
cisco Live!
Let's go

The bridge to possible

Think Like a TAC Engineer

A guide to Cisco Secure Firewall most common pain points

Ghada Hijazi, Technical Consulting Engineer

“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

- Escalation Engineer CX Security TAC
- 6 Years experience in Firewall TAC
- Currently working in Professional Services

SNORT®

CISCO CERTIFIED CCNP SECURITY

Agenda

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

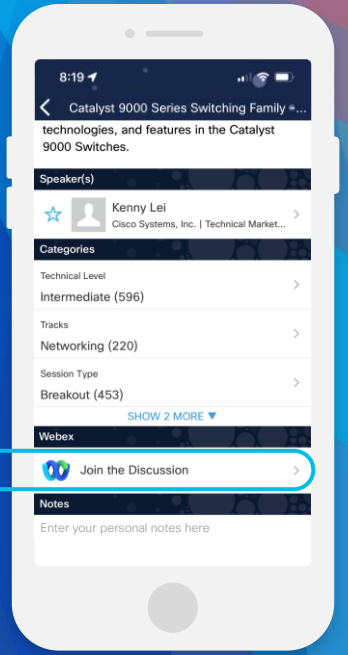
Questions?

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

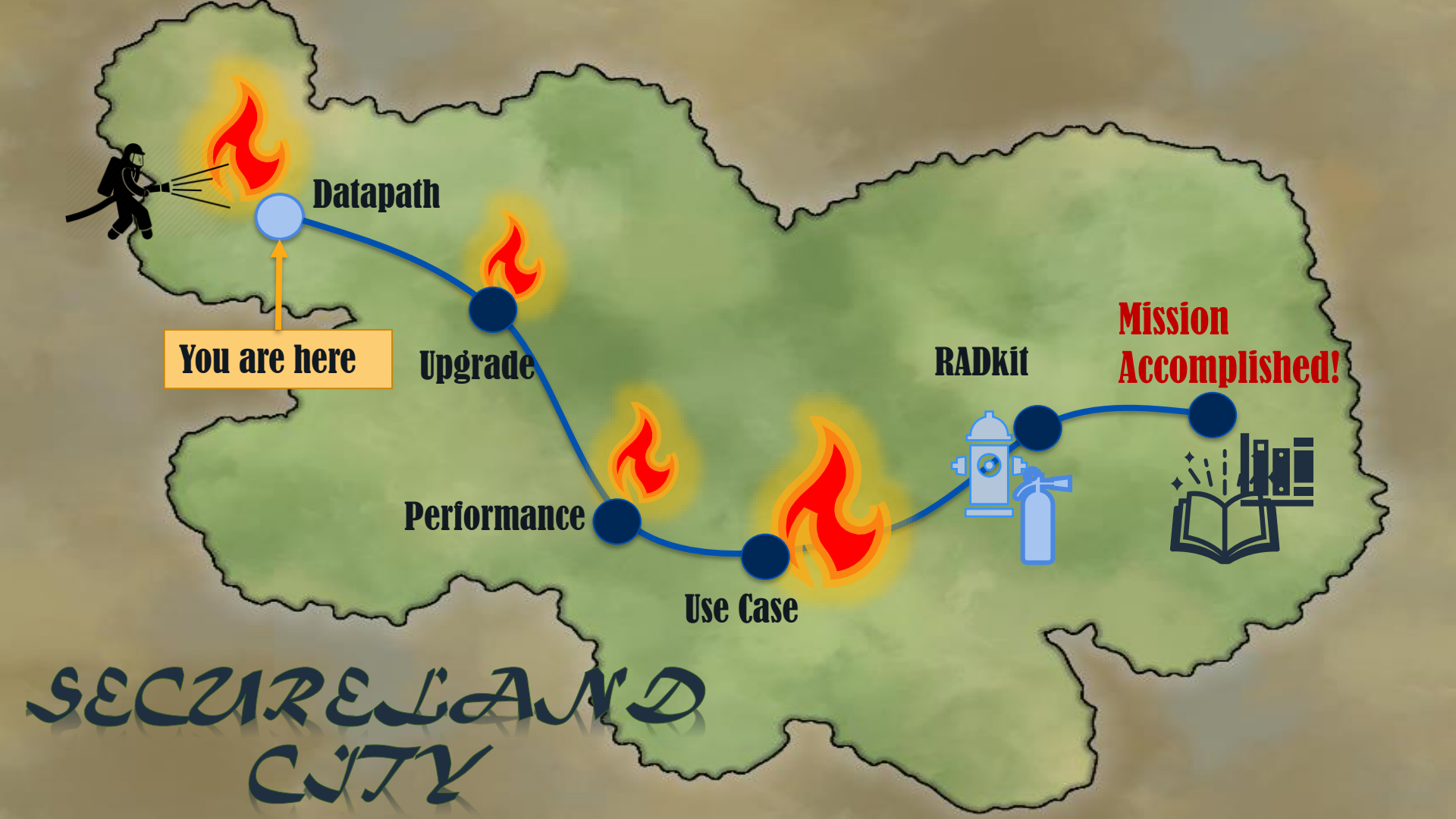
How

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 23, 2024.



https://ciscolive.ciscoevents.com/ciscolivebot/#BRKSEC-3533

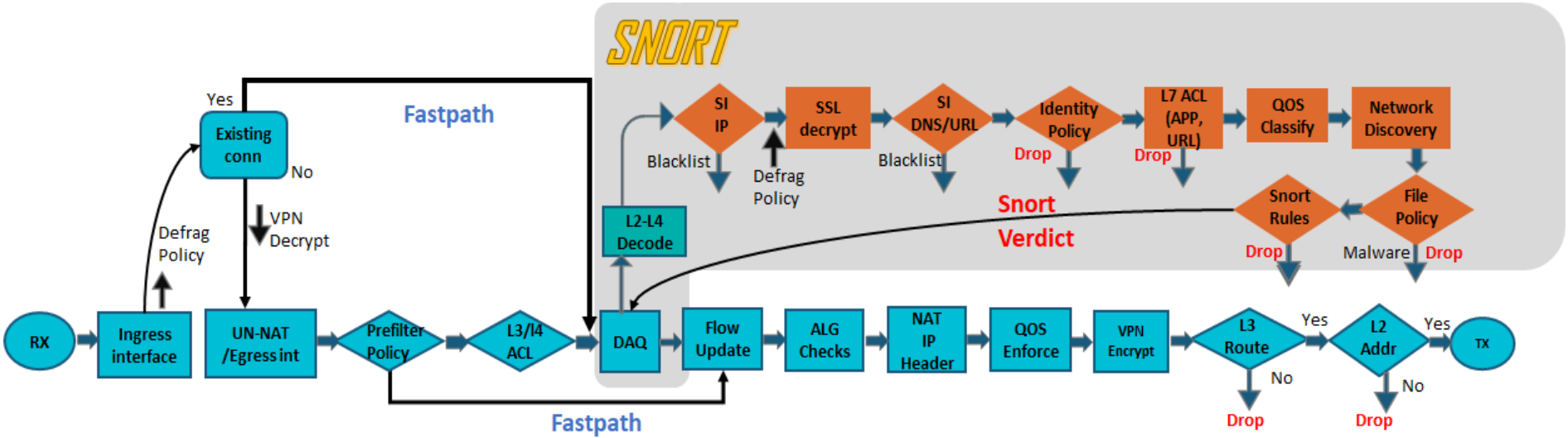

Datapath
You are here
Upgrade
Performance
Use Case
RADkit
Mission Accomplished!
SECURELAND CITY

