# أستكشاف أخطاء الاتصال الضار باستخدام جدار حماية المضيف وإصلاحها

## المحتويات



## المقدمة

يصف هذا المستند كيفية اكتشاف الاتصالات الضارة على نقطة نهاية Windows وحظرها باستخدام جدار حماية المضيف في نقطة النهاية الآمنة من Cisco.

## المتطلبات الأساسية

### المتطلبات

- يتوفر جدار حماية المضيف مع ميزة نقطة النهاية الآمنة وحزم Premier.
- إصدارات الموصل المدعومة
  - نظام التشغيل Windows (x64): موصل Windows الآمن لنقطة النهاية 8.4.2 والإصدارات الأحدث.
  - نظام التشغيل Windows (ARM): Secure Endpoint Windows Connector 8.4.4 والإصدارات الأحدث.

### المكونات المستخدمة

ال يقتصر هذا المستند على إصدارات برامج ومكونات مادية معينة.

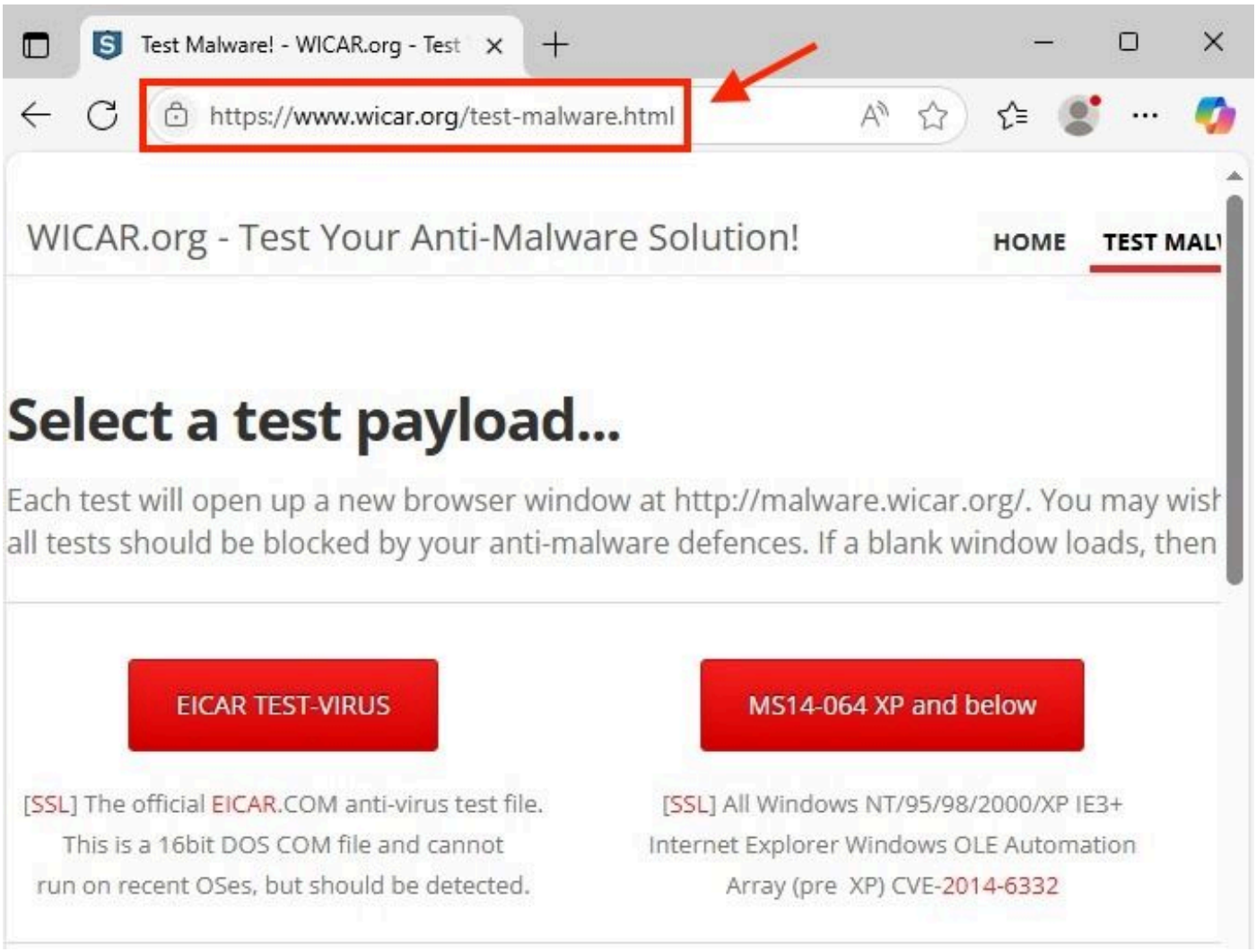
تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

## دليل أستكشاف الأخطاء وإصلاحها

يقدم هذا المستند دليل لحظر الاتصالات الضارة باستخدام جدار حماية مضيف نقطة النهاية الآمنة من Cisco. للاختبار، تستخدم صفحة الاختبار malware.wicar.org (208.94.116.246) لإنشاء دليل أستكشاف الأخطاء وإصلاحها.

