Firewall on Fire: Mastering High CPU Troubleshooting

Luis D. Restrepo Valencia
Technical Consulting Engineer, CX Centers EMEA

BRKSEC-2362

Webex App

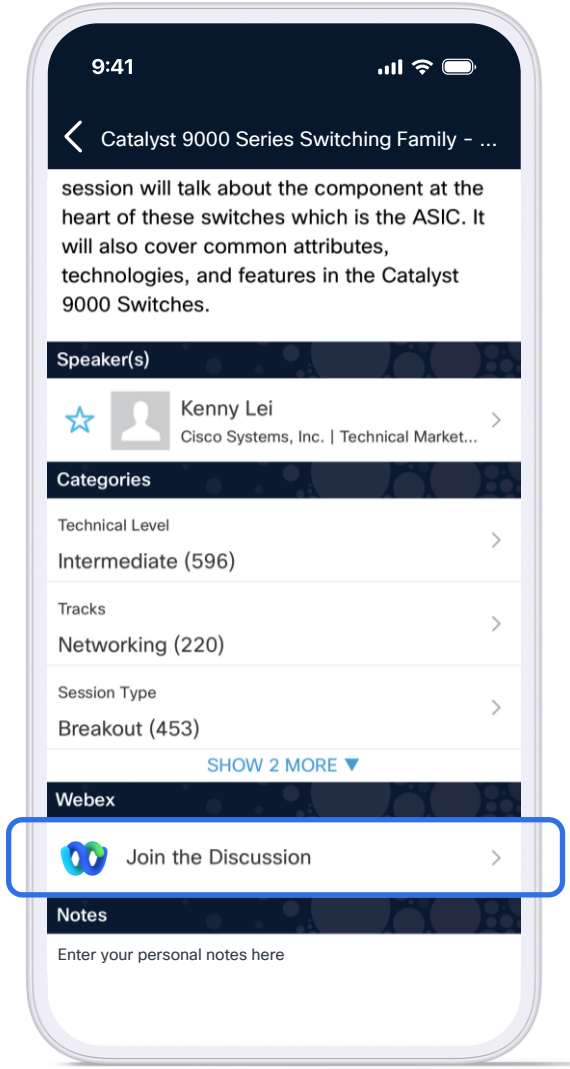
Questions?

Use Webex App to chat with the speaker after the session

How

1. Find this session in the Cisco Events 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 27, 2026.

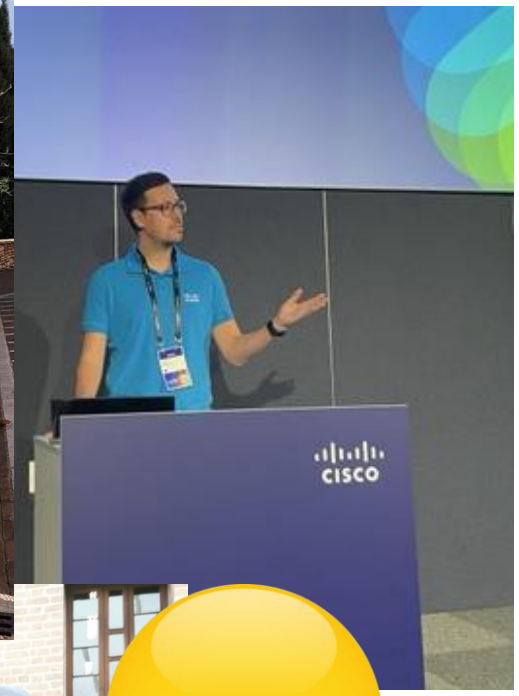


© 2026 Cisco and/or its affiliates. All rights reserved.

Your Presenter

Luis D. Restrepo Valencia

- Colombia
- A dozen years deep in the Cisco jungle.
  - AMER / EMEA Senior NGFW TAC
  - LATAM Partners Security Implementation Engineer.
- Passionate about network, sports ⚽ and languages.
- Traveling, Running and Eating (Perfect Balance).



© 2026 Cisco and/or its affiliates. All rights reserved.

Agenda

01 Introduction

02 Troubleshoot

03 Datapath

04 Control Point

05 Snort

© 2026 Cisco and/or its affiliates. All rights reserved.

cisco

Introduction

Disclaimer

- This session is focused on troubleshooting, basic knowledge on Secure Firewalls is suggested.
- Session troubleshoot is based on Snort 3, although same troubleshooting applies for Snort 2.
- In this presentation LINA refers to data path.
- LINA CPU troubleshoot is applicable for ASA high CPU troubleshooting scenarios.
- Additional hidden content, for post session review.
  - Datapath Bonus (Routing Loops, VPN, Offload) + Commands cheat sheet and documentation.

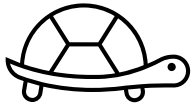
Terminology

- TP – Throughput
- DP – Datapath
- CP – Control Point
- OGS – Object Group Search
- IOO – Interface Object Optimization

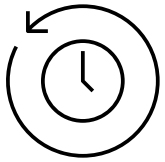
© 2026 Cisco and/or its affiliates. All rights reserved.

cisco

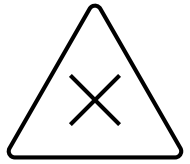
High CPU Processing – The Big Picture



Packet Drops / Latency



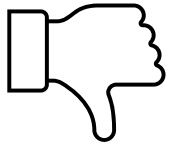
Unresponsive Management



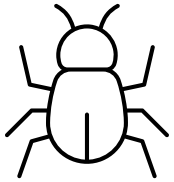
Service Disruption

KNOWN SYMPTOMS

Oversubscription



Misconfigurations / Bad Practices



Defects

COMMON TRIGGERS

© 2026 Cisco and/or its affiliates. All rights reserved.

What Features Can Impact CPU?

LINA

- Focused on L2-L4 functionalities.
- ARP, Routing, L3/L4 ACL's, NAT, TCP State Checking, S2S/RA VPN.
- Basic L7 inspection capabilities.

Snort

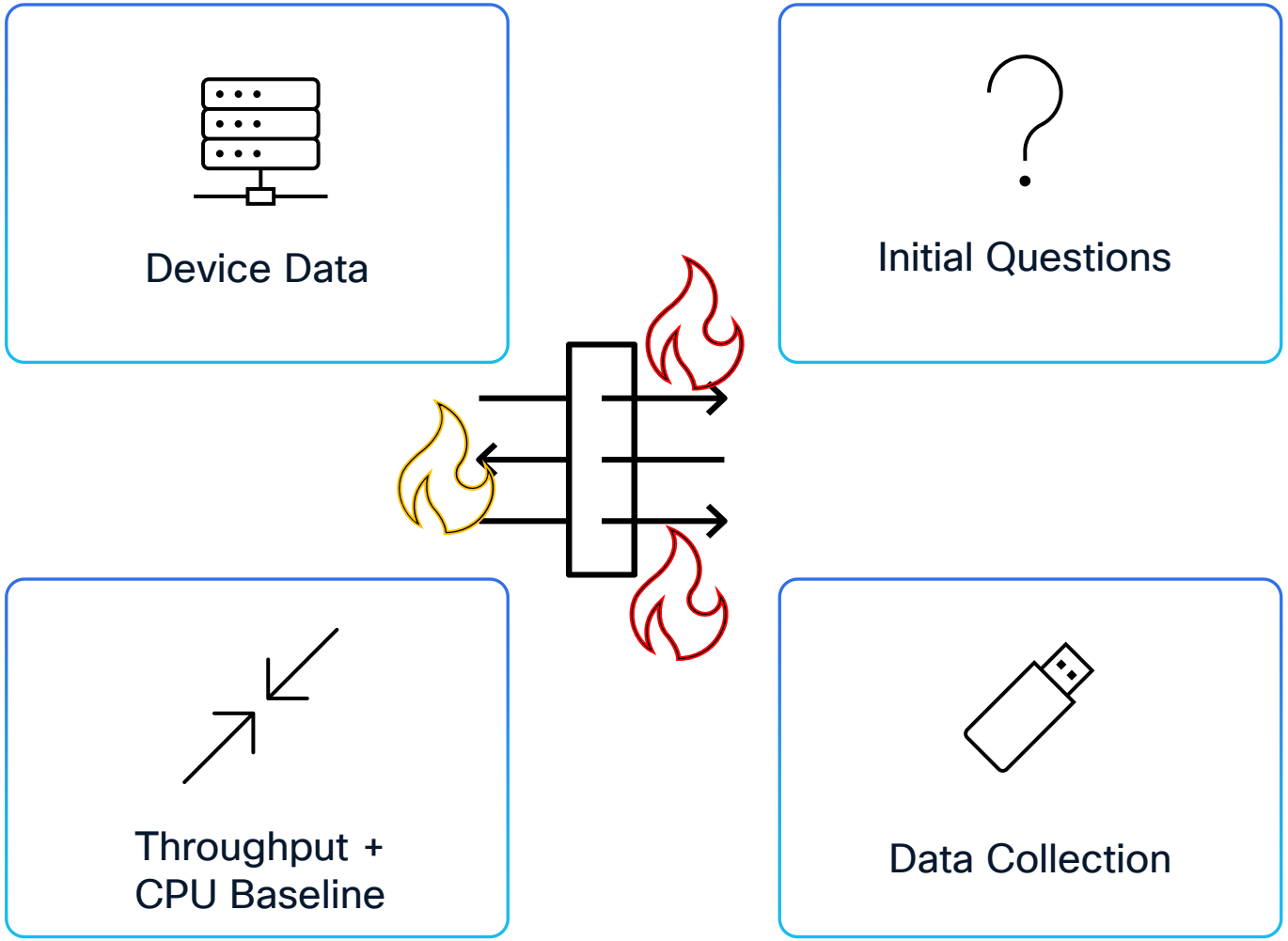
- Focused on L7 functionalities.
- Application, URL Filtering, IPS, SSL decryption, Geolocation, User Awareness, Security Intelligence.

© 2026 Cisco and/or its affiliates. All rights reserved.

cisco

Troubleshoot

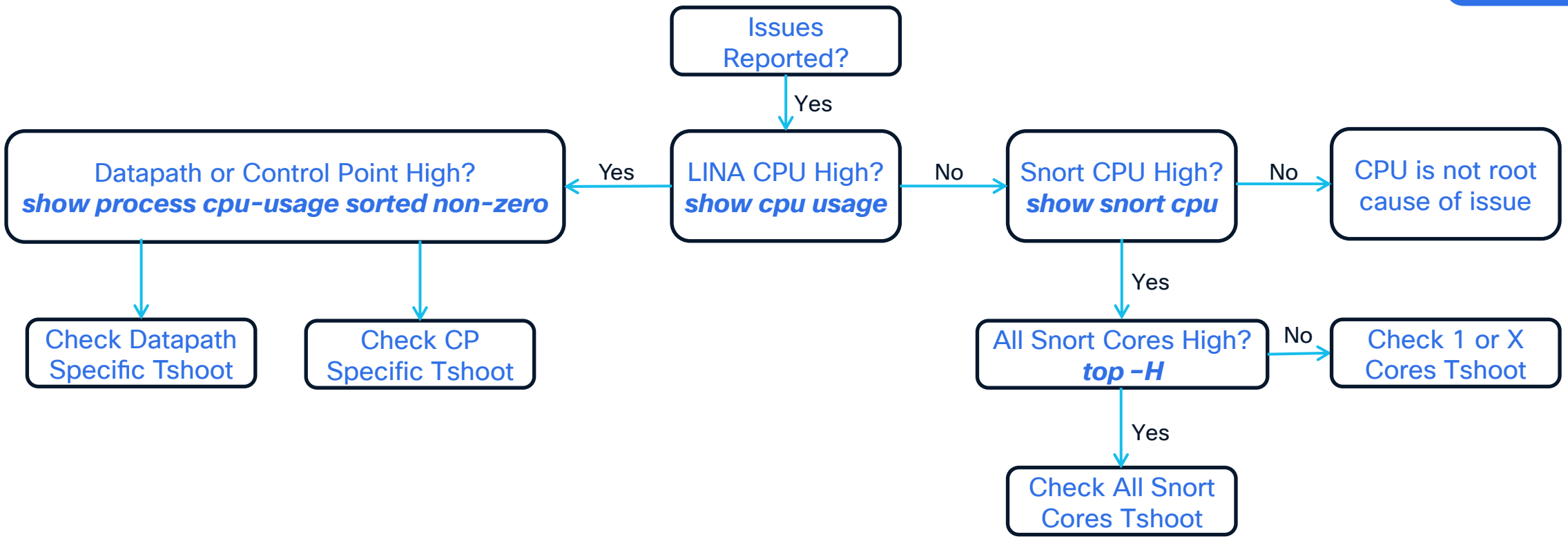
Day-0 Information



© 2026 Cisco and/or its affiliates. All rights reserved.

