SD-WAN Advanced Malware Protection (AMP) configureren voor integratie en probleemoplossing

Inhoud

Inleiding

Dit document beschrijft hoe u de integratie van Cisco SD-WAN Advanced Malware Protection (AMP) op een Cisco IOS® XE SD-WAN router kunt configureren en oplossen.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

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

Gebruikte componenten

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Overzicht van oplossing

Componenten

De SD-WAN AMP integratie is een integraal onderdeel van de SD-WAN edge security oplossing die zichtbaarheid en bescherming voor gebruikers bij een tak van Malware.

Het bestaat uit deze productcomponenten:

- **WAN Edge-router in een aftakking.** Dit is een Cisco IOS® XE router in controllermodus met beveiligingsfuncties in een UTD-container
- **AMP Cloud.** De AMP cloud infrastructuur reageert op bestandshash vragen met een dispositie
- **ThreatGrid**. De cloud-infrastructuur die een bestand kan testen op mogelijke malware in een sandbox-omgeving

Deze componenten werken samen om deze belangrijke functiemogelijkheden voor AMP te leveren:

- **Beoordeling van de bestandsnaam**

Het proces van SHA256 hash wordt gebruikt om het bestand te vergelijken met de Advanced Malware Protection (AMP)-cloudserver en toegang te krijgen tot de bedreigingsinformatie. Het antwoord kan Schoon, Onbekend, of Kwaadaardig zijn. Als het antwoord Onbekend is en als File Analysis is geconfigureerd, wordt het bestand automatisch voor verdere analyse ingediend.

- **Bestandsanalyse**

Een onbekend bestand wordt naar de ThreatGrid (TG) cloud gestuurd voor detonatie in een zandbak omgeving. Tijdens de detonatie, de zandbak vangt artefacten en observeert gedrag van het dossier, dan geeft het dossier een algemene score. Gebaseerd op de waarnemingen en de score, kan Threat Grid de bedreigingsreactie op Schoon of Kwaadaardig veranderen. De bevindingen van ThreatGrid worden doorgegeven aan de AMP-cloud, zodat alle AMP-gebruikers worden beschermd tegen nieuw ontdekte malware.

- **retrospectie**

Het houdt informatie over bestanden, zelfs nadat ze zijn gedownload, kunnen we rapporteren over bestanden die zijn vastgesteld als kwaadaardig nadat ze zijn gedownload. De aard van de bestanden kan veranderen op basis van de nieuwe bedreigingsinformatie die is verkregen door de AMP cloud. Deze herindeling genereert automatische kennisgevingen achteraf.

Op dit moment ondersteunt SD-WAN met AMP integratie bestandsinspectie voor de protocollen:

- HTTP
- SMTP
- IMAP
- POP3
- FTP
- SMB

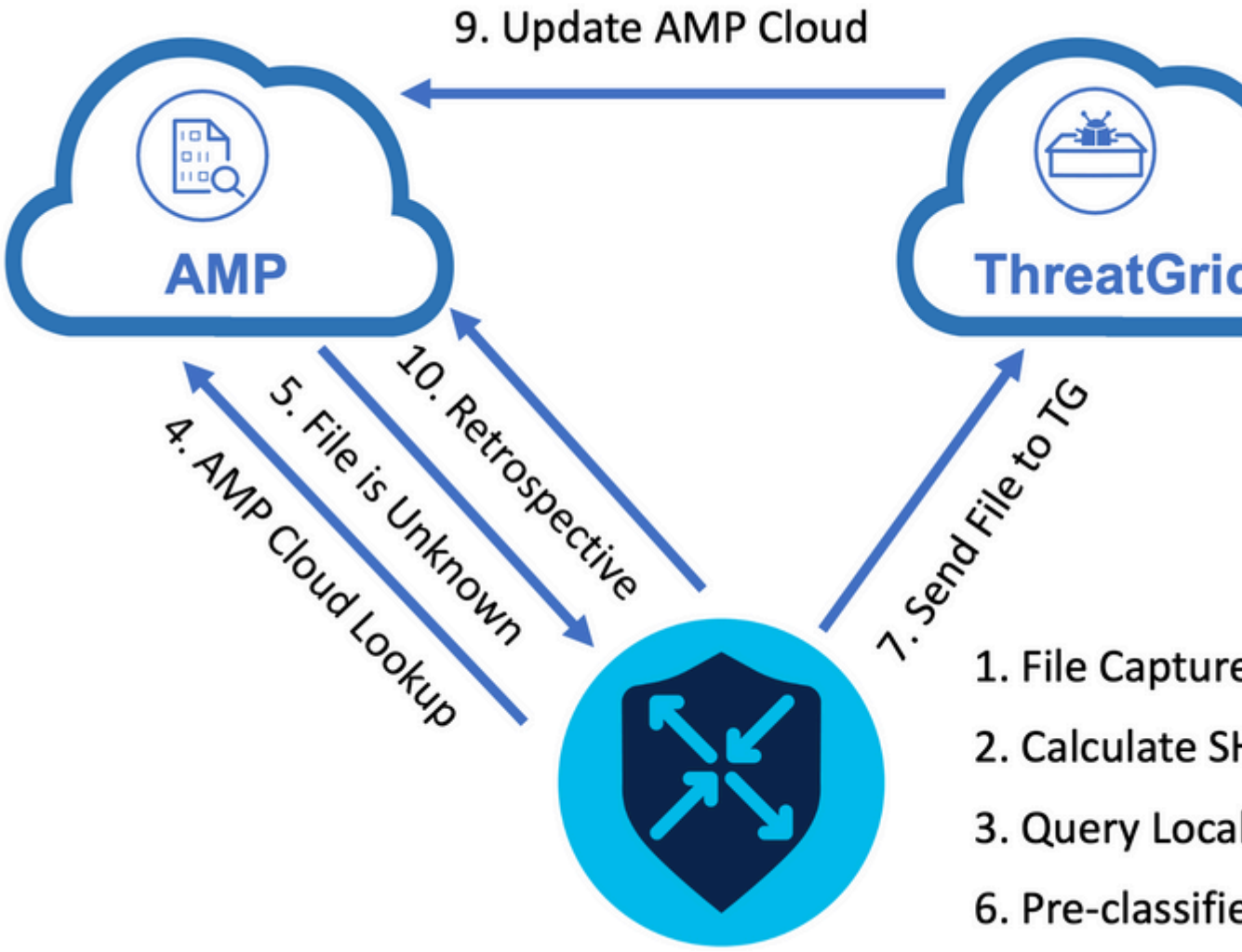
Opmerking: Bestandsoverdracht via HTTPS wordt alleen ondersteund door SSL/TLS-proxy.

