

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

 Firepower Management Center

Overview | Analysis | Policies | Devices | Objects | AMP | Intelligence

Deploy | Search | Alerts | Settings | Help | admin

Import/Export | Custom Product Mappings | User Third-Party Mappings

Filters:

Tag: Skype

Create Custom Detector

☐ share links

☐ share media

☐ share music

☐ share photos

☐ share video

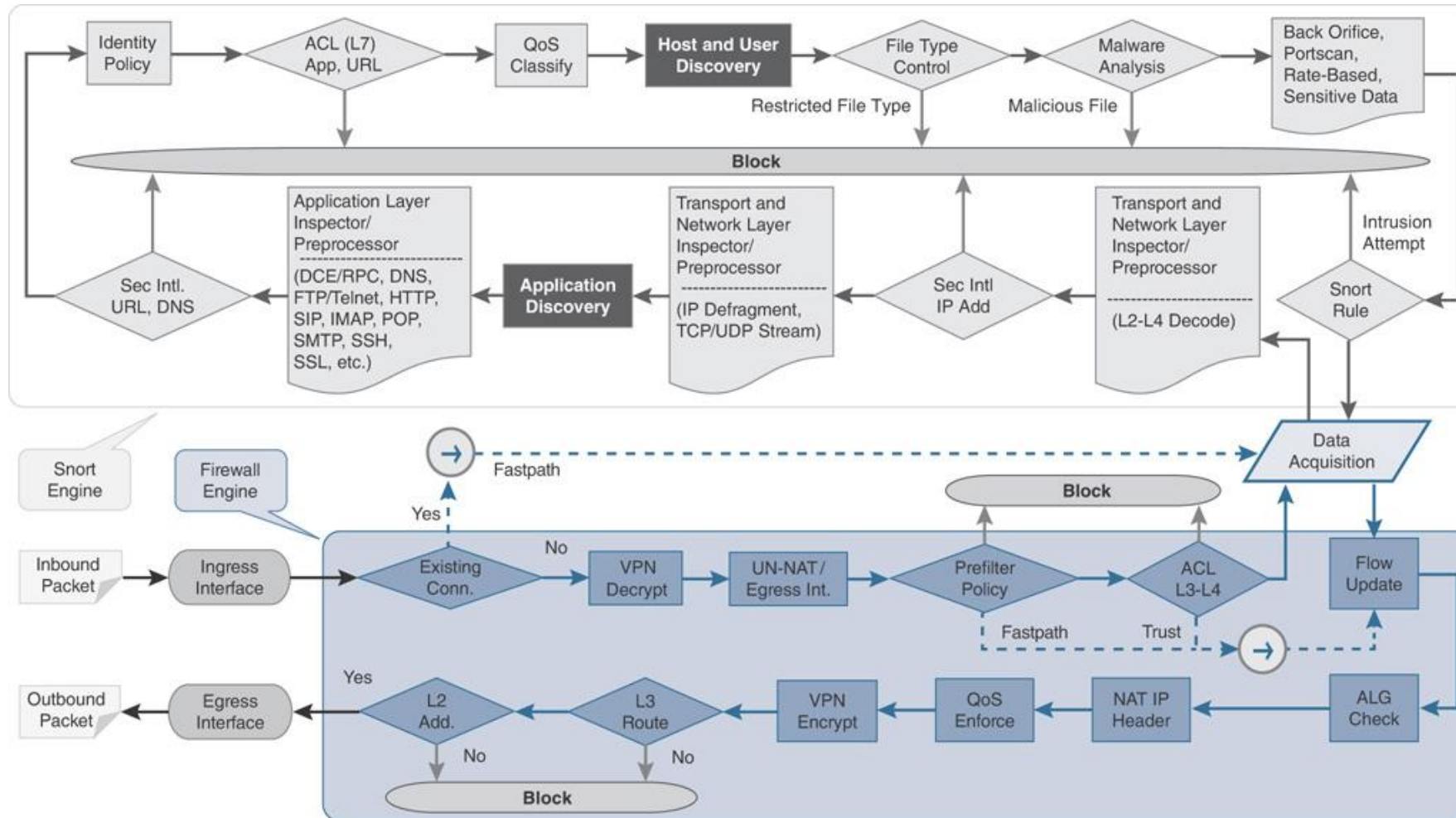
☒ Skype

☐ social network game

Name	Protocol	Details	Port(s)	State
Skype A software application that allows users to chat, make voice/ video calls, and transfer files over the Internet.	TCP/UDP	Skype		☒
Skype Auth Skype Authentication.	TCP/UDP	Skype Auth		☒
SSL Group "331" Group of SSL Host detectors.	TCP/UDP	Skype		☒