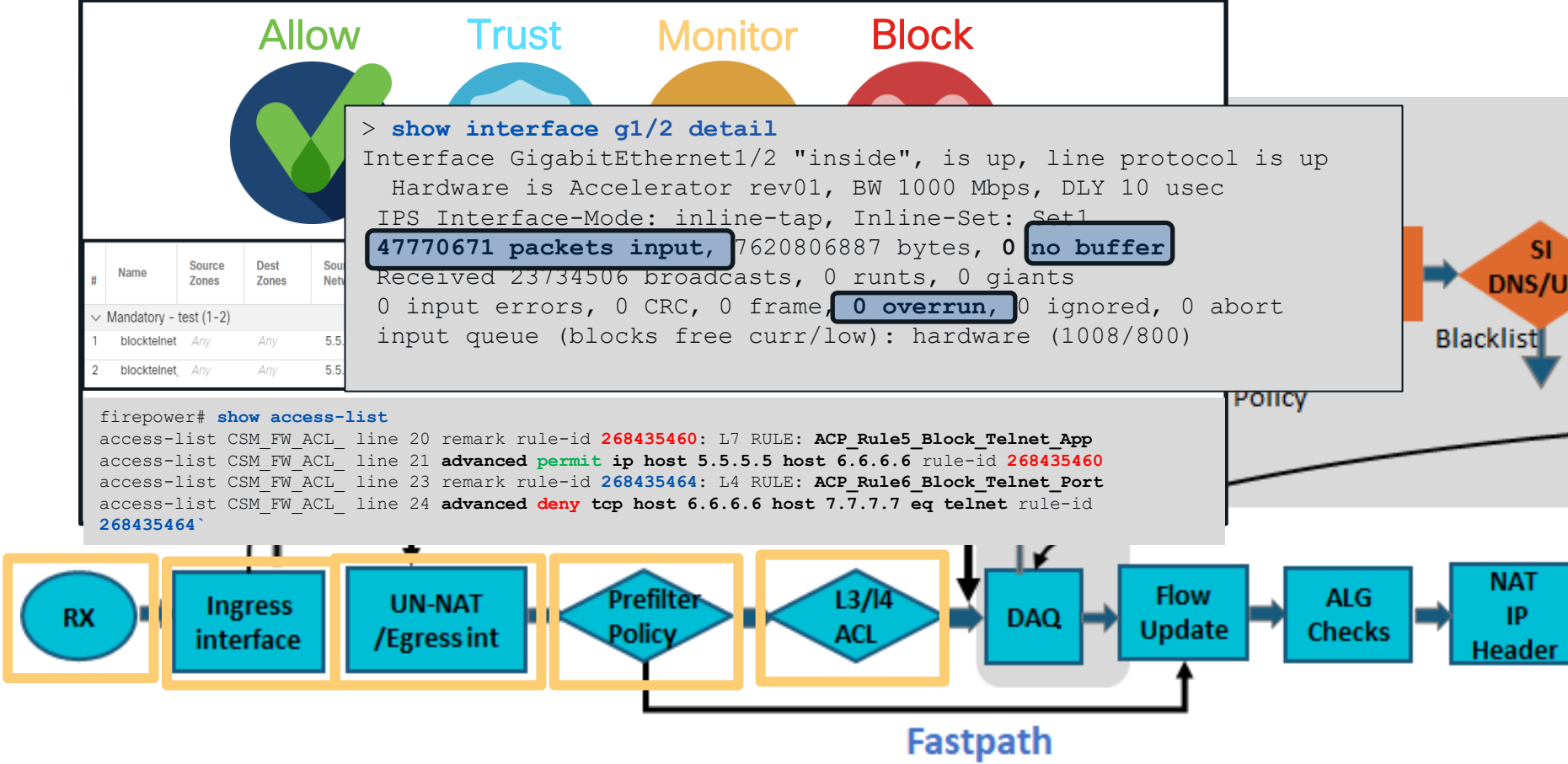
Datapath/Connectivity Issues

Secure Firewall Packet Processing – The Big Picture

Lina Engine

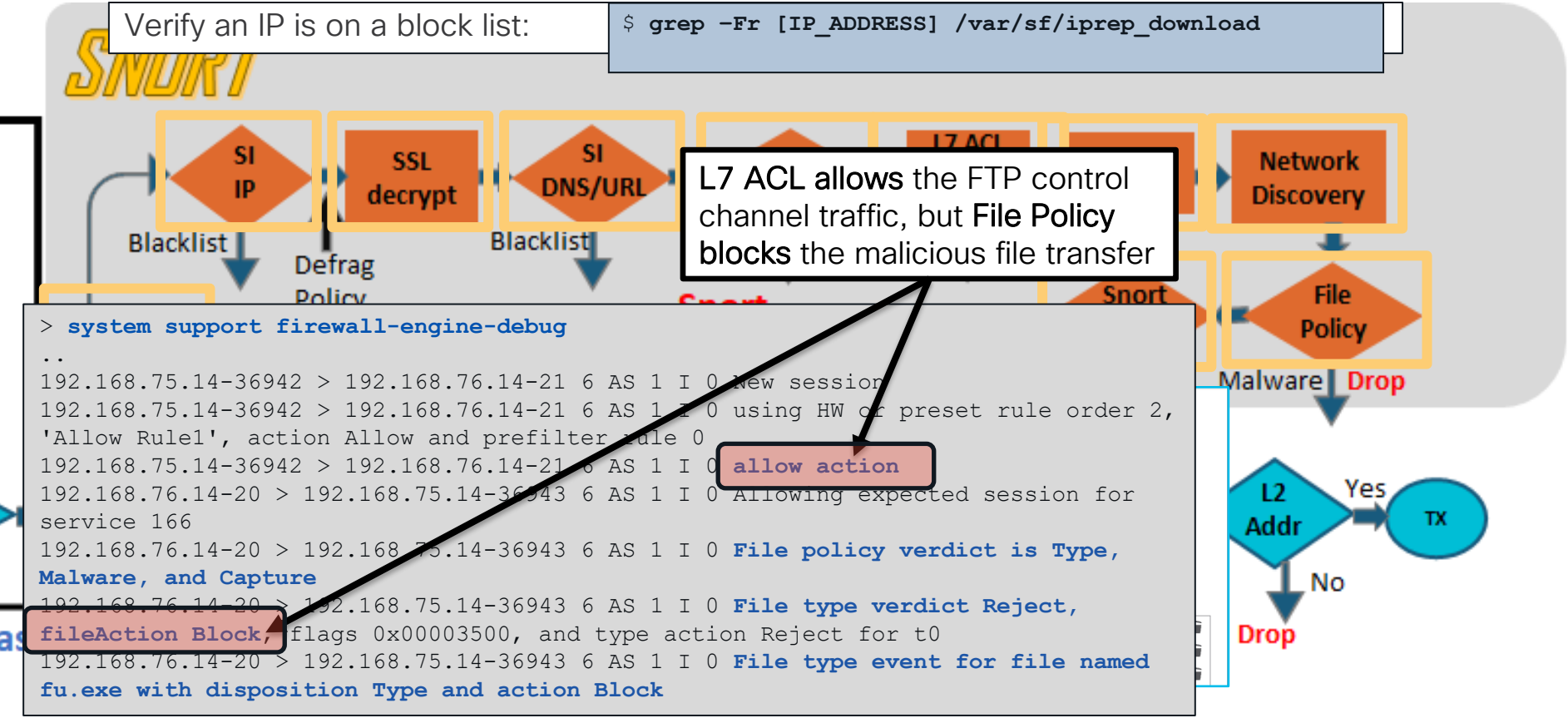
Snort Engine





Verify an IP is on a block list:

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



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

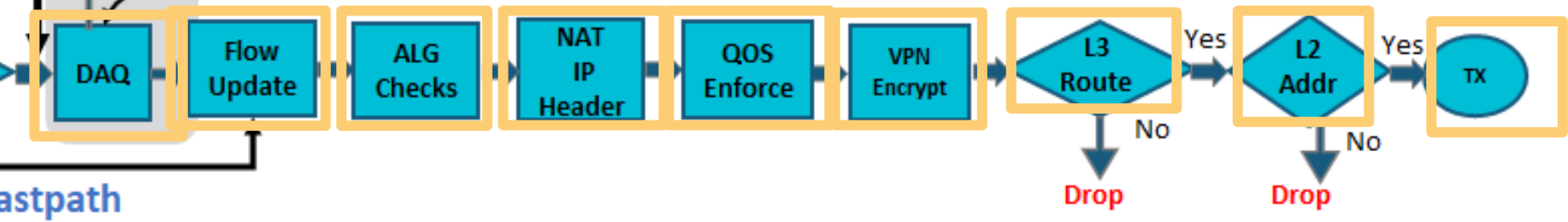
```
> system support firewall-engine-debug
..
192.168.75.14-36942 > 192.168.76.14-21 6 AS 1 I 0 New session
192.168.75.14-36942 > 192.168.76.14-21 6 AS 1 I 0 using HW or preset rule order 2,
'Allow Rule1', action Allow and prefilter rule 0
192.168.75.14-36942 > 192.168.76.14-21 6 AS 1 I 0 allow action
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
```

```
> 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)
```

```
> 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
```

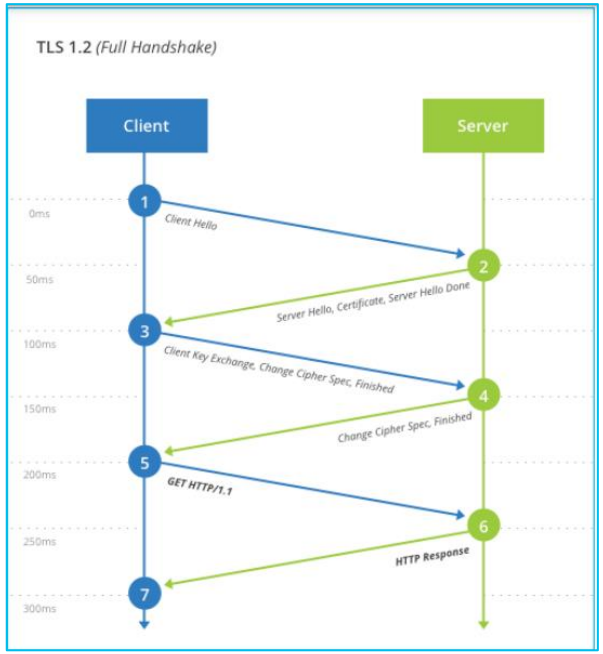
```
.77.40: icmp:
Phase: 16
4980 hits 140
```



Want more on SSL Decryption?

BRKSEC-3320

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

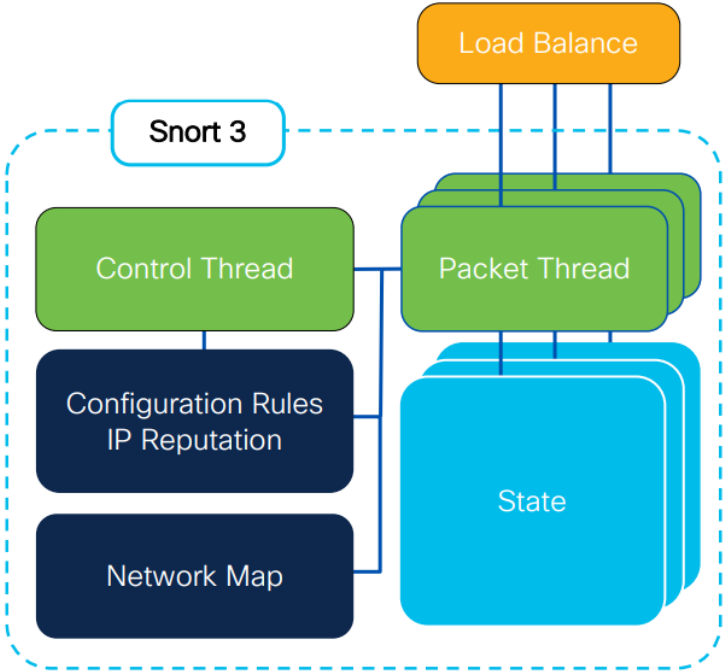


cisco Live!

More on Snort3?

BRKSEC-2484

Snort 3 with the Cisco Secure Firewall

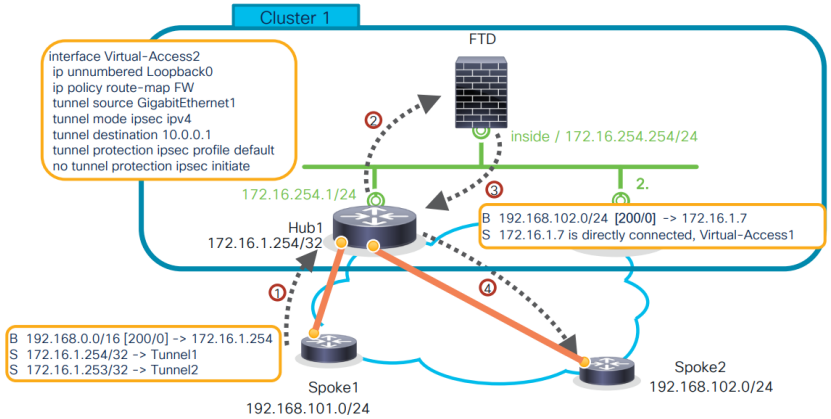


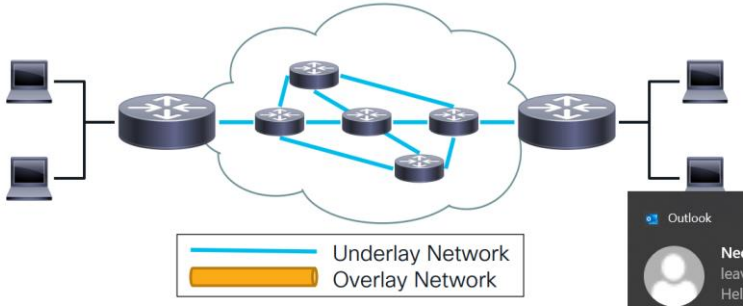
https://www.ciscolive.com/on-demand/on-demand-library.html?search=BRKSEC-2484#/session/1675722392971001tVHi

More on VPN with Cisco Secure Firewall?

