

Configurazione dell'integrazione di SD-WAN Advanced Malware Protection (AMP) e risoluzione dei problemi

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Panoramica della soluzione](#)

[Componenti](#)

[Flusso funzionalità](#)

[Configurazione integrazione SD-WAN AMP](#)

[Configura criterio di protezione da vManage](#)

[Verifica](#)

[Risoluzione dei problemi](#)

[Flusso di risoluzione dei problemi generale](#)

[Problemi di push delle policy in vManage](#)

[Integrazione AMP su Cisco Edge Router](#)

[Verifica integrità contenitore UTD](#)

Introduzione

Questo documento descrive come configurare e risolvere i problemi di integrazione di Cisco SD-WAN Advanced Malware Protection (AMP) su un router Cisco IOS® XE SD-WAN.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

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

Componenti usati

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali

conseguenze derivanti dall'uso dei comandi.

Panoramica della soluzione

Componenti

L'integrazione SD-WAN AMP è parte integrante della soluzione SD-WAN Edge Security che mira alla visibilità e alla protezione degli utenti di una filiale da malware.

È costituito dai seguenti componenti:

- WAN Edge Router su una filiale. Questo è un router Cisco IOS® XE in modalità controller con funzionalità di sicurezza in un contenitore UTD
- AMP Cloud L'infrastruttura cloud AMP risponde alle query di hash dei file con una disposizione
- ThreatGrid. Infrastruttura cloud in grado di eseguire il test di un file per il rilevamento di malware potenziale in un ambiente sandbox

Questi componenti interagiscono per fornire le seguenti funzionalità chiave per AMP:

- Valutazione della reputazione dei file

Processo dell'hash SHA256 utilizzato per confrontare il file con il server cloud Advanced Malware Protection (AMP) e accedere alle relative informazioni di intelligence sulle minacce. La risposta può essere Pulita, Sconosciuta o Dannosa. Se la risposta è Sconosciuto e l'analisi del file è configurata, il file viene automaticamente inviato per un'ulteriore analisi.

- Analisi file

File sconosciuto inviato al cloud ThreatGrid (TG) per la detonazione in un ambiente sandbox. Durante la detonazione, la sandbox cattura gli artefatti e osserva il comportamento del file, quindi assegna al file un punteggio complessivo. In base alle osservazioni e al punteggio, Threat Grid può modificare la risposta alla minaccia in Clean (Pulita) o Malicious (Dannosa). Le scoperte di ThreatGrid vengono segnalate al cloud AMP in modo che tutti gli utenti di AMP siano protetti dal malware appena scoperto.

- Retrosezione

Mantiene informazioni sui file anche dopo che sono stati scaricati, possiamo segnalare i file che sono stati ritenuti dannosi dopo che sono stati scaricati. L'eliminazione dei file potrebbe cambiare in base alle nuove informazioni sulle minacce acquisite dal cloud AMP. La riclassificazione genera notifiche retroattive automatiche.

Attualmente, SD-WAN con integrazione AMP supporta l'ispezione dei file per i protocolli:

