SD-WAN AMP(Advanced Malware Protection) 통합 및 문제 해결 구성

목차

소개

사전 요구 사항

- 요구 사항
- 사용되는 구성 요소

솔루션 개요

- 구성 요소
- 기능 흐름

SD-WAN AMP 통합 컨피그레이션

- vManage에서 보안 정책 구성

다음을 확인합니다.

문제 해결

- 일반 문제 해결 흐름
- vManage의 정책 푸시 문제
- Cisco Edge Router의 AMP 통합
  - UTD 컨테이너 상태 확인

소개

이 문서에서는 Cisco IOS® XE SD-WAN 라우터에서 Cisco SD-WAN AMP(Advanced Malware Protection) 통합을 구성하고 문제를 해결하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- AMP(Advanced Malware Protection)
- Cisco SD-WAN(소프트웨어 정의 WAN)

사용되는 구성 요소

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

솔루션 개요

구성 요소

SD-WAN AMP 통합은 SD-WAN 에지 보안 솔루션의 핵심 부분으로, 악성코드로부터 지사에 있는 사용자를 위한 가시성 및 보호를 목적으로 합니다.

이 제품군은 다음과 같은 제품 구성 요소로 이루어져 있습니다.

- 브랜치의 WAN 에지 라우터. UTD 컨테이너에 보안 기능이 있는 컨트롤러 모드의 Cisco IOS® XE 라우터입니다
- AMP 클라우드. AMP 클라우드 인프라는 성향으로 파일 해시 쿼리에 응답합니다
- ThreatGrid. 샌드박스 환경에서 파일에 잠재적인 악성코드가 있는지 테스트할 수 있는 클라우드 인프라

이러한 구성 요소가 함께 작동하여 AMP의 다음과 같은 주요 기능을 제공합니다.

- 파일 평판 평가

파일을 AMP(Advanced Malware Protection) 클라우드 서버와 비교하고 위협 인텔리전스 정보에 액세스하는 데 사용되는 SHA256 해시 프로세스입니다. 응답은 Clean(정상), Unknown(알 수 없음) 또는 Malicious(악성)일 수 있습니다. 응답이 Unknown이고 File Analysis(파일 분석)가 구성된 경우 추가 분석을 위해 파일이 자동으로 제출됩니다.

- 파일 분석

알려지지 않은 파일이 샌드박스 환경에서 디토네이션을 위해 TG(ThreatGrid) 클라우드에 제출됩니다. 터닝 과정에서 샌드박스는 아티팩트를 캡처하고 파일의 동작을 관찰한 다음 파일에 전체 점수를 부여합니다. 관찰 결과 및 점수를 기반으로 Threat Grid는 위협 대응을 Clean(정상) 또는 Malicious(악성)로 변경할 수 있습니다. ThreatGrid의 조사 결과는 AMP 클라우드에 다시 보고되므로 모든 AMP 사용자는 새로 발견된 악성코드로부터 보호됩니다.

- 회귀 분석

다운로드 후에도 파일에 대한 정보를 유지 관리하며, 다운로드 후 악성으로 확인된 파일에 대해 보고할 수 있습니다. 파일의 성향은 AMP 클라우드에서 얻은 새로운 위협 인텔리전스에 따라 변경될 수 있습니다. 이러한 재분류는 자동 소급 알림을 생성합니다.

현재 AMP가 통합된 SD-WAN은 다음 프로토콜에 대한 파일 검사를 지원합니다.

