配置SD-WAN高级恶意软件防护(AMP)集成和故障排除

目录

简介

本文档介绍如何在Cisco IOS® XE SD-WAN路由器上配置思科SD-WAN高级恶意软件防护(AMP)集成并对其进行故障排除。

先决条件

要求

Cisco 建议您了解以下主题：

- 高级恶意软件保护 (AMP)
- 思科软件定义的广域网(SD-WAN)

使用的组件

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

解决方案概述

组件

SD-WAN AMP集成是SD-WAN Edge安全解决方案不可分割的一部分，旨在为分支机构用户提供可视性和恶意软件防护。

它由以下产品组件组成：

- 分支机构的广域网边缘路由器。这是控制器模式下的Cisco IOS® XE路由器，在UTD容器中具有安全功能
- AMP云。AMP云基础设施以性质响应文件哈希查询
- ThreatGrid。可在沙盒环境中测试文件是否存在潜在恶意软件的云基础设施

这些组件协同工作，为AMP提供以下主要功能：

- 文件信誉评估

SHA256哈希的过程，用于将文件与高级恶意软件防护(AMP)云服务器进行比较，并访问其威胁情报信息。响应可以是“正常”、“未知”或“恶意”。如果响应为Unknown，并且配置了File Analysis，则系统会自动提交该文件以进行进一步分析。

- 文件分析

向ThreatGrid(TG)云提交未知文件，以便在沙盒环境中进行引爆操作。在引爆期间，沙盒捕获伪像并观察文件的行为，然后给出文件的总体得分。根据观察结果和得分，Threat Grid可以将威胁响应更改为“安全”或“恶意”。ThreatGrid的调查结果会报告给AMP云，这样所有AMP用户都能够防范新发现的恶意软件。

- 追溯

它维护有关文件的信息，即使在下载文件后，我们也可以报告下载后确定为恶意的文件。文件的处置方式可能会根据AMP云获得的新威胁情报发生变化。这种重新分类会生成自动追溯通知。

目前，集成AMP的SD-WAN支持以下协议的文件检查：

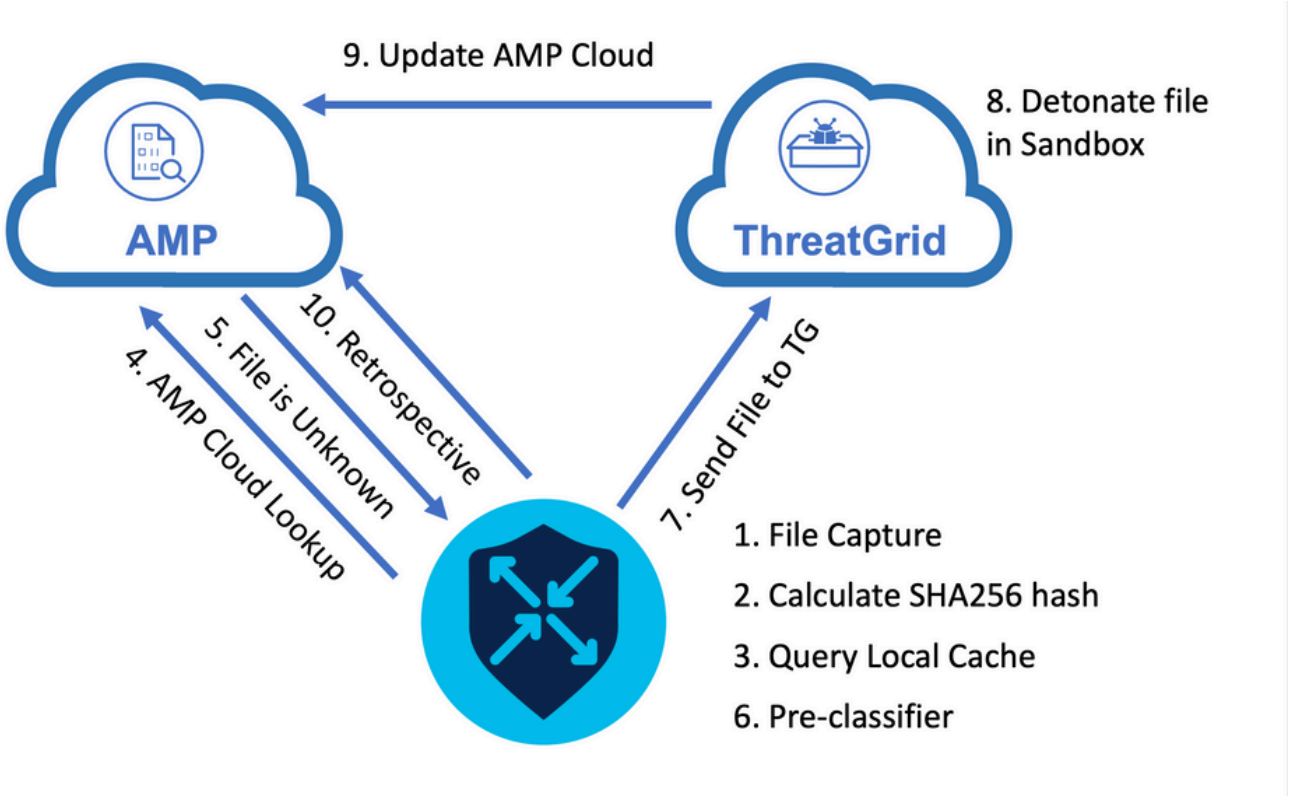
- HTTP
- SMTP
- IMAP
- POP3
- FTP
- 中小企业

