Securing Networks with

Cisco FTD

Chapter 7

Network Discovery Policy

Mohsen Kheradmand

Network Discovery Operations

- FTD can control an application when a monitored connection is established between a client and server, and the application in a session is identified
- To identify an application, the threat defense has to analyze the first few packets in a session
- Until the identification is complete , threat defense inspects those early packets , using the default intrusion policy
- Then, the FTD can act on the rest of the session traffic based on the access control rule on application filtering condition

Two separate stage of Application visibility and control (AVC) :

- Application discovery
- Host and user discovery

- The FTD first inspect the traffic by the *IP-based security intelligence* , then start *application discovery rules*
- The URL- and DNS-based security intelligence component can act after its underlying application is discovered

Application Detectors

- A network discovery policy enables Secure Firewall to discover applications, hosts, and users in a network
- Secure Firewall uses *application detectors* to identify the network applications running on a monitored network

There are mainly two sources for detectors:

System-provided detectors

- Cisco provides the latest detectors in a separate software package, called the Vulnerability Database (VDB)
- The VDB contains the fingerprints of various applications, operating systems, and client software
- VDB keeps a record of the known vulnerabilities.
- By VDB , firewall correlates the application with any known vulnerabilities to determine its impact

User-created detectors

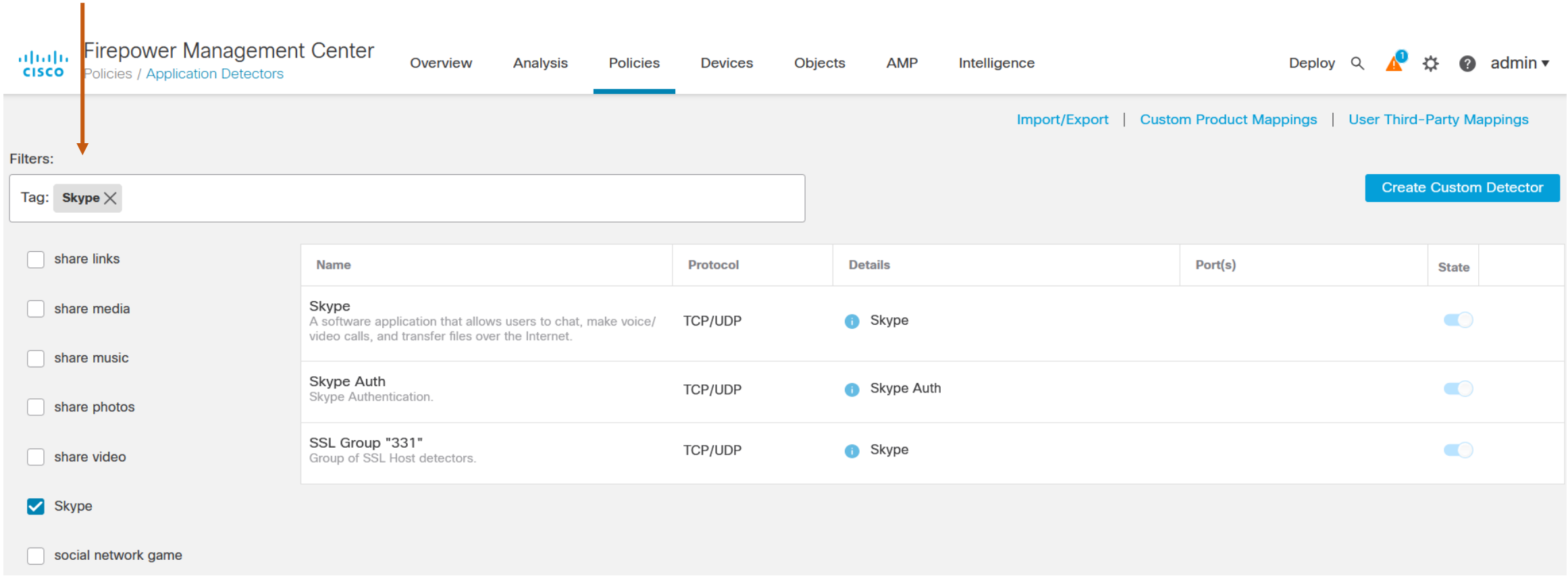
- You can create your own detectors based on patterns you notice on custom applications

Types of Application Detector

Internal detector	Detects protocol, client, and web applications. Internal detectors are always turned on; they are built in the software
Client detector	Detects client traffic. It also helps to infer an application protocol on a nonmonitored network
Web application detector	Detects traffic based on the contents in a payload of HTTP traffic
Port-based application protocol detector	Detects traffic based on well-known ports.
Fingerprint-based application protocol detector	Detects traffic based on application fingerprints
Custom application detector	Detects traffic based on user-defined patterns

