حظر DNS باستخدام FirePOWER Management Center

المحتويات

المقدمة

يصف هذا المستند إجراء إضافة قائمة نظام اسم المجال (DNS) إلى نهج DNS حتى يمكنك تطبيقها باستخدام معلومات الأمان (SI).

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- تكوين الدفاع ضد التهديد ASA55XX من Cisco
- تكوين مركز إدارة FireSIGHT التابع لشركة Cisco

المكونات المستخدمة

- Cisco ASA5506W-X Threat Defense (75)، الإصدار 6.2.3.4 (Build 42)
- مركز إدارة Cisco Firepower ل VMWare إصدار البرنامج: 6.2.3.4 (بنية 42)نظام التشغيل: Cisco Fire Linux OS 6.2.3 (Build13)

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

معلومات أساسية

يعمل Security Intelligence عن طريق حظر حركة المرور من وأ إلى عناوين IP وأ عناوين URL وأ أسماء المجالات التي لها سمعة سيئة معروفة. في هذا المستند، يكون التركيز الرئيسي وه إدراج اسم المجال في القائمة السوداء.

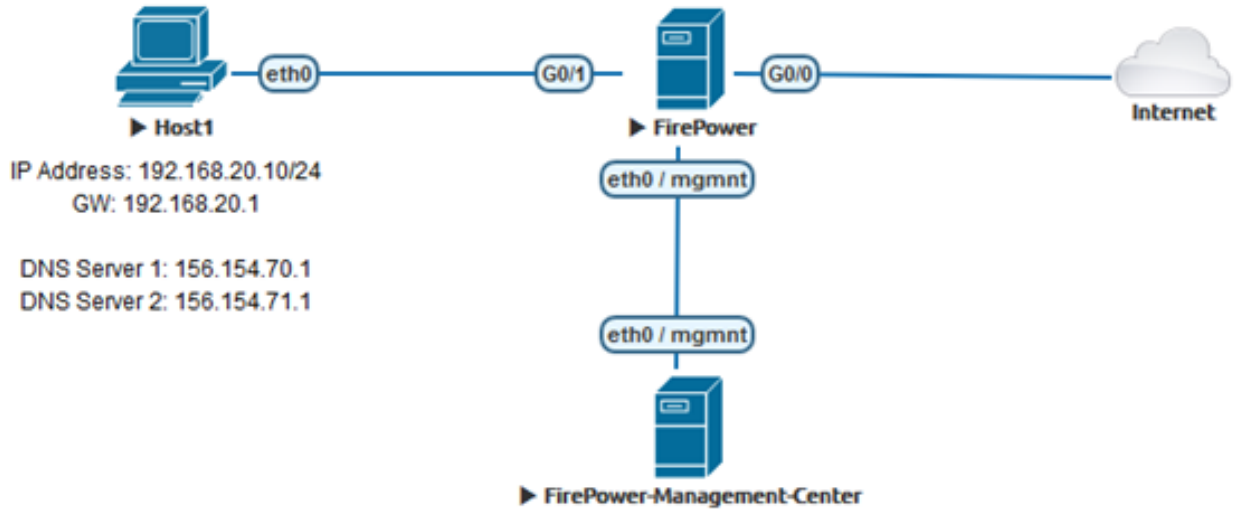
أستخدم المثال كتل 1 المجال:

- cisco.com

يمكنك إستخدام تصفية URL لحظر بعض هذه المواقع، ولكن المشكلة هي أن URL يجب أن يكون مطابقا تماما. ومن ناحية أخرى، يمكن أن تركز القائمة السوداء ل DNS مع SI على مجالات مثل "cisco.com" دون الحاجة إلى القلق حول أي مجالات فرعية أو تغييرات في URL.

في نهاية هذا المستند، يتم أيضا توضيح تكوين بطاقة Sinkhole إختياري.

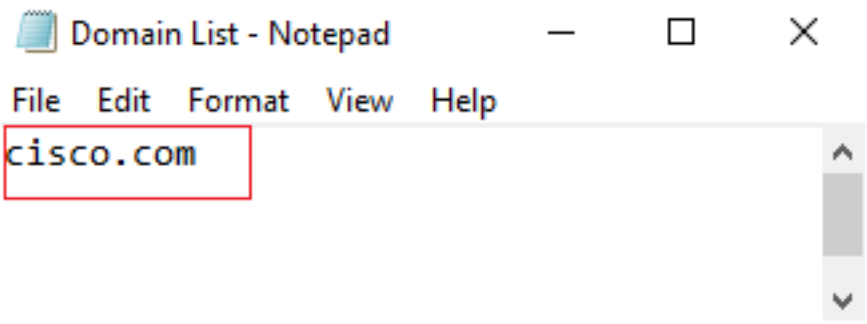
الرسم التخطيطي للشبكة



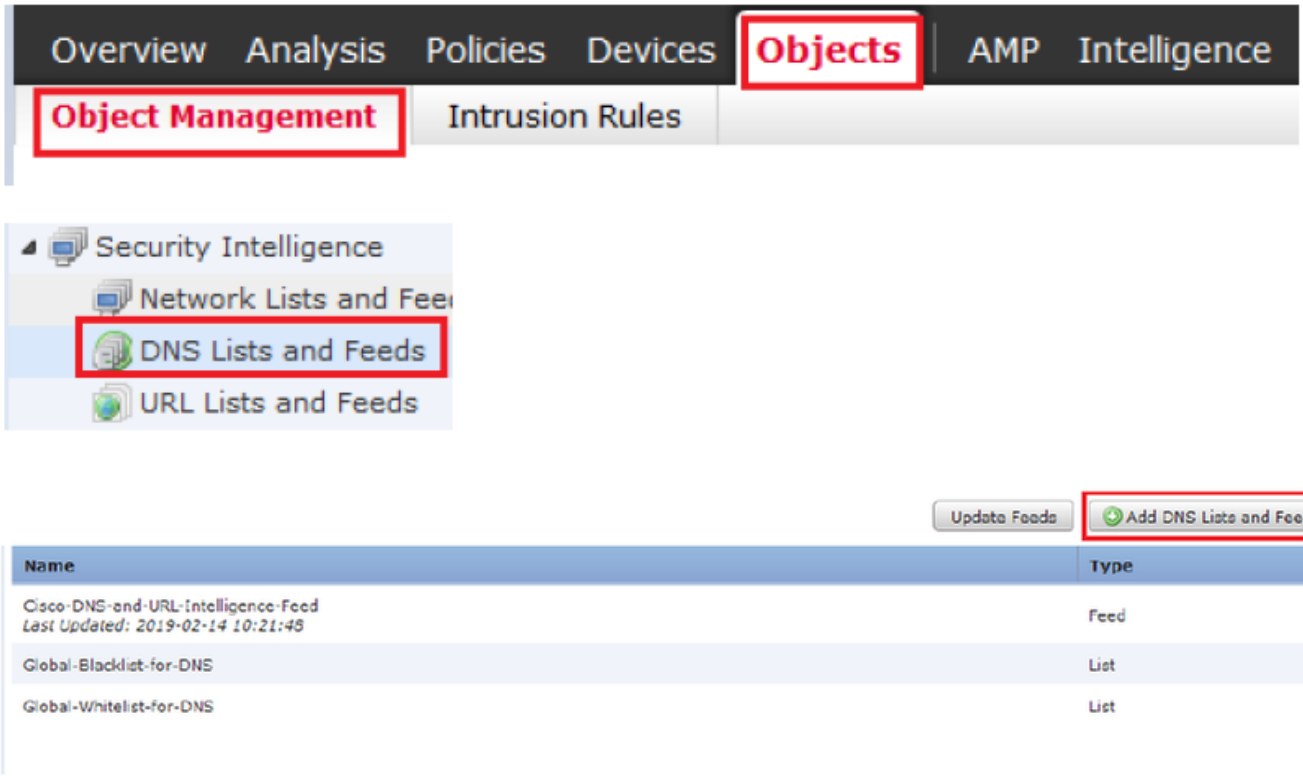
التكوين

تكوين قائمة DNS مخصصة باستخدام المجالات التي نريد حظر القائمة وتحميلها إلى FMC

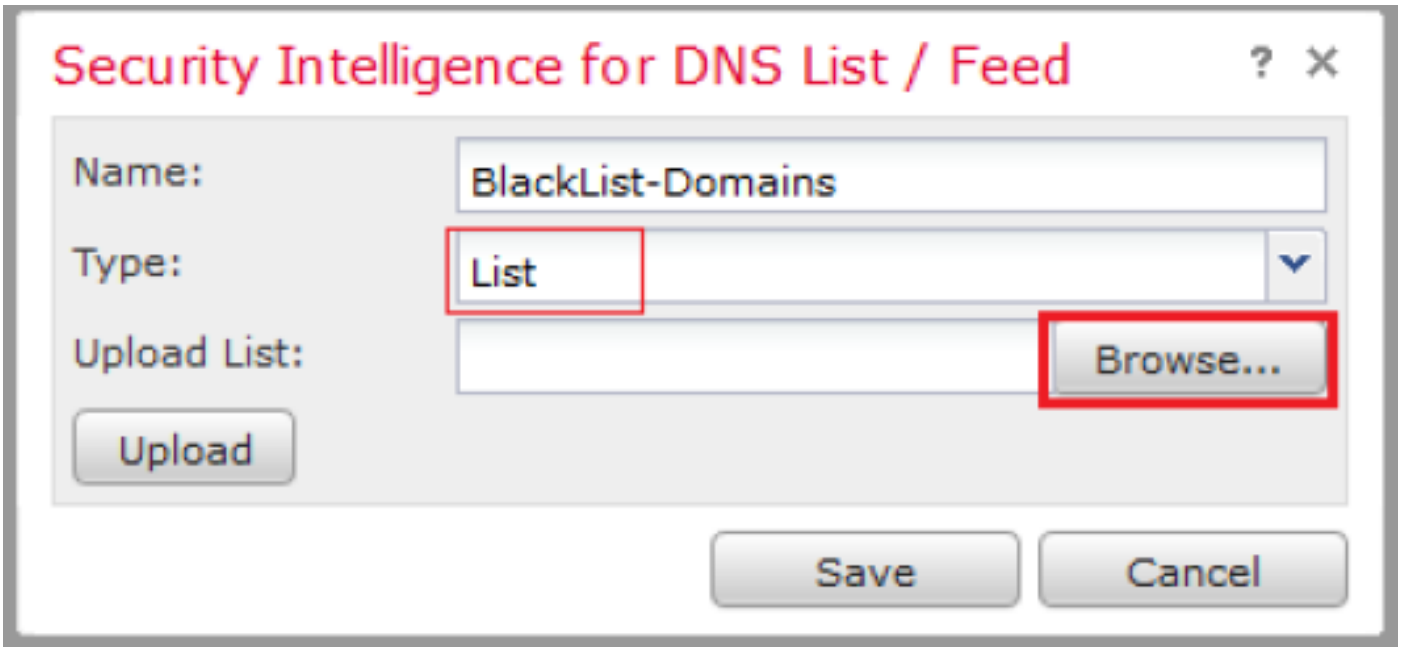
الخطوة 1. قم بإنشاء ملف .txt باستخدام المجالات التي تريد حظرها. احفظ ملف .txt على حاسبك:

