تكوين دمج الحماية المتقدمة من البرامج الضارة (AMP) عبر شبكة SD-WAN واستكشاف الأخطاء وإصلاحها

المحتويات

المقدمة

يصف هذا المستند كيفية تكوين الحماية المتقدمة من البرامج الضارة (AMP) من Cisco SD-WAN واستكشاف أخطاء التكامل والاتصال على موجه Cisco IOS® XE SD-WAN.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- الحماية المتقدمة من البرامج الضارة
- شبكة منطقة واسعة معرفة بالبرامج من Cisco (SD-WAN)

المكونات المستخدمة

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

نظرة عامة على الحل

المكونات

يعد دمج الحماية المتقدمة (AMP) عبر شبكة SD-WAN جزءا ال يتجزأ من حل الأمان الطرفي القائم على شبكة SD-WAN الذي يهدف إلى رؤية المستخدمين في أحد فروع البرامج الضارة وحمايتهم منه.

يتكون من مكونات المنتج التالية:

- موجه WAN Edge في فرع. هذا هو موجه Cisco IOS® XE في وضع وحدة التحكم مع ميزات الأمان في حاوية UTD
- مجموعة الحماية المتقدمة (AMP). تستجيب البنية الأساسية لشبكة AMP لاستعلامات تجزئة الملفات بإرجاع
- شبكة تهديدات الحماية. البنية الأساسية للسحابة التي يمكنها إختبار ملف للبرامج الضارة المحتملة في بيئة وضع الحماية

تعمل هذه المكونات معا لتوفير إمكانات الميزات الرئيسية التالية ل AMP:

- تقييم سمعة الملف

عملية تجزئة SHA256 المستخدمة لمقارنة الملف بخادم الشبكة "الحماية المتقدمة من البرامج الضارة" (AMP) والوصول إلى المعلومات الاستخباراتية الخاصة بالتهديدات الخاصة به. يمكن أن تكون الاستجابة نظيفة أو غير معروفة أو ضارة. إذا كانت الاستجابة غير معروفة، وإذا تم تكوين تحليل الملف، يتم إرسال الملف تلقائيا لمزيد من التحليل.

- تحليل الملفات

يتم إرسال ملف غير معروف إلى سحابة ThreatGrid (TG) للتفجير في بيئة وضع الحماية. خلال عملية التفجير، تلتقط أداة تحديد الوصول التداخل وتالحظ سلوكيات الملف، ثم تعطي الملف عالمة كاملة. بناء على المالحظات والعالمات، يمكن لشبكة التهديد تغيير إستجابة التهديد إلى نظيفة أو خبيثة. يتم إرسال نتائج ThreatGrid مرة أخرى إلى سحابة AMP حتى يتم حماية جميع مستخدمي AMP من البرامج الضارة المكتشفة حديثا.

- إستذكار

تحتفظ بمعلومات حول الملفات حتى بعد تنزيلها، يمكننا الإبلاغ عن الملفات التي تم تحديدها على أنها ضارة بعد تنزيلها. يمكن أن تتغير مصير الملفات استنادا إلى معلومات التهديد الجديدة التي حصلت عليها سحابة AMP. إن عملية إعادة التصنيف هذه تعمل على توليد إخطارات تلقائية بأثر رجعي.

حاليا، يدعم SD-WAN مع دمج AMP فحص الملفات للبروتوكوالت:

- HTTP
- SMTP
- إيماب
- POP3
- FTP

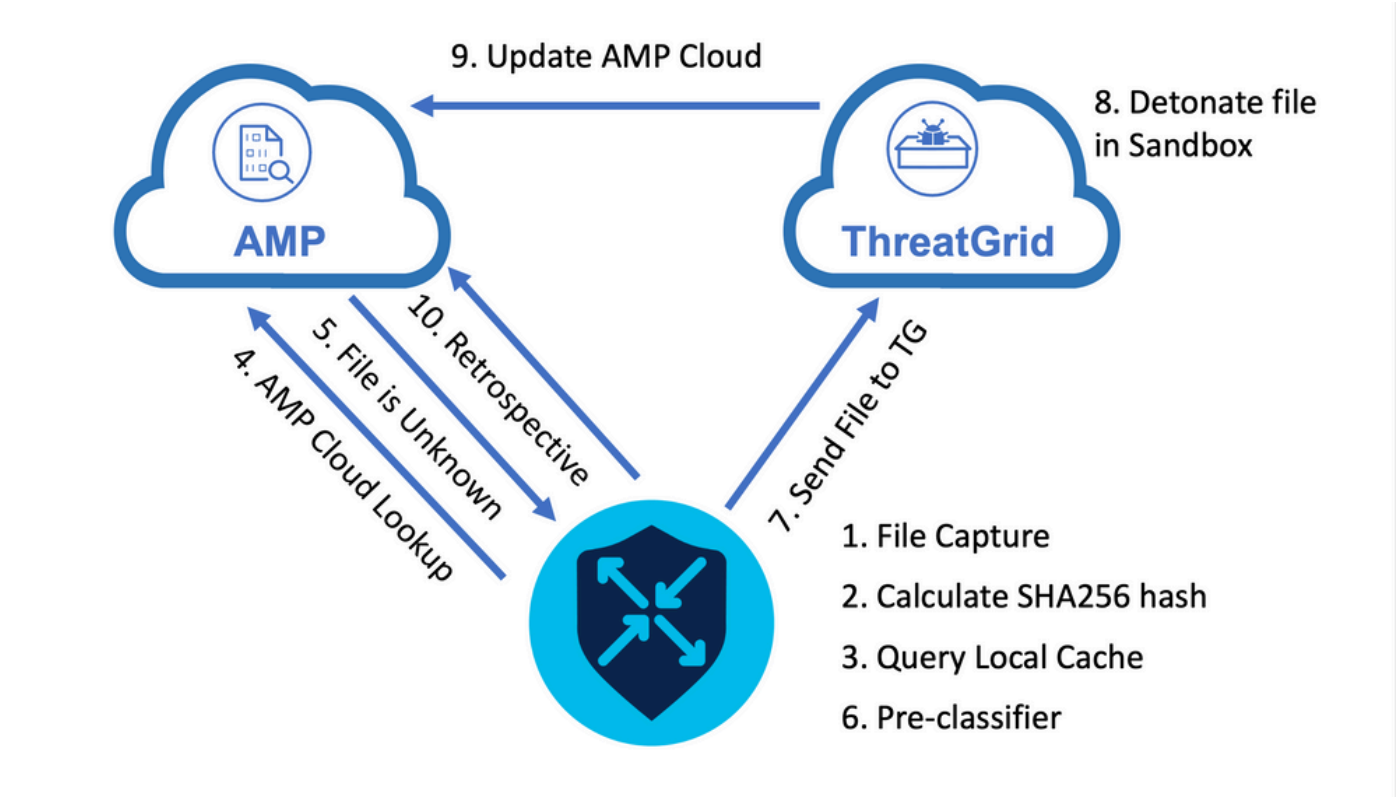
- الشركات الصغيرة والمتوسطة

ملاحظة: يتم دعم نقل الملفات عبر HTTPS فقط باستخدام وكيل SSL/TLS .

ملاحظة: يمكن إجراء تحليل الملف على ملف كامل فقط، وليس الملف المقسم إلى محتوى جزئي. على سبيل المثال، عند طلب عميل HTTP محتوى جزئي مع رأس النطاق والحصول على المحتوى الجزئي HTTP/1.1 206 مرة أخرى. في هذه الحالة، لأن تجزئة الملف الجزئية تختلف بشكل كبير عن الملف الكامل، فإن Snort يتخطى فحص الملف للمحتوى الجزئي.

تدفق الميزات

توضح الصورة التدفق عالي المستوى لتكامل SD-WAN AMP عندما يلزم إرسال ملف إلى ThreatGrid لتحليله.



للتدفق الظاهر:

1. يتم التقاط نقل الملفات للبروتوكولات المدعومة من AMP بواسطة حاوية UTD.
2. يتم حساب تجزئة SHA256 للملف.
3. يتم الاستعلام عن تجزئة SHA256 المحسوبة في مقابل نظام ذاكرة التخزين المؤقت المحلي في UTD لمعرفة ما إذا كان المصير النهائي معروفا بالفعل ولم تنته صلاحية ذاكرة التخزين المؤقت TTL.
4. إذا لم يكن هناك تطابق مع ذاكرة التخزين المؤقت المحلية، يتم بعد ذلك البحث عن تجزئة SHA256 مقابل سحابة AMP لاتخاذ إجراء المصير النهائي والإرجاع.
5. إذا كان المصير النهائي غير معروف وكان إجراء الاستجابة هو ACTION_SEND، يتم تشغيل الملف من خلال نظام التصنيف المسبق في UTD.

6. يحدد المصنف المسبق نوع الملف ويتحقق أيضا من صحة ما إذا كان الملف يحتوي على محتوى نشط.
7. في حالة استيفاء كل الشرطين، يتم إرسال الملف إلى ThreatGrid.
8. يقوم ThreatGrid بتفجير الملف في وضع حماية وتعيين درجة تهديد للملف.
9. تقوم ThreatGrid بتحديث مجموعة الحماية المتقدمة (AMP) استنادا إلى تقييم التهديد.
10. يستعلم الجهاز الطرفي عن سحابة AMP للاستعلام بأثر رجعي استنادا إلى الفاصل الزمني لنبضات القلب الذي يبلغ 30 دقيقة.