注意：只有SSL/TLS代理支持通过HTTPS进行文件传输。

注意：文件分析只能对一个完整的文件执行，而不能对分解为部分内容的文件执行。 例如，当HTTP客户端请求带有Range报头的部分内容并返回HTTP/1.1 206 Partial Content时。 在这种情况下，由于部分文件哈希值与完整文件有很大不同，Snort将跳过部分内容的文件检查。

功能流

该图描述了需要将文件提交到ThreatGrid进行分析时SD-WAN AMP集成的高级流程。



对于所示的流：

1. 支持AMP的协议的文件传输由UTD容器捕获。
2. 计算文件的SHA256散列。
3. 根据UTD中的本地缓存系统查询计算的SHA256哈希值，以查看性质是否已经知道，以及缓存TTL是否尚未过期。
4. 如果没有与本地缓存匹配的项，则根据AMP云查找SHA256散列以查找处置和返回操作。
5. 如果处置情况为UNKNOWN且响应操作为ACTION_SEND，则文件通过UTD中的预分类系统运行。
6. 预分类器确定文件类型，并验证文件是否包含活动内容。
7. 如果满足这两个条件，则文件将提交到ThreatGrid。
8. ThreatGrid会在沙盒中引爆文件，并为文件分配威胁评分。
9. ThreatGrid根据威胁评估更新AMP云。
10. 边缘设备根据30分钟的心跳间隔查询AMP云以追溯性。

SD-WAN AMP集成配置

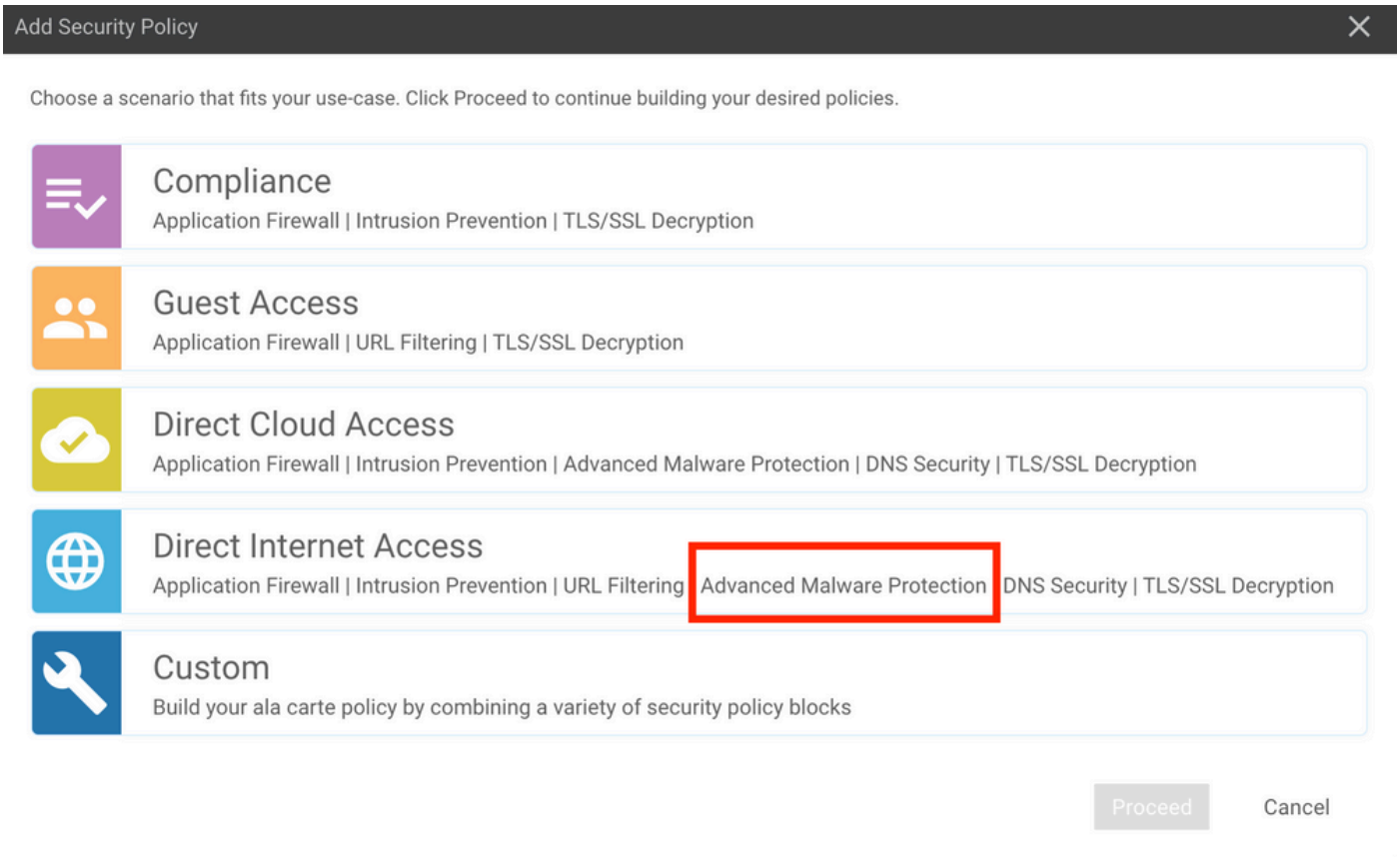
注意：在配置AMP功能之前，必须将安全虚拟映像上传到vManage。有关详细信息，请导航到安全虚拟映像。

