

SD-WAN Advanced Malware Protection(AMP)統合の設定とトラブルシューティング

内容

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[ソリューションの概要](#)

[コンポーネント](#)

[機能のフロー](#)

[SD-WAN AMP統合の設定](#)

[vManageからのセキュリティポリシーの設定](#)

[確認](#)

[トラブルシューティング](#)

[一般的なトラブルシューティングフロー](#)

[vManageでのポリシープッシュの問題](#)

[CiscoエッジルータでのAMPの統合](#)

[UTDコンテナの健全性の確認](#)

はじめに

このドキュメントでは、Cisco IOS® XE SD-WANルータでCisco SD-WAN Advanced Malware Protection(AMP)統合を設定し、トラブルシューティングする方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Advanced Malware Protection (AMP)
- Cisco Software-Defined Wide Area Network(SD-WAN)

使用するコンポーネント

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

ソリューションの概要

コンポーネント

SD-WAN AMPの統合は、ブランチのユーザをマルウェアから可視化し、保護することを目的としたSD-WANエッジセキュリティソリューションに不可欠な要素です。

次の製品コンポーネントで構成されています。

- ブランチのWANエッジルータ。これは、UTDコンテナにセキュリティ機能を備えたコントロールモードのCisco IOS® XEルータです
- AMP クラウド.AMPクラウドインフラストラクチャは、ファイルハッシュクエリに対して性質を持って応答します
- ThreatGridです。サンドボックス環境で潜在的なマルウェアのファイル进行测试できるクラウドインフラストラクチャ

これらのコンポーネントは連携して、AMPに次の主要な機能を提供します。

- ファイルレピュテーションアセスメント

高度なマルウェア防御(AMP)クラウドサーバとファイルを比較し、脅威インテリジェンス情報にアクセスするために使用されるSHA256ハッシュのプロセス。応答には、クリーン、不明、または悪意がある可能性があります。応答が「不明」で、ファイル分析が設定されている場合、ファイルは自動的に送信され、さらに分析が行われます。

- ファイル分析

サンドボックス環境でのデトネーションのために、不明なファイルがThreatGrid(TG)クラウドに送信されます。デトネーション中、サンドボックスはアーティファクトをキャプチャしてファイルの動作を観察し、ファイル全体のスコアを取得します。観察とスコアに基づいて、Threat Gridは脅威への対応をクリーンまたは悪意のある応答に変更できます。ThreatGridの結果はAMPクラウドに報告されるため、すべてのAMPユーザは新たに検出されたマルウェアから保護されます。

- レトロスペクシオン


ダウンロード後もファイルに関する情報を保持し、ダウンロード後に悪意があると判断されたファイルについてレポートできます。AMPクラウドで取得された新しい脅威インテリジェンスに基づいて、ファイルの性質が変わる可能性があります。この再分類により、自動的に遡及通知が生成されます。

