Securing Networks with

Cisco FTD

Chapter 10

Security Intelligence

Mohsen Kheradmand

Security intelligence

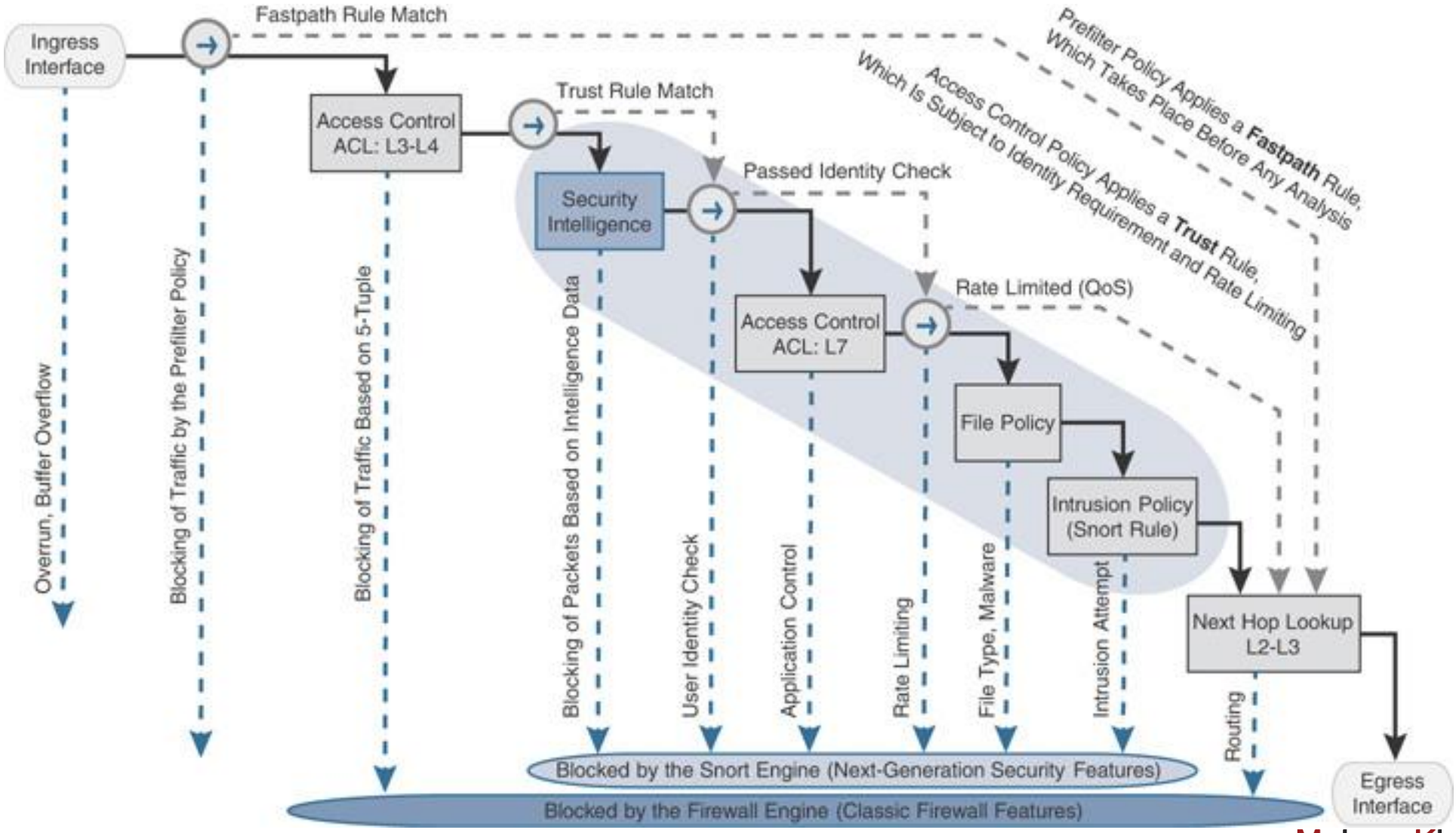
- Security Intelligence blocks a suspicious address dynamically without manual modification to the access control policy.
- It can block a packet before the packet goes through a deeper inspection process in the threat defense.
- It can optimize CPU and memory utilization, which can improve overall system 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

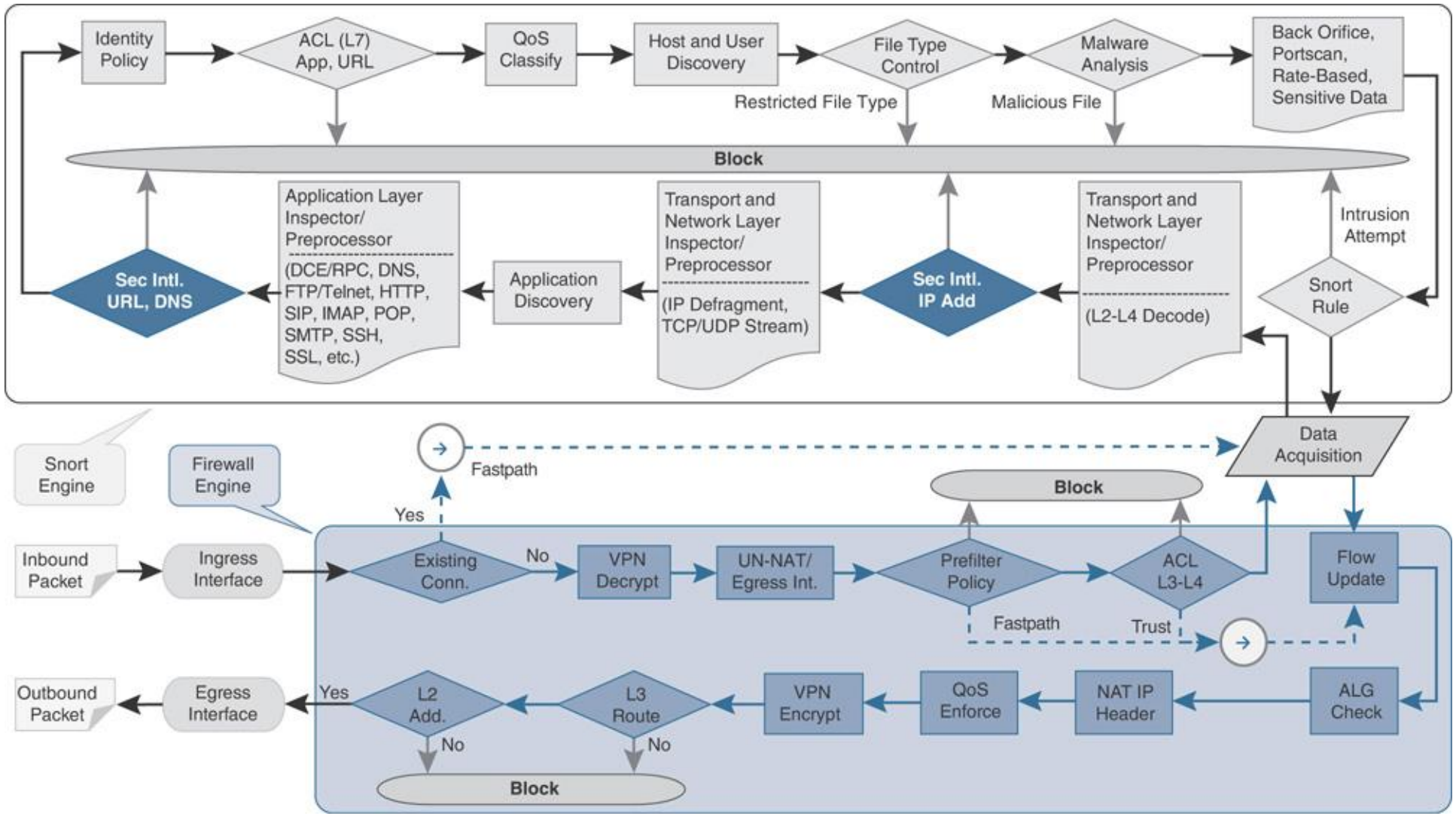
3 ways to input a suspicious address into the FTD :

- 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)

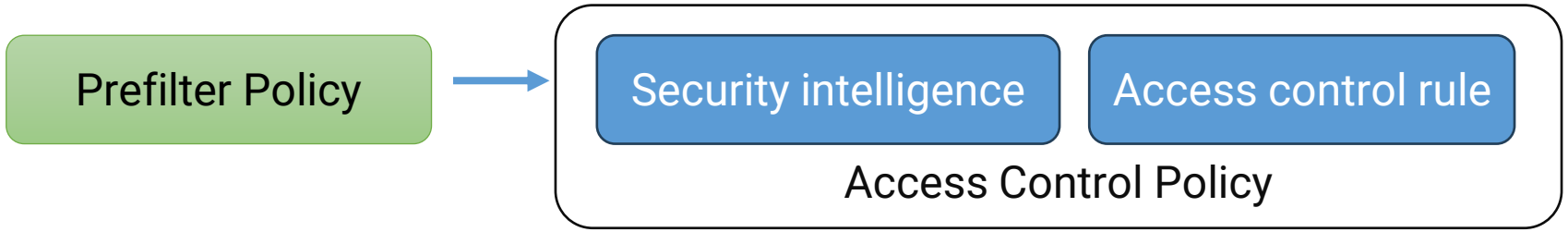


➢ Processing of Packets by Various Components of Security Engines (Highlighting Security Intelligence)