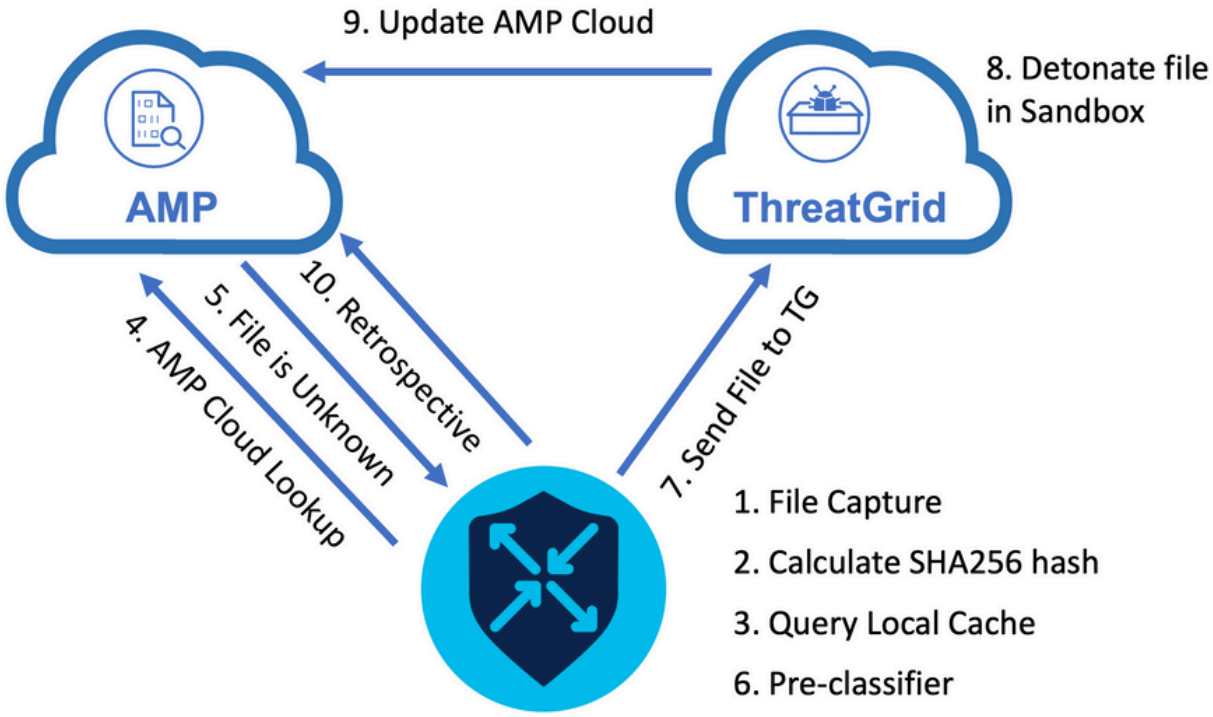
- HTTP
- SMTP
- IMAP
- POP3
- FTP
- SMB

참고: HTTPS를 통한 파일 전송은 SSL/TLS 프록시에서만 지원됩니다.

참고: 파일 분석은 전체 파일에서만 수행할 수 있으며, 일부 내용으로 나누어진 파일은 수행할 수 없습니다. 예를 들어, HTTP 클라이언트가 Range 헤더로 부분 콘텐츠를 요청하고 HTTP/1.1 206 Partial Content를 다시 가져올 때 이 경우 부분 파일 해시가 전체 파일과 크게 다르기 때문에 Snort는 부분 콘텐츠에 대한 파일 검사를 건너뜁니다.

기능 흐름

이 그림에서는 분석을 위해 파일을 ThreatGrid에 제출해야 할 때 SD-WAN AMP 통합을 위한 상위 레벨 플로우를 보여 줍니다.



표시된 플로우의 경우:

1. AMP 지원 프로토콜에 대한 파일 전송은 UTD 컨테이너에 의해 캡처됩니다.
2. 파일의 SHA256 해시가 계산됩니다.
3. UTD의 로컬 캐시 시스템에 대해 계산된 SHA256 해시를 쿼리하여 성향을 이미 알고 있으며 캐시 TTL이 만료되지 않았는지 확인합니다.
4. 로컬 캐시와 일치하는 항목이 없으면 SHA256 해시가 AMP 클라우드를 기준으로 조회되어 처리 및 반환 작업이 수행됩니다.
5. 속성이 UNKNOWN이고 응답 작업이 ACTION_SEND이면 파일이 UTD의 사전 분류 시스템을 통해 실행됩니다.
6. 사전 분류자는 파일 유형을 결정하고 파일에 액티브 컨텐트가 포함되어 있는지 확인합니다.
7. 두 조건이 모두 충족되면 파일이 ThreatGrid에 제출됩니다.
8. ThreatGrid는 샌드박스에서 파일을 폭파하고 파일에 위협 점수를 할당합니다.
9. ThreatGrid는 위협 평가를 기반으로 AMP 클라우드를 업데이트합니다.
10. 에지 디바이스는 하트비트 간격 30분을 기준으로 AMP 클라우드에 Retrospective를 쿼리합니다.