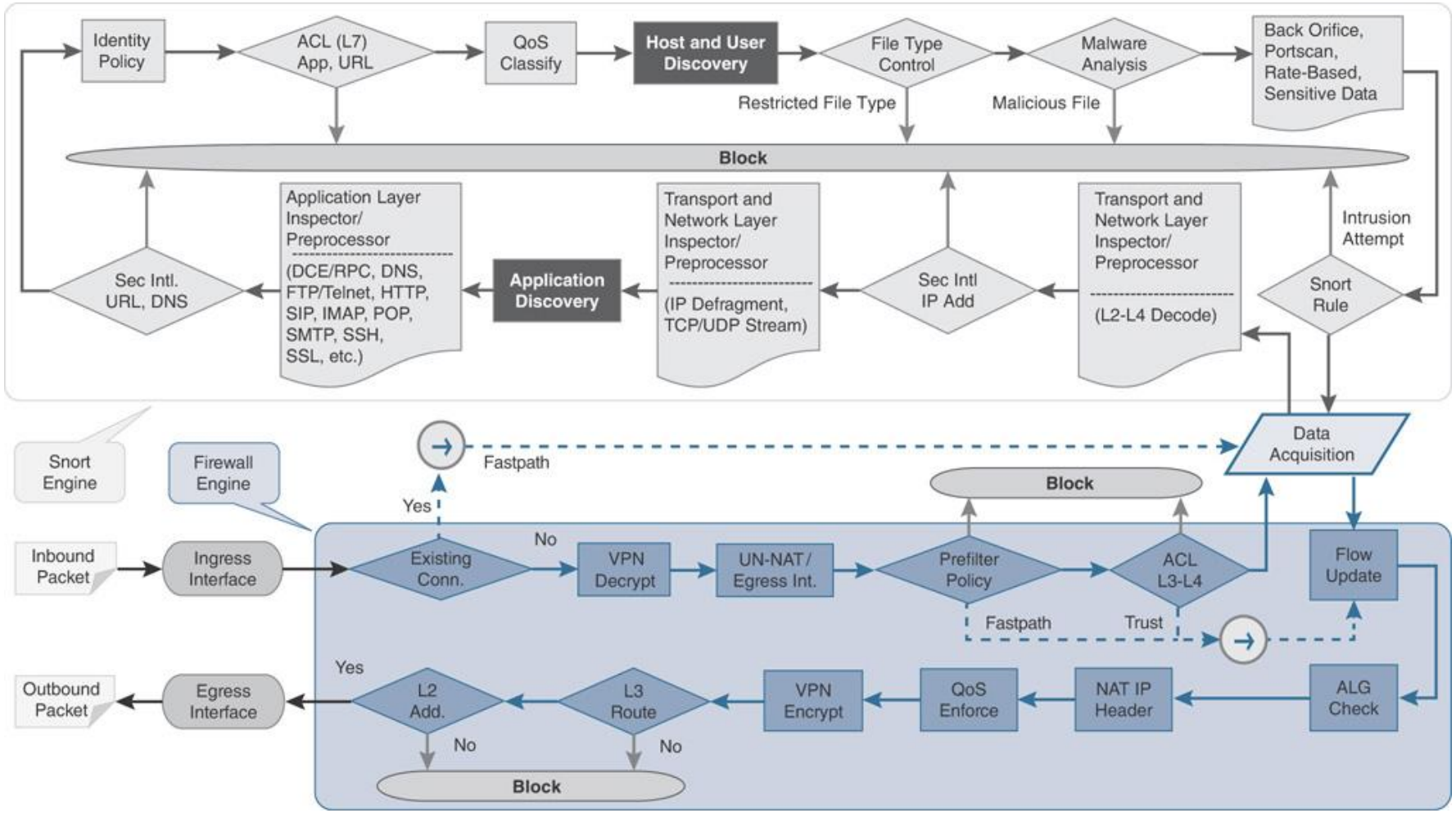
Policies > Application Detectors

- Search for Detectors that are related to Skype application



Network Discovery Operations

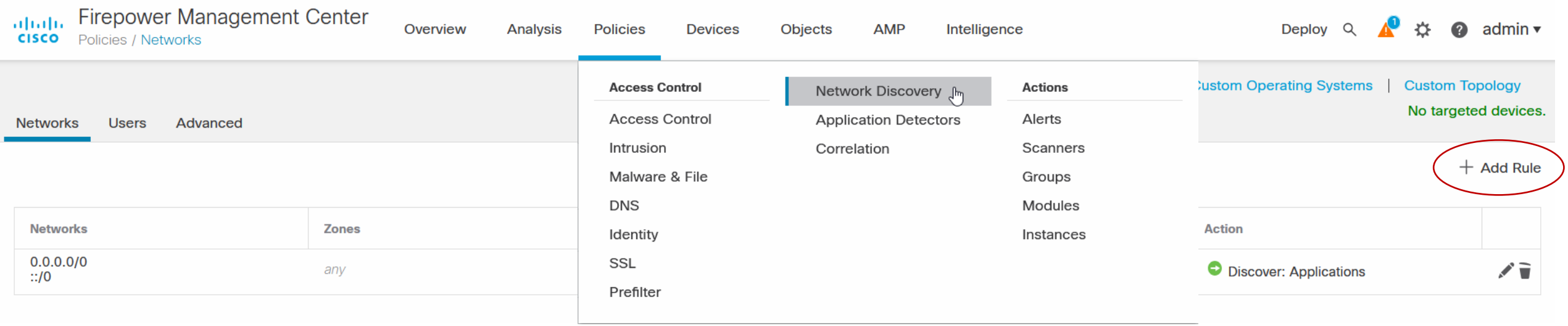
Processing of Packets by Various Components of Security Engines



MohsenKheradmand MK

Configurations

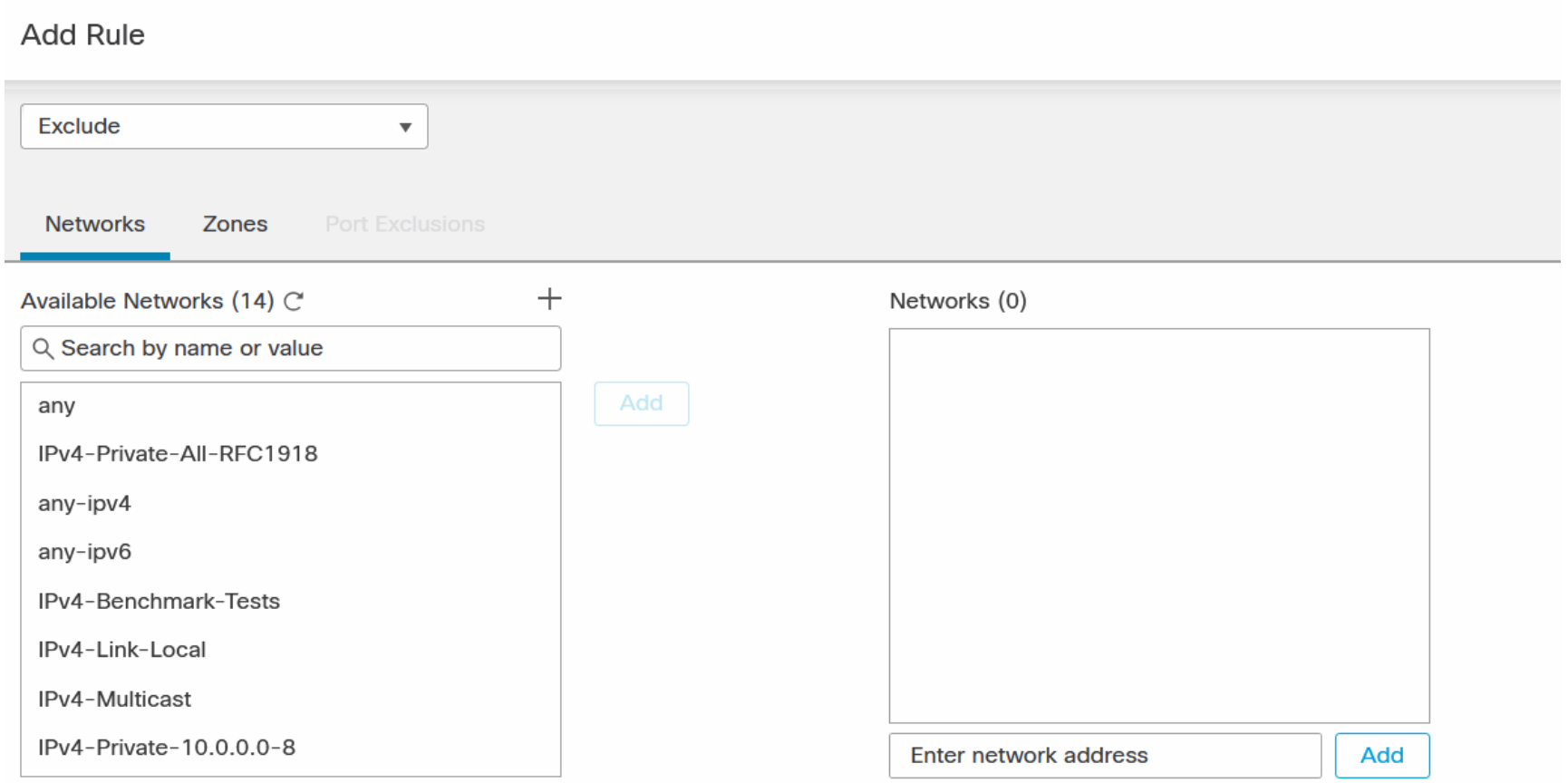
- Policies / Network Discovery
  - The default rule enable a Secure Firewall to discover applications from any observed networks
  - Don’t change it because Snort leverages this application discovery data for intrusion detection



