

# 27: Control file transfer and AMP

2019年7月21日 14:21

## 目录

1. 文件策略简介
2. File Policy-详细介绍（含配置界面介绍）
3. AMP介绍&限制
4. 许可说明
5. Object-File list
6. File Policy (AMP) - attached to ACP
7. AMP策略配置和效果
8. 最佳实践

## 1: 文件策略简介

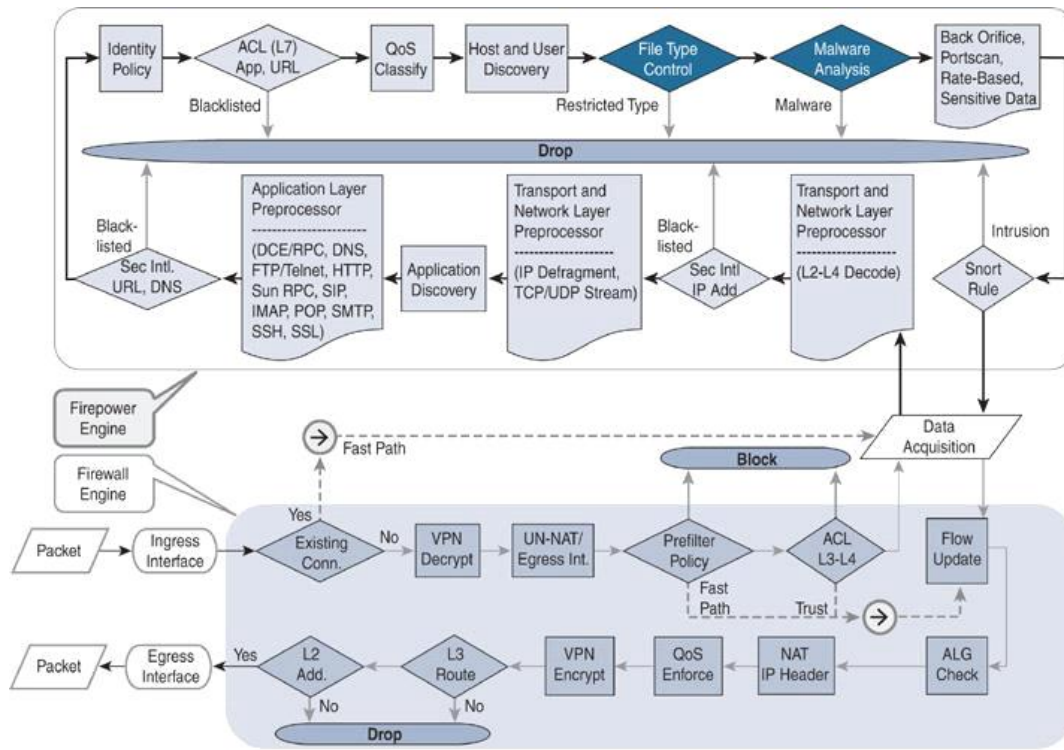
为了管理网络中传输的文件，Firepower提供了File Policy的单独策略，该策略可以检测文件类型：比如媒体文件（.mp3,.mpeg），可执行文件（.exe,.rpm）等，并且FTD可以在传输文件过程中对文件进行潜在恶意软件分析AMP。

**注意，若要block https或者SSL加密的流量的文件控制，则需要进行SSL解密才能进行内容识别**

那么文件策略有两个组件

- 文件类型控制（Threat许可即可）
- 恶意软件分析AMP（Malware许可AMP）

如图所示，文件控制策略在恶意文件分析策略前执行，若文件策略deny文件，则不执行AMP分析



## 2: File Policy 介绍

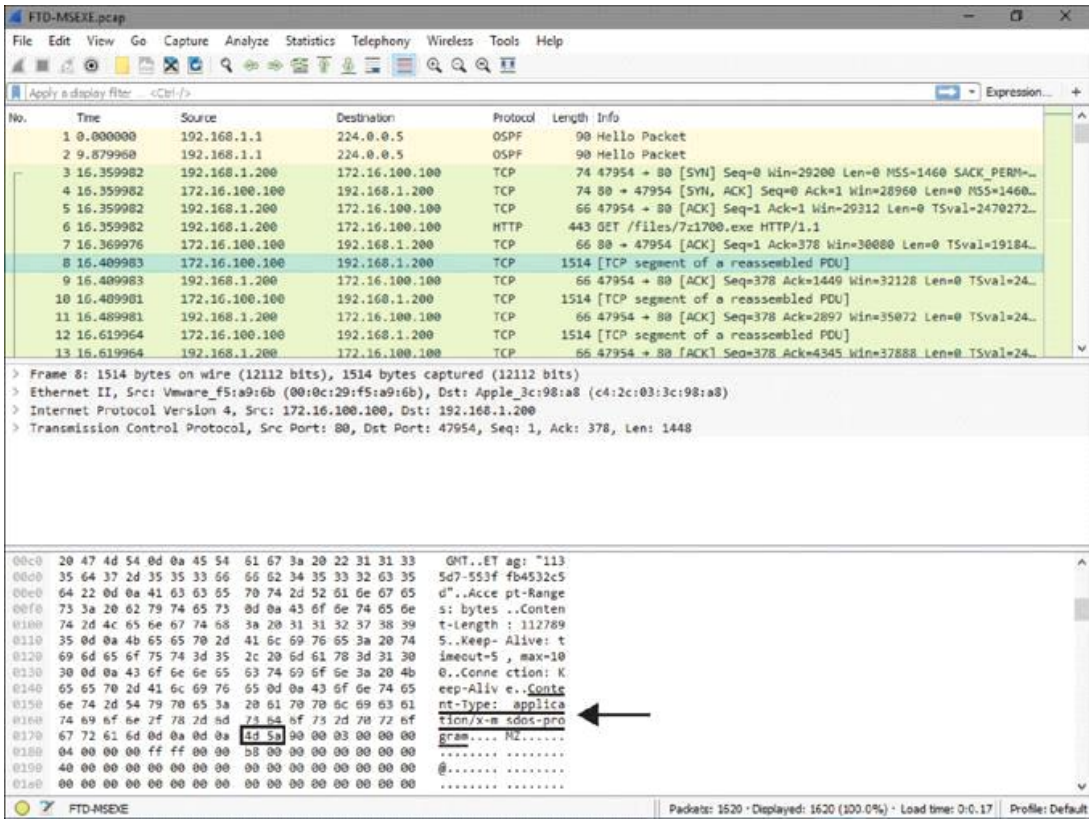
### 2.1: 文件类型检测技术

Firepower使用与文件相关的特殊元数据 { 幻数 (Magic Number) } 来识别文件格式。幻数是编码在文件中的唯一数字序列。当文件在网络中传输时, FTD使用来自数据包流的幻数进行匹配, 便于确定文件格式。

**举例:** 对于Microsoft可执行文件msexec, 幻数=4D 5A, 找到这个编号Snort就会在FTD上应用规则

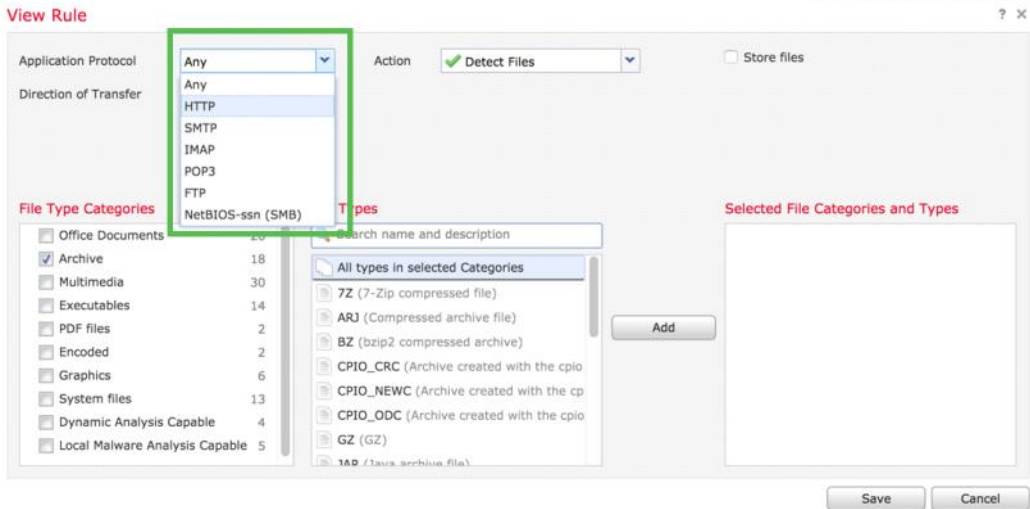
```
file type:MSEXEX; id:21; category:Executables,Dynamic Analysis Capable,Local Malware Analysis Capable; msg:"Windows/DOS executable file "; rev:1; content: | 4D 5A|; offset:0;
```

