

Securing Networks with
Cisco FTD

Chapter 14

Malware and File Policy

Mohsen Kheradmand

File Policy Essentials

- Unsafe downloads can spread viruses, malware, exploit kits, and other dangers
- Secure Firewall can block the download and upload of files based on file type (exe , dll , ...)
- A threat defense can analyze a file for potential malware when the file traverses a network
- By design, a threat defense can detect and block files based on their type before looking for malware
- To monitor and control file transfers, Secure Firewall offers a standalone policy known as a file policy



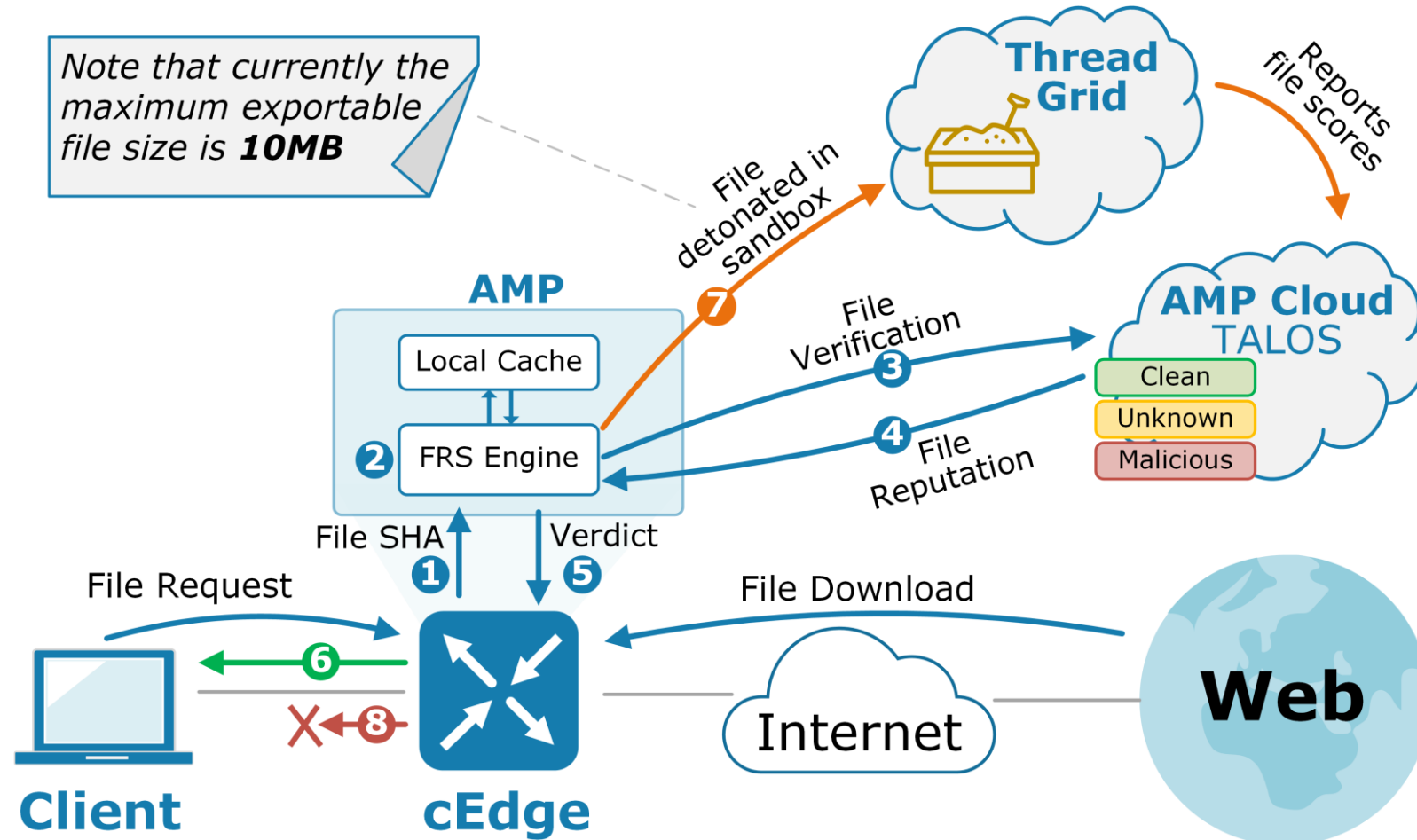
File Type Detection

- Secure Firewall uses the file magic numbers to identify the file format
- The file magic numbers are a sequence of unique hex characters that are encoded in file headers
- A threat defense can match the file magic numbers from the stream of packets
- For example, for a Microsoft executable (MSEXE) file, the file magic number is *4D 5A*
- To find this number, Snort uses the following rule on the threat defense :

```
file type:MSEXE; id:21; category:Executables,Dynamic Analysis  
Capable,Local Malware Analysis Capable; msg:"Windows/DOS  
executable file "; rev:1; content: | 4D 5A|; offset:0;
```

