

Securing Networks with
Cisco FTD

Chapter 10

Security Intelligence

Mohsen Kheradmand

Security intelligence

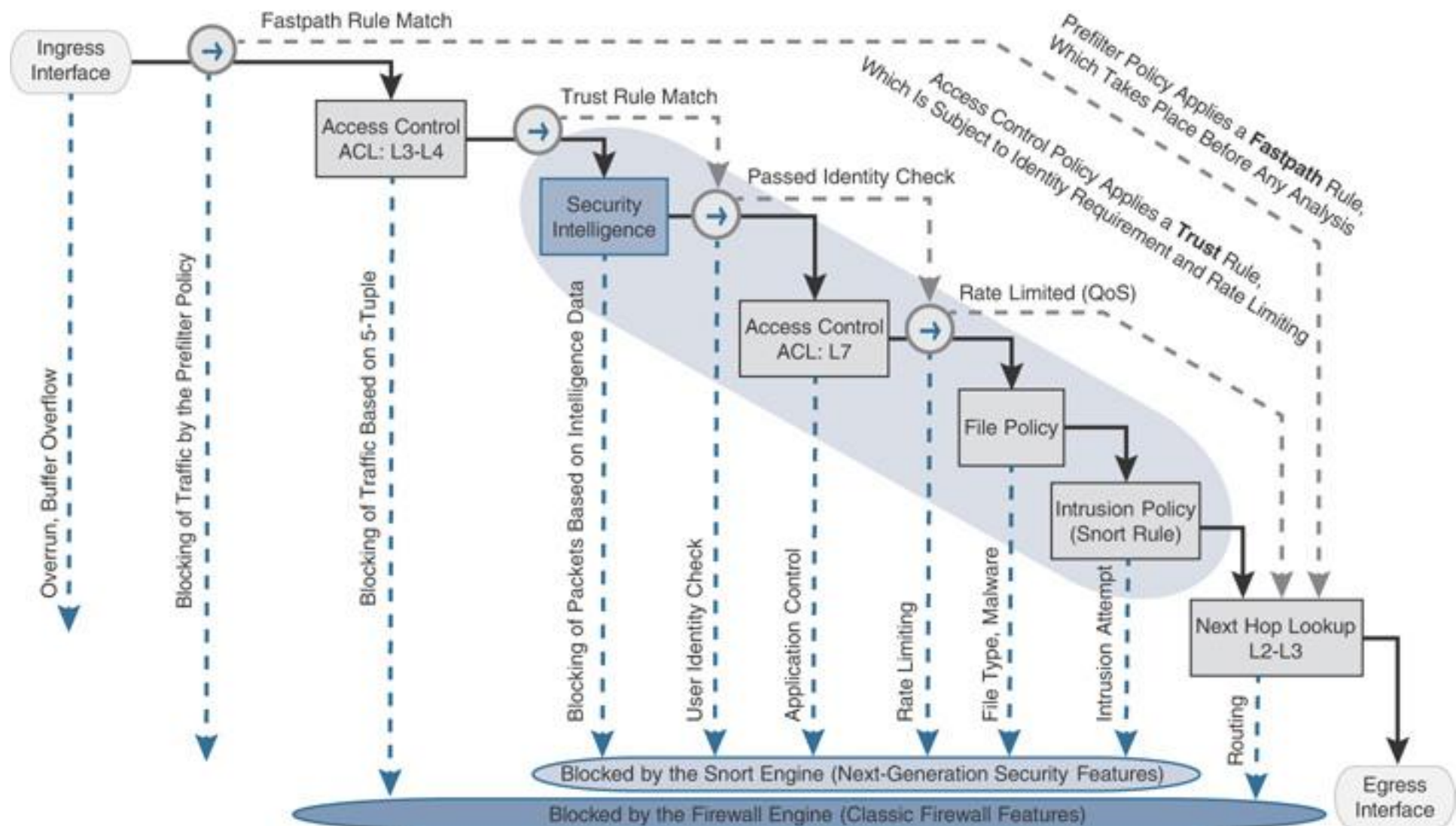
- Security Intelligence blocks a suspicious address dynamically without manual modification to the access control policy.
- It can block a packet before the packet goes through a deeper inspection process in the threat defense.
- It can optimize CPU and memory utilization, which can improve overall system performance.
- Secure Firewall also use the intelligence data to block malicious URLs and domain names

❑ This chapter focuses on blocking IP addresses. The next chapter discusses how to block malicious domain names

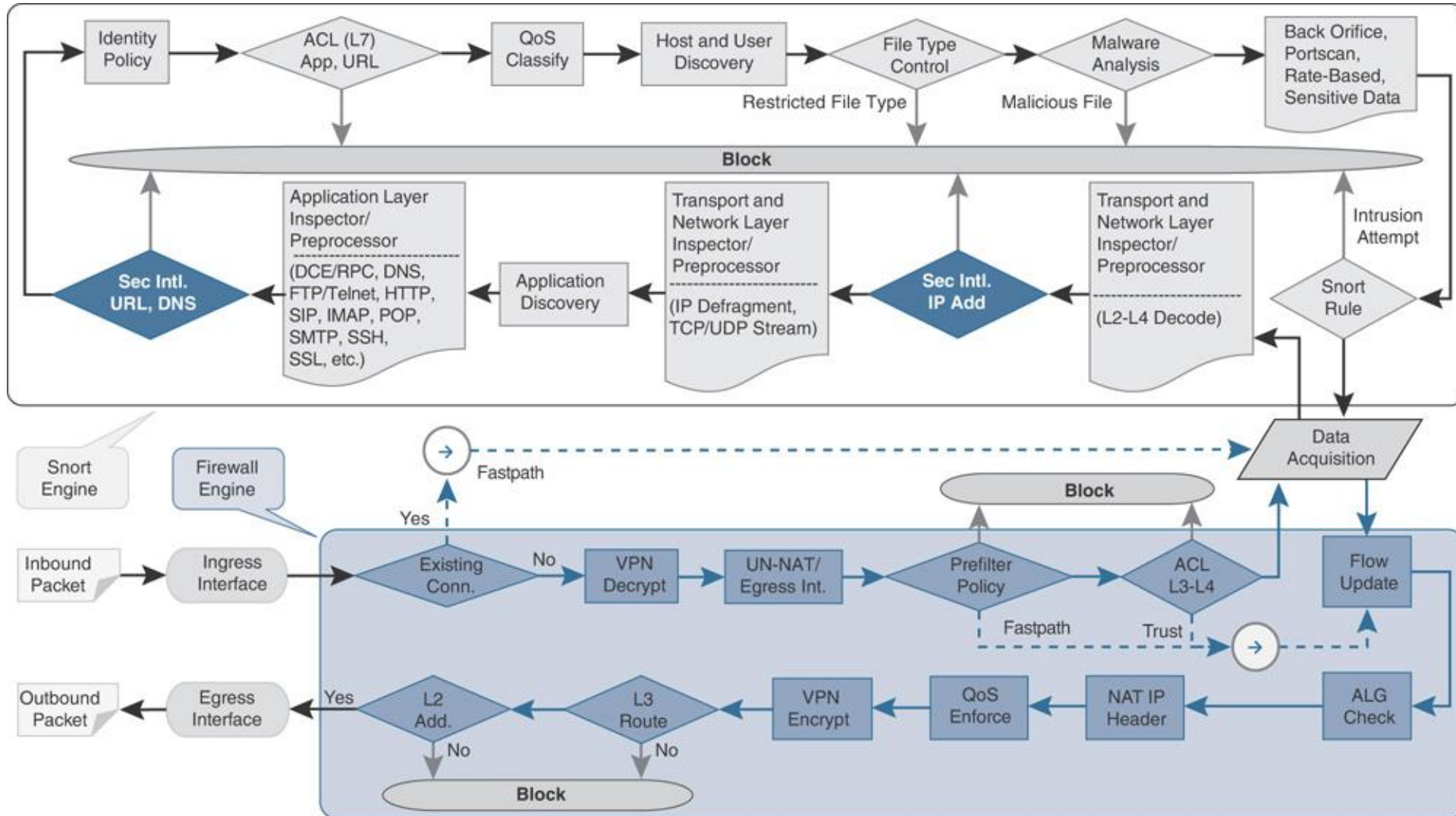
3 ways to input a suspicious address into the FTD :

- **Feed** : Automatic blocking of an address using the **Cisco intelligence feed** (provided by Cisco Talos team)
- **List** : Manual blocking of addresses in bulk using a **custom intelligence list** (a text file provided by administrator)
- **Context Menu** : Instant blocking of an address using the **context menu of the connection event page**

