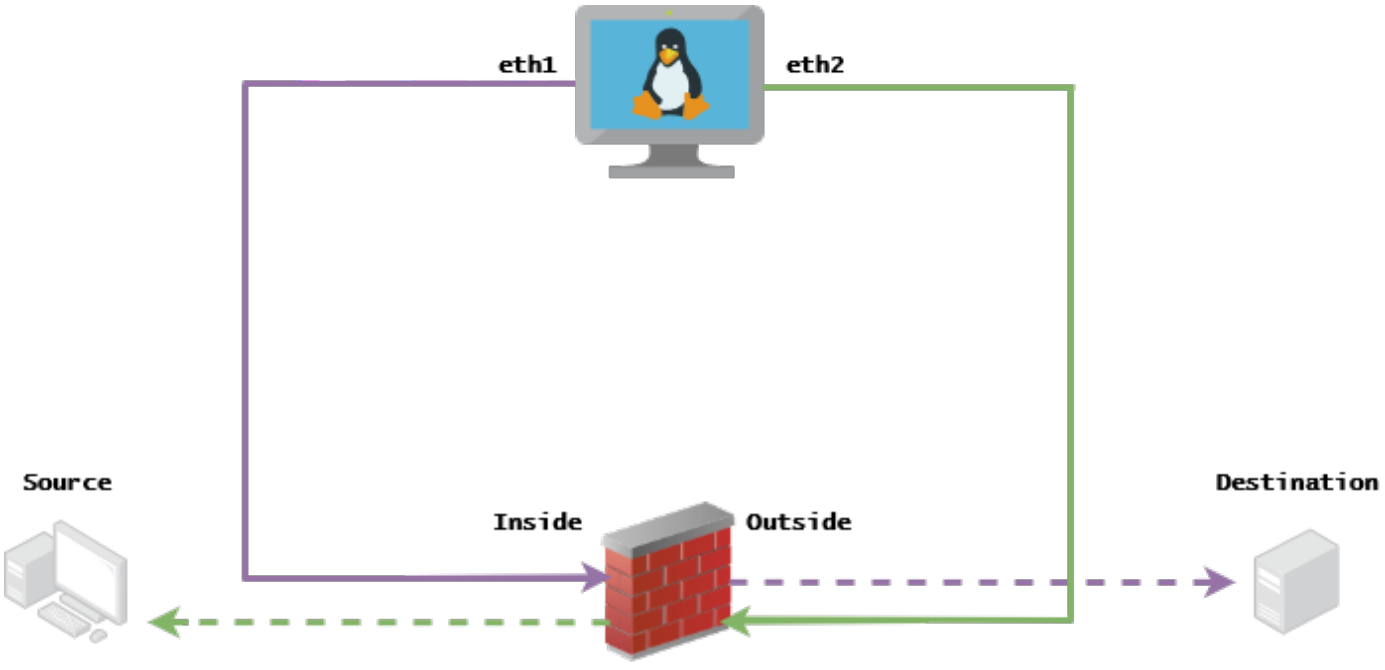
تكوين إعادة تشغيل TCP باستخدام بطاقتي واجهة شبكة (NICs) على Kali Linux

المحتويات

المقدمة

يصف هذا وثيقة TCP إعادة تشغيل أن يعيد حركة مرور الشبكة من ملفات PCAP محفوظة مع ربط التقاط أداة.

طوبولوجيا



المتطلبات

- VM مع kali Linux وبطاقتي واجهة شبكة (NICs)
- برنامج الإرسال فائق السرعة (FTD) (يفضل أن تتم إدارته بواسطة FMC)
- معرفة Linux لتشغيل الأوامر.

معلومات أساسية

إعادة تشغيل TCP هو أداة تستخدم لإعادة تشغيل حركة مرور الشبكة من ملفات PCAP المحفوظة باستخدام أدوات التقاط الحزم مثل wireshark أو TCPdump. يمكن أن يكون مفيدا للمواقف التي تحتاج فيها إلى نسخ حركة المرور لاختبار النتيجة على أجهزة الشبكة.