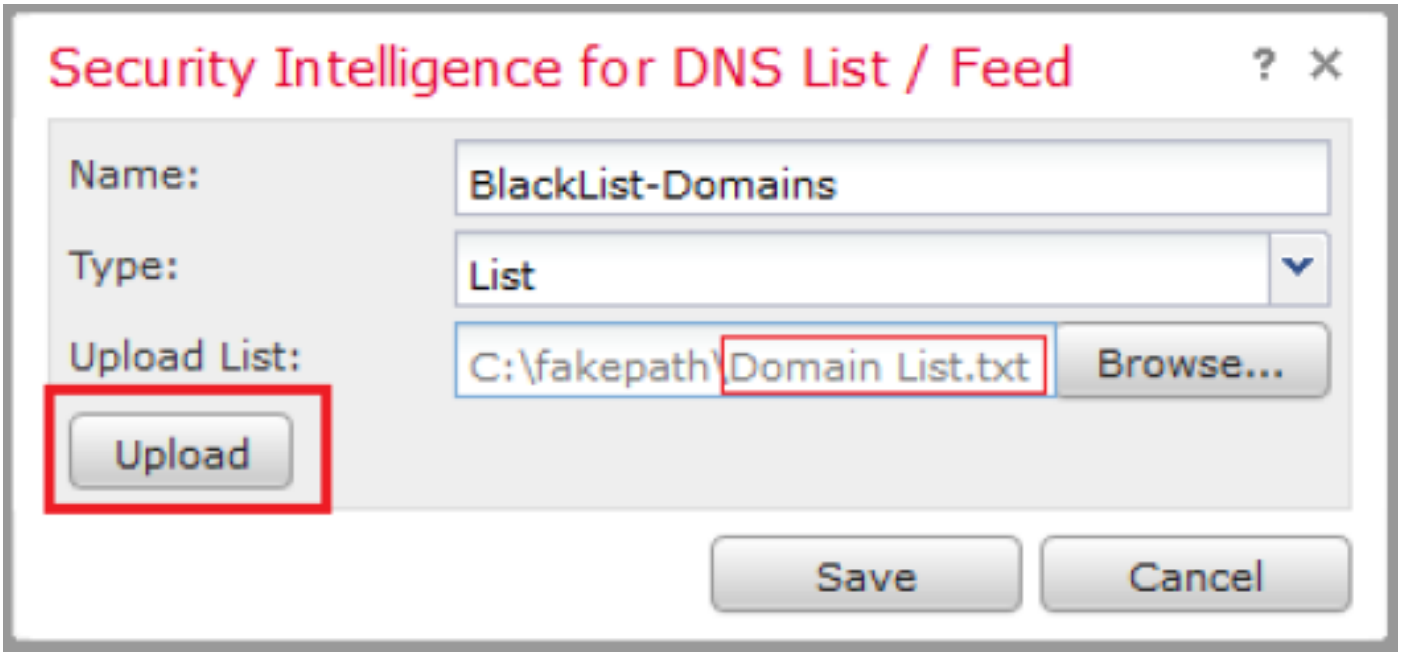


الخطوة 2. في FMC، انتقل إلى كائن >> إدارة الكائن >> قوائم DNS ونموذج ويب >> إضافة قائمة DNS ونموذج ويب.

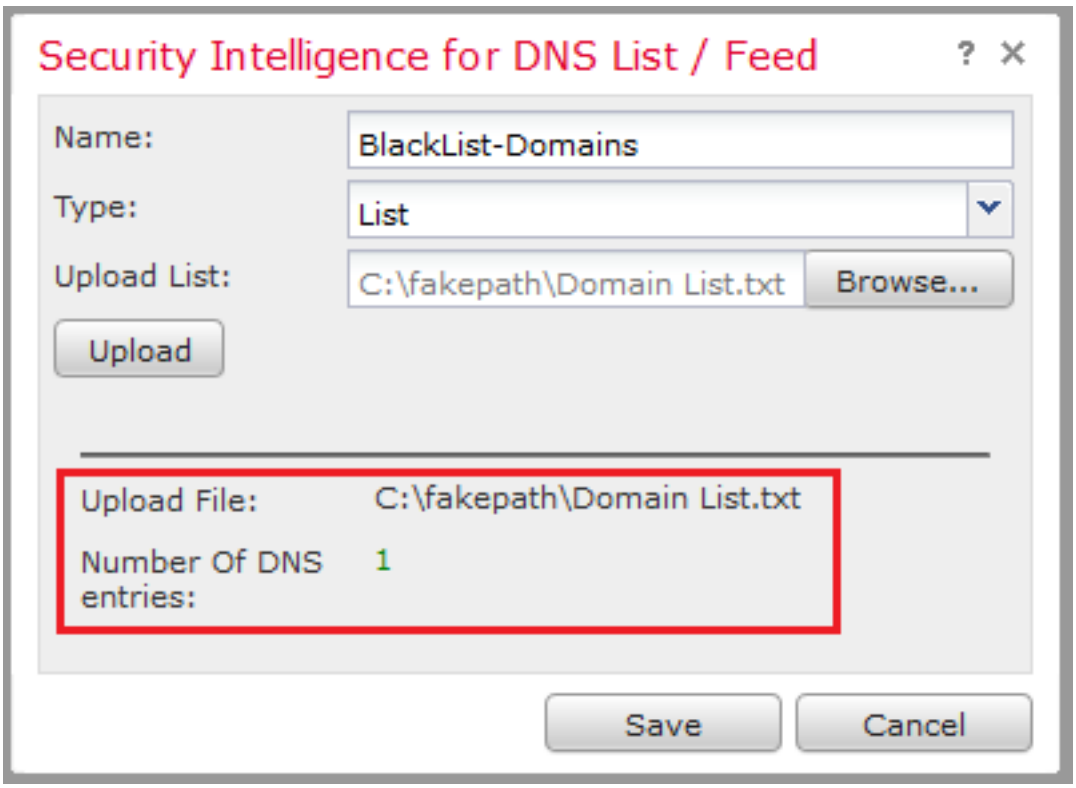


الخطوة 3. قم بإنشاء قائمة تسمى "BlackList-Domains"، ويجب أن يكون النوع قائمة ويجب تحميل ملف .txt مع المجالات المعنية كما هو موضح في الصور:





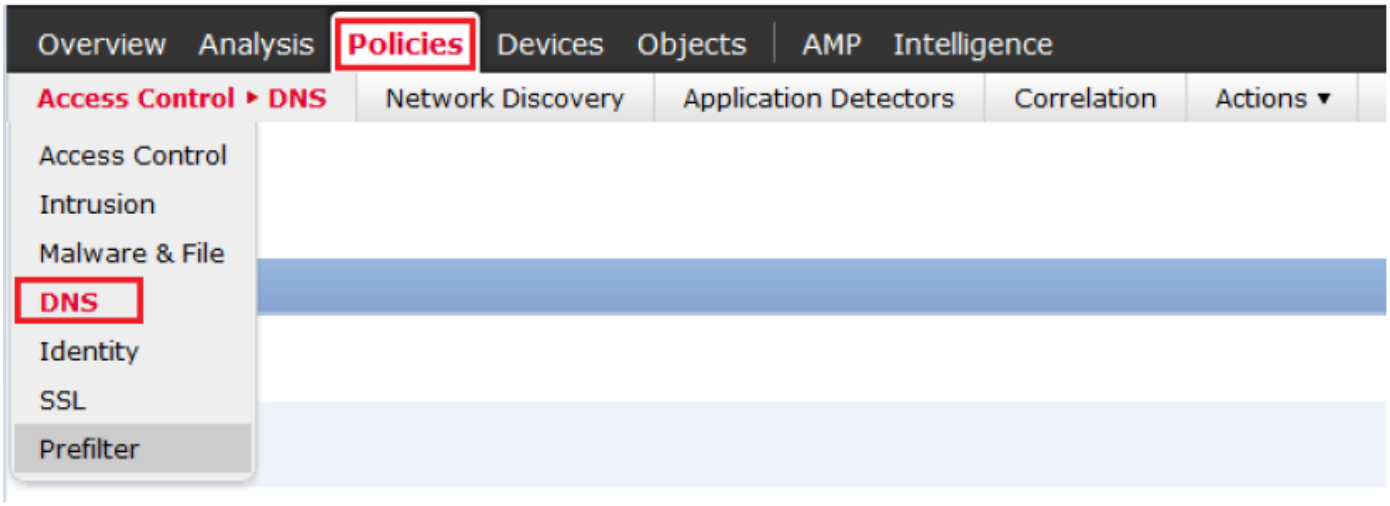
*لاحظ أنه عند تحميل ملف .txt، يجب أن يقرأ عدد إدخالات DNS جميع المجالات. في هذا المثال، إجمالي 1:

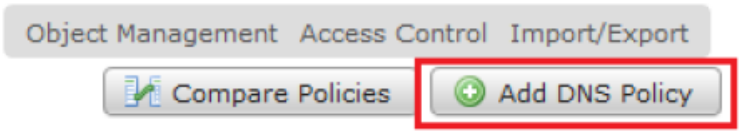


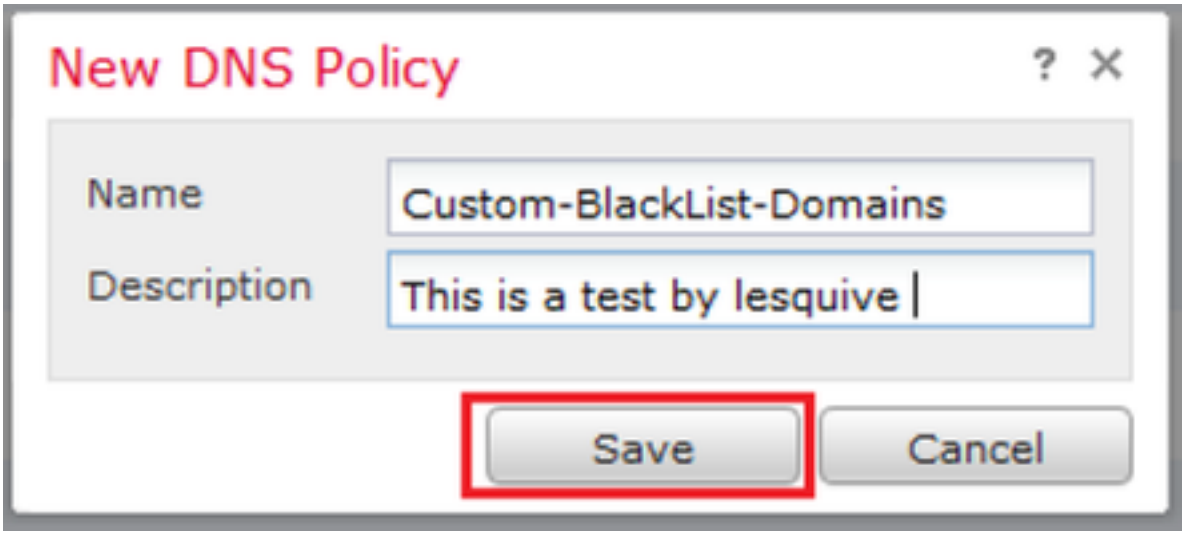
إضافة نهج DNS جديد باستخدام 'الإجراء الذي تم تكوينه ل 'المجال غير موجود'

*تأكد من إضافة منطقة مصدر وشبكة مصدر وقائمة DNS.