- HTTP
- SMTP
- IMAP

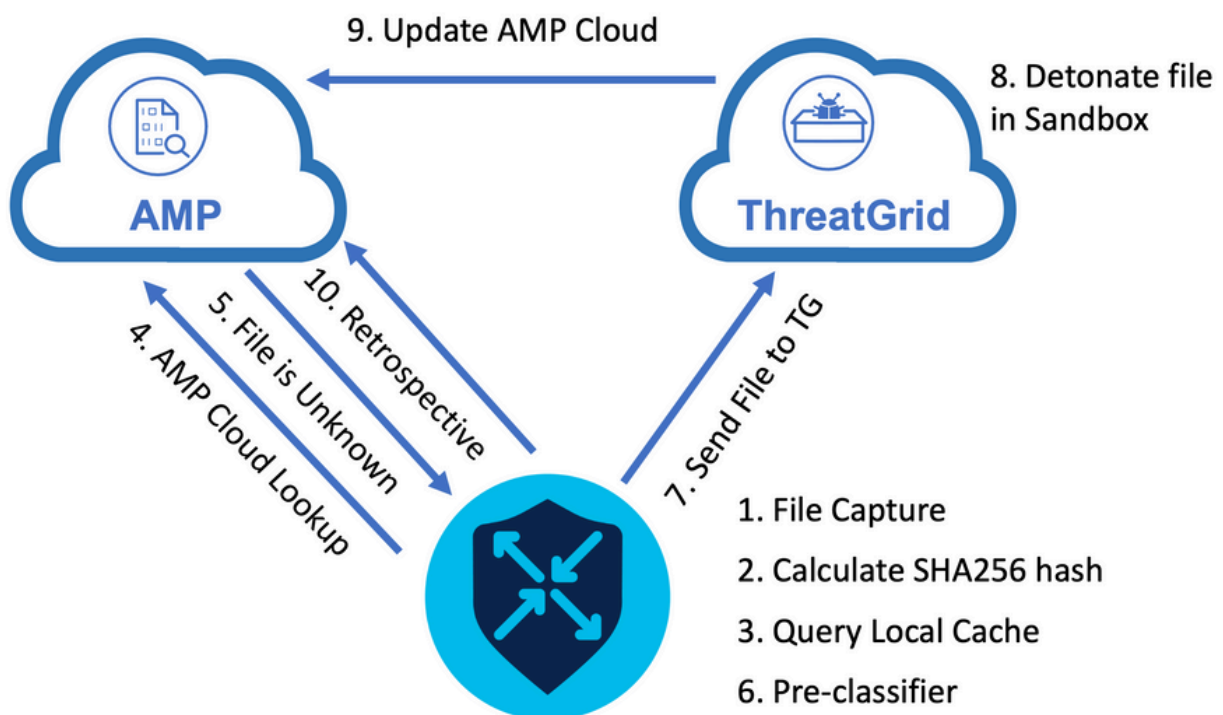
- POP3
- FTP
- PMI

✎ Nota: il trasferimento di file tramite HTTPS è supportato solo con il [proxy SSL/TLS](#).

✎ Nota: l'analisi dei file può essere eseguita solo su un file completo e non su un file suddiviso in contenuto parziale. Ad esempio, quando un client HTTP richiede un contenuto parziale con l'intestazione Range e recupera il contenuto parziale HTTP/1.1 206. In questo caso, poiché l'hash del file parziale è significativamente diverso dal file completo, Snort ignora l'ispezione del file per il contenuto parziale.

Flusso funzionalità

L'immagine mostra il flusso di alto livello per l'integrazione SD-WAN AMP quando un file deve essere inviato a ThreatGrid per l'analisi.




Per il flusso mostrato:


1. Il trasferimento di file per i protocolli supportati da AMP viene acquisito dal contenitore UTD.
2. Viene calcolato l'hash SHA256 per il file.
3. L'hash SHA256 calcolato viene interrogato sul sistema di cache locale in UTD per verificare se la disposizione è già nota e il TTL della cache non è scaduto.
4. Se non c'è corrispondenza con la cache locale, l'hash SHA256 viene cercato nel cloud AMP per una disposizione e un'azione di ritorno.
5. Se la disposizione è UNKNOWN e l'azione di risposta è ACTION_SEND, il file viene

eseguito attraverso il sistema di preclassificazione in UTD.

6. Il preclassificatore determina il tipo di file e verifica se il file contiene contenuto attivo.
7. Se vengono soddisfatte entrambe le condizioni, il file viene inviato a ThreatGrid.
8. ThreatGrid fa detonare il file in una sandbox e assegna al file un punteggio di rischio.
9. ThreatGrid aggiorna il cloud AMP in base alla valutazione della minaccia.
10. Il dispositivo perimetrale interroga il cloud AMP per la retrospettiva in base all'intervallo di heartbeat di 30 minuti.

Configurazione integrazione SD-WAN AMP

 Nota: è necessario caricare un'immagine virtuale di protezione in vManage prima di configurare la funzionalità AMP. Per ulteriori informazioni, passare a [Security Virtual Image](#) (Immagine virtuale di sicurezza).






 Nota: per informazioni sui requisiti di rete necessari per il corretto funzionamento della connettività AMP/ThreatGrid, vedere questo documento: [Indirizzi IP/nomi host obbligatori AMP/TG](#)

Configura criterio di protezione da vManage

Per abilitare AMP, passare a Configurazione -> Protezione -> Aggiungi criterio di protezione. Selezionare Accesso diretto a Internet e selezionare Procedi come mostrato nell'immagine.