如下展示了TCP数据包的幻数

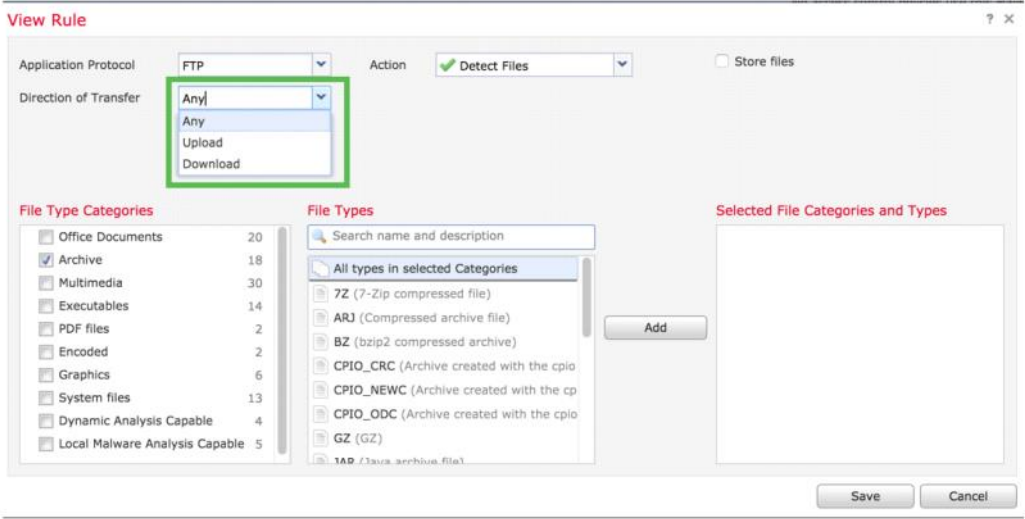


## 2.2: 根据文件的类型检测或阻止文件传输

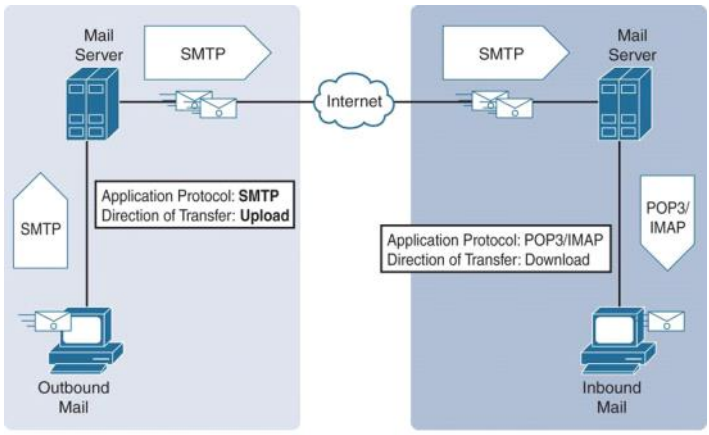
### 2.2.1: 选择在什么协议上检测（以下协议都可以文件传输）



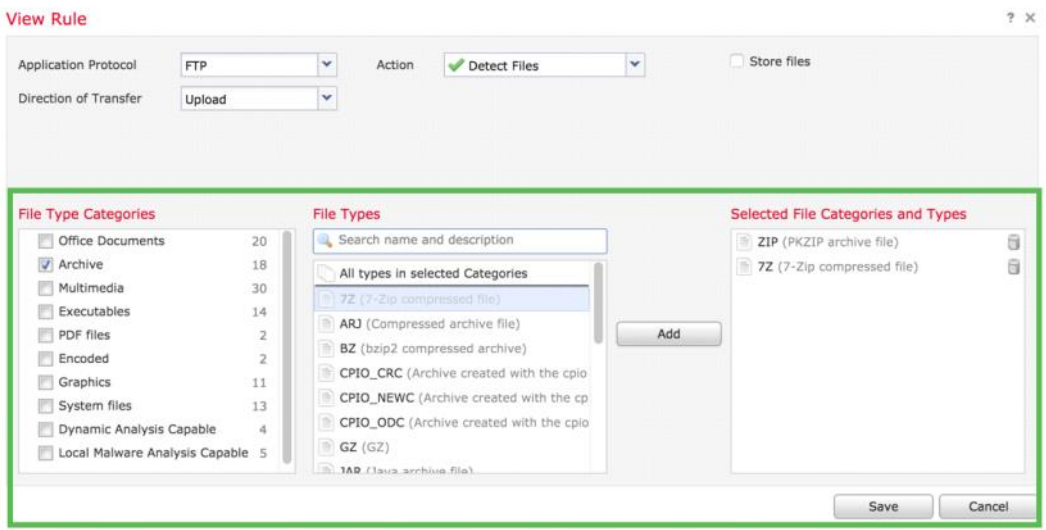
### 2.2.2: 选择检测的文件传输方向，下载/上传



备注：电子邮件的协议只可以选择单向传输（IMAP/POP3/SMTP）

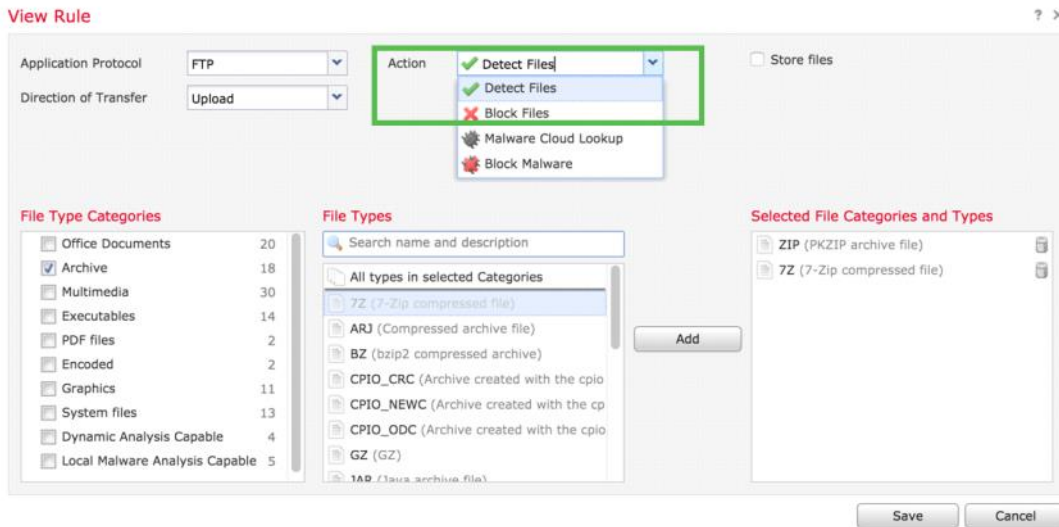


2.2.3: 选择检测哪些文件类型类别，比如这里选择 Archive=压缩类别 文件，选择压缩文件格式7z&ZIP



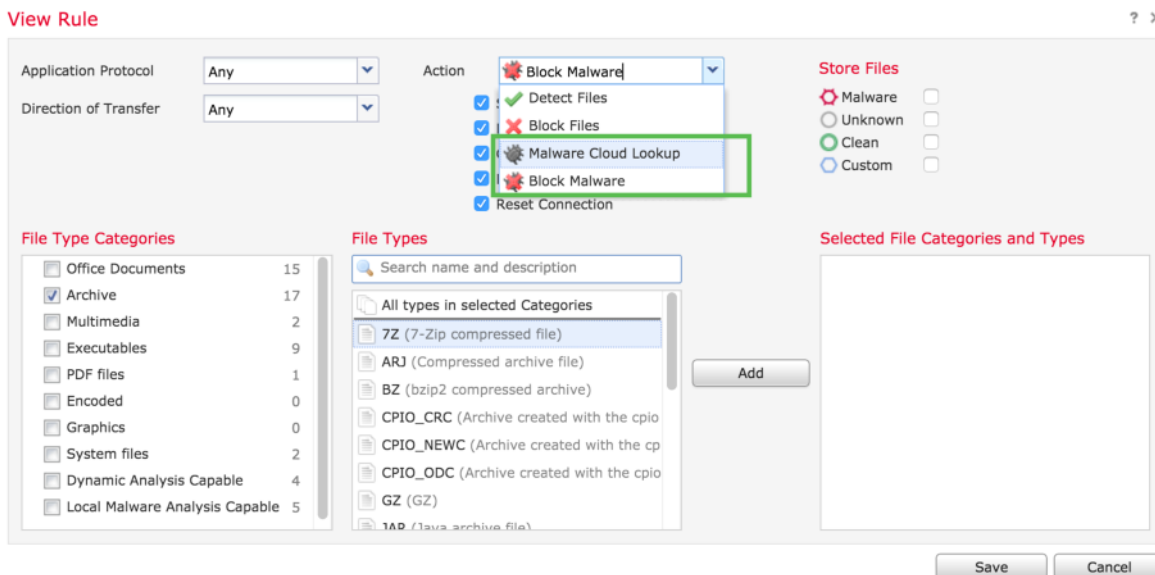
2.2.4: 选择正对 FTD上传的压缩文件类型7z格式的行为

- Detect Files=检测文件，该行为检测文件传输并将其记录为文件事件，不会中断传输
- Block Files = 阻塞文件，检测到文件规则选择的文件格式和类型就会阻塞该文件传输（最好搭配reset connection用）
- Reset connection可以让应用在连接超时前直接关闭

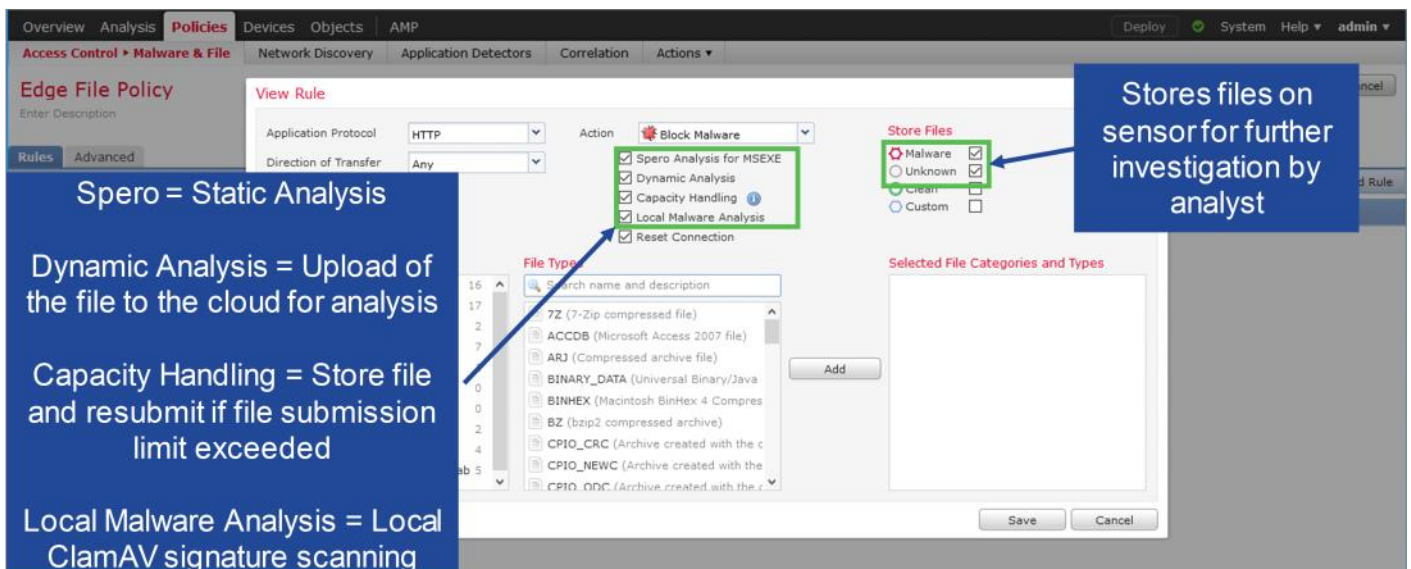


### 2.3: 两个利用AMP的行为（沙盒分析/阻塞恶意文件）

选择递交给云端sandbox分析（提交云端只会分析不会block）



如果是恶意文件就干掉



- **Spero Analysis:** 如果文件是符合条件的可执行文件，则设备可以分析文件的结构并将生成的Spero签名提交给AMP Threat Grid云。云使用此签名来确定文件是否包含恶意软件。

- **Local Malware Analysis:** 使用本地恶意软件检查引擎 (ClamAV) , 设备会检查符合条件的文件, 如果文件包含恶意软件并且文件规则已配置为阻止它, 则会阻止它, 并生成恶意软件事件。  
该设备还会生成文件组合报告, 详细说明文件的属性, 嵌入对象和可能的恶意软件。
- **Dynamic Analysis:** 如果设备将文件预分类为可能的恶意软件, 则无论设备是否存储文件, 它都会将这些文件提交给AMP Threat Grid云或AMP Threat Grid on-premises设备进行动态分析。AMP Threat Grid云或本地AMP Threat Grid设备在沙箱环境中运行该文件, 以确定该文件是否为恶意文件, 并返回描述文件包含恶意软件的可能性的威胁评分。从威胁评分中, 您可以查看动态分析摘要报告, 该报告详细说明了云分配威胁评分的原因。
- **Capacity Handling:** 容量处理→存储文件并在超出文件提交限制时重新提交
- **Store Files:** 将文件存储在**传感器上 (FTD)** , 供分析师进一步调查  
存储文件可以基于AMP给文件定义的类型进行存储, 比如只存储判定为恶意文件的文件到FTD, 或者只存储干净的文件

## 2.5: File Disposition—分类

A file can have one of the following file dispositions as a result of addition to a file list, or due to threat score: 由于添加到文件列表或威胁评分, 文件可以具有以下文件排列之一:

- **Malware**
- **Clean**
- **Unknown**
- **Custom Detection**
- **Unavailable**

A SHA-256 disposition is cached on FMC 在FMC上缓存SHA-256排列

- **Clean** disposition is cached for 4 hours
- **Unknown** disposition is cached for 1 hour
- **Malware** disposition is cached for 1 hour

## 2.6: 由于文件被添加到文件列表或威胁评分, 文件可以具有以下文件处置之一:

- **Malware:** 表示AMP云将文件归类为恶意软件, 本地恶意软件分析识别出恶意软件, 或者文件的威胁分数超过文件策略中定义的恶意软件阈值。
- **Clean:** 表示AMP云将文件归类为干净, 或者用户将文件添加到干净列表中。
- **Unknown:** 表示系统查询了AMP云, 但该文件尚未分配处置;换句话说, AMP云尚未对文件进行分类。
- **Custom Detection:** 表示用户将文件添加到自定义检测列表。
- **Unavailable:** 表示系统无法查询AMP云。你可能会看到这种倾向的一小部分事件;这是预期的行为。

## 2.7: File Policy (AMP) – File Policy Advanced Options

The screenshot shows the 'File Policy Advanced Options' configuration page. It includes sections for 'General' and 'Archive File Inspection'. Callouts provide the following explanations:

- Submit a file for file analysis that the system detects for the first time...**: This callout points to the 'First Time File Analysis' checkbox, which is checked.
- These 2 options are related to files in the Custom-Detection-List and Clean-List Objects**: This callout points to the 'Enable Custom Detection List' and 'Enable Clean List' checkboxes, both of which are checked.
- A file with Threat Score 'Very High' will be considered a Malware**: This callout points to the 'Mark files as malware based on dynamic analysis threat score' dropdown menu, which is set to 'Very High'.
- Check for Malware in compressed files**: This callout points to the 'Inspect Archives' checkbox, which is unchecked.

