Konfiguration der Integration und Fehlerbehebung von SD-WAN Advanced Malware Protection (AMP)

Inhalt

[Einleitung](#)
[Voraussetzungen](#)
[Anforderungen](#)
[Verwendete Komponenten](#)
[Lösungsüberblick](#)
[Komponenten](#)
[Funktionsablauf](#)
[Konfiguration der SD-WAN AMP-Integration](#)
[Konfigurieren der Sicherheitsrichtlinie über vManage](#)
[Überprüfung](#)
[Fehlerbehebung](#)
[Allgemeiner Fehlerbehebungsablauf](#)
[Richtlinien-Push-Probleme bei vManage](#)
[AMP-Integration auf Cisco Edge Router](#)
[UTD-Containerzustand überprüfen](#)

Einleitung

In diesem Dokument wird die Konfiguration und Fehlerbehebung bei der Integration von Cisco SD-WAN Advanced Malware Protection (AMP) in einen Cisco IOS® XE SD-WAN-Router beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

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

Verwendete Komponenten

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Lösungsüberblick

Komponenten

Die SD-WAN-AMP-Integration ist ein integraler Bestandteil der SD-WAN-Edge-Sicherheitslösung, die auf Transparenz und Schutz von Benutzern in Zweigstellen vor Malware abzielt.

Es besteht aus den folgenden Produktkomponenten:

- **WAN-Edge-Router in einer Außenstelle** Dies ist ein Cisco IOS® XE-Router im Controller-Modus mit Sicherheitsfunktionen in einem UTD-Container
- **AMP-Cloud.** Die AMP-Cloud-Infrastruktur reagiert auf Datei-Hash-Abfragen mit einer Einstufung.
- **ThreatGrid**: Cloud-Infrastruktur, die eine Datei in einer Sandbox-Umgebung auf potenzielle Malware testen kann

Diese Komponenten arbeiten zusammen, um folgende wichtige Funktionen für AMP bereitzustellen:

- **Dateireputationsanalyse**

Der SHA256-Hash-Prozess, der verwendet wird, um die Datei mit dem Advanced Malware Protection (AMP)-Cloud-Server zu vergleichen und auf dessen Bedrohungsinformationen zuzugreifen. Die Reaktion kann "Sauber", "Unbekannt" oder "Schädlich" sein. Wenn die Antwort Unbekannt ist und die Dateianalyse konfiguriert ist, wird die Datei automatisch zur weiteren Analyse weitergeleitet.

- **Dateianalyse**

Eine unbekannte Datei wird zur Detonation in einer Sandbox-Umgebung an die ThreatGrid (TG)-Cloud gesendet. Während der Detonation erfasst die Sandbox Artefakte und beobachtet das Verhalten der Datei. Anschließend erhält die Datei eine Gesamtbewertung. Basierend auf den Beobachtungen und Ergebnissen kann Threat Grid die Bedrohungsreaktion in Sauber oder Bösartig ändern. Die Ergebnisse von ThreatGrid werden an die AMP-Cloud zurückgemeldet, damit alle AMP-Benutzer vor neu erkannter Malware geschützt sind.

- **Retrospektion**

Es speichert Informationen über Dateien auch nach dem Download, können wir Berichte über Dateien, die als schädlich festgestellt wurden, nachdem sie heruntergeladen wurden. Der Status der Dateien kann sich aufgrund der neuen Bedrohungsinformationen ändern, die von der AMP-Cloud gewonnen wurden. Diese Neuklassifizierung generiert automatische retrospektive Benachrichtigungen.

Derzeit unterstützt SD-WAN mit AMP-Integration die Dateiprüfung für die folgenden Protokolle:

