تكوين قواعد ناقل محلي مخصص في Snort3 على FTD

المحتويات

المقدمة

يصف هذا المستند إجراء تكوين قواعد الاتصال المحلية المخصصة في SNORT3 على الدفاع ضد تهديد جدار الحماية (FTD).

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- مركز إدارة FireSIGHT (FMC) من Cisco
- الدفاع ضد تهديد جدار الحماية (FTD)

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

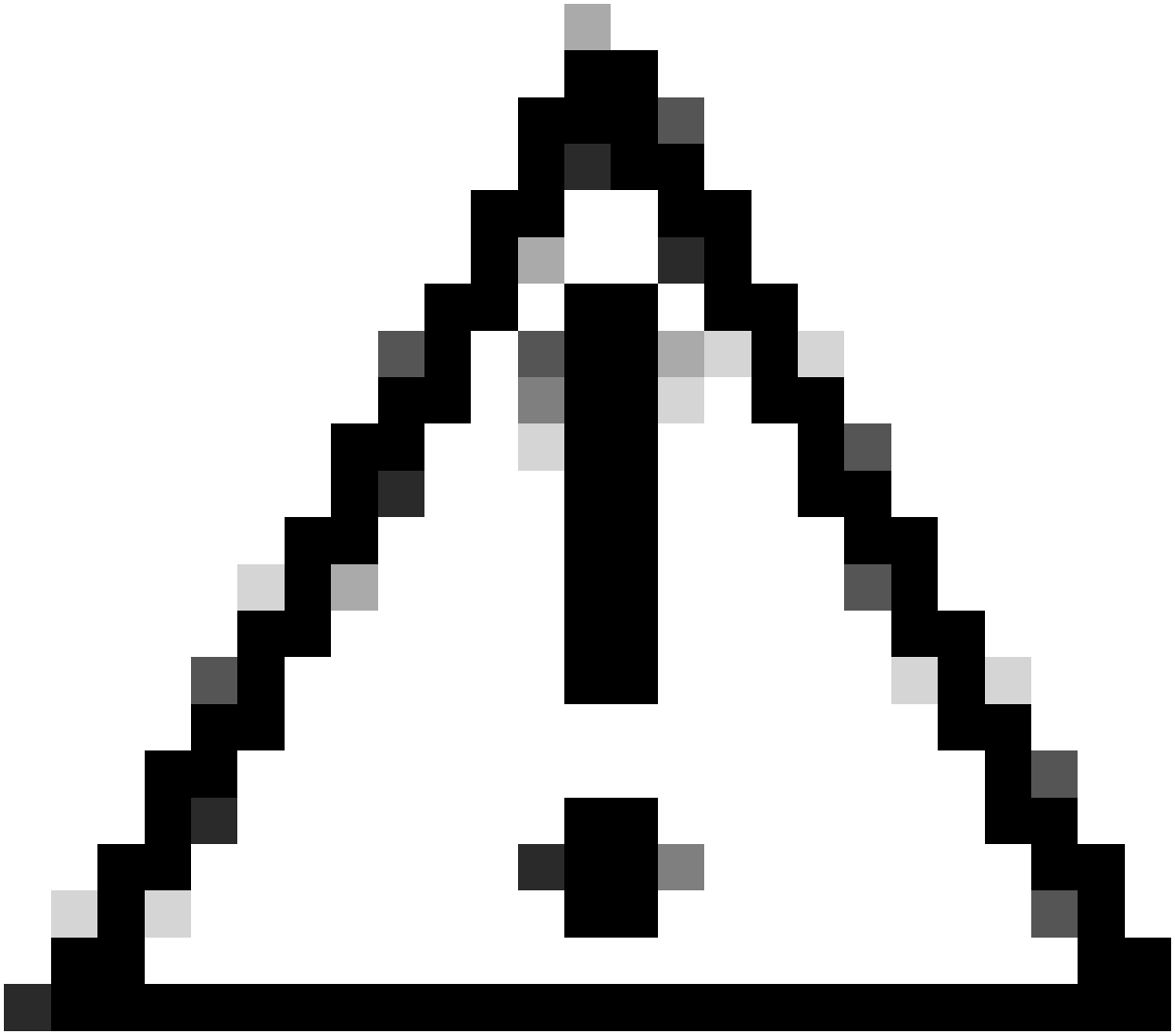
- مركز إدارة Cisco Firepower ل VMWare 7.4.1
- Cisco Firepower 2120 7.4.1

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

يدأ دعم برنامج Snort 3 في الدفاع ضد التهديدات مع مركز الإدارة في الإصدار 7. 0. بالنسبة للأجهزة الجديدة والمعوضة من الإصدار 7.0 والإصدارات الأحدث، يعتبر Snort 3 محرك الفحص الافتراضي.

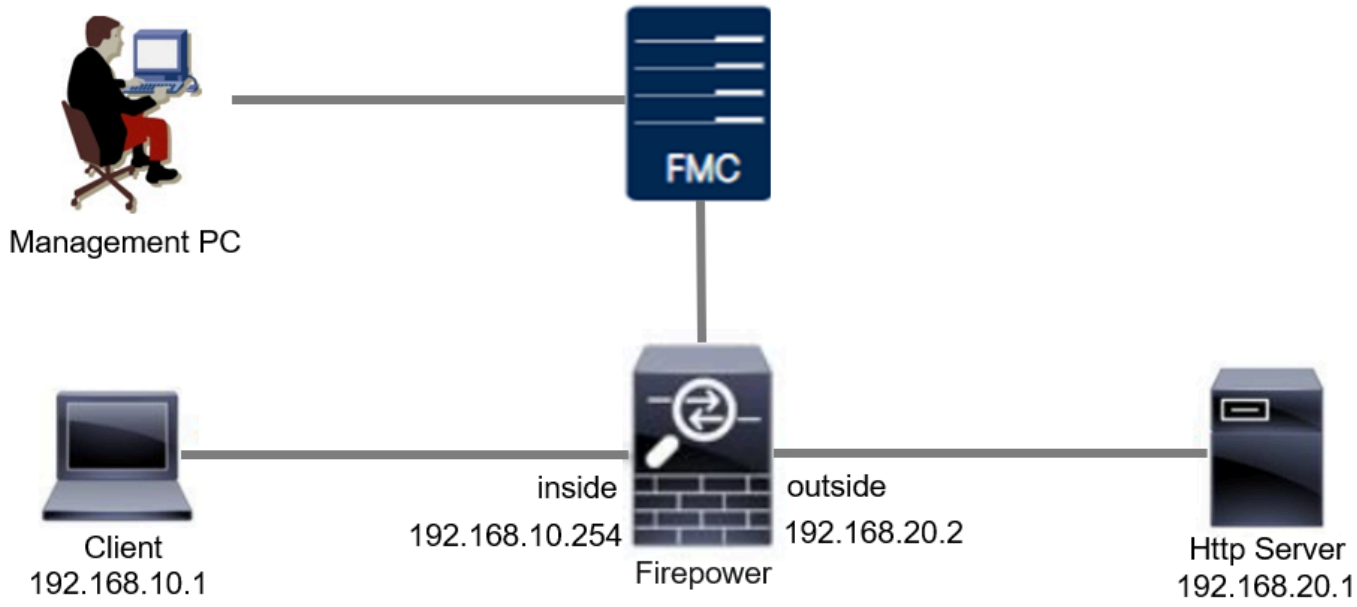
يقدم هذا المستند مثال لكيفية تخصيص قواعد الشرخ ل Snort 3، بالإضافة إلى مثال تحقق عملي. وعلى وجه الخصوص، يتم تقديم كيفية تكوين سياسة إقتحام والتحقق منها باستخدام قاعدة Snort مخصصة لإسقاط حزم HTTP التي تحتوي على سلسلة معينة (اسم المستخدم).



تحذير: يقع إنشاء قواعد اتصال محلية مخصصة وتوفير الدعم لها خارج نطاق تغطية دعم TAC. لذلك، يمكن إستخدام هذا المستند كمرجع فقط، وتطلب منك إنشاء هذه القواعد المخصصة وإدارتها وفقا لتقديرك ومسؤوليتك.

