Configurar integração e solução de problemas da Proteção avançada contra malware (AMP) SD-WAN

Contents

Introduction

Este documento descreve como configurar e solucionar problemas da integração do Cisco SD-WAN Advanced Malware Protection (AMP) em um roteador Cisco IOS® XE SD-WAN.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Advanced malware protection (AMP)
- Rede de longa distância definida por software da Cisco (SD-WAN)

Componentes Utilizados

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Visão geral da solução

Componentes

A integração SD-WAN AMP é parte integrante da solução de segurança de borda SD-WAN que visa a

visibilidade e a proteção para usuários em uma filial contra malware.

Ele consiste nos seguintes componentes do produto:

- **Roteador de borda WAN em uma filial.** Este é um roteador Cisco IOS® XE no modo controlador com recursos de segurança em um contêiner UTD
- **Nuvem da AMP.** A infraestrutura de nuvem da AMP responde a consultas de hash de arquivo com uma disposição
- **ThreatGrid**. A infraestrutura de nuvem que pode testar um arquivo em busca de possíveis malwares em um ambiente de sandbox

Esses componentes trabalham em conjunto para oferecer os seguintes recursos importantes para a AMP:

- **Avaliação de reputação do arquivo**

O processo de hash SHA256 usado para comparar o arquivo com o servidor de nuvem Advanced Malware Protection (AMP) e acessar suas informações de inteligência de ameaças. A resposta pode ser Limpa, Desconhecida ou Mal-intencionada. Se a resposta for Desconhecido e se a Análise de arquivo estiver configurada, o arquivo será enviado automaticamente para análise posterior.

- **Análise de arquivo**

Um arquivo desconhecido é enviado à nuvem do ThreatGrid (TG) para ser detonado em um ambiente de sandbox. Durante a detonação, a sandbox captura artefatos e observa os comportamentos do arquivo e, em seguida, atribui ao arquivo uma pontuação geral. Com base nas observações e na pontuação, o Threat Grid pode alterar a resposta à ameaça para Limpa ou Mal-intencionada. As descobertas do ThreatGrid são relatadas à nuvem da AMP para que todos os usuários da AMP estejam protegidos contra malware recém-descoberto.

- **Retrospecção**

Ele mantém informações sobre os arquivos mesmo depois que eles são baixados, nós podemos relatar sobre os arquivos que foram determinados como mal-intencionados depois que eles foram baixados. A disposição dos arquivos pode mudar com base na nova inteligência de ameaças obtida pela nuvem da AMP. Essa reclassificação gera notificações retrospectivas automáticas.

Atualmente, a SD-WAN com integração ao AMP oferece suporte à inspeção de arquivos para os protocolos:

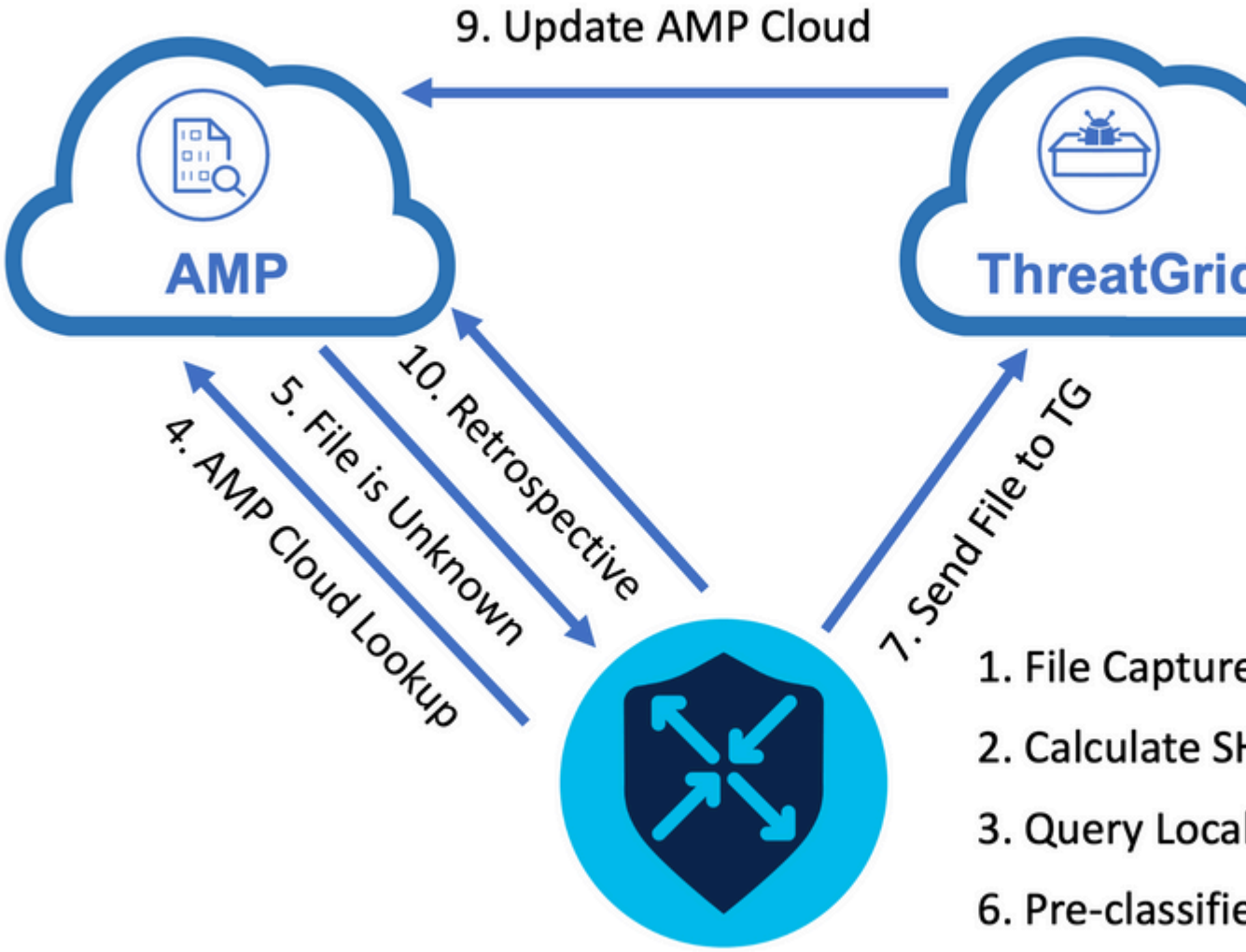
- HTTP
- SMTP
- IMAP
- POP3
- FTP
- SMB

Observação: a transferência de arquivos por HTTPS só é suportada com proxy SSL/TLS .

Observação: a análise de arquivos só pode ser executada em um arquivo completo, e não em arquivos quebrados em conteúdo parcial. Por exemplo, quando um cliente HTTP solicita conteúdo parcial com o cabeçalho Range e retorna o ***HTTP/1.1 206 Partial Content.*** Nesse caso, como o hash de arquivo parcial é significativamente diferente do arquivo completo, o Snort ignora a inspeção de arquivo para o conteúdo parcial.

Fluxo de recursos

A imagem mostra o fluxo de alto nível para integração da SD-WAN AMP quando um arquivo precisa ser enviado ao ThreatGrid para análise.



Para o fluxo mostrado:

1. A transferência de arquivos para protocolos compatíveis com AMP é capturada pelo contêiner UTD.
2. O hash SHA256 do arquivo é calculado.
3. O hash SHA256 calculado é consultado no sistema de cache local em UTD para ver se a disposição já é conhecida e o TTL de cache não expirou.
4. Se não houver correspondência com o cache local, o hash SHA256 será pesquisado na nuvem da AMP para uma ação de disposição e retorno.
5. Se a disposição for DESCONHECIDA e a ação de resposta for ACTION_SEND, o arquivo será executado pelo sistema de pré-classificação em UTD.
6. O pré-classificador determina o tipo de arquivo e também valida se o arquivo contém conteúdo ativo.
7. Se ambas as condições forem atendidas, o arquivo será enviado para o ThreatGrid.
8. O ThreatGrid detona o arquivo em uma área protegida e atribui ao arquivo uma pontuação de ameaça.
9. O ThreatGrid atualiza a nuvem da AMP com base na avaliação de ameaças.
10. O dispositivo de borda consulta a nuvem da AMP para Retrospectiva com base no intervalo de pulsação de 30 minutos.

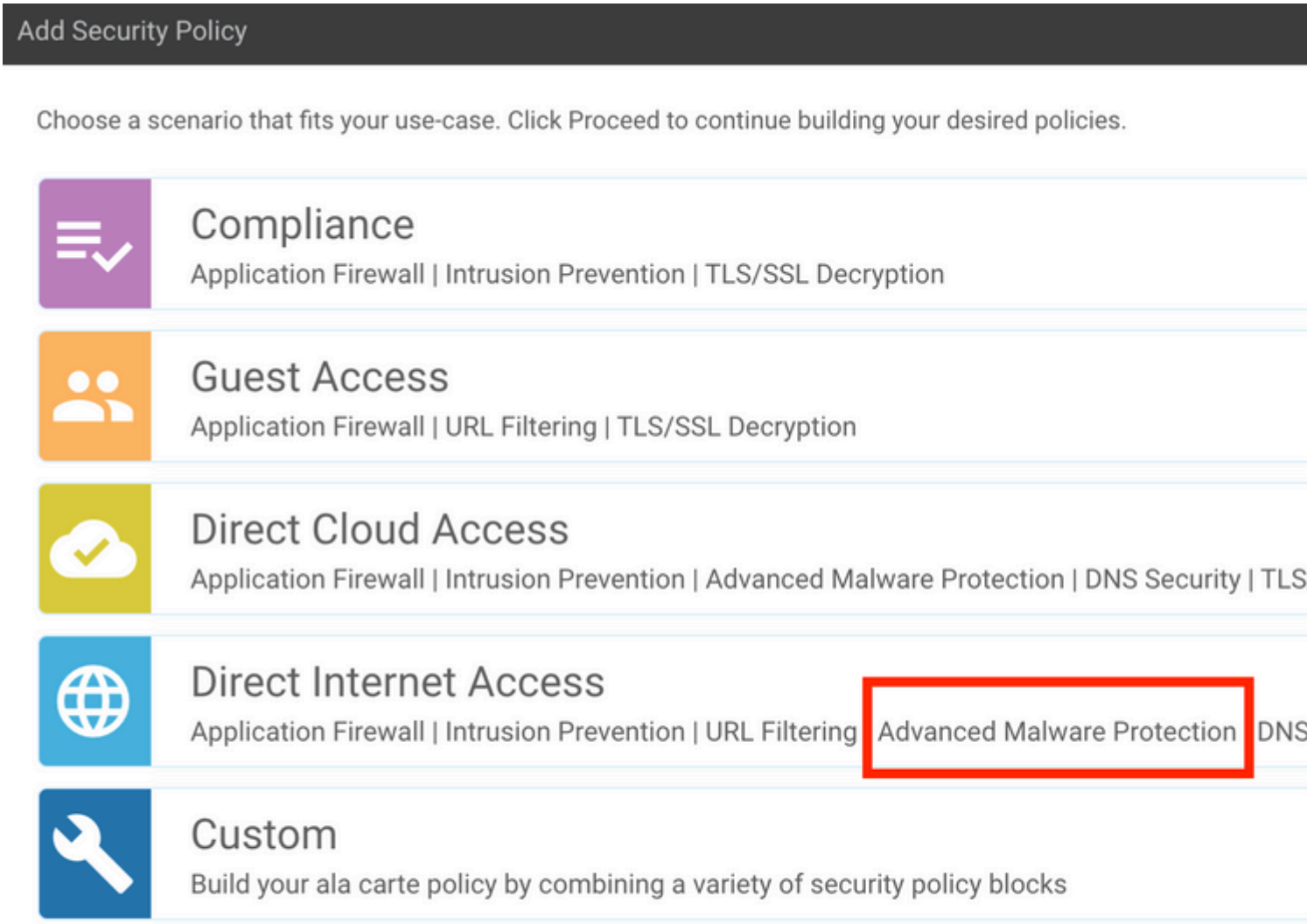
Configuração de integração da SD-WAN AMP