## خطوات التعرف على الاتصالات الضارة وحظرها

1. أولا، تحتاج إلى تحديد عنوان URL أو عنوان IP الذي تريد مراجعته وحظره. بالنسبة لهذا السيناريو، تفضل بزيارة موقع الويب consider malware.wicar.org.
2. تحقق مما إذا كان الوصول إلى عنوان URL هو successful. malware.wicar.org يعيد التوجيه إلى عنوان URL مختلف، كما هو موضح في الصورة.




عنوان URL ضار للمستعرض

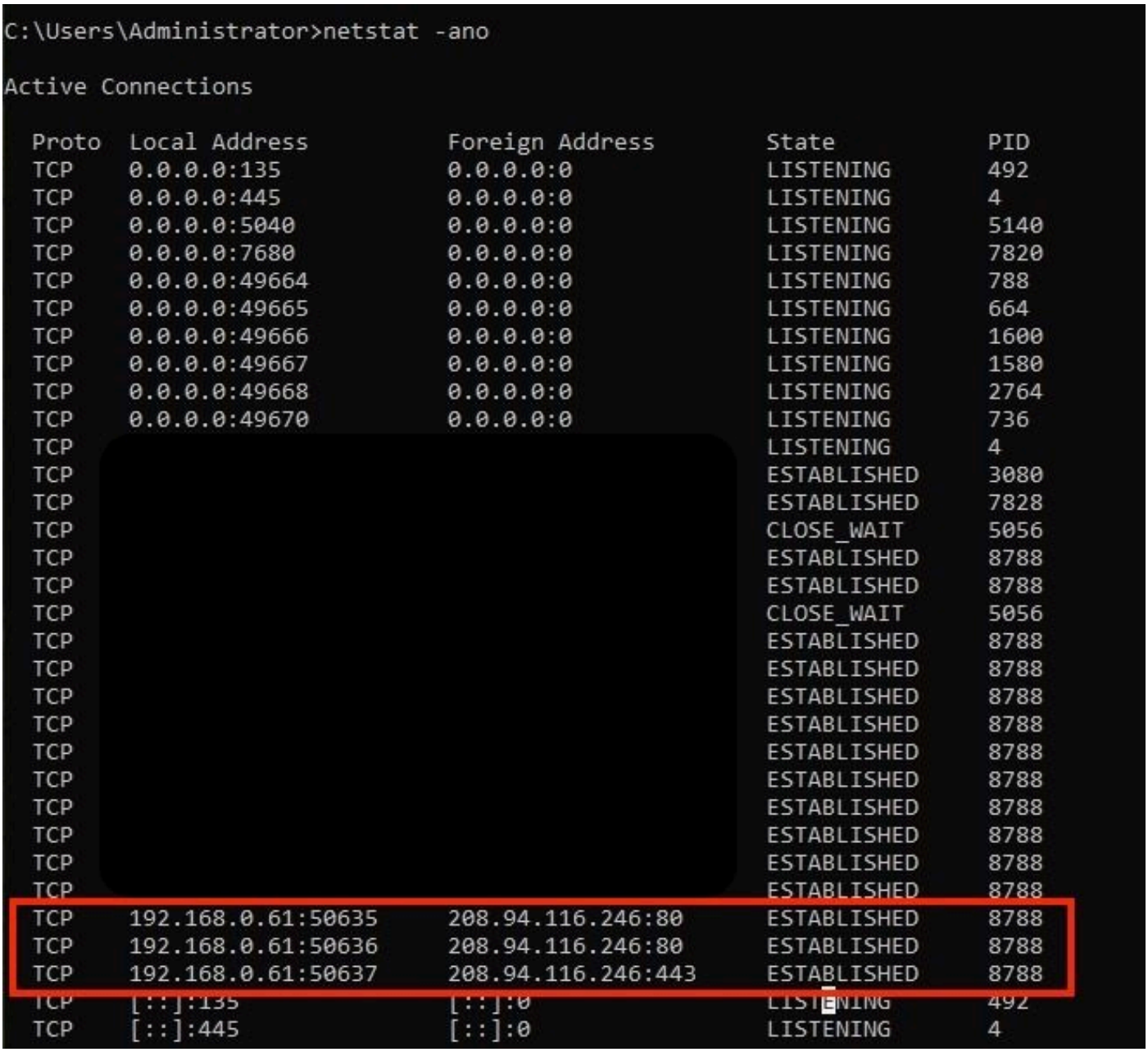
3. أستخدم الأمر nslookup لاسترداد عنوان IP المرتبط بعنوان URL malware.wicar.org.

```
C:\Users\Administrator>nslookup malware.wicar.org
Server:  dns-nextengo
Address:  10.2.9.164

Non-authoritative answer:
Name:    wicarmalware.nfshost.com
Addresses:  2607:ff18:80:6::6a08
          208.94.116.246
Aliases:  malware.wicar.org
```