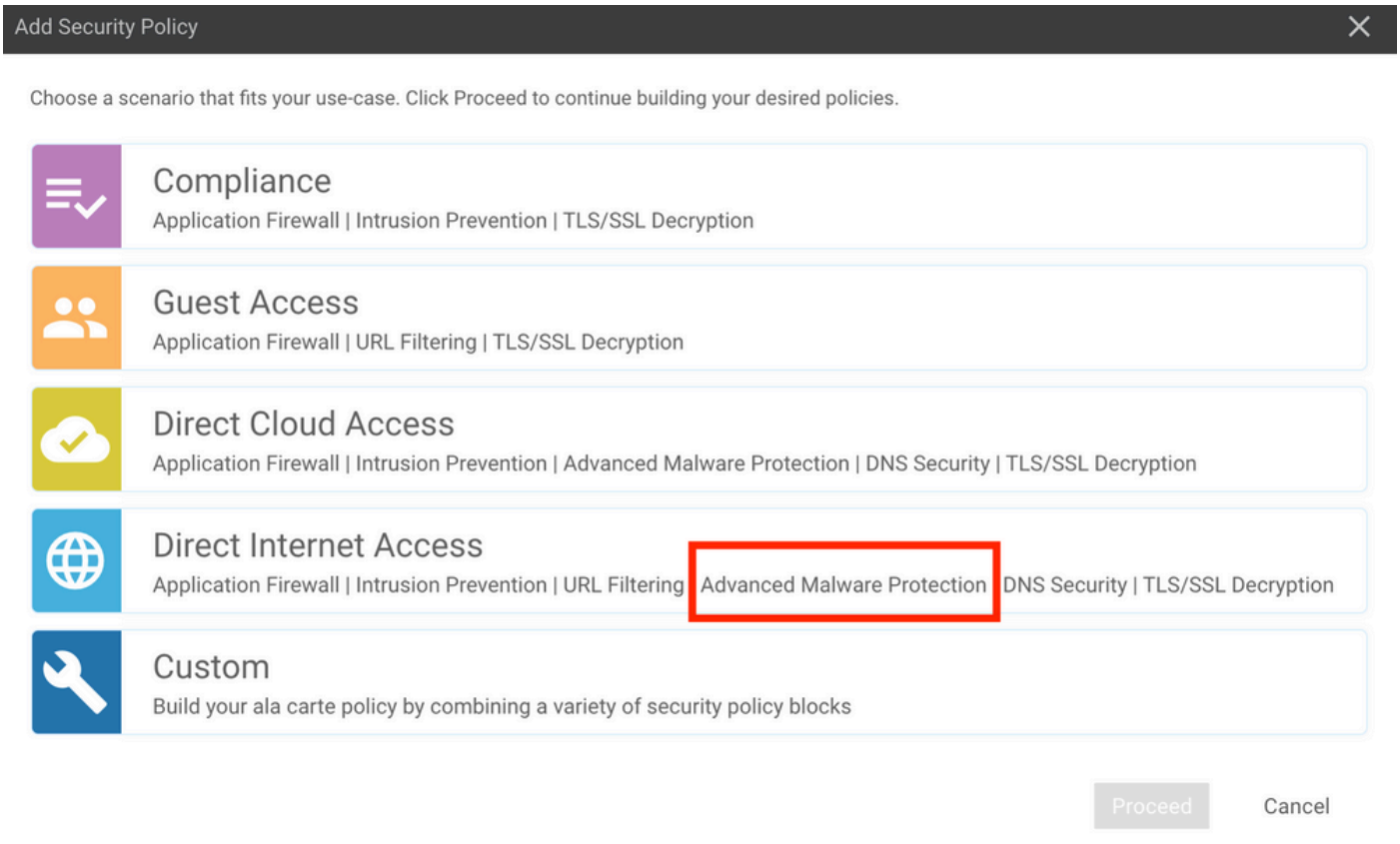
SD-WAN AMP 통합 컨피그레이션

참고: AMP 기능을 구성하기 전에 보안 가상 이미지를 vManage에 업로드해야 합니다. 자세한 내용을 보려면 Security Virtual Image(보안 가상 이미지)로 이동합니다.

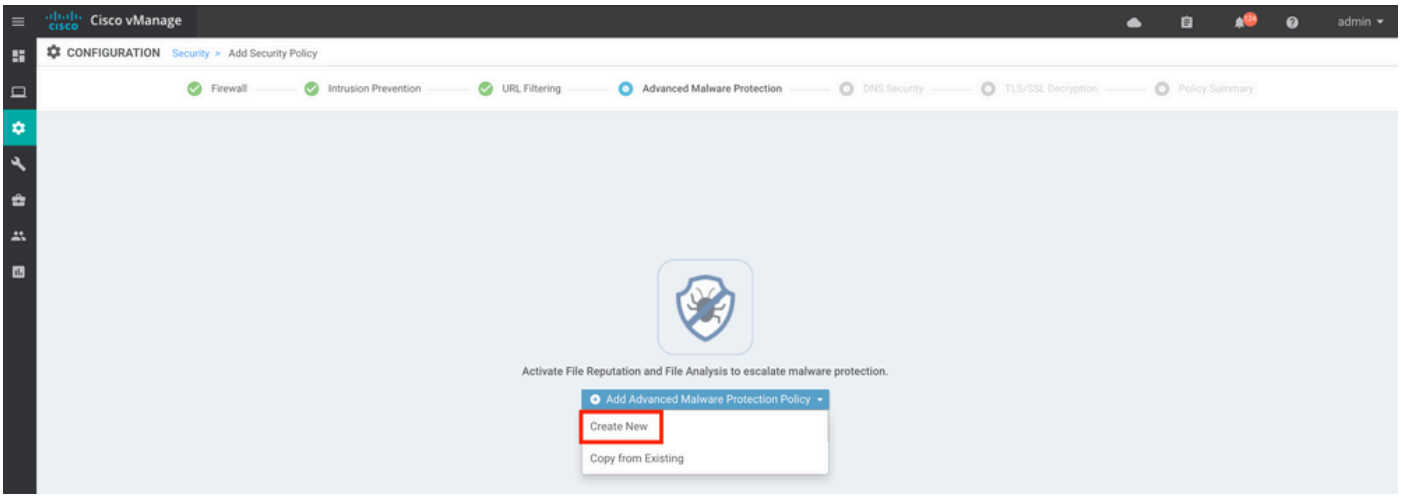
참고: AMP/ThreatGrid 연결이 올바르게 작동하려면 이 문서의 네트워크 요구 사항(AMP/TG 필수 IP 주소/호스트 이름)을 검토하십시오