注意：阅读本文档了解AMP/ThreatGrid连接正常工作的网络要求：AMP/TG所需的IP地址/主

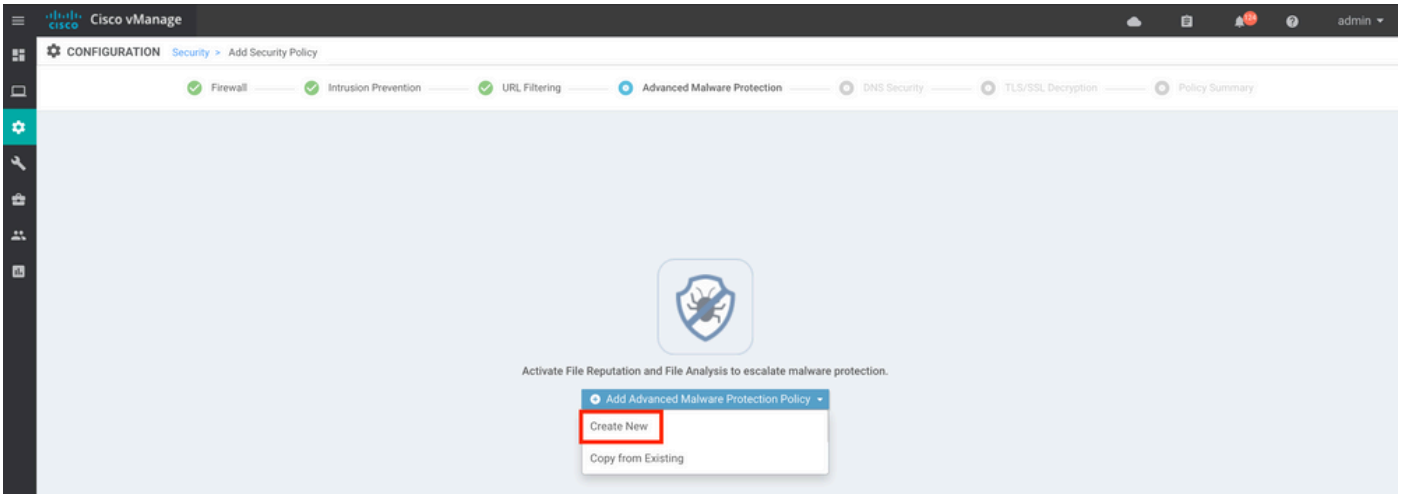
机名

从vManage配置安全策略

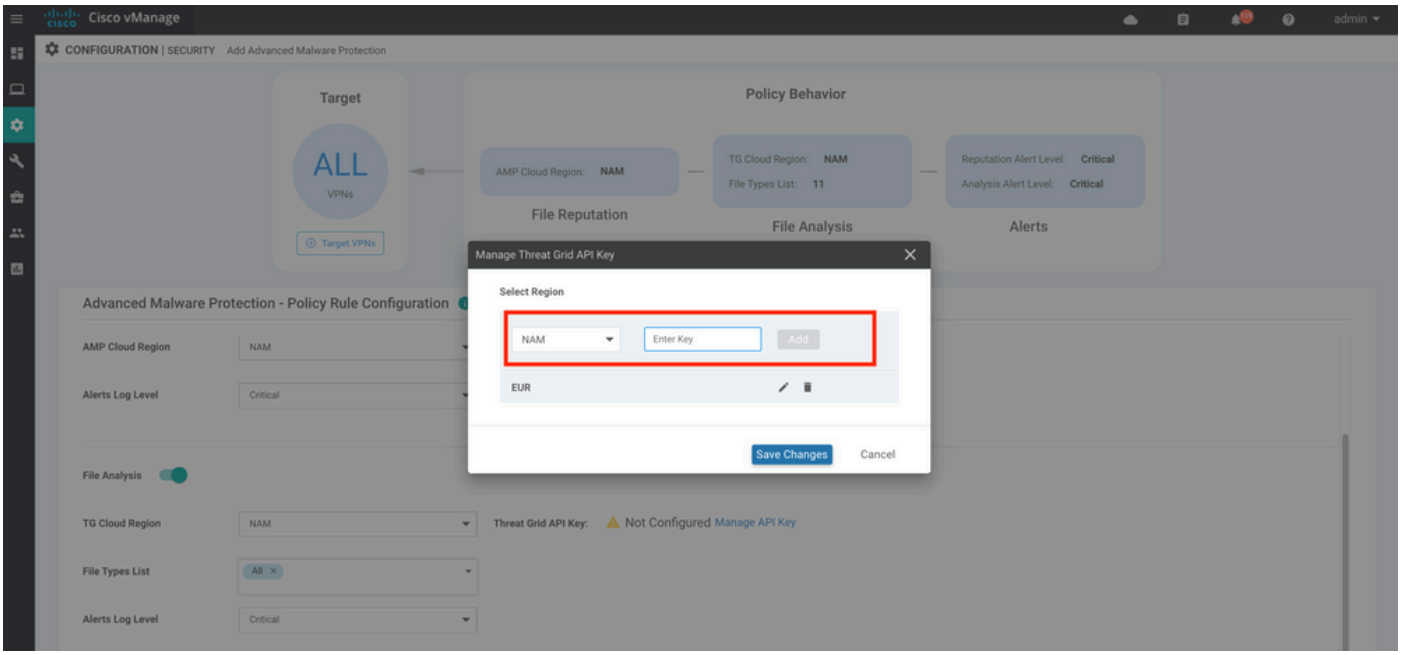
要启用AMP，请导航至配置 -> 安全 -> 添加安全策略。 选择Direct Internet Access并选择Proceed，如图所示。