BRKSEC-3058

Route based VPNs with Cisco Secure Firewall





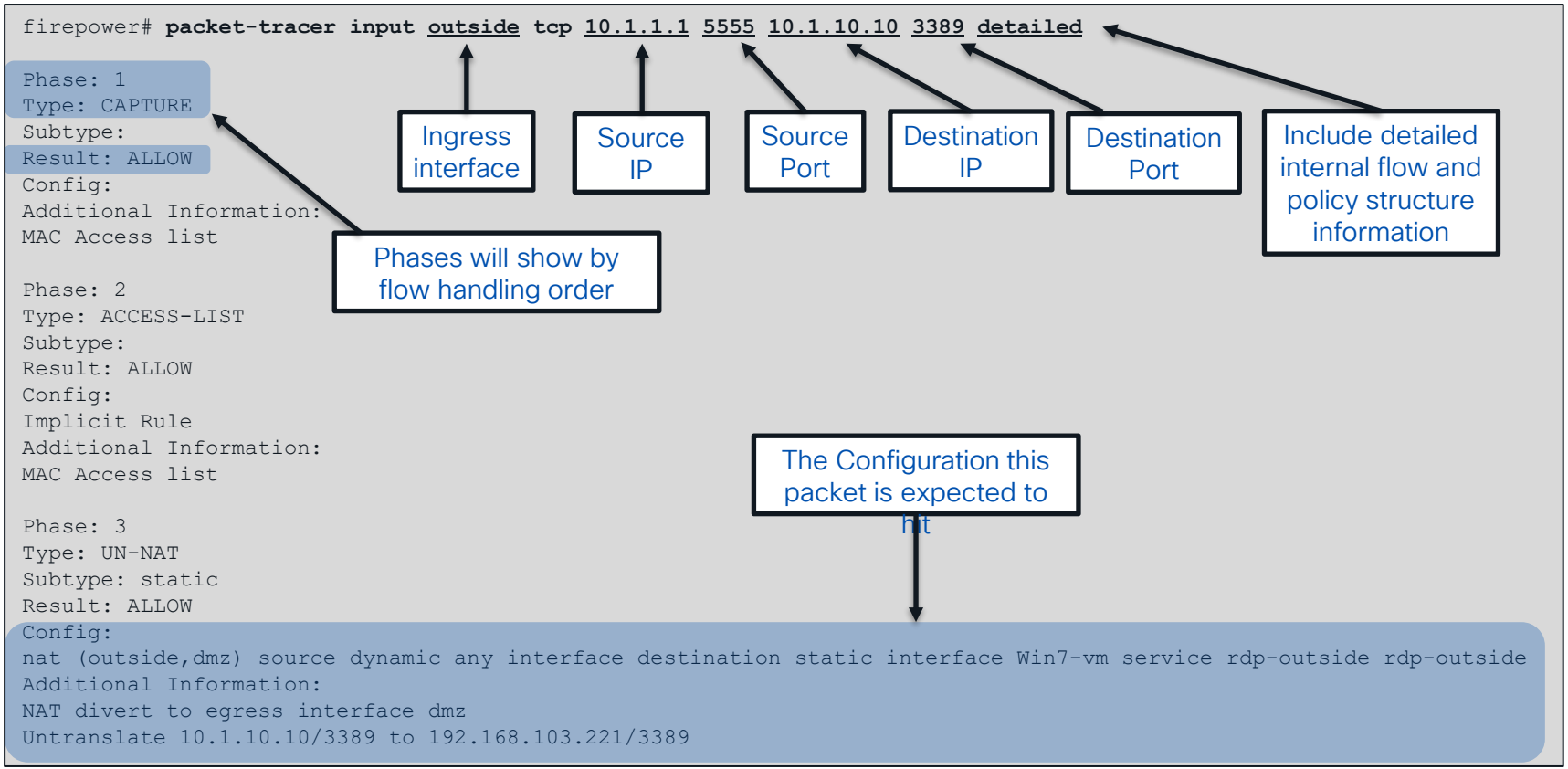
https://www.ciscolive.com/on-demand/on-demand-library.html?search=BRKSEC-3058#/session/1675722394754001t2R3

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

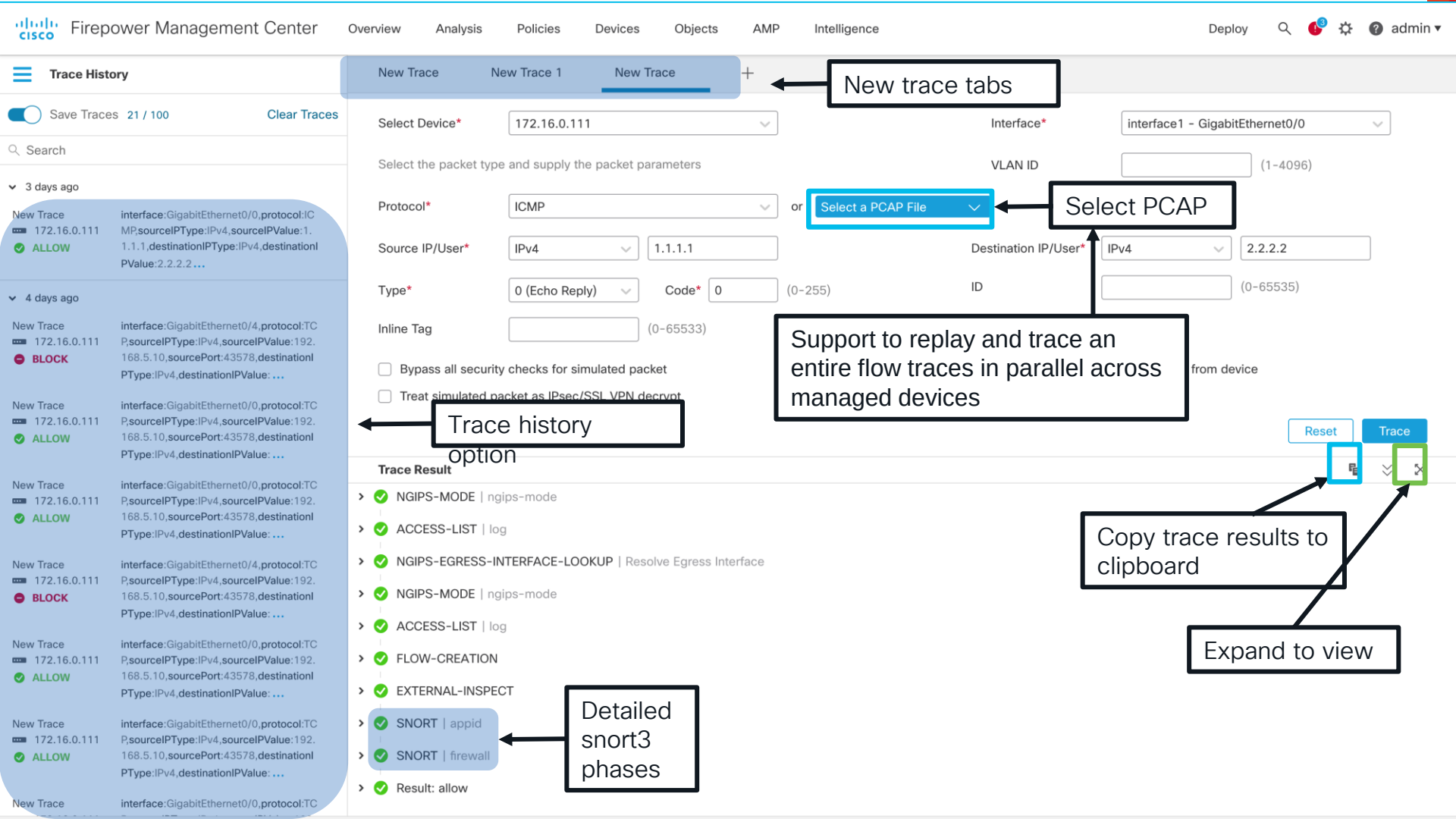
Note:
Troubleshooting file/show tech need to be collected before rebooting the device.

