

Mastering Intrusion Prevention Systems

CISCO Live !

Configuration, Components, and Best Practices

Anita Quintero
Customer Success Technical Leader

About your speaker

Anita Quintero

- Customer Success Technical Leader
- Focused on Security Portfolio
- CCIE Security
- Cisco employee since 2015

Free Time:

- Skiing, Photography
- Creating artwork with epoxy resin



Common Challenges When Deploying IPS

High volume of alerts and false positives

Risk of blocking legitimate traffic

Performance concerns

Limited visibility into encrypted traffic

Zero-day attacks

Scope of the Session

We will cover:

- Cisco Secure IPS components
- Cisco Secure IPS deployment best practices
- What's new in Cisco Secure IPS
- FMC managed deployment

We will **NOT** cover:

- IPS events analysis
- Troubleshooting
- Writing custom snort rules
- IPS in Snort2
- Cisco Secure Firewall initial deployment

You are in the right room if:

- New to Cisco Secure IPS; interested in deployment and functionality
- Have deployed Cisco IPS; want to learn what's new and best practices

Agenda

- 01 Cisco Secure IPS Deployment
- 02 SnortML
- 03 Day-2 Operations
- 04 Summary



Webex App

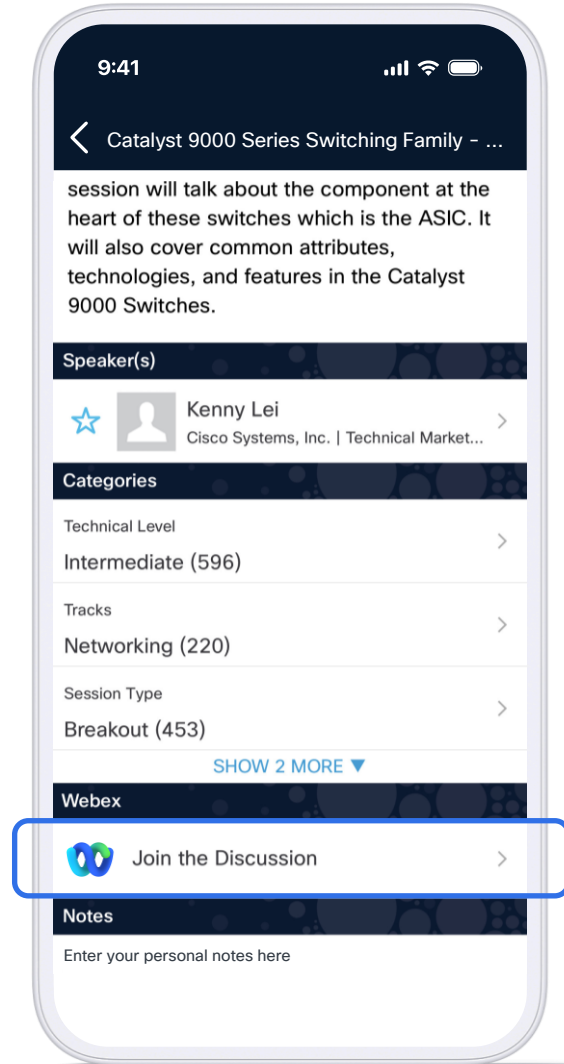
Questions?

Use Webex App to chat with the speaker after the session

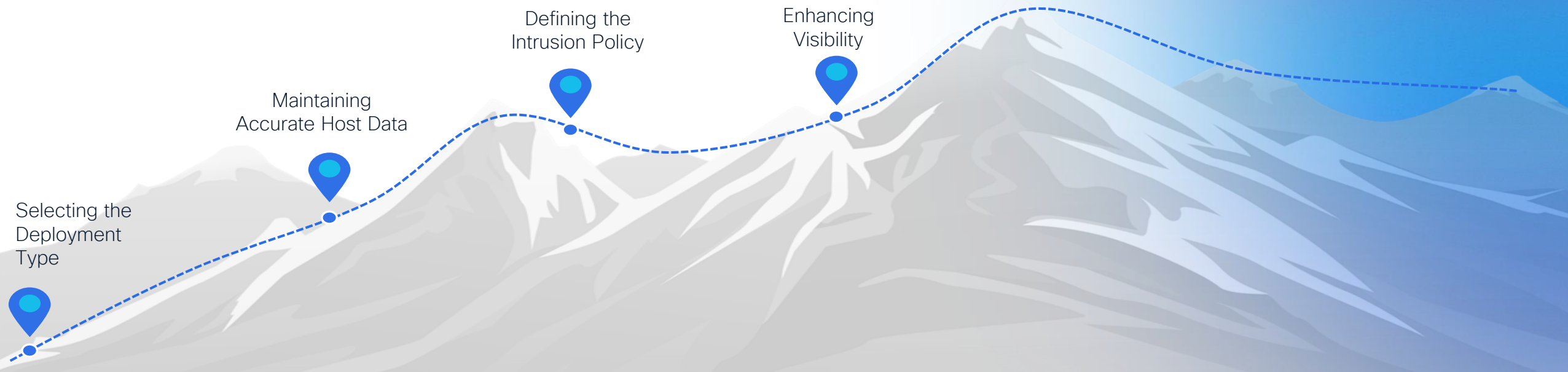
How

- 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

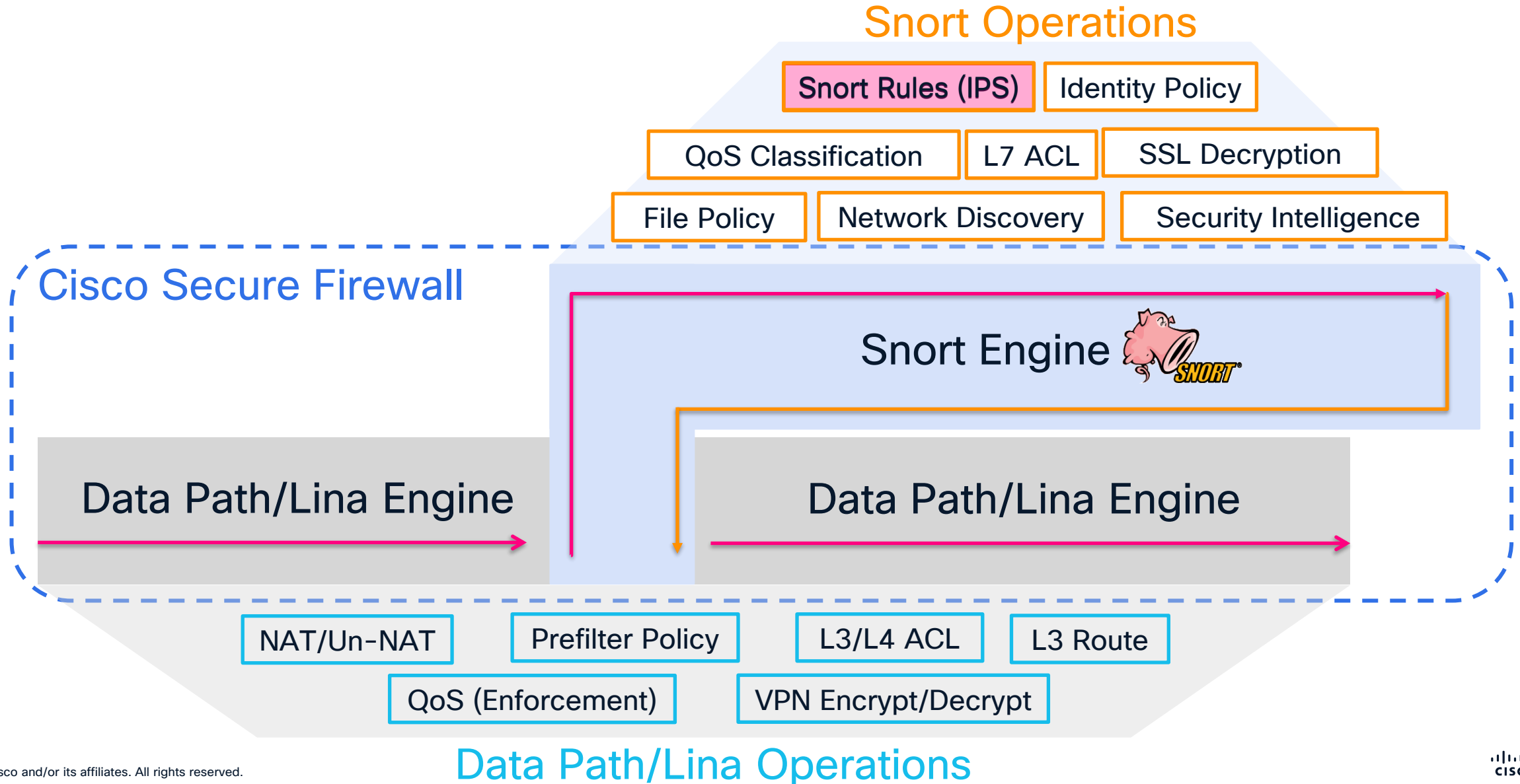
Webex spaces will be moderated by the speaker until February 27, 2026.



Cisco Secure IPS Deployment

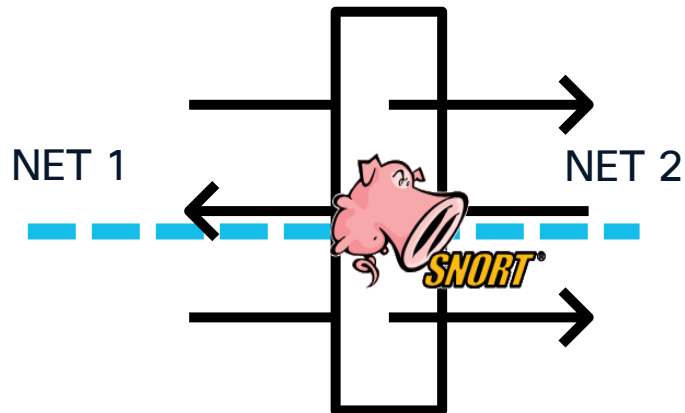


Cisco Secure Firewall Components and Operations



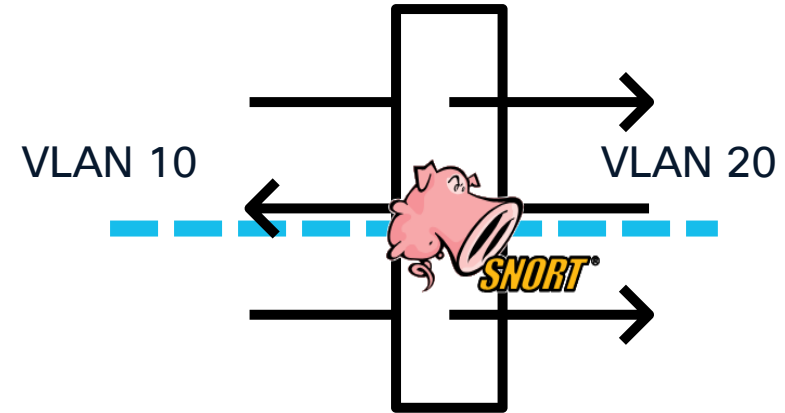
Cisco Secure Firewall Mode

Routed



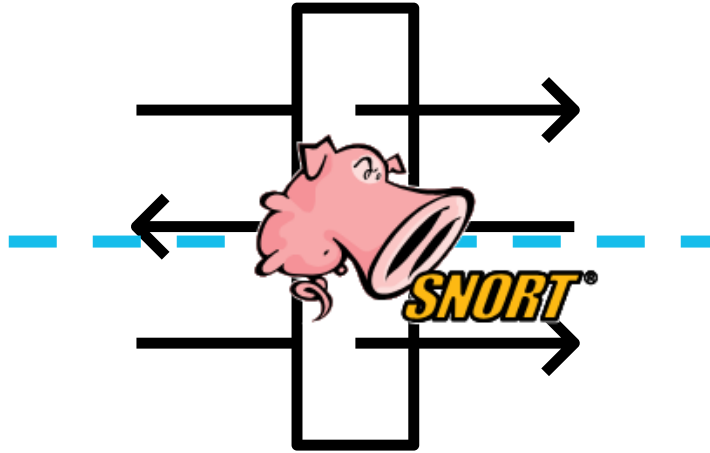
The firewall acts as a router hop, with each interface on a different subnet, routing traffic between bridge groups and routed interfaces.

Transparent



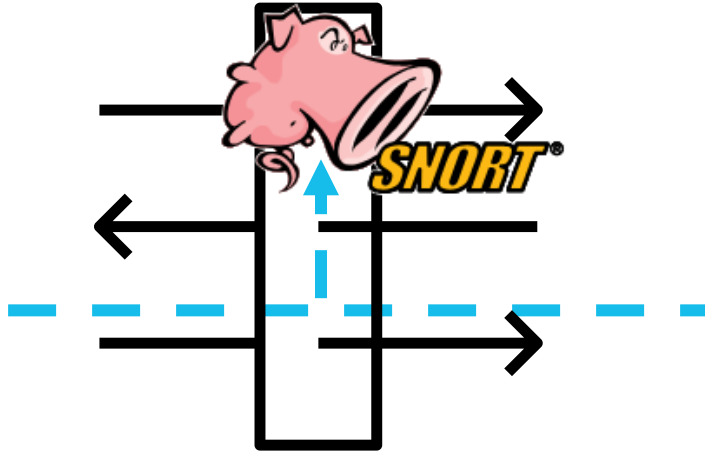
The firewall acts as a Layer 2 bridge, passing traffic between grouped interfaces without routing or appearing as a router hop.

IDS/IPS-only Mode



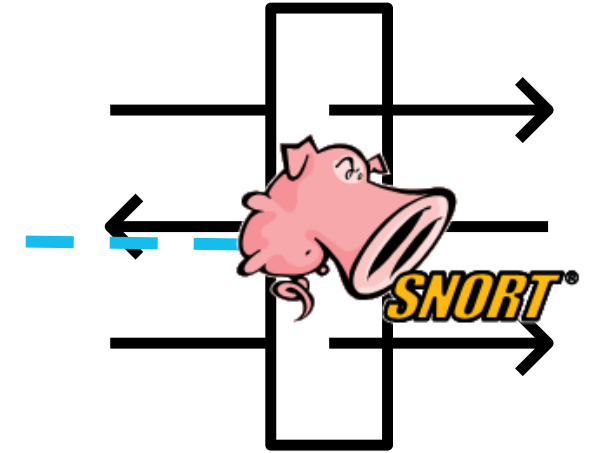
Inline

Pairs of interfaces that transparently forward all traffic through the device enabling inspection.



Inline Tap

Packets are copied for transmission, allowing analysis without impacting the network.



