السماح ب Traceroute من خلال الدفاع ضد تهديد الطاقة النارية (FTD)

المحتويات

المقدمة

يصف هذا وثيقة التشكيل أن يسمح ال traceroute من خلال FirePOWER تهديد الدفاع (FTD) عن طريق سياسة خدمة التهديد.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- مركز إدارة Firepower (FMC)
- Firepower Threat Defense (FTD)

المكونات المستخدمة

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

- تنطبق هذه المقالة على جميع منصات FirePOWER.
- برنامج الدفاع ضد تهديد FirePOWER من Cisco الذي يشغل الإصدار 6.4.0 من البرنامج.
- Cisco Firepower Management Center Virtual الذي يشغل الإصدار 6.4.0 من البرنامج.

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

traceroute لمساعدتك على تحديد المسار الذي تسلكه الحزم إلى وجهتها. يعمل traceroute عن طريق إرسال حزم نظام البيانات ألأساسي الموحد (UDP) إلى وجهة على منفذ غير صالح. نظرا لأن المنفذ غير صالح، فإن الموجهات على طول الطريق إلى الوجهة تستجيب باستخدام رسالة تجاوز وقت بروتوكول رسائل التحكم في الإنترنت (ICMP) الرسالة وتبلغ عن هذه الخطأ إلى جهاز الأمان القابل للتكيف (ASA).

يظهر ال traceroute نتيجة لكل تحقيق يرسل. يراد ف كل سطر من الإخراج قيمة مدة البقاء (TTL) بترتيب متزايد. يشرح هذا الجدول رموز المخرجات.

رمز الإخراج	الوصف
*	لم يتم تلقي أي إستجابة للتحقيق خلال فترة المهلة.
nn msec	لكل عقدة، وقت الذهاب والعودة (بالمللي ثانية) لعدد المسابير المحدد.
!N	يتعذر الوصول إلى شبكة ICMP.
!H	يتعذر الوصول إلى مضيف ICMP.
!P	يتعذر الوصول إلى ICMP.
!C	تم حظر ICMP إدارياً.
؟	خطأ ICMP غير معروف.

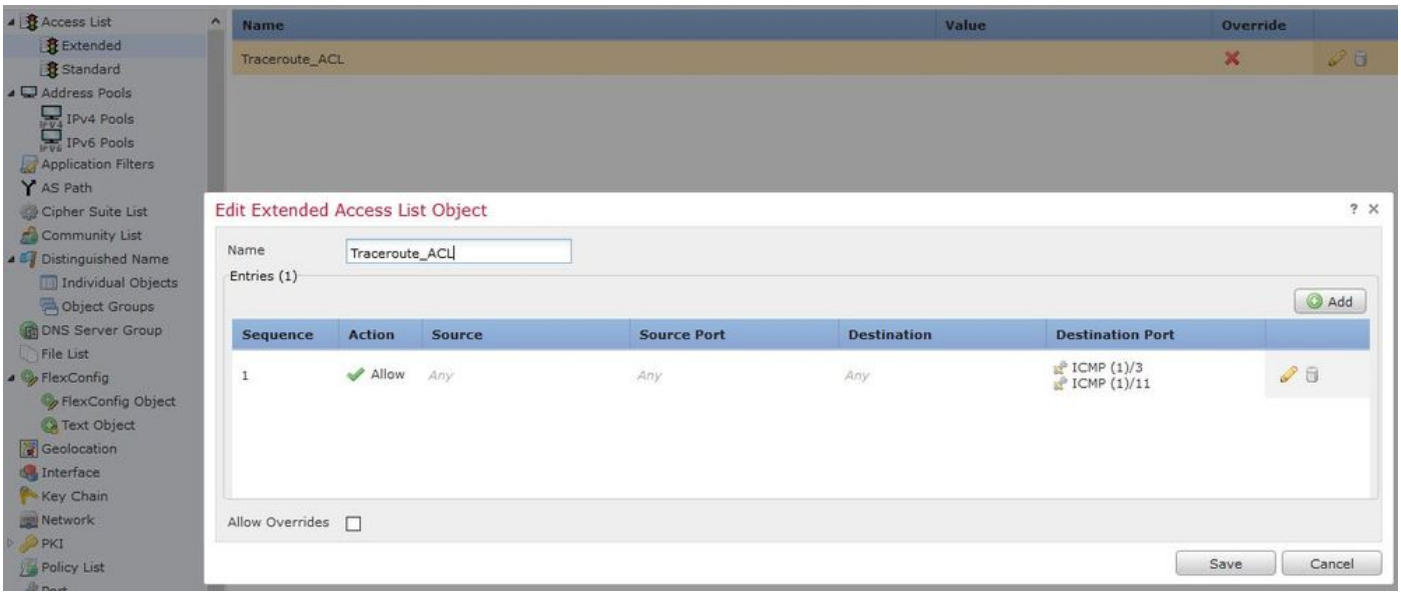
بشكل افتراضي، الظهر ال ASA على traceroutes كجنجل. ولجعلها تظهر، يلزمك تقليل وقت البقاء على الحزم التي تمر عبر ASA وزيادة حد المعدل على رسائل ICMP التي يتعذر الوصول إليها.

