
cisco Live!
Let's go

The bridge to possible

Secure Firewall – Threat Defense Data-Path Troubleshooting

A practical hands on lab

John Groetzinger, Technical Leader, CX
Foster Lipkey, Principal Engineer, CX

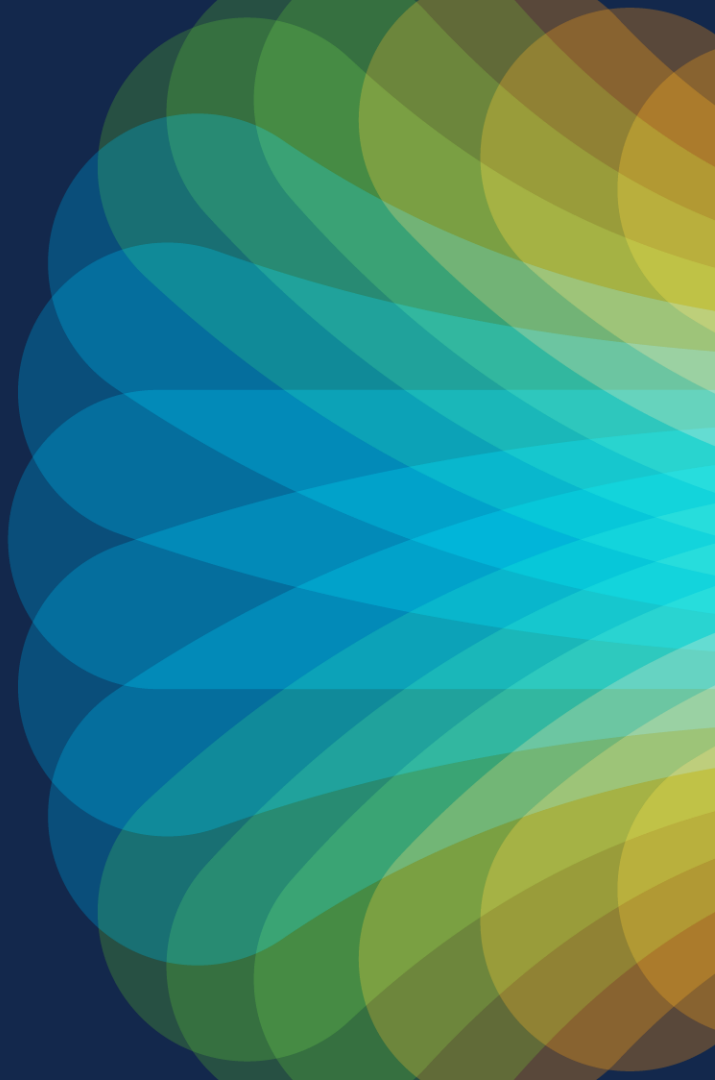
cisco Live!

LTRSEC-3880

Agenda

- Introduction
- Architecture Overview
- Troubleshooting Framework Overview
- Self-Paced Lab Scenarios
- Conclusion

Introduction



Your Presenters

John Groetzinger

- Technical Leader for Firepower TAC
- 12+ Years experience in Network Security
- Original Sourcefire employee
- Open Source, devops and Linux enthusiast

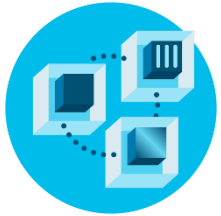
Your Presenters

Foster Lipkey

- TAC Security – Principal Engineer
- 12+ Years of Security Experience
- Snort Expert
- Sourcefire Veteran
- Automation Enthusiast
- Malware Detection Patent Holder

Snorty Collectables

Key Learning Objectives



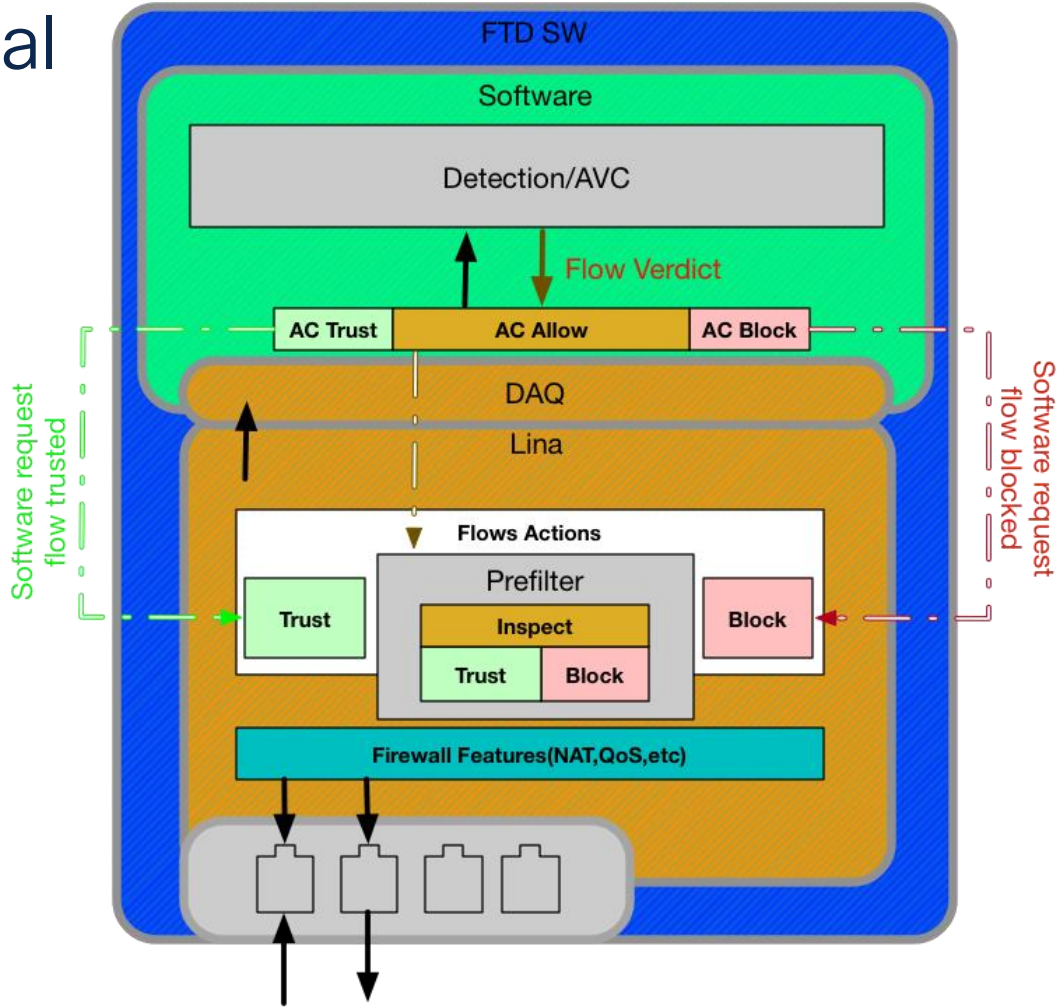
Hardware and Software Components in Firepower Systems

Framework to Isolate Problematic Component

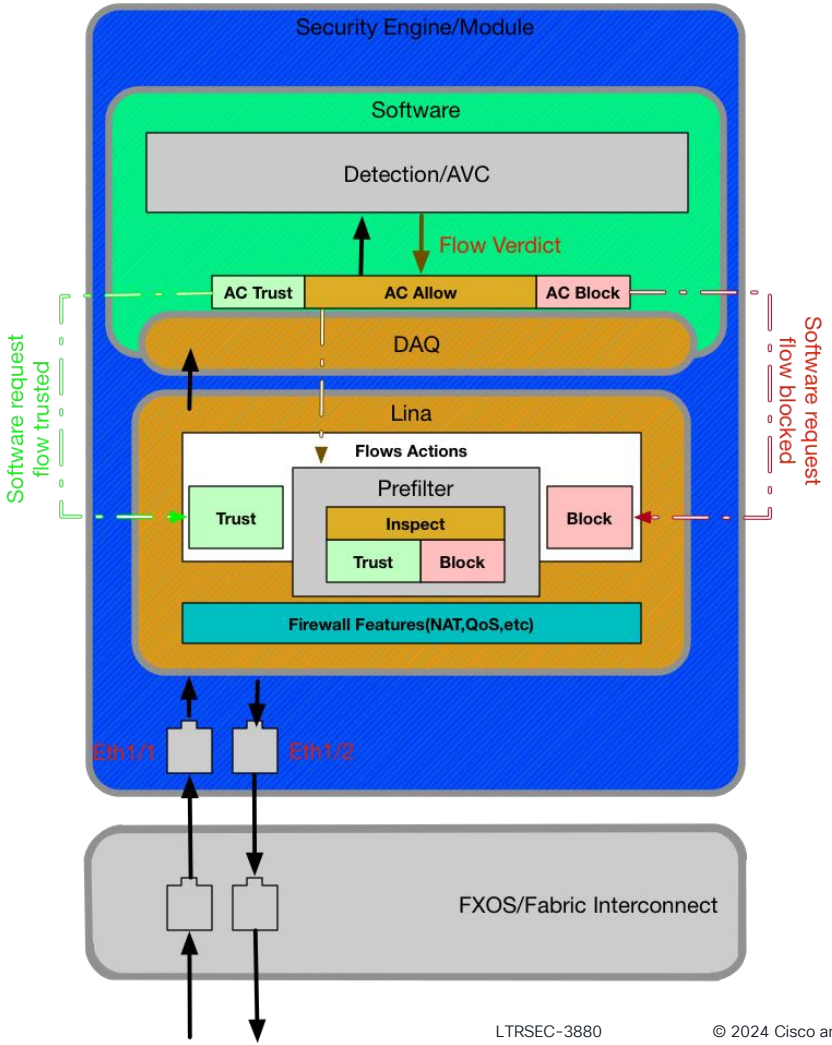
Individual Component Troubleshooting Skills

Architecture Overview

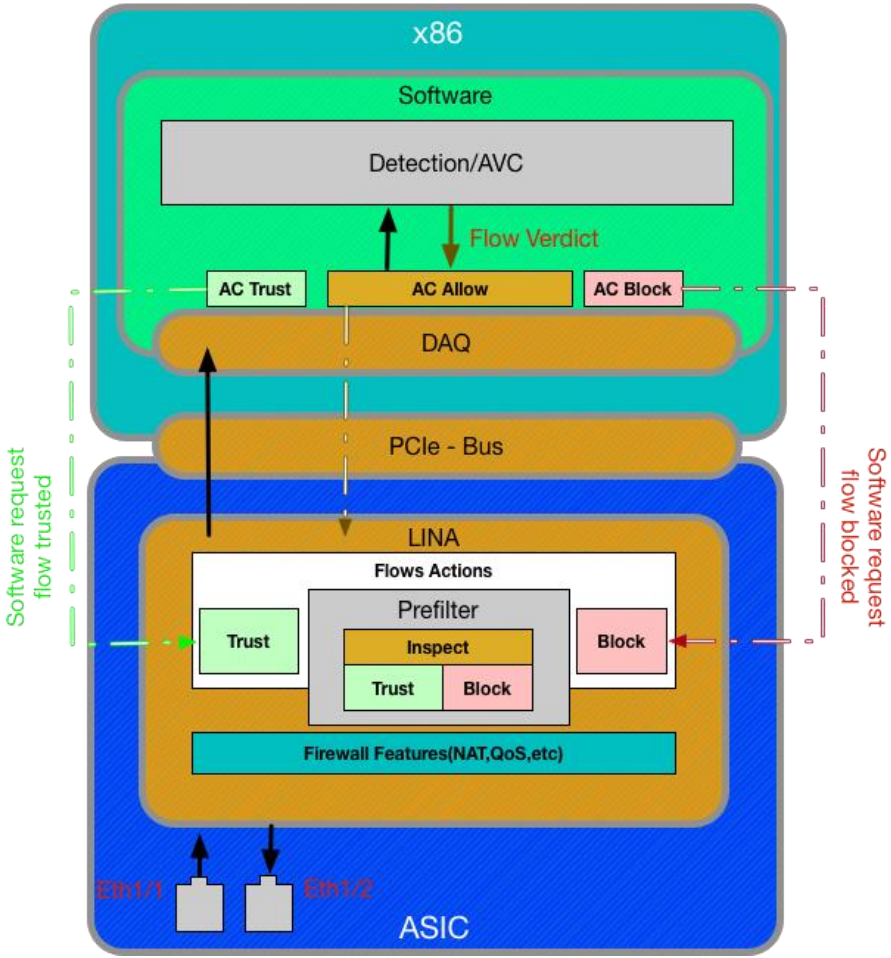
ASA/virtual FTD



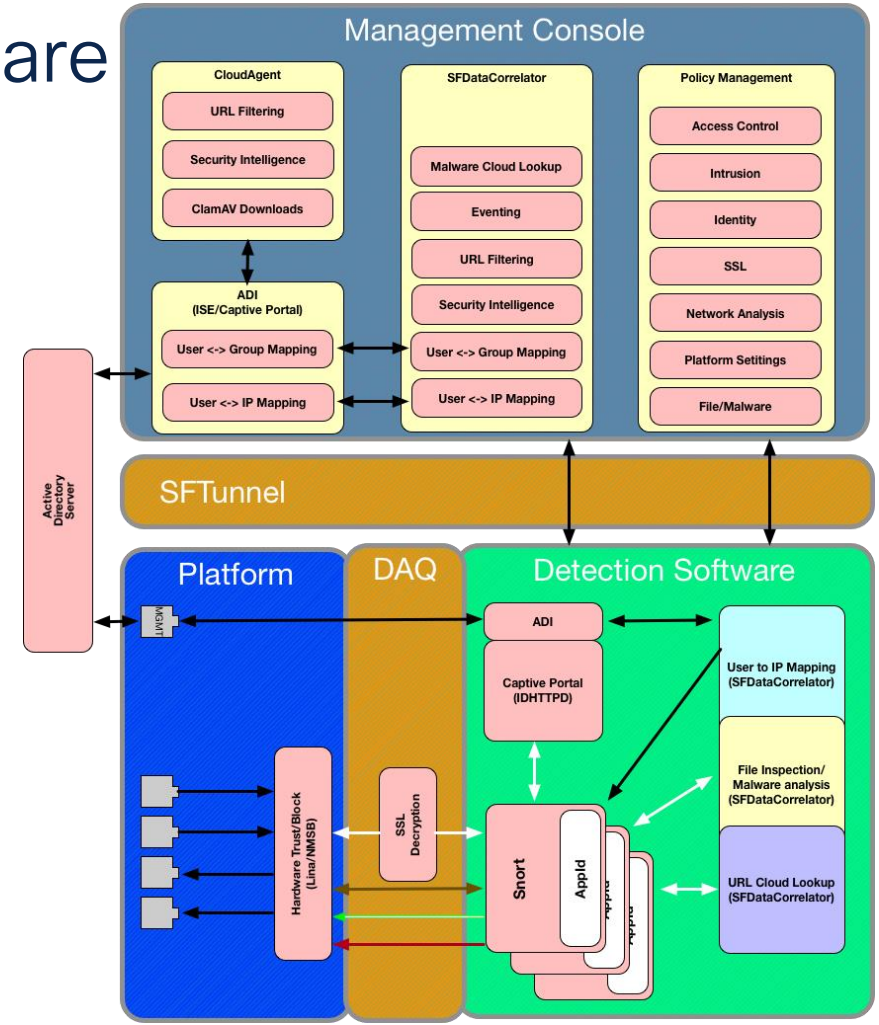
SSP (4100/9300)



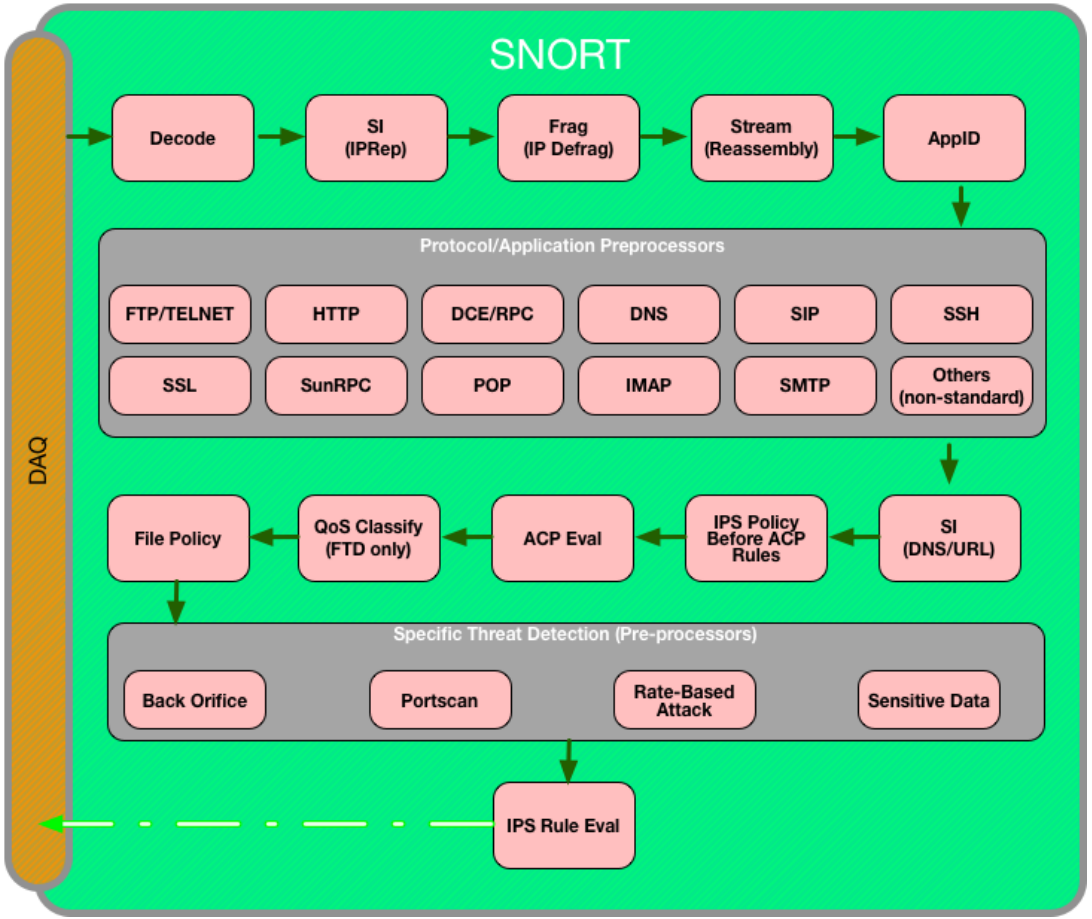
SSP (2100)



