Securing Networks with

Cisco FTD

Chapter 14

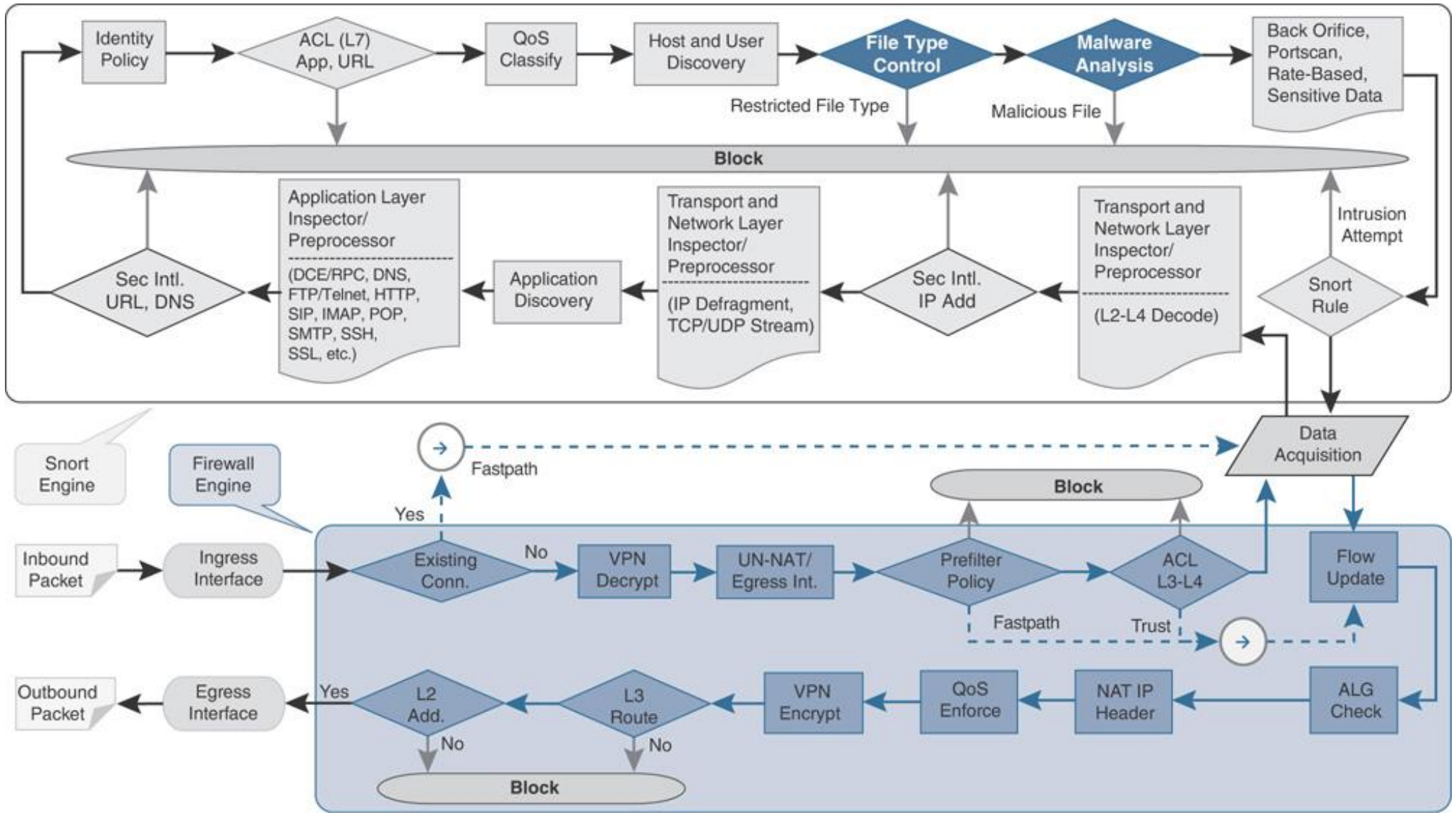
Malware and File Policy

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 Policy and Malware Analysis in Snort