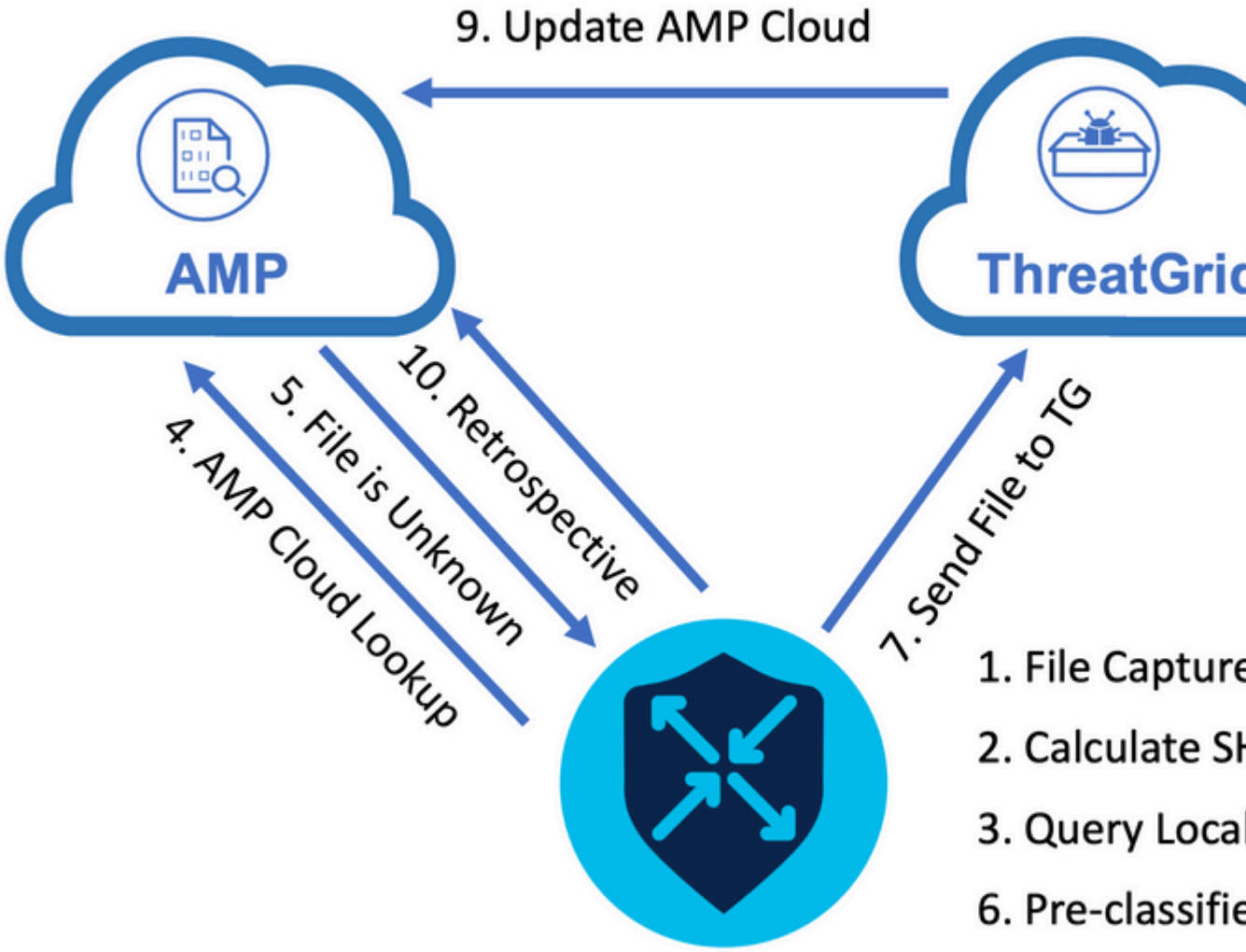
- HTTP
- SMTP
- IMAP
- POP3
- FTP
- KMU

Hinweis: Dateiübertragung über HTTPS wird nur mit SSL/TLS Proxy unterstützt.

Hinweis: Die Dateianalyse kann nur für eine vollständige Datei durchgeführt werden, und nicht für eine Datei, die in einen Teil des Inhalts aufgeteilt ist. Beispielsweise, wenn ein HTTP-Client partiellen Inhalt mit dem Range-Header anfordert und ***HTTP/1.1 206 partiellen Inhalt*** zurückruft**.** In diesem Fall überspringt Snort die Dateiprüfung für den partiellen Inhalt, da sich der partielle Dateihash erheblich von der vollständigen Datei unterscheidet.

Funktionsablauf

Die Abbildung zeigt den allgemeinen Fluss für die SD-WAN-AMP-Integration, wenn eine Datei zur Analyse an ThreatGrid gesendet werden muss.



Für den angezeigten Durchfluss:

1. Die Dateiübertragung für AMP-unterstützte Protokolle wird vom UTD-Container erfasst.
2. Der SHA256-Hash für die Datei wird berechnet.
3. Der berechnete SHA256-Hash wird für das lokale Cachesystem in UTD abgefragt, um festzustellen, ob die Einstufung bereits bekannt ist und die Cache-TTL nicht abgelaufen ist.
4. Wenn keine Übereinstimmung mit dem lokalen Cache besteht, wird der SHA256-Hash in der AMP-Cloud nach einer Einstufung und einer Rückgabeaktion durchsucht.
5. Wenn die Einstufung UNBEKANNT ist und die Antwortaktion ACTION_SEND lautet, wird die Datei über das Vorklassifizierungssystem in UTD ausgeführt.
6. Die Vorklassifizierung legt den Dateityp fest und überprüft auch, ob die Datei aktiven Inhalt enthält.
7. Wenn beide Bedingungen erfüllt sind, wird die Datei an ThreatGrid gesendet.
8. ThreatGrid zündet die Datei in einer Sandbox und weist ihr eine Bedrohungsbewertung zu.
9. ThreatGrid aktualisiert die AMP-Cloud basierend auf der Bedrohungsanalyse.
10. Das Edge-Gerät fragt die AMP-Cloud nach Retrospektive ab, basierend auf dem Heartbeat-Intervall von 30 Minuten.