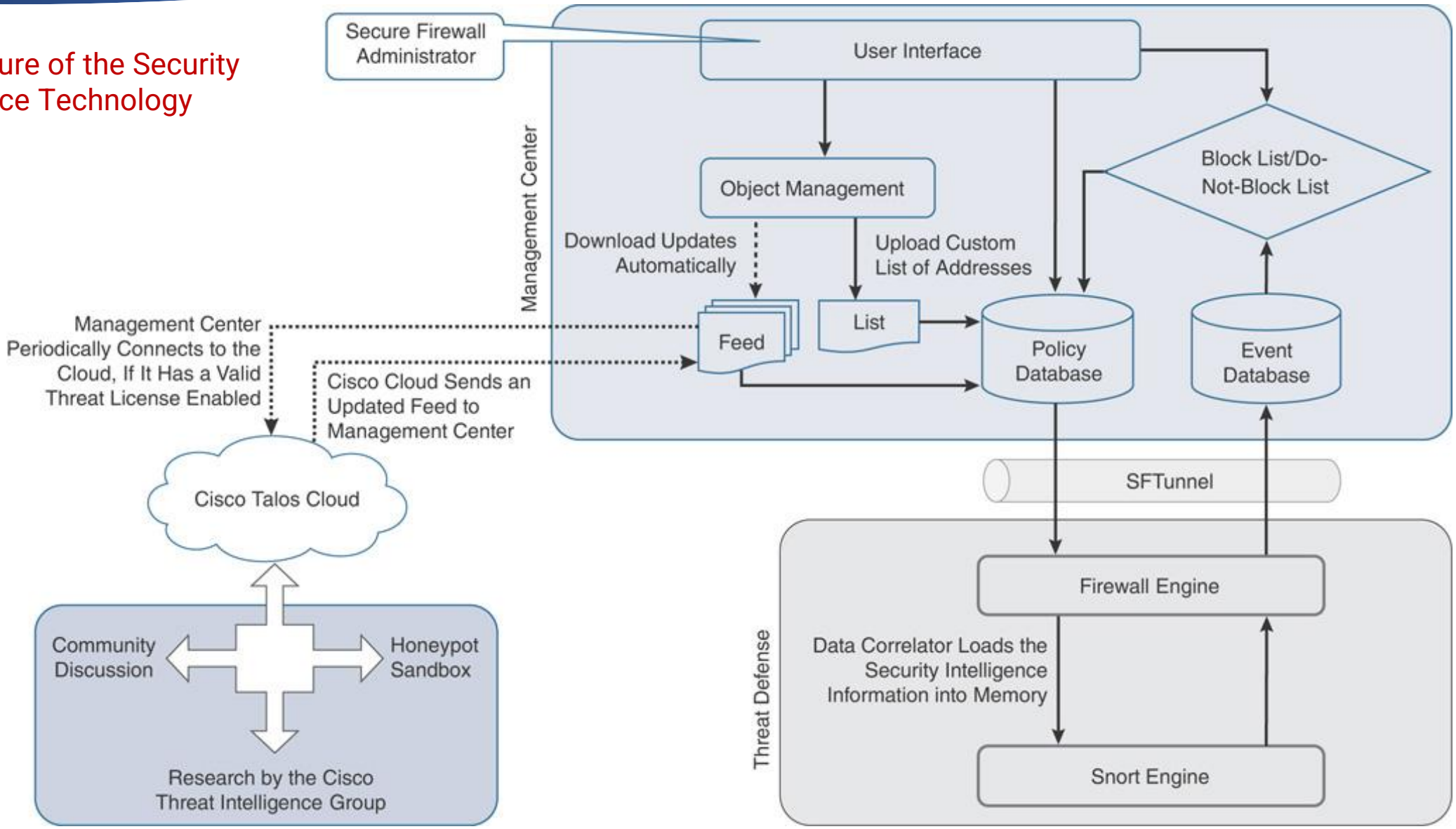
➢ Difference between ACP , Prefilter and Security intelligence

- 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

- Architecture of the Security Intelligence Technology

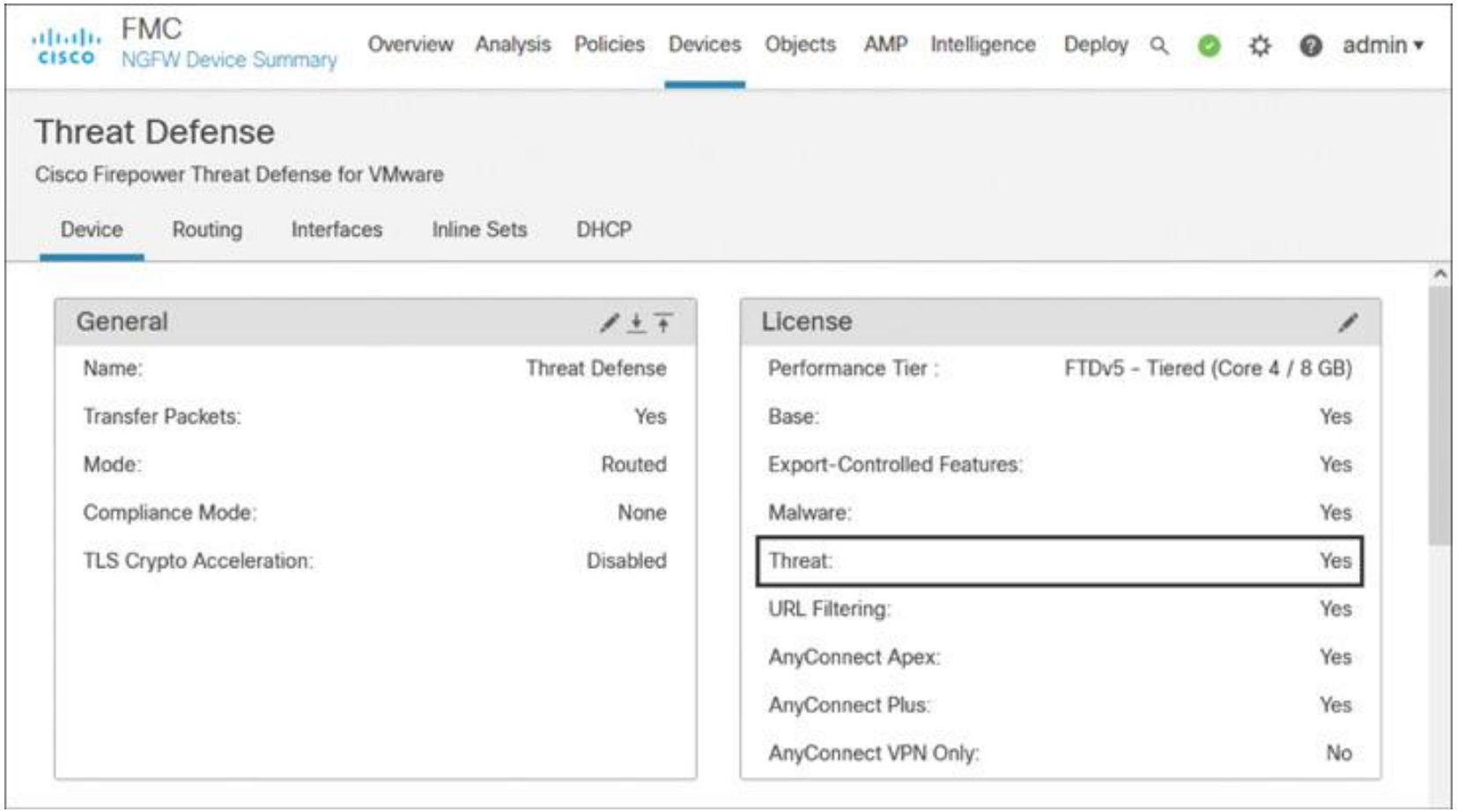


Before you enable security intelligence:

- ✓ 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

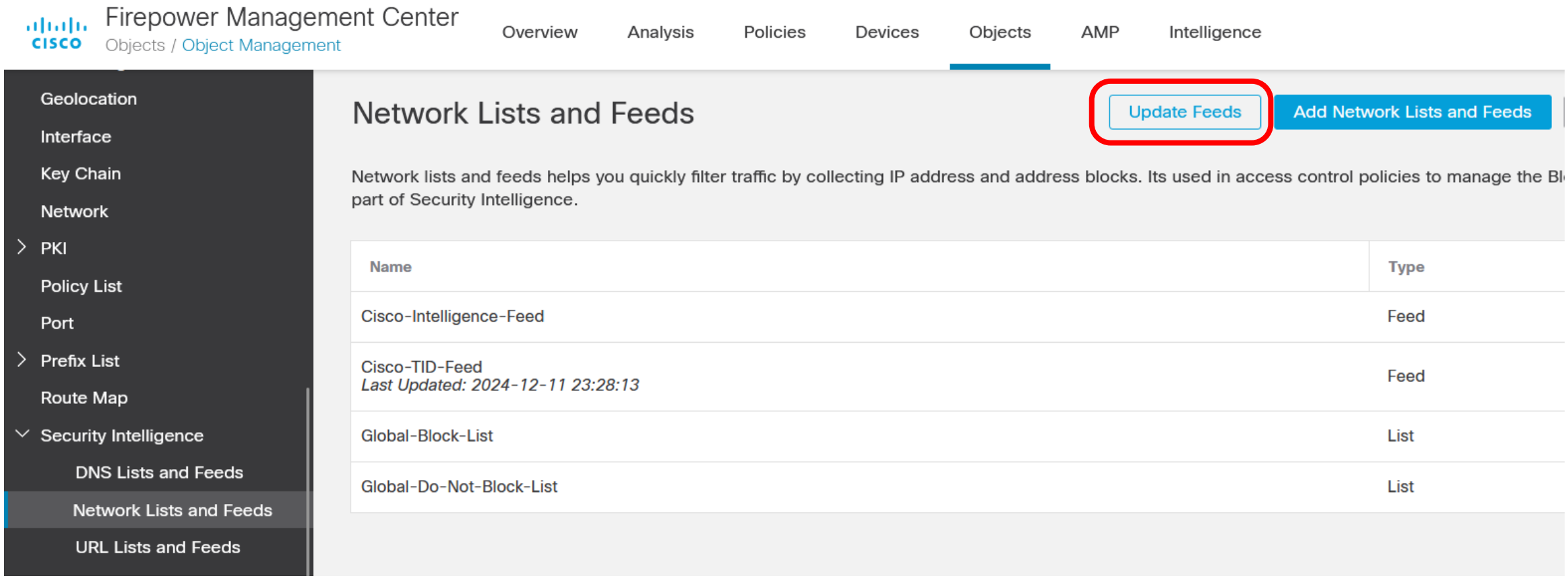
1) Security Intelligence requires **a threat license**



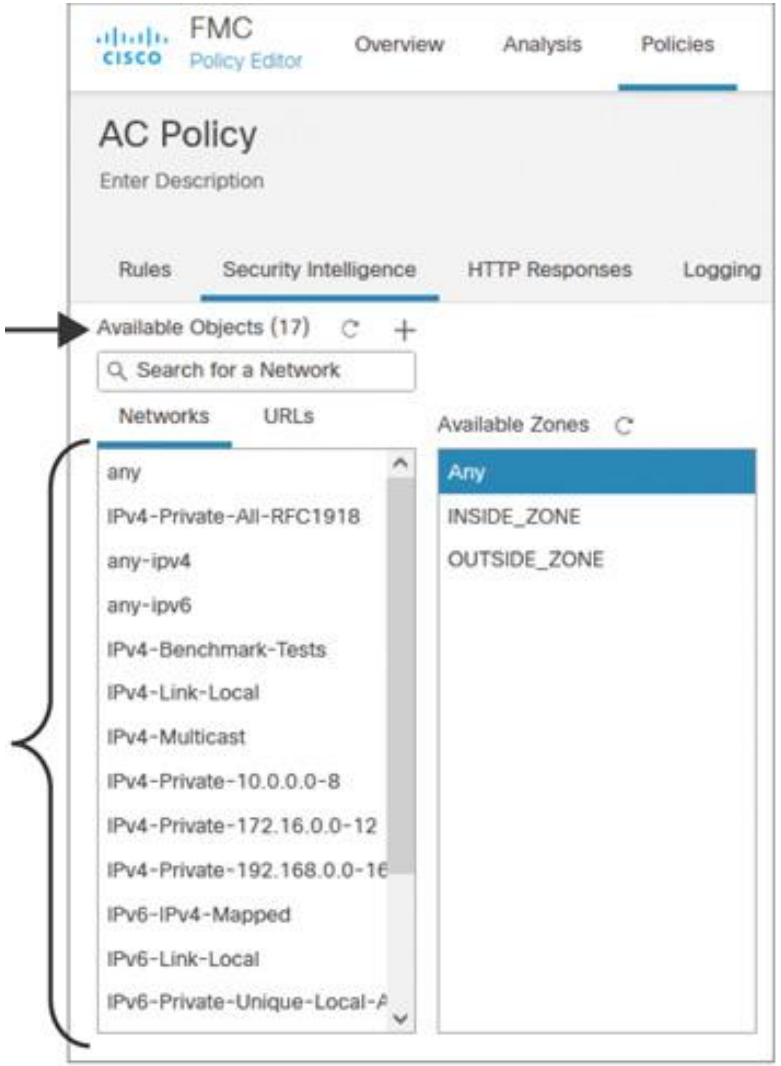
Security Intelligence prerequisites

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



Security Intelligence prerequisites



Default Network Objects (out of the box)