Packet Tracer

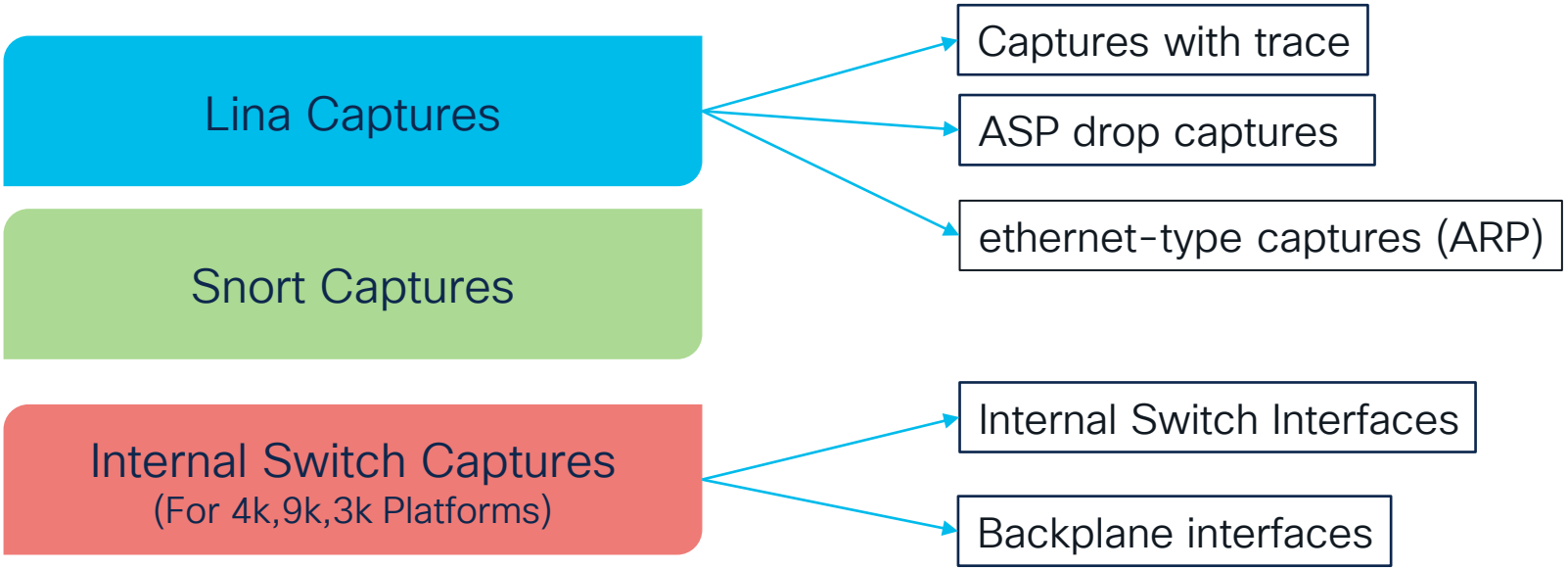


Packet Tracer Sample Output

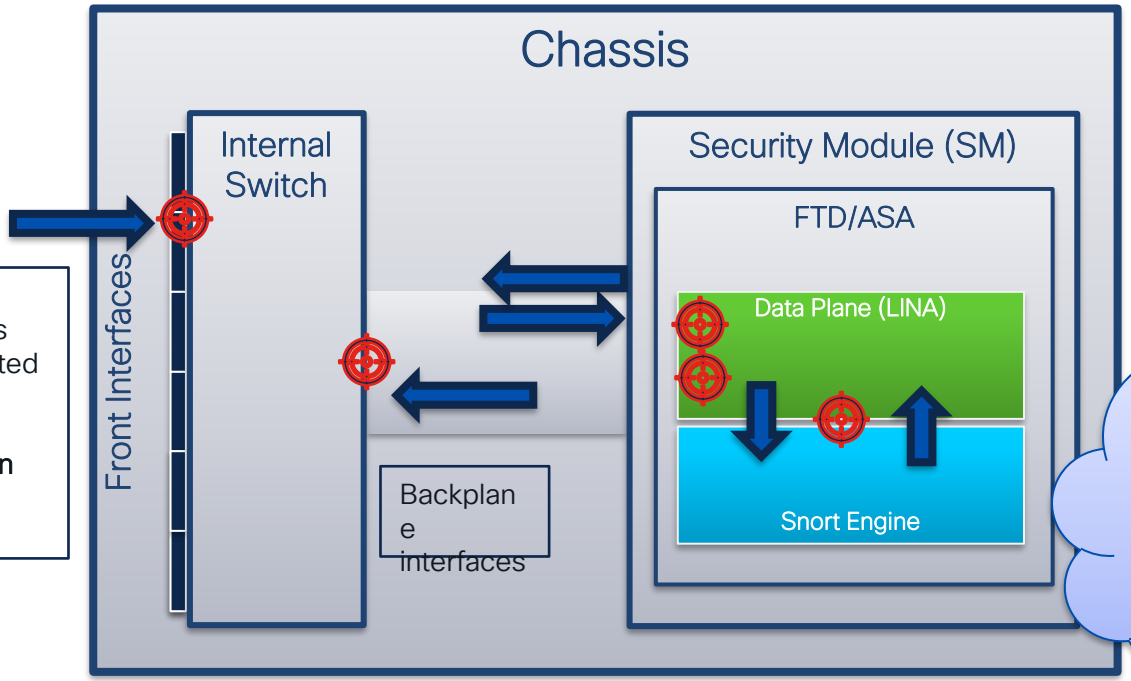
```
Phase: 4
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group outside_in in interface outside
access-list outside_in extended permit tcp any any eq 3389
Additional Information:
……
Phase: 12
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with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


Firepower Management Center
Overview
Analysis
Policies
Devices
Objects
AMP
Intelligence
Deploy
admin
Trace History
Save Traces 21 / 100
Clear Traces
Search
3 days ago
4 days ago
New Trace
172.16.0.111
ALLOW
BLOCK
New Trace
New Trace 1
New Trace
New trace tabs
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
from device
Support to replay and trace an entire flow traces in parallel across managed devices
Trace history option
Reset
Trace
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

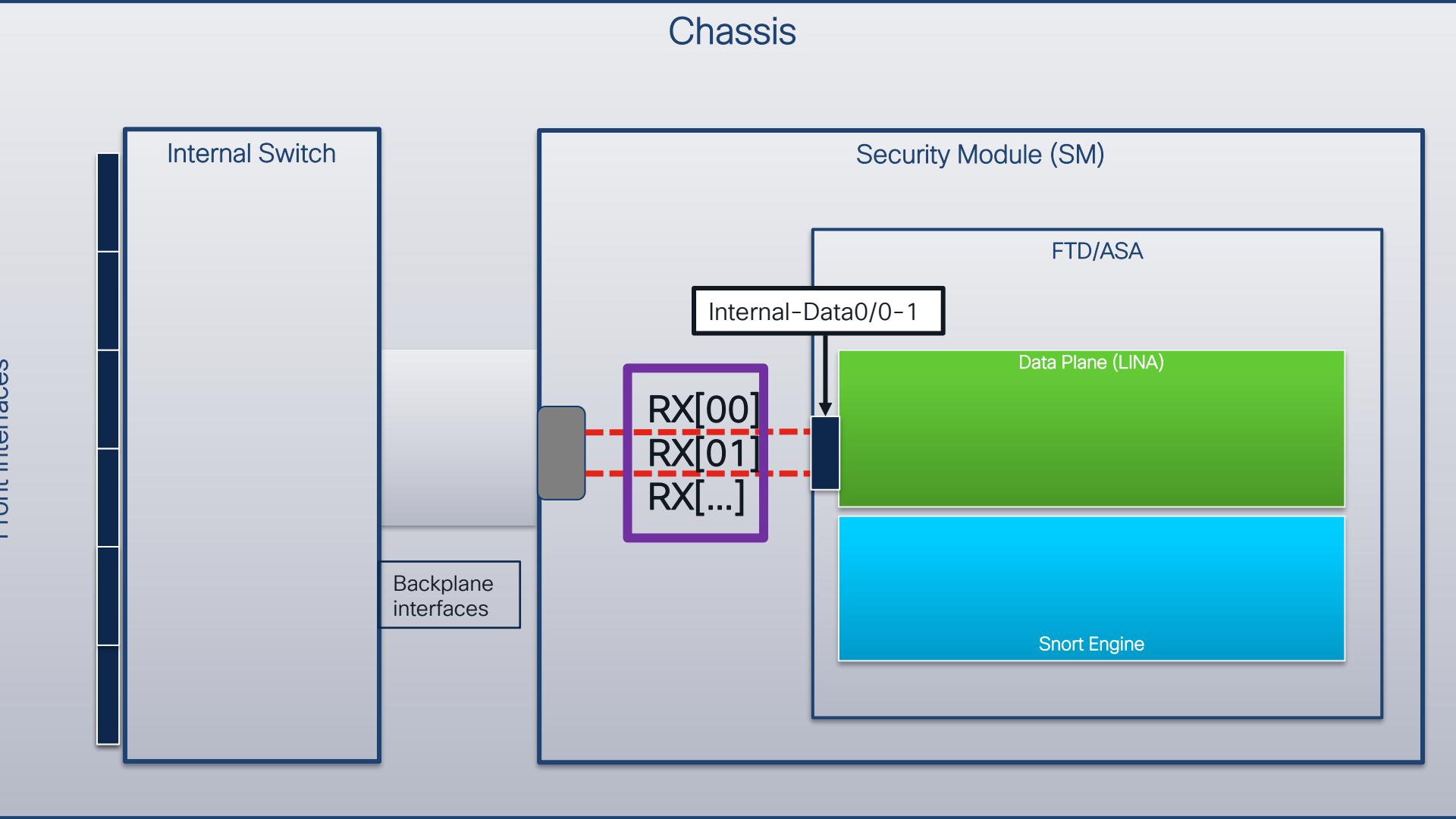


Capture Points For 41xx, 93xx and 31xx devices

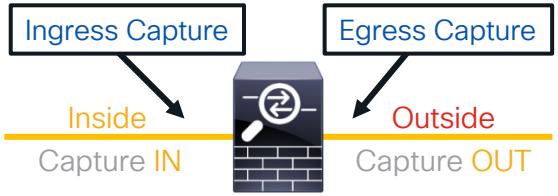


For the internal switch, captures are only supported in the **ingress** direction **(Egress direction capture is not possible)**

1100/2100 platforms do not officially support internal switch captures


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

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

ASP drops captures

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

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

ARP Captures

```
> 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

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:

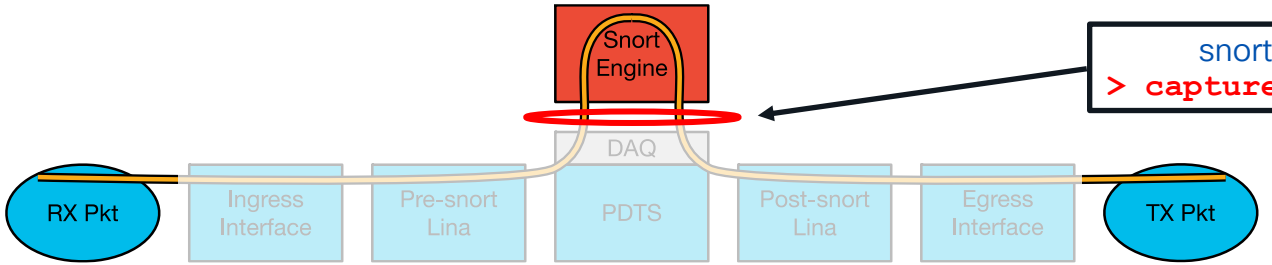
```
firepower# Capture capin interface inside headers-only buffer 10000000
```

New packet-tracer option to allow egress of simulated packets

- Transmit packet tracer simulated packet to destination.

```
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
```

Snort-side captures




```
> 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

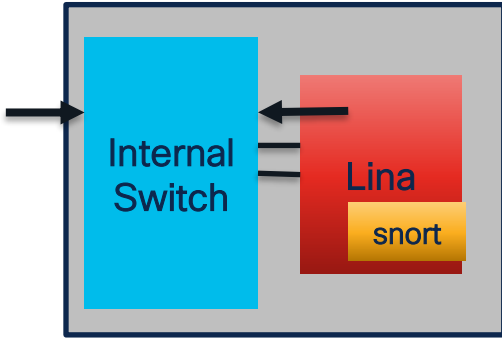
> capture-traffic
PCAPs are written to:
/ngfw/var/common/

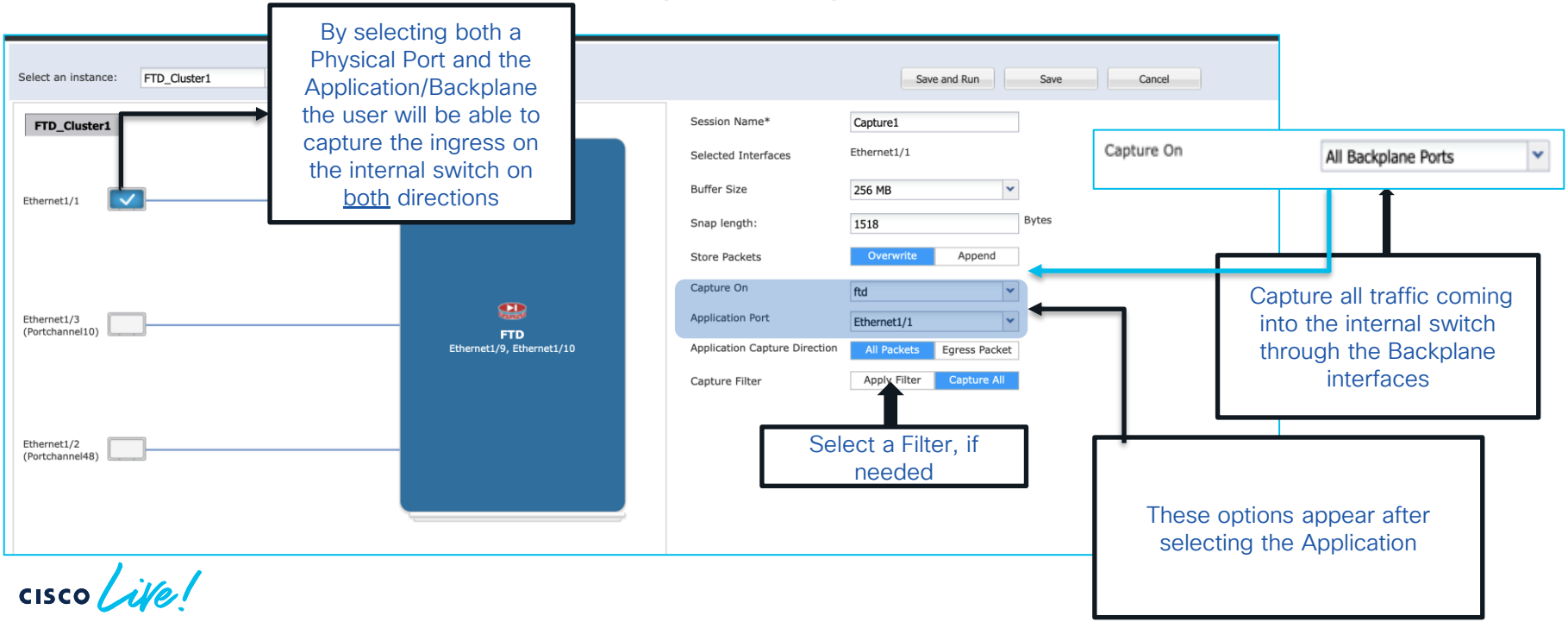
tcpdump -w FILE.pcap
Write the capture to file

TCPdump like format (BPF)

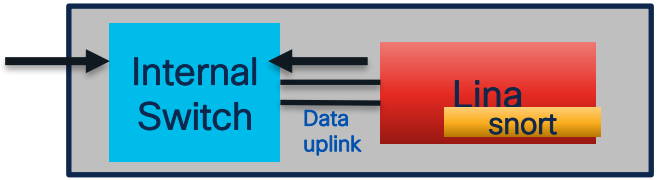
Internal Switch Captures
(for 41xx,3100 and 93xx)

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





Captures on 31xx platform



- 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

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"

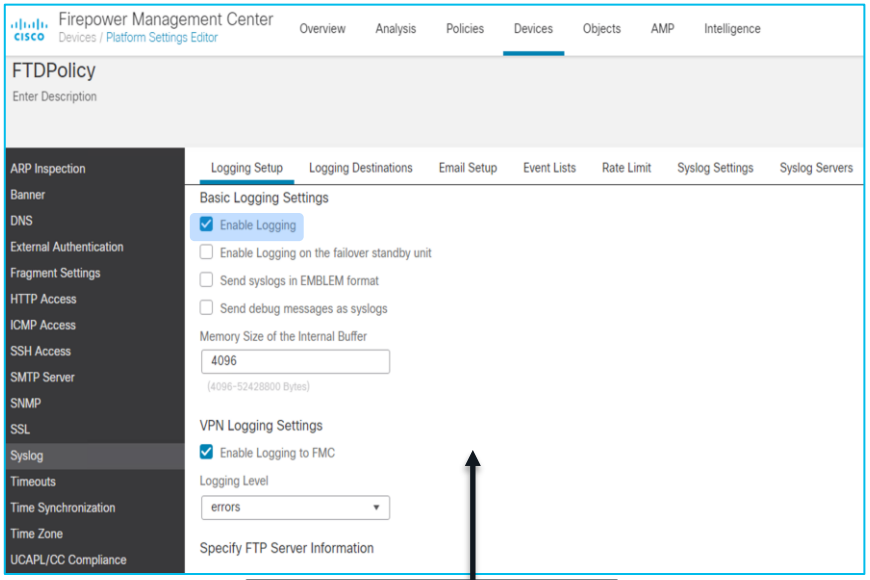
Match rule and action

Snort verdict sent to DAQ/PDTS

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.



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`"

Connection count
Useful for performance issues