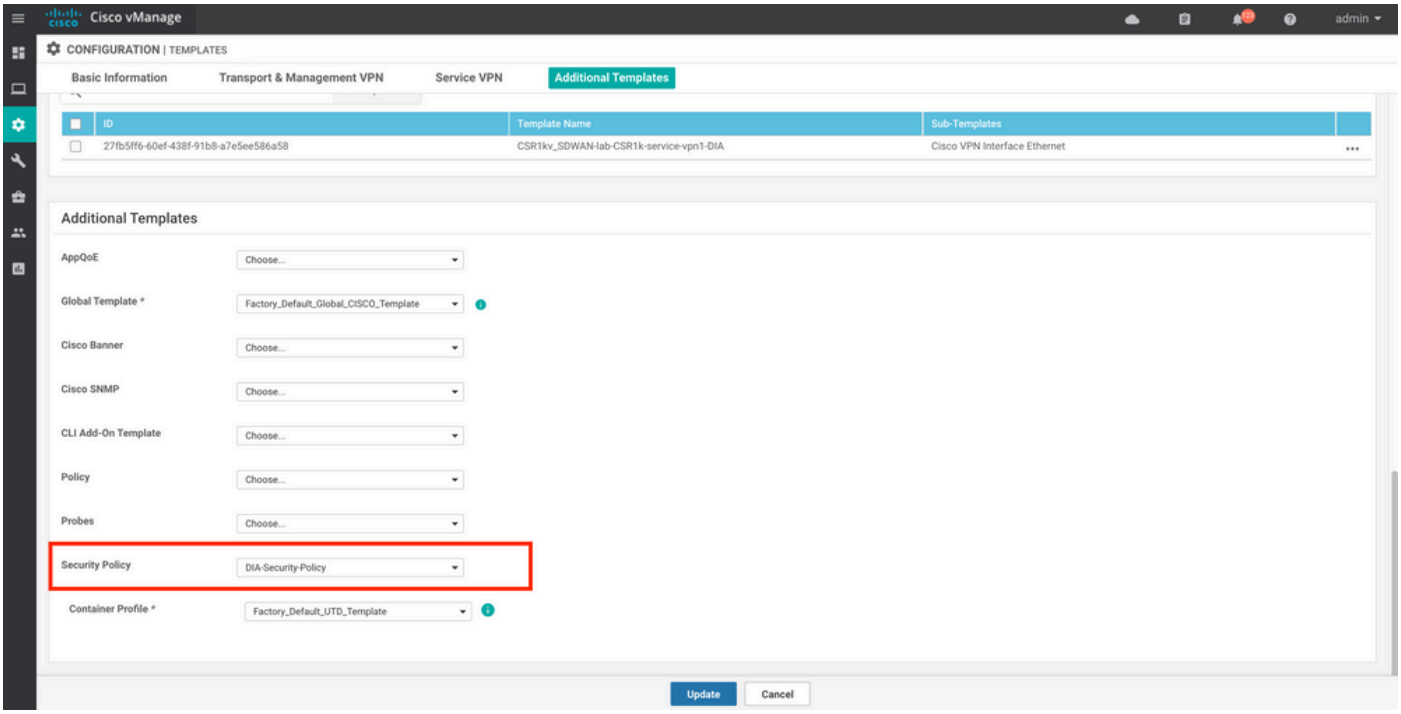
根据需要配置安全功能，直至其达到高级恶意软件防护功能。添加新的高级恶意软件防护策略。



提供策略名称。选择一个全局AMP云区域并启用文件分析。 对于使用ThreatGrid的文件分析，选择一个TG云区域，然后输入可从ThreatGrid门户的My ThreatGrid帐户下获取的ThreatGrid API密钥。



完成后，保存策略，并在Additional Templates -> Security Policy下将此安全策略添加到设备模板，如图所示。



使用更新的设备模板配置设备。

验证

设备模板成功推送到边缘设备后，可以从边缘路由器CLI验证AMP配置：

<#root>

```
branch1-edge1#show sdwan running-config | section utd
app-hosting appid utd
```

```
 app-resource package-profile cloud-low
 app-vnic gateway0 virtualportgroup 0 guest-interface 0
  guest-ipaddress 192.168.1.2 netmask 255.255.255.252
!
app-vnic gateway1 virtualportgroup 1 guest-interface 1
 guest-ipaddress 192.0.2.2 netmask 255.255.255.252
!
 start
utd multi-tenancy
utd engine standard multi-tenancy
threat-inspection profile IPS_Policy_copy
threat detection
policy balanced
logging level notice
!
utd global
```