الرسم التخطيطي للشبكة

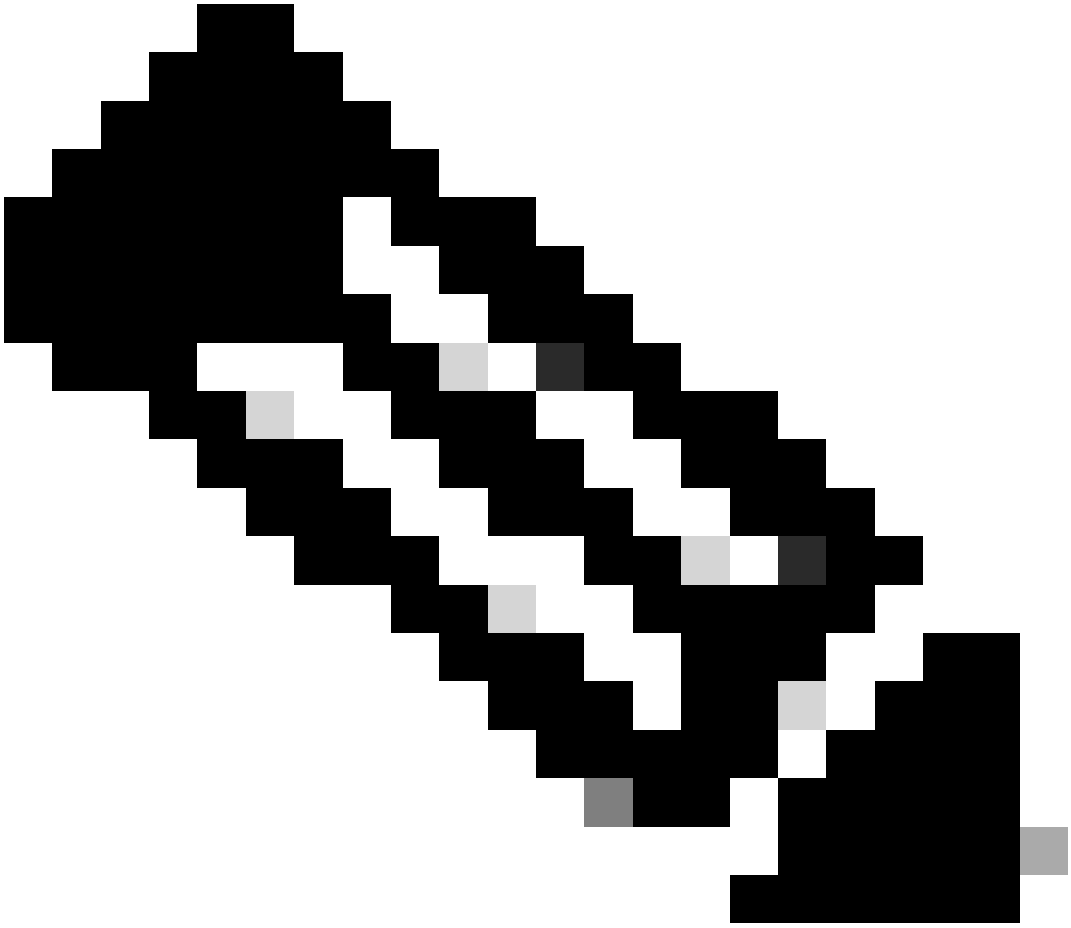
يقدم هذا المستند التكوين والتحقق لقاعدة الشوكة المحلية المخصصة في Snort3 على هذا المخطط.



الرسم التخطيطي للشبكة

التكوين

هذا هو تكوين قاعدة التكوين المحلية المخصصة لاكتشاف حزم إستجابة HTTP التي تحتوي على سلسلة محددة (اسم المستخدم) وإسقاطها.

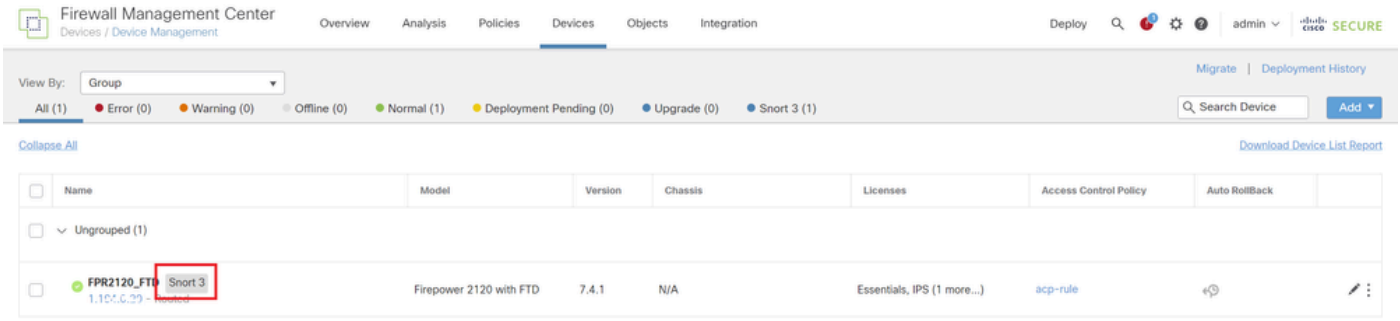


ملاحظة: حتى الآن، لا يمكن إضافة قواعد بيانات محلية مخصصة من صفحة Snort 3 All Rules في واجهة المستخدم الرسومية (GUI) لـ FMC. يجب إستخدام الطريقة المقدمة في هذا المستند.

الطريقة 1. إستيراد من Snort 2 إلى Snort 3

الخطوة 1. تأكيد إصدار الشخير

انتقل إلى الأجهزة>إدارة الأجهزة على FMC، انقر فوق أداة DeviceTab. تأكد من أن إصدار الشخير هو Snort3.



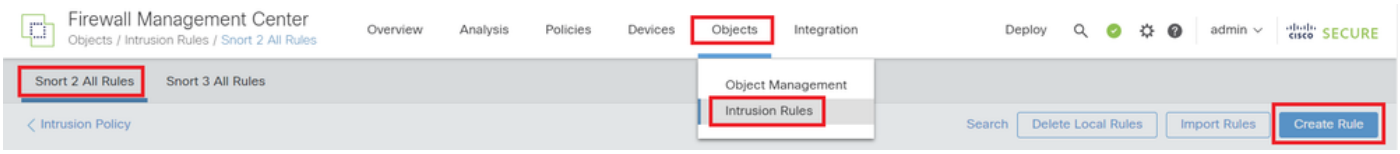
إصدار Snort

الخطوة 2. إنشاء أو تحرير قاعدة شخير محلية مخصصة في Snort 2

انتقل إلى كائنات > قواعد التطفل > Snort 2 All RuleOn FMC. انقر فوق إنشاء زر إنشاء قاعدة بيانات لإضافة قاعدة بيانات محلية مخصصة، أو انتقل إلى كائنات > قواعد التطفل > Snort 2 All Rules > القواعد المحلية على FMC، انقر فوق زر تحرير لتحرير قاعدة الشنطة المحلية المخصصة الموجودة.

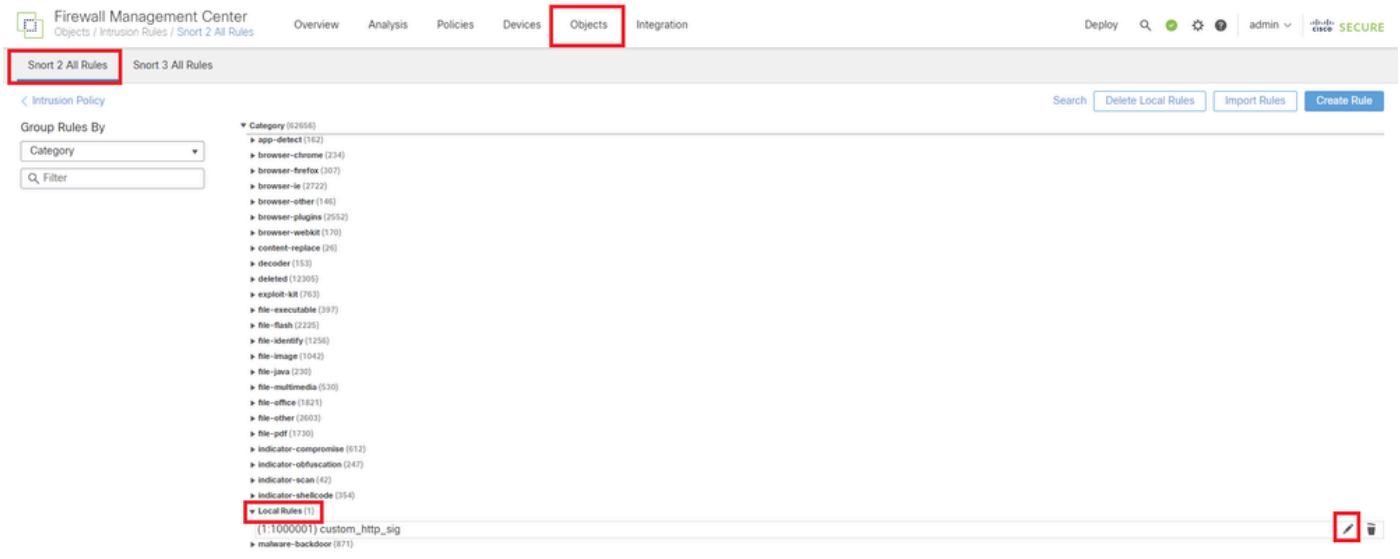
للحصول على تعليمات حول كيفية إنشاء قواعد بيانات محلية مخصصة في Snort 2، يرجى الرجوع إلى تكوين قواعد بيانات محلية مخصصة في Snort2 على FTD.