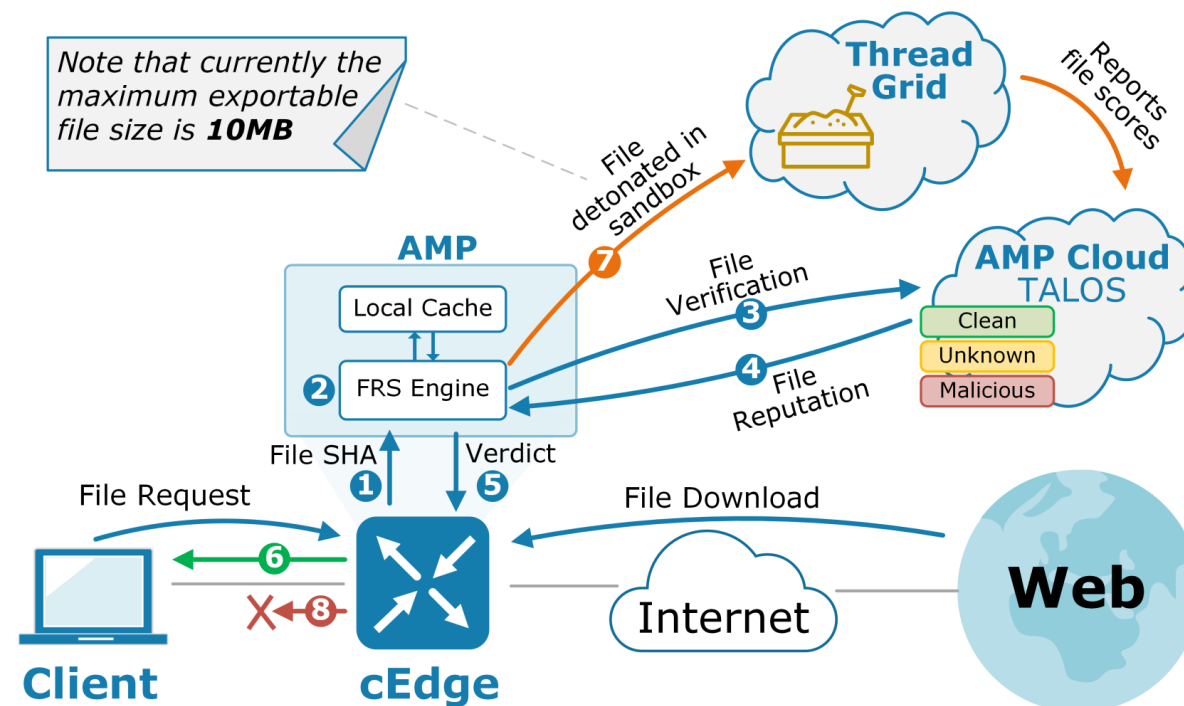
Malware Analysis

- Cisco Malware defense technology (also known as advanced malware protection or AMP)



How AMP works?

- 1) The router sends the file to the Snort file pre-processor for identification
- 2) The Snort calculates the SHA256 hash of a file to determine a file's state
it makes a local cache lookup to decide whether the hash is known to be **clean** or **malicious**.
- 3) If the hash does not match an entry in the local cache, the router sends the hash plus a context to the AMP cloud
- 4) The AMP cloud matches the SHA256 hash against the malware database and responds with a file reputation score.
- 5) The FTD decides to allow or block the file download based on the three responses by the AMP cloud:



- Clean
- Unknown
- Malicious

Secure Firewall can perform additional advanced analysis in the following order:

➤ **Spero analysis:**

- - This engine examines MSEXE files only
- - Analyzes the structural metadata and header of MSEXE files
- - Submits them in the form of a Spero signature to send to the AMP cloud
- - You can configure a file policy to perform Spero analysis locally without submitting to AMP cloud

➤ **Local analysis:**

- - Inspect files locally
- - Uses rules provided by the cisco Talos to detect the types of malware

➤ **Dynamic analysis:**

- - Sends a captured file to the cisco *sandbox* (Thread Grid) for dynamic malware analysis
- - Sandboxing can be performed either in the AMP cloud or by an on-premises appliance
- - The sandbox returns a threat score to the AMP cloud (1 to 100 , the lower is better)
- - You adjust the threshold level to the scores and define how FTD should treat a file as potential malware
- - Thread Grid requires a separate account

File and Malware Policy Prerequisites

- ✓ Make sure to install the appropriate licenses
(file policy needs Threat license , Malware analysis needs Threat + Malware license)
- ✓ A file policy uses the adaptive profiles feature , so enable it
(Policies > Access control > Access control policy > Advanced > Detection Enhancement Settings)
- ✓ When you want to block a file by using a file policy, use the Reset Connection option.
It enables the application sessions to close before the connection times out by itself
- ✓ Captured files can be stored in storage for forensic , but avoid store clean files (storage efficiency)
- ✓ You can limit the size of files to capture (optimal performance)
- ✓ If communication issues happened between Secure Firewall and the Cisco cloud, the FTD can hold the file transfer
(Default = 2 second , time is configurable in [Access control > Access control policy > Advanced > Threat Defense Service Policy](#))
- ✓ *Enable Automatic Local Malware Detection Updates* (communicate with the Talos cloud every 30 minutes for updates)
(System > Integration > Cloud Services > AMP for Networks)
- ✓ Make sure your network discovery policy is deployed and configured to discover applications
File policy leverages application detection to determine whether an application is capable of transmitting a file

Configuring a File Policy

Two step

- 1) Create a file policy
- 2) Create an access control rule and invoke the file policy within the access control rule

➤ Creating a File Policy

Policies > Access Control > Malware & File > New File Policy

The screenshot displays the Cisco Firepower Management Center interface. The top navigation bar includes the Cisco logo, the title 'Firepower Management Center', and a breadcrumb trail: 'Policies / Access Control / Malware & File'. The main navigation tabs are 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects', 'AMP', and 'Intelligence'. The 'Policies' tab is active, and a dropdown menu is open, showing a list of policy categories: 'Access Control', 'Network Discovery', 'Actions', 'Access Control', 'Application Detectors', 'Alerts', 'Intrusion', 'Correlation', 'Scanners', 'Malware & File' (highlighted with a mouse cursor), 'Groups', 'DNS', 'Modules', 'Identity', 'Instances', 'SSL', and 'Prefilter'. In the foreground, a 'New File Policy' dialog box is open, featuring a 'Name' field with the text 'File-Policy-1', a 'Description' field, and 'Cancel' and 'Save' buttons at the bottom. The background interface also shows a 'Compare Policies' button and a 'New File Policy' button.