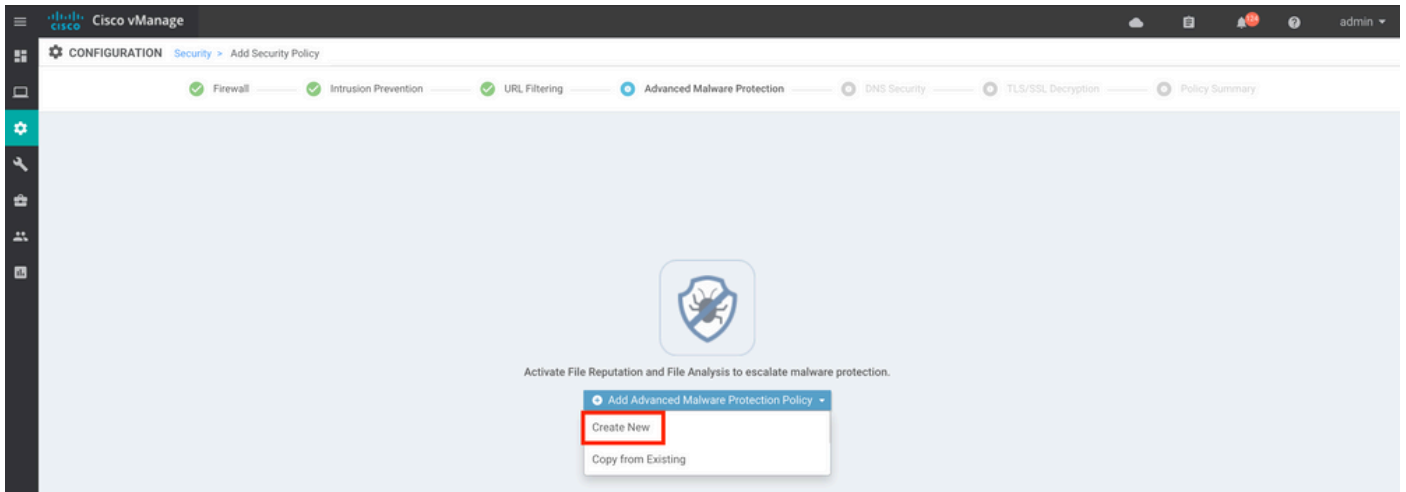
Add Security Policy ✕

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

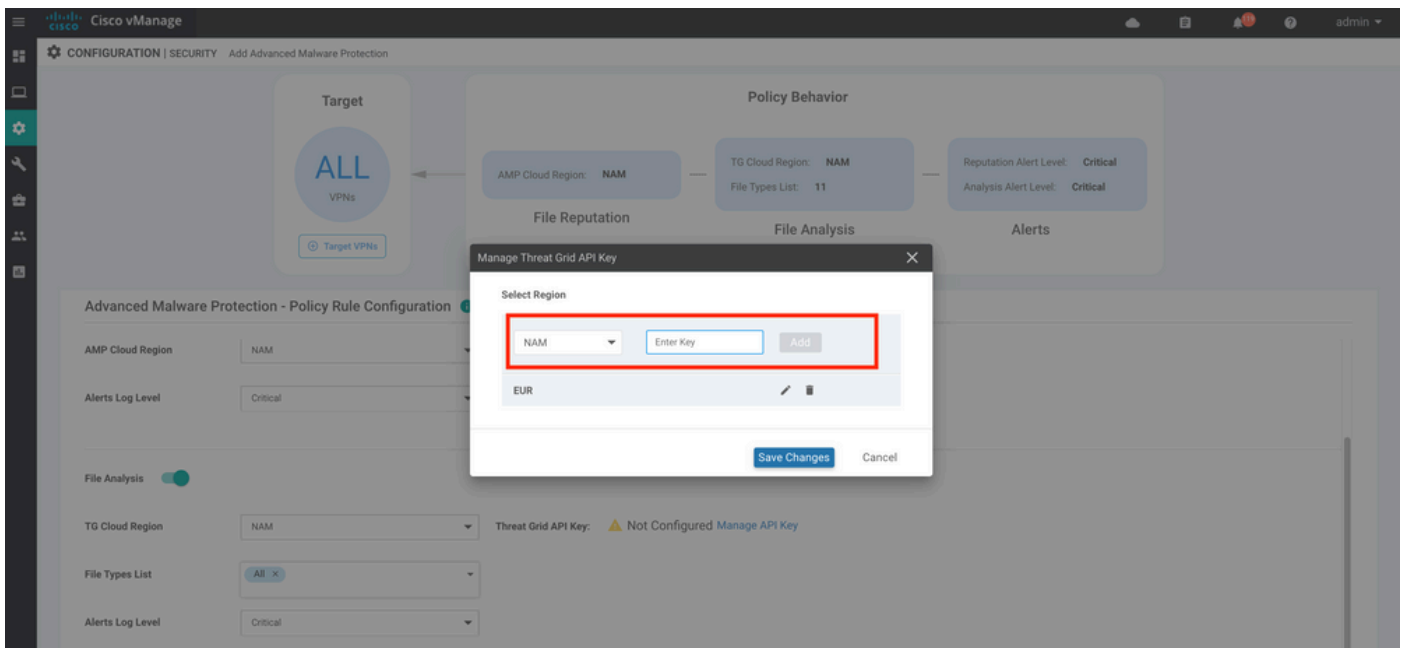
-  **Compliance**
Application Firewall | Intrusion Prevention | TLS/SSL Decryption
-  **Guest Access**
Application Firewall | URL Filtering | TLS/SSL Decryption
-  **Direct Cloud Access**
Application Firewall | Intrusion Prevention | Advanced Malware Protection | DNS Security | TLS/SSL Decryption
-  **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