إضافة قاعدة شرخيات محلية مخصصة جديدة كإظهار في الصورة.



إضافة قاعدة مخصص جديدة

قم بتحرير قاعدة شخبط محلية مخصصة موجودة كما هو موضح في الصورة. في هذا المثال، يحرر قاعدة مخصصة موجودة.

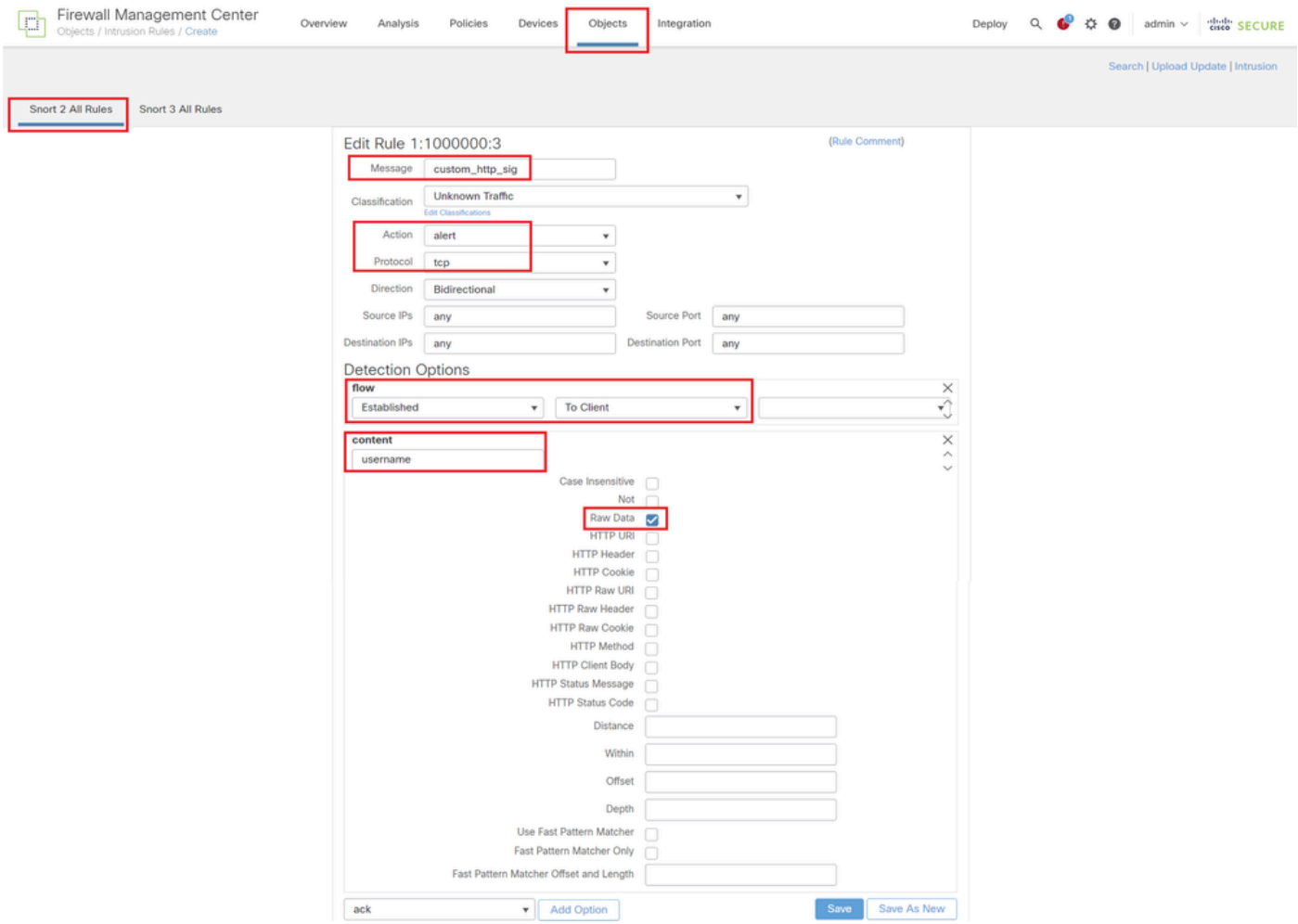


تحرير قاعدة مخصصة موجودة

أدخل معلومات التوقيع للكشف عن حزم HTTP التي تحتوي على سلسلة محددة (اسم

المستخدم).

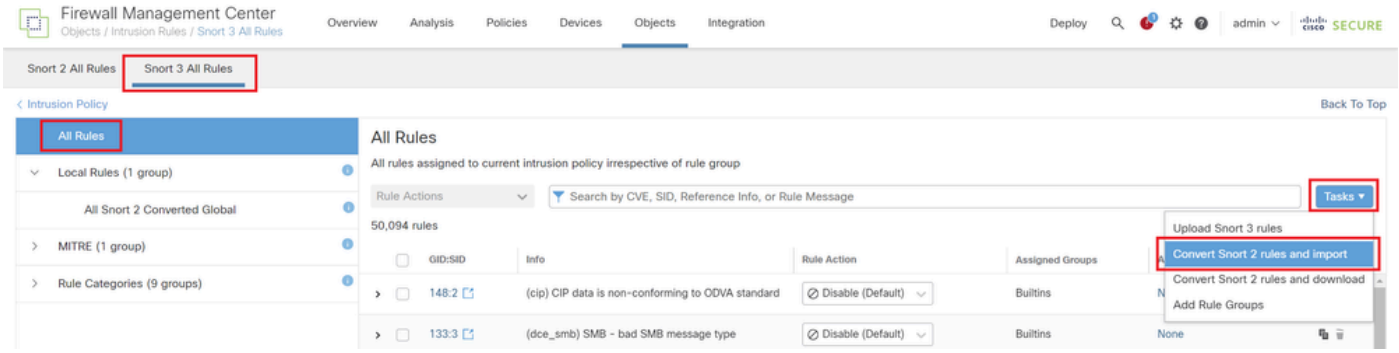
- رسالة: custom_http_sig
- الإجراء: تنبيه
- البروتوكول: TCP
- التدفق: مثبت للعميل
- المحتوى: اسم المستخدم (بيانات خام)