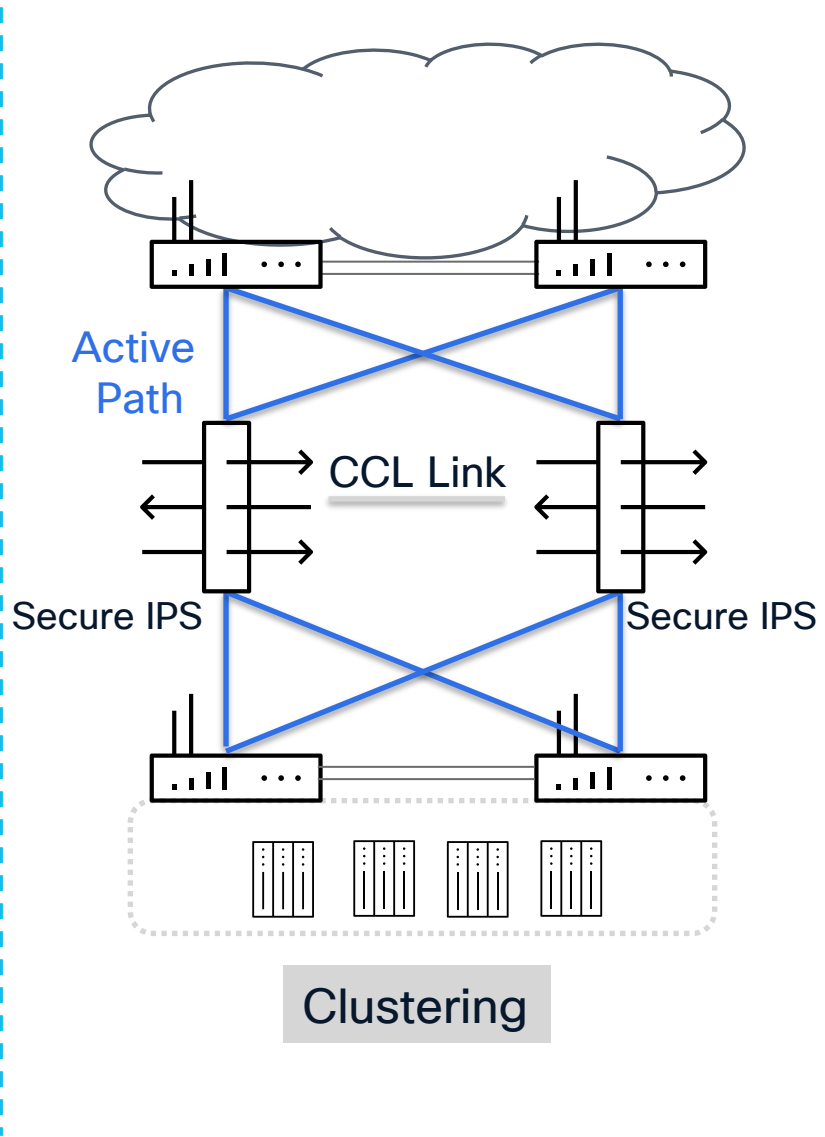
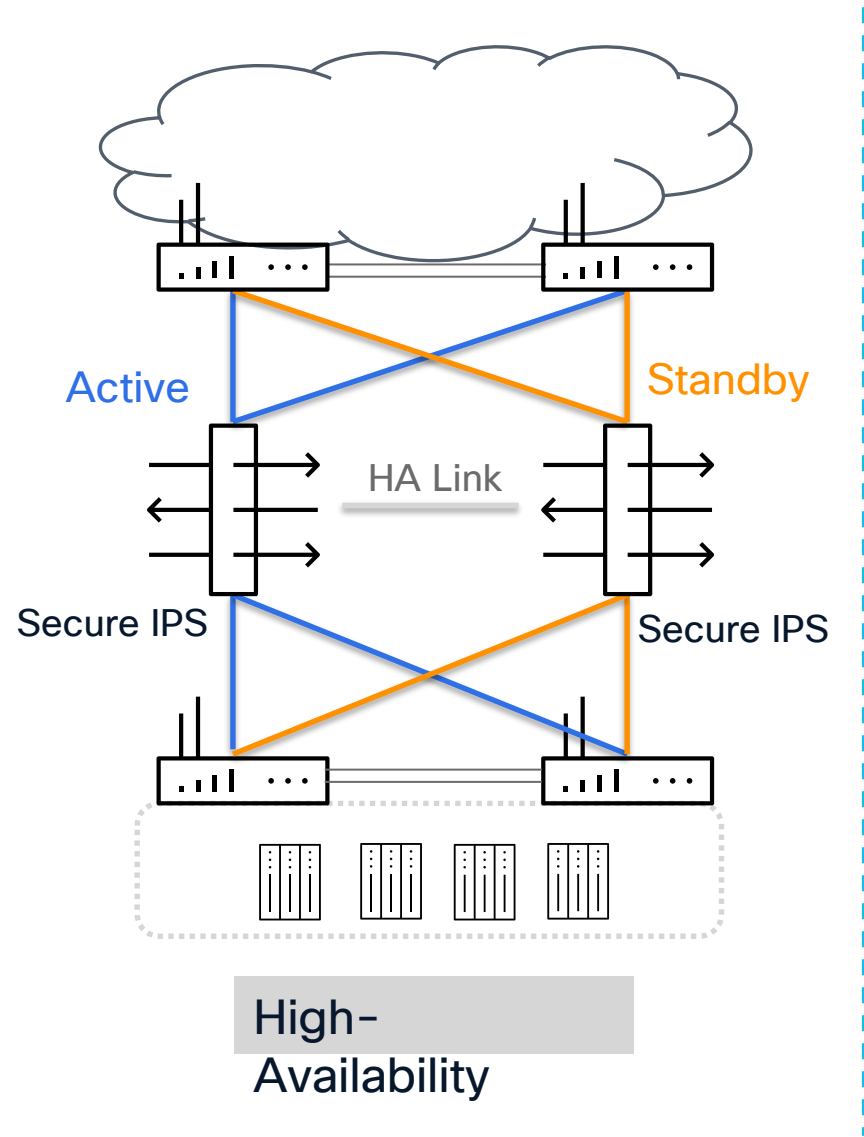
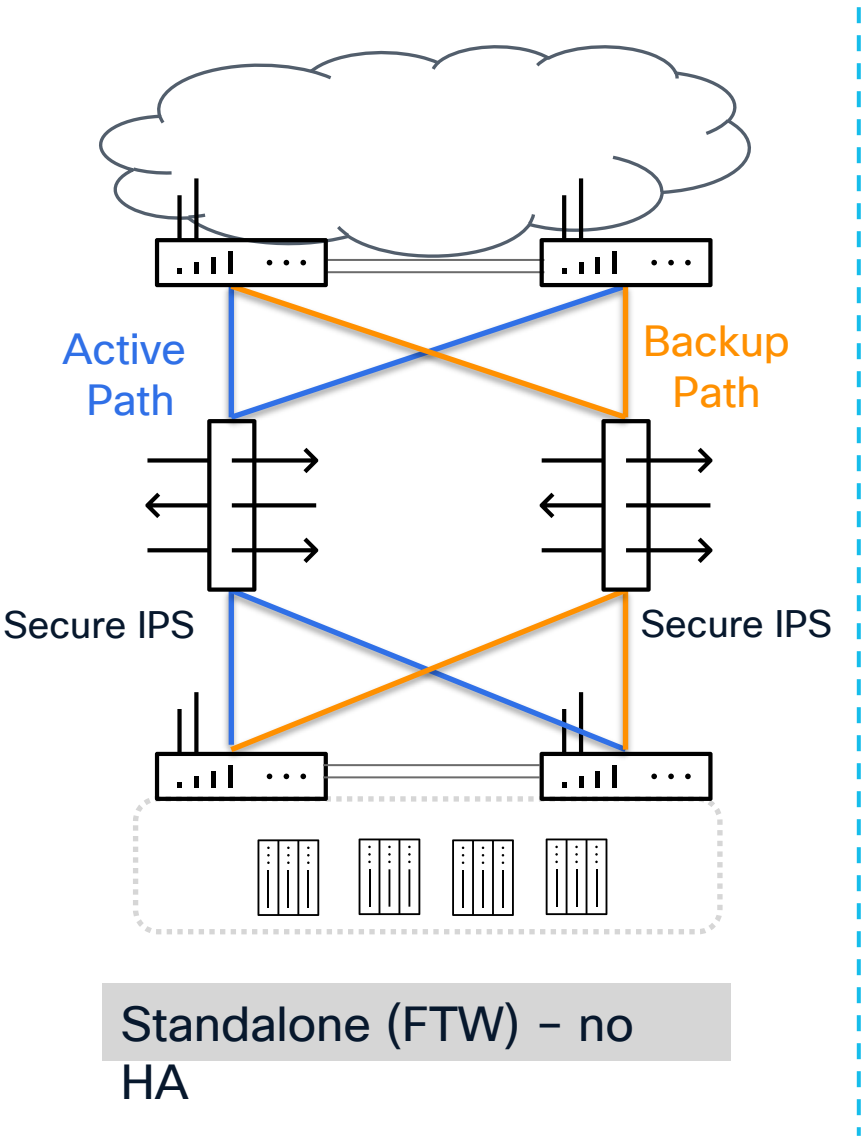
Passive

Monitoring traffic across a network using a switch SPAN port.

Interface Modes and Operations

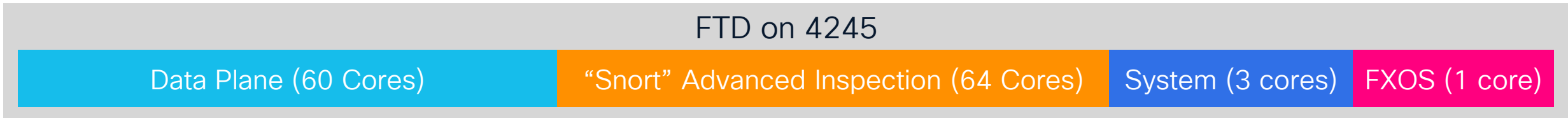
| | Routed | Bridge group | IPS-only |
|------------------------|--------|--------------|----------|
| Route Lookup | ✓ | | |
| MAC Lookup | | ✓ | |
| NAT/PAT | ✓ | ✓ | |
| Dynamic Routing | ✓ | | |
| VPN Features | ✓ | | |
| Deep packet inspection | ✓ | ✓ | ✓ |
| Clustering | ✓ | ✓ | ✓ |
| High-Availability | ✓ | ✓ | ✓ |

IPS Insertion Options



Performance Profiling for CPU Allocation

- FTD had a default CPU core allocation between Data Plane and Snort



- Tailor FTD to a specific use case with a configurable allocation
- Supported since FTD 7.3 (FTDv, 4100, 9300) and FTD 7.4.1 (3100, 4200)

| Name | Core allocation |
|--------------------------|--|
| Default | CPU cores allocated based on platform |
| VPN heavy with prefilter | 90% cores for data plane, 10% for Snort |
| VPN heavy | 60% cores for data plane, 40% for Snort |
| IPS heavy | 30% cores for data plane, 70% for Snort |

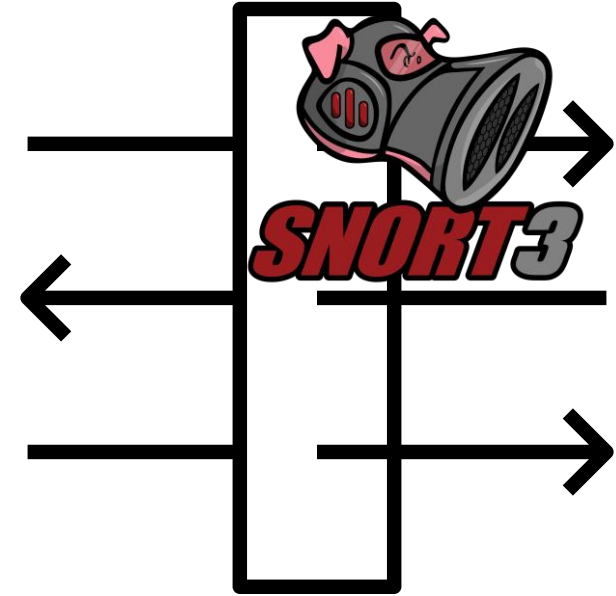
License Requirements

| License | Duration | Subscription Options | Granted Capabilities |
|-------------------|---|---|---|
| Essentials | Perpetual or Subscription Note Essentials subscription licenses are supported only on FTDv. | | <ul style="list-style-type: none"> • User and application control • Switching and routing • NAT |
| IPS | Subscription | <ul style="list-style-type: none"> • stand-alone subscription (T) • combination with URL Filtering (TC) • Malware defense (TM) • both (TMC) | <ul style="list-style-type: none"> • Intrusion detection and prevention • File control • Security Intelligence filtering |

Demo Details

Pre-configuration

- FTD and FMC initial configuration
- FTD registered in the FMC
- License enabled
- FTD basic configuration
 - Interfaces
 - NAT
 - Routing
 - ACP



FMCv – version 10.0
FTDv – version 10.0

Demo

Intrusion Policy Creation – Inspection Mode

- **Detection:**

- Performs detection and generates alerts only.
- No traffic is blocked in this mode.
- **Recommended** for initial deployment and baseline testing.

- **Prevention:**

- Actively takes action on traffic (e.g., dropping or blocking).
- Deploy only after testing and verifying the intrusion policy in Detection mode.

The screenshot shows the Firewall Management Center interface. A modal dialog titled "Create Intrusion Policy" is open. The dialog contains the following fields and options:

- Name ***: CL Intrusion Policy
- Description**: demo policy
- Inspection Mode**:
 - Detection
 - Prevention
- Base Policy**: Balanced Security and Connectivity

Below the "Inspection Mode" section, there is a note: "Intrusion rule actions are always applied. Connections that match a drop rule are blocked." At the bottom of the dialog are "Cancel" and "Save" buttons.

The background interface shows a table of intrusion policies with columns: Intrusion Policy, Description, Base Policy, and Usage Information. The table lists several policies, including "Demo", "IPS policy", "polityka ips", "Test", and "test policy".

Intrusion Policy Creation – Base Policy

| Policy | Description |
|------------------------------------|--|
| Connectivity Over Security | Minimal active rules (~600) prioritizing connectivity over security. |
| Balanced Security and Connectivity | The most popular policy balancing security and connectivity with ~10,000 active rules. |
| Security Over Connectivity | Provides the strongest security with ~23,000 active rules. Note: This may require tuning, increase firewall load, and reduce overall throughput. |
| Maximum Detection | Policy includes over 42,000 active rules; we recommend that you review and test this setting before deploying it into a production environment. |

Create Intrusion Policy ?