➤ Potential Reasons for a Packet Drop by a Threat Defense (Highlighting Security Intelligence)

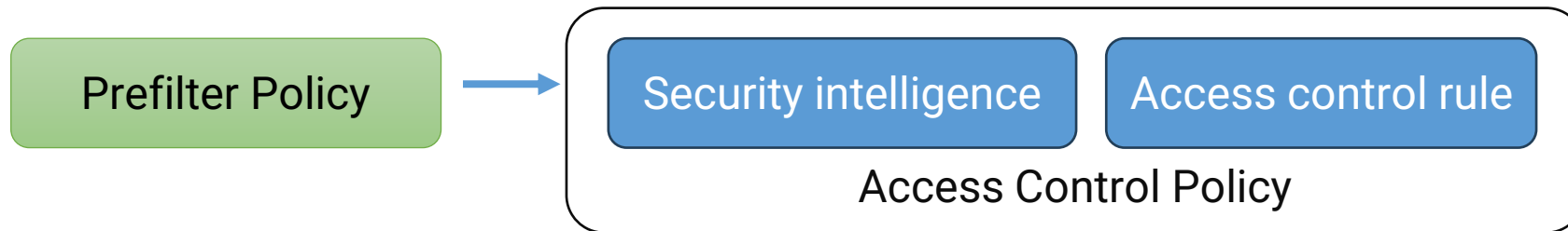


➤ Processing of Packets by Various Components of Security Engines (Highlighting Security Intelligence)



➤ Difference between ACP , Prefilter and Security intelligence

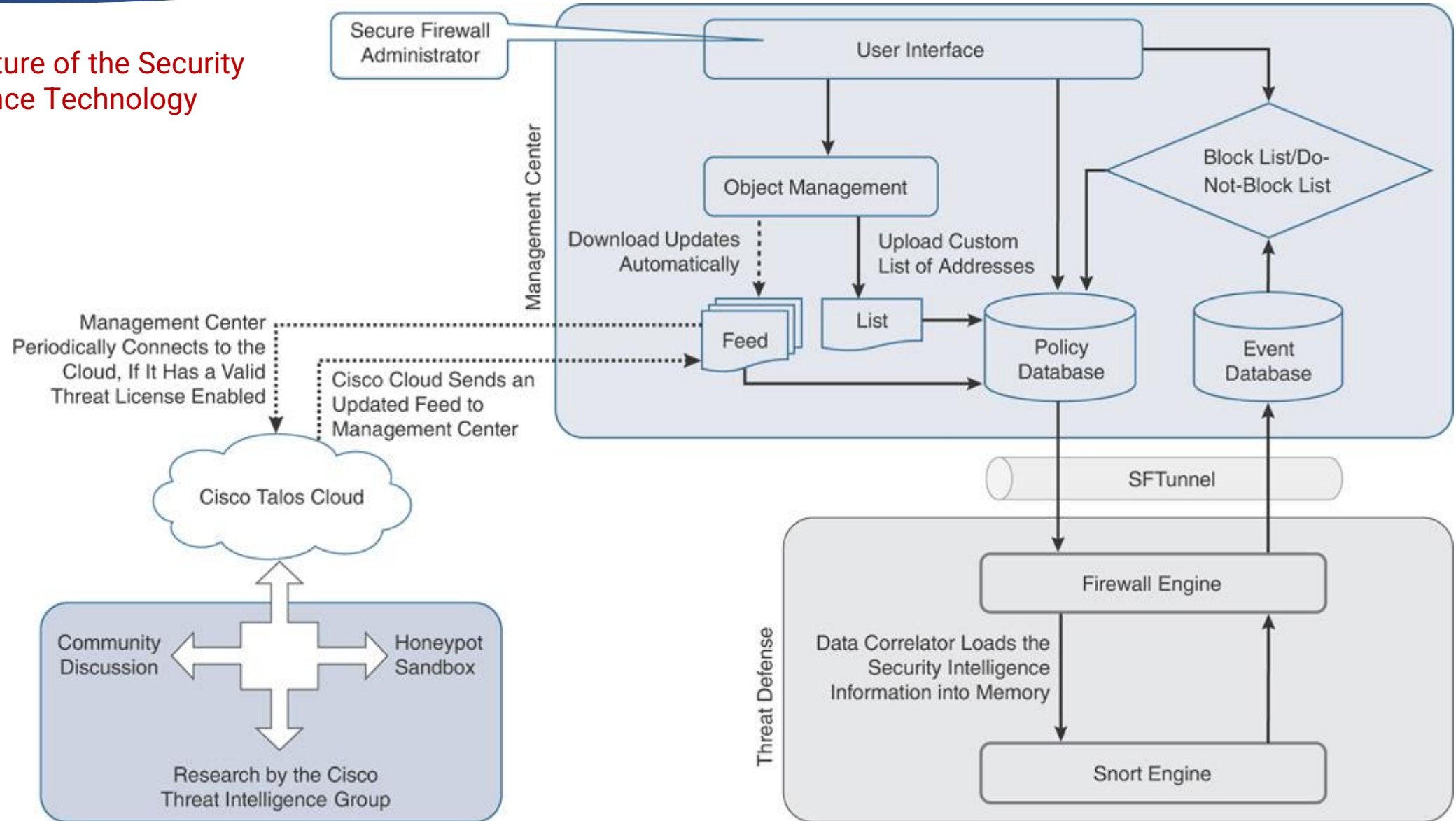
- Prefilter is processed before Access Control Policy (if action is Fastpath no ACP is processed)
- Security Intelligence is part of ACP with highest priority



- Traffic with no bad reputation and isn't part of a blacklist is processed by other access control modules and rules

Security Intelligence

- Architecture of the Security Intelligence Technology



Before you enable security intelligence:

- ✓ To block traffic based on 5 tuple (source-destination IP , port and protocol) , **better to use Prefilter** (better performance)
- ✓ To test a new feed for its impact , set the action of Security Intelligence **from Block to Monitor-only mode**
- ✓ You can use the Security Intelligence technology that you obtain from third-party security advisories (later in this chapter)
- ✓ Enable the health module for the Security Intelligence to generate alerts if the system fails to download or load into memory



Security Intelligence prerequisites

- 1) Security Intelligence requires **a threat license**

FMC

NGFW Device Summary

OverviewAnalysisPolicies**Devices**ObjectsAMPIntelligenceDeploy

admin

Threat Defense

Cisco Firepower Threat Defense for VMware

DeviceRoutingInterfacesInline SetsDHCP

General

Name:

Threat Defense

Transfer Packets:

Yes

Mode:

Routed

Compliance Mode:

None

TLS Crypto Acceleration:

Disabled

License

Performance Tier :

FTDv5 - Tiered (Core 4 / 8 GB)

Base:

Yes

Export-Controlled Features:

Yes

Malware:

Yes

Threat:

Yes

URL Filtering:

Yes

AnyConnect Apex:

Yes

AnyConnect Plus:

Yes

AnyConnect VPN Only:

No

Security Intelligence prerequisites

- 2) Updates the management center with the latest intelligence feed over the Internet
 - Objects > Object Management > Security Intelligence > Network Lists and Feeds and click the Update Feeds button

