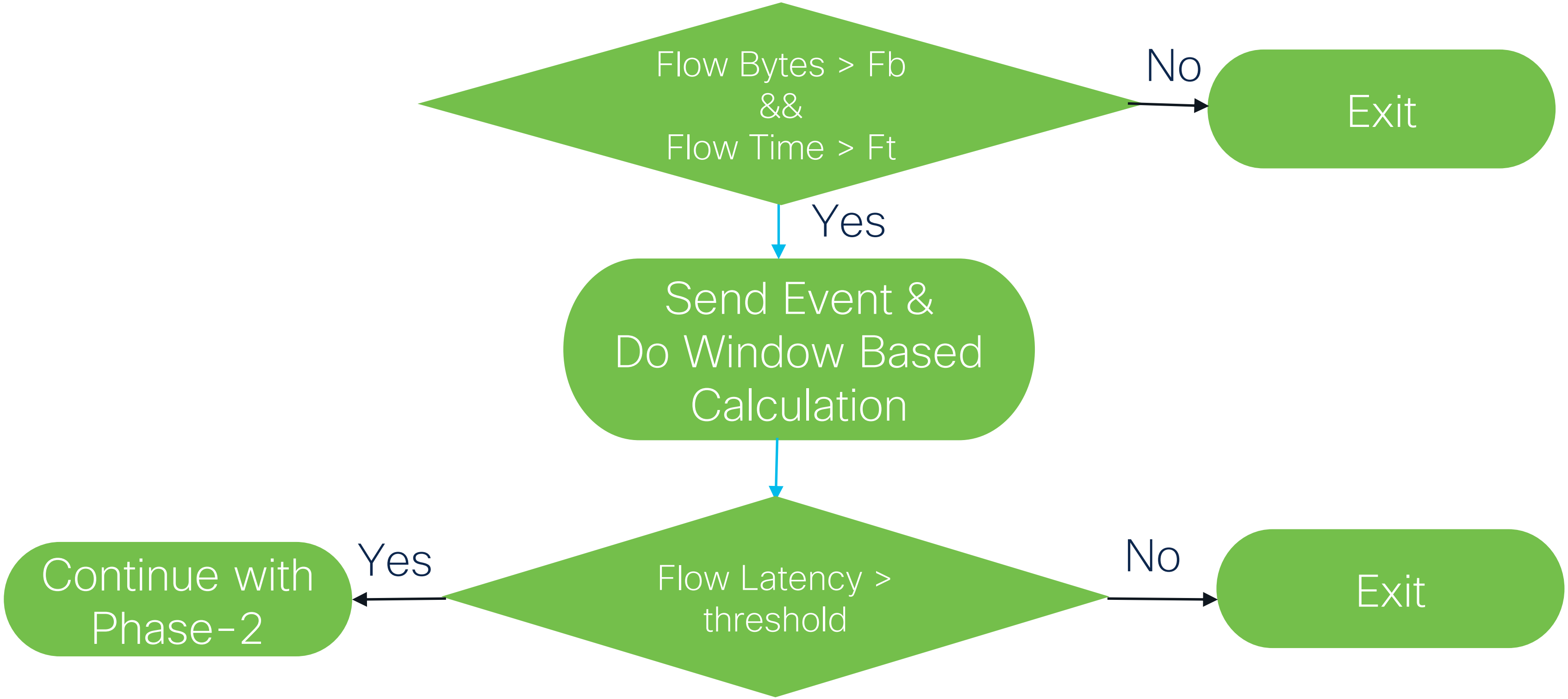
Connections with Application Details | Table View of Connection Events

Jump to...

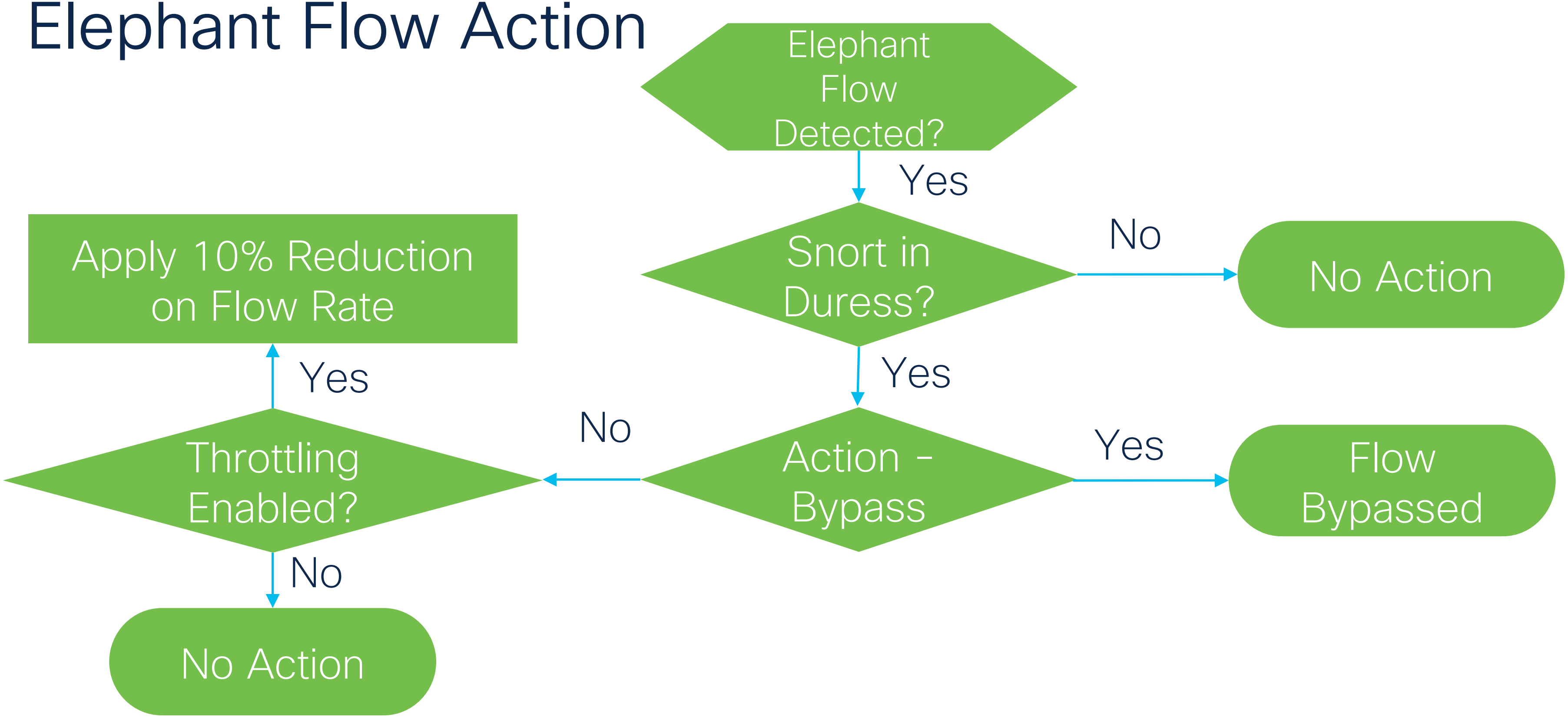
	□	↓ First Packet	Last Packet	Action	Reason	nitiator IP	Initiator Country	Responder IP	Responder Country	Ingress Security Zone	Egress Security Zone	Source Port / ICMP Type
▼	□	2022-01-13 10:53:39		Allow		40.1.1.20	USA	50.1.1.20	USA	inside_zone	outside_zone	43871 / tcp
▼	□	2022-01-13 10:53:39		Allow	Elephant Flow	40.1.1.20	USA	50.1.1.20	USA	inside_zone	outside_zone	43871 / tcp
▼	□	2022-01-13 10:53:20		Allow		40.1.1.20	USA	50.1.1.20	USA	inside_zone	outside_zone	42555 / tcp
▼	□	2022-01-13 10:51:18	2022-01-13 10:51:46	Trust	Elephant Flow Trusted	40.1.1.20	USA	50.1.1.20	USA	inside_zone	outside_zone	37387 / tcp
▼	□	2022-01-13 10:51:18		Allow		40.1.1.20	USA	50.1.1.20	USA	inside_zone	outside_zone	37387 / tcp
▼	□	2022-01-13 10:51:18		Allow	Elephant Flow	40.1.1.20	USA	50.1.1.20	USA	inside_zone	outside_zone	37387 / tcp

- Mid-flow event is generated as soon as system detects elephant flow
  Reason is set to **Elephant Flow**
- End of connection events will include action in **Reason** field
  For bypass action, **Reason** is set to **Elephant Flow Trusted**
  For throttle action, **Reason** is set to **Elephant Flow Throttled**

Elephant Flow Detection



Elephant Flow Action



7.3 Performance Profile for CPU Allocation

Background

- Resource Allocation (CPU Cores/Memory) for Deep Packet Inspection and Dataplane engine is fixed depending on the Cisco Secure Firewall platform
- This can lead to an overallocation or under allocation of CPU cores

What's New

- Customers can now Change the allocation of CPU cores using FMC.

Benefits

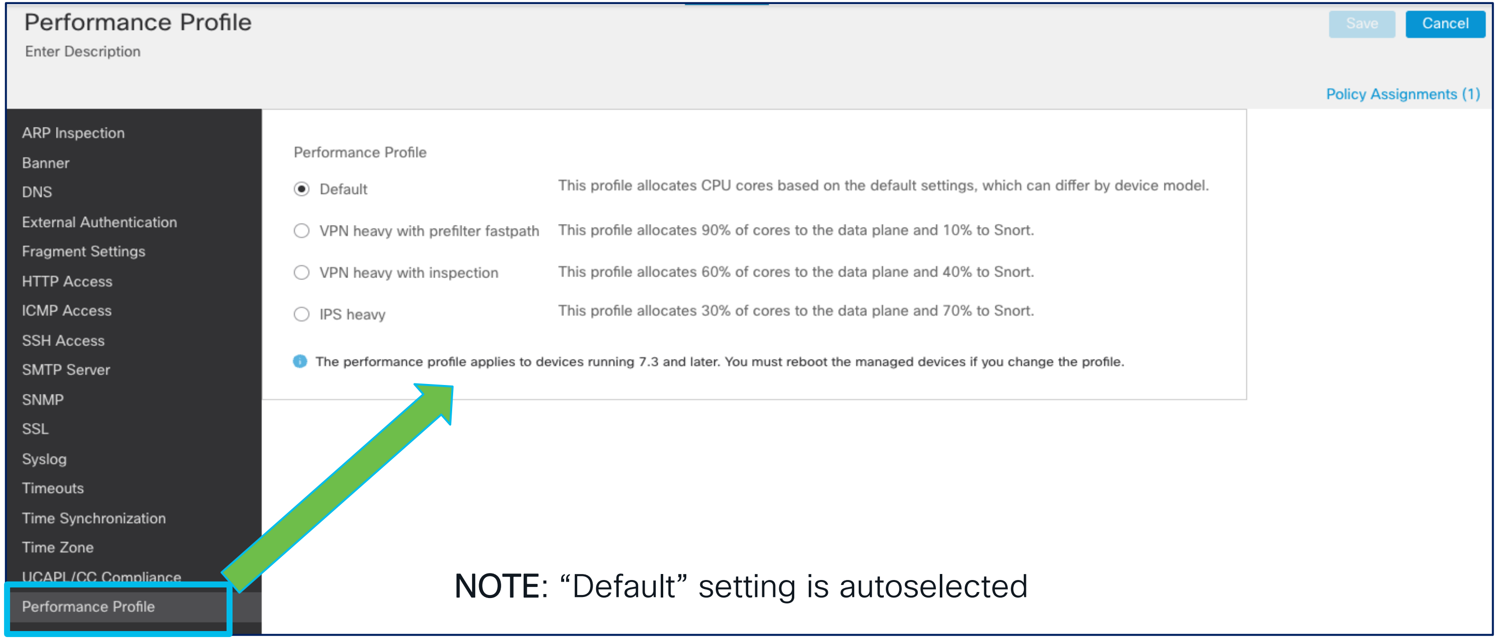
- Enables customers to optimize their CPU allocation based on deployment type.

Requirements

- FMC 7.3
- Configuration is only possible via the FMC GUI

7.3 Performance Profile Configuration

1. Go to Devices > Platform Settings > New Policy > Threat Defense Settings > Performance Profile
2. Pick the desired Performance Profile and click Save.



Performance Profile

- ● Default — This profile allocates CPU cores based on the default settings, which can differ by device model.
- ○ VPN heavy with prefilter fastpath — This profile allocates 90% of cores to the data plane and 10% to Snort.
- ○ VPN heavy with inspection — This profile allocates 60% of cores to the data plane and 40% to Snort.
- ○ IPS heavy — This profile allocates 30% of cores to the data plane and 70% to Snort.

The performance profile applies to devices running 7.3 and later. You must reboot the managed devices if you change the profile.