現在、AMP統合を備えたSD-WANは、次のプロトコルのファイルインスペクションをサポートしています。

- HTTP
- SMTP
- IMAP
- POP3

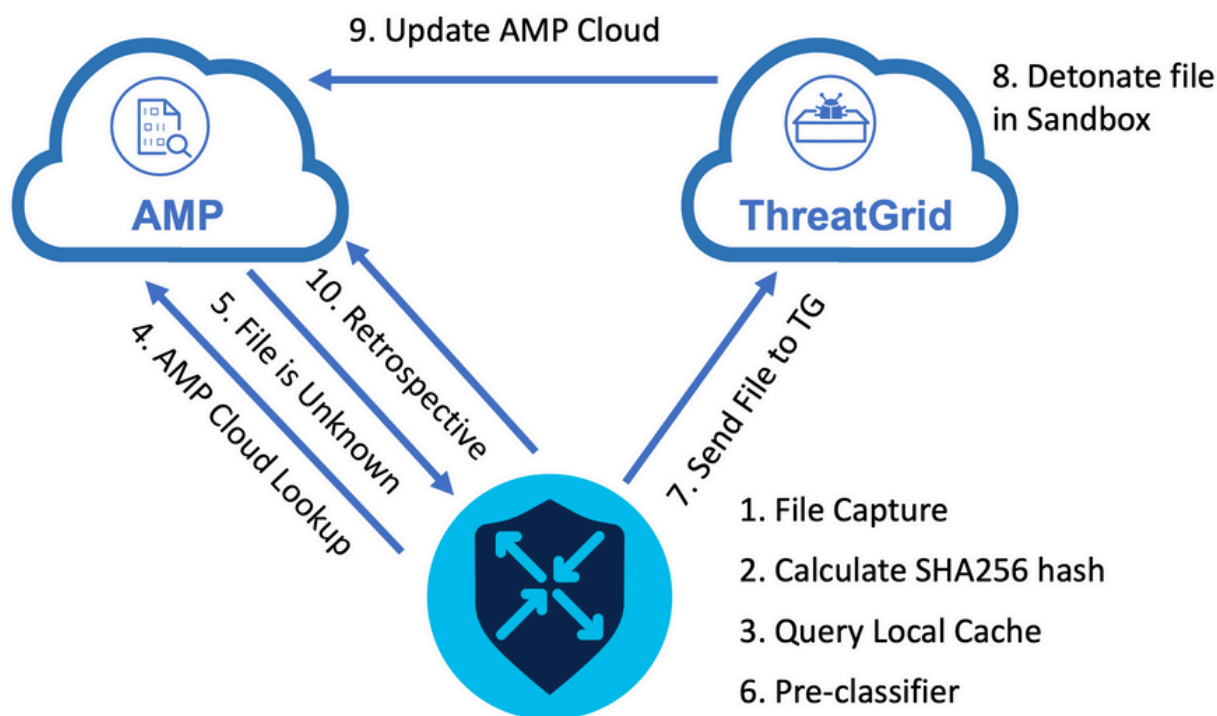
- FTP
- SMB

 注：HTTPS経由のファイル転送は、[SSL/TLSプロキシ](#)でのみサポートされています。

 注：ファイル分析はファイル全体に対してのみ実行でき、ファイルを部分的なコンテンツに分割することはできません。たとえば、HTTPクライアントがRangeヘッダーを含む部分的なコンテンツを要求し、HTTP/1.1 206 Partial Contentを取得する場合があります。この場合、部分ファイルハッシュが完全なファイルと大きく異なるため、Snortは部分コンテンツのファイルインスペクションをスキップします。

機能のフロー

この図は、分析のためにファイルをThreatGridに送信する必要がある場合の、SD-WAN AMP統合の高レベルフローを示しています。



示されているフローについて：


1. AMPがサポートするプロトコルのファイル転送は、UTDコンテナによってキャプチャされます。
2. ファイルのSHA256ハッシュが計算されます。
3. 計算されたSHA256ハッシュがUTDのローカルキャッシュシステムに照会され、廃棄がすでに既知で、キャッシュTTLが期限切れになっていないかが確認されます。
4. ローカルキャッシュと一致するものがない場合、SHA256ハッシュはAMPクラウドに対して検索され、廃棄と戻りアクションが行われます。
5. 廃棄がUNKNOWNで、応答アクションがACTION_SENDの場合、ファイルはUTDの事前分

類システムを介して実行されます。

6. 事前分類子はファイルタイプを決定し、ファイルにアクティブコンテンツが含まれているかどうかを検証します。
7. 両方の条件が満たされると、ファイルはThreatGridに送信されます。
8. ThreatGridはサンドボックス内のファイルを起爆処理し、ファイルに脅威スコアを割り当てます。
9. ThreatGridは、脅威評価に基づいてAMPクラウドを更新します。
10. エッジデバイスは、30分のハートビート間隔に基づいて、AMPクラウドにレトロスペクティブを照会します。

SD-WAN AMP統合の設定

 注：AMP機能を設定する前に、セキュリティ仮想イメージをvManageにアップロードする必要があります。詳細については、[Security Virtual Image](#)を参照してください。






 注：AMP/ThreatGrid接続が正しく動作するためのネットワーク要件については、このドキュメントを参照してください：[AMP/TG必須IPアドレス/ホスト名](#)

vManageからのセキュリティポリシーの設定

AMPを有効にするには、Configuration -> Security -> Add Security Policyの順に選択します。Direct Internet Accessを選択し、図に示すようにProceedを選択します。