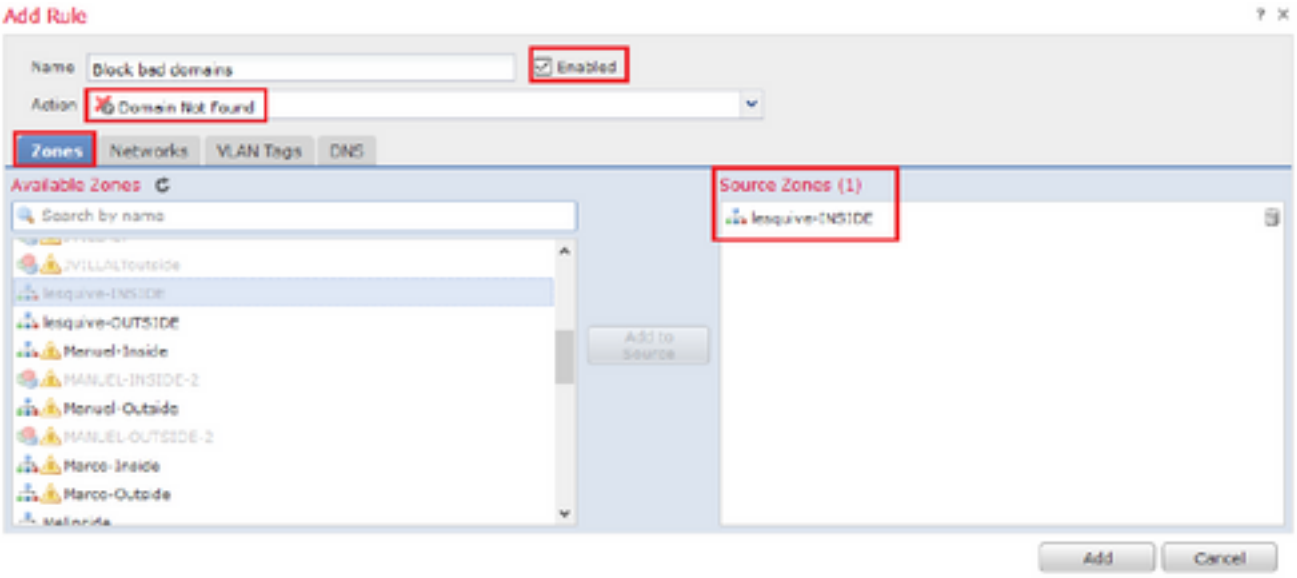
الخطوة 1. انتقل إلى السياسات >> التحكم في الوصول >> DNS >> إضافة سياسة DNS:

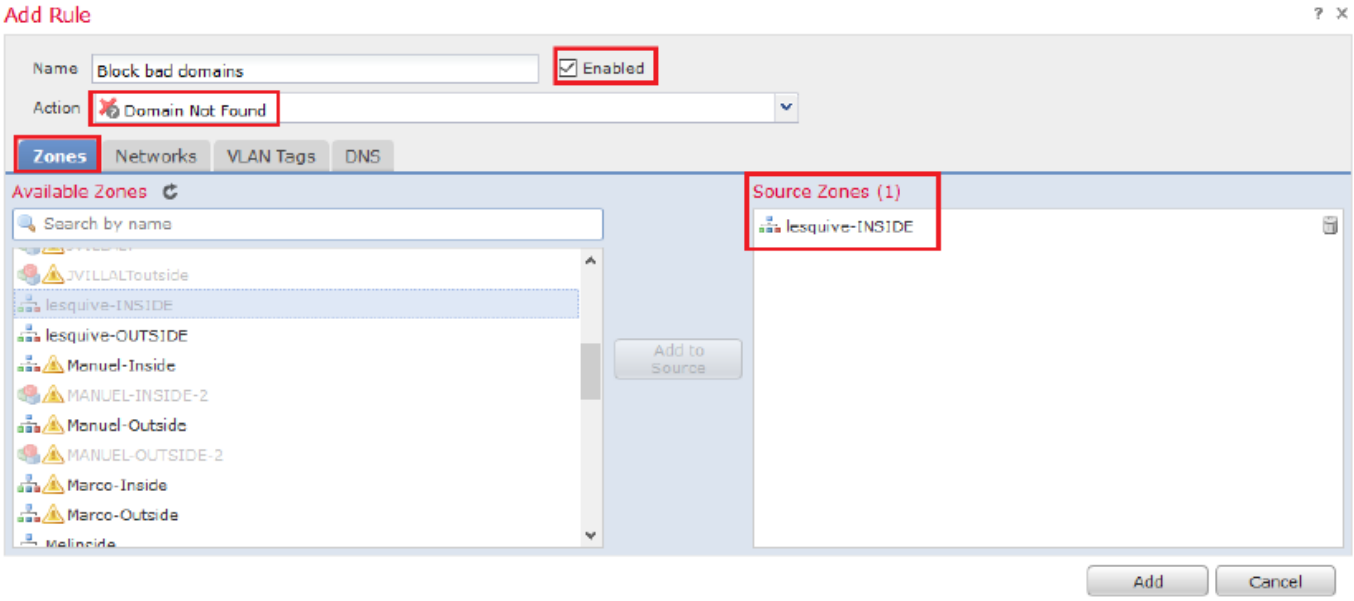


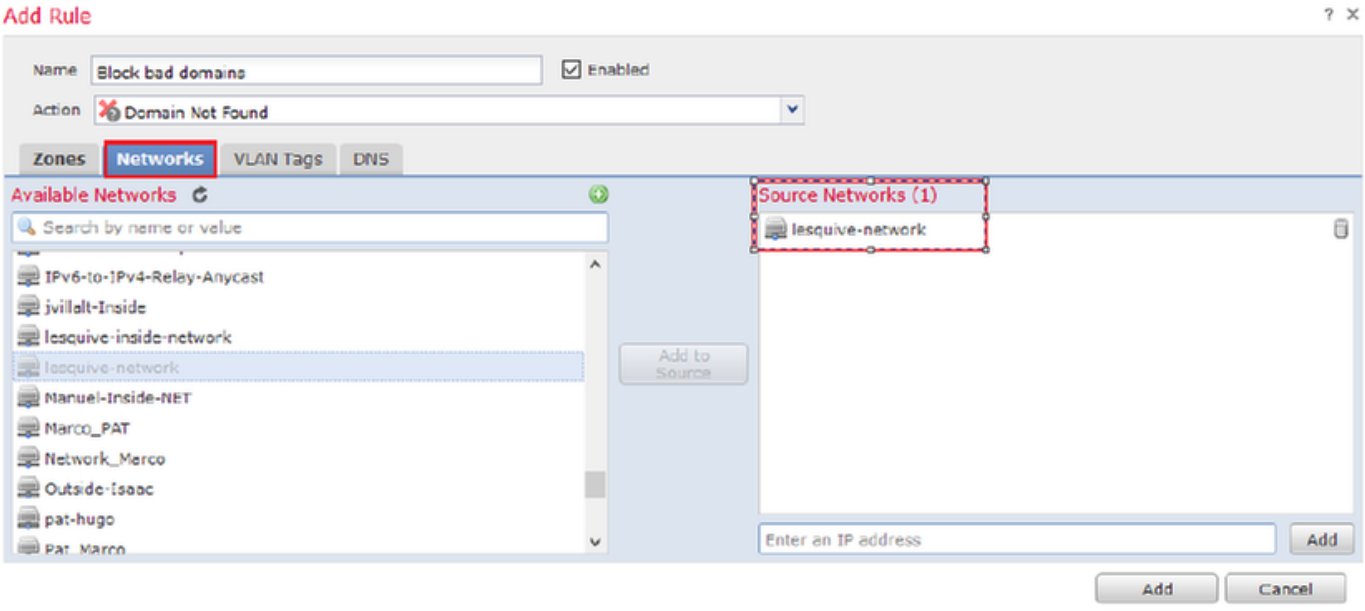


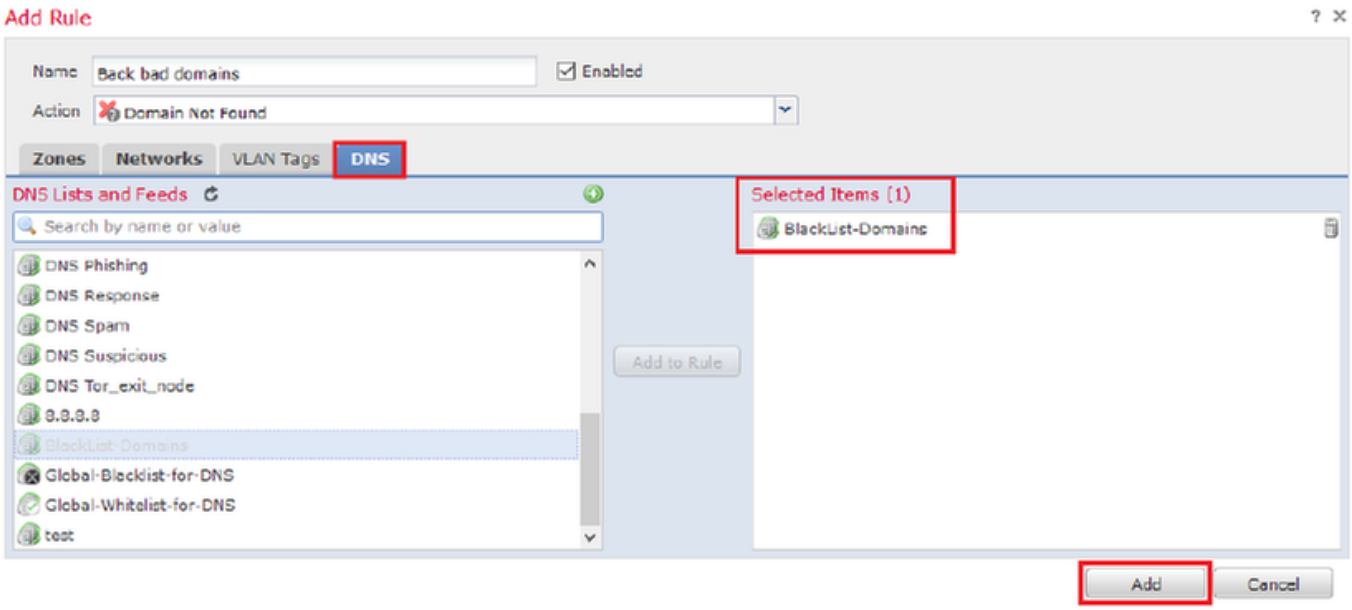


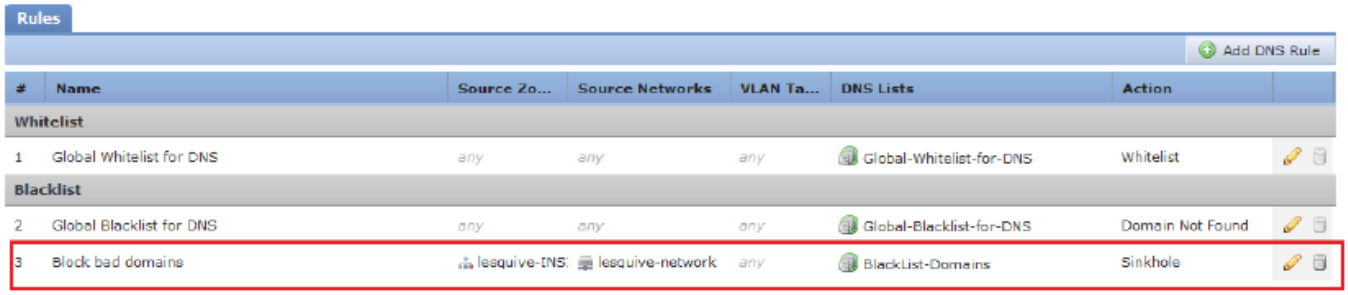
الخطوة 2. إضافة قاعدة DNS كما يظهر في الصورة:


Add Rule
Name
Block bad domains
Enabled
Action
Domain Not Found
Zones
Networks
VLAN Tags
DNS
Available Zones
Search by name
lesquive-OUTSIDE
Manuel-Inside
Manuel-Outside
Marco-Inside
Marco-Outside
Source Zones (1)
lesquive-INSIDE
Add to Source
Add
Cancel


Add Rule
Name
Block bad domains
Enabled
Action
Domain Not Found
Zones
Networks
VLAN Tags
DNS
Available Zones
Search by name
lesquive-INSIDE
lesquive-OUTSIDE
Manuel-Inside
MANUEL-INSIDE-2
Manuel-Outside
MANUEL-OUTSIDE-2
Marco-Inside
Marco-Outside
Source Zones (1)
lesquive-INSIDE
Add to Source
Add
Cancel


Add Rule
Name
Block bad domains
Enabled
Action
Domain Not Found
Zones
Networks
VLAN Tags
DNS
Available Networks
Search by name or value
IPv6-to-IPv4-Relay-Anycast
jvillalt-Inside
lesquive-inside-network
lesquive-network
Manuel-Inside-NET
Marco_PAT
Network_Marco
Outside-Isaac
pat-hugo
Source Networks (1)
lesquive-network
Add to Source
Enter an IP address
Add
Add
Cancel



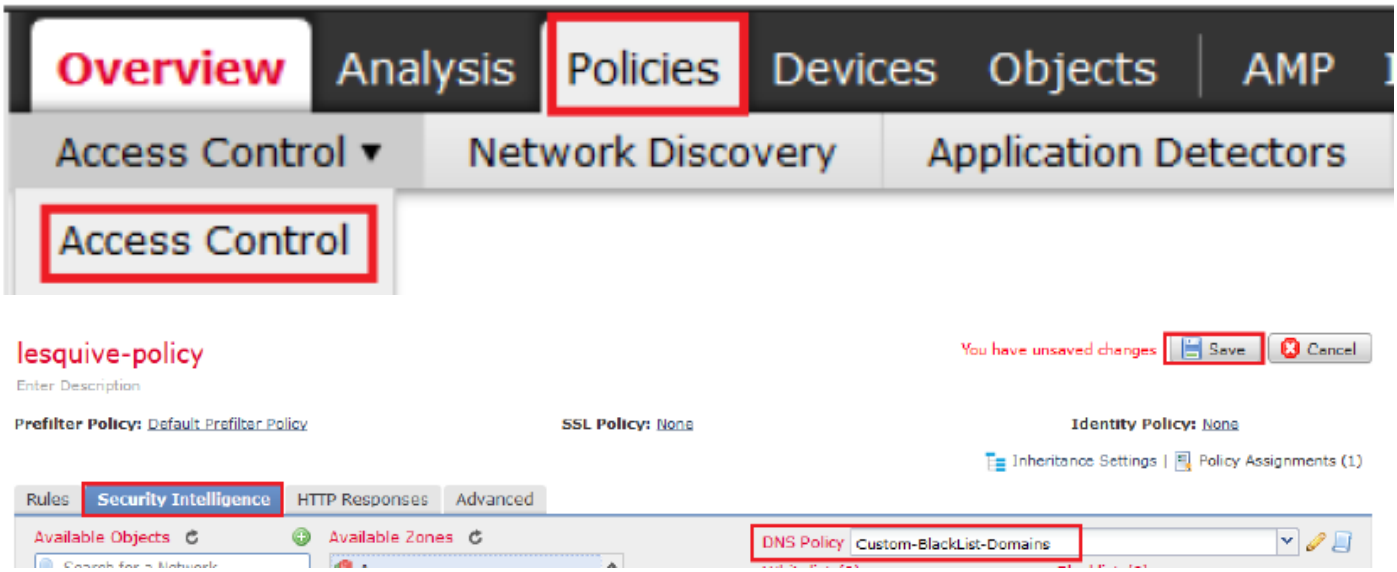


معلومات مهمة حول ترتيب القاعدة:

- دائما ما يكون العالم الأبيض هو الأول ويسبق جميع القواعد الأخرى.
- تظهر قاعدة Descendant DNS Whitelists فقط في عمليات النشر متعددة المجالات، في المجالات غير التابعة للورقة. دائما ما يكون المركز الثاني ويسبق جميع القواعد الأخرى ما عدا القاعدة البيضاء العالمية.
- يسبق قسم الأبيض قسم القائمة السوداء، وتكون قواعد القوائم البيضاء دائما أسبقية على قواعد أخرى.
- دائما ما تكون القائمة السوداء العالمية هي الأولى في قسم القائمة السوداء وتأخذ الأولوية على جميع قواعد الشاشات والقائمة السوداء الأخرى.
- تظهر قاعدة القوائم السوداء ل DNS التابع فقط في عمليات النشر متعددة المجالات، في المجالات غير التابعة للورقة. دائما ما تكون في المرتبة الثانية في قسم القائمة السوداء وتسبق جميع قواعد الشاشات والقائمة السوداء الأخرى ما عدا القائمة السوداء العالمية.
- يحتوي قسم القائمة السوداء على قواعد Monitor و BlackList.
- عندما تقوم بإنشاء قاعدة DNS أولا، يبقى موضع النظام في القسم الأبيض إذا قمت بتعيين عملية WhiteList، أو أخر في قسم القائمة السوداء إذا قمت بتعيين أي عملية أخرى

تعيين نهج DNS لنهج التحكم بالوصول الخاص بك

انتقل إلى السياسات >> التحكم في الوصول >> النهج الخاص ب FTD الخاص بك >> ذكاء الأمان >> نهج DNS وأضف النهج الذي أنشأته.

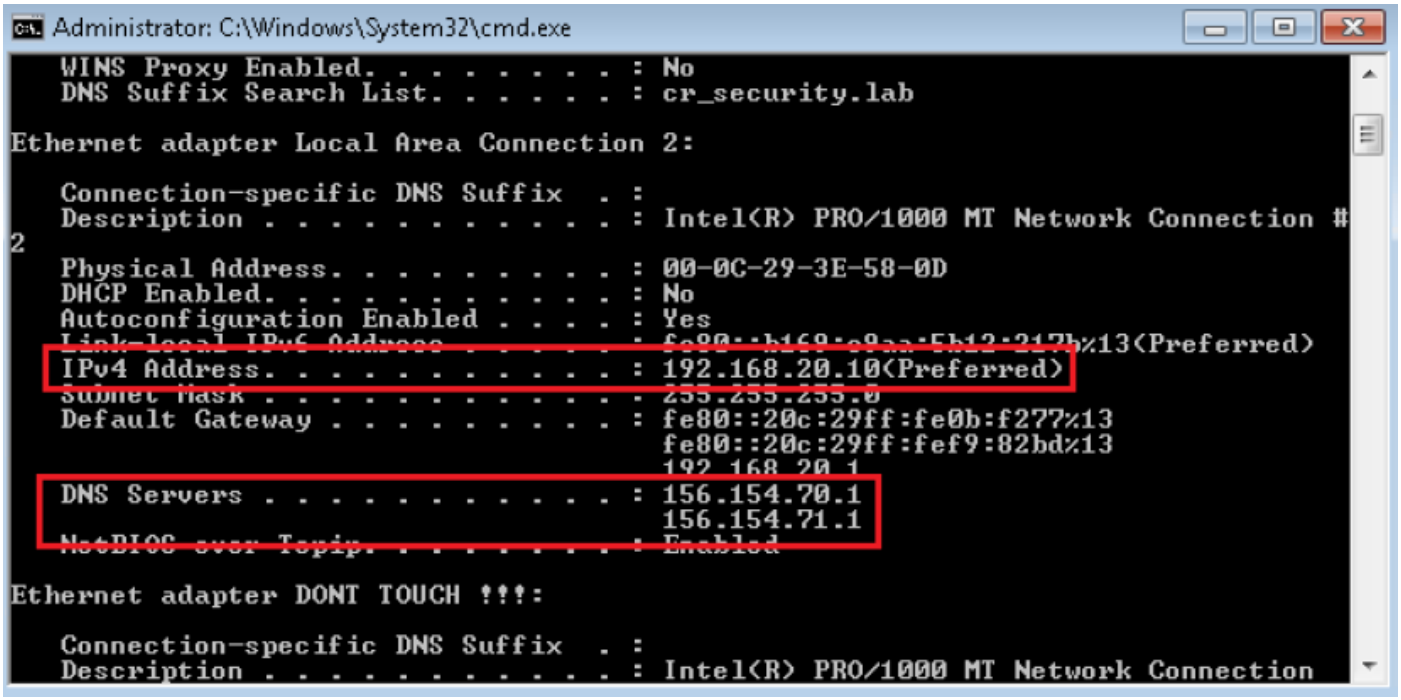


تأكد من نشر كافة التغييرات عند الانتهاء.