تحذير: إذا قمت بتقليل وقت البقاء، يتم إسقاط الحزم ذات مدة البقاء (TTL) رقم 1، ولكن يتم فتح اتصال للجلسة على افتراض أن الاتصال يمكن أن يحتوي على حزم ذات مدة البقاء (TTL) أكبر. لاحظ أنه يتم إرسال بعض الحزم، مثل حزم OSPF مرحبا، مع TTL = 1، لذلك قد يؤدي تحديد الوقت للعيش إلى عواقب غير متوقعة. تذكر هذه الاعتبارات عندما تحدد فئة حركة المرور.

التكوين

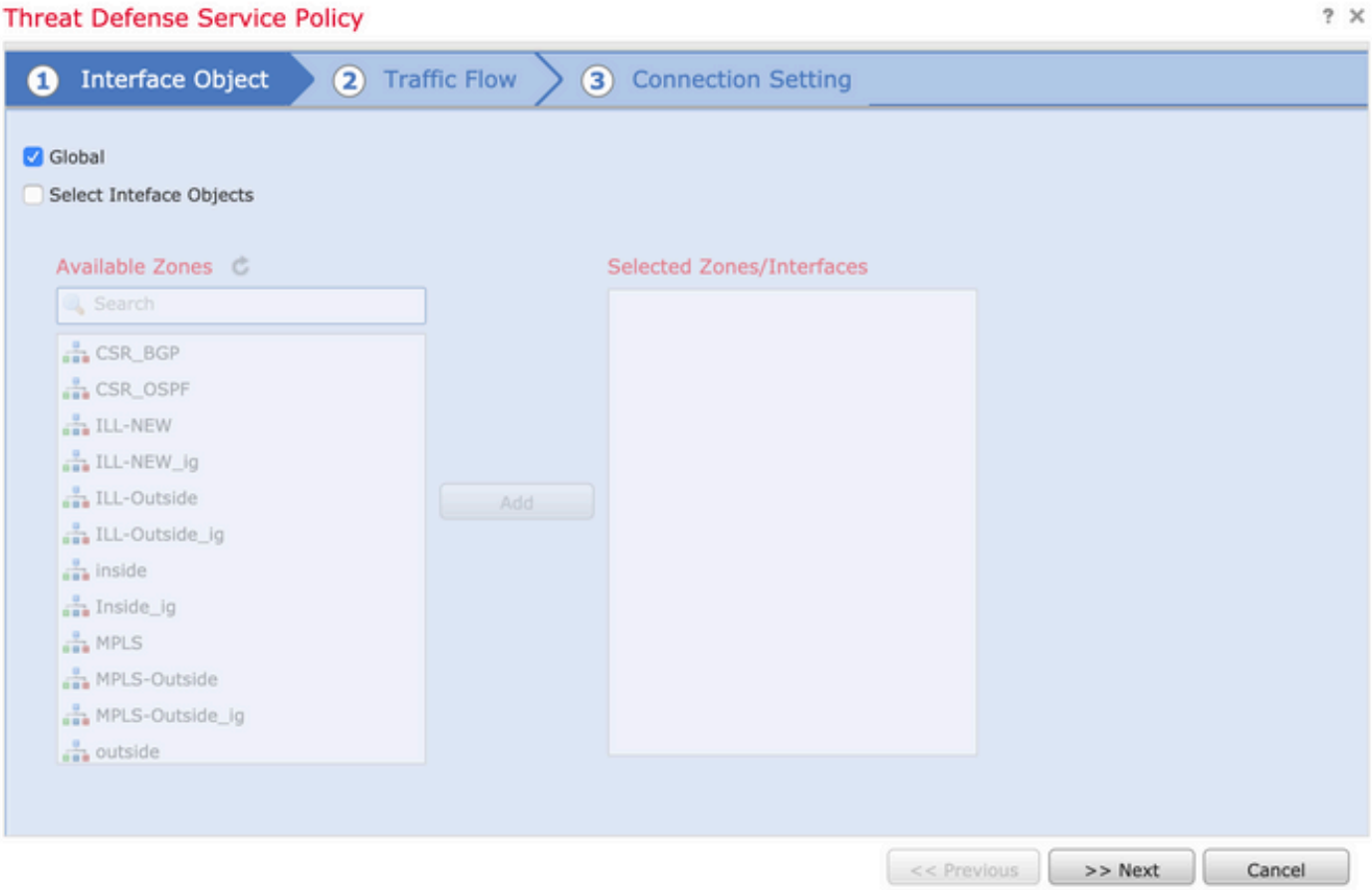
الخطوة 1. قم بإنشاء قائمة التحكم في الوصول (ACL) الموسعة التي تحدد فئة حركة المرور التي يلزم تمكين تقرير traceroute لها.