Opmerking: Bestandsanalyse kan alleen worden uitgevoerd op een volledig bestand en niet op een bestand dat is opgesplitst in gedeeltelijke inhoud. Bijvoorbeeld, wanneer een HTTP-client om gedeeltelijke inhoud met de Range header verzoekt en ***HTTP/1.1 206 Partiële inhoud*** terugkrijgt**.** In dit geval, omdat de gedeeltelijke hash van het bestand aanzienlijk verschilt van het volledige bestand, slaat Snort de bestandsinspectie voor de gedeeltelijke inhoud over.

Functiedoorloop

Het beeld toont de stroom op hoog niveau voor SD-WAN AMP integratie wanneer een bestand moet

worden ingediend bij ThreatGrid voor analyse.



Voor de aangegeven stroom:

1. De bestandsoverdracht voor door AMP ondersteunde protocollen wordt opgenomen in de UTD-container.
2. De SHA256 hash voor het bestand wordt berekend.
3. De berekende SHA256 hash wordt gevraagd tegen het lokale cache systeem in UTD om te zien of de verwerking al bekend is en de cache TTL niet is verlopen.
4. Als er geen match is met de lokale cache, dan wordt de SHA256 hash opgezocht tegen de AMP cloud voor een regeling en actie terug.
5. Als de dispositie ONBEKEND is en de reactie actie ACTION_SEND is, loopt het bestand door het pre-classificatiesysteem in UTD.
6. De voorclassificator bepaalt het bestandstype en valideert ook als het bestand actieve inhoud bevat.
7. Als beide voorwaarden worden vervuld, wordt het bestand ingediend bij ThreatGrid.
8. ThreatGrid laat het bestand in een zandbak ontploffen en kent het bestand een bedreigingsscore toe.
9. ThreatGrid werkt de AMP-cloud bij op basis van dreigingsevaluatie.
10. Het randapparaat vraagt de AMP wolk voor Retrospective gebaseerd op het hartslaginterval van 30 minuten.

