تكوين كائن FQDN على قائمة التحكم في الوصول الموسعة ل PBR على FMC

المحتويات

المقدمة

يصف هذا المستند إجراء تكوين كائن FQDN في قائمة الوصول الموسعة (ACL) للاستخدام في التوجيه المستند إلى السياسة (PBR).

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بهذه المنتجات:

- مركز إدارة جدار الحماية الآمن (FMC)
- الدفاع الآمن عن تهديد جدار الحماية (FTD)
- بي بي آر

المكونات المستخدمة

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

- الدفاع ضد تهديد Firepower ل VMware، الإصدار 7.6.0
- مركز إدارة جدار الحماية الآمن ل VMware، الإصدار 7.6.0

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

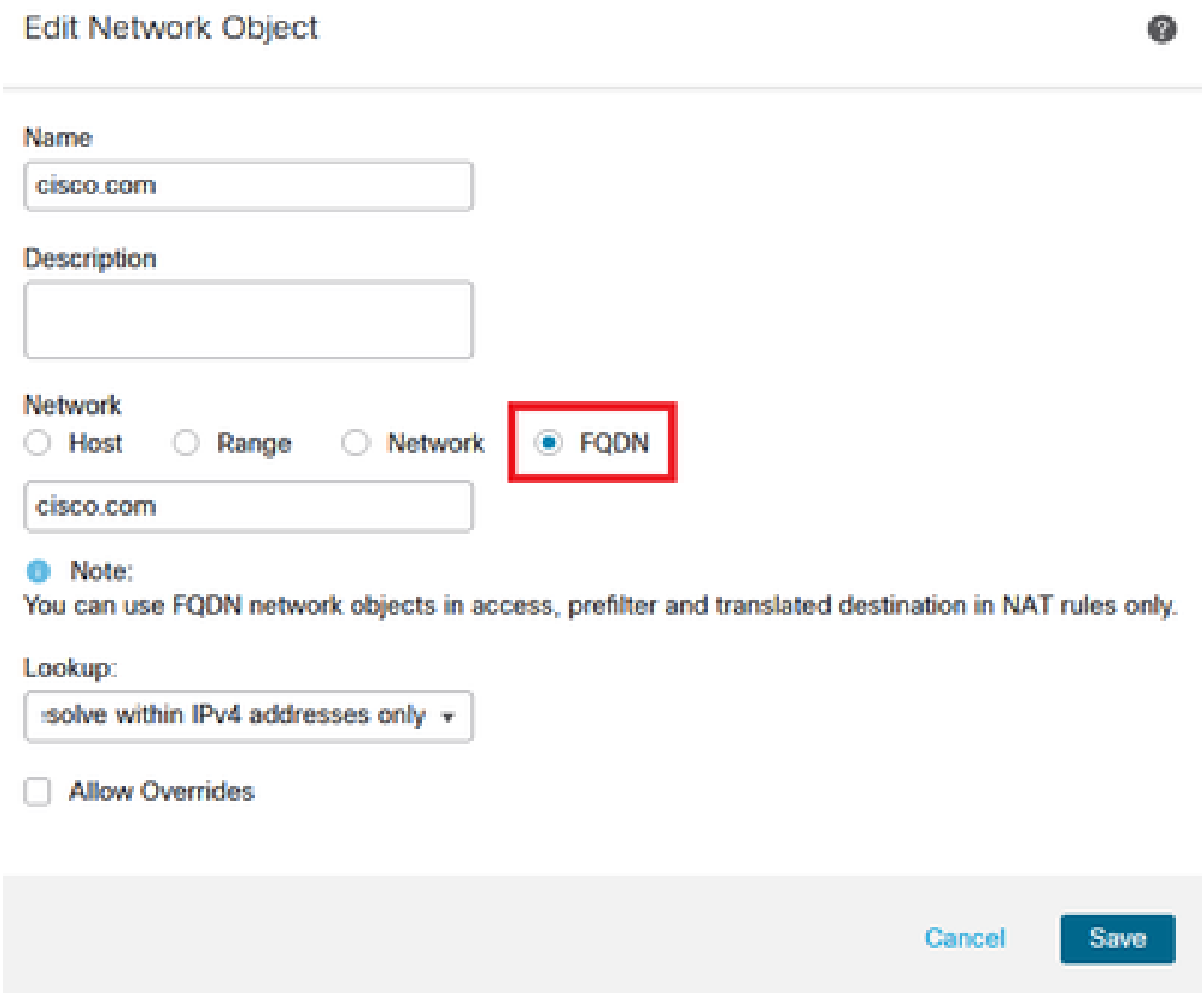
حالياً، لا يسمح FTD بتصفية حركة مرور غير HTTP باستخدام كائنات اسم المجال المؤهل بالكامل (FQDN) كما هو مذكور في معرف تصحيح الأخطاء من Cisco CSCuz98322.

هذه الوظيفة مدعومة على أنظمة ASA الأساسية، ومع ذلك، يمكن تصفية الشبكات والتطبيقات فقط على FTD.

يمكنك إضافة كائن FQDN إلى قائمة الوصول الموسعة لتكوين PBR باستخدام هذه الطريقة.