Virtual/Software diagram

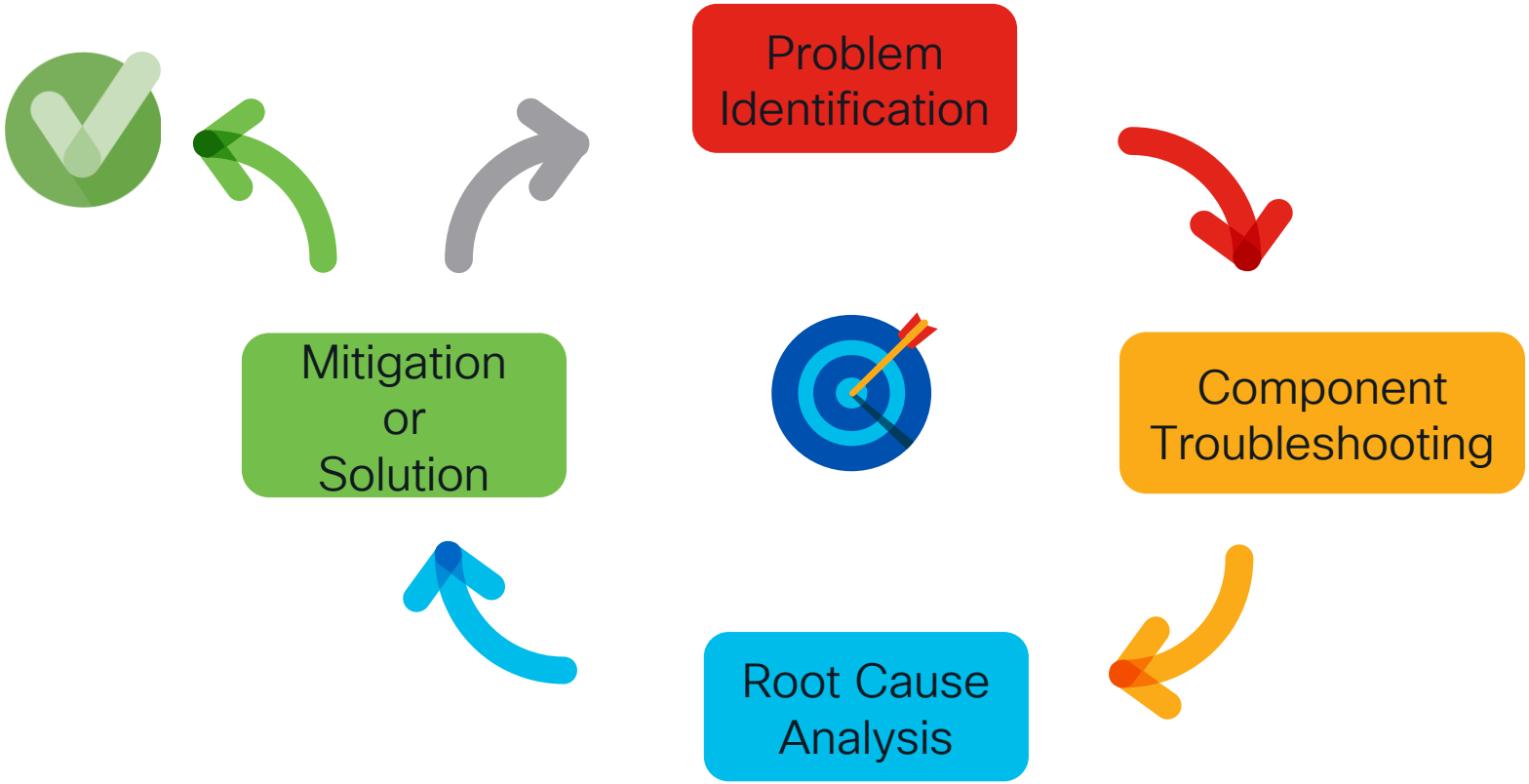


Virtual/Software diagram

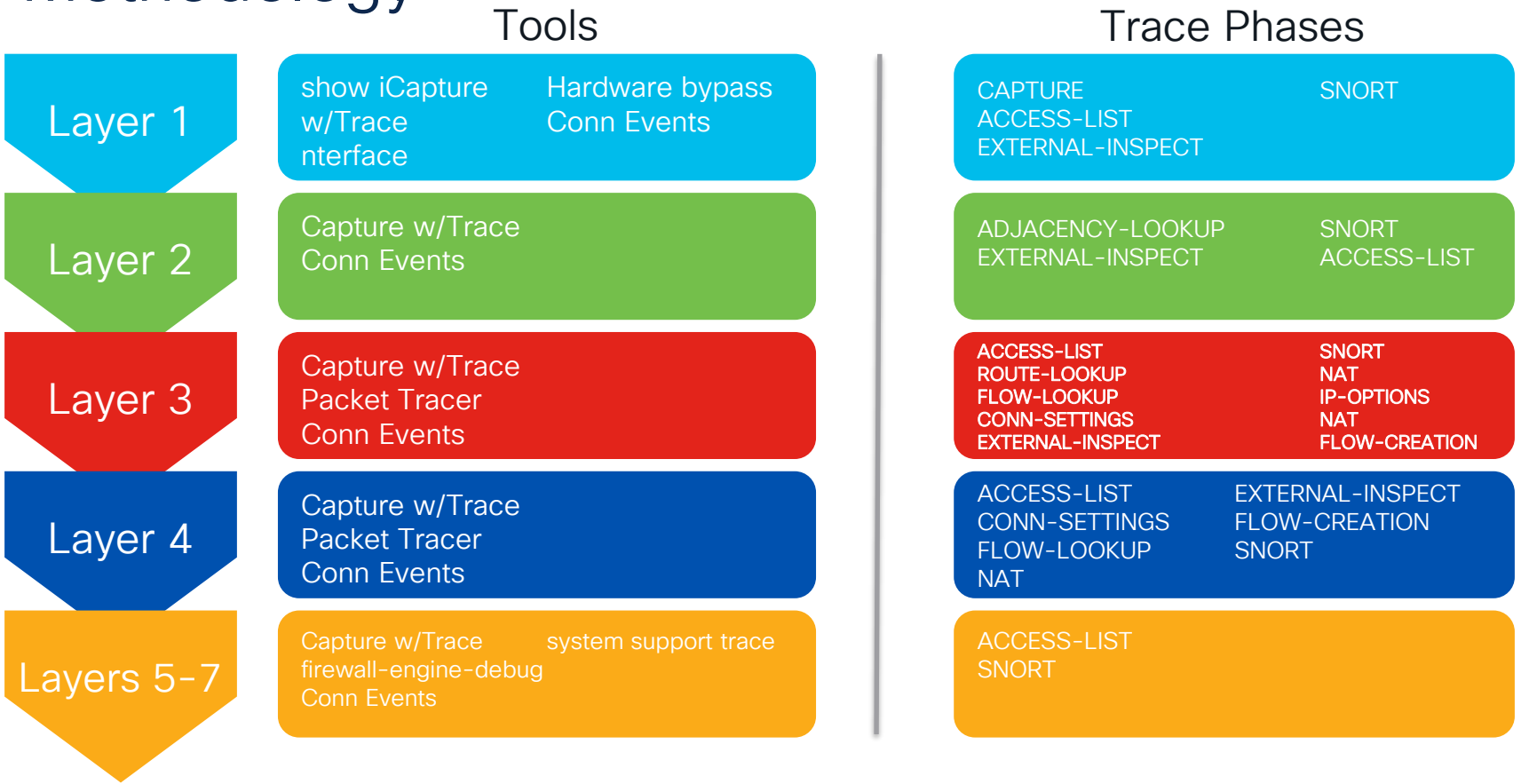


Troubleshooting Framework Overview

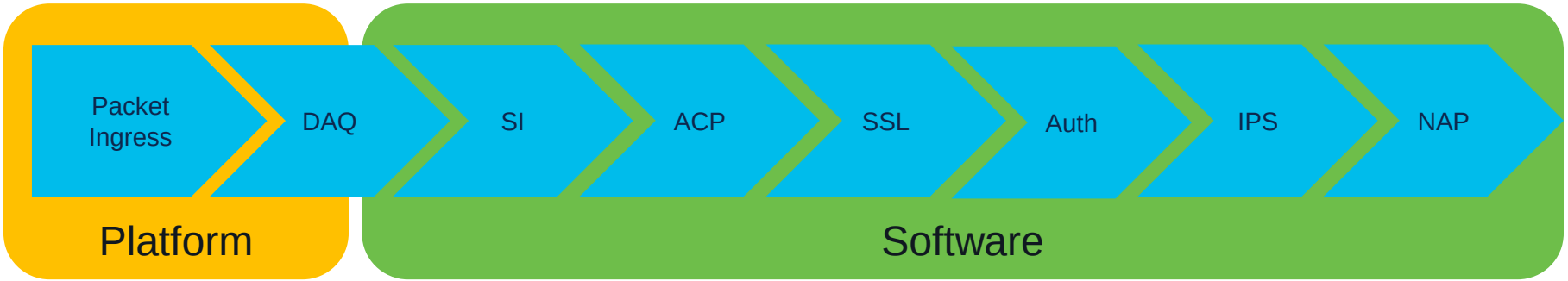
Troubleshooting Methodology



Methodology



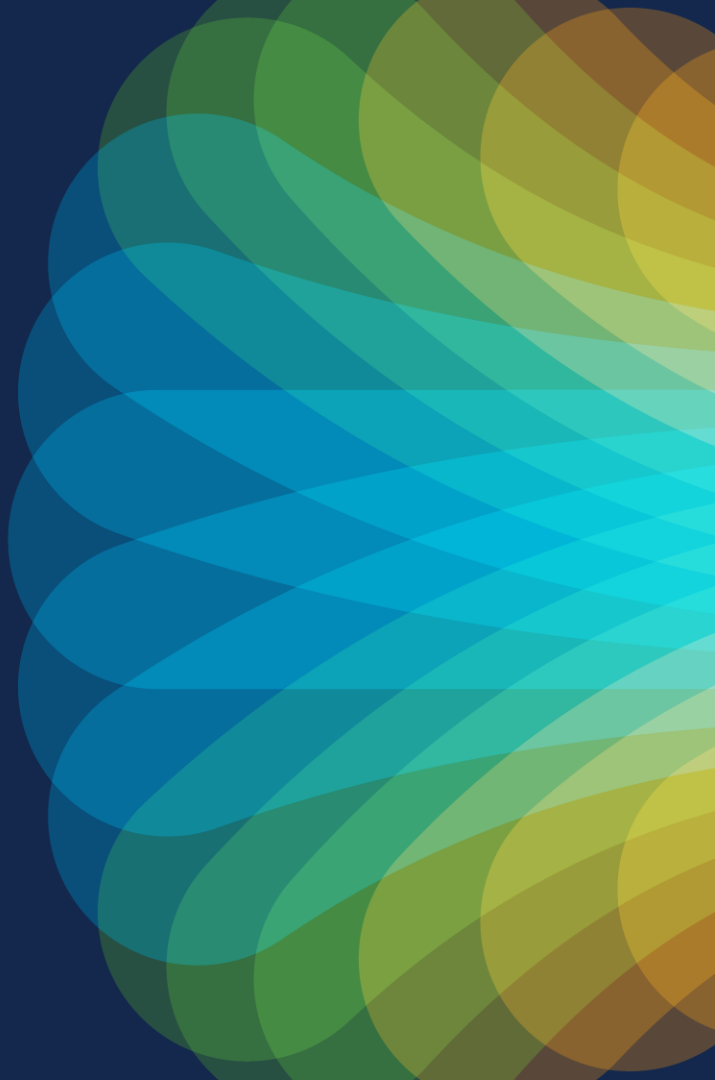
Firepower Data-Path Troubleshooting Framework flow diagram



Introduction to Problem Component Identification

Tool Introduction

- Capture w/Trace
- Prefilter policy



DAQ (Data Acquisition)

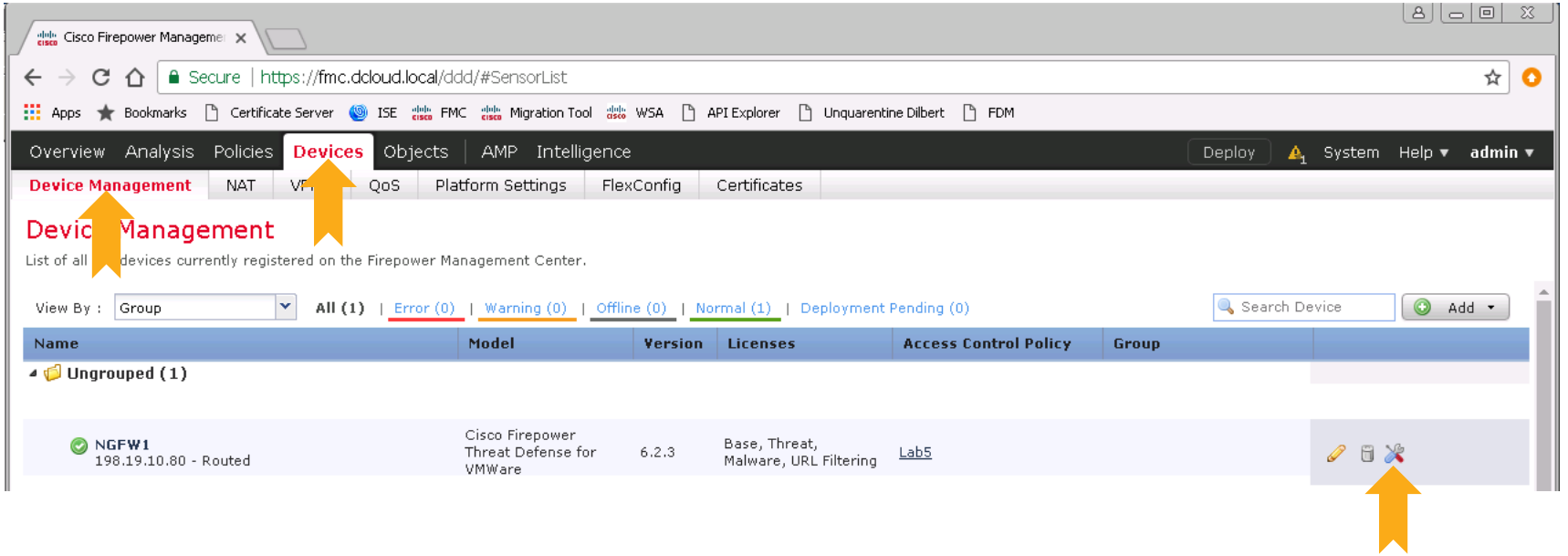
Tools

- **Capture W/ Trace**
- Debug Packet

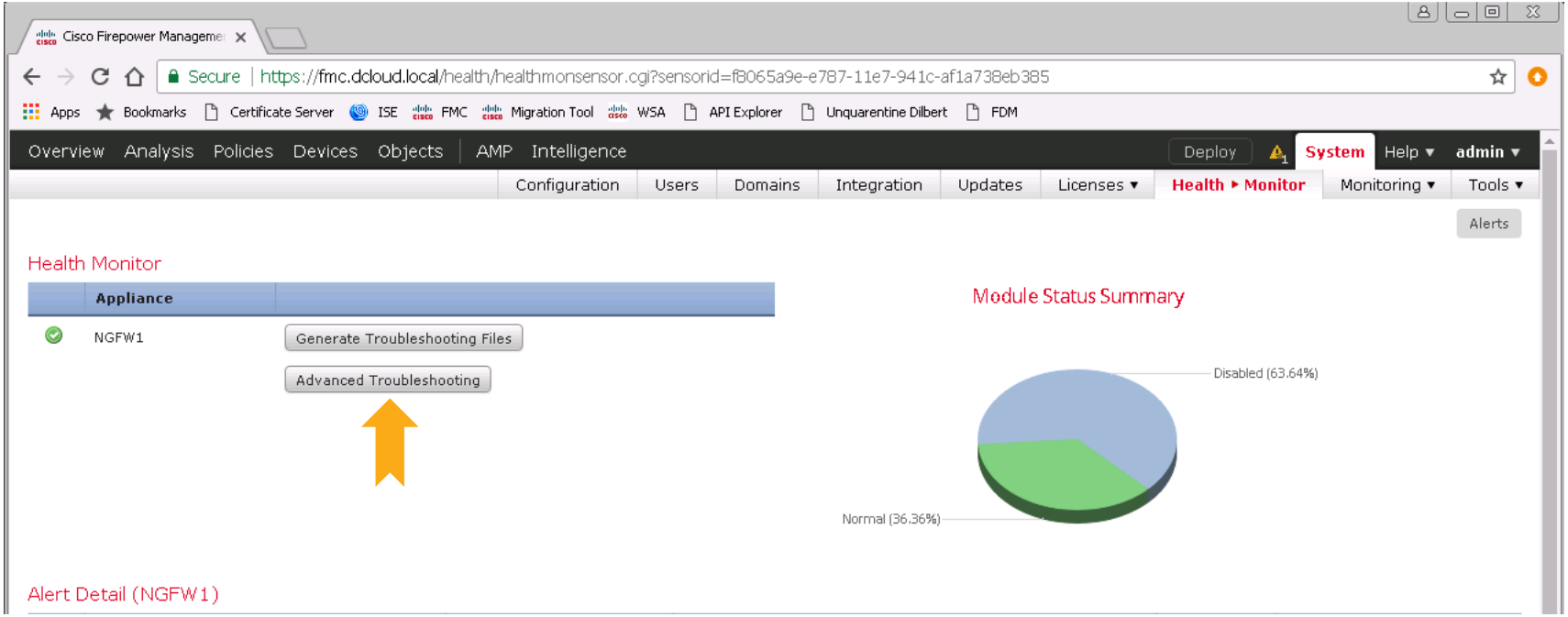
Remediations

- Prefilter Policy
  - Policies > Access Control > Prefilter
  - Create or edit Prefilter policy
  - Add a fastpath rule for the traffic
  - Make sure to use the Prefilter policy in the AC policy

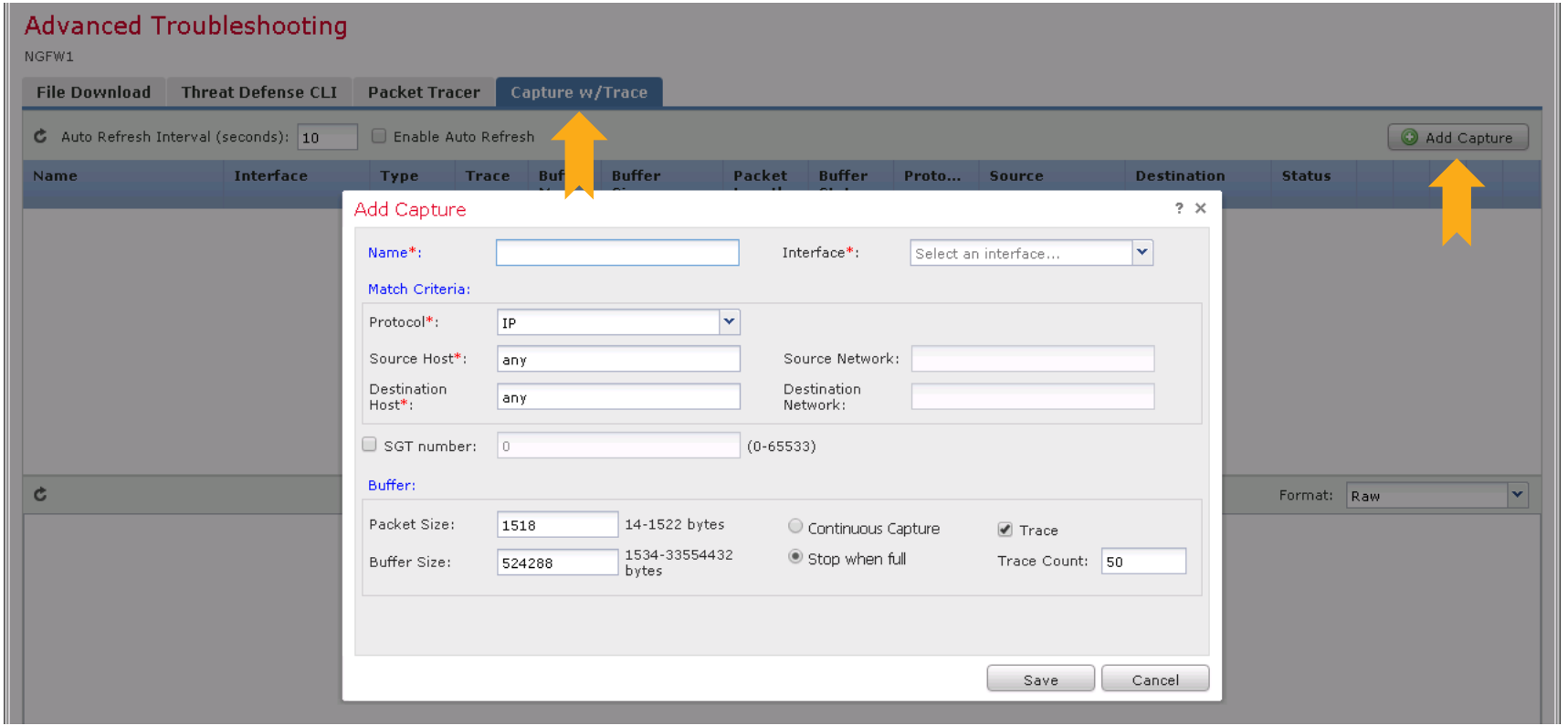
Capture w/Trace:

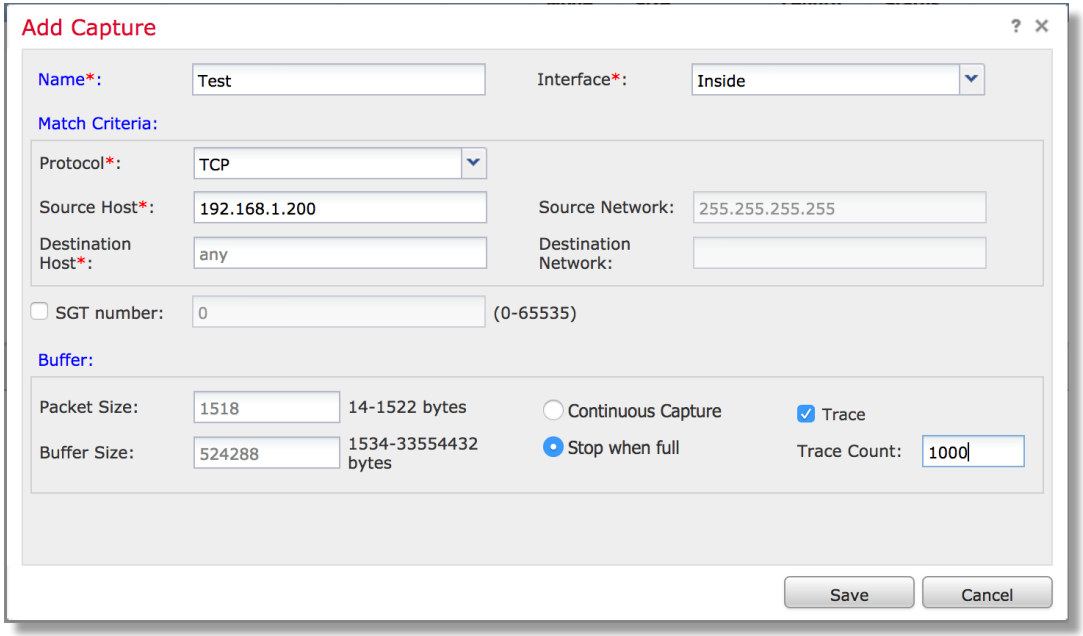


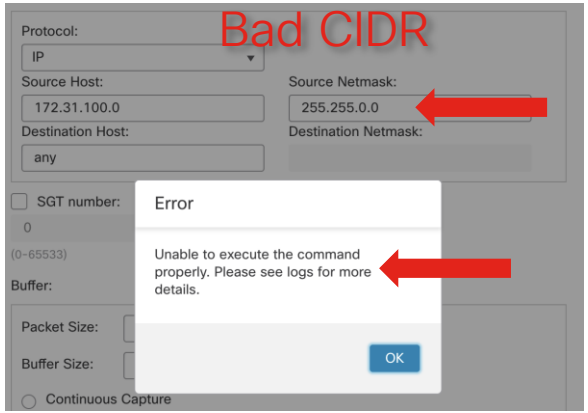
Capture w/Trace:



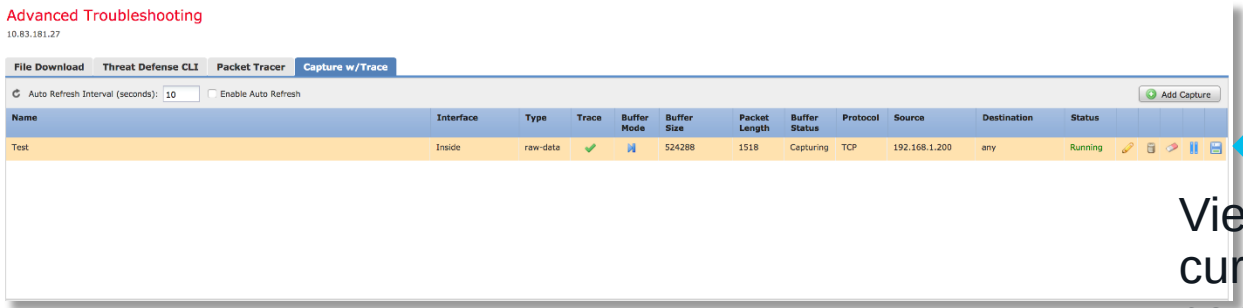
Capture w/Trace:





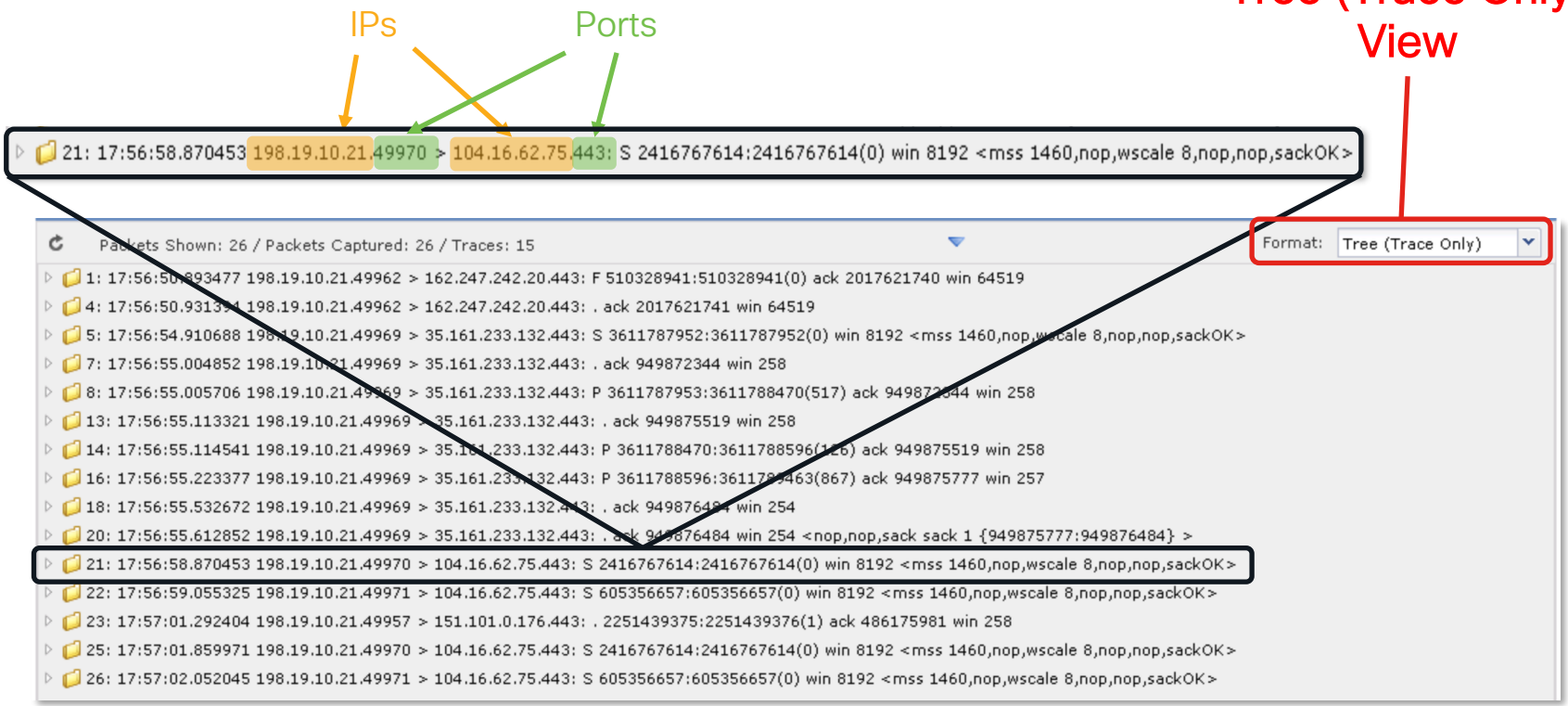


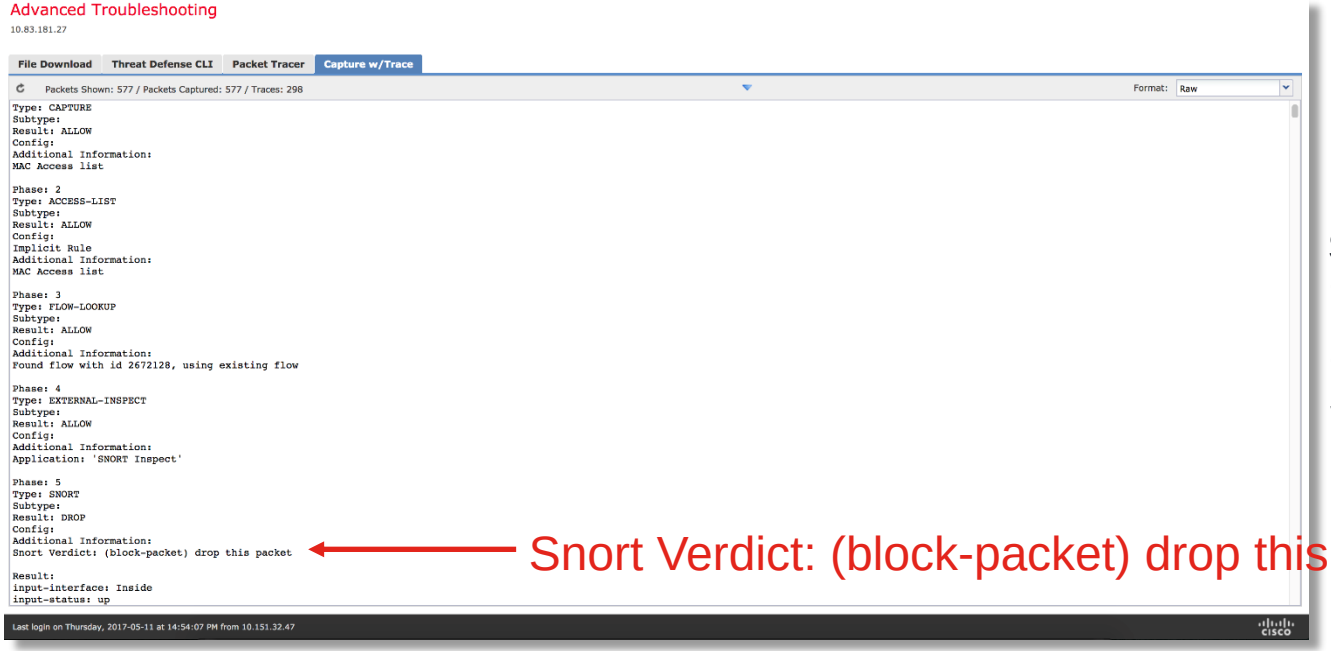
Clicking **Add Capture** button will display this popup window