Intelligence-Based Network Objects
(after the Feeds Update)

MohsenKheradmand MK

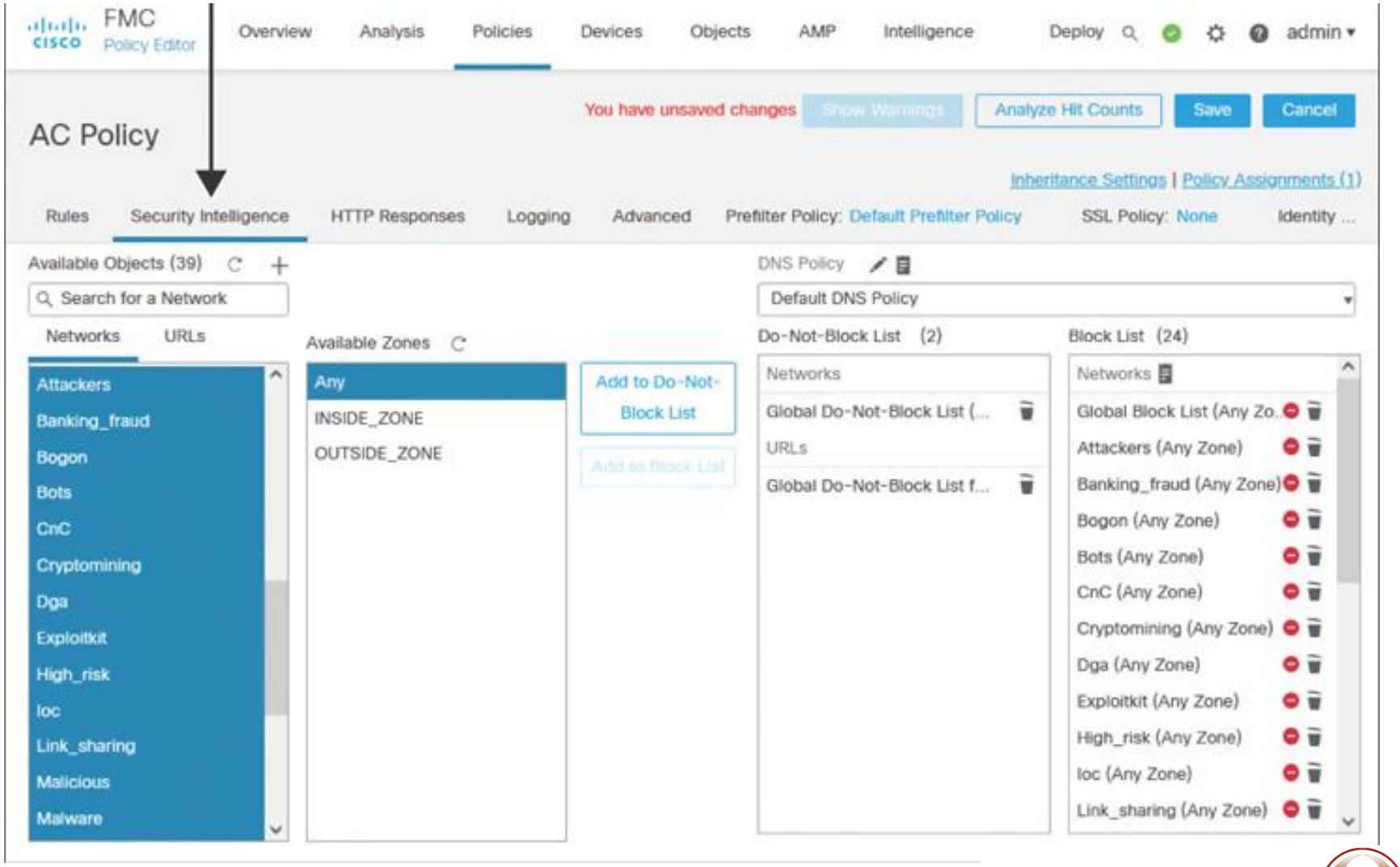
Automatic Blocking Using Intelligence Feed

- Security Intelligence based on **IP addresses**

- Policies > Access Control
  - Click pencil to edit
    - Select Security Intelligence

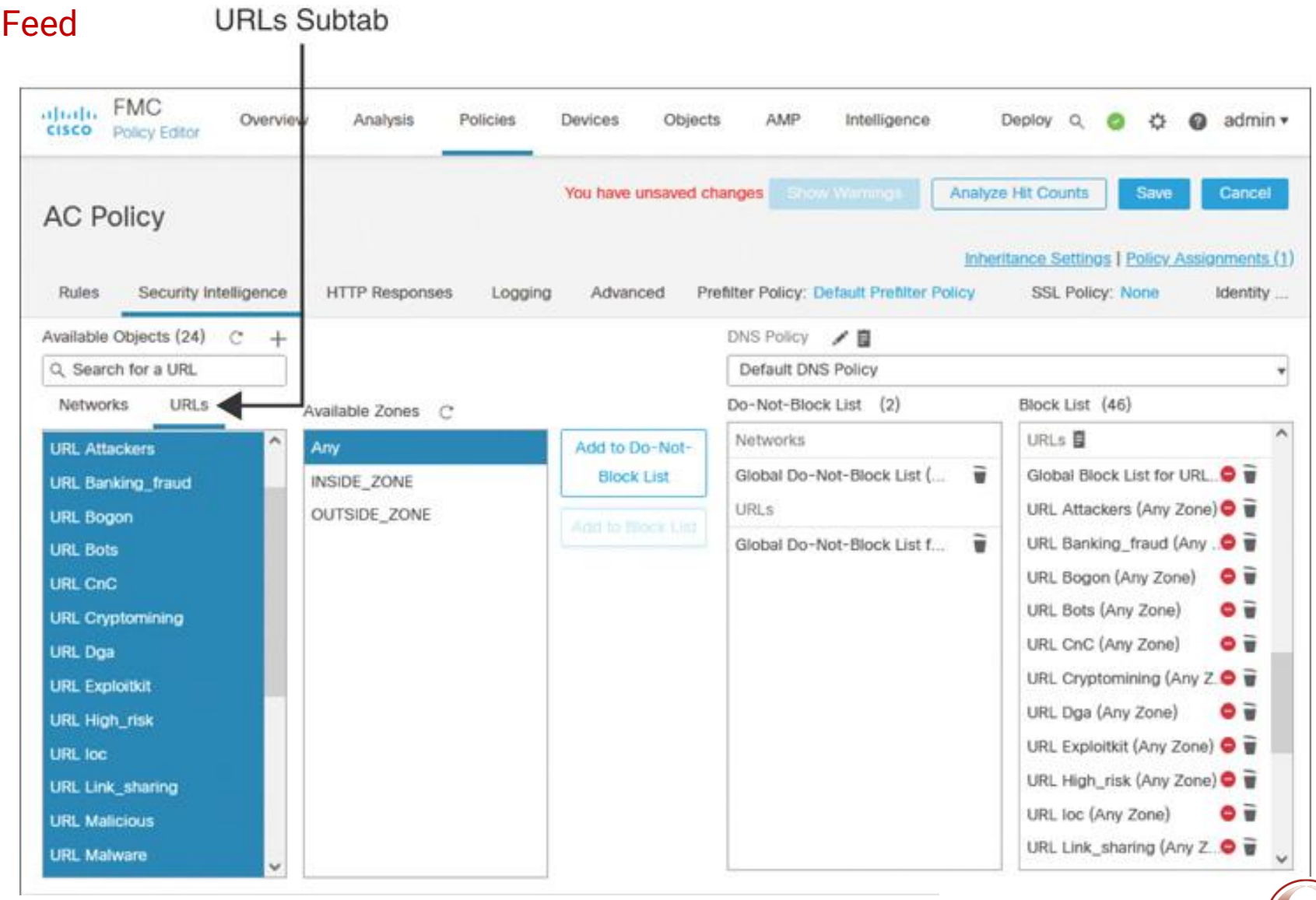
- Networks : select a category
- Optionally : select by Zones