التكوين

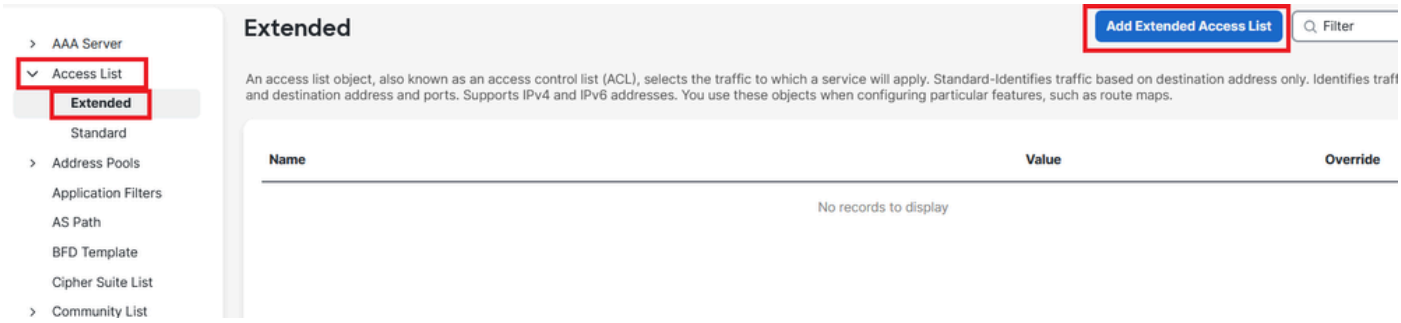
الخطوة 1. قم بإنشاء كائنات FQDN حسب الحاجة.



الصورة 1. قائمة كائن الشبكة

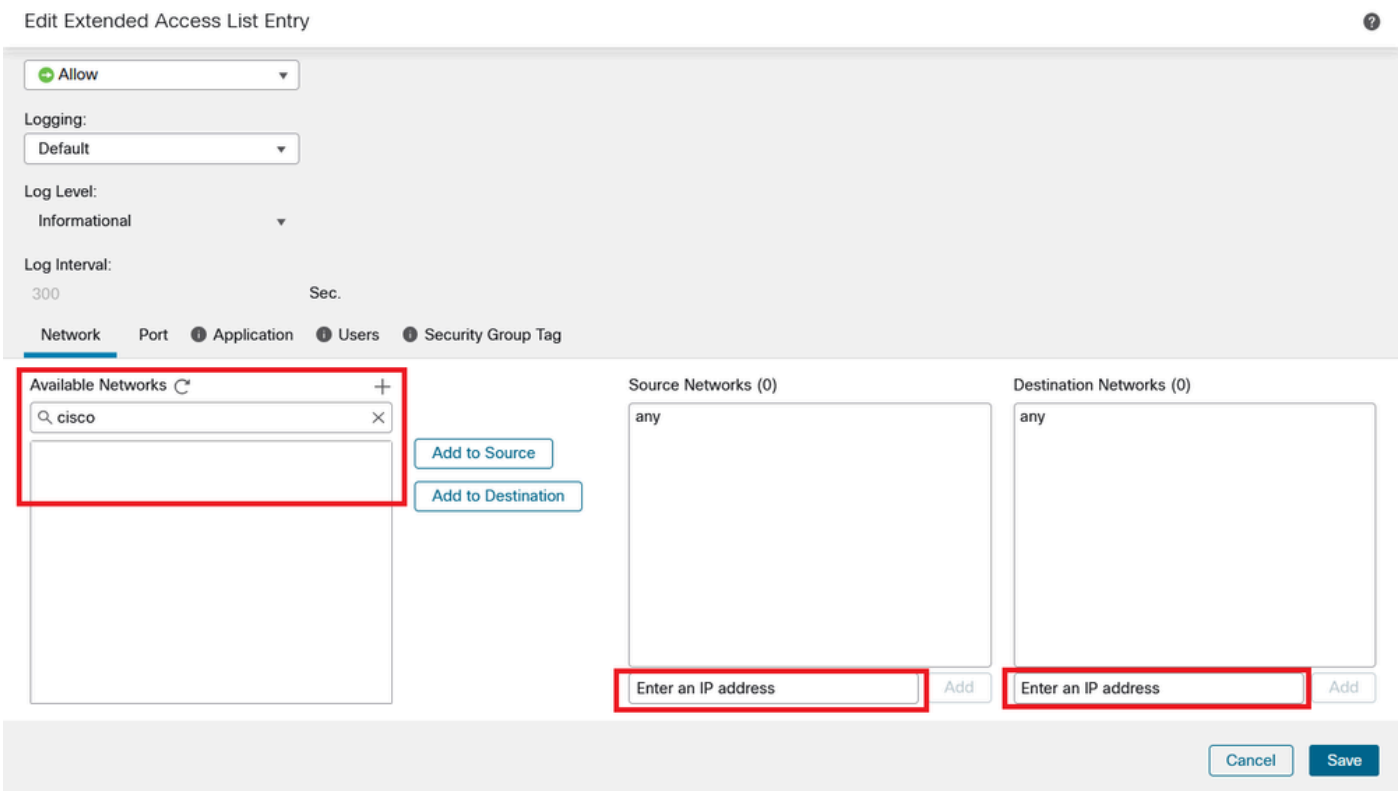
الخطوة 2. قم بإنشاء قائمة وصول موسعة تحت الكائنات > إدارة الكائن > قائمة الوصول >

موسعة.