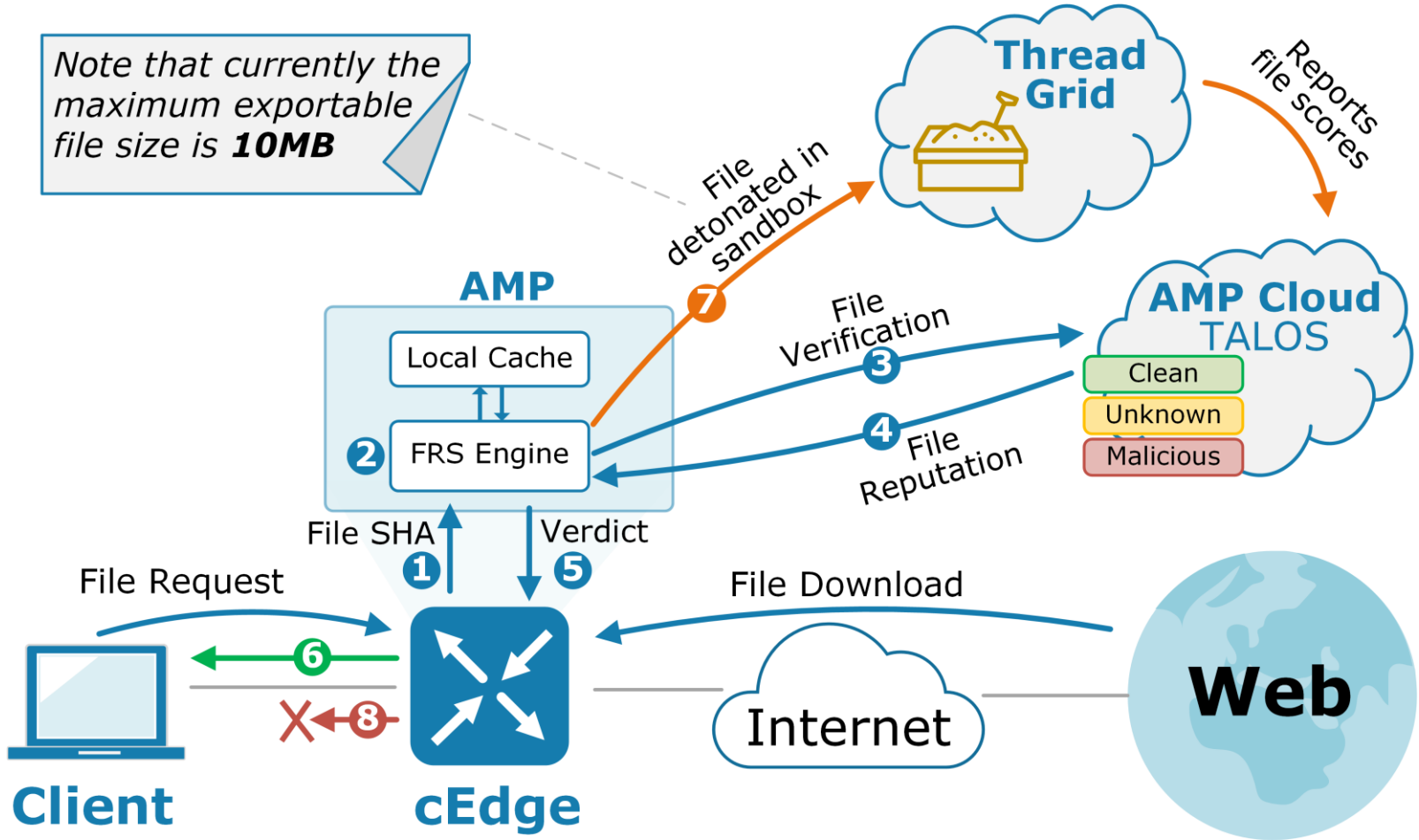
File Type Detection

- 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

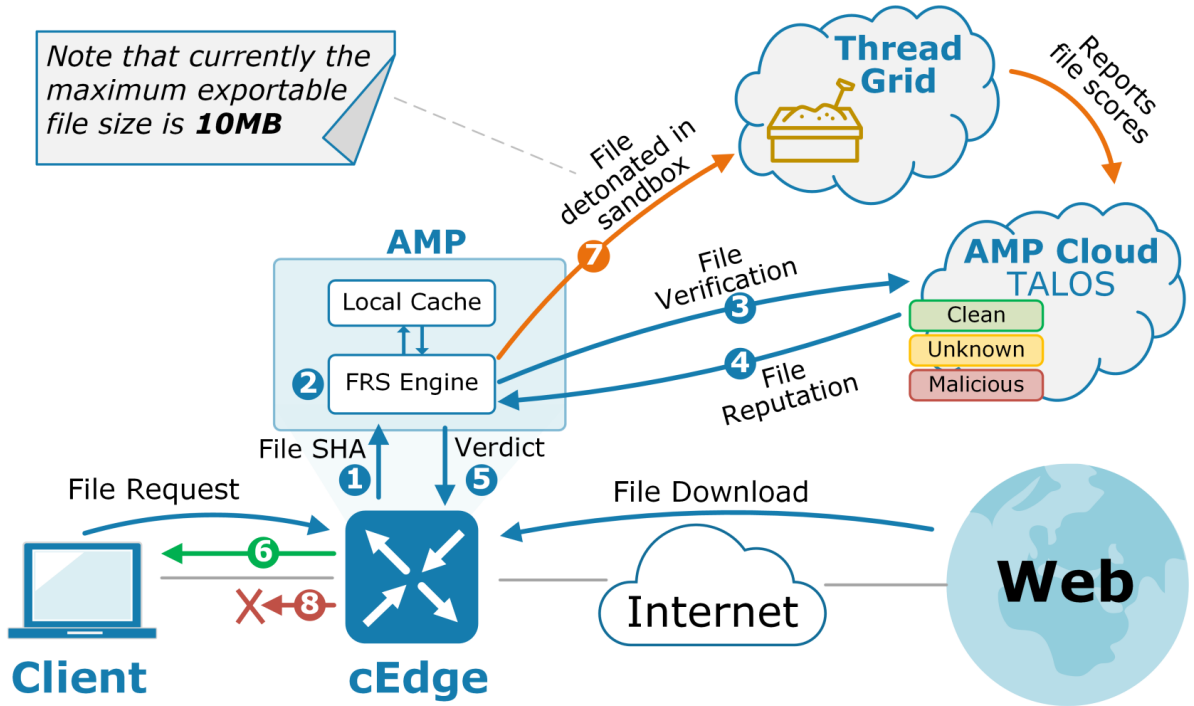
- Cisco Malware defense technology (also known as advanced malware protection or AMP)



Communications Between Secure Firewall and Cisco Clouds for Malware Analysis

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

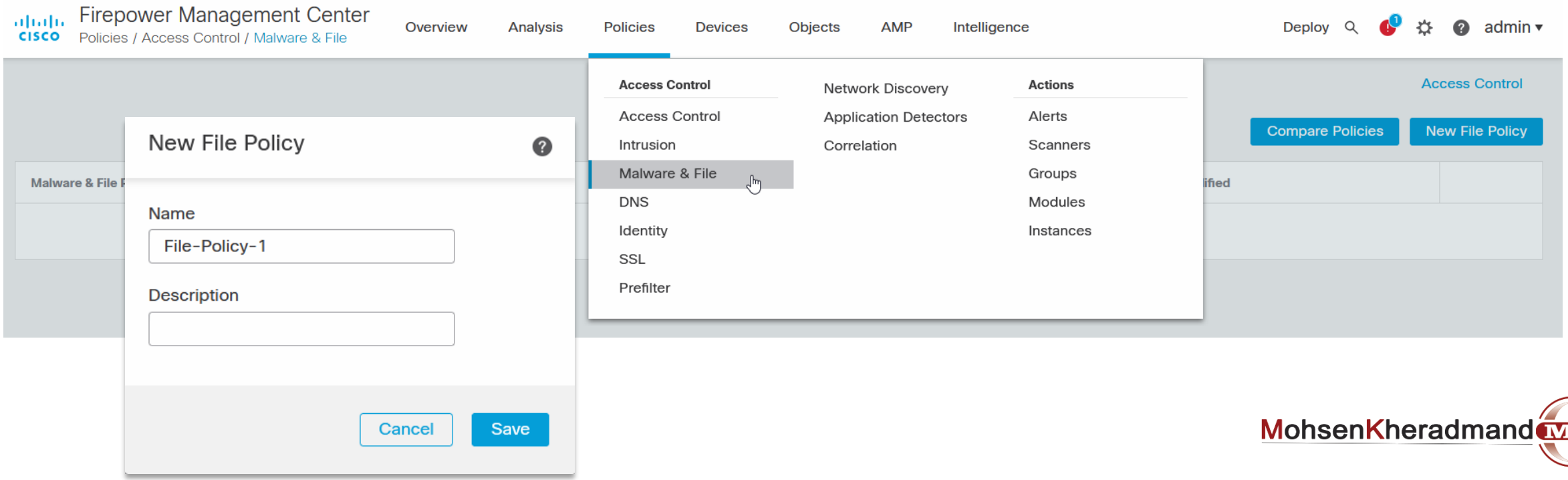
Configuring a File Policy

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

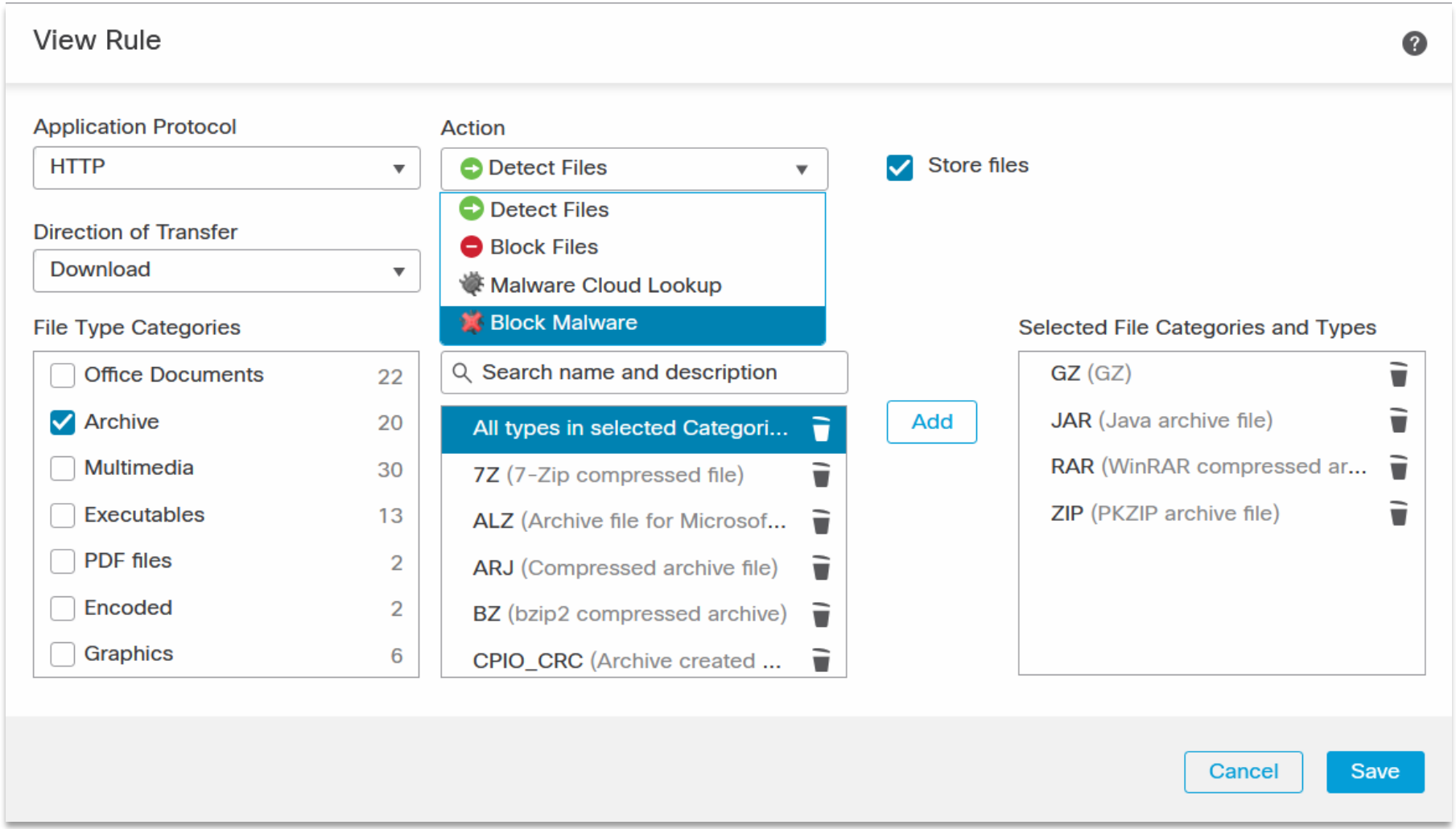
Policies > Access Control > Malware & File > New File Policy