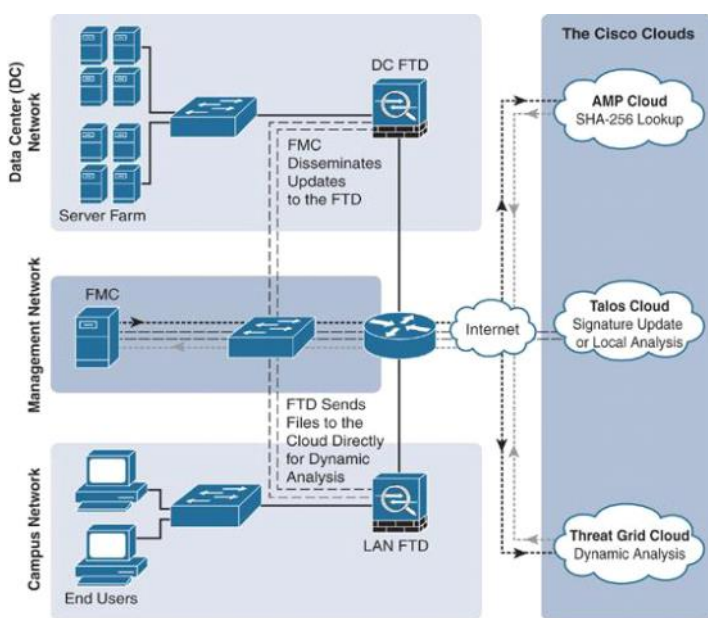
- **First Time Files Analysis:** 提交文件以进行系统首次检测到的文件分析。该文件必须与配置为执行恶意软件云查找和Spero, 本地恶意软件或动态分析的规则匹配。如果禁用此选项, 则首次检测到的文件将标记为“未知”处置。
- **Enable Custom Detection List & Enable Clean List:** 这两个选项与Custom-Detection-List和Clean-List Objects中的文件相关
- **Mark files as malware based on dynamic analysis threat score:** 威胁评分为“非常高”的文件将被视为恶意软件
- **Inspect Archives:** 检查压缩文件中的恶意软件

### 3: Advanced Malware Protection(AMP) 高级恶意代码保护



Cisco将AMP和Firepower集成一起，AMP可以让FTD在网络传输文件时，针对潜在恶意软件和病毒进行分析。为了分析过程并节省资源，FTD可以执行两种类型的恶意软件分析：本地/动态分析

#### 3.1: 文件分析原理☆☆



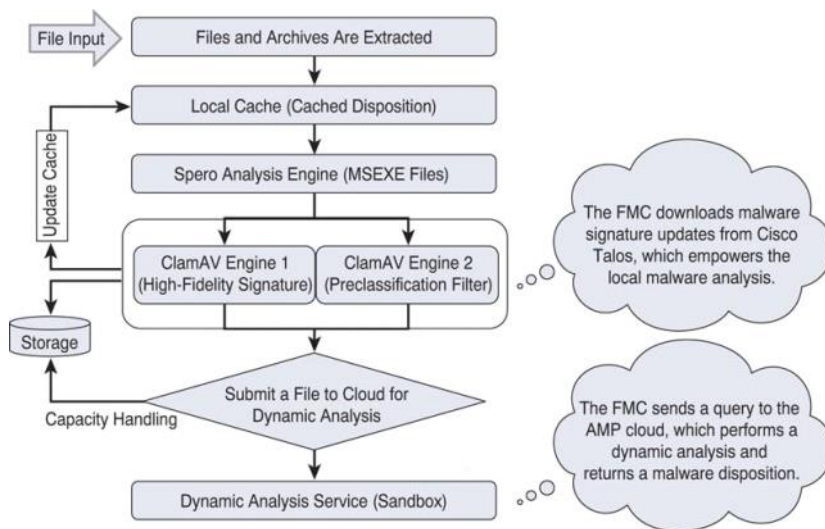
FTD默认会计算文件的SHA-256哈希值，并使用这个值确定文件的处理方式。FMC在将新查询发送给AMP Cloud前，会对缓存的处置执行中查找，这样可以提供更快查找结果并提高整体性能。

根据用户的文件策略配置操作，Firepower可以按如下顺序执行额外的高级分析

- **Spero analysis:** Spero分析引擎只检查MSEXE文件，它会分析MSEXE文件的结构，并将Spero特征提交给云
- **Local analysis:** FTD会使用两类规则集进行本地分析（高保真/预分类规则），FMC会从Talos下载高保真恶意软件特征，并将规则传递给FTD，FTD根据已知恶意软件匹配模式并分析文件，也会使用文件预分类过滤器优化资源利用率
- **Dynamic analysis:** 动态分析功能将捕获的文件提交到Threat Grid 沙箱以进行动态分析。沙箱环境可以在云中或在本地使用。经过分析，沙箱会返回威胁评分（一种将文件视为潜在恶意软件的评分系统）。文件策略允许您调整动态分析威胁评分的阈值级别。因此，您可以定义FTD设备何时应将文件视为潜在的恶意软件。

备注：动态分析有容量处理选项，让Firepower系统无法和云沙盒提交文件时暂停对文件评分

#### 3.2: Firepower的AMP技术架构工作流程



- 先比较文件的hash值和病毒库hash值有没有匹配的，有直接判定为病毒
- 如果没有，执行沙盒运行/解析该文件是否有问题

### 3.3: AMP for Networks

- |   |   |
|---|---|
| a. Snort understands network protocols  | Snort理解网络协议 (snort引擎)   |
| b. Files can be carved out of the network traffic   | 文件可以从网络流量中划分出来  |
| c. AMP detection techniques can be applied to the file  | AMP检测技术可应用于文件   |
| <ul style="list-style-type: none"> <li>• Hash lookups - both SHA 256 and Spero hashes</li> <li>• Local malware analysis (Clam AV) on the firewall</li> <li>• Submitting the file to Cisco Threat Grid for sandboxing</li> </ul> | 散列查找 - SHA 256和Spero散列<br>防火墙上的本地恶意软件分析 (Clam AV)<br>将文件提交到Cisco Threat Grid以进行沙盒处理(公网) |
| d. File transfers can be blocked  | 可以阻止文件传输  |
| e. Based on file type - this can be determined using the first block of the file. The entire file will be blocked.  | 基于文件类型 - 可以使用文件的第一个块来确定。整个文件都是受阻。   |
| f. Based on malware verdict - this requires analyzing the entire file. Only the last piece of the file transfer will be blocked.  | 基于恶意软件判决 - 这需要分析整个文件。只有文件的最后一块传输将被阻止。   |

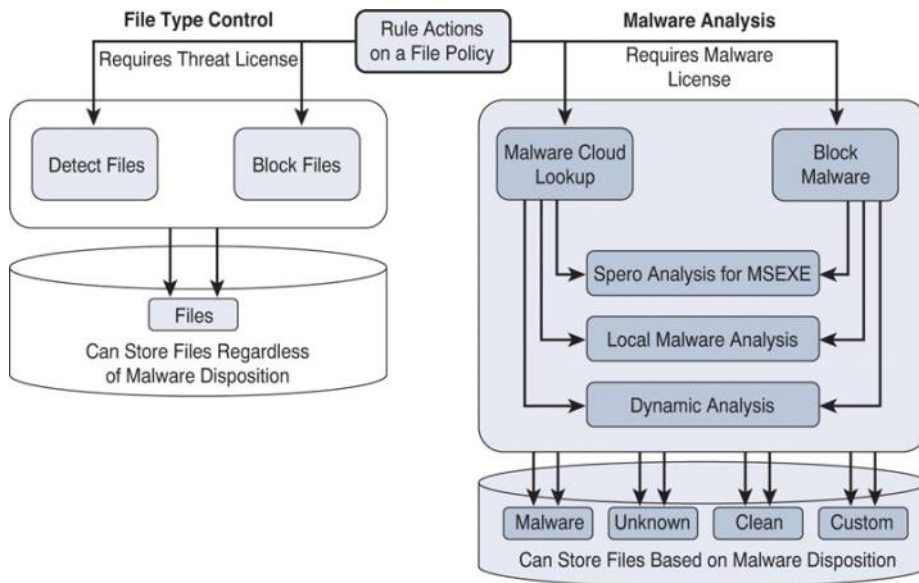
### 3.4: AMP策略的限制

- AMP策略需要购买AMP的许可 (将文件执行恶意代码检测)
- AMP策略和APP应用控制策略有冲突, APP控制优于AMP执行, 并且执行APP控制后可能不会再执行AMP策略
- AMP检测文件的最大最小单元都有默认限制, 可以更改
- 发送给AMP-Cloud沙盒分析: FTD/FMC必须可以连接沙盒的公网域名
- 高于100M的文件不会发送给AMP-Cloud
- 每个ACP规则只可以调用一个AMP策略 (注意这里是规则调用策略, 而不是规则调用规则)