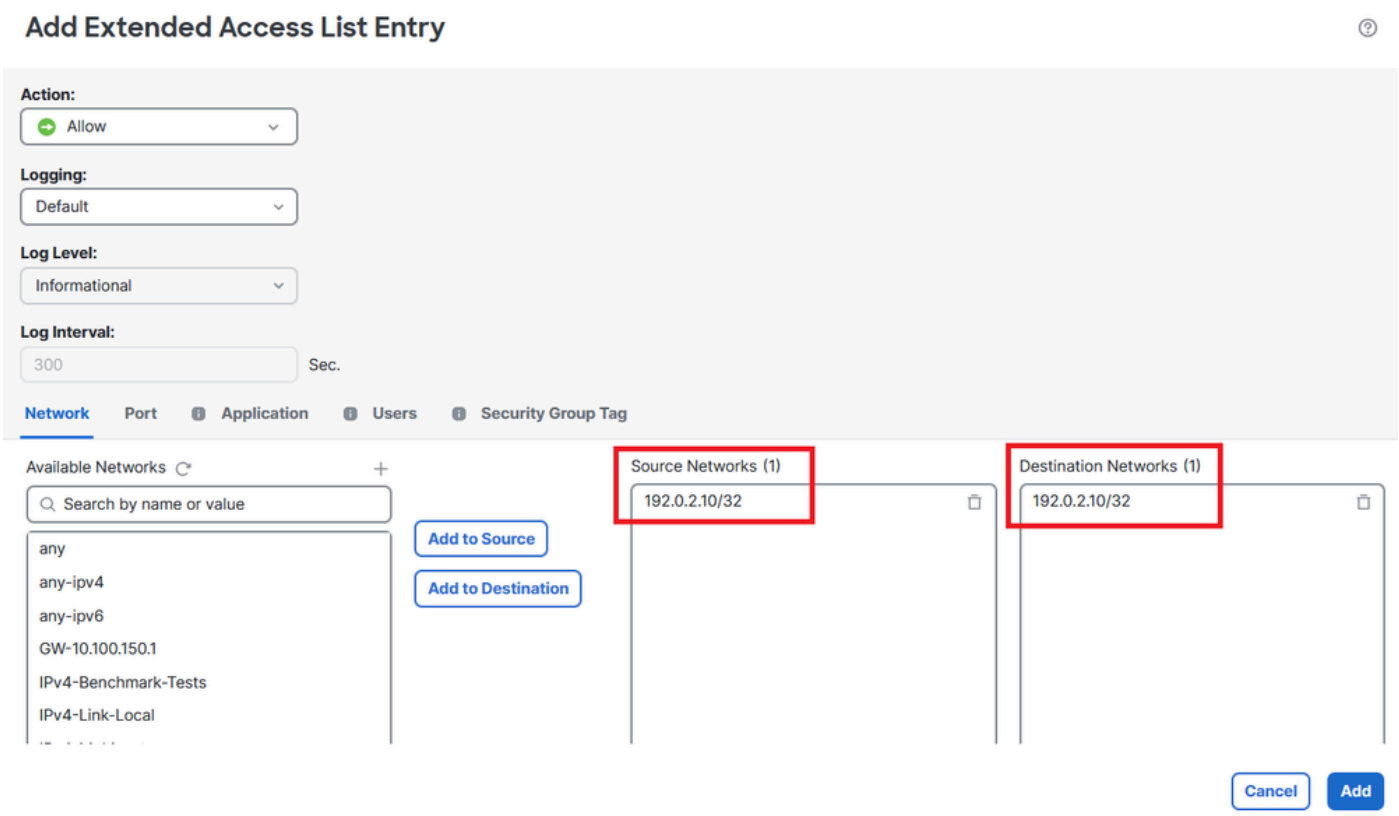
الصورة 2. قائمة قائمة الوصول الموسع

عند إضافة قاعدة جديدة، لاحظ أنه لا يمكنك رؤية كائن FQDN الذي قمت بتكوينه عند إجراء بحث على كائنات الشبكة لتحديد المصدر والوجهة.



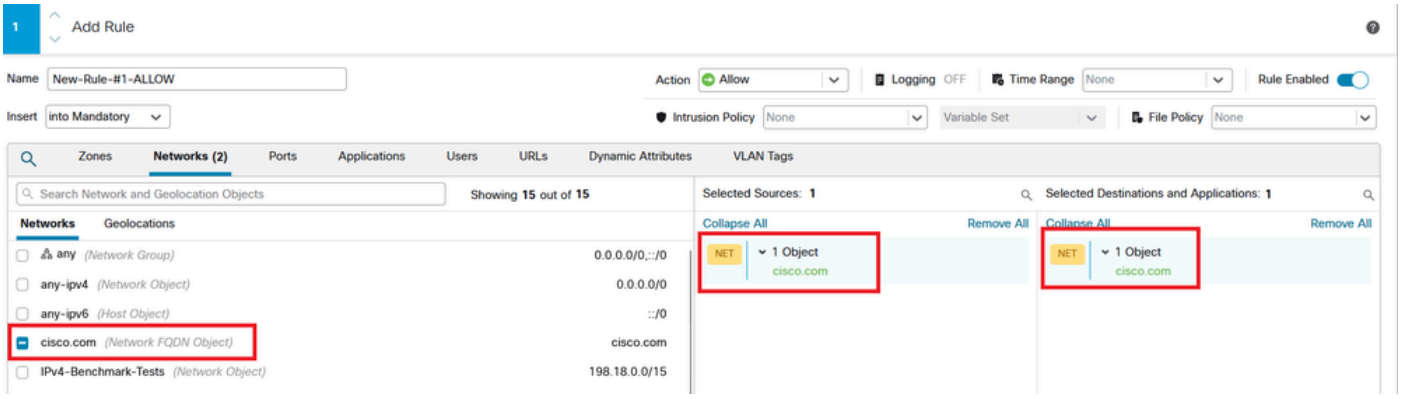
الصورة 3. قائمة قاعدة قائمة الوصول الموسعة الجديدة

الخطوة 3. قم بإنشاء قاعدة لا يمكن الوصول إليها بحيث يتم إنشاء قائمة التحكم في الوصول (ACL) الموسعة وتوافرها لتكوين PBR.