سجل الدخول إلى واجهة المستخدم الرسومية (GUI) الخاصة بوحدة التحكم FMC وانتقل إلى الكائنات > إدارة الكائنات > قائمة الوصول. حدد موسع من جدول المحتويات وأضف قائمة وصول موسعة جديدة.أدخل اسما للكائن، على سبيل المثال، تحت Traceroute_ACL،أضف قاعدة للسماح بالنوع 3 و 11 من ICMP واحفظه، كما هو موضح في الصورة:

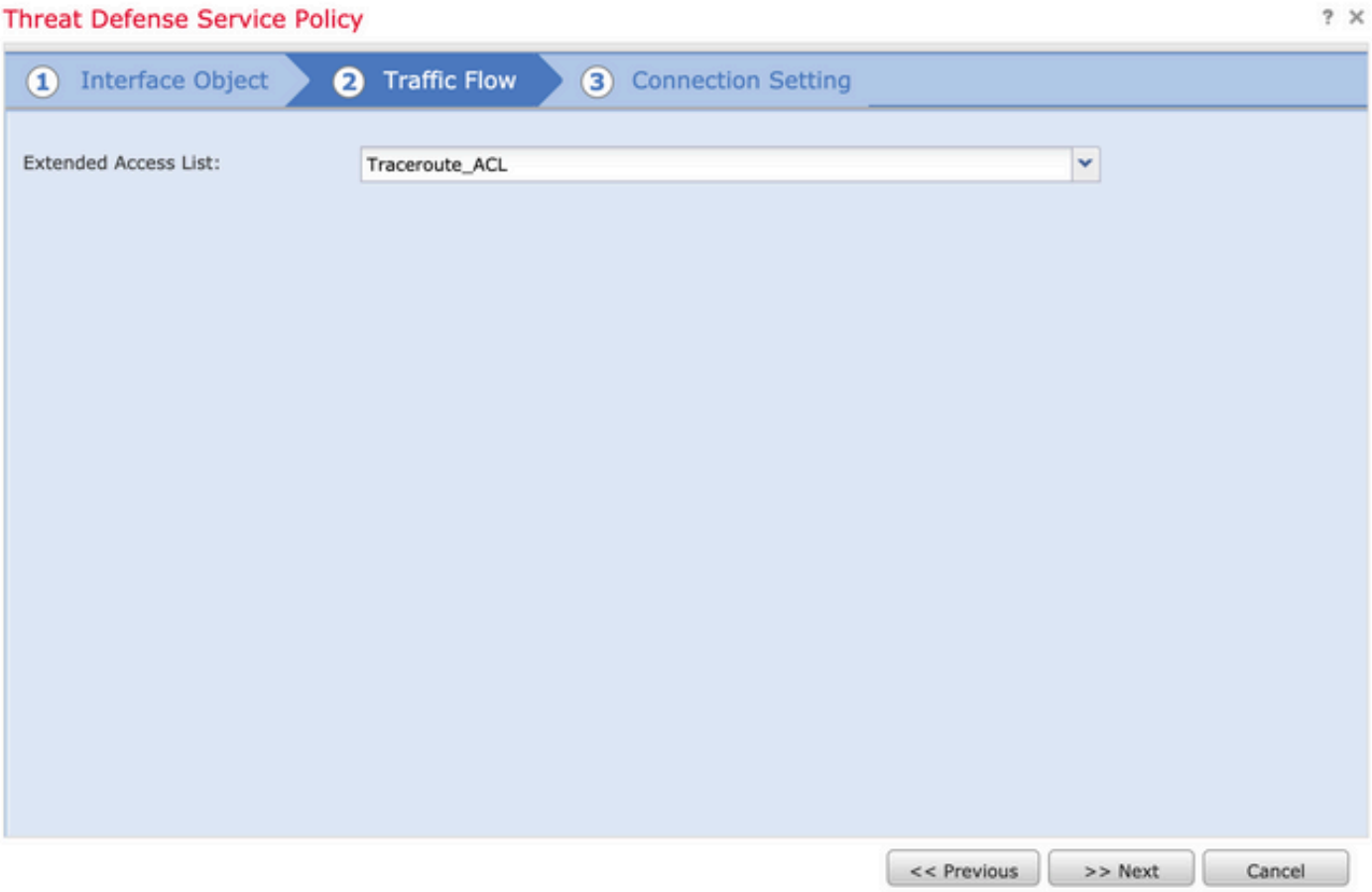


