فهم التحكم في الوصول المستند إلى ISE و FirePOWER باستخدام TrustSec

المحتويات

المقدمة

يستخدم Cisco TrustSec وضع علامات على إطارات إيثرنت من الطبقة 2 وتخطيطها لفصل حركة المرور دون التأثير على البنية الأساسية IP الموجودة. يمكن التعامل مع حركة المرور المميزة بتدابير أمان ذات مستويات أكثر دقة.

يسمح التكامل بين محرك خدمات الهوية (ISE) ومركز إدارة Firepower (FMC) بإبلاغ وضع علامات TrustSec من تفويض العميل، والذي يمكن إستخدامه من قبل Firepower لتطبيق سياسات التحكم في الوصول بناء على علامة مجموعة أمان العميل. يناقش هذا المستند خطوات دمج ISE مع تقنية Cisco Firepower.

المكونات المستخدمة

يستخدم هذا المستند المكونات التالية في إعداد المثال:

- Identity Services Engine (ISE)، الإصدار 2.1
- مركز إدارة Firepower (FMC)، الإصدار 6.x
- جهاز الأمان القابل للتكيف (ASA) 5506-X من Cisco، الإصدار 9.6.2
- وحدة جهاز الأمان القابل للتكيف (ASA) 5506-X FirePOWER النمطية، الإصدار 6.1

نظرة عامة

هناك طريقتان لجهاز إستشعار لاكتشاف رقم مجموعة الأمان (SGT) المعين لحركة المرور:

1. من خلال تخطيط IP للمستخدم
2. من خلال وضع علامات على العرافاء الداخليين

أسلوب تعيين User-IP

لضمان إستخدام معلومات TrustSec للتحكم في الوصول، يمر دمج ISE مع FMC بالخطوات التالية:

الخطوة 1: يسترجع FMC قائمة من مجموعات الأمان من ISE.

الخطوة 2: يتم إنشاء سياسات التحكم في الوصول على FMC التي تتضمن مجموعات الأمان كشرط.

الخطوة 3: عند مصادقة نقاط النهاية والتفويض باستخدام ISE، يتم نشر بيانات الجلسة إلى FMC.