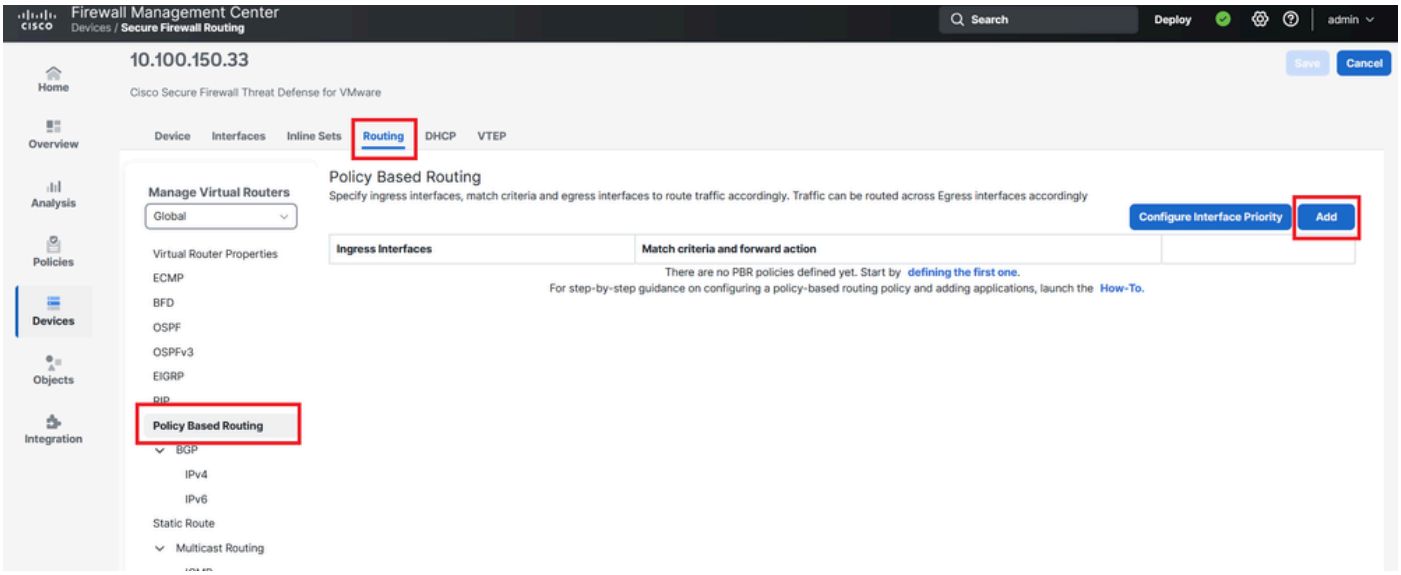
الصورة 4. تكوين قاعدة قائمة الوصول التي لا يمكن الوصول إليها

الخطوة 4. يجب إنشاء قاعدة على نهج التحكم في الوصول (ACP) تستهدف FTD الخاص بك باستخدام كائن FQDN. تقوم وحدة التحكم في إدارة الهيكل (FMC) بنشر كائن FQDN إلى FTD حتى يمكنك الرجوع إليه من خلال كائن FlexConfig.