 Firepower Management Center

Objects / Object Management

OverviewAnalysisPoliciesDevicesObjectsAMPIntelligence

Geolocation

Interface

Key Chain

Network

> PKI

Policy List

Port

> Prefix List

Route Map

> Security Intelligence

DNS Lists and Feeds

Network Lists and Feeds

URL Lists and Feeds

Network Lists and Feeds

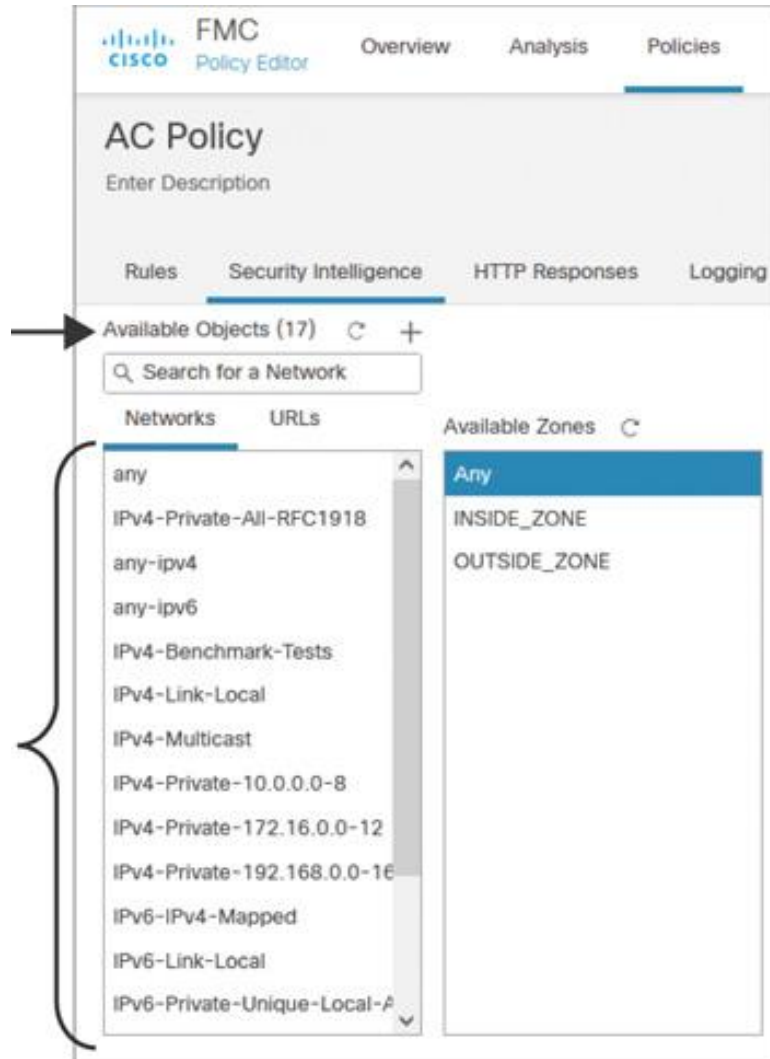
Update Feeds

Add Network Lists and Feeds

Network lists and feeds helps you quickly filter traffic by collecting IP address and address blocks. Its used in access control policies to manage the BL part of Security Intelligence.

Name	Type
Cisco-Intelligence-Feed	Feed
Cisco-TID-Feed Last Updated: 2024-12-11 23:28:13	Feed
Global-Block-List	List
Global-Do-Not-Block-List	List

Security Intelligence prerequisites



Default Network Objects (out of the box)



Intelligence-Based Network Objects
(after the Feeds Update)

Automatic Blocking Using Intelligence Feed

➤ Security Intelligence based on IP addresses

- Policies > Access Control
 - Click pencil to edit
 - Select Security Intelligence
- Networks : select a category
- Optionally : select by Zones
- Add selected to :
 - ☐ Block list
 - ☐ Do-not-Block list

The screenshot displays the Cisco FMC Policy Editor interface. At the top, the 'Policies' tab is selected. Below the navigation bar, the 'AC Policy' configuration page is shown. The 'Security Intelligence' sub-tab is active, indicated by a black arrow pointing to it. The interface includes a search bar for 'Available Objects (39)' and a list of categories: Networks, URLs, and Available Zones. The 'Networks' list is expanded, showing various threat categories like Attackers, Banking_fraud, Bogon, Bots, CnC, Cryptomining, Dga, Exploitkit, High_risk, loc, Link_sharing, Malicious, and Malware. The 'Available Zones' list shows 'Any', 'INSIDE_ZONE', and 'OUTSIDE_ZONE'. On the right, there are sections for 'DNS Policy' (set to Default DNS Policy), 'Do-Not-Block List (2)', and 'Block List (24)'. The 'Block List' section shows a list of selected items, including 'Attackers (Any Zone)', 'Banking_fraud (Any Zone)', 'Bogon (Any Zone)', 'Bots (Any Zone)', 'CnC (Any Zone)', 'Cryptomining (Any Zone)', 'Dga (Any Zone)', 'Exploitkit (Any Zone)', 'High_risk (Any Zone)', 'loc (Any Zone)', and 'Link_sharing (Any Zone)'. Buttons for 'Add to Do-Not-Block List' and 'Add to Block List' are visible. At the top right, there are buttons for 'Show Warnings', 'Analyze Hit Counts', 'Save', and 'Cancel'. A red notification bar at the top indicates 'You have unsaved changes'.

Automatic Blocking Using Intelligence Feed

➤ URL-based Security Intelligence

URLs Subtab

The screenshot displays the Cisco FMC Policy Editor interface. The top navigation bar includes tabs for Overview, Analysis, Policies, Devices, Objects, AMP, Intelligence, Deploy, and a search icon. The 'Policies' tab is active, showing the 'AC Policy' configuration. The 'Security Intelligence' subtab is selected, with the 'URLs' subtab highlighted. The 'Available Objects' list on the left contains 24 items, including URL Attackers, URL Banking_fraud, URL Bogon, URL Bots, URL CnC, URL Cryptomining, URL Dga, URL Exploitkit, URL High_risk, URL Ioc, URL Link_sharing, URL Malicious, and URL Malware. The 'Available Zones' list in the center includes Any, INSIDE_ZONE, and OUTSIDE_ZONE. The 'Do-Not-Block List' and 'Block List' on the right show the configured rules for blocking URLs. The 'Block List' contains 46 items, including Global Block List for URL, URL Attackers (Any Zone), URL Banking_fraud (Any Zone), URL Bogon (Any Zone), URL Bots (Any Zone), URL CnC (Any Zone), URL Cryptomining (Any Zone), URL Dga (Any Zone), URL Exploitkit (Any Zone), URL High_risk (Any Zone), URL Ioc (Any Zone), and URL Link_sharing (Any Zone).

Automatic Blocking Using Intelligence Feed

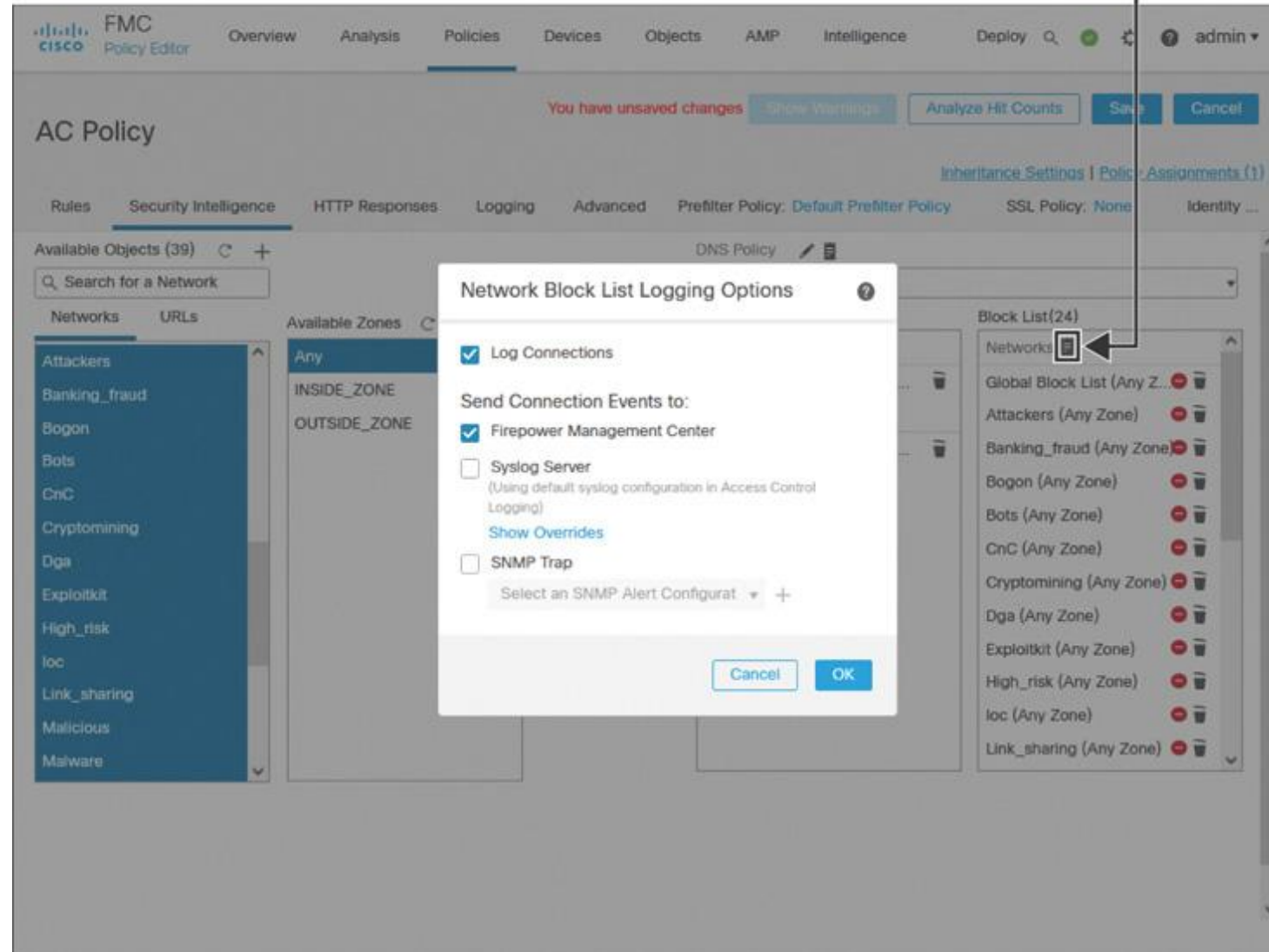
➤ Logging

- Under the Block List field, click the logging icon
- Check Log connections
- Check Log connections
- Check Firepower management center
- Optionally send logs to Syslog or SNMP server

