Securing Networks with

Cisco FTD

Chapter 12

URL Filtering

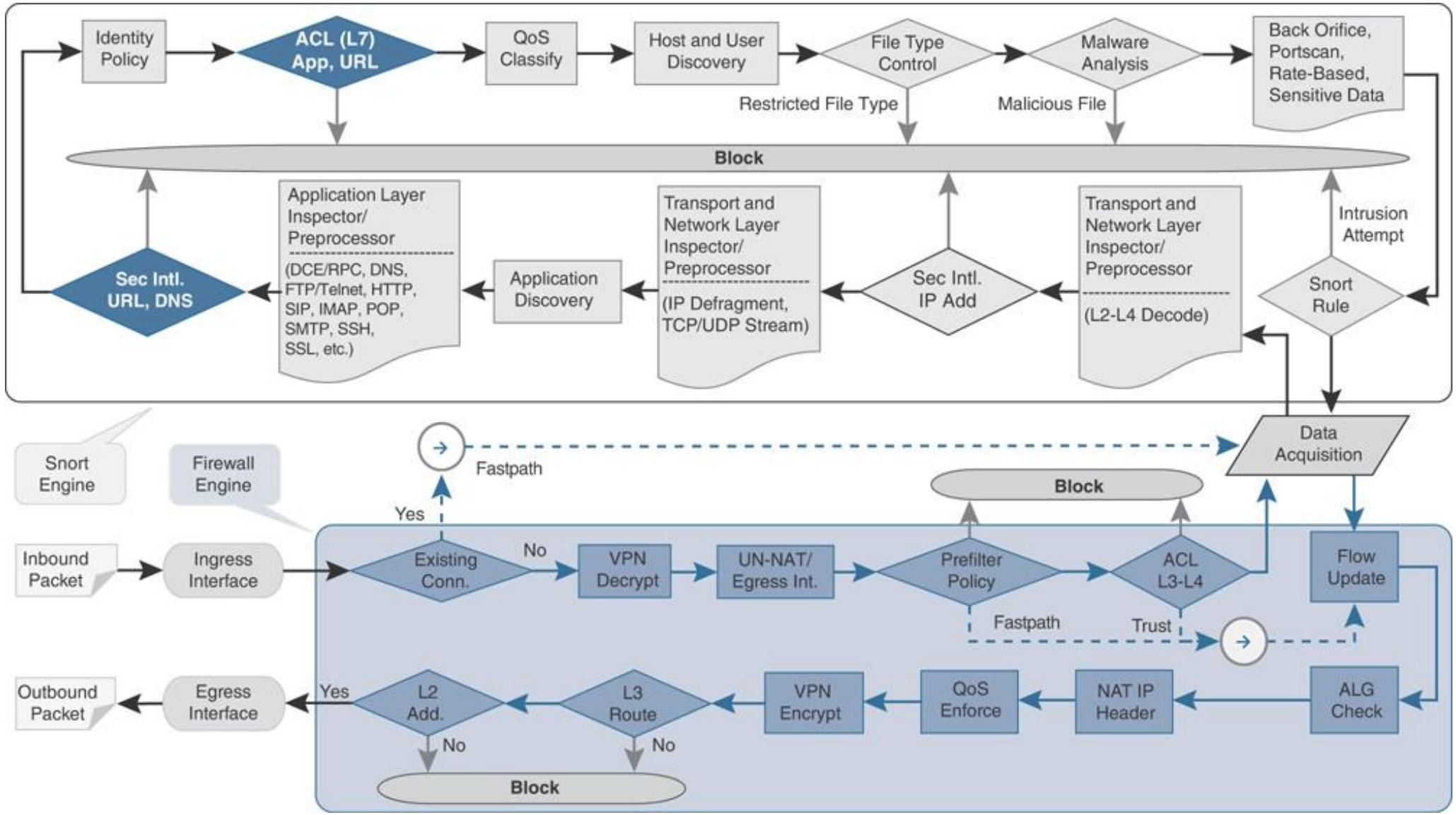
Mohsen Kheradmand

URL Filtering

- You can enable this feature to content. prevent your network hosts from accessing a specific type of URL
- Without manual changes to the access control rule , by dynamic policy
- You can use the FMC to download the URL database directly from the Cisco cloud
- The cloud categorize the URL database that maintains the Web Reputation Index (WRI)
- WRI calculated dynamically based on age and history of the site, reputation and location of the hosting IP address, and subject and context of the web
- Web Reputation Levels and Their Descriptions:

1)- Trusted (Well-known trustworthy)
2)- Favorable (Benign)
3)- Neutral (average with security risk)
4)- Questionable (Suspicious)
5)- Untrusted (High risk)