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



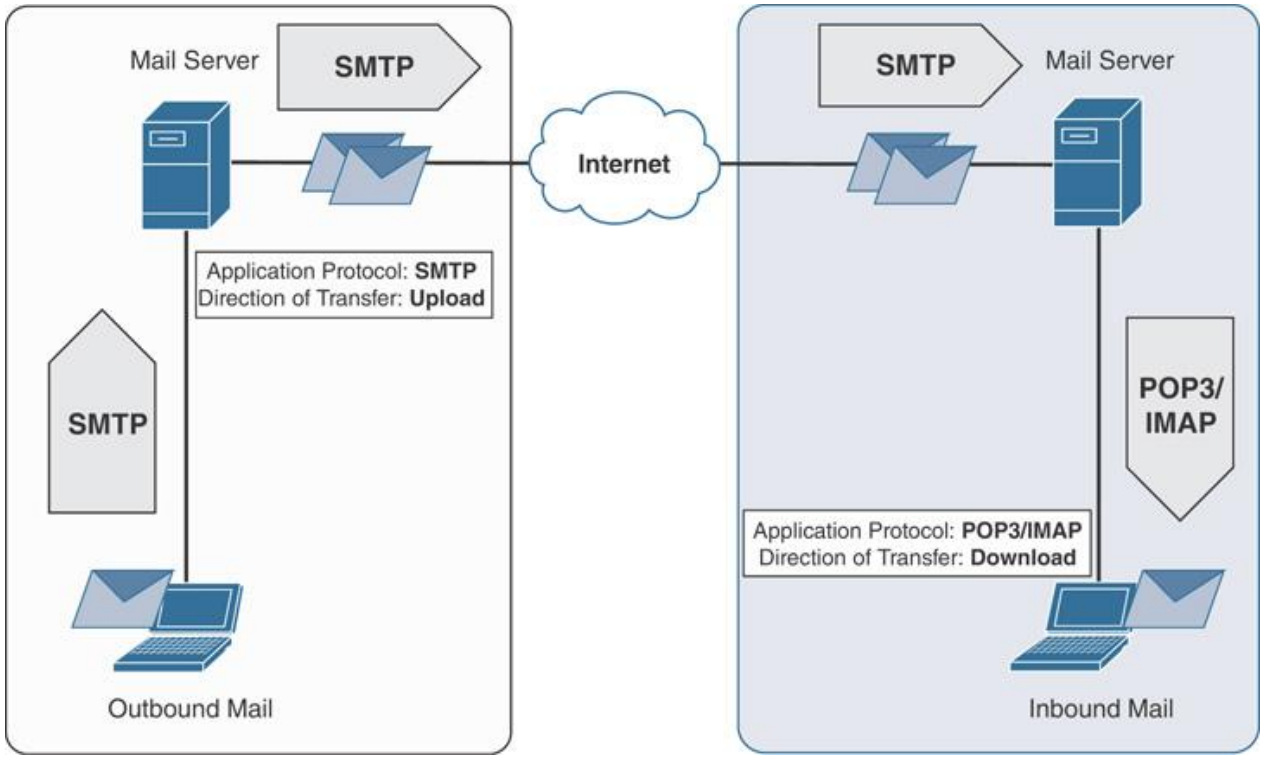
Configuring a File Policy

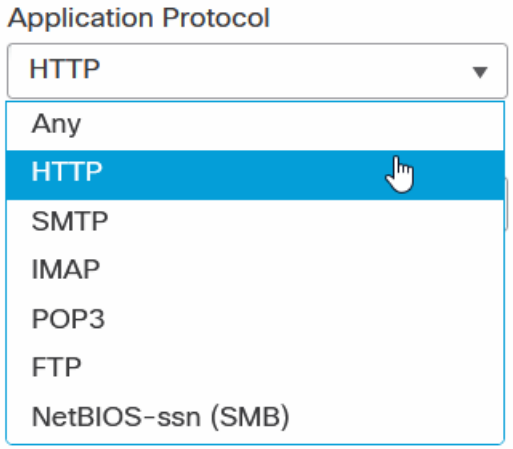
➢ Creating a File Policy

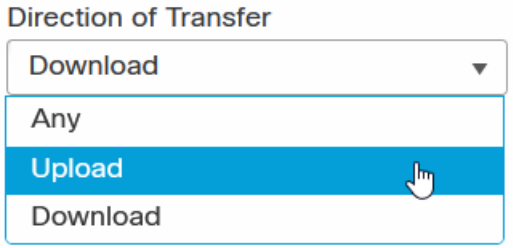
Application Protocol is the protocol by which the files are transferred

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)





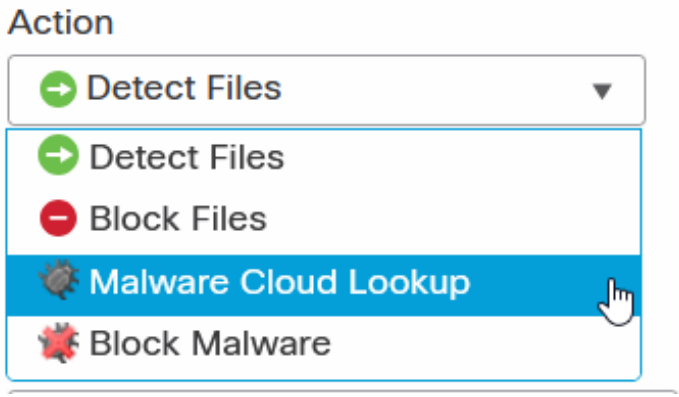


Configuring a File Policy

➢ Creating a File Policy

Action

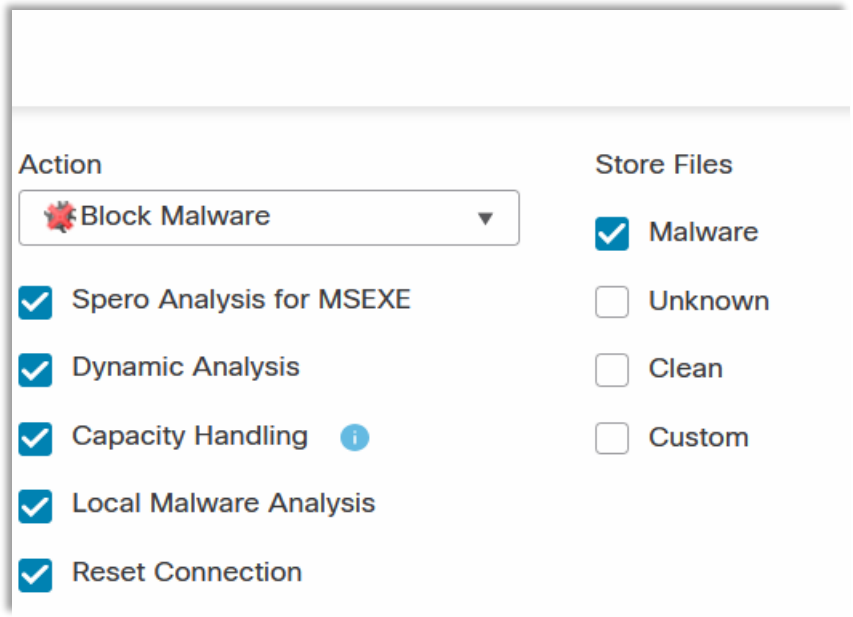
- Detect Files :
  - - Detects a file transfer and logs without interrupting
- Block Files :
  - - Blocks files based on the selected file types
- Malware Cloud Lookup :
  - - Perform malware analysis locally and remotely without interrupting
- Block Malware :
  - - Block inspected file if it is infected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

Configuring a File Policy

➢ Creating a File Policy



If you select Malware actions , You can enable :

- Spero Analysis for MSEXE :