- Click Add Rule to create new rule

Configurations

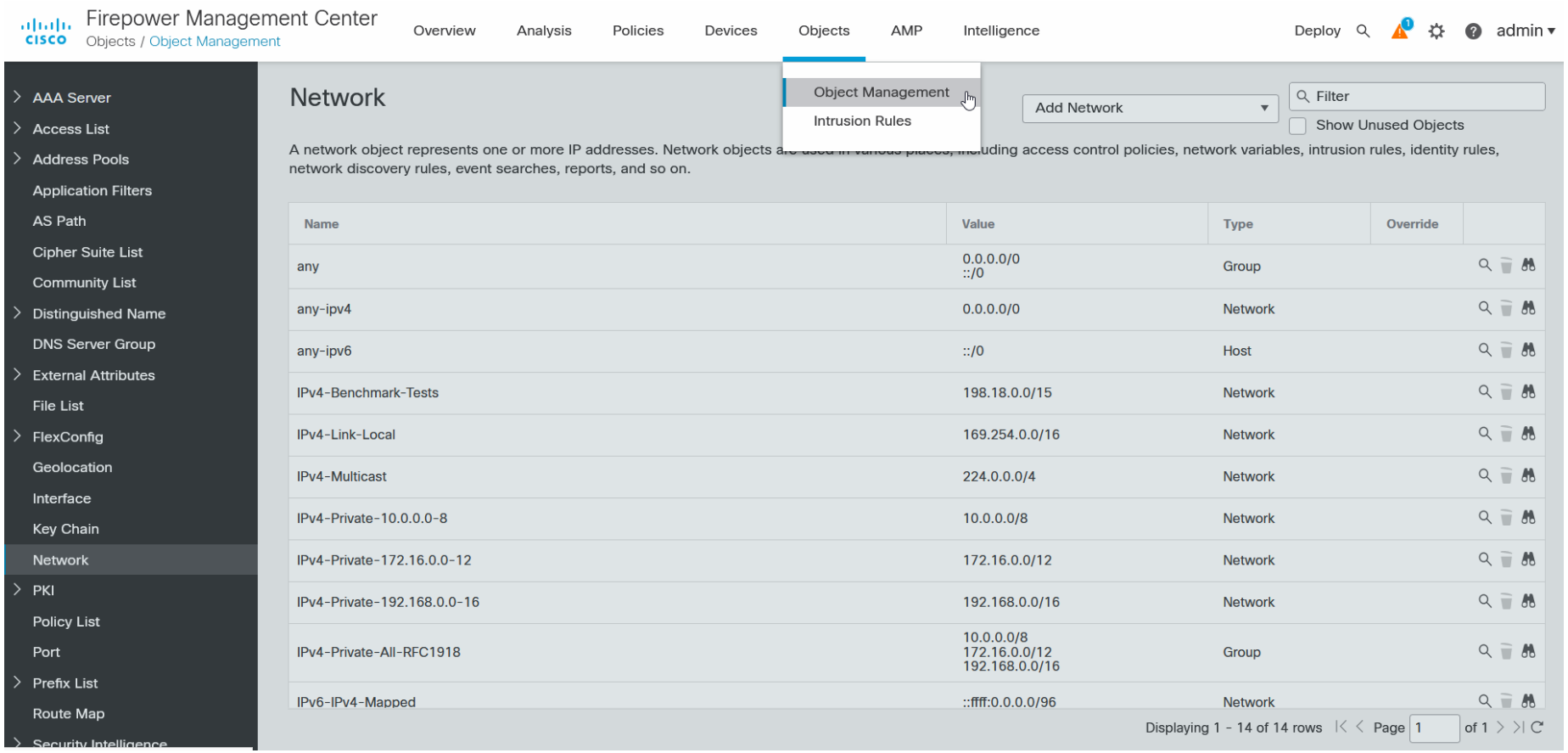
- First, add a rule to exclude the IP address of any intermediate NAT and load-balancing devices.
- To do that, select the Exclude action from the drop-down, and then select a network object



Configurations

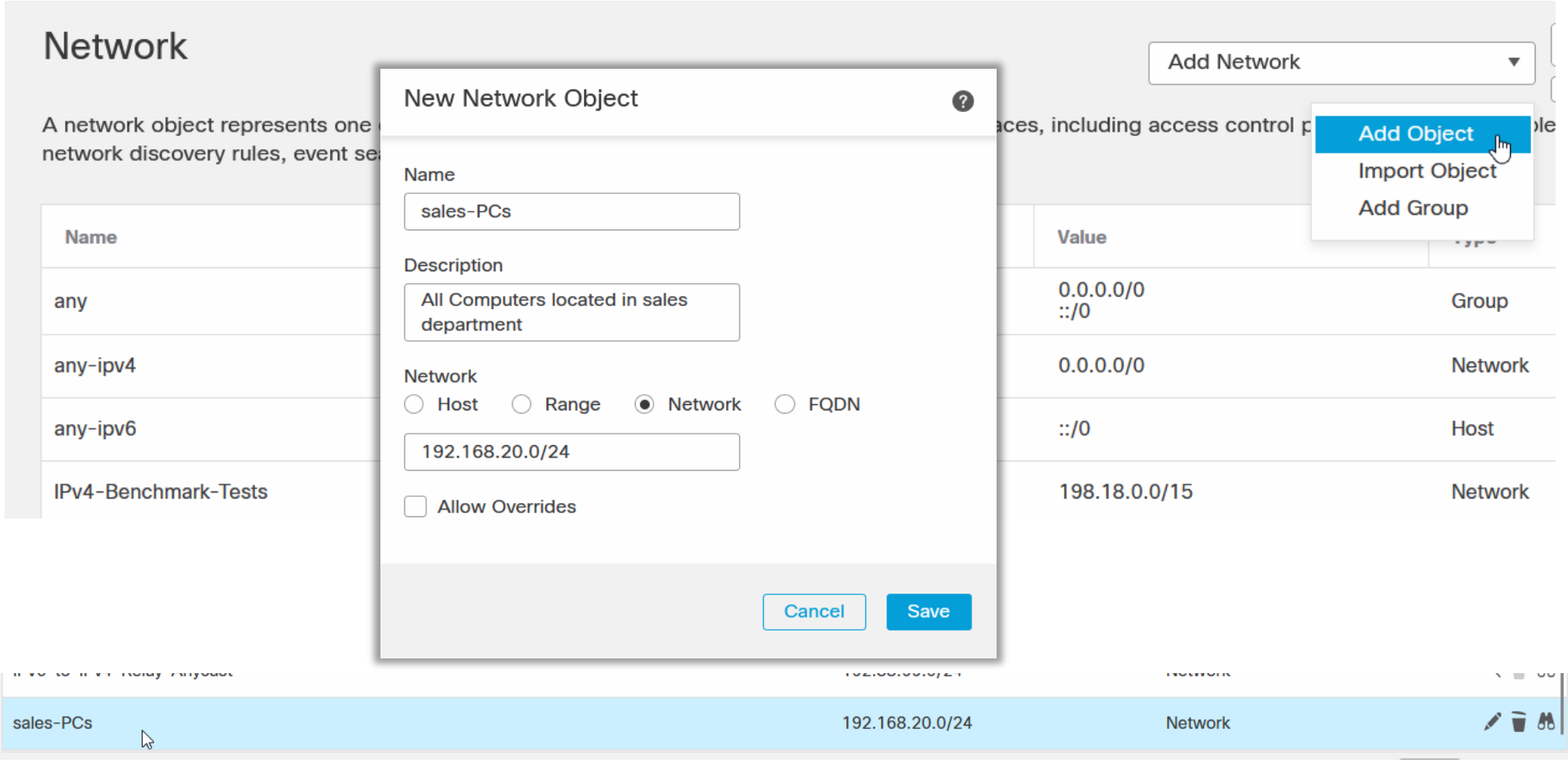
Reusable Objects

- You can create named objects for network addresses, port numbers, interfaces, VLAN tags, URLs, time ranges, access lists, and many more variable
- You can also group multiple objects into a single configuration, which is called an object group



