

Securing Networks with
Cisco FTD

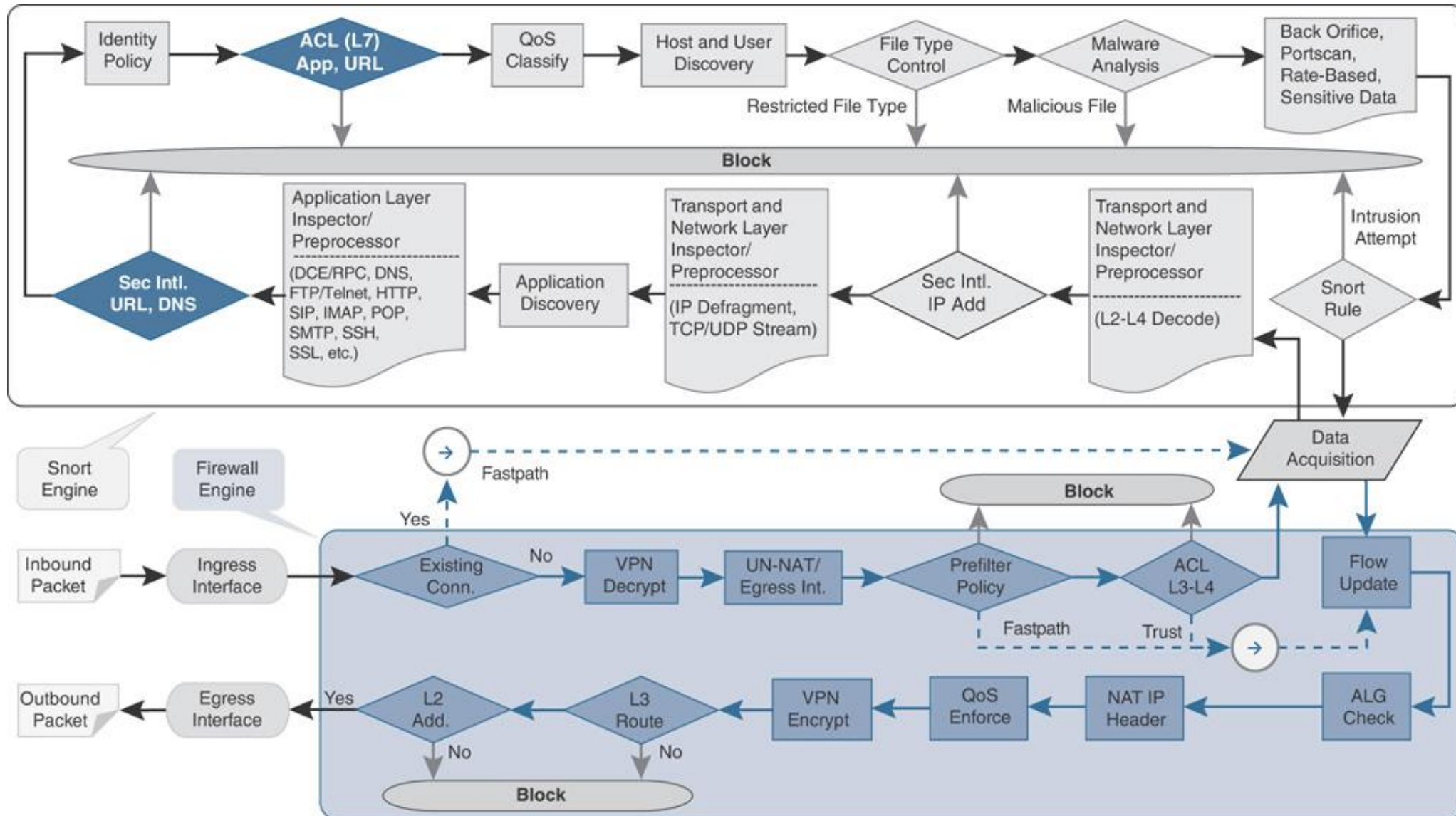
Chapter 12

URL Filtering

Mohsen Kheradmand

- 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



➤ 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

When you select the **Block** action, the system automatically selects all the reputation levels that are less trustworthy than your selected level.