When the configuration is complete, click **Save**

Finally, navigate to **Deploy > Deployment**

Logging Setting for Block List



Verifying the Action of Intelligence Feed

To see the action of Security Intelligence on live traffic

➤ Analysis > Connections > Security Intelligence Events

The screenshot displays the Cisco Firepower Management Center (FMC) interface. At the top, the navigation bar includes the Cisco logo, the title "Firepower Management Center", and the breadcrumb "Analysis / Connections / Security Intelligence Events". The main navigation tabs are "Overview", "Analysis" (which is selected), "Policies", and "Devices".

The "Security Intelligence Events" page is shown, with a sub-header "(switch workflow)". Below this, it states "No Search Constraints (Edit Search)". There are two tabs: "Security Intelligence with Application Details" (selected) and "Table View of Security Intelligence Events".

A "Jump to..." search bar is present. Below it, a table header is visible with columns: a checkbox, a dropdown arrow, "First Packet", "Last Packet", "Action", "Reason", "Initiator IP", "Initiator Country", and "Responder IP".

A dropdown menu is open from the "Analysis" tab, showing the following options: "Context Explorer", "Unified Events", a section header "Connections", "Events", "Security Intelligence Events" (highlighted with a mouse cursor), a section header "Intrusions", "Events", "Reviewed Events", and "Clipboard".

Verifying the Action of Intelligence Feed

You can also logs an associated connection event for connection attempt

➤ Analysis > Connections > Events



The screenshot shows the Cisco FMC Events page. The top navigation bar includes links for Overview, Analysis, Policies, Devices, Objects, AMP, Intelligence, Deploy, and a search icon. The main heading is "Connection Events" with a sub-link "(switch workflow)". Below this, there are links for "Bookmark This Page", "Reporting", "Dashboard", "View Bookmarks", and "Search". A "Predefined Searches" dropdown menu is also present. The page displays a table of connection events with the following columns: Action, Reason, Initiator IP, Responder IP, Security Intelligence Category, Source Port / ICMP Type, Destination Port / ICMP Code, and Access Control Rule. Two events are listed: one blocked due to IP Block and another allowed. The Security Intelligence Category for the blocked event is Phishing.

	↓ First Packet x	Action x	Reason x	Initiator IP x	Responder IP x	Security Intelligence Category x	Source Port / ICMP Type x	Destination Port / ICMP Code x	Access Control Rule x
▼	2021-10-03 08:37:26	Block	IP Block	192.168.1.2	23.94.7.9	Phishing	60390 / tcp	80 (http) / tcp	
▼	2021-10-03 08:11:11	Allow		192.168.1.2	23.94.7.9		60388 / tcp	80 (http) / tcp	Default Action

The Same Connection Gets Blocked When the Security Intelligence Is Enabled

Add to Do-Not-Block List

- Sometimes Cisco block an address and you disagree with that
- So on the Connection Events page right click the desired address and select :
 Add IP to DO-Not-Block list
- However , traffic to and from that address is still subject to any subsequent inspection

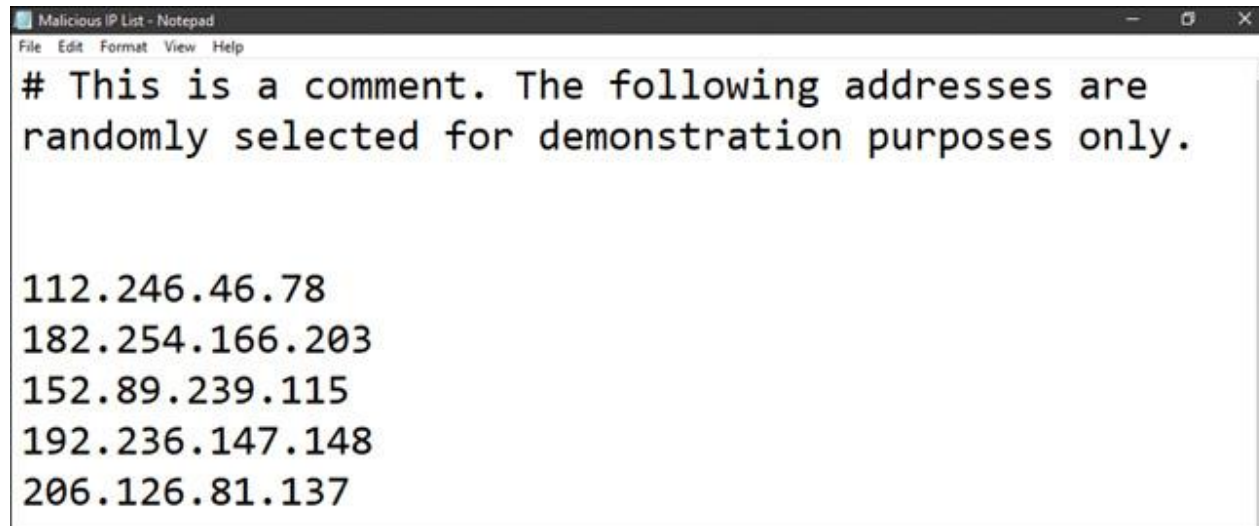
The screenshot shows the Cisco FMC Events interface. The top navigation bar includes links for Overview, Analysis, Policies, Devices, Objects, AMP, Intelligence, and Deploy. The main content area is titled 'Connection Events' and shows a table of events. A right-click context menu is open over a row with the Initiator IP 192.168.1.2, which has been blocked. The menu options include 'Open in New Window', 'Exclude', 'Whois', 'View Host Profile', 'Add IP to Block List', 'Add IP to Do-Not-Block List' (highlighted), 'Open in Context Explorer', 'AlienVault IP', 'IBM X-Force Exchange IP', and 'Looking Glass IP'.

	↓ First Packet x	Action x	Reason x	Initiator IP x	Responder IP x	Security Intelligence Category x	Source Port / ICMP Type x	Destination Port / ICMP Code x	Access Control Rule x
▼	2021-10-03 08:37:26	Block	IP Block	192.168.1.2	23.94.7.9	Destination	80 / http	80 / http	Default Action
▼	2021-10-03 08:11:11	Allow		192.168.1.2	23.94.7.9				

Manual Blocking Using Custom List

- To block a custom list of IP addresses

1) Create a txt file and Write or copy the potential malicious addresses into that



```
File Edit Format View Help
# This is a comment. The following addresses are
randomly selected for demonstration purposes only.

112.246.46.78
182.254.166.203
152.89.239.115
192.236.147.148
206.126.81.137
```

Manual Blocking Using Custom List

2) Object > Object Management

> Security intelligence

> Network Lists and Feeds

> Add Network Lists and Feeds

- Enter a name
- Select List from Type
- Click browse and select TXT file

The screenshot displays the Cisco FMC Object Management interface. The left sidebar shows the navigation menu with 'Security Intelligence' expanded. The main content area is titled 'Network Lists and Feeds' and contains a table of existing lists. A modal window is open for creating a new list.