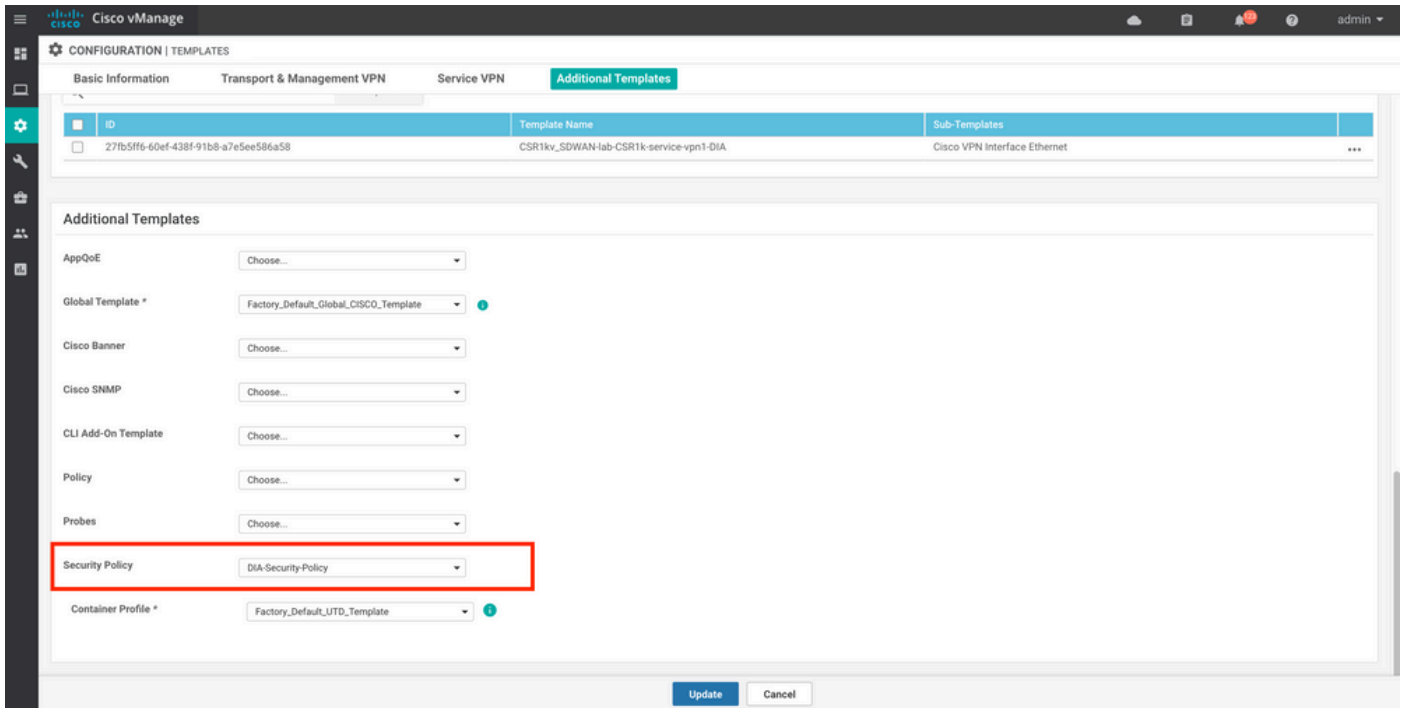
Configurare le funzioni di sicurezza in base alle esigenze fino a raggiungere la funzione Advanced Malware Protection. Aggiungere un nuovo criterio di protezione avanzata da malware.