```
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
```

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

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

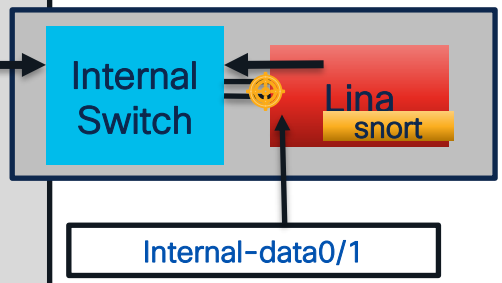
Interface Counters (show interface)

- 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
```



Events

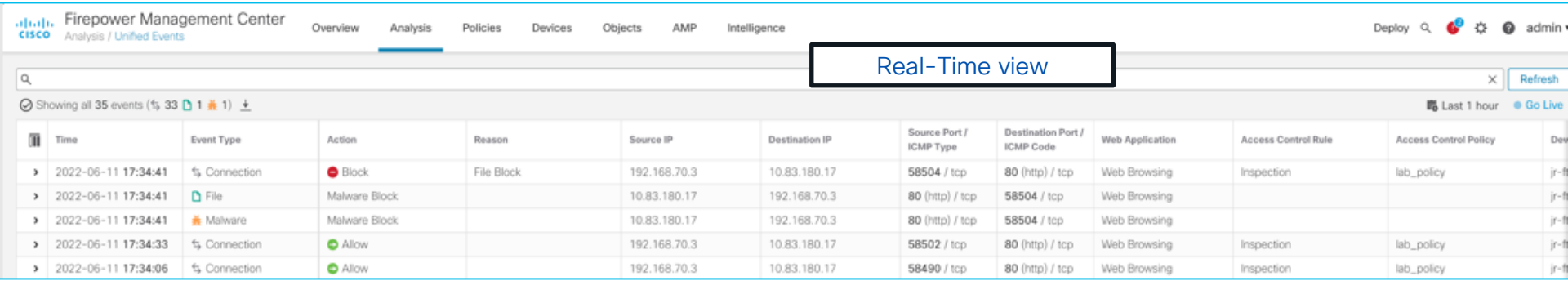
- Connection Events:

Navigate to “**Analysis** > **Connections** > **Events**” → Click “**Table View of Connection Events**”

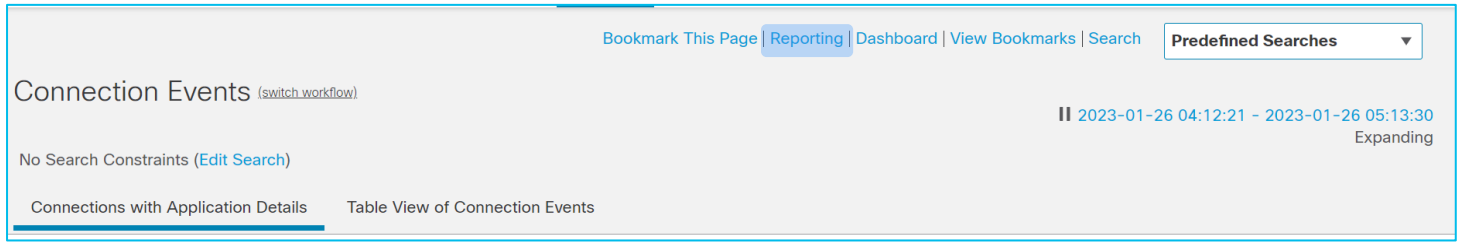
Connection events can be exported into reports (PDF, Excel) → Useful for sending to TAC.

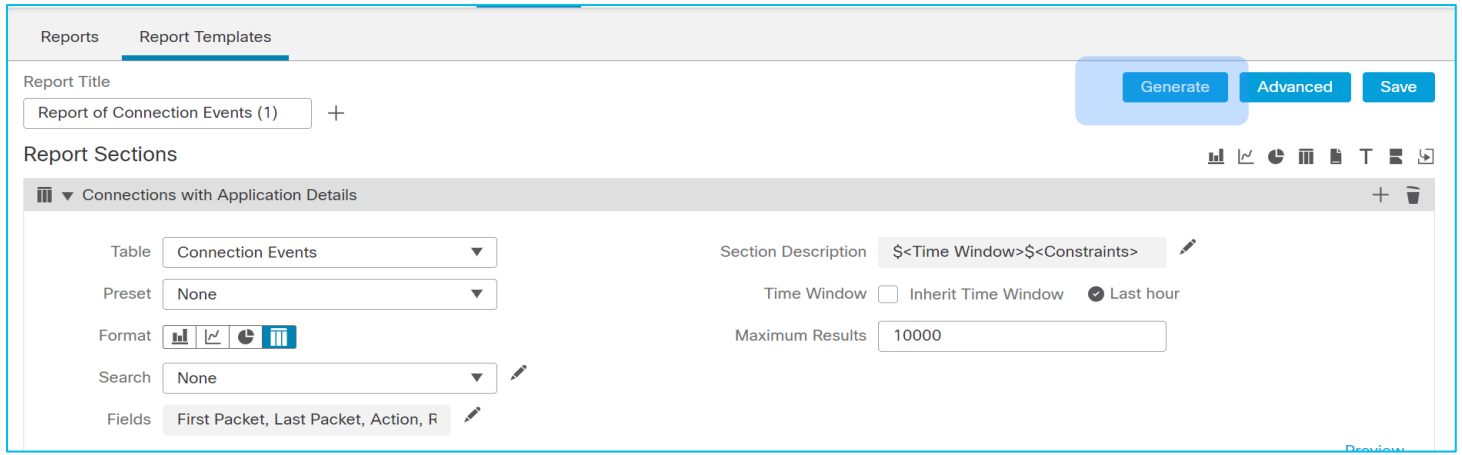
- Unified event viewer is added starting from version 7.x

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



Connection Events – Report Generation





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

TCP State Bypass

Still happening ?

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


Datapath
You are here
Upgrade
RADkit
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

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~~
You are here
RADkit
Performance
Use Case
SECURELAND CITY

Performance

CPU Issues

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

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,  1322064k 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

- 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
```

Heavy CPU load from SNMP traps.

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.

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

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*

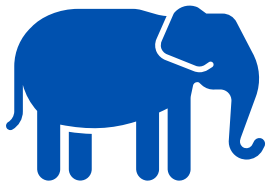
Elephant Flow Visibility

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 and isolate performance issues

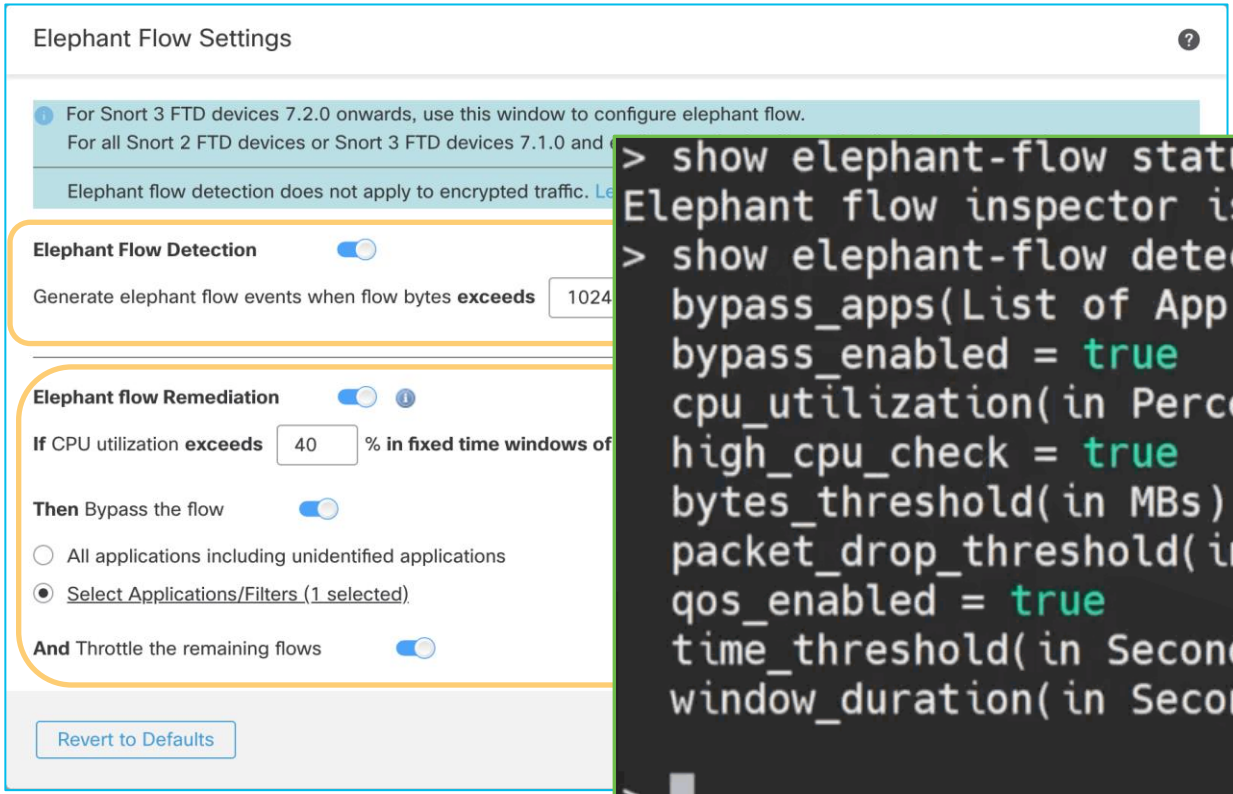
7.2 Release: Improved Detection and Remediation

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

Secure Firewall CLI Commands (Secure Firewall Version 7.2)

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

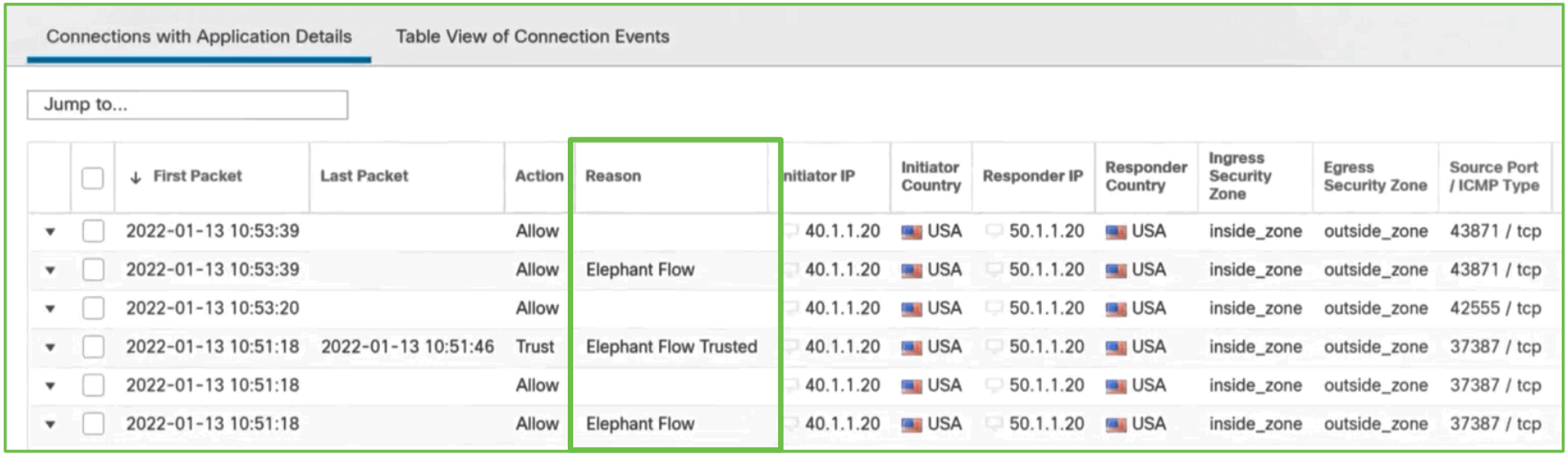