file-reputation

```
  cloud-server cloud-isr-asn.amp.cisco.com
  est-server cloud-isr-est.amp.cisco.com
!
```

file-analysis

```
 cloud-server isr.api.threatgrid.com
 apikey 0 <redacted>
!
!
```

file-analysis profile AMP-Policy-fa-profile

```
 file-types
  pdf
  ms-exe
  new-office
  rtf
  mdb
  mscab
  msole2
  wri
  xlw
  flv
  swf
!
 alert level critical
!
```

file-reputation profile AMP-Policy-fr-profile

```
 alert level critical
!
```

file-inspection profile AMP-Policy-fi-profile

analysis profile AMP-Policy-fa-profile

```
 reputation profile AMP-Policy-fr-profile


!
policy utd-policy-vrf-1
 all-interfaces
 file-inspection profile AMP-Policy-fi-profile


 vrf 1
 threat-inspection profile IPS_Policy_copy
exit
policy utd-policy-vrf-global
 all-interfaces
 file-inspection profile AMP-Policy-fi-profile


 vrf global
exit
no shutdown
```

故障排除

SD-WAN AMP集成涉及许多组件，如前所述。因此，进行故障排除时，必须建立一些关键分界点，将问题缩小到功能流中的组件：

1. vManage.vManage能否成功将带有AMP策略的安全策略推送到边缘设备？
2. 边缘。安全策略成功推送到边缘后，路由器是否捕获接受AMP检查的文件并将其发送到AMP/TG云？
3. AMP/TG云。如果边缘将文件发送到AMP或TG，它是否获得做出允许或丢弃决策所需的响应？

本文重点介绍边缘设备(2)以及各种数据平面工具，这些工具可用于帮助排除WAN边缘路由器上的AMP集成问题。

一般故障排除流程

使用此高级工作流程快速排除AMP集成涉及的各种组件故障，其主要目标是确定边缘设备与AMP/TG云之间的问题分界点。

1. AMP策略是否正确推送到边缘设备？
2. 检查UTD容器的常规运行状况。
3. 检查文件信誉并分析边缘上的客户端状态。
4. 检查文件传输是否转移到容器。这可以通过Cisco IOS® XE数据包跟踪完成。
5. 检查以确认边缘已成功与AMP/TG云通信。这可以通过EPC或数据包跟踪等工具完成。
6. 确保UTD根据AMP响应创建本地缓存。

本文档详细介绍这些故障排除步骤。

vManage上的策略推送问题

如AMP策略配置所示，AMP策略非常简单，没有很多配置选项。以下是需要考虑的一些常见问题：

1. vManage必须能够解析AMP的DNS名称，以及用于API访问的ThreatGrid云。如果在添加AMP策略后，vManage上的设备配置失败，请查看/var/log/nms/vmanage-server.log中是否存在错误。
2. 如配置指南中所述，“警报日志级别”已保留默认严重级别，或者“警告”（如有必要）。必须避免信息级日志记录，因为它可能会对性能产生负面影响。

要验证，请访问neo4j数据库并查看vmanagedbAPIKEYNODE表的内容。

```
neo4j@neo4j> match (n:vmanagedbAPIKEYNODE) return n; +----------
--------
--------+ | n | +----------
----------+ | (:vmanagedbAPIKEYNODE {_rid:
"0:ApiKeyNode:1621022413389:153", keyServerHostName: "isr.api.threatgrid.com", feature: "Amp", apiKey:
"$CRYPT_CLUSTER$IbGLEMGlYMNRy1s9P+WcfA==$dozo7tmRP1+HrvEnXQr4x1VxSViYkKwQ4HBAlhXWOtQ=", deviceID: "CSR-
07B6865F-7FE7-BA0D-7240-1BDA16328455"}) | +----------
----------+
```

思科边缘路由器上的AMP集成

检查UTD容器运行状况

使用show utd命令检查UTD容器的整体运行状况：

```
show utd engine standard config
show utd engine standard status
show platform hardware qfp active feature utd config
show platform hardware qfp active feature utd stats
show app-hosting detail appid utd
show sdwan virtual-application utd
```

检查UTD AMP状态

确保已启用文件检查：

<#root>

```
branch1-edge1#show sdwan utd dataplane config
 utd-dp config context 0
 context-flag 25427969
 engine Standard
 state enabled
 sn-redirect fail-open
 redirect-type divert
```

```
 threat-inspection not-enabled
 defense-mode not-enabled
 domain-filtering not-enabled
 url-filtering not-enabled
 all-interface enabled
 file-inspection enabled

utd-dp config context 1
 context-flag 25559041
 engine Standard
 state enabled
 sn-redirect fail-open
 redirect-type divert
 threat-inspection enabled
 defense-mode IDS
 domain-filtering not-enabled
 url-filtering not-enabled
 all-interface enabled
 file-inspection enabled
```

验证与AMP云的连接是否已启动：

<#root>

```
branch1-edge1#show utd engine standard status file-reputation
File Reputation Status:
        Process:
Running

        Last known status: 2021-06-17 16:14:20.357884-0400 [info] AMP module version 1.12.4.999
```

<#root>

```
branch1-edge1#show sdwan utd file reputation
utd-oper-data utd-file-reputation-status version 1.12.4.999
utd-oper-data utd-file-reputation-status status utd-file-repu-stat-connected

utd-oper-data utd-file-reputation-status message "Connected to AMP Cloud!"
```