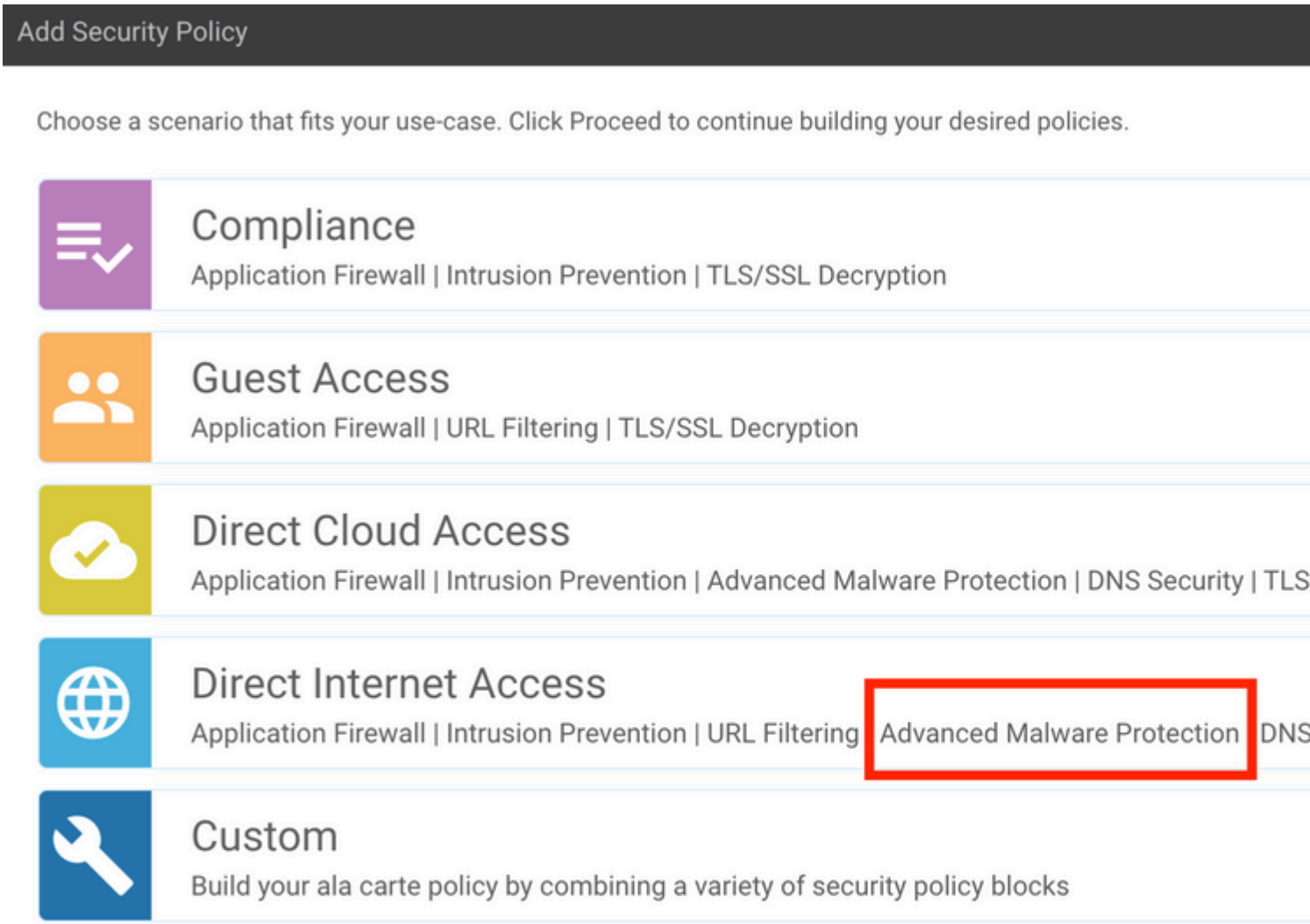
Configuratie van SD-WAN AMP

Opmerking: een beveiligings virtuele afbeelding moet naar vManager worden geüpload voordat de AMP-functieconfiguratie wordt uitgevoerd. Navigeer voor meer informatie naar Security Virtual Image.

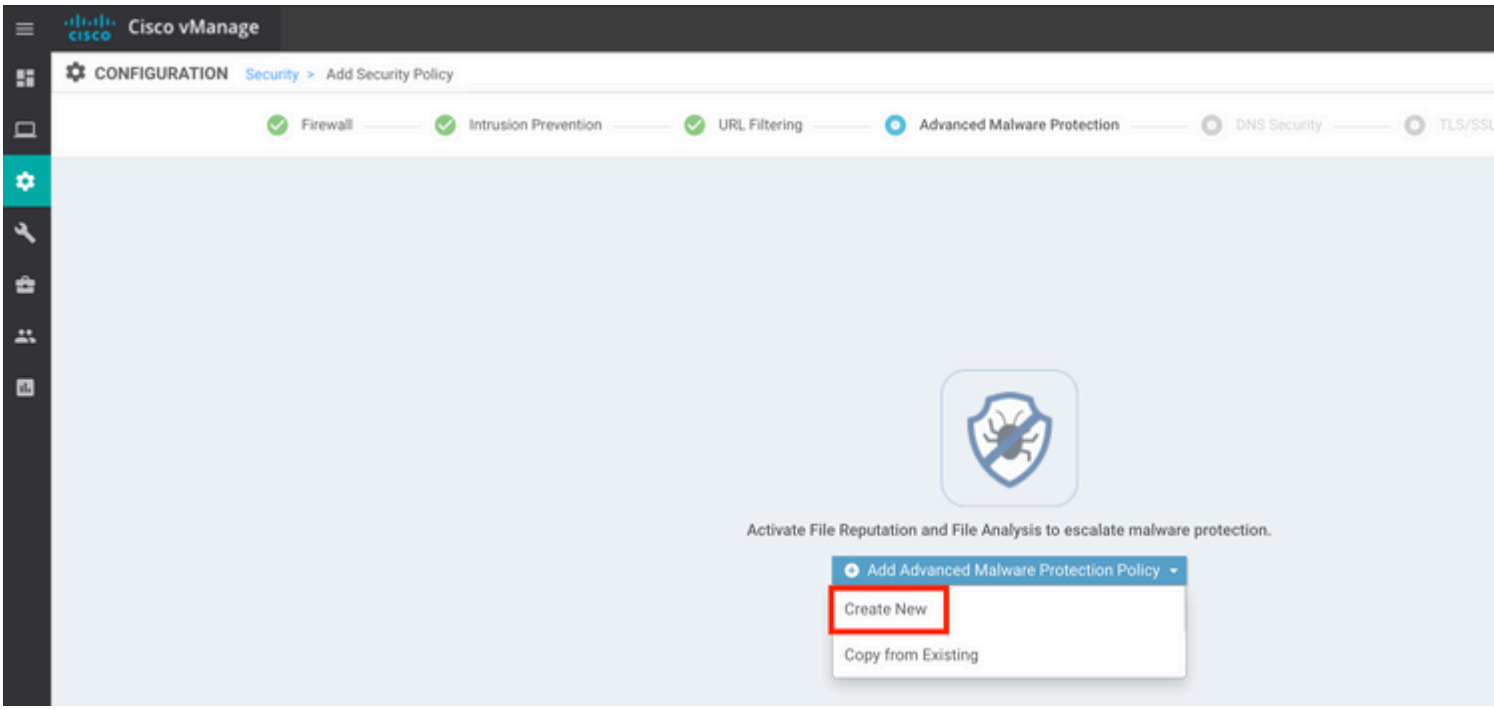
Opmerking: controleer dit document om te zien of de netwerkvereisten voor de AMP/ThreatGrid-connectiviteit correct werken: AMP/TG Vereiste IP-adressen/hostnamen