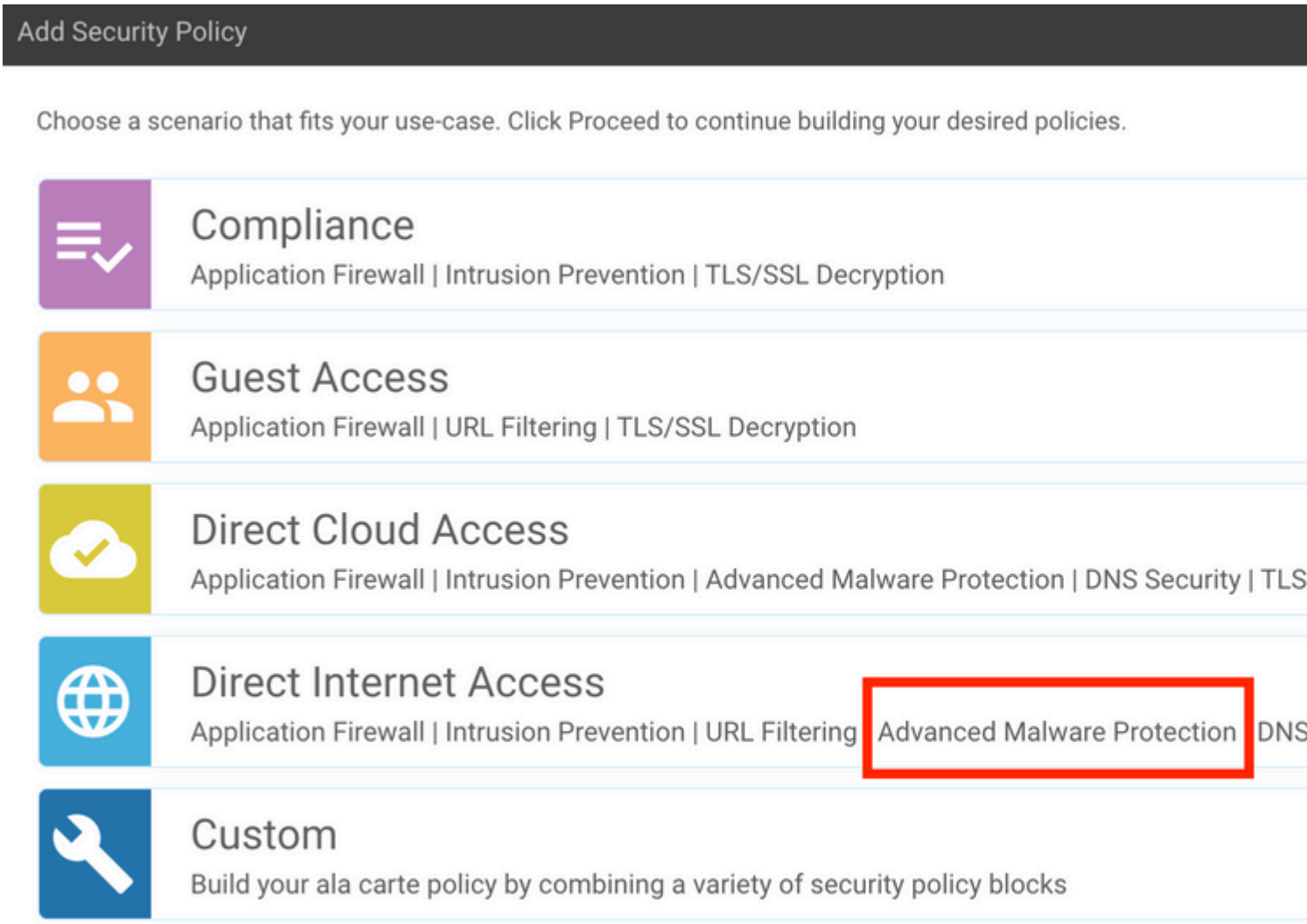
Konfiguration der SD-WAN AMP-Integration

Hinweis: Vor der Konfiguration der AMP-Funktionen muss ein virtuelles Sicherheits-Image in vManage hochgeladen werden. Weitere Informationen finden Sie unter Virtuelles Sicherheitsabbild .

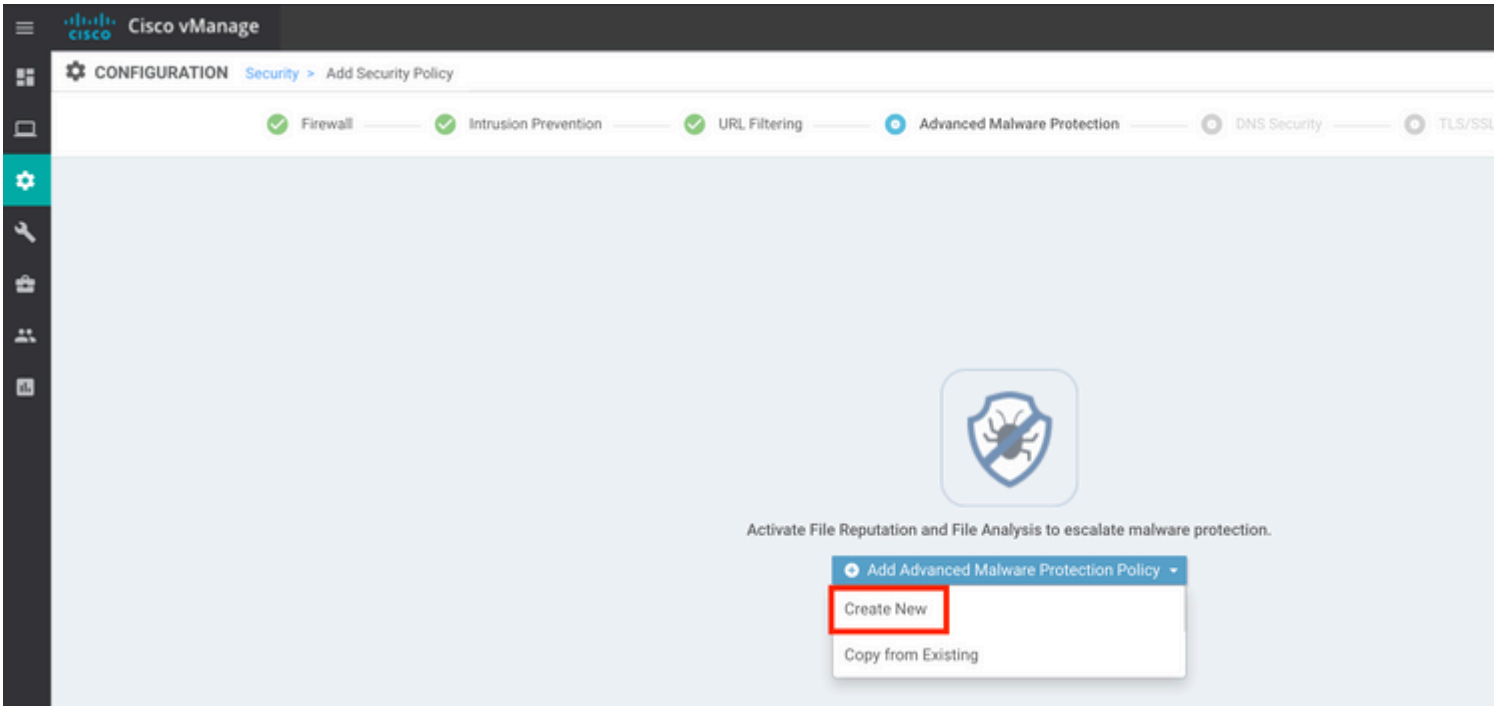
Hinweis: Lesen Sie dieses Dokument, um die Netzwerkanforderungen für die ordnungsgemäße Funktion der AMP/ThreatGrid-Verbindung zu überprüfen: Erforderliche IP-Adressen/Hostnamen für AMP/TG

