التحقق من قائمة SID مخصصة من أجهزة FMC و CLI باستخدام FirePOWER إستشعار GUI

المقدمة

يوضح هذا المستند كيفية الحصول على قائمة مخصصة بمعرف أمان (SID) من برنامج سطر الأوامر (CLI) لوحدة FirePOWER وأ FirePOWER (FTD) الدفاع ضد تهديد وواجهة المستخدم الرسومية (GUI) بوحدة التحكم FMC. يمكن العثور على معلومات SID على واجهة المستخدم الرسومية (GUI) الخاصة بوحدة التحكم FMC إذا قمت بالتنقل إلى ***البيانات لفطة > قواعد التطفل***. في بعض الحالات، من الضروري الحصول على قائمة بمعرف فئة المورد (SID) المتوفر من واجهة سطر الأوامر.

المتطلبات الأساسية

المتطلبات

cisco يوصي أن أنت تعرف هذا موضوع:

- الدفاع ضد تهديد FirePOWER (FTD) من Cisco
- خدمات جدار الحماية Cisco ASA مع FirePOWER
- مركز إدارة FireSIGHT (FMC) من Cisco
- معرفة ليونكس الأساسية

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدار البرنامج التالي:

- مركز إدارة Firepower 6.6.0
- الدفاع ضد تهديد Firepower 6.4.0.9
- وحدة FirePOWER 6.2.3.2

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.

معلومات أساسية

قاعدة ***التطفل*** هي مجموعة من الكلمات الأساسية والوسيطات التي يستخدمها النظام لاكتشاف محاولات إستغلال نقاط الضعف على شبكتك. بينما يقوم النظام بتحليل حركة مرور الشبكة، فإنه يقارن الحزم بالشروط المحددة في كل قاعدة. إذا تطابقت بيانات الحزمة مع جميع الشروط المحددة في قاعدة ما، تقوم القاعدة بتشغيل. إذا كانت القاعدة قاعدة تنبيه، فإنها تولد حدث إقتحام. إذا كانت قاعدة تمرير، فإنها تتجاهل حركة المرور. لقاعدة إسقاط في نشر داخلي، يقوم النظام بإسقاط الحزمة وإنشاء حدث. يمكنك عرض أحداث التطفل وتقييمها من وحدة تحكم الويب الخاصة بمركز إدارة Firepower.

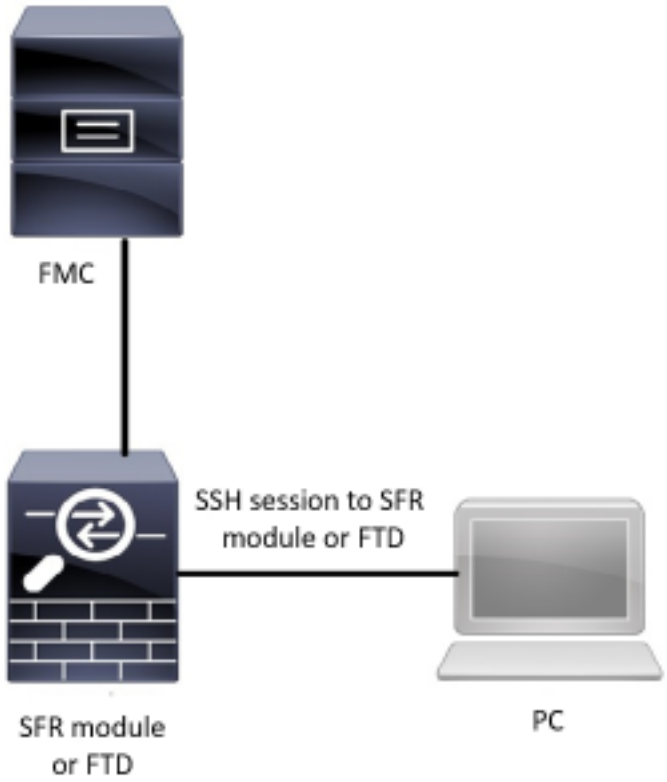
ويوفر نظام FirePOWER نوعين من قواعد الاختراق: ***قواعد الكائن المشترك وقواعد النص القياسية***. يمكن لمجموعة مع ولومات الأمان والبحوث (Talos) من Cisco إستخدام قواعد الكائن المشتركة الكتشاف الهجمات ضد نقاط الضعف بطرق ال يمكن لقواعد النص القياسية التقليدية إستخدامها. ال يمكن إنشاء قواعد كائن مشترك. عندما تتم كتابة قواعد طبطبة مخصصة قياسية نص قاعدة. قواعد نص قياسية، يجب إنشاء قاعدة نص قياسية مخصصة لضبط التطفل بنفسك، تذكر أن بعض أنواع الأحداث التي من المحتمل أن تراها. من خلال كتابة القواعد وتحديد رسالة حدث القاعدة، يمكنك التعرف بسهولة أكبر على حركة المرور التي تشير إلى الهجمات والتهرب من النهج.