- Add selected to :
  - ❑ Block list
  - ❑ Do-not-Block list



Automatic Blocking Using Intelligence Feed

- **URL-based** Security Intelligence

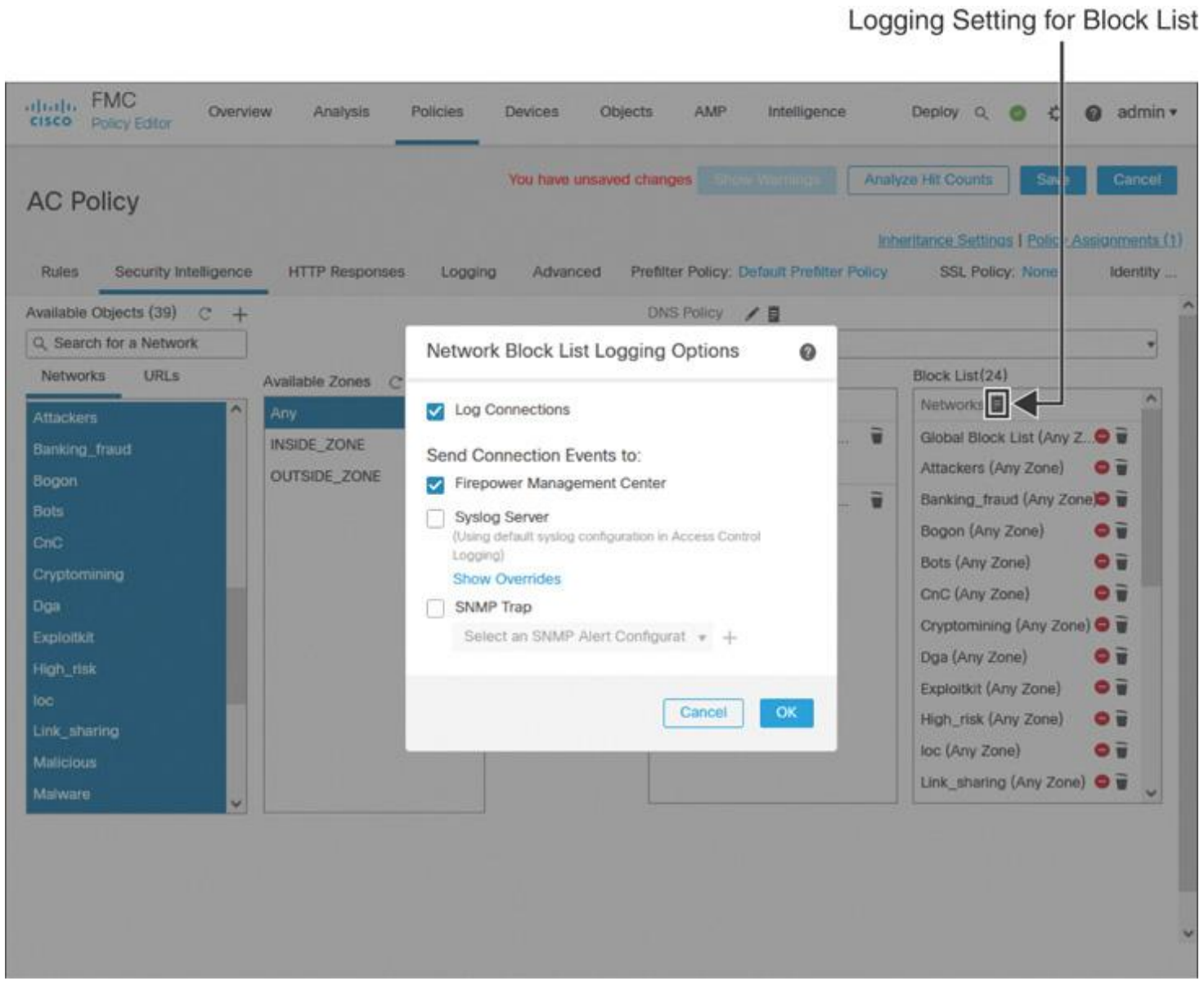


Automatic Blocking Using Intelligence Feed

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

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

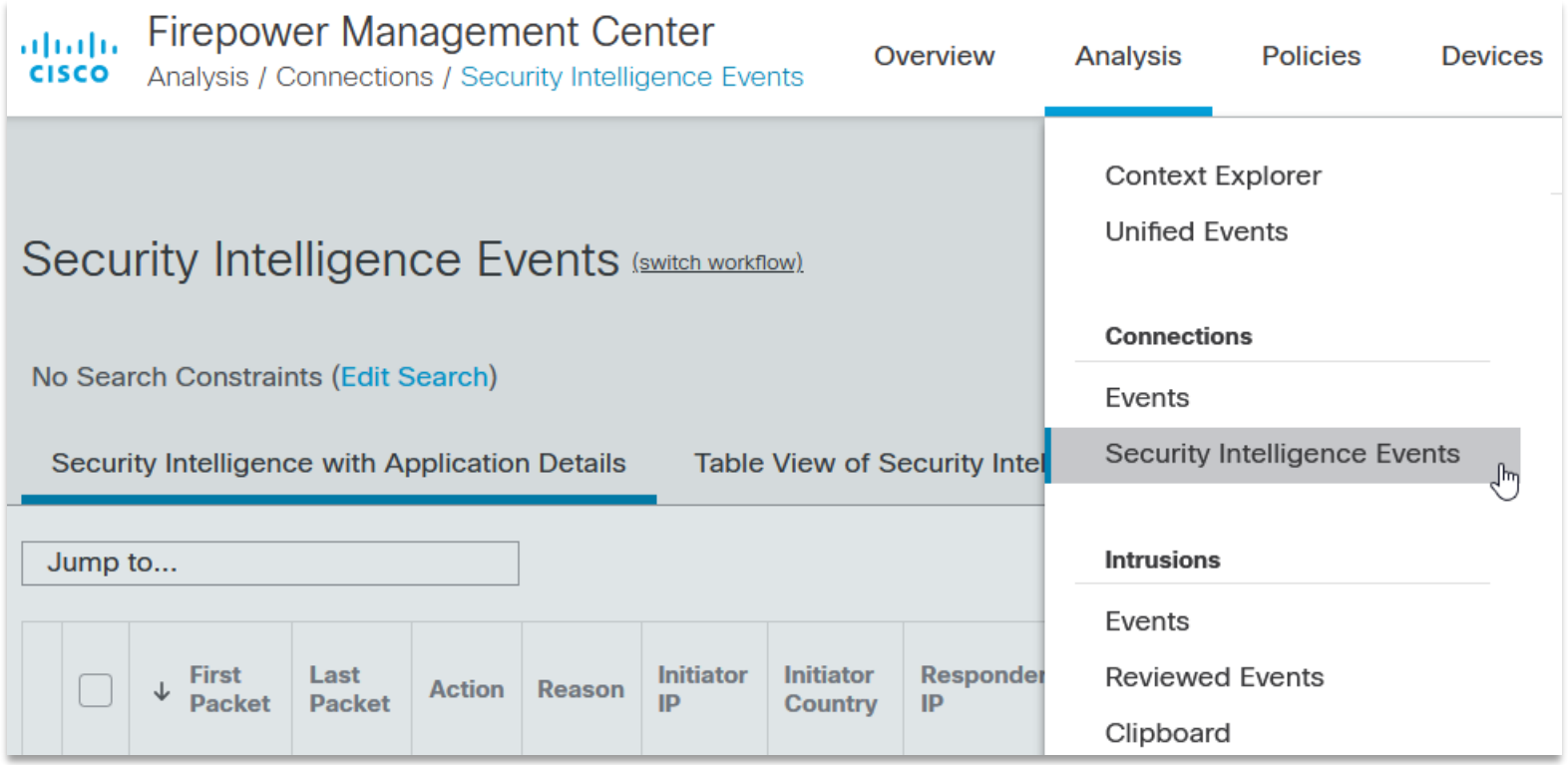
Finally, navigate to **Deploy** > **Deployment**



Verifying the Action of Intelligence Feed

To see the action of Security Intelligence on live traffic

- Analysis > Connections > Security Intelligence Events



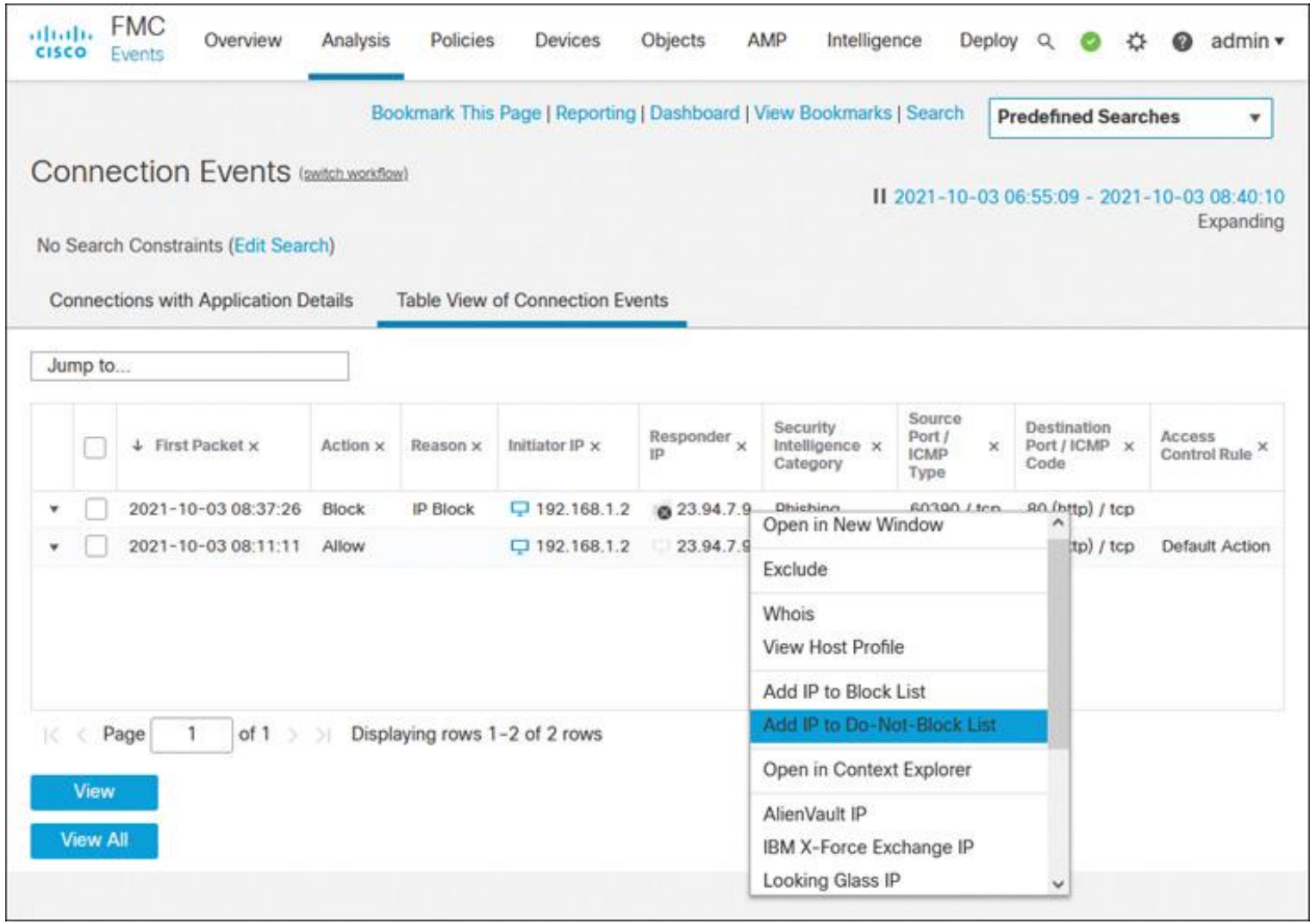
Verifying the Action of Intelligence Feed