View of all current captures

Capture w/Trace Tree view

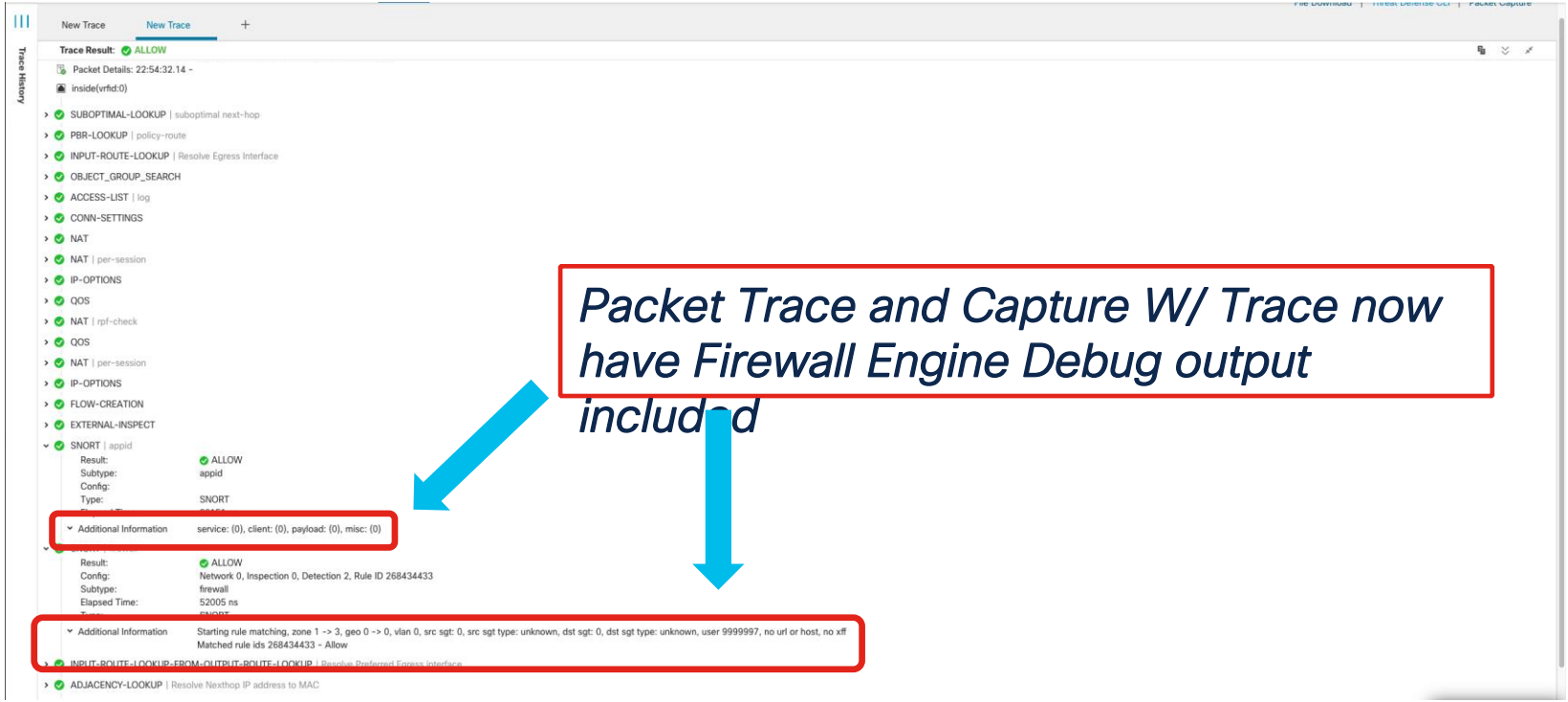




Example output shows the packet was blocked by Snort

Snort Verdict: (block-packet) drop this packet

Packet Tracer in FMC – Including Snort information



SHELL

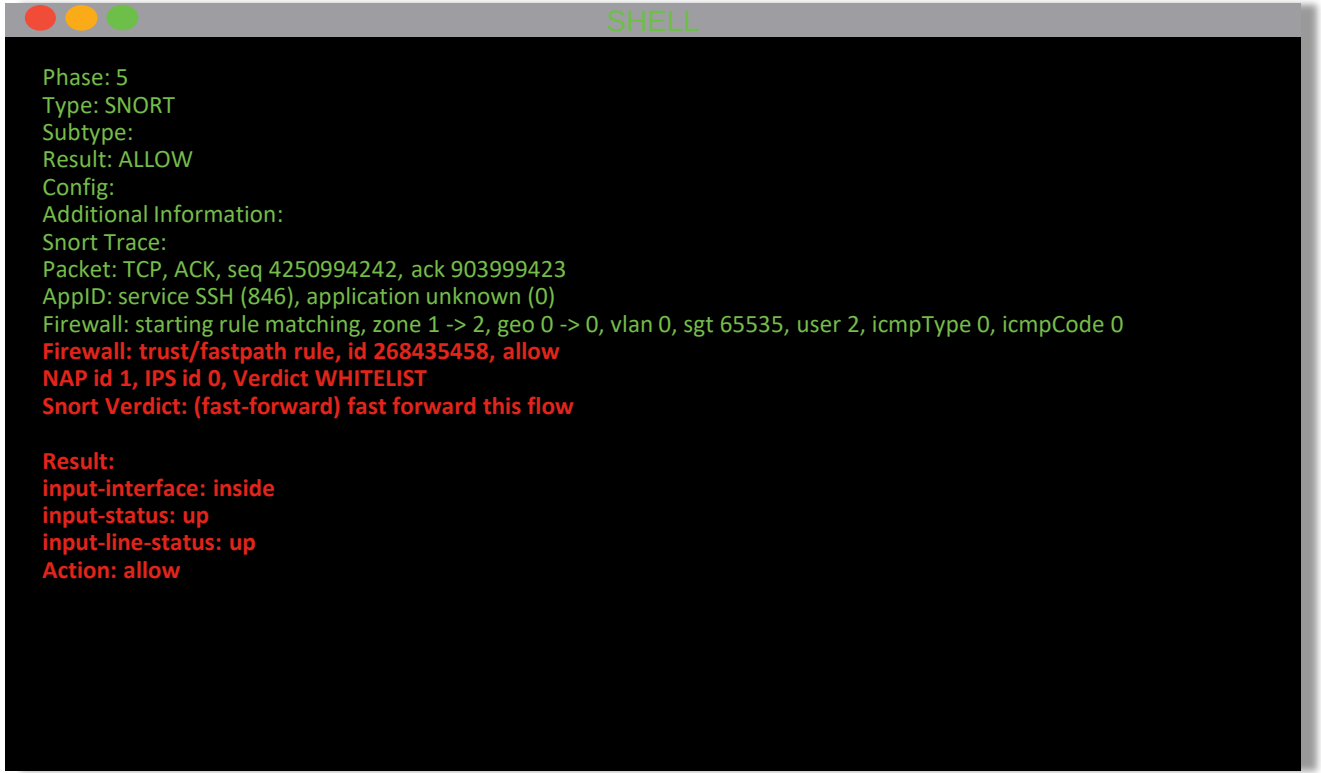
```
> capture ssh_traffic trace interface inside match tcp any any eq 22
> show capture ssh_traffic

7 packets captured

  1: 01:17:38.498906      192.168.62.70.48560 > 10.83.180.173.22: S 4250994241:4250994241(0) win 29200 <mss 1460,sackOK,timestamp 1045829951 0,nop,wscale 7>
  2: 01:17:38.510898      10.83.180.173.22 > 192.168.62.70.48560: S 903999422:903999422(0) ack 4250994242 win 17896 <mss 1380,sackOK,timestamp 513898266
1045829951,nop,wscale 7>
  3: 01:17:38.511402      192.168.62.70.48560 > 10.83.180.173.22: . ack 903999423 win 229 <nop,nop,timestamp 1045829956 513898266>
  4: 01:17:38.511982      192.168.62.70.48560 > 10.83.180.173.22: P 4250994242:4250994283(41) ack 903999423 win 229 <nop,nop,timestamp 1045829957
513898266>
  5: 01:17:38.513294      10.83.180.173.22 > 192.168.62.70.48560: . ack 4250994283 win 140 <nop,nop,timestamp 513898268 1045829957>
  6: 01:17:38.528125      10.83.180.173.22 > 192.168.62.70.48560: P 903999423:903999444(21) ack 4250994283 win 140 <nop,nop,timestamp 513898282
1045829957>
  7: 01:17:38.528613      192.168.62.70.48560 > 10.83.180.173.22: . ack 903999444 win 229 <nop,nop,timestamp 1045829961 513898282>
```

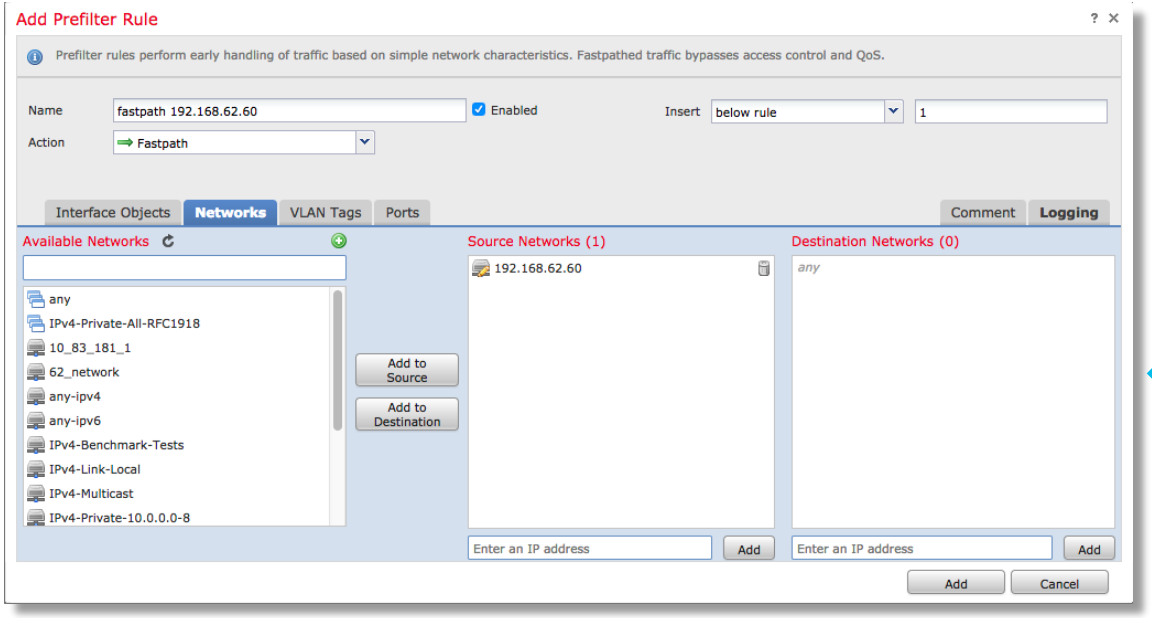
SHELL

```
> show capture ssh_traffic packet-number 4 trace

7 packets captured

  4: 01:17:38.511982      192.168.62.70.48560 > 10.83.180.173.22: P
4250994242:4250994283(41) ack 903999423 win 229 <nop,nop,timestamp
1045829957 513898266>
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
```

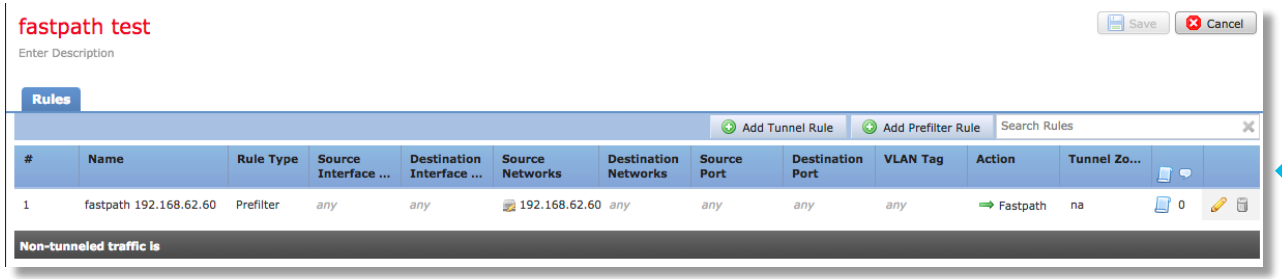
SHELL

```
Phase: 3
Type: FLOW-LOOKUP
Subtype:
Result: ALLOW
Config:
Additional Information:
Found flow with id 626406, using existing flow

Phase: 4
Type: EXTERNAL-INSPECT
Subtype:
Result: ALLOW
Config:
Additional Information:
Application: 'SNORT Inspect'
```

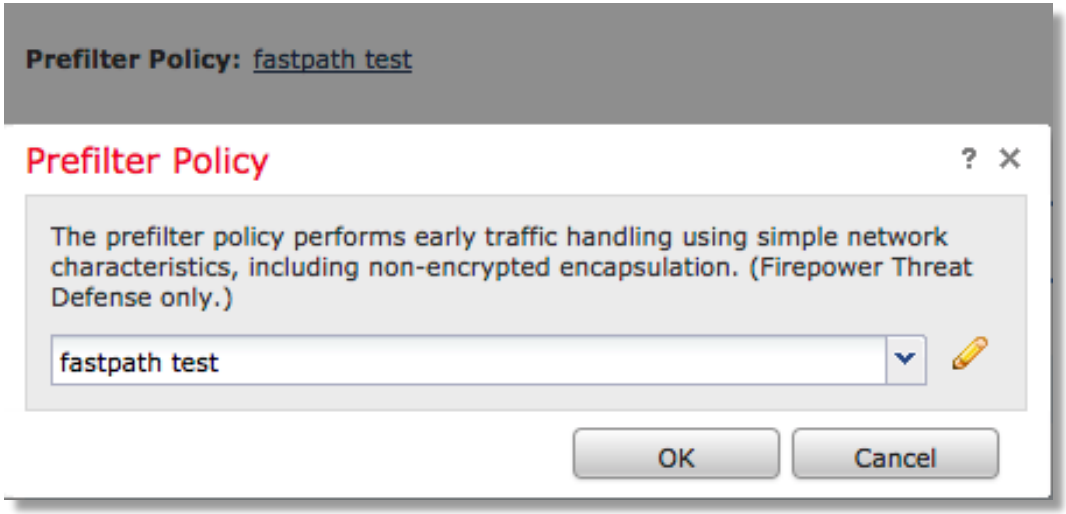




Clicking **Add Prefilter Rule** button will display this popup window.



View of all rules in the **fastpath test** Prefilter policy



From AC policy make sure the Prefilter Policy is set to the custom Prefilter Policy

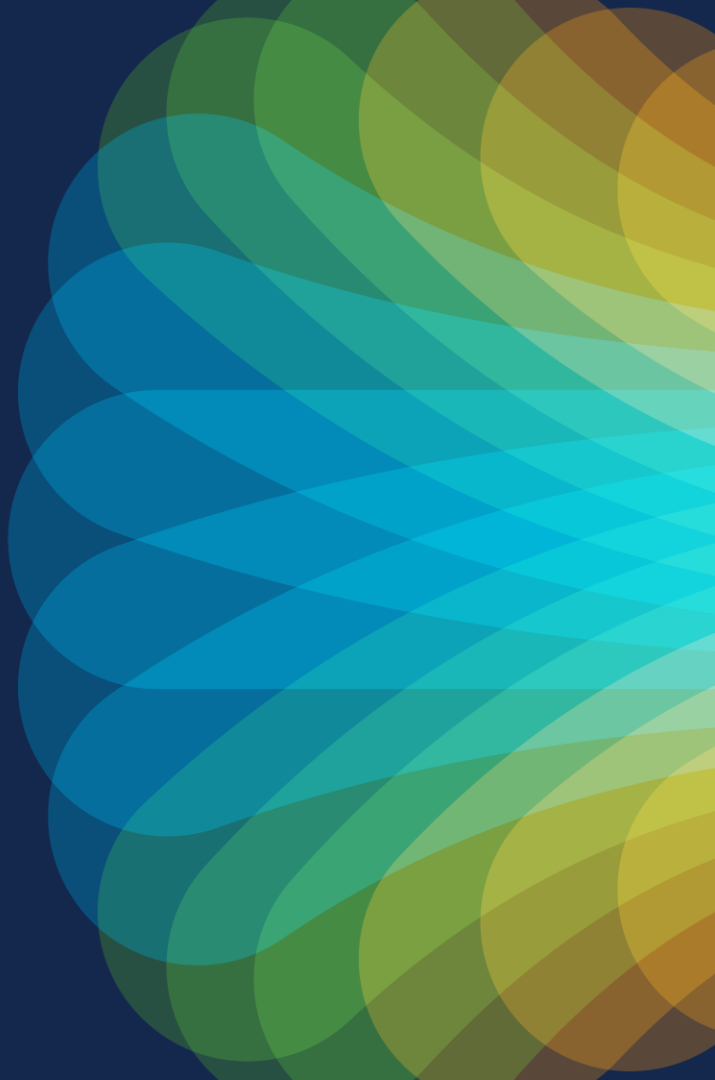
View of connection events matching

First Packet	Last Packet	Action	Reason	Initiator IP	Responder IP	Source Port / ICMP Type	Destination Port / ICMP Code	Prefilter Policy	Tunnel/Prefilter Rule
2017-05-15 16:05:14	2017-05-15 16:05:14	Fastpath		192.168.62.60	10.83.180.173	48480 / tcp	22 (ssh) / tcp	fastpath test	fastpath 192.168.62.60

Security Intelligence

Tool Introduction

- Connection / Security Intelligence Events
- Unified Event Viewer



Security Intelligence

Tools

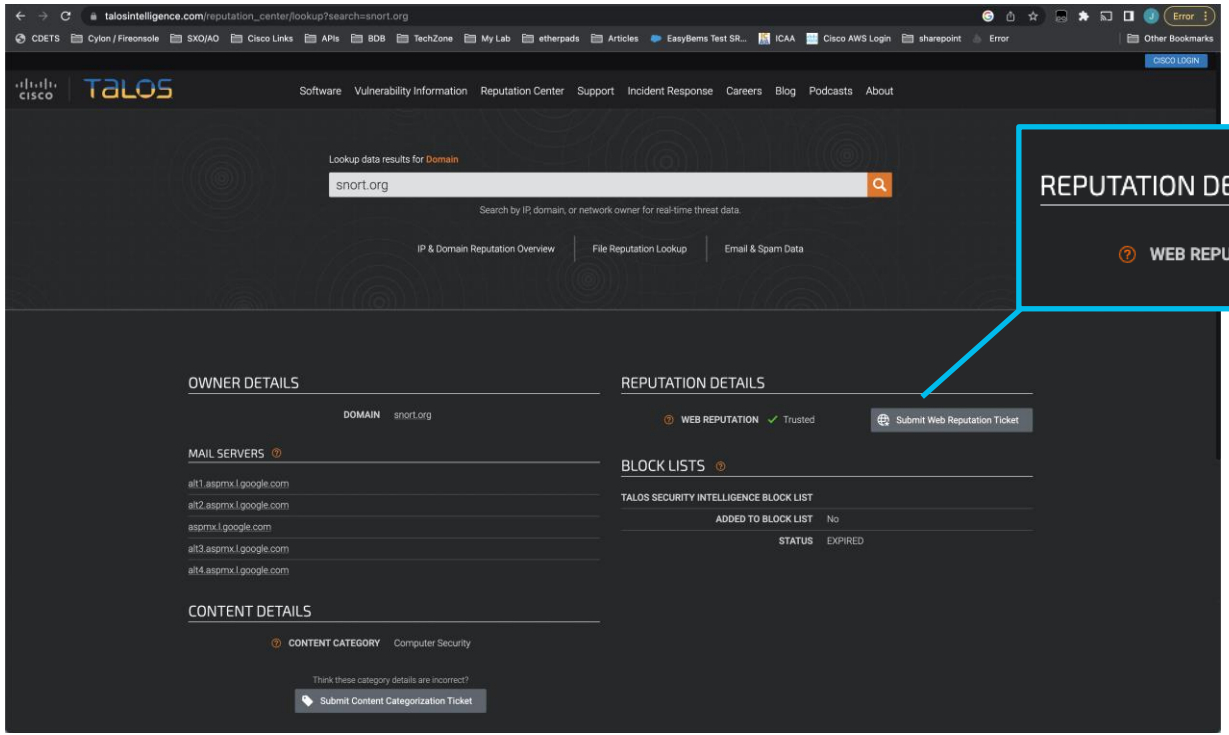
- **Capture W/ Trace**
- **Check SI events for Blocks**
  - **Analysis > Connections > Security Intelligence Events**
  - **Unified Event Viewer**

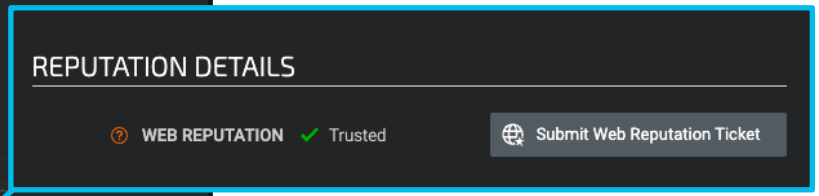
Remediations

- **Add to do-not-block IP/URL/DNS**
- **Remove IP/URL/DNS from Block List if custom list**
- **If reputation is wrong open Talos reputation ticket**