عند تمكين قاعدة نص قياسية مخصصة في سياسة أختراق مخصصة، تذكر أن بعض الكلمات القاعدة الأساسية والوسيطات تتطلب فك تشفير حركة المرور أو معالجتها مسبقا بطريقة معينة.

القاعدة ***المحلية المخصصة*** في نظام FirePOWER هي قاعدة Snort قياسية مخصصة تقوم بإدراجها بتنسيق ملف نصي ASCII من جهاز محلي. يتيح لك نظام FirePOWER إستيراد القواعد المحلية باستخدام واجهة الويب. إن الخطوات اللازمة لاستيراد القواعد المحلية مثالية، يتطلب المستخدم معرفة واضحة ومباشرة للغاية. ومع ذلك، لكتابة قاعدة محلية مثالية، يتطلب المستخدم معرفة متعمقة ببروتوكولات الشبكة والشبكة.

> **تحذير**: تأكد من إستخدام بيئة شبكة يتم التحكم فيها لاختبار أي قواعد إقتحام تكتبها قبل إستخدام القواعد في بيئة إنتاج. قد تؤثر قواعد التطفل المكتوبة بشكل سيء بشكل كبير على أداء النظام

الرسم التخطيطي للشبكة

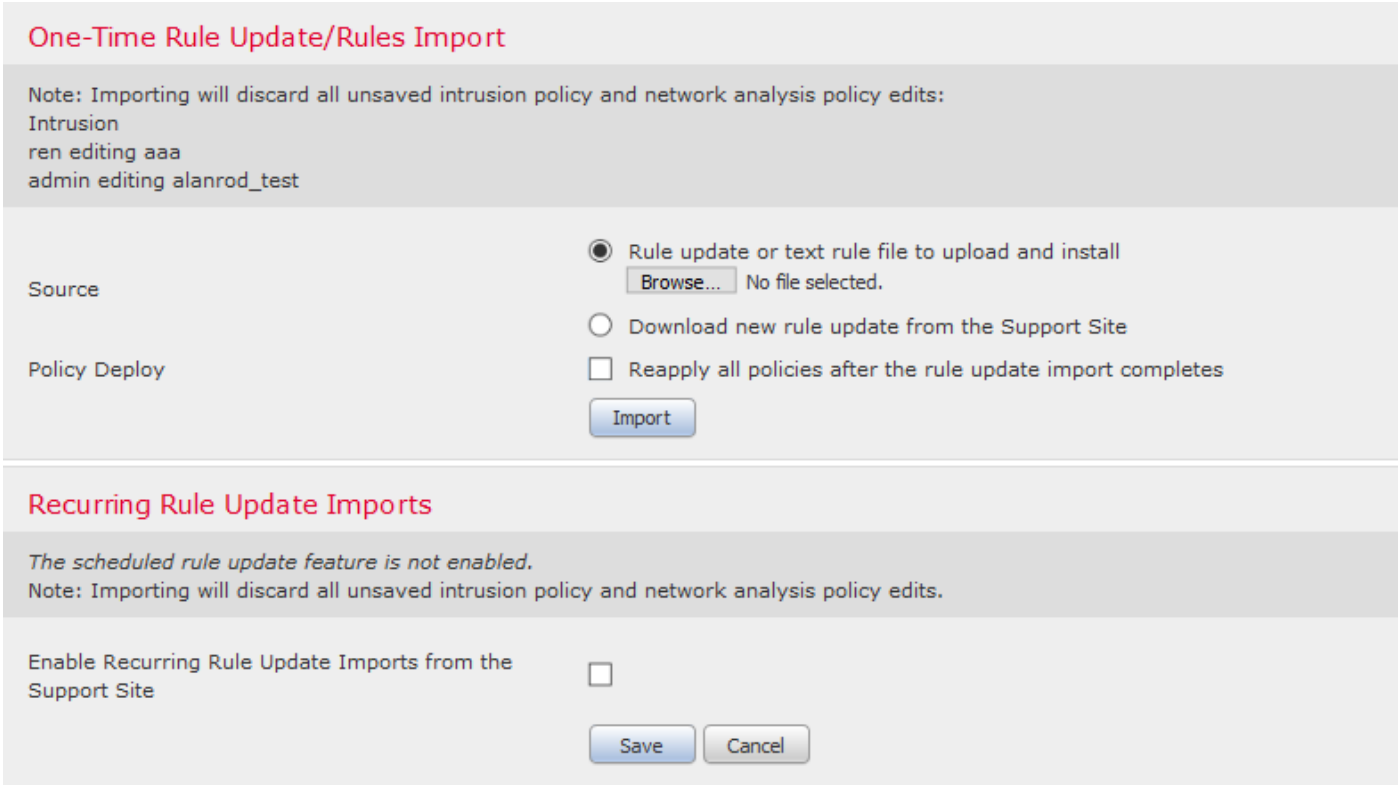


التكوين

إستيراد القواعد المحلية

قبل البدء، يجب التأكد من أن القواعد المدرجة في ملف المخصص ال تحتوي علي أي حروف خاصة. يتطلب مستورد القاعدة إستيراد كافة القواعد المخصصة باستخدام ترميز ASCII أو UTF-8. يشرح الإجراء الموضح أدناه كيفية إستيراد قواعد النص القياسية المحلية من جهاز محلي.

الخطوة 1. قم بالوصول إلى علامة التبويب **قواعد الاستيراد** بالانتقال إلى **الكائنات > قواعد التطفل > قواعد الاستيراد.** تظهر صفحة **تحديثات القواعد** كما هو موضح في الصورة أدناه:



الخطوة 2. حدد **تحديث القاعدة أو ملف القاعدة النصية لتحميله وتثبيته** وانقر **إستعراض** لتحديد ملف القاعدة المخصص

ملاحظة: يتم حفظ جميع القواعد التي تم تحميلها في فئة **القاعدة المحلية**

الخطوة 3. انقر فوق **استيراد**. تم إستيراد ملف القاعدة

ملاحظة: لا تستخدم أنظمة FirePOWER القاعدة الجديدة المحددة للتفتيش. لتنشيط قاعدة محلية، تحتاج إلى تمكينها في نهج التطفل، ثم تطبيق النهج.