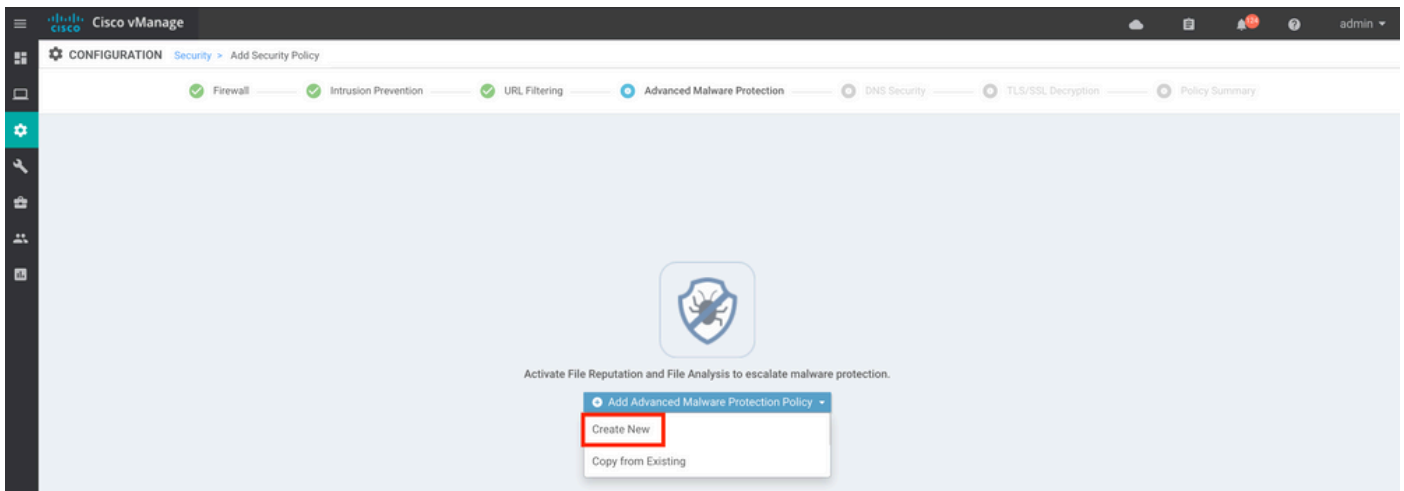
Add Security Policy ✕

Choose a scenario that fits your use-case. Click Proceed to continue building your desired policies.