  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

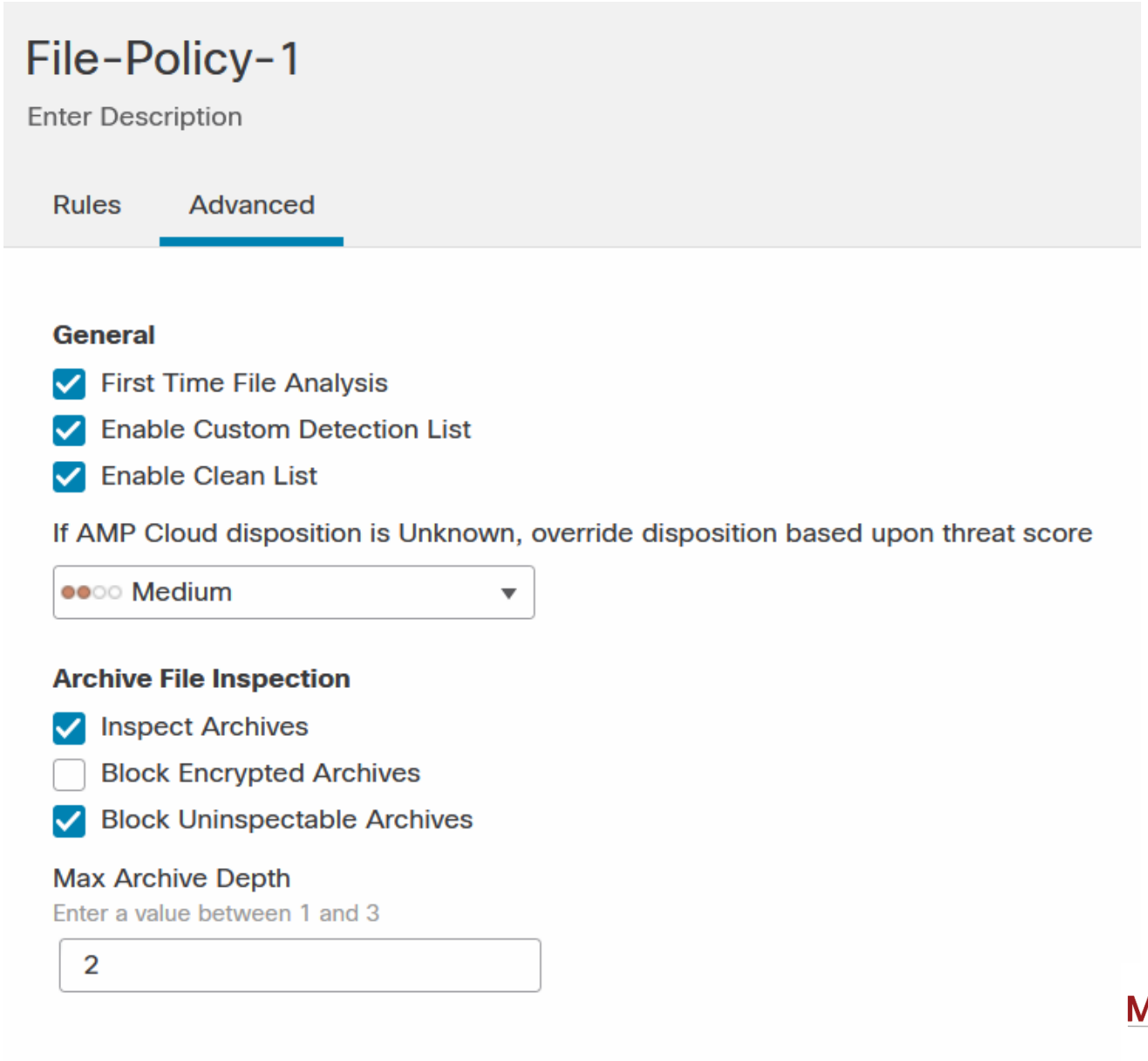
  Close application session before the connection times out

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

Configuring a File Policy

- Creating a File Policy

  Advanced tab

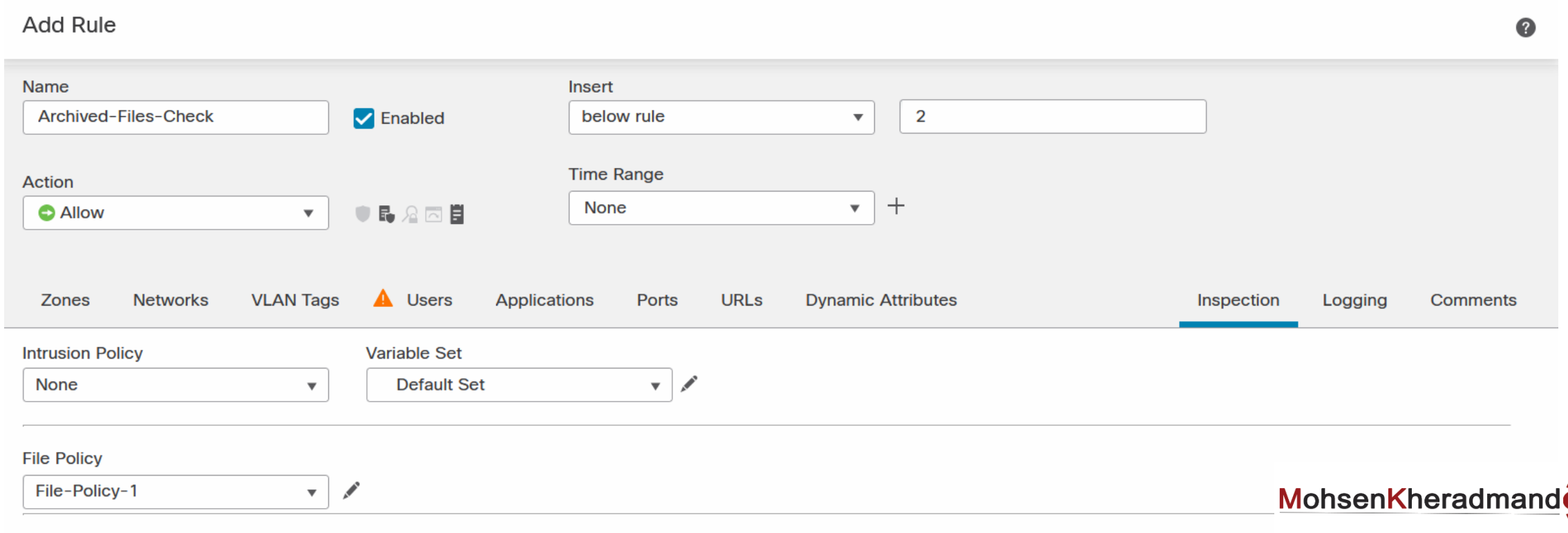


Configuring a File Policy

➢ 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

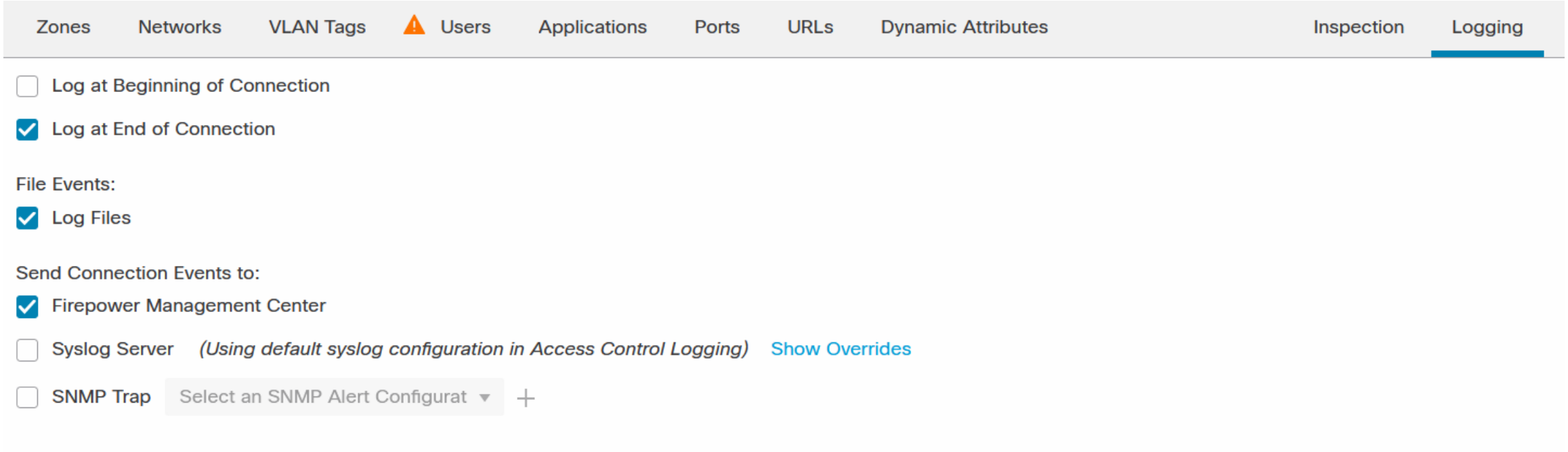
Note : only “allow“, “interactive block“, or “interactive block with reset“ can be used for malware and file policy in ACP



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.