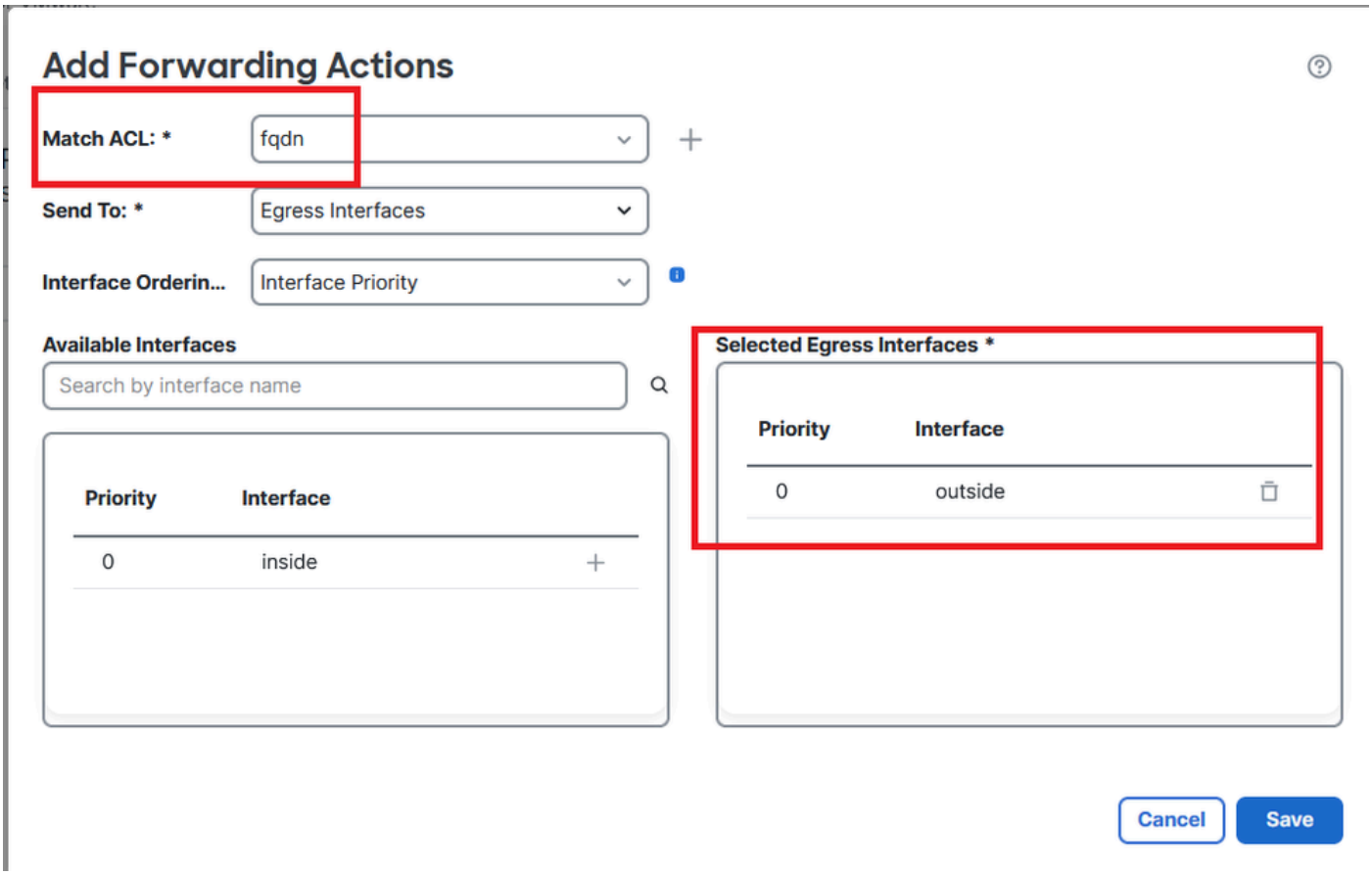
الصورة 5. قاعدة ACP مع كائن FQDN

الخطوة 5. انتقل إلى FTD على الأجهزة > إدارة الجهاز وحدد علامة التبويب توجيه وانتقل إلى قسم التوجيه المستند إلى السياسة.



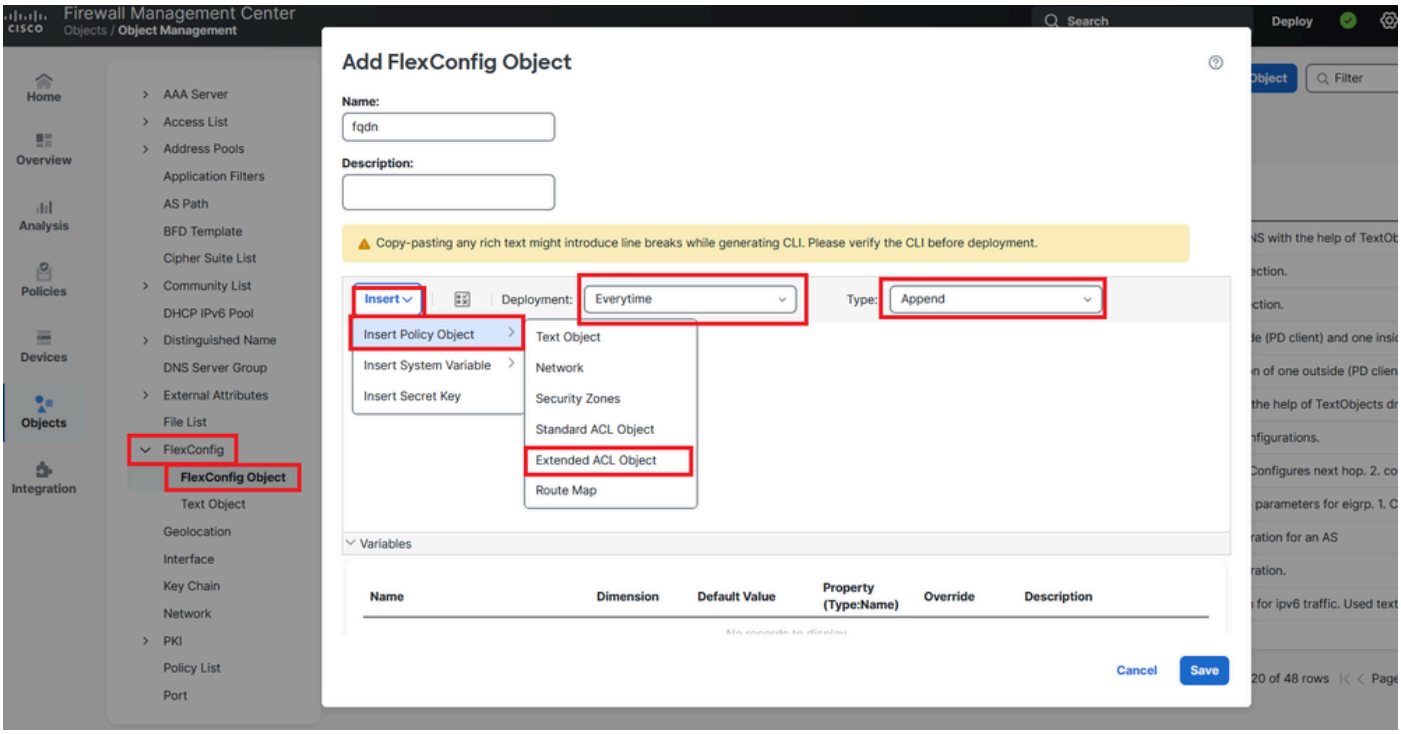
الصورة 6. قائمة PBR

الخطوة 6. قم بتكوين PBR على واجهة باستخدام قائمة التحكم في الوصول (ACL) التي تم تكوينها سابقا وتم نشرها.



