

# Case-1: Block Malware (应用AMP功能)

2019年12月7日 12:10

## 实验目的

**备注：SSL加密流量无法进行文件策略控制&恶意文件分析**

### 策略1：（使用AMP功能需要Malware许可）

- 阻止通过http传输的恶意文件：Office，可执行文件（包含这些文件类型的所有格式）
- 只使用本地恶意软件检查引擎（ClamAV）进行分析，若检测到恶意文件立即重置连接
- 并设置存储检查到的恶意文件到FTD设备
- 更改检查文件的默认大小限制

### 策略2：（使用Threat许可）

- 阻塞通过任何协议任何方向传输的PDF类型所有格式的文件，并将Block的文件存入FTD本地中

## 目录

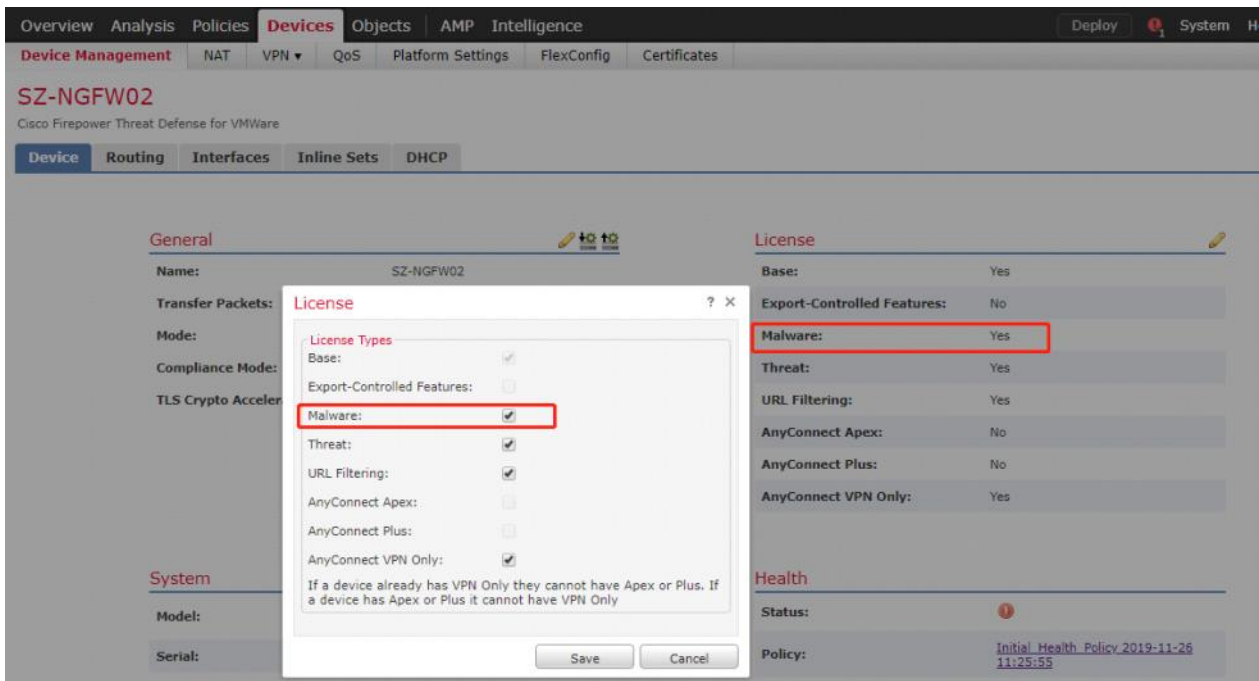
1. 配置文件策略前提准备
2. 创建恶意检测&文件策略
3. 创建文件规则1（AMP功能）
  - 创建文件策略 & 文件规则
  - 选择传输协议（http），并选择传输文件方向为双向（上传&下载）
  - 选择行为=block Malware，并选择本地ClamAV引擎分析文件，检测到恶意后重置连接
  - 选择将检测到的恶意文件存储到FTD上
  - 选择检测文件类别&类型（office, pdf, 可执行文件三种类别的所有类型文件）
4. 创建文件规则2（Threat威胁防御功能）
5. 调整文件策略的高级选项（可选）
6. 文件策略应用到ACP中并推送
7. 关于AMP检测和APP控制的冲突问题☆
8. 更改ACP的默认AMP策略值（可选）
9. 验证