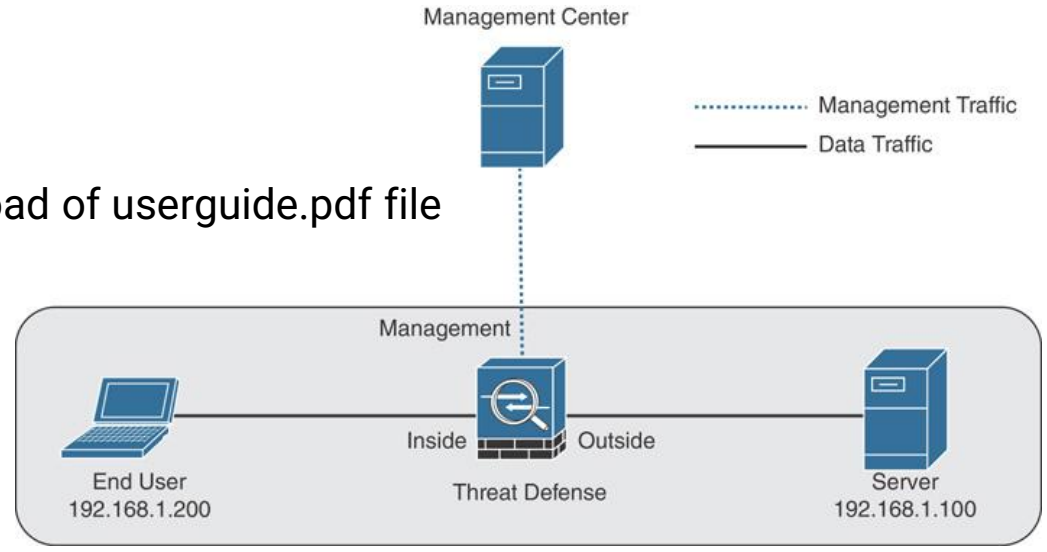


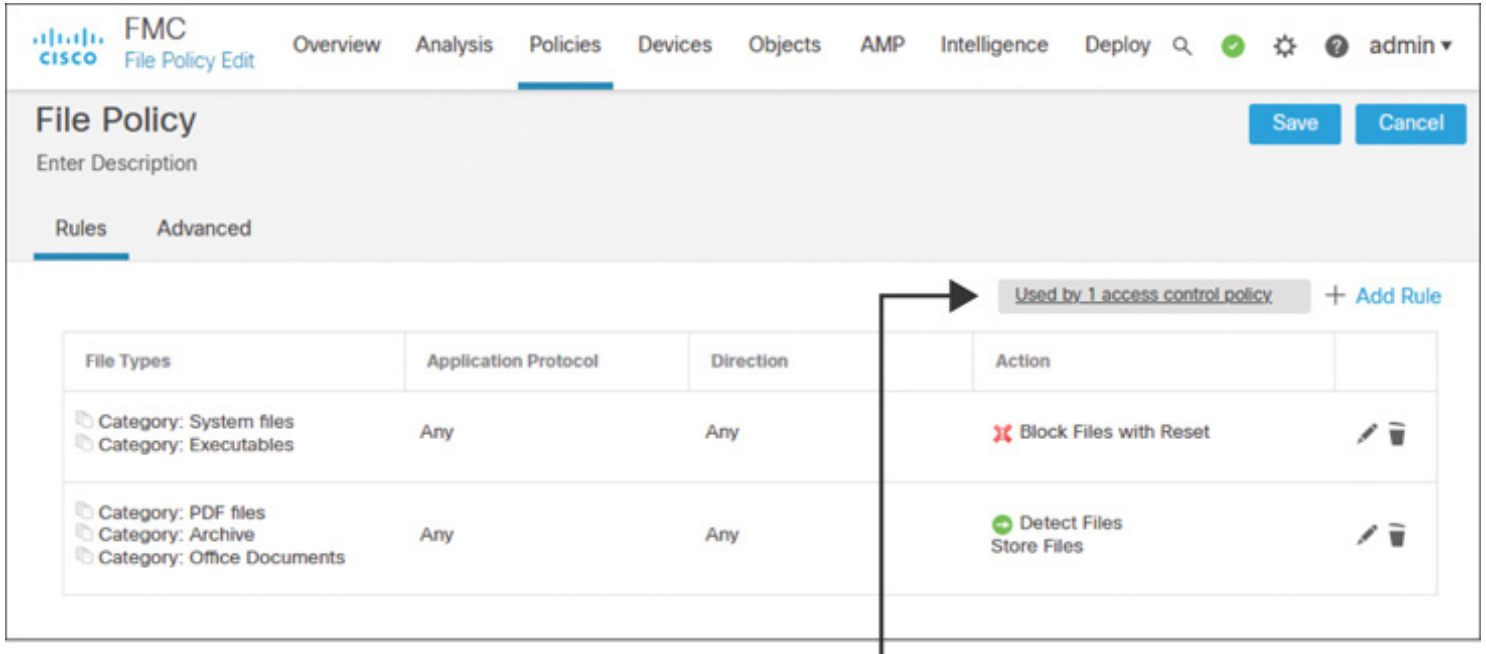
Verification

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



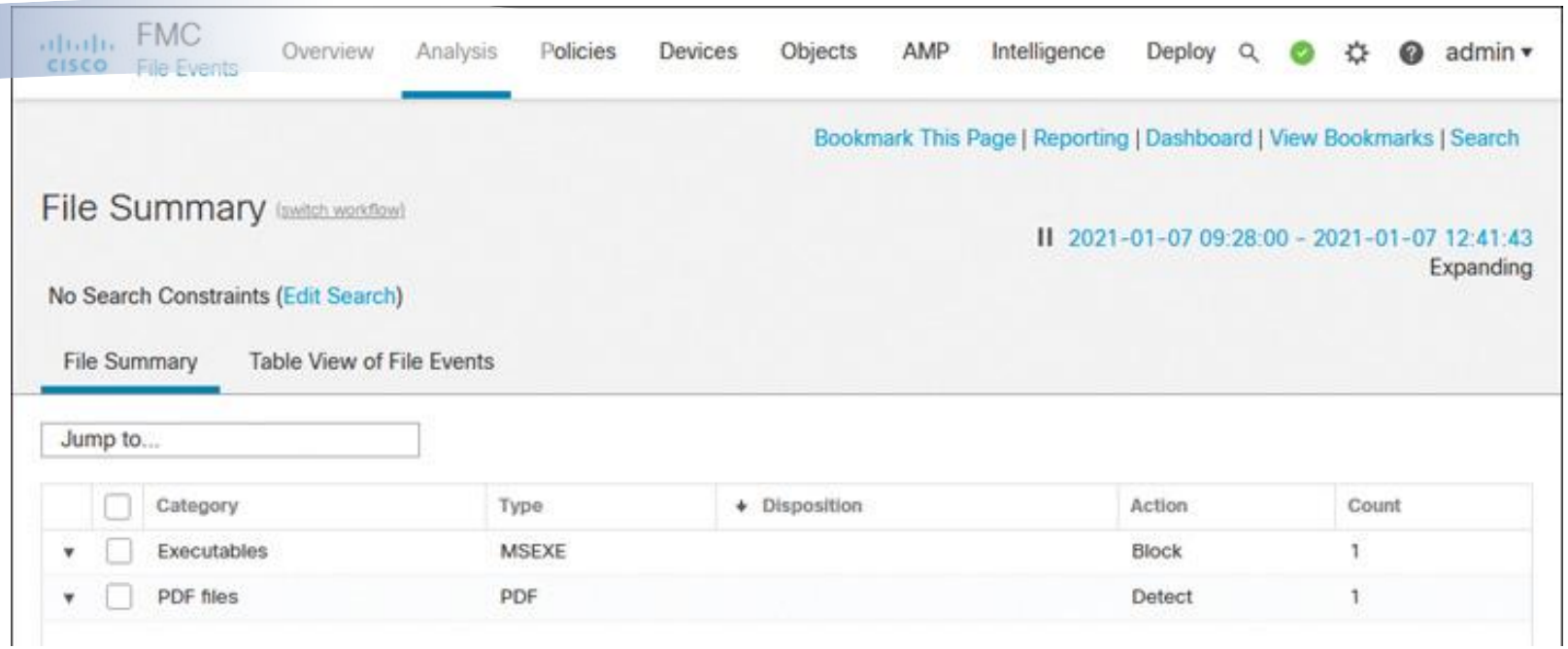


The New Malware and File Policy
Is Used by an Access Control Policy