URL Filtering

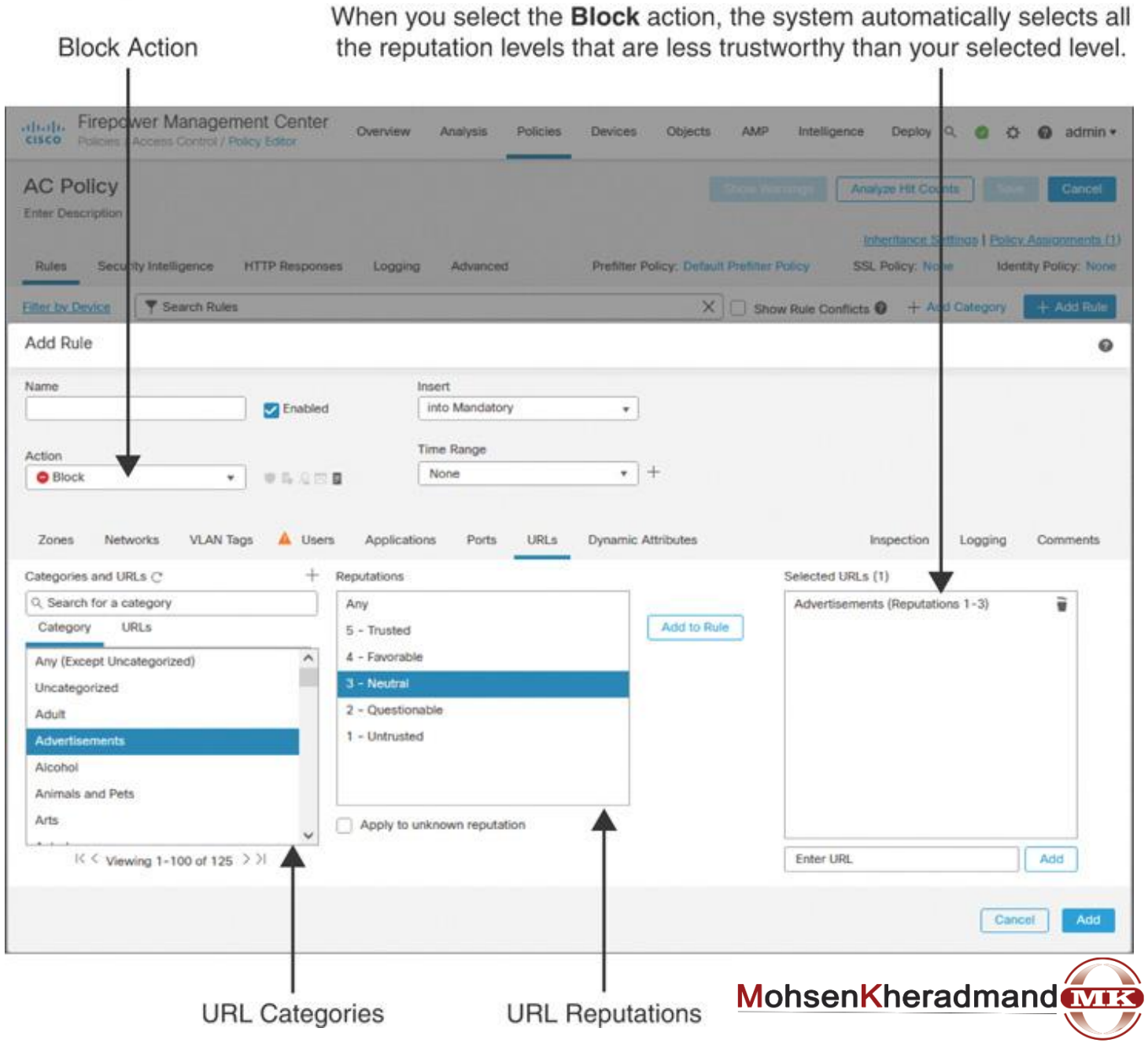


MohsenKheradmand

➢ URL Categories and Reputations in the ACP

- If you use Allow action for a certain reputation level the FMC allows that + all higher benign levels

- If you use Block action for a certain reputation level the FMC Blocks that + all higher riskier level