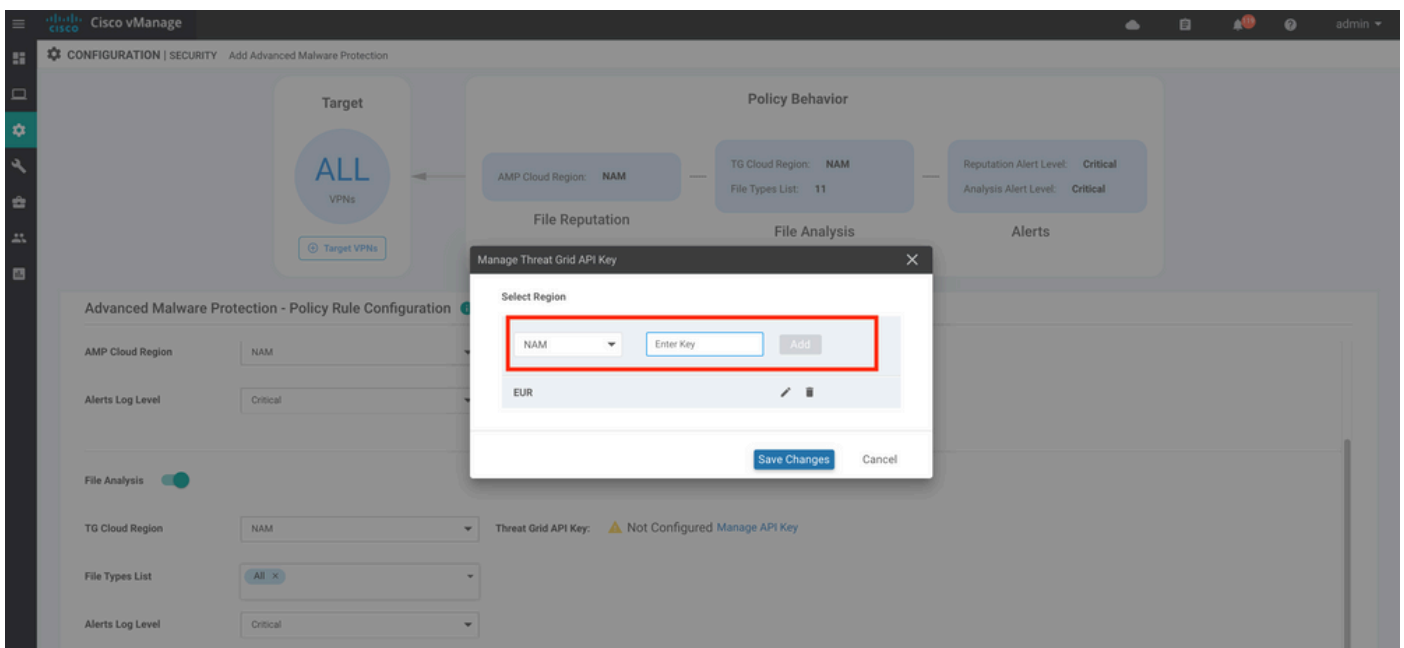
-  **Compliance**
Application Firewall | Intrusion Prevention | TLS/SSL Decryption
-  **Guest Access**
Application Firewall | URL Filtering | TLS/SSL Decryption
-  **Direct Cloud Access**
Application Firewall | Intrusion Prevention | Advanced Malware Protection | DNS Security | TLS/SSL Decryption
-  **Direct Internet Access**
Application Firewall | Intrusion Prevention | URL Filtering | **Advanced Malware Protection** | DNS Security | TLS/SSL Decryption
-  **Custom**
Build your ala carte policy by combining a variety of security policy blocks

Proceed Cancel

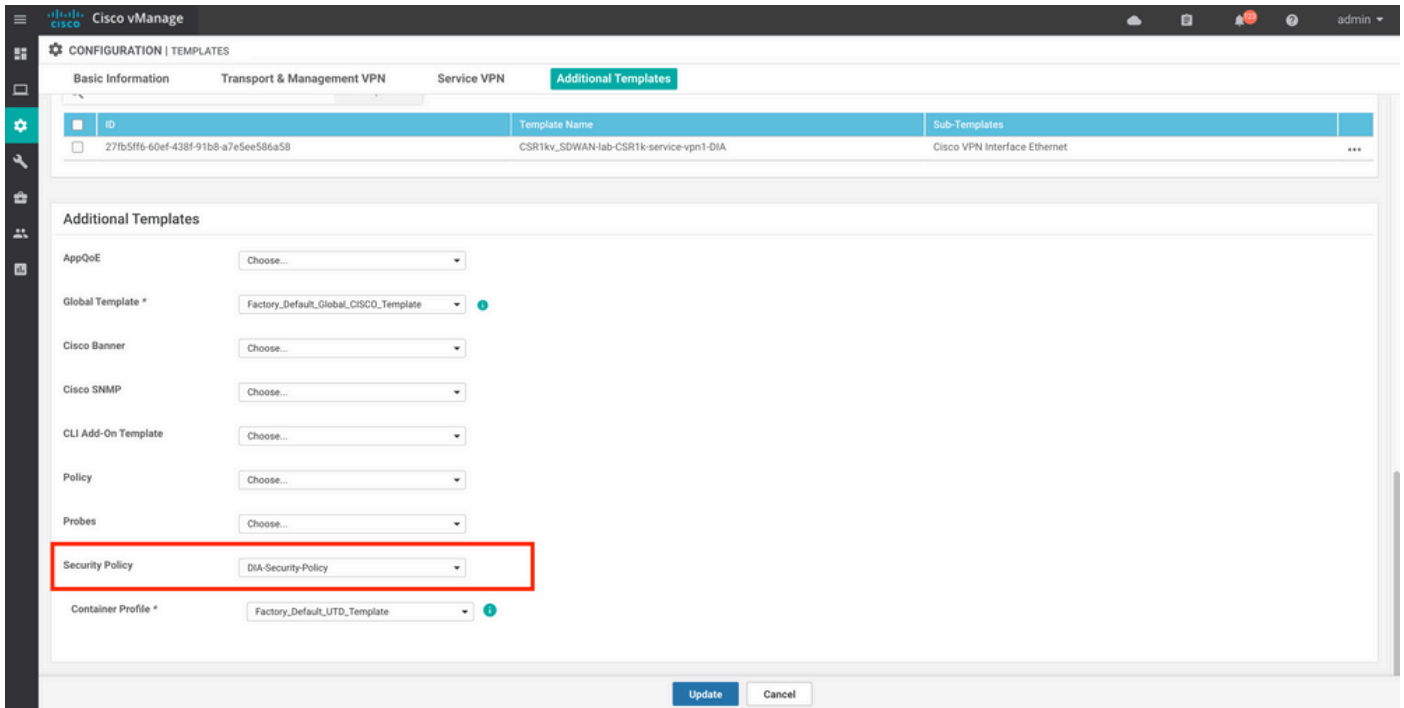
Advanced Malware Protection機能が有効になるまで、必要に応じてセキュリティ機能を設定します。新しい高度なマルウェア防御ポリシーを追加します。