vManage에서 보안 정책 구성

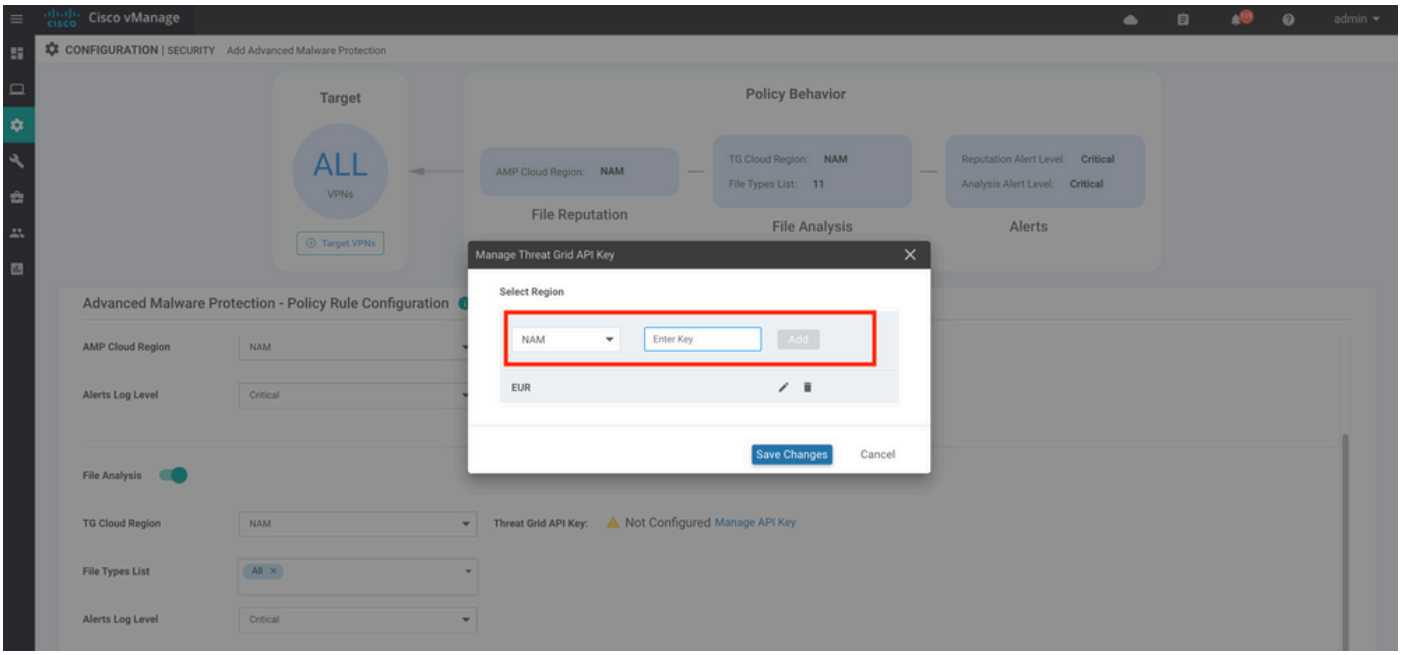
AMP를 활성화하려면 Configuration(컨피그레이션) -> Security(보안) -> Add Security Policy(보안 정책 추가)로 이동합니다. Direct Internet Access(직접 인터넷 액세스)를 선택하고 이미지에 표시된 대로 Proceed(진행)를 선택합니다.