## 1: 配置文件策略之前准备

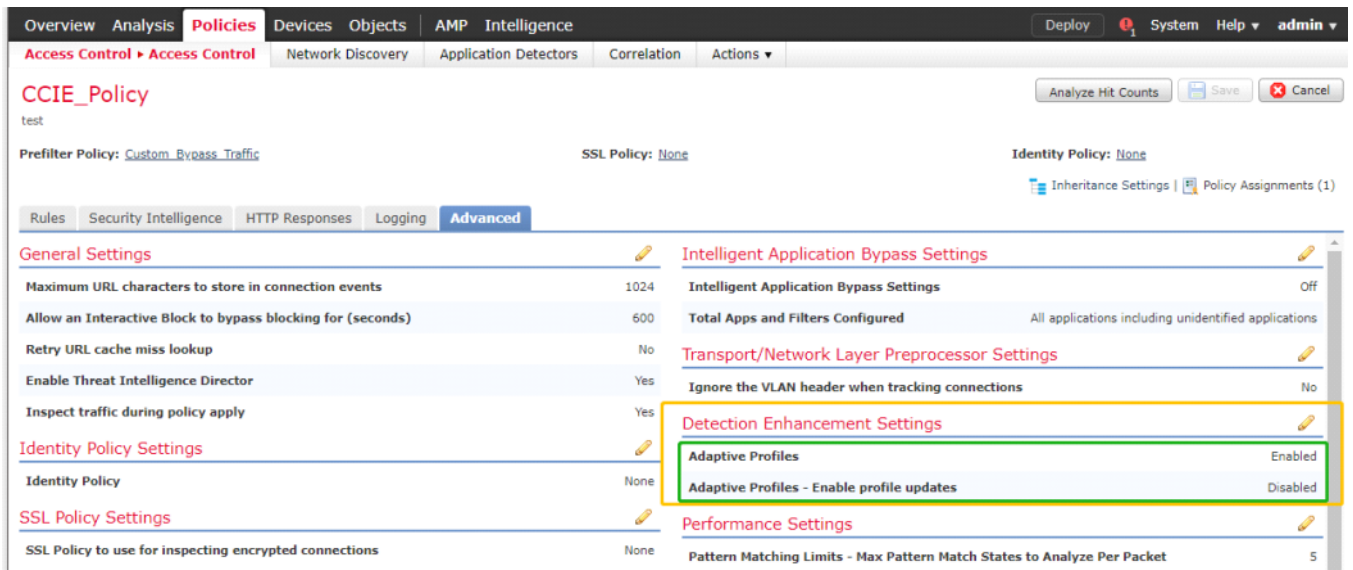
### 1.1: 部署前参考27章第八节最佳实践部署

### 1.2: 安装许可

基于文件类型Block，只需要Threat许可。基若需要执行恶意软件分析，需要Malware许可（AMP）

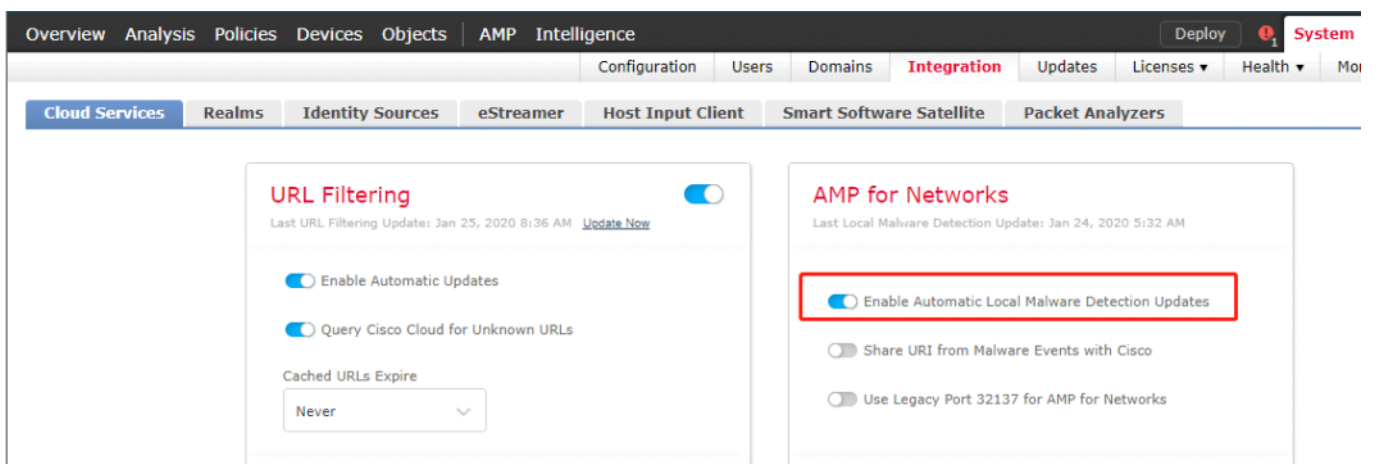


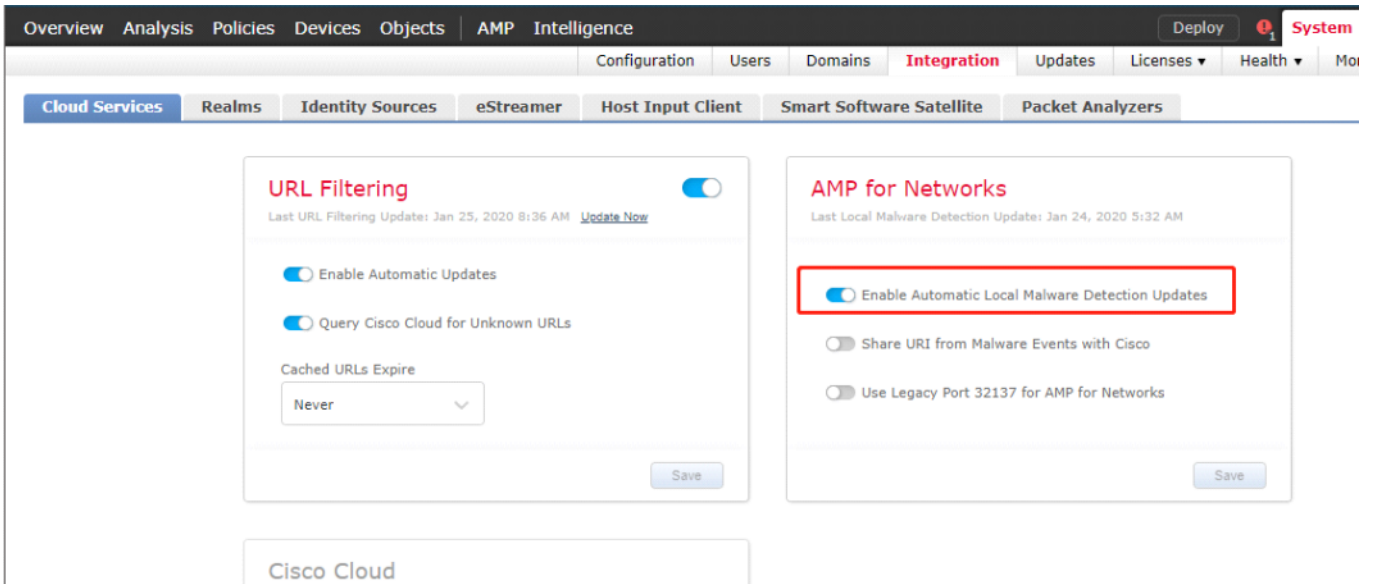
### 1.3: 确定自适应配置文件开启



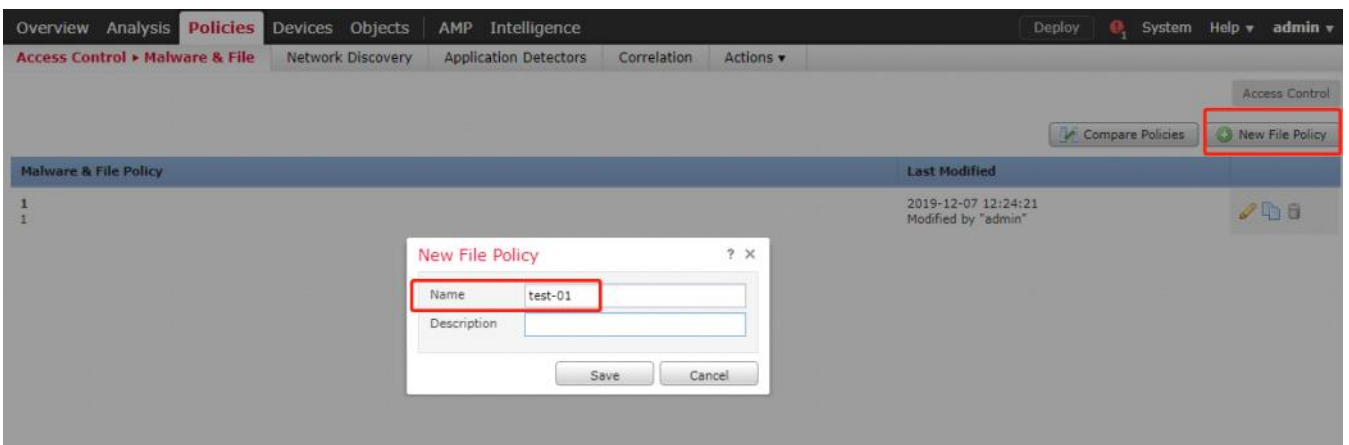
### 1.4: 确定开启本地恶意软件检测（AMP本地）更新

- 开启后FMC默认每隔30min和Talos通信，当有新的规则集可用FMC会自动下载用来丰富本地的AMP引擎
- 这里还可以选择将自己的恶意文件检测事件发送给Cisco进行登记备案（设计到数据问题）