الخطوة 2. قم بتكوين قاعدة سياسة الخدمة التي تقوم بخفض قيمة فترة البقاء.

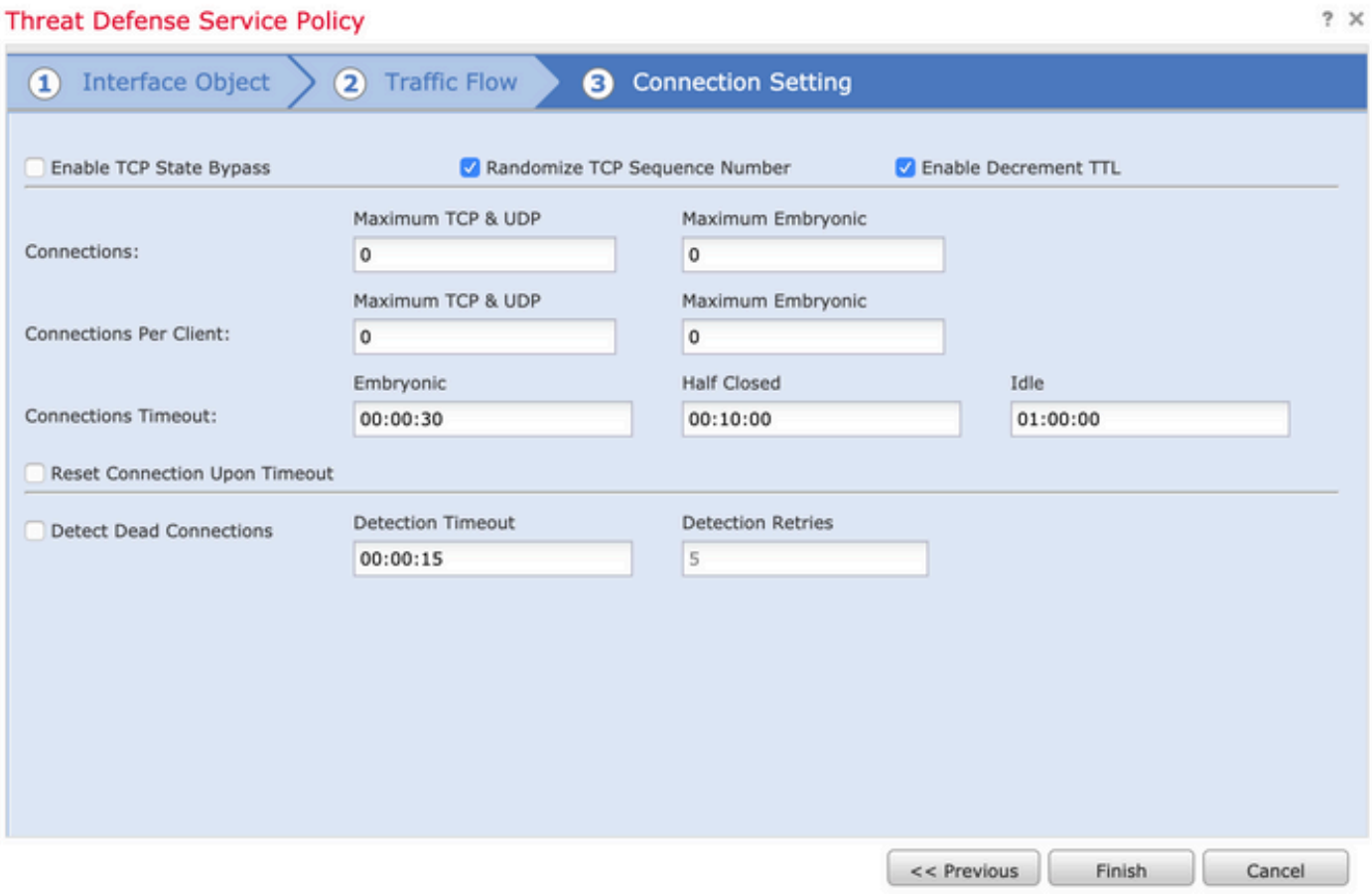
انتقل إلى السياساتالتحكم في الوصول ثم تحرير النهج المعين إلى الجهاز. تحت علامة التبويب خيارات متقدمة، قم بتحرير نهج خدمة الدفاع عن التهديدات، ثم أضف قاعدة جديدة من علامة التبويب إضافة قاعدة، ثم أختر خانة الاختيار عمومي لتطبيقه بشكل عام، وانقر فوق التالي، كما هو موضح في الصورة:



انتقل إلى تدفق حركة المرور > قائمة الوصول الموسعة ثم أختر كائن قائمة الوصول الموسعة من القائمة المنسدلة التي تم إنشاؤها في الخطوات السابقة. انقر الآن التالي، كما هو موضح في الصورة:



أختر خانة الاختيار enable decrement TTL وقم بتعديل خيارات الاتصال الأخرى (إختياري). انقر الآن إنهاء لإضافة القاعدة، ثم انقر فوق موافق، وحفظ التغييرات على نهج خدمة الدفاع عن التهديد، كما هو موضح في الصورة:

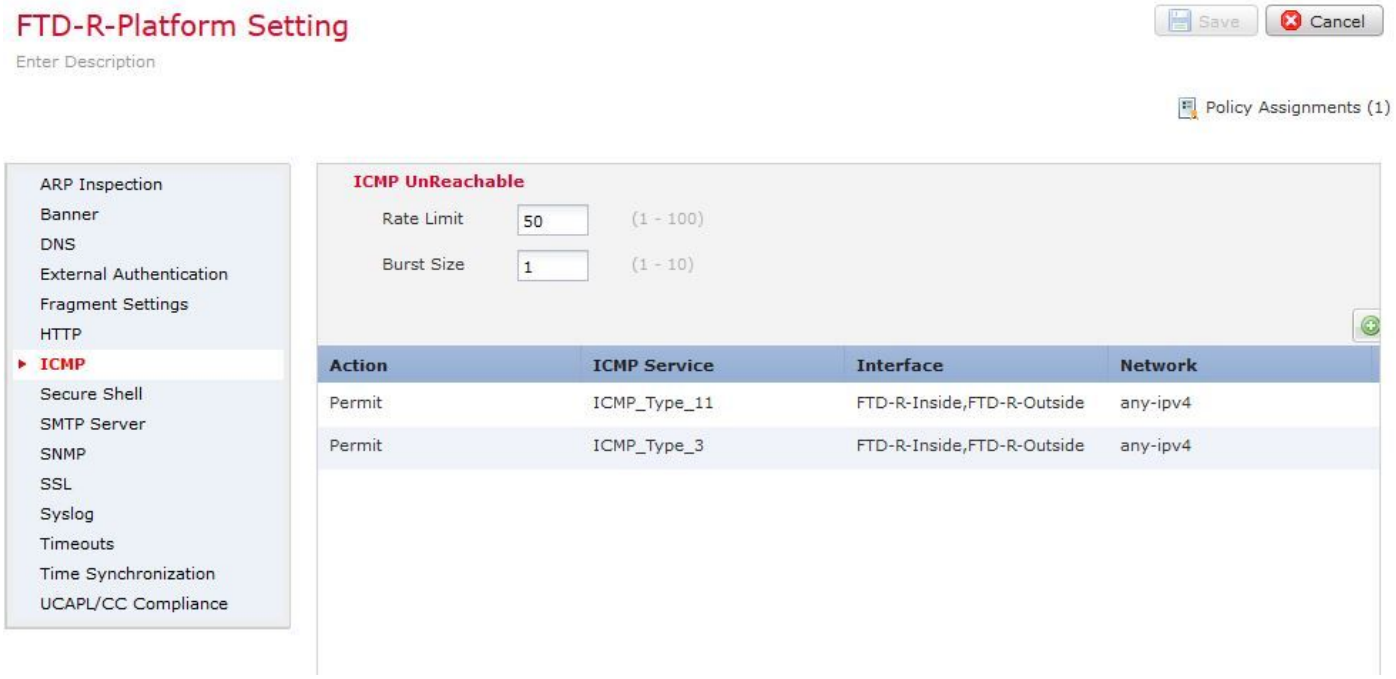


بمجرد اكتمال الخطوات السابقة، احفظ نهج التحكم في الوصول.

الخطوة 3. السماح ب ICMP من الداخل والخارج، وزيادة حد المعدل إلى 50 (إختياري).

انتقل إلى الأجهزة > إعدادات النظام الأساسي ثم حرر أو ينشئ نهج إعدادات النظام الأساسي للدفاع عن تهديد Firepower الجديد ويرتبطه بالجهاز. أختر ICMP من جدول المحتوى وقم بزيادة حد المعدل. على سبيل المثال، إلى 50 (يمكنك تجاهل حجم الاندفاع) ثم انقر فوق حفظ، ثم قم بالمتابعة لنشر النهج على الجهاز، كما هو موضح في الصورة:

- حد المعدل— يحدد حد معدل الرسائل التي يتعذر الوصول إليها، بين 1 و 100 رسالة في الثانية. الافتراضي هو رسالة واحدة في الثانية.
- حجم الاندفاع— يضبط معدل الاندفاع، بين 1 و 10. لا يستخدم النظام هذه القيمة حاليا.



⚠ تحذير: تأكد من أنه لا يمكن الوصول إلى وجهة ICMP (النوع 3) وأن الوقت الذي تجاوز ICMP (النوع 11) مسموح به من الخارج إلى الداخل في سياسة قائمة التحكم في الوصول (ACL) أو FastPath'ed في نهج التصفية المسبقة.

التحقق من الصحة

تحقق من التكوين من واجهة سطر الأوامر (CLI) ل FTD بمجرد اكتمال نشر النهج:

```
FTD# show run policy-map
!
policy-map type inspect dns preset_dns_map
---Output omitted---

class class_map_Traceroute_ACL
set connection timeout idle 1:00:00
set connection decrement-ttl
class class-default
!

FTD# show run class-map
!
class-map inspection_default

---Output omitted---

class-map class_map_Traceroute_ACL
match access-list Traceroute_ACL
!

FTD# show run access-l Traceroute_ACL
access-list Traceroute_ACL extended permit object-group ProxySG_ExtendedACL_30064773500 any any log
FTD#
```

استكشاف الأخطاء وإصلاحها

أنت يستطيع أخذ تقبض على FTD مدخل وخروج قارن ل الحركة مرور مثيرة أن يستكشف أكثر الإصدار.