NOTE: "Default" setting is autoselected

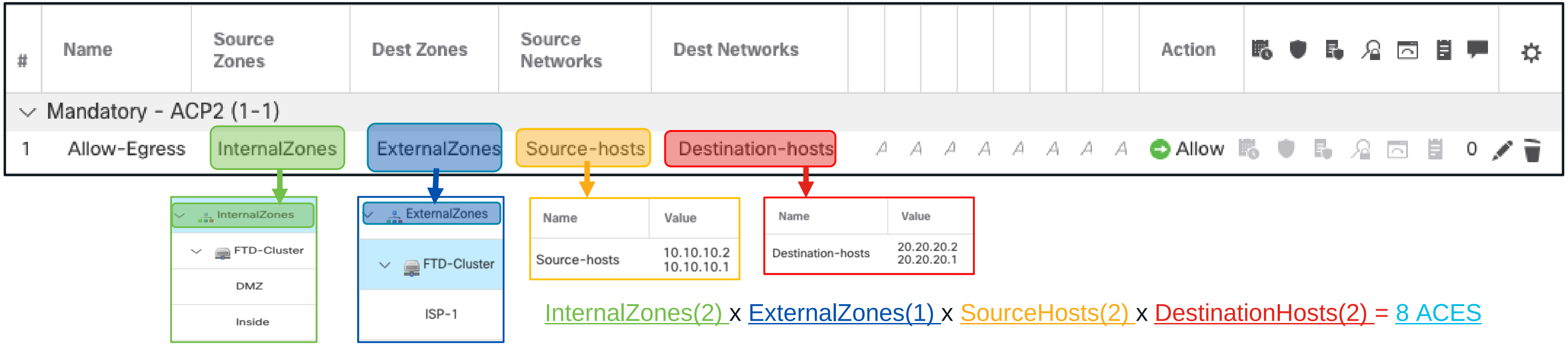
Lina Memory – Overview

- Lina memory:

```
firepower# show memory
Free memory:           250170904 bytes (47%)
Used memory:           286700008 bytes (53%)
-------------     ------------------
Total memory:          536870912 bytes (100%)
```

- Free memory may not recover immediately after conn spike due to caching.
- Connections, Xlates and ACL configuration are top users of shared memory.
- Asymmetric traffic may increase memory usage on snort side.

ACL Expansion



#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks									Action								
Mandatory - ACP2 (1-1)																						
1	Allow-Egress	InternalZones	ExternalZones	Source-hosts	Destination-hosts	A	A	A	A	A	A	A	A	Allow							0	

- InternalZones
  - FTD-Cluster
    - DMZ
    - Inside

- ExternalZones
  - FTD-Cluster
    - ISP-1

Name	Value
Source-hosts	10.10.10.2 10.10.10.1

Name	Value
Destination-hosts	20.20.20.2 20.20.20.1

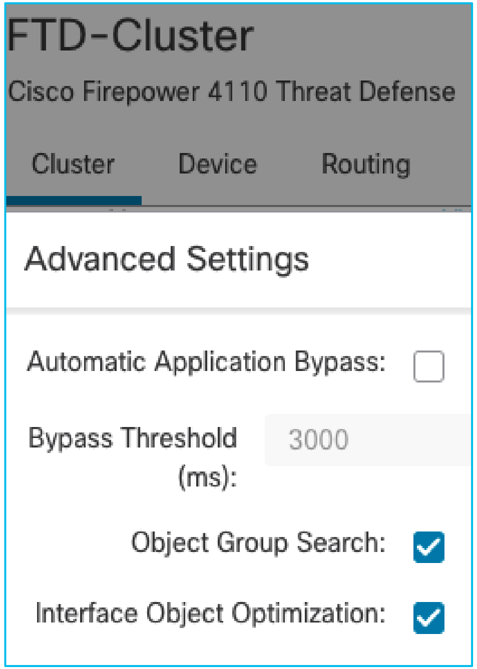
InternalZones(2) x ExternalZones(1) x SourceHosts(2) x DestinationHosts(2) = 8 ACES

```
> show access-list
access-list CSM_FW_ACL_ line 10 advanced permit ip ifc DMZ object-group Source-hosts ifc ISP-1 object-group Destination-hosts
  access-list CSM_FW_ACL_ line 10 advanced permit ip ifc DMZ host 10.10.10.2 ifc ISP-1 host 20.20.20.1 rule-id 268434437
  access-list CSM_FW_ACL_ line 10 advanced permit ip ifc DMZ host 10.10.10.2 ifc ISP-1 host 20.20.20.2 rule-id 268434437
  access-list CSM_FW_ACL_ line 10 advanced permit ip ifc DMZ host 10.10.10.1 ifc ISP-1 host 20.20.20.1 rule-id 268434437
  access-list CSM_FW_ACL_ line 10 advanced permit ip ifc DMZ host 10.10.10.1 ifc ISP-1 host 20.20.20.2 rule-id 268434437
access-list CSM_FW_ACL_ line 11 advanced permit ip ifc Inside object-group Source-hosts ifc ISP-1 object-group Destination-hosts
  access-list CSM_FW_ACL_ line 11 advanced permit ip ifc Inside host 10.10.10.2 ifc ISP-1 host 20.20.20.1 rule-id 268434437
  access-list CSM_FW_ACL_ line 11 advanced permit ip ifc Inside host 10.10.10.2 ifc ISP-1 host 20.20.20.2 rule-id 268434437
  access-list CSM_FW_ACL_ line 11 advanced permit ip ifc Inside host 10.10.10.1 ifc ISP-1 host 20.20.20.1 rule-id 268434437
  access-list CSM_FW_ACL_ line 11 advanced permit ip ifc Inside host 10.10.10.1 ifc ISP-1 host 20.20.20.2 rule-id 268434437
```

Access Control Rule Optimization

- Object Group Search (OGS)

- FTD 6.6+
- It will install just one rule, instead of expanding the Access Control Elements
- Might increase CPU usage during packet processing



FTD-Cluster

Cisco Firepower 4110 Threat Defense

Advanced Settings

Automatic Application Bypass: □

Bypass Threshold (ms): 3000

Object Group Search: ☑

Interface Object Optimization: ☑

Interface Object Optimization (IOO)

- FTD 6.7+
- Object-group CLI is enhanced to support interface type
- Interface Object-Group is supported for advanced Access-List
- Object Group Search is enhanced to support Interface Object Group

Access Control Rule Optimization

Object Group Search (OGS)

- Rule expansion with OGS disabled.

```
> show access-list
access-list CSM_FW_ACL_ line 10 advanced permit ip ifc DMZ object-group Source-hosts ifc ISP-1 object-group Destination-hosts rule-id
268434437
 access-list CSM_FW_ACL_ line 10 advanced permit ip ifc DMZ host 10.10.10.2 ifc ISP-1 host 20.20.20.1 rule-id 268434437
 access-list CSM_FW_ACL_ line 10 advanced permit ip ifc DMZ host 10.10.10.2 ifc ISP-1 host 20.20.20.2 rule-id 268434437
 access-list CSM_FW_ACL_ line 10 advanced permit ip ifc DMZ host 10.10.10.1 ifc ISP-1 host 20.20.20.1 rule-id 268434437
 access-list CSM_FW_ACL_ line 10 advanced permit ip ifc DMZ host 10.10.10.1 ifc ISP-1 host 20.20.20.2 rule-id 268434437

access-list CSM_FW_ACL_ line 11 advanced permit ip ifc Inside object-group Source-hosts ifc ISP-1 object-group Destination-hosts rule-id
268434437
 access-list CSM_FW_ACL_ line 11 advanced permit ip ifc Inside host 10.10.10.2 ifc ISP-1 host 20.20.20.1 rule-id 268434437
 access-list CSM_FW_ACL_ line 11 advanced permit ip ifc Inside host 10.10.10.2 ifc ISP-1 host 20.20.20.2 rule-id 268434437
 access-list CSM_FW_ACL_ line 11 advanced permit ip ifc Inside host 10.10.10.1 ifc ISP-1 host 20.20.20.1 rule-id 268434437
 access-list CSM_FW_ACL_ line 11 advanced permit ip ifc Inside host 10.10.10.1 ifc ISP-1 host 20.20.20.2 rule-id 268434437
```

- Rule expansion with OGS enabled.

```
firepower# show access-list
access-list CSM_FW_ACL_ line 10 advanced permit ip ifc DMZ object-group Source-hosts ifc ISP-1 object-group Destination-hosts rule-id
268434437
 access-list CSM_FW_ACL_ line 10 advanced permit ip ifc DMZ v4-object-group Source-hosts(2147483648) ifc ISP-1 v4-object-group
Destination-hosts(2147483649) rule-id 268434437
access-list CSM_FW_ACL_ line 11 advanced permit ip ifc Inside object-group Source-hosts ifc ISP-1 object-group Destination-hosts rule-
id 268434437
 access-list CSM_FW_ACL_ line 11 advanced permit ip ifc Inside v4-object-group Source-hosts(2147483648) ifc ISP-1 v4-object-group
Destination-hosts(2147483649) rule-id 268434437
```

Access Control Rule Optimization

Interface Object Optimization (IOO)

- Rule expansion with IOO disabled.

```
firepower# show access-list
access-list CSM_FW_ACL_ line 10 advanced permit ip ifc DMZ object-group Source-hosts ifc ISP-1 object-group Destination-hosts rule-id
268434437
  access-list CSM_FW_ACL_ line 10 advanced permit ip ifc DMZ v4-object-group Source-hosts(2147483648) ifc ISP-1 v4-object-group
Destination-hosts(2147483649) rule-id 268434437
access-list CSM_FW_ACL_ line 11 advanced permit ip ifc Inside object-group Source-hosts ifc ISP-1 object-group Destination-hosts rule-
id 268434437
  access-list CSM_FW_ACL_ line 11 advanced permit ip ifc Inside v4-object-group Source-hosts(2147483648) ifc ISP-1 v4-object-group
Destination-hosts(2147483649) rule-id 268434437
```

- Rule expansion with IOO enabled.

```
firepower# show access-list
access-list CSM_FW_ACL_ line 10 advanced permit ip object-group-ifc InternalZones object-group Source-hosts object-group-ifc
ExternalZones object-group Destination-hosts rule-id 268434437
  access-list CSM_FW_ACL_ line 10 advanced permit ip object-group-ifc igsz_00000_zsgi v4-object-group Source-hosts(2147483648) object-
group-ifc igsz_00001_zsgi v4-object-group Destination-hosts(2147483649) rule-id 268434437
```

7.6 Policy Analyzer And Optimizer (PAO)

Out of Memory from Access Rules

- Supported on Cloud Delivered FMC and On-Prem from version 7.2 and Higher
- Cross-launch from Firewall Management Center from 7.6
- FMC must be integrated with Cisco Security Cloud
- Detect and Analysis of rule inefficiencies
  Remediation: Optimize the anomalous rules.
- Reporting: Download pdf reports for analysis.

Expiry Rule Detection

Mergeable Rule Detection

Hit Count Insights

Remediation

Version Agnostic

7.6 Policy Analyzer And Optimizer (PAO)

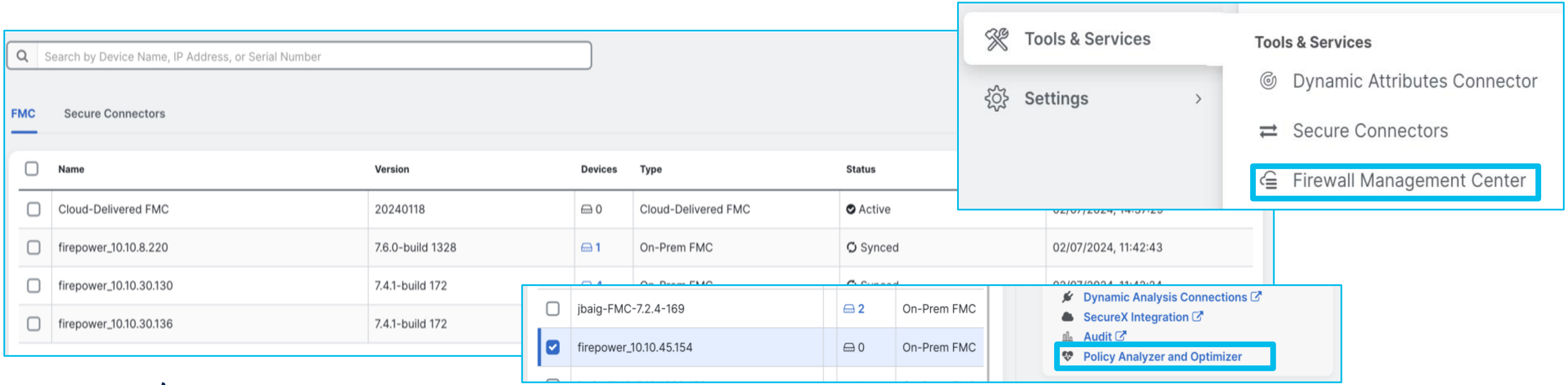
Firewall Management Center Listing in CDO

Once the Integration in Cisco Defense Organizer (CDO) is done, access control policies will automatically be exported and analyzed

CDO then lists all the Firewall Management Center(s) (FMC) onboarded into Cisco Defense Orchestrator (CDO).

In CDO. To see the list, go to Tools & Services -> Firewall Management Center

Users can then select the Firewall Device and select Policy Analyzer and Optimizer.