ポリシー名を指定します。グローバルAMPクラウド領域のいずれかを選択し、ファイル分析を有効にします。ThreatGridを使用したファイル分析では、TGクラウド領域のいずれかを選択し、ThreatGrid APIキーを入力します。このキーは、ThreatGridポータル(My ThreatGridアカウント)から取得できます。



完了したら、図に示すように、ポリシーを保存し、このセキュリティポリシーをデバイステンプレートのAdditional Templates -> Security Policyの下に追加します。



更新されたデバイステンプレートを使用してデバイスを設定します。

確認

デバイステンプレートがエッジデバイスに正常にプッシュされたら、エッジルータのCLIからAMP設定を確認できます。

```
<#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
```

トラブルシューティング

SD-WAN AMPの統合には、前述のように多くのコンポーネントが含まれます。そのため、トラブルシューティングを行う際には、問題を機能フロー内のコンポーネントに絞り込むための重要な境界ポイントを確立できることが重要です。

1. vManage.vManageは、AMPポリシーを含むセキュリティポリシーをエッジデバイスに正常にプッシュできますか。
2. エッジ。セキュリティポリシーがエッジに正常にプッシュされたら、ルータはAMPインスペクションの対象となるファイルをキャプチャし、AMP/TGクラウドに送信しますか。
3. AMP/TGクラウド。エッジがAMPまたはTGにファイルを送信した場合、許可またはドロップの決定に必要な応答を受け取りますか。

この記事は、WANエッジルータでのAMP統合に関する問題のトラブルシューティングに役立つさまざまなデータプレーンツールを備えたエッジデバイス(2)に焦点を当てることを目的としています。

一般的なトラブルシューティングフロー

エッジデバイスとAMP/TGクラウド間の問題の境界ポイントを確立する主な目的で、この高度なワークフローを使用して、AMP統合に関連するさまざまなコンポーネントを迅速にトラブルシューティングします。

1. AMPポリシーはエッジデバイスに正しくプッシュされますか。
2. UTDコンテナの全般的な状態をチェックします。
3. ファイルレピュテーションを確認し、エッジのクライアントステータスを分析します。
4. ファイル転送がコンテナに転送されているかどうかを確認します。これは、Cisco IOS® XEパケットトレースを使用して実行できます。
5. エッジがAMP/TGクラウドと正常に通信していることを確認します。これは、EPCやパケットトレースなどのツールを使用して実行できます。
6. UTDがAMP応答に基づいてローカルキャッシュを作成することを確認します。

このドキュメントでは、次のトラブルシューティング手順について詳しく説明します。

vManageでのポリシープッシュの問題

AMPポリシーの設定で示すように、AMPポリシーは設定オプションの多くなしでかなり単純です。一般的に考慮すべき事項を次に示します。

1. vManageは、APIアクセスのためにAMPおよびThreatGridクラウドのDNS名を解決する必要があります。AMPポリシーの追加後にvManageでデバイス設定が失敗する場合は、`/var/log/nms/vmanage-server.log`でエラーを確認します。
2. 構成ガイドに記載されているように、アラートログレベルはデフォルトの重大レベル、または警告（必要な場合）のままになっています。情報レベルのロギングはパフォーマンスに悪影響を及ぼす可能性があるため、使用しないでください。