Configuring a File Policy

➤ Creating a File Policy

- Click pencil to edit the Policy
- Click the Add Rule
- Select Application Protocol
- Select Direction of transfer
- Add file type from Categories
- Specify the Action to files
- You can store selected file
- Click Save

View Rule

Application Protocol

HTTP

Direction of Transfer

Download

File Type Categories

☐ Office Documents	22
☒ Archive	20
☐ Multimedia	30
☐ Executables	13
☐ PDF files	2
☐ Encoded	2
☐ Graphics	6

Action

→ Detect Files

→ Detect Files

→ Block Files

Malware Cloud Lookup

✖ Block Malware

☒ Store files

Search name and description

All types in selected Categori...

7Z (7-Zip compressed file)

ALZ (Archive file for Microsof...

ARJ (Compressed archive file)

BZ (bzip2 compressed archive)

CPIO_CRC (Archive created ...

Add

Selected File Categories and Types

GZ (GZ)

JAR (Java archive file)

RAR (WinRAR compressed ar...

ZIP (PKZIP archive file)

Cancel

Save

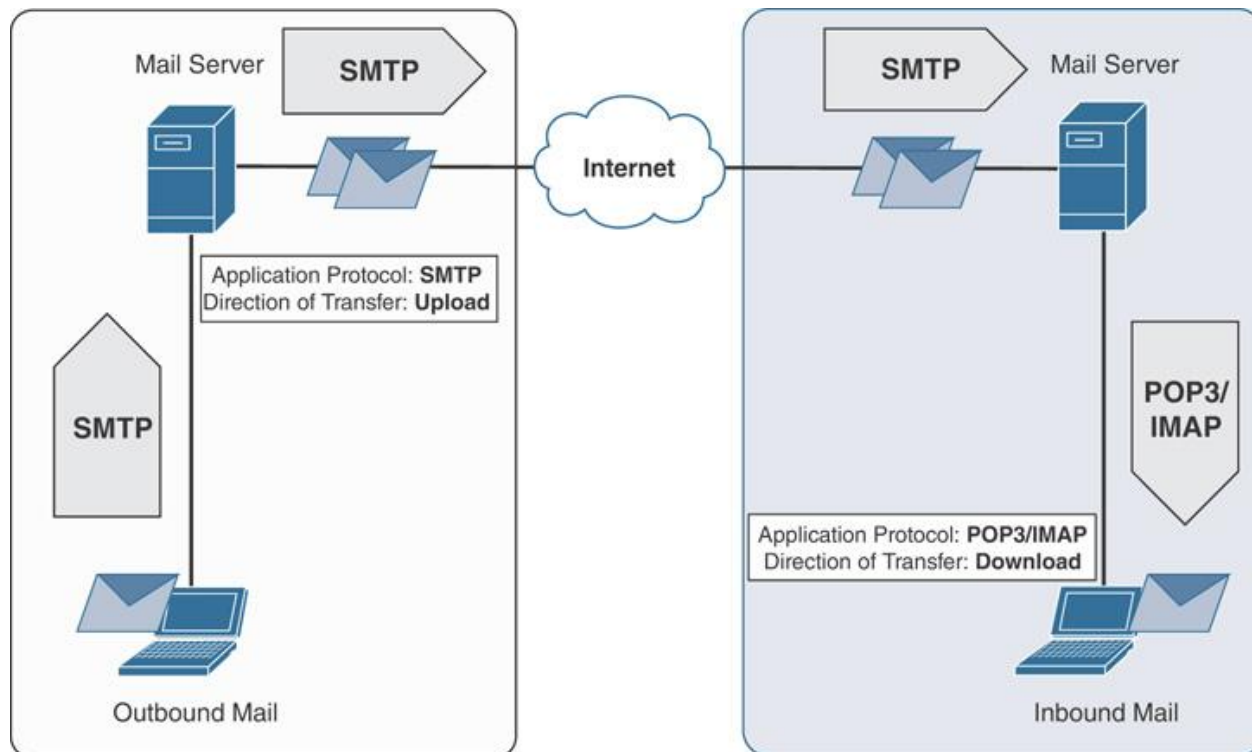
Configuring a File Policy

➤ Creating a File Policy

Application Protocol is the protocol by which the files are transferred

Direction of Transfer to analyze, can be in Upload or Download or any

- HTTP, FTP, and NetBIOS-ssn (SMB) protocols can be monitored in any direction
- SMTP (upload only) and POP3/IMAP (download)



Application Protocol

HTTP
Any
HTTP
SMTP
IMAP
POP3
FTP
NetBIOS-ssn (SMB)

Direction of Transfer

Download
Any
Upload
Download

Configuring a File Policy

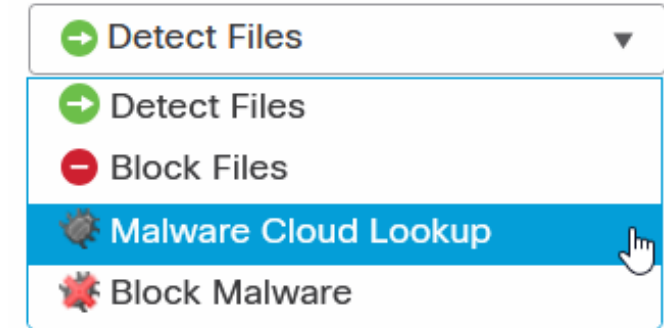
➤ Creating a File Policy

Action

- **Detect Files :**
 - - Detects a file transfer and logs without interrupting
- **Block Files :**
 - - Blocks files based on the selected file types
- **Malware Cloud Lookup :**
 - - Perform malware analysis locally and remotely without interrupting
- **Block Malware :**
 - - Block inspected file if it is infected with malware.