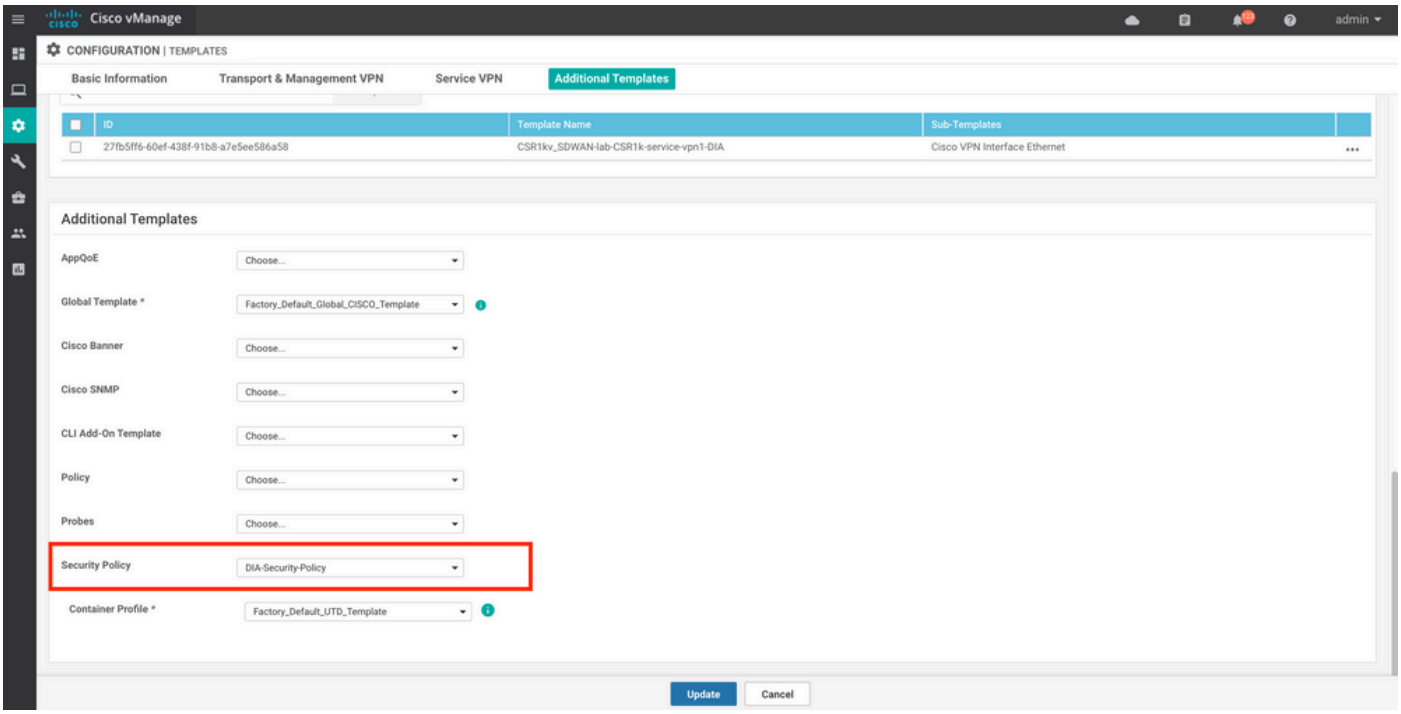
Advanced Malware Protection 기능에 도달할 때까지 원하는 대로 보안 기능을 구성합니다. 새 Advanced Malware Protection 정책을 추가합니다.



정책 이름을 제공합니다. 전역 AMP 클라우드 영역 중 하나를 선택하고 File Analysis(파일 분석)를 활성화합니다. File Analysis with ThreatGrid를 사용하려면 TG 클라우드 영역 중 하나를 선택하고 ThreatGrid API 키를 입력합니다. 이 키는 ThreatGrid 포털의 My ThreatGrid 어카운트 아래에 있습니다.



완료되면 정책을 저장하고 이미지에 표시된 대로 Additional Templates -> Security Policy(추가 템플릿 -> 보안 정책) 아래의 Device(디바이스) 템플릿에 이 보안 정책을 추가합니다.



업데이트된 디바이스 템플릿으로 디바이스를 구성합니다.

다음을 확인합니다.

디바이스 템플릿이 에지 디바이스로 성공적으로 푸시되면 에지 라우터 CLI에서 AMP 컨피그레이션을 확인할 수 있습니다.