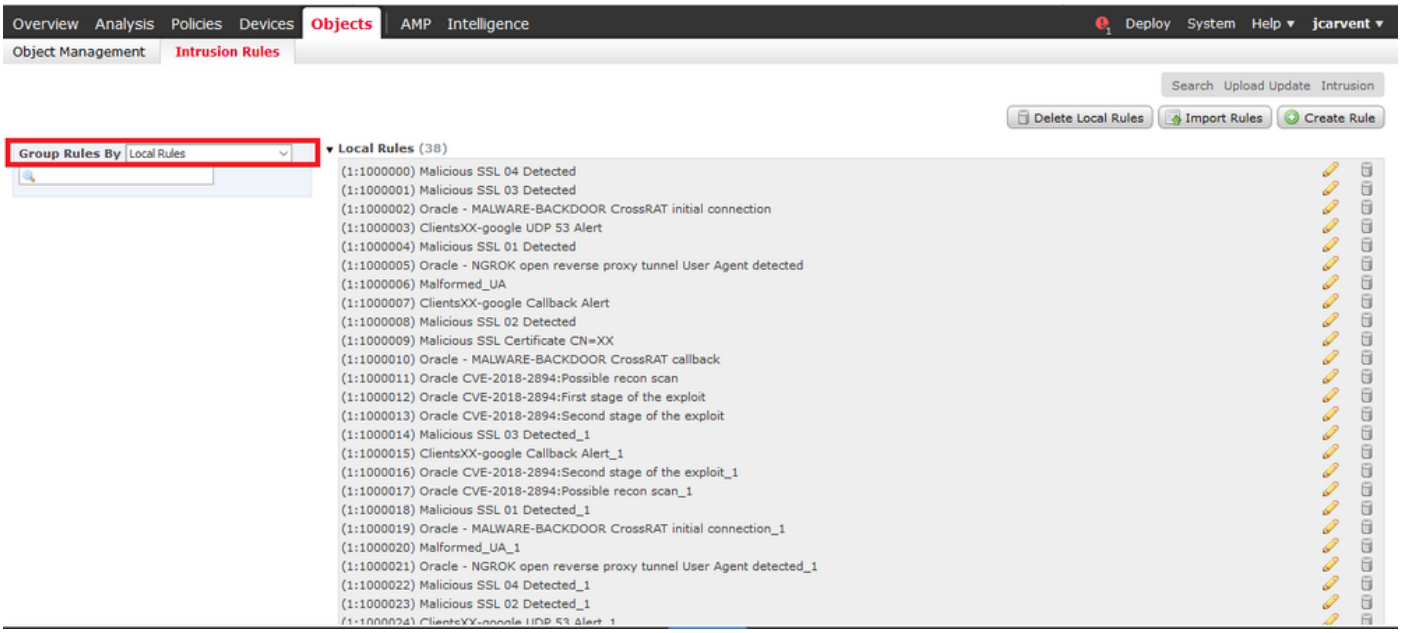
التحقق من الصحة

من FMC GUI

1. عرض القواعد المحلية المستوردة من واجهة المستخدم الرسومية (GUI) ل FMC

الخطوة 1. انتقل إلى **الكائنات > قواعد التطفل**

الخطوة 2. تحديد **القواعد المحلية** من **قواعد المجموعة**