- ✓ 1st and 2nd options , Detect Files and Block Files , allow you to control files based on their types
- ✓ 3rd and 4th options , enable you to control files based on file disposition (requires the malware license)
- ✓ The order of actions is Block Files , Block Malware, Malware Cloud Lookup, and Detect Files

Action



Configuring a File Policy

➤ Creating a File Policy

If you select Malware actions , You can enable :

- **Spero Analysis for MSEX** :

Submits Spero signature to the Spero engine in the AMP cloud

- **Dynamic analysis**

Sends files to Threat Grid (or local sandbox) for further inspection.

- **Capacity Handling**

Store the files that can not be submitted for dynamic analysis to disk for later submission

- **Local Malware analysis**

Inspect files based on local DB

- **Reset Connection**

Close application session before the connection times out

➤ Store Files : you can store inspected file in local storage for forensic

Action	Store Files
Block Malware	☒ Malware
☒ Spero Analysis for MSEX	☐ Unknown
☒ Dynamic Analysis	☐ Clean
☒ Capacity Handling	☐ Custom
☒ Local Malware Analysis	
☒ Reset Connection	

Configuring a File Policy

➤ Creating a File Policy

Advanced tab

File-Policy-1

Enter Description

Rules

Advanced

General

- ☒ First Time File Analysis
- ☒ Enable Custom Detection List
- ☒ Enable Clean List

If AMP Cloud disposition is Unknown, override disposition based upon threat score

☐ ☒ ☐ ☐ Medium ▼

Archive File Inspection

- ☒ Inspect Archives
- ☐ Block Encrypted Archives
- ☒ Block Uninspectable Archives

Max Archive Depth

Enter a value between 1 and 3

2

Configuring a File Policy

➤ Deploying a File Policy

- 1) Policies > Access Control > Access Control
- 2) Create a new policy or Modify existing Policy
- 3) Create a new Rule > inspection tab > File Policy

Note : only “allow”, “interactive block”, or “interactive block with reset” can be used for malware and file policy in ACP

Add Rule ?

Name	Archived-Files-Check	☒ Enabled	Insert	below rule	2
Action	Allow		Time Range	None	+
Zones Networks VLAN Tags Users Applications Ports URLs Dynamic Attributes <u>Inspection</u> Logging Comments					
Intrusion Policy	None	Variable Set	Default Set		
File Policy	File-Policy-1				

Configuring a File Policy

➤ Deploying a File Policy

- By enabling the File Policy in ACP , automatically enables logging for the file event
- Additionally, to view file policy logs in the connection event, you can manually enable Log at End of Connection.

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

☐ Log at Beginning of Connection

☒ Log at End of Connection

File Events:

☒ Log Files

Send Connection Events to:

☒ Firepower Management Center

☐ Syslog Server *(Using default syslog configuration in Access Control Logging)* [Show Overrides](#)

☐ SNMP Trap

Select an SNMP Alert Configurat ▼

 +

Verification

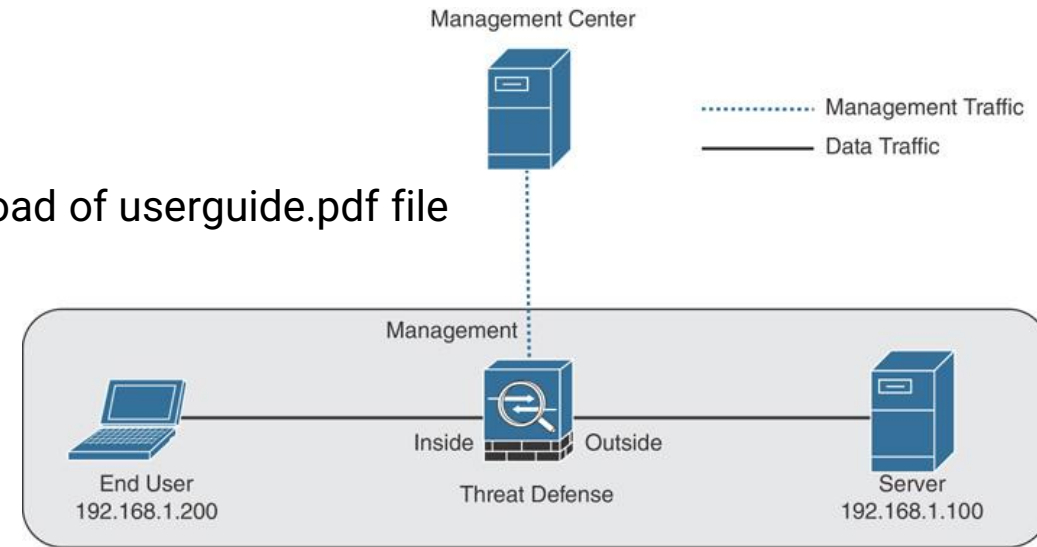
Example :

- Client computer, attempt to download two files from the Server
- File policy = **block** the download of the 7z1900.exe and **detect** the download of userguide.pdf file

File Policy configuration interface showing two rules:

File Types	Application Protocol	Direction	Action
Category: System files Category: Executables	Any	Any	Block Files with Reset
Category: PDF files Category: Archive Category: Office Documents	Any	Any	Detect Files Store Files

The New Malware and File Policy
Is Used by an Access Control Policy



Verification

Example :

Analysis > Files > File Events

The screenshot shows the Cisco FMC File Events page. The top navigation bar includes links for Overview, Analysis (selected), Policies, Devices, Objects, AMP, Intelligence, Deploy, and a user profile 'admin'. Below the navigation bar, there are links for 'Bookmark This Page', 'Reporting', 'Dashboard', 'View Bookmarks', and 'Search'. The main heading is 'File Summary' with a '(switch workflow)' link. To the right, a time range is displayed: '2021-01-07 09:28:00 - 2021-01-07 12:41:43' with an 'Expanding' status. Below this, it says 'No Search Constraints (Edit Search)'. There are two tabs: 'File Summary' (selected) and 'Table View of File Events'. A 'Jump to...' search box is present. The main table has columns: Category, Type, Disposition, Action, and Count. It shows two entries: 'Executables' (MSEXE) with a 'Block' action and count of 1, and 'PDF files' (PDF) with a 'Detect' action and count of 1.