Block Action

Firepower Management Center

Overview Analysis Policies Devices Objects AMP Intelligence Deploy

AC Policy

Enter Description

Rules Security Intelligence HTTP Responses Logging Advanced

Filter by Device Search Rules Show Rule Conflicts Add Category Add Rule

Add Rule

Name

Enabled

Action Block

Insert into Mandatory

Time Range None

Zones Networks VLAN Tags Users Applications Ports URLs Dynamic Attributes Inspection Logging Comments

Categories and URLs

Search for a category

Category URLs

Any (Except Uncategorized)

Uncategorized

Adult

Advertisements

Alcohol

Animals and Pets

Arts

Reputations

Any

5 - Trusted

4 - Favorable

3 - Neutral

2 - Questionable

1 - Untrusted

Apply to unknown reputation

Selected URLs (1)

Advertisements (Reputations 1-3)

Enter URL

Cancel Add

URL Categories

URL Reputations

➤ 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

When you select the **Block** action, the system automatically selects all the reputation levels that are less trustworthy than your selected level.

Block Action

URL Categories

URL Reputations

➤ URL Database

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.

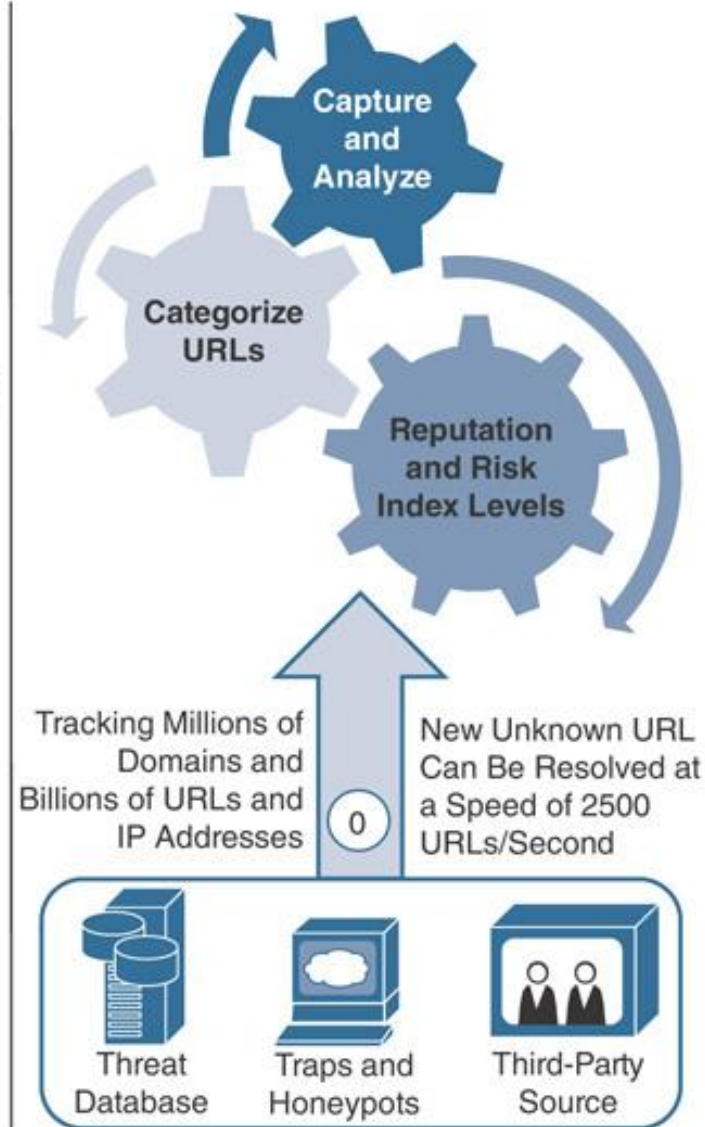
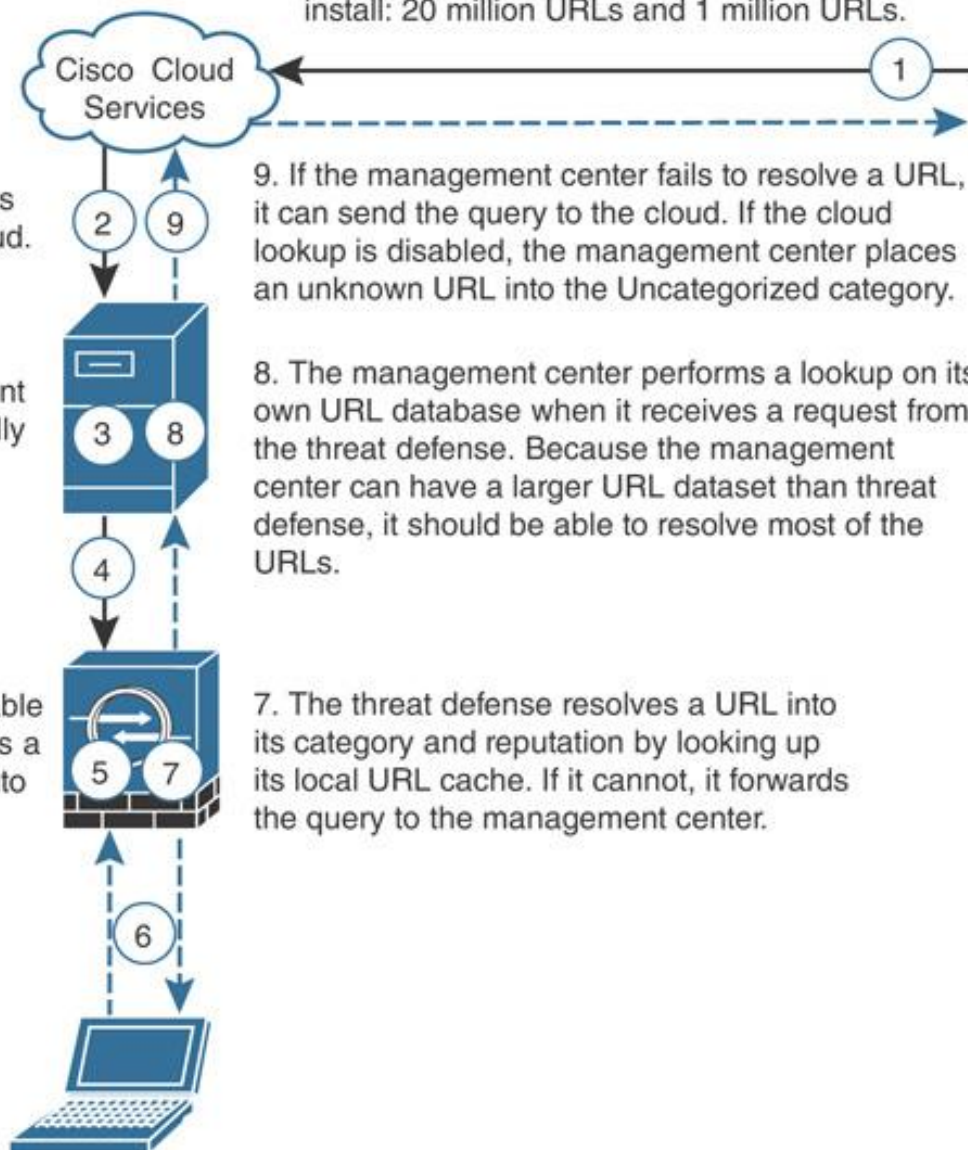
6. The threat defense inspects the end-user traffic and performs an immediate lookup on its local URL database.