Observação: uma imagem virtual de segurança deve ser carregada no vManage antes da configuração do recurso AMP. Para obter detalhes, navegue até Security Virtual Image .

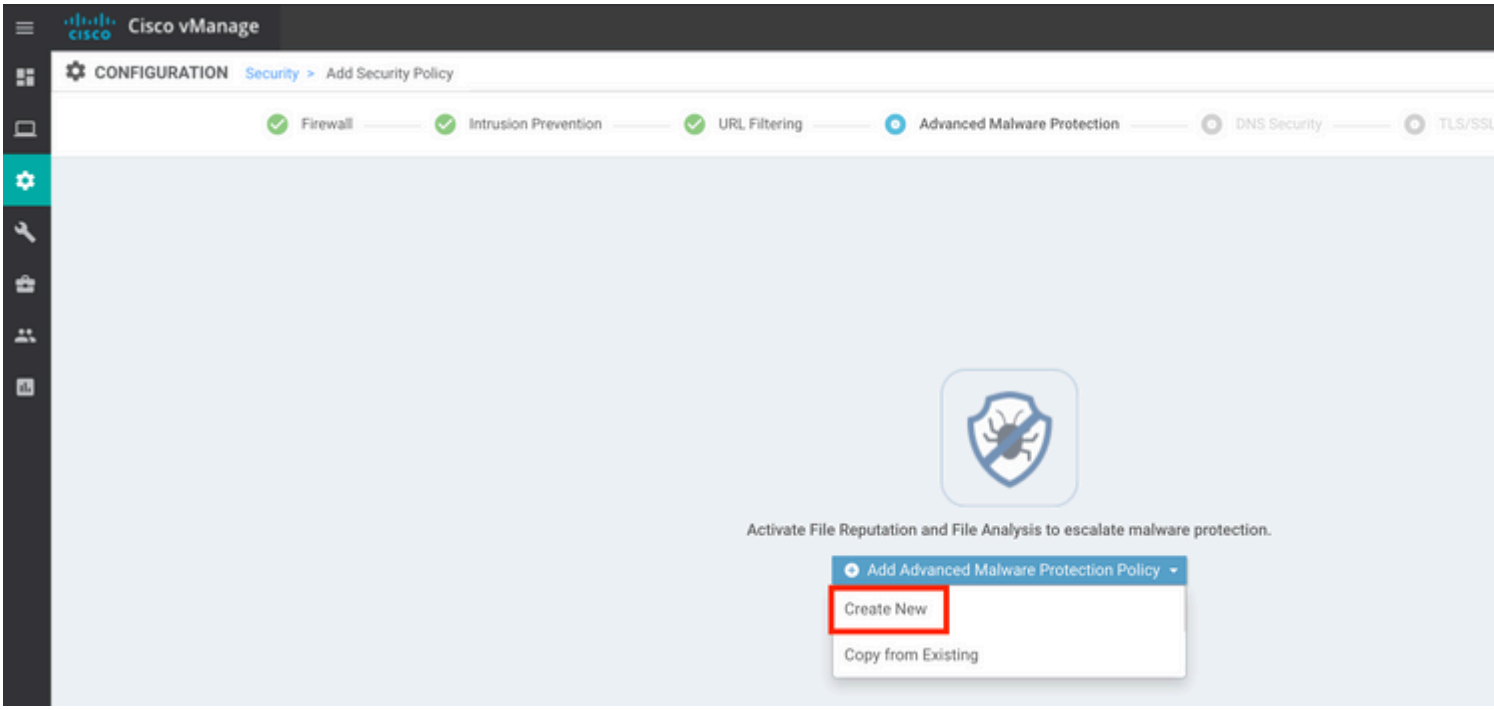
Observação: revise este documento para obter os requisitos de rede para que a conectividade do AMP/ThreatGrid funcione corretamente: Endereços IP/nomes de host obrigatórios do AMP/TG