Name *

Description

Inspection Mode

Detection Prevention

Intrusion rule actions are always applied. Connections that match a drop rule are blocked.

Base Policy

- Balanced Security and Connectivity ^
- Balanced Security and Connectivity ✓
- Connectivity Over Security
- Maximum Detection
- No Rules Active
- Security Over Connectivity
- test policy

Group Overrides and Security Level

- Security levels correspond with the base policies.
 - **Level 1** – Connectivity Over Security
 - **Level 2** – Balanced Security and Connectivity
 - **Level 3** – Security Over Connectivity
 - **Level 4** – Maximum Detection
- Security level for a rule group can be customized based on security needs.

The screenshot displays the Cisco Firewall Management Center interface for configuring intrusion policies. The main view is 'Rule Overrides' for a 'CL Intrusion Policy'. A table lists various rule groups with their security levels and override status. A modal window titled 'Edit Security Level' is open, showing a slider to adjust the security level. Two callout boxes highlight the 'Security Level' column in the table and the 'Edit Security Level' modal.

| Group Name | Security Level | Override | Rule Count | Action |
|-------------------|----------------|----------|------------|---------|
| Chrome | Level 1 | Exclude | 211 | Exclude |
| Firefox | Level 1 | Exclude | 309 | Exclude |
| Internet Explorer | Level 1 | Exclude | 2553 | Exclude |
| WebKit | Level 1 | Exclude | 168 | Exclude |

Modify the Security Level for Rule Category

Modify the Security Level for Rule Group

Rule Actions

| Rule Action | Description |
|-------------------|--|
| alert | generate an alert on the current packet |
| block | block the current packet and all the subsequent packets in this flow |
| drop | drop the current packet |
| reject | send response to client and terminate session. |
| rewrite | enables overwrite packet contents based on a "replace" option in the rules |
| disable | disable the rule |
| revert to default | revert to default action |

Base Policy → Group Overrides → Recommendations **Not in use** → **Rule Overrides** | Summary

Rule Overrides ⓘ [Back To Top](#)

107 items ⓘ ▾

Rule Categories / Browser / Chrome [Exclude](#)

Security Level ■■■□□ [Edit](#)

Description Rules for detecting exploits against the Chrome Web browser

Rule Action ⓘ Search by CVE, SID, Reference Info, or Rule Message ⓘ

211 rules **Presets:** [Alert \(0\)](#) | [Block \(20\)](#) | [Disabled \(191\)](#) | [Overridden \(0\)](#) | [Advanced Filters](#)

| <input type="checkbox"/> | GID:SID | Rule Details | Rule Action ⓘ | Set By | Assigned Groups |
|----------------------------|---------------------------|--------------|-------------------|-------------|---|
| > <input type="checkbox"/> | 1:52068 🔗 | BROWSER-C... | Block (Default) ^ | Base Policy | Chrome, Malicious ... 🔗 🗨 |
| > <input type="checkbox"/> | 1:52069 🔗 | BROWSER-C... | Block (Default) v | Base Policy | Chrome, Malicious ... 🔗 🗨 |
| > <input type="checkbox"/> | 1:49360 🔗 | BROWSER-C... | Alert | Base Policy | Chrome, Malicious ... 🔗 🗨 |
| > <input type="checkbox"/> | 1:49361 🔗 | BROWSER-C... | Rewrite | Base Policy | Chrome, Malicious ... 🔗 🗨 |
| > <input type="checkbox"/> | 1:53752 🔗 | BROWSER-C... | Drop | Base Policy | Chrome, Malicious ... 🔗 🗨 |
| > <input type="checkbox"/> | 1:53754 🔗 | BROWSER-C... | Reject | Base Policy | Chrome, Malicious ... 🔗 🗨 |
| > <input type="checkbox"/> | 1:53753 🔗 | BROWSER-C... | Disable | Base Policy | Chrome, Malicious ... 🔗 🗨 |
| > <input type="checkbox"/> | 1:53751 🔗 | BROWSER-C... | Revert to default | Base Policy | Chrome, Malicious ... 🔗 🗨 |
| > <input type="checkbox"/> | 1:53751 🔗 | BROWSER-C... | Block (Default) v | Base Policy | Chrome, Malicious ... 🔗 🗨 |

Recommended Rules

- Recommended Rules automatically tune your Snort rules for the applications, servers, and hosts in your network.
- They enable additional rules or optimize the current rule set by disabling rules for vulnerabilities that are not present in the network.
- Rule tuning is performed based on **host data** collected through passive and/or active discovery.

The screenshot shows the Cisco Recommended Rules configuration page for a policy named 'CL Intrusion Policy'. The page is divided into several sections: 'Base Policy', 'Group Overrides', 'Recommendations', 'Rule Overrides', and 'Summary'. The 'Recommendations' section is highlighted in red. A modal window titled 'Cisco Recommended Rules' is open, showing a 'Security Level' slider, an 'Accept Recommendation to Disable Rules' checkbox, a 'Protected Networks' dropdown menu, and buttons for 'Cancel', 'Generate', and 'Generate and Apply'. Below the modal, there is a 'Start using recommendations' section with a 'Start' button.

Annotations in pink boxes with arrows pointing to the interface elements:

- Increase the Security Level if you want to enable new rules
- Accept Recommendation to Disable Rules based on host profile
- Select Protected Network, leave blank for any-ipv4 any-ipv6
- Generate rules to review before applying

Recommended Rules

- After generating Recommended Rules:
 - Accept – to use Recommended Rules
 - Refresh – to re-generate Recommended Rules
 - Edit – to edit Networks and Security Level for which the Recommended Rules are generated
 - Discard – to discard Recommended Rules usage

Recommendations

Usage: In Use

Security Level

Generated on 2025-12-30 16:50:00 CET

Rule State 6375 rules recommended for 1 network i

Host Data for Recommended Rules

Host Profile

- IP Addresses: 192.168.100.11 (sjo-i3-vc2.cisco.com)
- NetBIOS Name
- Device (Hops): FTD (0)
- MAC Addresses (TTL): 00:50:56:8D:65:92 (VMware, Inc.) (128)
- Host Type: Host
- Last Seen: 2025-12-30 16:20:14
- Current User

Indications of Compromise (0)

Operating Systems (2)

| Vendor | Product | Version | Source |
|------------------|------------|----------------------|-------------|
| Microsoft, Corp. | Windows 10 | 22h2 | User: admin |
| Microsoft | Windows | 10 20h2.x, 10 21h2.x | Firepower |

Edit Operating System if needed

Manually edited Operating System

Automatically detected Operating System

- Discovered Hosts can be reviewed from the FMC **Events & Logs > Hosts > Network Map**.
- Based on these information Recommended Rules are generated.
- Information can be manually modified.

Asset Discovery and Enrichment

Passive Detection

A non-intrusive monitoring method where the firewall observes traffic to identify assets and ports without using probes or interfering with data flow.

Active Detection

The firewall sends probes directly to devices to elicit responses, enabling the identification of operating systems, services, and vulnerabilities not visible via passive monitoring.

Network Discovery Policy – Passive Detection

Best Practices:

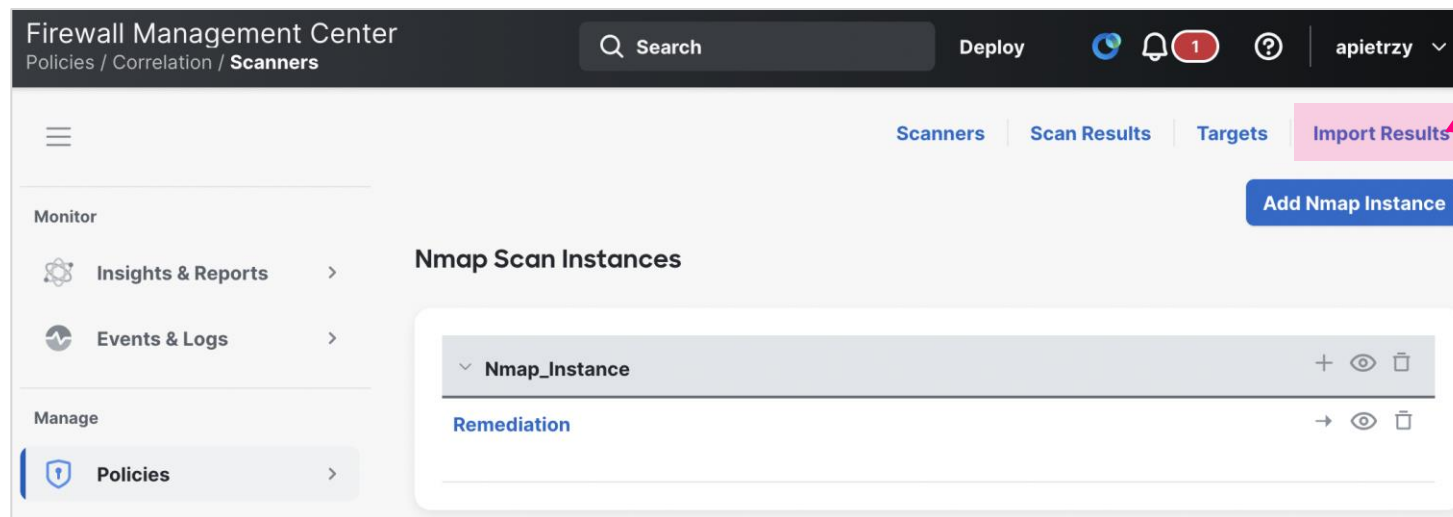
- Remove the default discovery rule, which includes the 0.0.0.0/0 and ::/0 subnets.
- Precisely define your company's internal network.
- The IPv4-Private-All-RFC1918 network object may be suitable initially if the networks in use are unknown or for identifying rogue networks.
- Exclude load balancers and NAT devices from discovery.

The screenshot displays the Cisco Firewall Management Center (FMC) interface. The top navigation bar includes the Cisco logo, the text 'Firewall Management Center', and the breadcrumb 'Policies / Advanced / Networks'. A search bar and a 'Deploy' button are also visible. The user profile 'apietryz' is shown in the top right. The main content area is titled 'Networks' and includes a sub-menu with 'Users' and 'Advanced'. A notification states 'Out of date on 1 targeted devices.' and there is an '+ Add Rule' button. A table lists the following policies:

| Networks | Zones | Source Port Exclusions | Destination Port Exclusions | Action |
|-------------------------------|-------|------------------------|-----------------------------|--------------------------------------|
| IPv4-Private-All-RFC1918 | any | none | none | Discover: Hosts, Users, Applications |
| Load_Balancers NAT_Devices | any | none | none | Exclude |

Nmap Scanning – Active Detection

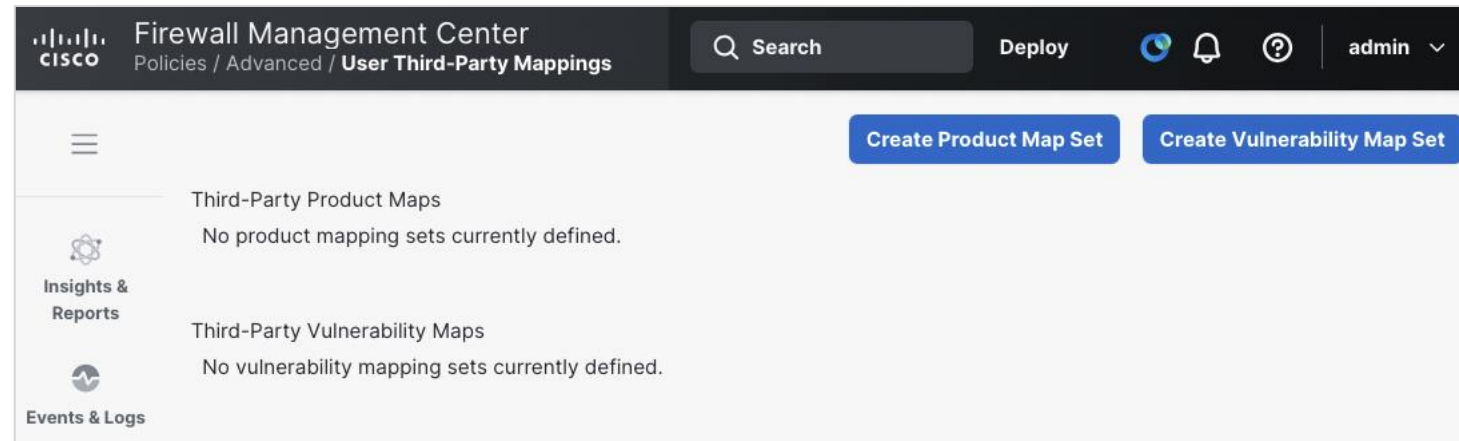
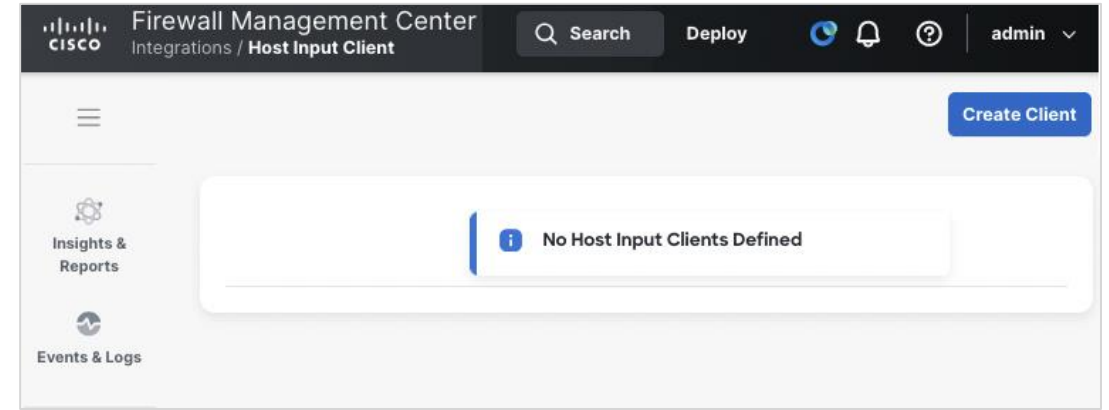
- You can use the embedded Nmap scanner within the FMC or FTD for network exploration.
- A strategic scanning plan is essential to ensure only necessary hosts and ports are targeted.
- **Best Practice:** Import Nmap scan results from a dedicated external scanner.