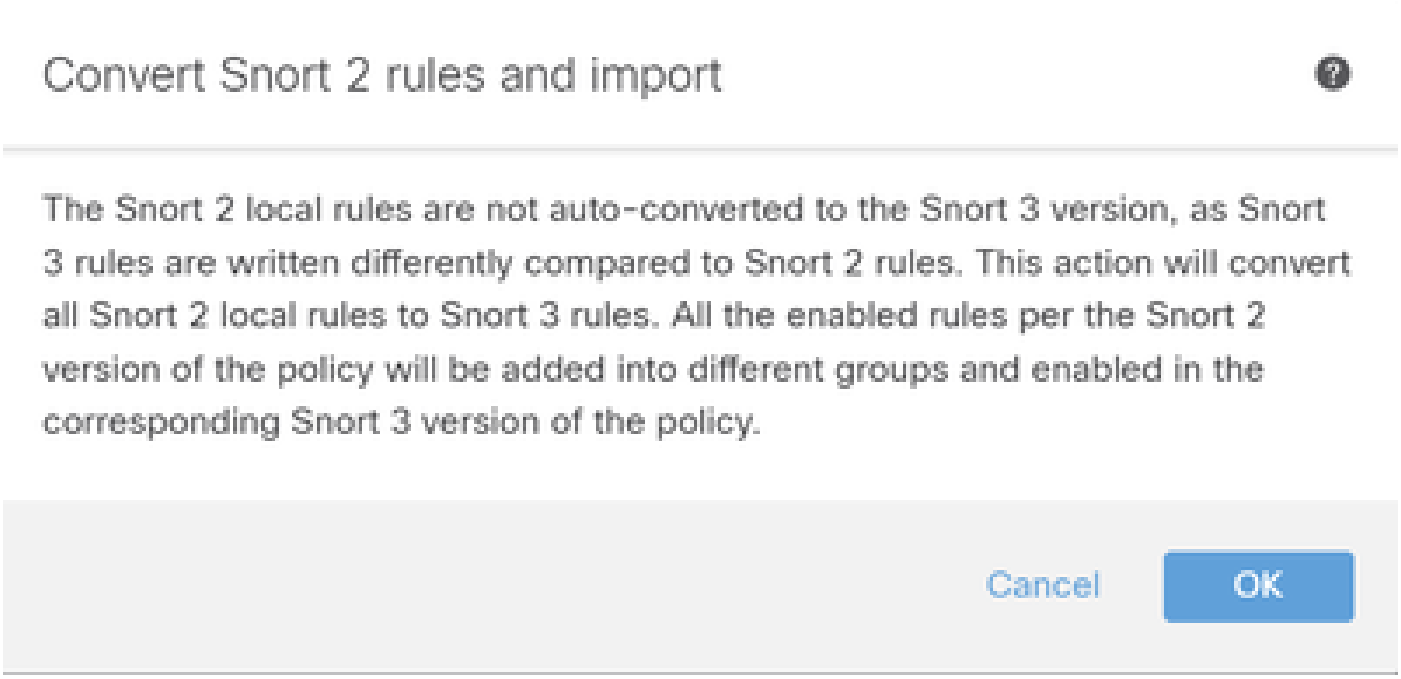
إدخال المعلومات الضرورية للقاعدة

الخطوة 3. إستيراد قواعد الشنط المحلية المخصصة من الشنورت 2 إلى الشنورة 3

انتقل إلى كائنات > قواعد التطفل > Snort 3 All Rules (قواعد التطفل) > All Rules (كل القواعد) على FMC، وانقر فوق تحويل قواعد Snort 2 واستيراد من قائمة تسريج المهام.

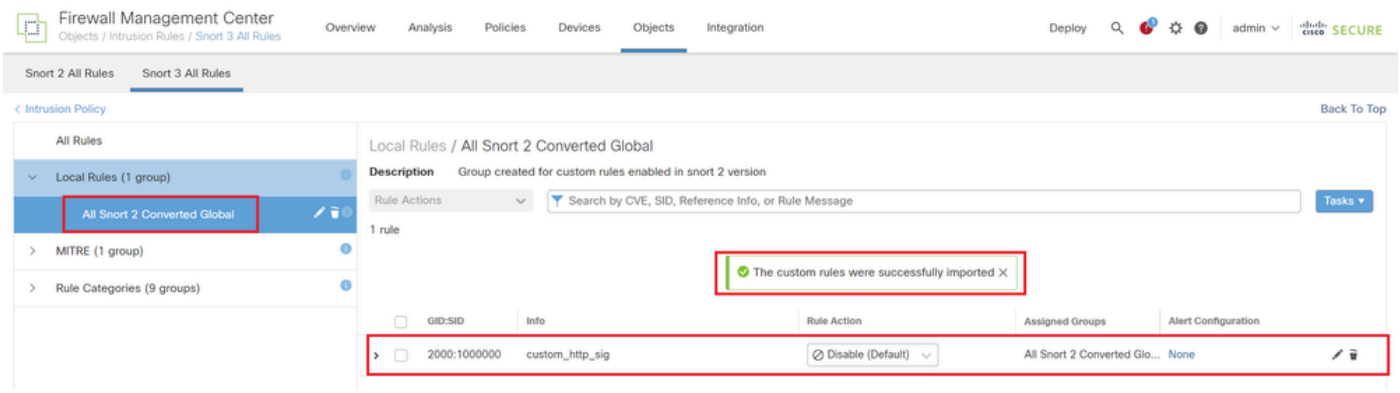


تحقق من رسالة التحذير وانقر فوق موافق.



رسالة تحذير

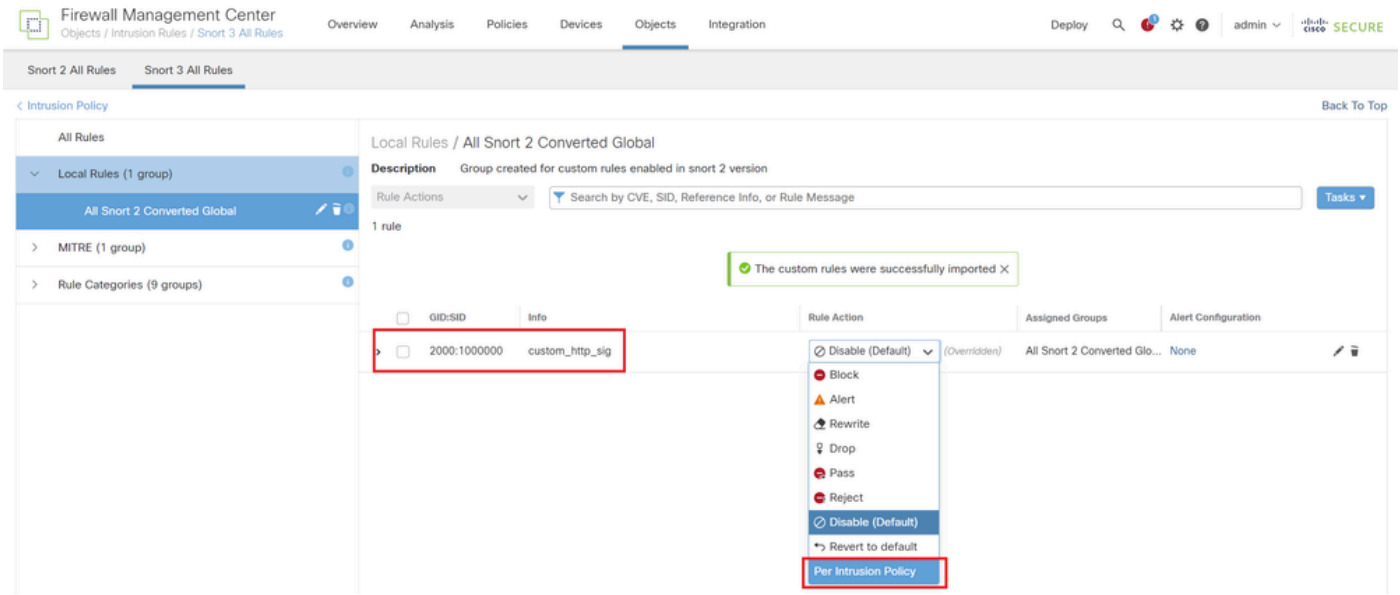
انتقل إلى كائنات > قواعد التطفل > Snort 3 All Rules على FMC، انقر فوق كافة المحولات العامة 2 التي تم تحويلها لتأكيد قاعدة الشخر المحلي المخصص التي تم إستيرادها.