## 4: 许可说明

- 如果拥有Threat许可, Firepower可以开启文件类型控制, 那么可以控制指定类型的文件传输
- 如果想针对文件执行AMP分析, 分析文件是不是包含恶意代码, 或者是不是病毒文件, 则需要AMP许可 (Malware)

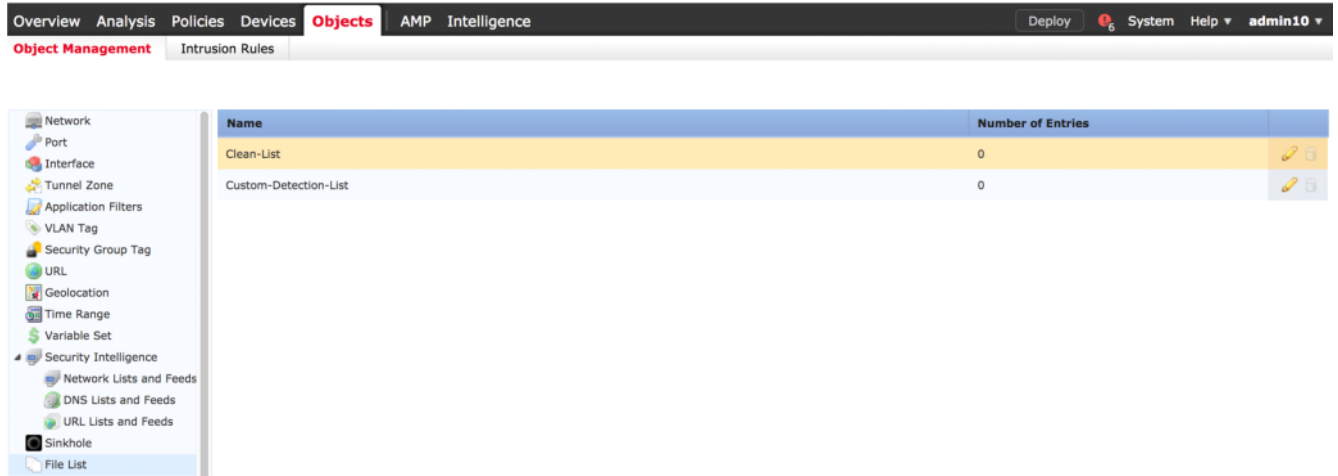




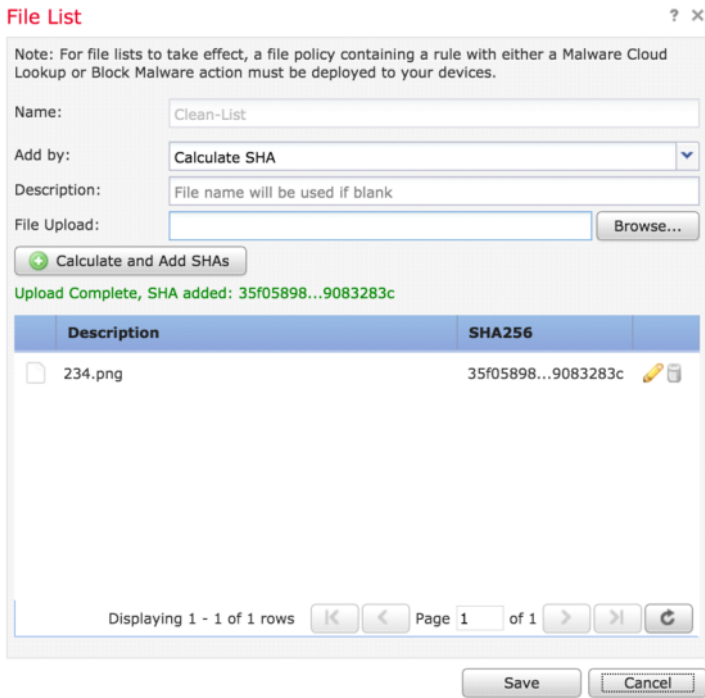
## 5: Objects—File list

该功能可以覆盖Cisco检测的结果，如果CiscoCloud判定文件为恶意文件，其实不是，你可以利用这个功能放行文件

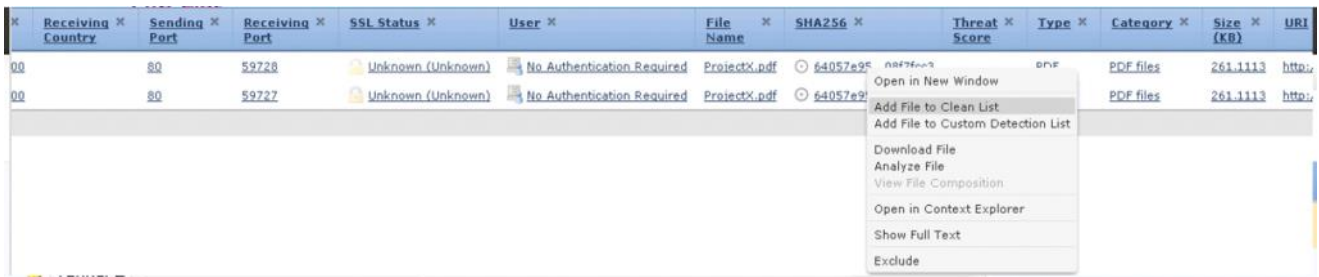
5.1: 默认有两个object-file list，一个干净的，一个自定义



5.2: 将一个23.png的文件添加到干净的object-file list中



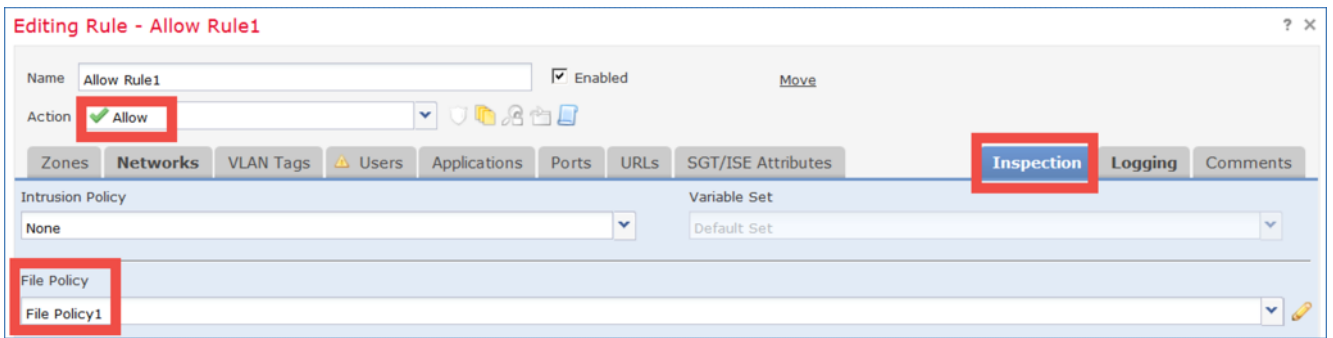
5.3: 可选将一个文件添加到干净的object-file list中



## 6: File Policy (AMP) – attached to ACP

### 6.1: 应用文件策略到ACP

A File Policy can be attached (添加) to the Access Control Policy rules that have action **Allow**