Category	Type	Disposition	Action	Count
Executables	MSEXE		Block	1
PDF files	PDF		Detect	1

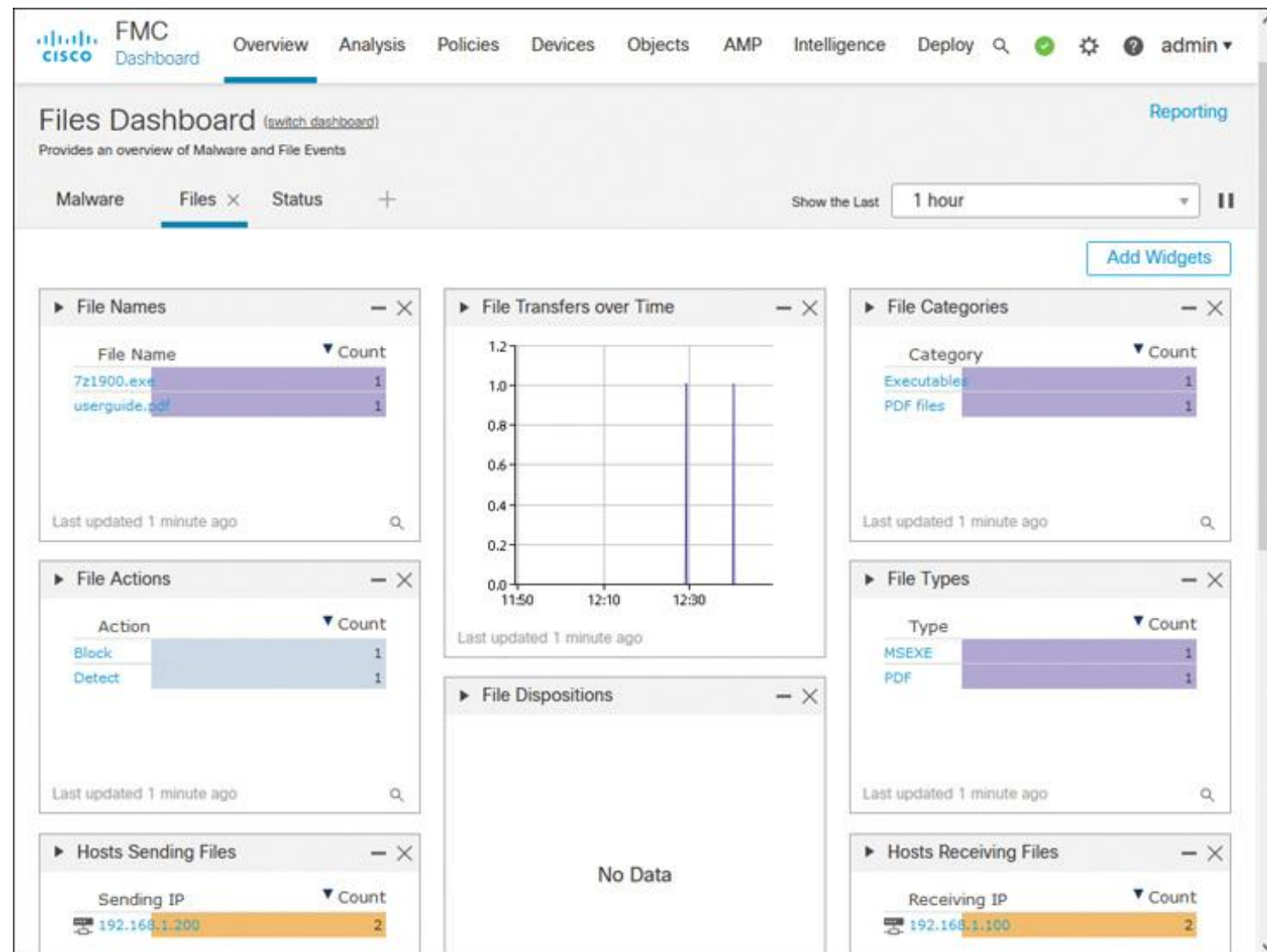
Because the Block Files action does not perform malware analysis, the Disposition column is blank.

The screenshot shows the same Cisco FMC File Events page, but with the 'Table View of File Events' tab selected. A black arrow points to this tab. The time range is updated to '2021-01-07 09:28:00 - 2021-01-07 12:40:40'. The table now has more columns: Time, Action, Sending IP, Receiving IP, File Name, SHA256, Threat Score, Type, and Category. It shows two detailed entries: one for '7z1900.exe' (MSEXE) blocked at 12:40:20, and another for 'userguide.pdf' (PDF) detected at 12:29:15.