Name	Type
Cisco-Intelligence-Feed Last Updated: 2021-	
Cisco-TID-Feed Last Updated: 2021-	
Global-Block-List	
Global-Do-Not-Block	

Security Intelligence for Network List / Feed

Name: Custom-List

Type: List

Upload List: C:\fakepath\Malicious IP List.txt Browse... Upload

Upload File: C:\fakepath\Malicious IP List.txt

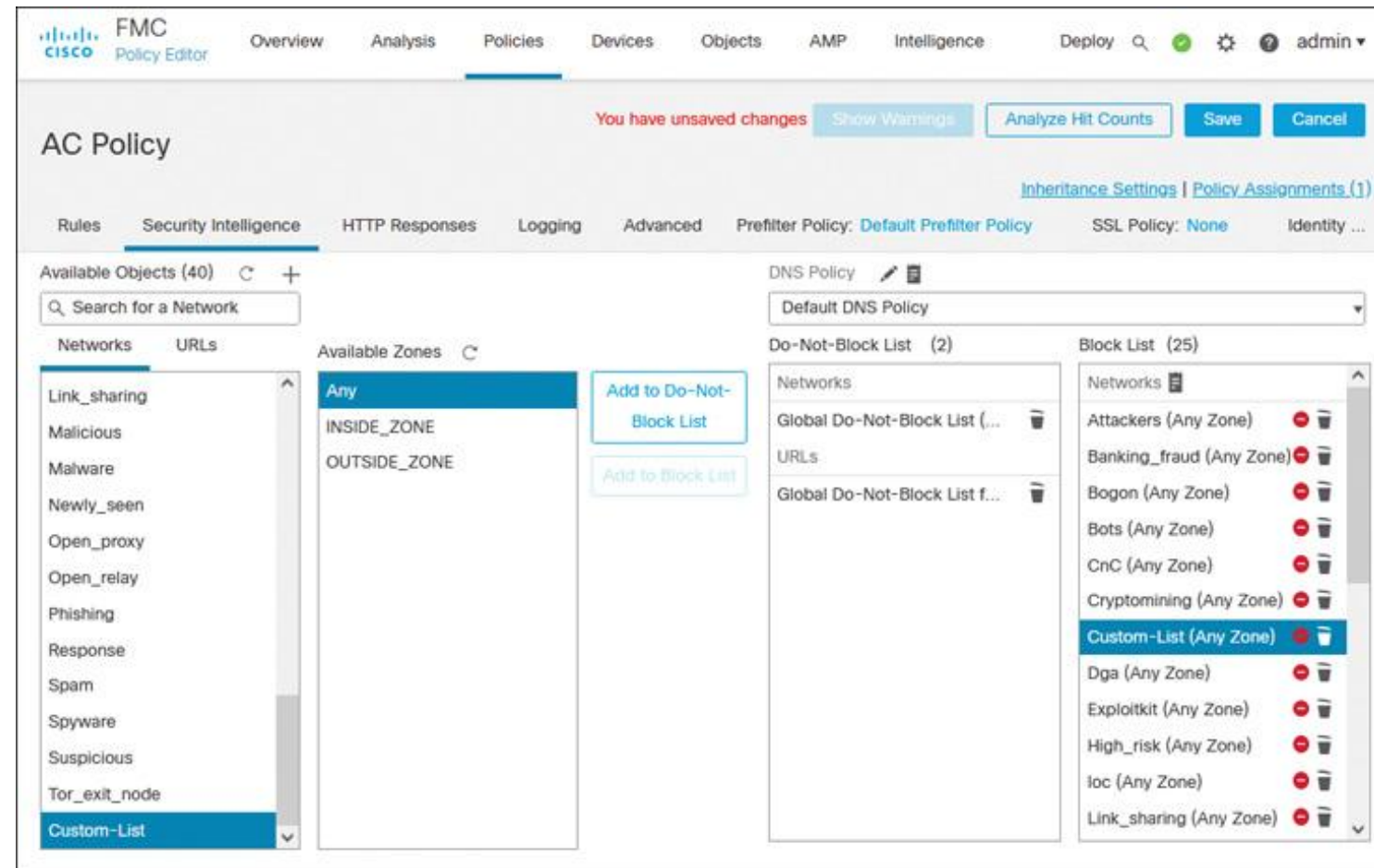
Number Of IPs: 5

Cancel Save

Manual Blocking Using Custom List

3) Policies > Access Control

- Edit the Policy that you want to deploy
- Select Security Intelligence tab
- select the custom network you want to block
- Click Add to Block List
- Save
- Deploy



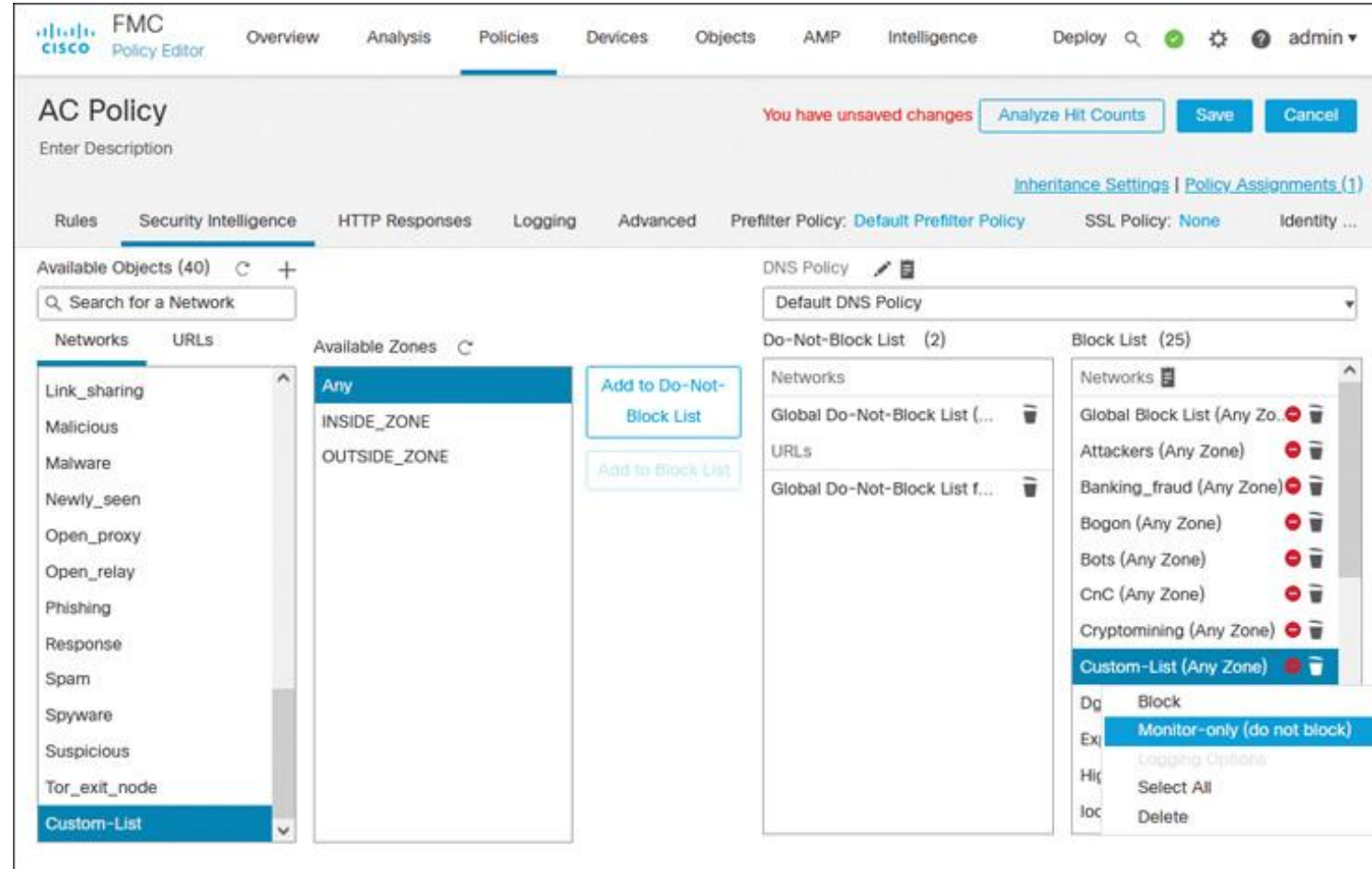
Security Intelligence in Monitor-Only Mode