You can also logs an associated connection event for connection attempt

- Analysis > Connections > Events

Add to Do-Not-Block List

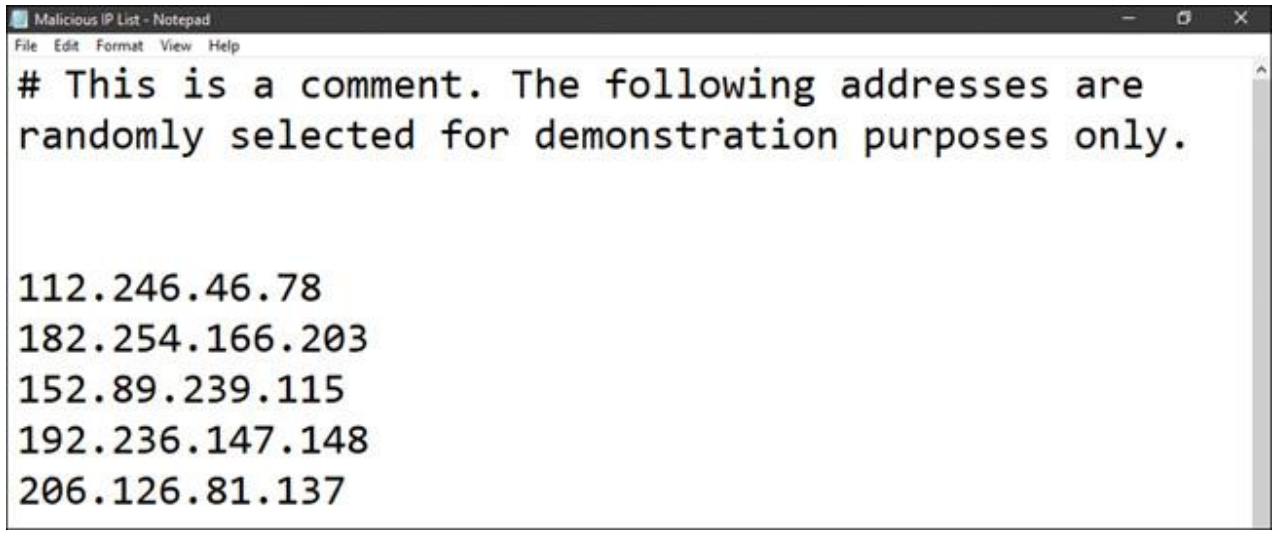
- Sometimes Cisco block an address and you disagree with that
- So on the Connection Events page right click the desired address and select :
  Add IP to DO-Not-Block list
- However , traffic to and from that address is still subject to any subsequent inspection



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



Manual Blocking Using Custom List

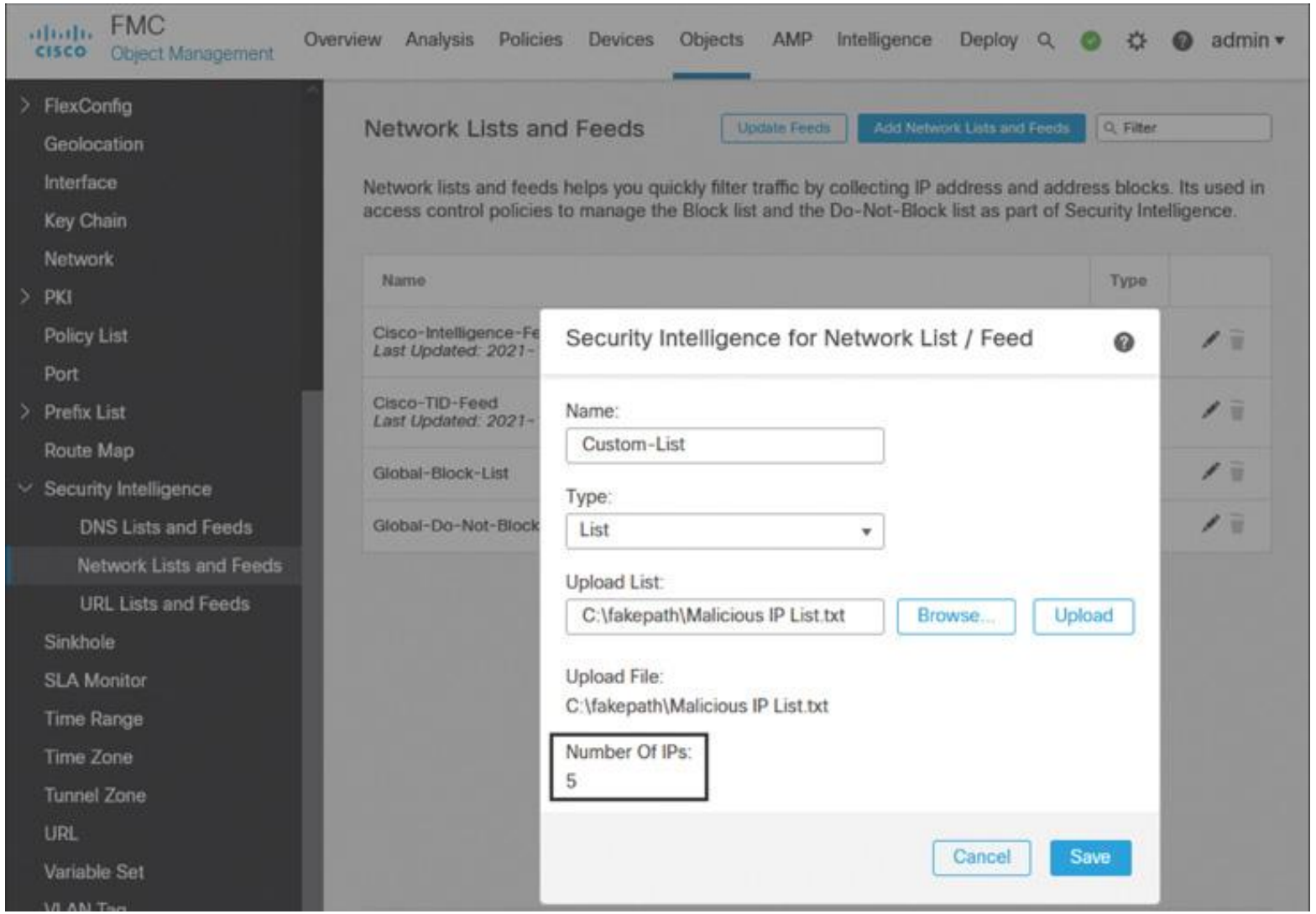
2) Object > Object Management

> Security intelligence

> Network Lists and Feeds

> Add Network Lists and Feeds

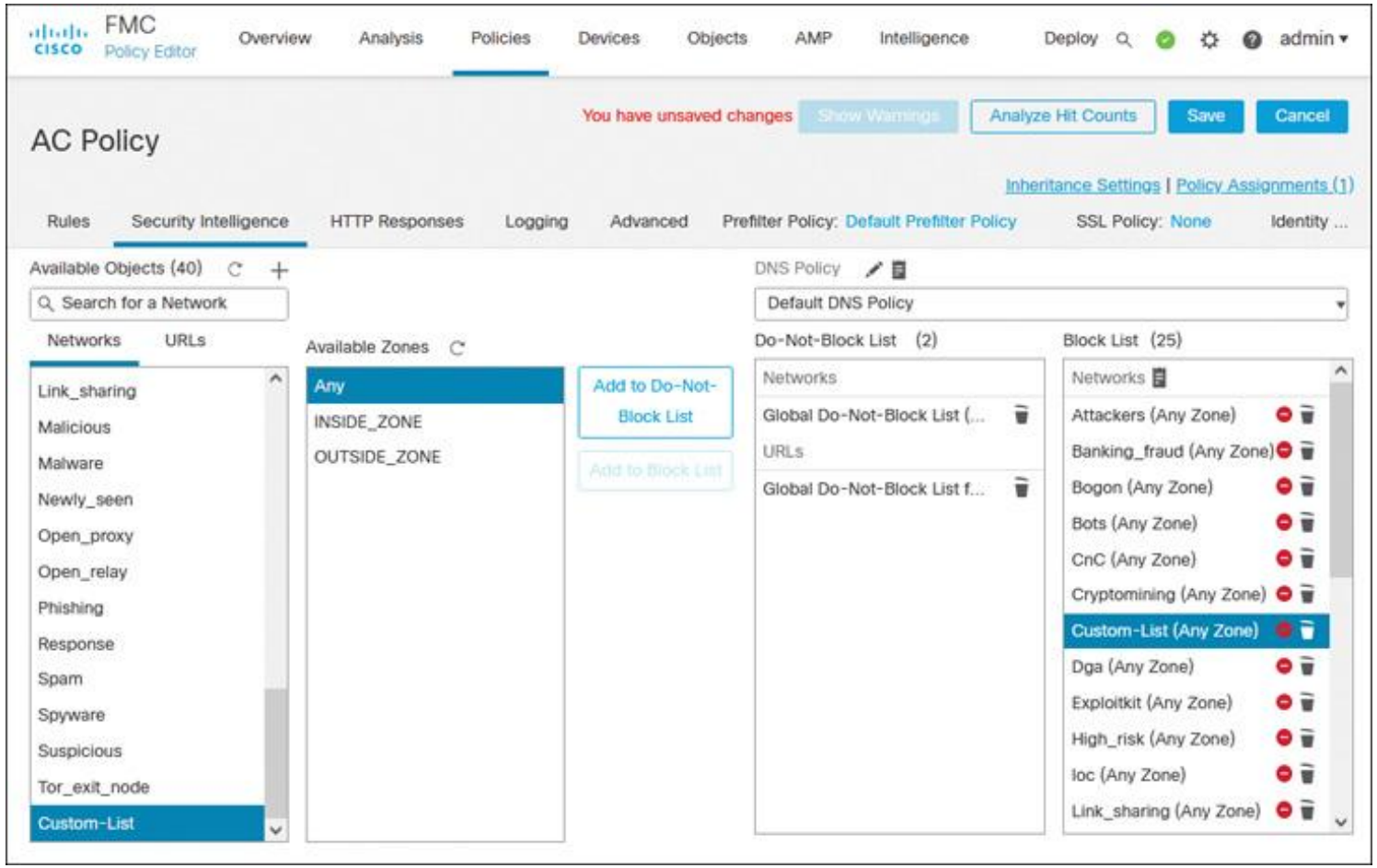
- Enter a name
- Select List from Type
- Click browse and select TXT file