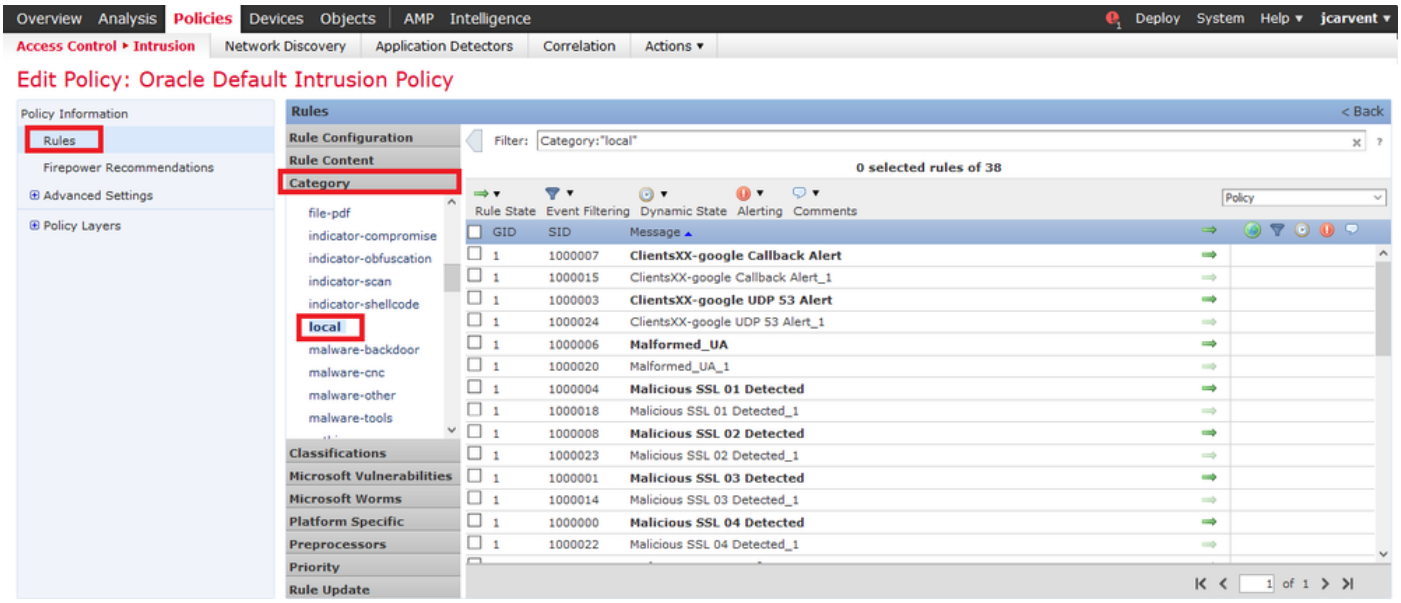
بشكل افتراضي، يقوم نظام FirePOWER بتعيين القواعد المحلية في حالة معطلة. يجب أن تقوم هذه القواعد المحلية بتعيين حالة القواعد المحلية يدويا قبل أن تتمكن من إستخدامها في سياسة التسلل.