Time	Action	Sending IP	Receiving IP	File Name	SHA256	Threat Score	Type	Category
2021-01-07 12:40:20	Block	192.168.1.200	192.168.1.100	7z1900.exe			MSEXE	Executables
2021-01-07 12:29:15	Detect	192.168.1.200	192.168.1.100	userguide.pdf	a6619969...27d53a6c		PDF	PDF files

Verification

Overview > Dashboards > Files Dashboard



Verification

- You can use the CLI to debug

system support firewall-engine-debug

If you run the this command while you attempt to transfer a file, you see detailed logs

```
> system support firewall-engine-debug
```

```
Please specify an IP protocol: tcp
```

```
Please specify a client IP address: 192.168.1.100
```

```
Please specify a client port:
```

```
Please specify a server IP address:
```

```
Please specify a server port:
```

```
Monitoring firewall engine debug messages
```

```
192.168.1.100-46592 > 192.168.1.200-80 6
```

```
AS 4-4 I 0 new firewall session
```

```
192.168.1.100-46592 > 192.168.1.200-80 6
```

```
AS 4-4 I 0 using HW or preset rule order 2,
```

```
'Rule for Files', action Allow and
```

```
prefilter rule 0
```

```
192.168.1.100-46592 > 192.168.1.200-80 6
```

```
AS 4-4 I 0 HitCount data sent for rule
```

```
id: 268461056,
```

Analyzing Malware Events

- Performs a Cloud Lookup

Analysis > File > File Events

Successful Malware Cloud Lookup

Different Actions Same File

	☐	Time X	Action X	Sending IP X	Receiving IP X	File Name X	SHA256 X	Threat Score X	Type X	Category X
▼	☐	2021-01-07 13:27:24	Malware Cloud Lookup	192.168.1.200	192.168.1.100	7z1900.exe	759aa04d...4bb7ef80		MSEXE	Executables
▼	☐	2021-01-07 12:52:08	Cloud Lookup Timeout	192.168.1.200	192.168.1.100	7z1900.exe	759aa04d...4bb7ef80		MSEXE	Executables
▼	☐	2021-01-07 12:40:20	Block	192.168.1.200	192.168.1.100	7z1900.exe			MSEXE	Executables
▼	☐	2021-01-07 12:29:15	Detect	192.168.1.200	192.168.1.100	userguide.pdf	a6619969...27d53a6c		PDF	PDF files

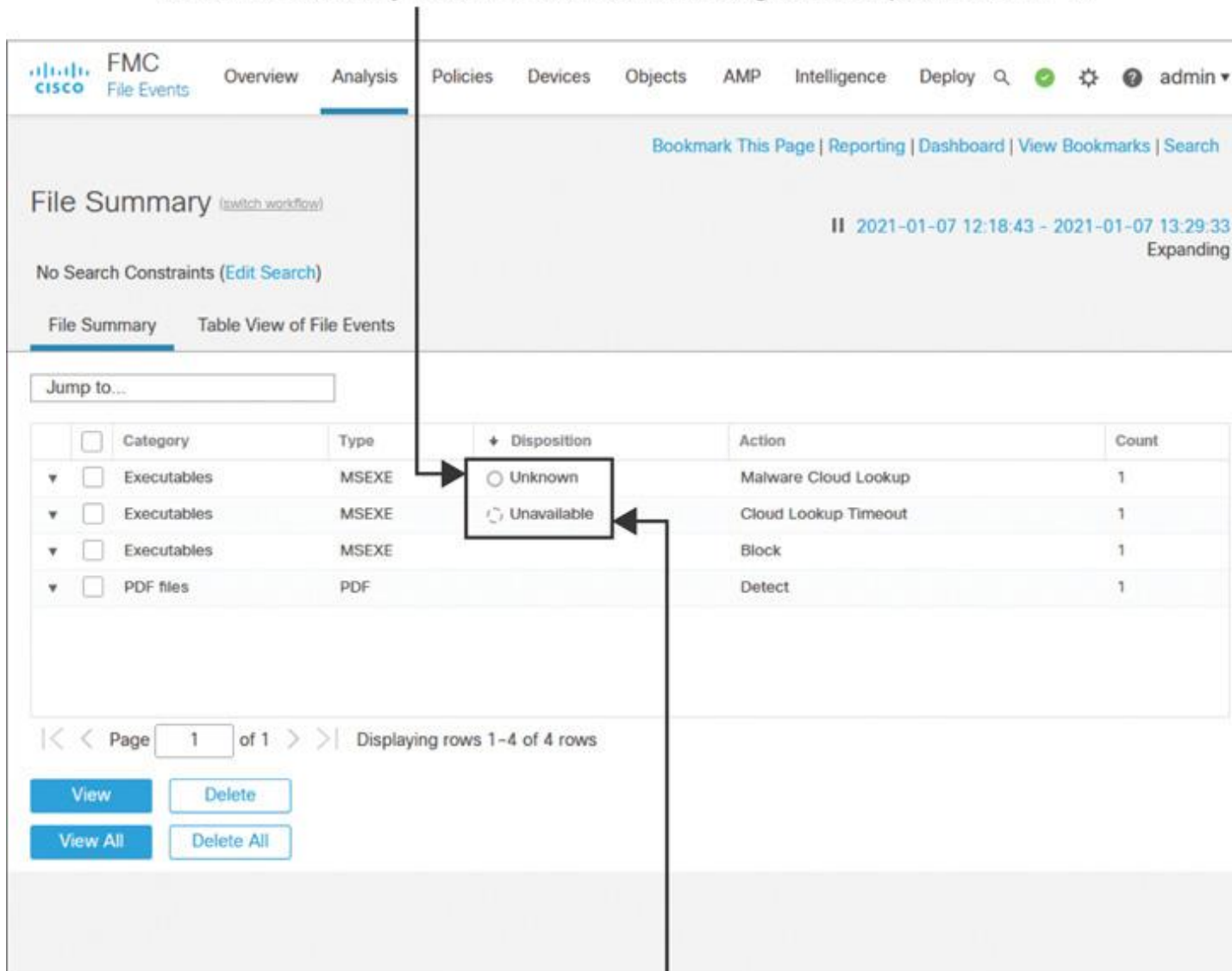
Page 1 of 1 Displaying rows 1-4 of 4 rows

View Delete View All Delete All

- Because the management center can communicate with the Cisco clouds, the threat defense returns Malware Cloud Lookup instead of Cloud Lookup Timeout.