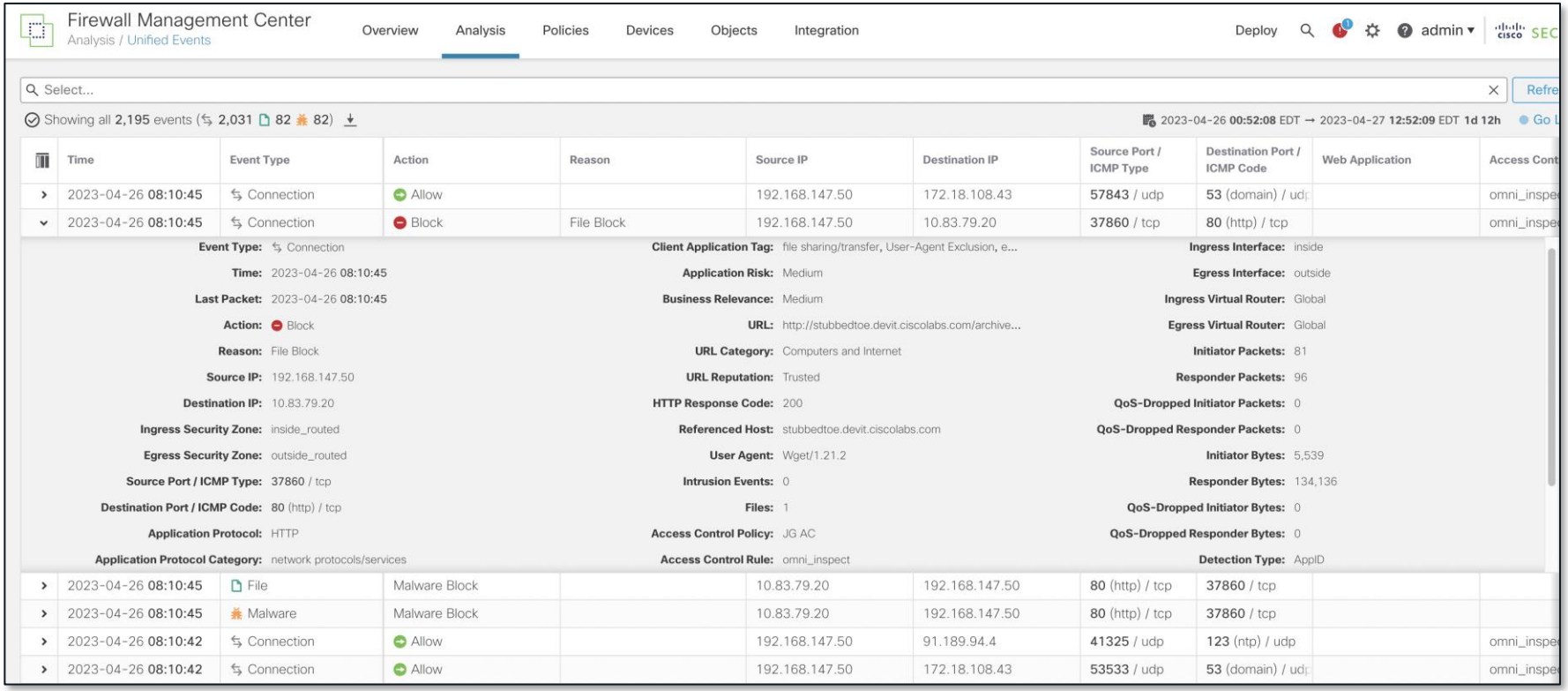
Talos Reputation Center

https://www.talosintelligence.com/reputation_center

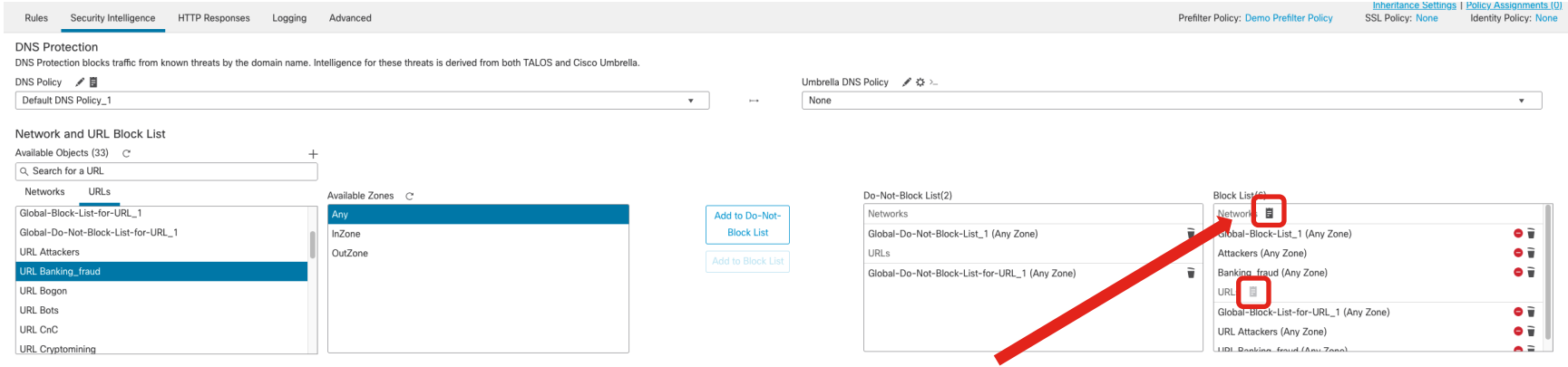




Unified Event Viewer



Security Intelligence - Logging



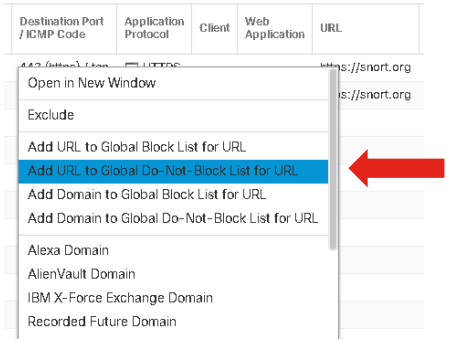
Ensure logging is enabled

Analysis > Connections > Security Intelligence Events

First Packet	Last Packet	Action	Reason	Initiator IP	Responder IP	Security Intelligence Category
2017-05-16 17:00:16		Domain Not Found	DNS Block	192.168.1.95	[redacted]	DNS Response
2017-05-16 16:57:50	2017-05-16 16:57:50	Block	URL Block	192.168.1.95	10.83.48.40	my_custom_url
2017-05-16 16:50:05		Block	IP Block	192.168.1.95	[redacted]	Malware

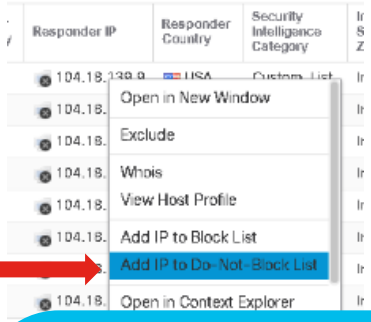
With logging enabled for all SI types you should be able to easily see what is being blocked by SI.

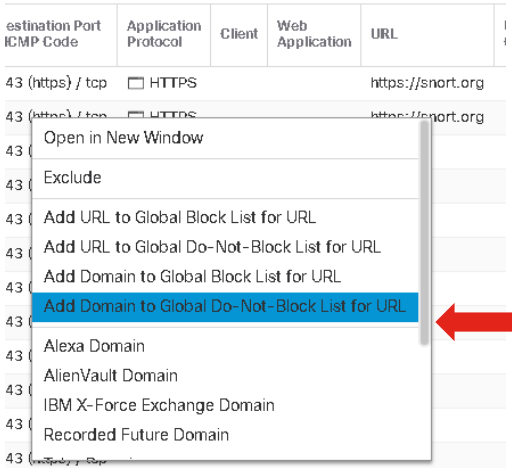
Security Intelligence – Domain and Global Lists



URL

IP



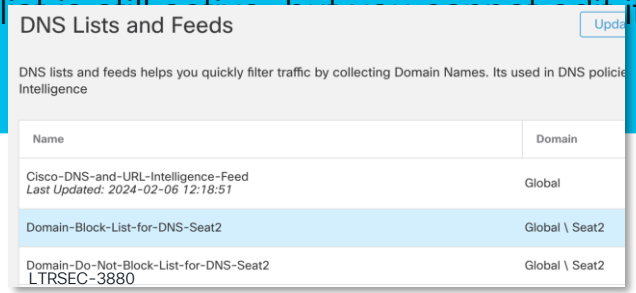


DNS

Do-Not-Block Lists

Important Note

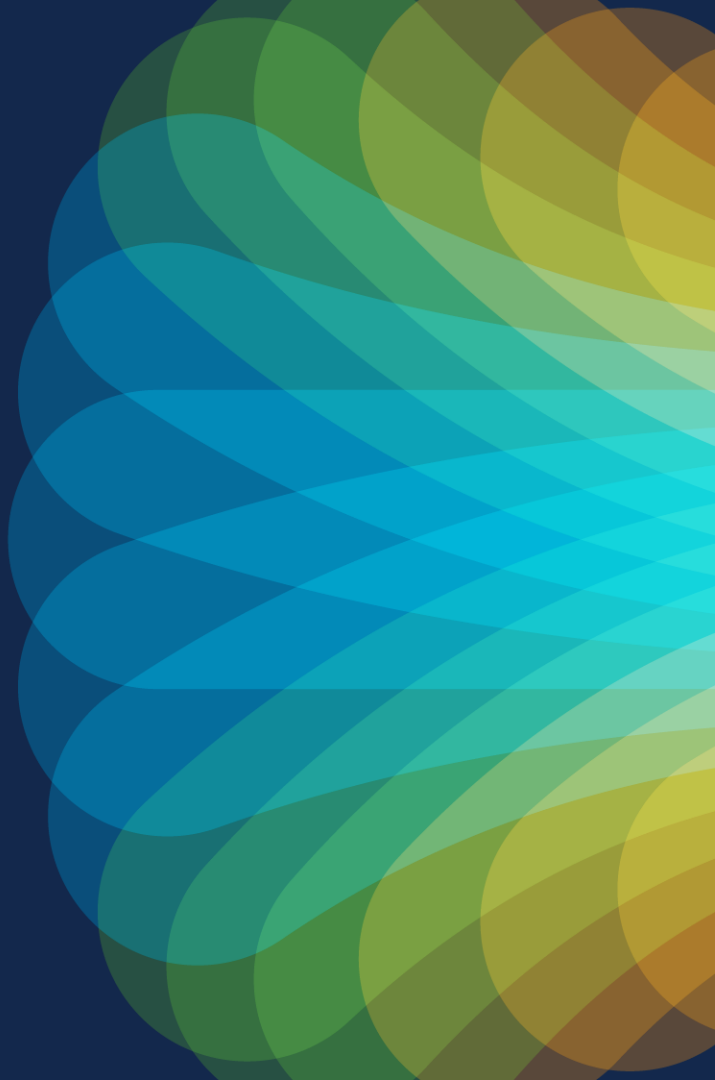
- Do-Not-Block lists are specific to FMC domain(tenant).
- A user in a sub-domain on FMC can only add to their domain Do-Not-Block list
- Global l… …t



Access Control

Tool Introduction

- firewall-engine-debug



Identification - Access Control Policy

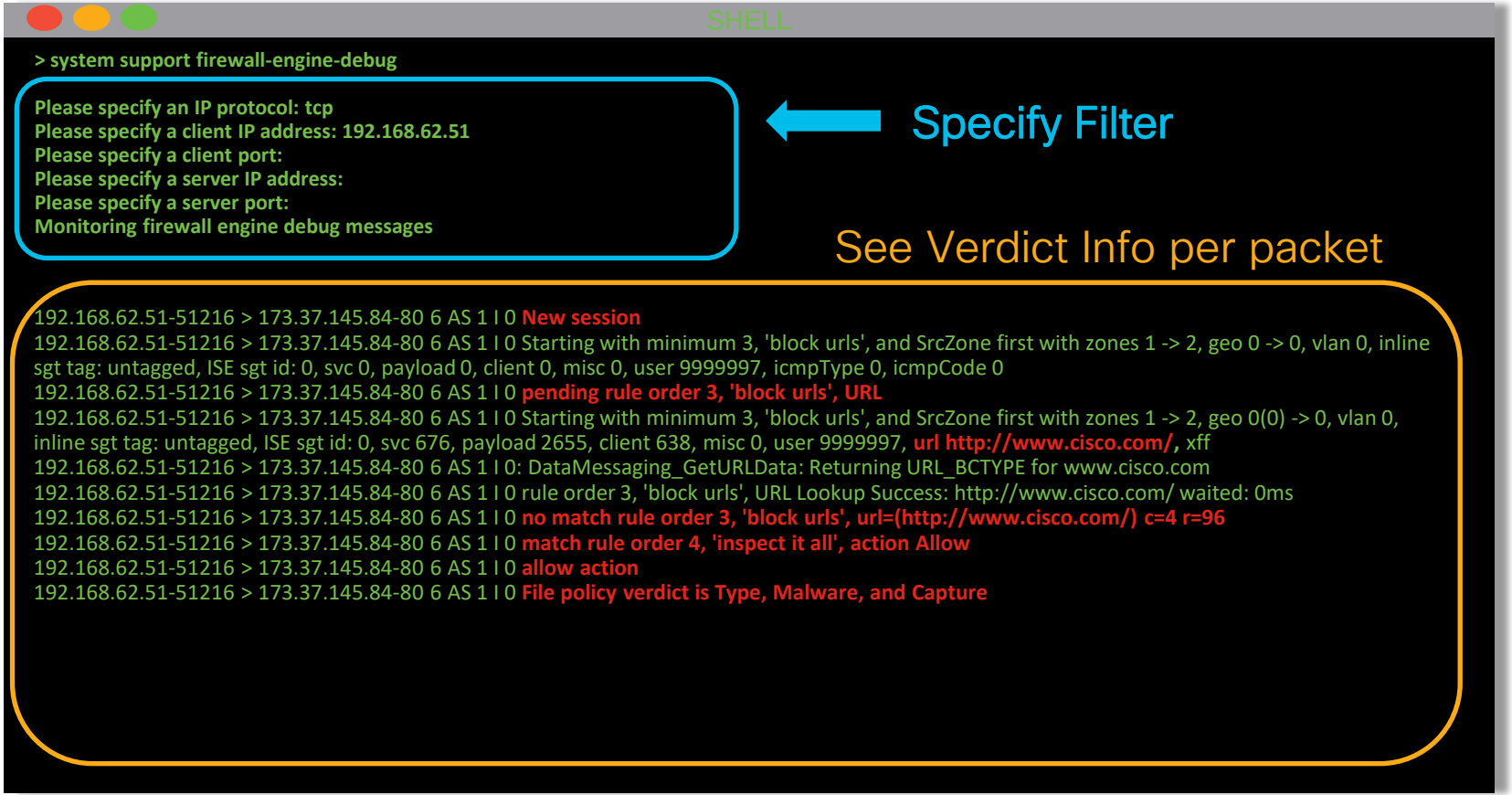
Tools

- **Capture W/ Trace**
- **Check Connection Events**
- **Firewall Engine Debug**
  > system support firewall-engine-debug

Remediations

- **Update Access Control Rule to comply with intent of the policy**
- **Create a trust rule for traffic above rule that is blocking**
- **Disable block rules**

system support firewall-engine-debug



system support firewall-engine-debug

SHELL

```
198.18.133.200-80 - 198.19.10.21-57952 6 Packet: TCP, ACK, seq 4158339379, ack 3255462552
198.18.133.200-80 - 198.19.10.21-57952 6 Stream: TCP session was already blocked, drop
198.18.133.200-80 - 198.19.10.21-57952 6 AppID: service unknown (0), application unknown (0), out-of-order
198.19.10.21-57952 > 198.18.133.200-80 6 Firewall: allow rule, 'Default Action', allow
198.19.10.21-57952 > 198.18.133.200-80 6 Snort: processed decoder alerts or actions queue, drop
198.19.10.21-57952 > 198.18.133.200-80 6 Snort id 0, NAP id 2, IPS id 1, Verdict BLACKLIST
198.19.10.21-57952 > 198.18.133.200-80 6 ===> Blocked by Stream
Verdict reason is sent to DAQ
```

Flow is blocklisted, to see reason you need to find first block message for this session

Check logging for block rules

#	Name	Sou... Zon...	Dest Zon...	Sou... Net...	Dest Net...	VLA...	Use...	App...	Sou...	Des...	URLs	ISE... Attr...	Acti...
Mandatory - My AC Policy (1-2)													
1	block with logging	any	any	any	any	any	any	YouT Youtu	any	any	any	any	Blocl 0
2	block no logging	any	any	any	any	any	any	any	any	any	Gaml	any	Blocl 0

Add trust rule

1	Trust traffic	any	any	192.	any	any	any	any	any	any	any	any	Trus 0
2	block with logging	any	any	any	any	any	any	YouT Youtu	any	any	any	any	Bloc 0
3	block no logging	any	any	any	any	any	any	any	any	any	Gam	any	Bloc 0

Create blank AC policy

#	Name	Sour... Zones	Dest Zones	Sour... Netw...	Dest Netw...	VLAN...	Users	Appli...	Sour...	Dest ...	URLs	ISE/... Attri...	Action
Mandatory - Test - No rules (-)													
There are no rules in this section. Add Rule or Add Category													
Default - Test - No rules (-)													
There are no rules in this section. Add Rule or Add Category													
Default Action													Intrusion Prevention: Balanced Security and Connectivity

#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN ...	Users	Applic...	Sourc...	Dest P...	URLs	ISE/S... Attrib...	Acti...
Mandatory - JG AC (all) (1-6)													
1	Trust ssh for host	Any	Any	192.168.0.7	Any	Any	Any	Any	Any	SSH	Any	Any	Trust
2	inspect	Any	Any	10.0.0.0/8	Any	Any	Any	Any	Any	Any	Any	Any	Allow
3	trust server backup	Any	Any	192.168.62.3	10.123.175.22	Any	Any	Any	Any	Any	Any	Any	Trust

Original Client IP (HTTP)

SSH Connection from 192.168.62.3 to 10.123.175.22

1. SYN 192.168.62.3 → 10.123.175.22
2. SYN,ACK 10.123.175.22 → 192.168.62.3
3. ACK 192.168.62.3 → 10.123.175.22
4. SSH 192.168.62.3 → 10.123.175.22

Starts evaluation at 'inspect' rule

Pending AppID

Service identified as SSH

No match 'inspect' rule (non-http)

Match 'trust server backup' rule and Trust flow

SYN
SYN,ACK
ACK
First SSH Packet (client to server)

SSH Connection from 192.168.62.3 to 10.123.175.22

firewall-engine-debug

SHELL

```
192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 I 0 New session
192.168.62.3-46594 > 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
192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 I 0 pending rule order 4, 'inspect', XFF wait for AppId

192.168.62.3-46594 > 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
192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 I 0 pending rule order 4, 'inspect', XFF wait for AppId

192.168.62.3-46594 > 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
192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 I 0 pending rule order 4, 'inspect', XFF wait for AppId

192.168.62.3-46594 > 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 846, payload -1, client 2000000846, misc 0, user 9999997, icmpType 0, icmpCode 0
192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 I 0 no match rule order 4, 'inspect', XFF non-http
192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 I 0 match rule order 5, 'trust server backup', action Trust
```

How to Map service ID (svc) to name

firewall-engine-debug

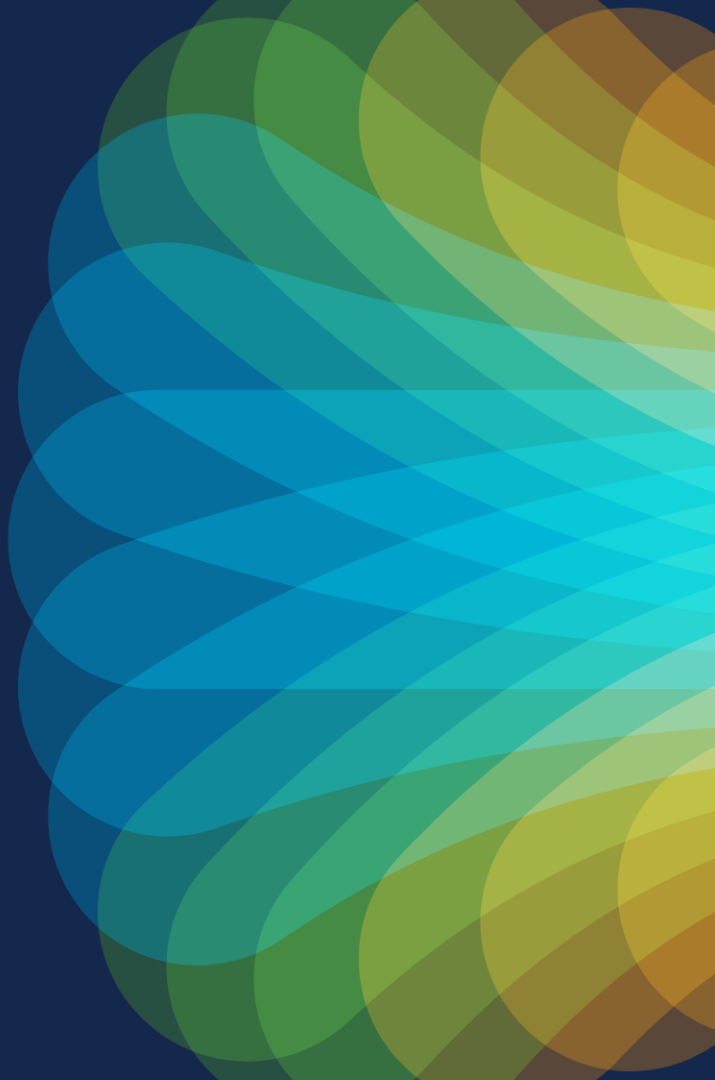
SHELL

```
192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 I 0 New session
192.168.62.3-46594 > 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
192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 I 0 pending rule order 4, 'inspect', XFF wait for AppId

[…omitted for brevity]

192.168.62.3-46594 > 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 846, payload -1, client 2000000846, misc 0, user 9999997, icmpType 0, icmpCode 0
192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 I 0 no match rule order 4, 'inspect', XFF non-http
192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 I 0 match rule order 5, 'trust server backup', action Trust



[! How to map service/application ID to name]
> expert
$ grep "^846[^0-9]" /var/sf/appid/odp/appMapping.data
846 SSH 32 0 0 ssh
```

Intrusion Prevention System (IPS)

Tool Introduction

- system support trace



Identification – Intrusion Policy

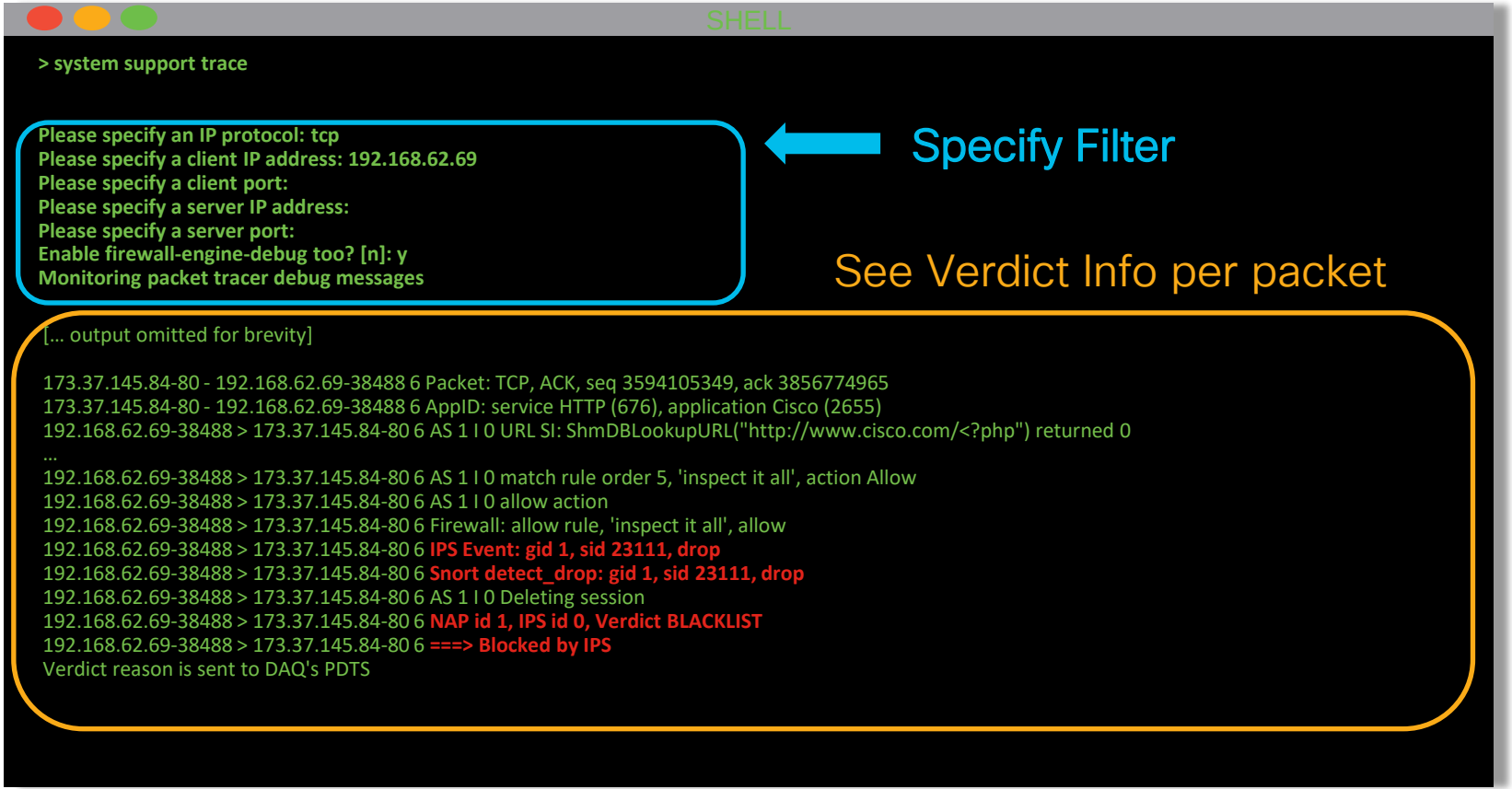
Tools

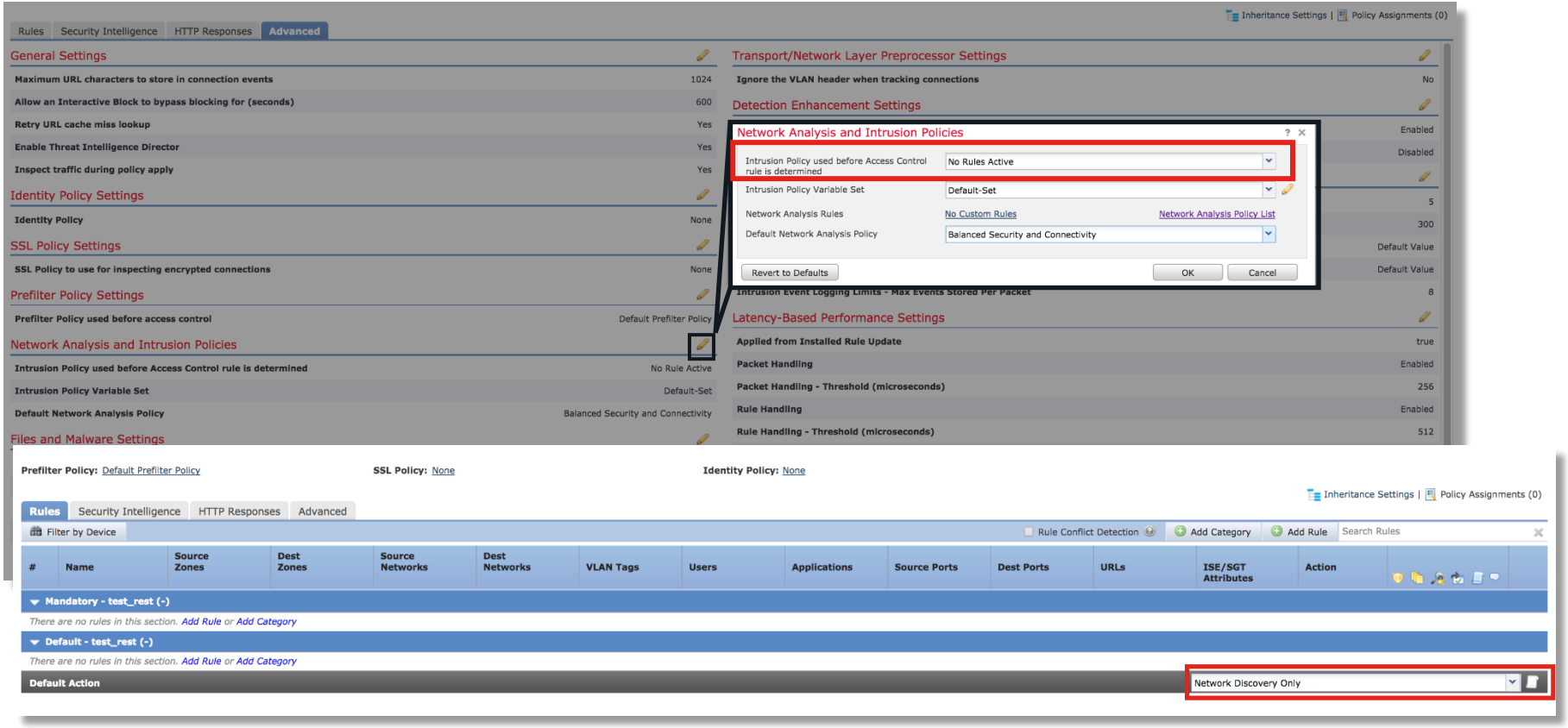
- **Capture W/ Trace**
- **Check Connection Events**
- **Review Snort Configurations**
- **Check Intrusion Events**
- **System Support Trace**