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



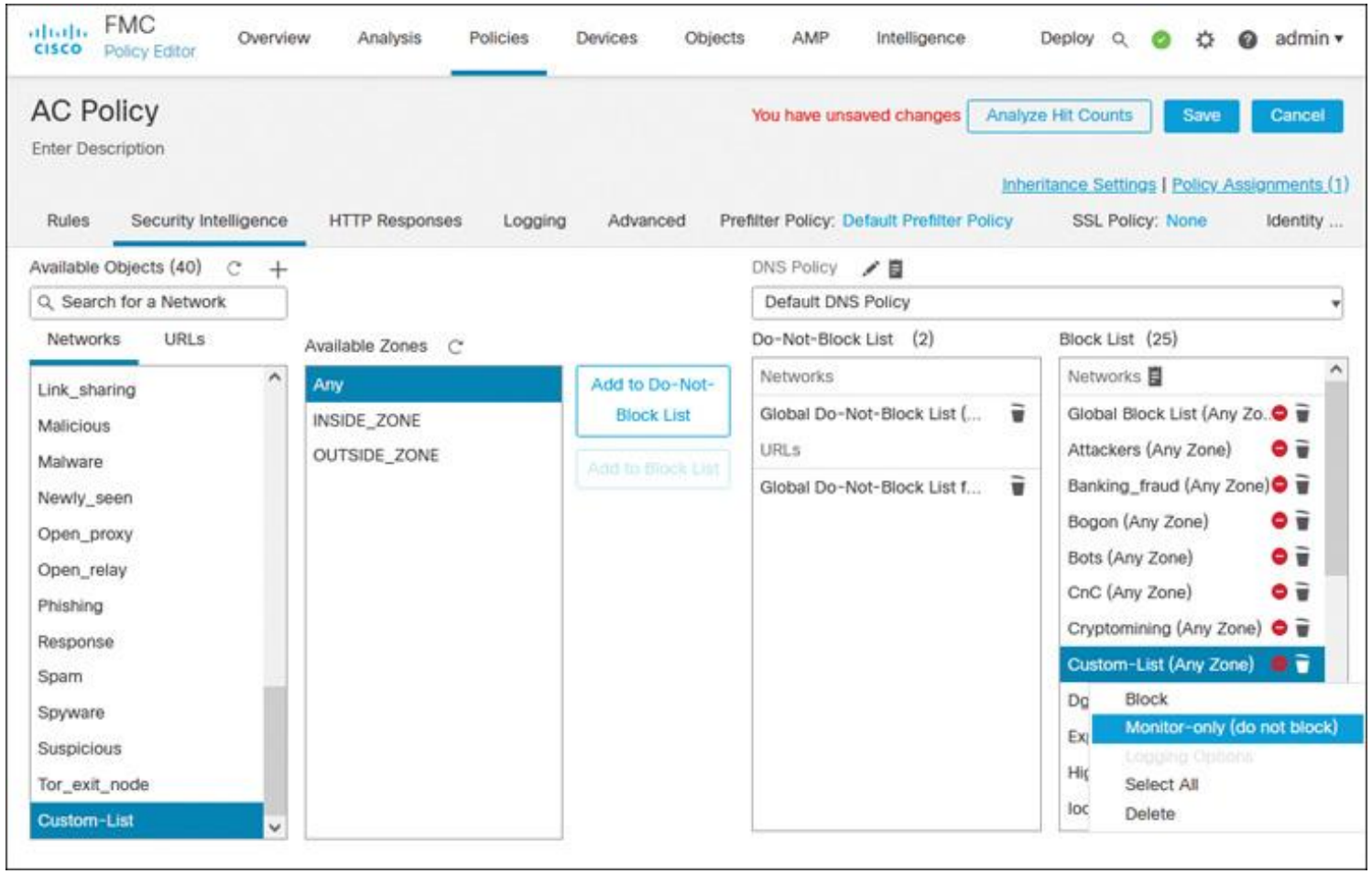
Security Intelligence in Monitor-Only Mode

> Access Control Policy

> Security Intelligence tab

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

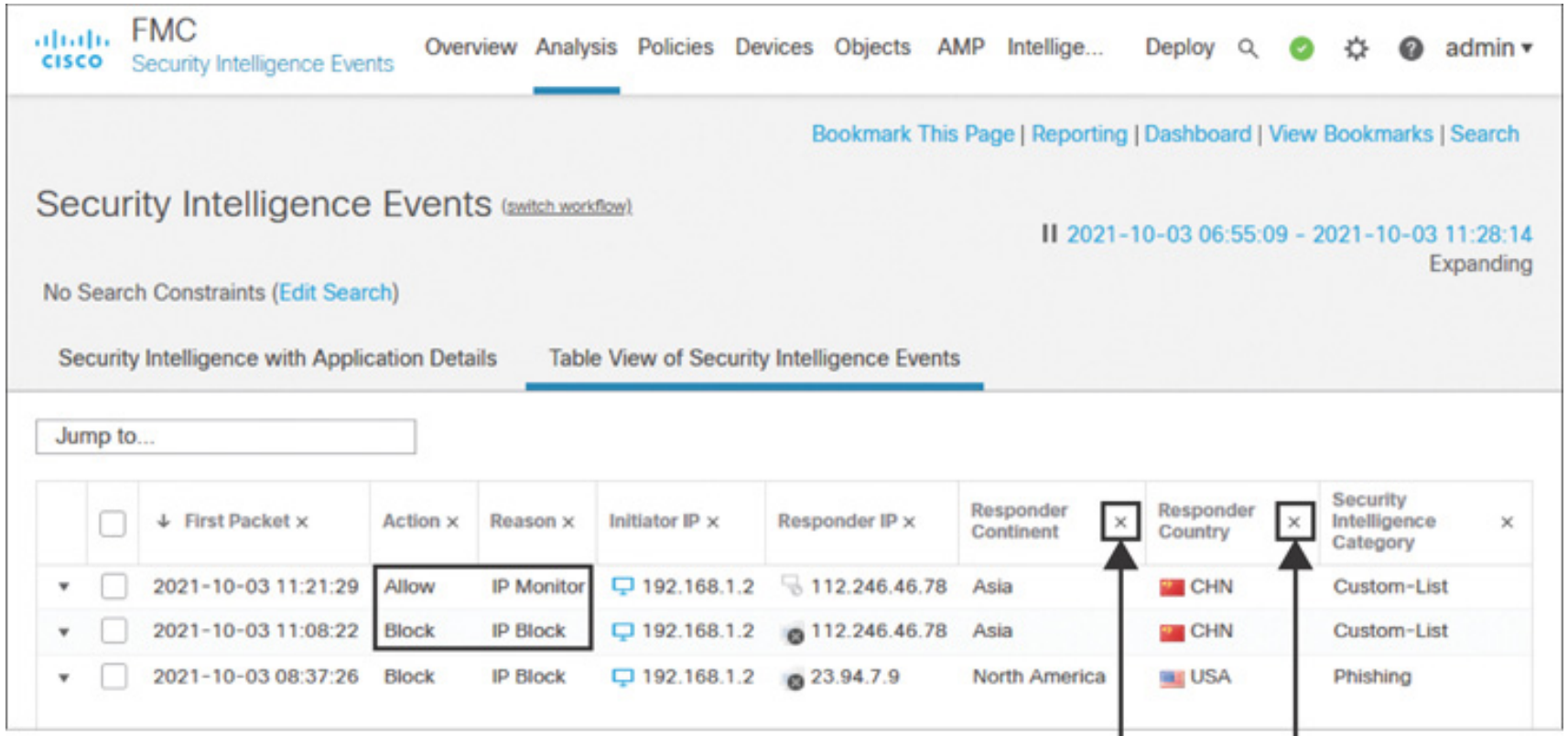
> select the Monitor-only (Do Not Block)



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

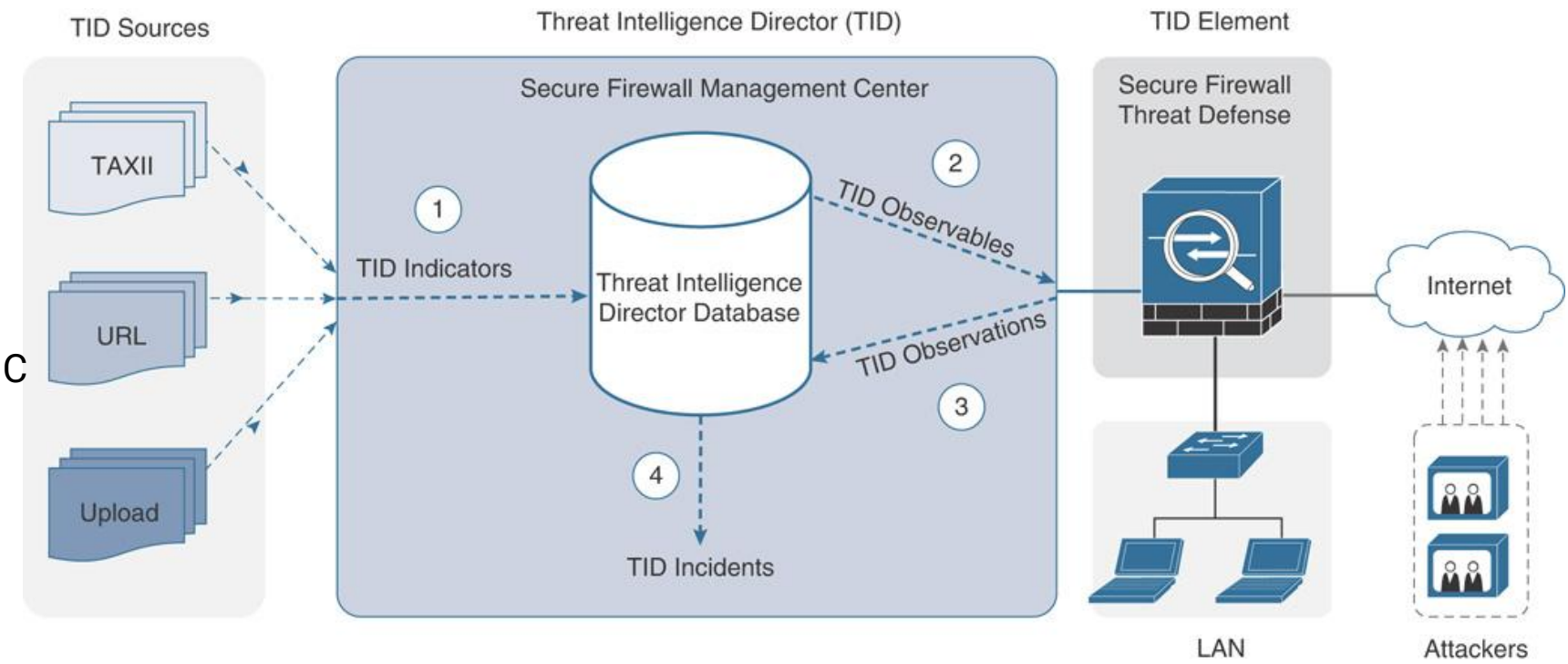
- The first connection attempt from host 192.168.1.2 to 112.246.46.78 was blocked
- However, the second attempt was allowed, and the connection was monitored.