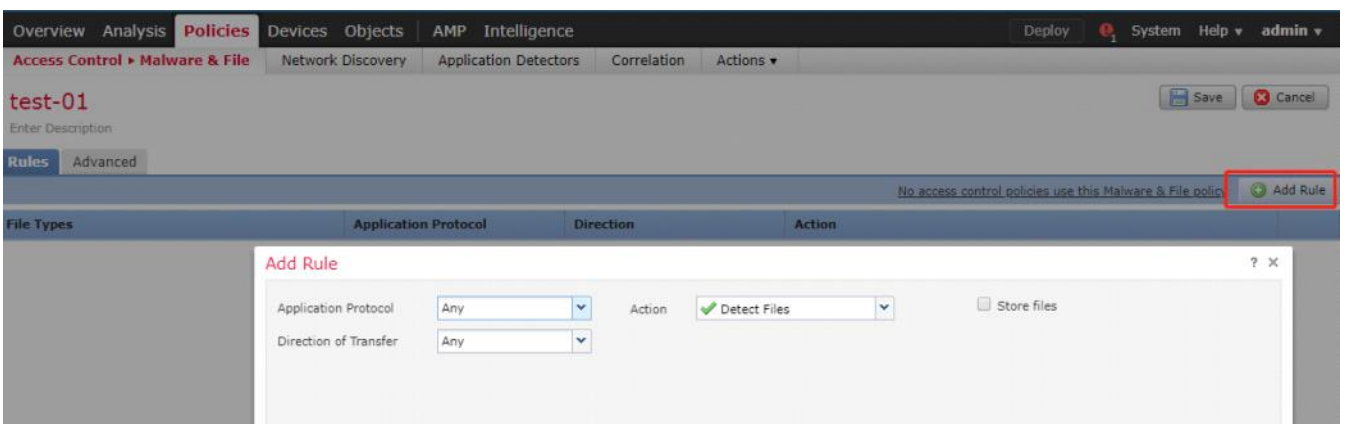




## 2: 创建恶意检测&文件策略

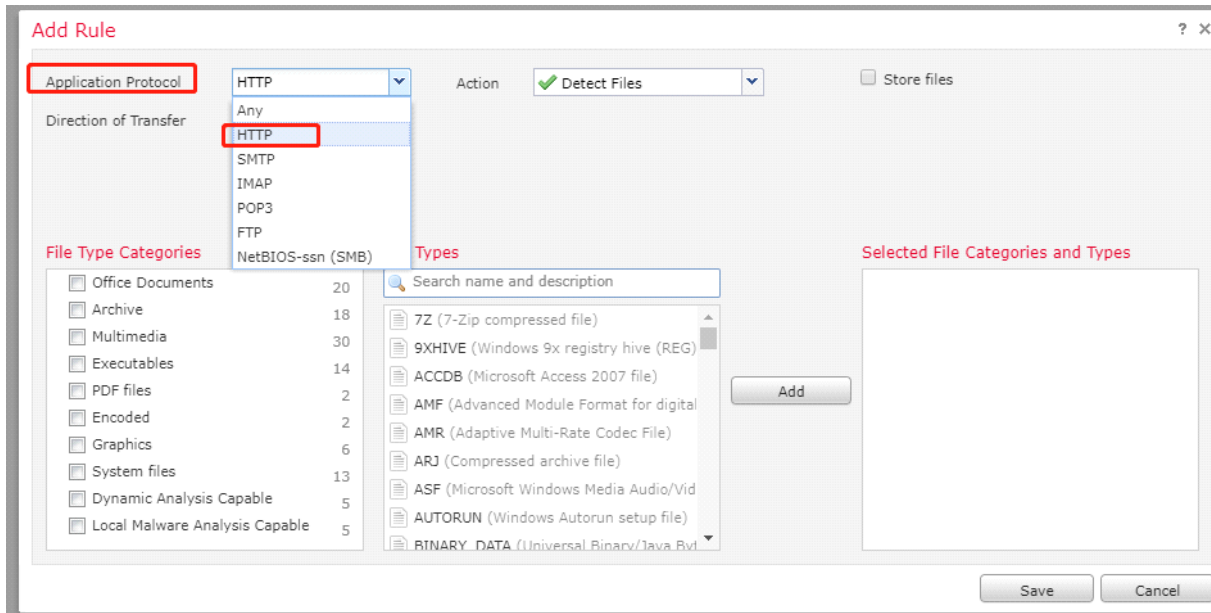


## 3: 创建文件规则1 (使用AMP功能)

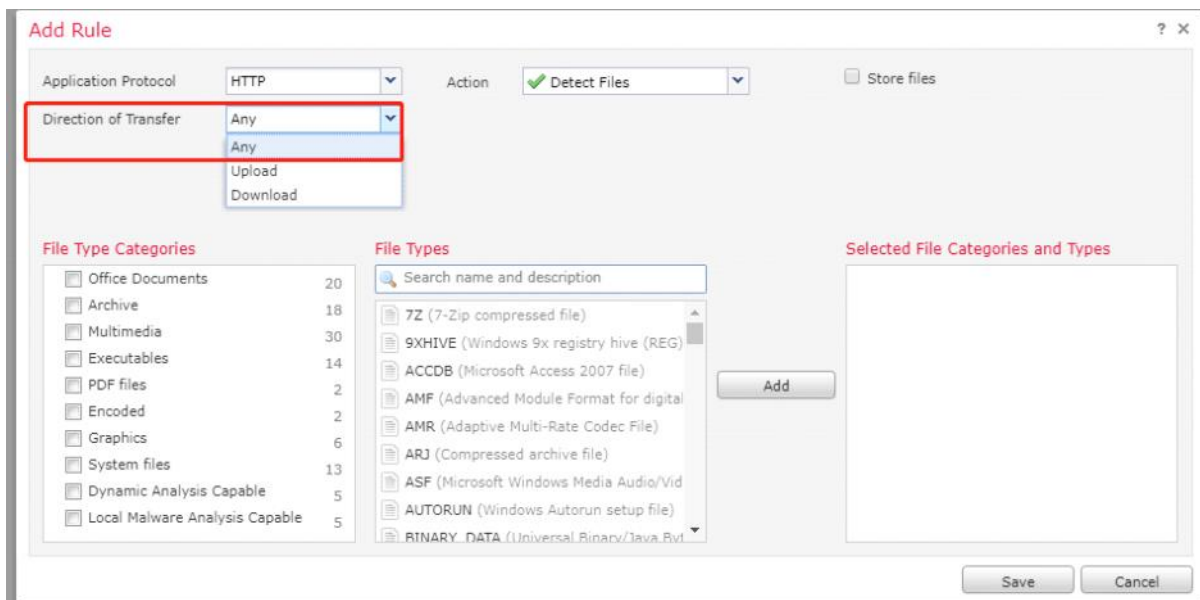


### 3.1: 选择文件传输协议=http, 选择传输文件方向为双向 (上传&下载)

3.1.1: 应用协议的意思是, 文件在哪些协议上传输



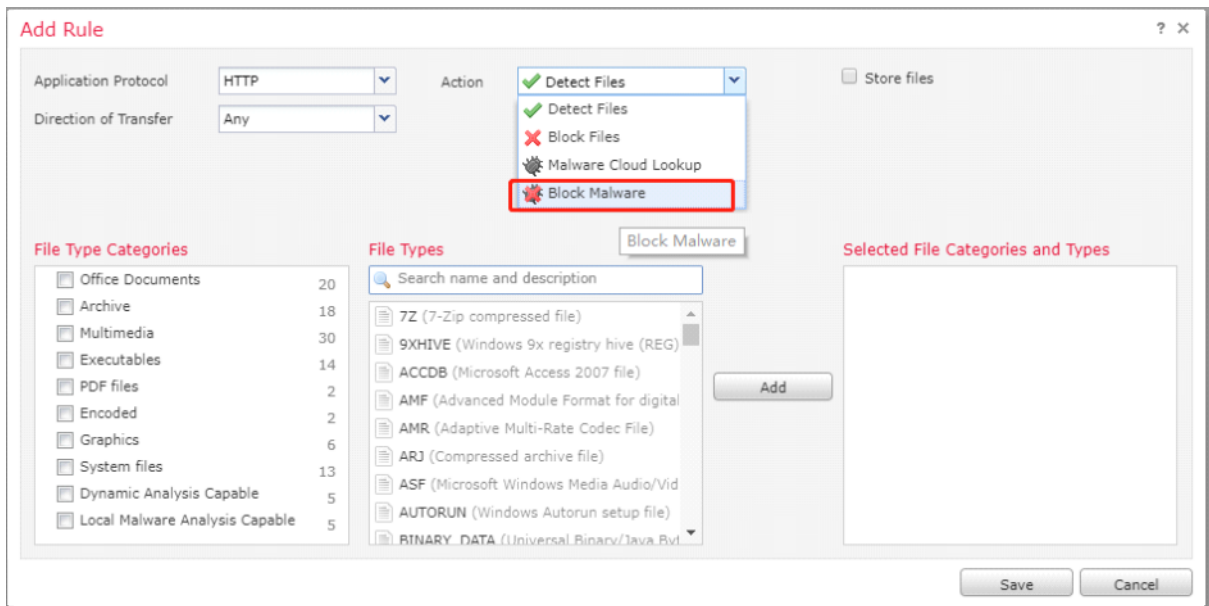
3.1.2: 选择传输方向any, 上下行



**备注:** 电子邮件的协议只可以选择单向传输 (IMAP/POP3/SMTP)  
SMTP是上传邮件到邮件服务器, POP3/IMAP是从邮件服务器下载邮件

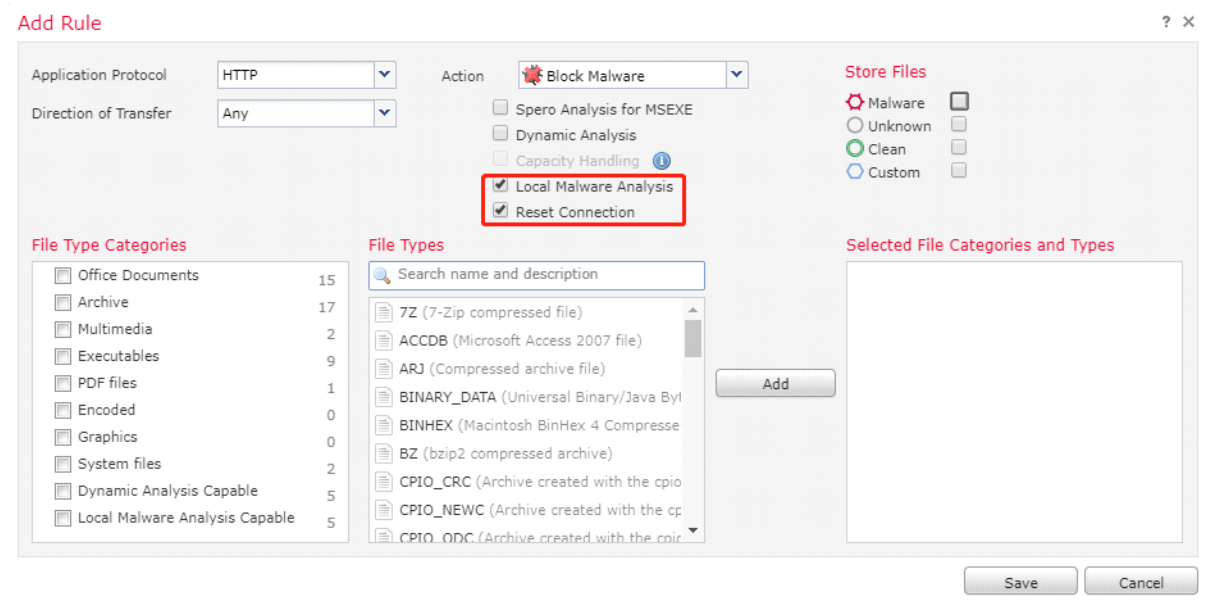
### 3.2: 配置文件规则行为 (block恶意文件+本地分析)