Network Discovery Operations

Processing of Packets by Various Components of Security Engines



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

Firepower Management Center

Policies / Networks

Overview Analysis Policies Devices Objects AMP Intelligence

Deploy 🔍 ⚠️ ⚙️ ? admin ▼

Custom Operating Systems | Custom Topology

No targeted devices.

+ Add Rule

Discover: Applications

- 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

Add Rule

Exclude ▼

Networks

Zones

Port Exclusions

Available Networks (14) ↻

+

Q Search by name or value

any
IPv4-Private-All-RFC1918
any-ipv4
any-ipv6
IPv4-Benchmark-Tests
IPv4-Link-Local
IPv4-Multicast
IPv4-Private-10.0.0.0-8

Add

Networks (0)

Enter network address

Add

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

The screenshot displays the Cisco Firepower Management Center (FMC) interface. The top navigation bar includes the Cisco logo, the title "Firepower Management Center", and tabs for Overview, Analysis, Policies, Devices, Objects, AMP, and Intelligence. The "Objects" tab is selected, and a sub-menu is open showing "Object Management" and "Intrusion Rules". The main content area is titled "Network" and contains a description: "A network object represents one or more IP addresses. Network objects are used in various places, including access control policies, network variables, intrusion rules, identity rules, network discovery rules, event searches, reports, and so on." Below this is a table of network objects.

Name	Value	Type	Override	
any	0.0.0.0/0 ::/0	Group		
any-ipv4	0.0.0.0/0	Network		
any-ipv6	::/0	Host		
IPv4-Benchmark-Tests	198.18.0.0/15	Network		
IPv4-Link-Local	169.254.0.0/16	Network		
IPv4-Multicast	224.0.0.0/4	Network		
IPv4-Private-10.0.0.0-8	10.0.0.0/8	Network		
IPv4-Private-172.16.0.0-12	172.16.0.0/12	Network		
IPv4-Private-192.168.0.0-16	192.168.0.0/16	Network		
IPv4-Private-All-RFC1918	10.0.0.0/8 172.16.0.0/12 192.168.0.0/16	Group		
IPv6-IPv4-Mapped	::ffff:0.0.0.0/96	Network		

At the bottom of the interface, it says "Displaying 1 - 14 of 14 rows" and "Page 1 of 1".

Configurations

Reusable Objects

Network

A network object represents one or more network discovery rules, event sources, and access control policies.

Add Network ▼

Add Object
Import Object
Add Group

New Network Object

Name: sales-PCs

Description: All Computers located in sales department

Network: ☐ Host ☐ Range ☒ Network ☐ FQDN

192.168.20.0/24

☐ Allow Overrides

Cancel Save

Name	Value	Type
any	0.0.0.0/0 ::/0	Group
any-ipv4	0.0.0.0/0	Network
any-ipv6	::/0	Host
IPv4-Benchmark-Tests	198.18.0.0/15	Network

sales-PCs 192.168.20.0/24 Network

Configurations

Reusable Objects

- > External Attributes
 - File List
- > FlexConfig
 - Geolocation
 - Interface
 - Key Chain
 - Network
- > PKI
 - Policy List
 - Port

Port

Port objects or groups represent different network discovery rules, port variables

Name
AOL
Bittorrent
DNS_over_TCP

New Port Objects

Name

RDP

Protocol

☒ TCP

☐ UDP

☐ ICMP

☐ IPv6-ICMP

☐ Other

All

Port

3389

Allow Overrides

☐

Cancel

Save

Add Port

and groups in various places in the systems web

- Add Object
- Import Object
- Add Group

	Value
	TCP (6)/5190
	TCP (6)/6881-6889
	TCP (6)/53

- Key Chain
- Network
- > PKI
- Policy List

RADIUS	UDP (17)/1645	  
RDP	TCP (6)/3389	  

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.