確認するには、neo4j DBにアクセスし、vmanagedbAPIKEYNODEテーブルの内容を表示します

。

```
neo4j@neo4j> match (n:vmanagedbAPIKEYNODE) return n; +-----+
+-----+ | n | +-----+
+-----+ | (:vmanagedbAPIKEYNODE {_rid:
"0:ApiKeyNode:1621022413389:153", keyServerHostName: "isr.api.threatgrid.com", feature: "Amp", apiKey:
"$CRYPT_CLUSTER$IbGLEMGIYMNRy1s9P+WcfA==$dozo7tmRP1+HrvEnXQr4x1VxSViYkKwQ4HBAIhXWotQ=", deviceID: "CSR-
07B6865F-7FE7-BA0D-7240-1BDA16328455"}) | +-----+
```

CiscoエッジルータでのAMPの統合

UTDコンテナの健全性の確認

show utdコマンドを使用して、UTDコンテナ全体の状態を確認します。

```
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
```

UTD AMPステータスの確認

ファイルインスペクションが有効になっていることを確認します。

<#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
```

AMPクラウドへの接続が確立されていることを確認します。

<#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!"
```

ThreatGridへの接続が確立されていることを確認します。

<#root>

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

Running

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

<#root>

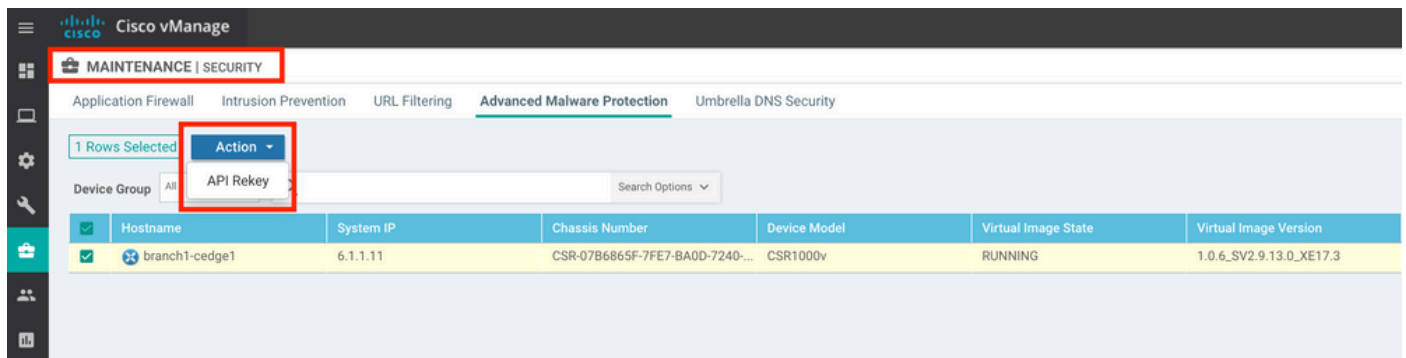
```
branch1-edge1#show sdwan utd file analysis
```

```
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"
```

ThreatGridプロセスでUpのステータスが表示されない場合は、APIキー再生成が役立ちます。APIキー再生成をトリガーするには、Maintenance -> Securityの順に移動します。