Remediations

- **Disable rule(s) impacting traffic**
- **Targeted intrusion policies**
- **Open SR for False Positive/Coverage**
- **Use No Rules Active policy**
- **Disable Drop when Inline**

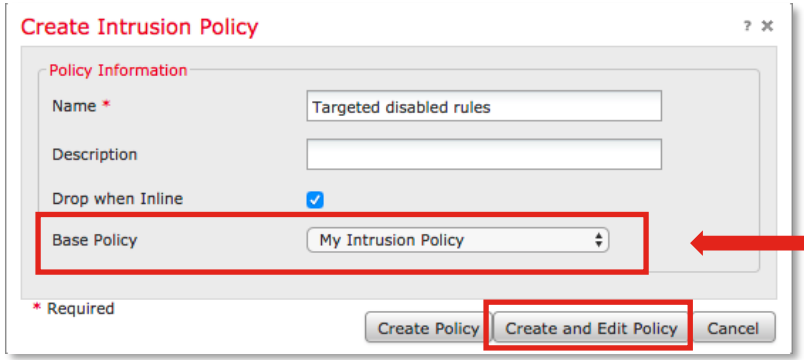
system support trace





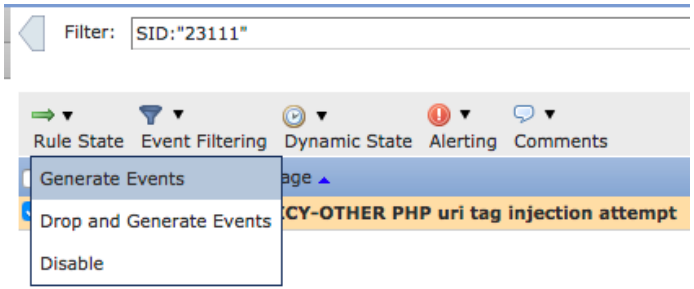
Targeted intrusion policy

Create a new Intrusion policy



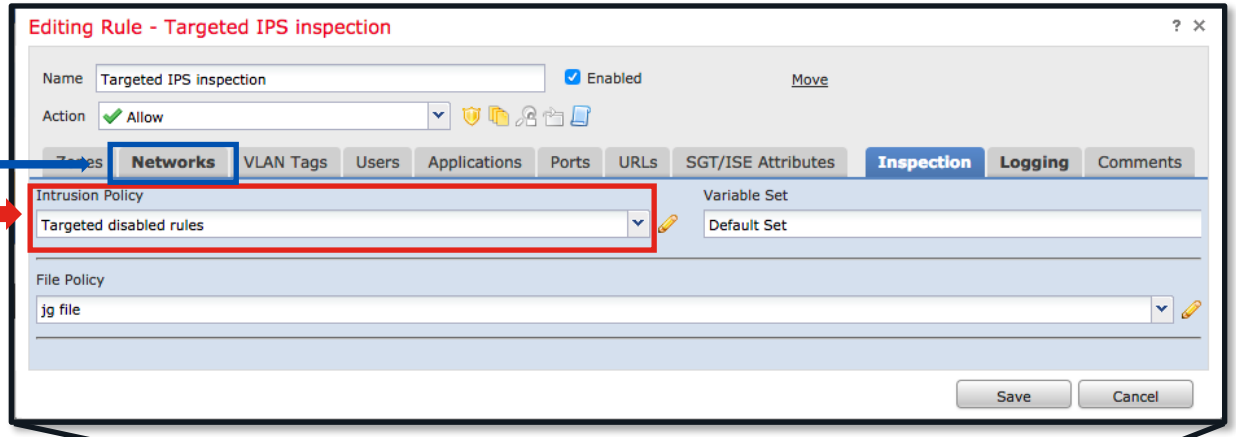
Use your custom policy as base policy

Create and edit policy and set rule state(s)



Add AC rule to use intrusion policy on targeted hosts

Targeted intrusion policy



Target source hosts

Use targeted policy

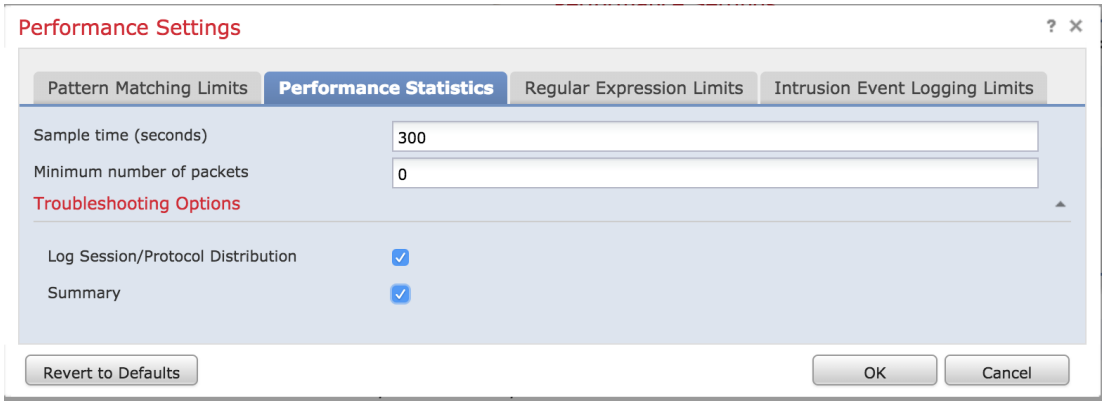
Snort Performance

Low IPS performance? … rule it out by FTD rule profiling!

Edit /ngfw/var/sf/detection_engines/<uuid>/ advanced/perf_monitor.conf

config profile_rules: print all, sort avg_ticks, filename /ngfw/var/log/profiling-rules.log

config profile_preprocs: print all, sort avg_ticks, filename /ngfw/var/log/profiling-preprocs.log



Restart Snort

pmtool restartbytype snort

Start rule profiling

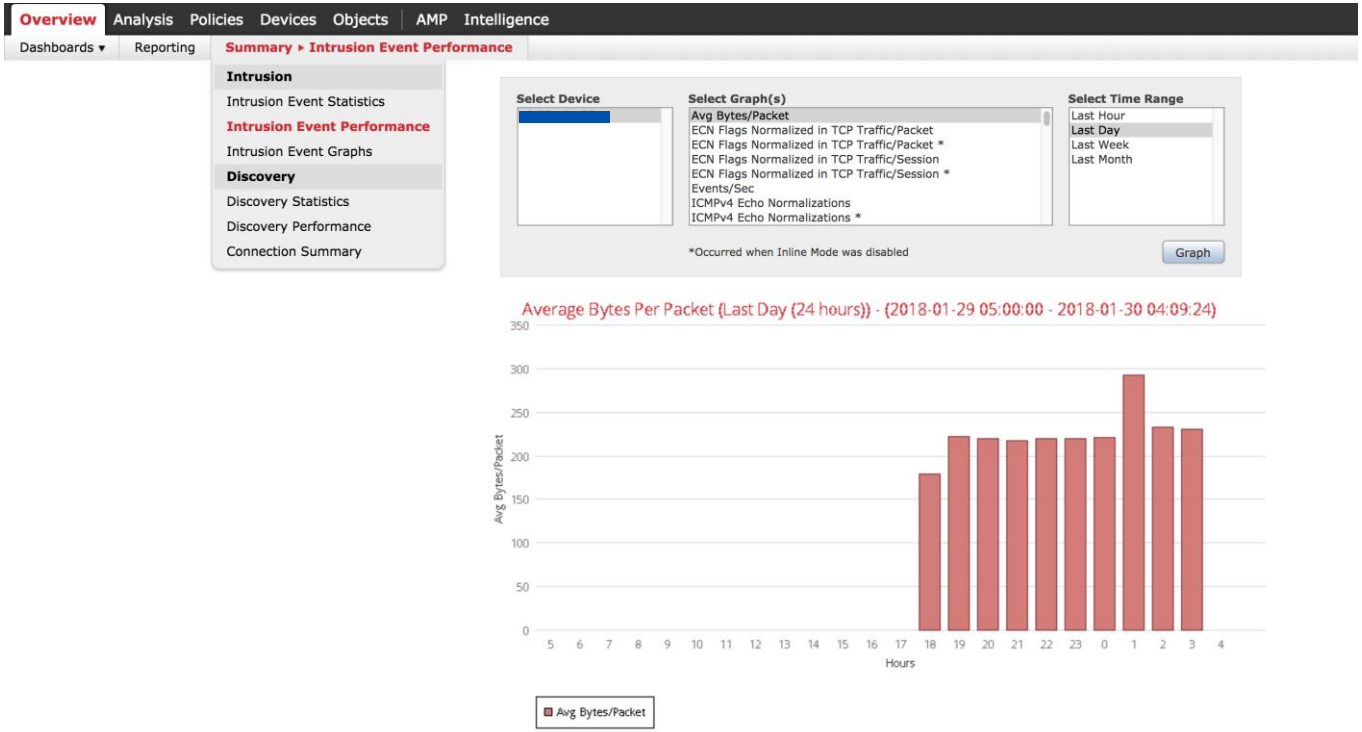
> system support run-rule-profiling

Low IPS performance? ... rule it out by FTD rule profiling!

```
Jan 30 10:34:07 ciscoasa SF-IMS[29795]: Preprocessor Profile Statistics (worst 100)
Jan 30 10:34:07 ciscoasa SF-IMS[29795]: ====================================================
Jan 30 10:34:07 ciscoasa SF-IMS[29795]:  Num           Preprocessor Layer     Checks      Exits          Microsecs  Avg/Check Pct of Caller Pct of Total
Jan 30 10:34:07 ciscoasa SF-IMS[29795]:  ===           ============ =====     ======      =====          =========  ========= ============= ============
Jan 30 10:34:07 ciscoasa SF-IMS[29795]:   1                 fwApp     0        388        388              13759     35.46         24.22        24.22
Jan 30 10:34:07 ciscoasa SF-IMS[29795]:   1              fwAppTP      1        363        363               5530     15.23         40.19         9.74
Jan 30 10:34:07 ciscoasa SF-IMS[29795]:   1            fwLibAppTP     2         52         52               4621     88.87         83.57         8.14
Jan 30 10:34:07 ciscoasa SF-IMS[29795]:   2           fwServicePat     1        123        123               4692     38.15         34.10         8.26
Jan 30 10:34:07 ciscoasa SF-IMS[29795]:   3           luaDetectors     1         72         72               3601     50.02         26.18         6.34
Jan 30 10:34:07 ciscoasa SF-IMS[29795]:   1                cisco     2         72         72               3596     49.96         99.87         6.33
Jan 30 10:34:07 ciscoasa SF-IMS[29795]:     1cisco_7e11c2fa-d3dd-42a9-b71a-8db3e71d9571     3         71         71               3410     48.03         94.81         6.00
Jan 30 10:34:07 ciscoasa SF-IMS[29795]:     2cisco_90d30535-1aec-4598-835a-e20c321b562e     3          1          1                175    175.25          4.87         0.31
Jan 30 10:34:07 ciscoasa SF-IMS[29795]:   4           fwClientPat     1         83         83                624      7.53          4.54         1.10
```

```
Jan 30 10:34:07 ciscoasa SF-IMS[29795]: Rule Profile Statistics (all rules)
Jan 30 10:34:07 ciscoasa SF-IMS[29795]: ============================================================
Jan 30 10:34:07 ciscoasa SF-IMS[29795]:    Num      SID GID Rev     Checks   Matches    Alerts          Microsecs  Avg/Check  Avg/Match Avg/Nonmatch   Disabled
Jan 30 10:34:07 ciscoasa SF-IMS[29795]:    ===      === === ===     ======   =======    ======          =========  =========  ========= ============   ========
Jan 30 10:34:07 ciscoasa SF-IMS[29795]:      1    42892   1   1          2         0         0                 24       12.2        0.0          12.2          0
Jan 30 10:34:07 ciscoasa SF-IMS[29795]: ============================================================================
```

Performance graphs from the WebUI



Why does Bytes/Packet matter?

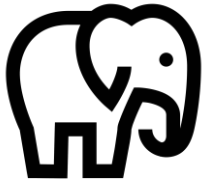
Reassembly…

Posted throughput ratings for the Firepower appliances are usually rated at 1518 bytes packets. Smaller packets results in more processing.

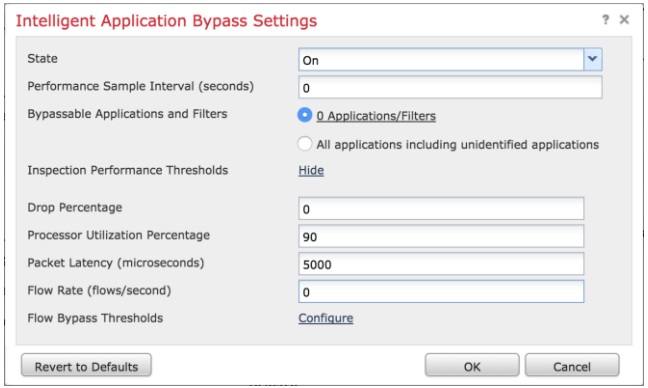
- 1MB of traffic with 1518 bytes/packets = ~ 658 packets
- 1MB of traffic with 400 bytes/packet = ~ 2500 packets

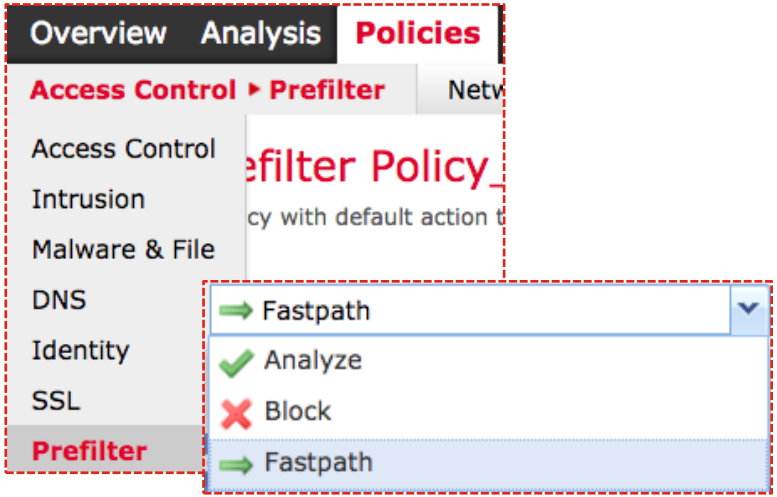
Every packet header must be evaluated and the packet has to be placed into the buffer for re-assembly. The larger number of packets to process requires more CPU time.

Let's talk about the elephant in the room…



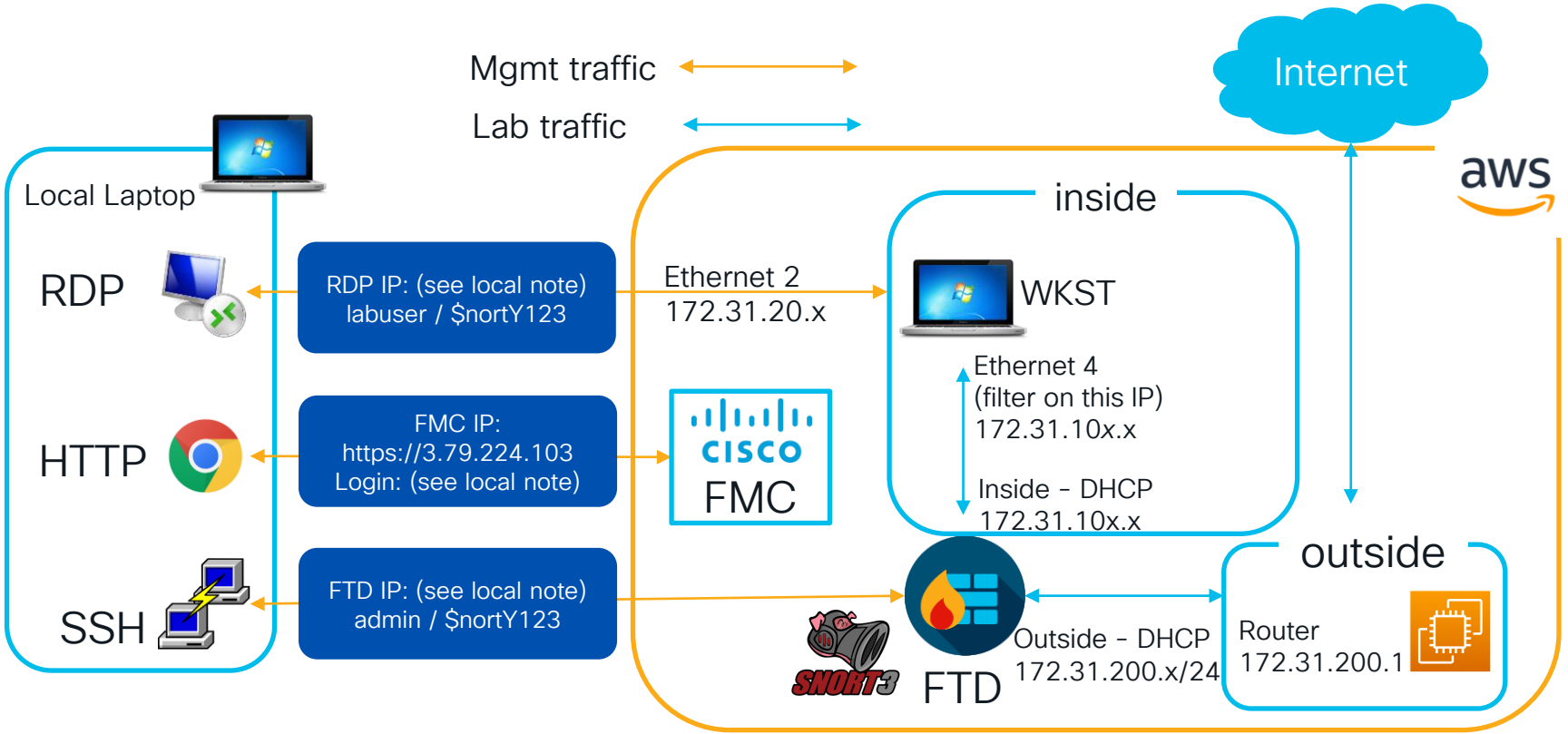
- Large flows are generally related backup, database replication, etc. which usually does not require inspection
- Sort Analysis > Connections for connection size to find top talkers
- Once we determine the top talkers, and confirm they can be safely ignored, we create trust rule for the IP conversations.
- Mitigations IAB / Pre-Filter fast-path





Lab Overview & Instructions

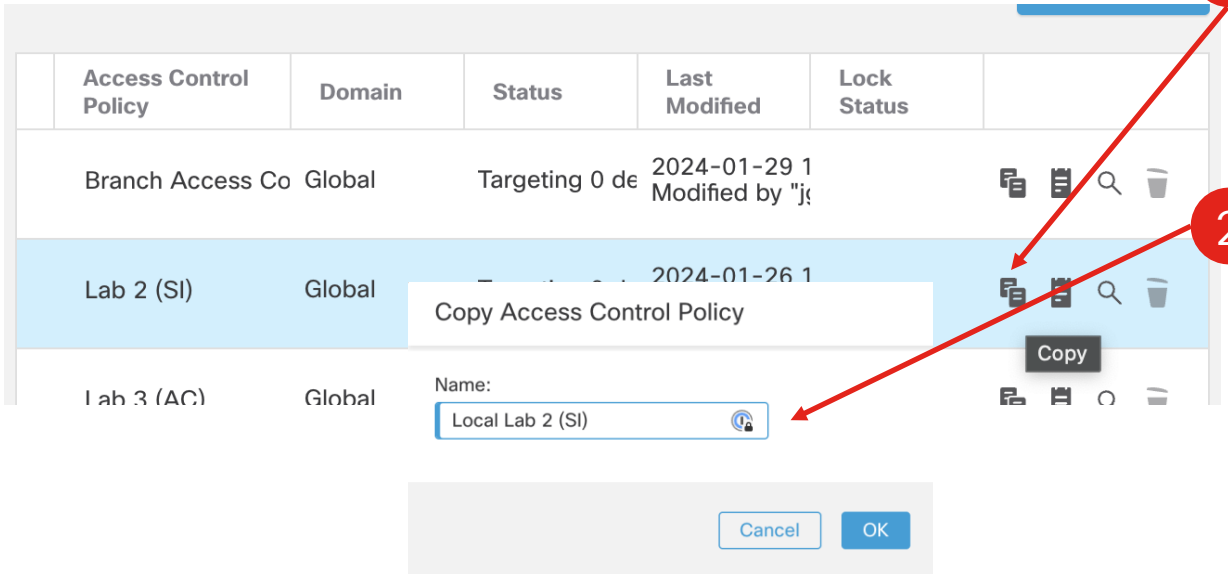
Lab Topology – Interfaces, IPs and Credentials



Make Copy of AC Policy in local domain

For labs 2-4 you will need to make a copy of the AC Policy in your local domain and assign it to the device and deploy in order to start the lab. Some example screenshots for doing this are below.

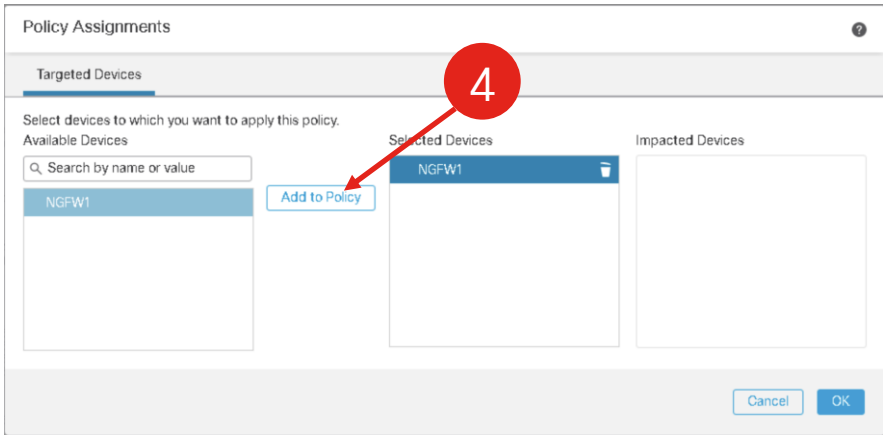
In the FMC UI Navigate to Polices > Access Control

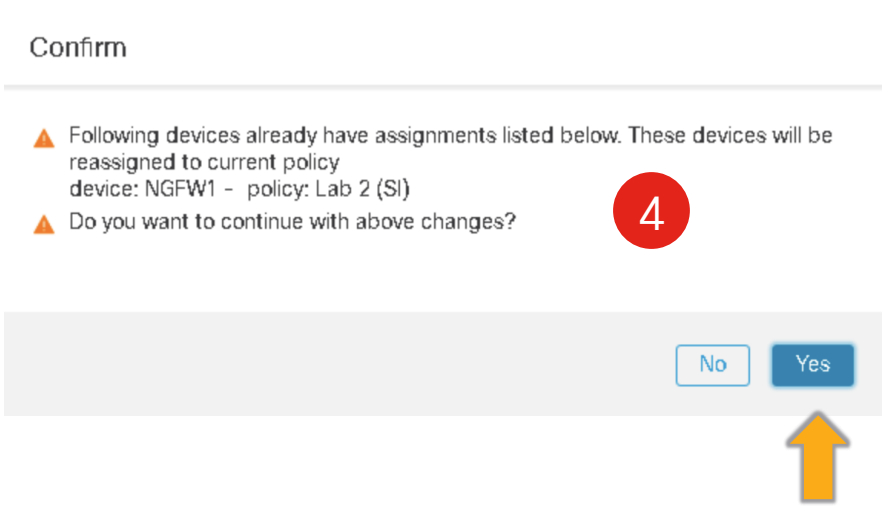


1 Click the copy icon next to the policy for the desired lab

2 Give it a name, hit OK then edit the new policy.

Make Copy of AC Policy in local domain (cont)





Goals / Best Practices / Hints

1. Fix the problem without degrading the security posture of the network
2. Avoid deploys as a troubleshooting step to save time
   - Leverage tools to identify the problem
   - Deploy when you have possible solution
3. Some labs may have more than 1 problem
4. Do NOT change your security zones
5. Ask for help if you are stuck

Note at the start of each lab you should not be able to reach the resource. If the resource is immediately available, something has gone wrong with lab setup. Please ask for help!