Starting CPU Flow Chart

REFERENCE



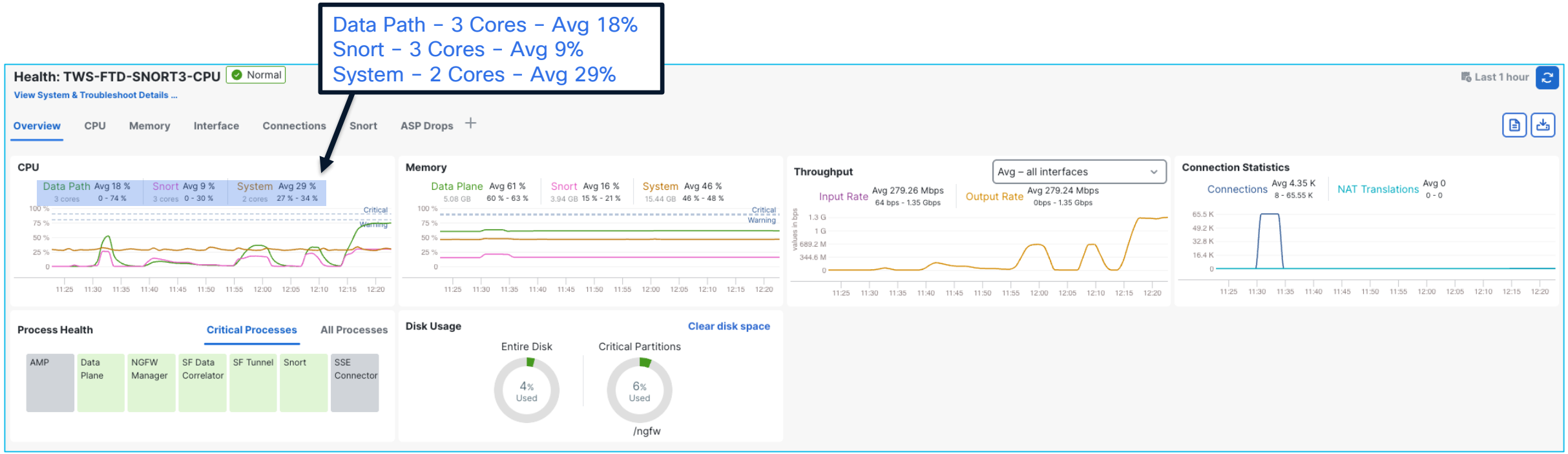
Confirm the findings with FMC Health Monitoring
System > Health > Monitor

© 2026 Cisco and/or its affiliates. All rights reserved.

cisco

FMC Health Monitoring

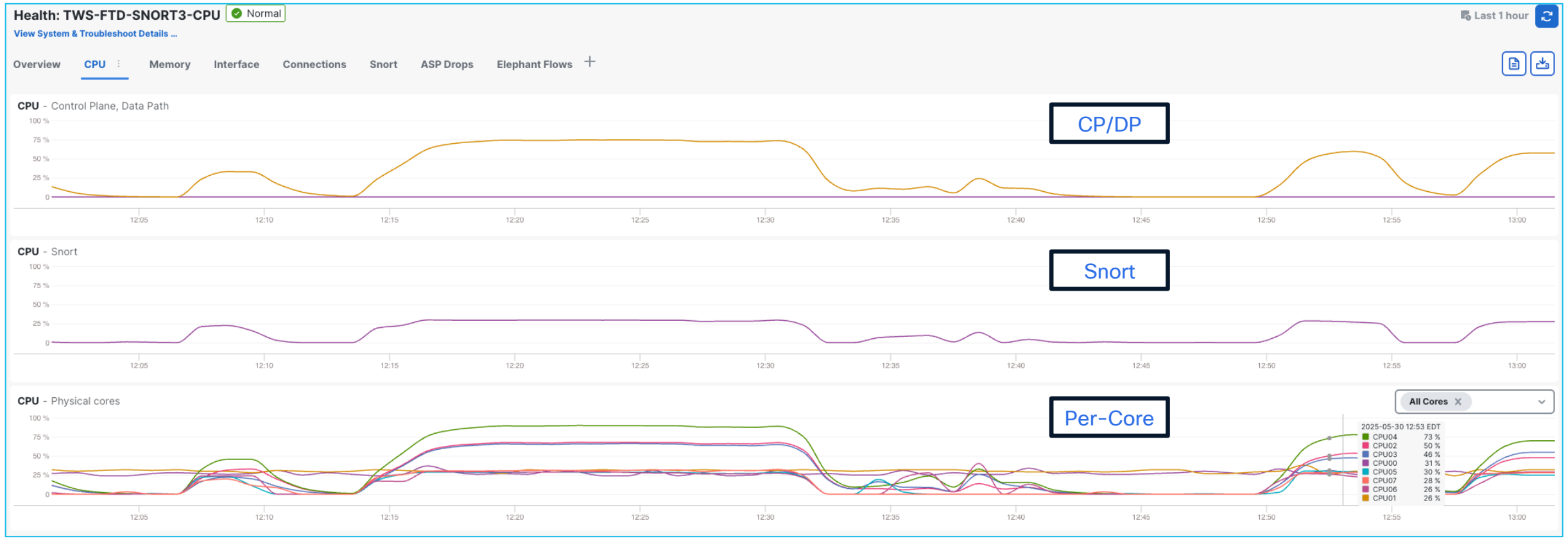
- LINA/Snort/Per-core utilization can be checked in **System > Health > Monitor**.
- If CPU tab is disabled, enable it from **System > Health > Policy**.



Pro Tip: CPU dashboard shows the number of cores for Data Path (LINA), Snort and System.

© 2026 Cisco and/or its affiliates. All rights reserved.

FMC Health Monitoring



© 2026 Cisco and/or its affiliates. All rights reserved.

CPU Allocation

The **sudo pmtool show affinity** command shows core allocation for LINA, Snort or System:

```
admin@firepower:~$ sudo pmtool show affinity


Affinity Status

System CPU Affinity: 0-1 (desired: 0-1)

Process CPU Affinity:
    CPU 0:
       1642c748-37dc-11f0-a8f7-45ad857e2884 (/ngfw/var/sf/detection_engines/1642c748-37dc-11f0-a8f7-45ad857e2884/snort3) (0-1, desired: 0-1,5-7)
    CPU 1:
       1642c748-37dc-11f0-a8f7-45ad857e2884 (/ngfw/var/sf/detection_engines/1642c748-37dc-11f0-a8f7-45ad857e2884/snort3) (0-1, desired: 0-1,5-7)
    CPU 2:
       lina (/ngfw/usr/local/sf/bin/consoled) (2-4, desired: 2-4)
    CPU 3:
       lina (/ngfw/usr/local/sf/bin/consoled) (2-4, desired: 2-4)
    CPU 4:
       lina (/ngfw/usr/local/sf/bin/consoled) (2-4, desired: 2-4)
    CPU 5:
       1642c748-37dc-11f0-a8f7-45ad857e2884 (/ngfw/var/sf/detection_engines/1642c748-37dc-11f0-a8f7-45ad857e2884/snort3) (0-1, desired: 0-1,5-7)
    CPU 6:
       1642c748-37dc-11f0-a8f7-45ad857e2884 (/ngfw/var/sf/detection_engines/1642c748-37dc-11f0-a8f7-45ad857e2884/snort3) (0-1, desired: 0-1,5-7)
    CPU 7:
       1642c748-37dc-11f0-a8f7-45ad857e2884 (/ngfw/var/sf/detection_engines/1642c748-37dc-11f0-a8f7-45ad857e2884/snort3) (0-1, desired: 0-1,5-7)

Process Affinity:
  lina (desired: 2-4, actual: 2-4)
```

System CPU Cores

LINA CPU Cores

Snort CPU Cores

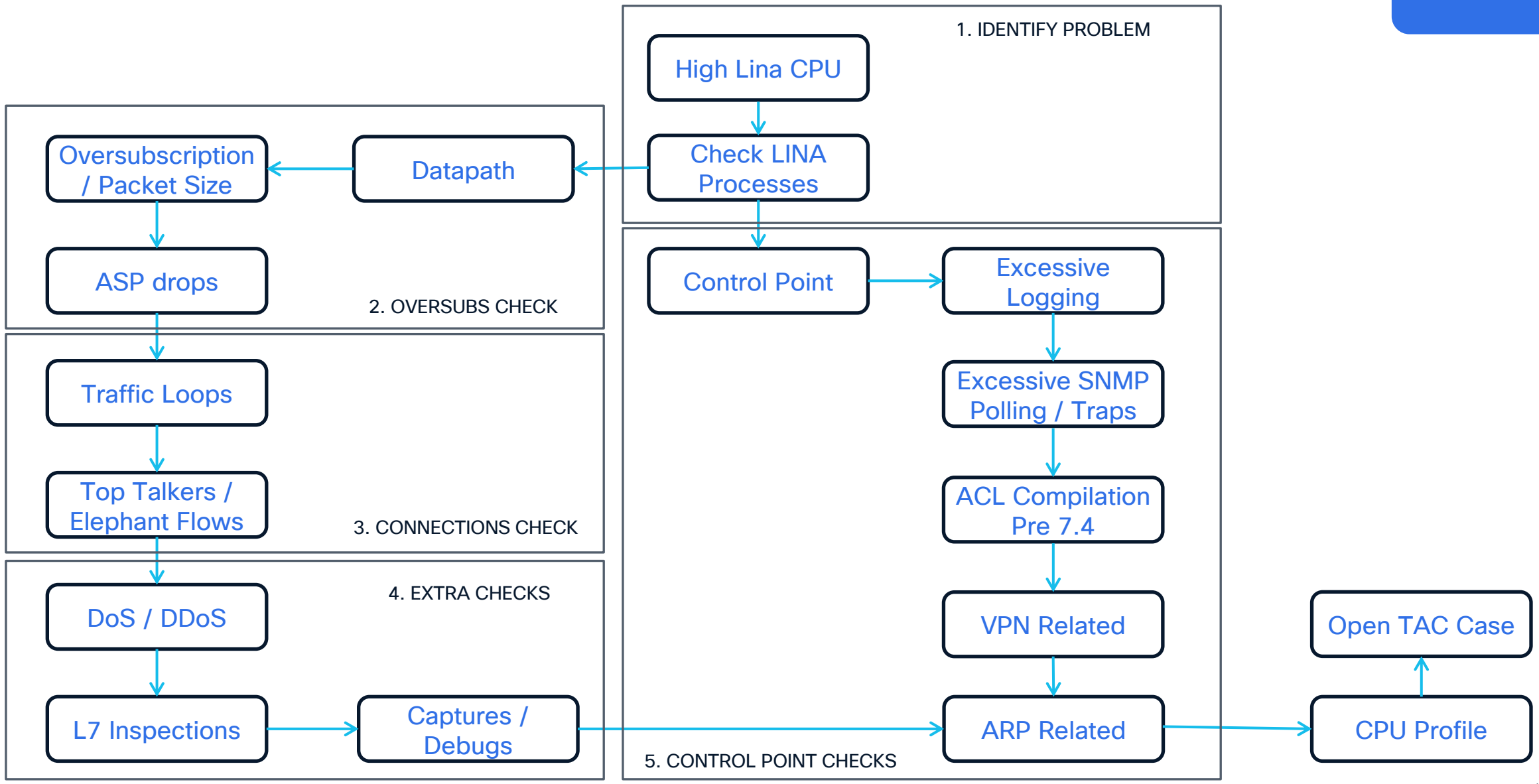
© 2026 Cisco and/or its affiliates. All rights reserved.

cisco

Datapath

LINA CPU Flow Chart

REFERENCE



© 2026 Cisco and/or its affiliates. All rights reserved.

Case Study 1 – LINA on Fire

Users are complaining about general connectivity issues. The issue has been going for quite some time but lately has been worse.

Environment:

- Hardware: FPR4145
- Software: FTD 7.2
- Deployment: Multi-Instance
- Firewall Mode: Routed Mode
- Redundancy: High-availability

© 2026 Cisco and/or its affiliates. All rights reserved.

LINA CPU General Commands

```
firepower# show cpu usage

CPU utilization for 5 seconds = 100%; 1 minute: 100%; 5 minutes: 100%

firepower# show process cpu-usage sorted non-zero

Hardware:   FPR4K-SM-44S
Cisco Adaptive Security Appliance Software Version 9.18(4)210
ASLR enabled, text region 55f17c6a6000-55f180d719c9

PC         Thread       5Sec     1Min     5Min   Process
   -          -         100%   100.0%   100.0%   DATAPATH-9-6828
   -          -         100%    99.9%    99.8%   DATAPATH-7-6826
   -          -        99.9%    99.8%    99.8%   DATAPATH-1-6820
   -          -        99.8%    99.9%    99.9%   DATAPATH-4-6823
   -          -        99.7%    99.9%    99.8%   DATAPATH-2-6821
   -          -        99.7%    99.8%    99.8%   DATAPATH-6-6825
   -          -        99.0%    99.5%    99.5%   DATAPATH-3-6822
   -          -        98.8%    99.5%    99.5%   DATAPATH-8-6827
   -          -        97.7%    97.6%    96.8%   DATAPATH-0-6819
   -          -        97.4%    97.5%    96.7%   DATAPATH-5-6824
0x000055f17f43659d   0x00001469c436c260     3.7%     3.2%     4.2%   ci/console
0x000055f17e816416   0x00001469c4368860     0.5%     0.5%     0.5%   ARP Thread
0x000055f17f52a43a   0x00001469c436b780     0.1%     0.1%     0.1%   update_cpu_usage
0x000055f17f43659d   0x00001469c435e540     0.1%     0.0%     0.0%   cli_xml_request_process
```

Total LINA CPU

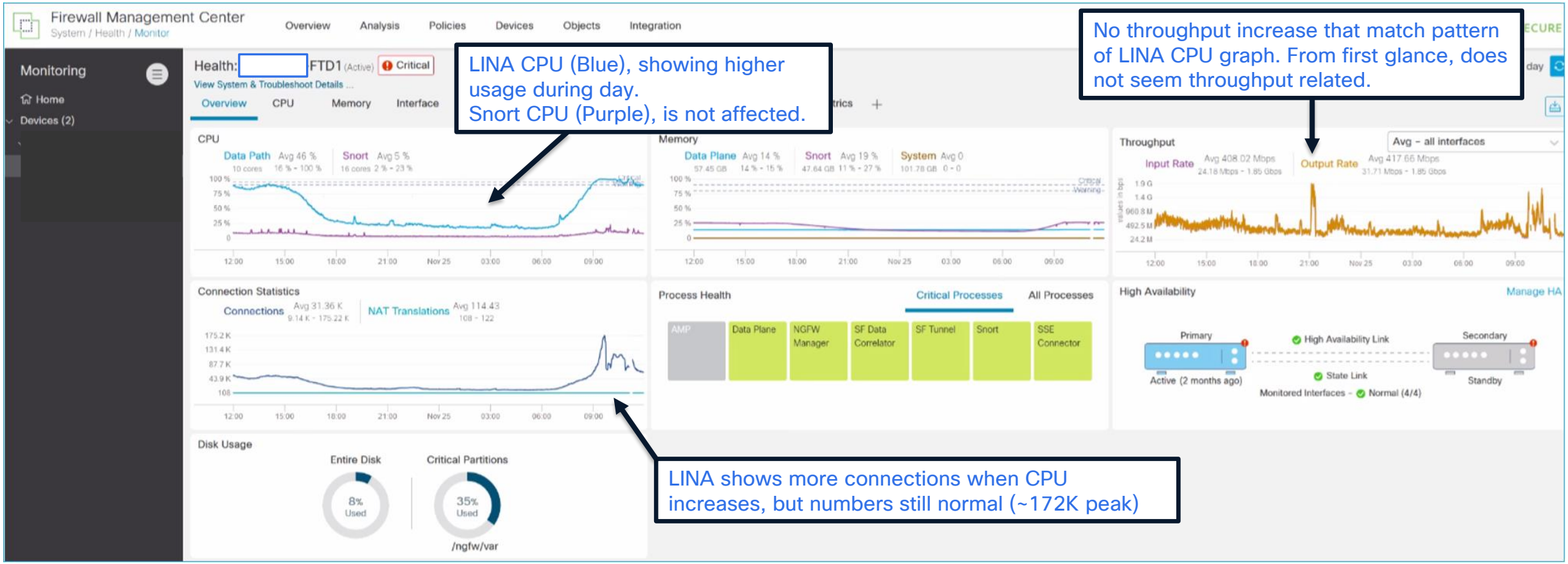
Datapath showing high usage

Pro Tip: Additional **show cpu detailed** command will show Core % (DP% + CP%) on a per-core basis.

© 2026 Cisco and/or its affiliates. All rights reserved.