تأكيد القاعدة المخصصة المستوردة

الخطوة 4. تغيير إجراء القاعدة

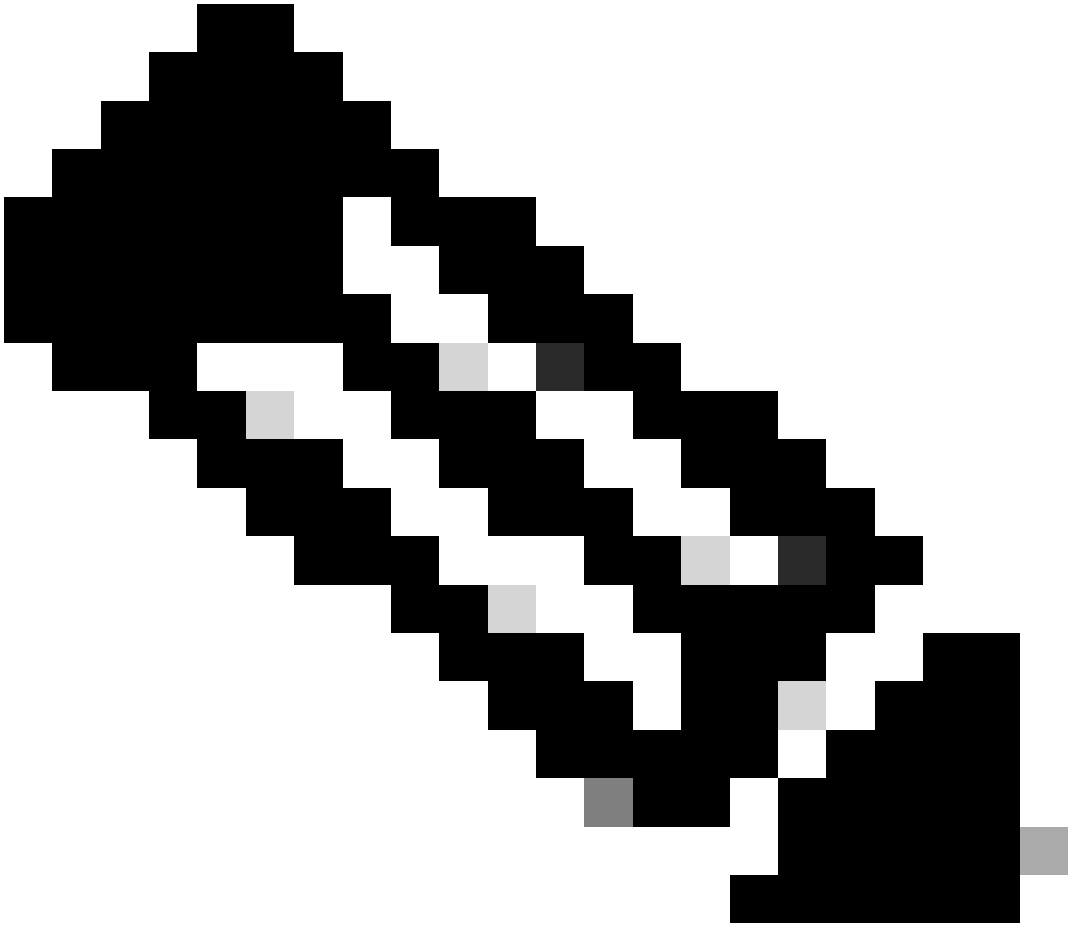
انقر فوق نهج كل تدخل وفقا لإجراء القاعدة الخاصة بالقاعدة المخصصة الهدف.



تغيير إجراء القاعدة

في شاشة تحرير إجراء القاعدة، أدخل معلومات إجراء النهج والقاعدة.

- النهج: snort_test
- إجراء القاعدة: حظر



مالحظة: إجراءات القاعدة هي:

حظر— إنشاء حدث، وحظر الحزمة المطابقة الحالية وكافة الحزم التالية في هذا االتصال.

تنبيه— يقوم بإنشاء أحداث فقط للحزمة المطابقة والا يقوم بإسقاط الحزمة أو االتصال.

إعادة الكتابة— يقوم بإنشاء حدث ويستبدل محتويات الحزمة استنادا إلى خيار االستبدال في القاعدة.

Pass— ال يتم إنشاء أي أحداث، يسمح للحزمة بالمرور دون إجراء مزيد من التقييم بواسطة أي قواعد snort تالية.

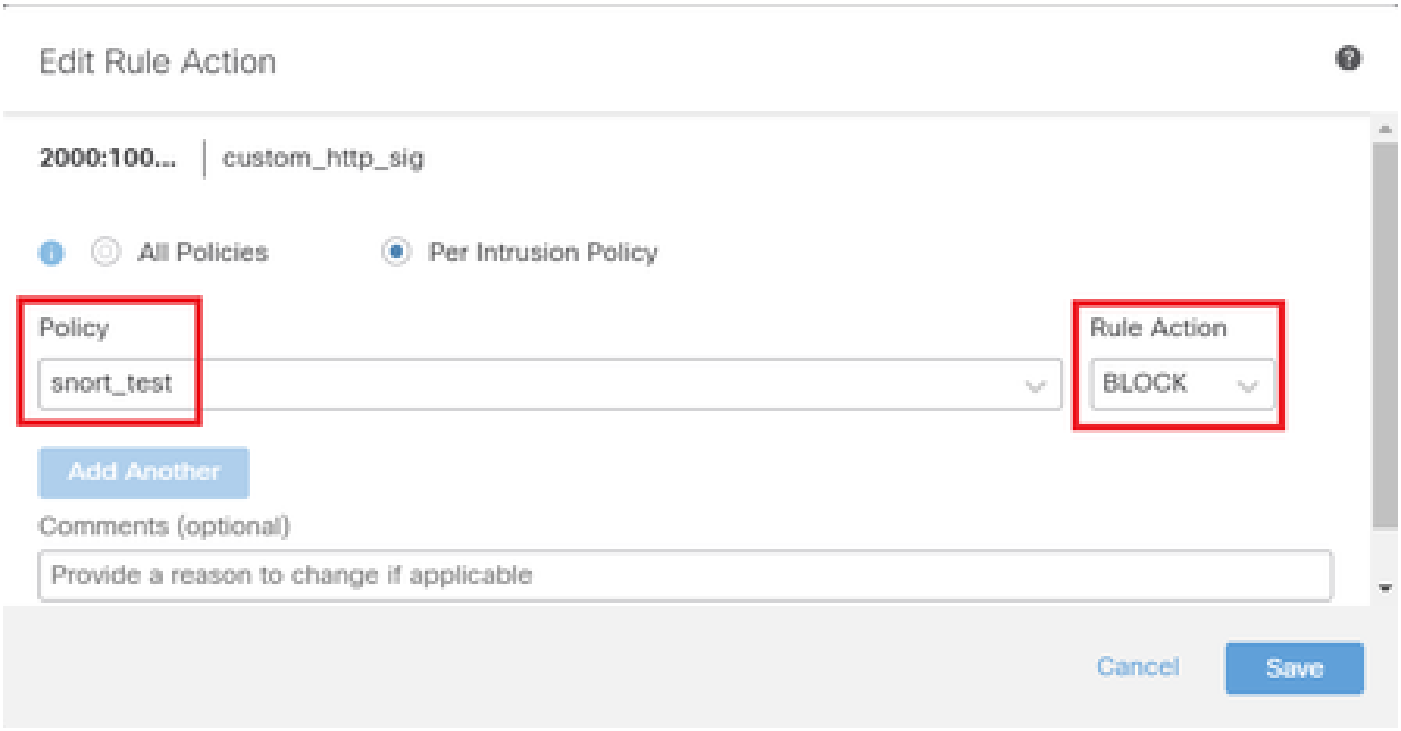
drop— يقوم بإنشاء الحدث، ويسقط الحزمة المطابقة والا يمنع المزيد من حركة المرور في هذا االتصال.

رفض— يقوم بإنشاء حدث، وإسقاط الحزمة المطابقة، ومنع حركة المرور اإلضافية في هذا االتصال وإرسال إعادة تعيين TCP إذا كان بروتوكول TCP لمضيف المصدر

والوجهة.

disable—لا يطابق حركة مرور البيانات مع هذه القاعدة. لم يتم إنشاء أي أحداث.

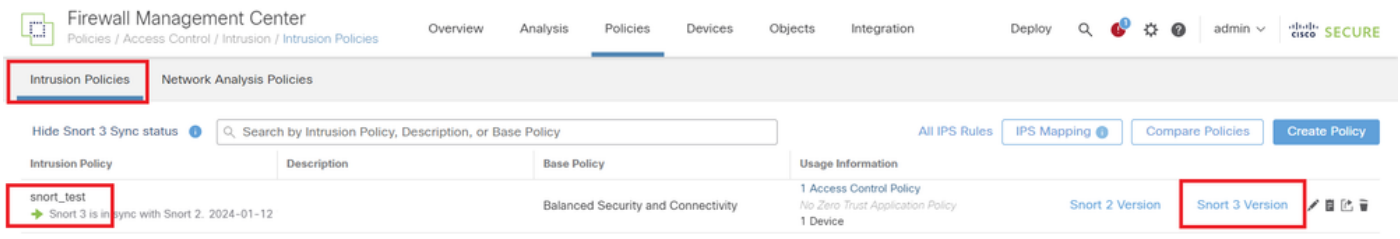
الافتراضي—يرجع إلى الإجراء الافتراضي للنظام.