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

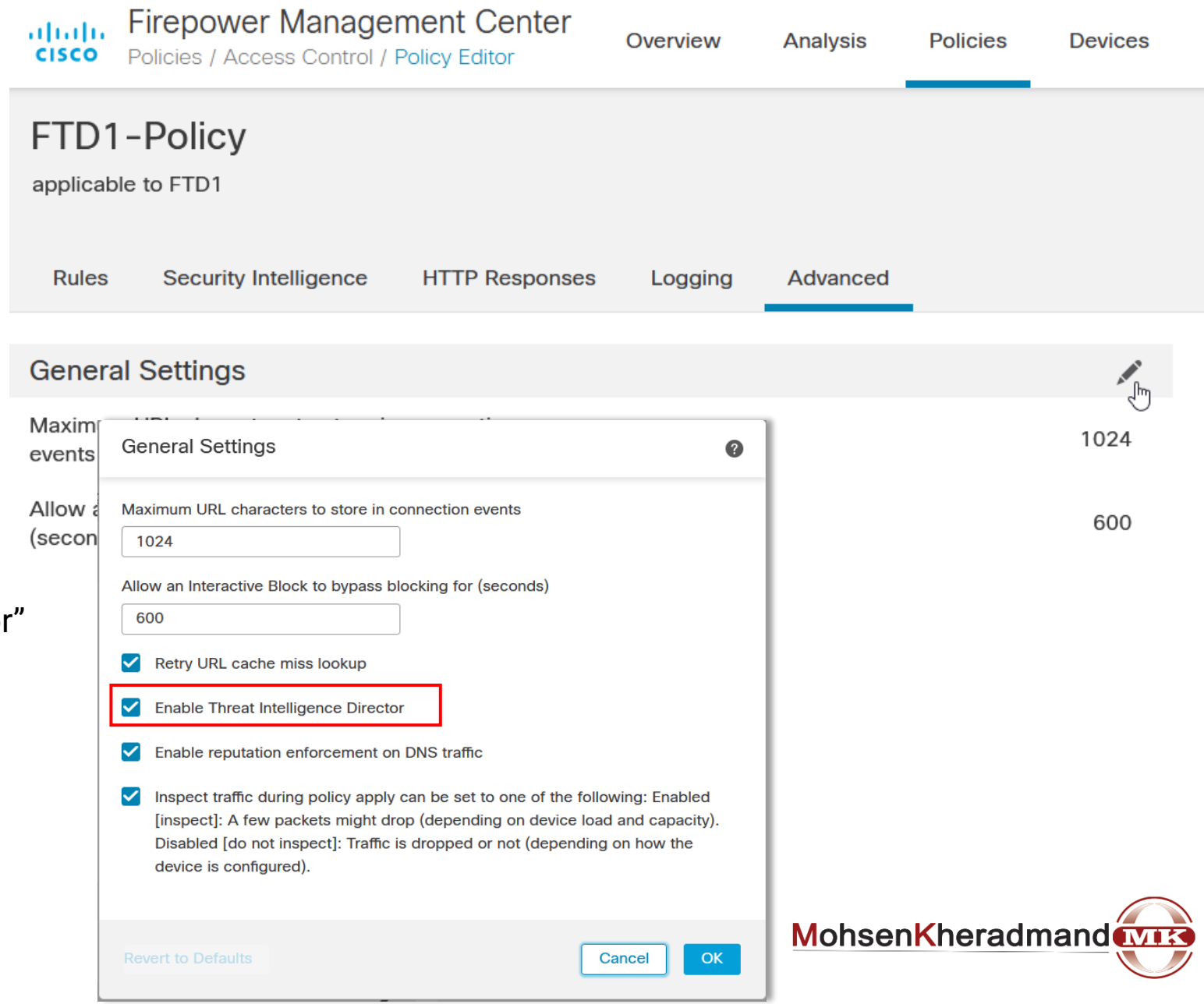


- ❑ **An indicator** shows all the characteristics associated with a threat.
- ❑ **Observables** represent individual characteristics (e.g. a SHA-256 value) associated with the threat
  "Each observable is a single IP, Domain, URL or hash value in which FTD looks inside traffic"

Threat Intelligence Director (TID)

Enabling Threat Intelligence Director

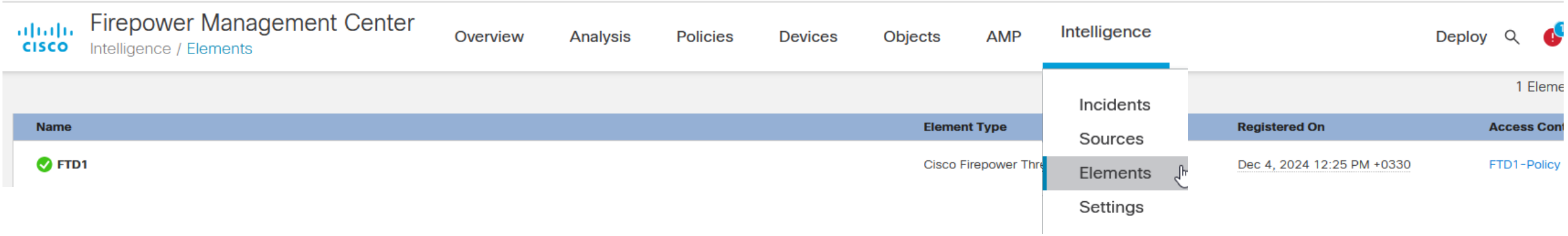
1) Policies > Access Control
2) Edit the desired Access control policy
3) Advanced tab
4) Edit the general setting
5) Select “Enable Threat Intelligence Director”
6) Save
7) Deploy



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



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:

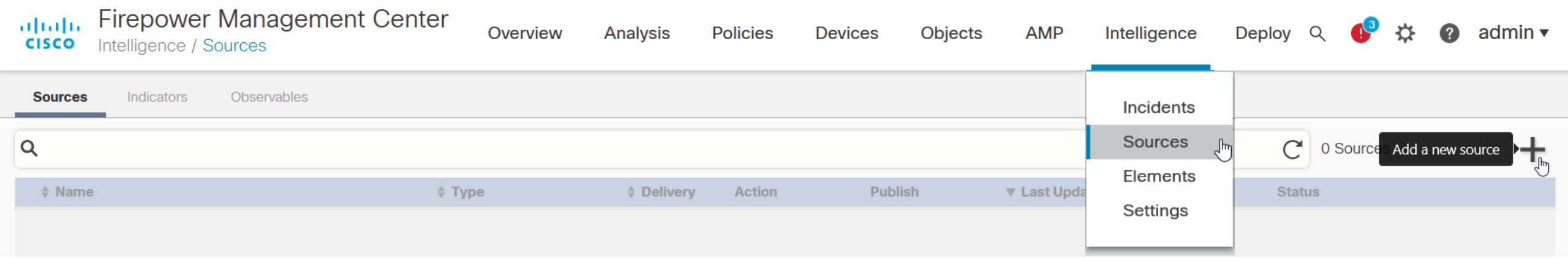
- *TAXII (Trusted Automated eXchange of Indicator Information):*
  - To download a large STIX file
  - When an update is available, TAXII adds only the incremental data instead of replacing the existing data
- URL
  - Using a URL, a management center can reach out to a remote server to fetch files from 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 **+**



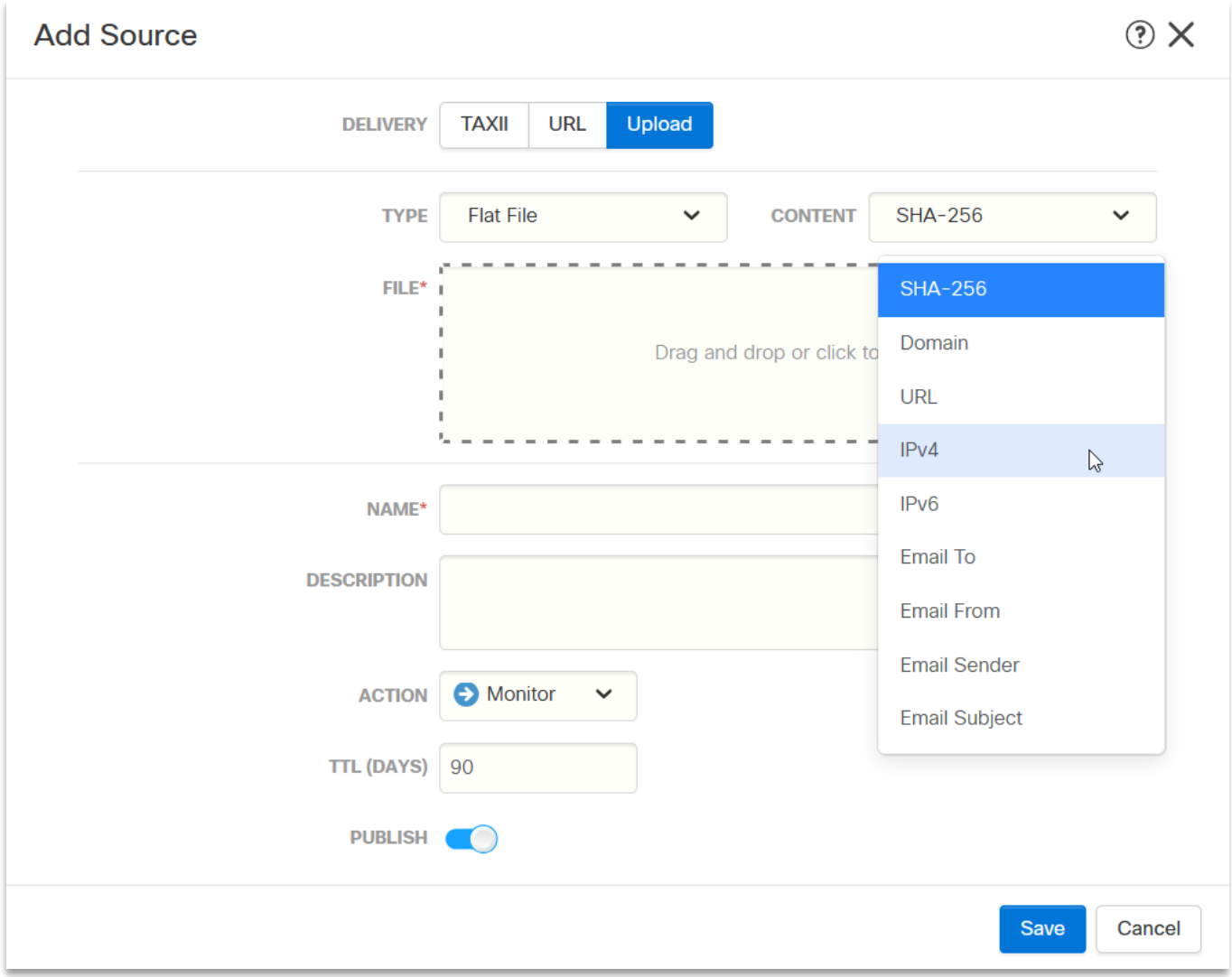
Threat Intelligence Director (TID)

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

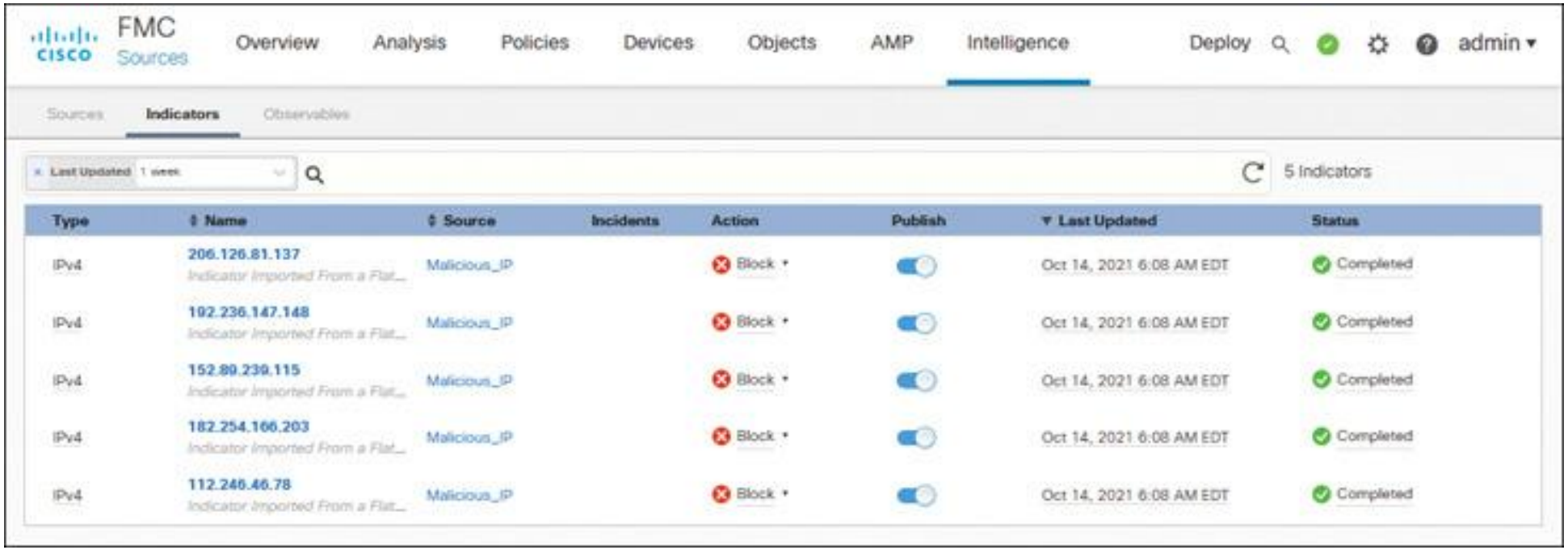


Threat Intelligence Director (TID)