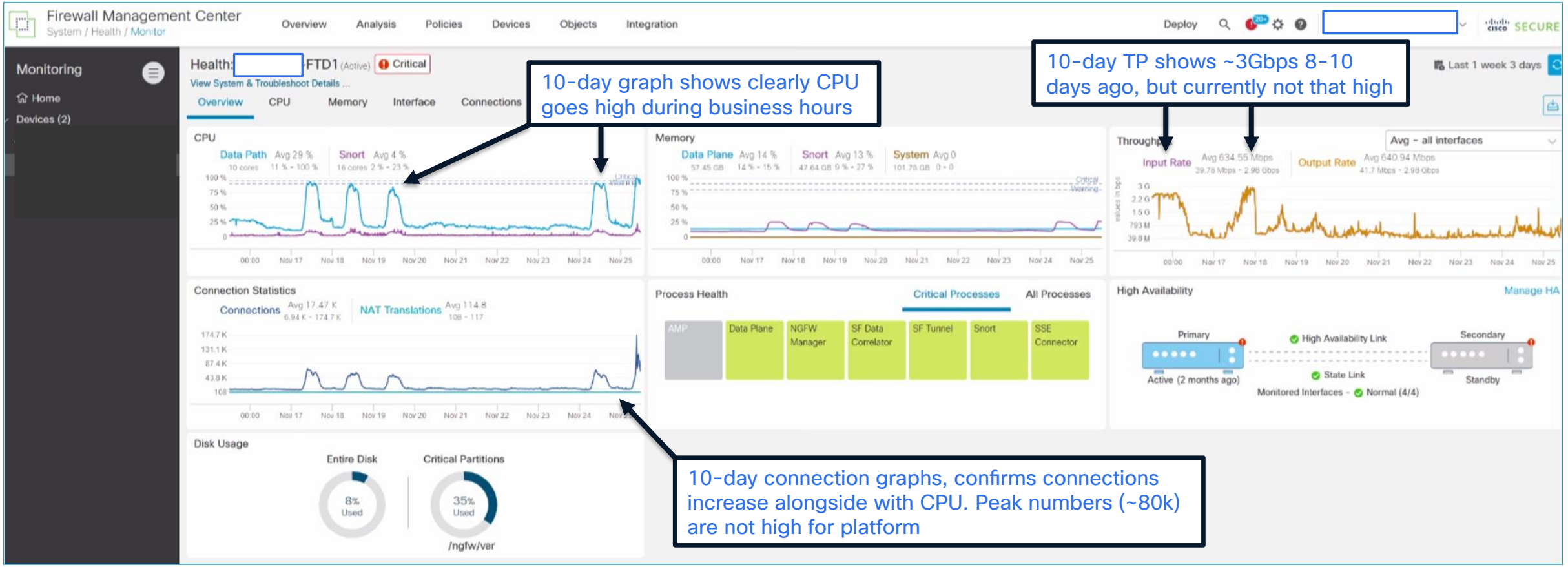
cisco

Health Monitoring Graphs



© 2026 Cisco and/or its affiliates. All rights reserved.

Health Monitoring Graphs



© 2026 Cisco and/or its affiliates. All rights reserved.

Health Monitoring Graphs

Pro Tip: The 1.7 Gbps in TP graph is not considering the packet size. Extrapolate the TP to a packet size of 1024 to compare with the data sheet numbers: 1.7 x 1024 / 600 = 2.9 Gbps

© 2026 Cisco and/or its affiliates. All rights reserved.

Device Datasheet

Detailed performance specifications and feature highlights

Table 1. Performance specifications and feature highlights for Cisco Secure Firewall 4100 with the Cisco Secure Firewall Threat Defense (TD) image

Features	4112	4115	4125	4145
Throughput: FW + AVC (1024B)	19 Gbps	33 Gbps	45 Gbps	53 Gbps
Throughput: FW + AVC + IPS (1024B)	19 Gbps	33 Gbps	45 Gbps	53 Gbps
Maximum concurrent sessions, with AVC	10 million	15 million	25 million	30 million

For native FTD

Pro Tip: Multi-instance is in use, therefore determine how many cores are allocated to it.

Resource profile assigned to FTD instance has 26 cores.

© 2026 Cisco and/or its affiliates. All rights reserved.

cisco

Performance Scaling Factor

For multi-instance calculate based on the number of CPU cores assigned to instance. Example 4145, 26 core instance

Max Snort TP * (1024B) = (<Max_TP> / <Snort_Core_Count_Native>) * <Snort_Cores_Allocated_Instance>
Max_TP = 53 Gbps (FW+AVC datasheet TP)
Snort_Core_Count_Native = 52 Snort cores for native device
Snort_Cores_Allocated_Instance = 14 Snort cores

Maximum Snort TP = (53/52)*14 = ~14.26 Gbps

Max DP TP * (1024B) = (<Max_TP> / <DP_Core_Count_Native>) * <DP_Cores_Allocated_Instance>
Max_TP = 53 Gbps (FW+AVC datasheet TP)
DP_Core_Count_Native = 32 Data Plane cores for native device
DP_Cores_Allocated_Instance = 10 Data Plane cores

Maximum Data Plane throughput = (53/32)*10 = ~16.56 Gbps

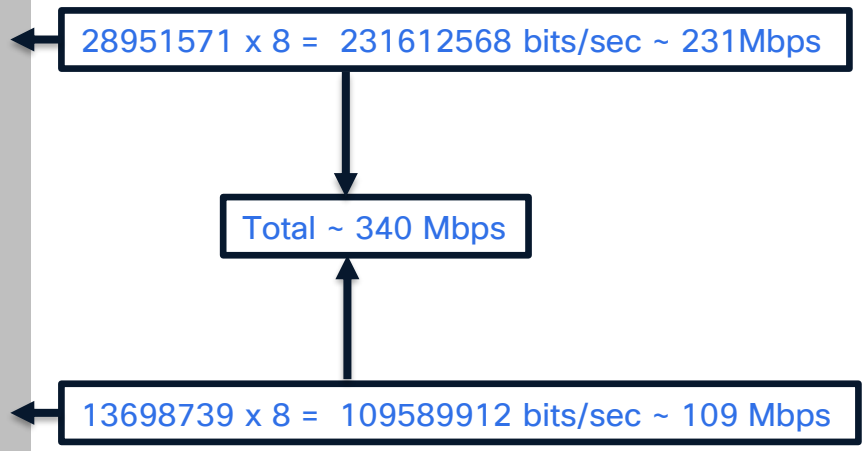
Instance is not oversubscribed. Usage (~2.9 Gbps), capacity (~16 Gbps).

© 2026 Cisco and/or its affiliates. All rights reserved.

Throughput

- Calculate total throughput by adding 1-minute bytes/sec input values of the data interfaces.
- It is important to avoid adding input and output values as this would be counting the same traffic twice.

```
firepower# show traffic
Outside:
    received (in 1551382.754 secs):
        202917629910 packets    227769205918440 bytes
        130000 pkts/sec    146816002 bytes/sec
    transmitted (in 1551382.754 secs):
        154625525290 packets    85187660910838 bytes
        99002 pkts/sec    54910000 bytes/sec
      1 minute input rate 27651 pkts/sec,  28951571 bytes/sec
      1 minute output rate 13755 pkts/sec,  2995746 bytes/sec
      1 minute drop rate, 531 pkts/sec
      5 minute input rate 60313 pkts/sec,  75439423 bytes/sec
      5 minute output rate 21177 pkts/sec,  3473033 bytes/sec
      5 minute drop rate, 314 pkts/sec
Inside:
    received (in 1551383.234 secs):
        317381008069 packets    188655585405840 bytes
        204000 pkts/sec    121604001 bytes/sec
    transmitted (in 1551383.234 secs):
        316293619576 packets    257917899740238 bytes
        203000 pkts/sec    166250002 bytes/sec
      1 minute input rate 22456 pkts/sec,  13698739 bytes/sec
      1 minute output rate 17742 pkts/sec,  9533586 bytes/sec
      1 minute drop rate, 931 pkts/sec
      5 minute input rate 29914 pkts/sec,  21096417 bytes/sec
      5 minute output rate 24766 pkts/sec,  16865052 bytes/sec
      5 minute drop rate, 882 pkts/sec
```



© 2026 Cisco and/or its affiliates. All rights reserved.

Packet Size

- Calculated from **show traffic** command, divide bytes/sec and pkts/sec values.
- Smaller packets results in more processing. Every packet header must be evaluated using more CPU.
  - 1MB of traffic with 1518 bytes/pkt = ~658 pkts
  - 1MB of traffic with 400 bytes/pkt = ~2500 pkts >>> Higher resource utilization.

28951571 / 27651 = 1047 Bytes/pkt

13698739 / 22456 = 610 Bytes/pkt

```
firepower# show traffic
Outside:
    received (in 1551382.754 secs):
        202917629910 packets    227769205918440 bytes
        130000 pkts/sec    146816002 bytes/sec
    transmitted (in 1551382.754 secs):
        154625525290 packets    85187660910838 bytes
        99002 pkts/sec    54910000 bytes/sec
      1 minute input rate 27651 pkts/sec,  28951571 bytes/sec
      1 minute output rate 13755 pkts/sec,  2995746 bytes/sec
      1 minute drop rate, 531 pkts/sec
      5 minute input rate 60313 pkts/sec,  75439423 bytes/sec
      5 minute output rate 21177 pkts/sec,  3473033 bytes/sec
      5 minute drop rate, 314 pkts/sec
Inside:
    received (in 1551383.234 secs):
        317381008069 packets    188655585405840 bytes
        204000 pkts/sec    121604001 bytes/sec
    transmitted (in 1551383.234 secs):
        316293619576 packets    257917899740238 bytes
        203000 pkts/sec    166250002 bytes/sec
      1 minute input rate 22456 pkts/sec,  13698739 bytes/sec
      1 minute output rate 17742 pkts/sec,  9533586 bytes/sec
      1 minute drop rate, 931 pkts/sec
      5 minute input rate 29914 pkts/sec,  21096417 bytes/sec
      5 minute output rate 24766 pkts/sec,  16865052 bytes/sec
      5 minute drop rate, 882 pkts/sec
```

© 2026 Cisco and/or its affiliates. All rights reserved.

cisco

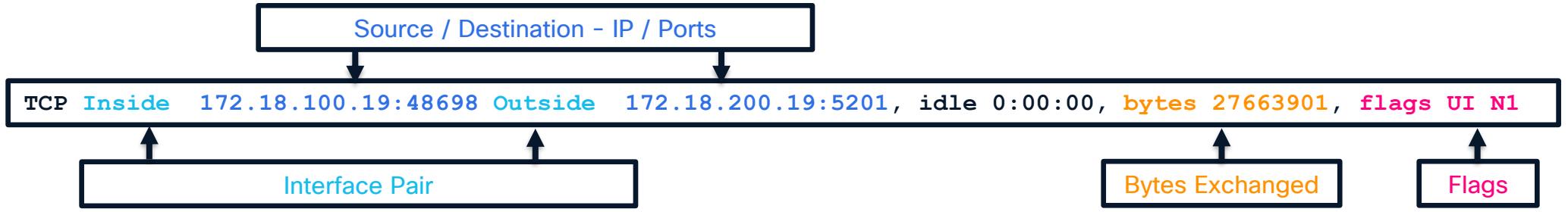
LINA Connections

```
firepower# show conn
36 in use, 236965 most used
Inspect Snort:
        preserve-connection: 22 enabled, 0 in effect, 236933 most enabled, 11 most in effect

TCP Inside  172.18.100.19:48698 Outside  172.18.200.19:5201, idle 0:00:00, bytes 27663901, flags UI N1
TCP Inside  172.18.100.19:48812 Outside  172.18.200.19:5201, idle 0:00:00, bytes 28383501, flags UI N1
TCP Inside  172.18.100.19:48704 Outside  172.18.200.19:5201, idle 0:00:00, bytes 25370053, flags UI N1
```

```
firepower# show conn detail
140 in use, 265 most used
Inspect Snort:
        preserve-connection: 126 enabled, 0 in effect, 252 most enabled, 0 most in effect

TCP Inside: 172.18.200.100/49668 Outside: 172.18.100.100/5201,
    flags UI N1, idle 0s, uptime 11s, timeout 1h0m, bytes 15353101
  Initiator: 172.18.200.100, Responder: 172.18.100.100
  Connection lookup keyid: 455111306

TCP Inside: 172.18.200.100/49450 Outside: 172.18.100.100/5201,
    flags UI N1, idle 0s, uptime 11s, timeout 1h0m, bytes 6508981
  Initiator: 172.18.200.100, Responder: 172.18.100.100
  Connection lookup keyid: 2263105626
```

HELPS IDENTIFYING

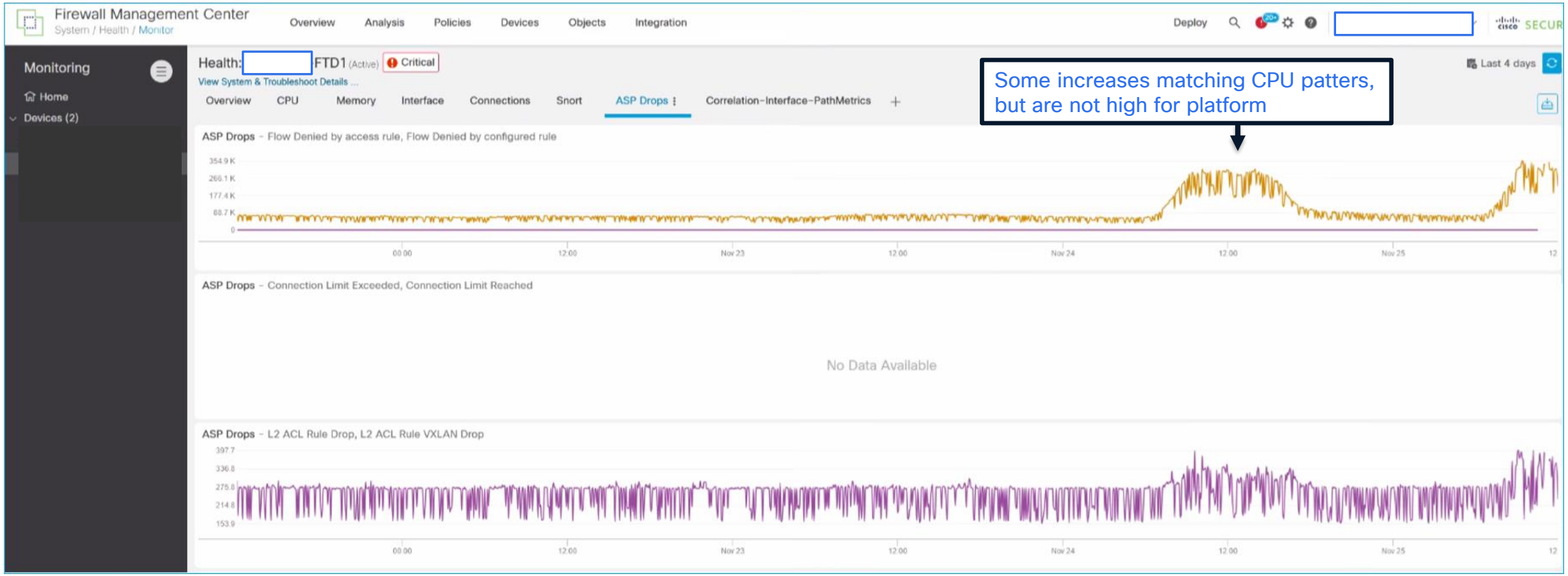
- **Top Talkers / DoS**
- **Traffic Loops**
- **Elephant Flows**



© 2026 Cisco and/or its affiliates. All rights reserved.