Specificare un nome per il criterio. Selezionare una delle aree cloud AMP globali e abilitare l'analisi dei file. Per l'analisi dei file con ThreatGrid usato, scegliere una delle aree del cloud TG e immettere la chiave API ThreatGrid, che può essere ottenuta dal portale ThreatGrid in Account ThreatGrid.



Al termine, salvare il criterio e aggiungerlo al modello di dispositivo in Modelli aggiuntivi -> Criteri di protezione come mostrato nell'immagine.



Configurare il dispositivo con il modello aggiornato.

Verifica

Una volta eseguito correttamente il push del modello di dispositivo al dispositivo periferico, la configurazione AMP può essere verificata dalla CLI di Edge Router:

```
<#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
```

Risoluzione dei problemi

L'integrazione SD-WAN AMP coinvolge molti componenti come descritto. Quando si tratta di risolvere un problema, è fondamentale essere in grado di stabilire alcuni punti di demarcazione chiave per limitare il problema ai componenti del flusso di funzionalità:

1. vManage. vManage è in grado di eseguire il push dei criteri di sicurezza con i criteri AMP nel dispositivo periferico?
2. Bordo. Una volta che il criterio di sicurezza è stato correttamente spostato al limite, il router acquisisce il file soggetto all'ispezione AMP e lo invia al cloud AMP/TG?
3. Cloud AMP/TG. Se il perimetro ha inviato il file ad AMP o TG, ottiene la risposta necessaria per prendere una decisione di consenso o di rifiuto?

Il presente articolo si concentra sul dispositivo periferico (2) con i vari strumenti del piano dati disponibili per aiutare a risolvere i problemi con l'integrazione AMP sul router perimetrale WAN.

Flusso di risoluzione dei problemi generale

Utilizzare questo flusso di lavoro di alto livello per risolvere rapidamente i problemi relativi ai vari componenti coinvolti nell'integrazione AMP con un obiettivo chiave per stabilire il punto di demarcazione del problema tra il dispositivo periferico e il cloud AMP/TG.

1. I criteri AMP sono stati spostati correttamente sul dispositivo periferico?
2. Controllare lo stato generale del contenitore UTD.
3. Controllare la reputazione del file e analizzare lo stato del client sul perimetro.
4. Verificare se il trasferimento di file viene deviato al contenitore. A tale scopo, è possibile eseguire la traccia dei pacchetti Cisco IOS® XE.
5. Verificare che lo spigolo comunichi con il cloud AMP/TG. A tale scopo, è possibile utilizzare strumenti quali EPC o packet-trace.
6. Verificare che UTD crei una cache locale in base alla risposta AMP.

Queste procedure di risoluzione dei problemi sono illustrate in dettaglio in questo documento.

Problemi di push delle policy in vManage

Come illustrato nella configurazione della policy AMP, la policy AMP è piuttosto semplice senza numerose opzioni di configurazione. Di seguito sono riportate alcune considerazioni comuni da tenere in considerazione:

1. vManage deve essere in grado di risolvere i nomi DNS per il cloud AMP e ThreatGrid per l'accesso API. Se la configurazione del dispositivo su vManage ha esito negativo dopo l'aggiunta del criterio AMP, controllare la presenza di errori nella chiave `/var/log/nms/vmanage-server.log`.
2. Come indicato nella guida alla configurazione, Alert Log Level ha lasciato il livello critico predefinito o Warning (Avviso) se garantito. È necessario evitare la registrazione a livello di informazioni, poiché può avere un impatto negativo sulle prestazioni.