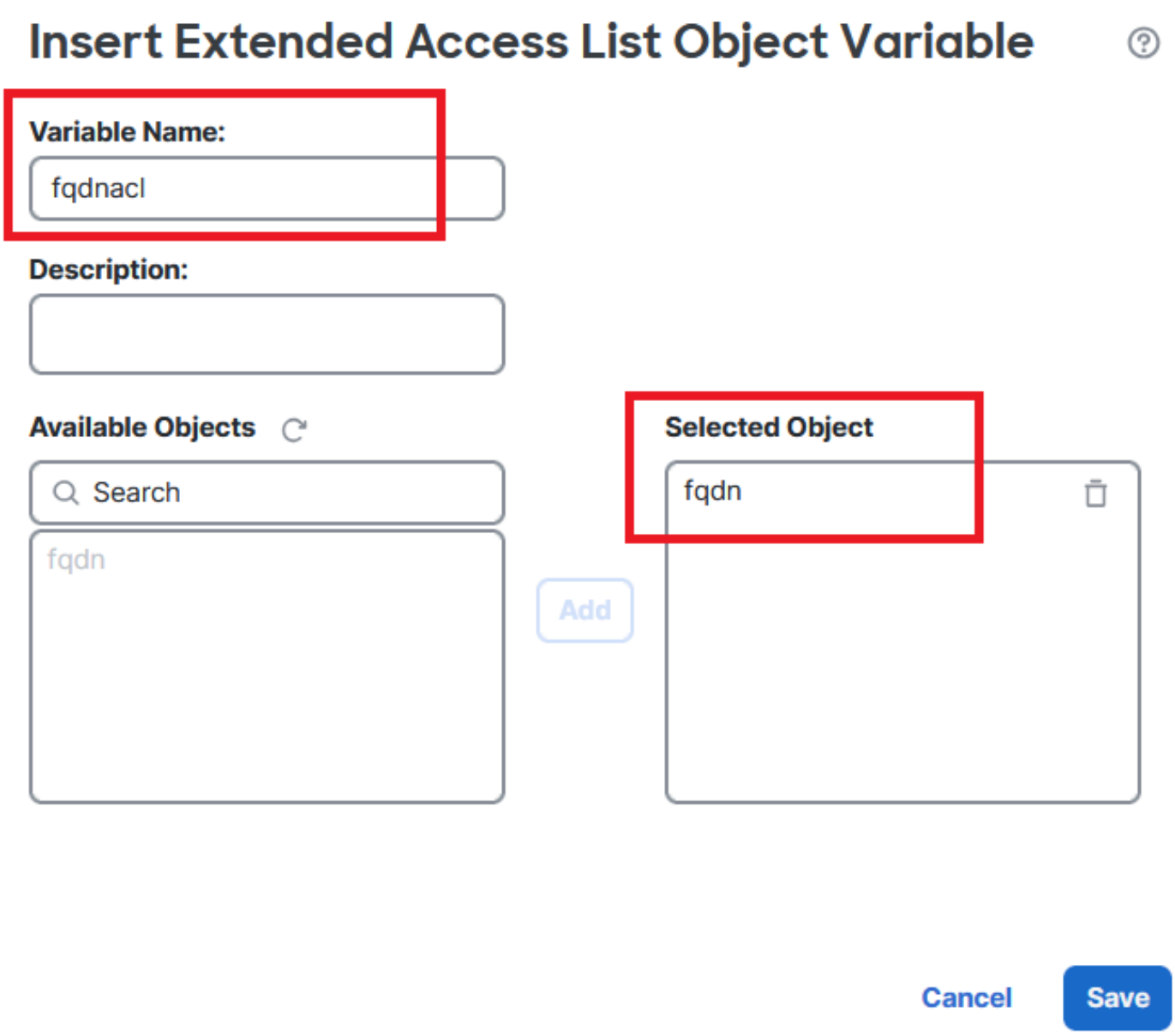
الصورة 7. واجهة PBR وقائمة تحديد قائمة التحكم في الوصول

الخطوة 7. انتقل إلى كائنات > إدارة الكائن > FlexConfig > كائن وقم بإنشاء كائن جديد.



الصورة 8. قائمة تكوين كائن FlexConfig

الخطوة 8. حدد إدراج > كائن قائمة التحكم في الوصول (ACL) الموسعة، وقم بتسمية المتغير وحدد قائمة التحكم في الوصول (ACL) الموسعة التي قمت بإنشائها مسبقا. تتم إضافة المتغير بالاسم الذي أستخدمته.



الصورة 9. إنشاء المتغير لكائن FlexConfig

الخطوة 9. أدخل هذا السطر لكل كائن FQDN تريده لقائمة التحكم في الوصول (ACL) الخاصة بك.