```
> show elephant-flow status
Elephant flow inspector is enabled
> show elephant-flow detection-config
  bypass_apps(List of App IDs) = '676:1'
  bypass_enabled = true
  cpu_utilization(in Percentage) = 1
  high_cpu_check = true
  bytes_threshold(in MBs) = 1
  packet_drop_threshold(in Percentage) =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

>
```

Detecting and Identifying Elephant Flows

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

Detecting and Identifying Elephant Flows



First Packet	Last Packet	Action	Reason	Initiator 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**

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

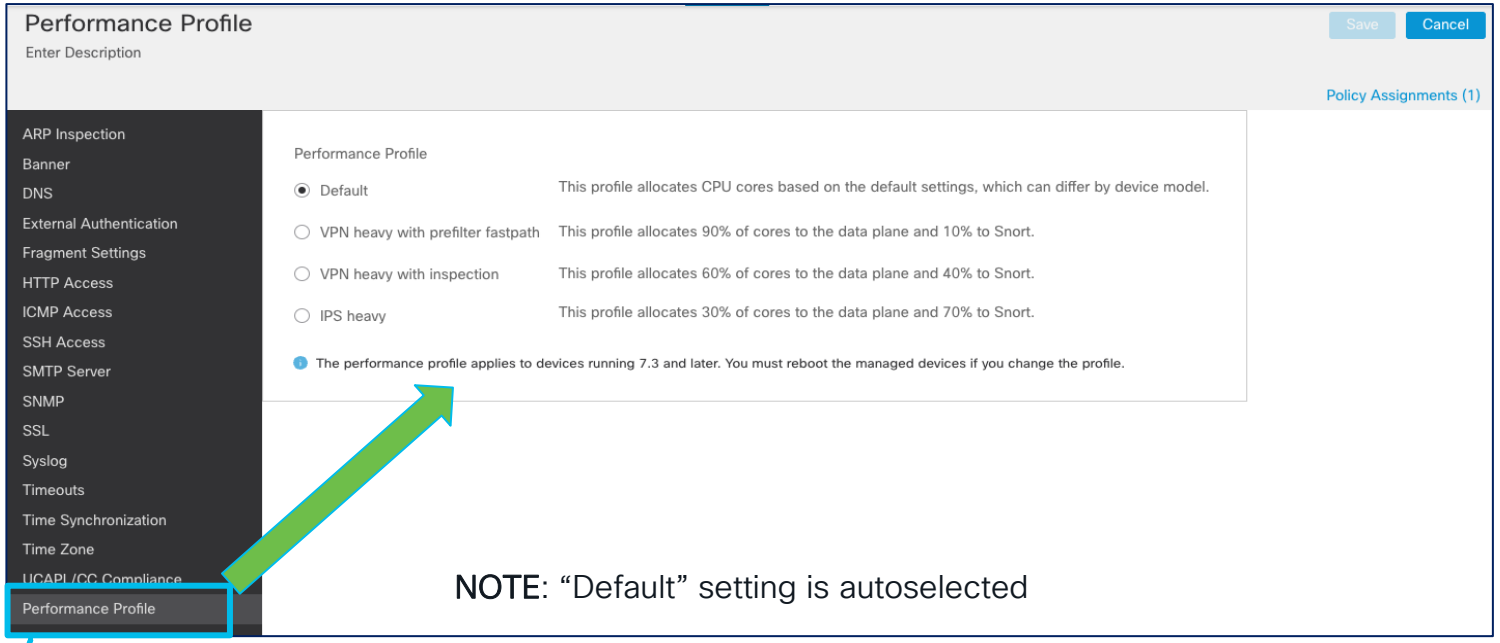
- Enables customers to optimize their CPU allocation based on deployment type.

Requirements

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

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.



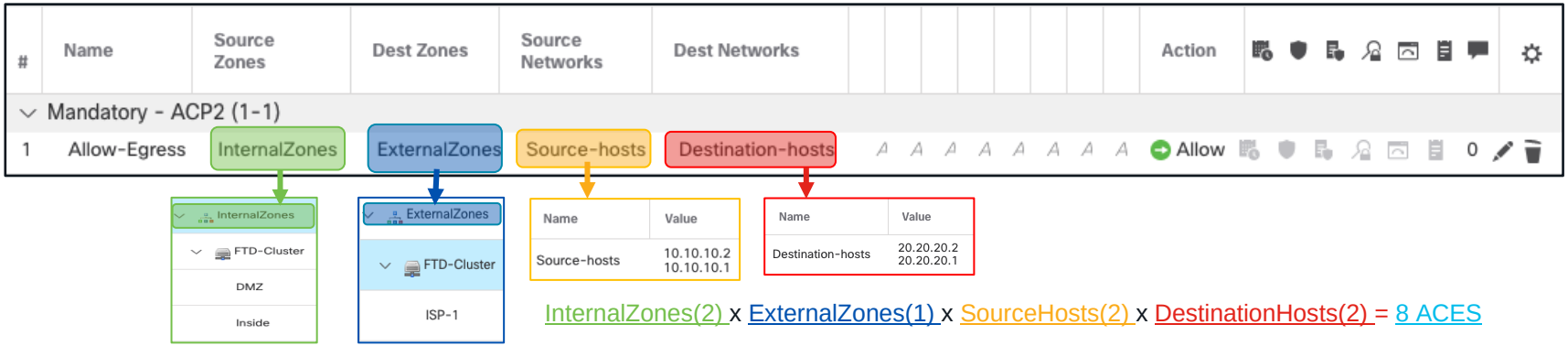
Lina Memory – Overview

- 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

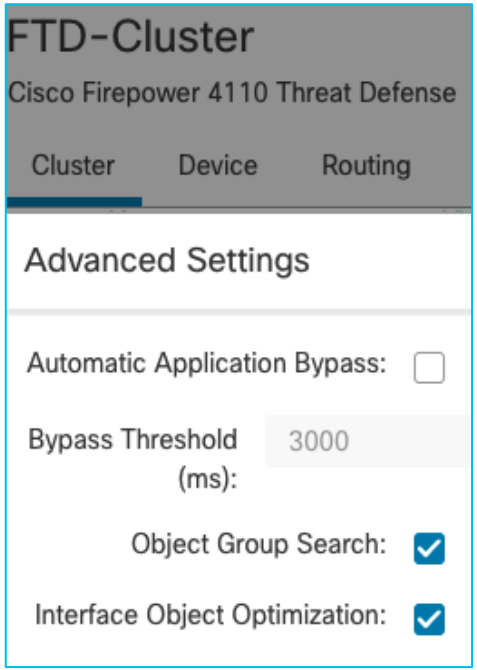



```
> show access-list
access-list CSM_FW_ACL_ line 10 advanced permit ip ifc DMZ object-group Source-hosts ifc ISP-1 object-group Destination-hosts
  access-list CSM_FW_ACL_ line 10 advanced permit ip ifc DMZ host 10.10.10.2 ifc ISP-1 host 20.20.20.1 rule-id 268434437
  access-list CSM_FW_ACL_ line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



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

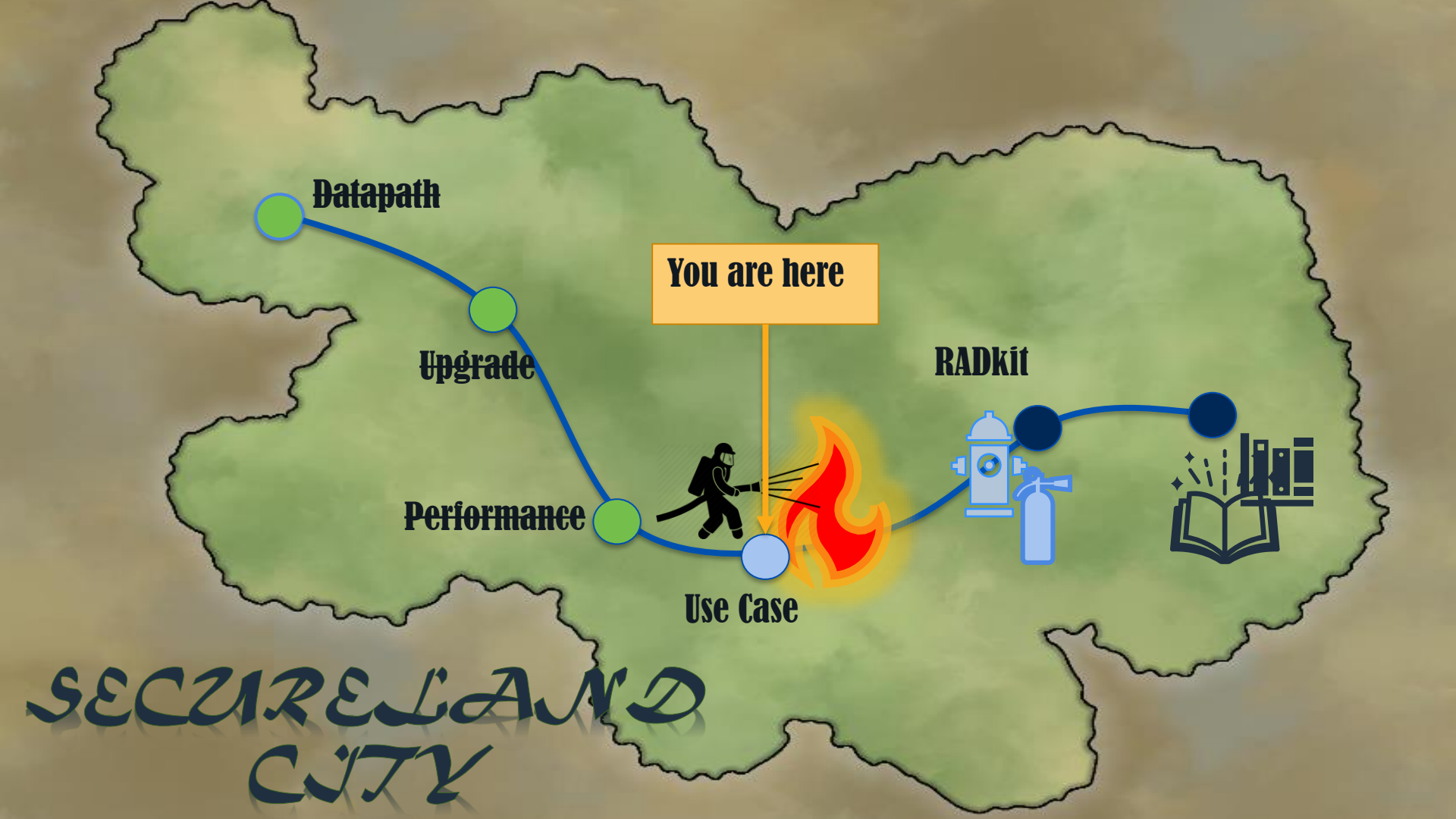
Interface Object Optimization (IOO)