<#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
```

문제 해결

SD-WAN AMP 통합에는 설명된 대로 많은 구성 요소가 포함됩니다. 따라서 트러블슈팅에 있어서는 몇 가지 주요 경계점을 설정하여 문제를 기능 흐름의 구성 요소로 좁힐 수 있어야 합니다.

1. vManage. vManage에서 AMP 정책이 포함된 보안 정책을 에지 디바이스에 성공적으로 푸시할 수 있습니까?
2. 에지. 보안 정책이 에지로 성공적으로 푸시되면 라우터는 AMP 검사 대상 파일을 캡처하여 AMP/TG 클라우드로 전송합니까?
3. AMP/TG 클라우드. 에지가 파일을 AMP 또는 TG로 보낸 경우 허용 또는 삭제 결정을 내리는 데 필요한 응답을 받습니까?

이 문서에서는 WAN 에지 라우터의 AMP 통합 문제를 해결하는 데 도움이 되는 다양한 데이터 플레인 도구를 사용하여 에지 장치(2)를 중점적으로 살펴봅니다.

일반 문제 해결 흐름

이 고급 워크플로를 사용하여 에지 장치와 AMP/TG 클라우드 간 문제의 경계점을 설정하는 주요 목표로 AMP 통합과 관련된 다양한 구성 요소의 문제를 신속하게 해결합니다.

1. AMP 정책이 에지 디바이스에 올바르게 푸시됩니까?
2. UTD 컨테이너의 일반적인 상태를 확인합니다.
3. 에지에서 파일 평판을 확인하고 클라이언트 상태를 분석합니다.
4. 파일 전송이 컨테이너로 전환되는지 확인합니다. 이 작업은 Cisco IOS® XE 패킷 추적을 통해 수행할 수 있습니다.
5. 에지가 AMP/TG 클라우드와 성공적으로 통신하는지 확인합니다. EPC 또는 패킷 추적과 같은 툴을 사용하여 이 작업을 수행할 수 있습니다.
6. UTD가 AMP 응답을 기반으로 로컬 캐시를 생성하는지 확인합니다.

이러한 트러블슈팅 단계는 이 문서에서 자세히 살펴봅니다.

vManage의 정책 푸시 문제

AMP 정책 컨피그레이션에서 보여주는 것처럼, AMP 정책은 많은 컨피그레이션 옵션 없이도 간단합니다. 다음은 몇 가지 일반적인 고려 사항입니다.

1. vManage는 API 액세스를 위한 AMP 및 ThreatGrid 클라우드의 DNS 이름을 확인할 수 있어야 합니다. AMP 정책을 추가한 후 vManage에서 디바이스 컨피그레이션이 실패할 경우 /var/log/nms/vmanage-server.log에서 오류를 확인하십시오.
2. 컨피그레이션 가이드에서 설명한 것처럼 Alerts Log Level(경고 로그 레벨)은 기본 Critical(위험) 레벨 또는 Warning(경고)이 보장되는 경우 Warning(경고)을 그대로 유지합니다. 정보 레벨 로깅은 성능에 부정적인 영향을 미칠 수 있으므로 피해야 합니다.

확인하려면 neo4j DB에 액세스하여 vmanagedbAPIKEYNODE 테이블의 내용을 확인합니다.

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

Cisco Edge Router의 AMP 통합

UTD 컨테이너 상태 확인

show utd 명령을 사용하여 전반적인 UTD 컨테이너 상태를 확인합니다.

```
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 상태 확인

파일 검사가 활성화되었는지 확인합니다.

<#root>

```
branch1-edge1#show sdwan utd dataplane config
 utd-dp config context 0
 context-flag 25427969
 engine Standard
 state enabled
 sn-redirect fail-open
 redirect-type divert
 threat-inspection not-enabled
 defense-mode not-enabled
 domain-filtering not-enabled
 url-filtering not-enabled
 all-interface enabled
 file-inspection enabled

utd-dp config context 1
 context-flag 25559041
 engine Standard
 state enabled
 sn-redirect fail-open
 redirect-type divert
 threat-inspection enabled
 defense-mode IDS
 domain-filtering not-enabled
```

```
 url-filtering not-enabled
 all-interface enabled
 file-inspection enabled
```

AMP 클라우드에 대한 연결이 설정되어 있는지 확인합니다.

<#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!"
```

ThreatGrid에 대한 연결이 설정되어 있는지 확인합니다.

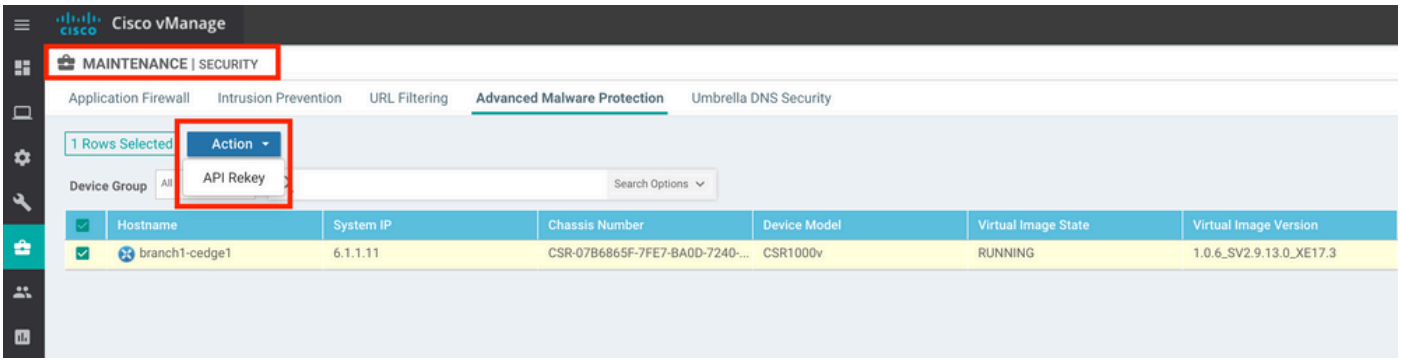
<#root>

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

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

<#root>