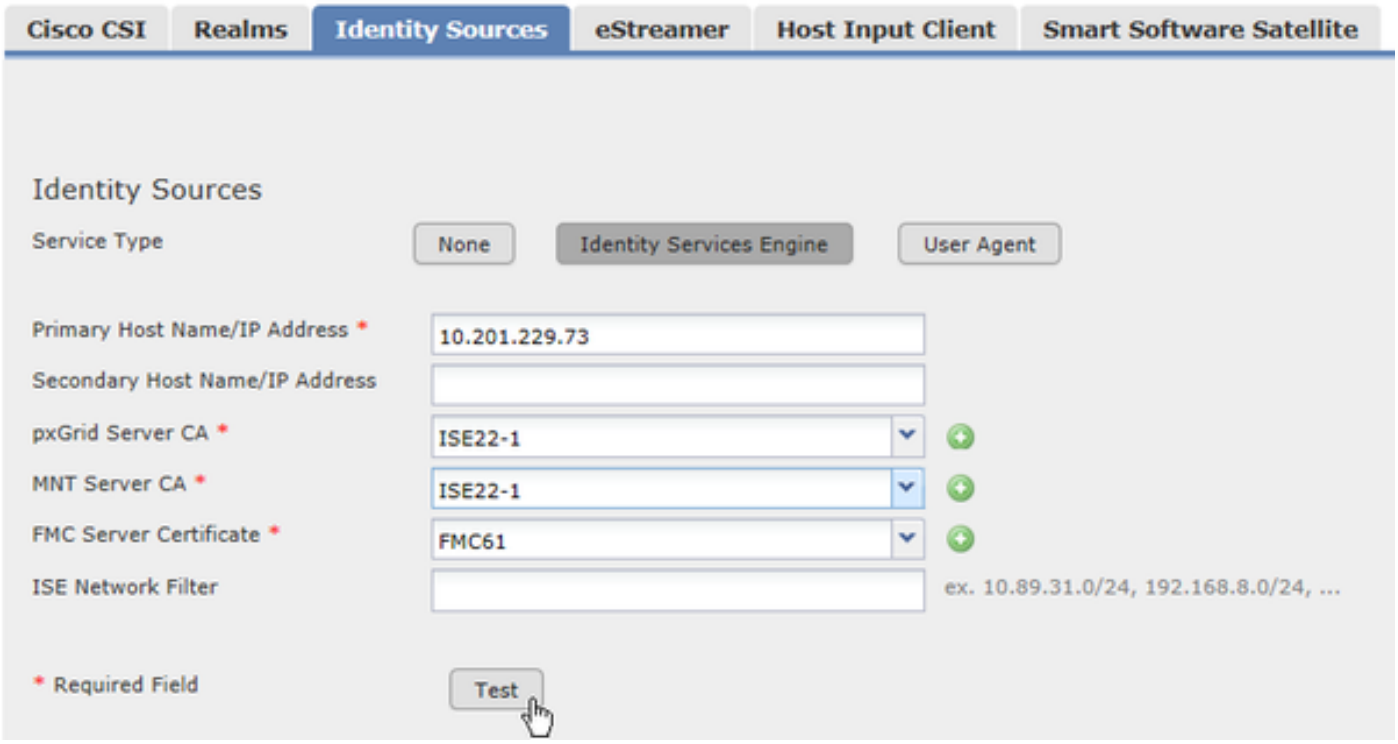
الخطوة 4: تقوم وحدة التحكم في إدارة الهيكل (FMC) ببناء ملف تخطيط مستخدم-ip-sgt، ودفعه إلى المستشعر.

الخطوة 5: يتم إستخدام عنوان IP المصدر لحركة المرور لمطابقة مجموعة الأمان باستخدام بيانات الجلسة من تخطيط User-IP.

الخطوة 6: إذا تطابقت مجموعة الأمان لمصدر حركة المرور مع الشرط في سياسة التحكم في الوصول، فيتم إتخاذ الإجراء بواسطة المستشعر وفقا لذلك.

تقوم وحدة التحكم في إدارة الهيكل (FMC) باسترداد قائمة برامج التوجيه الكامل عند حفظ تكوين دمج ISE تحت **النظام > الدمج > مصادر الهوية > محرك خدمات الهوية**.

> **ملاحظة**: لا يؤدي النقر على زر **الاختبار** (كما هو موضح أدناه) إلى تشغيل FMC لاسترداد بيانات الرقيب.



ويسير الاتصال بين وحدة إدارة الاتصالات الفيدرالية (FMC) و ISE بواسطة ADI (واجهة الدليل المجرد)، وهي عملية فريدة (يمكن أن يكون هناك مثيل واحد فقط) تعمل على FMC. عمليات أخرى تتعلق باشتراك FMC في ADI وطلب معلومات. والمكون الوحيد الذي يشترك حاليا في ADI هو Data Correlator.

ةدعاق يوتحت .ةيلحم تانايب ةدعاق يف بيقرلا ذاقنإب زنيرامل يف مكحتلا ةدحو موقت
ةمالع فرعم) اديرف افرعم FMC مدختست ،كلذ لدب نكلو ،بيقرلا مقرو مسا ىلع تانايبلا
ىلإ اضيأ هذه تانايبلا ةدعاق رشن متي .بيقرلا تانايب ةجلاعم دنع رشؤمك (ةنمآ زييمت
.رارقتسالا ةزهجأ

اذإ مت ريغت تاعومجم ناما ISE، لثم ةلازإ تاعومجملا وأ اهتفاضإ، موقي ISE عفدب مالعإ PXgrid
ىلإ FMC ثيدحتل ةدعاق تانايب SGT ةيلحملا.