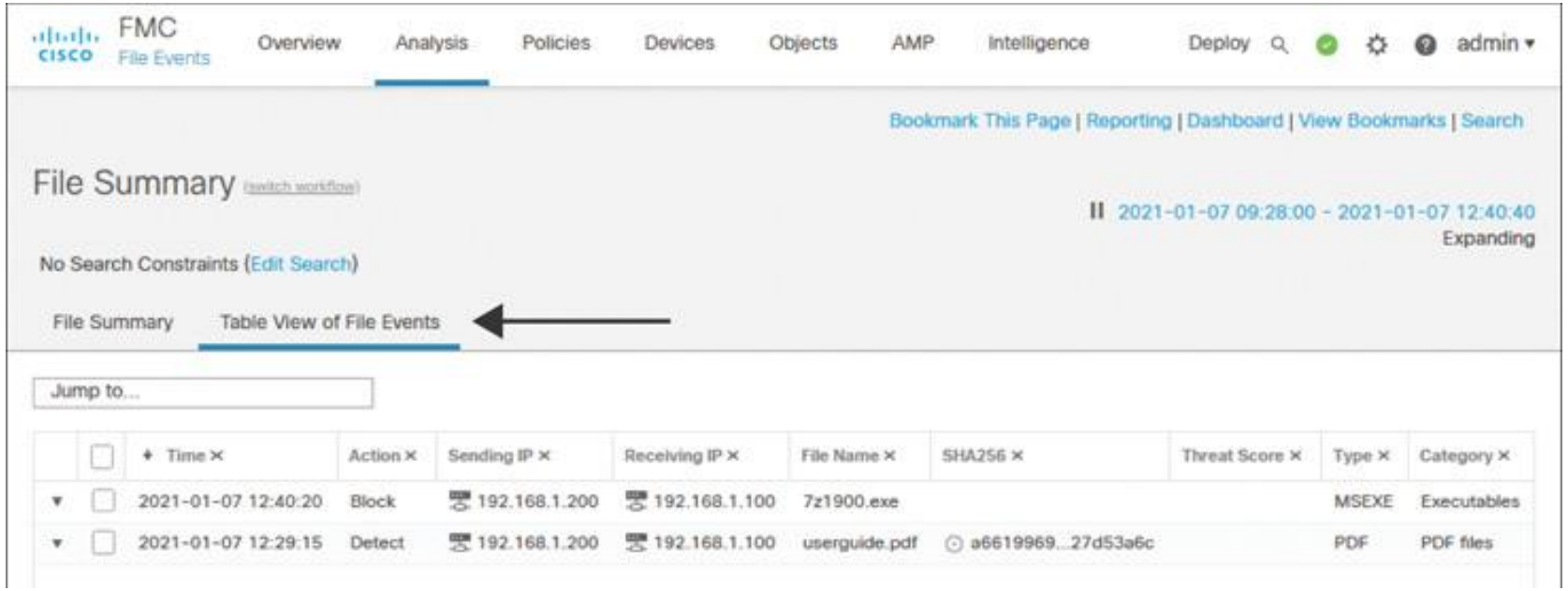
Verification

Example :

Analysis > Files > File Events

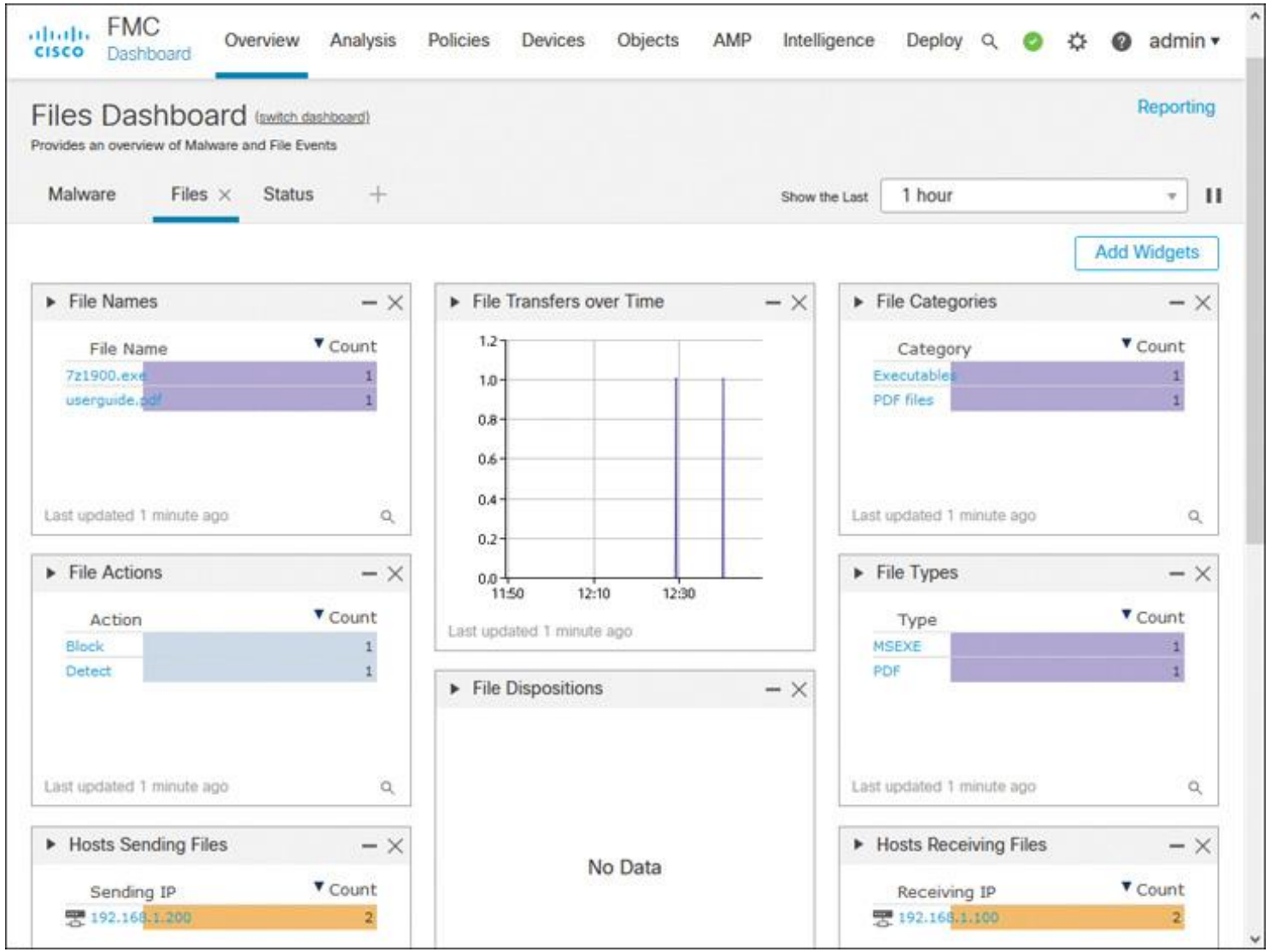


Because the Block Files action does not perform malware analysis, the Disposition column is blank.