Konfigurieren der Sicherheitsrichtlinie über vManage

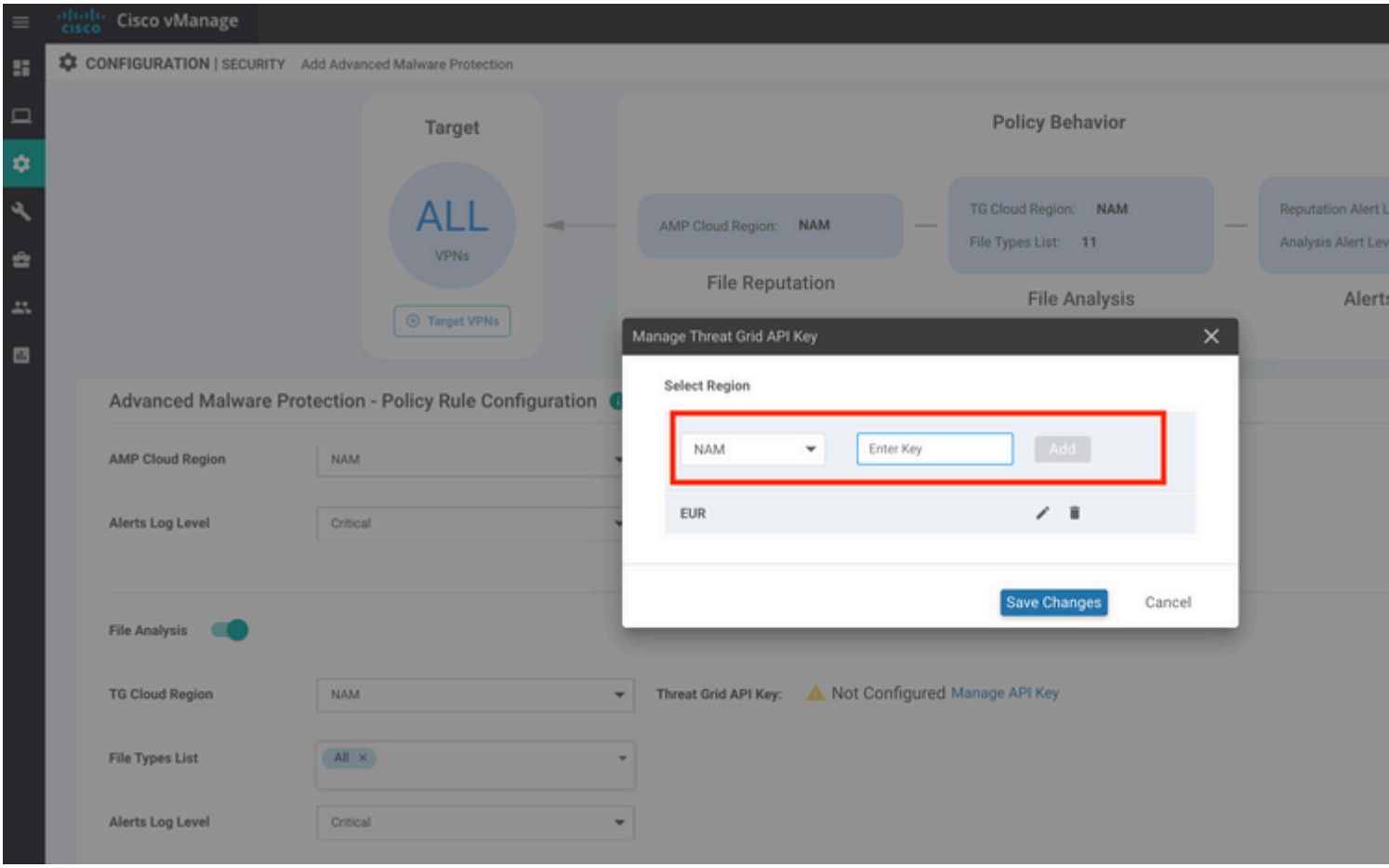
Um AMP zu aktivieren, navigieren Sie zu **Konfiguration** -> **Sicherheit** -> **Sicherheitsrichtlinie hinzufügen**. Wählen Sie Direct Internet Access und dann **Proceed (Weiter**) aus, wie im Bild dargestellt.