Per eseguire la verifica, accedere al database neo4j e visualizzare il contenuto della tabella vmanagedbAPIKEYNODE.

```
neo4j@neo4j> match (n:vmanagedbAPIKEYNODE) return n; +-----+
+-----+ | n | +-----+
+-----+ | (:vmanagedbAPIKEYNODE {_rid:
"0:ApiKeyNode:1621022413389:153", keyServerHostName: "isr.api.threatgrid.com", feature: "Amp", apiKey:
"$CRYPT_CLUSTER$bGLEMGIYMNRy1s9P+WcfA==$dozo7tmRP1+HrvEnXQr4x1VxSViYkKwQ4HBAIhXWOtQ=", deviceID: "CSR-
07B6865F-7FE7-BA0D-7240-1BDA16328455"}) | +-----+
+-----+ +-----+
```

Integrazione AMP su Cisco Edge Router

Verifica integrità contenitore UTD

Utilizzare i comandi show utd per verificare lo stato complessivo del contenitore UTD:

```
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
```

Controlla stato AMP UTD

Verificare che l'ispezione dei file sia abilitata:

<#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
```

Verificare che la connessione al cloud AMP sia attiva:

```
<#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!"
```

Verificare che la connessione a ThreatGrid sia attiva:

```
<#root>
```

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

```
Running
```

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

```
<#root>
```

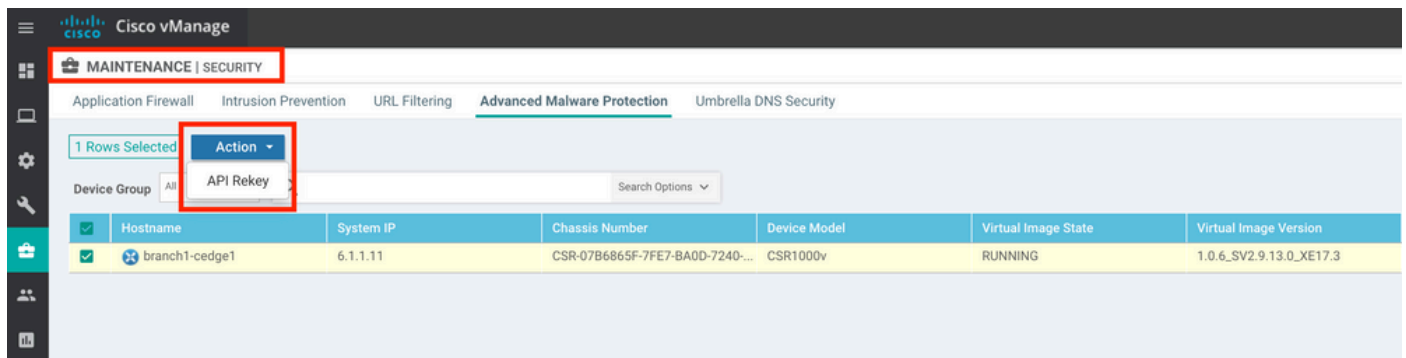
```
branch1-edge1#show sdwan utd file analysis
```