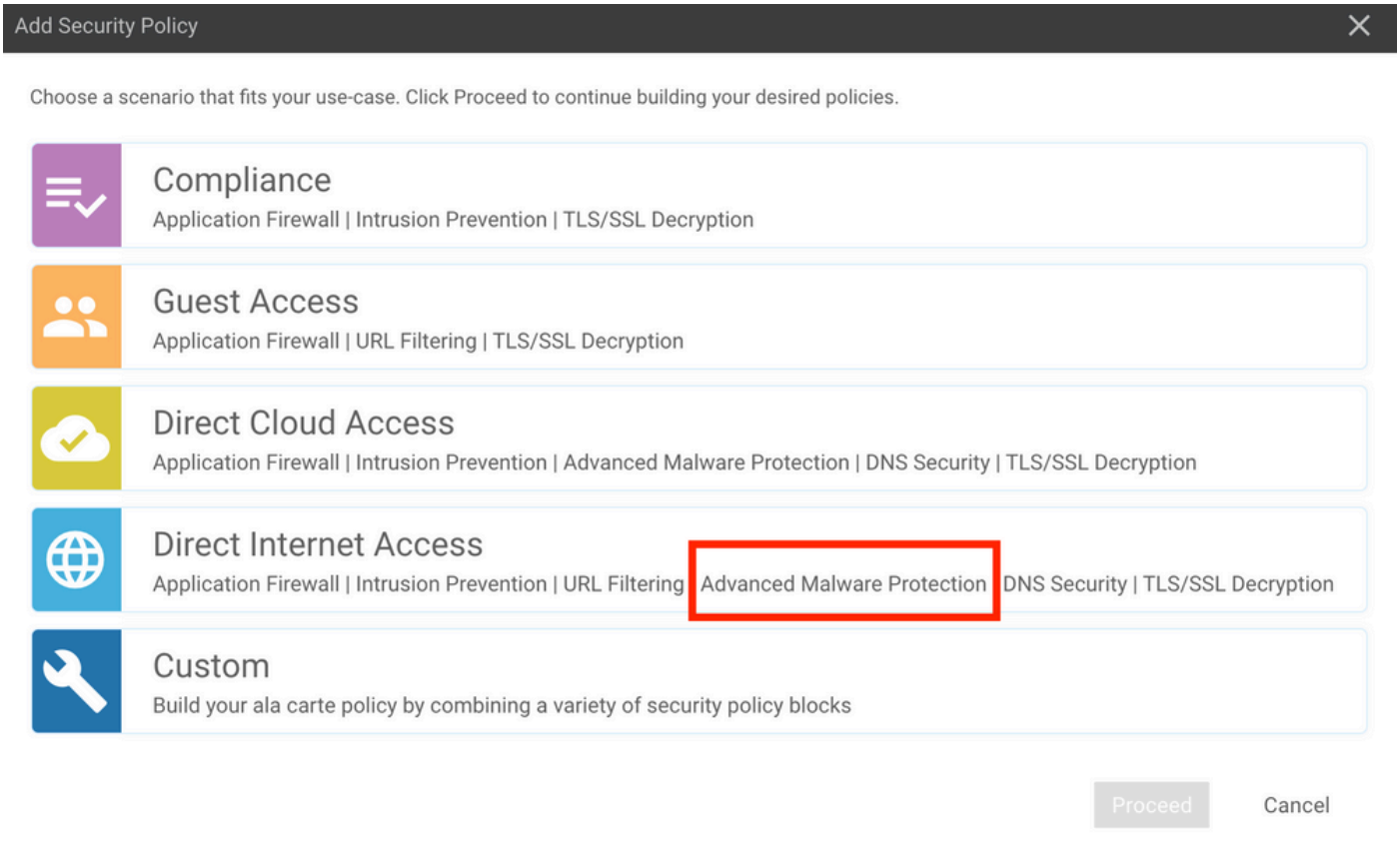
تكوين تكامل SD-WAN AMP

ملاحظة: يجب تحميل صورة الأمان الظاهرية إلى vManage قبل تكوين ميزة AMP. لمزيد من التفاصيل، انتقل إلى صورة الأمان الظاهرية .

ملاحظة: راجع هذا المستند لمتطلبات الشبكة لاتصال AMP/ThreatGrid ليعمل بشكل صحيح: عناوين IP/أسماء المضيفة المطلوبة لـ AMP/TG