Import Scan Results

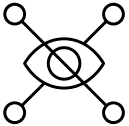
Enriching Network Map with Third-Party Data

- The **Host Input** feature allows you to import discovery data from third-party systems on your network.
- There are two methods for using the Host Input API to submit network map information: running the **nmimport** tool on the Management Center or using a **remote client**.
- To enable Cisco Recommended Rules, you must map the third-party vendor, product, and version to the corresponding Cisco product definitions.



The Importance of Precise Host Data

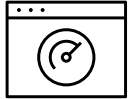
Accurate Asset Identification



Effective Vulnerability Mapping



Optimized Recommended Rules



Better Protection and Less False Positive Events



Variable Sets













- Variables are used in Snort rule headers to define specific traffic inspection criteria.
- The **\$HOME_NET** and **\$EXTERNAL_NET** variables are utilized in the majority of Cisco Talos rules.
 - **\$HOME_NET** represents the protected network and the primary target of threat actors.
 - **\$EXTERNAL_NET** represents the source or destination of threat-related traffic.
- **Best Practice:** Create custom Variable Sets rather than modifying the Default-Set.

New Variable Set

Name:

Description:

Add

| Variable Name | Type | Value | |
|-----------------------------|---------|------------------------|---|
| Customized Variables | | | |
| This category is empty | | | |
| Default Variables | | | |
| DNS_SERVERS | Network | HOME_NET |    |
| EXTERNAL_NET | Network | any |    |
| FILE_DATA_PORTS | Port | [HTTP_PORTS, 110, 143] |    |
| FTP_PORTS | Port | [2100, 3535, 21] |    |

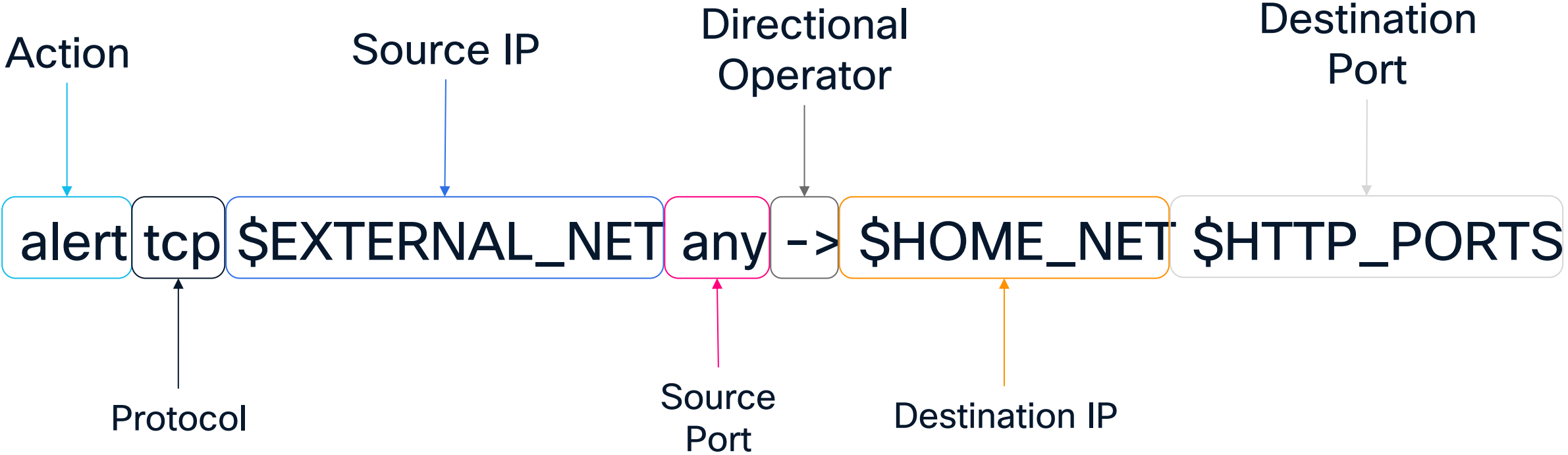
Cancel **Save**



SNORT Rule Example

```
alert tcp $EXTERNAL_NET any -> $HOME_NET 143 ( msg:"PROTOCOL-IMAP login brute force attempt";  
flow:to_server,established,no_stream; content:"LOGIN",fast_pattern,nocase; detection_filter:track by_dst,count 30,seconds 30;  
metadata:ruleset community; service:imap; reference:url,attack.mitre.org/techniques/T1110; classtype:suspicious-login; sid:2273;  
rev:12; )
```

Why Variable Sets Matters?

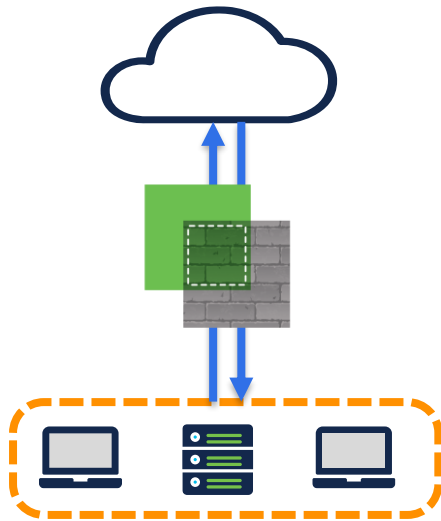


Variable Sets Recommendations

Internet Perimeter Deployment (North/South)

If your team requires a simple IPS deployment with a minimal number of alerts:

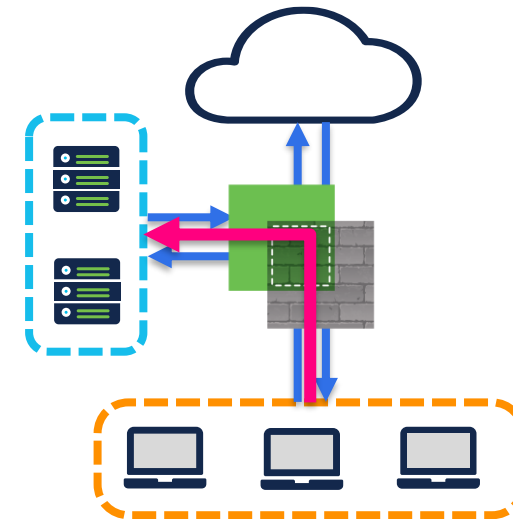
- **\$HOME_NET** specify the protected network
- **\$EXTERNAL_NET** configure as !HOME_NET



Internal IPS (East/West)

If your team is focused on threat hunting and is prepared to invest time in policy tuning

- **\$HOME_NET** specify the protected network
- **\$EXTERNAL_NET** configure as “any”.



Selecting Network Traffic for Inspection

- To inspect traffic using an intrusion policy, you must attach it to an **Access Control** rule.
- An intrusion policy applies to various traffic flows through **Allow** action within the Access Control policy.
- You can apply different IPS policies on the device giving you capabilities of tuning the level of security based on the use case.

Return to Access Control Policy Management

ACP

You have unsaved changes

Analyze Cancel Save

Packets → Prefilter Rules → Decryption → Security Intelligence → Identity → Access Control → More

Assigned to 1 device

Type to search Total 26 rules Add Category Add Rule

| Name | Action | Source | | Destination | | | Applications | Users |
|-------------------------------|---------|---------------|--------------------------------------|-------------|----------|-------|--------------|-------|
| | | Zones | Networks | Zones | Networks | Ports | | |
| ▼ Mandatory 26 rules (1 - 26) | | | | | | | | |
| 1 IPS rule test | → Allow | DMZ INSIDE | 172.168.0.0-net 192.168.100.0-net | OUTSIDE | Any | Any | Any | Any |

Rule 1: IPS rule test

Intrusion Policy

CL Intrusion Policy

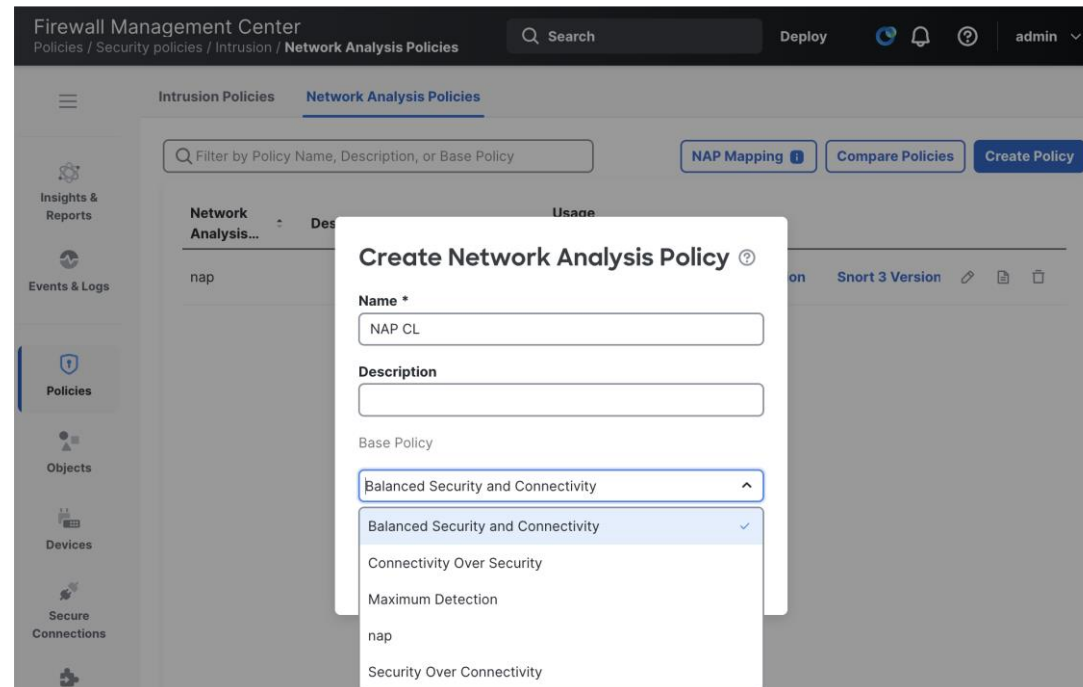
Variable Set

Variables

Cancel Confirm

Network Analysis Policy

- The Network Analysis Policy (NAP) controls advanced settings such as preprocessors (Snort 2) or inspectors (Snort 3).
- Inspectors decode and normalize network traffic in preparation for Snort inspection.
- The Network Analysis Policy should use **the same base policy** as your intrusion policy.
- **Caution:** Customizing the Network Analysis Policy is an advanced feature intended for expert users. Be aware that modifying a NAP can significantly impact traffic flow and system performance.



Access Control Policy – Advanced Settings

- In the **Network Analysis and Intrusion Policies** section under the **Advanced Settings** of the Access Control Policy:
 - Select the **Intrusion Policy used before Access Control rule is determined** and associate the relevant Variable Sets. This policy inspects traffic while the system performs application identification.
 - Select a user-created Network Analysis Policy (NAP).

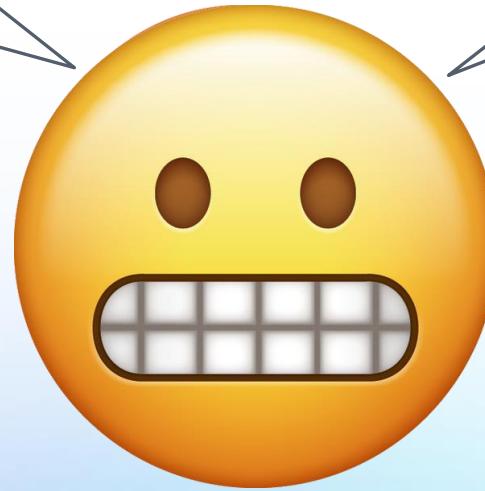
The screenshot shows the Cisco Firewall Management Center (FMC) interface. The main window displays the 'Policy Editor' for an Access Control Policy (ACP). The 'Advanced Settings' tab is active, and the 'Network Analysis and Intrusion Policies' section is highlighted in the left sidebar. A modal dialog is open, showing the configuration for these policies. The dialog includes the following fields and options:

- Intrusion Policy used before Access Control rule is determined:** A dropdown menu set to 'IPS policy - Windows'.
- Intrusion Policy Variable Set:** A dropdown menu set to 'Variables'.
- Network Analysis Rules:** A section with two options: 'No Custom Rules' (selected) and 'Network Analysis Policy List'.
- Default Network Analysis Policy:** A dropdown menu set to 'NAP CL'.

At the bottom of the dialog, there are three buttons: 'Revert to Defaults', 'Cancel', and 'OK'. The background interface shows a breadcrumb trail: 'Policies / Security policies / Policy Editor' and a navigation path: 'Packets → Prefilter Rules → Decryption → Security Intelligence → Identity → Access Control → Advanced Settings'. The top right corner shows a search bar, 'Deploy' button, and user information 'admin'.

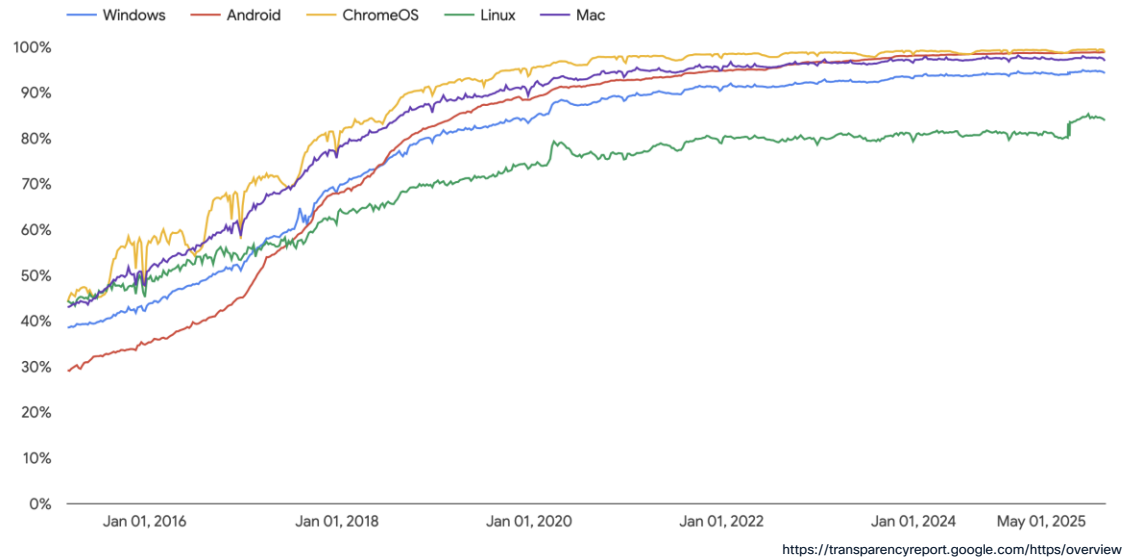
Am I missing something?