3.2.1: 选择行为=block Malware



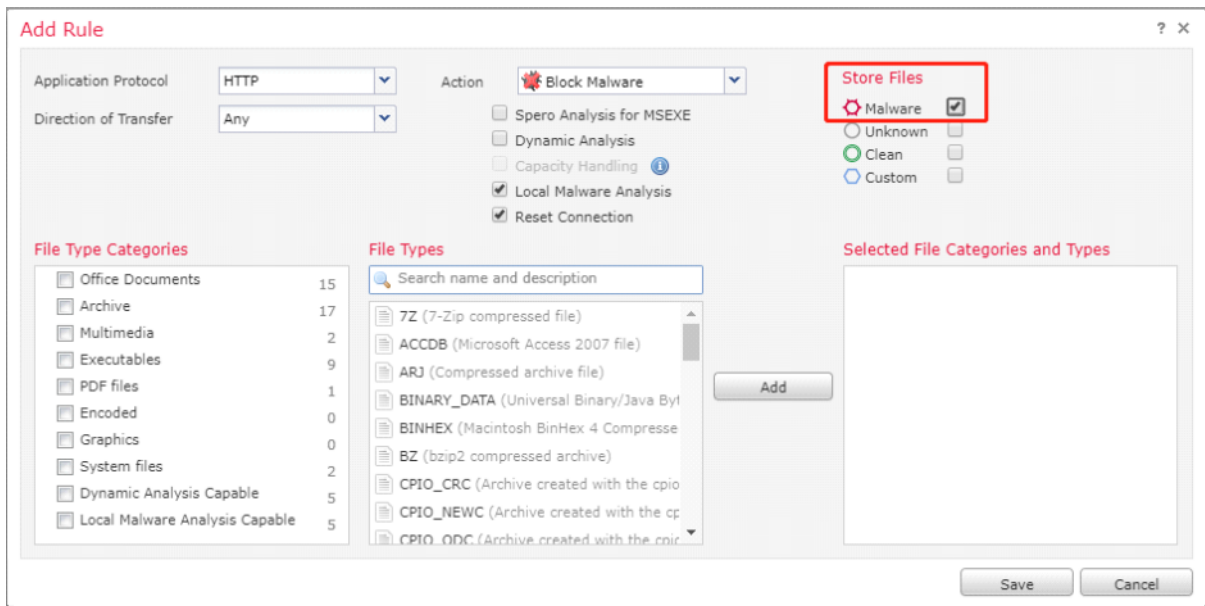
### 3.2.2: 选择本地ClamAV引擎分析文件，检测到恶意后重置连接☆☆

- 这里默认什么都不勾，FTD只会执行哈希值计算文件，将文件哈希和病毒哈希比较
- 勾了Spero会用Spero引擎对微软的EXE文件执行分析
- 勾选动态分析会找云Threat Grid沙河运行文件分析
- 勾选本地分析使用ClamAV
- 勾了重置连接会基于行为直接断开用户传输文件的session



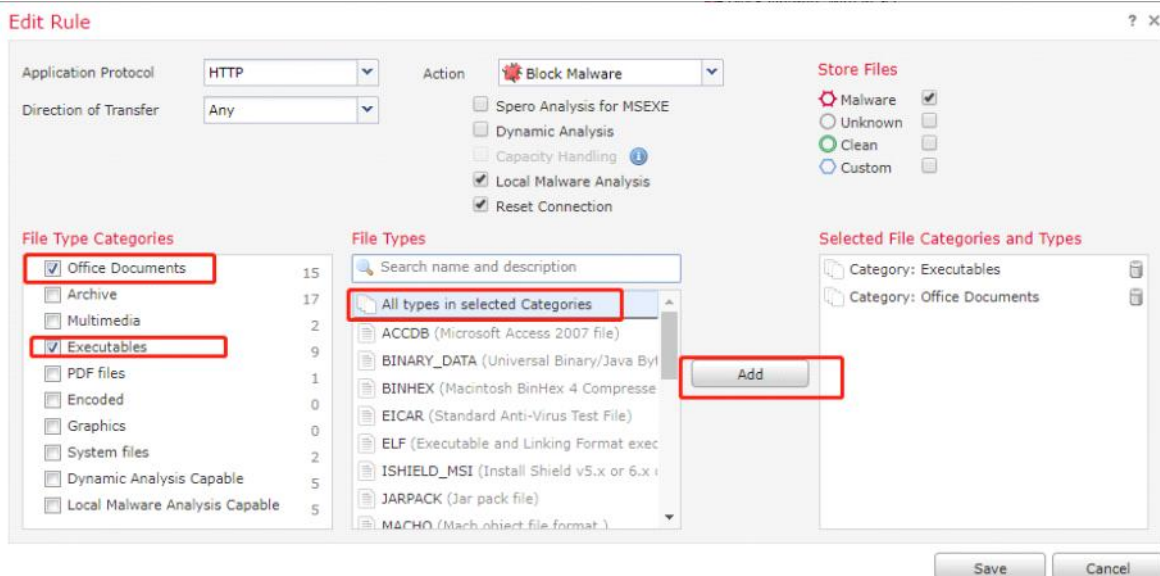
备注：这里也可以选择Dynamic Analysis找沙盒分析文件，但是要严谨，因为会导致传输慢，应用延迟卡顿等。