إخراج nslookup

4. بمجرد الحصول على عنوان IP الضار، تحقق من الاتصالات النشطة على نقطة النهاية باستخدام الأمر:netstat -ano.




Netstat لكافة الاتصالات

5. لعزل الاتصالات النشطة، قم بتطبيق عامل تصفية لعرض الاتصالات التي تم إنشاؤها فقط.

```
C:\Users\Administrator>netstat -ano | findstr ESTABLISHED
  TCP                                                    ESTABLISHED     3080
  TCP                                                    ESTABLISHED     7828
  TCP                                                    ESTABLISHED     8788
  TCP                                                    ESTABLISHED     8788
  TCP                                                    ESTABLISHED     8788
  TCP                                                    ESTABLISHED     8788
  TCP                                                    ESTABLISHED     8788
  TCP                                                    ESTABLISHED     8788
  TCP                                                    ESTABLISHED     8788
  TCP                                                    ESTABLISHED     8788
  TCP    192.168.0.61:50635     208.94.116.246:80       ESTABLISHED     8788
  TCP    192.168.0.61:50636     208.94.116.246:80       ESTABLISHED     8788
  TCP    192.168.0.61:50637     208.94.116.246:443      ESTABLISHED     8788

C:\Users\Administrator>
```

netstat للاتصالات الثابتة

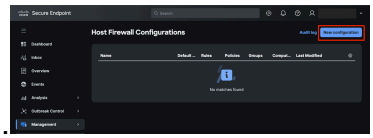
6. ابحث عن عنوان IP الذي تم الحصول عليه من DisplayCommand في الإخراج السابق. عينت المصدر ip، غاية ip، مصدر ميناء، وغاية ميناء.

- IP المحلي: 192.168.0.61
- IP عن بعد: 208.94.116.246
- المنفذ المحلي: غير قابل للتطبيق
- الوجهة بورتو 80 و 443

7. بمجرد الحصول على هذه المعلومات، انتقل إلى بوابة نقطة النهاية الآمنة من Cisco لإنشاء تكوين جدار حماية المضيف.

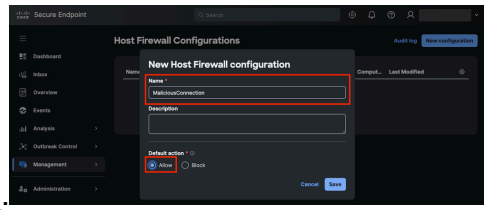
## تكوين جدار حماية المضيف وإنشاء القاعدة

1. انتقل إلى الإدارة > مضيف جدار الحماية انقر فوق تكوين جديد.