Additional Checks

- After ruling out oversubscription, top talkers and traffic loops, other suspects are:
  - Syslogs, SNMP, Inspections, ASP drops > However nothing unexpected after checking.



© 2026 Cisco and/or its affiliates. All rights reserved.

ASP Drops

- Can be used to check main reasons behind flow or packet drops.
- When seeing high CPU scenarios do the following:
  - Clear ASP drop counters: **clear asp drop**
  - Run **show asp drop** few times to identify the highest counter.
  - Configure drop-specific packet captures: **cap ASP type asp-drop <reason>**

```
firepower# show asp drop

Frame drop:
  Flow is being freed (flow-being-freed)                    21
  Unexpected packet (unexpected-packet)                     13
  No route to host (no-route)                          1045842
  Reverse-path verify failed (rpf-violated)             625454
  Flow is denied by configured rule (acl-drop)         1491856
  First TCP packet not SYN (tcp-not-syn)                 15005
  TCP failed 3 way handshake (tcp-3whs-failed)             112
  TCP RST/FIN out of order (tcp-rstfin-ooo)                167
  TCP packet failed PAWS test (tcp-paws-fail)                1
  Slowpath security checks failed (sp-security-failed)      25
  FP L2 rule drop (l2_acl)                              974637
  Interface is down (interface-down)                         8
  Dispatch queue tail drops (dispatch-queue-limit)         231

Last clearing: Never

Flow drop:

Last clearing: Never
```

```
firepower# cap ASP type asp-drop no-route
firepower#
firepower# show cap ASP
Target:     OTHER
Hardware:   FPR-1140
Cisco Adaptive Security Appliance Software Version 9.18(3)39
ASLR enabled, text region 55d1335bb000-55d137c43119

4 packets captured

   1: 14:41:05.029325        172.18.100.100.33448 > 172.19.220.100.53:  udp 39
Drop-reason:    (no-route)    No    route    to    host,    Drop-location:    frame
0x000055d135ca7895 flow (NA)/NA
   2: 14:41:05.029386        172.18.100.100.33448 > 172.19.220.100.53:  udp 39
Drop-reason:    (no-route)    No    route    to    host,    Drop-location:    frame
0x000055d135ca7895 flow (NA)/NA
   3: 14:41:06.811145        172.18.200.100.55448 > 172.19.220.100.53:  udp 39
Drop-reason:    (no-route)    No    route    to    host,    Drop-location:    frame
0x000055d135ca7895 flow (NA)/NA
   4: 14:41:06.811206        172.18.200.100.55448 > 172.19.220.100.53:  udp 39
Drop-reason:    (no-route)    No    route    to    host,    Drop-location:    frame
0x000055d135ca7895 flow (NA)/NA
4 packets shown
```

© 2026 Cisco and/or its affiliates. All rights reserved.

OGS & ACL Compilation

- Tmatch compile thread is related to ACL/NAT compilation. ACL optimization features like object group search (OGS) use it on compilation.

	Name	Action	Source		Destination		
			Zones	Networks	Zones	Networks	Ports
	Mandatory 1 rule (1 - 1)						
	1 Internet_Servers	Allow	Inside_Z	Lan_PCs	Outside_Z	Internet_Servers	Internet_Ports

OGS & IOO OFF (Expand)	2 Interfaces	X	4 Sources	X	1 Interface	X	4 Destinations	X 4 Ports = 128 ACE's
OGS ON & IOO OFF	2 Interfaces	X	1 Src OG	X	1 Interface	X	1 Dst OG	X 4 Ports = 8 ACE's
OGS ON & IOO ON	1 Int OG	X	1 Src OG	X	1 Interface	X	1 Dst OG	X 4 Ports = 4 ACE's

```
firepower# show processes cpu-usage sorted non-zero
Hardware:   NGFWv
Cisco Adaptive Security Appliance Software Version 9.14(1)1
ASLR enabled, text region 55ab57c65000-55ab5d237f9d
PC          Thread       5Sec     1Min     5Min    Process
0x000055ab59679c03   0x00002b446e2cf670    58.8%    56.7%    56.4%   tmatch compile thread
   -           -         1.2%     1.3%     1.2%   PTHREAD-3396
0x000055ab5962c002   0x00002b446e2ba1b0     1.1%     1.1%     1.1%   appAgent_monitor_nd_thread
```

```
firepower# show processes cpu-usage sorted non-zero
Hardware:   FPR4K-SM-44S
Cisco Adaptive Security Appliance Software Version 9.18(4)210
ASLR enabled, text region 55f17c6a6000-55f180d719c9
PC          Thread       5Sec     1Min     5Min    Process
   -           -         100%    100.0%   100.0%   DATAPATH-9-6828
   -           -         100%     99.9%    99.8%   DATAPATH-7-6826
```

Pro Tip: Keep in mind platform ACE limits and avoid object group nesting, even with OGS/IOO excessive amount of ACE's can lead to high CPU usage on datapath.

© 2026 Cisco and/or its affiliates. All rights reserved.

Case Study 1 – LINA on Fire – Conclusion

- Checks are now done towards access control elements and OGS check.
- 4145 recommended max ACE's is ~3M for Native Mode (32 cores allocated to LINA), ~1M for Container (10 cores allocated to LINA)

```
firepower# show access-list element-count
Total number of access-list elements: 44031
```

- OGS enabled value, the FTD instance has ~3.9M ACE's hidden behind OGS.
- CPU profile was collected to confirm and function calls pointed to OGS as using most CPU cycles.

Conclusion: In this case, the customer uses ~x4 times more ACEs than the maximum recommended values!

Solution:

- Reduce the number of ACEs in the policy.
- Disable OGS on FTD. This though will come at the cost of increased memory consumption.

© 2026 Cisco and/or its affiliates. All rights reserved.

cisco

CPU Profiler

```
firepower# show cpu profile
No profiling data.

firepower# cpu profile activate 10000
Activated CPU profiling for 10000 samples.
Use "show cpu profile" to display the progress or "show cpu profile
dump" to interrupt profiling and display the incomplete results.
firepower#
firepower# show cpu profile
CPU profiling started: 17:20:15.009 UTC Mon Sep 4 2025
CPU profiling currently in progress:
    Core 0: 538 out of 10000 samples collected.
    Core 1: 474 out of 10000 samples collected.
    Core 2: 776 out of 10000 samples collected.
    Core 3: 776 out of 10000 samples collected.
    Core 4: 776 out of 10000 samples collected.
    Core 5: 776 out of 10000 samples collected.
    CP: 540 out of 10000 samples collected.
Use "show cpu profile dump" to see the results after it is complete or
to interrupt profiling and display the incomplete results.
firepower#
firepower# show cpu profile
CPU profiling started: 17:20:15.009 UTC Mon Sep 4 2025
CPU Profiling has stopped.
    Core 0 done with 10000 samples
    Core 1 done with 10000 samples
    Core 2 done with 10000 samples
    Core 3 done with 10000 samples
    Core 4 done with 10000 samples
    Core 5 done with 10000 samples
    CP done with 10000 samples
Use "show cpu profile dump" to see the results.
firepower#
firepower# show logging | inc profiling
Sep  04  2025  17:20:15:  %FTD-7-711006:  CPU  profiling  has  started  for
10000 samples. Reason: None specified.
```

CPU profiles collecting samples

Collection sample complete

```
firepower# show cpu profile dump
Cisco Adaptive Security Appliance Software Version 9.18(3)39
Hardware:   FPR-1140
CPU profiling started: 17:20:15.009 UTC Mon Sep 4 2025
No CPU profiling process specified.
No CPU profiling trigger specified.
cores: 6

Process virtual address map:
----------------------------
152088dff000-15208c000000 rw-p 00000000 00:00 0
15208c000000-15208c021000 rw-p 00000000 00:00 0
15208c021000-152090000000 ---p 00000000 00:00 0
152091800000-152091a00000          rw-s          00000000          00:1c          495087
/mnt/hugetlb/lcmb_MEMPOOL_HEAPCACHE_0_N0/page_0
152091a00000-152091c00000          rw-s          00000000          00:1c          495088
/mnt/hugetlb/lcmb_MEMPOOL_HEAPCACHE_0_N0/page_1
152091c00000-152091e00000          rw-s          00000000          00:1c          495089
/mnt/hugetlb/lcmb_MEMPOOL_HEAPCACHE_0_N0/page_2
.
.
{0x000055d1351a9924,0x000055d134b379ee}       {0x000015210ae76ee7,0x000055d134b3d4d5}
{0x000055d136bbe294,0x000055d134b38e94}
 {0x000055d134b04383,0x000055d134b3d36a}      {0x000055d136bbe0a8,0x000055d134b38e94}
{0x000055d134b0438b,0x000055d134b379ee}
 {0x000055d134b3a1bc,0x000055d1351a994e}      {0x000015210c3c895d,0x000055d13668cd37}
{0x000055d136bbe0a8,0x000055d134b38e94}
 {0x000055d1351a9824,0x000055d134b379ee}      {0x000055d134b04383,0x000055d134b3d36a}
{0x000055d134b372b6,0x000055d134b3d36a}
 {0x000055d134b2342a,0x000055d134b3d380}      {0x000015210c3c897f,0x000055d1366bc3fc}
{0x000055d1351a9824,0x000055d134b379ee}
 {0x000055d135074c70,0x000055d136651cc3}      {0x000015210addbbed,0x000055d136680ca7}
{0x000055d134b043ab,0x000055d134b379ee}
 {0x000015210addbbed,0x000055d136680ca7}      {0x000055d136bbe03d,0x000055d134b38e94}
{0x000015210addbbed,0x000055d136680ca7}
 {0x000055d134b0438b,0x000055d134b379ee}      {0x000055d136bbe0a8,0x000055d134b38e94}
{0x000015210addbbed,0x000055d136680ca7}
```

Information to provide to TAC

© 2026 Cisco and/or its affiliates. All rights reserved.

cisco

Control Point

Case Study 2 – CPU Hogs

Recently every few minutes general connectivity issues have been reported across the HQ.

Environment:

- Hardware: FPR2110
- Software: FTD 7.2
- Firewall Mode: Routed Mode
- Redundancy: High-availability

© 2026 Cisco and/or its affiliates. All rights reserved.

Connectivity and Routing

Initially the following was seen:

```
firepower# ping 10.2.80.100
Type escape sequence to abort.
Sending 200, 100-byte ICMP Echos to 10.2.80.100, timeout is 2 seconds:
????????????????????????????????????????????????????????????????????
????????????????????!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
????????????????????????????????????????????????????????????????????
Success rate is 0 percent (30/200)

%OSPF-5-ADJCHG: Process 100, Nbr 10.1.1.26 on Vlan19 from FULL to DOWN, Neighbor Down: Dead timer expired
%OSPF-5-ADJCHG: Process 100, Nbr 10.1.1.26 on Vlan19 from LOADING to FULL, Loading Done
%OSPF-5-ADJCHG: Process 1, Nbr 10.1.1.26 on Vlan51 from FULL to DOWN, Neighbor Down: Dead timer expired
%OSPF-5-ADJCHG: Process 1, Nbr 10.1.1.26 on Vlan51 from LOADING to FULL, Loading Done

Jun 15  08:07:43.278: Neighbor 10.1.1.26, Interface LAN state changes from 2WAY to EXSTART
Jun 15  08:07:43.282: Neighbor 10.1.1.26, Interface LAN state changes from INIT to 2WAY
Jun 15  08:07:42.017: Neighbor 10.1.1.26, Interface LAN state changes from FULL to INIT
```

Intermittent connectivity is seen to servers

OSPF neighbors constantly flapping

Key data:

1. The only OSPF neighbours flapping are the ones towards FTD, others are stable.
2. There was no change on OSPF configuration.
3. Dead timer expired suggest OSPF hello packets missing, but those were reaching the firewall.

© 2026 Cisco and/or its affiliates. All rights reserved.

cisco

LINA CPU General Commands

- Focus switched towards performance as OSPF hello packets were not being processed by FTD:

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

CPU utilization for 5 seconds = 49%; 1 minute: 50%; 5 minutes: 51%


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

Hardware:   FPR-2110
Cisco Adaptive Security Appliance Software Version 9.18(3)39
ASLR enabled, text region aaab8e9000-aab05540bc
PC         Thread       5Sec     1Min     5Min   Process
   -          -        41.5%    36.7%    36.9%   DATAPATH-3-1299
   -          -        41.1%    38.3%    38.0%   DATAPATH-2-1298
   -          -        40.2%    37.4%    36.9%   DATAPATH-5-1301
   -          -        40.2%    36.4%    36.6%   DATAPATH-0-1296
   -          -        39.9%    36.1%    36.4%   DATAPATH-4-1300
   -          -        39.1%    36.9%    36.9%   DATAPATH-1-1297
0x000000aaacd54c2c   0x000000555774d200    25.5%    12.8%    13.2%   CP Processing
0x000000aaadd38b54   0x00000055577388a0     0.1%     0.1%     0.1%   OSPF-1 Hello
0x000000aaae0a020c   0x000000555773bee0     0.1%     0.5%     0.4%   cli_xml_request_process
0x000000aaaeeb5800   0x000000555775cde0     0.0%     0.1%     0.0%   cli_xml_server
0x000000aaae84ab8c   0x000000555773e5a0     0.0%     7.8%     9.9%   table_data_table
0x000000aaae797f4c   0x000000555773f140     0.0%    38.8%    36.8%   snmp_master_callback_thread
0x000000aaae797fcc   0x000000555773ed60     0.0%     4.5%     5.6%   snmp_client_callback_thread
0x000000aaae74a3d4   0x000000555773e1c0     0.0%     0.5%     0.1%   snmp_alarm_thread
```

Total LINA CPU

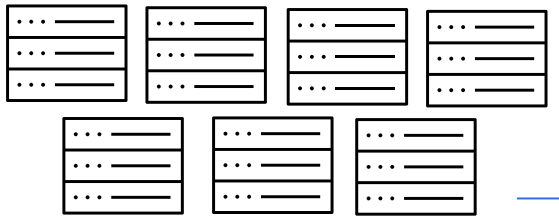
Datapath is not high

Abnormal CP processes showing spikes

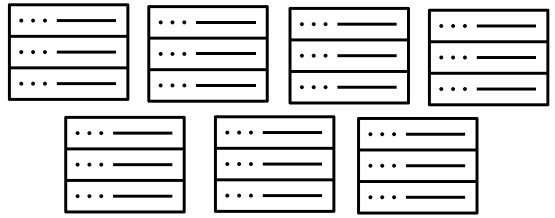
- Investigation can be focused on control point, specifically on CP processing and SNMP processes.

© 2026 Cisco and/or its affiliates. All rights reserved.

Syslog - SNMP



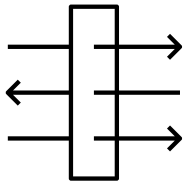
SYSLOG SERVERS



SNMP SERVERS

Basic Logging Settings

- [x] Enable logging
- [ ] Enable logging on the failover standby unit
- [ ] Send syslogs in EMBLEM format
- [x] Send debug messages as syslogs



Logging Destination	Syslog from All Event Class
Internal Buffer	Filter on Severity:7 - debugging
Syslog Servers	Filter on Severity:7 - debugging
SNMP Trap	Filter on Severity:7 - debugging
Console	Filter on Severity:7 - debugging

- (•) Enable All Syslog Messages

Logging Level: 7 - debugging

Syslog ID	Logging Level	Enabled
106015	(default)	⊖
106023	(default)	⊖
302013	(default)	⊖
302014	(default)	⊖
302015	(default)	⊖