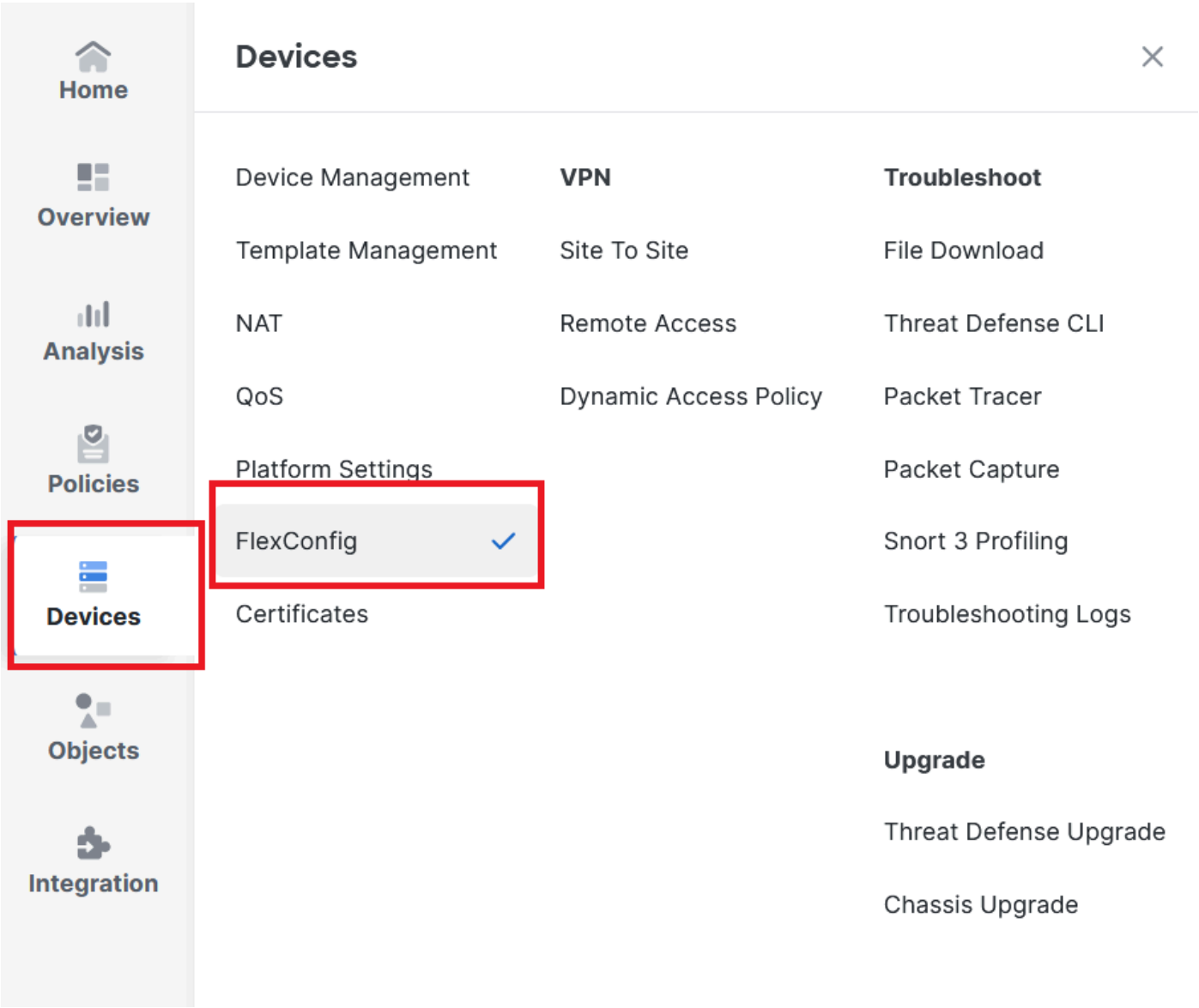
<#root>

```
access-li $
```

```
extended permit ip any object
```

الخطوة 10. احفظ كائن FlexConfig الخاص بك ك ك لك مرة > إضافة.

الخطوة 11.انتقل إلى قائمة نهج FlexConfig ضمن الأجهزة > FlexConfig.