Beveiligingsbeleid vanuit vManager configureren

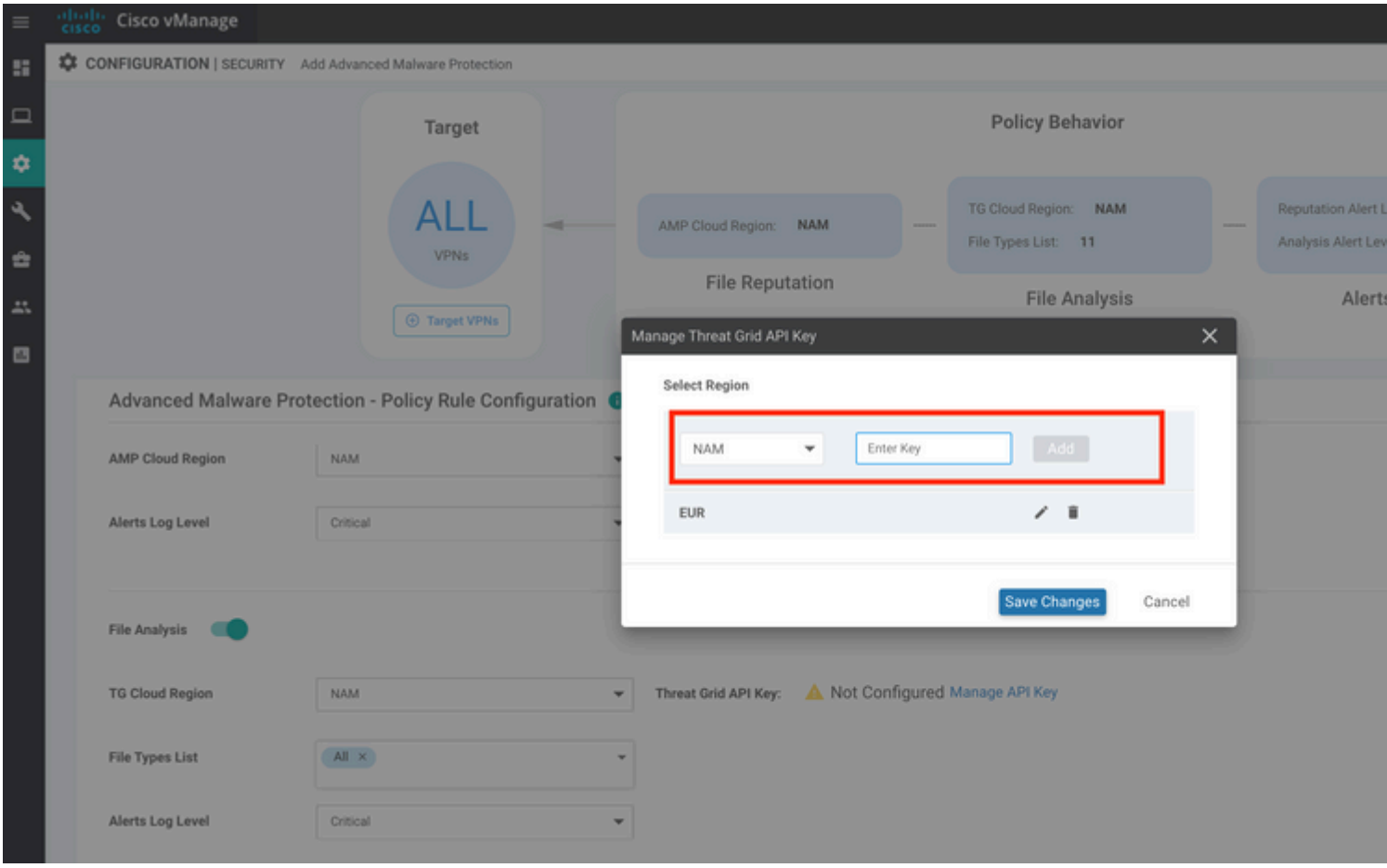
Als u Advanced Malware Protection (AMP) wilt inschakelen, navigeert u naar **Configuration** -> **Security** -> **Add Security Policy**. Selecteer Direct Internet Access en selecteer **doorgaan** zoals in het afbeelding.