Encryption!!



Encryption Has Become the Internet Standard

Percentage of pages loaded over HTTPS in Chrome by platform



“In October 2026, we will change the default settings of Chrome to enable “[Always Use Secure Connections](#)”. This means Chrome will ask for the user’s permission before the first access to any public site without HTTPS.”

<https://security.googleblog.com/2025/10/https-by-default.html>

“Roughly **95%** of all web traffic is encrypted.”

Cisco Secure Network Analytics (formerly Stealthwatch) Data Sheet

“Over **70%** of attacks are expected to use encryption.”

Cisco Secure Network Analytics (formerly Stealthwatch) Data Sheet

How quickly does Snort stop inspecting connections?

Without decryption, the inspection stops after only 4 packets.

| Event Type | Action | Source IP | Destination IP | Destination Port / ICMP Code | TLS Client SNI | Inspected Packets | TLS Actual Action | EVE Process Name |
|--------------|---------|---------------|----------------|------------------------------|----------------|-------------------|-------------------|------------------|
| ↔ Connection | → Allow | 172.16.136.96 | 18.239.83.46 | 443 (https) / tcp | www.onet.pl | 4 | Do Not Decrypt | chromium browser |
| ↔ Connection | → Allow | 172.16.136.96 | 18.239.83.46 | 443 (https) / tcp | www.onet.pl | 4 | Do Not Decrypt | chromium browser |

... and the firewall looks at the TCP handshake the initial TLS message from the client:

| | Time | Source | SPORT | Destination | DPORT | Protocol | Length | Info |
|---|----------|---------------|-------|---------------|-------|----------|--------|--|
| 1 | 0.000000 | 172.16.136.96 | 49934 | 18.239.83.46 | 443 | TCP | 66 | 49934 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 |
| 2 | 0.000500 | 18.239.83.46 | 443 | 172.16.136.96 | 49934 | TCP | 66 | 443 → 49934 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 |
| 3 | 0.000547 | 172.16.136.96 | 49934 | 18.239.83.46 | 443 | TCP | 54 | 49934 → 443 [ACK] Seq=1 Ack=1 Win=2097408 Len=0 |
| 4 | 0.000780 | 172.16.136.96 | 49934 | 18.239.83.46 | 443 | TLSv1.3 | 585 | Client Hello (SNI=www.onet.pl) |

With decryption enabled, Snort continued inspection (column available in 7.7+) for 10s of packets.

| Event Type | Action | Source IP | Destination IP | Destination Port / ICMP Code | TLS Client SNI | Inspected Packets | TLS Actual Action | EVE Process Name |
|--------------|---------|---------------|----------------|------------------------------|----------------|-------------------|-------------------|------------------|
| ↔ Connection | → Allow | 172.16.136.96 | 18.239.83.82 | 443 (https) / tcp | www.onet.pl | 21 | Decrypt (Resign) | chromium browser |
| ↔ Connection | → Allow | 172.16.136.96 | 18.239.83.82 | 443 (https) / tcp | www.onet.pl | 76 | Decrypt (Resign) | chromium browser |

Without decryption, we are essentially blind after the initial handshake...

Inspection scope without TLS/QUIC decryption.
(4 packets ...)

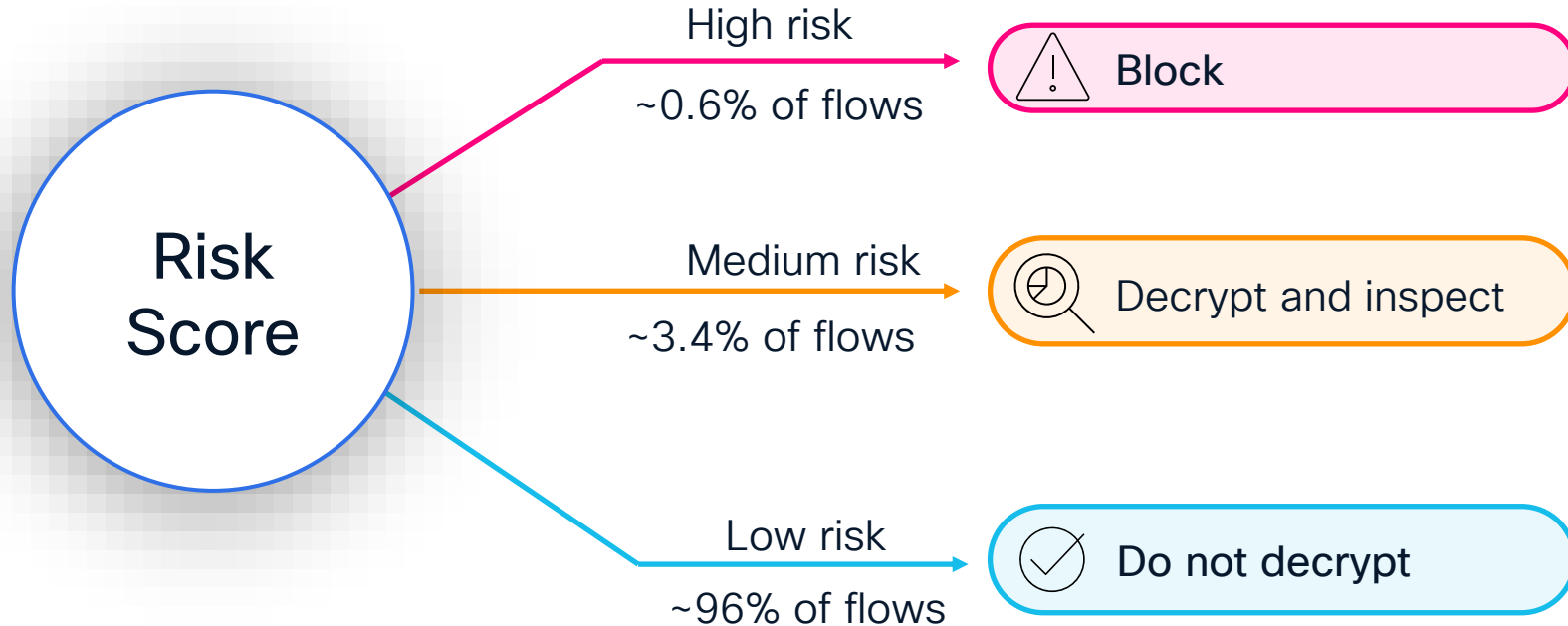
Wireshark packet capture (HTTPs connection to https://onet.pl)

| Time | Source | SPORT | Destination | DPORT | Protocol | Length | Info |
|------|----------|---------------|-------------|---------------|----------|--------|---|
| 1 | 0.000000 | 172.16.136.96 | 49934 | 18.239.83.46 | 443 | TCP | 66 49934 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM |
| 2 | 0.000500 | 18.239.83.46 | 443 | 172.16.136.96 | 49934 | TCP | 66 443 → 49934 [SYN, ACK] Seq=0 Ack=1 Win=65335 Len=0 MSS=1380 WS=64 SACK_PERM |
| 3 | 0.000547 | 172.16.136.96 | 49934 | 18.239.83.46 | 443 | TCP | 54 49934 → 443 [ACK] Seq=1 Ack=1 Win=2097408 Len=0 |
| 4 | 0.000780 | 172.16.136.96 | 49934 | 18.239.83.46 | 443 | TLV1.3 | 585 Client Hello (SNI=www.onet.pl) |
| 5 | 0.002136 | 18.239.83.46 | 443 | 172.16.136.96 | 49934 | TCP | 60 443 → 49934 [ACK] Seq=1 Ack=532 Win=64960 Len=0 |
| 6 | 0.142588 | 18.239.83.46 | 443 | 172.16.136.96 | 49934 | TLV1.3 | 1414 Server Hello, Change Cipher Spec, Application Data |
| 7 | 0.142588 | 18.239.83.46 | 443 | 172.16.136.96 | 49934 | TCP | 1414 443 → 49934 [ACK] Seq=1361 Ack=532 Win=64960 Len=1360 [TCP PDU reassembled in 8] |
| 8 | 0.142588 | 18.239.83.46 | 443 | 172.16.136.96 | 49934 | TLV1.3 | 800 Application Data, Application Data, Application Data |
| 9 | 0.142630 | 172.16.136.96 | 49934 | 18.239.83.46 | 443 | TCP | 54 49934 → 443 [ACK] Seq=532 Ack=3467 Win=2097408 Len=0 |
| 10 | 0.144132 | 172.16.136.96 | 49934 | 18.239.83.46 | 443 | TLV1.3 | 118 Change Cipher Spec, Application Data |
| 11 | 0.144272 | 172.16.136.96 | 49934 | 18.239.83.46 | 443 | TLV1.3 | 146 Application Data |
| 12 | 0.144402 | 172.16.136.96 | 49934 | 18.239.83.46 | 443 | TLV1.3 | 538 Application Data |
| 13 | 0.145355 | 18.239.83.46 | 443 | 172.16.136.96 | 49934 | TCP | 60 443 → 49934 [ACK] Seq=3467 Ack=596 Win=64896 Len=0 |
| 14 | 0.145433 | 18.239.83.46 | 443 | 172.16.136.96 | 49934 | TCP | 60 443 → 49934 [ACK] Seq=3467 Ack=688 Win=64832 Len=0 |
| 15 | 0.145433 | 18.239.83.46 | 443 | 172.16.136.96 | 49934 | TCP | 60 443 → 49934 [ACK] Seq=3467 Ack=1172 Win=64320 Len=0 |
| 16 | 0.156974 | 18.239.83.46 | 443 | 172.16.136.96 | 49934 | TLV1.3 | 304 Application Data, Application Data |
| 17 | 0.157080 | 172.16.136.96 | 49934 | 18.239.83.46 | 443 | TLV1.3 | 85 Application Data |
| 18 | 0.157585 | 18.239.83.46 | 443 | 172.16.136.96 | 49934 | TCP | 60 443 → 49934 [ACK] Seq=3717 Ack=1203 Win=64320 Len=0 |
| 19 | 0.166547 | 18.239.83.46 | 443 | 172.16.136.96 | 49934 | TCP | 1414 443 → 49934 [ACK] Seq=3717 Ack=1203 Win=64320 Len=1360 [TCP PDU reassembled in 33] |
| 20 | 0.166547 | 18.239.83.46 | 443 | 172.16.136.96 | 49934 | TCP | 1414 443 → 49934 [ACK] Seq=5077 Ack=1203 Win=64320 Len=1360 [TCP PDU reassembled in 33] |
| 21 | 0.166547 | 18.239.83.46 | 443 | 172.16.136.96 | 49934 | TCP | 1414 443 → 49934 [ACK] Seq=6437 Ack=1203 Win=64320 Len=1360 [TCP PDU reassembled in 33] |
| 22 | 0.166547 | 18.239.83.46 | 443 | 172.16.136.96 | 49934 | TCP | 1414 443 → 49934 [ACK] Seq=7797 Ack=1203 Win=64320 Len=1360 [TCP PDU reassembled in 33] |
| 23 | 0.166547 | 18.239.83.46 | 443 | 172.16.136.96 | 49934 | TCP | 1414 443 → 49934 [ACK] Seq=9157 Ack=1203 Win=64320 Len=1360 [TCP PDU reassembled in 33] |
| 24 | 0.166547 | 18.239.83.46 | 443 | 172.16.136.96 | 49934 | TCP | 1414 443 → 49934 [ACK] Seq=10517 Ack=1203 Win=64320 Len=1360 [TCP PDU reassembled in 33] |
| 25 | 0.166547 | 18.239.83.46 | 443 | 172.16.136.96 | 49934 | TCP | 222 443 → 49934 [PSH, ACK] Seq=11877 Ack=1203 Win=64320 Len=168 [TCP PDU reassembled in 33] |
| 26 | 0.166547 | 18.239.83.46 | 443 | 172.16.136.96 | 49934 | TCP | 1414 443 → 49934 [ACK] Seq=12045 Ack=1203 Win=64320 Len=1360 [TCP PDU reassembled in 33] |
| 27 | 0.166547 | 18.239.83.46 | 443 | 172.16.136.96 | 49934 | TCP | 1414 443 → 49934 [ACK] Seq=13405 Ack=1203 Win=64320 Len=1360 [TCP PDU reassembled in 33] |
| 28 | 0.166547 | 18.239.83.46 | 443 | 172.16.136.96 | 49934 | TCP | 1294 443 → 49934 [PSH, ACK] Seq=14765 Ack=1203 Win=64320 Len=1240 [TCP PDU reassembled in 33] |
| 29 | 0.166547 | 18.239.83.46 | 443 | 172.16.136.96 | 49934 | TCP | 1053 443 → 49934 [PSH, ACK] Seq=16005 Ack=1203 Win=64320 Len=999 [TCP PDU reassembled in 33] |
| 30 | 0.166594 | 172.16.136.96 | 49934 | 18.239.83.46 | 443 | TCP | 54 49934 → 443 [ACK] Seq=1203 Ack=17004 Win=2097408 Len=0 |
| 31 | 0.174644 | 18.239.83.46 | 443 | 172.16.136.96 | 49934 | TCP | 1414 443 → 49934 [ACK] Seq=17004 Ack=1203 Win=64320 Len=1360 [TCP PDU reassembled in 33] |
| 32 | 0.174644 | 18.239.83.46 | 443 | 172.16.136.96 | 49934 | TCP | 1414 443 → 49934 [ACK] Seq=18364 Ack=1203 Win=64320 Len=1360 [TCP PDU reassembled in 33] |
| 33 | 0.174644 | 18.239.83.46 | 443 | 172.16.136.96 | 49934 | TLV1.3 | 1414 Application Data |
| 34 | 0.174644 | 18.239.83.46 | 443 | 172.16.136.96 | 49934 | TCP | 1414 443 → 49934 [ACK] Seq=21884 Ack=1203 Win=64320 Len=1360 [TCP PDU reassembled in 48] |
| 35 | 0.174644 | 18.239.83.46 | 443 | 172.16.136.96 | 49934 | TCP | 1414 443 → 49934 [ACK] Seq=22444 Ack=1203 Win=64320 Len=1360 [TCP PDU reassembled in 48] |
| 36 | 0.174644 | 18.239.83.46 | 443 | 172.16.136.96 | 49934 | TCP | 382 443 → 49934 [PSH, ACK] Seq=23804 Ack=1203 Win=64320 Len=328 [TCP PDU reassembled in 48] |
| 37 | 0.174644 | 18.239.83.46 | 443 | 172.16.136.96 | 49934 | TCP | 1242 443 → 49934 [PSH, ACK] Seq=24132 Ack=1203 Win=64320 Len=1188 [TCP PDU reassembled in 48] |
| 38 | 0.174679 | 172.16.136.96 | 49934 | 18.239.83.46 | 443 | TCP | 54 49934 → 443 [ACK] Seq=1203 Ack=25320 Win=2097408 Len=0 |
| 39 | 0.175164 | 18.239.83.46 | 443 | 172.16.136.96 | 49934 | TCP | 1414 443 → 49934 [ACK] Seq=25320 Ack=1203 Win=64320 Len=1360 [TCP PDU reassembled in 48] |
| 40 | 0.175301 | 18.239.83.46 | 443 | 172.16.136.96 | 49934 | TCP | 1414 443 → 49934 [ACK] Seq=26680 Ack=1203 Win=64320 Len=1360 [TCP PDU reassembled in 48] |
| 41 | 0.175301 | 18.239.83.46 | 443 | 172.16.136.96 | 49934 | TCP | 898 443 → 49934 [PSH, ACK] Seq=28040 Ack=1203 Win=64320 Len=844 [TCP PDU reassembled in 48] |
| 42 | 0.175320 | 172.16.136.96 | 49934 | 18.239.83.46 | 443 | TCP | 54 49934 → 443 [ACK] Seq=1203 Ack=28884 Win=2097408 Len=0 |
| 43 | 0.183471 | 18.239.83.46 | 443 | 172.16.136.96 | 49934 | TCP | 1414 443 → 49934 [ACK] Seq=28884 Ack=1203 Win=64320 Len=1360 [TCP PDU reassembled in 48] |
| 44 | 0.183471 | 18.239.83.46 | 443 | 172.16.136.96 | 49934 | TCP | 1414 443 → 49934 [ACK] Seq=30244 Ack=1203 Win=64320 Len=1360 [TCP PDU reassembled in 48] |
| 45 | 0.183471 | 18.239.83.46 | 443 | 172.16.136.96 | 49934 | TCP | 1180 443 → 49934 [PSH, ACK] Seq=31604 Ack=1203 Win=64320 Len=1126 [TCP PDU reassembled in 48] |
| 46 | 0.183471 | 18.239.83.46 | 443 | 172.16.136.96 | 49934 | TCP | 1414 443 → 49934 [ACK] Seq=32730 Ack=1203 Win=64320 Len=1360 [TCP PDU reassembled in 48] |
| 47 | 0.183471 | 18.239.83.46 | 443 | 172.16.136.96 | 49934 | TCP | 1414 443 → 49934 [ACK] Seq=34090 Ack=1203 Win=64320 Len=1360 [TCP PDU reassembled in 48] |
| 48 | 0.183471 | 18.239.83.46 | 443 | 172.16.136.96 | 49934 | TLV1.3 | 1414 Application Data |
| 49 | 0.183471 | 18.239.83.46 | 443 | 172.16.136.96 | 49934 | TCP | 444 443 → 49934 [PSH, ACK] Seq=36810 Ack=1203 Win=64320 Len=390 [TCP PDU reassembled in 66] |
| 50 | 0.183471 | 18.239.83.46 | 443 | 172.16.136.96 | 49934 | TCP | 1242 443 → 49934 [PSH, ACK] Seq=37200 Ack=1203 Win=64320 Len=1188 [TCP PDU reassembled in 66] |
| 51 | 0.183471 | 18.239.83.46 | 443 | 172.16.136.96 | 49934 | TCP | 1414 443 → 49934 [ACK] Seq=38388 Ack=1203 Win=64320 Len=1360 [TCP PDU reassembled in 66] |
| 52 | 0.183514 | 172.16.136.96 | 49934 | 18.239.83.46 | 443 | TCP | 54 49934 → 443 [ACK] Seq=1203 Ack=39748 Win=2097408 Len=0 |
| 53 | 0.183541 | 18.239.83.46 | 443 | 172.16.136.96 | 49934 | TCP | 1414 443 → 49934 [ACK] Seq=39748 Ack=1203 Win=64320 Len=1360 [TCP PDU reassembled in 66] |
| 54 | 0.183541 | 18.239.83.46 | 443 | 172.16.136.96 | 49934 | TCP | 898 443 → 49934 [PSH, ACK] Seq=41108 Ack=1203 Win=64320 Len=844 [TCP PDU reassembled in 66] |
| 55 | 0.183551 | 172.16.136.96 | 49934 | 18.239.83.46 | 443 | TCP | 54 49934 → 443 [ACK] Seq=1203 Ack=41952 Win=2097408 Len=0 |
| 56 | 0.191339 | 18.239.83.46 | 443 | 172.16.136.96 | 49934 | TCP | 1414 443 → 49934 [ACK] Seq=41952 Ack=1203 Win=64320 Len=1360 [TCP PDU reassembled in 66] |
| 57 | 0.191339 | 18.239.83.46 | 443 | 172.16.136.96 | 49934 | TCP | 1414 443 → 49934 [ACK] Seq=43312 Ack=1203 Win=64320 Len=1360 [TCP PDU reassembled in 66] |
| 58 | 0.191362 | 172.16.136.96 | 49934 | 18.239.83.46 | 443 | TCP | 54 49934 → 443 [ACK] Seq=1203 Ack=44672 Win=2097408 Len=0 |
| 59 | 0.191418 | 18.239.83.46 | 443 | 172.16.136.96 | 49934 | TCP | 1414 443 → 49934 [ACK] Seq=44672 Ack=1203 Win=64320 Len=1360 [TCP PDU reassembled in 66] |
| 60 | 0.191418 | 18.239.83.46 | 443 | 172.16.136.96 | 49934 | TCP | 1414 443 → 49934 [ACK] Seq=46032 Ack=1203 Win=64320 Len=1360 [TCP PDU reassembled in 66] |