Goals / Best Practices / Hints

WKST Desktop background

This is **NOT** the inside IP, it is the RDP private IP. do not filter on this on the FTD, you will not see it there.

On your local desktop you will see a link to box that has all of the information for your personal lab. Use this to find the IPs you need to connect to and login information for the FMC, FTD, WKST.

Windows command tips

ctrl+r, type "**cmd**", press enter to get a terminal
route print – prints routes, make sure only 1 default route going to FTD
ipconfig – list interfaces and ip addresses
ping <host> – simple icmp ping test

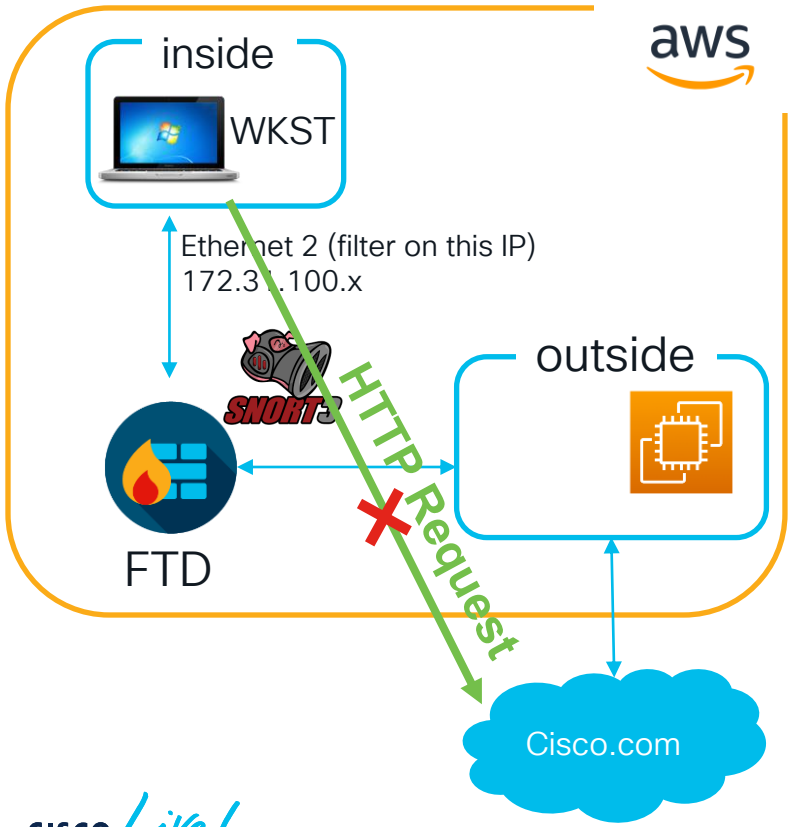
Lab 1

Introduction to Problem Component Identification

Lab 1 steps

1. Open an RDP session to WKST (IP address is on your sticky note)
2. Open a new window in chrome
3. Type “www.cisco.com” into the browser URL bar and hit enter
4. Troubleshoot! Figure out why this connection is being blocked and make the least intrusive change(s) to resolve the issue.

Lab 1 Scenario



Problem Description

WKST is unable to reach www.cisco.com

Instructions

Using the tools introduced, determine why the connection is unsuccessful.

Hints

- ✗ Prefilter policy fastpath
- ✓ Capture w/ Trace
- ✓ Ping next hop

Lab 1 Hints

- What is the first thing that a connection will do

Domain Name Resolution

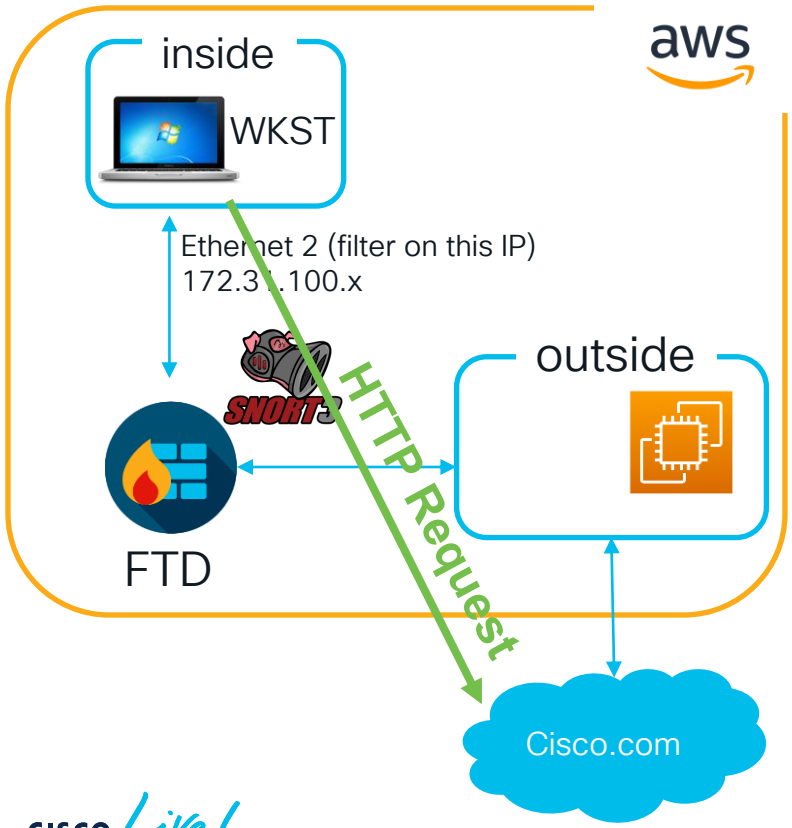
- What should be your Capture W/ Trace Filter

  - Protocol IP
  - Network 172.31.100.0 Netmask 255.255.252.0
  - Look for Port 53 traffic

Capture W/ Trace output structure

172.31.100.7.64579 > 8.8.8.8.53 UDP 28
Src IP.Port > Dst IP.Port Proto length

Lab 1 Solution



Root Cause

No route to host

Solution

Correct the default route by either specifying manually or by enabling DHCP route

Lab 1 – Troubleshooting

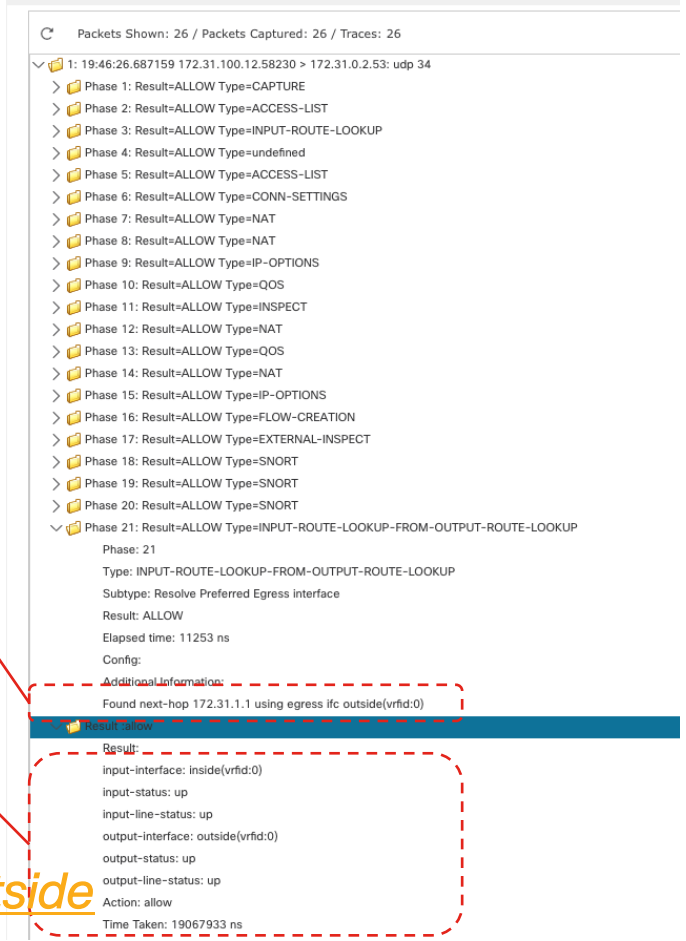
SHELL

```
> ping 172.31.1.1
Please use 'CTRL+C' to cancel/abort...
Sending 5, 100-byte ICMP Echos to 172.31.1.1, timeout is 2 seconds:
?????
Success rate is 0 percent (0/5)
>
```

SHELL

```
> show interface outside
Interface TenGigabitEthernet0/1 "outside", is up, line protocol is up
  Hardware is net_ena, BW 10000 Mbps, DLY 10 usec
        Auto-Duplex(Full-duplex), Auto-Speed(10000 Mbps)
        Input flow control is unsupported, output flow control is unsupported
        MAC address 020b.7c28.ac87, MTU 1500
        IP address 172.31.200.170, subnet mask 255.255.255.0
```

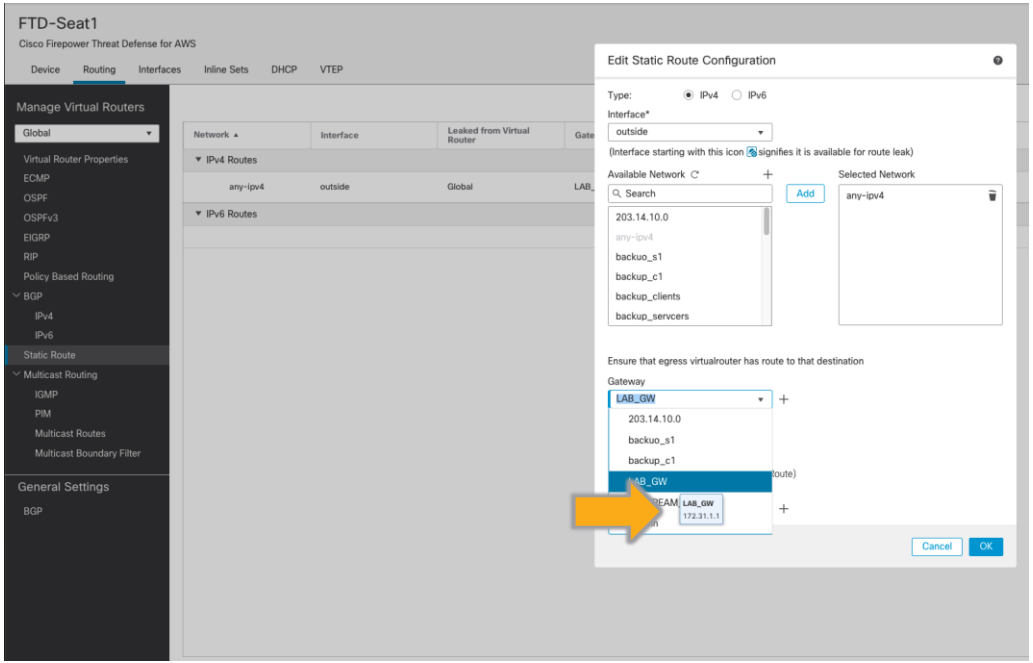
Capture w/trace



Notice that 172.31.1.1 is not in subnet for outside

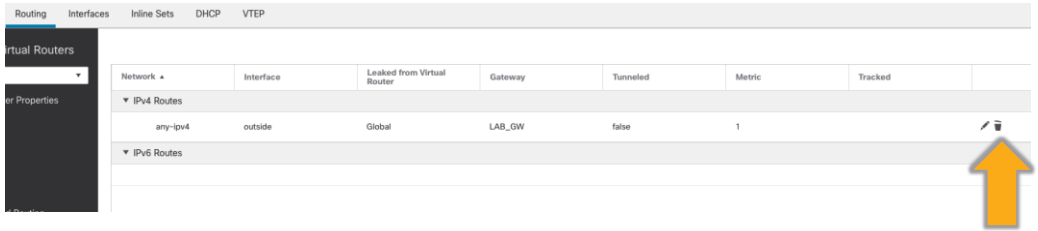
Lab 1 – Root Cause

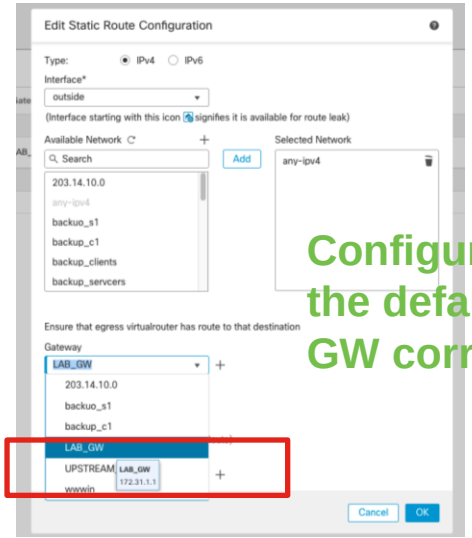
Misconfigured routes - Only static route is for GW 172.31.1.1 which is incorrect for the outside subnet 172.31.200.0/24 the GW should be 172.31.200.1



Lab 1 – Solution

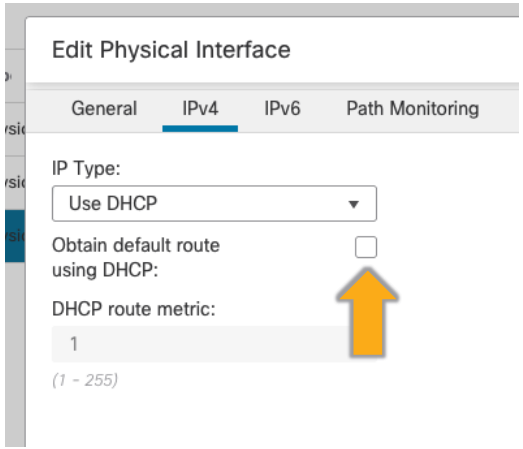
Step 1: Delete Static Route



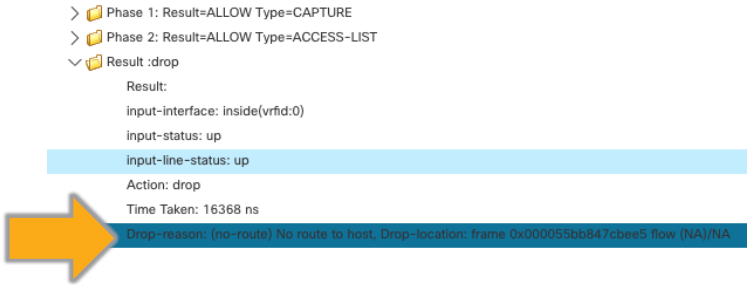


Configure the default GW correctly

Step 2: Set outside interface to use DHCP route



Lab 1 – Solution – Continued



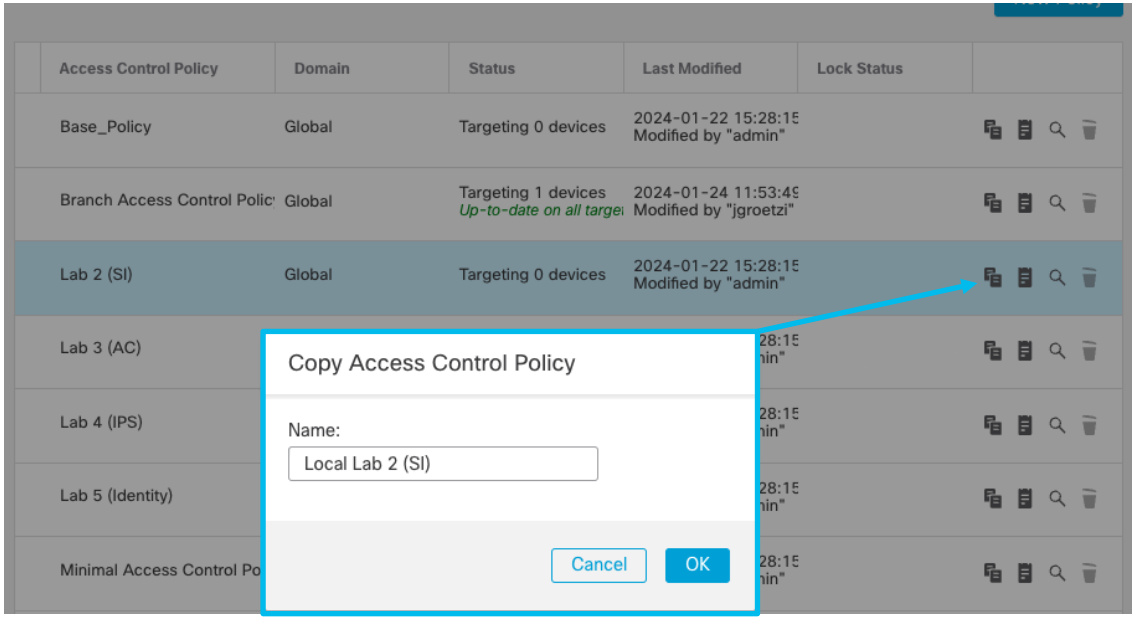
If you see this, you likely deleted the Static route, but didn't enable DHCP route

Lab 2 - Security Intelligence

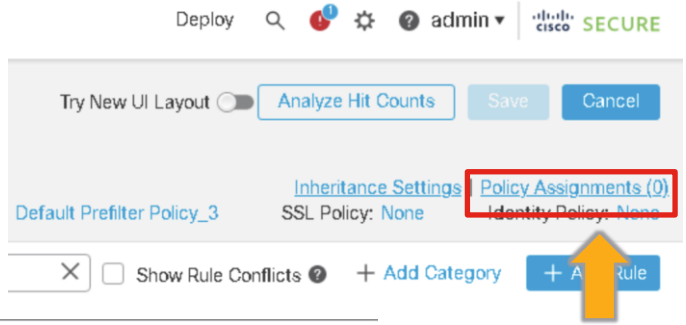
Lab 2 steps

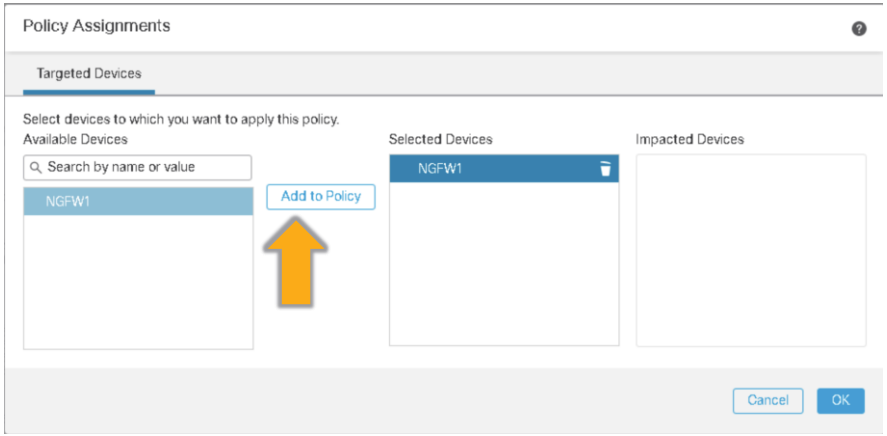
1. Make a copy of the “Lab 2 (SI)” AC Policy in your local domain and assign it to the FTD and deploy (see help slide)
2. Open an RDP session to WKST (see local note)
3. Open a new incognito window in chrome
4. Type “https://snort.org” into the browser URL bar and hit enter
5. Troubleshoot! Figure out why this connection is being blocked and make the least intrusive change(s) to resolve the issue.
6. Do NOT try to modify anything in the Global SI lists and do not delete them from the policy to fix this. Figure out how…..

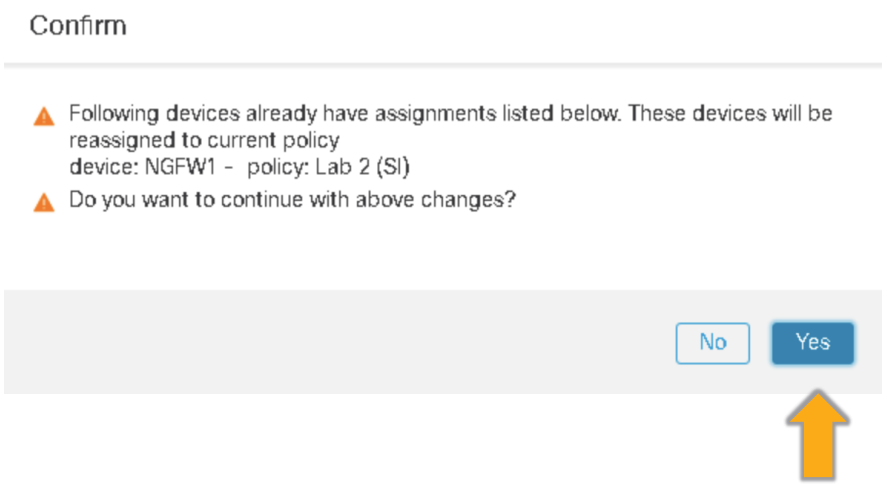
Make a copy of the “Lab 2 (SI)” AC Policy in your local domain



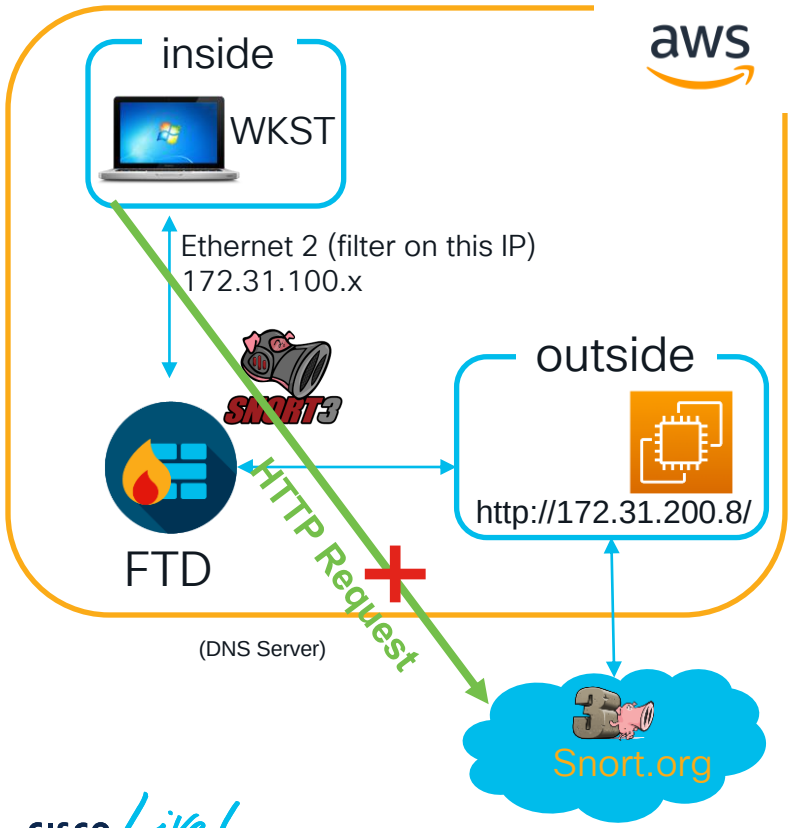
Assign Policy







Lab 2 Scenario



Problem Description

WKST is unable to reach snort.org

Instructions

1. Using the tools introduced, determine why you cannot reach snort.org.
2. BONUS Resolve the issue

Hints

- Connection Events
- Capture w/Trace

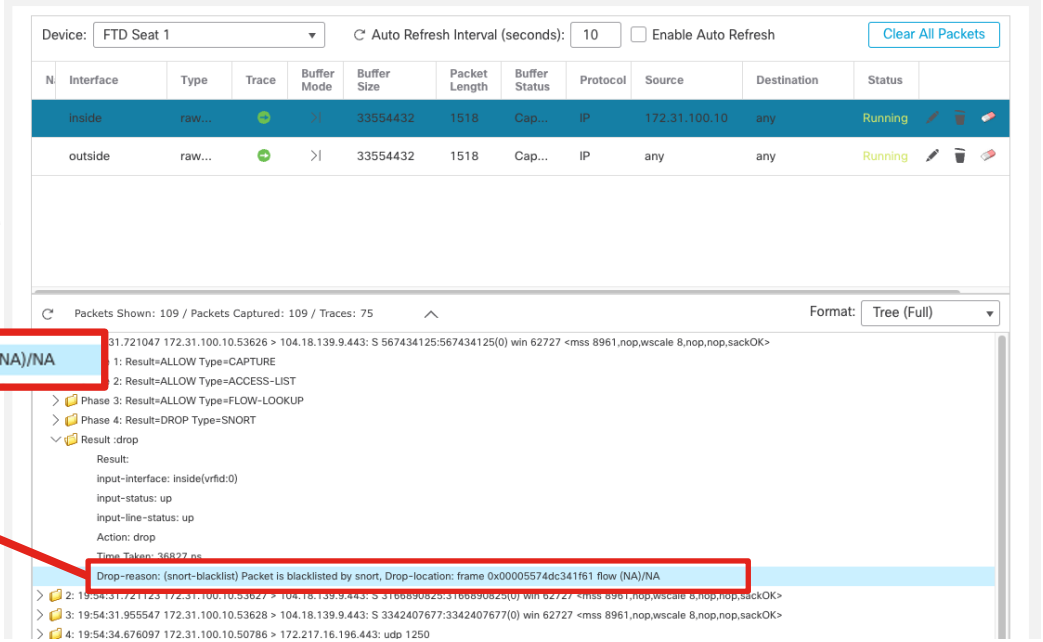
Lab 2 – Troubleshooting

Capture w/trace

Capture W/ Trace tells us its dropped by Security Intelligence..