Search by Device Name, IP Address, or Serial Number

FMC | Secure Connectors

□	Name	Version	Devices	Type	Status	
□	Cloud-Delivered FMC	20240118	0	Cloud-Delivered FMC	Active	02/07/2024, 14:37:25
□	firepower_10.10.8.220	7.6.0-build 1328	1	On-Prem FMC	Synced	02/07/2024, 11:42:43
□	firepower_10.10.30.130	7.4.1-build 172	4	On-Prem FMC	Synced	02/07/2024, 11:43:24
□	firepower_10.10.30.136	7.4.1-build 172				

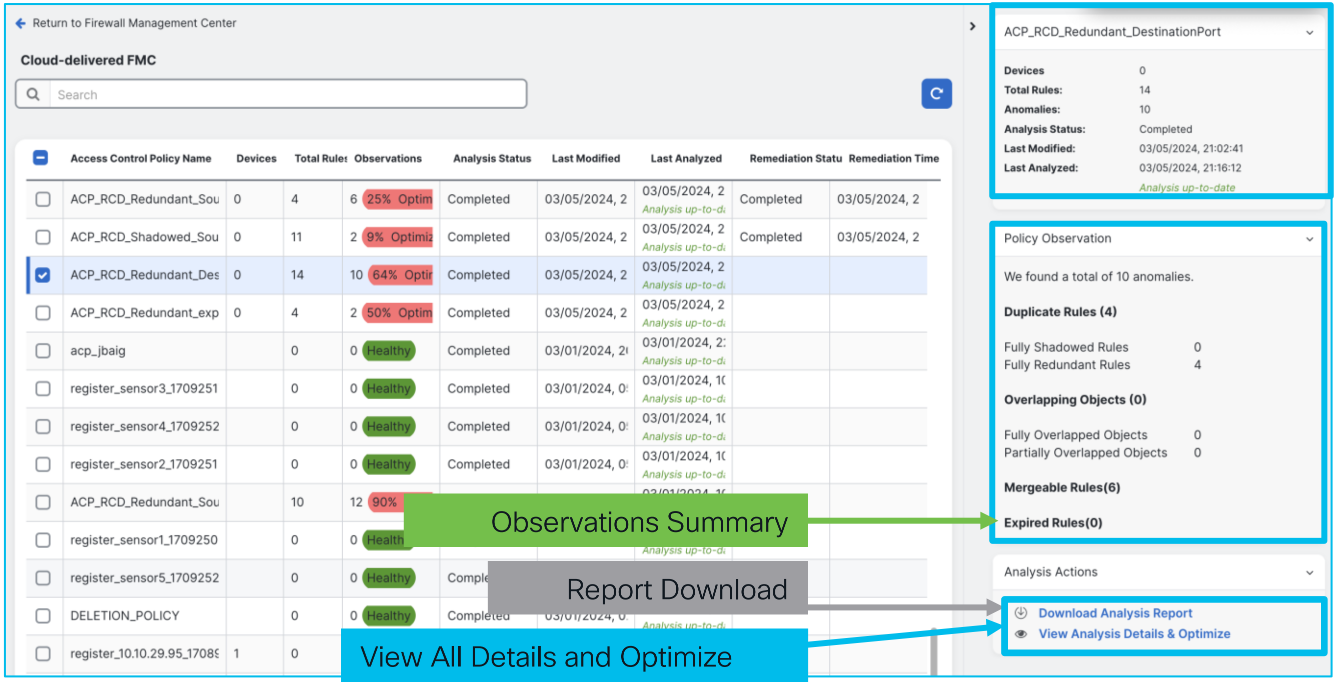
□	jbaig-FMC-7.2.4-169	2	On-Prem FMC
☑	firepower_10.10.45.154	0	On-Prem FMC

7.6 Policy Analyzer And Optimizer (PAO)

NEW

Firewall Management Center Listing in CDO

- The user will see the full list of analysed policies. By selecting a policy, an observation summary will show in the right pane.
  - If a user clicks on “View Details & Optimize,” they will be redirected to the Policy Analysis Summary Dashboard



Cloud-delivered FMC

☐	Access Control Policy Name	Devices	Total Rules	Observations	Analysis Status	Last Modified	Last Analyzed	Remediation Statu	Remediation Time
☐	ACP_RCD_Redundant_Sou	0	4	6 25% Optim	Completed	03/05/2024, 2	03/05/2024, 2 Analysis up-to-d	Completed	03/05/2024, 2
☐	ACP_RCD_Shadowed_Sou	0	11	2 9% Optimiz	Completed	03/05/2024, 2	03/05/2024, 2 Analysis up-to-d	Completed	03/05/2024, 2
☑	ACP_RCD_Redundant_Des	0	14	10 64% Optir	Completed	03/05/2024, 2	03/05/2024, 2 Analysis up-to-d		
☐	ACP_RCD_Redundant_exp	0	4	2 50% Optim	Completed	03/05/2024, 2	03/05/2024, 2 Analysis up-to-d		
☐	acp_jbaig		0	0 Healthy	Completed	03/01/2024, 2	03/01/2024, 2 Analysis up-to-d		
☐	register_sensor3_1709251		0	0 Healthy	Completed	03/01/2024, 0	03/01/2024, 1 Analysis up-to-d		
☐	register_sensor4_1709252		0	0 Healthy	Completed	03/01/2024, 0	03/01/2024, 1 Analysis up-to-d		
☐	register_sensor2_1709251		0	0 Healthy	Completed	03/01/2024, 0	03/01/2024, 1 Analysis up-to-d		
☐	ACP_RCD_Redundant_Sou		10	12 90%			03/01/2024, 1		
☐	register_sensor1_1709250		0	0 Health			Analysis up-to-d		
☐	register_sensor5_1709252		0	0 Healthy	Comple				
☐	DELETION_POLICY		0	0 Healthy	Completed	03/01/2024, 0	Analysis up-to-d		
☐	register_10.10.29.95_1708	1	0						

ACP_RCD_Redundant_DestinationPort

Devices	0
Total Rules:	14
Anomalies:	10
Analysis Status:	Completed
Last Modified:	03/05/2024, 21:02:41
Last Analyzed:	03/05/2024, 21:16:12 Analysis up-to-date

Policy Observation

We found a total of 10 anomalies.

Duplicate Rules (4)

Fully Shadowed Rules	0
Fully Redundant Rules	4

Overlapping Objects (0)

Fully Overlapped Objects	0
Partially Overlapped Objects	0

Mergeable Rules(6)

Expired Rules(0)

Analysis Actions

Observations Summary

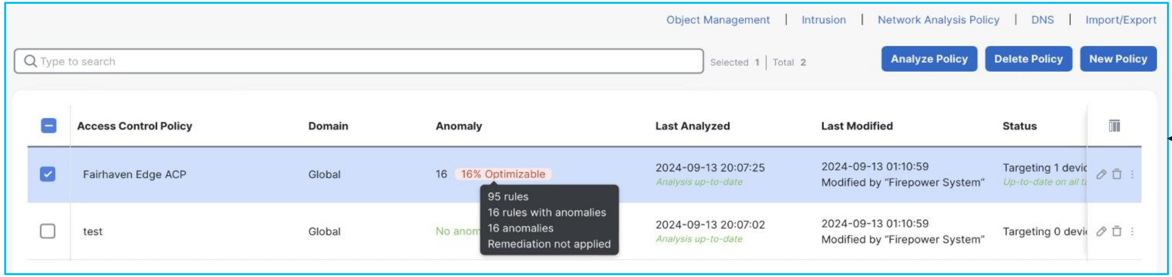
Report Download

View All Details and Optimize

7.6 Policy Analyzer And Optimizer (PAO)

Accessing from Firewall Management Center

- On Firewall Management Center version 7.6, you can also cross-launch directly into Policy Analyzer and Optimizer.

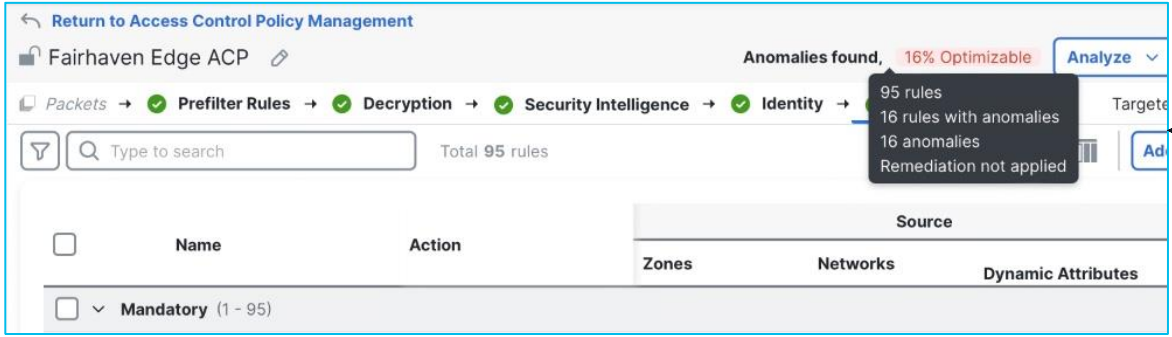


Object Management | Intrusion | Network Analysis Policy | DNS | Import/Export
Type to search
Selected 1 | Total 2
Analyze Policy
Delete Policy
New Policy

☐	Access Control Policy	Domain	Anomaly	Last Analyzed	Last Modified	Status
☑	Fairhaven Edge ACP	Global	16 16% Optimizable	2024-09-13 20:07:25 *Analysis up-to-date*	2024-09-13 01:10:59 Modified by "Firepower System"	Targeting 1 devic *Up-to-date on all ta*
☐	test	Global	No anom	2024-09-13 20:07:02 *Analysis up-to-date*	2024-09-13 01:10:59 Modified by "Firepower System"	Targeting 0 devic

95 rules
16 rules with anomalies
16 anomalies
Remediation not applied

From Firewall Management Center, navigate to **Policies** > **Access Control**. there are additional details displayed about Anomalies found within the policy



Return to Access Control Policy Management
Fairhaven Edge ACP
Anomalies found, 16% Optimizable
Analyze
Packets → Prefilter Rules → Decryption → Security Intelligence → Identity →
Targete
Type to search
Total 95 rules
Ad

95 rules
16 rules with anomalies
16 anomalies
Remediation not applied

☐	Name	Action	Source		
			Zones	Networks	Dynamic Attributes
☐	Mandatory (1 - 95)				

From within the policy editor the same Anomaly details can be seen.

Policy Analysis Summary Dashboard

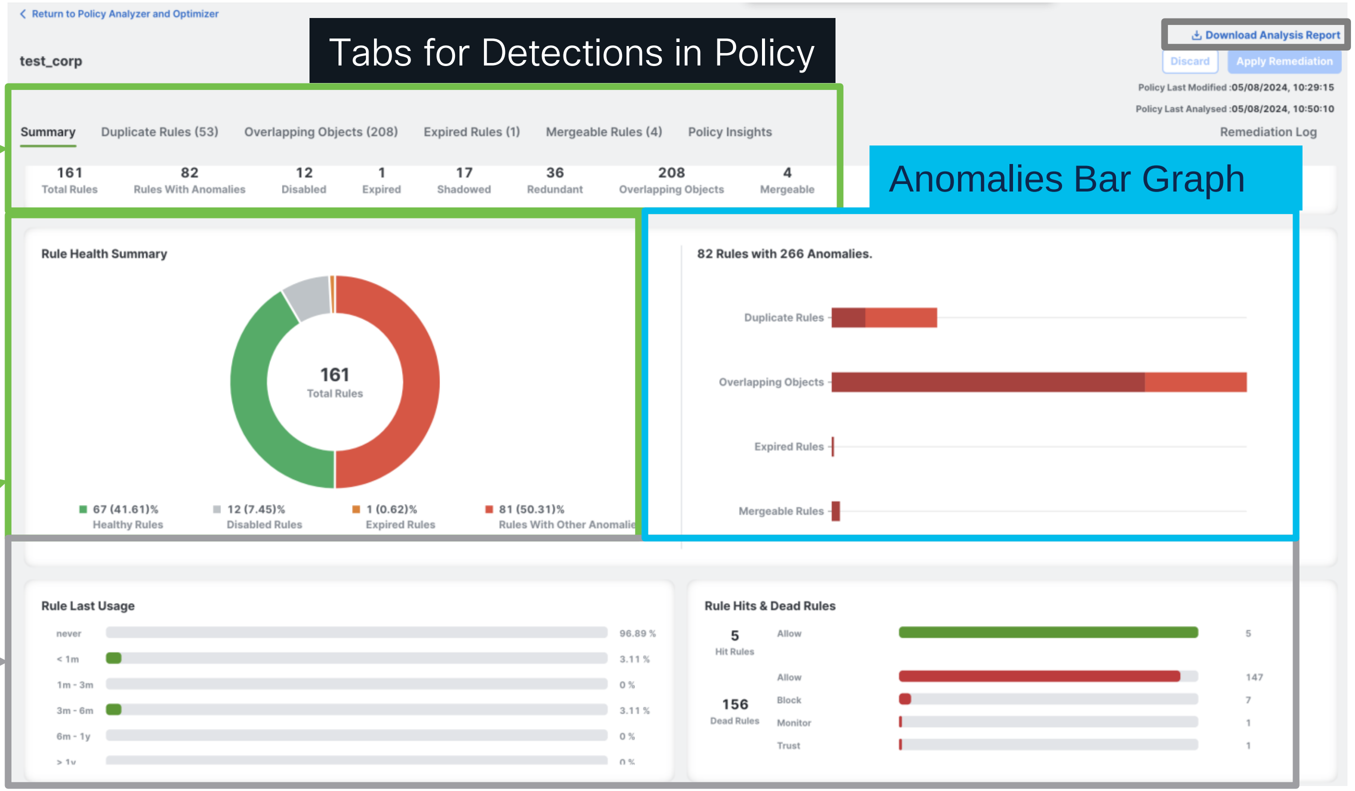
Report Download

This shows Analysis Summary dashboard.