Add Rule

Discover ☒ Hosts ☒ Users ☒ Applications

Networks Zones Port Exclusions

Available Networks (16) 

Search by name or value

- IPv4-Private-172.16.0.0-12
- IPv4-Private-192.168.0.0-16
- IPv6-IPv4-Mapped
- IPv6-Link-Local
- IPv6-Private-Unique-Local-Addresses
- IPv6-to-IPv4-Relay-Anycast
- sales-PCs
- Servers**

Add

Networks (2)

- sales-PCs 
- Servers 

Enter network address Add

Configurations

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

NetworksUsersAdvanced

+ Add Rule

Networks	Zones	Source Port Exclusions	Destination Port Exclusions	Action	
sales-PCs Servers	any	none	none	 Discover: Hosts, Users, Applications	 
LoadBalancer	Internet (Routed)	none	none	 Exclude	 
0.0.0.0/0 ::/0	any	none	none	 Discover: Applications	 

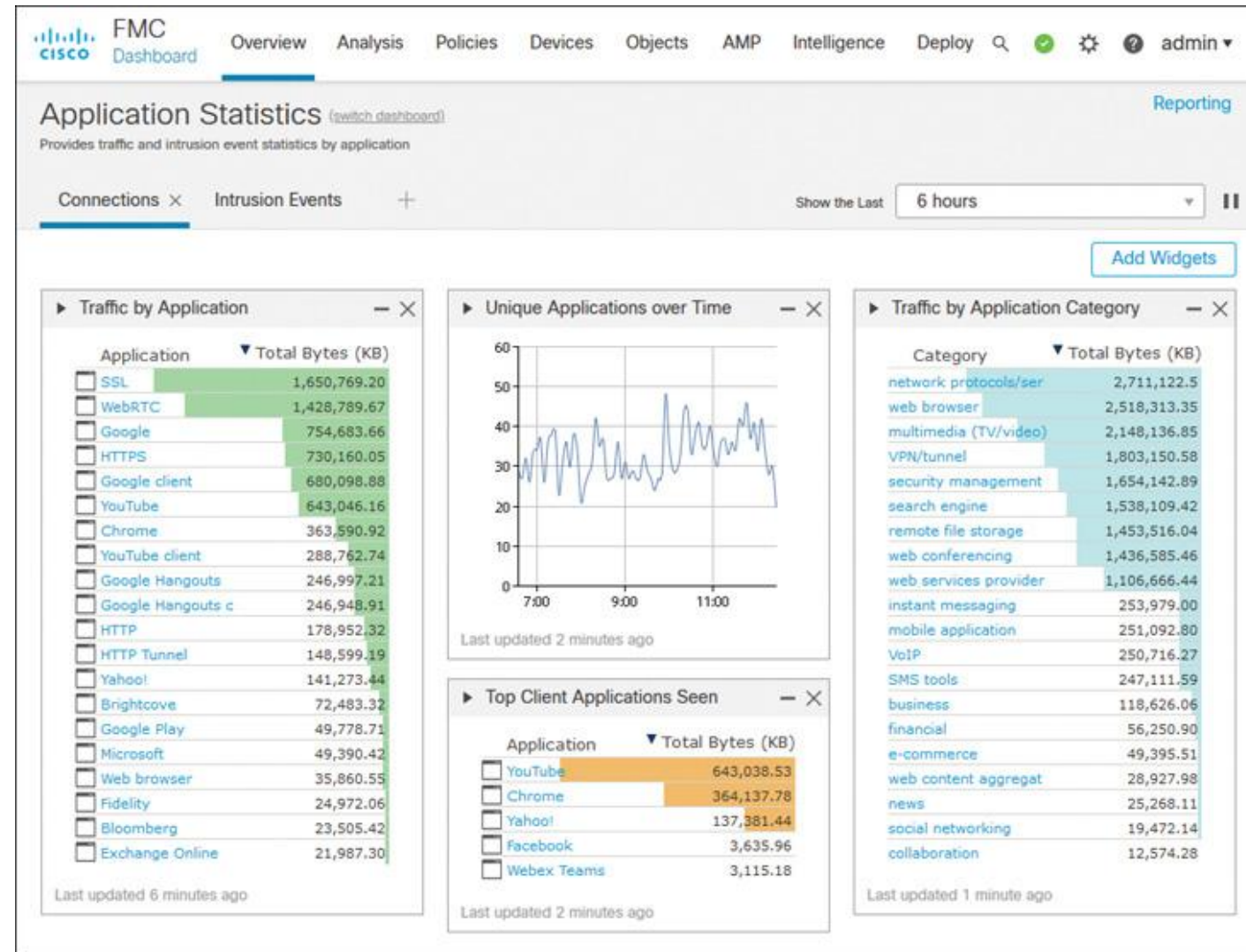