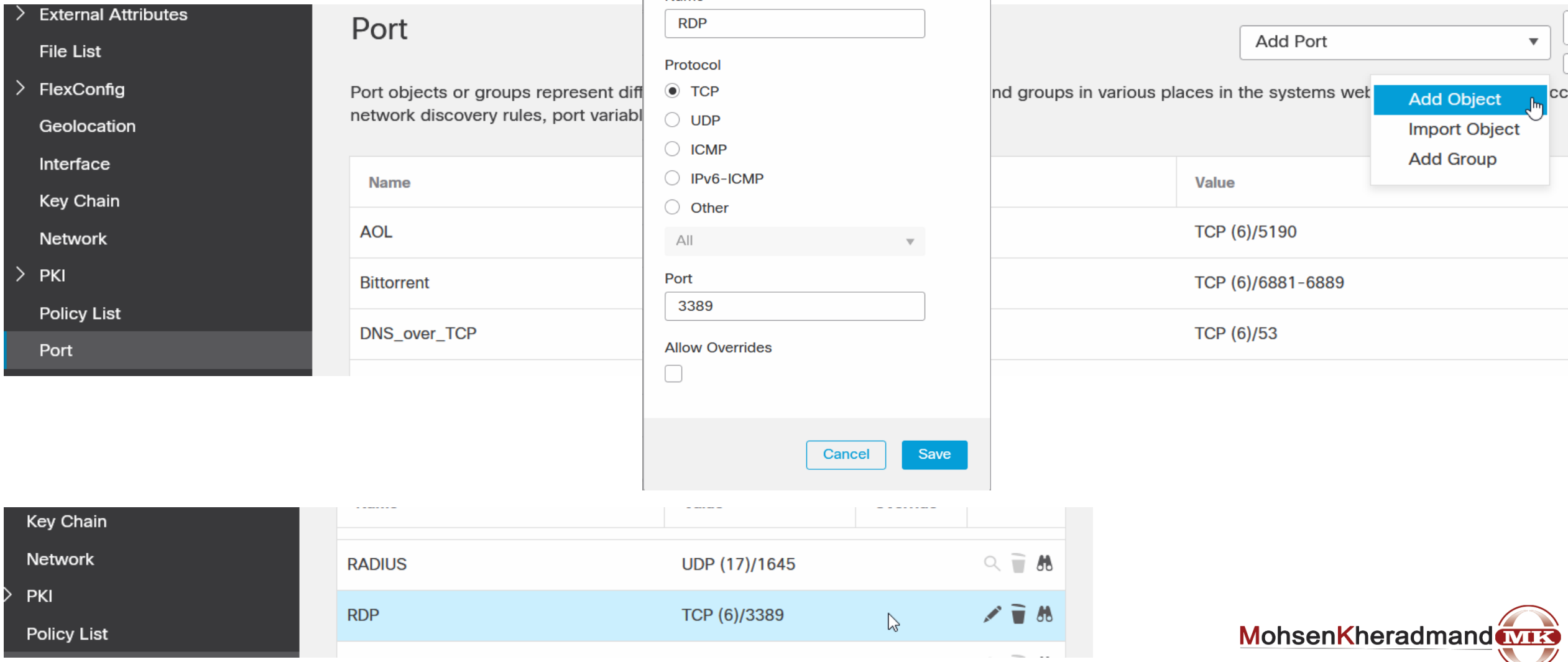
Configurations

Reusable Objects



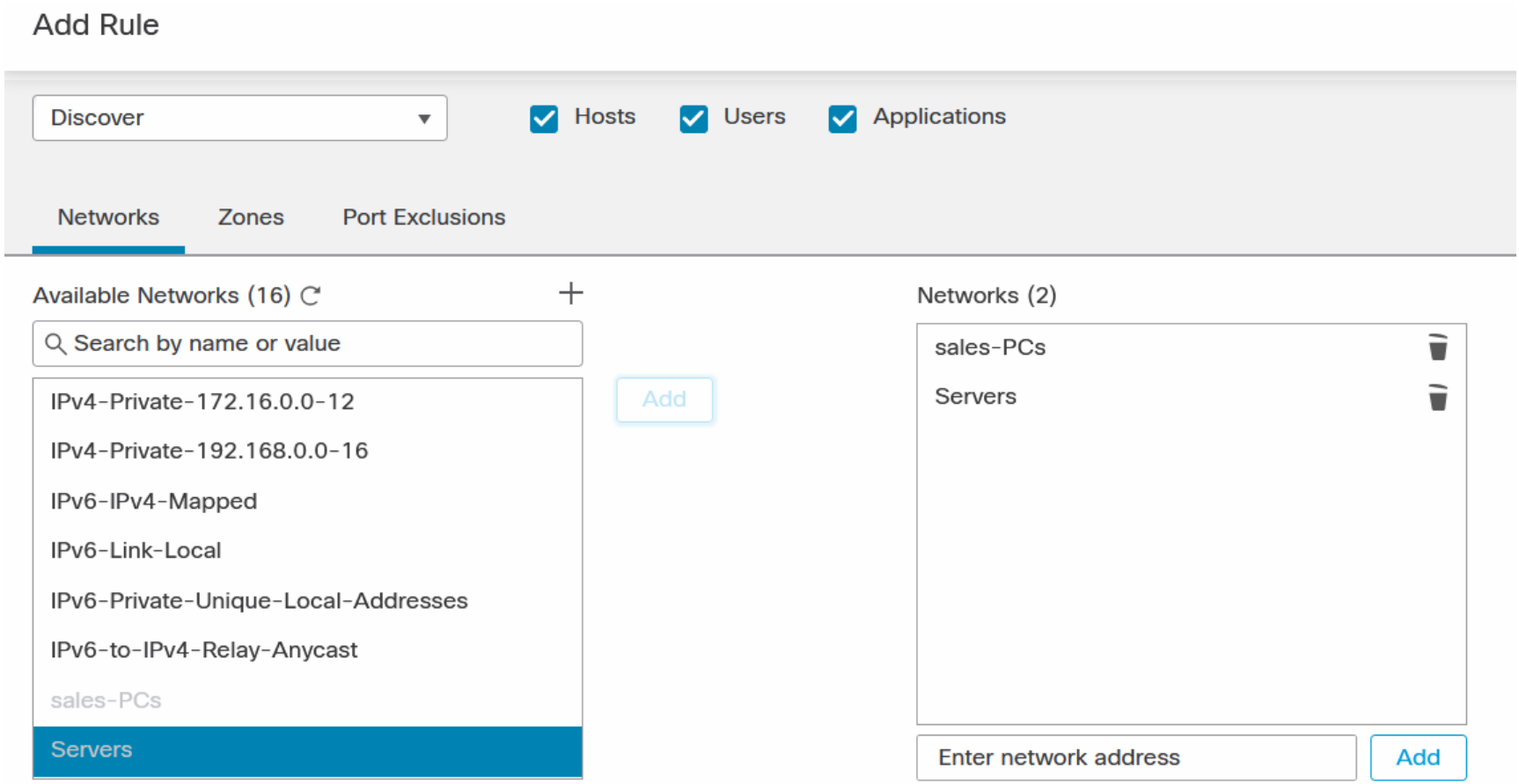
Configurations

Reusable Objects



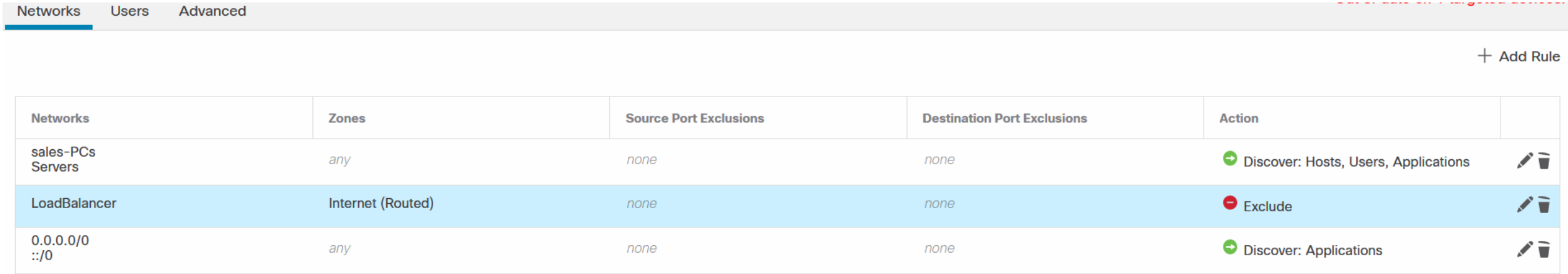
Configurations

1) Click the Add Rule button again
2) Select the Discover action
3) Enable Hosts, Users, and Applications
4) Add the desired network objects
5) Optionally select by zones
6) Optionally excludes non-desired ports
7) Click the Save button
8) deploy the network discovery policy on your threat defense.