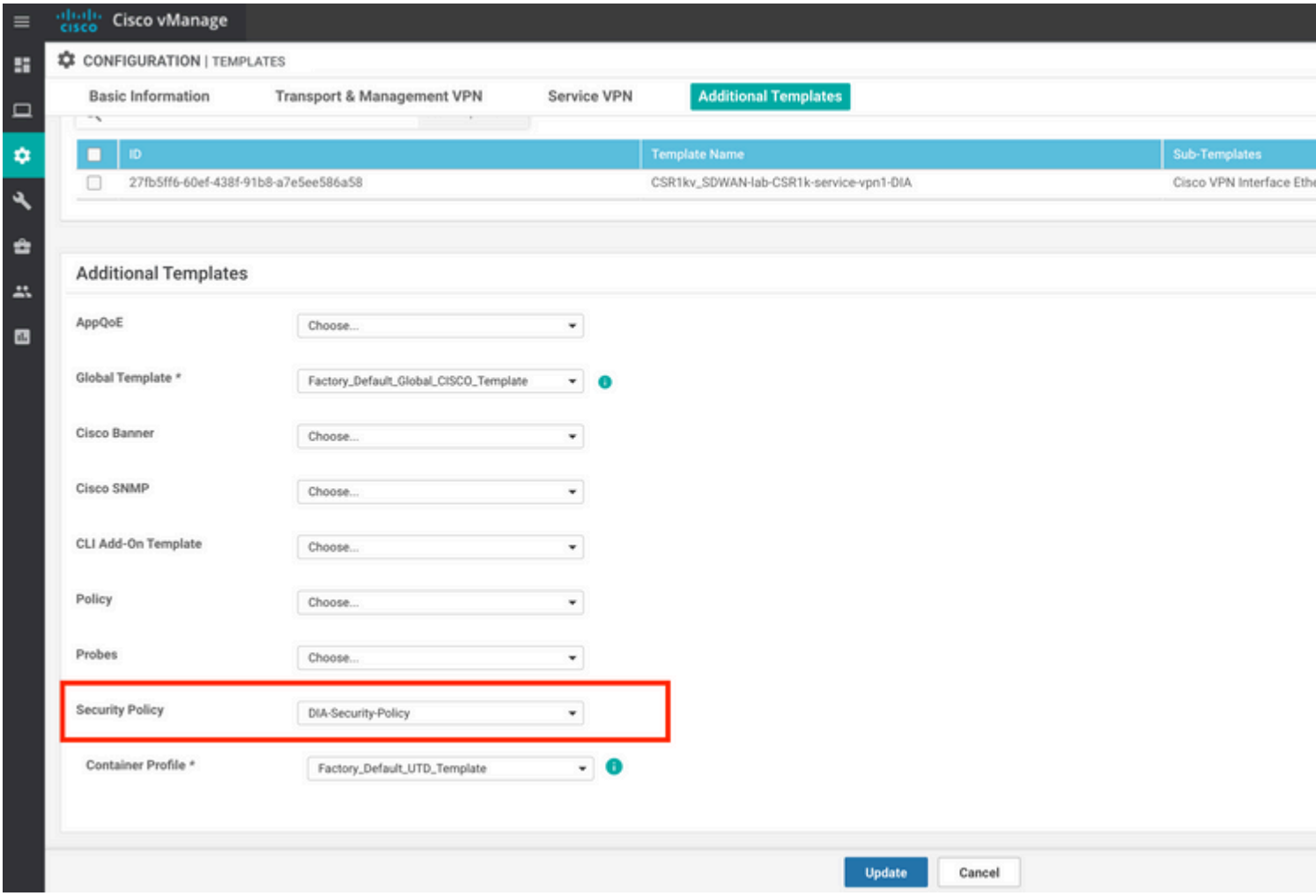
Konfigurieren Sie die Sicherheitsfunktionen wie gewünscht, bis die Advanced Malware Protection-Funktion aktiviert ist. Fügen Sie eine neue Advanced Malware Protection Policy hinzu.



Geben Sie einen Richtliniennamen an. Wählen Sie eine der globalen AMP-Cloud-Regionen aus, und aktivieren Sie die Dateianalyse. Wählen Sie für die Dateianalyse mit ThreatGrid eine der TG-Cloud-Regionen aus, und geben Sie den API-Schlüssel für ThreatGrid ein, den Sie im ThreatGrid-Portal unter **Mein ThreatGrid-Konto** abrufen können**.**



Speichern Sie anschließend die Richtlinie, und fügen Sie diese der Vorlage Gerät unter **Zusätzliche Vorlagen** -> **Sicherheitsrichtlinie** hinzu, wie im Bild dargestellt.



Konfigurieren Sie das Gerät mit der aktualisierten Gerätevorlage.

Überprüfung

Sobald die Gerätevorlage erfolgreich an das Edge-Gerät übertragen wurde, kann die AMP-Konfiguration über die CLI des Edge-Routers überprüft werden:

<#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
```

Fehlerbehebung

Die SD-WAN-AMP-Integration umfasst viele Komponenten, wie beschrieben. Bei der Fehlerbehebung ist es daher von entscheidender Bedeutung, einige zentrale Übergangspunkte festzulegen, um das Problem auf die Komponenten im Funktionsablauf einzugrenzen:

1. **vManage.** Kann vManage die Sicherheitsrichtlinie mit der AMP-Richtlinie erfolgreich auf das Edge-Gerät übertragen?
2. **Edge**. Wenn die Sicherheitsrichtlinie erfolgreich an den Edge übertragen wurde, erfasst der Router die Datei, die Gegenstand einer AMP-Inspektion ist, und sendet sie an die AMP-/TG-Cloud?
3. **AMP/TG Cloud.** Erhält der Edge, der die Datei an AMP oder TG gesendet hat, die erforderliche Antwort, um eine Entscheidung zum Zulassen oder Ablehnen zu treffen?

Dieser Artikel konzentriert sich auf das Edge-Gerät (2) mit den verschiedenen verfügbaren Datenebenen-Tools, um bei der Fehlerbehebung von Problemen mit der AMP-Integration am WAN-Edge-Router zu helfen.

Allgemeiner Fehlerbehebungsablauf

Nutzen Sie diesen allgemeinen Workflow, um die verschiedenen Komponenten der AMP-Integration schnell zu beheben. Dabei besteht ein Hauptziel darin, den Berührungspunkt zwischen dem Edge-Gerät und der AMP/TG-Cloud festzulegen.

1. Wird die AMP-Richtlinie korrekt auf das Edge-Gerät angewendet?
2. Überprüfen Sie den allgemeinen Zustand des UTD-Containers.
3. Überprüfen Sie die Dateireputation, und analysieren Sie den Client-Status am Edge.
4. Überprüfen Sie, ob die Dateiübertragung zum Container umgeleitet wird. Dies ist über die Cisco IOS® XE Packet Trace möglich.
5. Aktivieren Sie diese Option, um zu bestätigen, dass das Edge erfolgreich mit der AMP-/TG-Cloud kommuniziert. Dies kann mit Tools wie EPC oder Packet-Trace erfolgen.
6. Stellen Sie sicher, dass UTD auf Basis der AMP-Antwort einen lokalen Cache erstellt.

Diese Schritte zur Fehlerbehebung werden in diesem Dokument ausführlich behandelt.

Richtlinien-Push-Probleme bei vManage

Wie die AMP-Richtlinienkonfiguration zeigt, ist die AMP-Richtlinie relativ einfach, ohne dass viele Konfigurationsoptionen erforderlich sind. Hier einige gängige Punkte, die Sie beachten sollten:

1. vManage muss in der Lage sein, die DNS-Namen für AMP und ThreatGrid Cloud für den API-Zugriff aufzulösen. Wenn die Gerätekonfiguration auf vManage nach dem Hinzufügen der AMP-Richtlinie fehlschlägt, überprüfen Sie die **/var/log/nms/vmanage-server.log** auf Fehler.
2. Wie im Konfigurationsleitfaden angegeben, hat die Warnmeldungsprotokollebene die kritische

Standardstufe bzw. ggf. die Warnstufe beibehalten. Protokollierung auf Informationsebene muss vermieden werden, da dies negative Auswirkungen auf die Leistung haben kann.

Zur Verifizierung greifen Sie auf die neo4j DB zu und sehen den Inhalt der vmanagedbAPIKEYNODE Tabelle.

```
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"}) | +----------
----------
-----+
```

AMP-Integration auf Cisco Edge Router

UTD-Containerzustand überprüfen

Verwenden Sie die Befehle show utd, um die allgemeine Integrität des UTD-Containers zu überprüfen:

```
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-Status überprüfen

Stellen Sie sicher, dass die Dateiprüfung aktiviert ist:

<#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
```

Überprüfen Sie, ob die Verbindung zur AMP-Cloud aktiv ist:

<#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!"
```

Überprüfen Sie, ob eine Verbindung mit ThreatGrid besteht:

<#root>

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

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

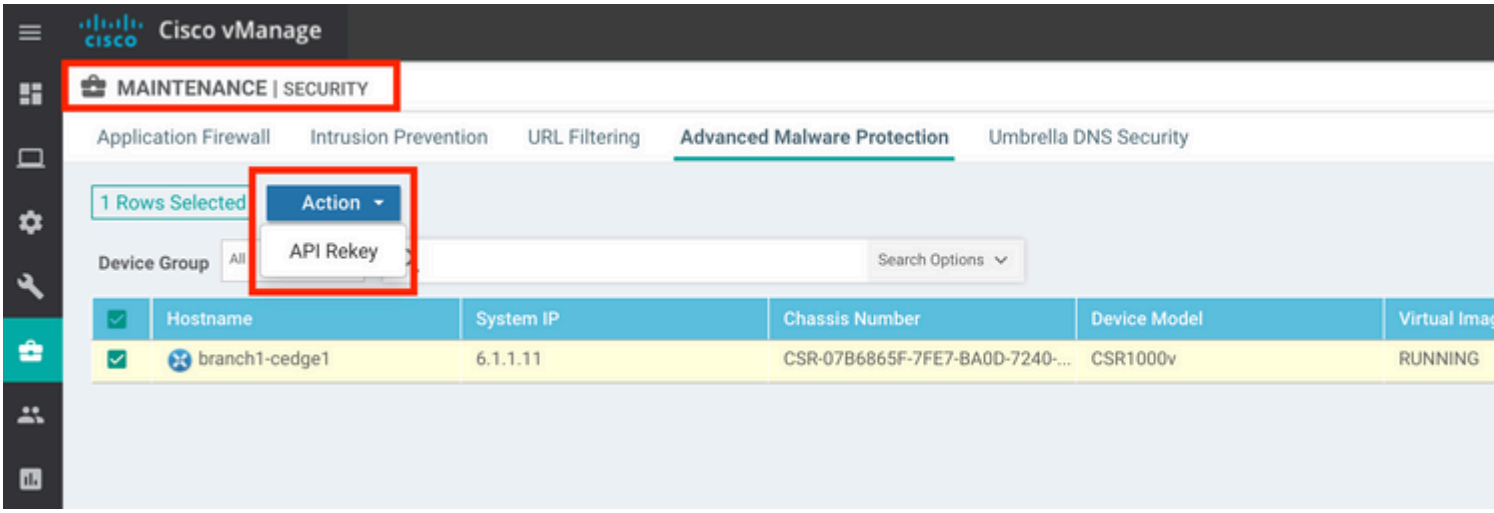
<#root>

```
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"
```

Wenn der ThreatGrid-Prozess nicht den Status Up (Hoch) anzeigt, ist ein API-Schlüssel hilfreich. Um einen API-Schlüssel auszulösen, navigieren Sie zu **Maintenance** -> **Security**:



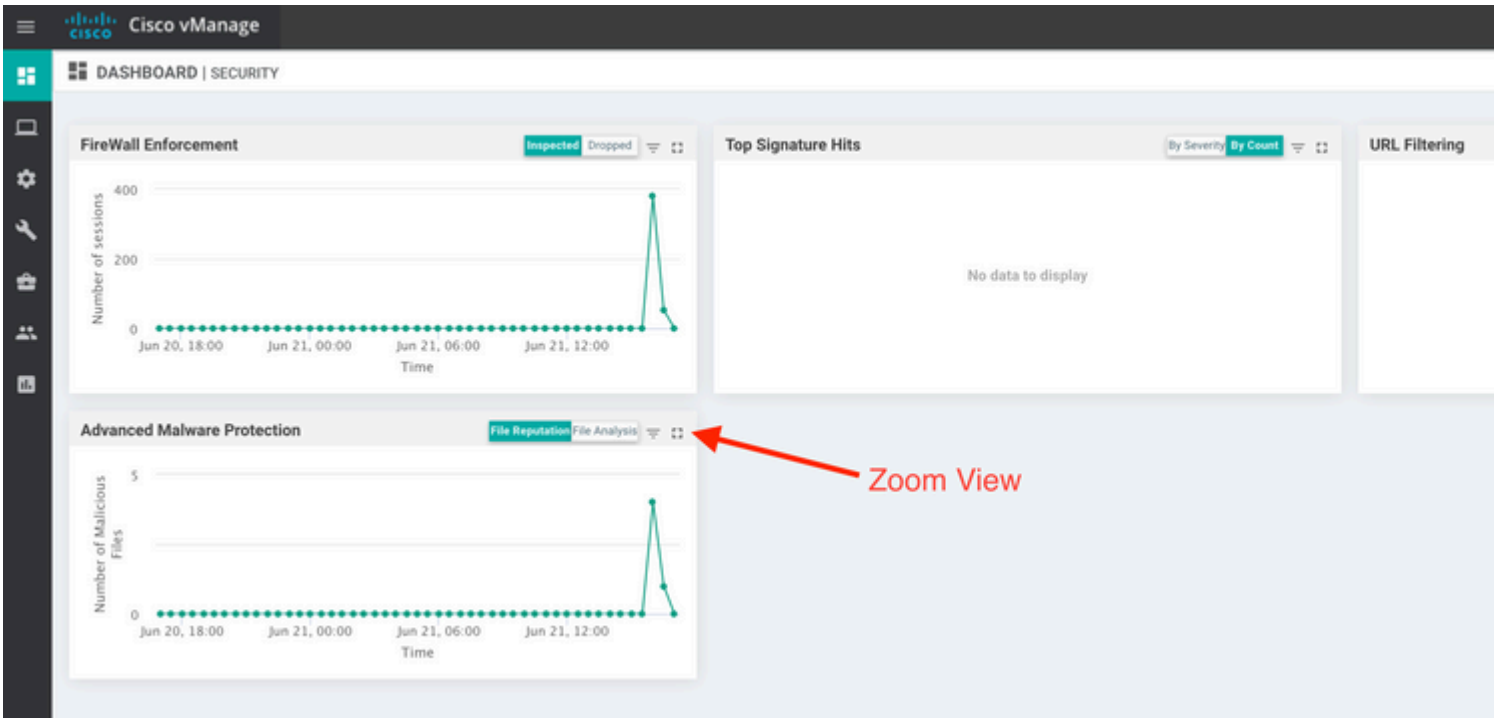
Hinweis: Ein API-Schlüssel löst einen Vorlagen-Push für das Gerät aus.