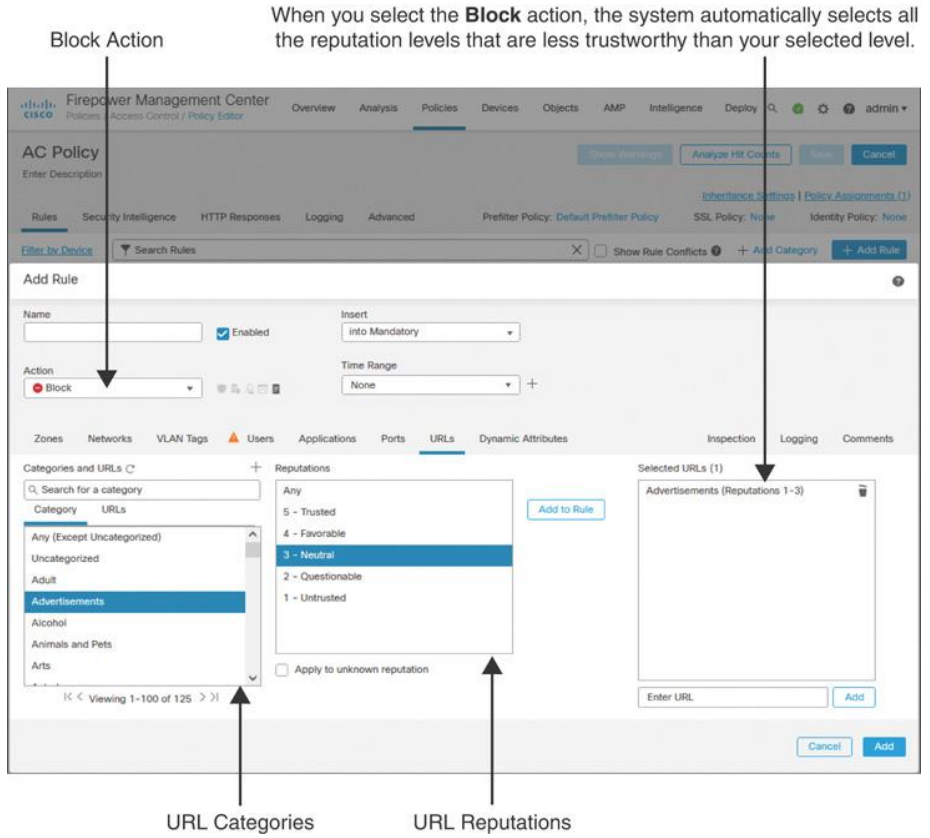


MohsenKheradmand MK

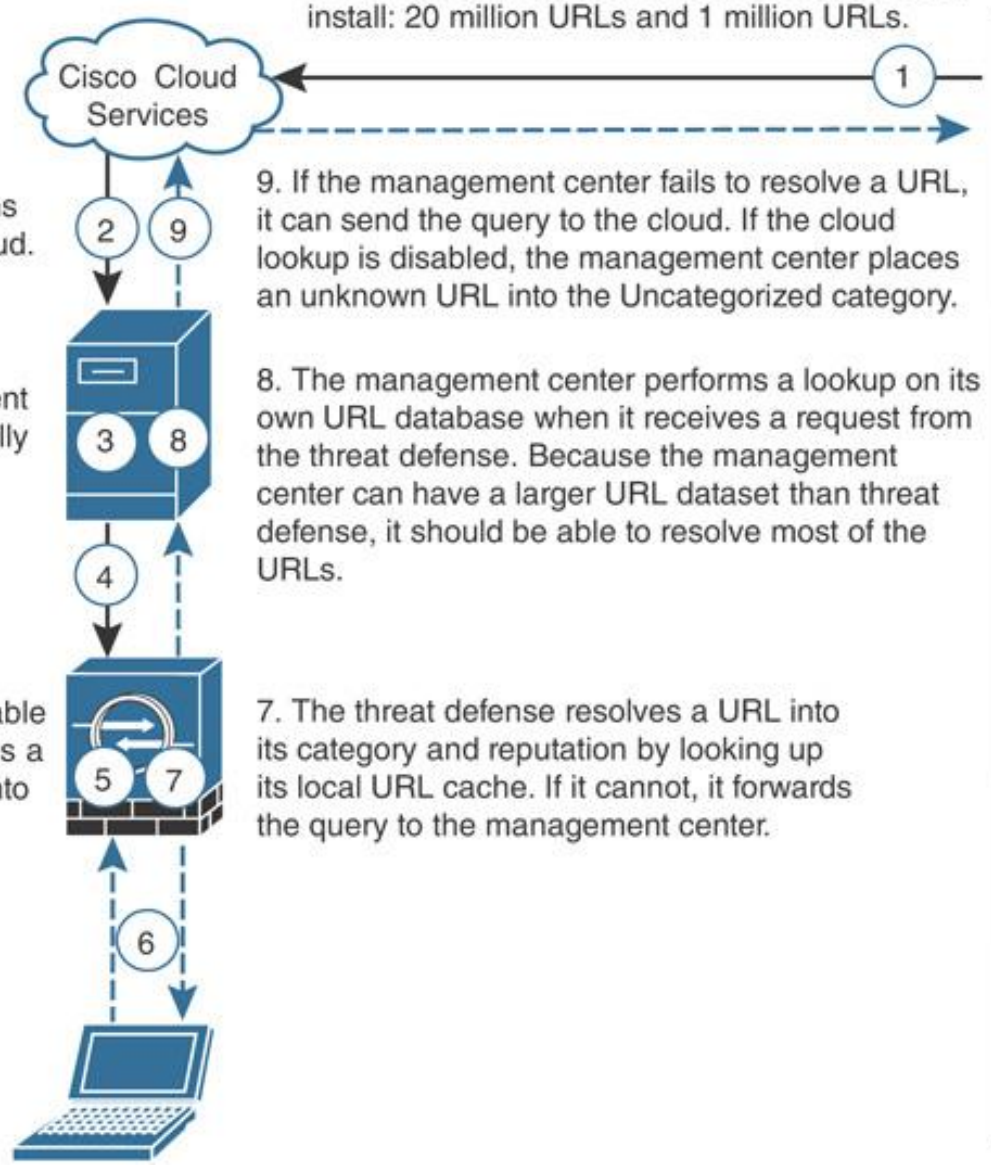
➢ URL Categories and Reputations in the ACP

- ➢ Firewall loads the URL dataset into its memory for a faster lookup
- ➢ The Cisco cloud publishes two types of datasets in a URL database:

Available Memory	Number of URLs in the Dataset
More than 3.4 GB	20 million URLs
Less than or equal to 3.4 GB	1 million URLs



➢ URL Database



1. Two types of datasets are published for local install: 20 million URLs and 1 million URLs.

2. The management center obtains a URL dataset from the Cisco cloud.

3. Depending on the size of available memory, the management center installs a URL dataset locally and loads it into its memory.