…But which Security Intelligence list?

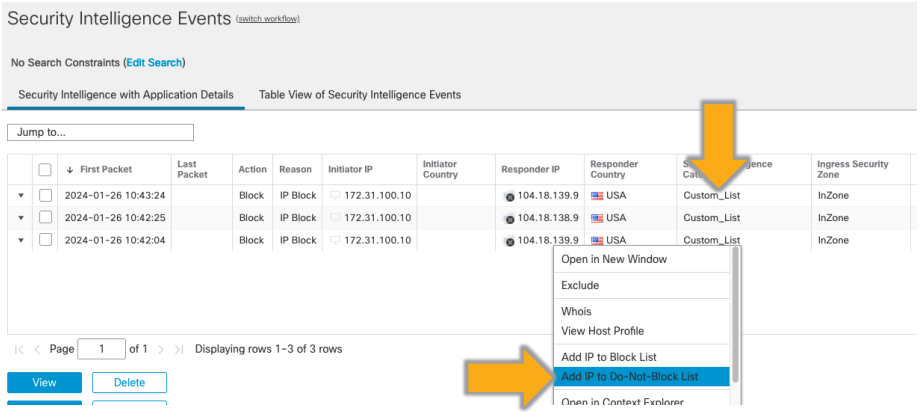
Drop-reason: (snort-blacklist) Packet is blacklisted by snort, Drop-location: frame 0x00005574dc341f61 flow (NA)/NA



Lab 2 – Continued

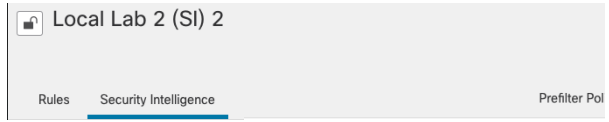
MAKE SURE LOGGING IS ENABLED

Delete URL and Network SI List



Lab 2 – Continued – Do-Not-Block-List

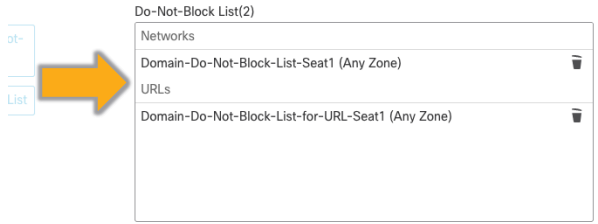
We added the IP to the Do-Not-Block List



…Why does it still not work?

Important Note

- Do-Not-Block lists are specific to FMC domain(tenant).
- A user in a sub-domain on FMC can only add to their domains Do-Not-Block list



Lab 2 – Solution

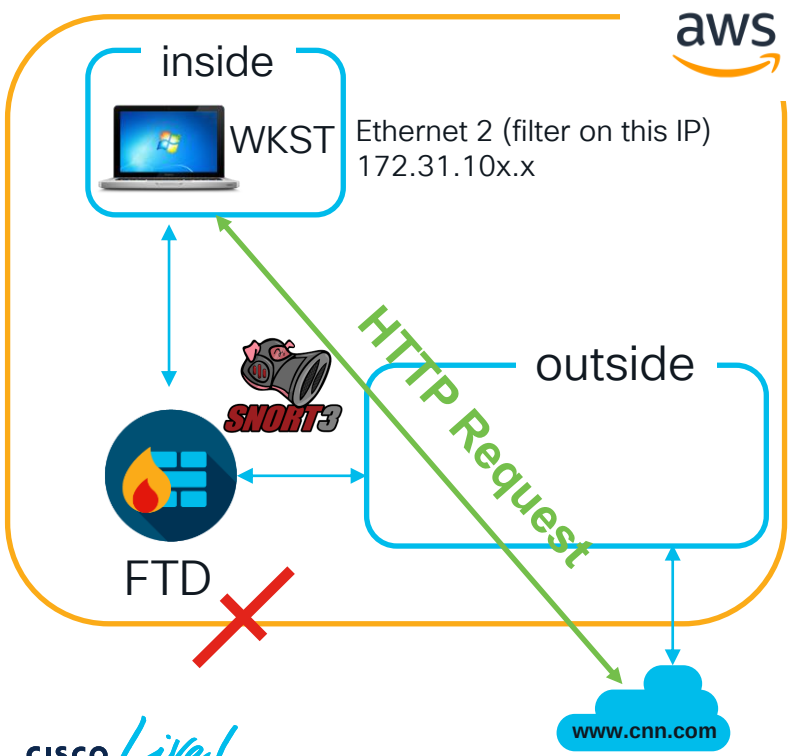
- Add Domain-Do-Not-Block URL & Network List to Access Control Policy
- Add the 2 Snort.org IP addresses to the Domain-Do-Not-Block-List
- Enable Logging for URL Security Intelligence Events
- Add snort.org to the URL Domain-Do-Not-Block-List

Lab 3- Access Control

Lab 3 steps

1. Make a copy of the “Lab 3 (AC)” AC Policy in your local domain and assign it to the FTD and deploy (see help slide)
2. Open an RDP session to your WKST (See local note for IP)
3. Open a new incognito window in chrome
4. Type “http://www.cnn.com” into the browser URL bar and hit enter
5. Troubleshoot! Figure out why this connection is being blocked and make the least intrusive change(s) to resolve the issue. You should only modify the configuration to allow cnn traffic but do not just fastpath at the top of the policy, that is too easy ;) find what is blocking and make the appropriate change(s). Once you have the site allowed, see if anything else on the page isn’t loading properly (but don’t worry about fixing everything for the lab, just main site loading is all that is required but feel free to do more to get the site working to learn more)

Lab 3 Scenario



Problem Description

WKST is unable to reach www.cnn.com

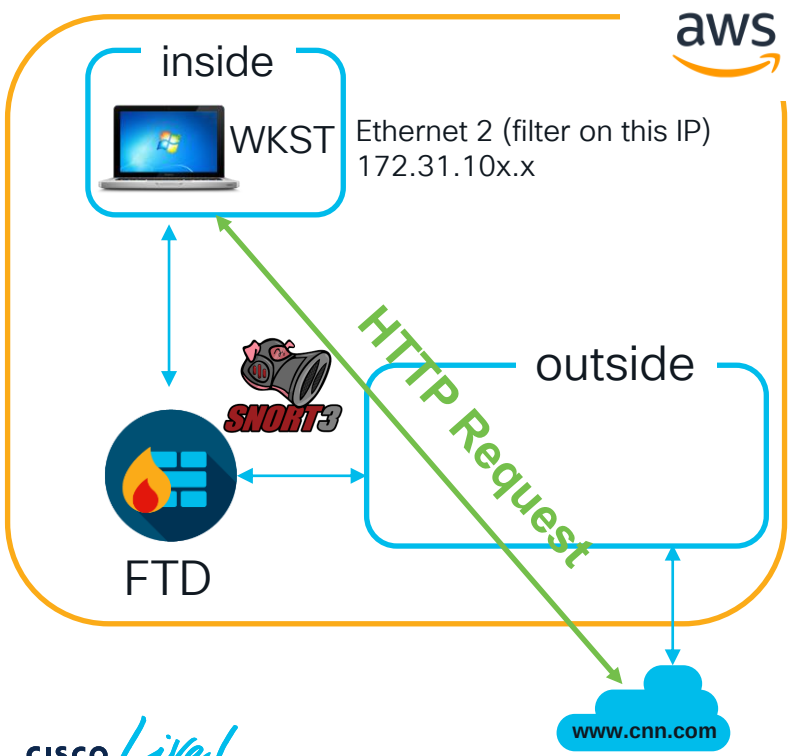
Instructions

Using the tools introduced, determine why the connection is unsuccessful.

Hints

- Prefilter policy fastpath
- Enable AC rule logging
- firewall-engine-debug

Lab 3 Solution



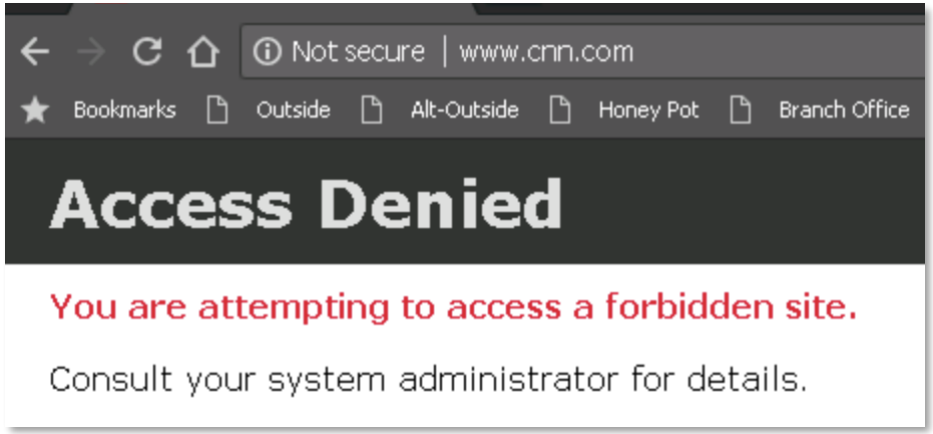
Root Cause

Multiple AC Rules blocking the connection

Solution

Correct the AC rules to allow the traffic

Lab 3 Troubleshooting

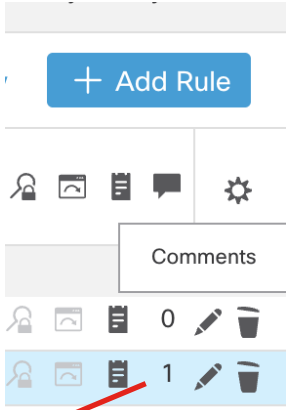


Connection events show this is being blocked by the "Block Fake News" AC Rule

Action	Initiator IP	Responder IP	Responder Country	Destination Port / ICMP Code	Application Protocol	Web Application	URL	Access Control Policy	Access Control Rule
Block with reset	172.31.100.10	146.75.119.5	USA	443 (https) / tcp	HTTPS	CNN.com	https://www.cnn.com	Local Lab 3 (AC)	Block Fake News
Block with reset	172.31.100.10	146.75.119.5	USA	443 (https) / tcp	HTTPS	CNN.com	https://www.cnn.com	Local Lab 3 (AC)	Block Fake News
Block with reset	172.31.100.10	146.75.119.5	USA	80 (http) / tcp	HTTP	CNN.com	http://www.cnn.com/favicon.ico	Local Lab 3 (AC)	Block Fake News

Lab 3 Troubleshooting

Check the rule comments...



Zones | Networks | VLAN Tags | Users | Applications | Ports | URLs | Dynamic Attributes | Inspection | Logging | Comments

Comment History

New Comment

Comment	User	Date
This is to troll Foster and is not a real rule. you can disable this any time.	jgroetzi	2024-1-25 21:06:23

Lab 3 Solution

Lab 3 Troubleshooting

Still Blocked…No Connection events!? Now what?

Option 1

Prefilter fastpath

Pros
- Might fix issue right away

Cons
- May allow unwanted traffic
- No inspection
- No immediate RC
- Requires config change

Option 2

firewall-engine-debug

Pros
- No config change
- Same inspection
- Immediate RC (maybe)

Cons
- Won't fix issue right away
- Higher Difficulty

Lab 3 Troubleshooting

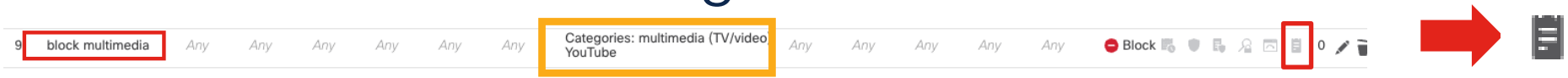
firewall-engine-debug

SHELL

```
> system support firewall-engine-debug

Please specify an IP protocol: tcp
Please specify a client IP address: 172.31.100.10
Please specify a client port:
Please specify a server IP address:
Please specify a server port:
Monitoring firewall engine debug messages

172.31.100.10 54851 -> 146.75.123.5 80 6 AS=0 ID=0 GR=1-1 New firewall session
172.31.100.10 54851 -> 146.75.123.5 80 6 AS=0 ID=0 GR=1-1 Starting with minimum 9, 'block multimedia', and VLan first with zones 3 -> 4, geo 0 -> 0, vlan 0, src sgt: 0, src sgt type: unknown, dst sgt: 0, dst sgt type: unknown, svc 0, payload 0, client 0, misc 0, user 9999997
172.31.100.10 54851 -> 146.75.123.5 80 6 AS=0 ID=0 GR=1-1 pending rule order 9, 'block multimedia', AppID
172.31.100.10 54851 -> 146.75.123.5 80 6 AS=0 ID=0 GR=1-1 app event with client changed, service changed, payload changed, referred no change, misc no change, url changed, tls host no change, bits 0x969C

172.31.100.10 54851 -> 146.75.123.5 80 6 AS=0 ID=0 GR=1-1 Starting with minimum 9, 'block multimedia', and VLan first with zones 3 -> 4, geo 0(xff 0) -> 0, vlan 0, src sgt: 0, src sgt type: unknown, dst sgt: 0, dst sgt type: unknown, svc 676, payload 1190, client 589, misc 0, user 9999997, url http://www.cnn.com/, host www.cnn.com, no xff

172.31.100.10 54851 -> 146.75.123.5 80 6 AS=0 ID=0 GR=1-1 match rule order 9, 'block multimedia', action Block
172.31.100.10 54851 -> 146.75.123.5 80 6 AS=0 ID=0 GR=1-1 Sending HTTP block response page (605 bytes)
172.31.100.10 54851 -> 146.75.123.5 80 6 AS=0 ID=0 GR=1-1 Deleting Firewall session
```

Lab 3 Troubleshooting

Enable logging



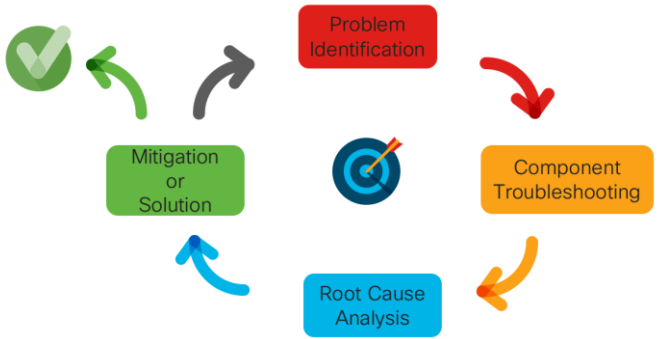
Action	Reason	Initiator IP	Initiator Country	Responder IP	Responder Country	Ingress Security Zone	Egress Security Zone	Source Port / ICMP Type	Destination Port / ICMP Code	Application Protocol	Client	Web Application	URL
Block		172.31.100.10		146.75.119.5	USA	InZone	OutZone	54403 / tcp	80 (http) / tcp	HTTP	Chrome	CNN.com	http://www.cnn.com/

CNN.com

Turner Broadcasting System's news website.

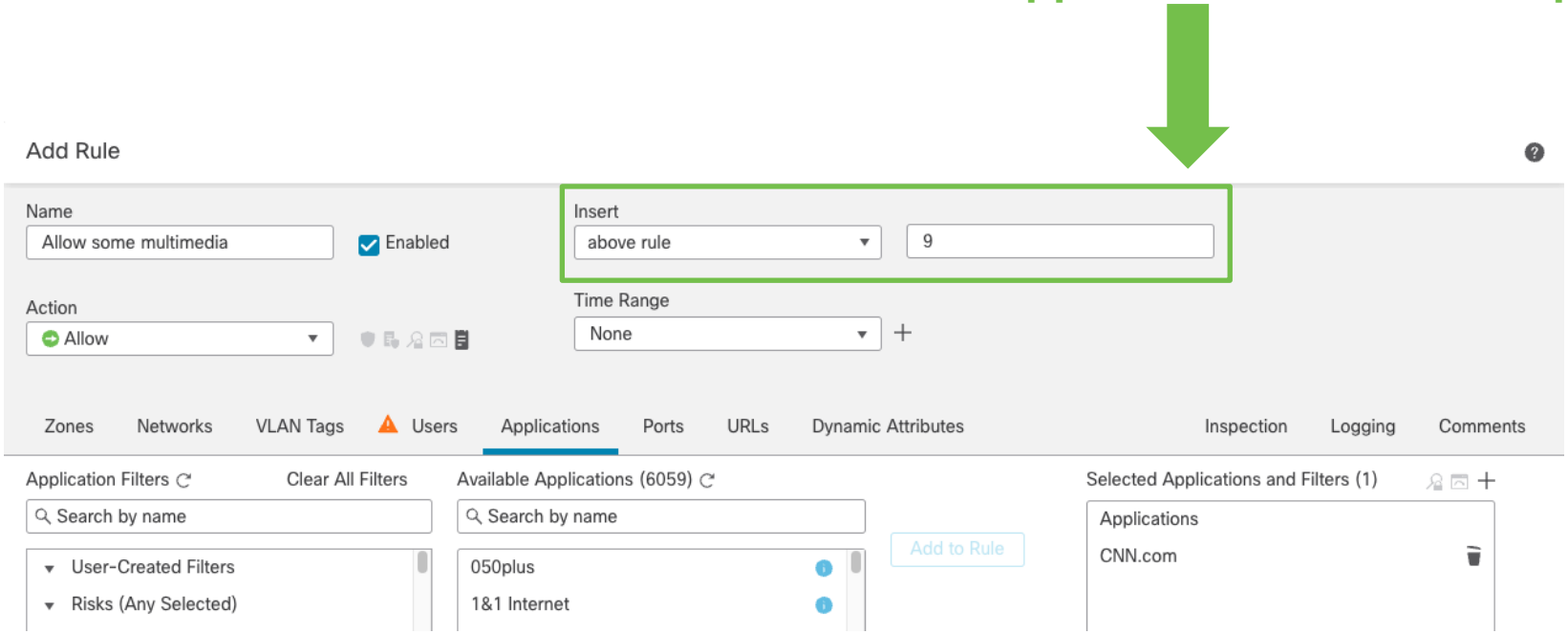
Type	Web Application
Risk	Very Low
Business Relevance	High
Categories	multimedia (tv/video), news
Tags	displays ads, NSG, SSL protocol

Context Explorer Wikipedia Google Yahoo! Bing



Lab 3 Solution

Add a rule above “block multimedia” (Rule 9) to allows certain apps and add CNN.com app



Lab 4 – Intrusion Prevention System (IPS)

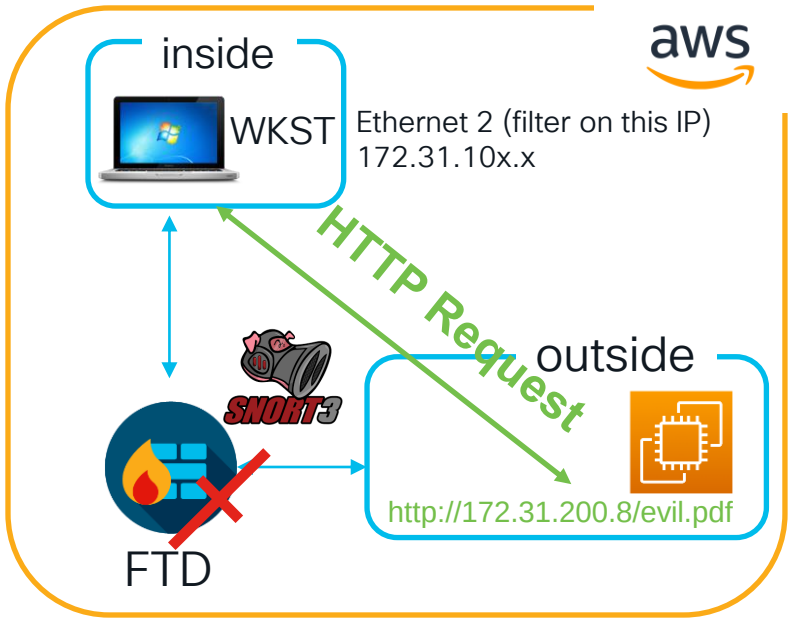
Lab 4 steps

1. Make a copy of the “Lab 4 (IPS)” AC Policy in your local domain and assign it to the FTD and deploy (see deploy help slide)
2. Open an RDP session to WKST (see local note for IP)
3. Open a new incognito window in chrome
4. Navigate to http://172.31.200.8/evil.pdf (browser may try to force https, type “http://”)
5. Troubleshoot! Figure out why this connection is being blocked and make the least intrusive change(s) to resolve the issue and retain as much security efficacy as possible (Pro Mode: Changes made should only impact 172.31.200.8).
6. Note: for proper completion of lab make sure you have a File event for the PDF

Use https://docs.snort.org/start/rules for snort3 rule documentation

Bonus: Multiple rules blocked this, can you make 1 rule which has the criteria of all rules that were blocking this and still match? If you do show the instructor for a prize.
Hint: https://docs.snort.org/rules/options/payload/http/req_resp_detection

Lab 4 Scenario



Problem Description

WKST is unable to download the file at http://172.31.20.8/evil.pdf

Instructions

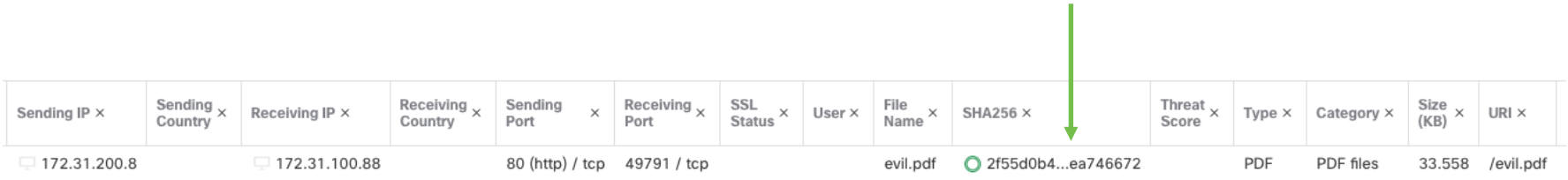
Using the tools introduced, determine why the connection is unsuccessful.

Hints

- Intrusion Events
- system support trace

Lab 4 Verify Completion

If the file is allowed you should see a file event with sha256
2f55d0b4d7bfe0f78636a990c8dd152245a0e6bc2daf3eee445c0300ea746672



Sending IP	Sending Country	Receiving IP	Receiving Country	Sending Port	Receiving Port	SSL Status	User	File Name	SHA256	Threat Score	Type	Category	Size (KB)	URI
172.31.200.8		172.31.100.88		80 (http) / tcp	49791 / tcp			evil.pdf	2f55d0b4...ea746672		PDF	PDF files	33.558	/evil.pdf

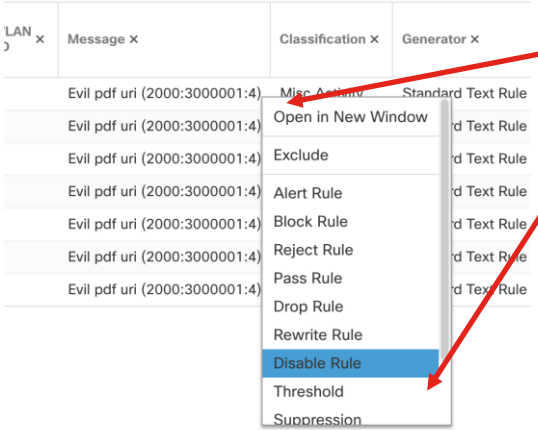
Please note: If you just fastpath traffic and the PDF loads but you still want to try the lab after you have downloaded the PDF be aware the browser local cache will prevent more downloads, clear browser cache/history before retrying.