- > Access Control Policy

- > Security Intelligence tab

- > From the Block List, right-click a category that you want to monitor

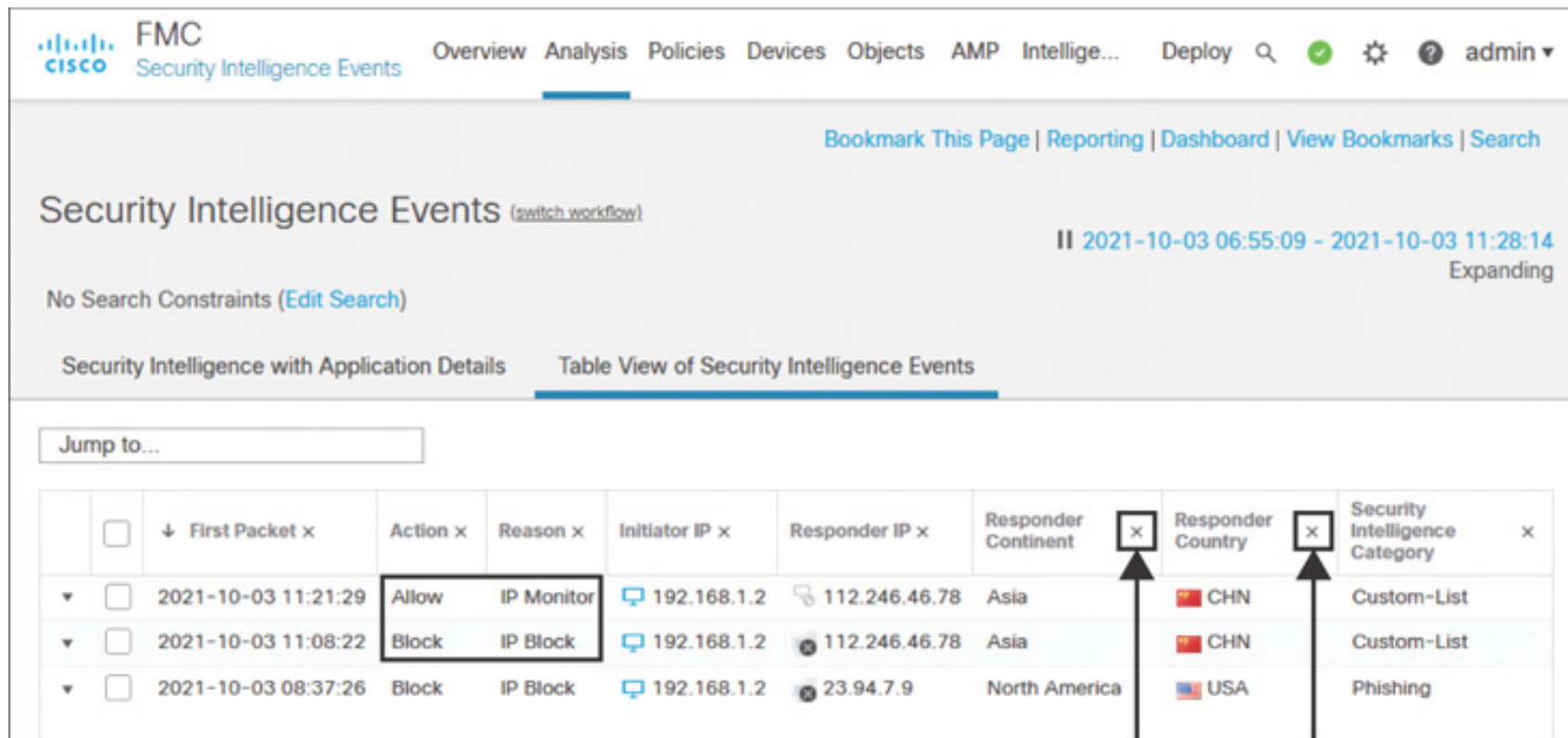
- > select the Monitor-only (Do Not Block)



Note : The threat defense does not support the Monitor-only mode for the Global Block List category.

Security Intelligence Events in Monitor-Only and Block Modes

- The first connection attempt from host 192.168.1.2 to 112.246.46.78 was blocked
- However, the second attempt was allowed, and the connection was monitored.



The screenshot displays the Cisco FMC Security Intelligence Events interface. The top navigation bar includes links for Overview, Analysis, Policies, Devices, Objects, AMP, Intelligence, Deploy, and a search icon. The main heading is "Security Intelligence Events" with a "(switch workflow)" link. Below this, there's a time range filter set to "2021-10-03 06:55:09 - 2021-10-03 11:28:14" and a status "Expanding". A search bar indicates "No Search Constraints (Edit Search)". The table view is titled "Table View of Security Intelligence Events".

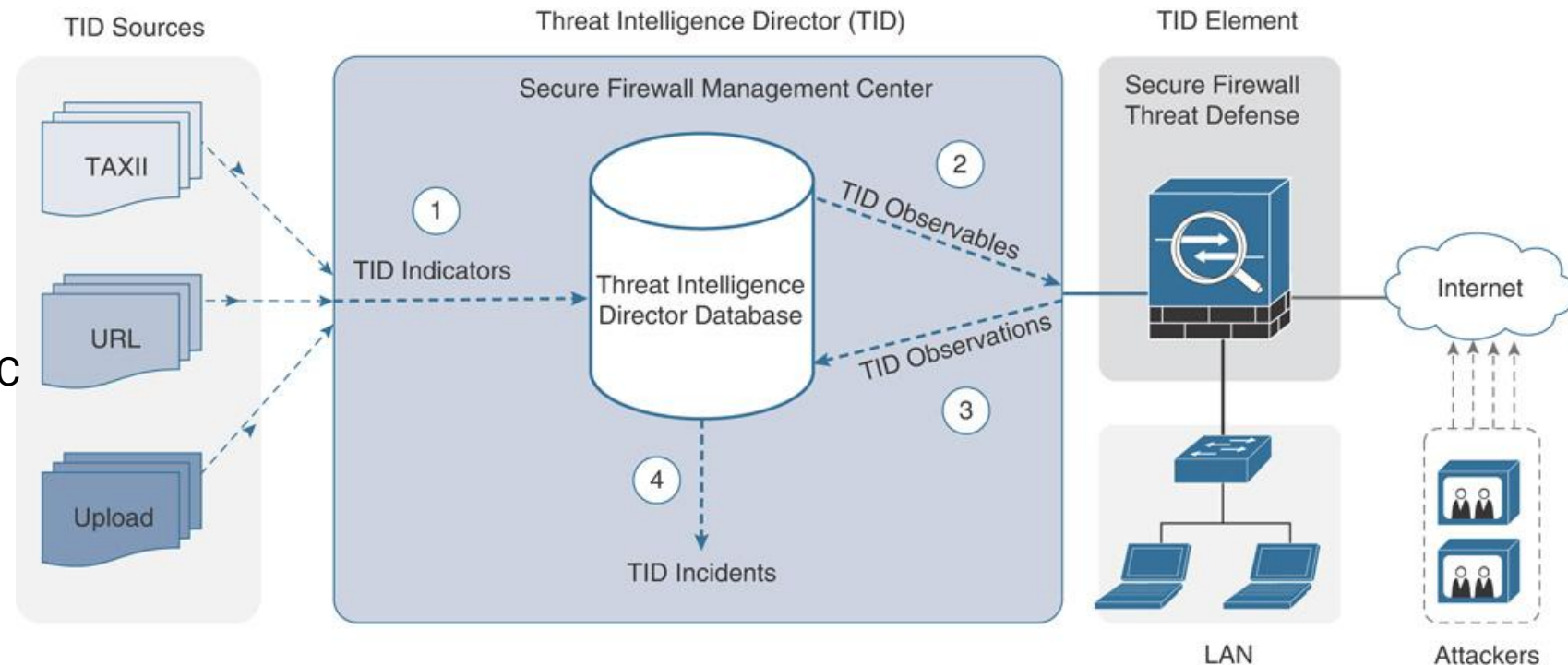
	☐	↓ First Packet x	Action x	Reason x	Initiator IP x	Responder IP x	Responder Continent x	Responder Country x	Security Intelligence Category x
▼	☐	2021-10-03 11:21:29	Allow	IP Monitor	192.168.1.2	112.246.46.78	Asia	CHN	Custom-List
▼	☐	2021-10-03 11:08:22	Block	IP Block	192.168.1.2	112.246.46.78	Asia	CHN	Custom-List
▼	☐	2021-10-03 08:37:26	Block	IP Block	192.168.1.2	23.94.7.9	North America	USA	Phishing

Use the x Icon to Add or Remove Data Points for Events

Threat Intelligence Director (TID)

- Secure Firewall can also analyze and block connections based on the threat intelligence data
- TID is enabled to obtain and aggregate intelligence data from third-party sources and publish to all of FTD devices