موقي ISE ،ناما ةعومجم ةمالع مادختساب نذأيو ISE عم ةقداصملاب مدختسملا موقي امدنع
مالعإب FMC نم لالخ PXgrid، امم يفوي رفعملا ةفرعمب نأب مدختسملا X نم قاطنلا Y ماق ليجستب
لوخدلا عم SGT Z. ذخأت FMC تامولعملا يف فلم نييعت مدختسملا-IP. مدختست FMC
تايمزراوخ ديدحتل تقولا ءاقبإل ةيلاعف دعب ءاهتنا ةحالصلا يتلا مت لوصحلا اهيلع ىلإ ةزهجأ رارقتسالا،
بسح مدى لمح ةكبشلا دوجوملا.

> **ةظحالم**: موقت ةدحو مكحتلا يف ةرادإ لكيهلا (FMC) عفدب عيمج تالاخدإ نييعت IP
> مدختسملل ىلإ ةزهجأ رارقتسالا. يكل عفدت FMC مسر طئارخلا، بجي نأ نوكت الوأ
> ىلع ةفرعم مدختسملاب نم لالخ قاطنلا. اذإ مل نكي مدختسملا يف لجس ةقاطبلا ءزج
> نم Realm، نلف فرعتت ةزهجأ رارقتسالا ىلع تامولعم نييعتلا ةصاخلا اذهب
> مدختسملا. متي ذخأ مدع نيمدختسملا جراخ نم قاطنلا ددرتلا يف رابتعالا تارادصإلل
> ةيلبقتسملا.

ماظن مدعي ال FirePOWER رادصإلا 0 .6 طيطختلا IP-User-Sgt. ال متي مادختسإ تامالعلا
ةيلعفلا يف ةكرح رورملا، وأ طيطخت SGT-IP يذلا مت هملعت نم SXP ىلع ASA. امدنع
نييعت نع ثحبتو ردصملا IP ناونع رخشلا ةيلمع ذخأت ،ةمداق رورم ةكرح رعشتسملا طقتلي
User-IP (يذلا متي هعفد ةطساوب ةدحو Firepower ةيطمنلا ىلإ ةيلمع رخشلا)، ثحبتو نع
فرعم Secure Tag. اذإ تناك تقباطت عم فرعم بيقرلا (سيلو مقر بيقرلا) يذلا مت هنيوكت
يف ةسايس مكحتلاب لوصولا، فسوف متي قيبطت ةسايسلا ىلع ةكرح رورملا.

طريقة وضع علامات في السطر

اءدب نم ASA رادصإلا 9.6.2 ةدحوو ASA FirePOWER رادصإلا 6.1، متي معد عضو تامالع بيقرلا
ةنمضملا. اذهو ينعي نأ ةدحولا ةيطمنلا FirePOWER ةرداق نآلا ىلع جارختسإ مقر بيقرلا
ةرشابم نم مزحلا نود دامتعالا ىلع طيطخت مدختسملا-IP يذلا هرفوت FMC. رفوي كلذ الح
ليدبا مكحتلل يف لوصولا دنتسملا ىلإ TrustSec امدنع ال نوكي مدختسملا ءزج نم
قاطنلا (لثم ةزهجألا ريغ ةرداقلا ىلع ةقداصم 802.1x).

عم طيرقة عضو تامالع يف السطر، ام لازت تاسجملا ردت ىلع FMC تاعومجم ةداعتسإلا
نم بيقرلا تانايب ةدعاق عفدو تقؤملا نيزختلا ةدعاق نم بيقرلا .لفسأل ةكرح لصت امدنع
رورملا يتلا مت عضو ةمالع اهيلع مقرب ةعومجم ناملأا ىلإ ASA، اذإ مت نيوكت ASA قثيل
بيقرلاب دراولا، فسوف متي ريرمت ةمالعلا ىلإ ةدحولا ةيطمنلا FirePOWER نم لالخ مسوتلا
تانايبلا. ذخأت ةدحولا ةيطمنلا Firepower ةمالعلا نم مزحلا اهمدختستو ةرشابم مييقتل
تاسايس مكحتلا يف لوصولا.