### 3.3: 选择将检测到的恶意文件存储到FTD上

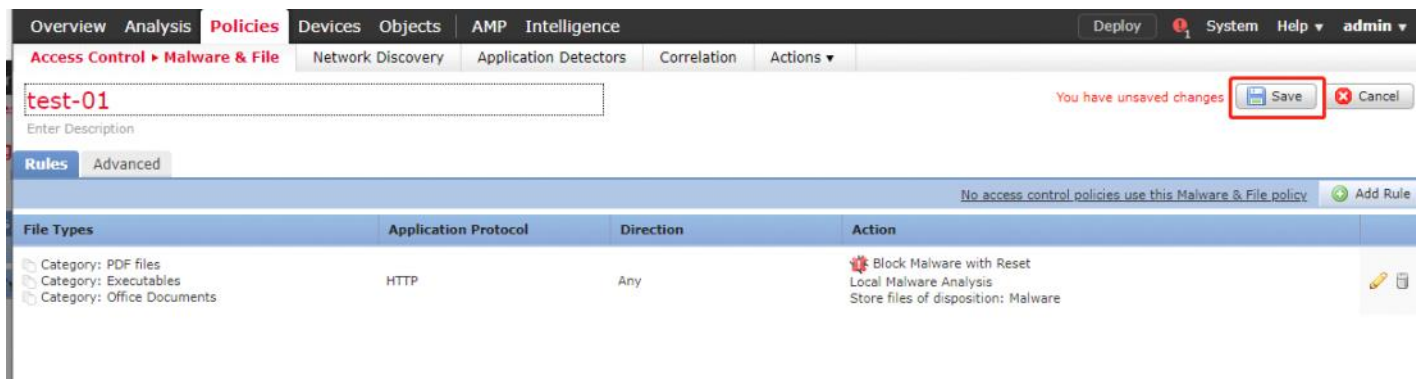


### 3. 4: 选择需要检测的文件类型的类别

#### 3. 4. 1: 办公文件+可执行文件的所有文件类型

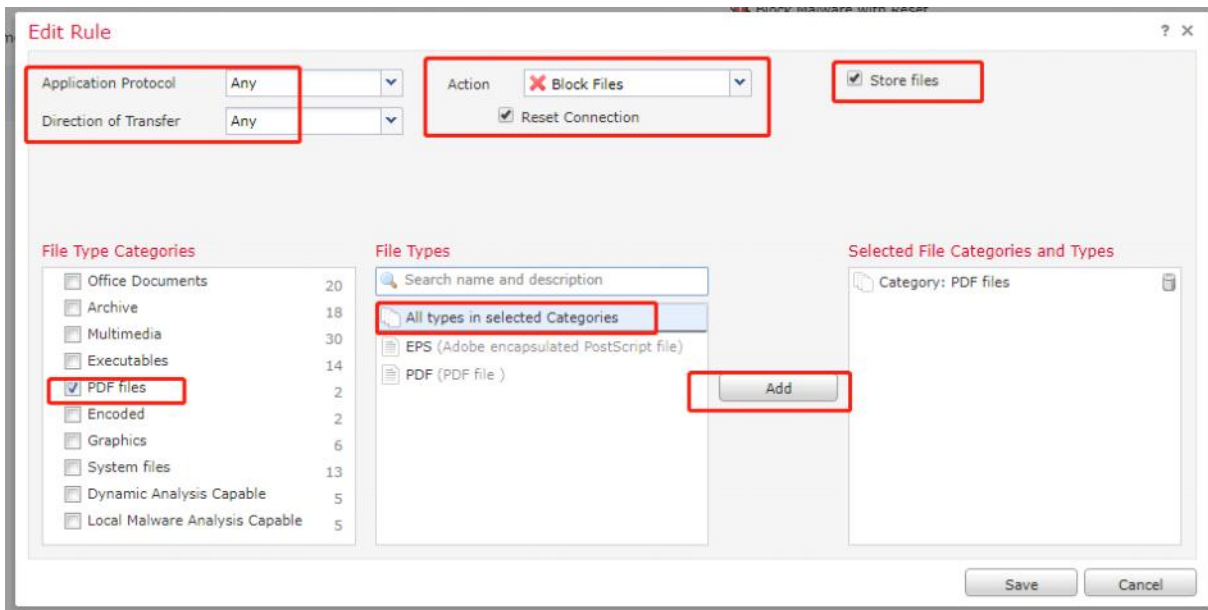


#### 3. 4. 2: 保存

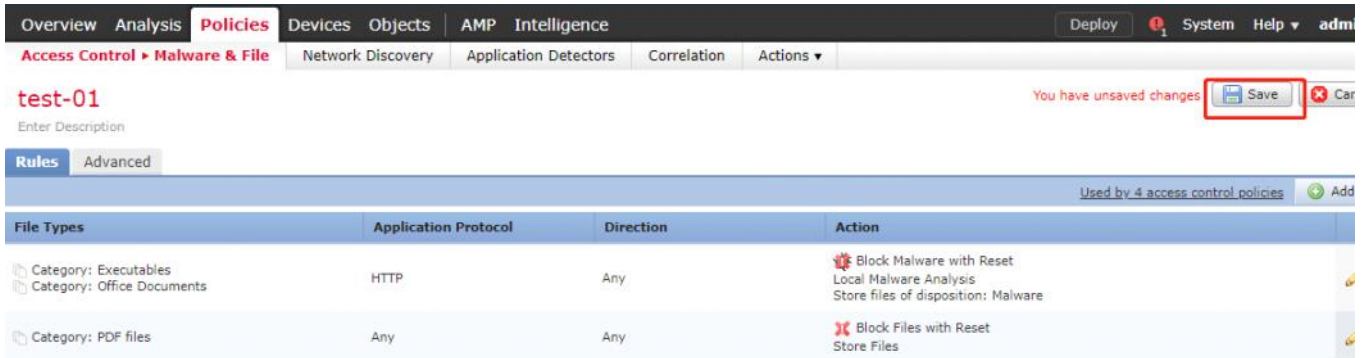


## 4: 创建文件规则2 (Threat威胁防御功能)

block所有PDF文件（2种格式），在所有协议的双方向传递都会被block

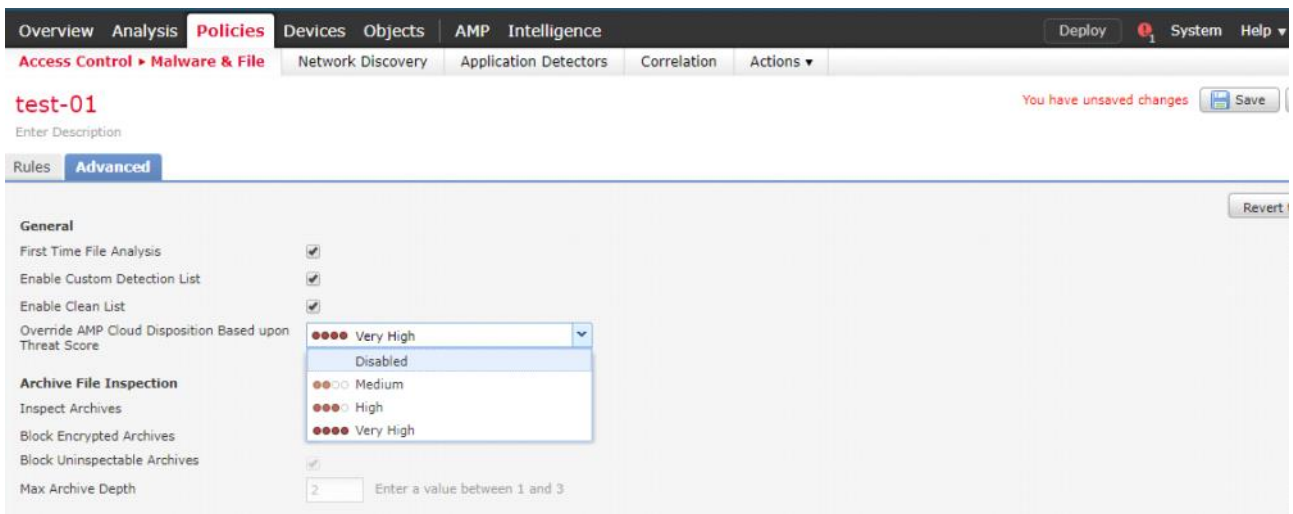


Save

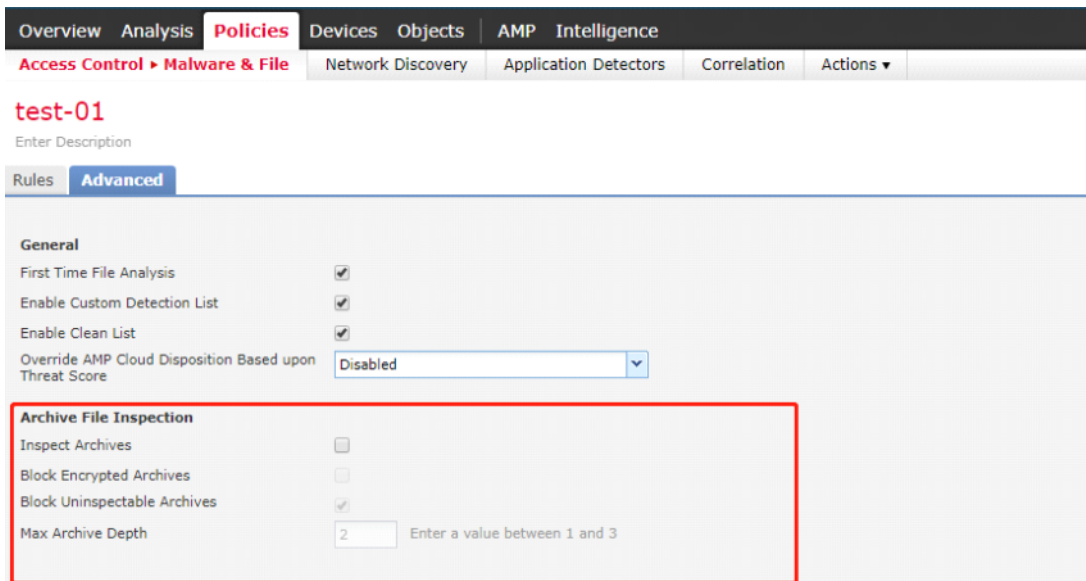