```
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"
```

Se il processo ThreatGrid non mostra lo stato Attivo, la reimpostazione della chiave API è di aiuto. Per attivare una nuova chiave API, passare a Manutenzione -> Sicurezza:



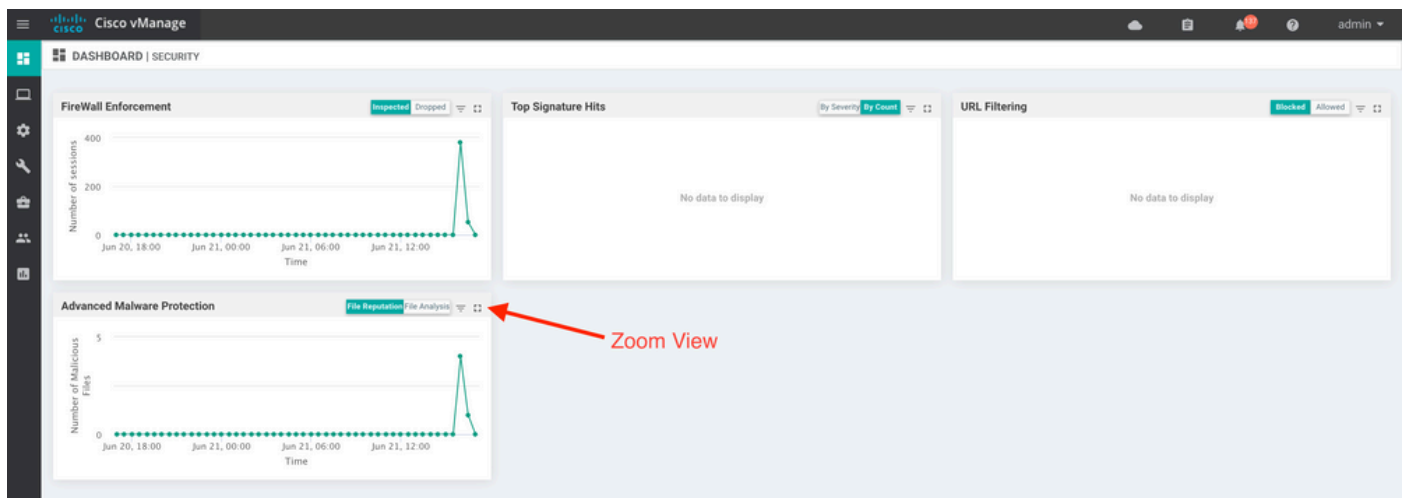
 Nota: la reimpostazione di una chiave API attiva un push di modello al dispositivo.

Monitoraggio dell'attività AMP su WAN Edge Router

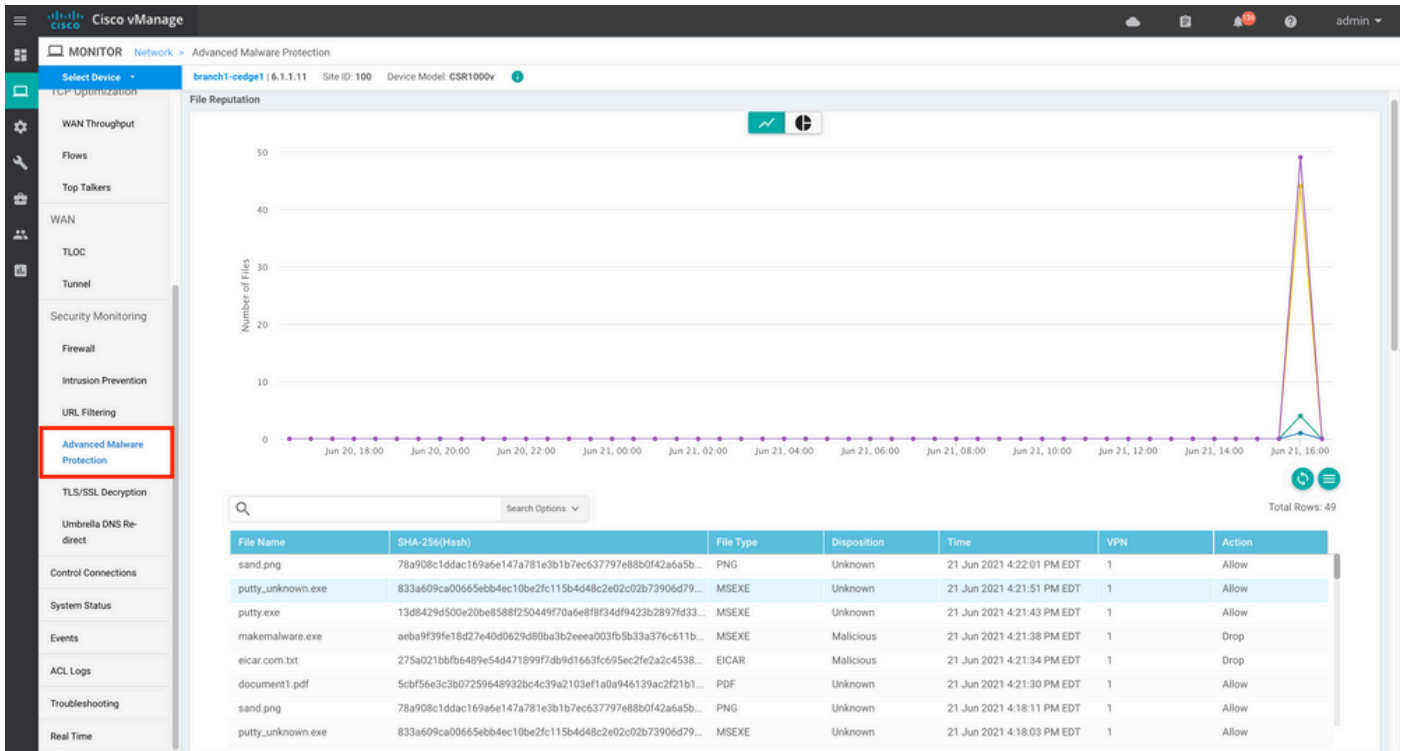
vManage

Da vManage, le attività relative ai file AMP possono essere monitorate dal dashboard di protezione o dalla Vista dispositivi.

Dashboard di protezione:



Visualizzazione dispositivo:



CLI

Verifica statistiche reputazione file:

```
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
```

Controllare le statistiche di analisi file:

```
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
```

Nota: è possibile ottenere ulteriori statistiche interne con il comando `show utd engine standard statistics file-reputation vrf global internal`.

Comportamento del piano dati

Il traffico del dataplane soggetto all'ispezione dei file in base ai criteri AMP configurati viene deviato al contenitore UTD per l'elaborazione. Questa condizione può essere confermata con l'uso di una traccia del pacchetto. Se il traffico non viene deviato correttamente al contenitore, non può verificarsi alcuna delle successive operazioni di ispezione dei file.

Cache locale file AMP

Il contenitore UTD dispone di una cache locale di hash SHA256, tipo di file, disposizione e azione basata sui risultati di ricerche precedenti nel cloud AMP. Il contenitore richiede una disposizione dal cloud AMP solo se l'hash del file non è presente nella cache locale. La cache locale ha un TTL di 2 ore prima dell'eliminazione.

```
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

Codice smaltimento AMP:

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

Codice azione AMP:

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

Per ottenere l'hash SHA256 completo per i file, che è molto importante per risolvere uno specifico problema di verdetto dei file, usare l'opzione `detail` del comando:

```
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>
```

Per eliminare le voci della cache locale del motore UTD, utilizzare il comando:

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

Esegui debug UTD

I debug utd possono essere abilitati per la risoluzione dei problemi AMP:


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

L'output del comando debug può essere recuperato direttamente dalla shell di sistema all'indirizzo /tmp/rp/trace/vman_utd_R0-0.bin oppure è possibile copiare il file di trace nel file system del router eseguendo la procedura seguente:

```
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#
```

Per visualizzare il registro di traccia UTD:

```
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_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>
```

 Nota: nella versione 20.6.1 e successive, il modo per recuperare e visualizzare i registri di traccia utd è in linea con il flusso di lavoro di traccia standard con il comando show logging process vman module utd

Verifica della comunicazione da Edge a Cloud

Per verificare la comunicazione tra il dispositivo periferico e il cloud AMP/TG, è possibile utilizzare EPC sul router perimetrale WAN per confermare la comunicazione bidirezionale tra i servizi cloud:

```
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
```

Problemi correlati a AMP e TG Cloud

Una volta confermata, la periferica perimetrale acquisisce correttamente il file e lo invia ad AMP/TG per l'analisi, ma il verdetto non è corretto, richiede la risoluzione dei problemi AMP o il cloud Threatgrid, che esula dall'ambito di questo documento. Le informazioni sono importanti quando vengono presentate le questioni relative all'integrazione:

- Account ThreatGrid Organizzazione
- Timestamp
- ID analisi dispositivo (ad esempio, CSR-07B6865F-7FE7-BA0D-7240-1BDA16328455), è il numero di chassis del router perimetrale WAN.
- Hash SHA256 completo per il file in questione

Informazioni correlate

- [Guida alla configurazione della sicurezza SD-WAN](#)
- [Portale ThreatGrid](#)
- [Documentazione e supporto tecnico – Cisco Systems](#)

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).