- Rule Health Summary
- Anomalies bar graph
- Rule Hits Insights
- Anomaly tabs

Pie Chart of Observations

Rule Hits Insights



Tabs for Detections in Policy

Anomalies Bar Graph

< Return to Policy Analyzer and Optimizer

test_corp

Download Analysis Report

Discard　Apply Remediation

Policy Last Modified :05/08/2024, 10:29:15

Policy Last Analysed :05/08/2024, 10:50:10

Remediation Log

Summary　Duplicate Rules (53)　Overlapping Objects (208)　Expired Rules (1)　Mergeable Rules (4)　Policy Insights

161	82	12	1	17	36	208	4
Total Rules	Rules With Anomalies	Disabled	Expired	Shadowed	Redundant	Overlapping Objects	Mergeable

Rule Health Summary

82 Rules with 266 Anomalies.

Rule Last Usage

never	96.89 %
< 1m	3.11 %
1m - 3m	0 %
3m - 6m	3.11 %
6m - 1y	0 %
> 1y	0 %

Rule Hits & Dead Rules

5 Hit Rules	Allow	5
156 Dead Rules	Allow	147
	Block	7
	Monitor	1
	Trust	1

~~Datapath~~
~~Upgrade~~
~~Performance~~
You are here
Use Case
SECURELAND CITY

Case Study

A day in the life of a TAC engineer

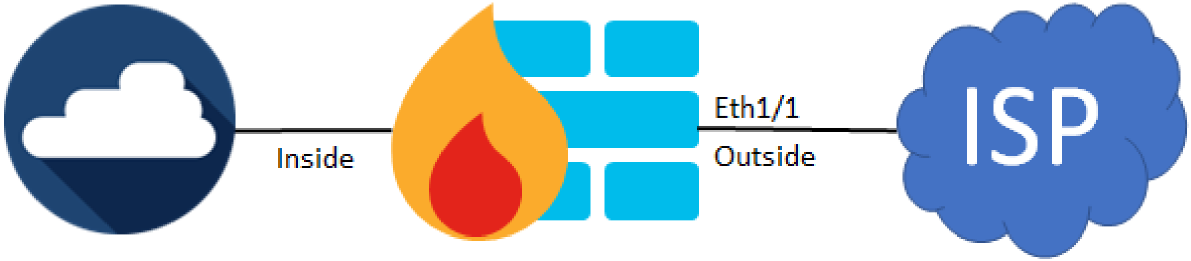
Incoming P1 Case

Case Number: 681920398 **Customer**: Secureland Solutions **Severity**: P1
Title: Seeing Flaps on Cisco Switch **Platform:** FPR2120
Problem Description: This switch is connecting to ISP and we see link is continuously flapping. Need involvement of Cisco TAC for this issue.

What Questions to ask:

1) Clear Problem Description!!!!
2) When did the issue start and what changes were made?
3) What is the impact?
4) Topology
5) Symptoms
6) Troubleshoot file and show tech

Post Interrogation Problem Description

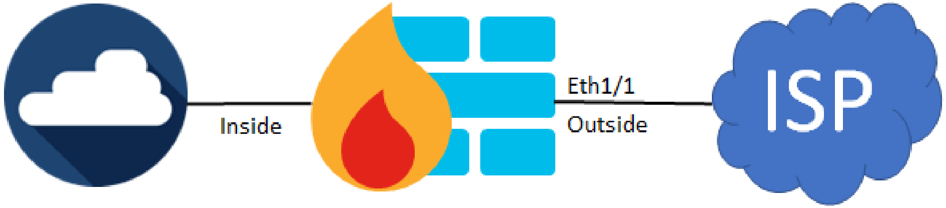


- Trigger of the issue was an ISP router reload.
- FTD outside interface flaps (Interface Status goes Up and Down) after the reload.
- Once Interface status is stable (remains up), restoration of services can take **5 to 20** minutes.
- No full outage, but major packet loss, performance degradation of **to-the-box**, and **through-the-box** traffic.
- SSH to the box is randomly terminated

Pings from directly and physically connected host

```
Type escape sequence to abort.
Sending 100, 100-byte ICMP Echos to
10.203.86.148, timeout is 2 seconds:
!!..!...!..!!.!!!!!!!!!!!!!!!!..!!!.....!!!!!!!!!!...!.!.!...!!!.!!!!!
!.!!!!!!!!..!!!!!.!!!!!.!..!!!
Success rate is 69 percent (69/100), round-
trip min/avg/max = 1/1/8 ms
```

Analysis of Existing Data



- No major increase in resource usage (conn, conn-rate, xlate, inspect, perfmon etc.) except syslogs → `show resource usage`

```
                                    Current   Peak    Limit
Syslogs [rate]                       0        52480   unlimited
```

Before

```
Syslogs [rate]                      22993     52480   unlimited
```

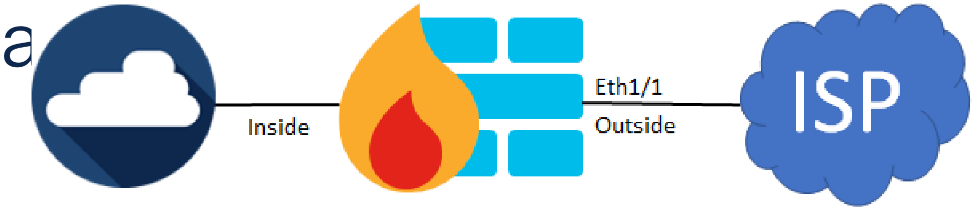
After

- Elevated CPU usage

```
------------------- show cpu usage -------------------
CPU utilization for 5 seconds = 4%; 1 minute: 6%; 5 minutes: 5%
Current control plane usage versus the control plane cores elapsed for:
        5 seconds = 1.2%; 1 minute: 1.2%; 5 minutes: 1.0%
```

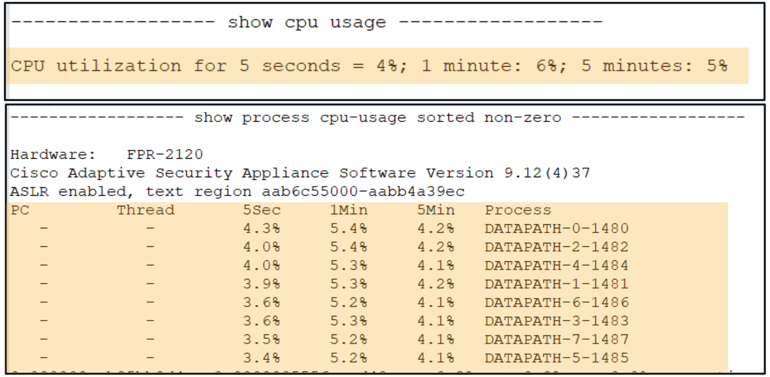
```
------------------- show cpu usage -------------------
CPU utilization for 5 seconds = 62%; 1 minute: 26%; 5 minutes: 32%
Current control plane usage versus the control plane cores elapsed for:
        5 seconds = 93.0%; 1 minute: 33.5%; 5 minutes: 43.1%
```

Analysis of Existing Data



- Multiple processes (DP, Logger, CP processing) have elevated CPU usage:

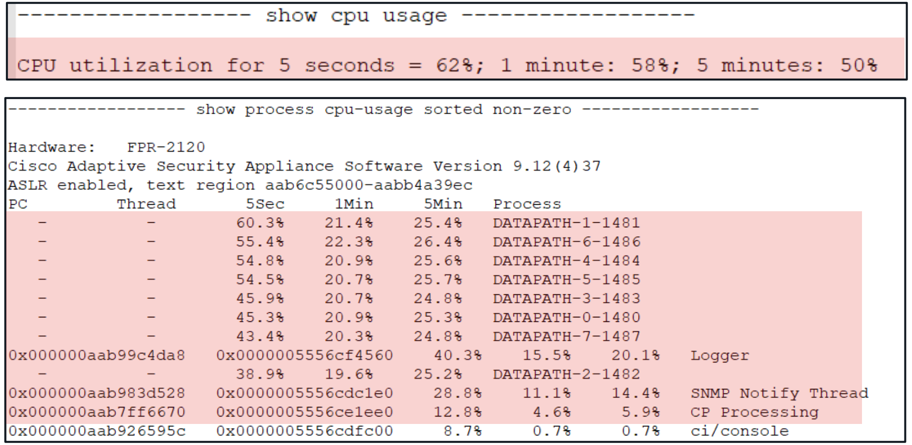
Before



```
------------------ show cpu usage ------------------

CPU utilization for 5 seconds = 4%; 1 minute: 6%; 5 minutes: 5%
```

```
----------------- show process cpu-usage sorted non-zero -----------------

Hardware:   FPR-2120
Cisco Adaptive Security Appliance Software Version 9.12(4)37
ASLR enabled, text region aab6c55000-aabb4a39ec
PC          Thread         5Sec      1Min      5Min    Process
   -             -          4.3%      5.4%      4.2%    DATAPATH-0-1480
   -             -          4.0%      5.4%      4.2%    DATAPATH-2-1482
   -             -          4.0%      5.3%      4.1%    DATAPATH-4-1484
   -             -          3.9%      5.3%      4.2%    DATAPATH-1-1481
   -             -          3.6%      5.2%      4.1%    DATAPATH-6-1486
   -             -          3.6%      5.3%      4.1%    DATAPATH-3-1483
   -             -          3.5%      5.2%      4.1%    DATAPATH-7-1487
   -             -          3.4%      5.2%      4.1%    DATAPATH-5-1485
```

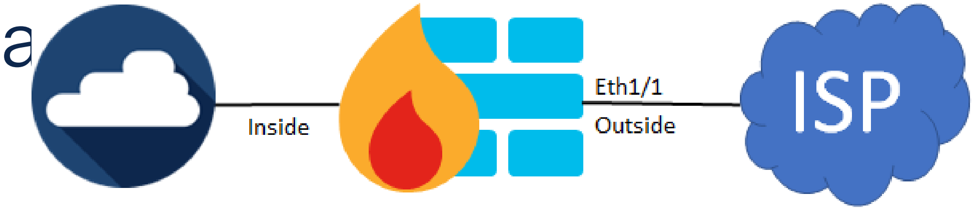
After



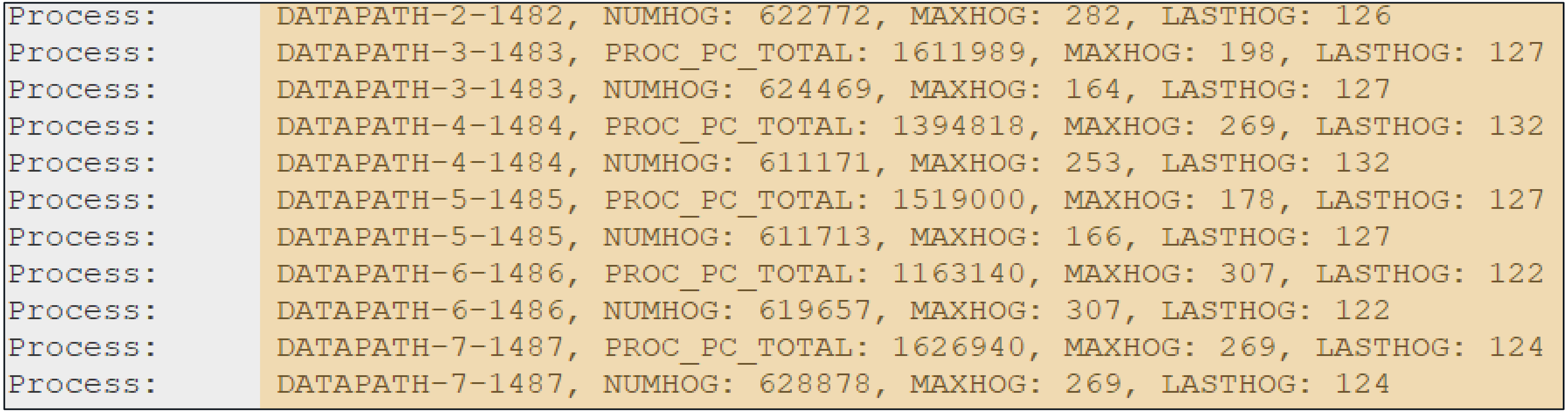
```
------------------ show cpu usage ------------------

CPU utilization for 5 seconds = 62%; 1 minute: 58%; 5 minutes: 50%
```

```
----------------- show process cpu-usage sorted non-zero -----------------

Hardware:   FPR-2120
Cisco Adaptive Security Appliance Software Version 9.12(4)37
ASLR enabled, text region aab6c55000-aabb4a39ec
PC            Thread         5Sec      1Min      5Min    Process
   -               -          60.3%     21.4%     25.4%    DATAPATH-1-1481
   -               -          55.4%     22.3%     26.4%    DATAPATH-6-1486
   -               -          54.8%     20.9%     25.6%    DATAPATH-4-1484
   -               -          54.5%     20.7%     25.7%    DATAPATH-5-1485
   -               -          45.9%     20.7%     24.8%    DATAPATH-3-1483
   -               -          45.3%     20.9%     25.3%    DATAPATH-0-1480
   -               -          43.4%     20.3%     24.8%    DATAPATH-7-1487
0x000000aab99c4da8   0x0000005556cf4560     40.3%     15.5%     20.1%    Logger
   -               -          38.9%     19.6%     25.2%    DATAPATH-2-1482
0x000000aab983d528   0x0000005556cdc1e0     28.8%     11.1%     14.4%    SNMP Notify Thread
0x000000aab7ff6670   0x0000005556ce1ee0     12.8%      4.6%      5.9%    CP Processing
0x000000aab926595c   0x0000005556cdfc00      8.7%      0.7%      0.7%    ci/console
```