2. تمكين قاعدة محلية من نهج التطفل

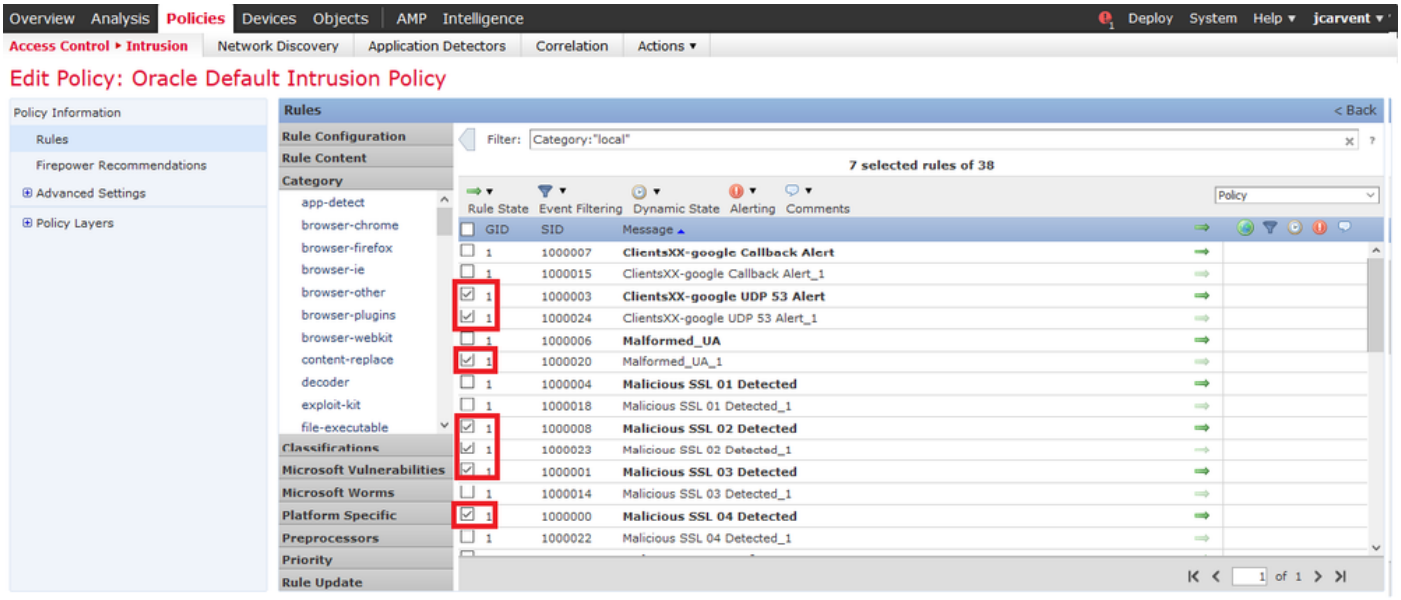
الخطوة 1. انتقل إلى صفحة محرر السياسات ضمن **السياسات > الاختراق > نهج الاختراق**

الخطوة 2. حدد **القواعد** في اللوحة اليسرى

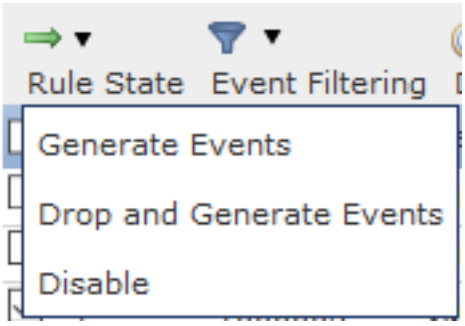
الخطوة 3. تحت **الفئة**، حدد **محلي**. يجب أن تظهر جميع القواعد المحلية إذا كانت متوفرة:



الخطوة 4. حدد القواعد المحلية المطلوبة:



الخطوة 5.بعد تحديد القواعد المحلية المطلوبة، حدد حالة من **حالة القاعدة**



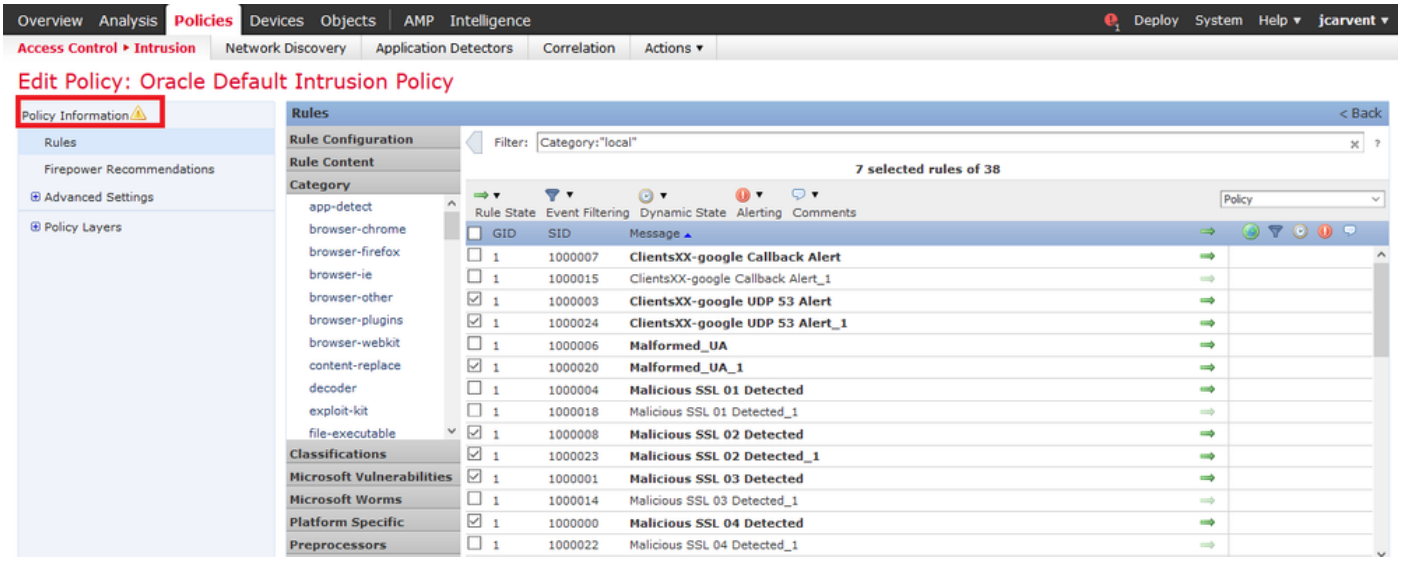
تتوفر الخيارات التالية:

- **إنشاء الأحداث:** تمكين القاعدة وإنشاء حدث

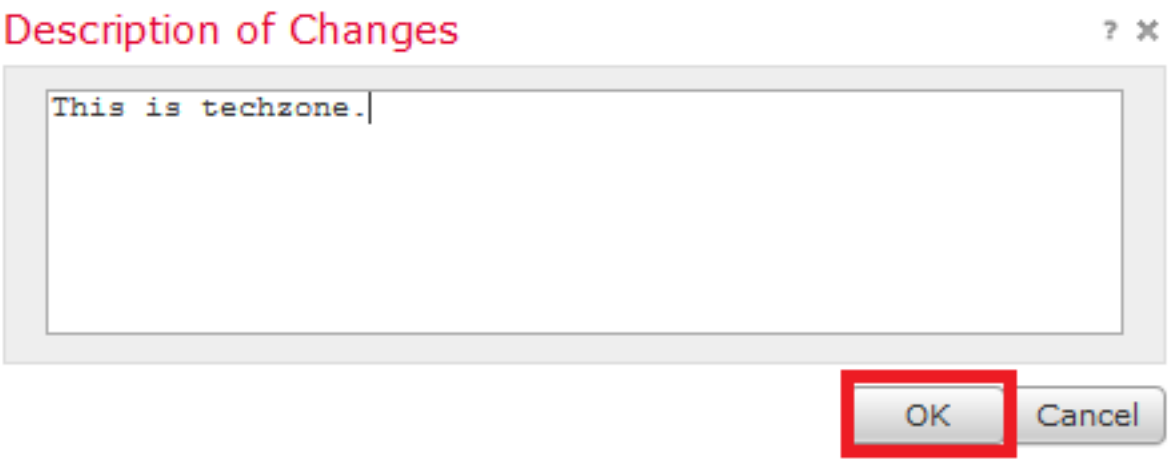
- **إسقاط الأحداث وتوليدها:** تمكين القاعدة وإسقاط حركة المرور وإنشاء حدث