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



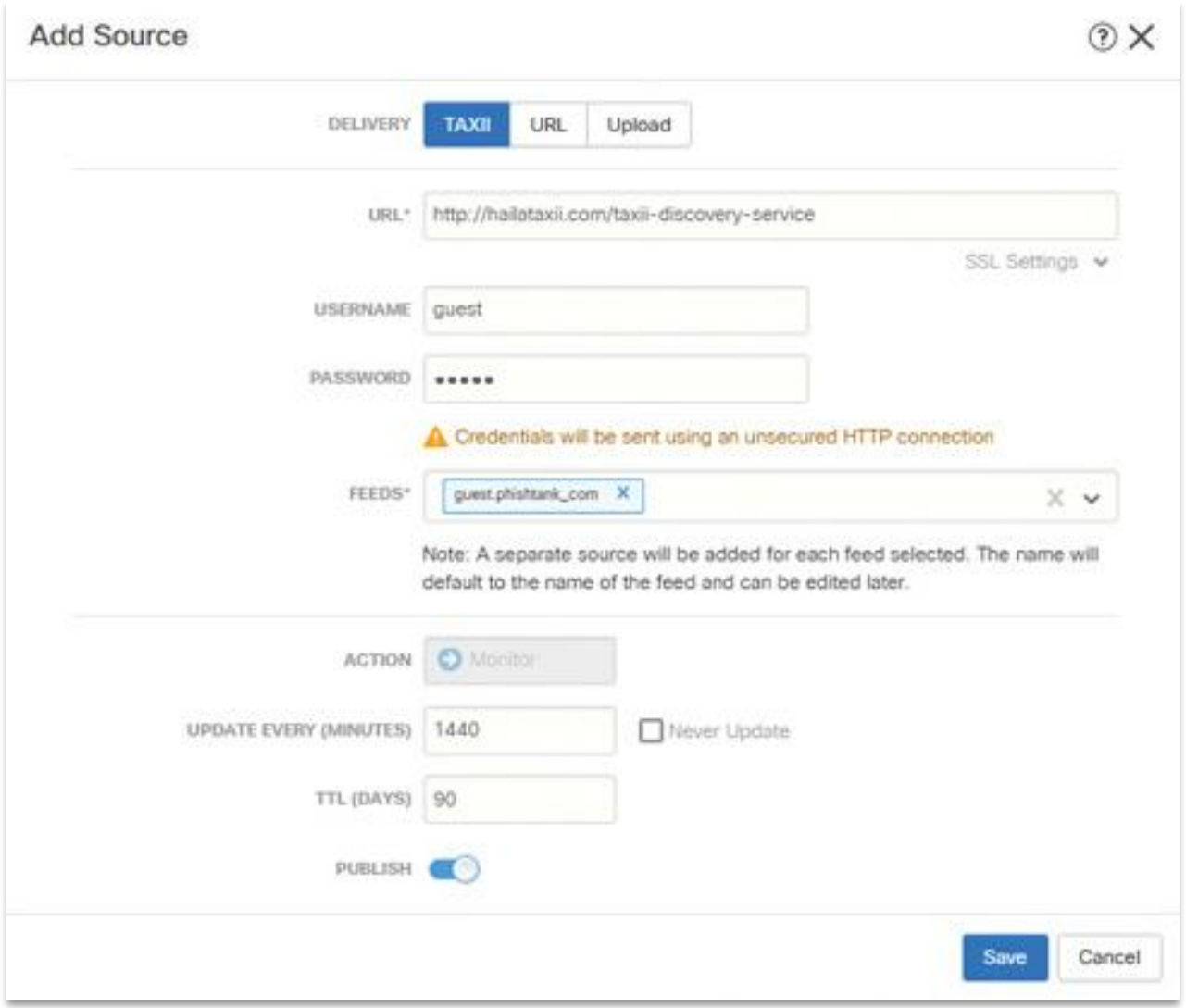
Threat Intelligence Director (TID)

Adding Sources and Importing Indicators

TAXII:

- You can import thousands of indicators in bulk from third-party source using the TAXII service.

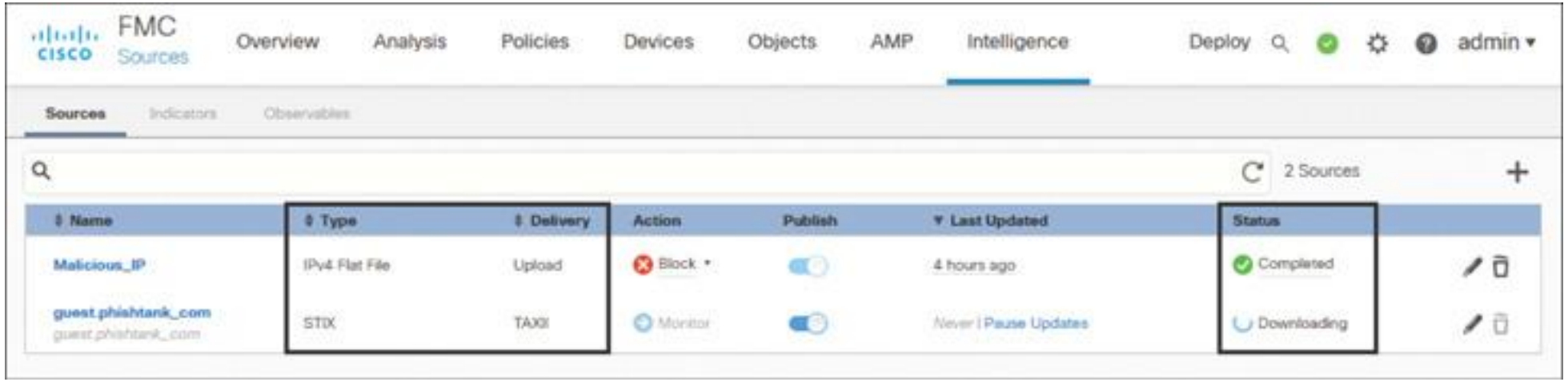
- Enter the URL of TAXII source
- Enter username and password of the URL



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.



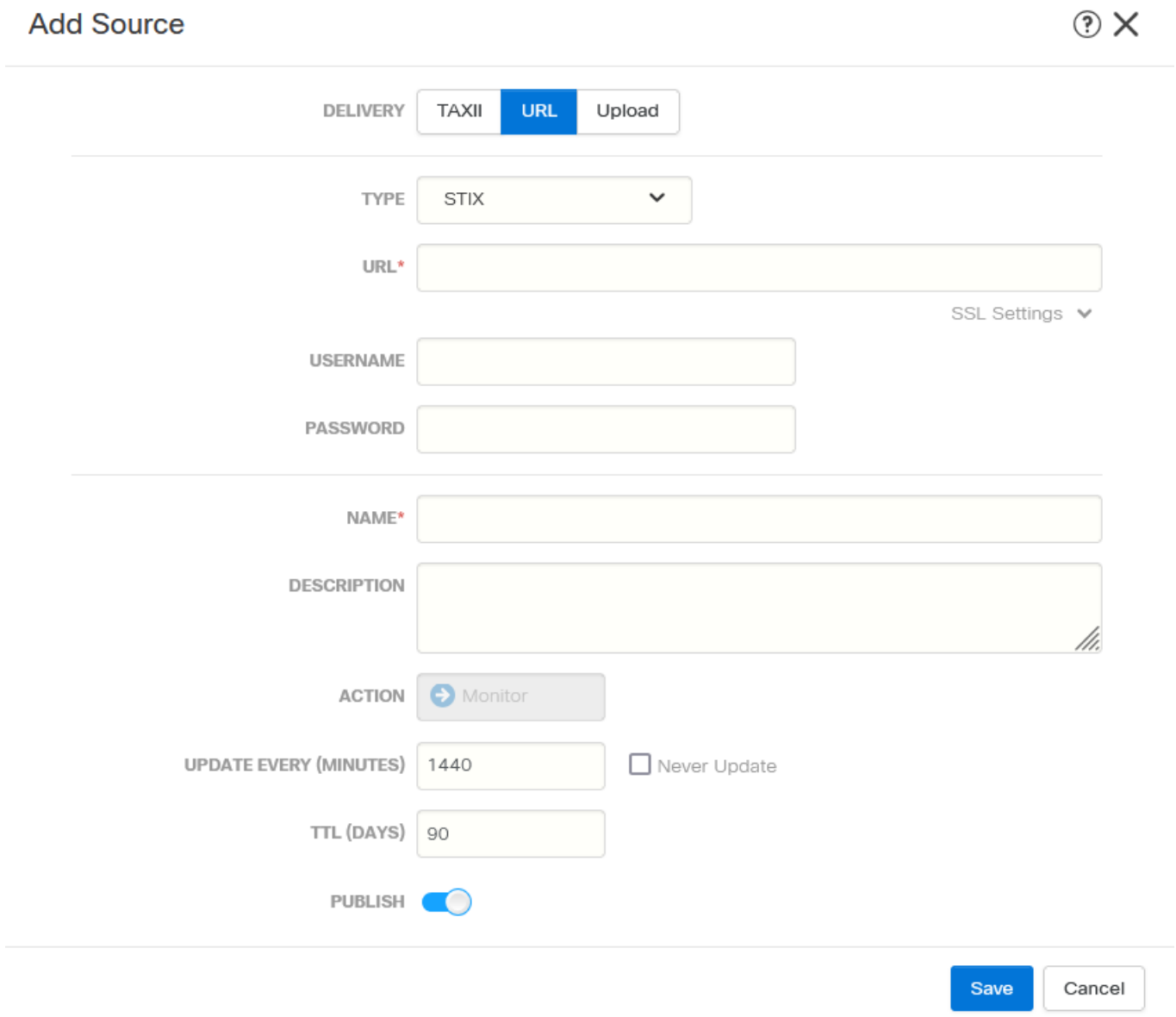
Downloading a STIX File Using the TAXII Service

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



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**