```
firepower# %FTD-7-111009: User 'enable_1' executed cmd: show service-policy police
%FTD-7-111009: User 'enable_1' executed cmd: show interface detail
%FTD-7-111009: User 'enable_1' executed cmd: show memory
%FTD-7-111009: User 'enable_1' executed cmd: show blocks
%FTD-7-111009: User 'enable_1' executed cmd: show asp drop
%FTD-7-111009: User 'enable_1' executed cmd: show disk0:
%FTD-7-111009: User 'enable_1' executed cmd: show firewall
%FTD-7-111009: User 'enable_1' executed cmd: show route all summary
%FTD-7-111009: User 'enable_1' executed cmd: show ipv6 route all summary
%FTD-7-111009: User 'enable_1' executed cmd: show resource usage resource Routes
%FTD-7-111009: User 'enable_1' executed cmd: show crypto ipsec stats
%FTD-7-111009: User 'enable_1' executed cmd: show cluster info
%FTD-7-111009: User 'enable_1' executed cmd: show vpn-sessiondb
%FTD-7-111009: User 'enable_1' executed cmd: show access-list element-count
%FTD-7-111009: User 'enable_1' executed cmd: show snort statistics
%FTD-7-111009: User 'enable_1' executed cmd: show asp inspect-dp snort queues
%FTD-7-111009: User 'enable_1' executed cmd: show cpu detailed
%FTD-7-111009: User 'enable_1' executed cmd: show asp inspect-dp snort counters zeros
%FTD-7-111009: User 'enable_1' executed cmd: show memory
%FTD-7-111009: User 'enable_1' executed cmd: show running-config failover
%FTD-7-111009: User 'enable_1' executed cmd: show aaa-server
%FTD-7-111009: User 'enable_1' executed cmd: show aaa login-history
%FTD-7-111009: User 'enable_1' executed cmd: show zero-trust statistics
%FTD-7-111009: User 'enable_1' executed cmd: show cpu detailed
%FTD-7-111009: User 'enable_1' executed cmd: show clns protocol
%FTD-7-111009: User 'enable_1' executed cmd: show xlate count
%FTD-7-111009: User 'enable_1' executed cmd: show conn count
%FTD-7-111009: User 'enable_1' executed cmd: show perfmon detail
```

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

Hardware:   FPR-2110
Cisco Adaptive Security Appliance Software Version 9.18(3)39
ASLR enabled, text region aaab8e9000-aab05540bc
PC          Thread       5Sec     1Min     5Min    Process
   -           -         45.5%    33.1%    34.2%   DATAPATH-0-
1296
   -           -         45.2%    33.2%    34.3%   DATAPATH-2-
1298
   -           -         44.5%    31.0%    33.6%   DATAPATH-4-
1300
   -           -         44.5%    31.6%    33.7%   DATAPATH-3-
1299
   -           -         44.0%    31.6%    33.9%   DATAPATH-1-
1297
   -           -         44.0%    32.5%    34.2%   DATAPATH-5-
1301
0x000000aaacd54c2c   0x000000555774d200     23.3%     5.9%
10.2%   CP Processing
0x000000aaae74a3d4   0x000000555773e1c0      1.5%    30.8%
20.2%   logger
0x000000aaae84ab8c   0x000000555773e5a0      1.0%    11.8%
11.0%   table_data_table
0x000000aaae6acbac   0x0000005557740880      0.7%     0.1%
0.0%   SNMP ContextThread
0x000000aaae7690e8   0x0000005557763e40      0.1%     0.0%
0.0%   snmp_logging_thread
0x000000aaae797f4c   0x000000555773f140      0.0%    54.1%
40.9%   snmp_master_callback_thread
0x000000aaae797fcc   0x000000555773ed60      0.0%     6.7%
6.2%   snmp_client_callback_thread
```

© 2026 Cisco and/or its affiliates. All rights reserved.

cisco

Control Point Troubleshoot Commands

```
firepower# show asp event dp-cp

DP-CP EVENT QUEUE                    QUEUE-LEN  HIGH-WATER
Punt Event Queue                             0        2048
Routing Event Queue                          0           0
Identity-Traffic Event Queue                 0          50
PTP-Traffic Event Queue                      0           0
General Event Queue                          0         230
Syslog Event Queue                           0        8192
Non-Blocking Event Queue                     0           0
Midpath High Event Queue                     0           0
Midpath Norm Event Queue                     0           0
Crypto Event Queue                           0         285
HA Event Queue                               0           4
HA Ctl Event Queue                           0           2
Threat-Detection Event Queue                 0           6
SCP Event Queue                              0           0
ARP Event Queue                              0        1741

EVENT-TYPE          ALLOC ALLOC-FAIL ENQUEUED ENQ-FAIL  RETIRED 15SEC-RATE
punt              6819998          0  6689208   130790  6819998       2678
inspect-snmp      6815675          0  6684886   130789  6815675       2639
syslog           20145641          0  6001574 14144067 20145641      11941
adj-absent         416300          0   415560      740   416300          6

firepower# show logging queue

        Logging Queue length limit : 512 msg(s)
        147345 msg(s) discarded due to queue overflow
        0 msg(s) discarded due to memory allocation failure
        Current 0 msg on queue, 83 msgs most on queue
```

ENQ-FAIL identified for SNMP/Syslog

```
firepower# show snmp-server statistics
379045 SNMP packets input
    0 Bad SNMP version errors
    0 Unknown community name
    0 Illegal operation for community name supplied
    0 Encoding errors
    351047 Number of requested variables
…
360058 SNMP packets output
    0 Too big errors (Maximum packet size 1500)
    0 No such name errors
    0 Bad values errors
    0 General errors
    351056 Response PDUs
    9 Trap PDUs

firepower# show run snmp-server
snmp-server group Priv v3 priv
snmp-server user fwuser Priv v3 engineID
80000009fe105eb4ad2d225e1f5b5f7456c6d10ecb52b4f3bd encrypted auth sha
3b:6d:32:98:e3:12:f0:4b:c5:f3:1e:fe:be:b8:19:55:a1:37:ab:dc priv aes
128 ed:87:93:ca:4c:68:70:d3:4f:11:ea:a8:42:6f:eb:f7
snmp-server host ngfw-management 10.2.80.11 version 3 fwuser
snmp-server host ngfw-management 10.2.83.70 version 3 fwuser
snmp-server host ngfw-management 10.2.84.14 poll version 3 fwuser
.
.
.
.
.
snmp-server host ngfw-management 10.2.87.22 poll version 3 fwuser
```

More than 30 SNMP servers identified

© 2026 Cisco and/or its affiliates. All rights reserved.

cisco

Case Study 2 – CPU Hogs – Conclusion

```
firepower# show processes cpu-hog

Hardware:   FPR-2110
Cisco Adaptive Security Appliance Software Version 9.18(3)39
ASLR enabled, text region aaab8e9000-aab05540bc

Process:      snmp_master_callback_thread, PROC_PC_TOTAL: 336671, MAXHOG: 524, LASTHOG: 4
MAXHOG At:    05:34:48 UTC Jul 5 2025
LASTHOG At:   14:14:47 UTC Jul 5 2025
PC:           0x000000aaae797f4c (suspend)

Process:      snmp_master_callback_thread, NUMHOG: 23064, MAXHOG: 546, LASTHOG: 468
MAXHOG At:    11:05:16 UTC Jul 5 2025
LASTHOG At:   14:13:27 UTC Jul 5 2025
PC:           0x000000aaae797f28 (suspend)
Call stack:   0x000000aaae797f28  0x000000aaac65003c  0x000000aaac64ffb8
```

Process causing CPU hog
Maximum hog (ms)
Last hog (ms)
Recorded dates

500ms SNMP hogs were recorded

Evaluate symptoms

Drops/delays on packets/system
Voice-Video quality problems
Slow down entire system
Dynamic routing protocols flaps

Determine how often

Determine hog length

Determine process

Check Related Config

Solution:

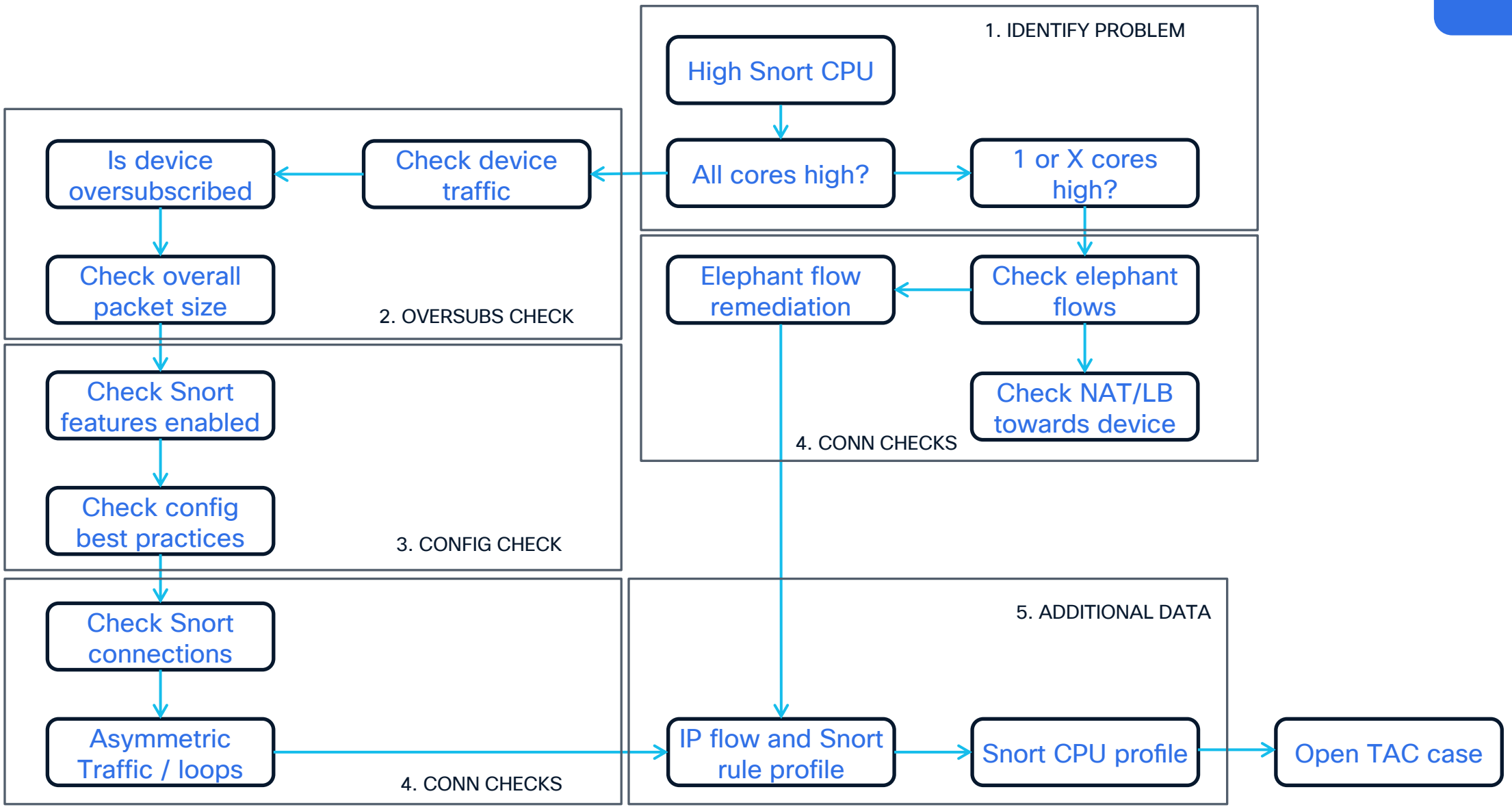
- Hogs caused by any process, when long and recurrent can have impact on other punted traffic like routing protocols.
- Modifying SNMP polling timers and reducing server number fixed the issue.

© 2026 Cisco and/or its affiliates. All rights reserved.

Snort

Snort CPU Flow Chart

REFERENCE



© 2026 Cisco and/or its affiliates. All rights reserved.

cisco

Case Study 3 – Snort on Fire

Customer is setting a new remote location, few users and servers have been added to the network (around 15% of total) and the firewall is showing high Snort CPU utilization ~75% for specific instance.

Environment:

- Hardware: FPR1220
- Software: FTD 7.7
- Firewall Mode: Routed Mode
- Redundancy: High-availability

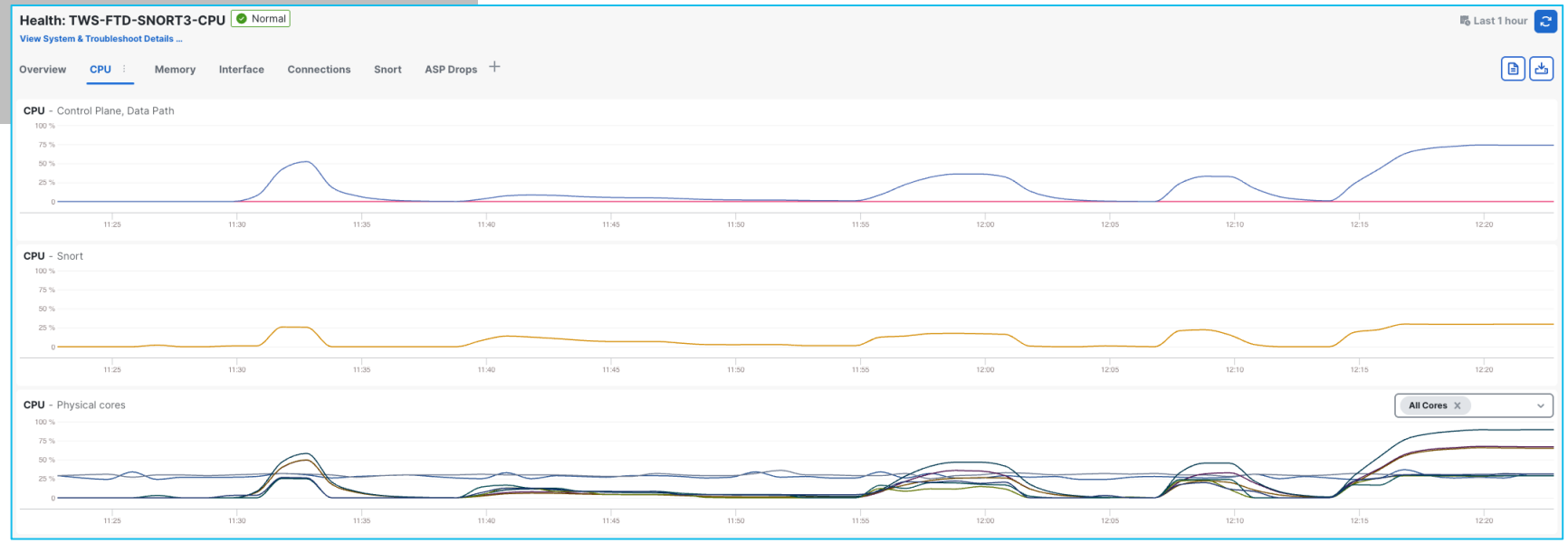
© 2026 Cisco and/or its affiliates. All rights reserved.