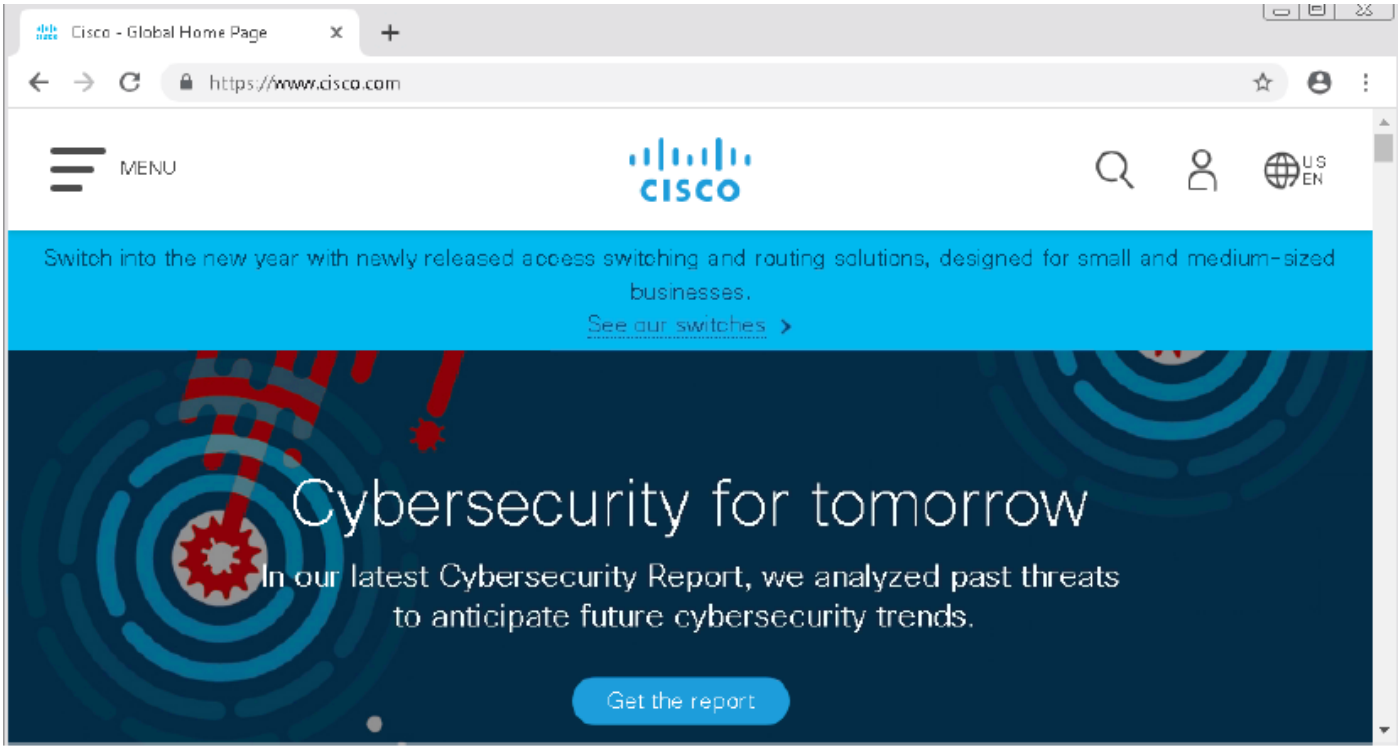
التحقق من الصحة

قبل تطبيق نهج DNS

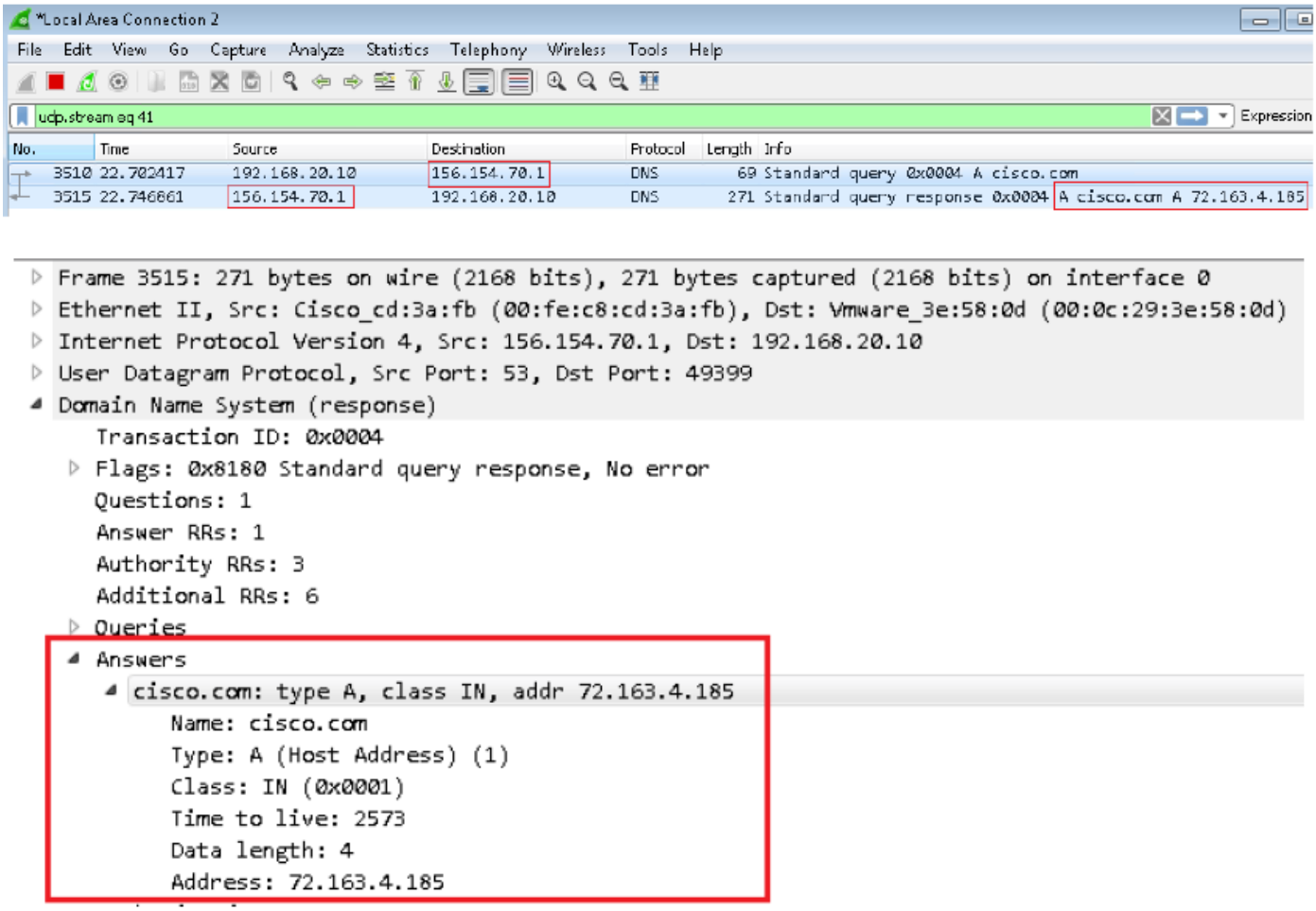
الخطوة 1. تحقق من معلومات خادم DNS وعنوان IP على الجهاز المضيف كما هو موضح في الصورة:



الخطوة 2. تأكد من أنه يمكنك الانتقال إلى cisco.com كما هو موضح في الصورة:

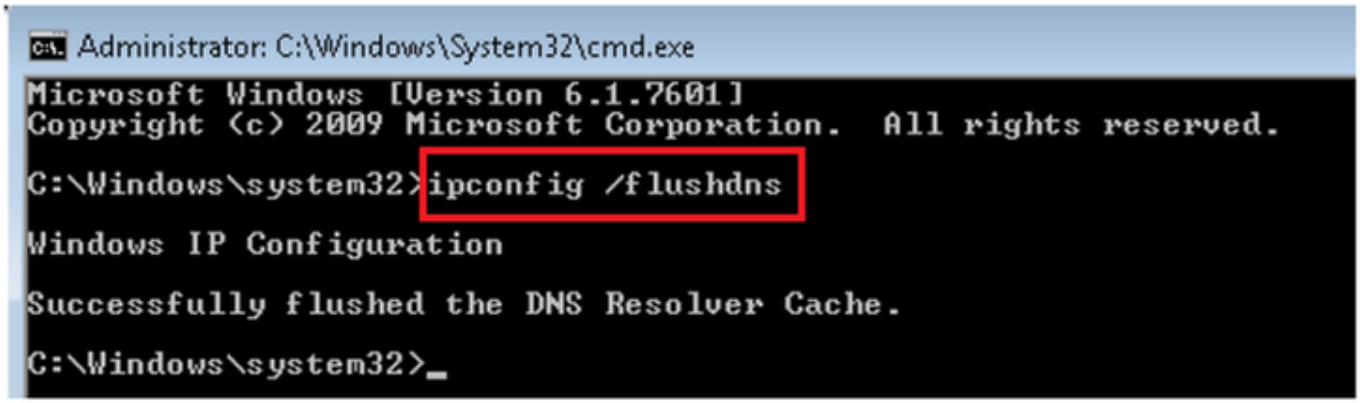


الخطوة 3. التأكيد باستخدام التقاط الحزم أن DNS تم حله بشكل صحيح:

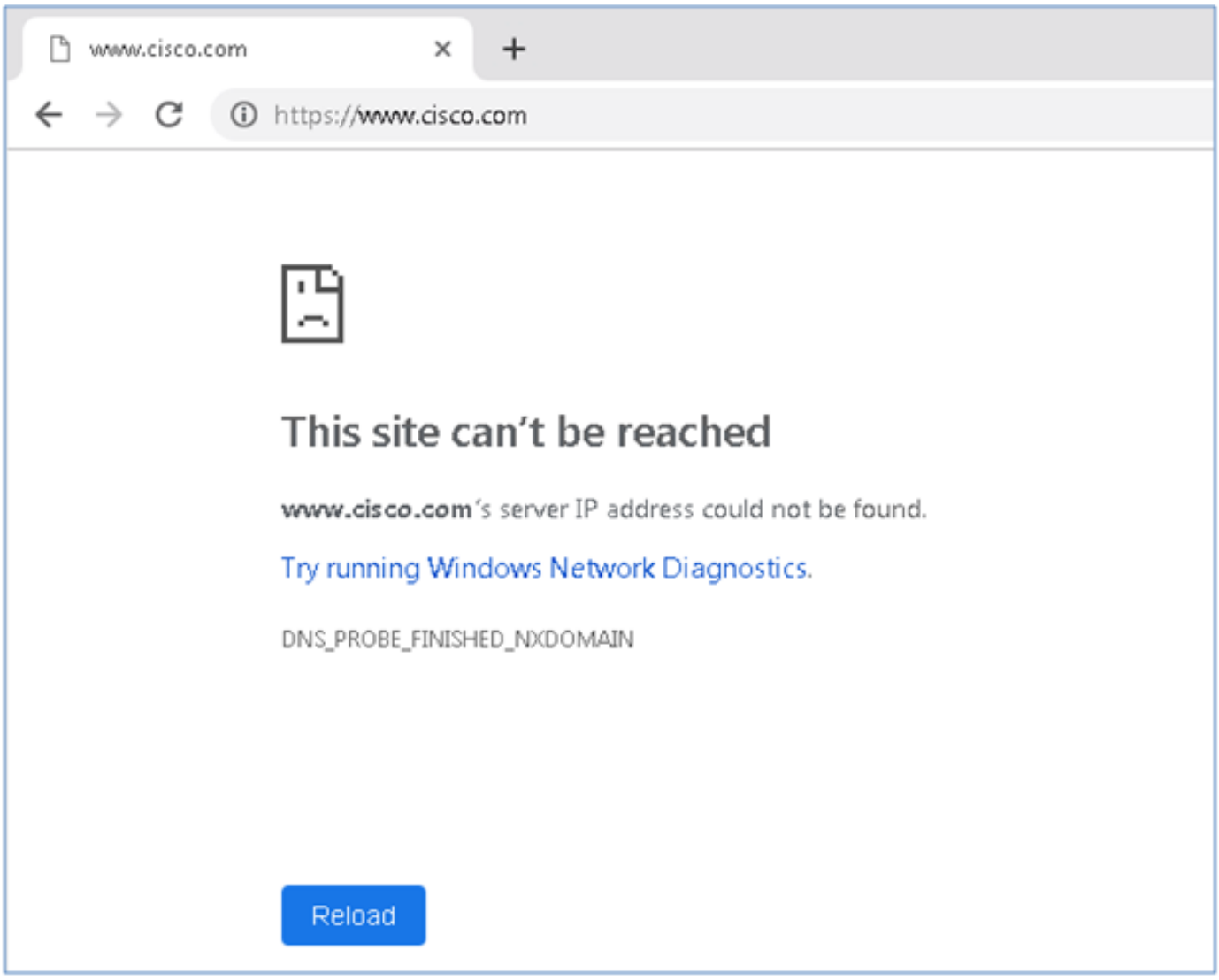


بعد تطبيق نهج DNS

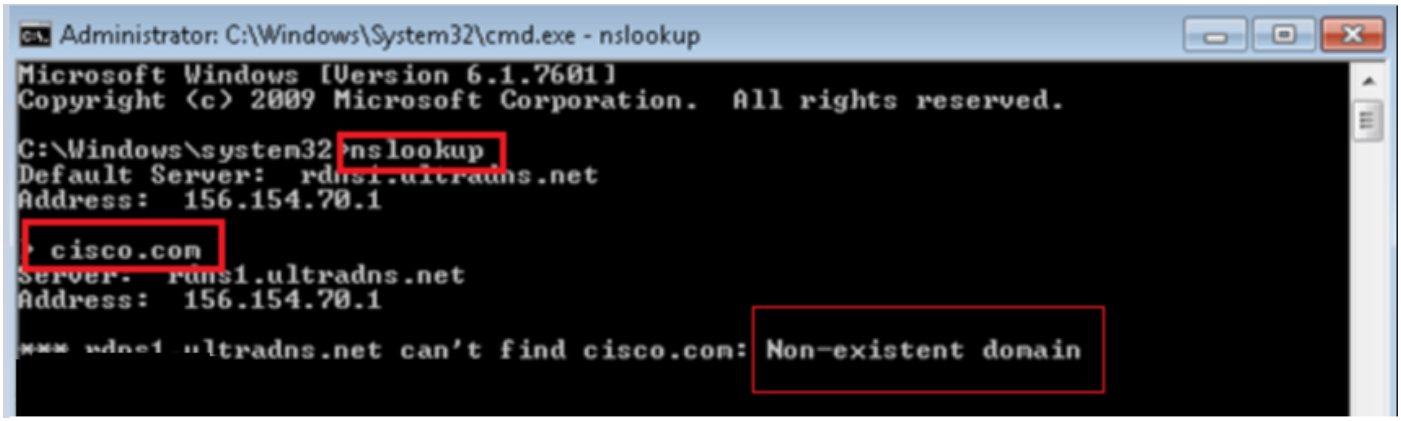
الخطوة 1. قم بمسح ذاكرة التخزين المؤقت ل DNS على مضيفك باستخدام الأمر **ipconfig /flushdns.**



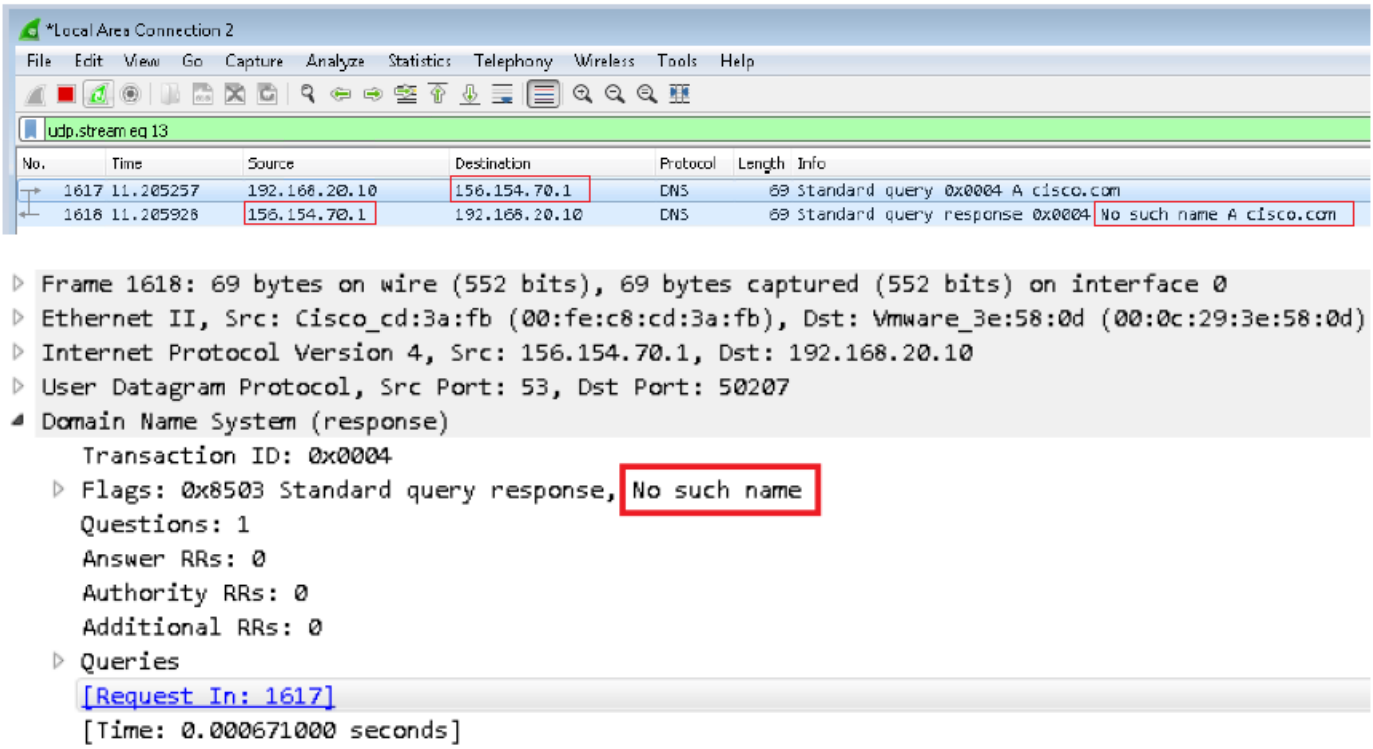
الخطوة 2. انتقل إلى المجال المعني باستخدام مستعرض ويب. ولابد أن يكون الوصول إلى هذه المعلومات غير ممكن:



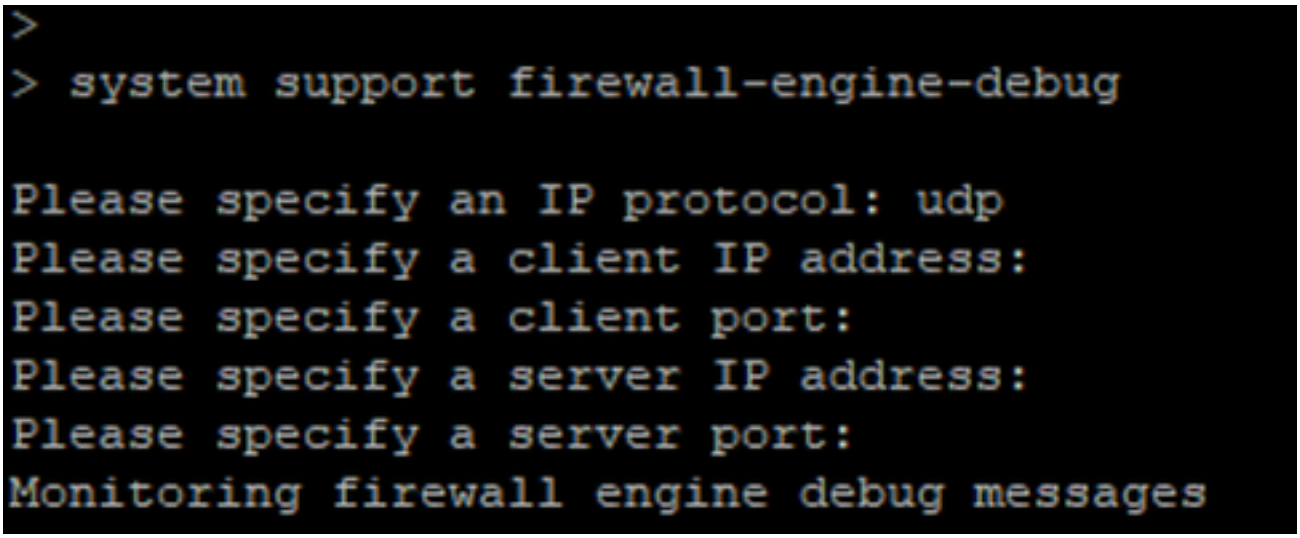
الخطوة 3. حاول إصدار **nslookup** على المجال cisco.com. فشل تحليل الاسم.



الخطوة 4. تظهر صور الحزم إستجابة من FTD، بدلا من خادم DNS.



الخطوة 5. تشغيل تصحيح الأخطاء في FTD CLI: دعم النظام جدار الحماية-engine-debug وتحديد بروتوكول UDP.