Analysis of Existing Data

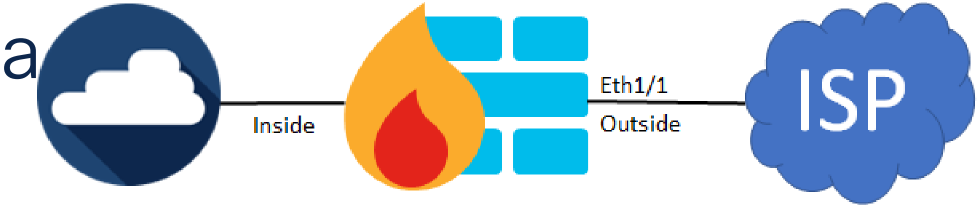


- CPU Hogs in DATAPATH process → `show process cpu-hog`

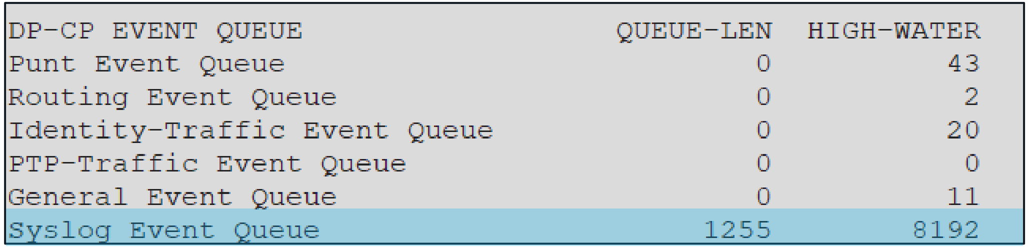


```
Process:     DATAPATH-2-1482, NUMHOG: 622772, MAXHOG: 282, LASTHOG: 126
Process:     DATAPATH-3-1483, PROC_PC_TOTAL: 1611989, MAXHOG: 198, LASTHOG: 127
Process:     DATAPATH-3-1483, NUMHOG: 624469, MAXHOG: 164, LASTHOG: 127
Process:     DATAPATH-4-1484, PROC_PC_TOTAL: 1394818, MAXHOG: 269, LASTHOG: 132
Process:     DATAPATH-4-1484, NUMHOG: 611171, MAXHOG: 253, LASTHOG: 132
Process:     DATAPATH-5-1485, PROC_PC_TOTAL: 1519000, MAXHOG: 178, LASTHOG: 127
Process:     DATAPATH-5-1485, NUMHOG: 611713, MAXHOG: 166, LASTHOG: 127
Process:     DATAPATH-6-1486, PROC_PC_TOTAL: 1163140, MAXHOG: 307, LASTHOG: 122
Process:     DATAPATH-6-1486, NUMHOG: 619657, MAXHOG: 307, LASTHOG: 122
Process:     DATAPATH-7-1487, PROC_PC_TOTAL: 1626940, MAXHOG: 269, LASTHOG: 124
Process:     DATAPATH-7-1487, NUMHOG: 628878, MAXHOG: 269, LASTHOG: 124
```

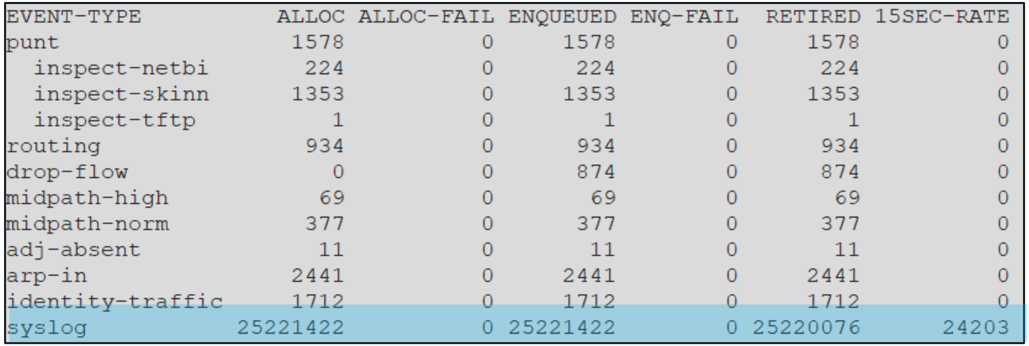
Analysis of Existing Data



- ASP DP-CP events → `show asp event dp-cp`

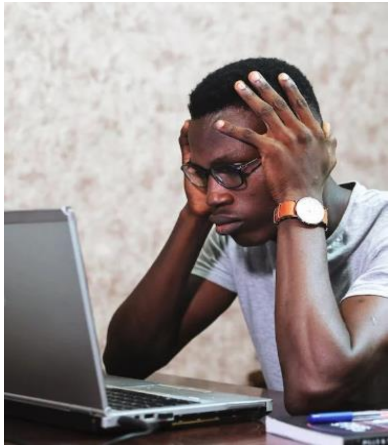


```
DP-CP EVENT QUEUE                        QUEUE-LEN  HIGH-WATER
Punt Event Queue                                 0          43
Routing Event Queue                              0           2
Identity-Traffic Event Queue                     0          20
PTP-Traffic Event Queue                          0           0
General Event Queue                              0          11
Syslog Event Queue                            1255        8192
```

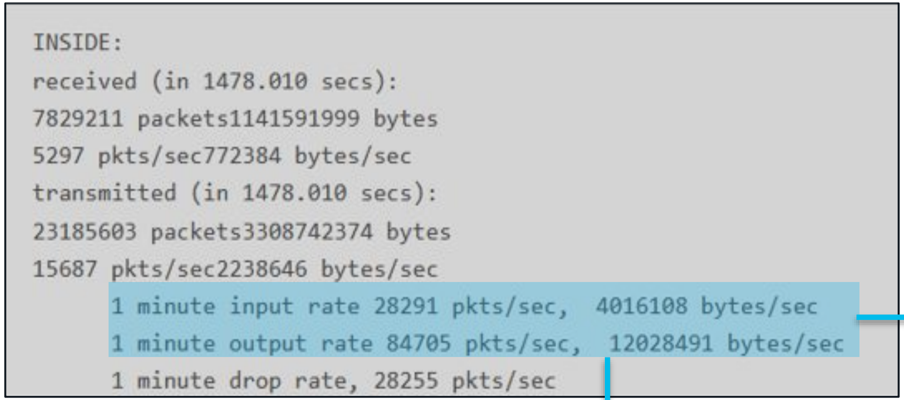


```
EVENT-TYPE            ALLOC ALLOC-FAIL ENQUEUED ENQ-FAIL  RETIRED 15SEC-RATE
punt                   1578          0     1578        0     1578          0
  inspect-netbi         224          0      224        0      224          0
  inspect-skinn        1353          0     1353        0     1353          0
  inspect-tftp            1          0        1        0        1          0
routing                 934          0      934        0      934          0
drop-flow                 0          0      874        0      874          0
midpath-high             69          0       69        0       69          0
midpath-norm            377          0      377        0      377          0
adj-absent               11          0       11        0       11          0
arp-in                 2441          0     2441        0     2441          0
identity-traffic       1712          0     1712        0     1712          0
syslog             25221422          0 25221422        0 25220076      24203
```

No logs are found in customer syslog servers during the issue!

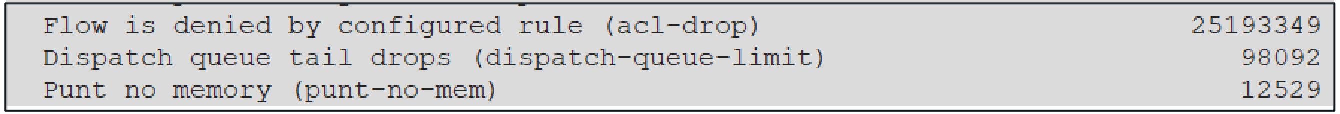


Analysis of Existing Data



```
INSIDE:
received (in 1478.010 secs):
7829211 packets1141591999 bytes
5297 pkts/sec772384 bytes/sec
transmitted (in 1478.010 secs):
23185603 packets3308742374 bytes
15687 pkts/sec2238646 bytes/sec
      1 minute input rate 28291 pkts/sec,  4016108 bytes/sec
      1 minute output rate 84705 pkts/sec,  12028491 bytes/sec
      1 minute drop rate, 28255 pkts/sec
```

- `Show ASP Drops`: highest are **acl-drop** and **dispatch-queue-limit**



```
  Flow is denied by configured rule (acl-drop)                 25193349
  Dispatch queue tail drops (dispatch-queue-limit)                98092
  Punt no memory (punt-no-mem)                                    12529
```

- Interface/throughput stats → `show traffic`:

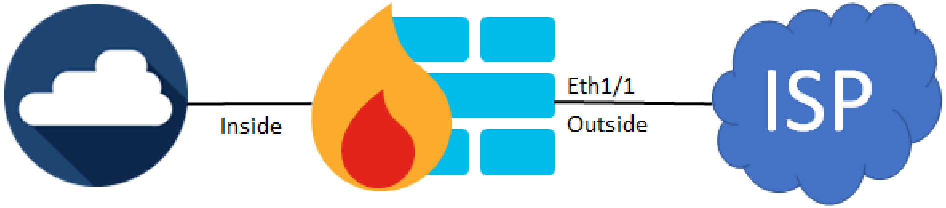
Before

Input Bytes	Input Packets	Input Pkt Size	Output Bytes	Output Packets	Output Pkt Size
75,544 bytes/s	214 pkts/s	353 bytes	75,546 bytes/s	214 pkts/s	353 bytes

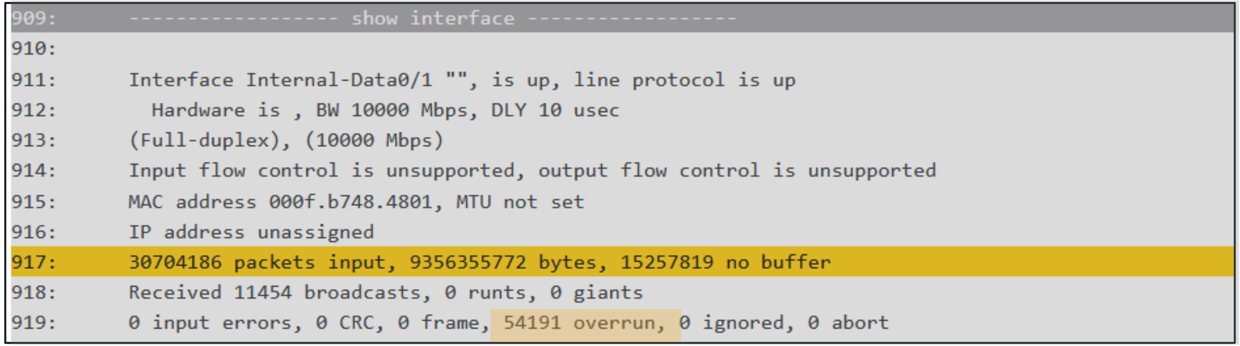
After

Input Bytes	Input Packets	Input Pkt Size	Output Bytes	Output Packets	Output Pkt Size
4,016,108 bytes/s	28,291 pkts/s	142 bytes	12,031,961 bytes/s	84,740 pkts/s	142 bytes

Analysis of Existing Data



Interface/throughput stats: significant no buffer and overrun errors during the incident:

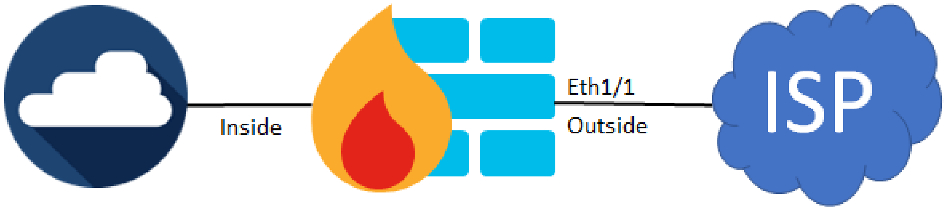


```
        ------------------ show interface ------------------

        Interface Internal-Data0/1 "", is up, line protocol is up
          Hardware is , BW 10000 Mbps, DLY 10 usec
        (Full-duplex), (10000 Mbps)
        Input flow control is unsupported, output flow control is unsupported
        MAC address 000f.b748.4801, MTU not set
        IP address unassigned
        30704186 packets input, 9356355772 bytes, 15257819 no buffer
        Received 11454 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 54191 overrun, 0 ignored, 0 abort
```