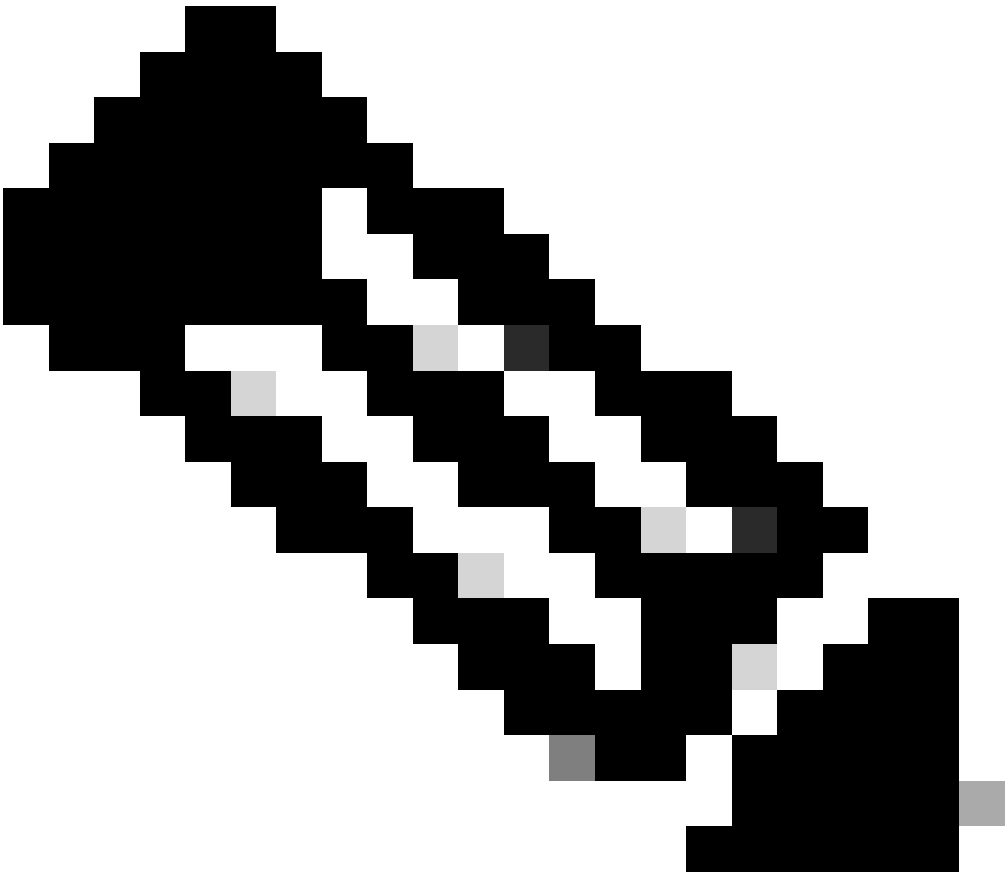



التكوين الجديد لجدار حماية المضيف

2. حدد اسم والإجراء الافتراضي. في هذه الحالة، حدد السماح.

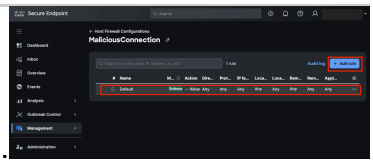



اسم تكوين جدار حماية المضيف والإجراء الافتراضي



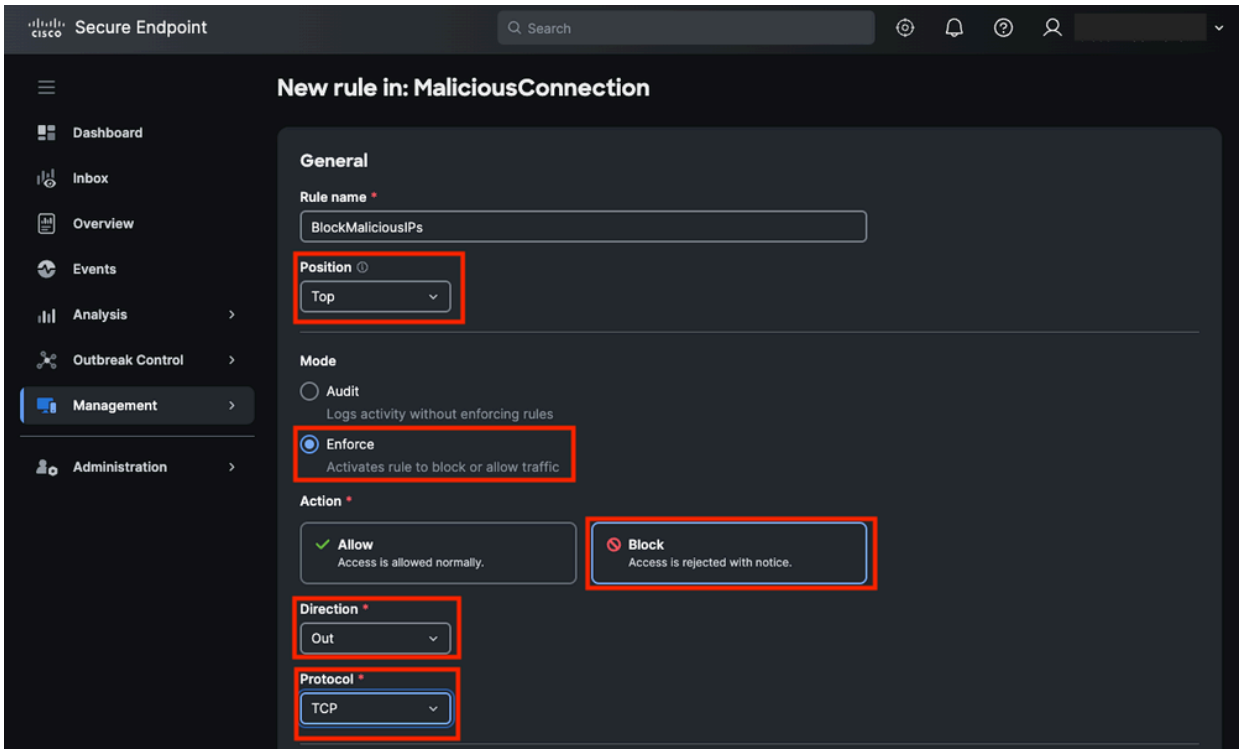
ملاحظة: تذكر أنك تقوم بإنشاء قاعدة حظر، ولكن يجب أن تسمح لحركة المرور الأخرى بتجنب التأثير على الاتصالات الشرعية.