بجي نأ يوتحي ASA ىلع نيوكت TrustSec حيحص ىلع ةهجاولا يقلتل ةكرح رورملا يتلا مت
عضو ةمالع اهيلع:

```
interface GigabitEthernet1/1
 nameif inside
 cts manual
  policy static sgt 6 trusted
 security-level 100
```

```
 ip address 10.201.229.81 255.255.255.224
```

> **ةظحالم**: ال معدي وضع تامالع ىلع InLine إال اإلصدار 9.6.2 نم ASA واإلصدارات األعلى. ال ررمت اإلصدارات السابقة نم ASA ةمالع األمان نم اللخ ةحول البيانات إلى الوحدة النمطية FirePOWER. إذا ناك زاهج إستشعار معدي وضع تامالع في السطر، فإنه سيحاول أوال إستخراج ةمالع نم ةكرح المرور. إذا مل متي زييمت ةكرح المرور، فإن المستشعر عجري إلى ةقيرط طيطخت User-IP.

استكشاف األخطاء وإصالحها

نم الصدفة المقيدة لجهاز FirePOWER

لعرض سياسة التحكم في الوصول التي مت اهعفد نم FMC:

```
> show access-control-config
.
.

.
. ===============[ Rule Set: (User) ]================ ---------------[ Rule: DenyGambling ]-----
---------- Action : Block ISE Metadata : Security Group Tags: [7:6]

    Destination Ports      : HTTP (protocol 6, port 80)
                             HTTPS (protocol 6, port 443)
    URLs
      Category             : Gambling
      Category             : Streaming Media
      Category             : Hacking
      Category             : Malware Sites
      Category             : Peer to Peer
    Logging Configuration
      DC                   : Enabled
      Beginning            : Enabled
      End                  : Disabled
      Files                : Disabled
    Safe Search            : No
    Rule Hits              : 3
    Variable Set           : Default-Set
```

> **ةظحالم**: تحدد ددع تامالع ةعومجم التأمين نيمقر: [7:6]. في هذه المجموعة نم األرقام، 7" وه المعرف الفريد لقاعدة بيانات الرقيب المحلية، والمعروف طقف ةحولل التحكم في إدارة الهيكل (FMC) والمستشعر. "6" وه الرقم الفعلي للرقيب المعروف لجميع األطراف.

 لعرض السجالت التي مت إنشاؤها دنع ةجلاعم SFR لحركة المرور الواردة وتقييم جهن الوصول:

```
> system support firewall-engine-debug

Please specify an IP protocol:
Please specify a client IP address: 10.201.229.88
Please specify a client port:
```

```
Please specify a server IP address:
Please specify a server port:
Monitoring firewall engine debug messages
```

رطسلا يف تامالع عضو عم ةدراولا رورملا ةكرحل ءاطخألا حيحصت-كرحم-ةيامحلا رادج ىلع لاثم:

```
10.201.229.88-52243 > 104.28.4.103-80 6 AS 0 I 1 Starting with minimum 0, id 0 and IPProto first
with zones -1 -> -1,
geo 0(0) -> 0, vlan 0, sgt tag: 6, svc 676, payload 0, client 686, misc 0, user 9999999, url
http://www.poker.com/, xff
10.201.229.88-52243 > 104.28.4.103-80 6 AS 0 I 1: DataMessaging_GetURLData: Returning URL_BCTYPE
for www.poker.com
10.201.229.88-52243 > 104.28.4.103-80 6 AS 0 I 1 rule order 1, 'DenyGambling', URL Lookup
Success: http://www.poker.com/ waited: 0ms
10.201.229.88-52243 > 104.28.4.103-80 6 AS 0 I 1 rule order 1, 'DenyGambling', URL
http://www.poker.com/ Matched Category: 27:96 waited: 0ms
10.201.229.88-52243 > 104.28.4.103-80 6 AS 0 I 1 match rule order 1, 'DenyGambling', action
Block
10.201.229.88-52243 > 104.28.4.103-80 6 AS 0 I 1 sending block response of 474 bytes
```