Lab 4 Troubleshooting (events)

Unified Event Viewer (UEV)

Lab 4 Solution (Variant: Disable IPS Rule from global rule settings)

Analysis > Intrusions > Events

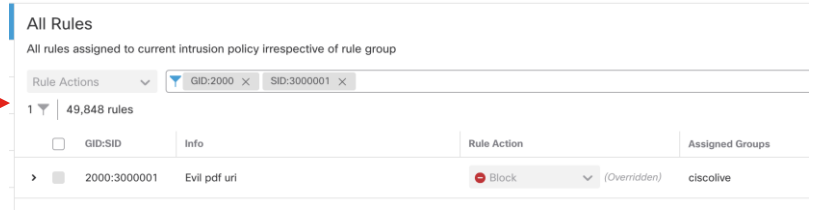


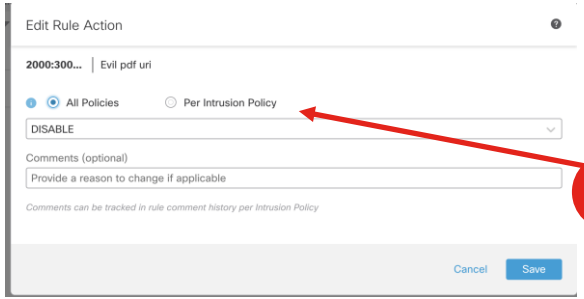
1

Right click on the rule message > Disable Rule takes you to the global snort3 rules

2a

If there are no IPS policies in your local domain you will see this view and you can not make changes from here since all polices are in global domain. You will need to create a new IPS policy in your domain



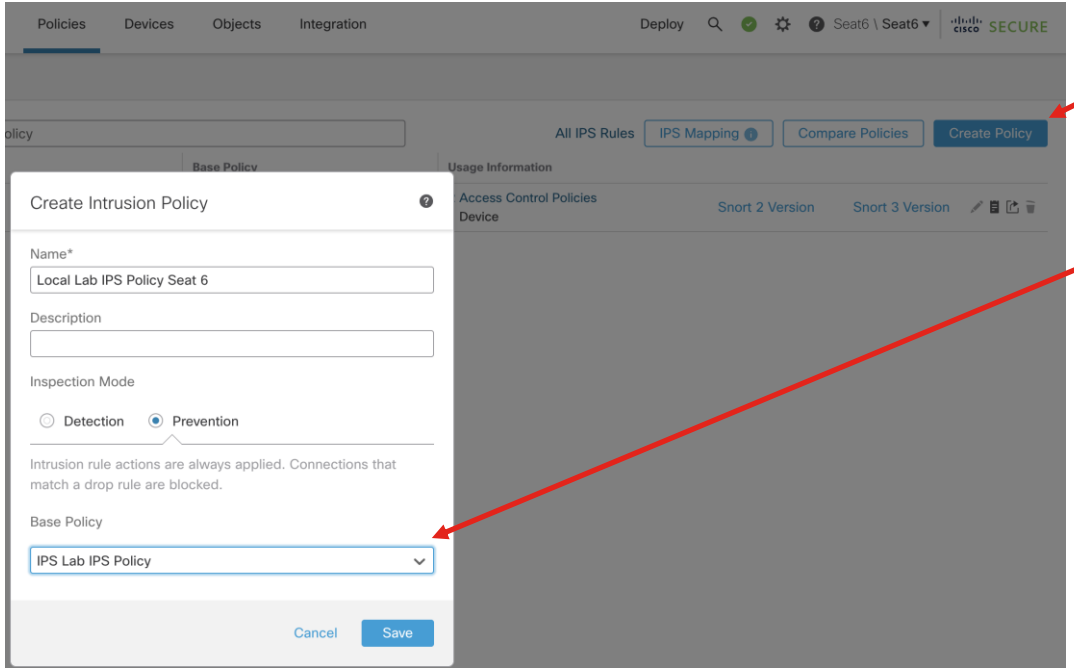


2b

If there are IPS policies in your local domain you will see this view and you can disable per policy from here

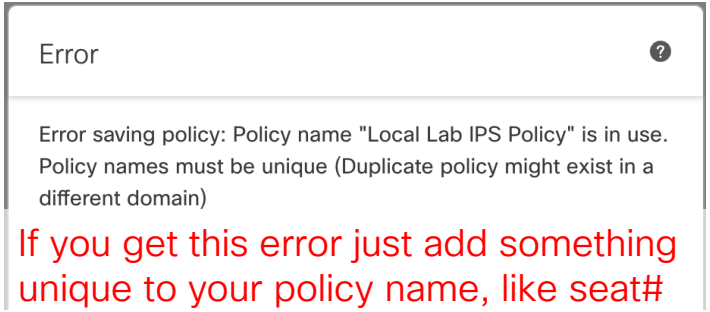
Lab 4 Solution (make new IPS policy)

Navigate to Policies > Intrusion and create a new policy. Use “IPS Lab IPS Policy” as the base policy to keep same security posture.



1 Create new Policy

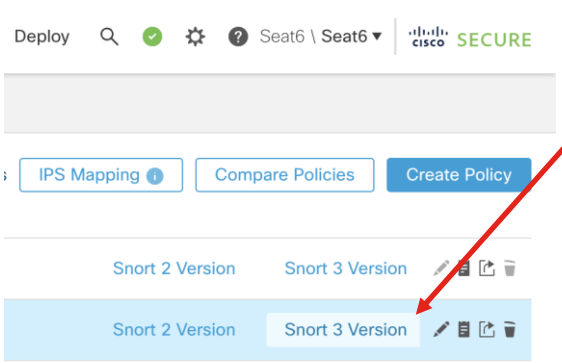
2 Use “IPS Lab IPS Policy” as base policy



If you get this error just add something unique to your policy name, like seat#

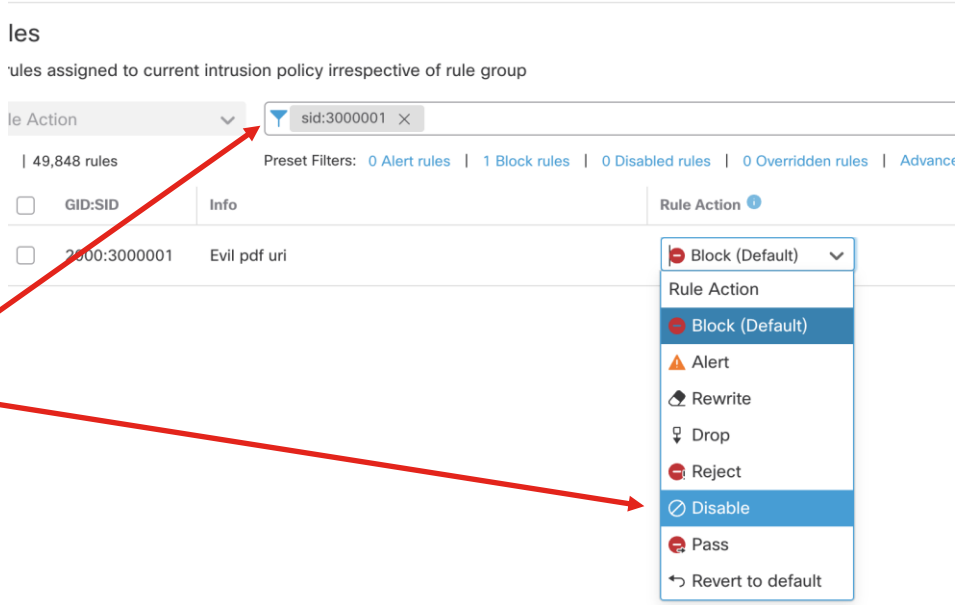
Lab 4 Solution (edit new IPS policy)

Edit the newly created IPS Policy



1

Click “Snort 3 Version” to edit the policy rules

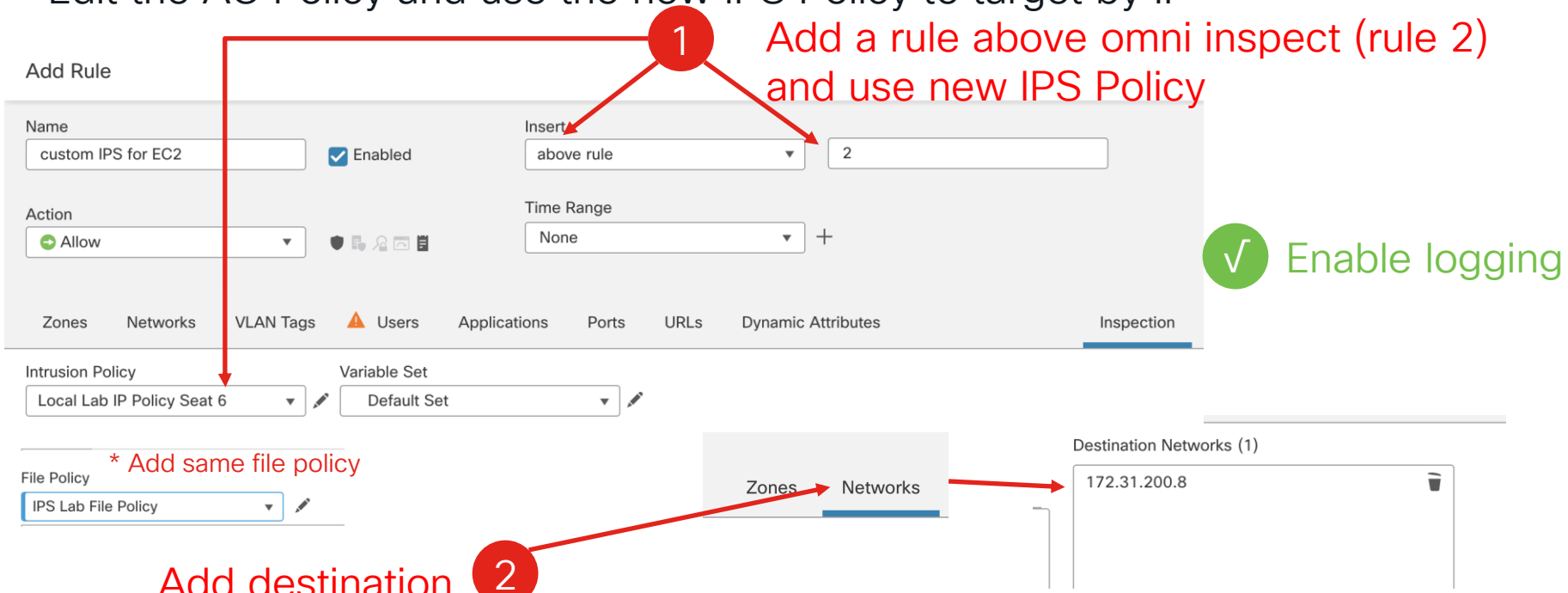


2

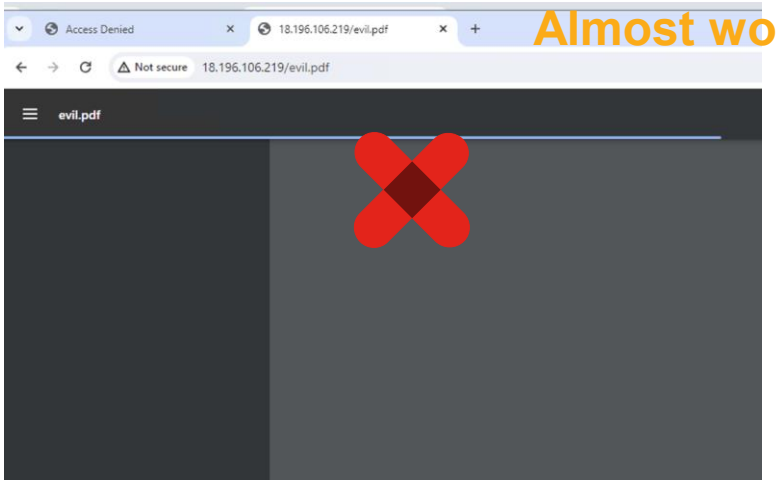
Filter on the sid and disable the rule

Lab 4 Solution (edit AC policy)

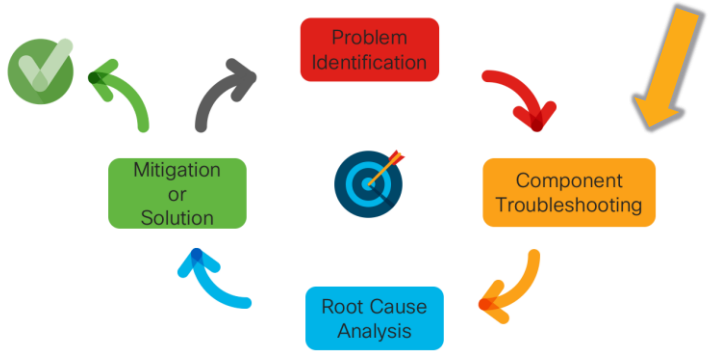
Edit the AC Policy and use the new IPS Policy to target by IP



Lab 4 Troubleshooting



Almost working…but still blocked…what next?



system support trace!

Lab 4 Troubleshooting

Trace

SHELL

```
> system support trace

Please specify an IP protocol: tcp
Please specify a client IP address:
Please specify a client port:
Please specify a server IP address: 172.31.200.8
Please specify a server port: 80
Enable firewall-engine-debug too? [n]: n
Monitoring packet tracer debug messages
[…Omitted for brevity…]

172.31.200.8 80 -> 172.31.100.87 51617 6 AS=0 ID=0 GR=1-1 Packet 1297: TCP ***A****, 02/07-07:39:13.504353, seq 1778302888, ack
988312753, dsize 1380
172.31.200.8 80 -> 172.31.100.87 51617 6 AS=0 ID=0 GR=1-1 File: Type-PDF found
172.31.200.8 80 -> 172.31.100.87 51617 6 AS=0 ID=0 GR=1-1 Event: 2000:3000002:4, Action block
172.31.200.8 80 -> 172.31.100.87 51617 6 AS=0 ID=0 GR=1-1 Stream: pending block, drop
172.31.200.8 80 -> 172.31.100.87 51617 6 AS=0 ID=0 GR=1-1 Policies: Network 0, Inspection 0, Detection 5
172.31.200.8 80 -> 172.31.100.87 51617 6 AS=0 ID=0 GR=1-1 Verdict: blacklist
172.31.200.8 80 -> 172.31.100.87 51617 6 AS=0 ID=0 GR=1-1 Verdict Reason: ips, block
```

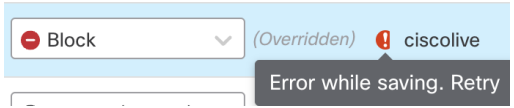
Lab 4 Solution (Find the suppression)

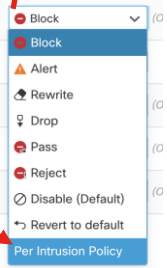
Snort configurations

Go to Objects > Intrusion Rules [Snort3 All Rules]
Then expand the local rules group and click “ciscolive”

2000:3000002	detect PDF options	Block (Default) (Overridden)	ciscolive	Suppression	
2000:3000005	this is a bad rule, do not even look	Disable (Default)	ciscolive	None	
2000:3000006	no bad-mouthing snort3!	Block (Default) (Overridden)	ciscolive	None	
2000:3000003	block evil text	Block (Default) (Overridden)	ciscolive	None	
2000:3000004	johns test rule	Alert (Default) (Overridden)	ciscolive	None	

If trying to disable from this view you may get an error since this is trying to set the global setting and you don’t have permission from this domain. Select “Per Intrusion Policy” instead



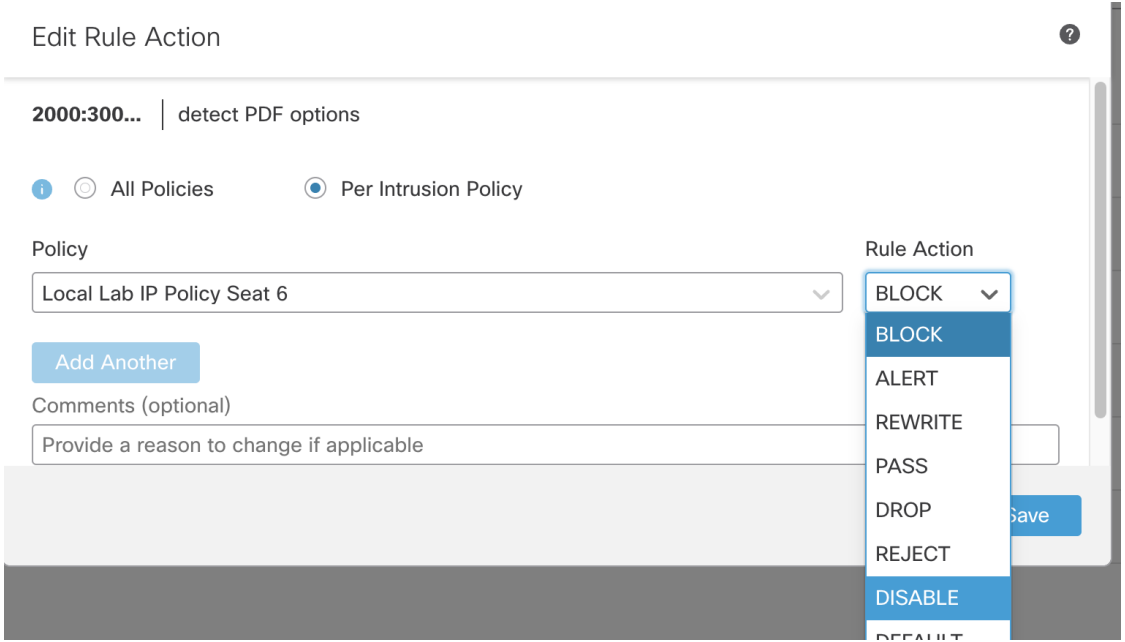


Alternatively, you can go to the intrusion policy to disable it

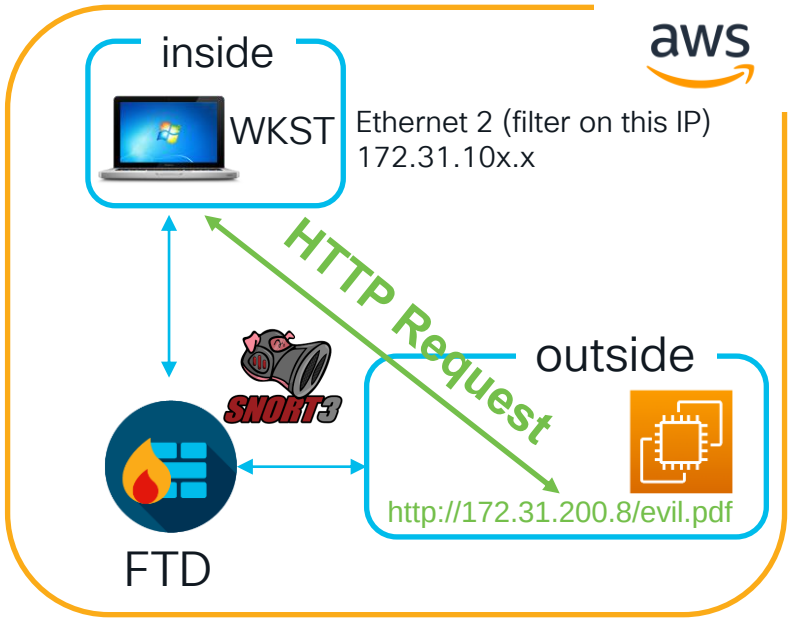
Lab 4 Solution

Snort configurations

Disable for local IPS policy from Global rules view



Lab 4 Solution

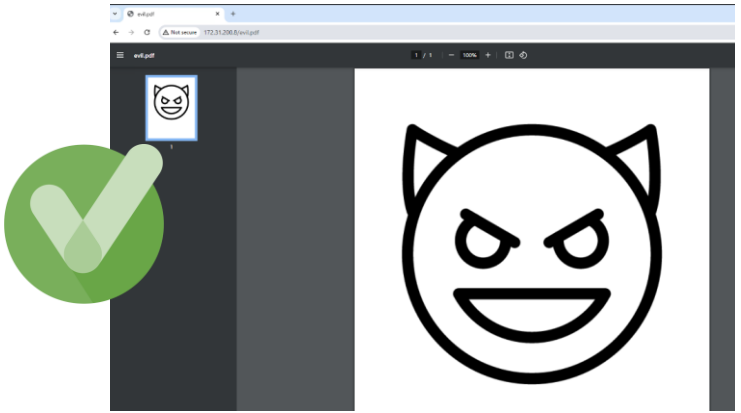


Root Cause

Multiple IPS Rules blocking the connection

Solution

Disable the IPS rules using a custom IPS policy and AC rule to only target the EC2 instance IP



Lab 4 Pro Mode Check and Extra Questions

1. If you navigate to the external IP of the EC2 from WKST (http://18.196.106.219/evil.pdf), is the pdf blocked? If you targeted the internal IP of the EC2 correctly this should still be blocked (Assuming no local cache of the PDF)
2. Can you find the “hidden” text message in the PDF?
3. Go to /evil.txt uri on the EC2, is it blocked? It should block if you didn’t break security posture during lab.
4. There is a rule for that text message, why didn’t the IPS rule block the text in the PDF but it blocked the text in the .txt file?

Lab 4 Bonus

Bonus: Multiple rules blocked this pdf, can you make 1 rule which has the criteria of **all** of the rules that were successfully blocking this and still match? If you do show the instructor for a prize.
i.e. if 3 rules blocked this then can you combine all of the constraints (rule bodies) from those rules into 1 rule and have it block the pdf?
If you do show the instructor for a prize.

Hint: https://docs.snort.org/rules/options/payload/http/req_resp_detection

Continuing Education

Cisco Secure Firewall YouTube

Knowledge from TAC / TMEs

- New Feature Walkthroughs
- Troubleshooting Tips
- Automation Guides

Cisco Secure Firewall YouTube Channel

The bridge to possible

Cisco Security Beta Programs

Influence product design
Design research participants shape the look, feel, & functionality of new product features and offerings

Attention to Feedback
Beta customer bugs and enhancements receive high visibility & priority

Top notch communication
Private conference calls with product team

Training
Customers receive early training & experience with new features

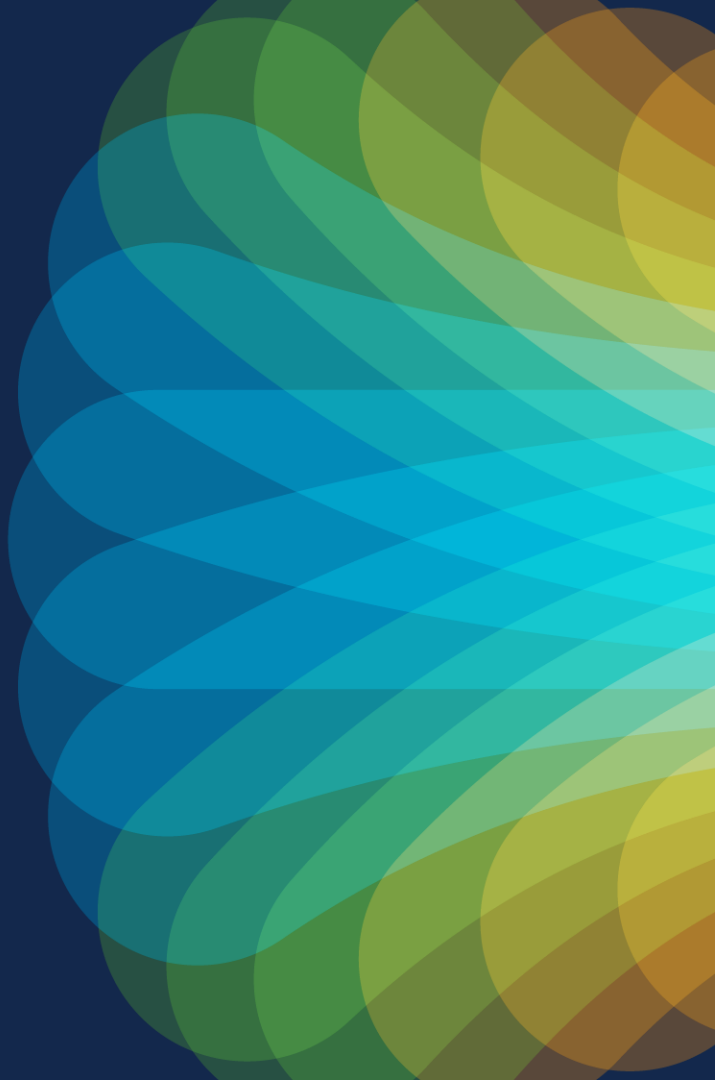
Customer Support
Feature experts will be on-hand & responsive to your issues

Sign-Up Now: https://cs.co/security-beta

cisco Live!

The bridge to possible

Thank you



cisco Live!


cisco Live!
Let's go