3. تحقق من إنشاء القاعدة الافتراضية وانقر فوق إضافة قاعدة.

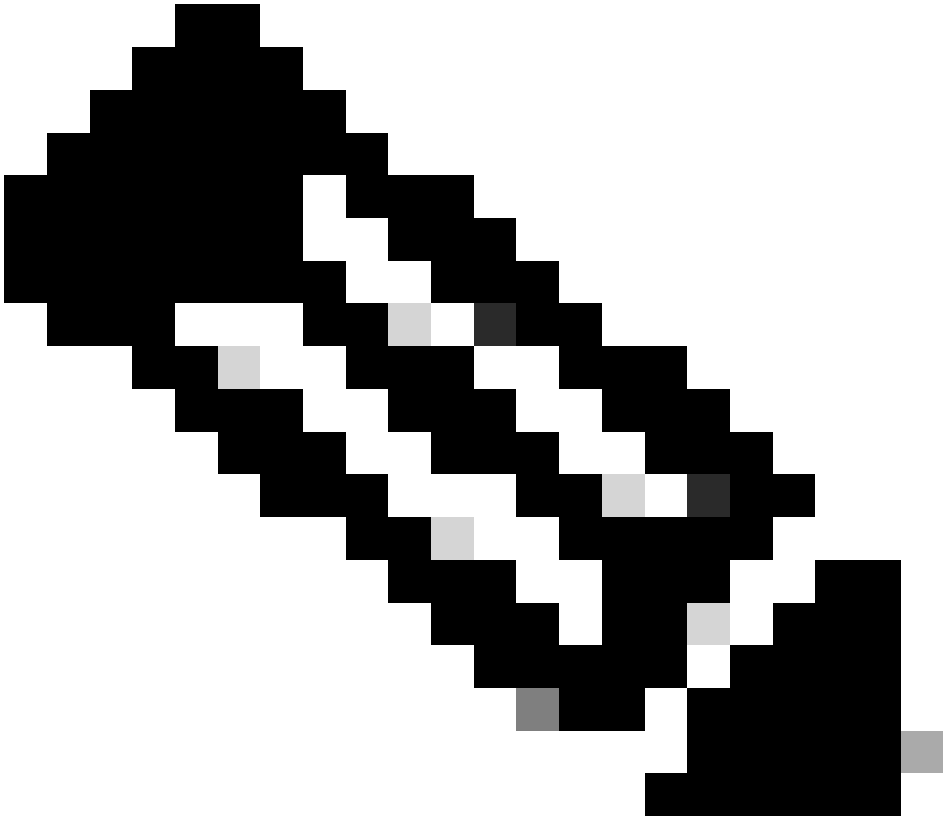


إضافة قاعدة في جدار حماية المضيف

4. قم بتعيين اسم وتعيين المعلمات التالية:
   - الموضع: أعلى
   - الوضع: فرض
   - الإجراء: حظر
   - الإتجاه: خارج
   - البروتوكول: TCP

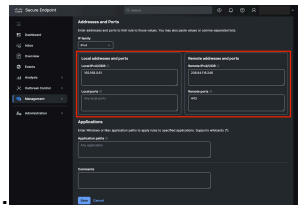



محددات القاعدة العامة



ملاحظة: عندما تخاطب إتصالات خبيثة من نقطة نهاية داخلية إلى وجهة خارجية، عادة إلى الإنترنت، الإتجاه يستطيع دائما كنت خارج.