Analyzing Malware Events

Unknown Disposition Means That the Management Center Connects to the Cloud Successfully but the Cloud Has Not Assigned a Disposition to a File



The screenshot shows the Cisco FMC File Events Analysis page. The top navigation bar includes links for Overview, Analysis, Policies, Devices, Objects, AMP, Intelligence, Deploy, and a search icon. The main content area is titled "File Summary" and shows a time range of "2021-01-07 12:18:43 - 2021-01-07 13:29:33" with an "Expanding" status. Below the summary, there is a table of file events. The table has columns for Category, Type, Disposition, Action, and Count. The Disposition column is highlighted with a box, and a line points from the "Unknown" disposition to the text above. The table contains four rows of data:

Category	Type	Disposition	Action	Count
Executables	MSEXE	Unknown	Malware Cloud Lookup	1
Executables	MSEXE	Unavailable	Cloud Lookup Timeout	1
Executables	MSEXE		Block	1
PDF files	PDF		Detect	1

At the bottom of the table, there are buttons for "View", "Delete", "View All", and "Delete All". The page also shows a "Page 1 of 1" indicator and "Displaying rows 1-4 of 4 rows".

Unavailable Disposition Means That the Management Center Is Unable to Connect to the Cloud or Perform a Lookup for a File

Analyzing Malware Events

The Cisco cloud can return one of the following dispositions for a query:

Malware: If Cisco determines that a file is malware

Clean: If Cisco finds no malicious pattern on a file

Unknown: If Cisco has not assigned a disposition (malware or clean) to a file

The screenshot displays the Cisco FMC (File Management Console) interface for configuring a File Policy. The top navigation bar includes tabs for Overview, Analysis, Policies (selected), Devices, Objects, AMP, Intelligence, and Deploy. The main heading is 'File Policy' with a 'Save' button and a 'Cancel' button. Below the heading, there are tabs for 'Rules' and 'Advanced'. The 'Rules' tab is active, showing a table with one rule. The rule is defined by the following parameters:

File Types	Application Protocol	Direction	Action
- Category: System files - Category: PDF files - Category: Executables - Category: Archive (1 more...)	Any	Any	- Block Malware with Reset - Spero Analysis - Dynamic Analysis - Capacity Handling - Local Malware Analysis - Store files of disposition: Malware, Unknown

At the top right of the rule table, it indicates 'Used by 1 access control policy' and provides a '+ Add Rule' link.

Analyzing Malware Events

The Threat Defense Blocking a File with a Very High Threat Score

FMC File Events Overview Analysis Policies Devices Objects AMP Intelligence Deploy admin

File Summary [\(switch workflow\)](#) 2021-01-06 19:14:00 - 2021-01-07 15:57:07 Expanding

No Search Constraints [\(Edit Search\)](#)

File Summary Table View of File Events

Jump to...

	Time	Action	Sending IP	Receiving IP	File Name	SHA256	Threat Score	Type
☐	2021-01-07 13:39:26	Malware Block	192.168.1.200	192.168.1.100	suspicious.exe	131f95c5...bdfd8267	Very High	EICAR
☐	2021-01-07 13:39:26	Malware Block	192.168.1.200	192.168.1.100	suspicious.exe	131f95c5...bdfd8267	Very High	EICAR
☐	2021-01-07 13:39:26	Malware Block	192.168.1.200	192.168.1.100	suspicious.exe	131f95c5...bdfd8267	Very High	EICAR
☐	2021-01-07 13:39:26	Malware Block	192.168.1.200	192.168.1.100	suspicious.exe	131f95c5...bdfd8267	Very High	EICAR
☐	2021-01-07 13:39:26	Malware Block	192.168.1.200	192.168.1.100	suspicious.exe	131f95c5...bdfd8267	Very High	EICAR
☐	2021-01-07 13:39:26	Malware Block	192.168.1.200	192.168.1.100	suspicious.exe	131f95c5...bdfd8267	Very High	EICAR
☐	2021-01-07 13:39:26	Malware Block	192.168.1.200	192.168.1.100	suspicious.exe	131f95c5...bdfd8267	Very High	EICAR
☐	2021-01-07 13:39:26	Malware Block	192.168.1.200	192.168.1.100	suspicious.exe	131f95c5...bdfd8267	Very High	EICAR
☐	2021-01-07 13:39:26	Malware Block	192.168.1.200	192.168.1.100	suspicious.exe	131f95c5...bdfd8267	Very High	EICAR
☐	2021-01-07 13:39:26	Malware Block	192.168.1.200	192.168.1.100	suspicious.exe	131f95c5...bdfd8267	Very High	EICAR
☐	2021-01-07 13:27:24	Malware Cloud Lookup	192.168.1.200	192.168.1.100	7z1900.exe	759aa04d...4bb7ef80		MSEXE
☐	2021-01-07 12:52:08	Cloud Lookup Timeout	192.168.1.200	192.168.1.100	7z1900.exe	759aa04d...4bb7ef80		MSEXE
☐	2021-01-07 12:40:20	Block	192.168.1.200	192.168.1.100	7z1900.exe			MSEXE
☐	2021-01-07 12:29:15	Detect	192.168.1.200	192.168.1.100	userguide.pdf	a6619969...27d53a6c		PDF

Page 1 of 1 Displaying rows 1-14 of 14 rows

View Delete View All Delete All

Overriding a Malware Disposition

- If you disagree with a file disposition ,
override this outcome by using a file list.