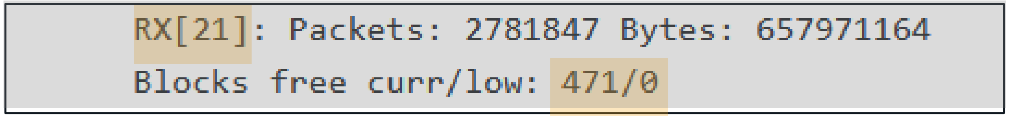
No buffer/overruns increase only when ISP router is reloaded and during the next 5-20 minutes even if the router is up.

$$\frac{15257819 \text{ no buffer}}{30704186 \text{ packets input} + 15257819 \text{ no buffer}} \quad \text{~33\%}$$

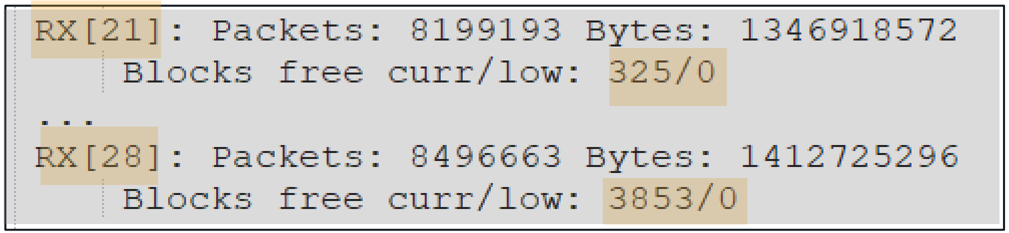
Analysis of Existing Data



Interface/throughput stats: RX21 always has low=0, RX28 - frequently, but not always.
Conn stats → nothing special



```
        RX[21]: Packets: 2781847 Bytes: 657971164
        Blocks free curr/low: 471/0
```

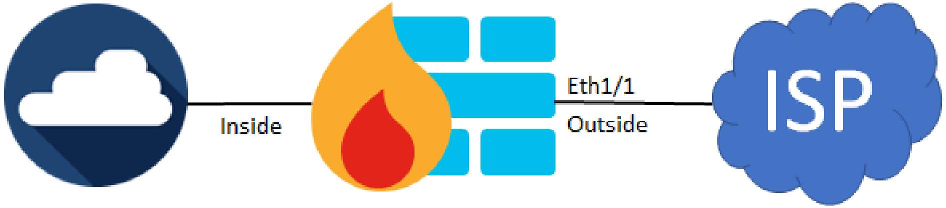


```
RX[21]: Packets: 8199193 Bytes: 1346918572
    Blocks free curr/low: 325/0
...
RX[28]: Packets: 8496663 Bytes: 1412725296
    Blocks free curr/low: 3853/0
```

Preliminary Case Study Conclusion

- Symptoms can be explained by significant increase in packet drops due to **no buffer/overruns** (potentially caused by CPU hogs/high CPU utilization)**.**
- Based on input/output rate, a routing loop is suspected.
- Based on **minimal** change in resources (conn/conn rate/perfmon etc.), connection table analysis, **connection per second (CPS)** is not the problem. No evidence that **through-the-box** connections are the trigger.
- Based on **low=0** only on specific RX rings, a limited set of conns with high PPS rate are suspected.
- Overall, mainly due to lack of captures and syslogs, existing data is not sufficient for RCA.

Next Step



- Schedule Maintenance window to reproduce the issue.
- Compare output between working and non-working scenario.
- Ensure you have SSH and Console access to FTD.
- Configure/Increase logging buffer.
- Collect the following outputs

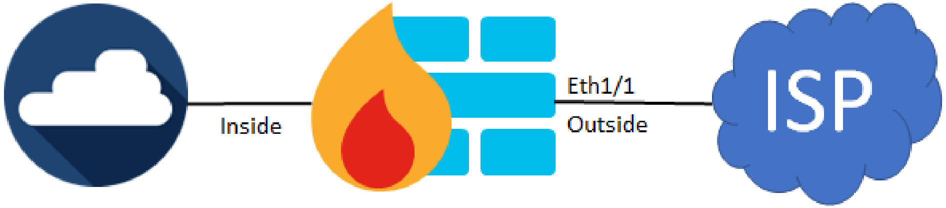
```
Show clock
Clear asp drop
Clear asp event dp-cp
Clear arp statistics
Clear traffic
Clear service policy
Clear process cpu-hog
Clear logging buffer
Clear interface
Terminal pager 24
```

```
Cap capin interface inside headers-only buffer 10000000
Cap capout interface outside headers-only max 10000000
Show conn detail
Show route
Show asp table routing
show asp drops
Show logging buffer
Show traffic
Show interface
Show service policy
Show process cpu-hog
```

Export capture as pcap

Analysis of Collected Data

Buffer logs



High rate of syslogs **106016** indicating receipt of spoofed packets:

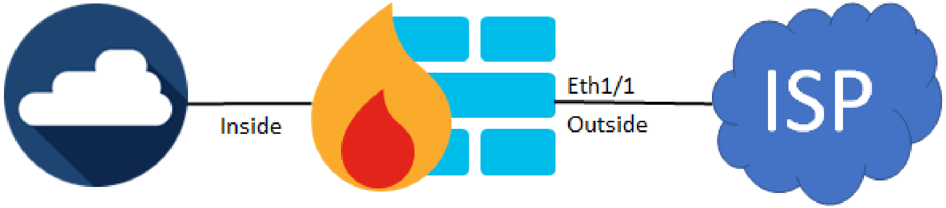
```
%FTD-session-2-106016: Deny IP spoof from (10.103.55.11) to 192.168.25.12 on interface INSIDE
%FTD-session-2-106016: Deny IP spoof from (10.103.55.11) to 192.168.25.13 on interface INSIDE
%FTD-session-2-106016: Deny IP spoof from (10.103.55.11) to 192.168.25.12 on interface INSIDE
%FTD-session-2-106016: Deny IP spoof from (10.103.55.11) to 192.168.25.13 on interface INSIDE
%FTD-session-2-106016: Deny IP spoof from (10.103.55.11) to 192.168.25.12 on interface INSIDE
%FTD-session-2-106016: Deny IP spoof from (10.103.55.11) to 192.168.25.13 on interface INSIDE
%FTD-session-2-106016: Deny IP spoof from (10.103.55.11) to 192.168.25.12 on interface INSIDE
```

```
Interface Port-channel8.3002 "INSIDE", is up, line protocol is up
IP address 10.103.55.11, subnet mask 255.255.255.248
```

```
logging host INSIDE 192.168.25.12
logging host INSIDE 192.168.25.13
logging host INSIDE 172.16.193.33
logging host INSIDE 10.52.0.127
```

Analysis of Collected Data

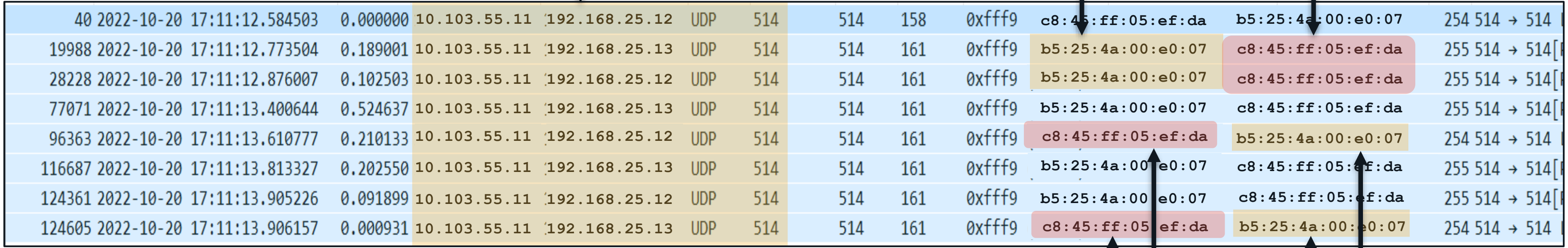
Captures



Firewall to Syslog Server

Firewall MAC Address (Source)

Peer MAC Address (Destination)

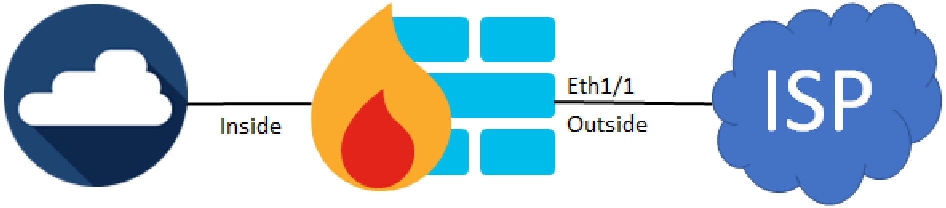


```
    40 2022-10-20 17:11:12.584503  0.000000 10.103.55.11  192.168.25.12 UDP 514  514 158 0xfff9 c8:45:ff:05:ef:da b5:25:4a:00:e0:07 254 514 → 514
 19988 2022-10-20 17:11:12.773504  0.189001 10.103.55.11  192.168.25.13 UDP 514  514 161 0xfff9 b5:25:4a:00:e0:07 c8:45:ff:05:ef:da 255 514 → 514[
 28228 2022-10-20 17:11:12.876007  0.102503 10.103.55.11  192.168.25.12 UDP 514  514 161 0xfff9 b5:25:4a:00:e0:07 c8:45:ff:05:ef:da 255 514 → 514[
 77071 2022-10-20 17:11:13.400644  0.524637 10.103.55.11  192.168.25.13 UDP 514  514 161 0xfff9 b5:25:4a:00:e0:07 c8:45:ff:05:ef:da 255 514 → 514[
 96363 2022-10-20 17:11:13.610777  0.210133 10.103.55.11  192.168.25.12 UDP 514  514 161 0xfff9 c8:45:ff:05:ef:da b5:25:4a:00:e0:07 254 514 → 514
116687 2022-10-20 17:11:13.813327  0.202550 10.103.55.11  192.168.25.13 UDP 514  514 161 0xfff9 b5:25:4a:00:e0:07 c8:45:ff:05:ef:da 255 514 → 514[
124361 2022-10-20 17:11:13.905226  0.091899 10.103.55.11  192.168.25.12 UDP 514  514 161 0xfff9 b5:25:4a:00:e0:07 c8:45:ff:05:ef:da 255 514 → 514[
124605 2022-10-20 17:11:13.906157  0.000931 10.103.55.11  192.168.25.13 UDP 514  514 161 0xfff9 c8:45:ff:05:ef:da b5:25:4a:00:e0:07 254 514 → 514
```

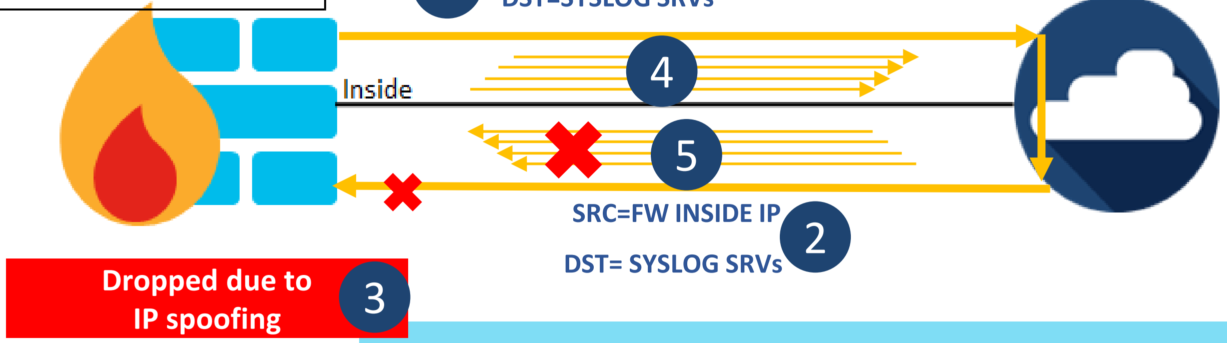
Peer MAC Address (Source)

Firewall MAC address (Destination)

Analysis of Collected Data



```
logging host INSIDE 192.168.25.12
logging host INSIDE 192.168.25.13
logging host INSIDE 172.16.193.33
logging host INSIDE 10.52.0.127
```