على Lina، بينما يتم تنفيذ traceroute، يمكن أن هو ظاهر بما أن هذا لكل رجاء على المسار حتى يصل إلى IP الهدف.

```
ftd64# capture icmp interface inside real-time match icmp any any

Warning: using this option with a slow console connection may
         result in an excessive amount of non-displayed packets
         due to performance limitations.

Use ctrl-c to terminate real-time capture


   1: 00:22:04.192800       10.0.0.1 > 10.10.10.11 icmp: time exceeded in-transit
   2: 00:22:04.194432       10.0.0.1 > 10.10.10.11 icmp: time exceeded in-transit
   3: 00:22:04.194447       10.0.0.1 > 10.10.10.11 icmp: time exceeded in-transit
   4: 00:22:04.194981       172.16.1.1 > 10.10.10.11 icmp: time exceeded in-transit
   5: 00:22:04.194997       172.16.1.1 > 10.10.10.11 icmp: time exceeded in-transit
   6: 00:22:04.201130       10.122.149.1 > 10.10.10.11 icmp: time exceeded in-transit
   7: 00:22:04.201146       10.122.149.1 > 10.10.10.11 icmp: time exceeded in-transit
   8: 00:22:04.201161       172.16.1.1 > 10.10.10.11 icmp: time exceeded in-transit
   9: 00:22:04.201375       10.0.114.197 > 10.10.10.11 icmp: time exceeded in-transit
  10: 00:22:04.201420       10.0.254.225 > 10.10.10.11 icmp: time exceeded in-transit
  11: 00:22:04.202336       10.122.149.1 > 10.10.10.11 icmp: time exceeded in-transit
  12: 00:22:04.202519       10.0.127.113 > 10.10.10.11 icmp: time exceeded in-transit
  13: 00:22:04.216022       10.0.127.113 > 10.10.10.11 icmp: time exceeded in-transit
  14: 00:22:04.216038       10.0.127.113 > 10.10.10.11 icmp: time exceeded in-transit
  15: 00:22:04.216038       10.0.114.197 > 10.10.10.11 icmp: time exceeded in-transit
  16: 00:22:04.216053       10.0.114.197 > 10.10.10.11 icmp: time exceeded in-transit
  17: 00:22:04.216297       172.18.127.245 > 10.10.10.11 icmp: 172.18.127.245 udp port 33452 unreachabl
  18: 00:22:04.216312       10.0.254.225 > 10.10.10.11 icmp: time exceeded in-transit
  19: 00:22:04.216327       10.0.254.225 > 10.10.10.11 icmp: time exceeded in-transit
```