## 5: 调整文件策略高级选项 (可选)

可以调整动态分析威胁评分的级别（低的话会增加恶意文件数量，推荐没必要直接disable）

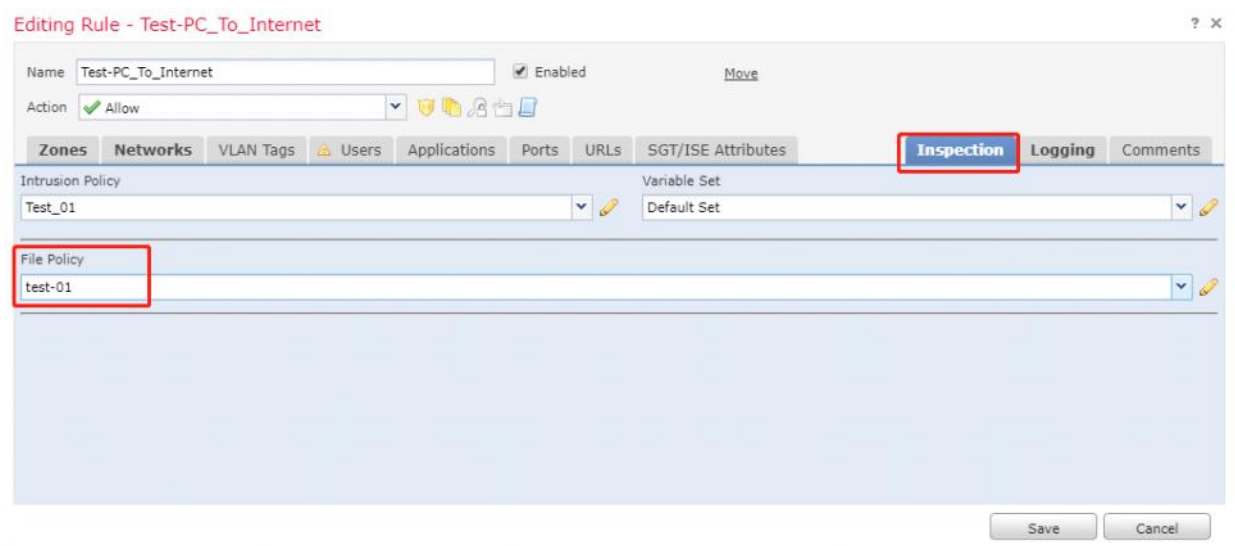


是否开启文档内容检测，以及定义对嵌套存档文件的检测深度



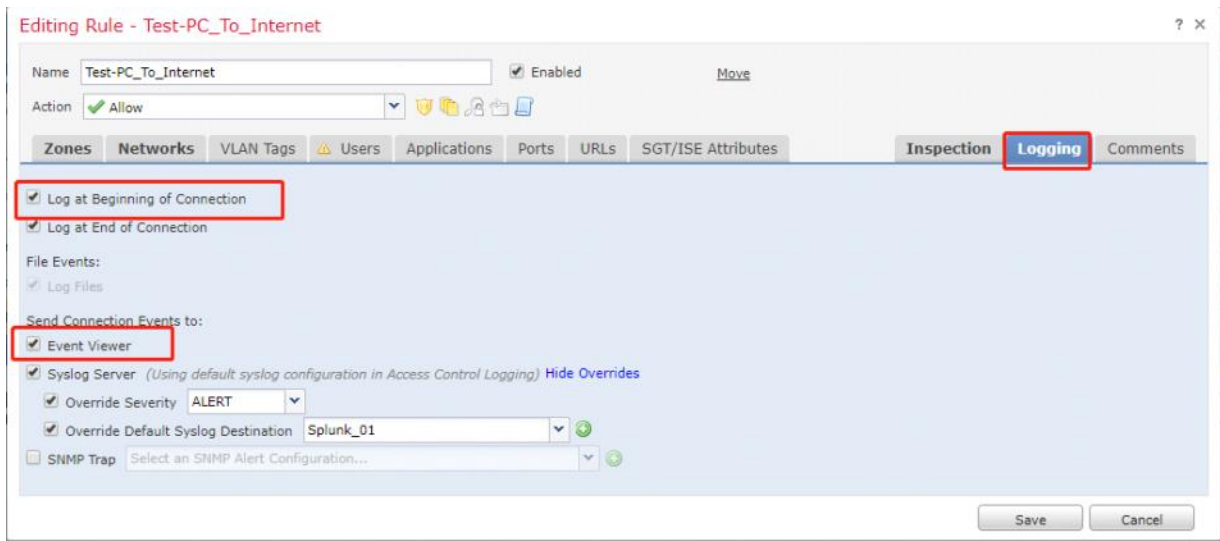
## 6: 文件策略应用到ACP规则中

每个ACP规则只可以调用一个Fire-Policy

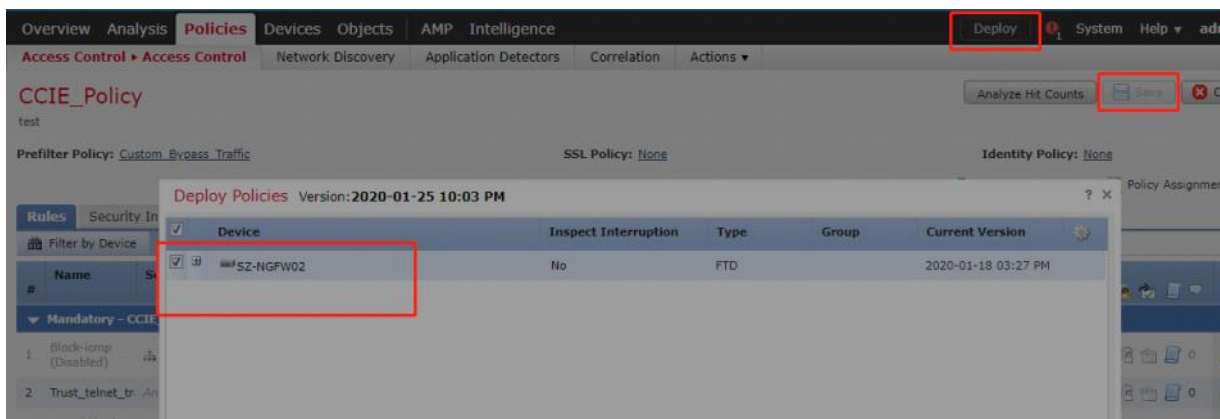


推荐记录log，只选择连接开始比较好。。





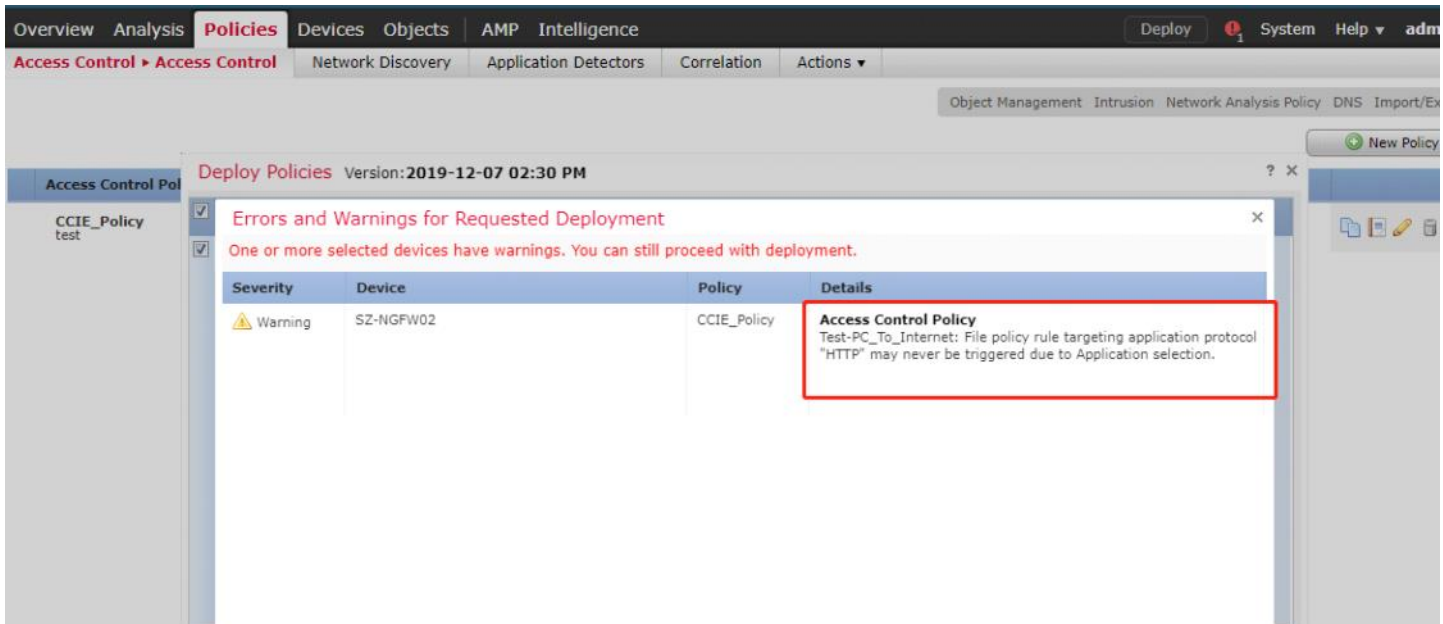
将策略推送下去时提示Snort引擎重启会导致流量中断，但是实际测试其实也没丢包。。。