إجراء تحرير القاعدة

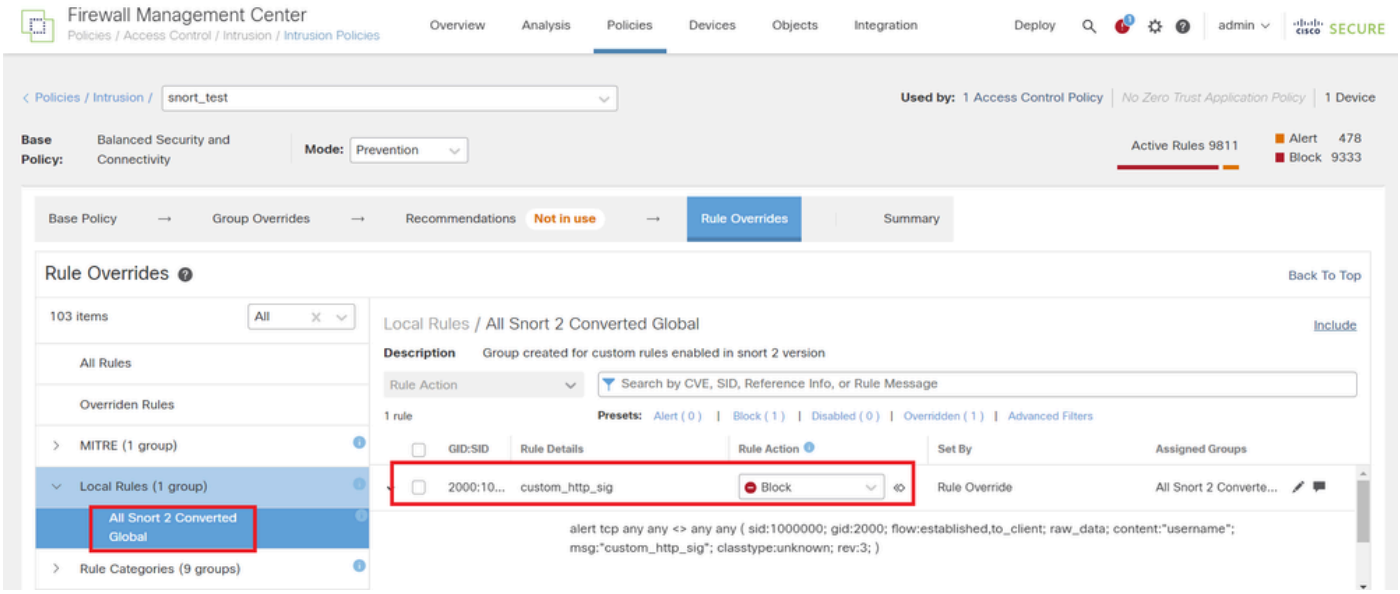
الخطوة 5. تأكيد قاعدة الشخيرات المحلية المخصصة المستوردة

انتقل إلى السياسات > سياسات الاقتحام على FMC، انقر فوق إصدار Snort 3 المقابل لنهج الاقتحام الهدف في الصف.



تأكيد القاعدة المخصصة المستوردة

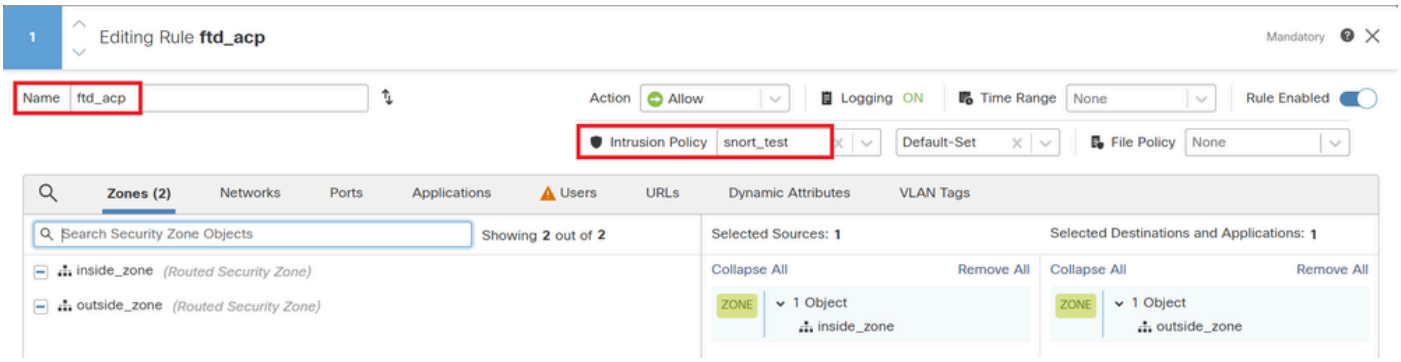
انقر فوق القواعد المحلية > كافة المحولات العمومية المحولة ل Snort 2 للتحقق من تفاصيل قاعدة الشنجة المحلية المخصصة.



تأكيد القاعدة المخصصة المستوردة

الخطوة 6. ربط سياسة التسلل بقاعدة سياسة التحكم في الوصول (ACP)

انتقل إلىPolicies>وحدة التحكم في الوصول من خلال FMC، أربط سياسة الاقتحام مع ACP.



القاترار بقاعدة ACP

الخطوة 7. نشر التغييرات

نشر التغييرات على FTD.

نشر التغييرات

الطريقة 2. تحميل ملف محلي

الخطوة 1. تأكيد إصدار Snort

نفس الخطوة 1 في الطريقة 1.

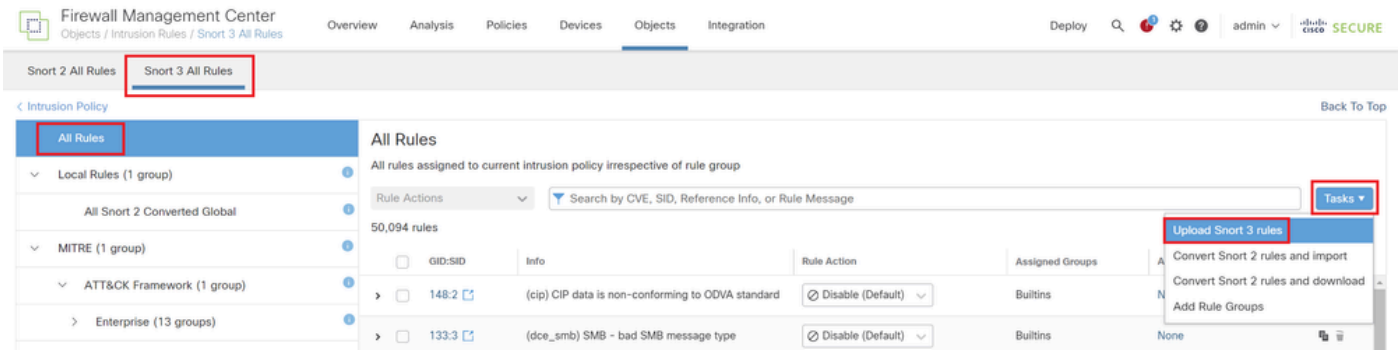
الخطوة 2. إنشاء قاعدة شرخيات محلية مخصصة

قم بإنشاء قاعدة بيانات محلية مخصصة وحفظها يدويا في ملف محلي يسمى custom-rules.txt.

```
alert tcp any any <> any any ( sid:1000000; flow:established,to_client; raw_data; content:"username"; m
```