إذا قمت بتمكين الحصول على إخراج أكثر تفصيلي على واجهة سطر الأوامر (CLI) من Lina، قم بتنفيذ traceroute باستخدام الخيارات "-I" و "-N" معا.

```
[ On the Client PC ]

# traceroute 10.18.127.245 -I -n

Note: You may not observe any difference between traceroute with or without -I switch. The difference i


[ On FTD Lina CLI ]

ftd64# capture icmp interface inside real-time match icmp any any

Warning: using this option with a slow console connection may
```

```
        result in an excessive amount of non-displayed packets
        due to performance limitations.

Use ctrl-c to terminate real-time capture


    1: 18:37:33.517307       10.10.10.11 > 172.18.127.245 icmp: echo request
    2: 18:37:33.517642       10.10.10.11 > 172.18.127.245 icmp: echo request
    3: 18:37:33.517658       10.10.10.11 > 172.18.127.245 icmp: echo request
    4: 18:37:33.517658       10.10.10.11 > 172.18.127.245 icmp: echo request
    5: 18:37:33.517673       10.10.10.11 > 172.18.127.245 icmp: echo request
    6: 18:37:33.517673       10.10.10.11 > 172.18.127.245 icmp: echo request
    7: 18:37:33.517673       10.10.10.11 > 172.18.127.245 icmp: echo request
    8: 18:37:33.517749       10.10.10.11 > 172.18.127.245 icmp: echo request
    9: 18:37:33.517749       10.10.10.11 > 172.18.127.245 icmp: echo request
   10: 18:37:33.517764       10.10.10.11 > 172.18.127.245 icmp: echo request
   11: 18:37:33.517764       10.10.10.11 > 172.18.127.245 icmp: echo request
   12: 18:37:33.517826       10.10.10.11 > 172.18.127.245 icmp: echo request
   13: 18:37:33.517826       10.10.10.11 > 172.18.127.245 icmp: echo request
   14: 18:37:33.517826       10.10.10.11 > 172.18.127.245 icmp: echo request
   15: 18:37:33.517932       10.10.10.11 > 172.18.127.245 icmp: echo request
   16: 18:37:33.517932       10.10.10.11 > 172.18.127.245 icmp: echo request
   17: 18:37:33.522464       10.0.0.1 > 10.10.10.11 icmp: time exceeded in-transit
   18: 18:37:33.522510       10.0.0.1 > 10.10.10.11 icmp: time exceeded in-transit
   19: 18:37:33.522510       10.0.0.1 > 10.10.10.11 icmp: time exceeded in-transit
   20: 18:37:33.522632       172.16.1.1 > 10.10.10.11 icmp: time exceeded in-transit
   21: 18:37:33.522647       172.16.1.1 > 10.10.10.11 icmp: time exceeded in-transit
   22: 18:37:33.522647       172.16.1.1 > 10.10.10.11 icmp: time exceeded in-transit
   23: 18:37:33.523852       10.0.114.197 > 10.10.10.11 icmp: time exceeded in-transit
   24: 18:37:33.523929       10.0.114.197 > 10.10.10.11 icmp: time exceeded in-transit
   25: 18:37:33.523944       10.0.114.197 > 10.10.10.11 icmp: time exceeded in-transit
   26: 18:37:33.524066       10.0.127.113 > 10.10.10.11 icmp: time exceeded in-transit
   27: 18:37:33.524127       10.0.254.225 > 10.10.10.11 icmp: time exceeded in-transit
   28: 18:37:33.524127       10.0.127.113 > 10.10.10.11 icmp: time exceeded in-transit
   29: 18:37:33.524142       10.0.127.113 > 10.10.10.11 icmp: time exceeded in-transit
   30: 18:37:33.526767       10.122.149.1 > 10.10.10.11 icmp: time exceeded in-transit