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

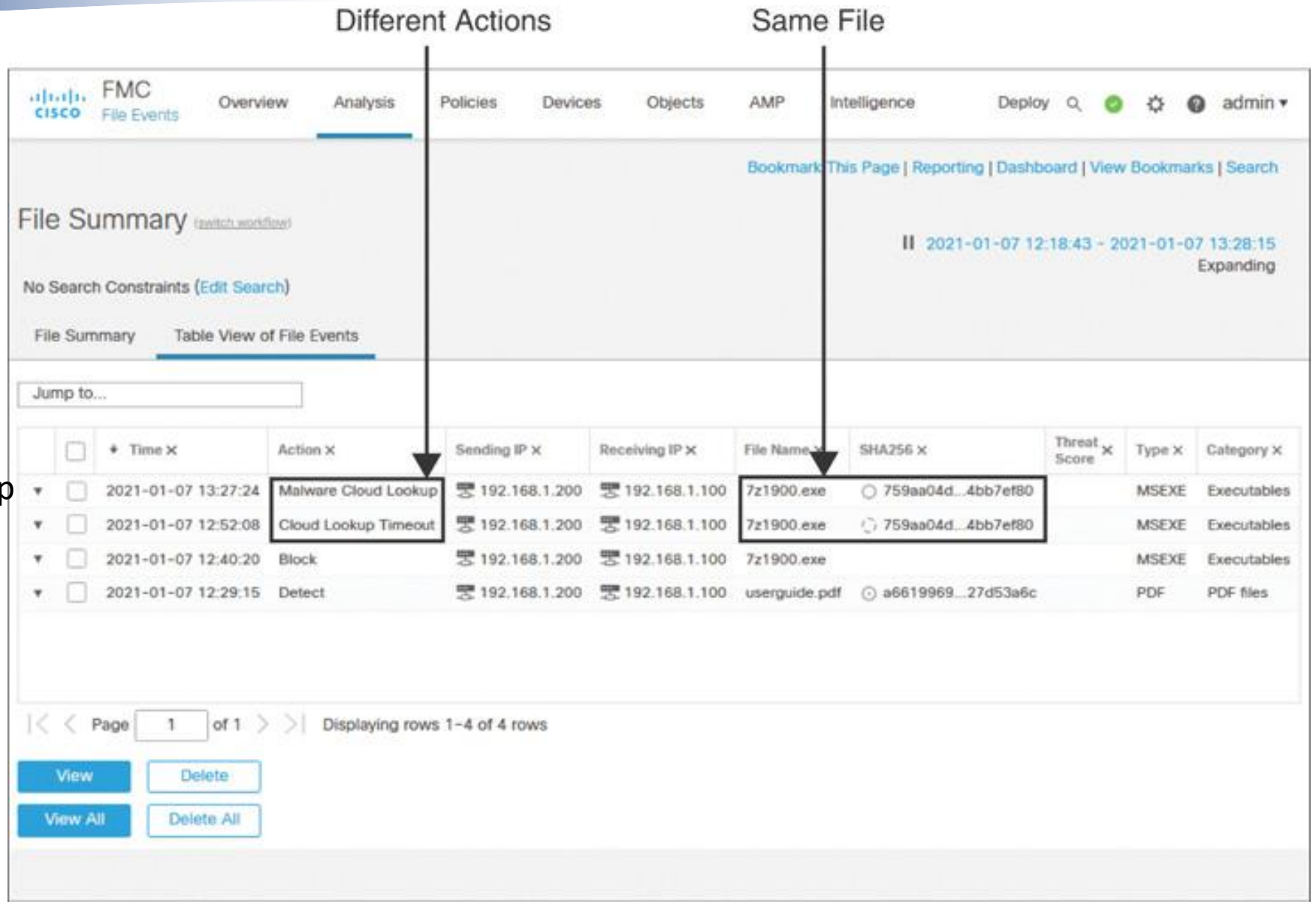
```
> system support firewall-engine-debug

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

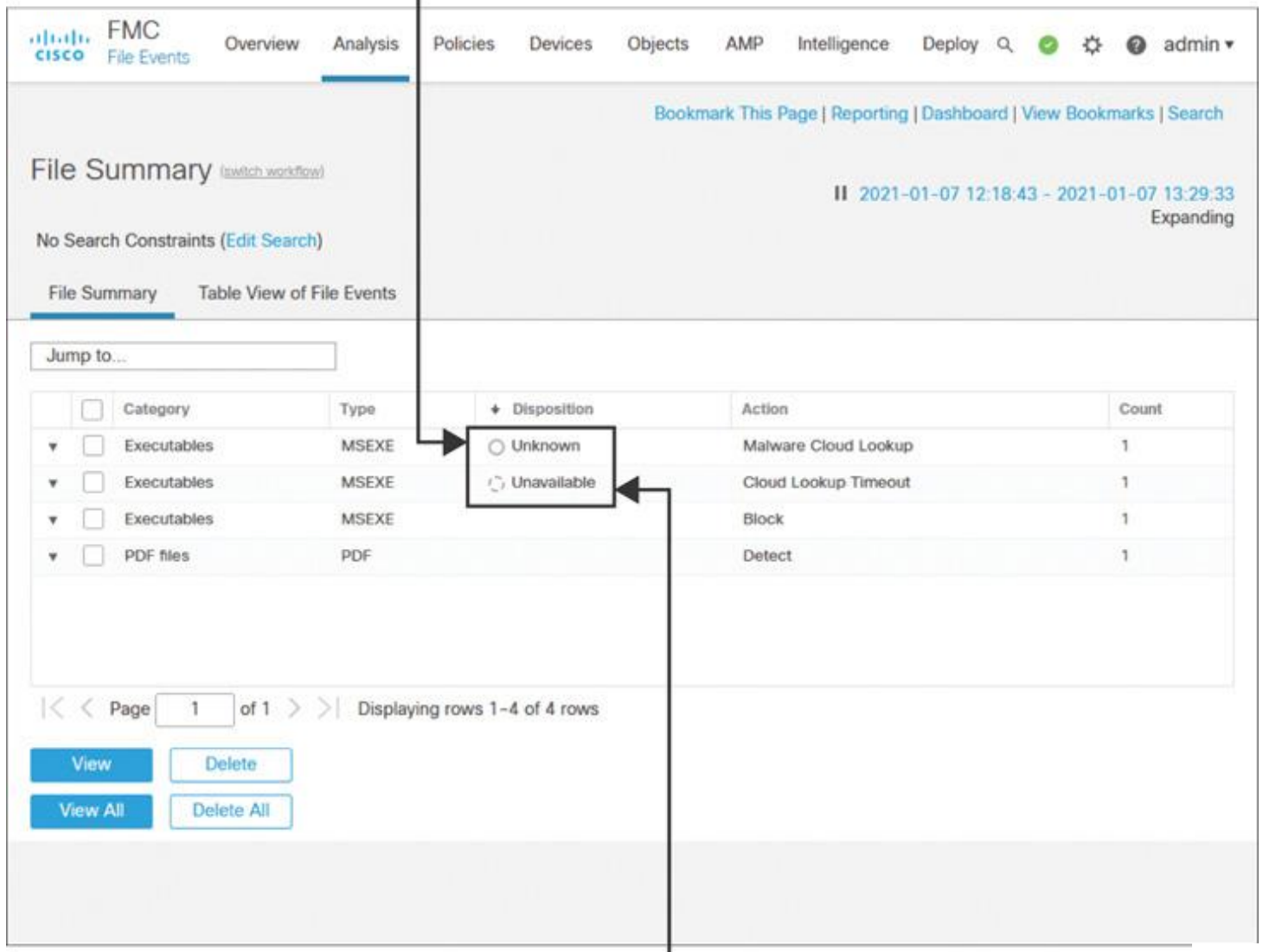
Successful Malware Cloud Lookup



- 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

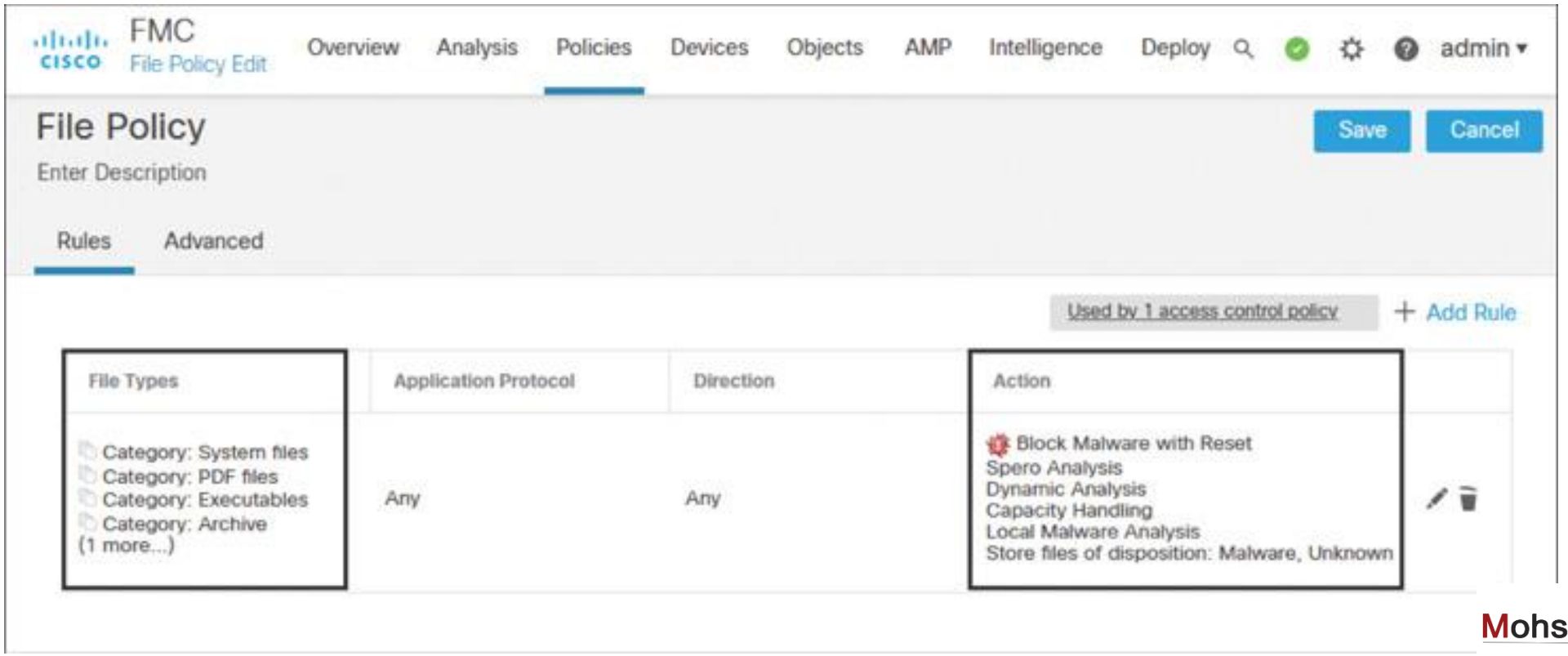


Unavailable Disposition Means That the Management Center Is Unable to Connect to the Cloud or Perform a Lookup for a File