Verification

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

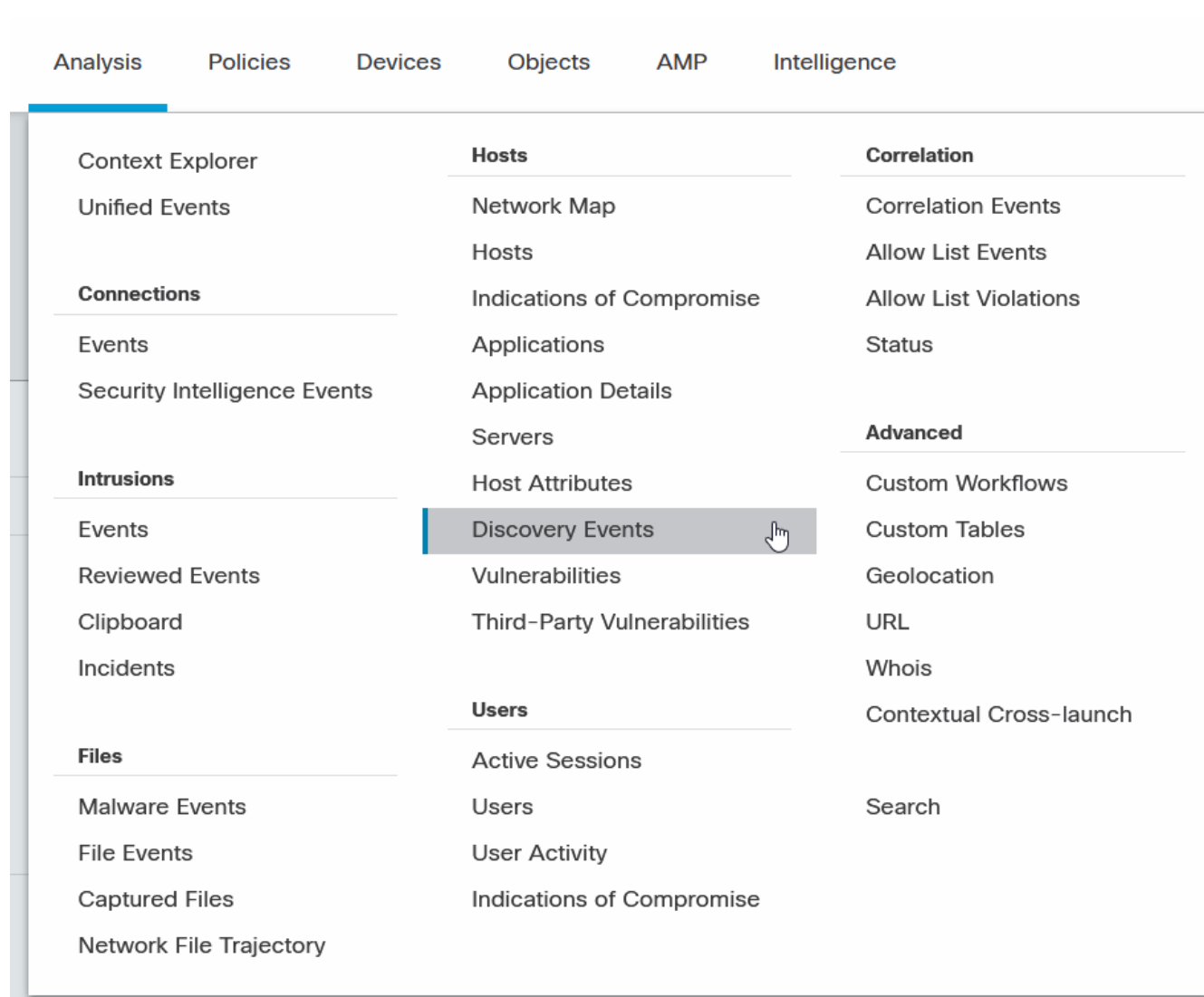


Verification

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

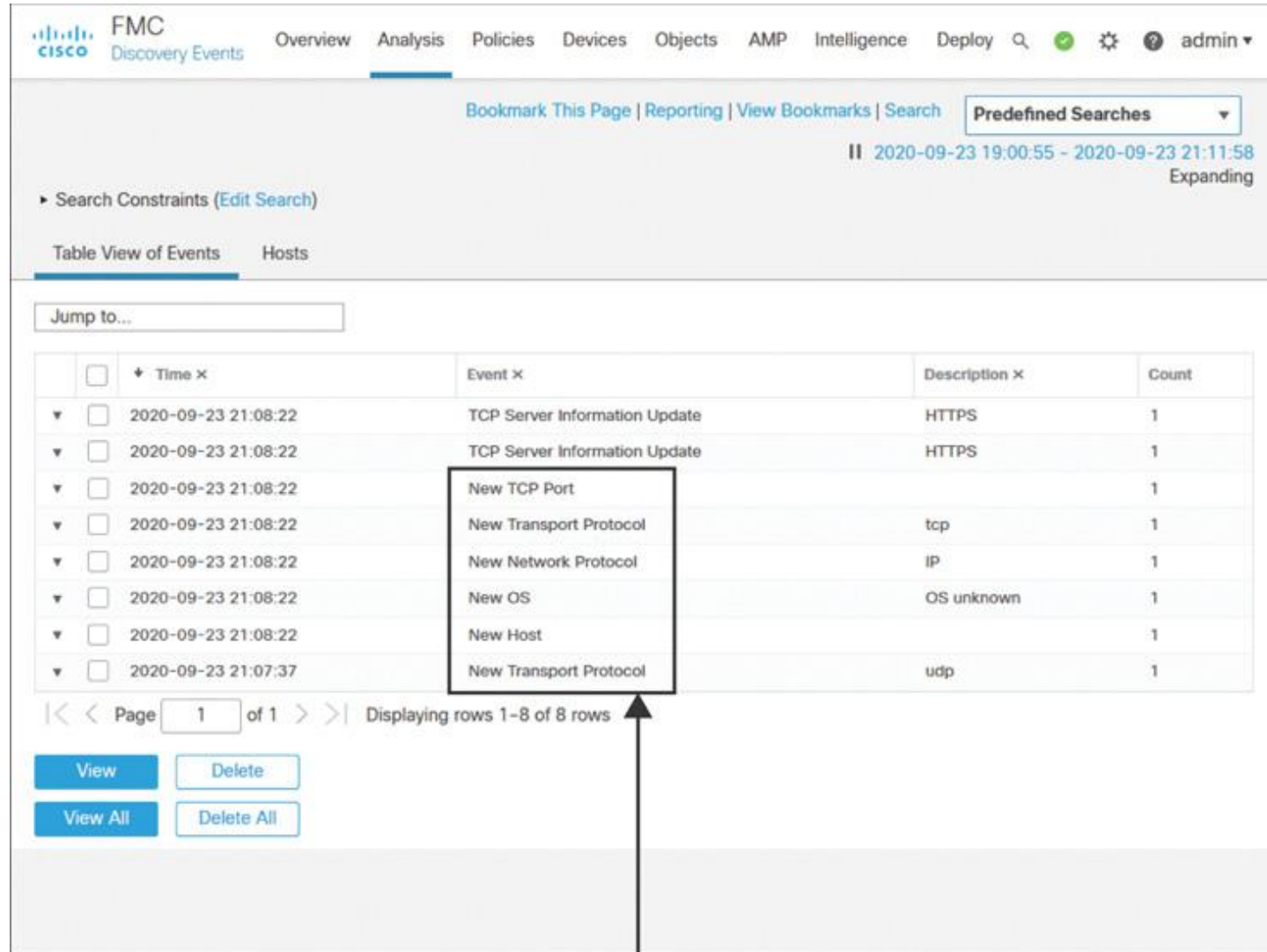


Table with 5 columns: Time, Event, Description, Count. The table displays 8 rows of discovery events. A red box highlights the following rows:

Time	Event	Description	Count
2020-09-23 21:08:22	New TCP Port	https	1
2020-09-23 21:08:22	New Transport Protocol	tcp	1
2020-09-23 21:08:22	New Network Protocol	ip	1
2020-09-23 21:08:22	New OS	OS unknown	1
2020-09-23 21:08:22	New Host		1
2020-09-23 21:07:37	New Transport Protocol	udp	1

Discovery of Port, Protocol, New Operating System, Host

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

Operating Systems on Some of the Hosts Are Not Discovered Yet

Discovery of Port, Protocol, New Operating System, and Host

	OS Vendor	OS Name	OS Version	Count
☐	unknown	unknown	unknown	1,264
☐	pending	pending	pending	126
☐	Microsoft	Windows	Vista, 7, 8, Server 2012, 8.1, Server 2012 R2, 10, Server 2016	1
☐	Apple	Mac OSX	10.8.4, Server 10.8.4	1
☐	CentOS	Linux	7.2, 7.3	1
☐	Ubuntu	Linux	10.04, 13.10, 14.04, 16.x	1
☐	Apple	iOS	11.x, 12.0	1
☐	Red Hat	Enterprise Linux	7.5, 7.6	1
☐	Google	Android	7.0	1

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.

The screenshot shows the Cisco FMC web interface for editing a 'Health Policy'. The left sidebar contains a list of health modules, with 'Host Limit' selected. The main panel displays the configuration for the 'Health Policy' (last modified: 2021-08-08 07:36:16). The configuration includes a 'Policy Name' field set to 'Health Policy', a 'Policy Description' field, a 'Description' field set to 'Monitors Host Limit Usage', and an 'Enabled' toggle set to 'On'. Below these are two numeric input fields: 'Critical number Hosts' set to 10 and 'Warning number Hosts' set to 50. At the bottom right, there are 'Cancel' and 'Save Policy and Exit' buttons.

Field	Value
Policy Name	Health Policy
Policy Description	
Description	Monitors Host Limit Usage
Enabled	On
Critical number Hosts	10
Warning number Hosts	50

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

The Threat Defense Can Discover Hundreds of Hosts from the Internet in Few Minutes

Filter by IP and MAC addresses

Unique hosts: 1406

- ▶ 171 (3)
- ▼ 172 (125)
 - ▶ 172.58 (1)
 - ▶ 172.93 (1)
 - ▶ 172.104 (4)
 - ▶ 172.105 (5)
 - ▶ 172.128 (1)
 - ▶ 172.190 (1)
 - ▼ 172.217 (109)
 - ▶ 172.217.2 (8)
 - ▶ 172.217.5 (6)
 - ▶ 172.217.7 (26)
 - ▶ 172.217.8 (7)
 - ▶ 172.217.9 (7)
 - ▶ 172.217.12 (6)
 - ▶ 172.217.13 (13)
 - ▶ 172.217.15 (10)
 - ▶ 172.217.129 (3)
 - ▶ 172.217.135 (9)
 - ▶ 172.217.164 (14)
 - ▶ 172.252 (1)
 - ▶ 172.253 (2)

Discovery of Hosts in the External Network Can Consume Additional Resources and Licenses from Secure Firewall