Configurar a política de segurança do vManage

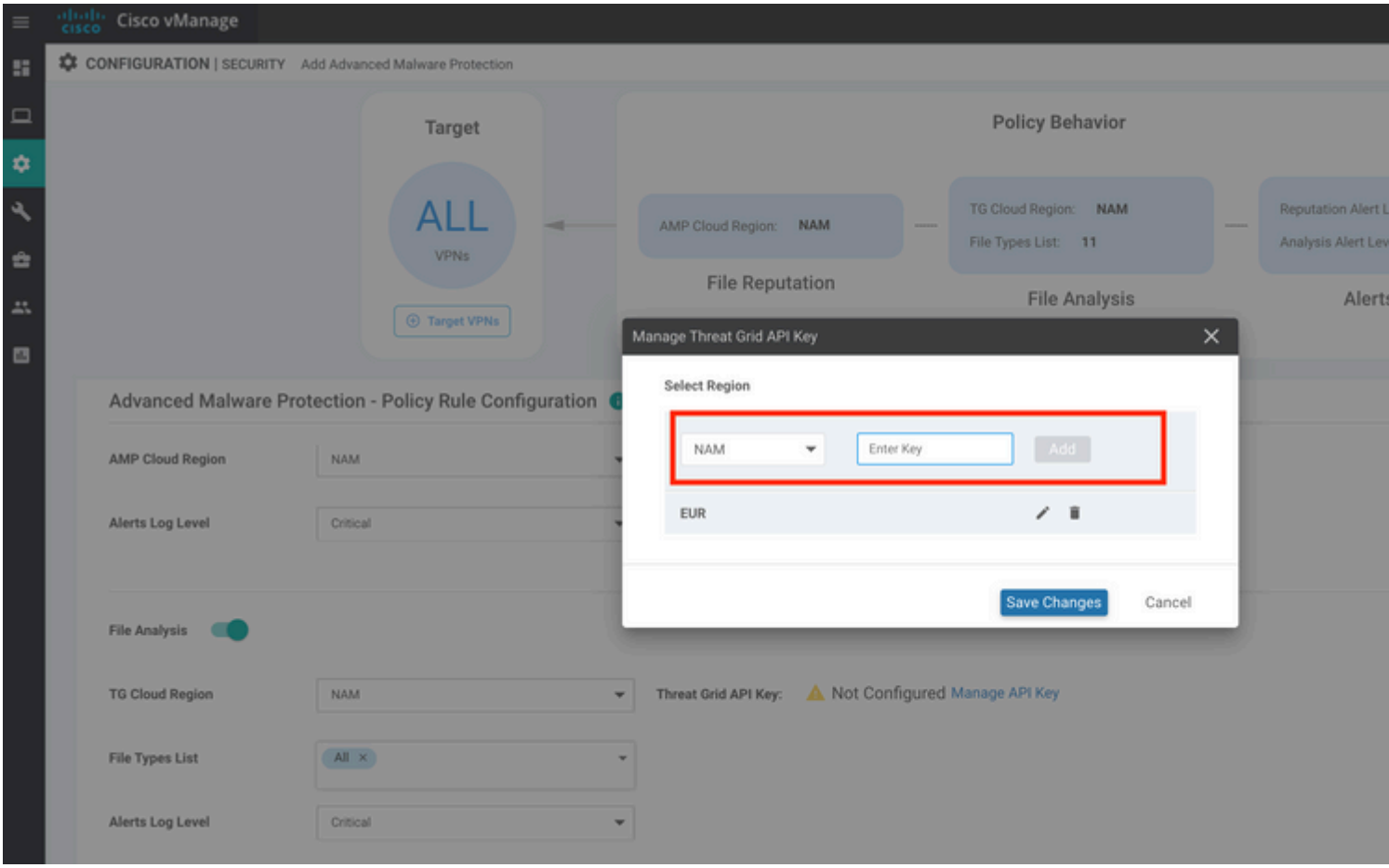
Para ativar o AMP, navegue até **Configuration** -> **Security** -> **Add Security Policy**. Selecione Direct Internet Access e selecione **Proceed** conforme mostrado na imagem.