With decryption, Snort disengages after preempting all checks.
(as many packets as needed)

Cisco Encrypted Visibility Engine (EVE)

Encrypted Visibility Engine (EVE) provides visibility into encrypted traffic without decryption, using metadata and traffic patterns to detect and block malicious activity while preserving data privacy.



Intelligent Decryption Bypass utilizes EVE and Talos reputation to assess risk in real time, enabling low-risk encrypted connections to bypass the decryption process.

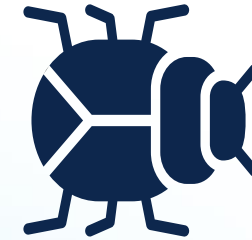
FTD
7.7+



[BRKSEC-3320 - Pig-in-the-middle -TLS Decryption and Encrypted Visibility Engine Deep Dive on Cisco Secure Firewall](#)

The IPS is deployed, rules are patched, encryption is handled, and the firewall is double-checked! Now it's time to relax.

Unless....



...a zero-day's about to crash the party!

The Unseen Threat - Zero-Day Attacks

No Warning

They strike before anyone knows there's a problem.

High Impact

Can lead to massive data breaches, significant financial losses, operational disruption, and even compromise critical infrastructure.

No Immediate Fix

Since the vulnerability is unknown, there's no official patch or security update to prevent exploitation.

SnortML

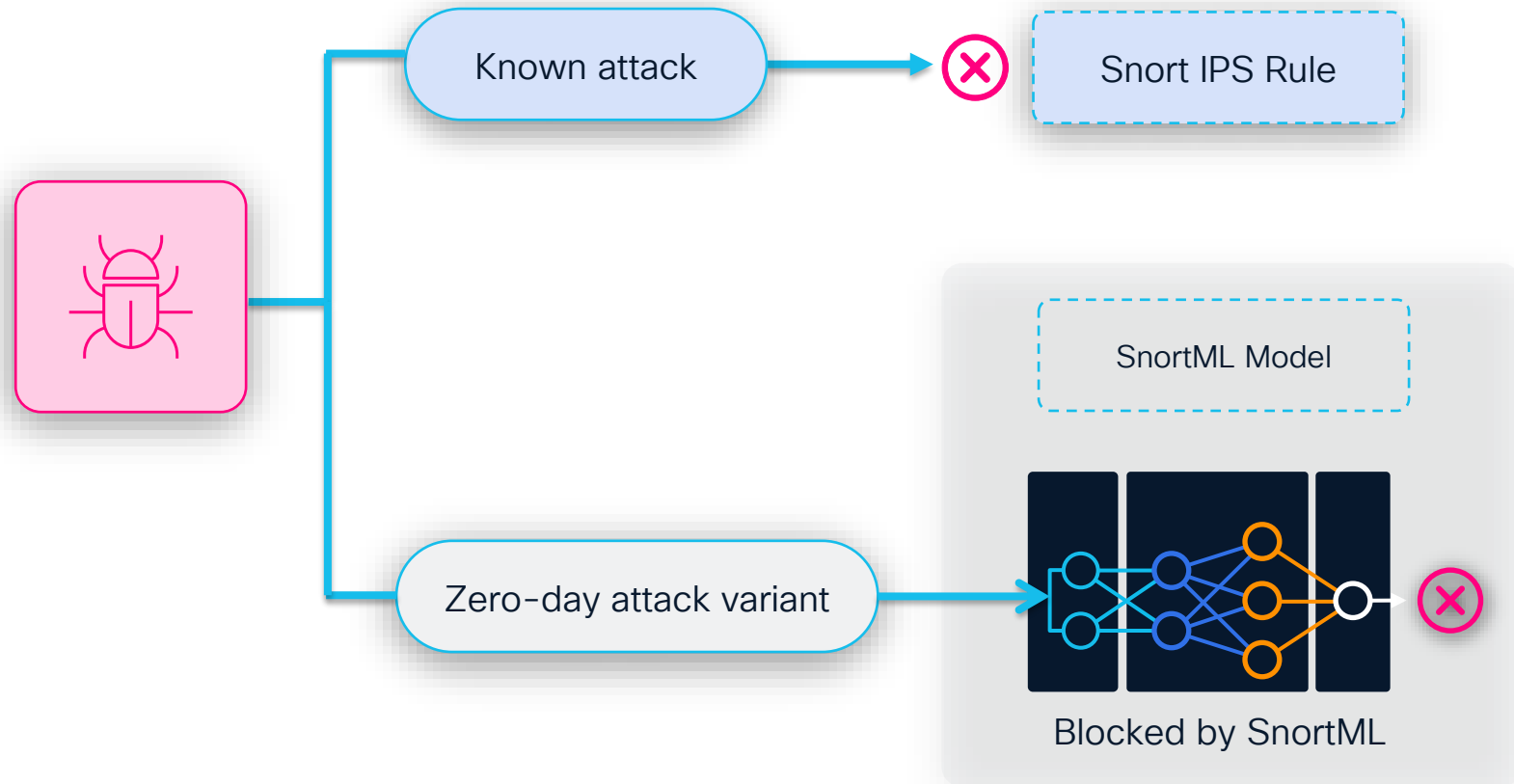


SnortML - Neural Network-Based Exploit Detector

SnortML is a machine learning-based detection engine designed to identify zero-day attacks; it functions in parallel with standard Snort IPS signatures

SnortML protects against:

- SQL Injection (7.6+)
- HTTP command injection



SnortML - Components

snort_ml_engine

The core management module responsible for the "intelligence" of the detection system.

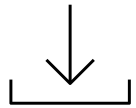
- Loads pre-trained machine learning models.
- Instantiates neural network classifiers.
- Makes classifiers available for inspection.

snort_ml_inspector

The operational module that interfaces directly with network data and acts on findings.

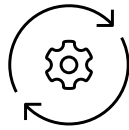
- Subscribes to Snort service inspector data.
- Passes data to classifiers for analysis.
- Triggers alerts or blocks malicious traffic.

Detection Workflow: From Data to Alert



1. Data Subscription

Inspector subscribes to HTTP data, through the publish/subscribe interface



2. Classification

Data is passed to the engine's neural Classifier for analysis



3. Probability Score

The engine calculates the probability of an exploit.



4. Action & Alert

Generates alerts or blocks the malicious traffic

Demo

Enabling the SnortML – Intrusion Policy

- To use SnortML the relevant Snort rule must be enabled.
- The SnortML IPS rules have the following characteristics:
 - **GID:** 411
 - **Rule message:** prepended with '(snort_ml)'
 - **Enabled** by default only in **Maximum Detection** IPS policy. For other base policies SnortML rule is disabled by default.

The screenshot displays the Firewall Management Center interface for configuring the 'CL Intrusion Policy'. The 'Rule Overrides' tab is active, showing a list of 107 items. A search filter for 'GID=411' is applied, resulting in 52,053 rules. The 'Rule Action' dropdown menu is open, and 'Block' is selected. The interface also shows the 'Base Policy' as 'Balanced Security and Connectivity' and the 'Mode' as 'Detection'.

| GID:SID | Rule Details | Rule Action | Set By | Assigned Groups |
|---------|--------------------|-------------|-------------|-----------------|
| 411:1 | (snort_ml) pote... | Block | Base Policy | Builtins |

Enabling the SnortML – NAP Policy

- The **snort_ml** inspector must be enabled in the Network Analysis Policy to utilize SnortML.
- This inspector is **enabled** by default in the "**Maximum Detection**" base policy but is disabled in all other base policy configurations.