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

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.

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.



➤ Prerequisites:

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

The screenshot displays the Cisco Firepower Management Center interface for configuring a device named FTD1. The 'Devices' tab is active in the top navigation bar. Below the device name, the 'Device' sub-tab is selected. The 'License' configuration panel is shown on the right, with the 'URL Filtering' option highlighted by a red rectangle, indicating it is enabled (Yes).

General	
Name:	FTD1
Transfer Packets:	Yes
Mode:	Routed
Compliance Mode:	None
TLS Crypto Acceleration:	Disabled

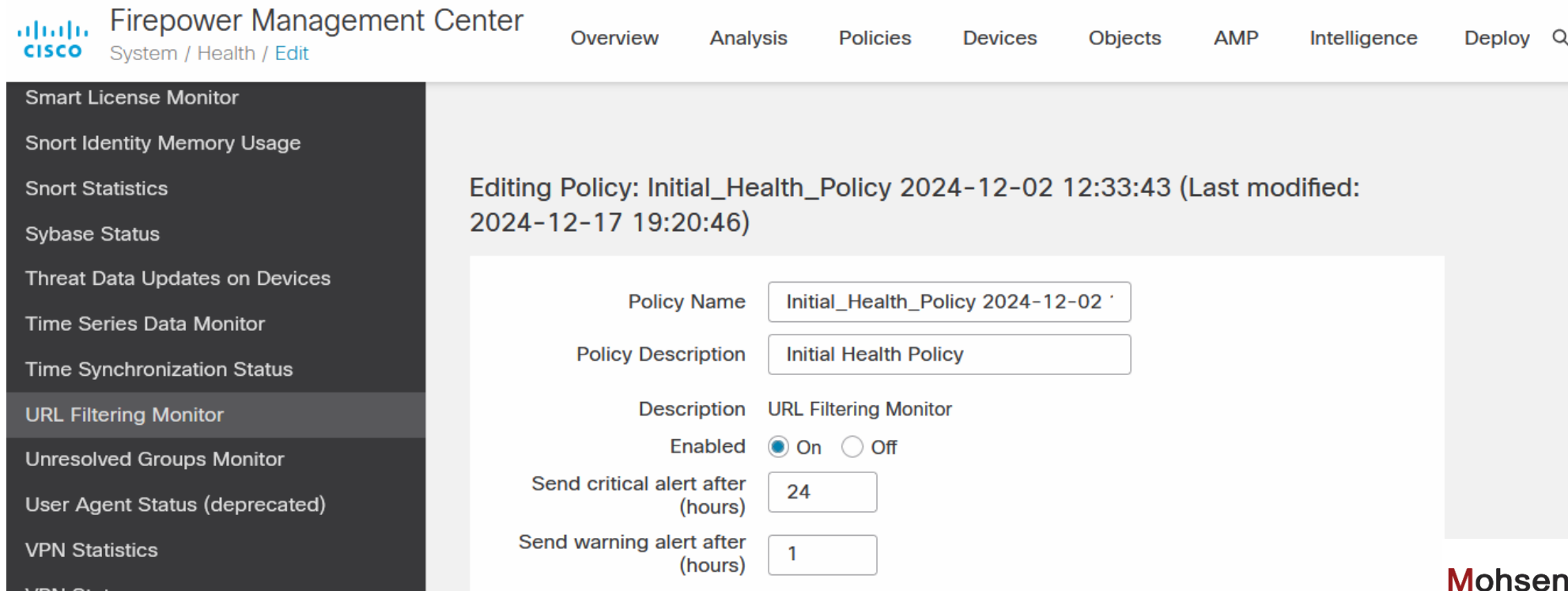
License	
Performance Tier :	FTDv5 - Tiered (Core 4 / 8 GB)
Base:	Yes
Export-Controlled Features:	No
Malware:	Yes
Threat:	Yes
URL Filtering:	Yes
AnyConnect Apex:	No
AnyConnect Plus:	No
AnyConnect VPN Only:	No

➤ 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



The screenshot shows the Cisco Firepower Management Center (FMC) interface. The top navigation bar includes the Cisco logo, the title "Firepower Management Center", and a breadcrumb trail "System / Health / Edit". The main navigation menu on the left lists various health modules, with "URL Filtering Monitor" selected and highlighted. The main content area displays the configuration for the "Initial_Health_Policy" (last modified: 2024-12-17 19:20:46). The configuration form includes fields for "Policy Name", "Policy Description", "Description", "Enabled" status, "Send critical alert after (hours)", and "Send warning alert after (hours)".

Field	Value
Policy Name	Initial_Health_Policy 2024-12-02
Policy Description	Initial Health Policy
Description	URL Filtering Monitor
Enabled	☒ On ☐ Off
Send critical alert after (hours)	24
Send warning alert after (hours)	1

➤ Prerequisites:

Make sure Cisco Cloud Services is enabled for URL Filtering

[System](#) > [integration](#) > [Cloud services](#)