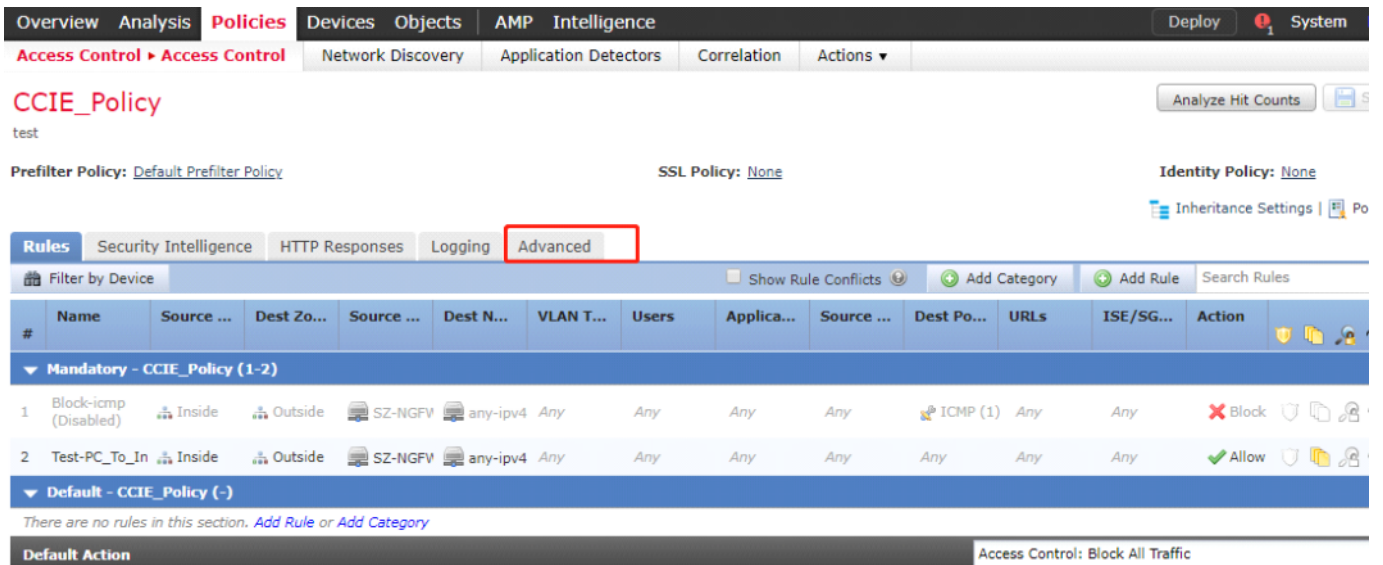


The icon denotes that a **File Policy** is attached to the ACP Rule



## 6.2: File Policy (AMP) - ACP Advance tuning

每个ACL都有默认的AMP规则参数，比如检查文件的大小，发送给AMP-Cloud文件大小设定可以在ACL中更改



Overview Analysis **Policies** Devices Objects AMP Intelligence Deploy System Help admin

Access Control Access Control Network Discovery Application Detectors Correlation Actions

### CCIE\_Policy

test

Prefilter Policy: [Default Prefilter Policy](#) SSL Policy: [None](#) Identity Policy: [None](#)

[Inheritance Settings](#) [Policy Assignments](#)

Rules Security Intelligence HTTP Responses Logging **Advanced**

**Identity Policy** None

**SSL Policy Settings**

SSL Policy to use for inspecting encrypted connections None

**Prefilter Policy Settings**

Prefilter Policy used before access control Default Prefilter Policy

**Network Analysis and Intrusion Policies**

Intrusion Policy used before Access Control rule is determined No Rule Active

Intrusion Policy Variable Set Default-Set

Default Network Analysis Policy Balanced Security and Connectivity

**Threat Defense Service Policy**

Threat Defense Service Rule(s) 0

**Files and Malware Settings**

Limit the number of bytes inspected when doing file type detection	1460
Allow file if cloud lookup for Block Malware takes longer than (seconds)	2
Do not calculate SHA256 hash values for files larger than (in bytes)	10485760
Minimum file size for advanced file inspection and storage (bytes)	6144
Maximum file size for advanced file inspection and storage (bytes)	1048576
Minimum file size for dynamic analysis testing (bytes)	6144
Maximum file size for dynamic analysis testing (bytes)	1048576

**Adaptive Profiles - Enable profile updates** Disabled

**Performance Settings**

Pattern Matching Limits - Max Pattern Match States to Analyze Per Packet 5

Performance Statistics - Sample Time (seconds) 300

Regular Expression - Limit Default Value

Regular Expression - Recursion Limit Default Value

Intrusion Event Logging Limits - Max Events Stored Per Packet 8

**Latency-Based Performance Settings**

Applied from Installed Rule Update true

**Packet Handling** Enabled

Packet Handling - Threshold (microseconds) 256

**Rule Handling** Enabled

Rule Handling - Threshold (microseconds) 512

Rule Handling - Consecutive Threshold Violations Before Suspending Rule 3

Rule Handling - Suspension Time (seconds) 10

1. 默认情况下，只会检查前1460字节
2. 等待云响应的时间有多长
3. 默认情况下，仅针对最大10MB的文件检查恶意软件
4. 不会捕获小于6KB的文件
5. 不会捕获大于1MB的文件。这还指定了检查的归档（压缩文件）的大小。
6. 将发送到Cloud for Dynamic Analysis的最小和最大文件大小

## 7: 文件策略后效果展示

Overview **Analysis** Policies Devices Objects System Help Global demo\_user

Context Explorer Connections Intrusions **Files Malware Events** Hosts Users Vulnerabilities Correlation Custom Lookup Search

Bookmark This Page Report Designer Dashboard View Bookmarks Search

### Malware Summary

Malware Summary Table View of Malware Events

No Search Constraints (Edit Search)

Jump to...

Detection Name	File Name	File SHA256	File Type	Count
	1515658069-1-1517134105-1517360776-1515657333-1515657926-mpas-d_bd_1.225.2931.0.exe	60c8ad6d_d15a411e	MSEXE	76
	1515658069-1-1517134093-1517360764-1515657321-1515657914-5563f5a3033de5864b98090591358062.exe	ae23cdc2_34cf5b73	MSEXE	63
	1515658069-1-1517137894-1517364565-1515661122-1515661715-AM_Delta_Patch_1.225.3050.0.exe	ab9d1518_8f8962d0	MSEXE	45
W32.A39AB89113-95.SBX.TG	1515658069-1-1517137875-1517364546-1515661103-1515661696-grd2.xls	a39ab891_b1fd35dd	MSOLE2	39
	1515658069-1-1517137859-1517364530-1515661087-1515661680-Cineget_Installer.exe	90a67a98_8a58b680	MSEXE	38
	1515658069-1-1517132881-1517359552-1515656109-1515656702-nvstlink.exe	c0f5b7fc_ee8770d1	MSEXE	38
	1515672473-1-1517157947-1517384618-1515681175-1515681768-3df420aeb3d0c086e5b9a782e455f05b3326a979.exe	68bd5d5c_f473cb18	MSEXE	25
	1515672473-1-1517151141-1517377812-1515674962-2b86f562fa701ee713aa1a6121fff8684b31421.exe	774e2a1f_f56ff2a5	MSEXE	6

Malware Summary (switch workflow)

Malware Summary > Table View of Malware Events

2018-01-11 04:58:27 - 2018-01-11 10:58:27

No Search Constraints (Edit Search)

Jump to... 查看详细信息

Detection Name	File Name	File SHA256	File Type	Count
	1515658069-1-1517134105-1517360776-1515657333-1515657926-mpas-d_bd_1.225.2931.0.exe	60c8ad6d_d15a411e	MSEXE	76
	1515658069-1-1517134093-1517360764-1515657321-1515657914-5563f5a3033de5864b98090591358062.exe	ae23cdc2_34cf5b73	MSEXE	63
	1515658069-1-1517137894-1517364565-1515661122-1515661715-AM_Delta_Patch_1.225.3050.0.exe	ab9d1518_8f8962d0	MSEXE	45
W32_A39AB89113-95_SBX.TG	1515658069-1-1517137875-1517364546-1515661103-1515661696-grd2.xls	a39ab891_b1fd35dd	MSOLE2	39
	1515658069-1-1517137859-1517364530-1515661087-1515661680-Cineqet_Installer.exe	90a67a98_8a58b680	MSEXE	38
	1515658069-1-1517132881-1517359552-1515656109-1515656702-nvstlink.exe	c0f5b7fc_ee8770d1	MSEXE	38
	1515672473-1-1517157947-1517384618-1515681175-1515681768-3df420aeb3d0c086e5b9a782e455f05b3326a979.exe	68bd5d5c_fd73cb18	MSEXE	25
	1515672473-1-1517151141-1517377812-1515674369-1515674962-2b86f562ffa701ee713aa1a6121fff8684b31421.exe	774e2a1f_f56ff2a5	MSEXE	6

Malware Summary (switch workflow)

Malware Summary > Table View of Malware Events

2017-03-27 System Help Global \ demo\_user\_

Search Constraints (Edit Search)

Jump to... 查看详细信息

Time	Action	Sending IP	Sending Country	Receiving IP	Receiving Country	Sending Port	Receiving Port	SSL State
2017-03-27 11:33:07	Custom Detection Block	192.168.1.200		172.16.1.200		80	59229	Unk