نم عضو ريبخلا زاهج FirePOWER

> **ريذحت**: ضرغل طقف رمألا ليغشتب مق .ماظنلا ءادأ ىلع ةيلاتلا تاداشرإلا رثؤت دق أ فاشكتسا ءاطخألا اهحالصإو ،وأ امدنع بلطي مهدنس معد Cisco هذه البيانات.

ةدحو موقت FirePOWER عفدب طيطخت User-IP ىلإ ةيلمع ةيلحملا تروشلا. امم ققحتلل هفرعي Snort لوح نييعتلا ،كنكمي مادختسإ رمألا يلاتلا لاسرإل مالعتسالا ىلإ Snort:

```
> system support firewall-engine-dump-user-identity-data

Successfully commanded snort.
```

ضرعل البيانات، لخدأ ىلإ عضو ريبخلا:

```
> expert

admin@firepower:~$
```

ئشني snort فلم تحت غيرفت /var/sf/detection_engines/GUID/instance-x ليلد. مسا فلم غيرفتلا وه user_identity.dump.

```
admin@firepower:/var/sf/detection_engines/7eed8b44-707f-11e6-9d7d-e9a0c4d67697/instance-1$ sudo
cat user_identity.dump
Password:

---------------- IP:USER ---------------- ---------------- Host ::ffff:10.201.229.88 -----------
----- ::ffff:10.201.229.88: sgt 7, device_type 313, location_ip ::ffff:10.201.229.94
::ffff:10.201.229.88:47 realm 3 type 1 user_pat_start 0

-------------------
USER:GROUPS
-------------------
~
```

يوضح الإخراج أعلاه أن Snort على دراية بعنوان IP 10.201.229.94 الذي تم تعيينه على معرف القرية 7، وهو رقم القرية 6 (الضيوف).

من مركز إدارة Firepower

يمكنك مراجعة سجلات ADI للتحقق من الاتصال بين FMC و ISE. للعثور على سجلات مكون ADI، تحقق من ملف /var/log/messages على FMC. ستالحظ سجلات مثل أدناه:

```
ADI_ISE_Test_Help:adi.ISEConnection [INFO] Preparing ISE Connection objects...
ADI_ISE_Test_Help:adi.ISEConnection [INFO] Preparing subscription objects...
ADI_ISE_Test_Help:adi.ISEConnection [INFO] subscribed successfully to
EndpointProfileMetaDataCapability
ADI_ISE_Test_Help:adi.ISEConnection [INFO] registered callback for capability
EndpointProfileMetaDataCapability
ADI_ISE_Test_Help:adi.ISEConnection [INFO] subscribed successfully to
TrustSecMetaDataCapability
ADI_ISE_Test_Help:adi.ISEConnection [INFO] registered callback for capability
TrustSecMetaDataCapability
ADI_ISE_Test_Help:adi.ISEConnection [INFO] subscribed successfully to
SessionDirectoryCapability
ADI_ISE_Test_Help:adi.ISEConnection [INFO] registered callback for capability
SessionDirectoryCapability
ADI_ISE_Test_Help:adi.ISEConnection [INFO] Connecting to ISE server...
ADI_ISE_Test_Help:adi.ISEConnection [INFO] Beginning to connect to ISE server...
.
.

.
.
ADI_ISE_Test_Help:adi.ISEConnection [INFO] ...successfully connected to ISE server.
ADI_ISE_Test_Help:adi.ISEConnection [INFO] Starting bulk download
.
.
```

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).