- **تعطيل:** لا يمكن القاعدة، لا توجد أحداث

الخطوة 6. بمجرد تحديد حالة القاعدة، انقر فوق خيار **معلومات السياسة** في اللوحة اليسرى



الخطوة 7. حدد الزر **تنفيذ التغييرات** وقدم وصفا موجزا للتغييرات. انقر فوق **OK** لاحقا. تم التحقق من صحة نهج الاقتحام.



ملاحظة: يفشل التحقق من صحة النهج إذا قمت بتمكين قاعدة محلية مستوردة تستخدم الكلمة الأساسية للحد المهمل بالإضافة إلى ميزة حد حدث الاقتحام في سياسة الاقتحام.

الخطوة 8. نشر التغييرات

من FTD أو SFR وحدة CLI

1. عرض القواعد المحلية المستوردة من FTD أو SFR module CLI

الخطوة 1. إنشاء جلسة SSH أو CLI من وحدة SFR النمطية أو FTD

الخطوة 2. انتقل إلى وضع الخبير

```
> expert
admin@firepower:~$
```

الخطوة 3. الحصول على امتيازات المسؤول

```
admin@firepower:~$ sudo su -
```

الخطوة 4. اكتب كلمة المرور الخاصة بك

```
admin@firepower:~$ sudo su -
Password:
root@firepower:~#
```

الخطوة 5. انتقل إلى **/ngfw/var/sf/detection_engines/UUID/intrusion/**

```
root@firepower:/home/admin# cd /ngfw/var/sf/detection_engines/70f28390-f73d-11de-acfc-
2369c038cbc9/intrusion/
root@firepower:/ngfw/var/sf/detection_engines/70f28390-f73d-11de-acfc-2369c038cbc9/intrusion#
```

ملاحظة: إذا كنت تستخدم وحدة SFR، فال تستخدم /ngfw/var/sf/detection_engines/*/مسار التطفل. إستخدام VAR/**SF/detection_engines/*/intrusion**

الخطوة 6. قم بتقديم الأمر التالي

```
grep -Eo "sid:*([0-9]{1,8})" */*local.rules
```
ارجع إلى الصورة أدناه كمثال عمل:

```
root@firepower:/ngfw/var/sf/detection_engines/70f28390-f73d-11de-acfc-2369c038cbc9/intrusion#
grep -Eo "sid:*([0-9]{1,8})" */*local.rules
sid:1000008
sid:1000023
sid:1000007
sid:1000035
sid:1000004
sid:1000000
...
```
هذا سوف يسرد قائمة معرفات العميل التي تم تكوينها بواسطة الوحدة النمطية FTD أو SFR.

استكشاف الأخطاء وإصلاحها

الخطوة 1. تأكد من إنشاء جلسة SSH إلى وحدة SFR النمطية أو FTD، من FMC detection_engines غير مدرج

الخطوة 2. الأمر grep -eo "sid:*([0-9]{1،8})" */*local.rules ستعمل فقط تحت دليل التسلل، لا يمكن إستخدام الأمر من دليل آخر

الخطوة 3. أستخدم الأمر grep -eo "sid:*([0-9]{1،8})" */*.rules للحصول على قائمة SID كاملة من جميع الفئات

أفضل الممارسات لاستيراد قواعد التطفل المحلية

لاحظ الإرشادات عند إستيراد ملف قاعدة محلي:

- يتطلب مستورد القواعد أن يتم إستيراد كافة القواعد المخصصة في ملف نص عادي مشفر في UTF-8 أو ASCII
- يمكن أن يحتوي اسم الملف النصي على أحرف أبجدية رقمية ومسافات وليس هناك أحرف خاصة غير شرطة سفلية (_)، نقطة (.)، شرطة (-)
- يقوم النظام باستيراد القواعد المحلية السابقة بحرف البوند الواحد (#)، ولكن يتم فوضع علامة عليها كمحذوف
- يقوم النظام باستيراد القواعد المحلية التي تسبقها أحرف بالبوند الواحد (#) والا يقوم باستيراد القواعد المحلية التي تسبقها أحرف باوندان (##)
- لا يمكن أن تحتوي القواعد على أي أحرف هروب
- لا يتوجب عليك تحديد معرف المولد (GID) عند إستيراد قاعدة محلية. إذا قمت بذلك، حدد GID 1 فقط لقاعدة نص قياسية
- عند إستيراد قاعدة للمرة الأولى، قم بما يلي *ليس* تحديد a معرف الشيخ (SID) أو رقم المراجعة. يتجنب هذا التصادم مع SIDs لقواعد أخرى، بما في ذلك القواعد المحذوفة. سيقوم النظام تلقائيا بتعيين القاعدة SID المخصص التالي المتاح للقاعدة وهو 1 أو أكثر ورقم المراجعة 100000
- إذا كان يجب عليك إستيراد قواعد مع SIDs، يجب أن تكون SIDs أرقام فريدة بين 1،000،000

و 9،999،999

- في نشر متعدد المجالات، يعين النظام SIDs إلى قاعدة مستوردة من بركة مشتركة يستعمل بكل مجال على المركز إدارة Firepower. إذا قام العديد من المسؤولين باستيراد القواعد المحلية في نفس الوقت، فقد يظهر SIDs داخل مجال واحد على أنه غير تسلسلي، لأن النظام قام بتعيين الأرقام المتتالية في التسلسل إلى مجال آخر
- عند إستيراد إصدار محدث من قاعدة محلية قمت باستيرادها مسبقا، أو عند إعادة تثبيت قاعدة محلية قمت بحذفها، **يجب** تضمين SID الذي تم تعيينه بواسطة النظام ورقم مراجعة أكبر من رقم المراجعة الحالي. يمكنك تحديد رقم المراجعة لقاعدة حالية أو محذوفة بواسطة تحرير القاعدة

ملاحظة: يقوم النظام بزيادة رقم المراجعة تلقائيا عند حذف قاعدة محلية، وهذا جاز يسمح لك بإعادة وضع القواعد المحلية. يتم نقل جميع القواعد المحلية المحذوفة من فئة القاعدة المحلية إلى فئة القاعدة المحذوفة.

- قم باستيراد القواعد المحلية الموجودة في "المركز الأساسي لإدارة FirePOWER" في وقت لاحق لتجنب مشاكل ترقيم SID
- يفشل الاستيراد إذا كانت القاعدة تحتوي على أي مما يلي:SID أكبر من 2147483647 أو غاية ميناء أن يكون أطول من 64 رمز
- يفشل التحقق من صحة النموذج إذا قمت بتمكين قاعدة محلية مستوردة تستخدم الكلمة الأساسية **الحد** المهمل بالاقتران مع ميزة حد حدث الاقتحام في سياسة الاقتحام
- يتم حفظ كافة القواعد المحلية المستوردة تلقائيا في فئة القاعدة المحلية
- يقوم النظام دائما بتعيين القواعد المحلية التي تقوم باستيرادها إلى حالة القاعدة المعطلة. يجب تعيين حالة القواعد المحلية يدويا قبل أن تتمكن من إستخدامها في سياسة التطفل الخاصة بك

معلومات ذات صلة

فيما يلي بعض المستندات للرجوع إليها فيما يتعلق بمعرف الأمان (SID) الخاص بالشخير:

تحديث قواعد التطفل

https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/System_Software_Updates.html#ID-2259-00000356

محرر قواعد التطفل

https://www.cisco.com/c/en/us/td/docs/security/firepower/660/configuration/guide/fpmc-config-guide-v66/the_intrusion_rules_editor.html

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).