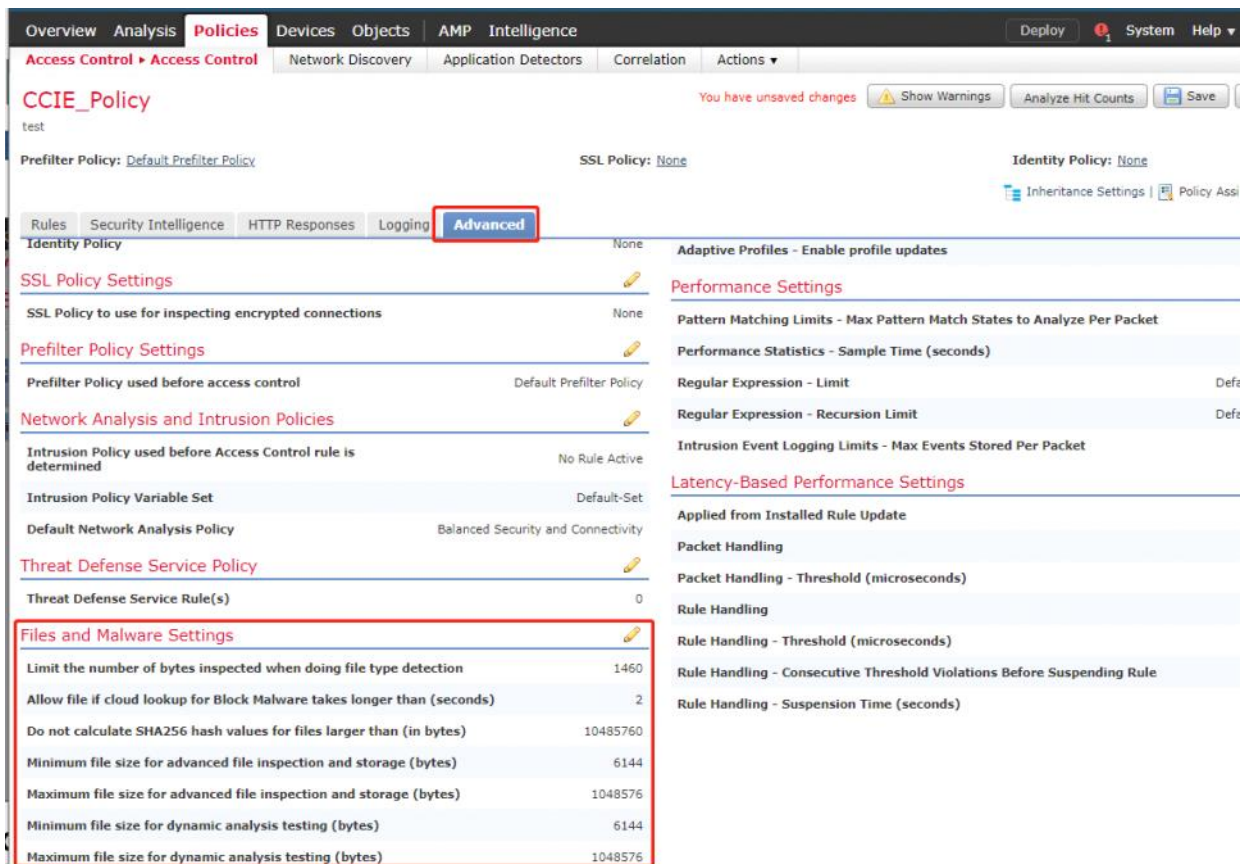
## 7: 文件策略和APP控制策略冲突

如果同一条规则中既有APP控制策略，又有AMP策略

APP控制策略包含了AMP检测的传输协议的话，那么APP控制策略优先，AMP策略可能不会生效



## 8: 更改ACP的默认文件策略值 (可选)

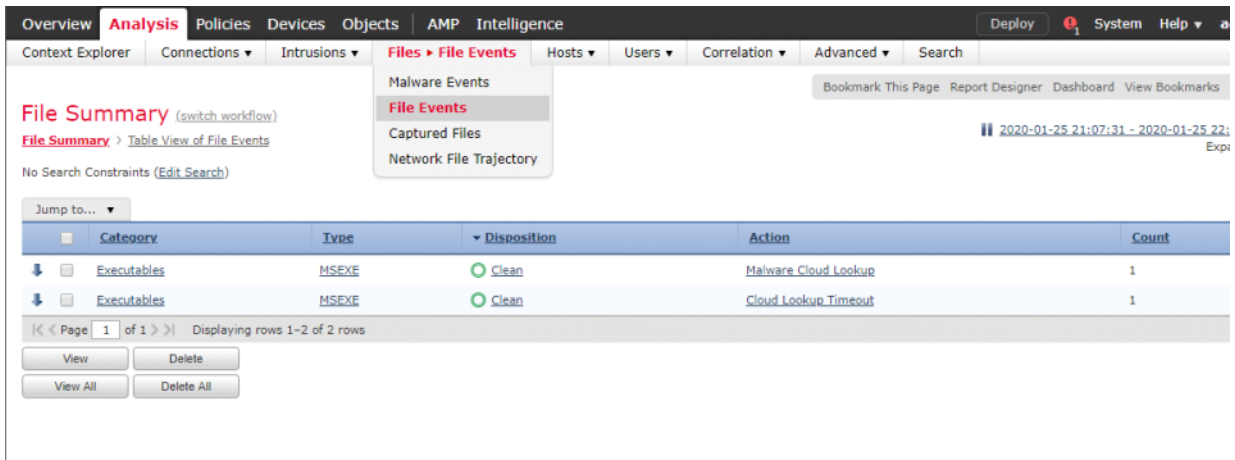




## 9: 验证

### 9.1: 验证EXE规则, 检测恶意EXE, block

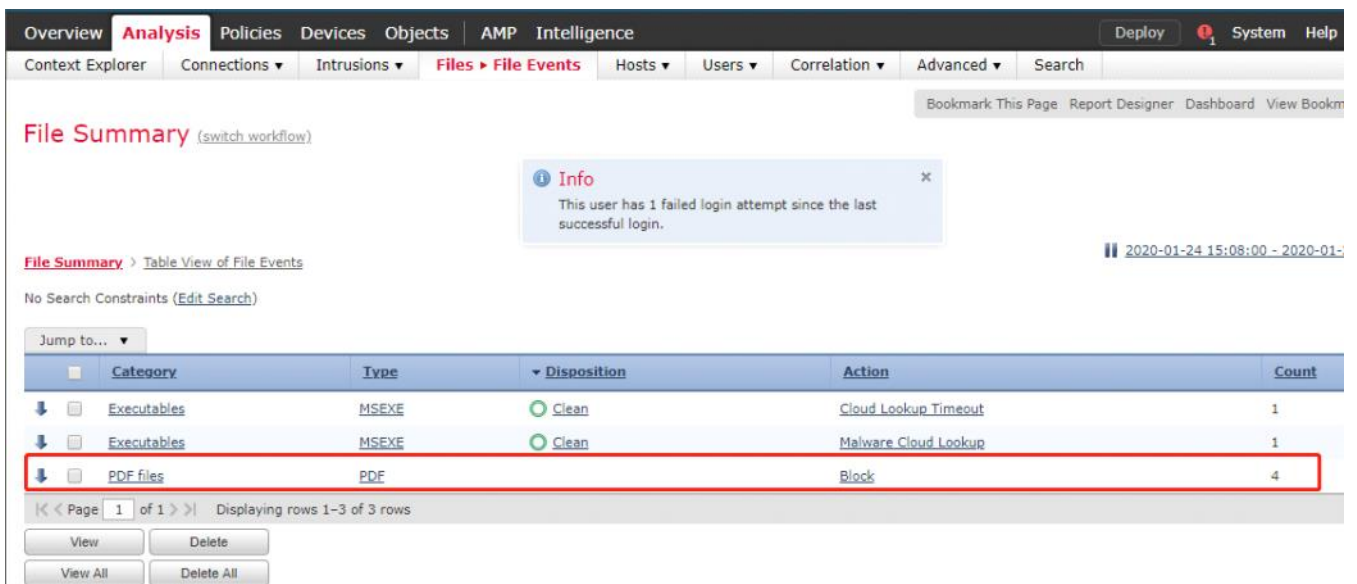
可以看到检测到两个EXE执行文件是干净的, 放行了



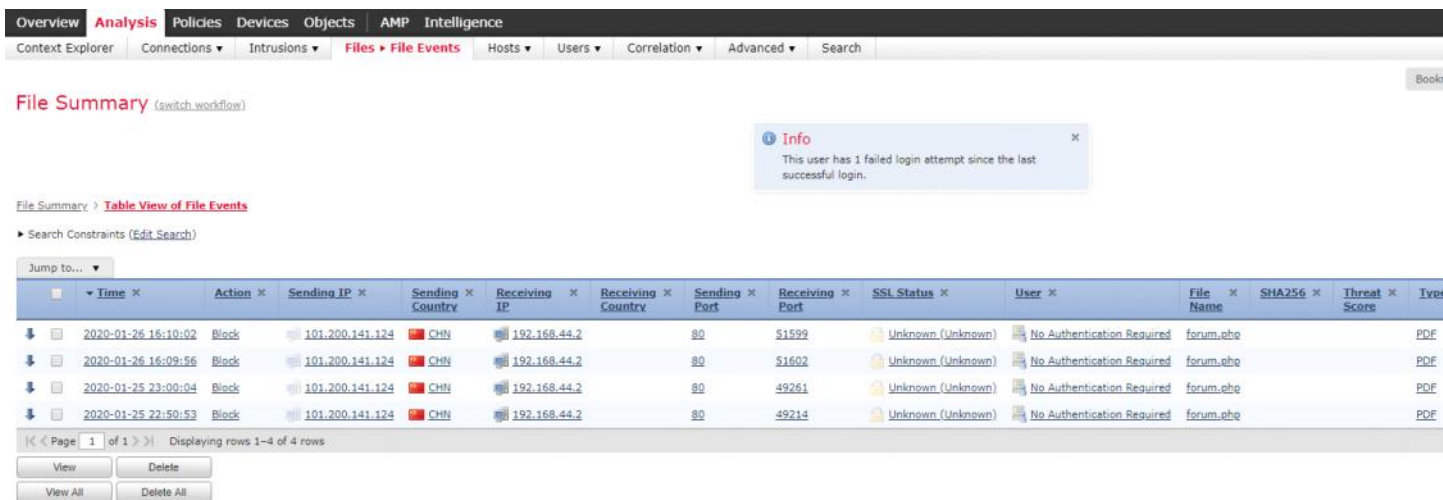
### 9.2: 验证规则2, 通过http传输PDF直接被block并且还跳提示 ☆