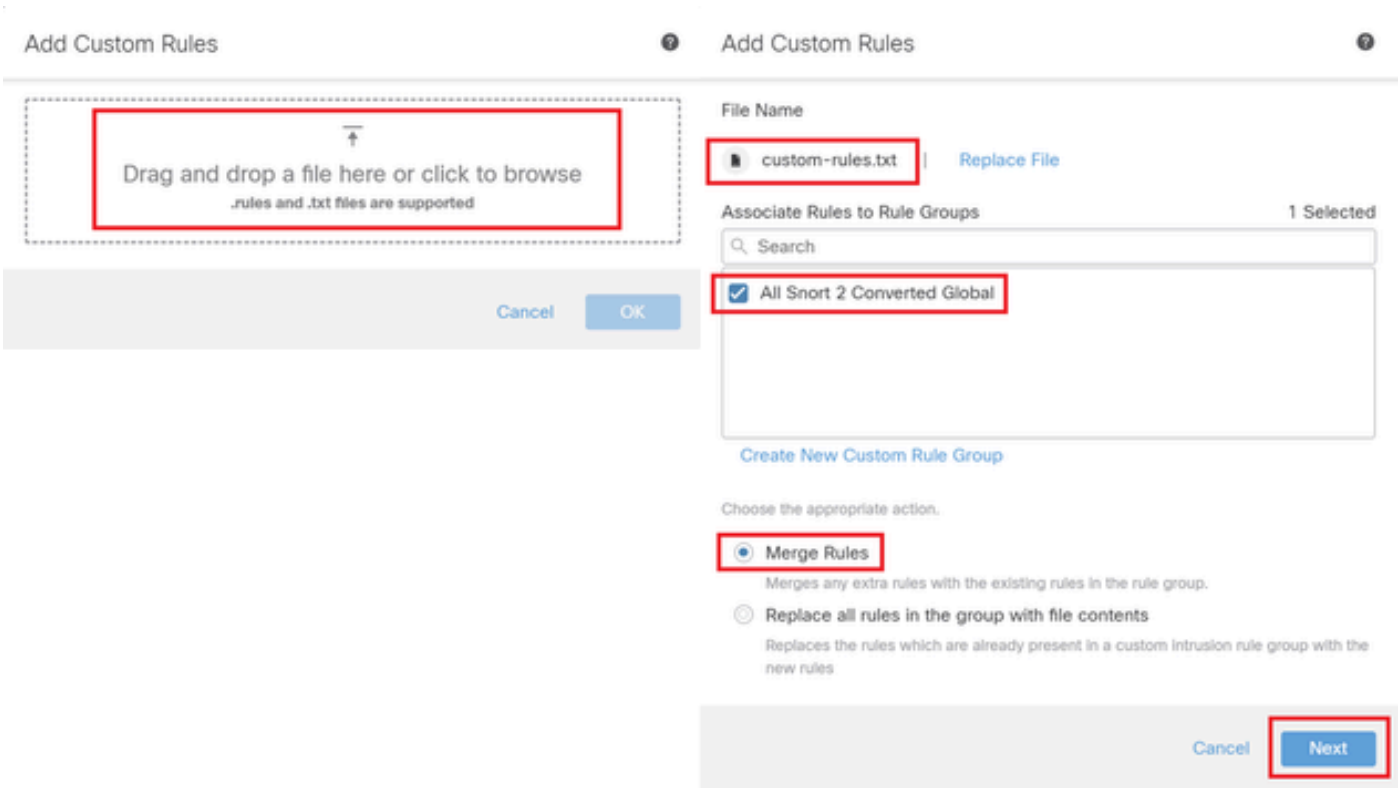
الخطوة 3. تحميل قاعدة الشخر المحلي المخصص

انتقل إلى كائنات > قواعد الاقتحام > Snort 3 كافة القواعد > جميع القواعد على FMC، انقر فوق تحميل قواعد Snort 3 من قائمة تسريح المهام.



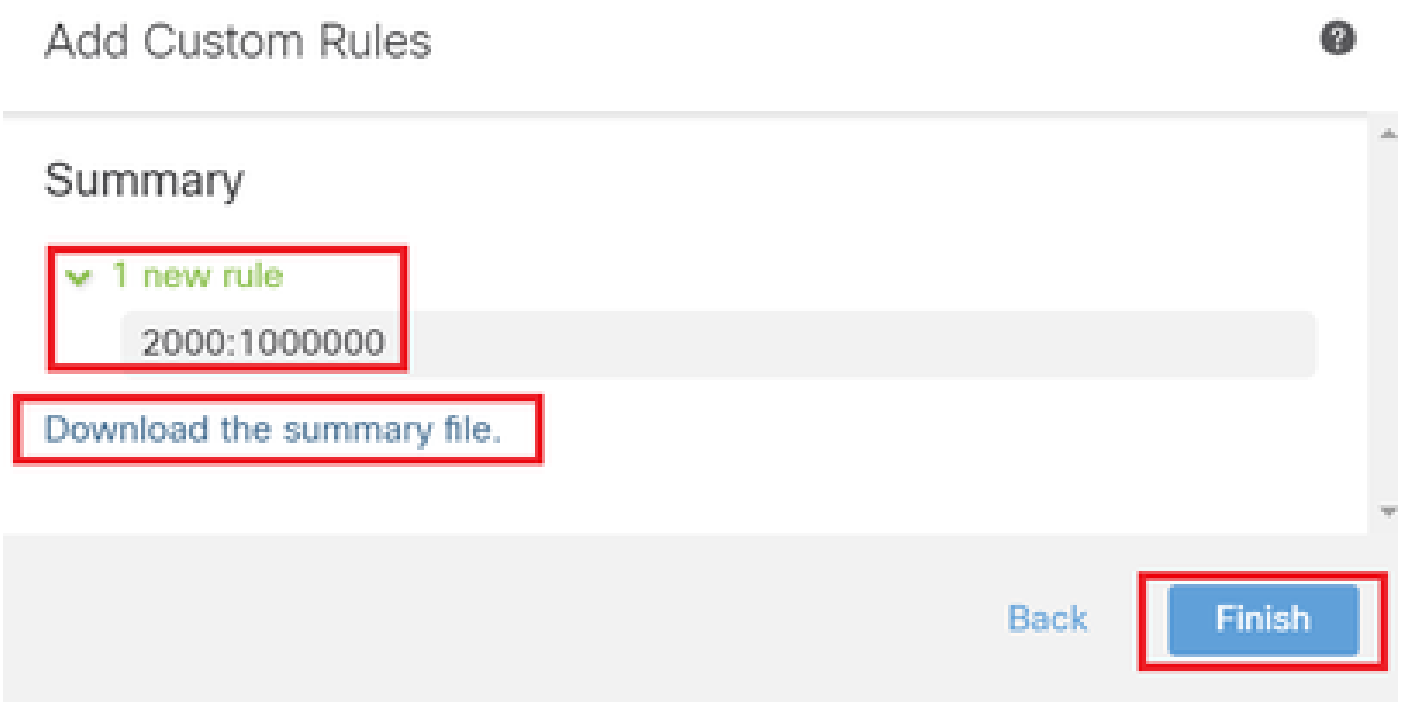
تحميل القاعدة المخصصة

في شاشة إضافة قواعد مخصصة، قم بسحب وإفلات ملف custom-rules.txt المحلي، حدد مجموعات القواعد والإجراء المناسب (دمج القواعد في هذا المثال)، ثم انقر زر التالي.



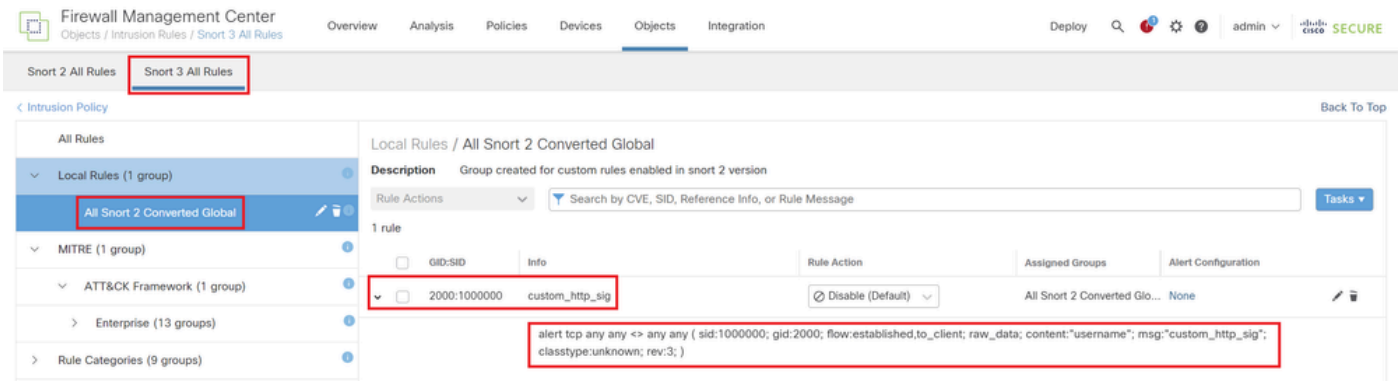
إضافة قاعدة مخصصة

تأكد من تحميل ملف القاعدة المحلية بنجاح.