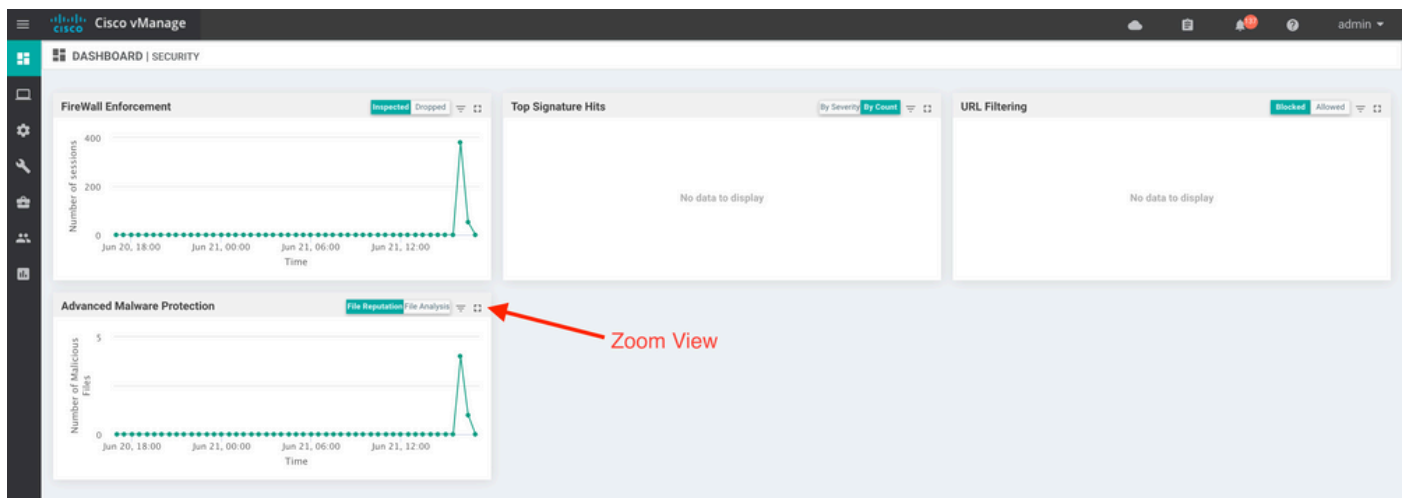
注：APIキー再生成によって、デバイスへのテンプレートプッシュがトリガーされます。