Snort CPU – 1/X Cores High

```
admin@firepower:~$ top -H -p $(pidof snort3)
top - 16:59:15 up,  3:53,  1 user,  load average: 4.30, 4.12, 4.00
Threads: 31 total,   0 running, 31 sleeping,   0 stopped,   3 zombie
%Cpu(s): 45.9 us,  6.6 sy,  0.9 ni, 46.5 id,  0.0 wa,  0.0 hi,  0.0 si,  0.0 st
MiB Mem :  15813.0 total,   5689.5 free,   7511.0 used,   2612.6 buff/cache
MiB Swap:  11600.2 total,  10734.2 free,    866.0 used.   6901.9 avail Mem

  PID USER      PR  NI    VIRT    RES    SHR S  %CPU  %MEM     TIME+ COMMAND
19183 root       1 -19 3324244 647784  70136 S  78.7   4.0  12:41.19 snort.core-5
19184 root       1 -19 3324244 647784  70136 S   0.0   4.0   0:00.91 snort.core-6
19185 root       1 -19 3324244 647784  70136 S   0.0   4.0   0:25.62 snort.core-7

> show snort cpu
Id       Pid      30sec    2min     5min

0        19183    75.3%    74.9%    74.2%
1        19184     0.0%     0.0%     0.0%
2        19185     0.0%     0.0%     0.0%

Summary           25.1%    24.9%    24.7%
```

Snort Instances PID and Usage

One CPU showing higher usage



© 2026 Cisco and/or its affiliates. All rights reserved.

Snort CPU – All Cores High

REFERENCE

```
admin@firepower:~$ top -H
top - 09:06:07 up 7 days, 19:28,  1 user,  load average: 7.59, 6.94, 5.67
Threads:  31 total,   3 running,  28 sleeping,   0 stopped,   0 zombie
%Cpu(s): 74.7 us,  6.7 sy,  1.0 ni, 17.6 id,  0.0 wa,  0.0 hi,  0.0 si,  0.0 st
MiB Mem :  15813.0 total,   5446.2 free,   7892.4 used,   2474.4 buff/cache
MiB Swap:  11600.2 total,  10734.4 free,    865.8 used.   6520.2 avail Mem

  PID USER      PR  NI    VIRT    RES    SHR S  %CPU  %MEM     TIME+ COMMAND
49522 root       1 -19 4825052   1.2g  70324 R  99.9   7.8  78:59.35 snort.core-6
49523 root       1 -19 4825052   1.2g  70324 R  99.9   7.8  78:17.00 snort.core-7
49521 root       1 -19 4825052   1.2g  70324 R  99.7   7.8  75:34.49 snort.core-5
49255 root       1 -19 4825052   1.2g  70324 S   4.7   7.8 282:44.79 snort3

> show snort cpu
Id       Pid      30sec    2min     5min

0        49521    74.5%    74.6%    74.5%
1        49522    74.1%    74.3%    72.2%
2        49523    75.2%    75.0%    75.0%

Summary           74.6%    74.6%    73.9%
```

All cores with high utilization

Snort Instances PID and Usage

© 2026 Cisco and/or its affiliates. All rights reserved.

Snort Features

Consider impact of different Snort features on device performance.

Decryption Policies

File Policies

Intrusion + NAP

Poorly written IPS rules

URL

Excessive Logging

Discovery Misconfigure

Certain Preprocessors

© 2026 Cisco and/or its affiliates. All rights reserved.

Configuration Best Practices – ACP

CONSIDER RULE ACTIONS AND CLASSIFY YOUR TRAFFIC

Monitor

Not used permit/deny traffic
Purpose forces conn logging

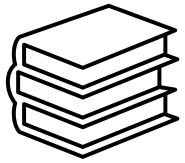
Trust

Security Intelligence
Identity Policy
QoS

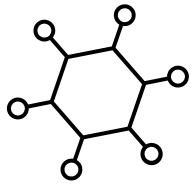
Allow

Trust Inspections +
Network Discovery
Intrusion/NAP Policy
File Policy

CONSIDER WHAT TO AVOID



Avoid Excessive Logging



Avoid Overloaded Rules

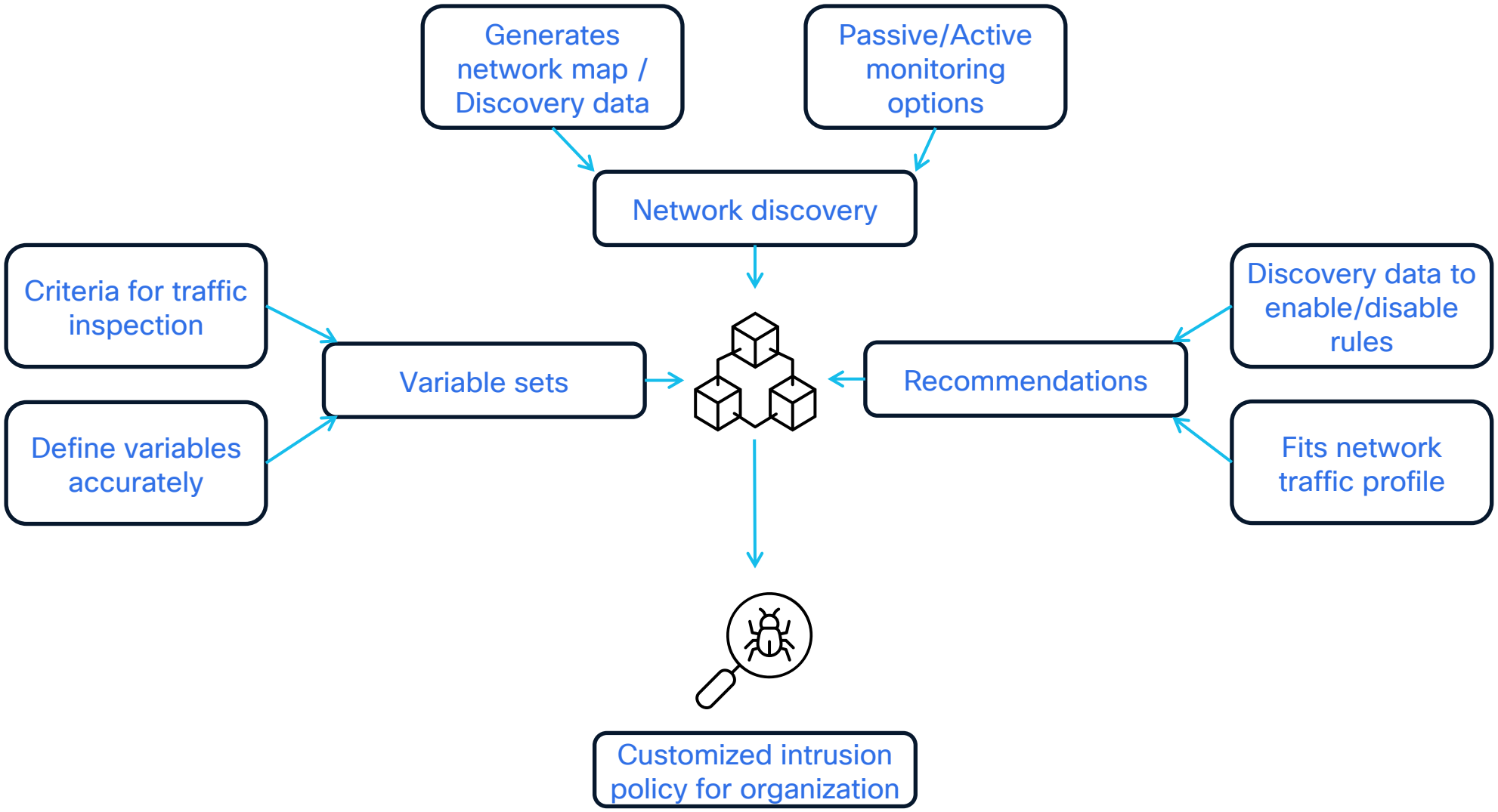
Avoid Duplicated / Shadowed Rules

RULE ORDERING

- Specific Before General
- Blocking Before Trust - Allow
- L3-L4 Before L7 (APP/URL)
- URL Filtering Before APP
- Rules with Intrusion - File

© 2026 Cisco and/or its affiliates. All rights reserved.

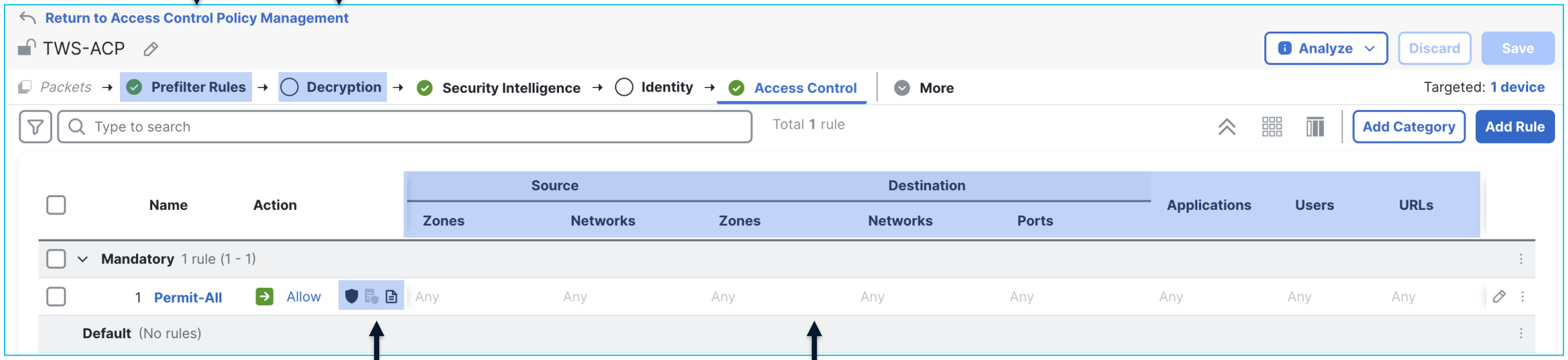
Variable Sets, Discovery and Recommendations



© 2026 Cisco and/or its affiliates. All rights reserved.

ACP

Prefilter in use, no decryption policy

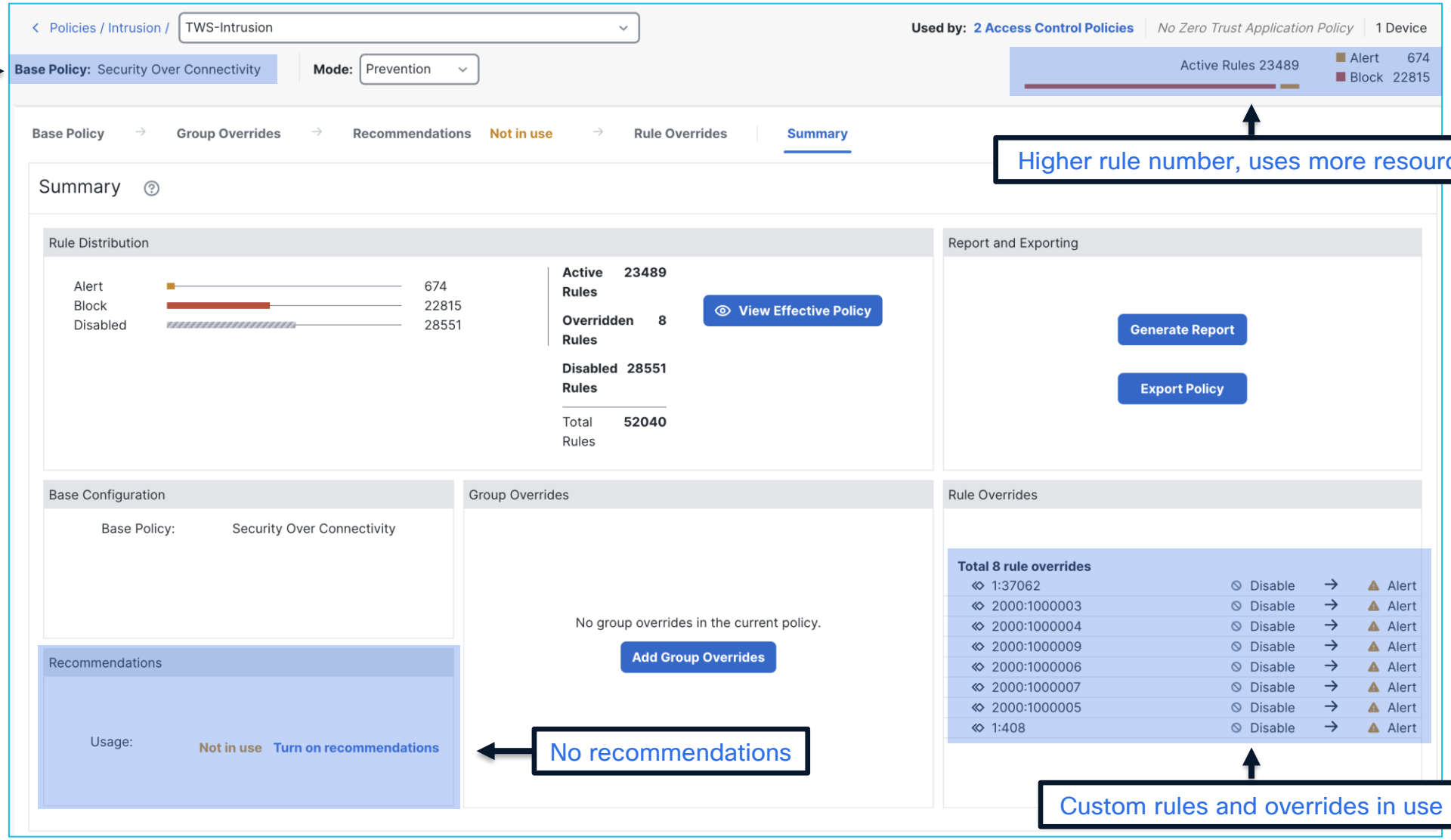


Intrusion policy, no file policy and double logging enabled

Single rule allowing all traffic

© 2026 Cisco and/or its affiliates. All rights reserved.