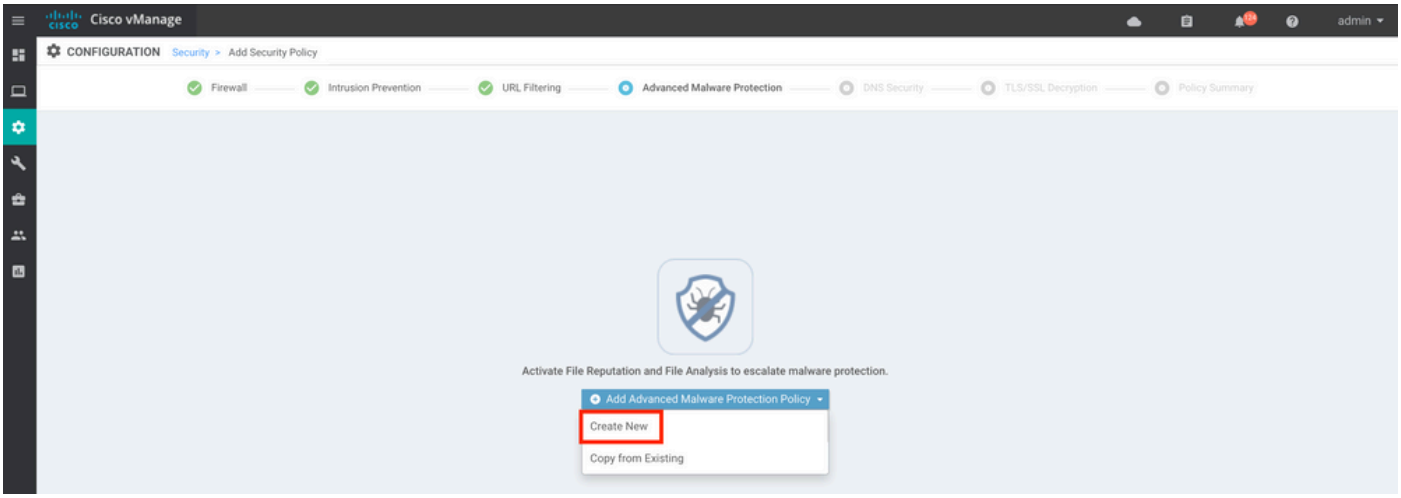
تكوين نهج الأمان من vManage

لتمكين AMP، انتقل إلى التكوين ->الأمان ->إضافة نهج الأمان. حدد الوصول المباشر إلى الإنترنت وحدد متابعة كما هو موضح في الصورة.