Configurations

1) The result will be showed and you can deploy or edit each one of them to FTDs



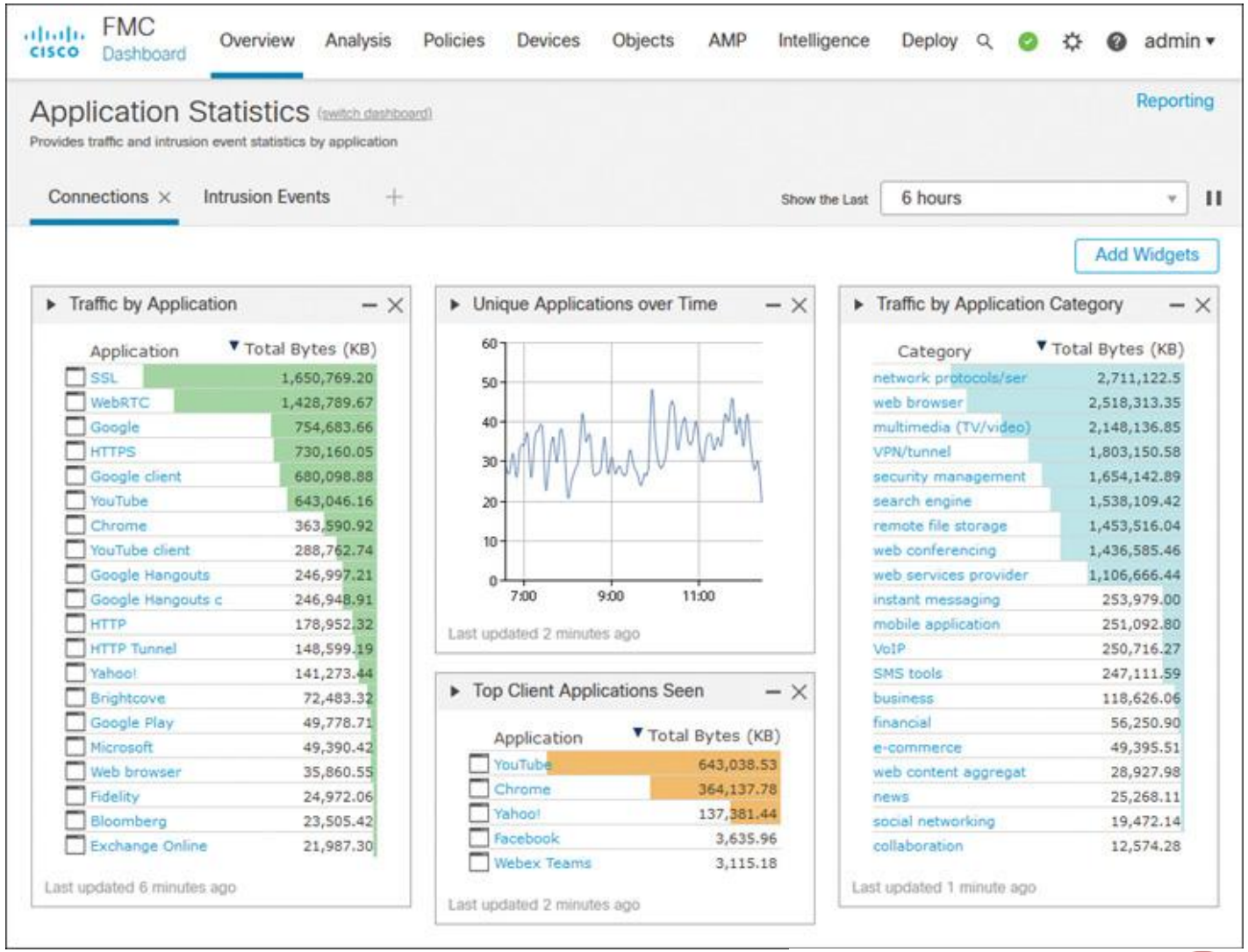
Verification

Analyzing Application Discovery

Overview > Dashboards > Application Statistics

The dashboard shows several data points in widgets

The FMC allows to add, remove, or modify any widgets

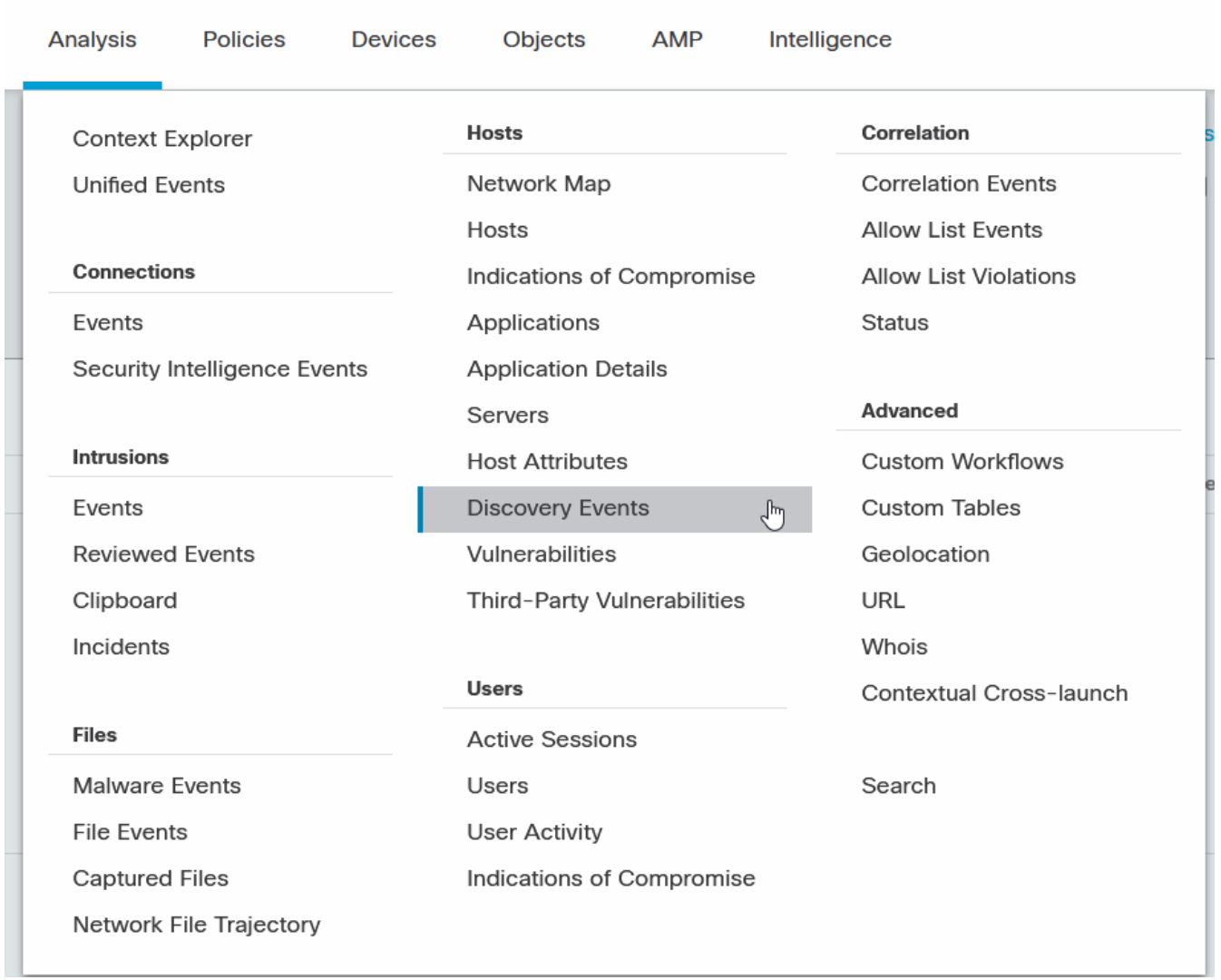


Verification

Analyzing Discovery Events

Analysis > Discovery Events

You can also click on other event types like Connections, Intrusions , etc.