Jump to... 查看详细信息

Detection Name	File Name	File SHA256	File Type	Count
	1515658069-1-1517134105-1517360776-1515657333-1515657926-mpas-d_bd_1.225.2931.0.exe	60c8ad6d_d15a411e	MSEXE	76
	1515658069-1-1517134093-1517360764-1515657321-1515657914-5563f5a3033de5864b98090591358062.exe	ae23cdc2_34cf5b73	MSEXE	63
	1515658069-1-1517137894-1517364565-1515661122-1515661715-AM_Delta_Patch_1.225.3050.0.exe	ab9d1518_8f8962d0	MSEXE	45
W32_A39AB89113-95_SBX.TG	1515658069-1-1517137875-1517364546-1515661103-1515661696-grd2.xls	a39ab891_b1fd35dd	MSOLE2	39
	1515658069-1-1517137859-1517364530-1515661087-1515661680-Cineqet_Installer.exe	90a67a98_8a58b680	MSEXE	38
	1515658069-1-1517132881-1517359552-1515656109-1515656702-nvstlink.exe	c0f5b7fc_ee8770d1	MSEXE	38
	1515672473-1-1517157947-1517384618-1515681175-1515681768-3df420aeb3d0c086e5b9a782e455f05b3326a979.exe	68bd5d5c_fd73cb18	MSEXE	25
	1515672473-1-1517151141-1517377812-1515674369-1515674962-2b86f562ffa701ee713aa1a6121fff8684b31421.exe	774e2a1f_f56ff2a5	MSEXE	6

FMC展示文件轨迹特性追踪效果

7.1: 10.57分发现从火狐六看起下载一个未知文件

Overview Analysis Policies Devices Objects FireAMP Health System Help admin

Context Explorer Connections Intrusions Files Network File Trajectory Hosts Users Vulnerabilities Correlation Custom Search

### Network File Trajectory for 0517f034...588e1374

File SHA-256: 0517f034...588e1374  
 File Name: WindowsMediaInstaller.exe  
 File Type: MSEXE  
 File Category: Executables  
 Current Disposition: Malware  
 Threat Score: High

First Seen: 2013-12-06 10:57:13 on 10.4.10.183  
 Last Seen: 2013-12-06 18:17:27 on 10.4.10.183  
 Event Count: 7  
 Seen On: 4 hosts  
 Seen On Breakdown: 2 senders → 3 receivers

**Trajectory**

Dec 06, 2013

10.4.10.183  
 10.5.11.8  
 10.3.4.51  
 10.5.60.66

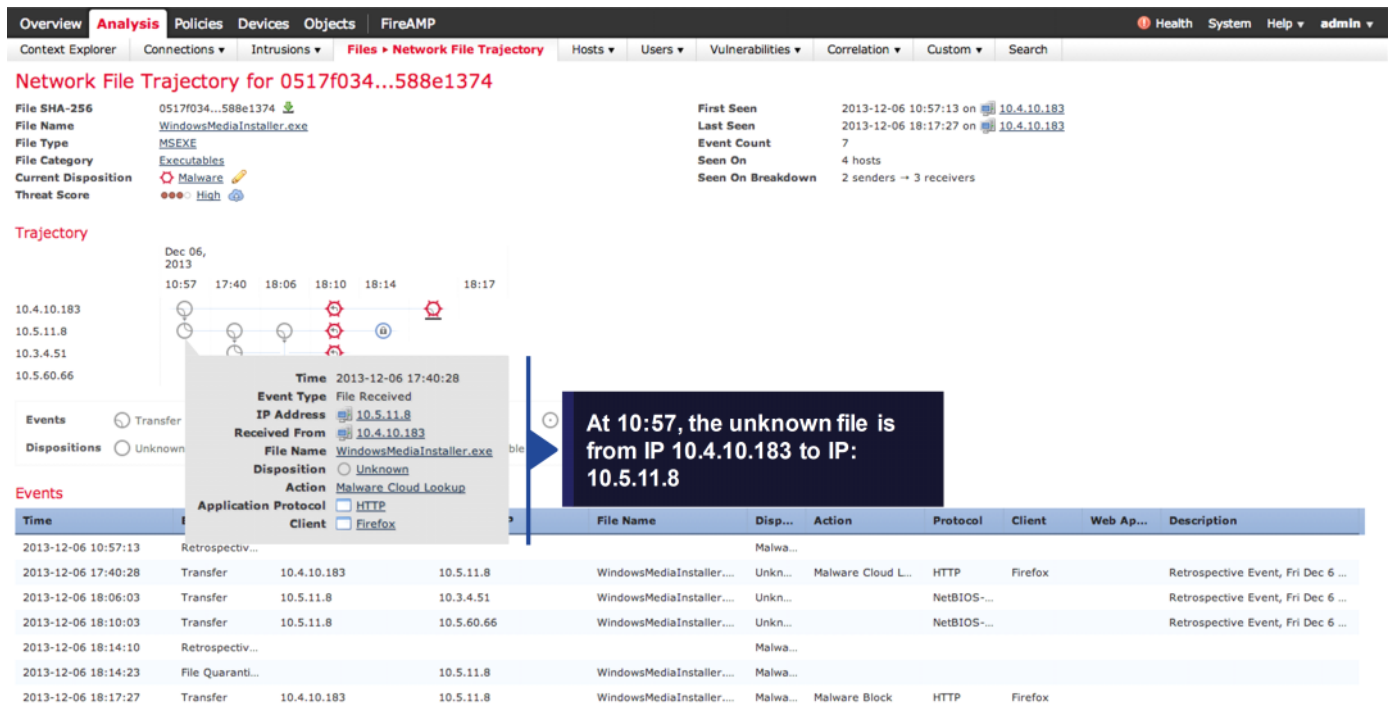
Events: Transfer, Dispositions: Unknown

**Events**

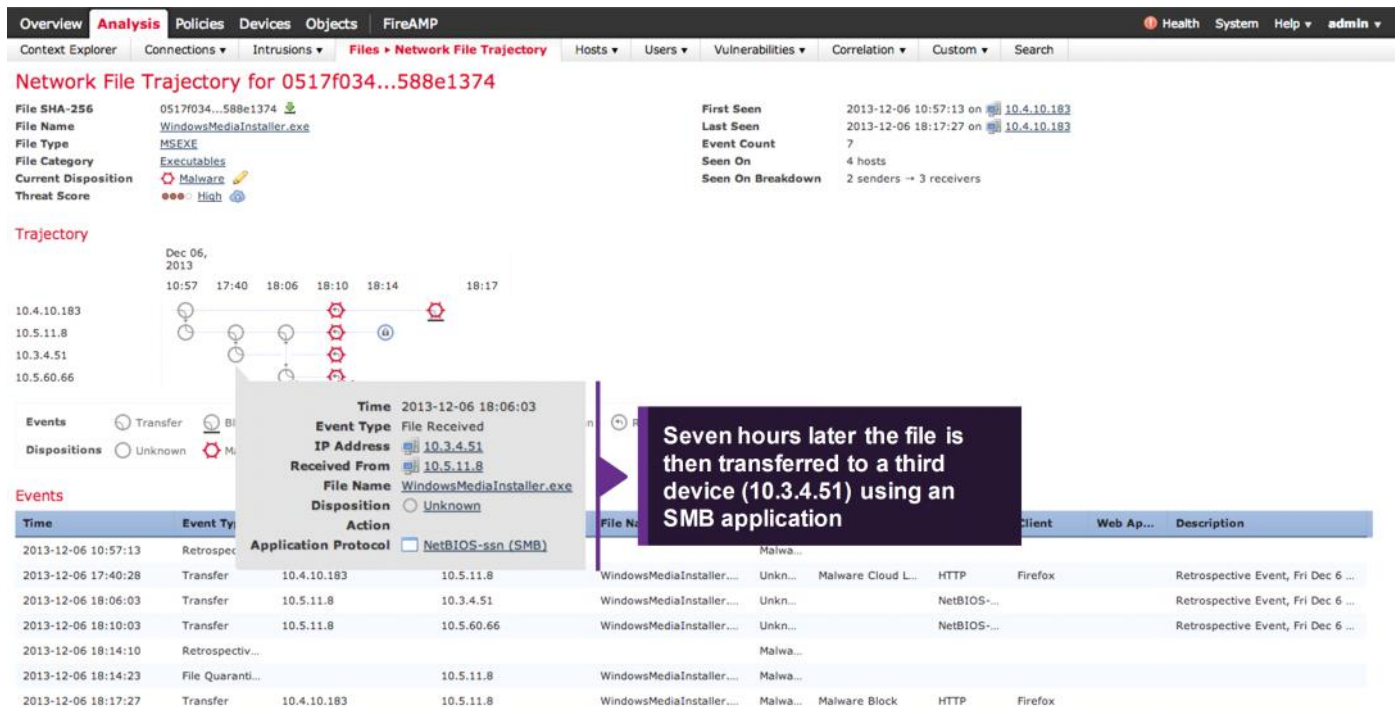
Time	Event Type	IP Address	Sent To	File Name	Disposition	Action	Application Protocol	Client
2013-12-06 10:57:13	Retrospectiv...				Malwa...			
2013-12-06 17:40:28	Transfer	10.4.10.183	10.5.11.8	WindowsMediaInstalle...	Unkn...	Malware Cloud L...	HTTP	Firefox
2013-12-06 18:06:03	Transfer	10.5.11.8	10.3.4.51	WindowsMediaInstalle...	Unkn...		NetBIOS-...	
2013-12-06 18:10:03	Transfer	10.5.11.8	10.5.60.66	WindowsMediaInstalle...	Unkn...		NetBIOS-...	
2013-12-06 18:14:10	Retrospectiv...				Malwa...			
2013-12-06 18:14:23	File Quaranti...		10.5.11.8	WindowsMediaInstalle...	Malwa...			
2013-12-06 18:17:27	Transfer	10.4.10.183	10.5.11.8	WindowsMediaInstalle...	Malwa...	Malware Block	HTTP	Firefox