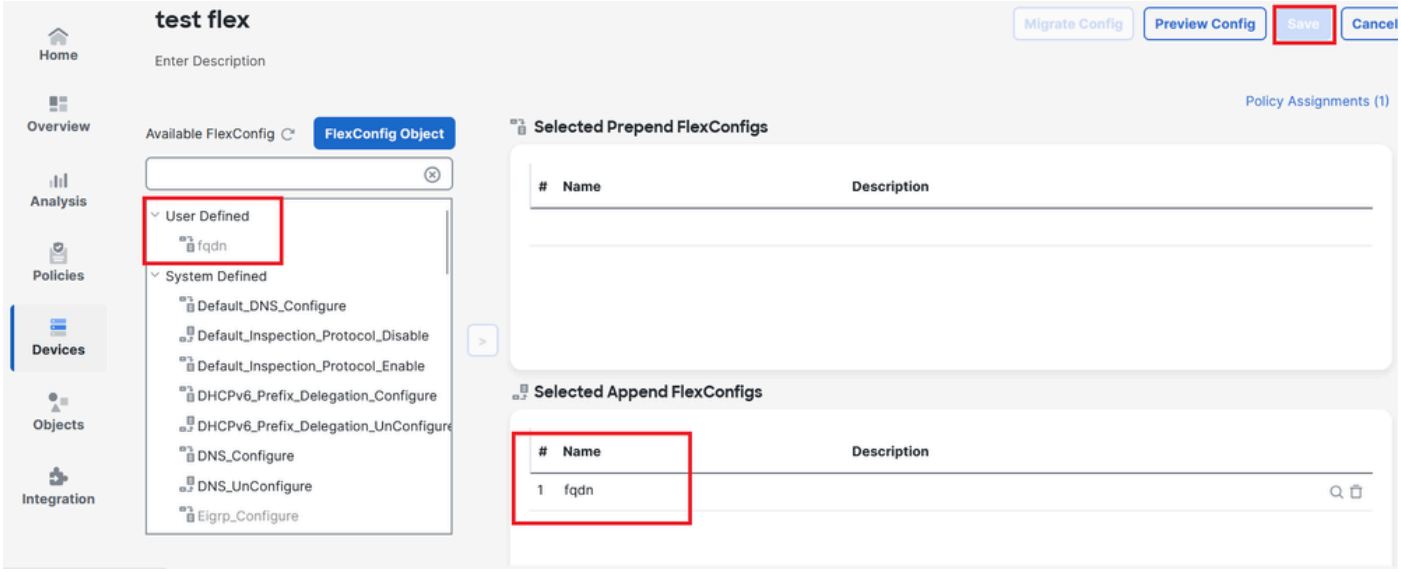


الصورة 10. مسار قائمة نهج FlexConfig

الخطوة 12. قم بإنشاء نهج FlexConfig جديد أو حدد نهج تم تعيينه بالفعل ل FTD الخاص بك.

الصورة 11. تحرير سياسة FlexConfig جديدة أو إنشاؤها

الخطوة 13. أضف كائن FlexConfig إلى النهج، واحفظ و نشر.



الصورة 12. إضافة كائن FlexConfig إلى سياسة FlexConfig

التحقق من الصحة

تتضمن واجهة الدخول الخاصة بك مسار السياسة مع خريطة المسار التي تم إنشاؤها تلقائيا.

<#root>

firepower#

show run interface gi0/0

!
interface GigabitEthernet0/0
 nameif inside
 security-level 0
 ip address 10.100.151.2 255.255.255.0

policy-route route-map FMC_GENERATED_PBR_1727116778384

يحتوي مخطط المسار على قائمة التحكم في الوصول (ACL) المحددة باستخدام واجهة الوجهة المستخدمة.

<#root>

firepower#

show run route-map FMC_GENERATED_PBR_1727116778384

!
route-map FMC_GENERATED_PBR_1727116778384 permit 5

match ip address fqdn

```
set adaptive-interface cost outside
```

تحتوي قائمة الوصول على المضيف المستخدم للمرجع والقاعدة الإضافية التي أضفتها من خلال FlexConfig.

```
<#root>

firepower#

show run access-list fqdn

access-list fqdn extended permit ip host 192.0.2.10 host 192.0.2.10

access-list fqdn extended permit ip any object cisco.com
```

أنت يستطيع عملت ربط tracer من المدخل قارن كمصدر أن يدقق أنت ضربت ال PBR مرحلة.

```
<#root>

firepower#

packet-tracer input inside tcp 10.100.150.1 12345 fqdn cisco.com 443

Mapping FQDN cisco.com to IP address 72.163.4.161

[...]
Phase: 3

Type: PBR-LOOKUP

Subtype: policy-route
Result: ALLOW
Elapsed time: 1137 ns

Config:

route-map FMC_GENERATED_PBR_1727116778384 permit 5

 match ip address fqdn

 set adaptive-interface cost outside

Additional Information:
```

```
 Matched route-map FMC_GENERATED_PBR_1727116778384, sequence 5, permit


 Found next-hop 10.100.150.1 using egress ifc outside


[...]
Result:

input-interface: inside(vrfid:0)


input-status: up
input-line-status: up

output-interface: outside(vrfid:0)


output-status: up
output-line-status: up
Action: allow
Time Taken: 140047752 ns
```

المشكلات الشائعة

توقف PBR عن العمل بعد عملية نشر ثانية

الرجاء التحقق مما إذا كانت قائمة الوصول ال تزال تحتوي على قاعدة كائن FQDN.

في هذه الحالة، يمكنك أن ترى القاعدة لم تعد هنا.

```
firepower# show run access-list fqdn
access-list fqdn extended permit ip host 192.0.2.10 host 192.0.2.10
firepower#
```

تحقق من إعداد كائن FlexConfig على أنه نشر: AllTime and type: Append. يتم تطبيق القاعدة في كل مرة على عمليات النشر المستقبلية.

ال يحل FQDN

عند محاولة إختبار اتصال FQDN، تحصل على رسالة حول اسم المضيف غير صالح.

```
<#root>

firepower#

ping cisco.com
```

```
                ^
ERROR: % Invalid Hostname
```

تحقق من تكوين DNS. يجب أن يكون لديك خوادم DNS يمكن الوصول إليها على مجموعة الخوادم الخاصة بك، ويجب أن تكون واجهات بحث المجال قادرة على الوصول إليها.

```
<#root>

firepower#

show run dns


dns domain-lookup outside


DNS server-group DefaultDNS
DNS server-group dns

name-server 208.67.222.222


name-server 208.67.220.220


dns-group dns

firepower#

ping 208.67.222.222


Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 208.67.222.222, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 170/202/280 ms
firepower#

ping cisco.com


Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 72.163.4.161, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 120/140/190 ms.
```

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).