Analyzing Malware Events

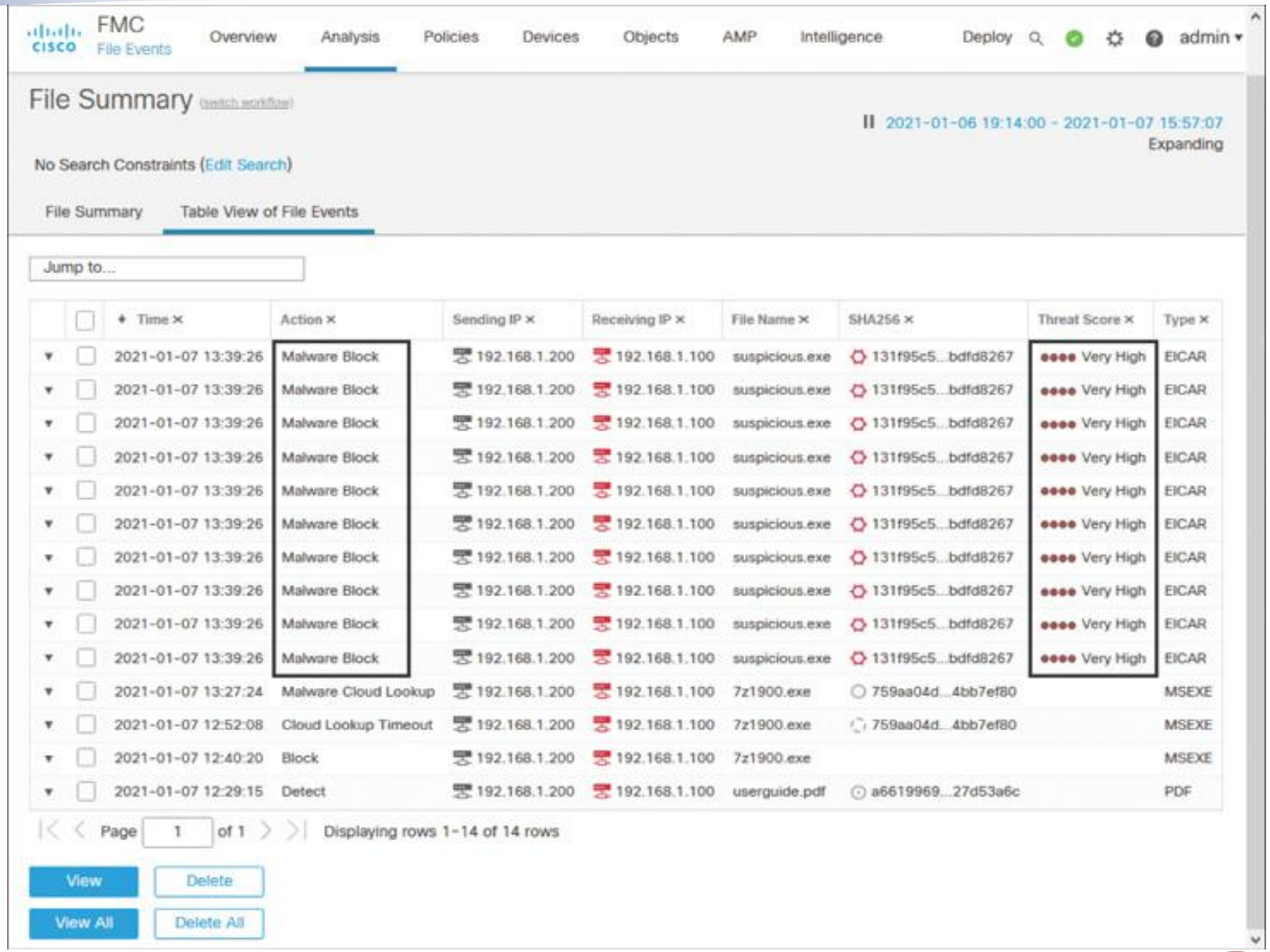
The Cisco cloud can return one of the following dispositions for a query:

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



Analyzing Malware Events

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

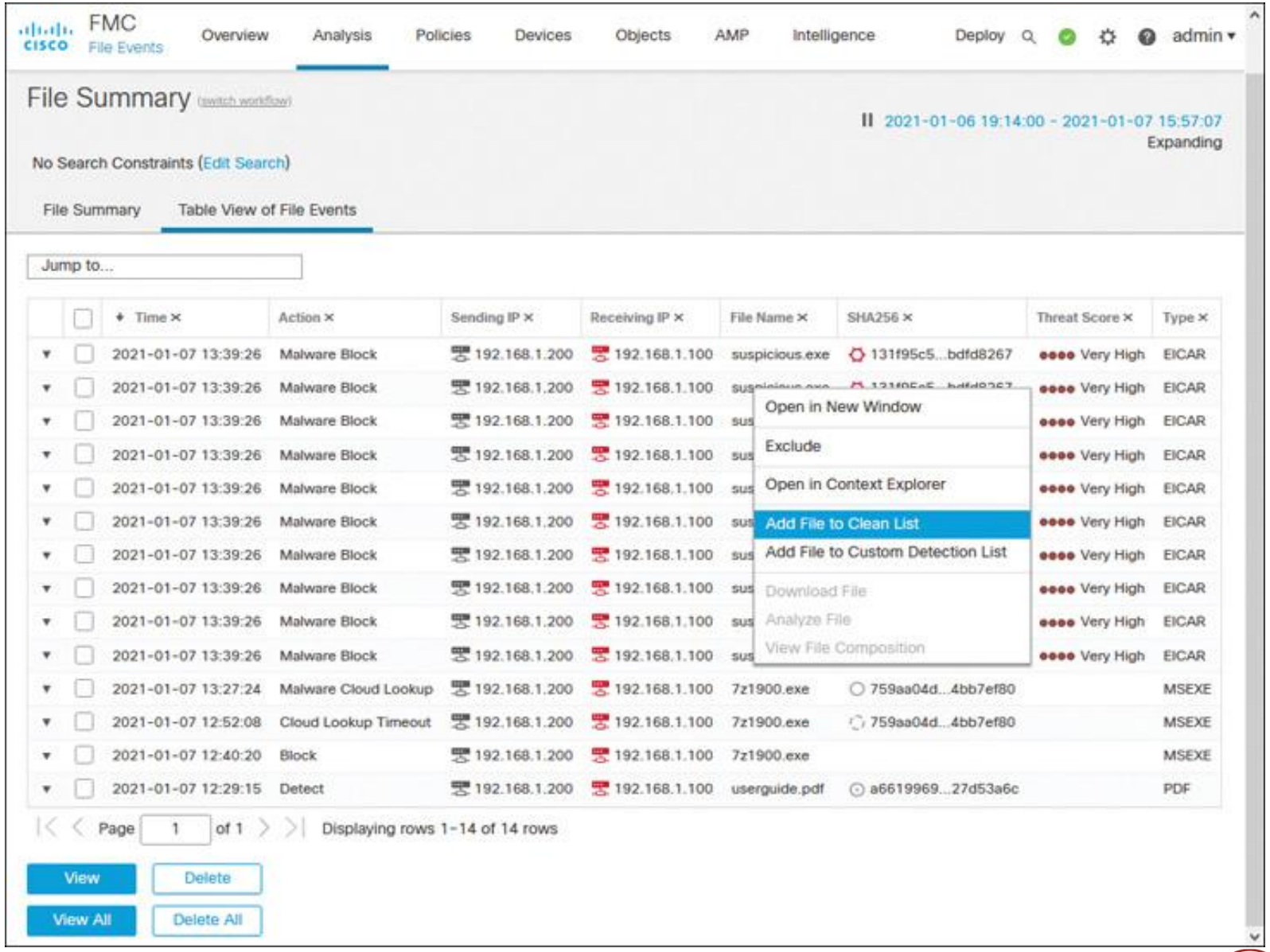


Overriding a Malware Disposition

- 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



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.