5. حدد عناوين IP المحلية والوجهة:
   - IP المحلي: 192.168.0.61
   - IP عن بعد: 208.94.116.246
   - أترك حقل PortField المحلي فارغا.



   - ثبتت الغاية ميناء إلى 80 و 443، هذا يرادف إلى HTTP و HTTPS.

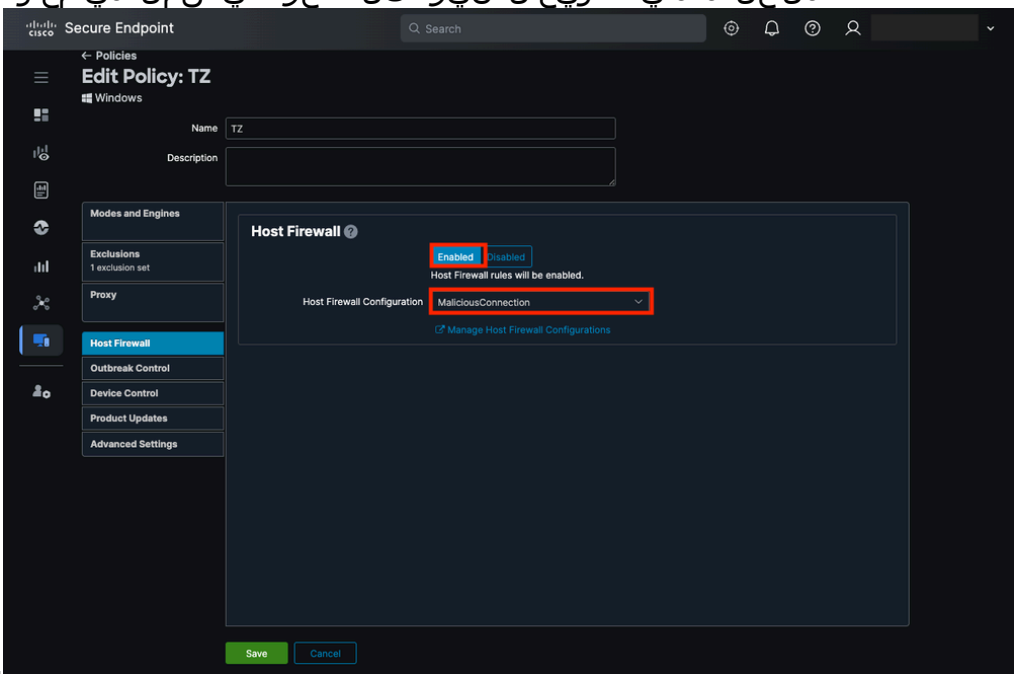
عناوين القاعدة والمنافذ

6. أخيرا، انقر فوق حفظ.

## تمكين جدار حماية المضيف في السياسة وتعيين التكوين الجديد

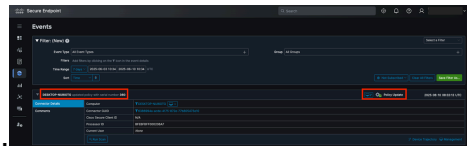
1. في مدخل نقطة النهاية الآمنة، انتقل إلى الإدارة > السياسات وحدد السياسة المرتبطة بنقطة النهاية حيث تريد حظر النشاط الضار.
2. انقر فوق Editand انتقل إلى علامة التبويب جدار الحماية للمضيف.

3. قم بتمكين ميزة جدار حماية المضيف وحدد التكوين الأخير، في هذه الحالة MaliciousConnection.




جدار حماية المضيف الذي تم تمكينه في نهج نقطة النهاية الآمنة

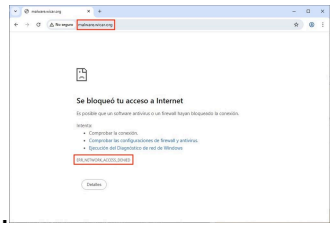
4. انقر فوق حفظ.




5. أخيرا، تحقق من تطبيق نقطة النهاية لتغييرات النهج.

حدث تحديث السياسة

## التحقق من صحة التكوين محليا




1. أستخدم عنوان URL malware.eicar.org في مستعرض لتأكيد حظره.