   31: 18:37:33.526843       10.122.149.1 > 10.10.10.11 icmp: time exceeded in-transit
   32: 18:37:33.526843       10.122.149.1 > 10.10.10.11 icmp: time exceeded in-transit
   33: 18:37:33.527652       10.10.10.11 > 172.18.127.245 icmp: echo request
   34: 18:37:33.527697       10.10.10.11 > 172.18.127.245 icmp: echo request
   35: 18:37:33.527713       10.10.10.11 > 172.18.127.245 icmp: echo request
   36: 18:37:33.527728       10.10.10.11 > 172.18.127.245 icmp: echo request
   37: 18:37:33.527987       10.10.10.11 > 172.18.127.245 icmp: echo request
   38: 18:37:33.528033       10.10.10.11 > 172.18.127.245 icmp: echo request
   39: 18:37:33.528048       10.10.10.11 > 172.18.127.245 icmp: echo request
   40: 18:37:33.528048       10.10.10.11 > 172.18.127.245 icmp: echo request
   41: 18:37:33.528064       10.10.10.11 > 172.18.127.245 icmp: echo request
   42: 18:37:33.528064       10.10.10.11 > 172.18.127.245 icmp: echo request
   43: 18:37:33.528079       10.10.10.11 > 172.18.127.245 icmp: echo request
   44: 18:37:33.528094       10.10.10.11 > 172.18.127.245 icmp: echo request
   45: 18:37:33.528094       10.10.10.11 > 172.18.127.245 icmp: echo request
   46: 18:37:33.532870       10.0.254.225 > 10.10.10.11 icmp: time exceeded in-transit
   47: 18:37:33.532885       10.0.254.225 > 10.10.10.11 icmp: time exceeded in-transit
   48: 18:37:33.533679       172.18.127.245 > 10.10.10.11 icmp: echo reply
   49: 18:37:33.533694       172.18.127.245 > 10.10.10.11 icmp: echo reply
   50: 18:37:33.533694       172.18.127.245 > 10.10.10.11 icmp: echo reply
   51: 18:37:33.533694       172.18.127.245 > 10.10.10.11 icmp: echo reply
   52: 18:37:33.533694       172.18.127.245 > 10.10.10.11 icmp: echo reply
   53: 18:37:33.533724       172.18.127.245 > 10.10.10.11 icmp: echo reply
   54: 18:37:33.533724       172.18.127.245 > 10.10.10.11 icmp: echo reply
   55: 18:37:33.533724       172.18.127.245 > 10.10.10.11 icmp: echo reply
   56: 18:37:33.533740       10.10.10.11 > 172.18.127.245 icmp: echo request
```

```
  57: 18:37:33.533816       10.10.10.11 > 172.18.127.245 icmp: echo request
  58: 18:37:33.533831       10.10.10.11 > 172.18.127.245 icmp: echo request
  59: 18:37:33.537066       172.18.127.245 > 10.10.10.11 icmp: echo reply
  60: 18:37:33.537081       172.18.127.245 > 10.10.10.11 icmp: echo reply
  61: 18:37:33.537081       172.18.127.245 > 10.10.10.11 icmp: echo reply
  62: 18:37:33.538500       172.18.127.245 > 10.10.10.11 icmp: echo reply
  63: 18:37:33.538500       172.18.127.245 > 10.10.10.11 icmp: echo reply
  64: 18:37:33.539217       172.18.127.245 > 10.10.10.11 icmp: echo reply
64 packets shown.
0 packets not shown due to performance limitations.
```

تلميح: معرف تصحيح الأخطاء من Cisco CSCvq79913. يتم إسقاط حزم أخطاء ICMP لـ PDTS_info فارغ. تأكد من إستخدام عامل التصفية المسبق لـ ICMP، ويفضل لحركة مرور الإرجاع من النوع 3 و 11.

معلومات ذات صلة

الدعم التقني والمستندات - Cisco Systems

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).