验证与ThreatGrid的连接是否已启用：

<#root>

```
branch1-edge1#show utd engine standard status file-analysis
File Analysis Status:
        Process:
```

```
Running

        Last Upload Status: No upload since process init
```

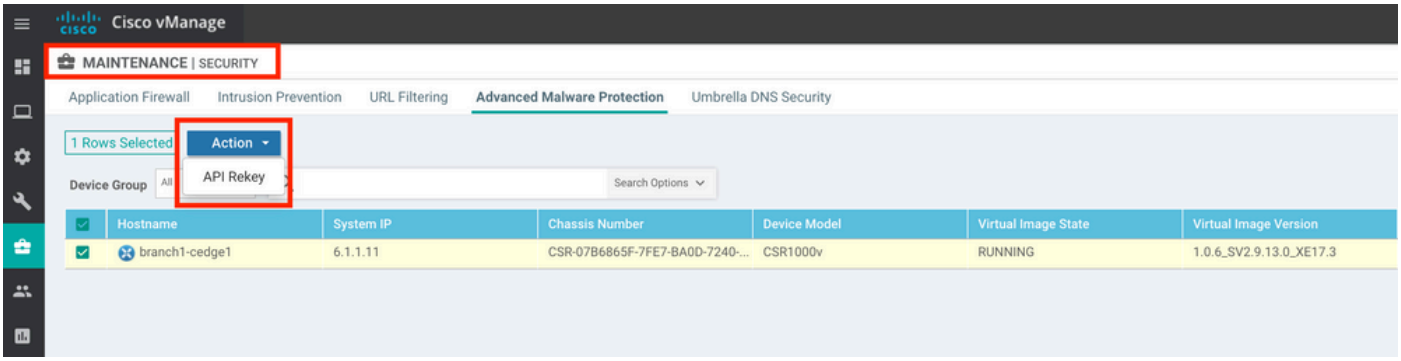
<#root>

```
branch1-edge1#show sdwan utd file analysis

utd-oper-data utd-file-analysis-status status tg-client-stat-up


utd-oper-data utd-file-analysis-status backoff-interval 0
utd-oper-data utd-file-analysis-status message "TG Process Up"
```

如果ThreatGrid进程未显示Up状态，则API重新生成密钥会有所帮助。要触发API重新生成密钥，请导航到维护 -> 安全:



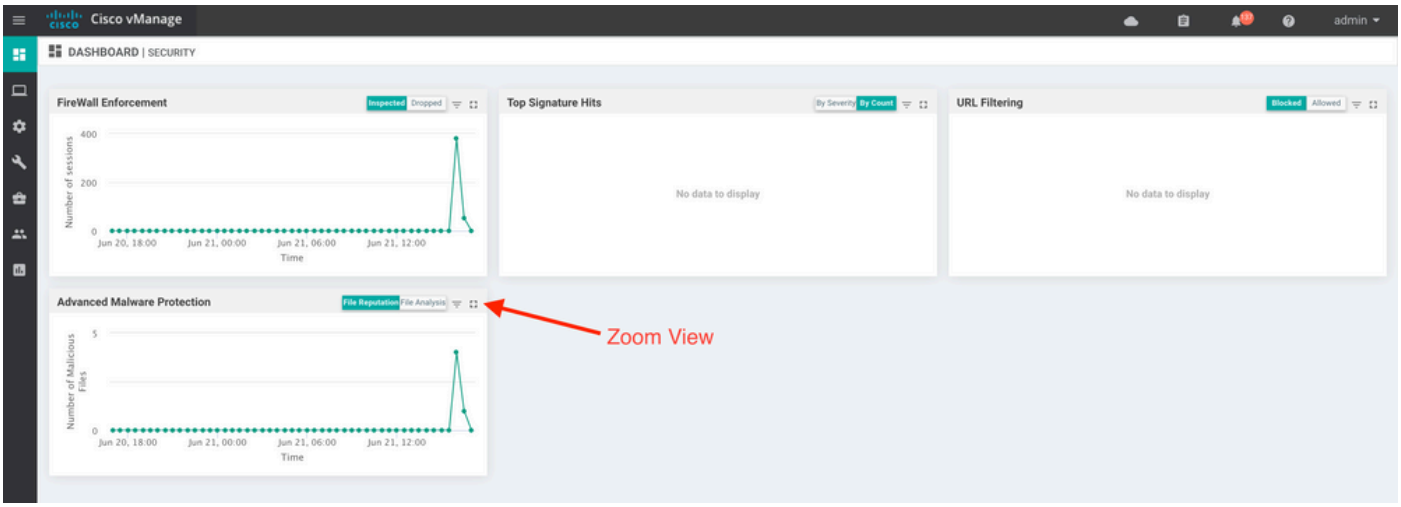
注意：API重新生成密钥会触发向设备的模板推送。

广域网边缘路由器上的AMP活动监控

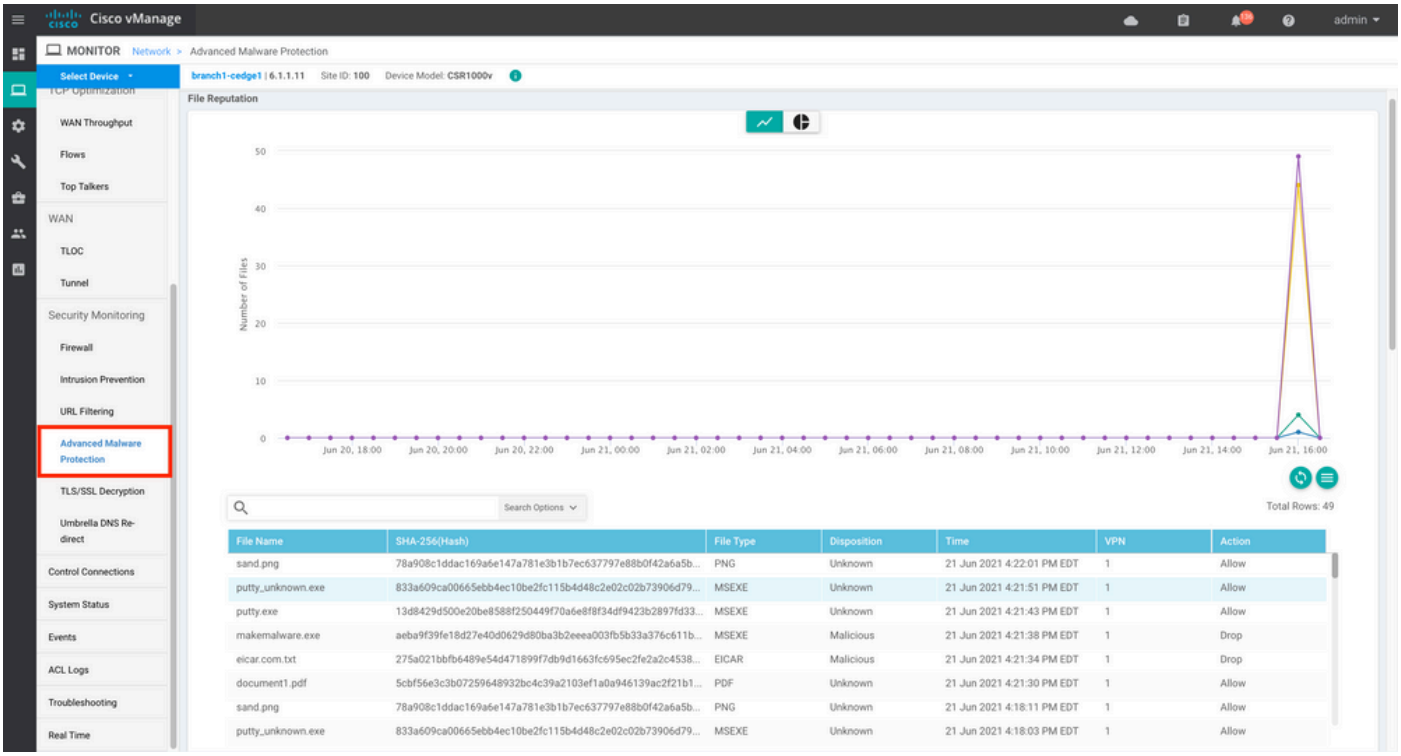
vManage

通过vManage，可以从安全控制面板或设备视图监控AMP文件活动。

安全仪表板:



设备视图：



CLI

检查文件信誉统计信息：

```
branch1-edge1#show utd engine standard statistics file-reputation
File Reputation Statistics
--------------------------
File Reputation Clean Count:            1
File Reputation Malicious Count:        4
File Reputation Unknown Count:         44
File Reputation Requests Error:         0
File Reputation File Block:             4
File Reputation File Log:              45
```

检查文件分析统计信息：

```
branch1-edge1#show utd engine standard statistics file-analysis
File Analysis Statistics
------------------------
File Analysis Request Received:         2
File Analysis Success Submissions:      2
File Analysis File Not Interesting:     0
File Analysis File Whitelisted:         0
File Analysis File Not Supported:       0
File Analysis Limit Exceeding:          0
File Analysis Failed Submissions:       0
File Analysis System Errors:            0
```

注意：可以使用命令show utd engine standard statistics file-reputation vrf global internal获取其他内部统计信息。

数据平面行为

根据已配置的AMP策略进行文件检查的Dataplane流量将转移到UTD容器中进行处理。这可以通过使用数据包跟踪进行确认。如果流量没有正确转移至容器，则不会发生任何后续文件检查操作。

AMP本地文件缓存

UTD容器具有SHA256散列、文件类型、处置情况和基于先前AMP云查找结果的操作的本地缓存。如果文件散列不在本地缓存中，则容器仅从AMP云请求处置情况。在删除缓存之前，本地缓存的TTL为2小时。

```
branch1-edge1#show utd engine standard cache file-inspection
Total number of cache entries: 6
File Name|                      SHA256|             File Type|        Disposition|         action|
-------------------------------------------------------------------------------------------------------
sand.png              78A908C1DDAC169A                     69                  1                 1
putty.exe             13D8429D500E20BE                     21                  1                 2
makemalware.exe       AEBA9F39FE18D27E                     21                  3                 2
putty_unknown.exe     833A609CA00665EB                     21                  1                 2
document1.pdf         5CBF56E3C3B07259                    285                  1                 1
eicar.com.txt         275A021BBFB6489E                    273                  3                 2
```