- 1) FMC get **indicators** from 3rd party
- 2) FMC publish **observables** to FTD
- ✓ FTD inspect the traffic
- 3) Then FTD reports **observation** to FMC
- 4) FMC generates incidents



- ❑ **An indicator** shows all the characteristics associated with a threat.
- ❑ **Observables** represent individual characteristics (e.g. a SHA-256 value) associated with the threat
"Each observable is a single IP, Domain, URL or hash value in which FTD looks inside traffic"

Threat Intelligence Director (TID)

Enabling Threat Intelligence Director

- 1) Policies > Access Control
- 2) Edit the desired Access control policy
- 3) Advanced tab
- 4) Edit the general setting
- 5) Select "Enable Threat Intelligence Director"
- 6) Save
- 7) Deploy

The screenshot shows the Firepower Management Center interface. The top navigation bar includes 'Policies / Access Control / Policy Editor', 'Overview', 'Analysis', 'Policies', and 'Devices'. The main content area is titled 'FTD1-Policy' and 'applicable to FTD1'. The 'Advanced' tab is selected, showing 'General Settings'. A dialog box is open with the following settings:

- Maximum URL characters to store in connection events: 1024
- Allow an Interactive Block to bypass blocking for (seconds): 600
- ☒ Retry URL cache miss lookup
- ☒ Enable Threat Intelligence Director
- ☒ Enable reputation enforcement on DNS traffic
- ☒ Inspect traffic during policy apply can be set to one of the following: Enabled [inspect]: A few packets might drop (depending on device load and capacity). Disabled [do not inspect]: Traffic is dropped or not (depending on how the device is configured).

At the bottom of the dialog box, there are buttons for 'Revert to Defaults', 'Cancel', and 'OK'.

Threat Intelligence Director (TID)

Enabling Threat Intelligence Director

- After the policy deployment is successful, navigate to Intelligence > Elements
- Wait a few seconds for the green status icon to appear

The screenshot shows the Cisco Firepower Management Center (FMC) interface. The top navigation bar includes the Cisco logo, the title 'Firepower Management Center', and the breadcrumb 'Intelligence / Elements'. The main navigation tabs are Overview, Analysis, Policies, Devices, Objects, AMP, and Intelligence. The Intelligence tab is selected, and a dropdown menu is open, showing options: Incidents, Sources, Elements (highlighted), and Settings. Below the navigation bar, a table displays the elements. The table has columns: Name, Element Type, Registered On, and Access Control. One element is listed: 'FTD1' with a green status icon, 'Cisco Firepower Threat Defense' as the element type, 'Dec 4, 2024 12:25 PM +0330' as the registered on date, and 'FTD1-Policy' as the access control policy.

Name	Element Type	Registered On	Access Control
FTD1	Cisco Firepower Threat Defense	Dec 4, 2024 12:25 PM +0330	FTD1-Policy

Threat Intelligence Director (TID)

Adding Sources and Importing Indicators

The FMC supports two types of files to ingest sources:

➤ **STIX (Structured Threat Information Expression):**

- A standard used by cybersecurity communities to describe and share threat intelligence information
- A STIX file supports complex indicators

➤ **Flat file:**

- ASCII text files
- They support simple indicators.

Threat Intelligence Director (TID)

Adding Sources and Importing Indicators

The FMC can obtain a **STIX** or a **flat** file in 3 ways:

❖ *TAXII (Trusted Automated eXchange of Indicator Information):*

- To download a large STIX file
- When an update is available, TAXII adds only the incremental data instead of replacing the existing data

❖ URL

- Using a URL, a management center can reach out to a remote server to fetch files from it.

❖ Upload

- Upload the file directly from your computer to the management center, by the browser.

Threat Intelligence Director (TID)

Adding Sources and Importing Indicators

Click **Intelligence > Sources**

Click **+**

The screenshot displays the Cisco Firepower Management Center (FMC) web interface. The top navigation bar includes the Cisco logo, the title "Firepower Management Center", and a breadcrumb trail "Intelligence / Sources". The main navigation menu contains links for Overview, Analysis, Policies, Devices, Objects, AMP, Intelligence, and Deploy. The "Intelligence" menu is expanded, showing a dropdown with options: Incidents, Sources (highlighted with a mouse cursor), Elements, and Settings. Below the navigation bar, there are tabs for "Sources", "Indicators", and "Observables". The "Sources" tab is active, showing a search bar and a table with columns: Name, Type, Delivery, Action, Publish, Last Update, and Status. To the right of the table, there is a refresh button, a status indicator "0 Sources", and a button "Add a new source" with a plus icon. A user profile "admin" is visible in the top right corner.

Threat Intelligence Director (TID)

Adding Sources and Importing Indicators

Select TID source type (TAXII , URL , Upload)

Upload:

- Upload the file and assign a name to this source
- Select Content type
- Choose Action (monitor or Block)
- Click Save

Add Source ? ✕

DELIVERY TAXII URL Upload

TYPE Flat File ▼ CONTENT SHA-256 ▼

FILE* Drag and drop or click to upload

NAME*

DESCRIPTION

ACTION ➔ Monitor ▼

TTL (DAYS)

PUBLISH ☒

Save Cancel

SHA-256

Domain

URL

IPv4

IPv6

Email To

Email From

Email Sender

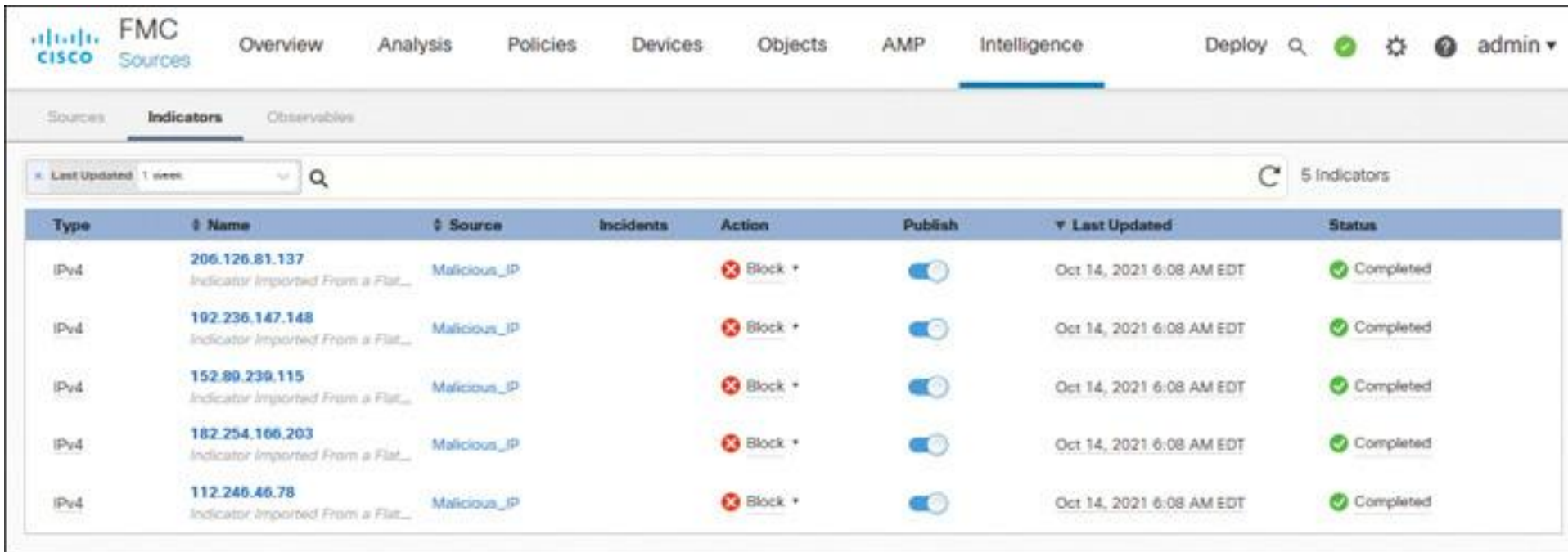
Email Subject

Threat Intelligence Director (TID)

Adding Sources and Importing Indicators

Go to the indicators tab

You will notice all the IP addresses that are included in the uploaded file are imported as TID indicators