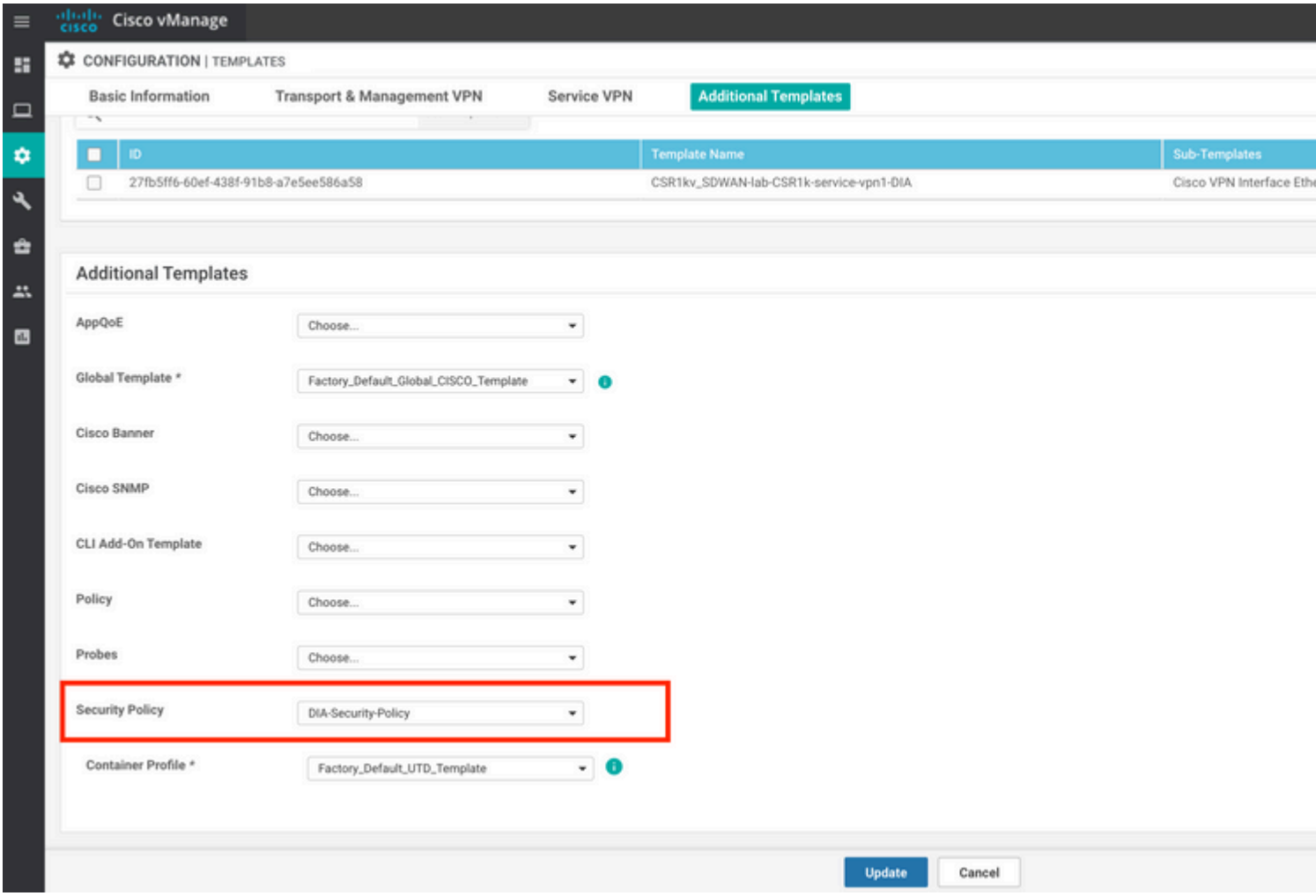
Configure os recursos de segurança conforme desejado até chegar ao recurso Proteção avançada contra malware. Adicione uma nova Política de proteção avançada contra malware.



Forneça um nome de política. Selecione uma das regiões globais da nuvem da AMP e habilite a análise de arquivos. Para a análise de arquivos com o ThreatGrid usado, escolha uma das regiões de nuvem do TG e insira a chave da API do ThreatGrid, que pode ser obtida no portal do ThreatGrid em **Minha conta do ThreatGrid.**



Depois de concluído, salve a política e adicione a política de segurança ao modelo do dispositivo em **Modelos adicionais** -> **Política de segurança**, como mostrado na imagem.



Configure o dispositivo com o modelo de dispositivo atualizado.

Verificar

Depois que o modelo do dispositivo for enviado com êxito para o dispositivo de borda, a configuração da AMP poderá ser verificada na CLI do Roteador de Borda:

<#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
```

Troubleshoot

A integração da SD-WAN AMP envolve vários componentes, conforme descrito. Portanto, quando se trata de solucionar problemas, é essencial poder estabelecer alguns pontos de demarcação importantes para limitar o problema aos componentes no fluxo de recursos:

1. **vManage.** O vManage pode enviar com êxito a política de segurança com a política AMP para o dispositivo de borda?
2. **Borda**. Depois que a política de segurança é enviada com êxito para a borda da rede, o roteador captura o arquivo sujeito à inspeção do AMP e o envia para a nuvem do AMP/TG?
3. **Nuvem AMP/TG.** Se a borda tiver enviado o arquivo para a AMP ou TG, ele obterá a resposta necessária para tomar uma decisão de permissão ou remoção?

O objetivo deste artigo é concentrar-se no dispositivo de borda (2) com as várias ferramentas de plano de dados disponíveis para ajudar a solucionar problemas com a integração da AMP no roteador de borda da WAN.

Fluxo de Troubleshooting Geral

Use esse fluxo de trabalho de alto nível para solucionar rapidamente os vários componentes envolvidos na integração do AMP com um objetivo importante para estabelecer o ponto de demarcação do problema entre o dispositivo de borda e a nuvem AMP/TG.

1. A política da AMP é enviada corretamente para o dispositivo de borda?
2. Verifique a integridade geral do contêiner UTD.
3. Verifique a reputação do arquivo e analise o status do cliente na borda.
4. Verifique se a transferência de arquivo foi desviada para o contêiner. Isso pode ser feito com o rastreamento de pacotes do Cisco IOS® XE.
5. Verifique se a borda se comunica com êxito com a nuvem AMP/TG. Isso pode ser feito com ferramentas como EPC ou packet-trace.
6. Certifique-se de que o UTD crie um cache local com base na resposta do AMP.

Estas etapas de Troubleshooting são examinadas em detalhes neste documento.

Problemas de envio de política no vManage

Como mostrado na configuração da política da AMP, a política da AMP é bastante direta sem muitas opções de configuração. Aqui estão algumas coisas comuns a serem consideradas:

1. O vManage deve ser capaz de resolver os nomes DNS para AMP e a nuvem do ThreatGrid para acesso à API. Se a configuração do dispositivo falhar no vManage após a política de AMP ser adicionada, verifique se há erros no **/var/log/nms/vmanage-server.log**.
2. Como observado no guia de configuração, o Nível de registro de alertas deixou o nível crítico padrão,

ou Aviso, se garantido. O registro em nível de informação deve ser evitado, pois pode ter um impacto negativo no desempenho.

Para verificar, acesse o BD neo4j e exiba o conteúdo da tabela vmanagedbAPIKEYNODE.

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

Integração da AMP no Cisco Edge Router

Verificar Integridade do Contêiner UTD

Use os comandos show utd para verificar a integridade geral do contêiner 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
```

Verificar status da AMP UTD

Verifique se a inspeção de arquivo está habilitada:

<#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
```

Verifique se a conexão com a nuvem da AMP está ativa:

<#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!"
```

Verifique se a conexão com o ThreatGrid está ativa:

<#root>

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

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

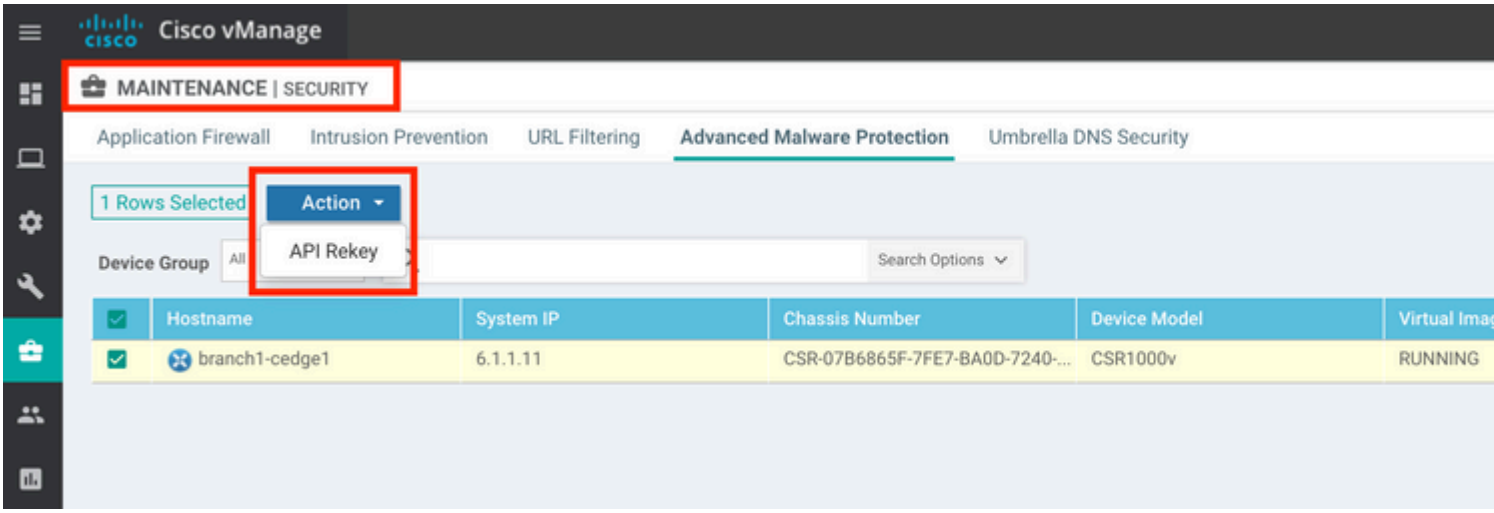
<#root>

```
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 o processo do ThreatGrid não mostrar um status de Ativo, uma rechave de API será útil. Para disparar uma nova chave de API, navegue para **Manutenção** -> **Segurança**:



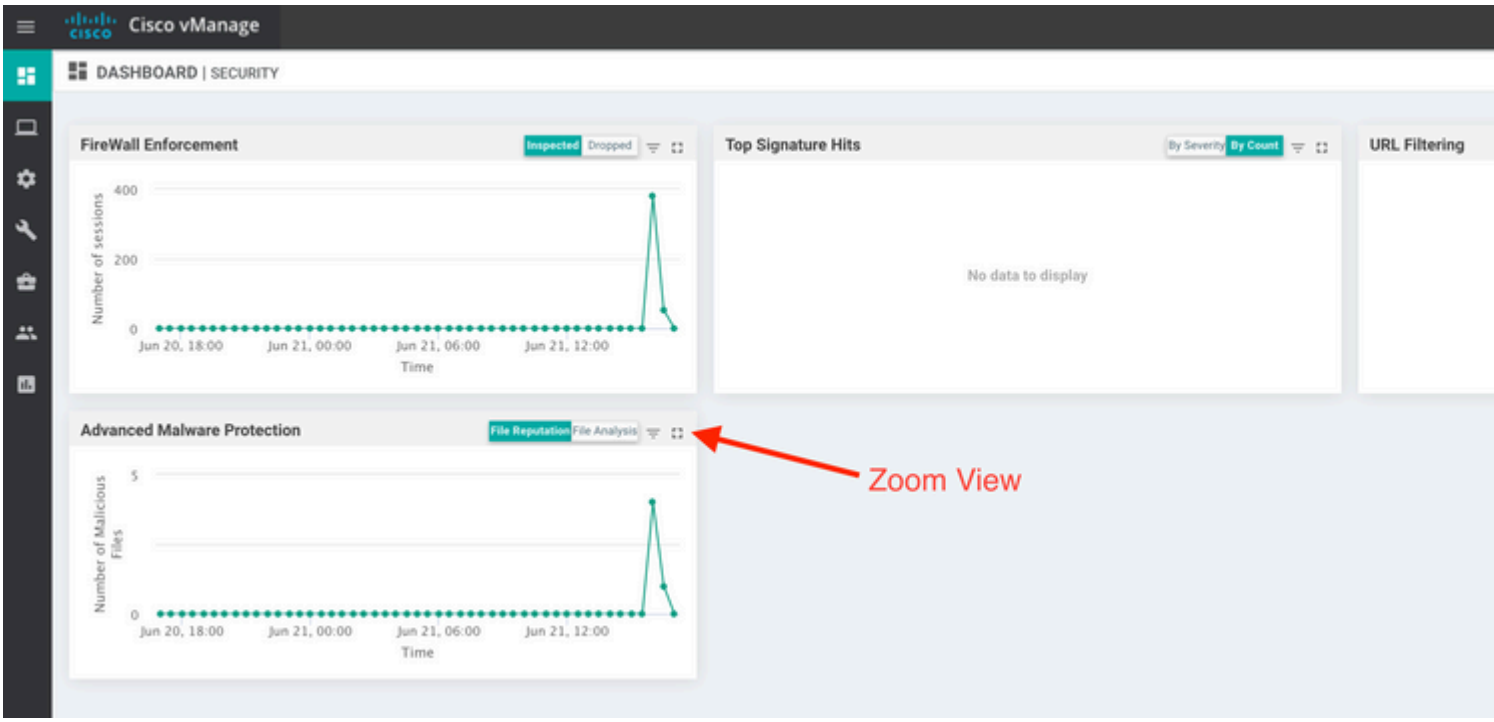
Observação: uma rechave de API aciona um envio de modelo para o dispositivo.

Monitoramento de atividade da AMP no roteador de borda da WAN

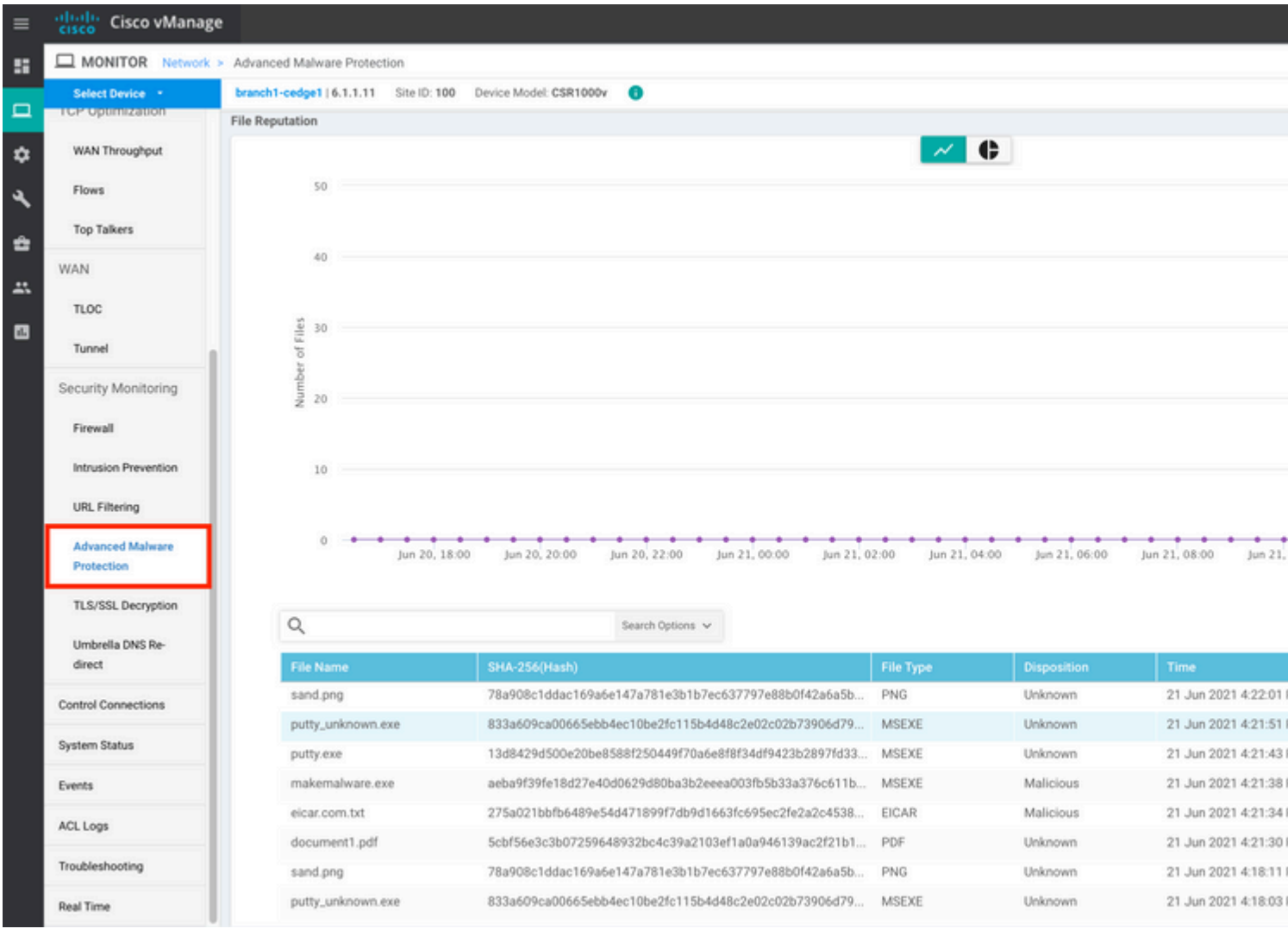
vManage

No vManage, as atividades do arquivo AMP podem ser monitoradas no painel de segurança ou na Device View.

Painel de segurança:



Exibição do dispositivo:



CLI

Verificar estatísticas de reputação do arquivo:

```
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
```

Verificar estatísticas de análise de arquivo:

```
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: estatísticas internas adicionais podem ser obtidas com o comando ***show utd engine standard statistics file-reputation vrf global internal***.

Comportamento do Dataplane

O tráfego de dataplane sujeito a inspeção de arquivo com base na política de AMP configurada é desviado para o contêiner UTD para processamento. Isso pode ser confirmado com um rastreamento de pacote usado. Se o tráfego não for desviado corretamente para o contêiner, nenhuma das ações de inspeção de arquivo subsequentes poderá ocorrer.

Cache de arquivos locais do AMP

O contêiner UTD tem um cache local de hash SHA256, tipo de arquivo, disposição e ação com base em resultados de pesquisa de nuvem AMP anteriores. O contêiner somente solicita uma disposição da nuvem AMP se o hash do arquivo não estiver no cache local. O cache local tem um TTL de 2 horas antes de ser excluído.

```
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
```

Código de disposição da AMP:

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

Código de ação da AMP:

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

Para obter o hash SHA256 completo para os arquivos, o que é muito importante para resolver problemas de um determinado resultado de arquivo, use a opção detail do 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: 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>
```

Para remover as entradas de cache local do mecanismo UTD, use o comando:

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

Executar depurações de UTD

As depurações de utd podem ser ativadas para solucionar problemas do AMP:

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

A saída da depuração pode ser recuperada diretamente do shell do sistema em **/tmp/rp/trace/vman_utd_R0-0.bin**, ou copie o arquivo de rastreamento para o sistema de arquivos do roteador com as seguintes etapas:

```
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#
```

Para exibir o log de rastreamento de 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,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>
```

> **Observação**: em 20.6.1 e posterior, a maneira de recuperar e visualizar os registros de rastreamento utd está de acordo com o fluxo de trabalho de rastreamento padrão com o **comando show logging process vman module utd** ... comando.

Verifique a comunicação da borda da rede com a nuvem

Para verificar se o dispositivo de borda se comunica com a nuvem AMP/TG, o EPC no WAN Edge Router pode ser usado para confirmar se há comunicação bidirecional de/para os serviços de nuvem:

```
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 e TG Problemas relacionados à nuvem

Depois de confirmado, o dispositivo de borda captura corretamente o arquivo e o envia para o AMP/TG para análise, mas o veredito está incorreto, ele requer a solução de problemas do AMP ou a nuvem do Threatgrid, que está fora do escopo deste documento. As informações são importantes quando problemas de integração são apresentados:

- Organização da conta do ThreatGrid
- Carimbo de data/hora
- ID de análise do dispositivo (por exemplo, CSR-07B6865F-7FE7-BA0D-7240-1BDA16328455), esse é o número do chassi do roteador de borda WAN.
- Hash SHA256 completo para o arquivo em questão

Informações Relacionadas

- Guia de configuração de segurança da SD-WAN
- Portal ThreatGrid
- Suporte Técnico e Documentação - Cisco Systems

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.