4. The management center disseminates the URL database updates to the threat defense.

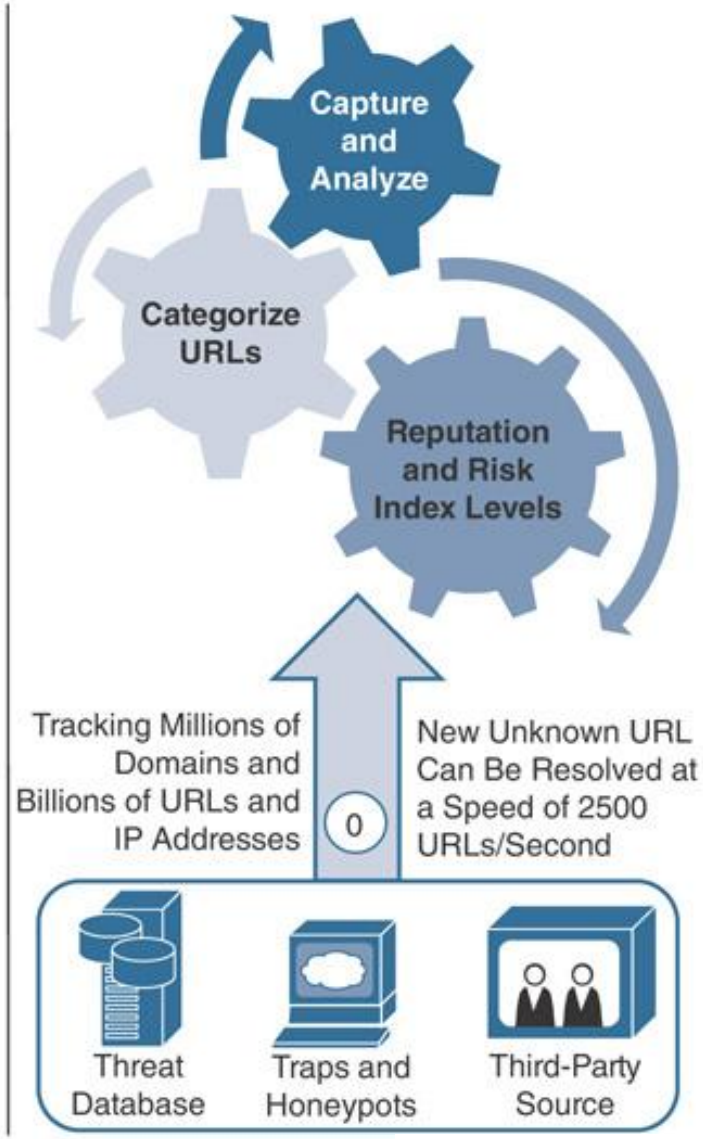
5. Depending on the size of available memory, the threat defense installs a URL dataset locally and loads it into its memory.

6. The threat defense inspects the end-user traffic and performs an immediate lookup on its local URL database.

7. The threat defense resolves a URL into its category and reputation by looking up its local URL cache. If it cannot, it forwards the query to the management center.