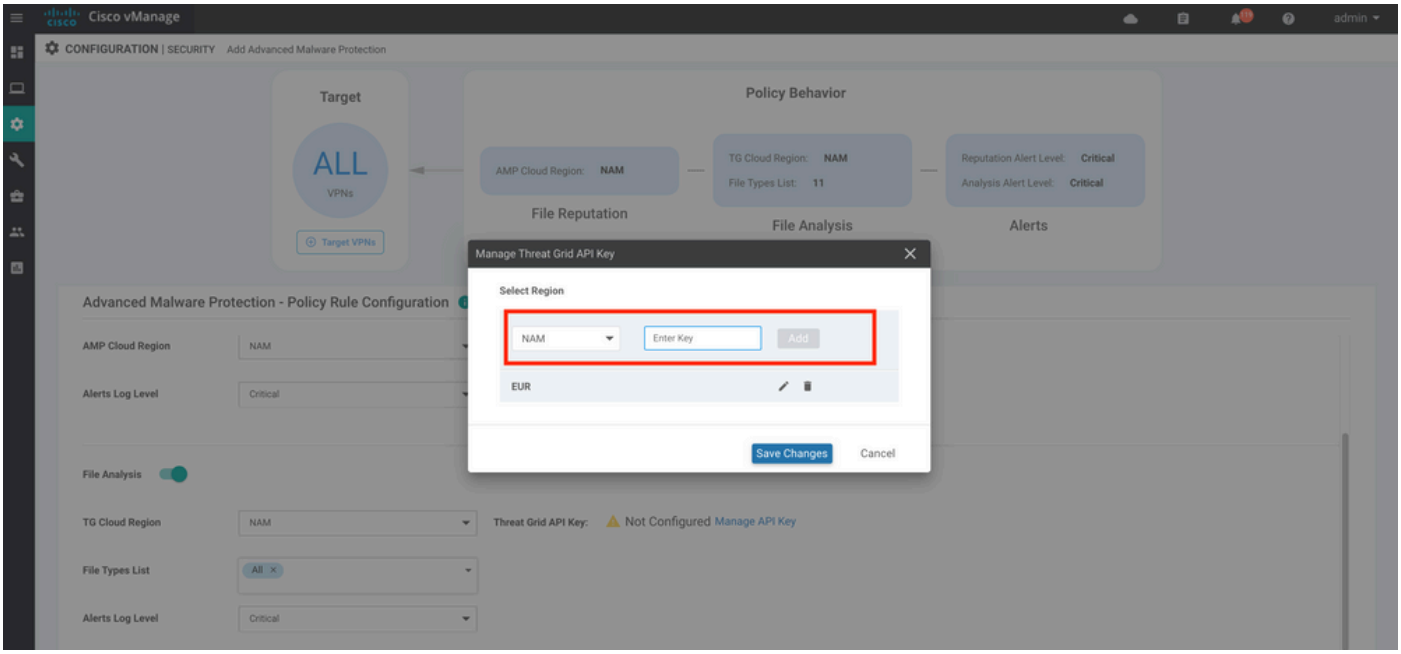


قم بتكوين ميزات الأمان حسب الرغبة حتى تصل إلى ميزة "الحماية المتقدمة من البرامج

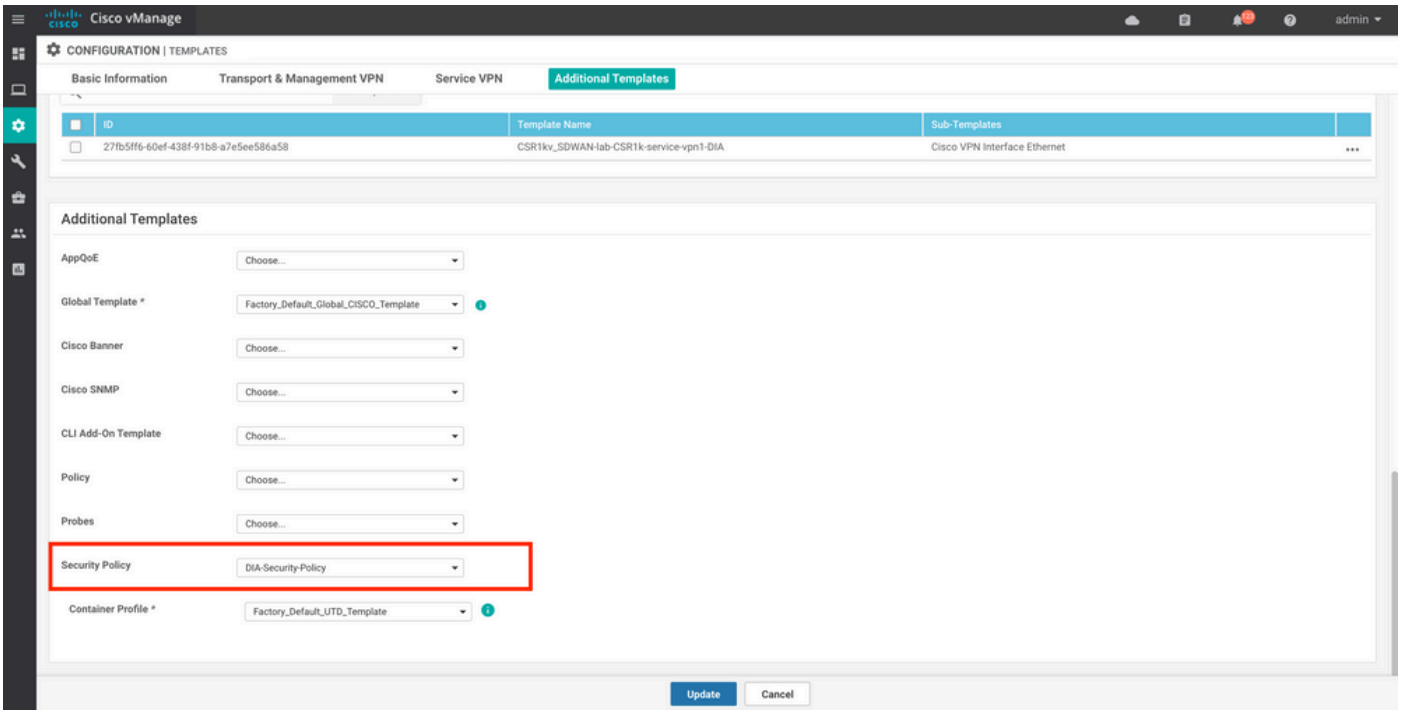
الضارة". إضافة نهج حماية متقدم جديد للبرامج الضارة.



قم بتوفير اسم نهج. حدد إحدى مناطق سحابة AMP العمومية وقم بتمكين تحليل الملفات. لتحليل الملفات باستخدام ThreatGrid، أختر إحدى مناطق Tg Cloud، وأدخل مفتاح API ل ThreatGrid، والذي يمكن الحصول عليه من مدخل ThreatGrid تحت حساب ThreatGrid الخاص بي.



بمجرد الانتهاء، احفظ النهج وأضف نهج الأمان هذا إلى قالب الجهاز ضمن قوالب إضافية ->نهج الأمان كما هو موضح في الصورة.



قم بتكوين الجهاز باستخدام قالب الجهاز الذي تم تحديثه.

التحقق من الصحة

بمجرد دفع قالب الجهاز بنجاح إلى جهاز الحافة، يمكن التحقق من تكوين AMP من واجهة سطر الأوامر (CLI) لموجه الحافة:

<#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
```

استكشاف الأخطاء وإصلاحها

يتضمن تكامل الحماية المتقدمة من البرامج الضارة (SD-WAN) العديد من المكونات كما هو موضح. لذلك عندما يتعلق الأمر باستكشاف الأخطاء وإصلاحها، فمن المهم للغاية أن تكون قادرا على إنشاء بعض النقاط الرئيسية لترسيم الحدود لتضييق المشكلة حتى المكونات في تدفق الميزات:

1. vManage. هل يمكن لـ vManage دفع نهج الأمان بنجاح باستخدام نهج AMP إلى الجهاز الطرفي؟
2. Edge. بمجرد دفع سياسة الأمان بنجاح إلى الحافة، هل يقوم الموجه بالتقاط الملف الخاضع لفحص AMP وإرساله إلى سحابة AMP/TG؟
3. سحابة AMP/TG. إذا كانت الحافة قد أرسلت الملف إلى AMP أو TG، هل تحصل على الاستجابة التي تحتاجها لاتخاذ قرار السماح أو الإسقاط؟

تهدف هذه المقالة إلى التركيز على الجهاز الطرفي (2) مع أدوات مستوى البيانات المختلفة المتاحة للمساعدة في أستكشاف أخطاء تكامل AMP على موجه WAN Edge وإصلاحها.

تدفق عام لاستكشاف الأخطاء وإصلاحها

أستخدم سير العمل عالي المستوى هذا لاستكشاف أخطاء المكونات المختلفة المتعلقة بتكامل AMP وإصلاحها بسرعة بهدف أساسي يتمثل في تحديد نقطة تعيين المشكلة بين جهاز الحافة وسحابة AMP/TG.

1. هل يتم دفع سياسة AMP بشكل صحيح إلى جهاز الحافة؟
2. تحقق من الصحة العامة لحاوية UTD.
3. تحقق من سمعة الملف وقم بتحليل حالة العميل على الحافة.
4. تحقق مما إذا تم توجيه الملف إلى الحاوية. ويمكن القيام بذلك باستخدام تتبع حزمة Cisco IOS® XE.
5. تحقق لتأكيد اتصال الحافة بنجاح بسحابة AMP/TG. ويمكن القيام بذلك باستخدام أدوات مثل EPC أو تتبع الحزم.
6. تأكد من أن UTD يقوم بإنشاء ذاكرة تخزين مؤقت محلية بناء على إستجابة AMP.

يتم فحص خطوات أستكشاف الأخطاء وإصلاحها هذه بالتفصيل في هذا المستند.

مشكلات زيادة السياسات في vManage

وكما هو موضح مع عملية تهيئة سياسة حماية مستوى الإدارة (AMP)، فإن سياسة حماية مستوى الإدارة (AMP) تتسم بالوضوح دون توفر الكثير من خيارات التهيئة. إليك بعض الأمور الشائعة التي ينبغي التأمل فيها:

1. يجب أن يكون vManage قادرا على حل أسماء DNS الخاصة بسحابة AMP و ThreatGrid للوصول إلى واجهة برمجة التطبيقات. إذا فشل تكوين الجهاز على vManage بعد إضافة نهج AMP، فتحقق من /var/log/nms/vmanage-server.log بحثا عن أخطاء.
2. وكما تمت الإشارة في دليل التكوين، فقد ترك مستوى سجل التنبيهات المستوى الافتراضي الحرج أو التحذير إذا كان ذلك ضروريا. يجب تجنب التسجيل على مستوى المعلومات لأنه قد يكون له تأثير سلبي على الأداء.

للتحقق، قم بالوصول إلى Neo4j DB وعرض محتويات جدول 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"}) | +---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------+
```

دمج AMP على موجه Cisco Edge

التحقق من صحة حاوية UTD

أستخدم أوامر show utd للتحقق من سلامة حاوية UTD الإجمالية:

```
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
```

التحقق من حالة UTD AMP

تأكد من تمكين فحص الملفات:

<#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
```

تحقق من تشغيل الاتصال بسحابة AMP:

```
<#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!"
```

تحقق من تشغيل الاتصال ب ThreatGrid:

```
<#root>

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

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

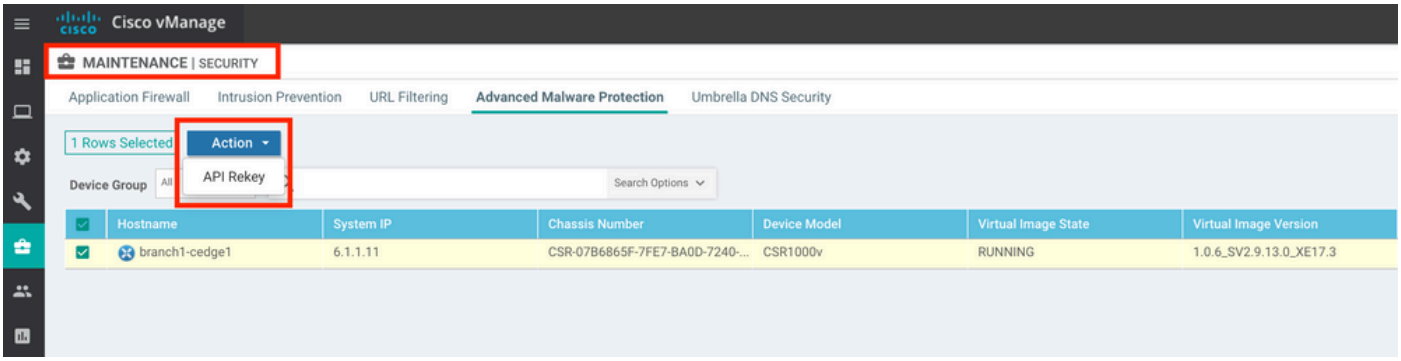
```
<#root>
```

```
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"
```

إذا لم تظهر عملية ThreatGrid حالة Up، فيساعد مفتاح واجهة برمجة التطبيقات (API). لتشغيل مفتاح واجهة برمجة تطبيقات، انتقل إلى الصيانة ->الأمان:



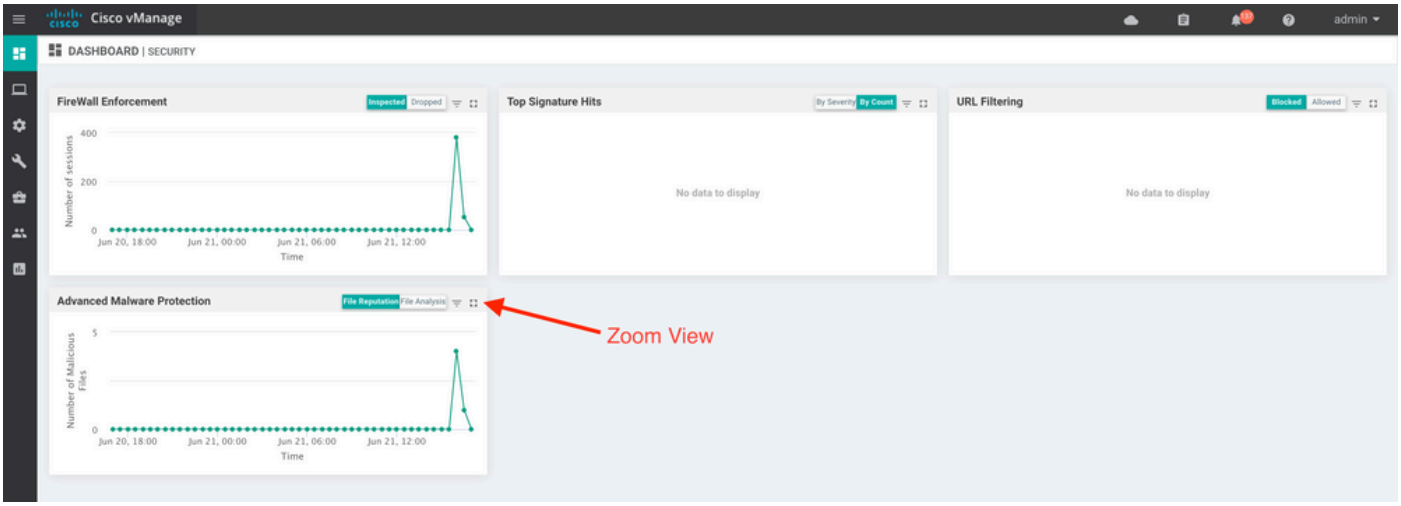
ملاحظة: يقوم مفتاح إعادة توجيه واجهة برمجة تطبيقات بتشغيل دفع قالب إلى الجهاز.