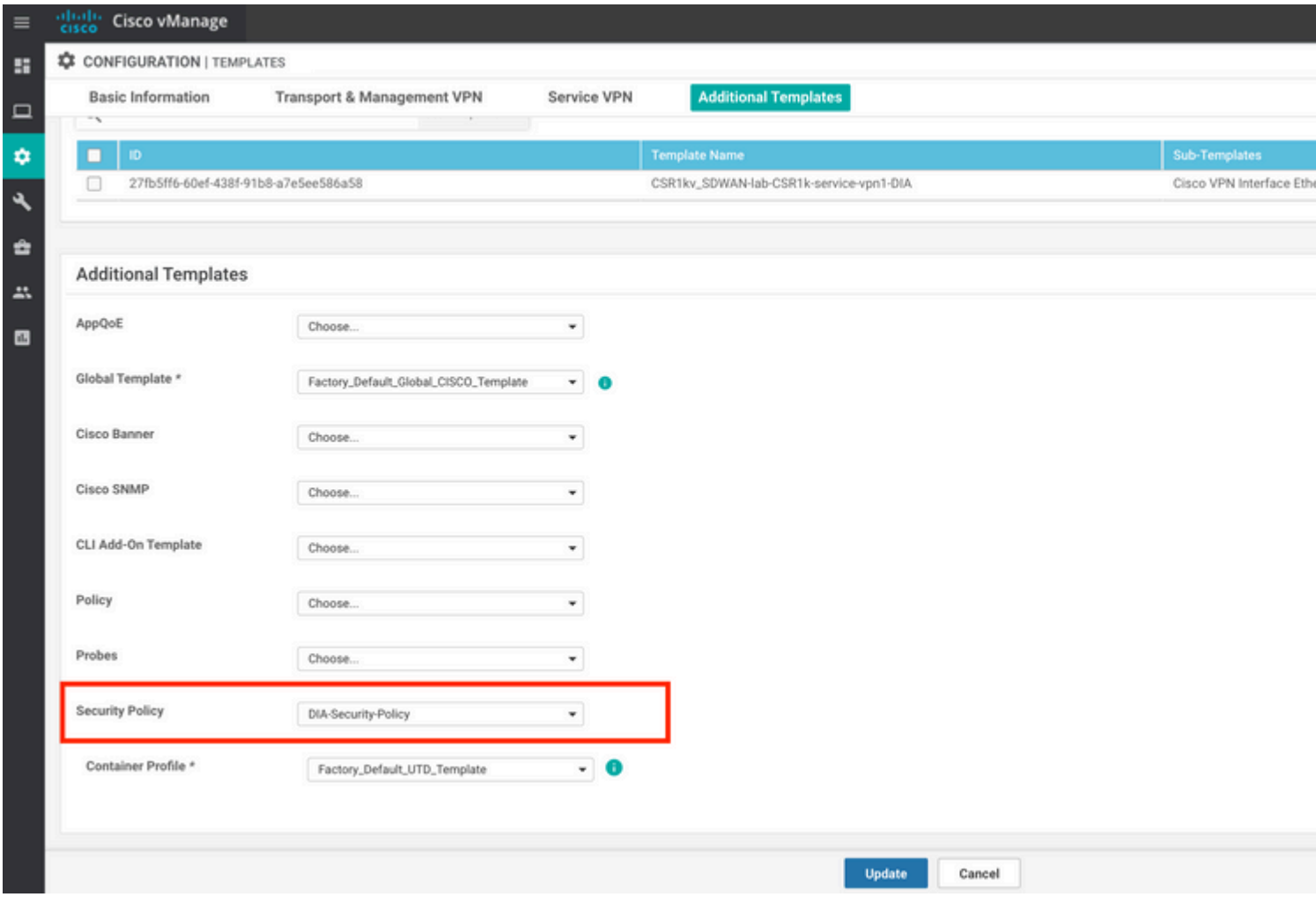
Configureer de beveiligingsfuncties naar wens tot de Advanced Malware Protection functie wordt ingeschakeld. Voeg een nieuw Advanced Malware Protection Policy toe.



Geef een naam op voor het beleid. Selecteer een van de wereldwijde AMP-cloudgebieden en laat File Analysis toe. Voor Bestandsanalyse waarbij ThreatGrid wordt gebruikt, kiest u een van de TG-cloudgebieden en voert u de ThreatGrid API-toets in die kan worden verkregen bij het ThreatGrid-portal onder **Mijn ThreatGrid-account.**



Als u dit hebt gedaan, slaat u het beleid op en voegt u dit beveiligingsbeleid toe aan de apparaatsjabloon onder **Aanvullende sjablonen** -> **Beveiligingsbeleid** zoals in de afbeelding.



Configureer het apparaat met de bijgewerkte apparaatsjabloon.

Verifiëren

Zodra het apparaatsjabloon met succes naar het randapparaat is gedrukt, kan de AMP-configuratie worden geverifieerd vanuit de Edge-router CLI:

<#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
```

Problemen oplossen

De SD-WAN AMP integratie heeft betrekking op vele componenten zoals beschreven. Dus als het op probleemoplossing aankomt, is het cruciaal om in staat te zijn om enkele belangrijke afbakeningspunten vast te stellen om het probleem te beperken tot de componenten in de functiestroom:

1. **vManage.** Kan vManager het beveiligingsbeleid met het AMP-beleid naar het randapparaat duwen?
2. **Rand**. Wanneer het beveiligingsbeleid met succes naar de rand is gedrukt, neemt de router het bestand op dat onderworpen is aan AMP-inspectie en stuurt hij het naar de AMP/TG-cloud?
3. **AMP/TG-cloud.** Als de rand het bestand naar AMP of TG heeft verzonden, krijgt het dan de reactie die nodig is om een besluit toe te staan of te laten vallen?

Dit artikel is bedoeld om te focussen op het randapparaat (2) met de verschillende gegevensvlak tools die beschikbaar zijn om problemen met AMP-integratie op de WAN Edge-router op te lossen.

Algemene stroom voor probleemoplossing

Gebruik deze werkstroom op hoog niveau om snel problemen op te lossen met de verschillende componenten die betrokken zijn bij AMP integratie met een belangrijke doelstelling om het afbakeningspunt van het probleem tussen het randapparaat en de AMP/TG cloud te bepalen.

1. Wordt het AMP-beleid correct naar het randapparaat geduwd?
2. Controleer de algemene gezondheid van de UTD-container.
3. Controleer de reputatie van het bestand en analyseer de status van de client aan de rand.
4. Controleer of de bestandsoverdracht naar de container is verlegd. Dit kan worden gedaan met het Cisco IOS® XE-pakketspoor.
5. Controleer of de rand met succes communiceert met de AMP/TG-cloud. Dit kan worden gedaan met tools zoals EPC of packet-trace.
6. Zorg ervoor dat UTD een lokale cache maakt op basis van de AMP-respons.

Deze stappen voor probleemoplossing worden in detail in dit document onderzocht.

Policy Push Problemen met vManager

Zoals getoond met de AMP beleidsconfiguratie, is het AMP beleid vrij ongecompliceerd zonder veel configuratieopties. Hier zijn een paar alledaagse dingen om rekening mee te houden:

1. vManager moet de DNS-namen voor AMP- en ThreatGrid-cloud voor API-toegang kunnen oplossen. Als de apparaatconfiguratie op vManager mislukt nadat het AMP-beleid is toegevoegd, controleert u op **/var/log/nms/vmanage-server.log** op fouten.
2. Zoals in de configuratiehandleiding is aangegeven, heeft het Alerts Log Level het standaard kritische niveau verlaten, of Waarschuwing indien nodig. Vastlegging op Info-niveau moet worden vermeden, aangezien dit een negatief effect kan hebben op de prestaties.

Om te verifiëren, heb toegang tot de neo4j DB en bekijk de inhoud van de vmanagedAPIKEYNODE tabel.

```
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-integratie op Cisco Edge-router

Controleer de gezondheid van UTD-containers

Gebruik de opdrachten show utd om de algehele gezondheid van de UTD-container te controleren:

```
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
```

Controleer UTD AMP-status

Controleer of bestandsinspectie is ingeschakeld:

<#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`

Controleer of de verbinding met de AMP-cloud actief is:

<#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!"
```

Controleer of de verbinding met ThreatGrid is geactiveerd:

<#root>

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

`Running`

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

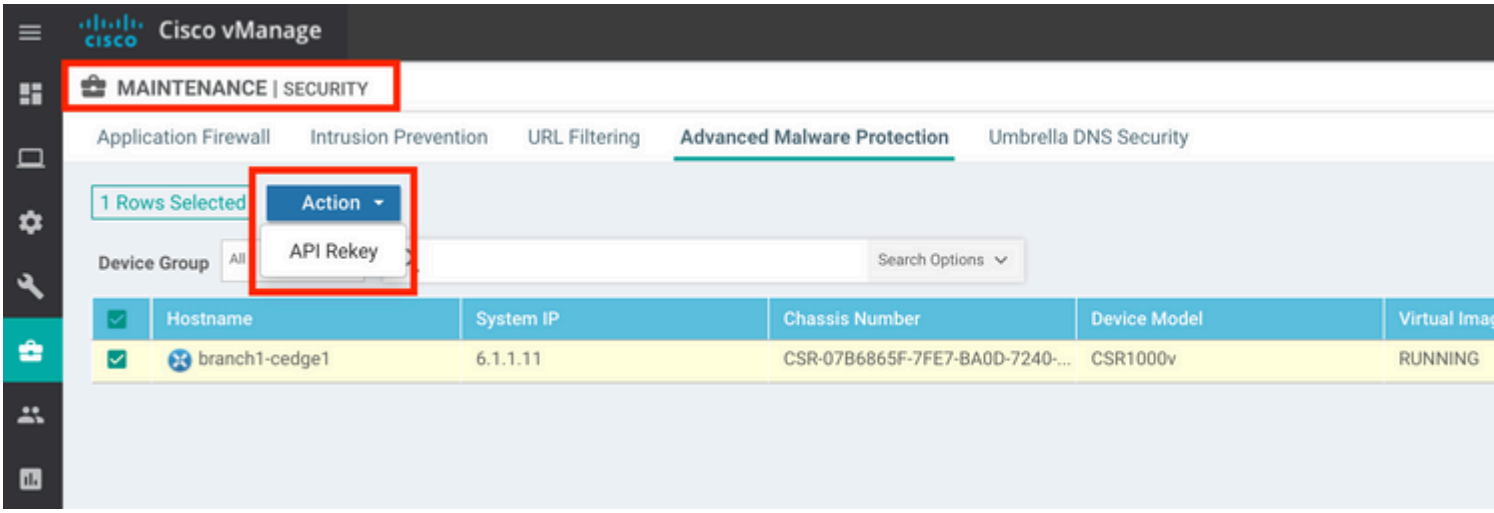
<#root>