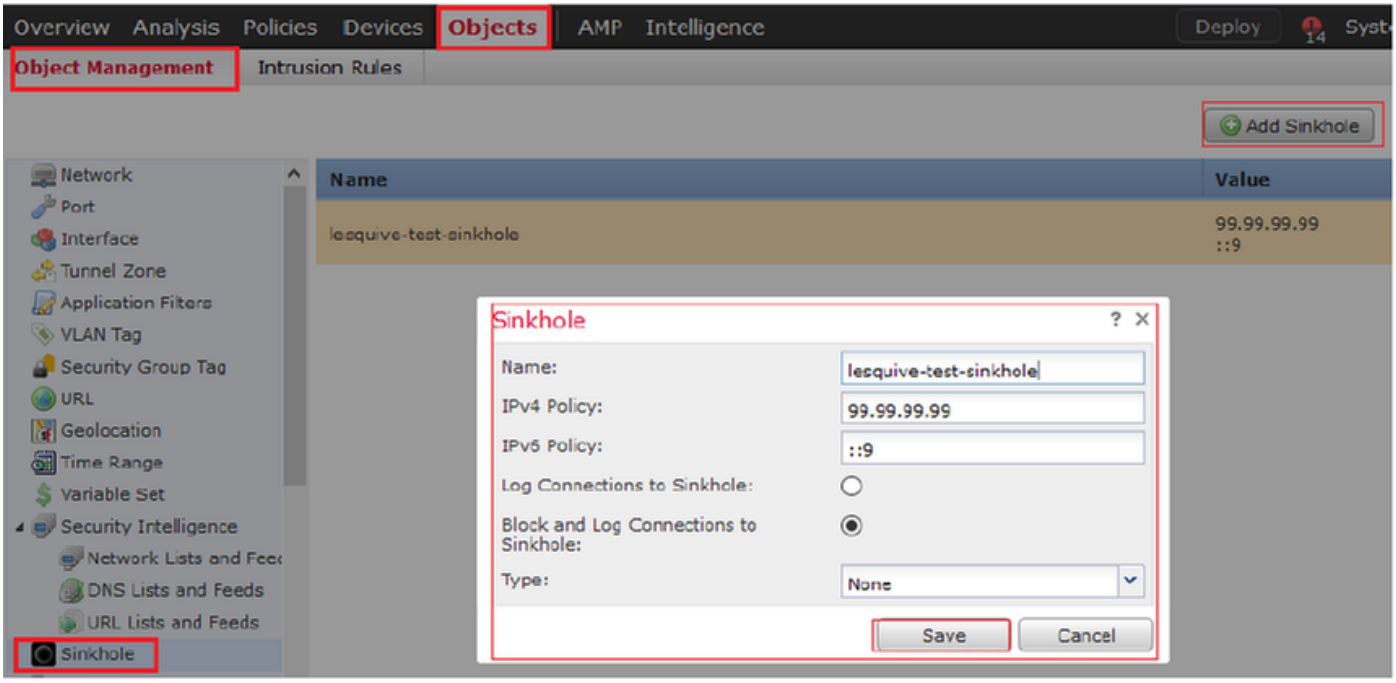
*تصحيح الأخطاء عند تطابق cisco.com:

```
> system support firewall-engine-debug

Please specify an IP protocol: udp
Please specify a client IP address:
Please specify a client port:
Please specify a server IP address:
Please specify a server port:
Monitoring firewall engine debug messages

192.168.20.10-61373 > 156.154.70.1-53 17 AS 1 I 0 DNS SI shared mem lookup returned 0 for cisco.com.cr_security.lab
192.168.20.10-61373 > 156.154.70.1-53 17 AS 1 I 0 Skipping DNS rule lookup for cisco.com.cr_security.lab since we've already gotten a response
192.168.20.10-61373 > 156.154.70.1-53 17 AS 1 I 0 Got end of flow event from hardware with flags 00000000
192.168.20.10-61374 > 156.154.70.1-53 17 AS 1 I 1 DNS SI shared mem lookup returned 0 for cisco.com.cr_security.lab
192.168.20.10-61374 > 156.154.70.1-53 17 AS 1 I 1 Skipping DNS rule lookup for cisco.com.cr_security.lab since we've already gotten a response
192.168.20.10-61374 > 156.154.70.1-53 17 AS 1 I 1 Got end of flow event from hardware with flags 00000000
192.168.20.10-61375 > 156.154.70.1-53 17 AS 1 I 1 DNS SI shared mem lookup returned 1 for cisco.com
192.168.20.10-61375 > 156.154.70.1-53 17 AS 1 I 1 Starting SrcZone first with intfs 1 -> 0, vlan 0
192.168.20.10-61375 > 156.154.70.1-53 17 AS 1 I 1 using rule order 1, id 1 action Allow
192.168.20.10-61375 > 156.154.70.1-53 17 AS 1 I 1 using rule order 2, id 3 action DNS NXDomain
192.168.20.10-61375 > 156.154.70.1-53 17 AS 1 I 1 using rule order 3, id 5 action DNS NXDomain
192.168.20.10-61375 > 156.154.70.1-53 17 AS 1 I 1 Got DNS list match. si list 1048620
192.168.20.10-61375 > 156.154.70.1-53 17 AS 1 I 1 Firing DNS action DNS NXDomain
192.168.20.10-61375 > 156.154.70.1-53 17 AS 1 I 1 Injecting NX domain reply.
192.168.20.10-61375 > 156.154.70.1-53 17 AS 1 I 1 DNS SI: Matched rule order 3, Id 5, si list id 1048620, action 22, reason 2048, SI Categories 1048620,0
192.168.20.10-61376 > 156.154.70.1-53 17 AS 1 I 0 DNS SI shared mem lookup returned 1 for cisco.com
192.168.20.10-61376 > 156.154.70.1-53 17 AS 1 I 0 Starting SrcZone first with intfs 1 -> 0, vlan 0
192.168.20.10-61376 > 156.154.70.1-53 17 AS 1 I 0 using rule order 1, id 1 action Allow
192.168.20.10-61376 > 156.154.70.1-53 17 AS 1 I 0 using rule order 2, id 3 action DNS NXDomain
192.168.20.10-61376 > 156.154.70.1-53 17 AS 1 I 0 using rule order 3, id 5 action DNS NXDomain
192.168.20.10-61376 > 156.154.70.1-53 17 AS 1 I 0 Got DNS list match. si list 1048620
192.168.20.10-61376 > 156.154.70.1-53 17 AS 1 I 0 Firing DNS action DNS NXDomain
192.168.20.10-61376 > 156.154.70.1-53 17 AS 1 I 0 Injecting NX domain reply.
192.168.20.10-61376 > 156.154.70.1-53 17 AS 1 I 0 DNS SI: Matched rule order 3, Id 5, si list id 1048620, action 22, reason 2048, SI Categories 1048620,0
```