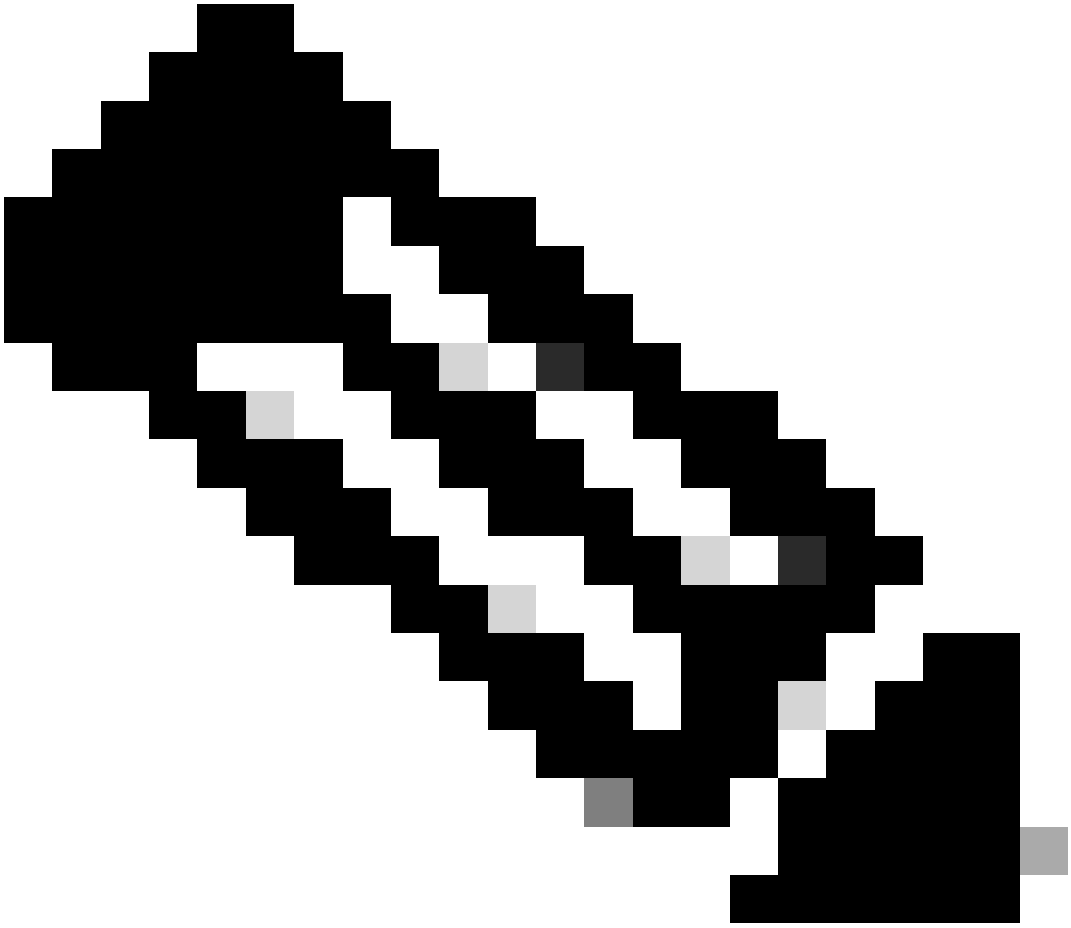
تم رفض الوصول إلى الشبكة عن طريق المستعرض

2. بعد تأكيد الحظر، تحقق من عدم تأسيس أية إتصالات. أستخدم الأمر netstat - ano | تم إنشاء FindSTR لضمان عدم ظهور IP المرتبط بعنوان URL الضار (208.94.116.246).

## مراجعة السجلات

1. على نقطة النهاية، انتقل إلى المجلد:

C:\Program Files\Cisco\AMP\<Connector version>\FirewallLog.csv



ملاحظة: يوجد ملف السجل في المجلد <install directory>\Cisco\AMP\<Connector version>\FirewallLog.csv