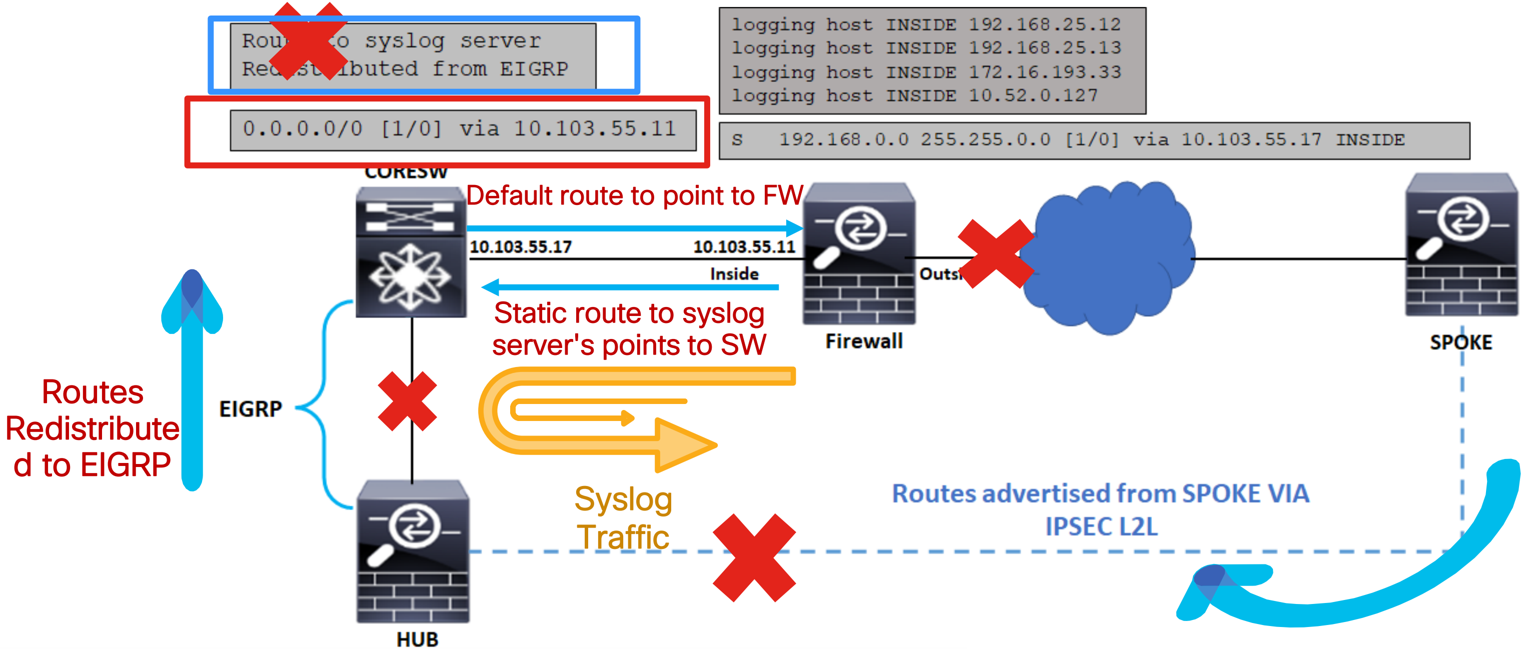


1. FTD sends log to each syslog server.
2. Upstream device sends syslog packet back to FTD.
3. Self-originated packets are considered as spoofed and dropped. 106016 is generated.
4. For each syslog 106016 FTD generates new syslogs to 4 destinations.
5. Repeat #2-#4.

Analysis of Collected Data

Inside
Eth1/1
Outside
ISP

Q: Why FTD receives self-originated packets on inside interface?



```
~~Route to syslog server~~
~~Redistributed from EIGRP~~
```

```
0.0.0.0/0 [1/0] via 10.103.55.11
```

```
logging host INSIDE 192.168.25.12
logging host INSIDE 192.168.25.13
logging host INSIDE 172.16.193.33
logging host INSIDE 10.52.0.127
```

```
S   192.168.0.0 255.255.0.0 [1/0] via 10.103.55.17 INSIDE
```

CORESW
Default route to point to FW
10.103.55.17
10.103.55.11
Inside
Outsi
Firewall
SPOKE
Static route to syslog server's points to SW
Routes Redistributed to EIGRP
EIGRP
Syslog Traffic
Routes advertised from SPOKE VIA IPSEC L2L
HUB

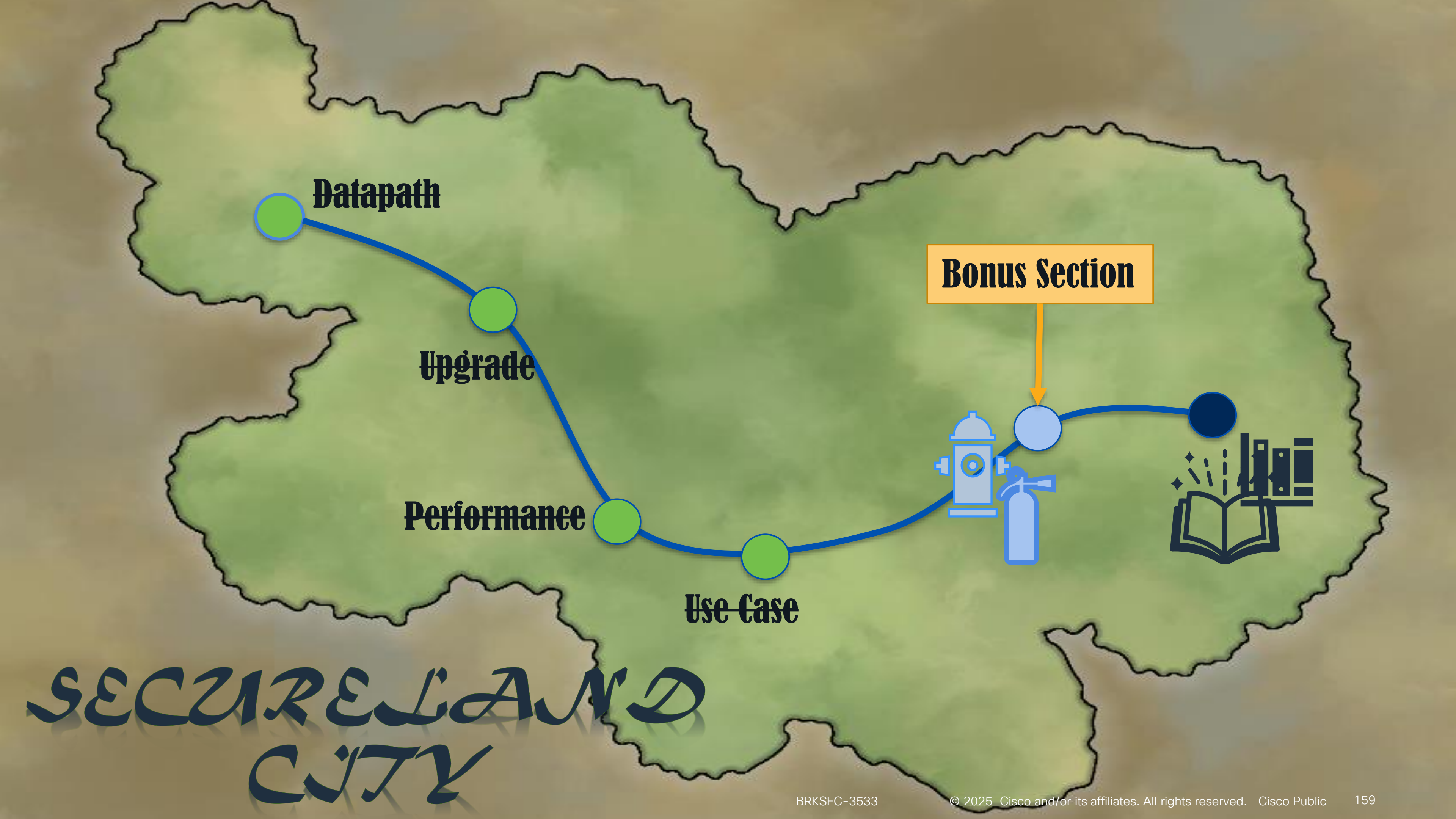
Not a routing loop!

Suboptimal routing on peer + lack of rate limit 106016 on Firewall

Case Study Final Conclusion

For your reference

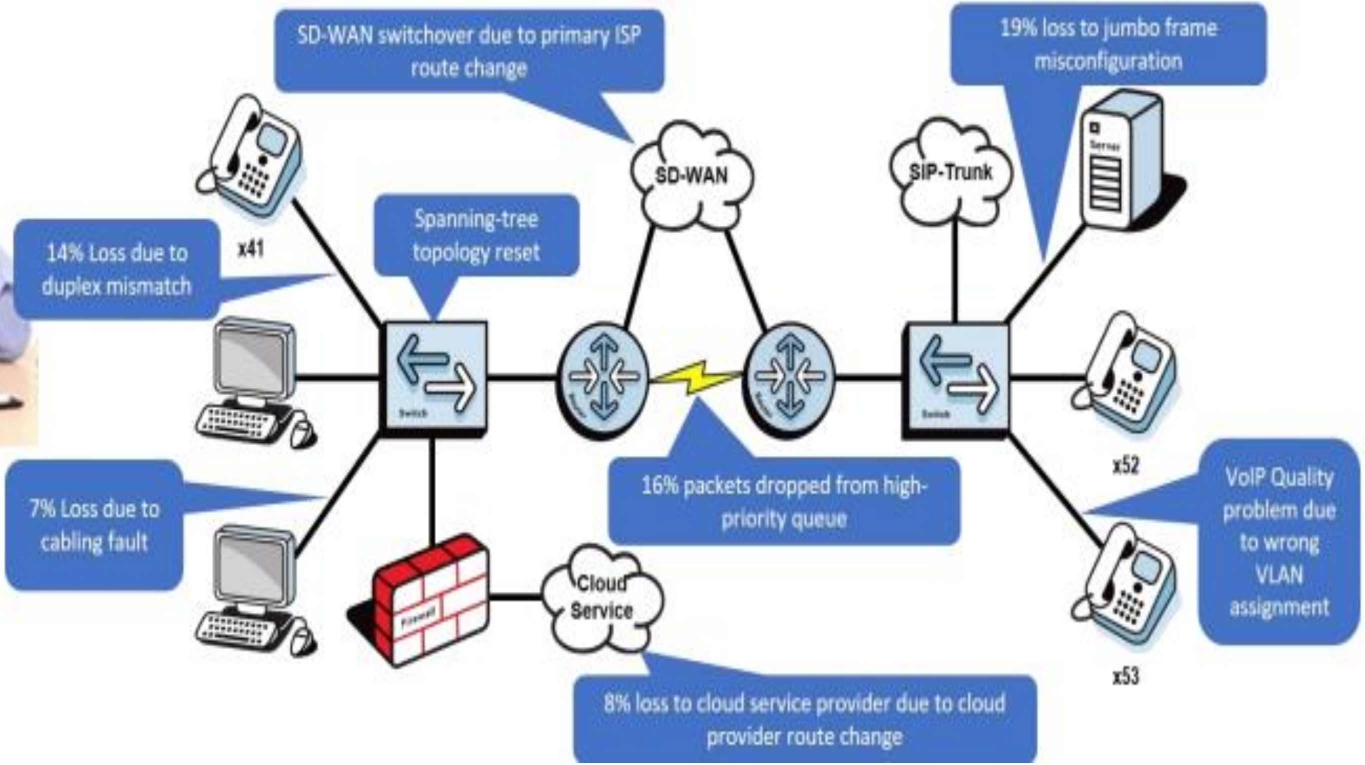
- When ISP router is reloaded, Eth1/1 is down and routing on customer devices changes.
- Peer device sends FTD **self-originated** syslog packets back FTD.
- Each received FTD **self-originated** packet is dropped due to IP spoofing and **106016** syslog is generated.
- For each dropped packets due to IP spoofing, a new syslog is generated and send to **4** syslog servers.
- Peer device sends these packets back to FTD > Exponential growth in TX/RX rate > CPU hogs > drops due to no buffer.
- Eth1/1 goes up > due to major packet loss DMVPN conn re-establishment takes longer time (5-20 minutes).
- While Eth1/1 is UP and DMVPN is DOWN, no change in routing.
- At some point DMVPN becomes up, routing is re-converged, peer device receives routes to syslog servers via EIGRP/DMVPN.
- Don’t always rely on logs from external syslog server
- Not a routing loop.
- Main RC: Suboptimal routing on peer + lack of rate limit syslog for 106016.
- Workaround: Apply rate limit for 106016.


~~Datapath~~
~~Upgrade~~
~~Performance~~
~~Use Case~~
Bonus Section
SECURELAND CITY

Cisco RADKit

(Remote Automation Development Kit)

How painful is this?