تأكيد نتيجة التحميل

انتقل إلى كائنات > قواعد التطفل > Snort 3 كافة القواعد على FMC، انقر فوق جميع المحولات العامة المحولة 2 لتأكيد قاعدة الشخ المحلي المخصص التي تم تحميلها.



تفاصيل القاعدة المخصصة

الخطوة 4. تغيير إجراء القاعدة

نفس الخطوة 4 في الطريقة 1.

الخطوة 5. تأكيد قاعدة الشخيرات المحلية المخصصة التي تم تحميلها

نفس الخطوة 5 في الطريقة 1.

الخطوة 6. ربط سياسة التسلل بقاعدة سياسة التحكم في الوصول (ACP)

نفس الخطوة 6 في الطريقة 1.

الخطوة 7. نشر التغييرات

نفس الخطوة 7 في الطريقة 1.

التحقق من الصحة

الخطوة 1. ضبط محتويات الملف في خادم HTTP

اضبط محتويات ملف test.txt على جانب خادم HTTP على اسم المستخدم.

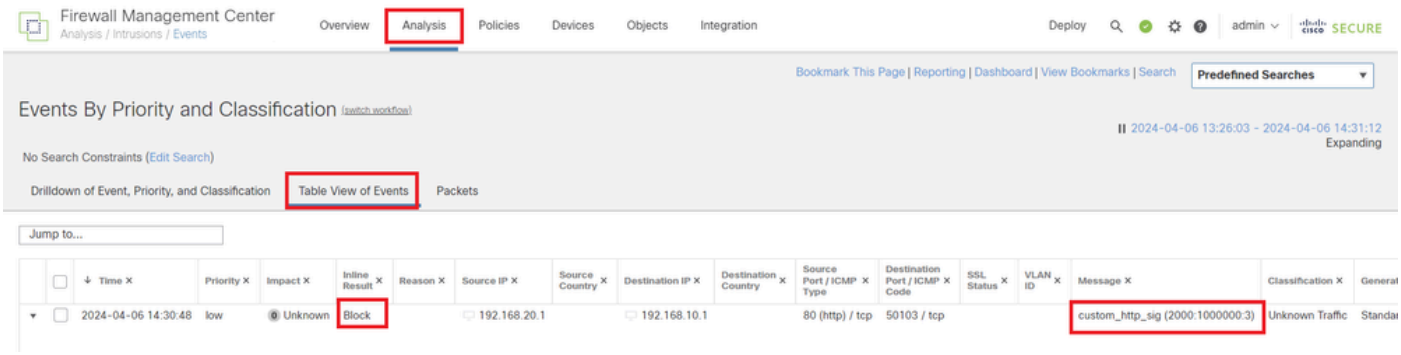
الخطوة 2. طلب HTTP الأولي

قم بالوصول إلى خادم HTTP (192.168.20.1/test.txt) من مستعرض العميل (192.168.10.1) وتأكد من حظر اتصال HTTP.

طلب HTTP الأولي

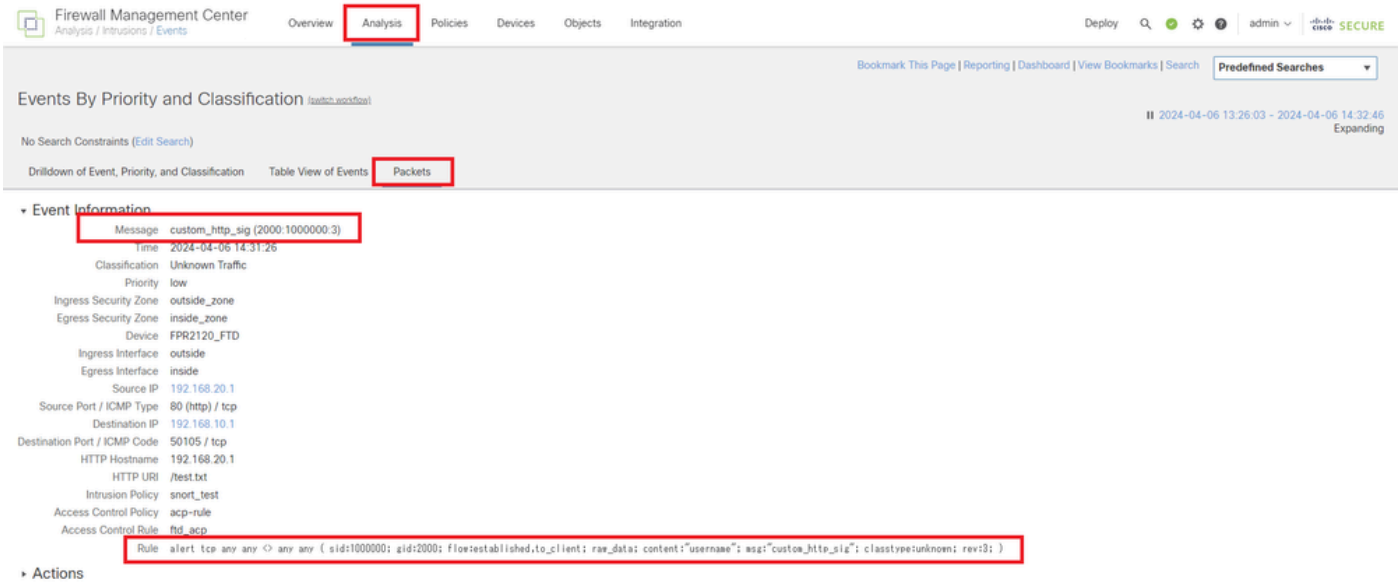
الخطوة 3. تأكيد حدث التطفل

انتقل إلىAnalysis>Intrusion>EventSon FMC، أكد أن حدث Intrusion تم إنشاؤه بواسطة قاعدة الشنجة المحلية المخصصة.



حدث إقتحام

ClickPacketStab، تأكيد تفاصيل حدث التطفل.



تفاصيل حدث الاقتحام

الأسئلة المتداولة (FAQ)

س : ما هو الموصى به ، نورت 2 أو نورت 3 ؟
أ: بالمقارنة مع Snort 2، يوفر Snort 3 سرعات معالجة محسنة ومميزات جديدة، مما يجعله الخيار الموصى به بشكل أكبر.

س: بعد الترقية من إصدار FTD قبل الإصدار 7. 0 إلى الإصدار 7. 0 أو إصدار أحدث، هل يتم تحديث إصدار snort تلقائيا إلى الإصدار 3 ؟
ال ، محرك التفتيش ال يزال في شورت 2. الاستخدام Snort 3 بعد الترقية، يجب تمكينه بشكل صريح. الاحظ أنه من المخطط إهمال إصدار Snort 2 في المستقبل وأنه من المستحسن بشدة التوقف عن إستخدامه الآن.

س : هل من الممكن تحرير قاعدة مخصصة موجودة في النصف الثالث ؟
أ: ال، ال يمكنك تحريره. لتحرير قاعدة مخصصة معينة، يجب حذف القاعدة ذات الصلة وإعادة إنشائها.

استكشاف الأخطاء وإصلاحها

قم بتشغيل system support trace الأمر لتأكيد السلوك على FTD. في هذا المثال، يتم حظر حركة مرور HTTP بواسطة قاعدة IPS (2000:100000:3).

<#root>

>

system support trace

```
Enable firewall-engine-debug too? [n]: y
Please specify an IP protocol: tcp
Please specify a client IP address: 192.168.10.1
```

```
Please specify a client port:
Please specify a server IP address: 192.168.20.1
Please specify a server port:

192.168.10.1 50104 -> 192.168.20.1 80 6 AS=0 ID=4 GR=1-1 Firewall: allow rule, '

ftd_acp

', allow

192.168.20.1 80 -> 192.168.10.1 50103 6 AS=0 ID=4 GR=1-1

Event

:

2000:1000000:3

, Action

block


192.168.20.1 80 -> 192.168.10.1 50103 6 AS=0 ID=4 GR=1-1 Verdict: blacklist
192.168.20.1 80 -> 192.168.10.1 50103 6 AS=0 ID=4 GR=1-1 Verdict Reason:

ips, block
```

المرجع

دليل تكوين برنامج Cisco Secure Firewall Management Center 3

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).