An unknown file is present on IP: 10.4.10.183, having been downloaded from Firefox

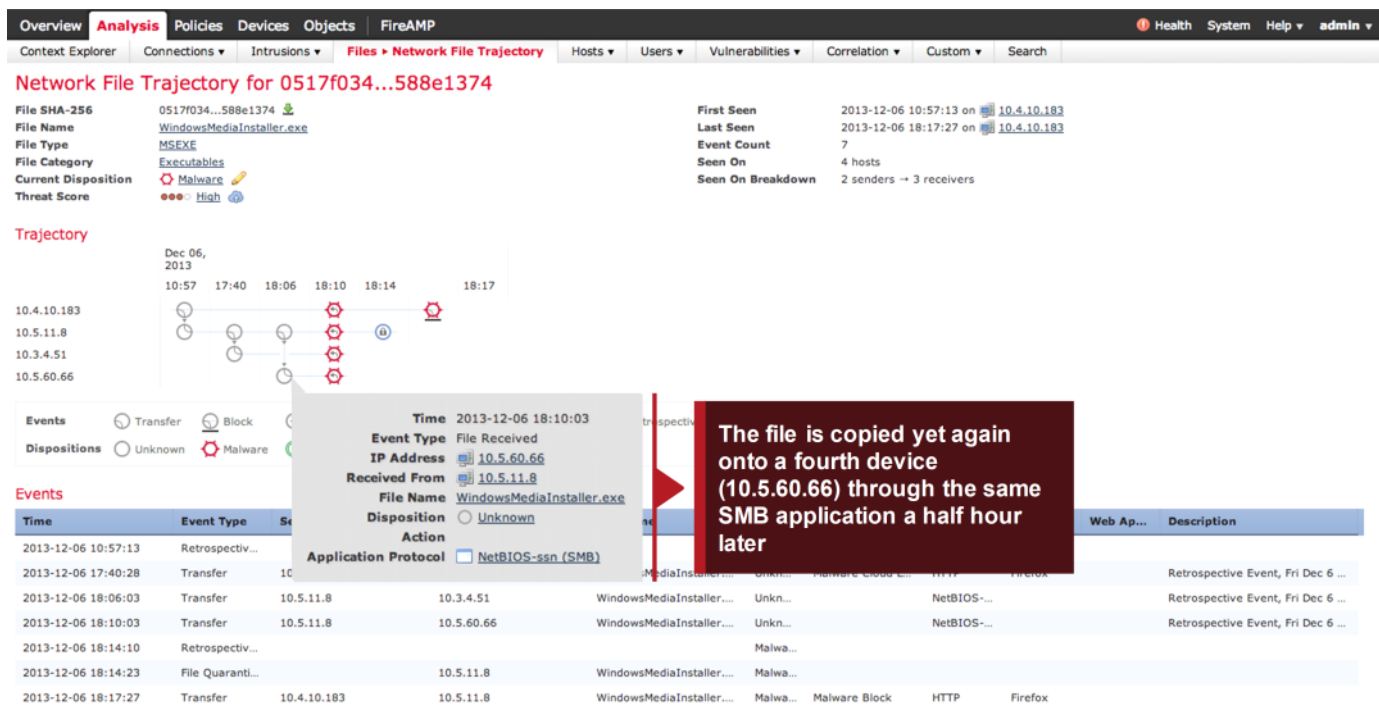
7.2: 10.57 同时这个未知文件从10.4.10.183传送给10.5.11.8



7.3: 7小时后，10.5.11.9使用SMB将文件传送给10.3.4.51



7.4: 半小时后，该文件再次通过相同的SMB应用程序复制到第四台设备（10.5.60.66）上



7.5: 思科集体安全情报云已经了解到该文件是恶意的，并且会立即为所有四个设备提出追溯事件。

在6:14，我们看到一个回顾性事件出现了。所以它同时出现在4台机器上。到目前为止，我们的处置已经从我们认为未知的事物变为现在已知的恶意软件。因此，我们已经警告这四台机器和防御中心中的每一台，在环境中找到了恶意软件，使用户能够跟踪该文件在网络中的传播方式，并了解后膛的范围。

同时，具有FireAMP端点连接器的设备会对追溯事件作出反应，并立即停止并隔离新检测到的恶意软件（必须有anyconnect-ampendpoint才可以做到。。）



7.6: 第一次攻击后8小时，恶意软件会尝试通过原始入口点重新进入系统，但会被识别并阻止。

后来该文件再次尝试在网络中移动。这一次，有人试图通过HTTP使用应用程序Firefox发送文件。因为现在已知该文件是恶意软件，所以此传输被阻止。



## 8: 最佳实践

- 如果要使用文件策略阻止文件，请使用“重置连接”选项。它允许应用程序会话在连接自身超时之前关闭。
- 如果要将捕获的文件下载到桌面，请确保在下载之前在桌面上采取其他预防措施。该文件可能感染了可能对您的桌面有害的恶意软件。



- 保持文件大小的限制为一个较小值来提高性能。访问控制策略允许您限制文件大小。它会使用以下行为：
  - 将文件发送到云以进行动态分析
  - 本地存储文件
  - 计算文件的SHA-256哈希值
- 万一Firepower系统与Cisco云之间发生通信故障，当文件与“阻止恶意软件”操作匹配规则时，FTD可以在短时间内保留文件传输。尽管此保留期限是可配置的，但是思科建议您使用默认值。

每个ACL都有默认的AMP规则参数，比如检查文件的大小，发送给AMP-Cloud文件大小设定可以在ACL中更改

The screenshot shows the 'Advanced' tab of the 'CCIE\_Policy' configuration page. The 'Files and Malware Settings' section is highlighted with a red box. The settings are as follows:

Setting	Value
Limit the number of bytes inspected when doing file type detection	1460
Allow file if cloud lookup for Block Malware takes longer than (seconds)	2
Do not calculate SHA256 hash values for files larger than (in bytes)	10485760
Minimum file size for advanced file inspection and storage (bytes)	6144
Maximum file size for advanced file inspection and storage (bytes)	1048576
Minimum file size for dynamic analysis testing (bytes)	6144
Maximum file size for dynamic analysis testing (bytes)	1048576

1. 默认情况下，只会检查前1460字节
2. 等待云响应的时间有多长
3. 默认情况下，仅针对最大10MB的文件检查恶意软件
4. 不会捕获小于6KB的文件
5. 不会捕获大于1MB的文件。这还指定了检查的归档（压缩文件）的大小。
6. 将发送到Cloud for Dynamic Analysis的最小和最大文件大小

# Malware Policies

利用缺省的“Advanced”环境变量，除非有特殊要求。如果需要检测压缩文件内的病毒，勾选“Inspect Archives”

建议按照下面参数进行文件策略配置