The screenshot shows the Cisco Firepower Management Center interface. The top navigation bar includes the Cisco logo, the title 'Firepower Management Center', and a breadcrumb trail 'System / Integration / Cloud Services'. Below this is a secondary navigation bar with tabs: 'Cloud Services' (selected), 'Realms', 'Identity Sources', 'High Availability', 'eStreamer', 'Host Input Client', and 'Smart Software Manager On-Prem'. The main content area is divided into two panels. The left panel is titled 'URL Filtering' and has a toggle switch that is turned on. Below the title, it shows 'Last URL Filtering Update: Never' with a link to 'Update Now'. There are two toggle switches: 'Enable Automatic Updates' (turned on) and 'Query Cisco Cloud for Unknown URLs' (turned on). Below these is a dropdown menu for 'Cached URLs Expire' set to 'After 1 Week'. At the bottom of the panel is a link 'Dispute URL categories and reputations' with an external link icon, and a 'Save' button. The right panel is titled 'AMP for Networks' and shows 'Last Local Malware Detection Update: 2021-06-15 08:51:02'. It has two toggle switches: 'Enable Automatic Local Malware Detection Updates' (turned on) and 'Share URI from Malware Events with Cisco' (turned off). At the bottom of the panel is a 'Save' button.

Firepower Management Center
System / Integration / Cloud Services

Overview Analysis Policies Devices Objects AMP Intelligence

Cloud Services Realms Identity Sources High Availability eStreamer Host Input Client Smart Software Manager On-Prem

URL Filtering

Last URL Filtering Update: Never [Update Now](#)

☒ Enable Automatic Updates

☒ Query Cisco Cloud for Unknown URLs

Cached URLs Expire
After 1 Week

[Dispute URL categories and reputations](#)

Save

AMP for Networks

Last Local Malware Detection Update: 2021-06-15 08:51:02

☒ Enable Automatic Local Malware Detection Updates

☐ Share URI from Malware Events with Cisco

Save

➤ 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](#)