AMP处置代码：

```
0 NONE
1 UNKNOWN
2 CLEAN
3 MALICIOUS
```

AMP操作代码：

```
0 UNKNOWN
1 ALLOW
2 DROP
```

要获取文件的完整SHA256哈希值（这对于解决特定文件判定问题非常重要），请使用命令的detail选项：

```
branch1-edge1#show utd engine standard cache file-inspection detail
SHA256: 78A908C1DDAC169A6E147A781E3B1B7EC637797E88B0F42A6A5B59810B8E7EE5
amp verdict: unknown
amp action: 1
amp disposition: 1
reputation score: 0
retrospective disposition: 0
amp malware name:
file verdict: 1
TG status: 0
file name: sand.png
filetype: 69
create_ts: 2021-06-21 16:58:1624309104
sig_state: 3
-----------------------------------------------------------------------------------------
SHA256: 13D8429D500E20BE8588F250449F70A6E8F8F34DF9423B2897FD33BBB8712C5F
amp verdict: unknown
amp action: 2
amp disposition: 1
reputation score: 0
retrospective disposition: 0
amp malware name:
file verdict: 1
TG status: 7
file name: putty.exe
filetype: 21
create_ts: 2021-06-21 16:58:1624309107
sig_state: 3
-----------------------------------------------------------------------------------------
SHA256: AEBA9F39FE18D27E40D0629D80BA3B2EEEA003FB5B33A376C611BB4D8FFD03A6
amp verdict: malicious
amp action: 2
amp disposition: 3
reputation score: 95
retrospective disposition: 0
amp malware name: W32.AEBA9F39FE-95.SBX.TG
file verdict: 1
TG status: 0
file name: makemalware.exe
filetype: 21
create_ts: 2021-06-21 16:58:1624309101
sig_state: 3
<SNIP>
```

要取消对UTD引擎本地缓存条目的路由，请使用命令：

```
clear utd engine standard cache file-inspection
```

运行UTD调试

可以启用utd调试以排除AMP问题：

```
debug utd engine standard file-reputation level info
debug utd engine standard file-analysis level info
debug utd engine standard climgr level info
```

可以直接从系统外壳中检索调试输出(位于/tmp/rp/trace/vman_utd_R0-0.bin)，或者按以下步骤将跟踪文件复制到路由器文件系统：

```
branch1-edge1#app-hosting move appid utd log to bootflash:
Successfully moved tracelog to bootflash:/iox_utd_R0-0_R0-0.5113_0.20210622110241.bin.gz
branch1-edge1#
```

要查看UTD跟踪日志，请执行以下操作：

```
branch1-edge1#more /compressed bootflash:/iox_utd_R0-0_R0-0.5113_0.20210622110241.bin.gz
<snip>
2021-06-22 10:35:04.265:(#1):SPP-FILE-INSPECTION File signature query: sig_state = 3
2021-06-22 10:35:04.266:(#1):SPP-FILE-INSPECTION start_time : 1624372489, current_time : 1624372504,Dif
2021-06-22 10:35:04.266:(#1):SPP-FILE-INSPECTION amp_cache_node_exists:: Entry
2021-06-22 10:35:04.266:(#1):SPP-FILE-INSPECTION Signature not found in cache
2021-06-22 10:35:04.266:(#1):SPP-FILE-INSPECTION file_type_id = 21
2021-06-22 10:35:04.266:(#1):SPP-FILE-INSPECTION Write to cbuffer
2021-06-22 10:35:04.266:(#1):SPP-FILE-INSPECTION Sent signature lookup query to Beaker
2021-06-22 10:35:04.266:(#1):SPP-FILE-INSPECTION File Name = /putty_unknown.exe, file_name = /putty_unk
2021-06-22 10:35:04.266:(#1):SPP-FILE-INSPECTION amp_extract_filename :: Extracted filename 'putty_unkn
2021-06-22 10:35:04.266:(#1):SPP-FILE-INSPECTION amp_cache_add:: Entry
2021-06-22 10:35:04.266:(#1):SPP-FILE-INSPECTION amp_cache_allocate:: Entry
2021-06-22 10:35:04.266:(#1):SPP-FILE-INSPECTION Return FILE_VERDICT_PENDING
<SNIP>
```


注意：在20.6.1及更高版本中，检索和查看utd tracelogs的方式与使用show logging process vman module utd ...命令的标准跟踪工作流程一致。

验证从边缘到云的通信

要验证边缘设备与AMP/TG云通信，可以使用广域网边缘路由器上的EPC来确认与云服务之间是否存在双向通信：

```
branch1-edge1#show monitor capture amp parameter
monitor capture amp interface GigabitEthernet1 BOTH
monitor capture amp access-list amp-cloud
monitor capture amp buffer size 10
monitor capture amp limit pps 1000
```

AMP和TG云相关问题

一旦确认边缘设备正确捕获文件并将其发送到AMP/TG进行分析，但判定不正确，则需要AMP故障排除或Threatgrid云，这不在本文档的讨论范围之内。在出现集成问题时，这些信息非常重要：

- ThreatGrid帐户组织
- 时间戳
- 设备分析ID(例如，CSR-07B6865F-7FE7-BA0D-7240-1BDA16328455)，这是广域网边缘路由器的机箱编号。
- 完成有问题的文件的SHA256哈希

相关信息

- SD-WAN安全配置指南
- ThreatGrid门户
- 技术支持和文档 - Cisco Systems

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。