The screenshot shows the Cisco Firewall Management Center interface. The left sidebar lists various policies, with 'snort_ml' selected and highlighted in a pink box. The main area displays the configuration for 'snort_ml'. An 'Override Configuration' dialog box is open, showing a JSON configuration where the 'enabled' field is set to 'true', highlighted in a pink box. The dialog also includes a 'JSON syntax ok' status and 'OK' and 'Cancel' buttons. Below the dialog, the 'Default Configuration' and 'Overridden Configuration' are shown, with the 'Overridden Configuration' showing 'enabled' set to 'false', also highlighted in a pink box.

```
1 {
2   "snort_ml": {
3     "type": "singleton",
4     "enabled": true,
5     "data": {
6       "uri_depth": -1,
7       "client_body_depth": 0
8     }
9   }
}
```

```
{
  "snort_ml": {
    "type": "singleton",
    "enabled": false,
    "data": {
      "uri_depth": -1,
      "client_body_depth": 0
    }
  }
}
```

SnortML

SnortML matches

| Time | Event Type | Action | Source IP | Destination IP | Source Port / ICMP Type | Destination Port / ICM... | Intrusion Message | Other Enrichment |
|-----------------------|------------|--------|--------------|----------------|-------------------------|---------------------------|--|-------------------------------------|
| > 2024-08-01 03:55:45 | Intrusion | Block | 10.0.104.100 | 10.0.105.100 | 16458 / tcp | 4430 / tcp | (snort_ml) potential threat found in HTTP parameters via Neural Net... | Rule Categories: Protocol: Builtins |
| > 2024-08-01 03:55:38 | Intrusion | Block | 10.0.104.100 | 10.0.105.100 | 16259 / tcp | 4430 / tcp | (snort_ml) potential threat found in HTTP parameters via Neural Net... | Rule Categories: Protocol: Builtins |
| > 2024-08-01 03:54:43 | Intrusion | Block | 10.0.104.100 | 10.0.105.100 | 14641 / tcp | 4430 / tcp | (snort_ml) potential threat found in HTTP parameters via Neural Net... | Rule Categories: Protocol: Builtins |
| > 2024-08-01 03:54:38 | Intrusion | Block | 10.0.104.100 | 10.0.105.100 | 14495 / tcp | 4430 / tcp | (snort_ml) potential threat found in HTTP parameters via Neural Net... | Rule Categories: Protocol: Builtins |



SnortML rule

URL metadata

| | |
|---------------|--|
| Snort ID | 411:1:1 |
| Snort Version | 3 |
| Snort Rule | <code>alert (gid:411; sid:1; rev:1; msg:"(snort_ml) potential threat found in HTTP parameters via Neural Network Based Exploit Detection"; metadata: policy max-detect-ips alert, rule-type preproc; classtype:unknown;)</code> |
| File | |
| URL | <code>/admin/user/action/index.php?n=guest&c=0&m=search&s=forum&wert=-1%25%22%20U...</code> |

Day-2 Operations



Snort Rule Updates

- Update Snort rules regularly to ensure the latest Cisco Talos CVE coverage.
- Use Recurring Rule Updates for timely and consistent updates.
- Use manual rule updates for air-gapped deployments.
- Snort rules are **NOT** released on a fixed schedule; instead, updates are provided as new threats and vulnerabilities are identified.

The screenshot displays the Firewall Management Center interface, specifically the 'Rule Updates' section. The breadcrumb navigation shows 'Administration / Upgrades & updates / Content Updates / Rule Updates'. The interface is divided into three tabs: 'VDB Updates', 'Rule Updates' (selected), and 'Geolocation Updates'. On the left, a navigation menu includes 'Insights & Reports', 'Objects', 'Devices', 'Secure Connections', 'Integrations', 'Troubleshooting', and 'Administration'. The main content area shows the current status: 'Running Snort Rule update version: 2025-12-10-001-vrt' and 'Running Lightweight Security Package (LSP) version: lsp-rel-20251210-1906'. Two buttons are visible: 'Delete All Local Rules' and 'Rule Update Log'. Below this, there are two sections: 'One-Time Rule Update/Rules Import' and 'Recurring Rule Update Imports'. The 'One-Time Rule Update/Rules Import' section has a 'Manual update' callout box. It includes a 'Source' dropdown with a 'Browse...' button, a 'Policy Deploy' checkbox, and an 'Import' button. The 'Recurring Rule Update Imports' section has an 'Automatic update' callout box. It includes a checkbox for 'Enable Recurring Rule Update Imports from the Support Site' (checked), an 'Import Frequency' dropdown set to 'Daily', a time selection (4:15 AM), a location dropdown set to 'Europe/Warsaw', a 'Policy Deploy' checkbox, and 'Cancel' and 'Save' buttons. Two red callout boxes with arrows point to the version information: 'Running Snort2 Snort Rule Package (SRU)' points to the top version, and 'Running Snort3 Lightweight Security Package (LSP)' points to the bottom version.

Where to find Snort3 Rule Updates?

- Lightweight Security Package (LSP) updates are available for download for each platform from software.cisco.com under the "Firepower Coverage and Content Updates" software type.
- Click on the package name to view additional details.

Software Download

Downloads Home / Security / Firewalls / Next-Generation Firewalls (NGFW) / Secure Firewall Threat Defense Virtual / Firepower Coverage and Content Updates- LSP

Search...

Expand All Collaps

All Release

SRU VDB GeoDB

SRU

SRU LSP VDB GeoDB

GeoDB

LSP

VDB

Details

Description : Lightweight Security Package 20251210-1906 For FTD Version 6.7+ or FMC 7.0+ **Do not untar.**

Release : LSP

Release Date : 11-Dec-2025

FileName : lsp-rel-20251210-1906.tar.xz.REL.tar

Size : 69.06 MB (72417280 bytes)

MD5 Checksum : ddda840ea36d5c96470fe7747f8fa0ab

SHA512 Checksum : edea39ddf0cd04fe7b2242f84a158999 ...

[New Rules](#) [Modified Rules](#) [LSP 20251210-1906](#) [Advisories](#)

New rules added in the LSP release

Modified rules in the LSP release

Defense Virtual

Related Links and Documentation

- No related links or documentation -

| Release Date | Size | |
|--------------|----------|--|
| 11-Dec-2025 | 69.06 MB | Download Add to Cart Share |
| 09-Dec-2025 | 68.45 MB | Download Add to Cart Share |

Update Recommended Rules Periodically

- Recommended Rules rely on dynamic data, such as Snort rules, vulnerabilities, and host attributes.
- Update Recommended Rules periodically to maintain their accuracy and effectiveness.
- **Best Practice:** Use scheduled tasks to automate the update process for recommendations.

Firewall Management Center
Administration / Advanced / Add Task

New Task

Job Type: Cisco Recommended Rules
(Cisco Recommended Rules must first be configured in the selected policies)

Schedule task to run: Once Recurring

Start On: January 5, 2026 Europe/Warsaw

Repeat Every: 1 Hours Days Weeks Months

Run At: 11:00 Pm

Repeat On: Sunday Monday Tuesday Wednesday Thursday Friday Saturday

Job Name: []

Policies: All Policies

polityka ips
IPS policy - Windows
Demo
CL Intrusion Policy

Comment: []

Email Status To: Not available. You must set up your mail relay host.

Cancel Save

Select Cisco Recommended Rules as a Job Type

Select time and frequency of the task

Select IPS Policies for update

Performance Analysis and Optimization

- The **Snort3 Rule Profiling** helps administrators optimize IPS policies by pinpointing rules causing performance issues without needing Snort 3 reload or restart.
- Identifies and analyzes the performance impact of individual IPS rules within Snort 3.
- Collects data on processing time for the top 100 IPS rules, highlighting those with the highest resource use.
- Saves profiling results in JSON format for review and historical analysis, supporting targeted rule management and tuning efforts to maintain optimal IPS performance

Profiling History

Rule Profiling
CPU Profiling

Select device for Rule Profiling

FTD

Stop
Start

Only Snort 3 devices running Version 7.6 and later are supported and listed here.

Rule Profiling Results - FTD - 28 seconds ago [Download Snapshot](#)

Start: 2026-01-26 18:09:34 CET
 Access Control Policy: ACP
 VDB: 416
 Snort Version: 3.9.3.1-61
Finish: 2026-01-26 18:12:17 CET
 Access Control Policy revision time: 2026-01-23 11:08:33 CET
 LSP: lsp-rel-20260121-2008
 Device Version: 10.0.0-140

Filter by % of Snort time Total 40

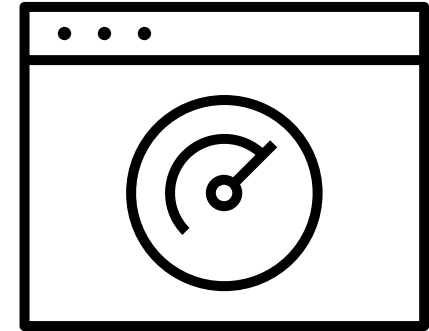
| Gid:Sid | Rule Description | % of Snort Time | Rev | Checks | Matches | Alerts | Time (µs) | Avg/Check | Avg/Match | Avg/Non-Match | Timeouts | Suspends |
|---------|---|-----------------|-----|--------|---------|--------|-----------|-----------|-----------|---------------|----------|----------|
| 1:23224 | EXPLOIT-KIT Redkit exploit kit landing page Requested - 8Digit.html | 0.00003% | 13 | 17 | 0 | 0 | 143 | 8 | 0 | 8 | 0 | 0 |
| 1:28585 | FILE-PDF Adobe Acrobat Reader OTF font head table size overflow atte... | 0.00001% | 8 | 16 | 0 | 0 | 49 | 3 | 0 | 3 | 0 | 0 |
| 1:47030 | MALWARE-CNC Win.Malware.Innaput variant outbound connection | 0.00001% | 1 | 37 | 0 | 0 | 44 | 1 | 0 | 1 | 0 | 0 |
| 1:37651 | MALWARE-TOOLS Win.Trojan.Downloader outbound connection attempt | 0.00001% | 3 | 6 | 0 | 0 | 42 | 7 | 0 | 7 | 0 | 0 |

Inspect Everything? Think Again

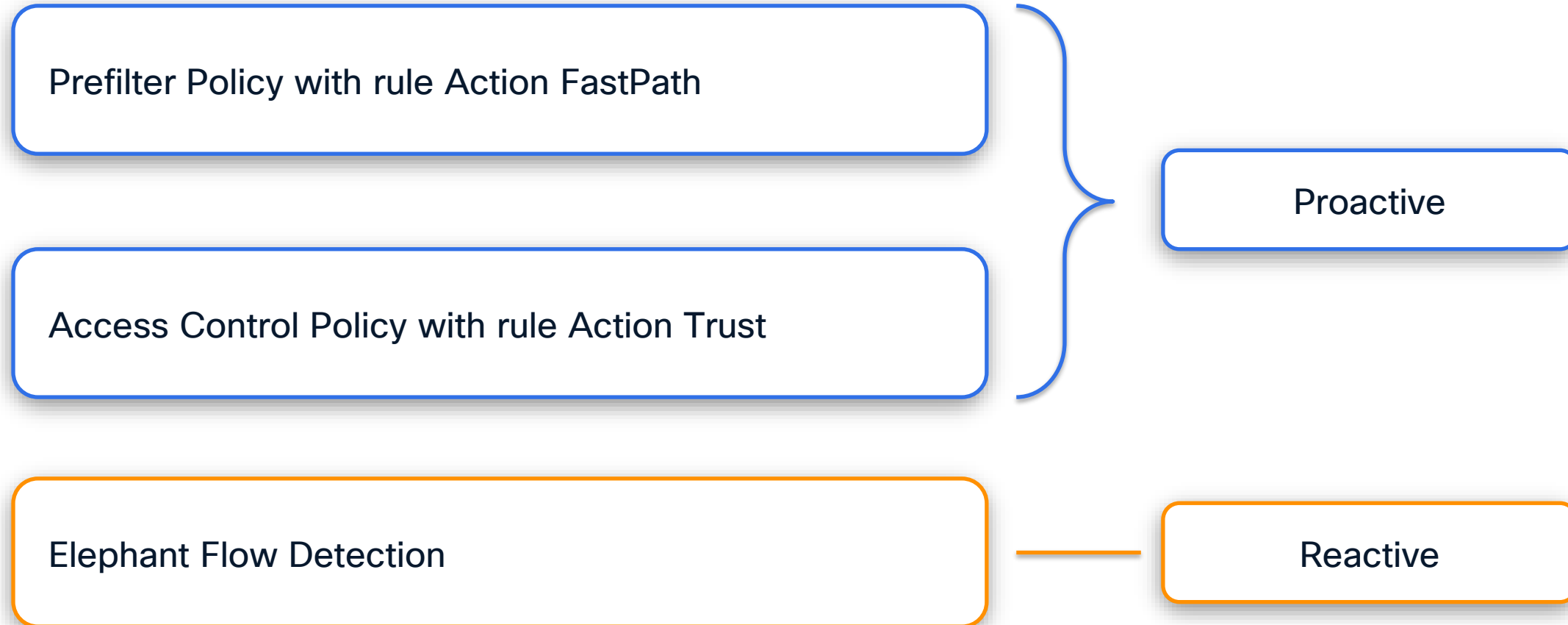
Enabling **Intrusion Prevention** inspection can impact system performance, depending on the traffic profile, enabled rules, and hardware resources. It is important to selectively inspect traffic rather than inspecting everything.

Traffic Candidates for IPS Inspection Exclusion:

- VPN traffic that is going through the device
- SQL traffic between trusted endpoints on the internal network
- Scanner traffic
- Voice/video
- Backups
- Management traffic (sftunnel) that traverses FTD