- 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
```


Datapath
Upgrade
Performance
You are here
Use Case
RADkit
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
```

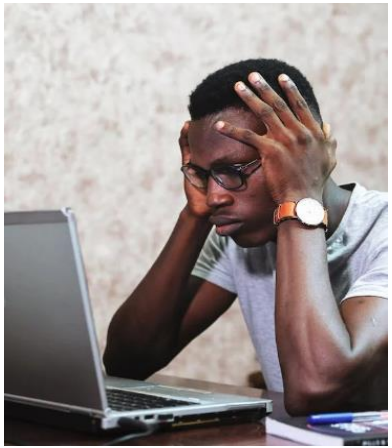
Analysis of Existing Data

- 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:

```
909:      ------------------ show interface ------------------
910:
911:      Interface Internal-Data0/1 "", is up, line protocol is up
912:        Hardware is , BW 10000 Mbps, DLY 10 usec
913:      (Full-duplex), (10000 Mbps)
914:      Input flow control is unsupported, output flow control is unsupported
915:      MAC address 000f.b748.4801, MTU not set
916:      IP address unassigned
917:      30704186 packets input, 9356355772 bytes, 15257819 no buffer
918:      Received 11454 broadcasts, 0 runts, 0 giants
919:      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.

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

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 Da

Captures

Firewall to Syslog Server

Firewall MAC Address (Source)

Peer MAC Address (Destination)

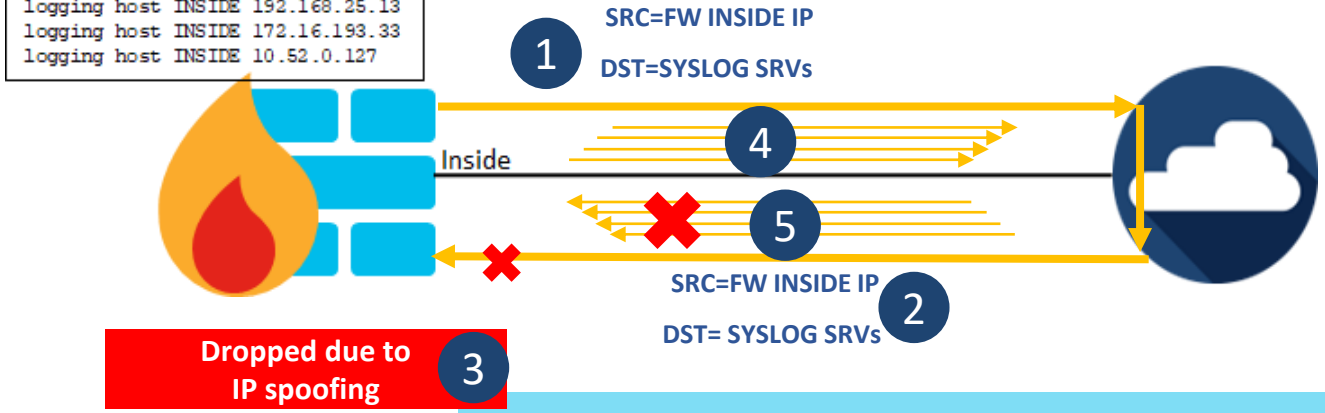
40	2022-10-20 17:11:12.584503	0.000000	10.103.55.11	192.168.25.12	UDP	514	514	158	0xfff9	c8:45:ff:05:ef:da	b5:25:4a:00:e0:07	254	514 → 514
19988	2022-10-20 17:11:12.773504	0.189001	10.103.55.11	192.168.25.13	UDP	514	514	161	0xfff9	b5:25:4a:00:e0:07	c8:45:ff:05:ef:da	255	514 → 514
28228	2022-10-20 17:11:12.876007	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

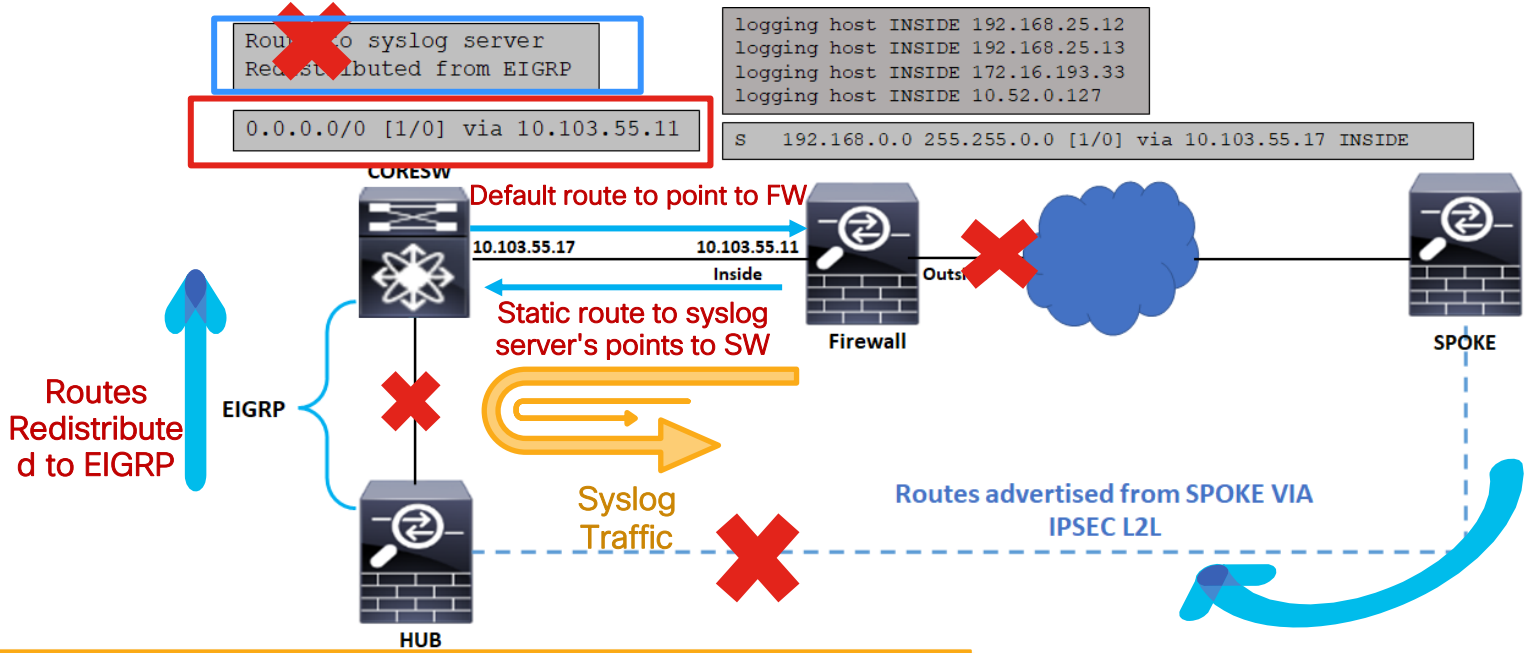