FMC Sources							
Overview Analysis Policies Devices Objects AMP Intelligence Deploy 🔍 ⚙️ ? admin ▼							
Sources Indicators Observables							
x Last Updated 1 week 🔍 5 Indicators							
Type	Name	Source	Incidents	Action	Publish	Last Updated	Status
IPv4	206.126.81.137 Indicator Imported From a Flat...	Malicious_IP		❌ Block +	☒	Oct 14, 2021 6:08 AM EDT	✅ Completed
IPv4	192.236.147.148 Indicator Imported From a Flat...	Malicious_IP		❌ Block +	☒	Oct 14, 2021 6:08 AM EDT	✅ Completed
IPv4	152.80.239.115 Indicator Imported From a Flat...	Malicious_IP		❌ Block +	☒	Oct 14, 2021 6:08 AM EDT	✅ Completed
IPv4	182.254.166.203 Indicator Imported From a Flat...	Malicious_IP		❌ Block +	☒	Oct 14, 2021 6:08 AM EDT	✅ Completed
IPv4	112.246.46.78 Indicator Imported From a Flat...	Malicious_IP		❌ Block +	☒	Oct 14, 2021 6:08 AM EDT	✅ Completed

Threat Intelligence Director (TID)

Adding Sources and Importing Indicators

TAXII:

- You can import thousands of indicators in bulk from third-party source using the TAXII service.
- Enter the URL of TAXII source
- Enter username and password of the URL

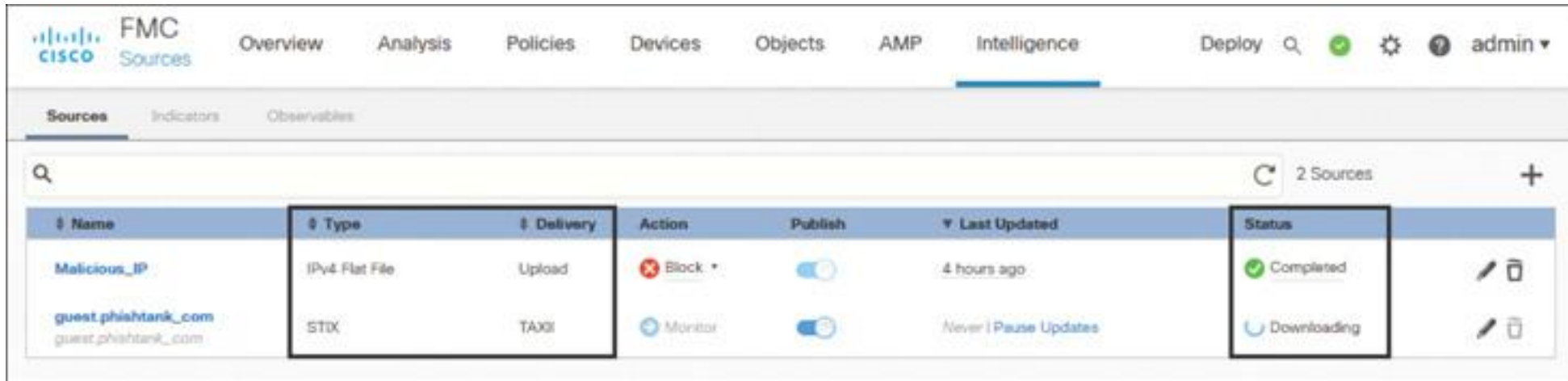
The screenshot shows the 'Add Source' dialog box with the following fields and options:

- DELIVERY:** TAXII (selected), URL, Upload
- URL*:** http://hailotaxii.com/taxii-discovery-service
- SSL Settings:** (dropdown menu)
- USERNAME:** guest
- PASSWORD:** (masked with dots)
- Warning:** Credentials will be sent using an unsecured HTTP connection
- FEEDS*:** guest.phishtank.com (selected from a dropdown)
- Note:** A separate source will be added for each feed selected. The name will default to the name of the feed and can be edited later.
- ACTION:** Monitor (selected)
- UPDATE EVERY (MINUTES):** 1440 (input field) and Never Update (checkbox)
- TTL (DAYS):** 90 (input field)
- PUBLISH:** (toggle switch, currently on)
- Buttons:** Save, Cancel

Threat Intelligence Director (TID)

Adding Sources and Importing Indicators

After STIX is downloaded, observables are published automatically, without any redeployment of the access control policy.



The screenshot shows the Cisco FMC Sources page. The 'Intelligence' tab is selected. Under the 'Sources' sub-tab, there are two sources listed. The first source, 'Malicious_IP', is of type 'IPv4 Flat File' and has a status of 'Completed'. The second source, 'guest.phishtank.com', is of type 'STIX' and has a status of 'Downloading'. The 'Status' column is highlighted with a red box.

Name	Type	Delivery	Action	Publish	Last Updated	Status
Malicious_IP	IPv4 Flat File	Upload	Block	On	4 hours ago	Completed
guest.phishtank.com	STIX	TAXII	Monitor	On	Never Pause Updates	Downloading

Downloading a STIX File Using the TAXII Service

Threat Intelligence Director (TID)

Adding Sources and Importing Indicators

URL:

- Select STIX or Flat file from Type menu
- Enter the URL of STIX or Flat file
- Enter username and password of the URL
- Enter a name
- Select Action type
- Save

Add Source



DELIVERY

TAXII **URL** Upload

TYPE

STIX ▼

URL*

SSL Settings ▼

USERNAME

PASSWORD

NAME*

DESCRIPTION

ACTION

➔ Monitor

UPDATE EVERY (MINUTES)

1440

☐ Never Update

TTL (DAYS)

90

PUBLISH

☒

Save

Cancel

Threat Intelligence Director (TID)

Checking Indicators Using the TAXII

- Go to the Indicators tab again

Thousands of indicators are being populated from the third-party source

When traffic is blocked by TID, you can find the events on the **Intelligence > Incidents** page

Thousands of Indicators

40,282 Indicators

Type	Name	Source	Incidents	Action	Publish	Last Updated	Status
URL	phishTank.com id:5217540... This URL (https://www.jugos...	guest.phishtank_c...		Monitor *	☒	Oct 14, 2021 3:31 PM UTC	Completed
URL	phishTank.com id:5238626... This URL (https://www.jugos...	guest.phishtank_c...		Monitor *	☒	Oct 14, 2021 3:31 PM UTC	Completed
URL	phishTank.com id:5254951... This URL (https://www.jugos...	guest.phishtank_c...		Monitor *	☒	Oct 14, 2021 3:31 PM UTC	Completed
URL	phishTank.com id:6940829... This URL (https://mailingser...	guest.phishtank_c...		Block *	☒	Oct 14, 2021 3:33 PM UTC	Completed
URL	phishTank.com id:6987279... This URL (https://docs.goog...	guest.phishtank_c...		Block *	☒	Oct 14, 2021 3:32 PM UTC	Completed
URL	phishTank.com id:7001901... This URL (https://bansebas...	guest.phishtank_c...		Block *	☒	Oct 14, 2021 3:28 PM UTC	Completed
URL	phishTank.com id:7009239... This URL (https://onyet.com...	guest.phishtank_c...		Monitor *	☒	Oct 14, 2021 3:27 PM UTC	Completed
URL	phishTank.com id:7035952... This URL (https://fukerv.my...	guest.phishtank_c...		Monitor *	☒	Oct 14, 2021 3:27 PM UTC	Completed
URL	phishTank.com id:7053648... This URL (https://zula-bede...	guest.phishtank_c...		Monitor *	☒	Oct 14, 2021 3:27 PM UTC	Completed
URL	phishTank.com id:7057475... This URL (https://v9ve/SyN...	guest.phishtank_c...		Monitor *	☒	Oct 14, 2021 3:28 PM UTC	Completed
URL	phishTank.com id:7057653... This URL (https://angbra.co...	guest.phishtank_c...		Monitor *	☒	Oct 14, 2021 3:28 PM UTC	Completed
URL	phishTank.com id:7059019... This URL (https://www.grad...	guest.phishtank_c...		Monitor *	☒	Oct 14, 2021 3:28 PM UTC	Completed
URL	phishTank.com id:7064803... This URL (https://binocra.c...	guest.phishtank_c...		Monitor *	☒	Oct 14, 2021 3:28 PM UTC	Completed
URL	phishTank.com id:7066891... This URL (https://concheck...	guest.phishtank_c...		Monitor *	☒	Oct 14, 2021 3:28 PM UTC	Completed
URL	phishTank.com id:7067086... This URL (https://forms.offic...	guest.phishtank_c...		Monitor *	☒	Oct 14, 2021 3:28 PM UTC	Completed

Changing Action