```
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"
```

Als het ThreatGrid-proces geen status van Up weergeeft, helpt een API-sleutel. Om een API-rekey te activeren, navigeer naar **Onderhoud** -> **Beveiliging**:



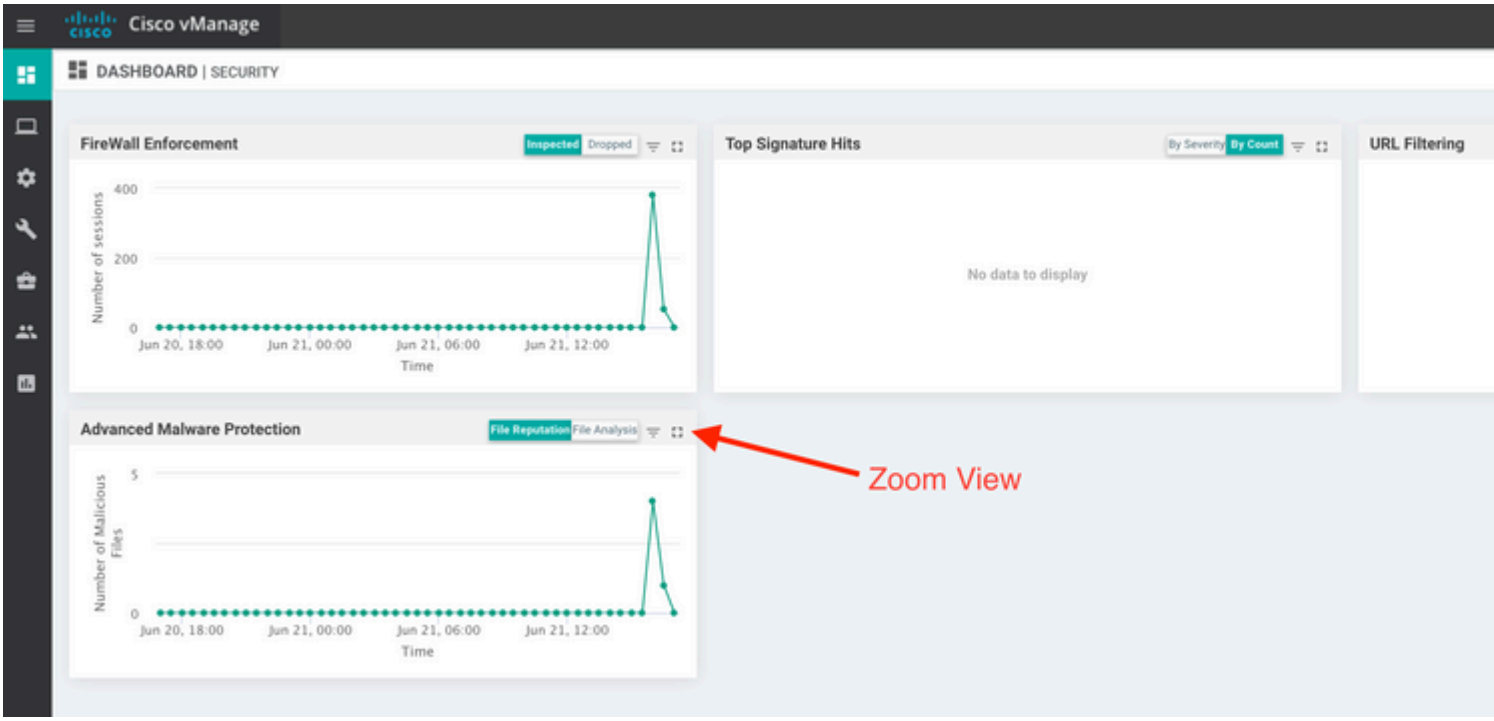
Opmerking: Een API rekey activeert een sjabloonduw naar het apparaat.

AMP-activiteitsbewaking op WAN Edge-router

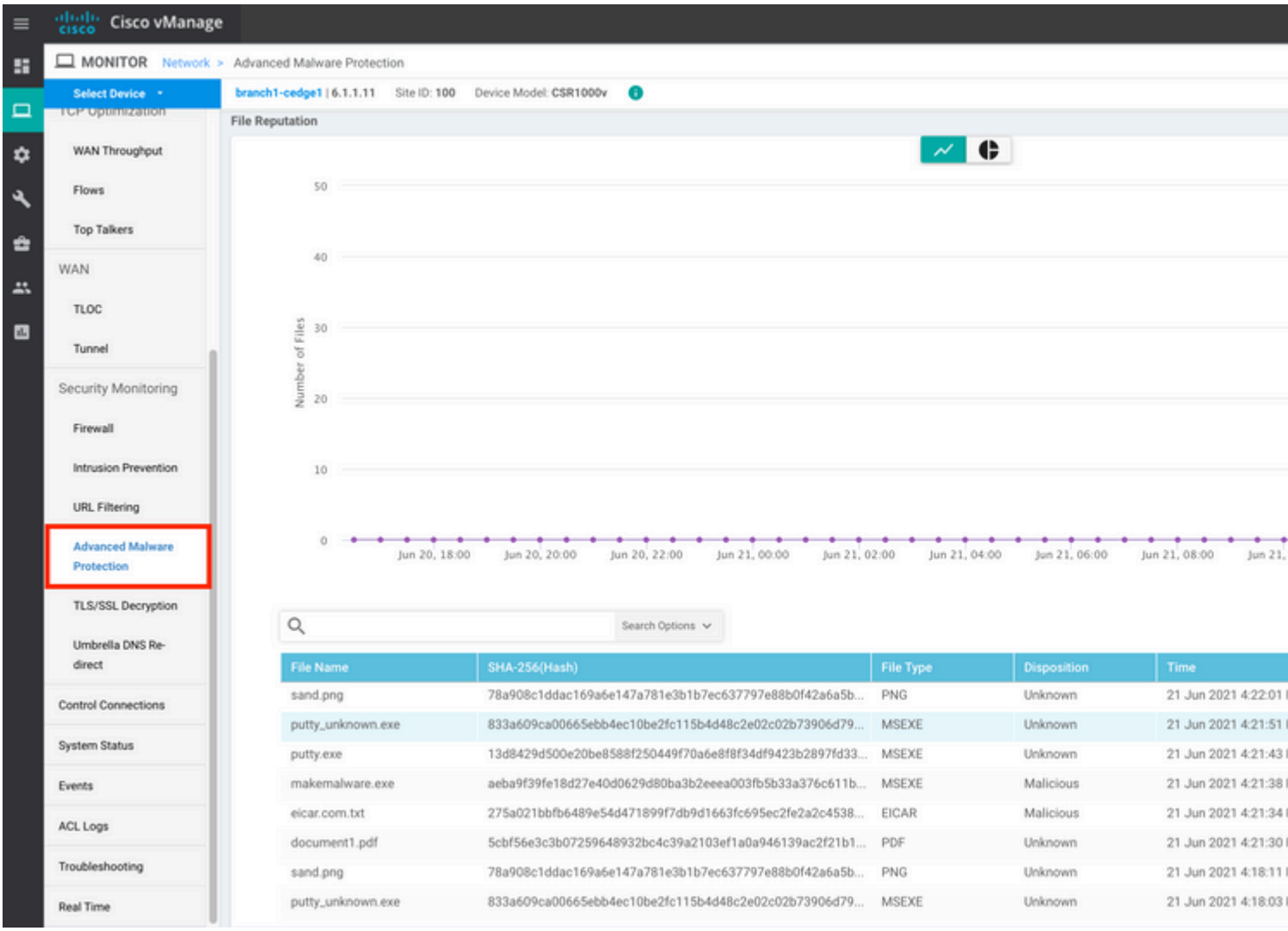
vManage

Vanaf vManager kunnen de activiteiten van het AMP-bestand worden gevolgd vanaf het security dashboard of vanuit de Apparaatweergave.

Beveiligingsdashboard:



Apparaatweergave:



CLI

Bekijk de reputatiestatistieken van het bestand:

```
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
```

Controleer de statistieken van de bestandsanalyse:

```
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
```

Opmerking: aanvullende interne statistieken kunnen worden verkregen met de opdracht ***toon utd engine standard statistics file-reputation vrf global internal***.

Dataplane-gedrag

Het dataplane-verkeer dat onderworpen is aan bestandsinspectie op basis van het geconfigureerde AMP-beleid wordt voor verwerking naar de UTD-container geleid. Dit kan met een gebruikt pakketspoor worden bevestigd. Als het verkeer niet naar behoren naar de container is omgeleid, kan geen van de volgende bestandsinspecties plaatsvinden.

Lokale bestandscache voor AMP

De UTD-container heeft een lokaal cachegeheugen van SHA256 hash, bestandstype, dispositie en actie gebaseerd op eerdere AMP cloud lookup resultaten. De container vraagt alleen een schikking uit de AMP cloud als de bestandshash niet in de lokale cache is. De lokale cache heeft een TTL van 2 uur voordat de cache wordt verwijderd.

```
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
```

Afwikkelingscode AMP:

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

Actiecode:

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

Om de volledige SHA256 hash voor de bestanden te verkrijgen, die zeer belangrijk is om problemen op te lossen met een specifieke bestandsvonnis, gebruik de detailoptie van de opdracht:

```
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>
```

Gebruik de opdracht om de lokale cache-ingangen van de UTD-engine te detecteren:

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

UTD-debugs uitvoeren

De utd debugs kunnen worden ingeschakeld om AMP problemen op te lossen:

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

De debug-uitvoer kan direct van de systeemshell worden opgehaald op **/tmp/rp/trace/vman_utd_R0-0.bin**, of het traceerbestand naar het routerbestandssysteem kopiëren met de stappen:

```
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#
```

U kunt het UTD-sporenlogboek als volgt weergeven:

```
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>
```

> **Opmerking**: In 20.6.1 en later is de manier om de utd tracelogs op te halen en te bekijken in lijn met de standaard sporenworkflow met de **show logging proces vman module utd** ... uit.

Controleer de communicatie van Edge naar de cloud

Om te controleren of het Edge-apparaat communiceert met de AMP/TG-cloud, kan EPC op de WAN Edge-router worden gebruikt om te bevestigen dat er sprake is van bidirectionele communicatie van/naar de cloudservices:

```
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
```

Problemen met AMP en TG Cloud

Zodra het is bevestigd, neemt het randapparaat het bestand correct op en stuurt het naar AMP/TG voor analyse, maar de uitspraak is onjuist, vereist AMP probleemoplossing of Threatgrid cloud, die buiten het bereik van dit document valt. De informatie is belangrijk wanneer integratiekwesties worden gepresenteerd:

- ThreatGrid-accountorganisatie
- tijdstempel
- ID voor apparaatanalyse (bijvoorbeeld CSR-07B6865F-7FE7-BA0D-7240-1BDA16328455), dit is het chassisnummer voor de WAN Edge-router.
- Complete SHA256 hash voor het bestand in kwestie

Gerelateerde informatie

- Configuratiehandleiding SD-WAN beveiliging
- ThreatGrid-portal
- Technische ondersteuning en documentatie â€“ Cisco Systems

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.