There are two types of file lists:

- Clean list
- Custom detection list



FMC

File Events

Overview

Analysis

Policies

Devices

Objects

AMP

Intelligence

Deploy

Q

admin ▼

File Summary (switch workflow)

2021-01-06 19:14:00 - 2021-01-07 15:57:07

Expanding

No Search Constraints [\(Edit Search\)](#)

File Summary

Table View of File Events

Jump to...

		Time ×	Action ×	Sending IP ×	Receiving IP ×	File Name ×	SHA256 ×	Threat Score ×	Type ×
▼	☐	2021-01-07 13:39:26	Malware Block	 192.168.1.200	 192.168.1.100	suspicious.exe	 131f95c5...bdfd8267	●●●● Very High	EICAR
▼	☐	2021-01-07 13:39:26	Malware Block	 192.168.1.200	 192.168.1.100	suspicious.exe	 131f95c5...bdfd8267	●●●● Very High	EICAR
▼	☐	2021-01-07 13:39:26	Malware Block	 192.168.1.200	 192.168.1.100	suspicious.exe	 131f95c5...bdfd8267	●●●● Very High	EICAR
▼	☐	2021-01-07 13:39:26	Malware Block	 192.168.1.200	 192.168.1.100	suspicious.exe	 131f95c5...bdfd8267	●●●● Very High	EICAR
▼	☐	2021-01-07 13:39:26	Malware Block	 192.168.1.200	 192.168.1.100	suspicious.exe	 131f95c5...bdfd8267	●●●● Very High	EICAR
▼	☐	2021-01-07 13:39:26	Malware Block	 192.168.1.200	 192.168.1.100	suspicious.exe	 131f95c5...bdfd8267	●●●● Very High	EICAR
▼	☐	2021-01-07 13:39:26	Malware Block	 192.168.1.200	 192.168.1.100	suspicious.exe	 131f95c5...bdfd8267	●●●● Very High	EICAR
▼	☐	2021-01-07 13:39:26	Malware Block	 192.168.1.200	 192.168.1.100	suspicious.exe	 131f95c5...bdfd8267	●●●● Very High	EICAR
▼	☐	2021-01-07 13:39:26	Malware Block	 192.168.1.200	 192.168.1.100	suspicious.exe	 131f95c5...bdfd8267	●●●● Very High	EICAR
▼	☐	2021-01-07 13:39:26	Malware Block	 192.168.1.200	 192.168.1.100	suspicious.exe	 131f95c5...bdfd8267	●●●● Very High	EICAR
▼	☐	2021-01-07 13:39:26	Malware Block	 192.168.1.200	 192.168.1.100	suspicious.exe	 131f95c5...bdfd8267	●●●● Very High	EICAR
▼	☐	2021-01-07 13:27:24	Malware Cloud Lookup	 192.168.1.200	 192.168.1.100	7z1900.exe	 759aa04d...4bb7ef80		MSEXE
▼	☐	2021-01-07 12:52:08	Cloud Lookup Timeout	 192.168.1.200	 192.168.1.100	7z1900.exe	 759aa04d...4bb7ef80		MSEXE
▼	☐	2021-01-07 12:40:20	Block	 192.168.1.200	 192.168.1.100	7z1900.exe			MSEXE
▼	☐	2021-01-07 12:29:15	Detect	 192.168.1.200	 192.168.1.100	userguide.pdf	 a6619969...27d53a6c		PDF

<< Page 1 of 1 >>

Displaying rows 1-14 of 14 rows

View

Delete

View All

Delete All

Open in New Window

Exclude

Open in Context Explorer

Add File to Clean List

Add File to Custom Detection List

Download File

Analyze File

View File Composition

Network Trajectory

- The management center allows you to track and visualize the path of a file by using the network file trajectory feature

➤ Files > Network Trajectory.

The screenshot displays the Cisco FMC Network File Trajectory interface. The top navigation bar includes links for Overview, Analysis, Policies, Devices, Objects, AMP, Intelligence, and Deploy. The main content area shows details for a specific file trajectory.

File Details:

- File SHA256: 131f95c5...bdfd8267
- File Name: suspicious.exe
- File Size (KB): 0.0674
- File Type: EICAR
- File Category: Executables
- Current Disposition: Malware
- Threat Score: None
- Detection Name: EICAR

Event Details:

- First Seen: 2021-01-07 13:39:26 on 192.168.1.200 by No Authentication Required
- Last Seen: 2021-01-07 13:39:26 on 192.168.1.200 by No Authentication Required
- Event Count: 10
- Seen On: 1 hosts
- Seen On Breakdown: 1 sender → 0 receivers

Trajectory Diagram:

The trajectory diagram shows a sequence of events starting from the source IP 192.168.1.200 on Jan 07 at 13:39. The diagram consists of a series of red gear icons connected by a line, representing the file's path through the network.

Events and Dispositions Legend:

- Events: Transfer, Block, Create, Move, Execute, Scan, Retrospective, Quarantine
- Dispositions: Unknown, Malware, Clean, Custom, Unavailable

Events Table:

Time	Event Ty	Sending IP	Receiving IP	User	File Name	Disp	Action	Protoc	Client	Web A	De...
2021-01...	Tra...	192.168...	192.168...	No Authe...	suspiciou...	Mi	Malwa...	H...	Fl...		
2021-01...	Tra...	192.168...	192.168...	No Authe...	suspiciou...	Mi	Malwa...	H...	Fl...		
2021-01...	Tra...	192.168...	192.168...	No Authe...	suspiciou...	Mi	Malwa...	H...	Fl...		