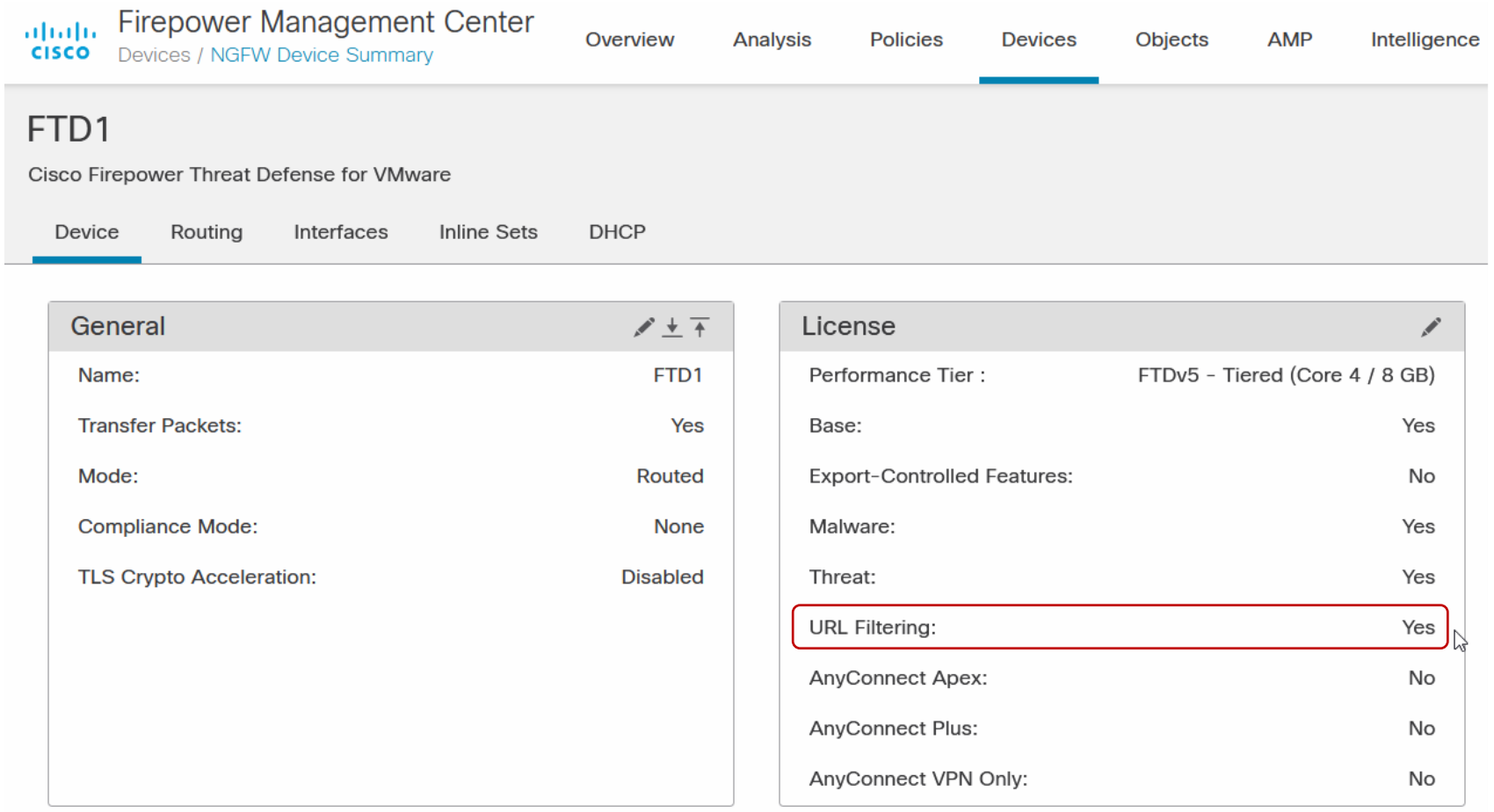
8. The management center performs a lookup on its own URL database when it receives a request from the threat defense. Because the management center can have a larger URL dataset than threat defense, it should be able to resolve most of the URLs.

9. If the management center fails to resolve a URL, it can send the query to the cloud. If the cloud lookup is disabled, the management center places an unknown URL into the Uncategorized category.



➢ Prerequisites:

- ✓ A URL Filtering license is necessary (the threat license is required before you enable URL Filtering.)