The Subnets Can Be Expanded to Find Details of the Discovered Hosts

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

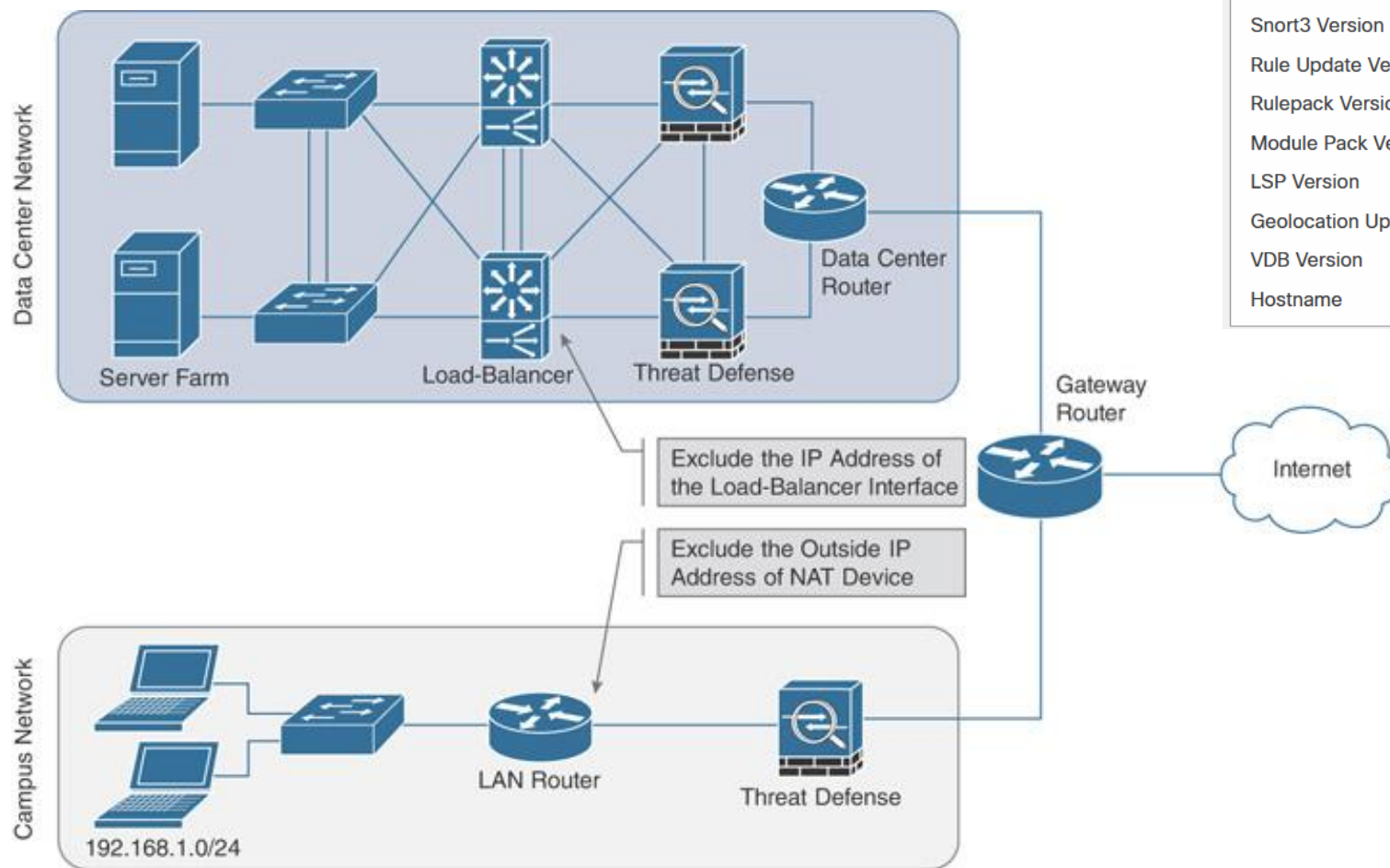
Policies > network discovery > advanced

The screenshot displays the Cisco FMC Advanced Policy configuration interface. The top navigation bar includes tabs for Overview, Analysis, Policies, Devices, Objects, AMP, Intelligence, and Deploy. The 'Policies' tab is selected, and the 'Advanced' sub-tab is active, indicated by a circled '1'. The main content area shows various settings for network discovery, including General Settings, Identity Conflict Settings, and Network Discovery Data Storage Settings. The 'Network Discovery Data Storage Settings' section is highlighted with a circled '2'. A modal dialog titled 'Edit Data Storage Settings' is open, showing options for 'When Host Limit Reached' (Drop hosts, Don't insert new hosts) and timeout values (Server Timeout: 10080, Client Timeout: 10080). The 'Drop hosts' option is selected, indicated by a circled '3'. The dialog also includes 'Cancel' and 'Save' buttons.

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