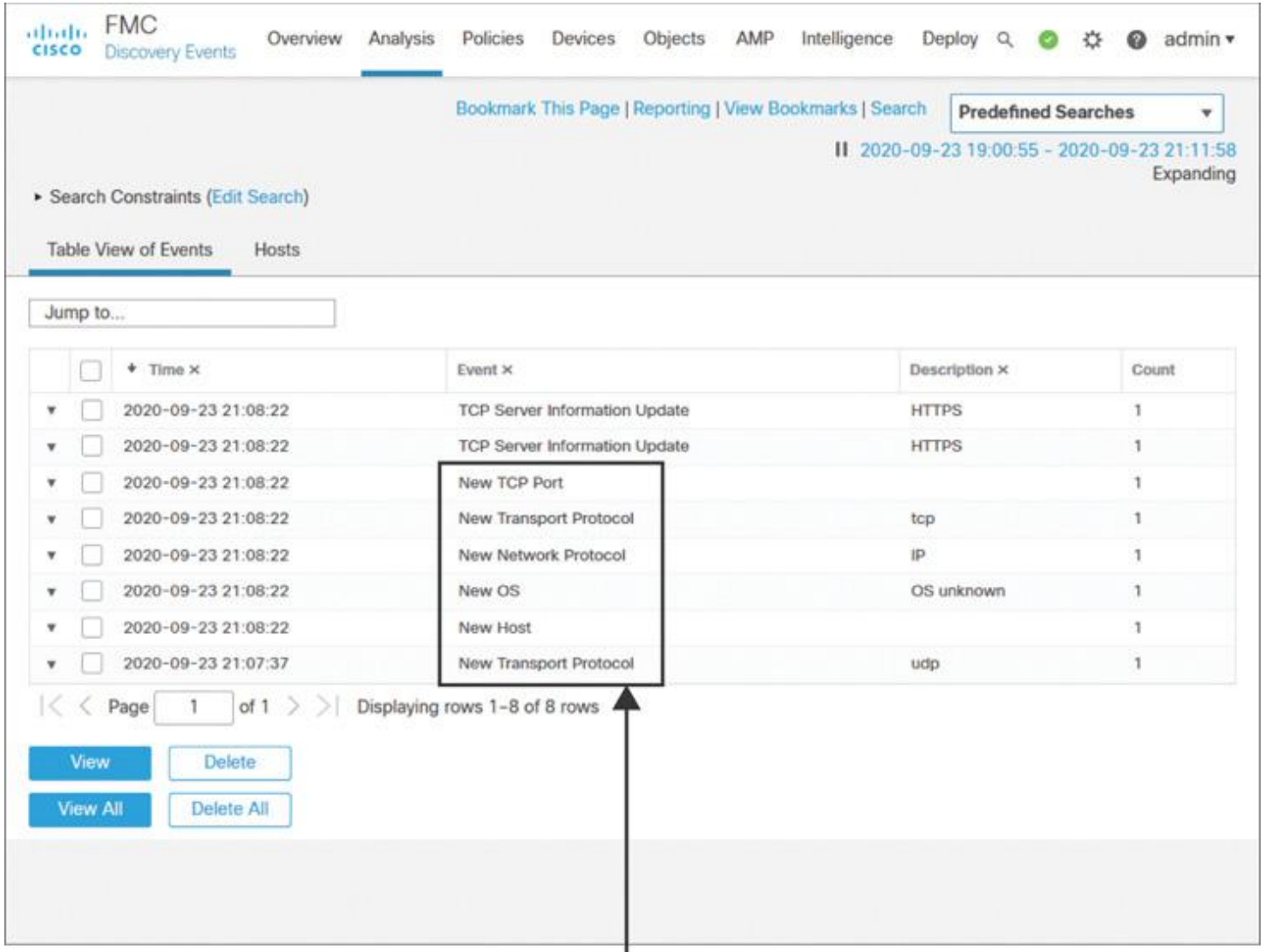


Verification

Analyzing Discovery Events

Analysis > Discovery Events

These events are generated when a new port , protocol, operating system, and host are discovered



Verification

Analyzing Host Discovery

Analysis > Hosts > Hosts

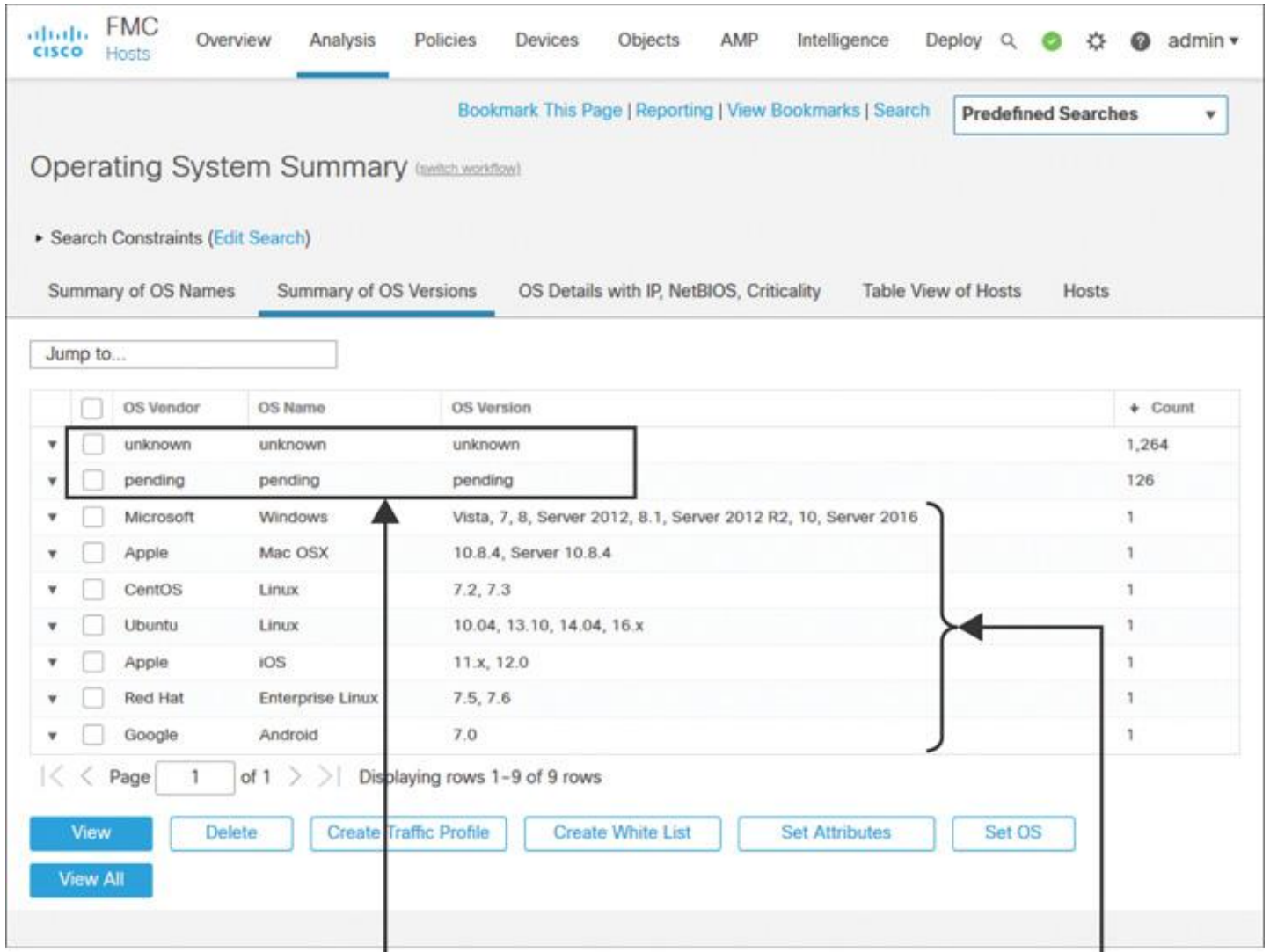
Shows the operating systems running on a monitored network

Secure Firewall can identify most of the operating systems, with their details

Pending = FTD is currently analyzing the collected data or waiting on more information