AMP-Aktivitätsüberwachung auf WAN-Edge-Router

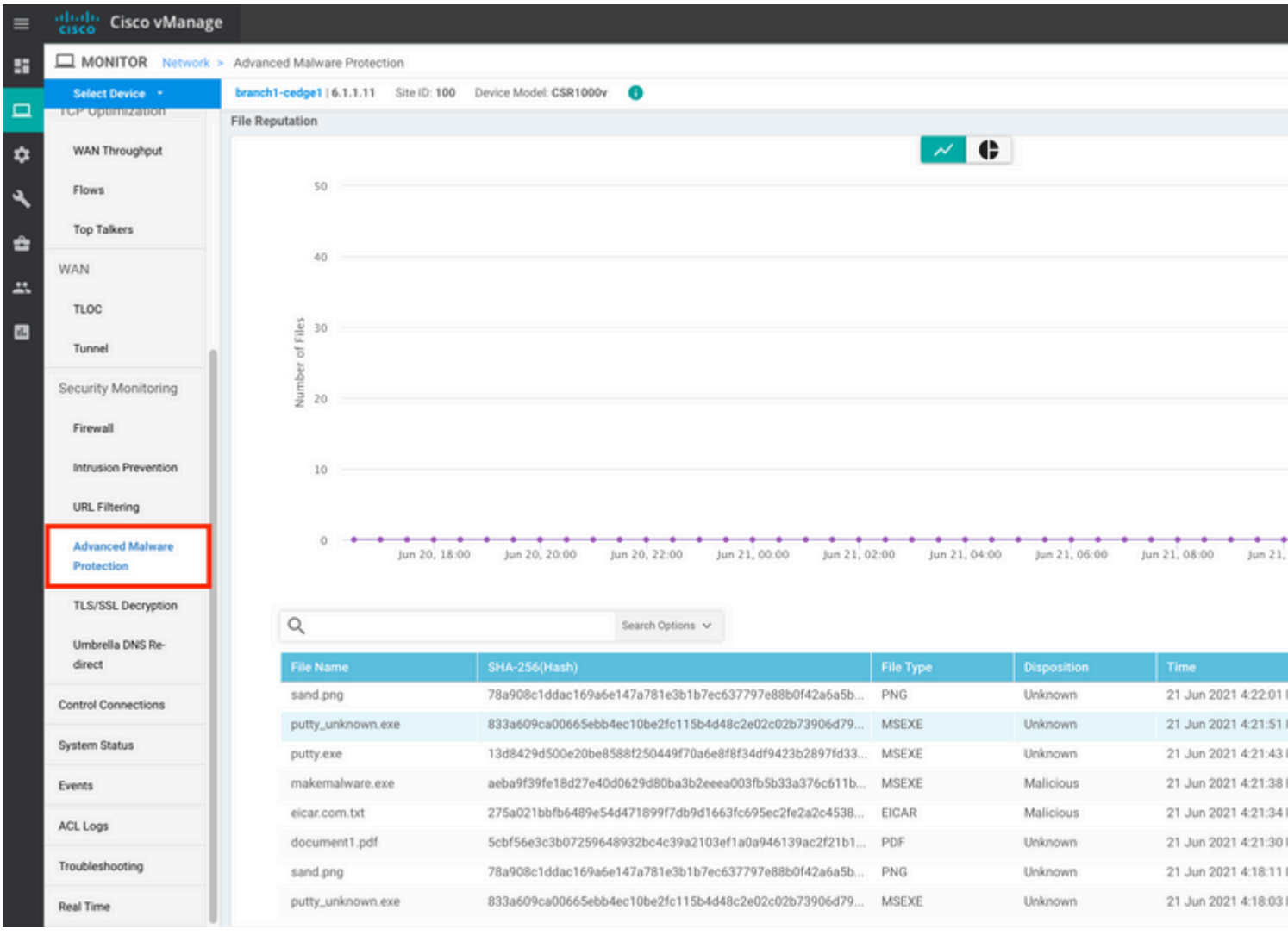
vManage

In vManage können die AMP-Dateiaktivitäten entweder über das Security Dashboard oder in der Geräteansicht überwacht werden.

Sicherheits-Dashboard



Geräteansicht:



CLI

Dateireputationsstatistiken überprüfen:

```
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
```

Statistiken zur Dateianalyse überprüfen:

```
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
```

Hinweis: Mit dem Befehl ***show utd engine standard statistics file-reputation vrf global internal*** können zusätzliche interne Statistiken abgerufen werden.

Verhalten des Datenblatts

Datenflugverkehr, der auf der Grundlage der konfigurierten AMP-Richtlinie einer Dateiüberprüfung unterzogen wird, wird zur Verarbeitung an den UTD-Container umgeleitet. Dies kann mit einer Paketverfolgung bestätigt werden. Wenn der Datenverkehr nicht ordnungsgemäß zum Container umgeleitet wird, kann keine der nachfolgenden Dateiüberprüfungsaktionen ausgeführt werden.

Cache für lokale AMP-Dateien

Der UTD-Container verfügt auf der Grundlage früherer AMP-Cloud-Suchergebnisse über einen lokalen Cache mit SHA256-Hash, Dateityp, Einstufung und Aktion. Der Container fordert nur dann eine Disposition von der AMP-Cloud an, wenn sich der Datei-Hash nicht im lokalen Cache befindet. Der lokale Cache verfügt über eine TTL von 2 Stunden, bevor der Cache gelöscht wird.

```
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-Dispositionscode:

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

AMP-Aktionscode:

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

Um den vollständigen SHA256-Hash für die Dateien zu erhalten, was sehr wichtig ist, um Probleme mit einem bestimmten Dateiurteil zu beheben, verwenden Sie die Detailoption des Befehls:

```
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>
```

Verwenden Sie den folgenden Befehl, um die lokalen Cache-Einträge des UTD-Moduls zu löschen:

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

Ausführen von UTD-Debuggen

Die utd-Fehlerbehebungen können zur Behebung von AMP-Problemen aktiviert werden:

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

Die Debug-Ausgabe kann direkt aus der System-Shell unter **/tmp/rp/trace/vman_utd_R0-0.bin** abgerufen werden, oder Sie kopieren die Trace-Datei in das Router-Dateisystem, indem Sie die folgenden Schritte ausführen:

```
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#
```

So zeigen Sie das UTD-Protokoll an:

```
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_unkno
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>
```

Hinweis: In 20.6.1 und höher ist der Weg zum Abrufen und Anzeigen der utd tracelogs im Einklang mit dem Standard-Trace-Workflow mit dem **show logging-Prozess vman module utd** ... aus.

Überprüfen der Kommunikation vom Edge zur Cloud

Um zu überprüfen, ob das Edge-Gerät mit der AMP/TG-Cloud kommuniziert, kann mithilfe des EPC auf dem WAN-Edge-Router bestätigt werden, dass eine bidirektionale Kommunikation zu/von den Cloud-Services besteht:

```
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 und TG Cloud-bezogene Probleme

Sobald bestätigt wurde, dass das Edge-Gerät die Datei korrekt erfasst und zur Analyse an AMP/TG sendet. Das Urteil ist jedoch falsch. Daher ist eine Fehlerbehebung für AMP oder eine Threatgrid-Cloud erforderlich, auf die in diesem Dokument nicht näher eingegangen wird. Die Informationen sind bei der Darstellung von Integrationsfragen wichtig:

- Organisation des ThreatGrid-Kontos
- Zeitstempel
- Geräteanalyse-ID (z. B. CSR-07B6865F-7FE7-BA0D-7240-1BDA16328455): Dies ist die Chassis-Nummer für den WAN-Edge-Router.
- Vollständiger SHA256-Hash für die betreffende Datei

Zugehörige Informationen

- SD-WAN-Sicherheitskonfigurationshandbuch
- ThreatGrid-Portal
- Technischer Support und Dokumentation für Cisco Systeme

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.