Intrusion

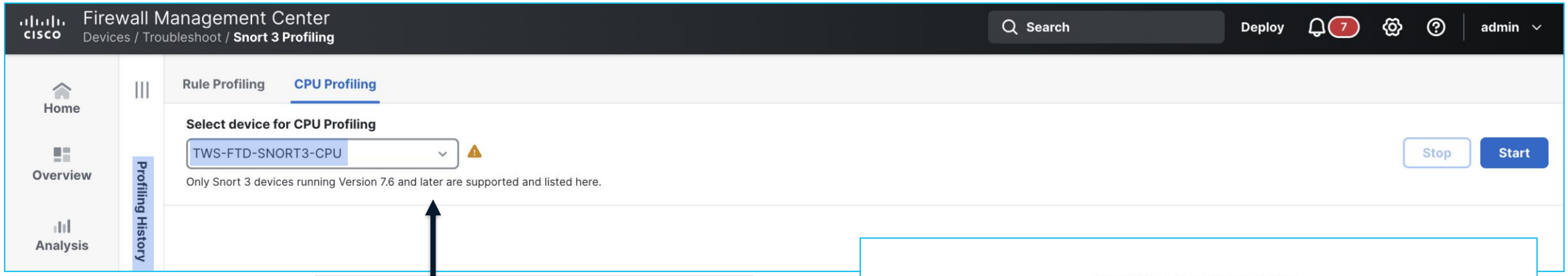


© 2026 Cisco and/or its affiliates. All rights reserved.

Snort CPU Profiling

FMC 7.6

- Profiles the CPU time taken by modules/inspectors to process packets in each time interval.
- Results displays processing time taken by all modules during sessions.
- Available under **Devices > Snort 3 profiling > CPU profiling**.



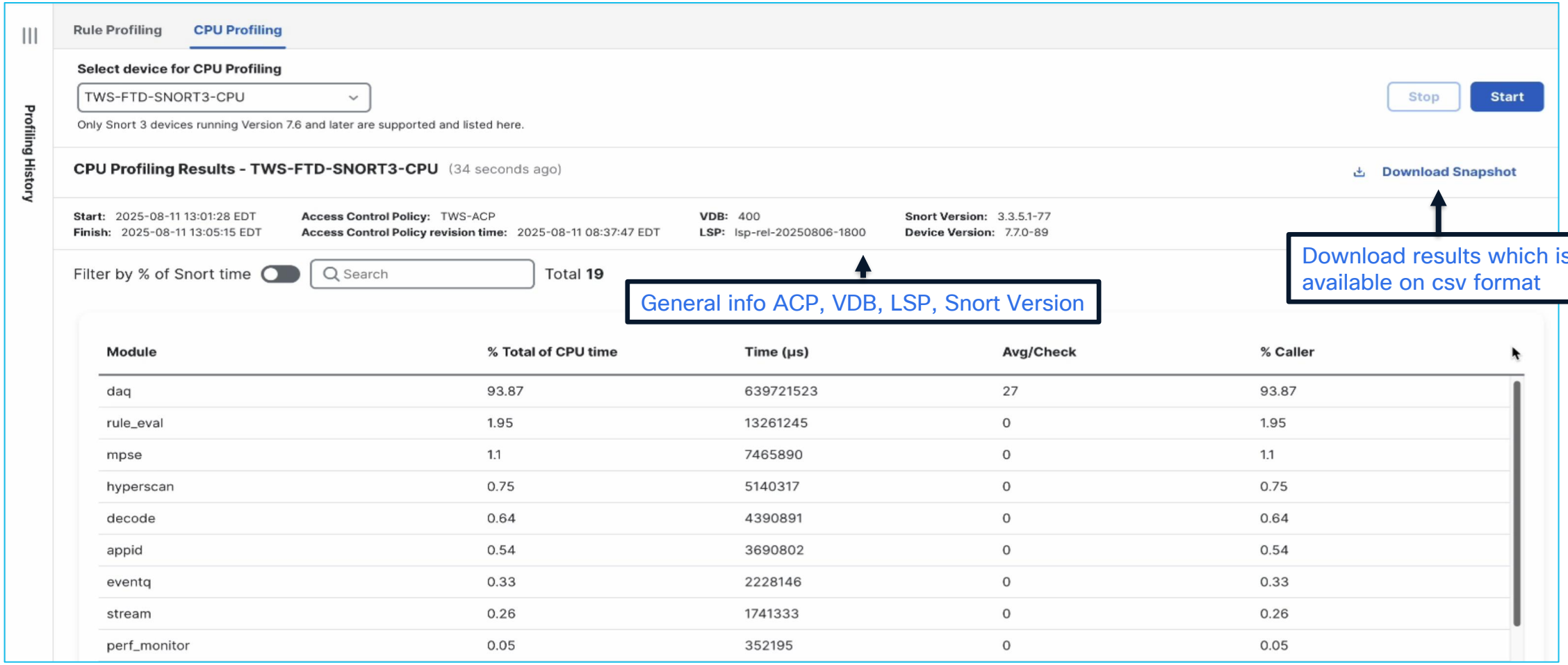
Choose the FTD for running rule profiling

Historical data is available for later review

Shows up after starting the rule profiling, can also be monitored from FMC tasks

© 2026 Cisco and/or its affiliates. All rights reserved.

Snort CPU Profiling



Download results which is available on csv format

General info ACP, VDB, LSP, Snort Version

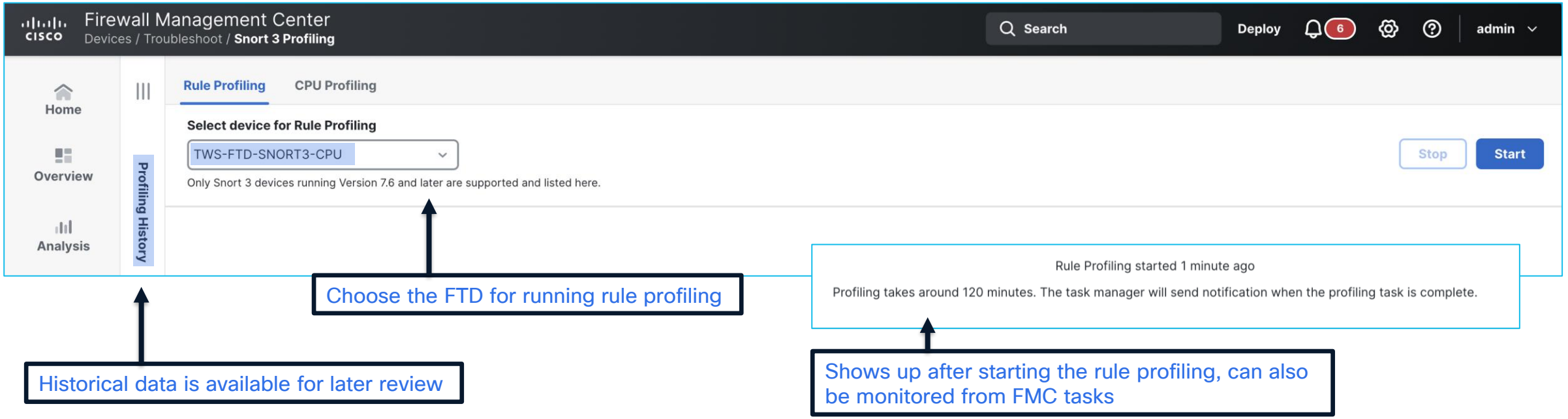
From the results nothing seems abnormal

© 2026 Cisco and/or its affiliates. All rights reserved.

Snort Rule Profiling

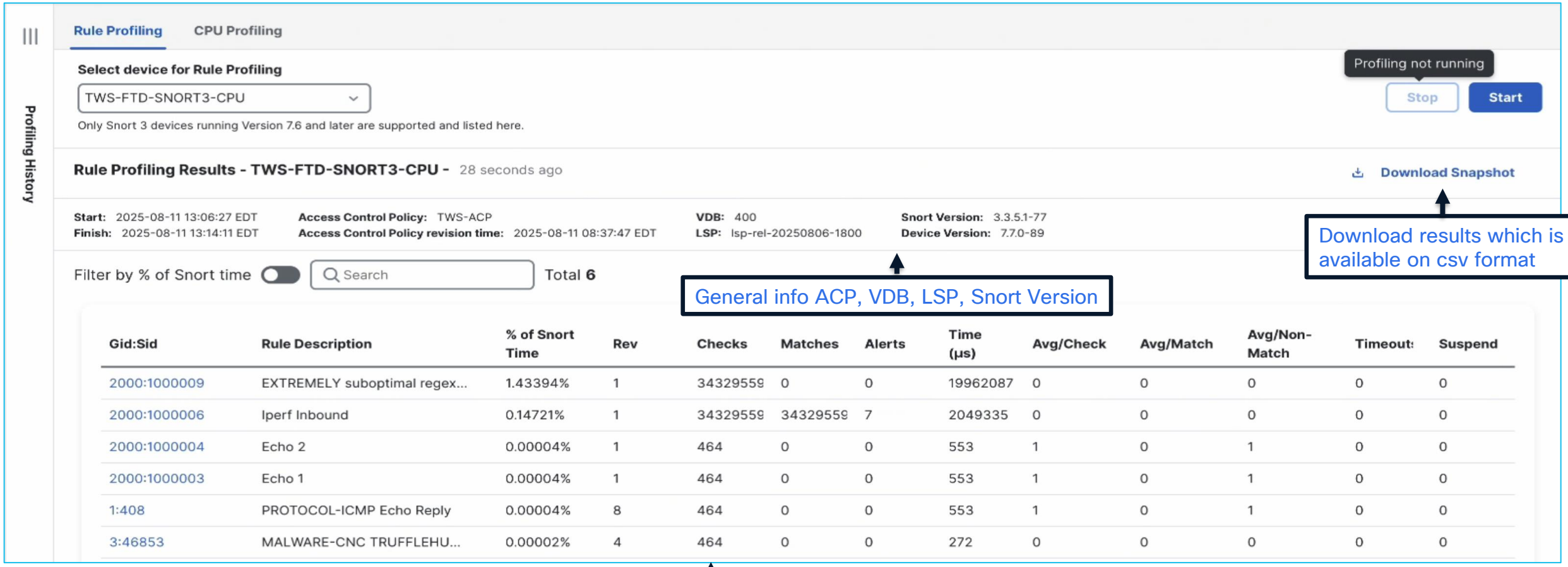
FMC 7.6

- Available for both Snort 2 and Snort 3 on CLI, on FMC 7.6+ UI Snort 3 only.
- Collects processing time, average checks and matches per Snort intrusion rule.
- Rule Profiler displays the 100 IPS rules which took the most time to check. Does not require Snort 3 reload/restart.
- Run in **Devices > Snort 3 Profiling > Rule Profiling**



© 2026 Cisco and/or its affiliates. All rights reserved.

Snort Rule Profiling



Download results which is available on csv format

General info ACP, VDB, LSP, Snort Version

Custom rules on top, 2000:1000009 is concerningly high

© 2026 Cisco and/or its affiliates. All rights reserved.

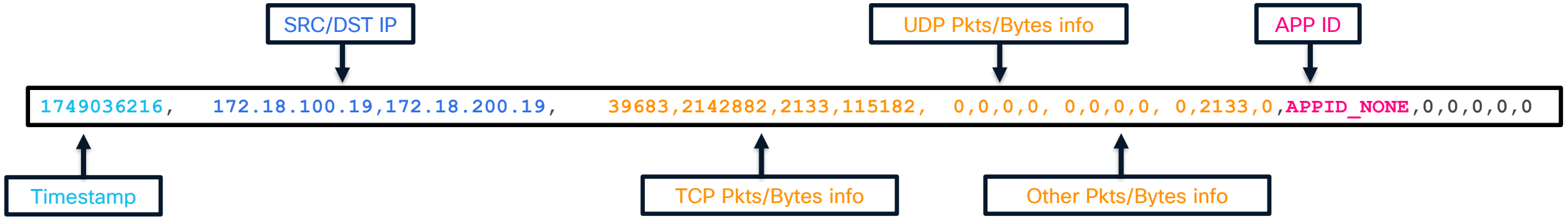
Snort IP Flow

```
> system support flow-ip-profiling start flow-ip-file flowipjun4

> system support flow-ip-profiling show
Snort flow ip profiling is enabled
```

Collects per instance flows

```
> system support flow-ip-profiling stop
File created in : /ngfw/var/sf/detection_engines/1642c748-37dc-11f0-a8f7-45ad857e2884/instance-3/flowipjun4
File created in : /ngfw/var/sf/detection_engines/1642c748-37dc-11f0-a8f7-45ad857e2884/instance-2/flowipjun4
File created in : /ngfw/var/sf/detection_engines/1642c748-37dc-11f0-a8f7-45ad857e2884/instance-1/flowipjun4

admin@firepower:~$ ls -lah /ngfw/var/common/
total 352K
drwxr-sr-x  2 admin admin  135 Jun  4 11:27 .
drwxr-xr-x 15 root  root  4.0K May 23 13:39 ..
-rw-rw-r--  1 root  admin  98K Jun  4 11:27 flowip_statistics.tar
```

TAR file is under /ngfw/var/common/



Pro Tip: In case of high CPU on specific instance, analyze its flow dumps. Optionally, use CSV parsers like excel.

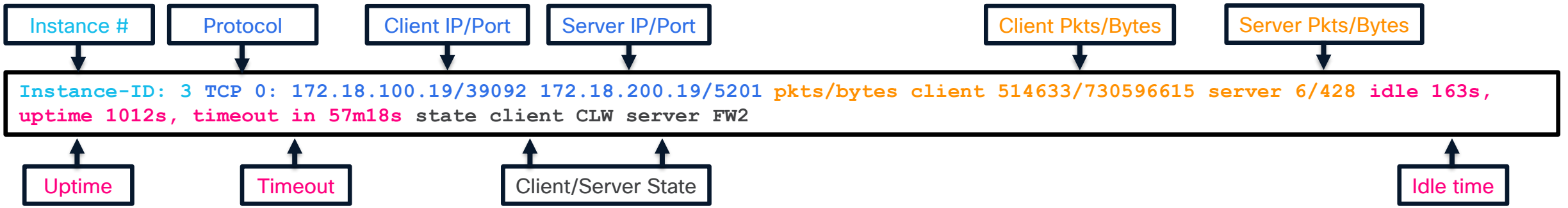
© 2026 Cisco and/or its affiliates. All rights reserved.