Unknown= the pattern of packets does not match an application detector

Updating the VDB can reduce the number of unknown discovery events



Verification

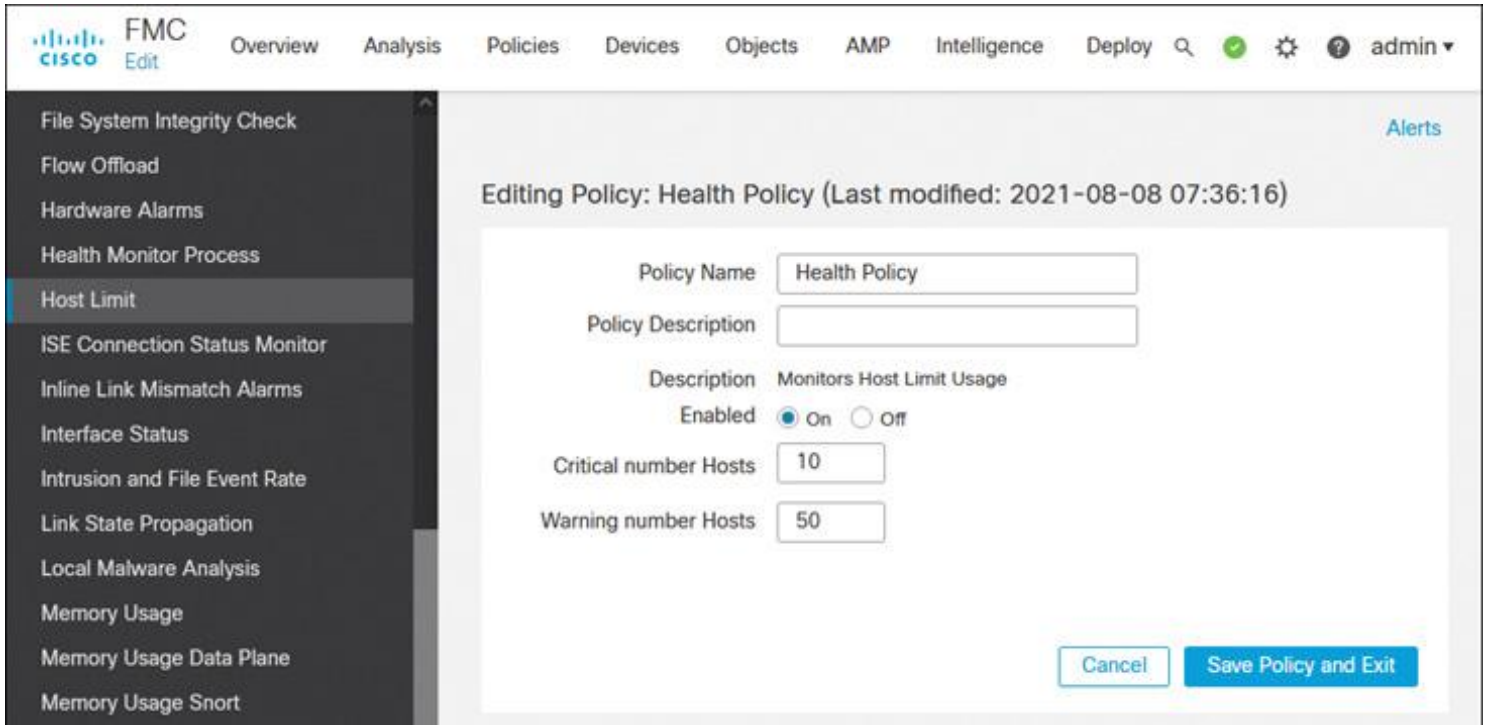
Analyzing Host Discovery

- Undiscovered New Host : If you identify a host that has not been detected by the threat defense so :

A. Check whether the management center generates any health alerts for exceeding the host limits

System > Health > Policy

Enable a health module to trigger an alert when the management center exceeds its host limit.