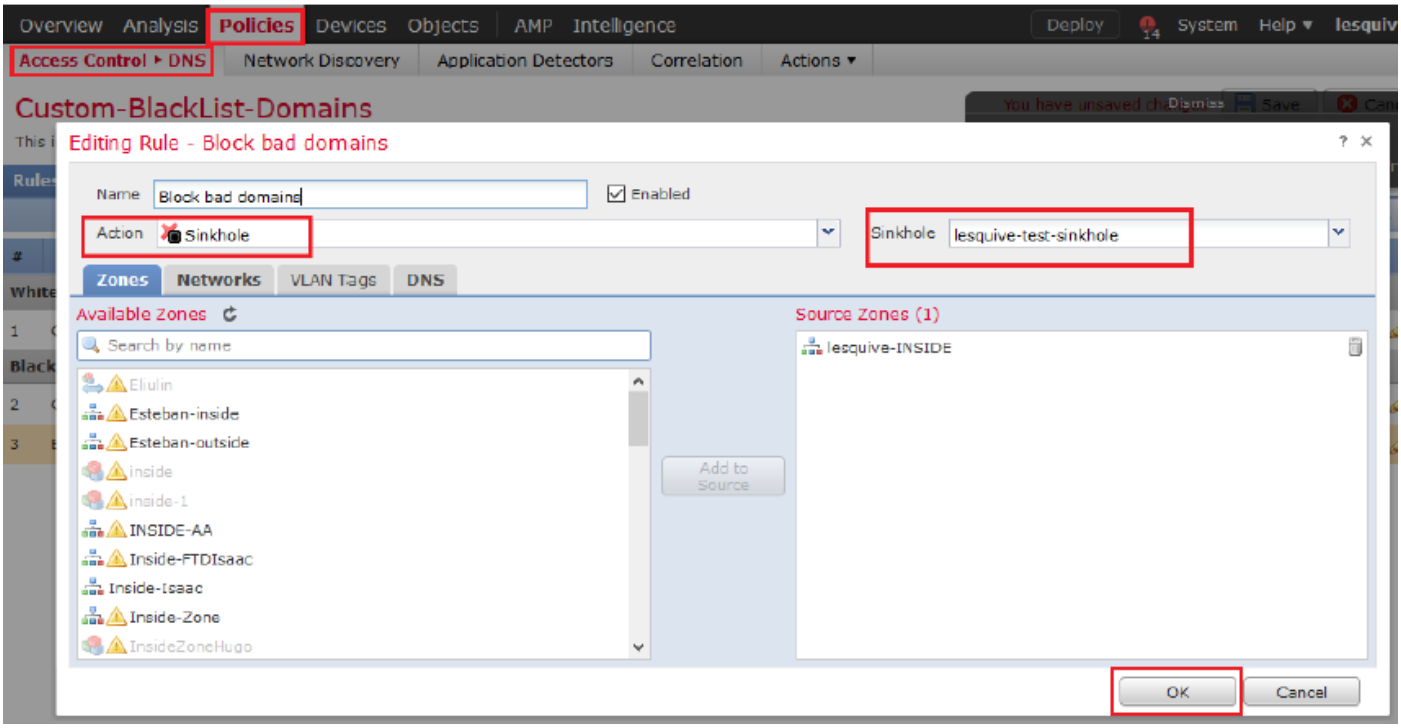
تهيئة بطاقة StackSlot الاختيارية

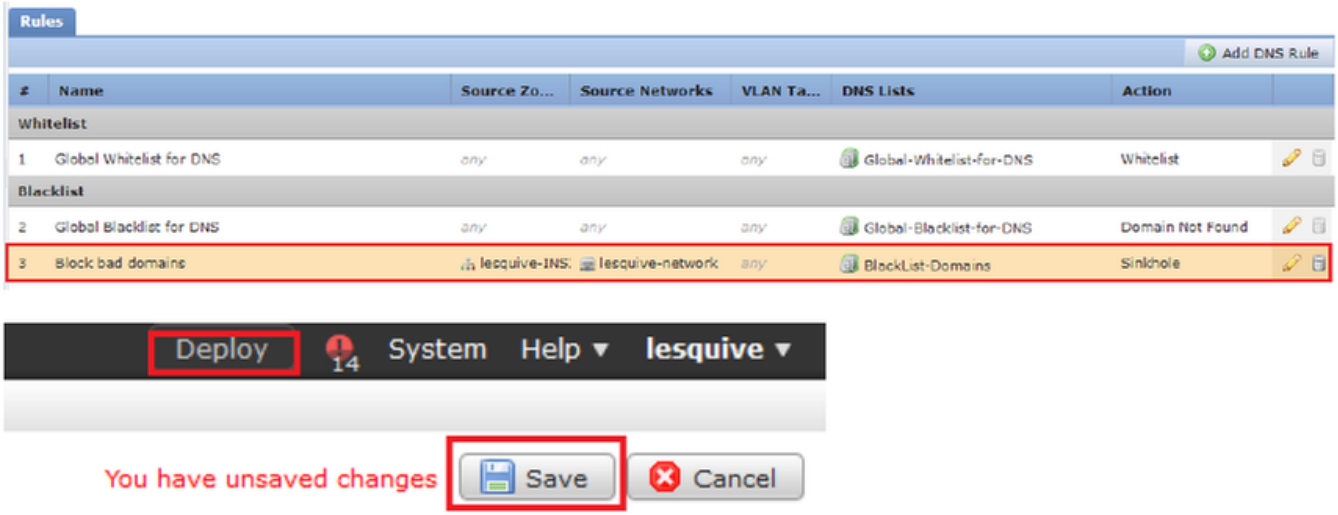
DNS Sinkhole هو خادم DNS يوفر معلومات خاطئة. بدلا من إرجاع إستجابة DNS "بدون مثل هذا الاسم" إلى استعلامات DNS على المجالات التي تقوم بحظرها، فإنها ترجع عنوان IP مزيف.

الخطوة 1. انتقل إلى الكائنات >> إدارة الكائنات >> فتحة الدائرة >> أضف فتحة البداية وقم بإنشاء معلومات عنوان IP المزيف.

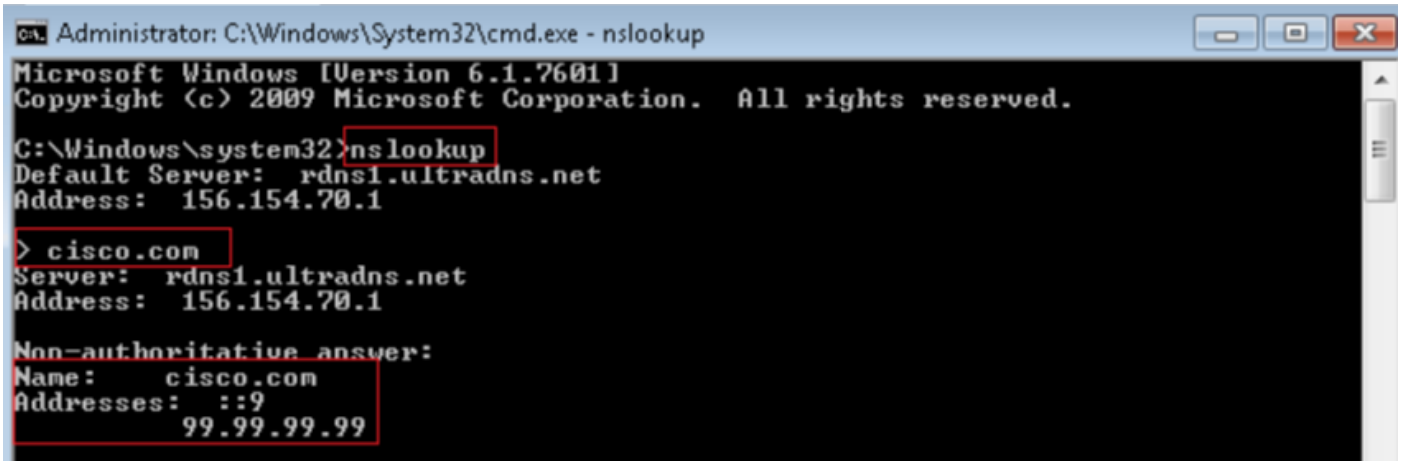


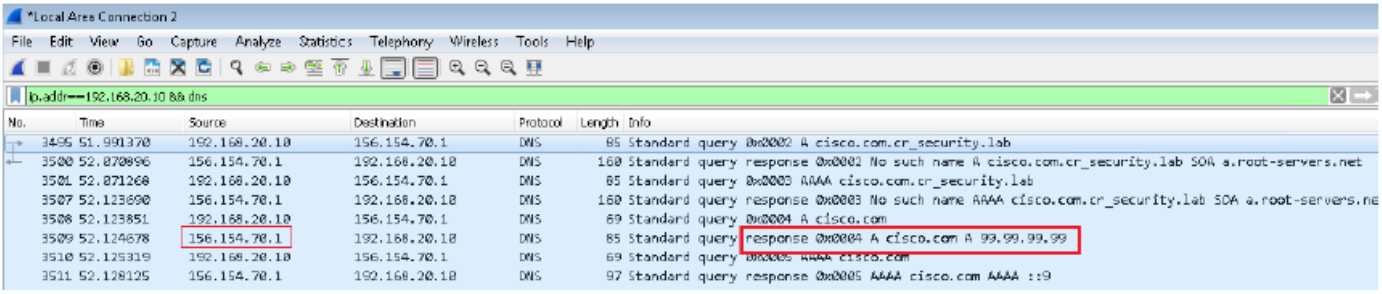
الخطوة 2. تطبيق الثقب السفلي على نهج DNS ونشر التغييرات على FTD.





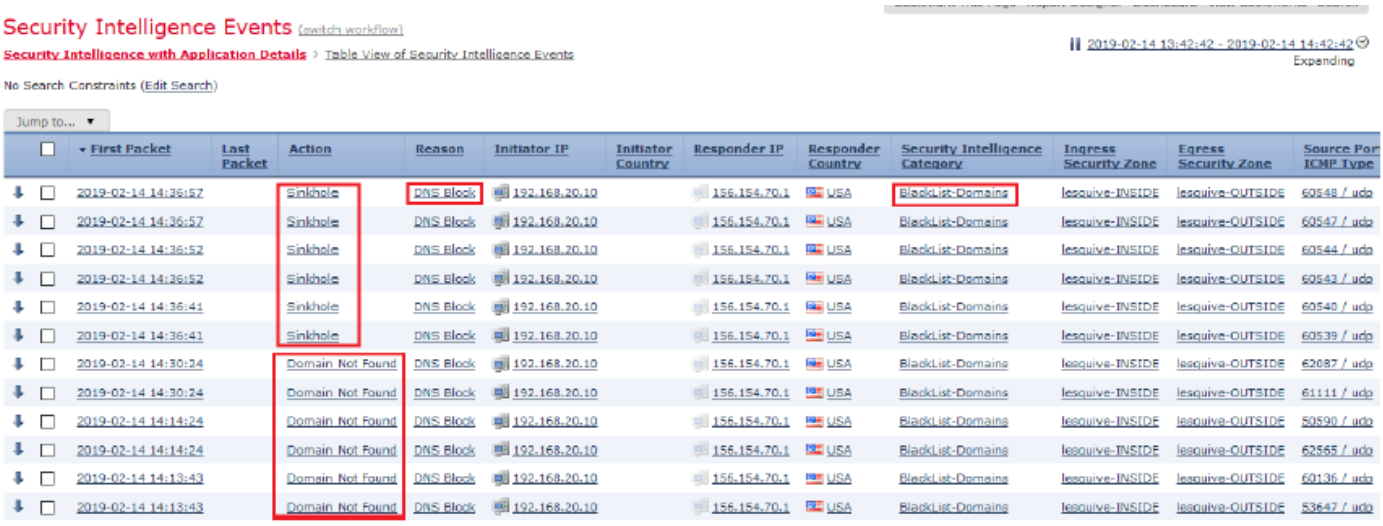
تأكد من عمل الحل





استكشاف الأخطاء وإصلاحها

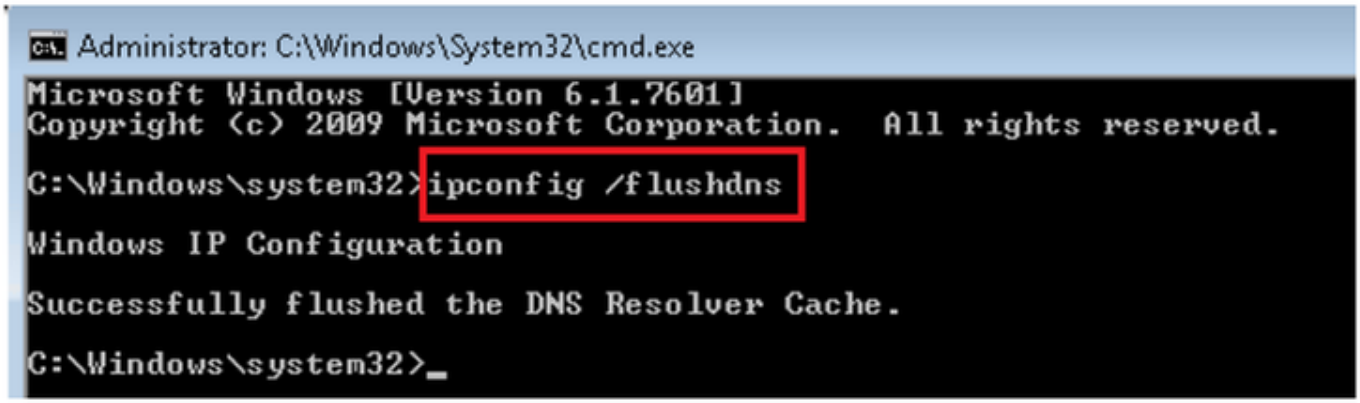
انتقل إلى Analysis (التحليل) > Connections >> Security Intelligence Events (إتصالات معلومات الأمان) لتعقب جميع الأحداث التي يتم تشغيلها بواسطة SI طالما قمت بتمكين تسجيل الدخول إلى نهج DNS:



يمكنك أيضا إستخدام الأمر **system support firewall-engine-debug** على FTD الذي تتم إدارته بواسطة FMC.

```
>
> system support firewall-engine-debug

Please specify an IP protocol: udp
Please specify a client IP address:
Please specify a client port:
Please specify a server IP address:
Please specify a server port:
Monitoring firewall engine debug messages
```

يمكن أن تكون عمليات التقاط الحزم مفيدة لتأكيد أن طلبات DNS تجعلها في خادم FTD. ال تنس مسح ذاكرة التخزين المؤقت على المضيف المحلي عند الاختبار.


Administrator: C:\Windows\System32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.
C:\Windows\system32>ipconfig /flushdns
Windows IP Configuration
Successfully flushed the DNS Resolver Cache.
C:\Windows\system32>

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).