New Task

Job Type Update URL Filtering Database ▼

Schedule task to run ☐ Once ☒ Recurring

Start On December ▼ 18 ▼ 2024 ▼ Asia/Tehran

Repeat Every 1 ▼ ▲ ▼ ☐ Hours ☒ Days ☐ Weeks ☐ Months

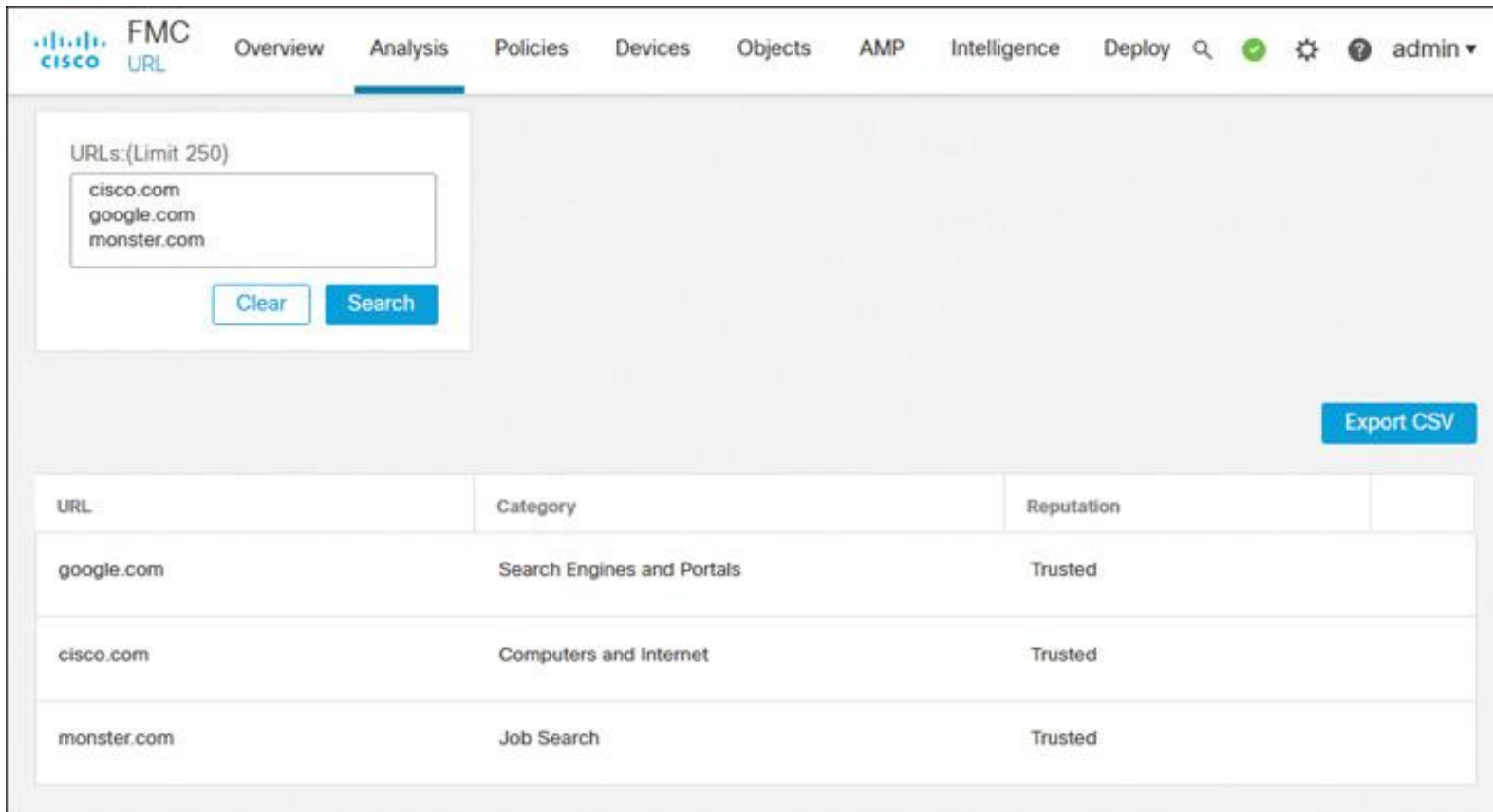
Run At 11:00 ▼ Pm ▼

Job Name Custom URL Dataset1

➤ 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 the exact categories and reputations of any websites , you can search it :

[Analyze > Advanced > URL](#)



The screenshot shows the Cisco FMC URL Filtering interface. The top navigation bar includes tabs for Overview, Analysis (selected), Policies, Devices, Objects, AMP, Intelligence, and Deploy. A search bar and user profile (admin) are also visible. The main content area has a search box labeled "URLs:(Limit 250)" containing "cisco.com", "google.com", and "monster.com". Below the search box are "Clear" and "Search" buttons. An "Export CSV" button is located on the right. The results are displayed in a table with columns for URL, Category, and Reputation.

URL	Category	Reputation
google.com	Search Engines and Portals	Trusted
cisco.com	Computers and Internet	Trusted
monster.com	Job Search	Trusted

➤ URL Filtering Configuration

- Blocking URLs of a certain category

➤ Policies > Access Control > Access Control > Add rule > URLs

Add Rule ?

Name: ☒ Enabled Insert:

Action: Time Range: +

Zones Networks VLAN Tags **Users** Applications Ports URLs Dynamic Attributes Inspection Logging Comments

Categories and URLs + Reputations

Category	URLs
Arts	
Astrology	
Auctions	
Bogon	
Botnets	
Business and Industry	
Cannabis	

Any
5 - Trusted
4 - Favorable
3 - Neutral
2 - Questionable
1 - Untrusted

☒ Apply to unknown reputation

Add to Rule

Selected URLs (3)

- Adult (Reputations 1-2 and unknown)
- Alcohol (Reputations 1-2 and unknown)
- Botnets (Reputations 1-3 and unknown)

Enter URL

Cancel Add

➤ URL Filtering

- Blocking U
- Allowing a
- Handling

Blocking the "Job Search" URL Category

Connection Events (switch workflow)

Search Constraints (Edit Search)

Connections with Application Details Table View of Connection Events

Jump to...

		Action ×	Source Port / ICMP Type ×	Destination Port / ICMP Code ×	URL ×	URL Category ×	URL Reputation ×	Access Control Rule ×	
▼	☐	2020-12-12 10:44:11	Block	9620 / tcp	443 (https) / tcp	https://www.dice.com	Job Search	Trusted	Job Search Rule
▼	☐	2020-12-12 10:44:08	Block	9619 / tcp	443 (https) / tcp	https://www.monster.com	Job Search	Trusted	Job Search Rule
▼	☐	2020-12-12 10:44:05	Allow	9609 / tcp	443 (https) / tcp	https://www.google.com	Search Engines and Portals	Trusted	Default Action

Page 1 of 1 >> | << | Displaying rows 1-3 of 3 rows

View View All

Allowing the General "Search Engines" Category