WANエッジルータでのAMPアクティビティのモニタリング

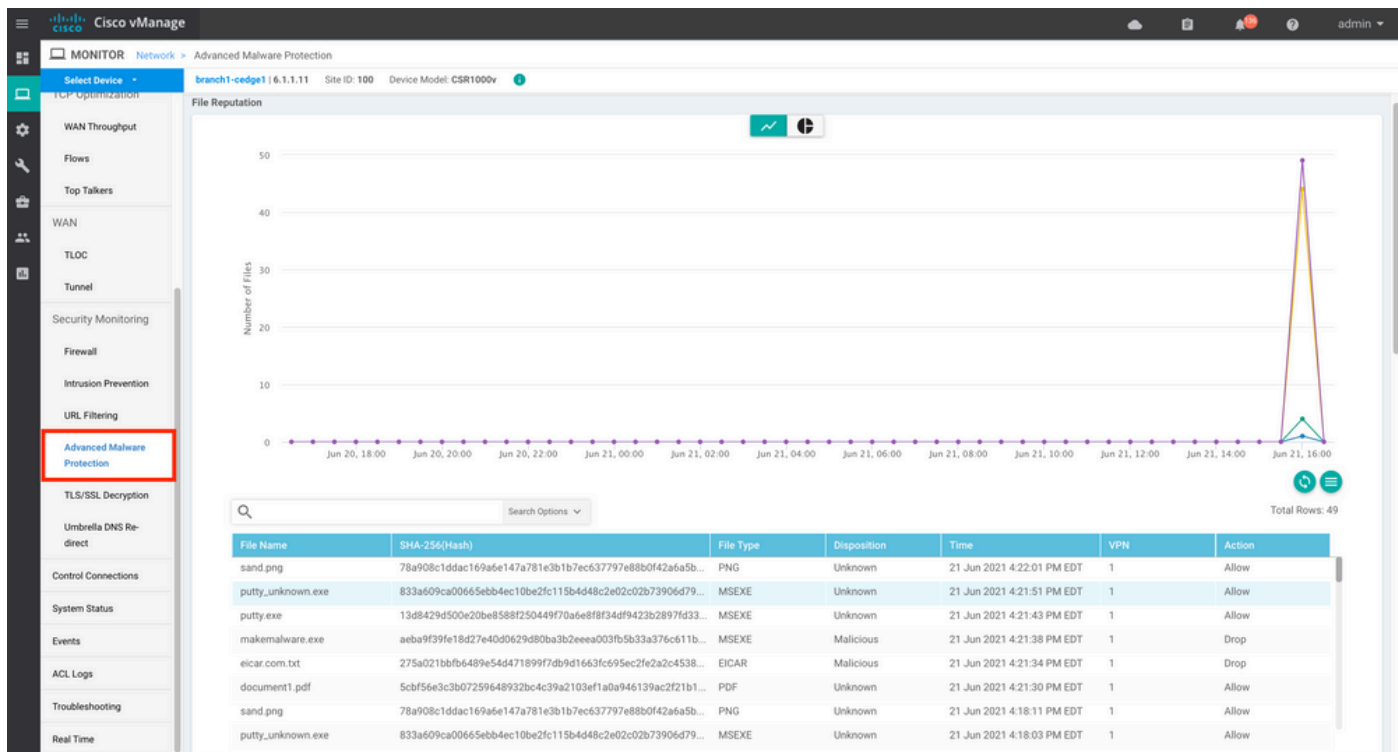
vManage

vManageでは、セキュリティダッシュボードまたはデバイスビューからAMPファイルアクティビティを監視できます。

セキュリティダッシュボード:



デバイスビュー:



CLI を使う場合：

ファイルレピュテーション統計情報を確認します。

```
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
```

ファイル分析の統計情報を確認します。

```
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：追加の内部統計情報は、show utd engine standard statistics file-reputation vrf global internalコマンドで取得できます。

データプレーンの動作

設定されたAMPポリシーに基づくファイルインスペクションの対象となるデータプレーントラフィックは、UTDコンテナに転送されて処理されます。これは、パケットトレースを使用して確認できます。トラフィックがコンテナに正しく転送されない場合、後続のファイルインスペクションアクションは発生しません。

AMPローカルファイルキャッシュ

UTDコンテナには、以前のAMPクラウドのルックアップ結果に基づいて、SHA256ハッシュ、ファイルタイプ、廃棄、アクションのローカルキャッシュがあります。ファイルハッシュがローカルキャッシュに存在しない場合、コンテナはAMPクラウドからの廃棄のみを要求します。ローカルキャッシュのTTLは、キャッシュが削除されるまでの2時間です。

```
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廃棄コード：

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

AMPアクションコード：

- 0 UNKNOWN
- 1 ALLOW
- 2 DROP

ファイルの完全なSHA256ハッシュを取得するには（これは、特定のファイル判定の問題をトラブルシューティングするために非常に重要です）、コマンドのdetailオプションを使用します。

```
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: AEBA9F39FE18D27E40D0629D80BA3B2EEEEA003FB5B33A376C611BB4D8FFD03A6
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>
```

UTDエンジンのローカルキャッシュエントリを検出するには、次のコマンドを使用します。

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

UTDデバッグの実行

AMPの問題をトラブルシューティングするには、utdデバッグを有効にします。


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

デバッグ出力は、/tmp/rp/trace/vman_utd_R0-0.binのシステムシェルから直接取得するか、次の手順を使用してトレースファイルをルータのファイルシステムにコピーできます。

```
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#
```

UTDトレースログを表示するには、次の手順を実行します。

```
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,Diff
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_unkn
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:20.6.1以降では、utdトレースログを取得して表示する方法は、show logging process vman module utd ...コマンドによる標準トレースワークフローに従っています。

エッジからクラウドへの通信の確認

エッジデバイスがAMP/TGクラウドと通信していることを確認するには、WANエッジルータのEPCを使用して、クラウドサービスとの間で双方向通信が行われていることを確認します。

```
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およびTGクラウド関連の問題

確認された時点で、エッジデバイスはファイルを正しくキャプチャし、分析のためにAMP/TGに送信しますが、判定が正しくないため、AMPのトラブルシューティングまたはThreatgridクラウドが必要です。これは、このドキュメントの範囲外です。統合に関する問題を提示する際には、次の情報が重要になります。

- ThreatGridアカウント組織
- タイムスタンプ
- デバイス分析ID(CSR-07B6865F-7FE7-BA0D-7240-1BDA16328455など)。これは、WANエッジルータのシャーシ番号です。
- 問題のファイルのSHA256ハッシュを完了します。

関連情報

- [SD-WANセキュリティ設定ガイド](#)
- [ThreatGridポータル](#)
- [テクニカル サポートとドキュメント - Cisco Systems](#)

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。