Connection Hashing (5-Tuple)

FTD 7.6

- Connections distributed to different Snort instances is based on 5-tuple.
- Command **show snort flows** finds connections with highest num of bytes, pkts, bytes/sec (BPS), in all or specific instances.

```
> show snort flows
No flows are dumped in /var/sf/detection_engines/1642c748-37dc-11f0-a8f7-45ad857e2884/file-3
Instance-ID: 2 ICMP 0: 172.18.200.19 type 3 172.18.100.19 pkts/bytes client 1/590 server 0/0 idle 1s, uptime 1s, timeout 2s
Instance-ID: 1 UDP 0: 172.18.100.19/1346 172.18.200.19/5201 pkts/bytes client 42758863/31727076346 server 0/0 idle 0s, uptime 1135s, timeout in 2m1s
Instance-ID: 1 UDP 0: 172.18.100.19/1351 172.18.200.19/5201 pkts/bytes client 41769218/30992759756 server 0/0 idle 0s, uptime 1122s, timeout in 2m1s
```



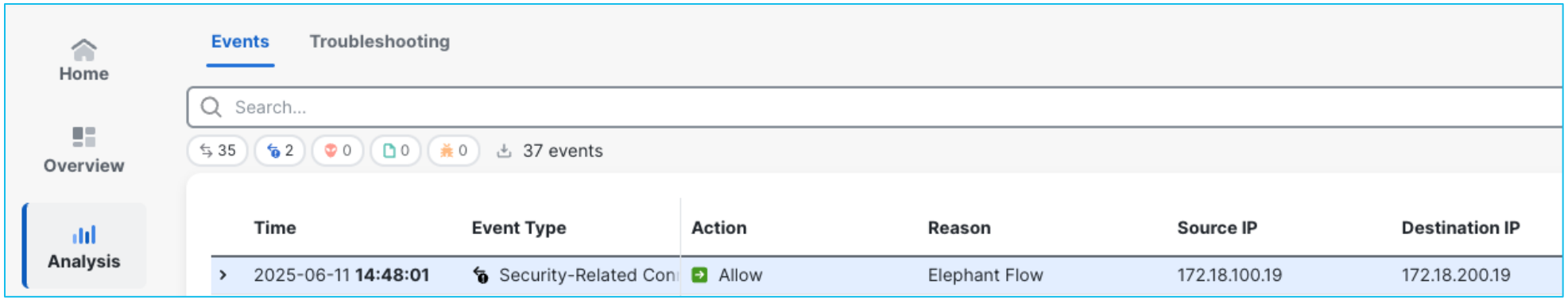
© 2026 Cisco and/or its affiliates. All rights reserved.

Elephant Flows

- Elephant flows are large, long duration and fast transmit flows with high ability to cause duress for snort cores.
- Even small number of them, can occupy a disproportionate share of total bandwidth over a period.

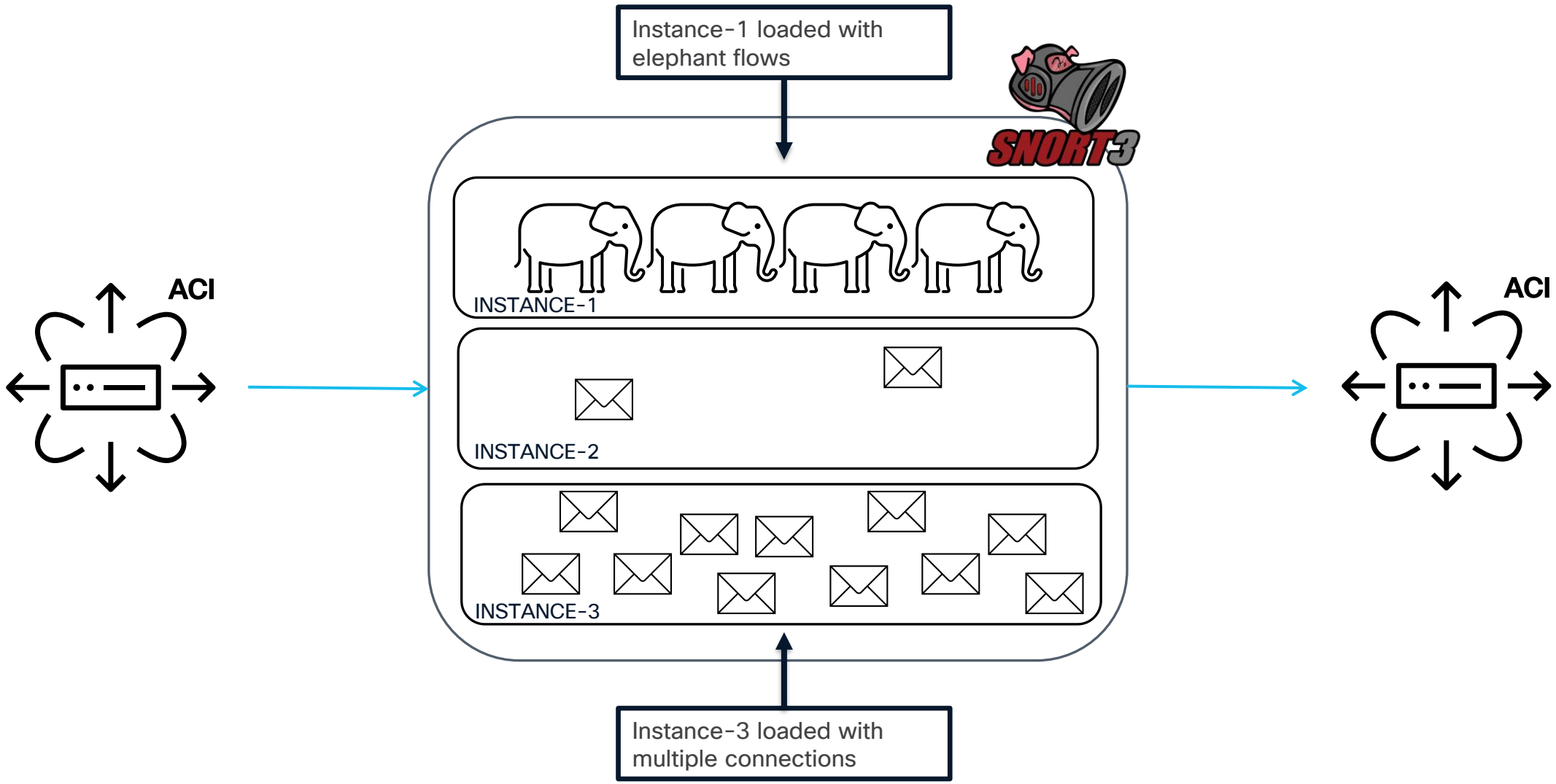
```
> show snort flows
Instance-ID: 1 UDP 0: 172.18.100.19/1346 172.18.200.19/5201 pkts/bytes client 42758863/31727076346 server 0/0 idle 0s, uptime 1135s, timeout in 2m1s
Instance-ID: 1 UDP 0: 172.18.100.19/1351 172.18.200.19/5201 pkts/bytes client 41769218/30992759756 server 0/0 idle 0s, uptime 1122s, timeout in 2m1s

> show conn
13 in use, 236965 most used
Inspect Snort:
        preserve-connection: 3 enabled, 0 in effect, 236933 most enabled, 11 most in effect

TCP Inside  172.18.100.19:1346 Outside  172.18.200.19:5201, idle 0:01:45, bytes 31503543773, flags UI N1N3
TCP Inside  172.18.100.19:1351 Outside  172.18.200.19:5201, idle 0:01:45, bytes 30674243193, flags UI N1N3

firepower# show conn detail
 N - inspected by Snort (1 - preserve-connection enabled, 2 - preserve-connection in effect, 3 - elephant-flow, 4 - elephant-flow bypassed, 5 - elephant-flow
throttled, 6 - elephant-flow exempted, 7 - fast-forwarded flow, 8 - whitelisted flow, 9 - down/busy failopened)
```

~30G Elephant flows are visible on both LINA and Snort



© 2026 Cisco and/or its affiliates. All rights reserved.

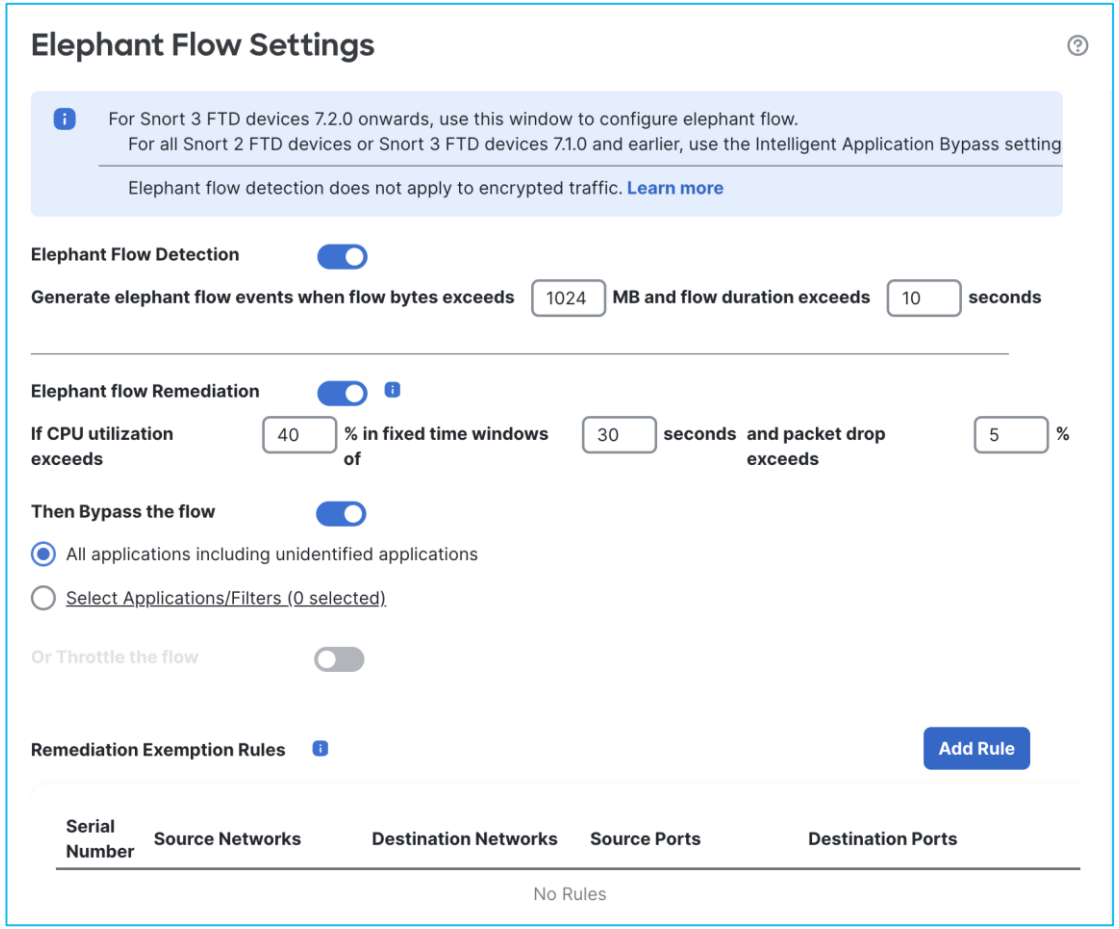
Elephant Flows



© 2026 Cisco and/or its affiliates. All rights reserved.

Elephant Flows Remediation

- Use when multiple elephant flows are causing one or more cores to be on high CPU.
- Since 7.2+ the remediation has two actions that can be applied to reduce system stress: Bypass/Throttle.

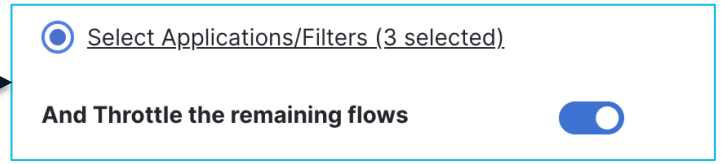


Feature not available for 2100 series

Characteristics to mark flow as elephant flow

Define triggers like:
- CPU utilization %
- Time
- Packet drop %

Application filters are required to enable throttle the flow



Traffic to be exempted from remediation

© 2026 Cisco and/or its affiliates. All rights reserved.

Case Study 3 – Snort on Fire – Conclusion

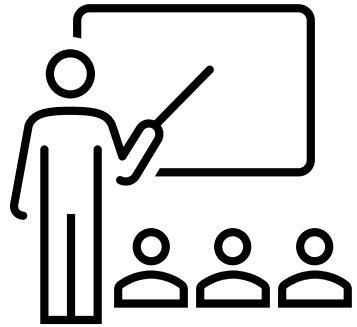
- Custom intrusion rules using more CPU cycles due to miss/suboptimal configuration were removed.
- Advices for ACP best practices were given.
- Snort core was under high usage due to multiple elephant flows (Stress test run between customer servers).
- The customer stopped stress test during production hours.
- Elephant flow remediation was configured to help snort cores on this situations.

© 2026 Cisco and/or its affiliates. All rights reserved.

Learnings & Call For Action

What did you learn?

- How to approach high CPU troubleshooting for LINA and Snort.
- How important the baseline and use of health monitoring can be.
- Best practices learned from pro tips.
- How CPU related issues may show misleading symptoms at the beginning.



Call for action!

- Define your CPU (LINA & Snort) and throughput (General & VPN) baseline.
- Calculate throughput values based on your resource profile when using multi-instance.
- Enable CPU health monitoring in your FMC if not enabled.
- Add troubleshooting flows and commands sheets to your notes.
- Reach out to me if you want to discuss CPU issues and/or have additional questions.

© 2026 Cisco and/or its affiliates. All rights reserved.

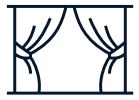
Complete your session surveys

Complete your surveys in the Cisco Events App.

Complete a minimum of 4 session surveys and the overall event survey to receive a unique Cisco Live t-shirt.
(from 11:30 on Thursday, while supplies last)

© 2026 Cisco and/or its affiliates. All rights reserved.

Continue your education



Visit the Cisco Showcase for related demos

Book your one-on-one Meet the Engineer meeting

Visit the Technical Solutions Clinics to discuss your technical questions

Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs

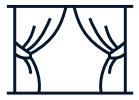
Visit the On-Demand Library for more sessions at CiscoLive.com/On-Demand

Contact me at: https://www.linkedin.com/in/luis-d-restrepo-ab831ab5/

© 2026 Cisco and/or its affiliates. All rights reserved.

cisco

Continue your education



Achieving High Availability with Secure Access and Secure Firewall.
[LABSEC-2755]

Troubleshooting of Data-Path on Cisco Secure Firewall Threat Defense.
[LABSEC-2550]

Cisco Secure Firewall Threat Defense: Deep Dive into Traffic Control.
[LABSEC-2981]

Enhancing Network Security with Encrypted Visibility Engine on Secure Firewall Threat Defense.
[LABSEC-2392]

Contact me at: https://www.linkedin.com/in/luis-d-restrepo-ab831ab5/

© 2026 Cisco and/or its affiliates. All rights reserved.

Thank you

cisco Live !


CISCO