如果deny MP4文件, 系统不会提示的

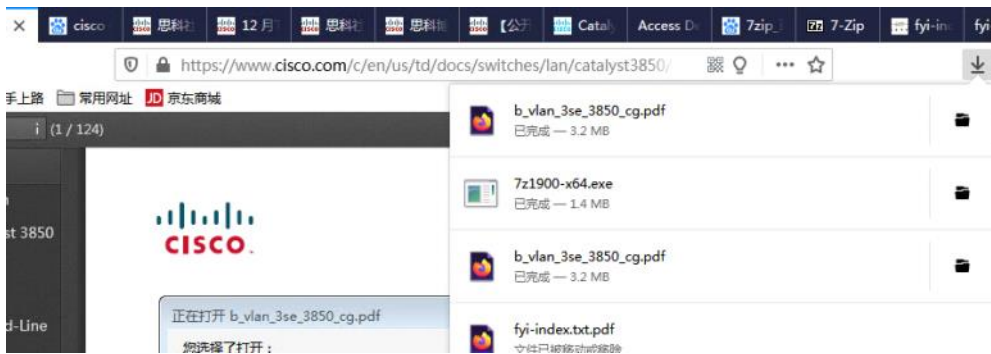




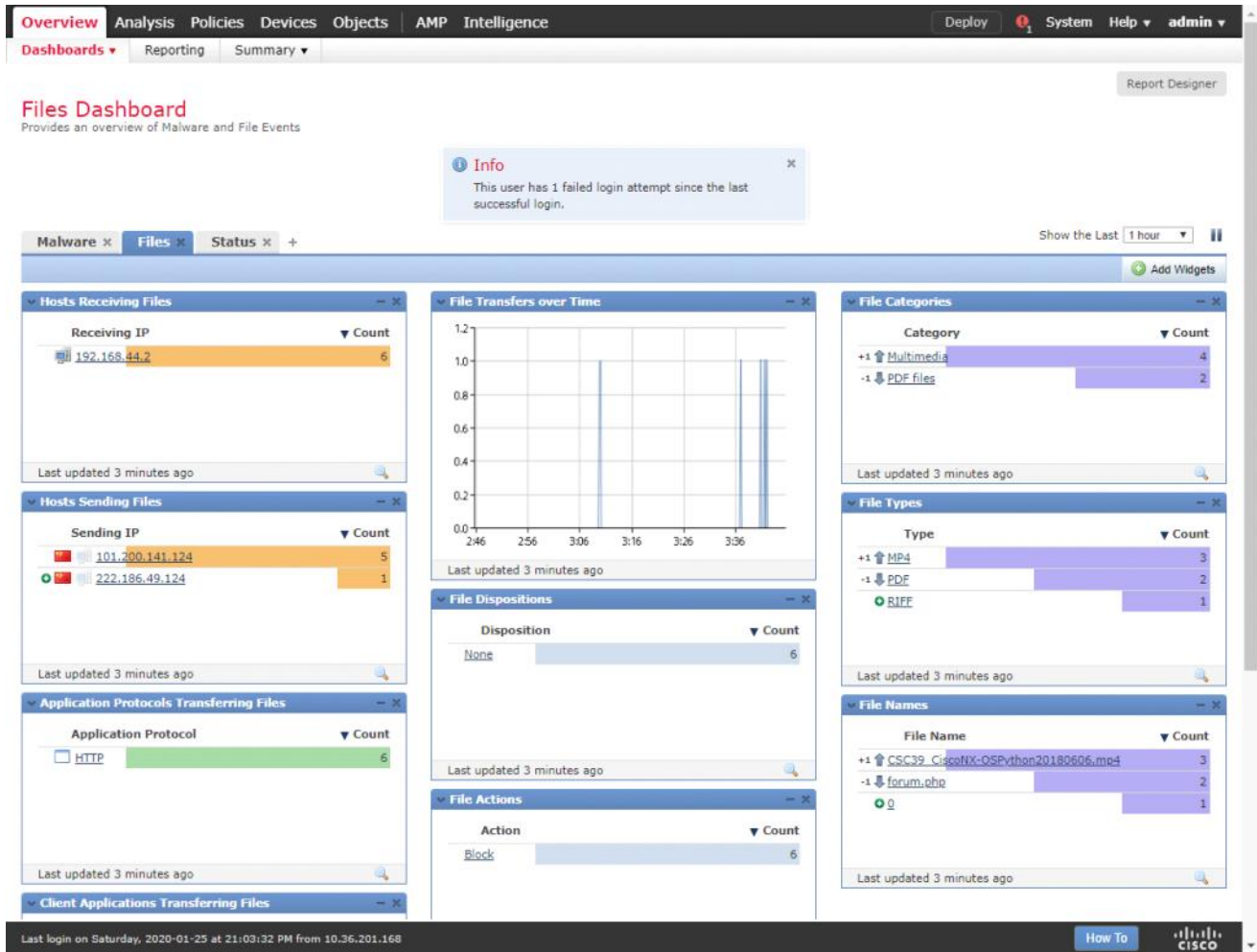
点进去可以看到文件传递的详细信息，什么时候传递，谁传递给谁



### 9.3: Https传递PDF测试，文件控制策略压根没用，因为SSL加密了防火墙没法识别流量内容



## 9.4: 校验专门的Files Dashboard



## 9.5: 在FTD上debug防火墙引擎对PDF流量的处理

> `system support firewall-engine-debug`

Please specify an IP protocol: `tcp`  
 Please specify a client IP address: `192.168.1.200`  
 Please specify a client port:  
 Please specify a server IP address:  
 Please specify a server port:  
 Monitoring firewall engine debug messages

```
192.168.1.200-58374 > 172.16.100.100-80 6 AS 4 I O New session
192.168.1.200-58374 > 172.16.100.100-80 6 AS 4 I O Starting with minimum 0, id 0 and
SrcZone first with zones -1 -> -1, geo 0(0) -> 0, vlan 0, sgt tag: untagged,
svc 0, payload 0, client 0, misc 0, user 9999997, url , xff
192.168.1.200-58374 > 172.16.100.100-80 6 AS 4 I O match rule order 2, 'Access Rule
for File Policy', action Allow
192.168.1.200-58374 > 172.16.100.100-80 6 AS 4 I O allow action
192.168.1.200-58374 > 172.16.100.100-80 6 AS 4 I O URL SI:
ShmDBLookupURL("http://172.16.100.100/files/userguide.pdf") returned 0
192.168.1.200-58374 > 172.16.100.100-80 6 AS 4 I O Starting with minimum 0, id 0 and
SrcZone first with zones -1 -> -1, geo 0(0) -> 0, vlan 0, sgt tag: untagged, svc
```

```
676, payload 0, client 638, misc 0, user 9999997, url http://172.16.100.100/files/userguide.pdf, xff
192.168.1.200-58374 > 172.16.100.100-80 6 AS 4 I 0 match rule order 2, 'Access Rule for File Policy', action Allow
192.168.1.200-58374 > 172.16.100.100-80 6 AS 4 I 0 allow action
. <Output omitted for brevity> . 192.168.1.200-58374 > 172.16.100.100-80 6 AS 4 I 0 File policy verdict is Type, Malware, and Capture
192.168.1.200-58374 > 172.16.100.100-80 6 AS 4 I 0 File type verdict Log, fileAction Log, flags 0x00001100, and type action Log for type 285 of instance 0
192.168.1.200-58374 > 172.16.100.100-80 6 AS 4 I 0 File type event for file named userguide.pdf with disposition Type and action Log . <Output omitted for brevity>
> ^C
```