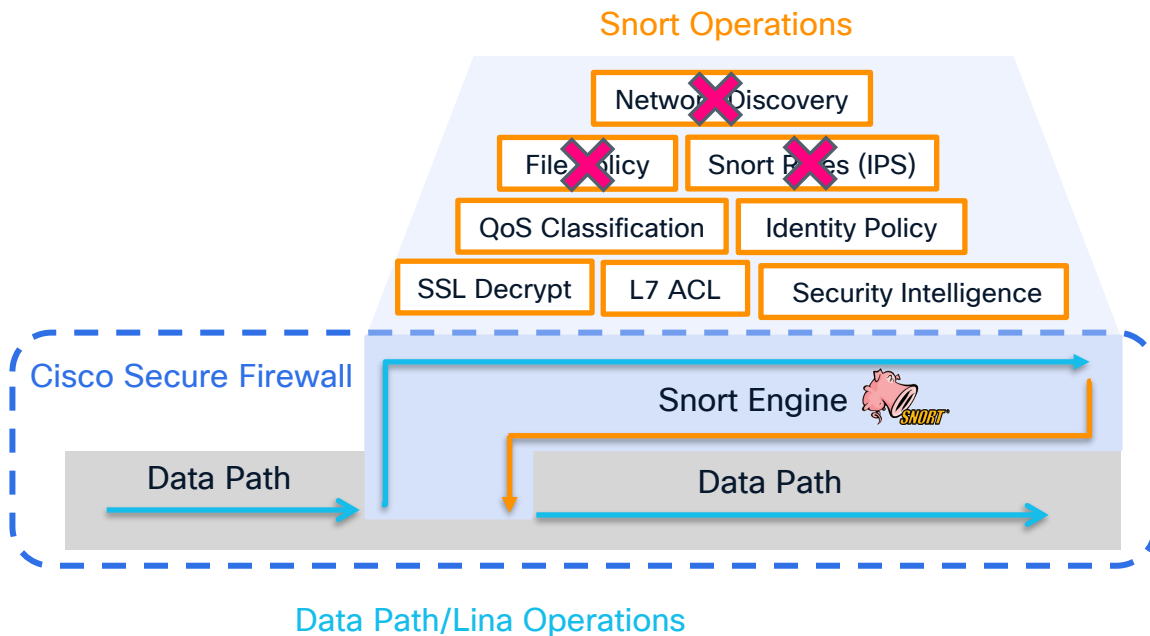
Ways to Exclude Traffic from IPS



Proactive Exclusion – Trust vs FastPath

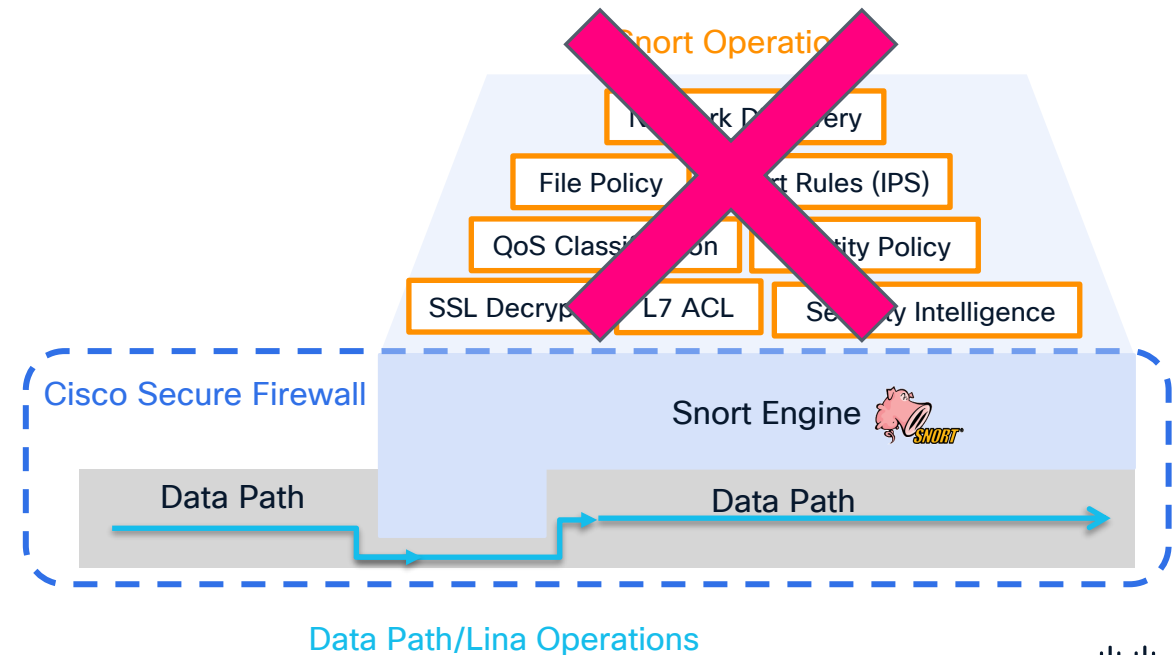
Trust Action

- The Trust action allows traffic to pass without deep inspection (IPS and File) or Network Discovery.
- Other Snort Operation will be still performed.



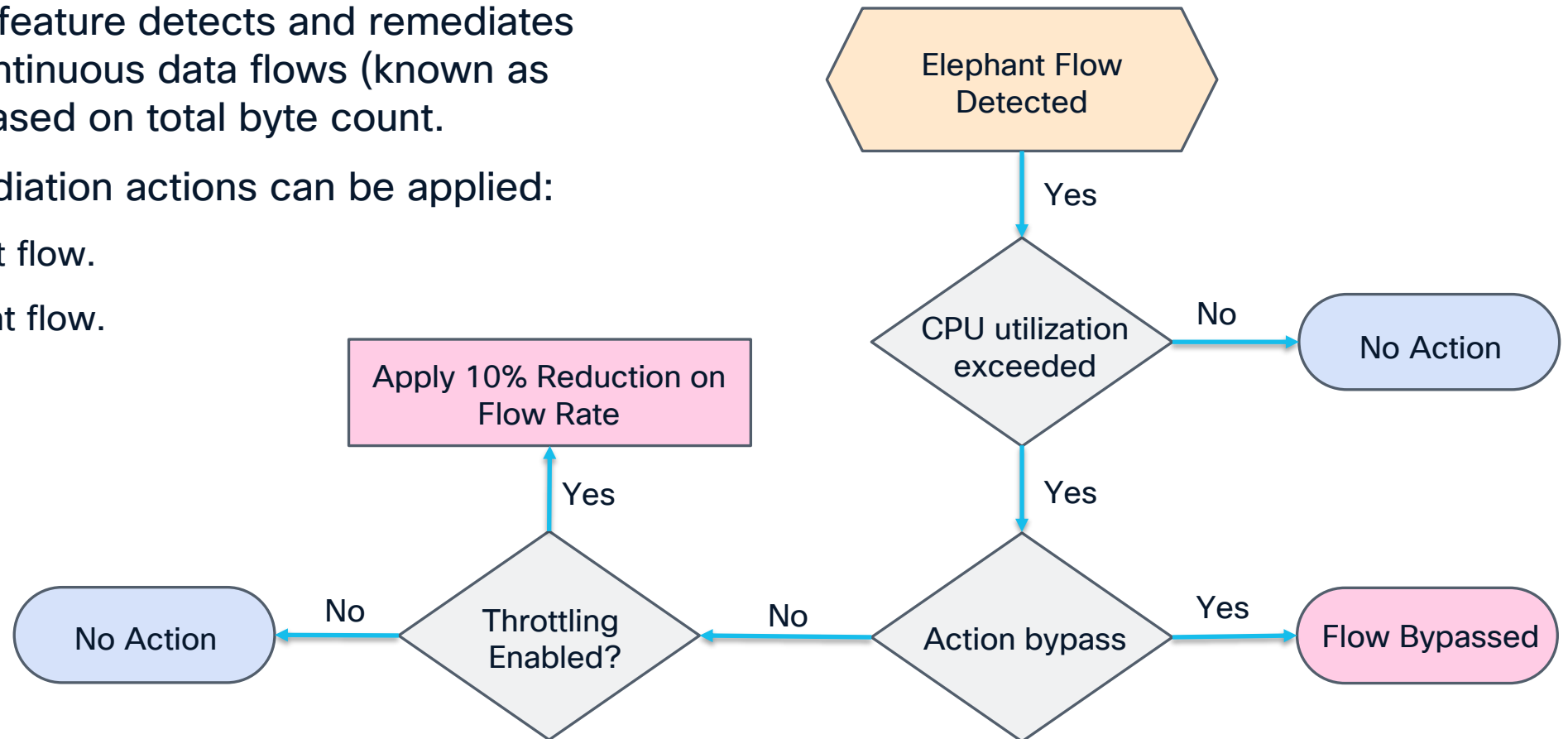
FastPath Action

- Fastpathing traffic in the prefilter stage bypasses all further inspection and handling.
- No traffic sent to Snort.



Elephant Flow Detection

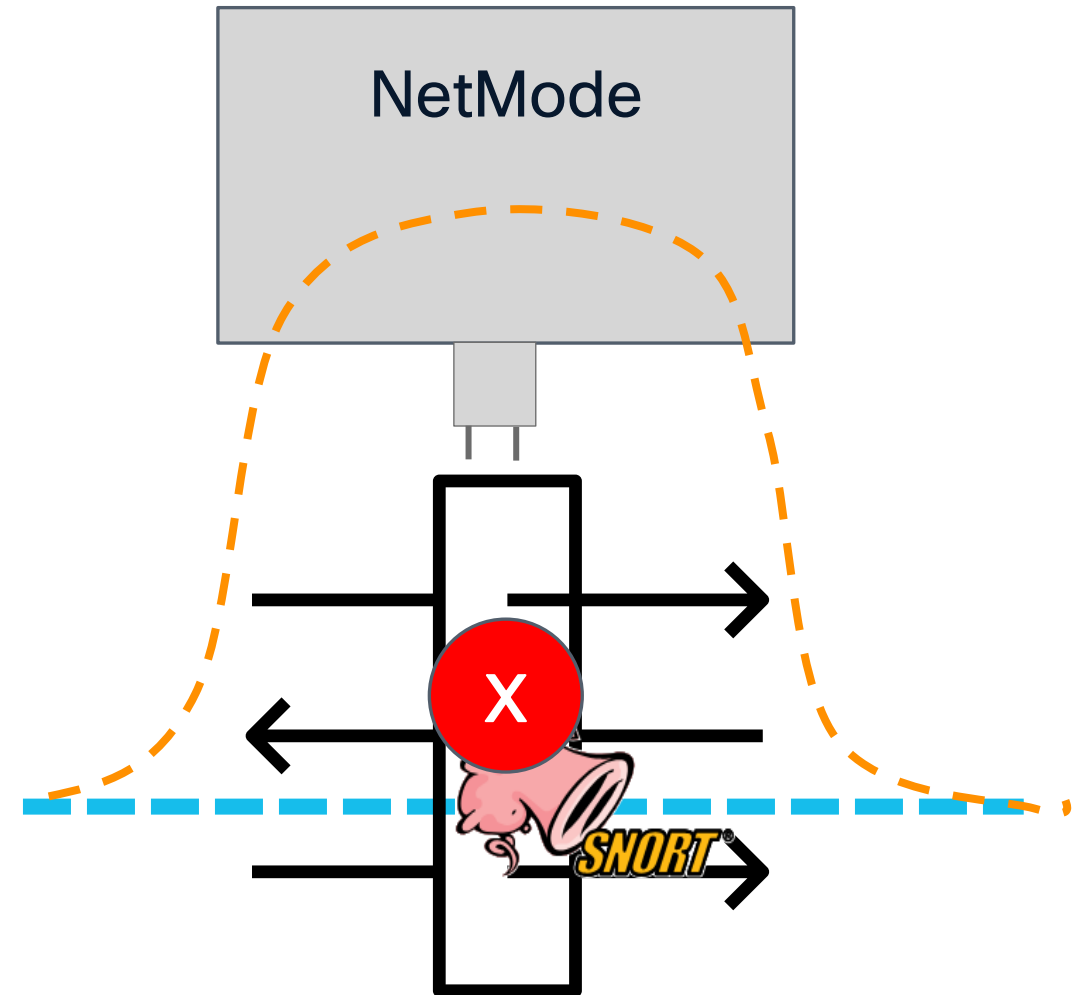
- The **Elephant Flow** feature detects and remediates extremely large, continuous data flows (known as "elephant flows") based on total byte count.
- The following remediation actions can be applied:
 - **Bypass** the elephant flow.
 - **Throttle** the elephant flow.



Hardware Bypass

- **Hardware Bypass** ensures that traffic continues to flow between an inline interface pair during a catastrophic outage. This feature is used to maintain network connectivity in the event of software or hardware failures.
- Hardware Bypass can be **triggered** in the following scenarios:
 - Firewall Threat Defense crash
 - Firewall Threat Defense reboot
 - Security Module reboot
 - Chassis crash
 - Chassis reboot
 - Manual trigger
 - Chassis power loss
 - Security Module power loss

Available on 2100, 3100, 4100, 4200, 9300 and 6100



Software Bypass

Snort Fail Open

- In inline **fail-open** deployments, traffic is passed uninspected through the software bridge when Snort is busy or down.
- Once Snort recovers, it performs a mid-session pickup on existing traffic.
- This feature is exclusively available for **inline pairs**.

Add Inline Set ?

General **Advanced**

Tap Mode:

Propagate Link State:

Strict TCP Enforcement:

Snort Fail Open: Busy Down

i Enabling Snort Fail Open might allow traffic unrestricted.

Cancel **OK**

Snort Bypass – CLI

- Enable Snort bypass via the FTD CLI using this command: **configure snort snort-bypass-enable**
- Once enabled, packets will bypass Snort and will no longer be sent for processing.
- **Caution:** Use it only under TAC supervision.

```
> configure snort snort-bypass-enable
```

```
-----
Executing this command will circumvent the firewall, allowing traffic that would typically be blocked.
Please be cautioned: this command is not intended for customer use.
Enable behaviour is not persistent across [reboots /restarts /reloads]
These utilities are designed solely for troubleshooting purposes.
-----
```

```
Do you still want to continue?
Please enter 'YES' or 'NO': YES
```

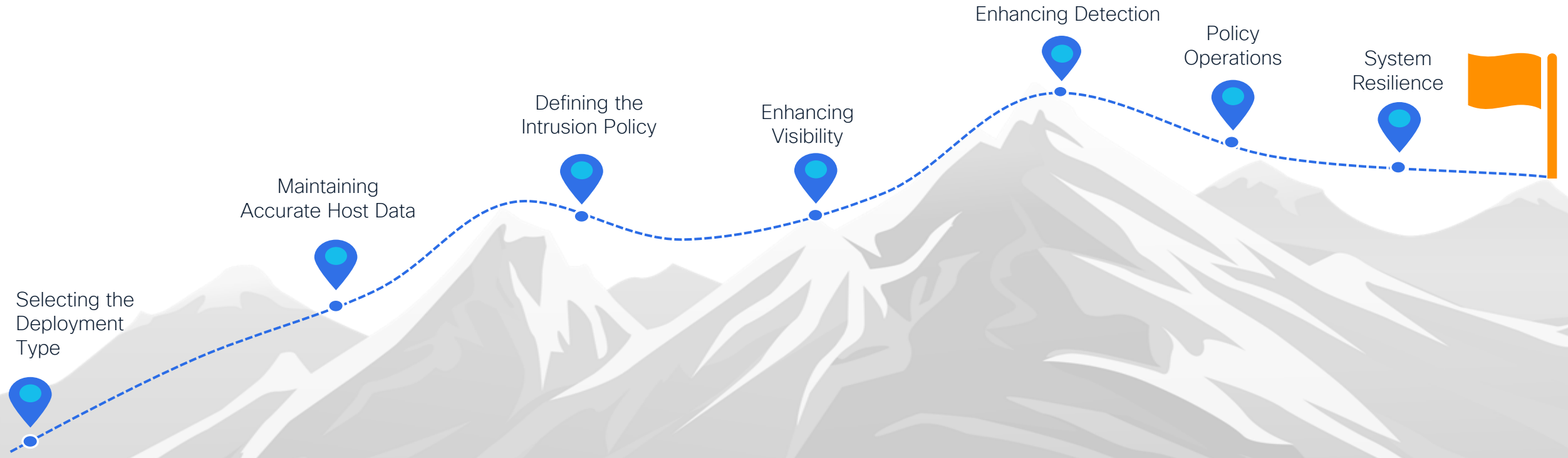
```
Enable command executed successfully .
```

```
If enabled inadvertently, use the following command to disable:
>configure snort3 snort-bypass-disable
```

```
Current state: ENABLED
```

Summary

IPS Deployment Journey



“

**Every unchecked setting today is a
risk waiting for tomorrow**

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)

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: apietry@cisco.com

Thank you

CISCO Live !