```
logging host INSIDE 192.168.25.12
logging host INSIDE 192.168.25.13
logging host INSIDE 172.16.193.33
logging host INSIDE 10.52.0.127
```



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

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



Not a routing loop!

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

Case Study Final Conclusion

- 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.

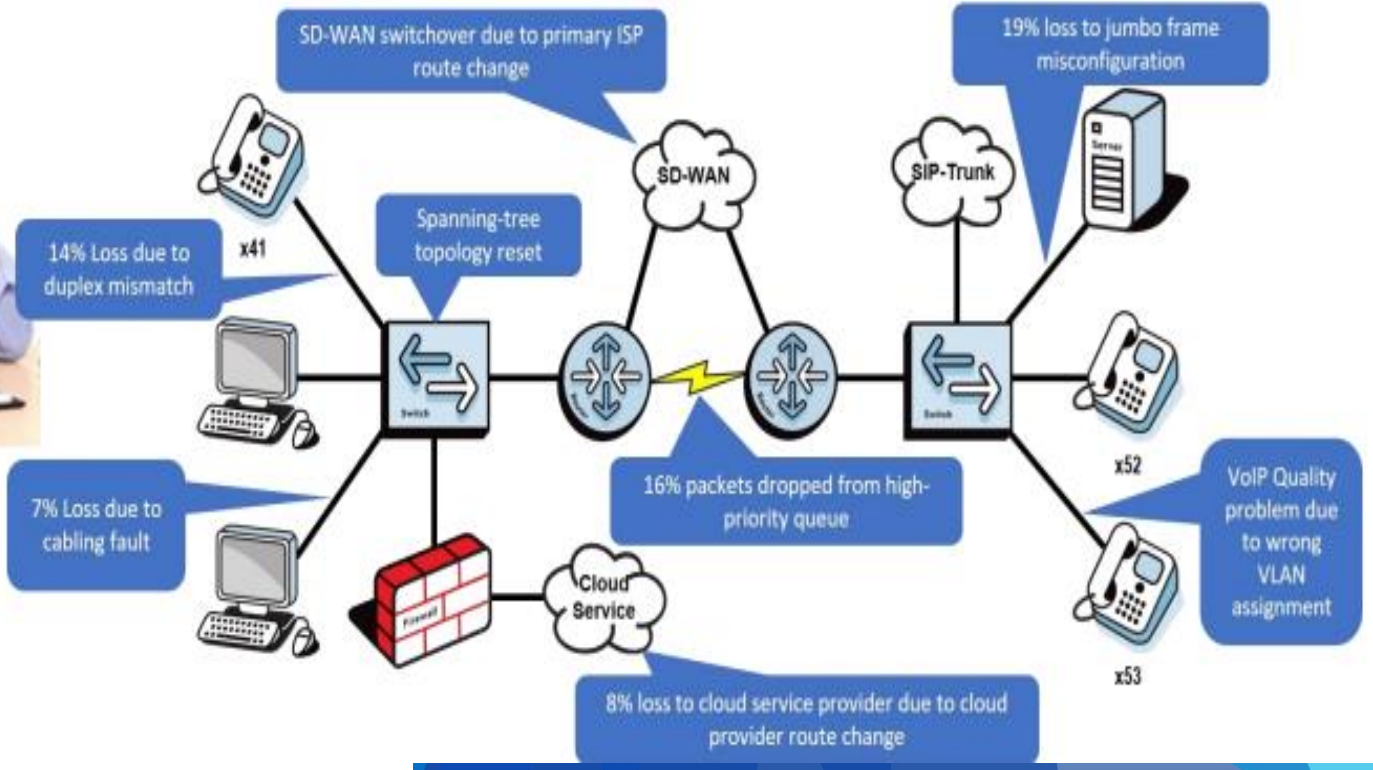

You are here
~~Datapath~~
~~Upgrade~~
~~Performance~~
~~Use Case~~
RADkit
SECURELAND
CITY

Cisco RADKit

(Remote Automation Development Kit)

cisco Live!

How painful is this?



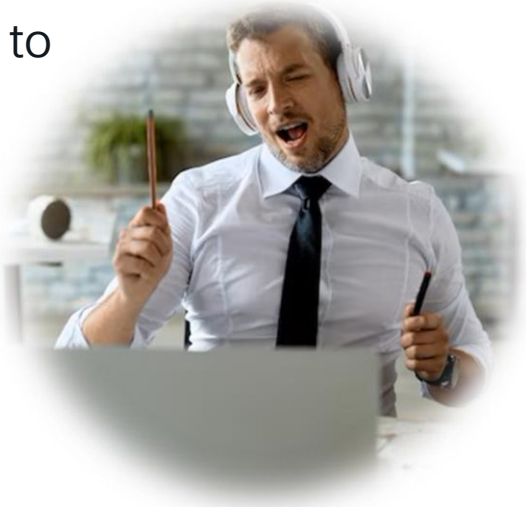
Why RADkit?

- 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

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.



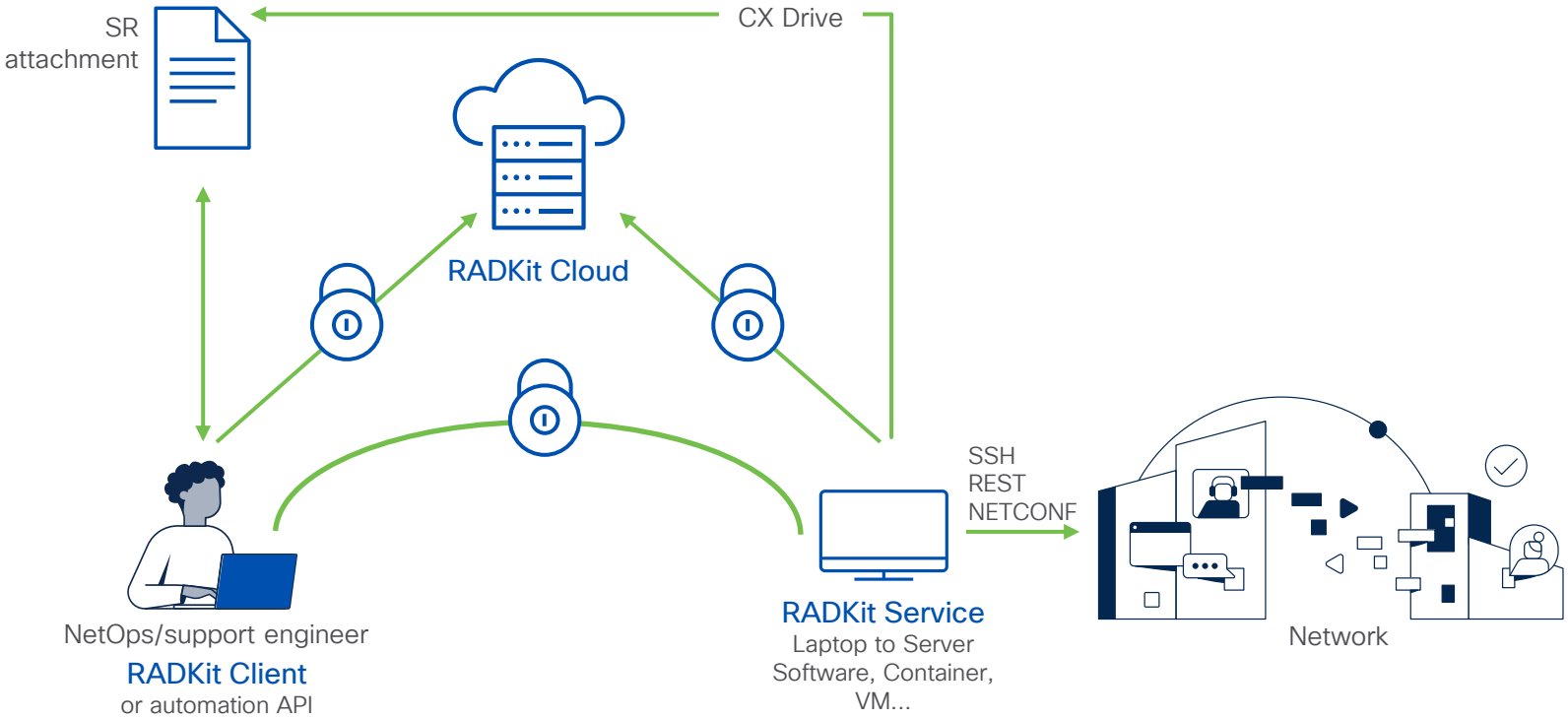
- Full **authentication**, **authorization, access-control and encryption**.

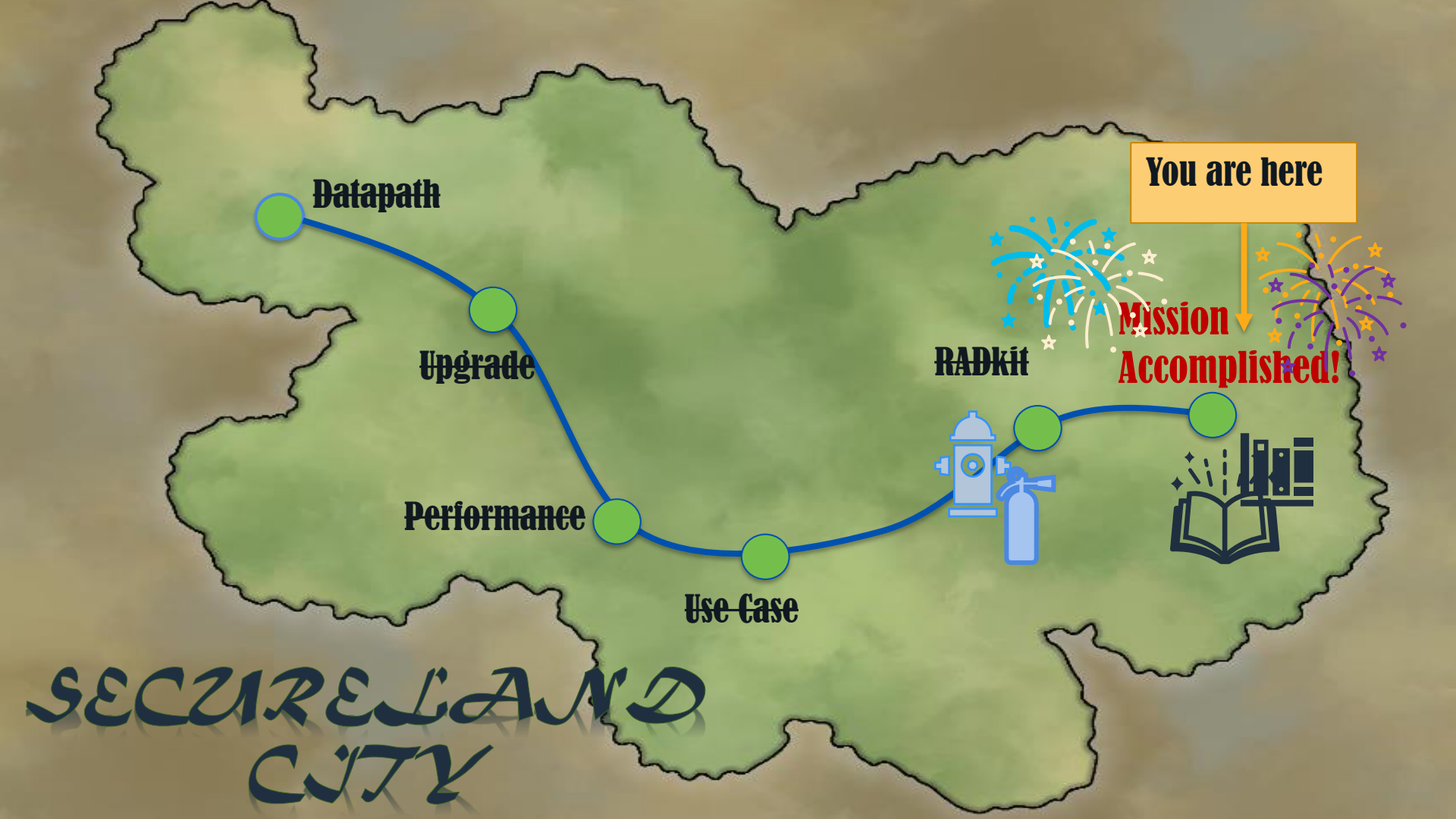
- **Collect** data, monitor, troubleshoot, **download**, **upload** or even connect to **CLI.**

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

RADKit Architecture – Client-Service

Cisco Remote Automation Development Kit (RADKit)




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

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 after 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!

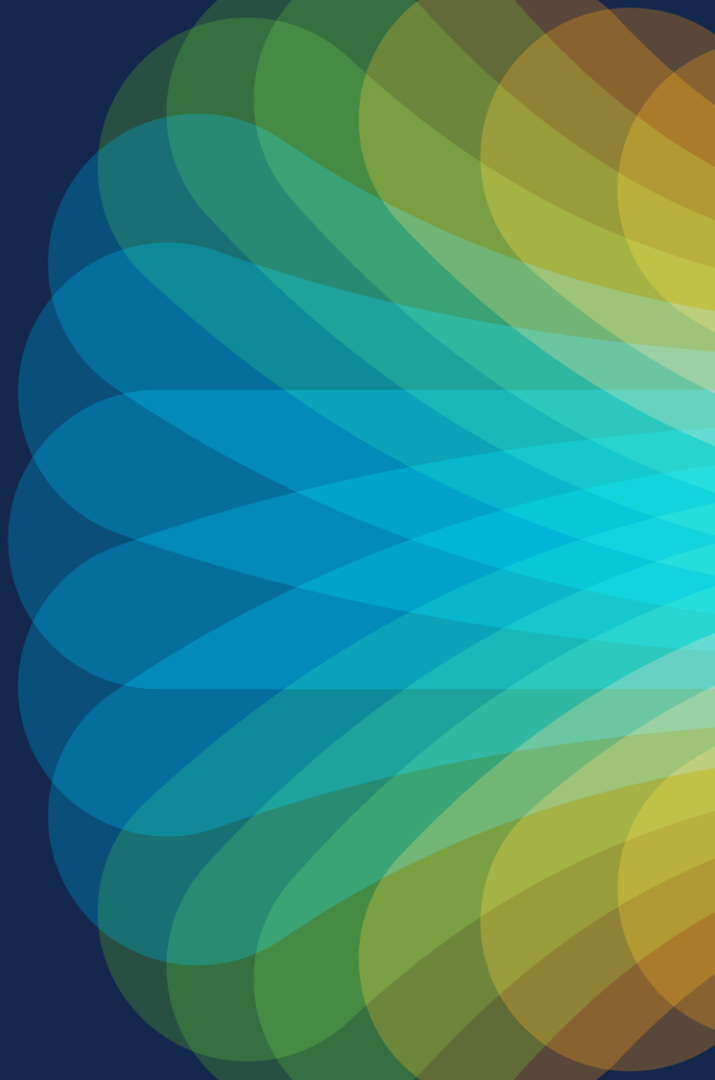
“A problem well put is half solved.”

John Dewey

References

The bridge to possible

Thank you



cisco Live!


cisco Live!
Let's go