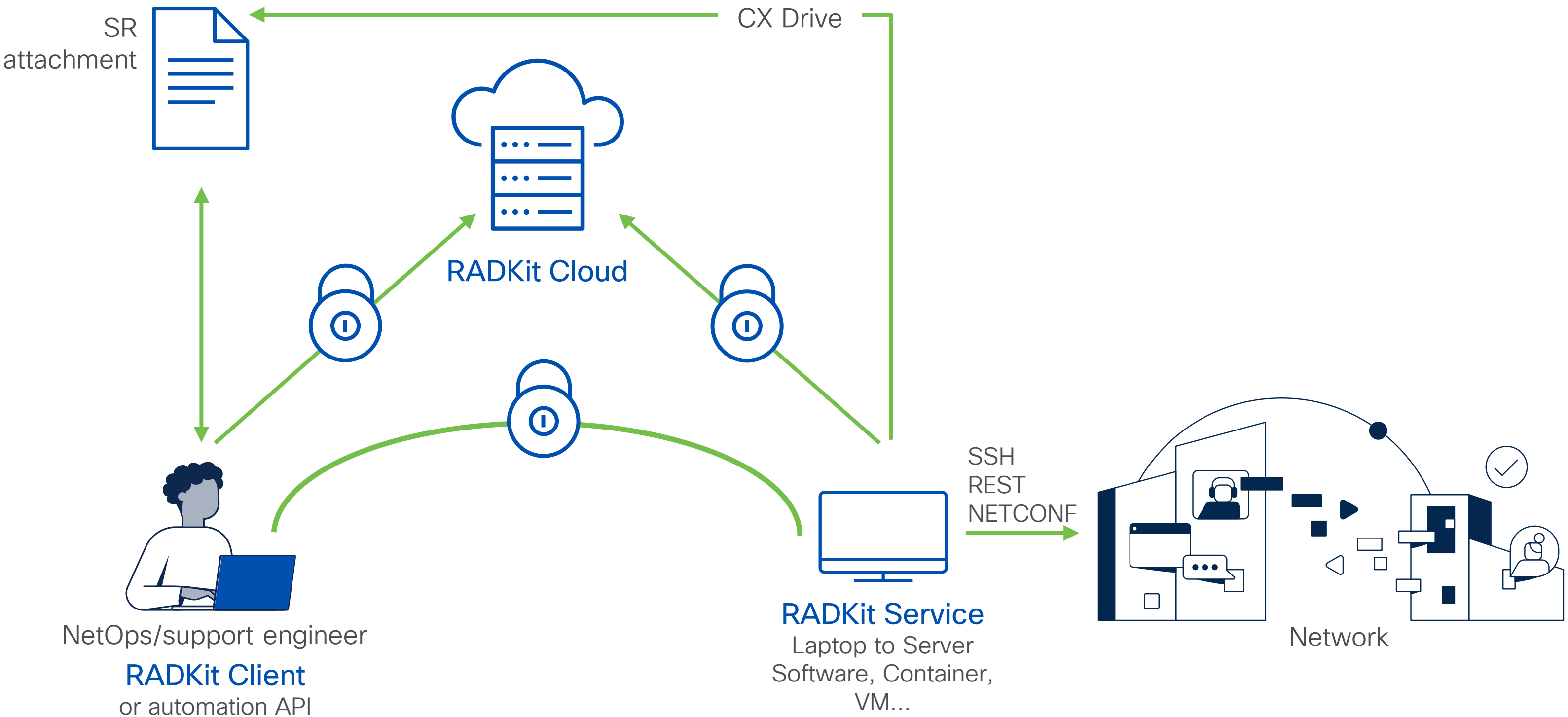
SD-WAN switchover due to primary ISP route change
19% loss to jumbo frame misconfiguration
SD-WAN
SIP-Trunk
Server
x41
14% Loss due to duplex mismatch
Spanning-tree topology reset
Switch
16% packets dropped from high-priority queue
x52
VoIP Quality problem due to wrong VLAN assignment
7% Loss due to cabling fault
Firewall
Cloud Service
x53
8% loss to cloud service provider due to cloud provider route change

Why RADkit?

- Screensharing, Ping-Pong emails.
- Long hours watching the troubleshooter.
- Travel to customer/site might be needed
- Multi-device data collection is tedious.
- Frequent data collection can be frustrating
- Automation is complex

RADKit Architecture – Client-Service

Cisco Remote Automation Development Kit (RADKit)



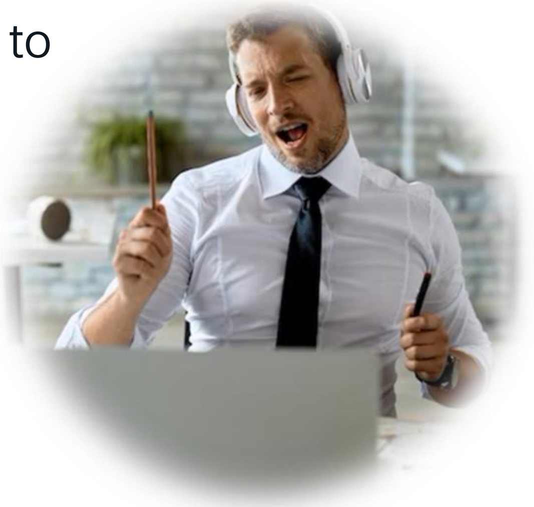
What is RADKit?

- Interactively or programmatically manage remote equipment terminals, WebUI’s, desktops or APIs.

- Customers may grant access to their devices inventory to individual users, for example: TAC engineers.

- Full **authentication, authorization, access-control and encryption**.

- **Collect** data, monitor, troubleshoot, **download, upload** or even connect to **CLI.**



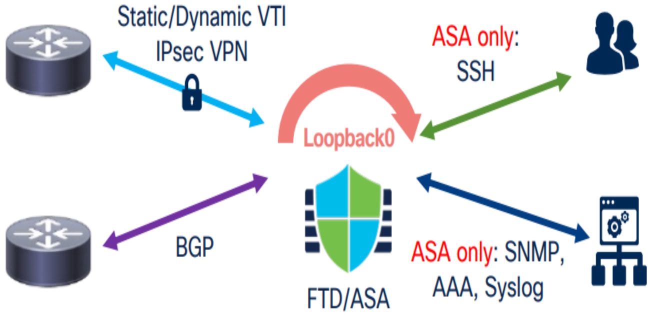
- Efficiently automate frequent or complex tasks with network-wide API’s.

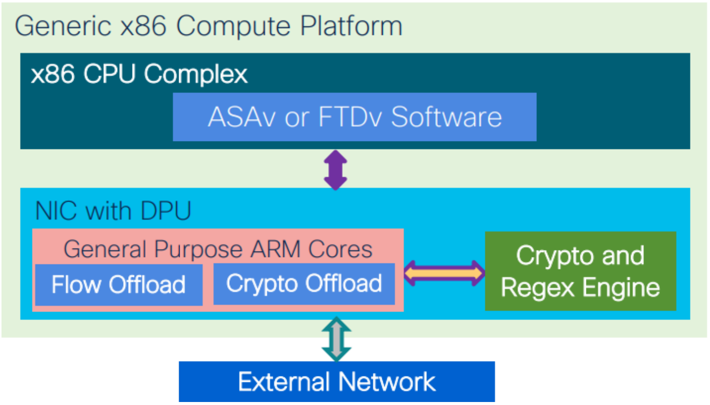
~~Datapath~~
~~Upgrade~~
~~Performance~~
~~Use Case~~
You are here
Mission Accomplished!
SECURELAND CITY

Latest on Cisco Secure Firewall?

BRKSEC-2236

Keeping Up on Network Security with Cisco Secure Firewall





https://www.ciscolive.com/on-demand/on-demand-library.html?zid=pp&search=BRKSEC-2236#/session/1670019638549001n8Eh

Wrap-up

Wrap-Up : What did you Learn?

- Utilize the available troubleshooting tools to isolate if connectivity issues are caused by the Firewall.
- Determine if there are oversubscription and troubleshoot performance issues.
- Upgrade failure troubleshooting.
- A well described problem statement can lead to a faster case resolution.
- Take outputs before and when issue happens and compare between working and none working scenarios.
- Try to collect as many of the command outputs possible before contacting Cisco TAC and **before rebooting the device**.

Call to Action

Download the PDF version of the session to check the hidden slides.

Visit the On-Demand Library for more sessions at ciscolive.com/on-demand.

Check the reference section for further information and details.

Test in lab and have fun!

Webex App

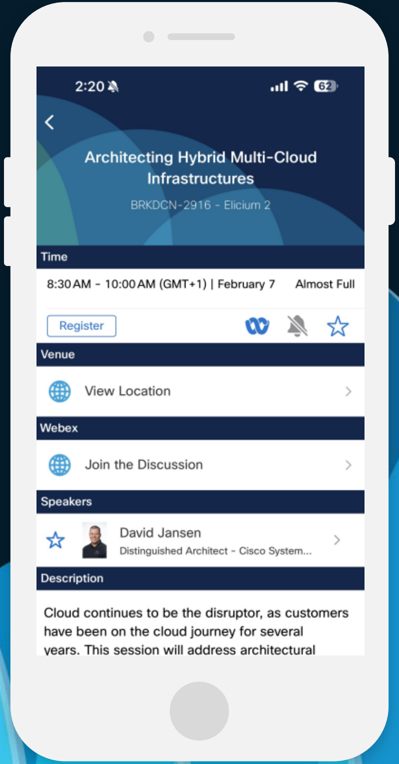
Questions?

Use the Webex app 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 the Webex app or go directly to the Webex space
4. Enter messages/questions in the Webex space

Webex spaces will be moderated by the speaker until February 28, 2025.



2:20

Architecting Hybrid Multi-Cloud Infrastructures

BRKDCN-2916 - Elicium 2

Time

8:30 AM - 10:00 AM (GMT+1) | February 7 Almost Full

Register

Venue

View Location

Webex

Join the Discussion

Speakers

David Jansen
Distinguished Architect - Cisco System...

Description

Cloud continues to be the disruptor, as customers have been on the cloud journey for several years. This session will address architectural

cisco Live!

Fill Out Your Session Surveys

Participants who fill out a minimum of 4 session surveys and the overall event survey will get a unique Cisco Live t-shirt.

(from 11:30 on Thursday, while supplies last)

All surveys can be taken in the Cisco Events mobile app or by logging in to the Session Catalog and clicking the 'Participant Dashboard'

Content Catalog

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 ciscolive.com/on-demand. Sessions from this event will be available from March 3.

Contact me at: ghijazi@cisco.com

Join our Security Research Community

Participating in design research gives you a place to share your thoughts and experiences to influence the future of Cisco Security Products.

Security

Network Security

Learn about a broad range of solution and technologies which will help you better understand how to secure your network. You will find topics such as FTD, VPN, SASE, Meraki Security Policies and Network Analytics.

START

Monday, February 10 | 2:00 p.m.
BRKSEC-2708
Cisco SDWAN Use Cases & Best Practices

Tuesday, February 11 | 8:00 a.m.
BRKSEC-2057
Secure Connectivity Anywhere - The Evolution of Cisco Remote Access Technologies

Tuesday, February 11 | 12:00 p.m.
BRKSEC-2236
Keeping Up on Network Security with Cisco Secure Firewall

Tuesday, February 11 | 4:00 p.m.
BRKIOT-2882
Implementing Segmentation in Industrial Networks

Wednesday, February 12 | 9:30 a.m.
BRKSEC-2708
Cisco SDWAN Use Cases & Best Practices

Wednesday, February 12 | 1:00 p.m.
BRKSEC-3274
TAC and Engineering on Cisco Secure Firewall Threat Detection Performance - Performance Profiling tools, Tuning and Best Practices

Wednesday, February 12 | 5:00 p.m.
BRKSEC-2239
Cisco Secure Firewall Platforms Deep Dive

Thursday, February 13 | 8:30 a.m.
BRKSEC-3320
Pig-in-the-Middle - TLS Decryption and Encrypted Visibility Engine Deep Dive on Cisco Secure Firewall

Thursday, February 13 | 10:45 a.m.
BRKSEC-3935
Think Like a TAC Engineer: Troubleshooting Secure Client Remote Access Issues

Thursday, February 13 | 1:00 p.m.
BRKSEC-2821
Securing Industrial Networks: Strategies and Best Practices

Friday, February 14 | 9:15 a.m.
BRKSEC-3533
Think Like a TAC Engineer: A Guide to Cisco Secure Firewall most Common Pain Points

FINISH

Friday, February 14 | 11:15 a.m.
BRKSEC-2086
Optimizing Security and Agility: Leveraging SD-WAN Capabilities in Cisco Secure Firewall

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

> *“A problem well put is half solved.”*
>
> John Dewey

References

References

- Clarify Firepower Threat Defense Access Control Policy Rule Actions https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/212321-clarify-the-firepower-threat-defense-acc.html
- Use Firepower Threat Defense Captures and Packet Tracer https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/212474-working-with-firepower-threat-defense-f.html
- Cisco Secure Firewall Configuration Guide https://www.cisco.com/c/en/us/support/security/firepower-ngfw/products-installation-and-configuration-guides-list.html
- Firepower Management Center Configuration Guide https://www.cisco.com/c/en/us/td/docs/security/firepower/70/configuration/guide/fpmc-config-guide-v70.html

References

- Process Single Stream Large Session (Elephant Flow) by Firepower Services
https://www.cisco.com/c/en/us/support/docs/security/firepower-management-center/200420-Processing-of-Single-Stream-Large-Sessio.html
- Elephant Flow Detection
https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/management-center/device-config/720/management-center-device-config-72/elephant-flow.html
- ASA 8.3 and Later: Monitor and Troubleshoot Performance Issues
https://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/113185-asaperformance.html
- Troubleshooting Secure Firewall Upgrade Issues
https://www.cisco.com/c/dam/en/us/products/se/2022/10/SC_Ops/EMEA_TAC_Security_Workshop_Monday_10th_Oct_2022_Secure_Firewall_2_of_4_.pdf

References

- Secure Firewall 3100 Troubleshooting: https://www.cisco.com/c/dam/en/us/products/se/2022/10/SC_Ops/EMEA_TAC_Security_Workshop_Monday_10th_Oct_2022_Secure_Firewall_1_of_4_.pdf
- Troubleshooting Registration Issues Between FMC and Firepower Devices:
- https://www.cisco.com/c/dam/en/us/products/se/2022/10/SC_Ops/EMEA_TAC_Security_Workshop_Monday_10th_Oct_2022_Secure_Firewall_4_of_4_.pdf
- Radkit Documentation:

https://radkit.cisco.com/docs/pages/links.html

Thank you

GO **BEYOND**