```
branch1-edge1#show sdwan utd file analysis
utd-oper-data utd-file-analysis-status status tg-client-stat-up

utd-oper-data utd-file-analysis-status backoff-interval 0
utd-oper-data utd-file-analysis-status message "TG Process Up"
```

ThreatGrid 프로세스에 Up 상태가 표시되지 않으면 API rekey가 도움이 됩니다. API rekey를 트리거하려면 Maintenance -> Security로 이동합니다.



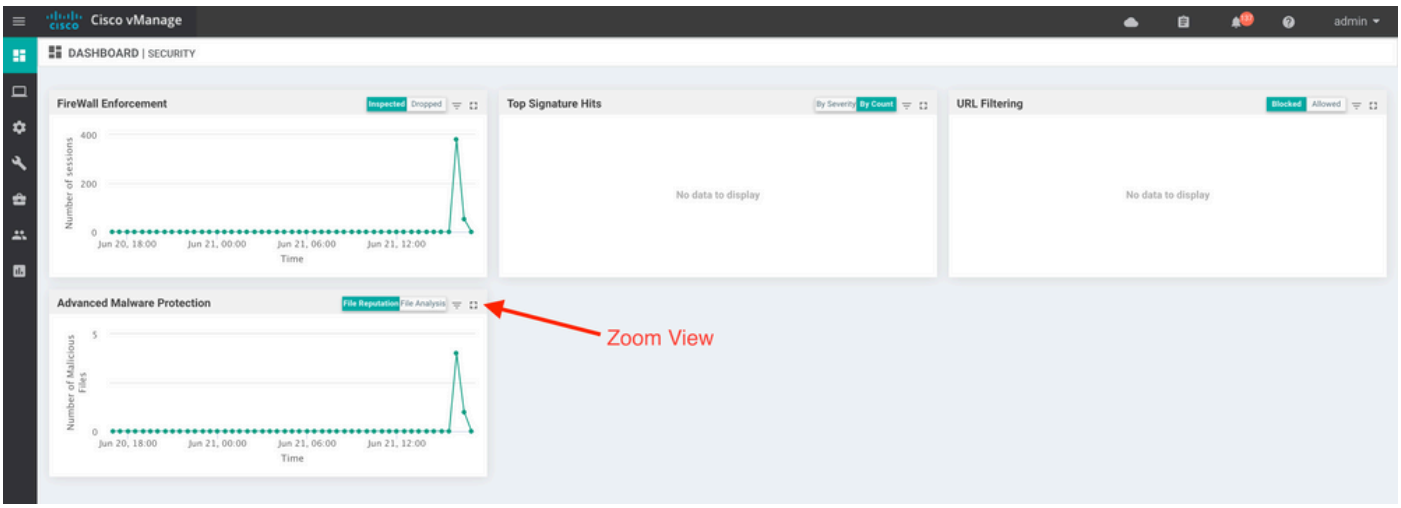
참고: API rekey는 디바이스에 대한 템플릿 푸시를 트리거합니다.

WAN 에지 라우터의 AMP 활동 모니터링

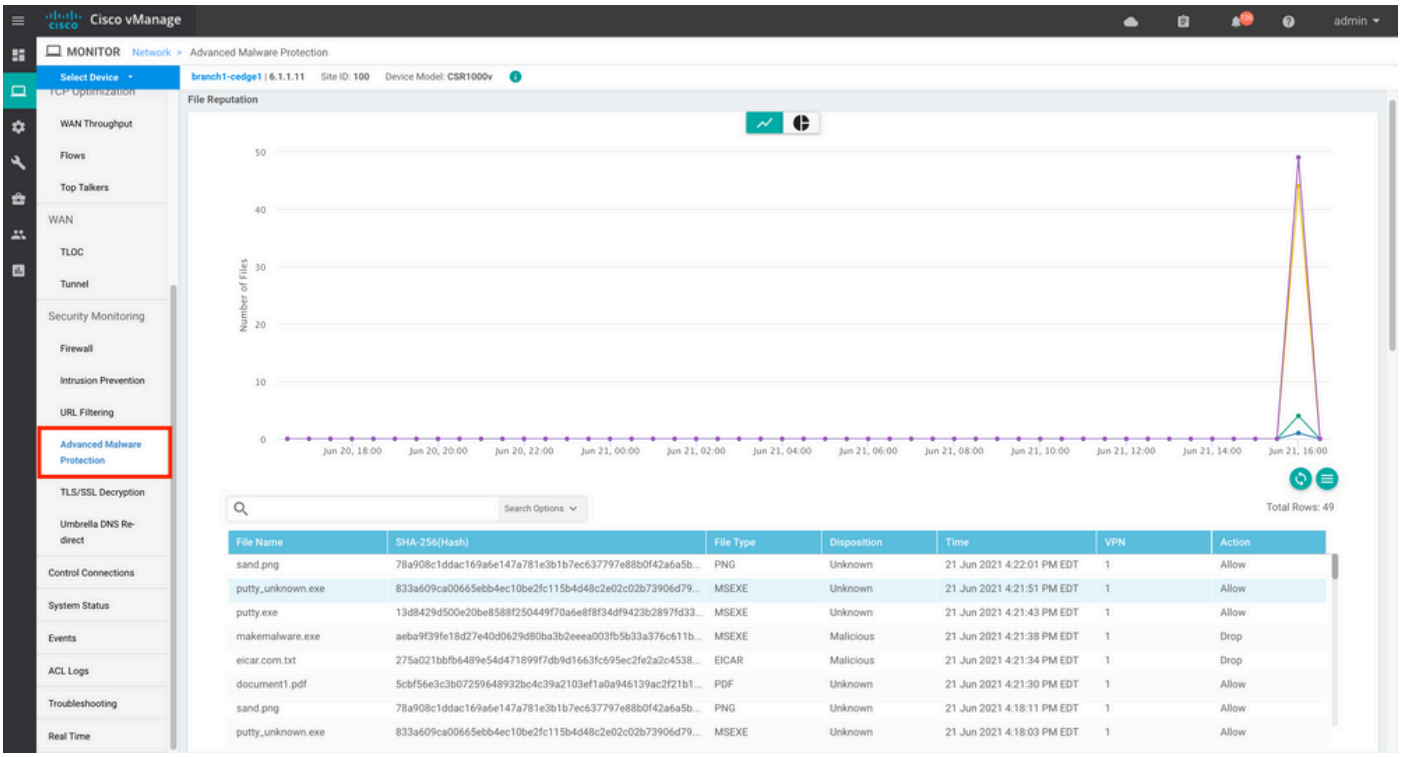
vManage

vManage의 보안 대시보드 또는 Device View에서 AMP 파일 활동을 모니터링할 수 있습니다.

보안 대시보드:



장치 보기:



CLI

파일 평판 통계 확인:

```
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
```

파일 분석 통계 확인:

```
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
```

참고: 추가 내부 통계는 show utd engine standard statistics file-reputation vrf global internal 명령을 사용하여 얻을 수 있습니다.

데이터 플레인 동작

구성된 AMP 정책에 따라 파일 검사의 대상이 되는 데이터 플레인 트래픽은 처리를 위해 UTD 컨테이너로 전환됩니다. 이는 사용된 패킷 추적을 통해 확인할 수 있습니다. 트래픽이 컨테이너에 제대로 전환되지 않으면 후속 파일 검사 작업이 수행되지 않습니다.

AMP 로컬 파일 캐시

UTD 컨테이너에는 이전 AMP 클라우드 조회 결과에 따른 SHA256 해시, 파일 유형, 성향 및 작업의 로컬 캐시가 있습니다. 컨테이너는 파일 해시가 로컬 캐시에 없는 경우에만 AMP 클라우드에서 처리를 요청합니다. 로컬 캐시의 TTL은 2시간이며, 이 시간이 지나면 캐시가 삭제됩니다.

```
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 분류 코드:

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

AMP 작업 코드:

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

파일에 대한 전체 SHA256 해시를 가져오려면 다음 명령의 detail 옵션을 사용합니다. 이는 특정 파일 판정 문제를 해결하기 위해 매우 중요합니다.

```
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>
```

UTD 엔진 로컬 캐시 항목을 제거하려면 다음 명령을 사용합니다.

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

UTD 디버그 실행

AMP 문제를 트러블슈팅하기 위해 utd 디버그를 활성화할 수 있습니다.

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

디버그 출력은 /tmp/rp/trace/vman_utd_R0-0.bin에서 시스템 셸에서 직접 검색하거나 다음 단계와 함께 추적 파일을 라우터 파일 시스템에 복사할 수 있습니다.

```
branch1-edge1#app-hosting move appid utd log to bootflash:
Successfully moved tracelog to bootflash:/iox_utd_R0-0_R0-0.5113_0.20210622110241.bin.gz
branch1-edge1#
```

UTD 추적 로그를 보려면

```
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_unk
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>
```

참고: 20.6.1 이상에서는 utd tracelogs를 검색하고 보는 방법이 show logging process vman module utd ... 명령의 표준 추적 워크플로와 일치합니다.

에지에서 클라우드로의 통신 확인

에지 디바이스가 AMP/TG 클라우드와 통신하는지 확인하기 위해 WAN 에지 라우터의 EPC를 사용하여 클라우드 서비스와 양방향 통신이 이루어졌는지 확인할 수 있습니다.

```
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 및 TG 클라우드 관련 문제

엣지 디바이스가 파일을 올바르게 캡처하여 분석을 위해 AMP/TG에 전송하지만 판정이 정확하지 않은 것으로 확인되면 AMP 트러블슈팅 또는 Threatgrid 클라우드가 필요하며, 이는 이 문서의 범위를 벗어납니다. 이 정보는 통합 문제가 발생할 때 중요합니다.

- ThreatGrid 어카운트 조직
- 타임스탬프
- 디바이스 분석 ID(예: CSR-07B6865F-7FE7-BA0D-7240-1BDA16328455)는 WAN 에지 라우터의 섀시 번호입니다.
- 문제의 파일에 대한 SHA256 해시 완료

관련 정보

- SD-WAN 보안 컨피그레이션 가이드
- ThreatGrid 포털
- 기술 지원 및 문서 – Cisco Systems

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.