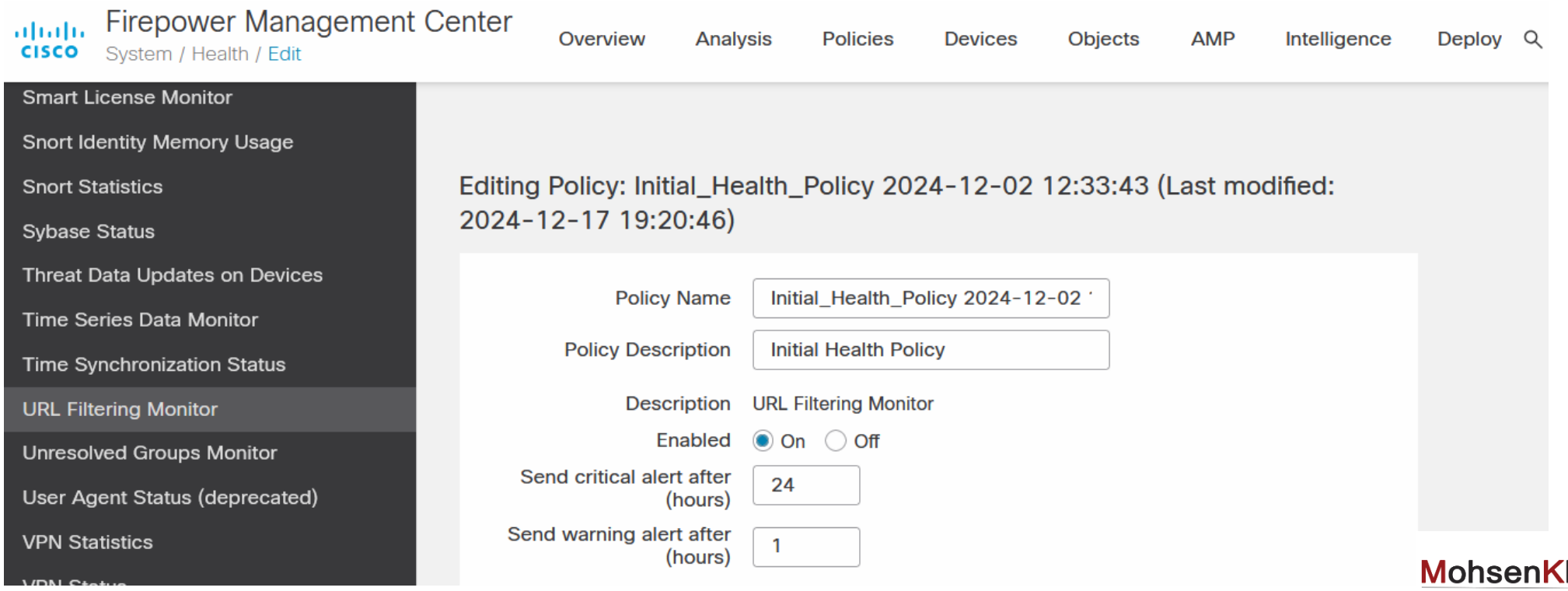


➢ Prerequisites:

Check whether the URL Filtering Monitor health module is enabled in the current health policy

This module enables the FMC to generate alerts if it fails to deploy a URL dataset to FTD or fails to download the latest URLs

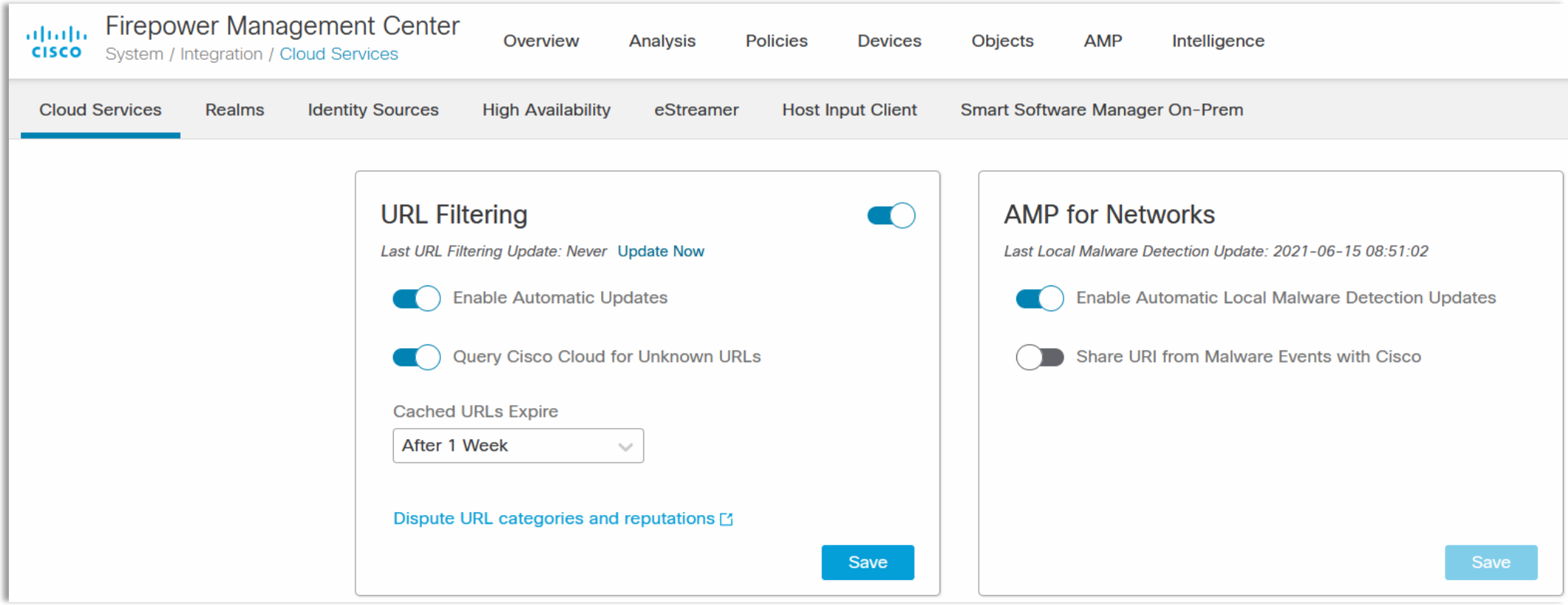
System > Health > Policy > select URL Filtering Monitor



➢ Prerequisites:

Make sure Cisco Cloud Services is enabled for URL Filtering

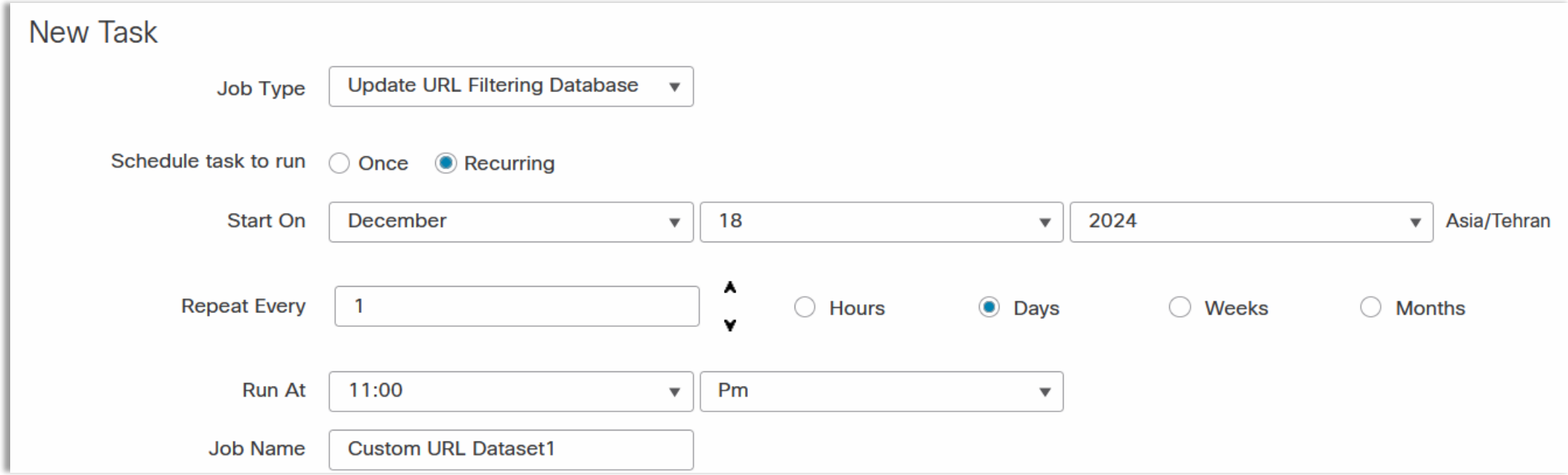
System > integration > Cloud services



➢ Prerequisites:

- The management center communicates with Cisco Cloud Services every 30 minutes
- But you can disable Automatic Update from Cloud service and create a scheduled task for URL database updates

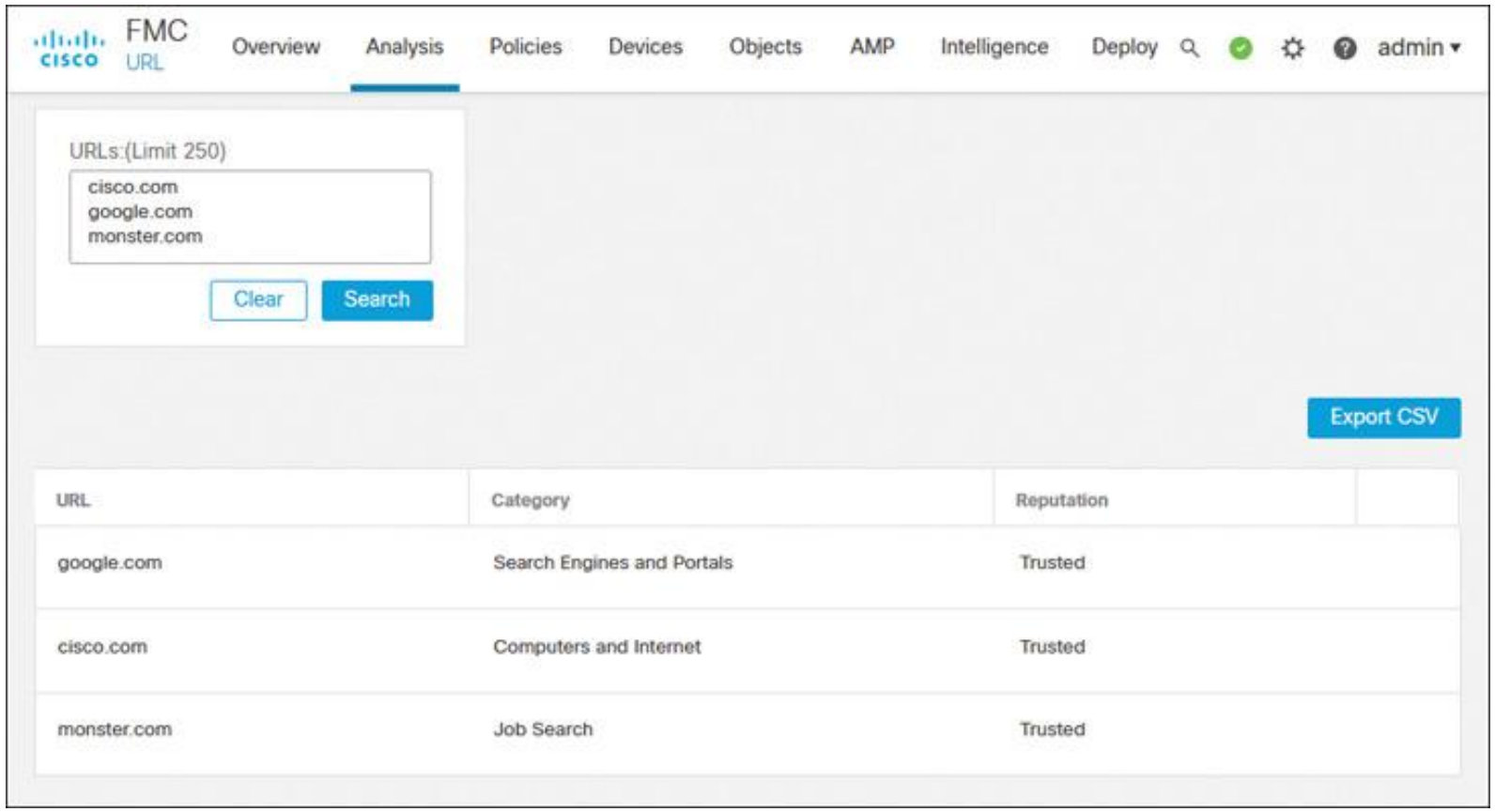
System > Tools > Scheduling > Add Task



➢ Prerequisites:

- If FTD blocks a connection during DNS resolution, a URL lookup for that connection is not necessary (improve performance)
- If you are not sure about unsure about the exact categories and reputations of any websites , you can search it :

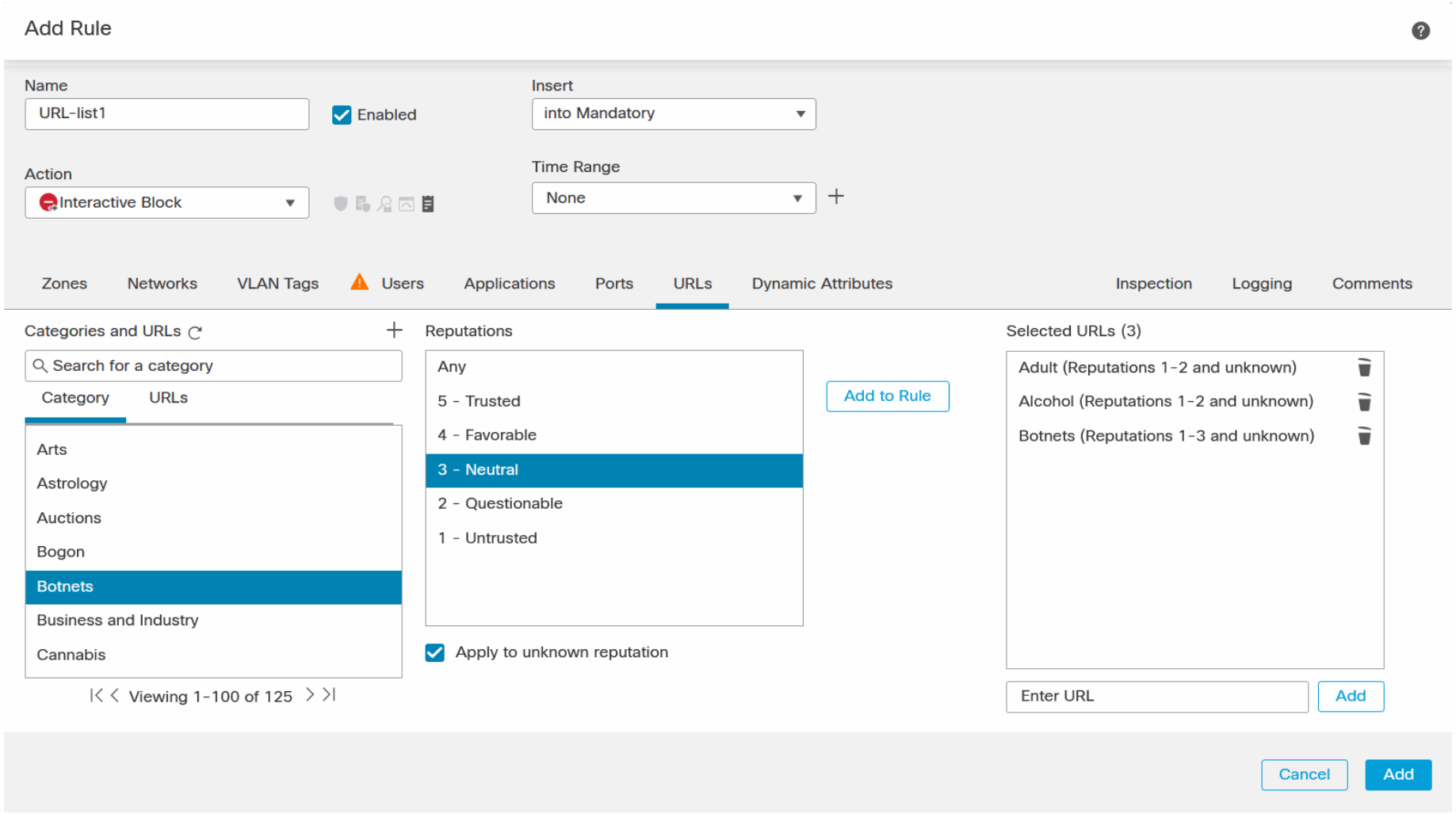
Analyze > Advanced > URL



➢ URL Filtering Configuration

- Blocking URLs of a certain category

➢ Policies > Access Control > Access Control > Add rule > URLs



MohsenKheradmand MK

- URL Filtering

  - Blocking U
  - Allowing a
  - Handling u