Verification

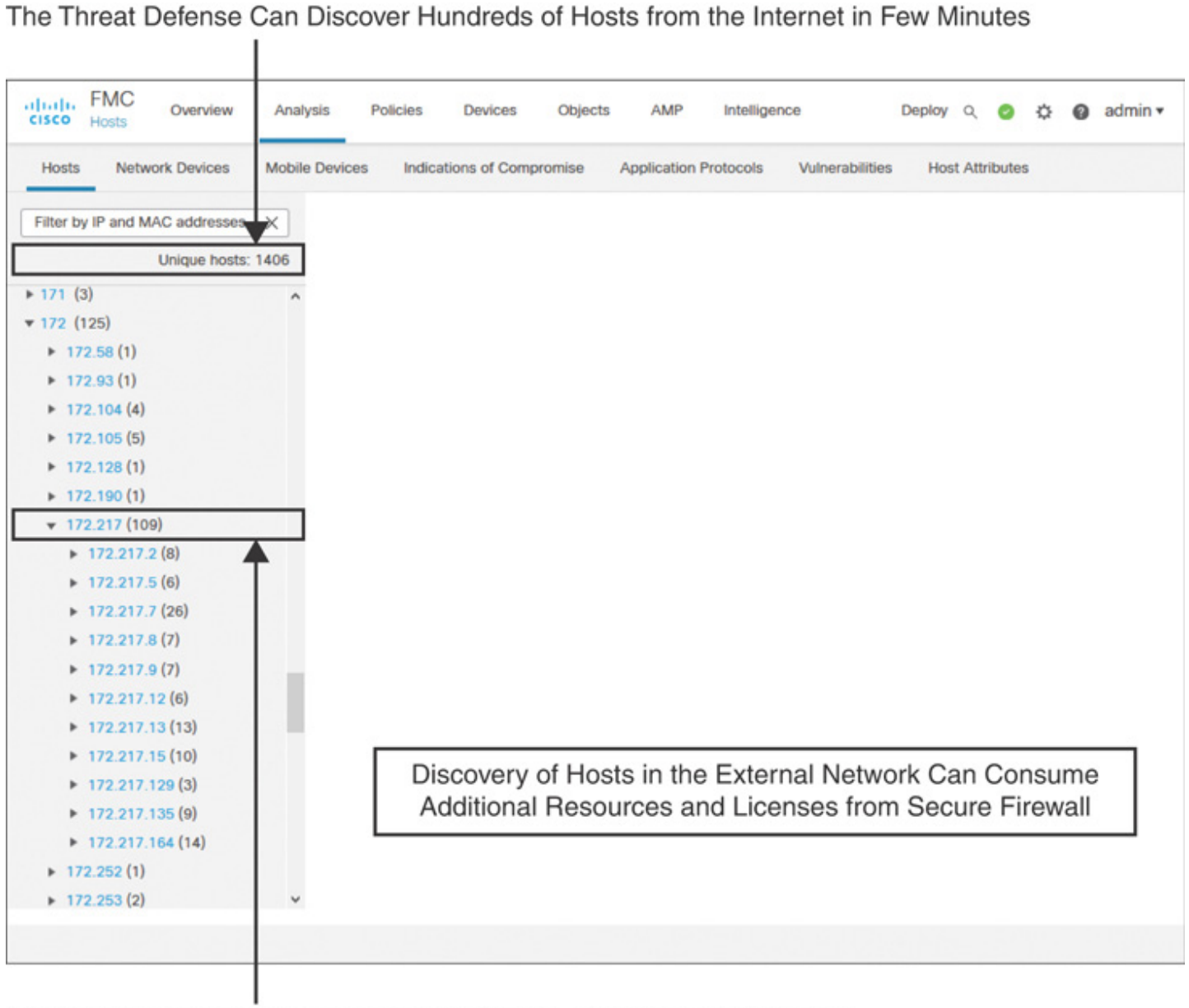
Analyzing Host Discovery

- Undiscovered New Host

B. Compare discovered host by FTD with host limit for a management center model

Analysis > Network Map > Hosts

Management Center Model	Host Limit
FMCv25	50,000
FMCv300	150,000



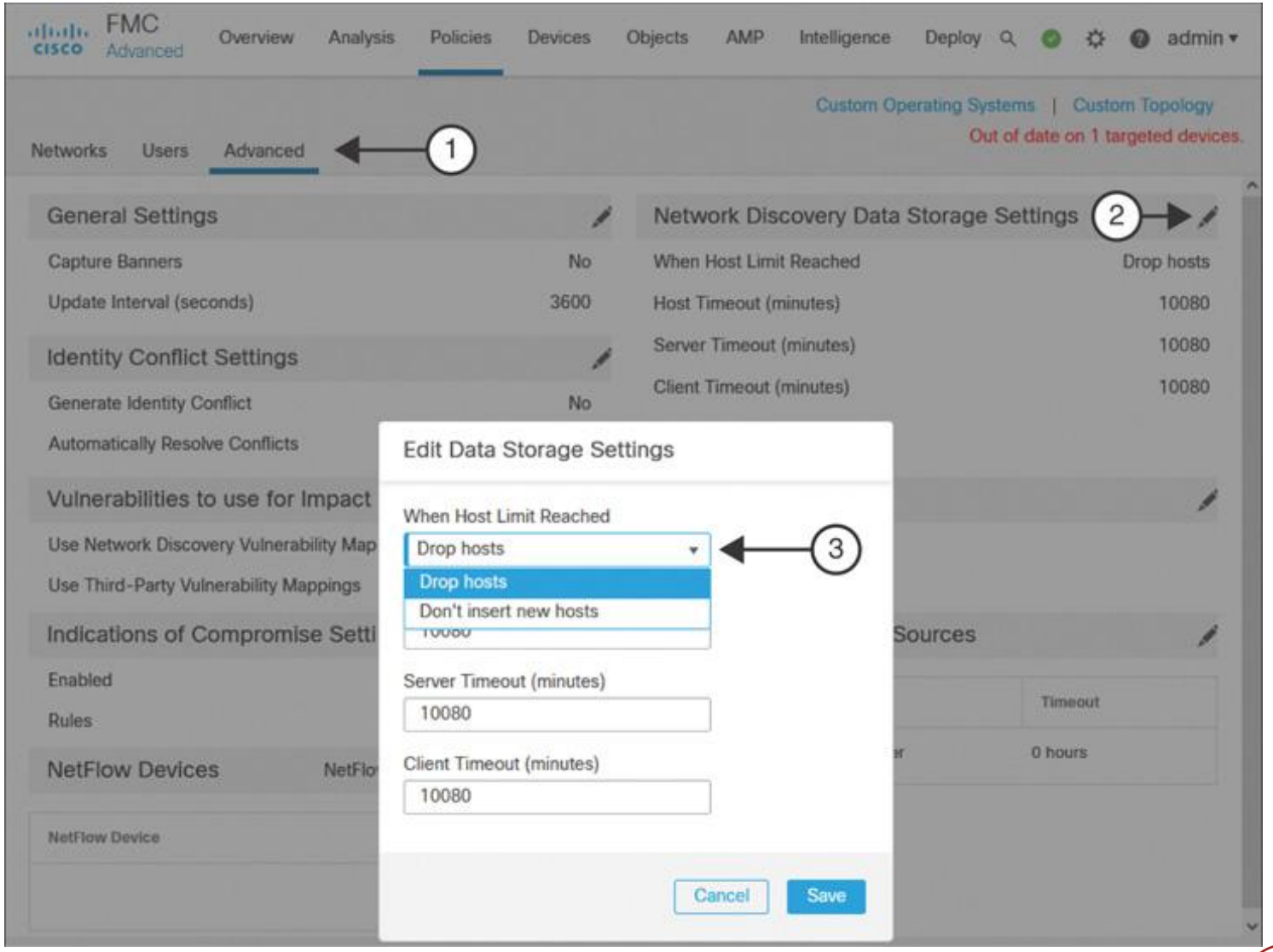
Verification

Analyzing Host Discovery

- Undiscovered New Host

C. configure a policy to stop discovering any new hosts or to drop the earliest discoveries when the FMC reaches its limit

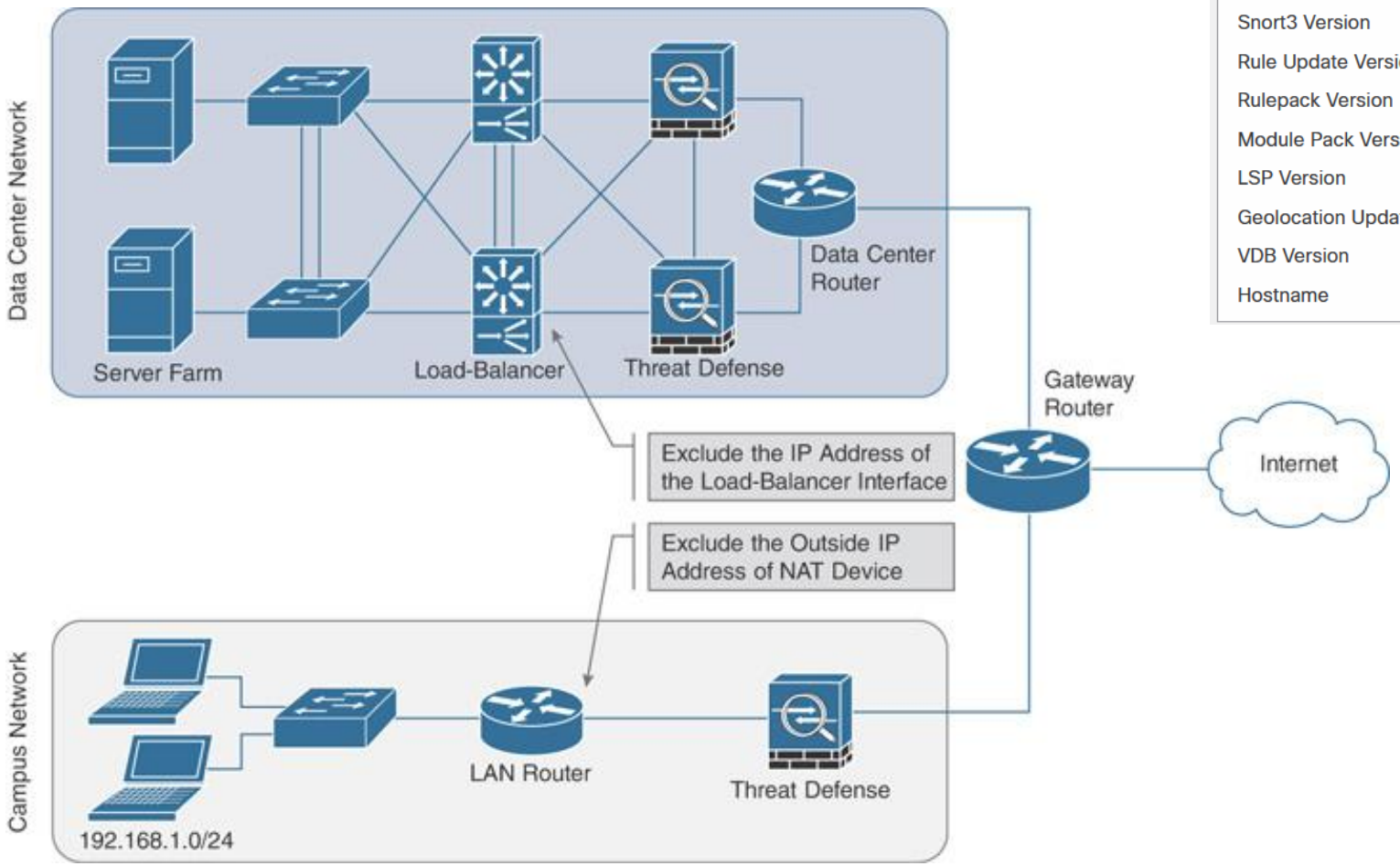
Policies > network discovery > advanced



Best Practices for Network Discovery

- Keep the VDB version up to date (check version in Help > About)
- The default rule for application discovery is 0.0.0.0/0 and::/0 , don’t change it (snort use it to discover intrusions)
- Always limit the scope of your discovery policy within your internal network
- Exclude the IP addresses of any NAT and load-balancing devices (These devices can hide computers running behind them)
- You can also exclude any ports from being monitored (reduces the number of discovery events)
- Avoid creating overlapping rules that include the same hosts
- Deploy the threat defense as close as possible to the hosts (faster detection)
- If you want to discover certain subnets or ports do not use trust rule about them in Access control policy or prefilter policy

Best Practices for Network Discovery



Model	Cisco Firepower Management Center for VMware
Serial Number	None
Software Version	7.0.1 (build 84)
OS	Cisco Firepower Extensible Operating System (FX-OS) 2.10.1 (build175)
Snort Version	2.9.18 (Build 1026)
Snort3 Version	3.1.0.100 (Build 11)
Rule Update Version	2021-05-03-001-vrt
Rulepack Version	2551
Module Pack Version	2907
LSP Version	lsp-rel-20210503-2107
Geolocation Update Version	None
VDB Version	build 338 (2020-09-24 12:58:48)
Hostname	FMC