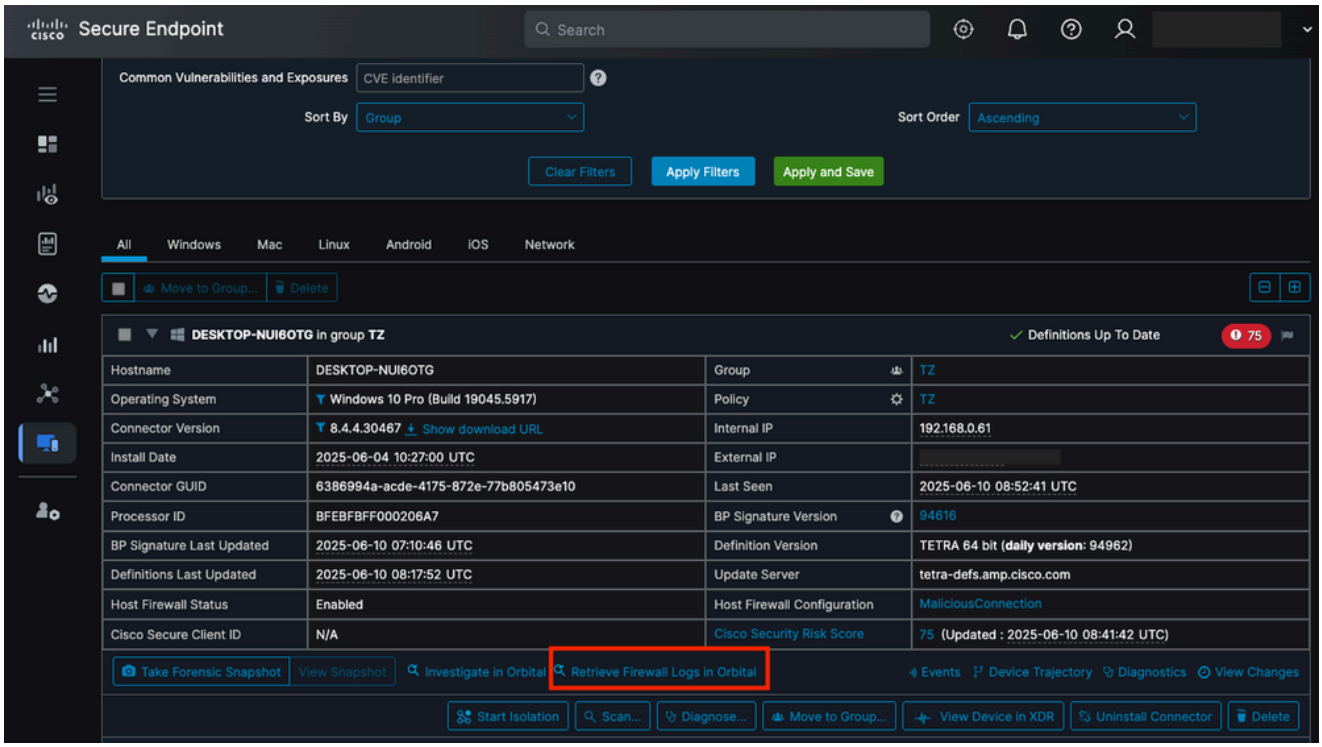
---

2. افتح ملف CSV للتحقق من التطابقات لقاعدة إجراء الحظر. أستخدم عامل تصفية للتمييز بين "السماح" واتصالات "الحظر".

سجلات جدار الحماية في ملف CSV

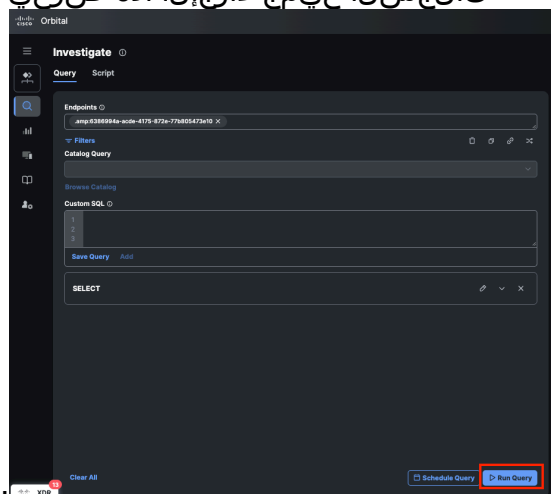
## إستخدام المدار لاسترداد سجلات جدار الحماية

1. في مدخل نقطة النهاية الآمنة، انتقل إلى الإدارة > أجهزة الكمبيوتر، وحدد موقع نقطة النهاية، وانقر فوق إسترداد سجلات جدار الحماية في المدار. يقوم هذا الإجراء بإعادة توجيهك إلى البوابة المدارية.



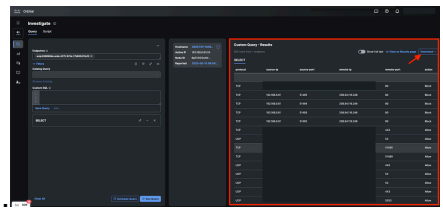

زر استرداد سجلات جدار الحماية في المدار

2. في المدخل المداري، انقر فوق تشغيل الاستعلام. يعرض هذا الإجراء جميع السجلات المسجلة على نقطة النهاية لجدار حماية المضيف.




تشغيل الاستعلام من المدار

3. تكون المعلومات مرئية في Resultstab، أو يمكنك تنزيلها.



نتائج الاستعلام من المدار

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).