مراقبة نشاط AMP على موجه WAN Edge

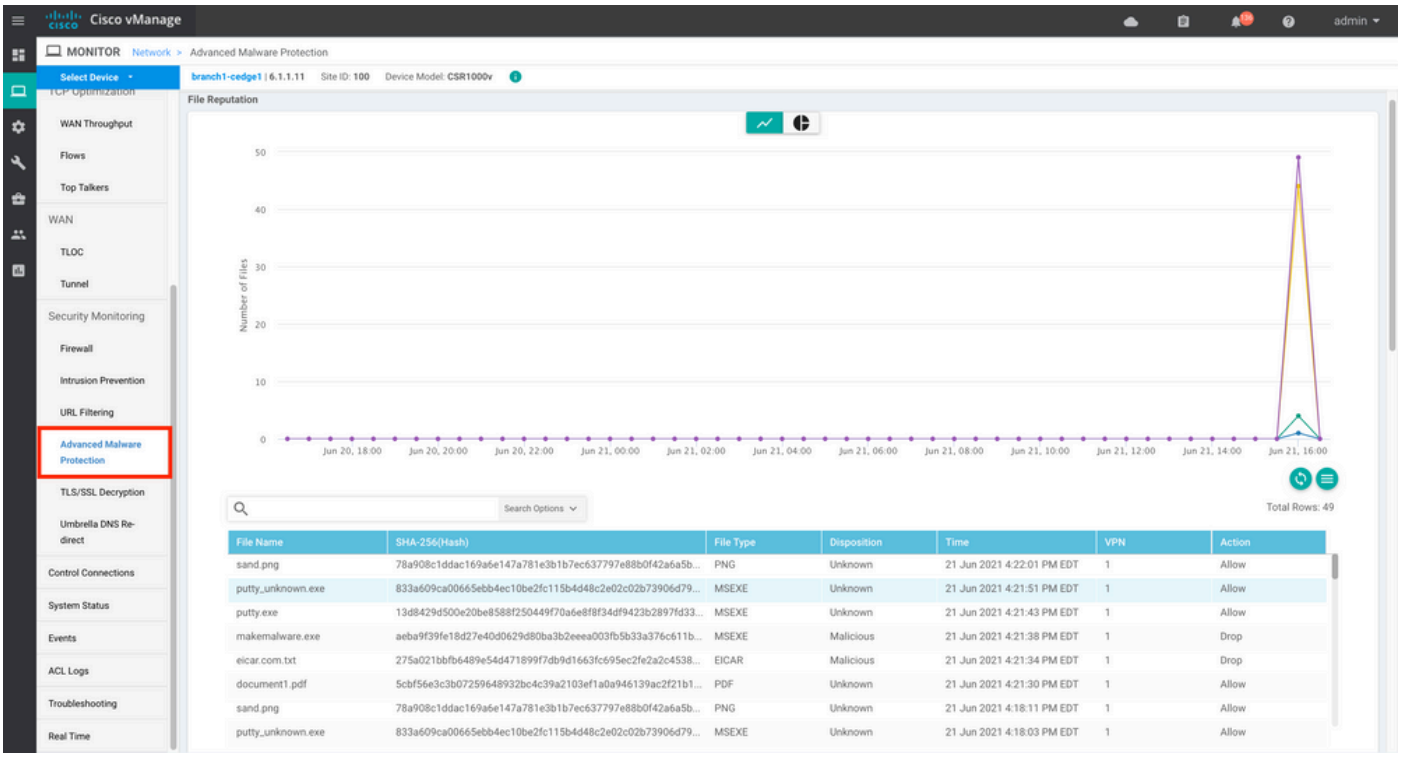
vManage

من vManage، يمكن مراقبة أنشطة ملف AMP إما من لوحة معلومات الأمان أو من طريقة عرض الجهاز.

لوحة معلومات الأمان:



عرض الجهاز:



CLI

التحقق من إحصائيات سمعة الملف:

```
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
```

فحص إحصائيات تحليل الملفات:

```
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
```

ملاحظة: يمكن الحصول على إحصائيات داخلية إضافية باستخدام الأمر show utd engine standard statistics file-reputation vrf global internal.

سلوك مستوى البيانات

يتم توجيه حركة مرور بيانات مستوى البيانات التي تخضع لفحص الملفات استنادا إلى نهج AMP الذي تم تكوينه إلى حاوية UTD لمعالجتها. يمكن تأكيد ذلك باستخدام تتبع الحزمة المستخدم. إذا لم يتم توجيه حركة المرور بشكل صحيح إلى الحاوية، فلن يحدث أي من إجراءات فحص الملفات التالية.

ذاكرة التخزين المؤقت للملفات المحلية لـ AMP

تحتوي حاوية UTD على ذاكرة تخزين مؤقت محلية من تجزئة SHA256 ونوع الملف والتصرف والإجراء استنادا إلى نتائج البحث السابقة عن مجموعة AMP. تطلب الحاوية المصير النهائي من سحابة AMP فقط إذا لم تكن تجزئة الملف موجودة في ذاكرة التخزين المؤقت المحلية. تحتوي ذاكرة التخزين المؤقت المحلية على مدة TTL تبلغ 2 ساعات قبل حذف ذاكرة التخزين المؤقت.

```
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
```

رمز المصير النهائي لـ AMP:

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

رمز إجراء AMP:

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

من أجل الحصول على تجزئة SHA256 الكاملة للملفات، وهو أمر مهم للغاية لإثارة مشاكل

مع عينة في حكم الملف، أستخدم خيار التفاصيل للأمر:

```
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>
```

لتحديد إدخالات ذاكرة التخزين المؤقت المحلية لمحرك UTD، أستخدم الأمر:

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

تشغيل تصحيح أخطاء UTD

يمكن تمكين تصحيح أخطاء UTD الاستكشاف أخطاء AMP وإصلاحها:

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

يمكن إستردادإخراج تصحيح الأخطاء مباشرة من shell النظام على /tmp/rp/trace/vman_utd_R0-0.bin، أو نسخ ملف التتبع إلى نظام ملف الموجه باستخدام الخطوات:

```
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#
```

لعرض سجل تتبع 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_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>
```

ملاحظة: في الإصدار 20.6.1 والإصدارات الأحدث، توقف طريقة إسترداد عمليات التتبع باستخدام الأمر show logging process vman module utd وعرضها مع سير عمل التتبع القياسي باستخدام الأمر utd الطرازي ...

التحقق من الاتصال من Edge إلى السحابة

للتحقق من توافق جدار الحماية مع سحابة AMP/TG، يمكن إستخدام EPC على موجه WAN Edge لتأكيد وجود اتصال ثنائي الإتجاه إلى/من خدمات السحابة:

```
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
```

المشاكل المتعلقة بسحابة AMP و TG

بمجرد التأكد من أن جهاز الحافة يلتقط الملف بشكل صحيح ويرسله إلى AMP/TG للتحليل، ولكن الحكم غير صحيح، فإنه يتطلب أستكشاف أخطاء AMP وإصلاحها أو سحابة ThreatenedGrid، والتي تقع خارج نطاق هذه المستند. وتكتسي المعلومات أهمية عند عرض مسائل التكامل:

- مؤسسة حساب ThreatGrid
- طابع زمني
- معرف تحليل الأجهزة (على سبيل المثال، CSR-07B6865F-7FE7-BA0D-7240-1BDA16328455)، هذا هو رقم الهيكل لموجه حافة WAN.
- تجزئة SHA256 الكاملة للملف المعني

معلومات ذات صلة

- دليل تكوين أمان SD-WAN
- بوابة ThreatGrid
- الدعم التقني والمستندات - Cisco Systems

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).