تتمثل العملية الأساسية لإعادة تشغيل TCP في إعادة إرسال جميع الحزم من ملف (ملفات) الإدخال بسرعة تسجيلها أو معدل بيانات محدد، بسرعة تصل إلى قدرة الجهاز.

هناك طرق أخرى لتنفيذ هذا الإجراء، ومع ذلك، فإن الغرض من هذه المقالة هو تحقيق إعادة تشغيل TCP دون الحاجة إلى موجه متوسط.

التنفيذ

تكوين FTD:

1. قم بتكوين الواجهات الداخلية/الخارجية باستخدام IP على نفس المقطع الذي تمتلكه على جهاز الالتقاط الخاص بك:

No.	Time	Source	Destination
1	0.000000	172.16.211.177	192.168.73.97

- **المصدر:** 172.16.211.177
- **الوجهة**: 192.168.73.97

FMC > الأجهزة > إدارة الأجهزة > الواجهات > تحرير كل واجهة

> **تلميح**: من أفضل الممارسات تخصيص كل واجهة في شبكة VLAN مختلفة لإبقاء حركة المرور معزولة.

running-config (مثال)

```
interface Ethernet1/1
 nameif Outside
 ip address 192.168.73.34 255.255.255.0
!
interface Ethernet1/2
 nameif Inside
 security-level 0
 ip address 172.16.211.34 255.255.255.0
```

2. قم بتكوين المسارات الثابتة من الأجهزة المضيفة إلى بواباتها وإدخالات ARP المزيفة إليها. انظر الأمثلة عبارة عن بوابات غير موجودة.

FMC > Devices > Device Management > Routes > Select your FTD > Routing > Static Route > Add Route

running-config (مثال)

```
route Inside 172.16.211.177 172.16.211.100 1
route Outside 192.168.73.97 192.168.73.100 1
```

أستخدم الباب الخلفي لأداة LinaConfigTool لتكوين إدخالات ARP المزيفة:

1. تسجيل الدخول إلى واجهة سطر الأوامر (CLI) الخاصة ب FTD
2. الانتقال إلى وضع الخبراء
3. رفع الامتيازات الخاصة بك (sudo su)

مثال تكوين LinaConfigTool

```
/usr/local/sf/bin/LinaConfigTool "arp Inside 172.16.211.100 dead.deed.deed"
/usr/local/sf/bin/LinaConfigTool "arp Outside 192.168.73.100 dead.deed.deed"
/usr/local/sf/bin/LinaConfigTool "write mem"
```

3. قم بتعطيل عشوائية رقم التسلسل المتساوي.

1. إنشاء قائمة وصول موسعة: **Go to FMC > Objects > Access List > Extended > Add Extended Access List**قم بإنشاء قائمة التحكم في الوصول (ACL) بمعاملات "السماح بأي"
2. تعطيل عشوائية رقم التسلسل: **Go to FMC > Policies > Access Control > Select your ACP > Advanced > Threat Defense Service Policy**إضافة قاعدة وتحديد **Global** حدد منشئ ال ACL السابق **Extended ACL**إلغاء التحقق **Randomize TCP Sequence Number**

التكوين الجاري (running-config)

```
policy-map global_policy
class class-default
set connection random-sequence-number disable
```

تهيئة لينوكس:

1. تكوين IP لكل واجهة (يستند هذا إلى أي واحد ينتمي إلى الشبكة الفرعية الداخلية والشبكة الفرعية الخارجية) ifconfig ethX <ip_address> netmask <mask> مثال: ifconfig eth1 172.16.211.35 netmask 255.255.255.0
2. (اختياري) قم بتكوين كل واجهة في شبكة VLAN مختلفة
3. نقل ملف PCAP إلى خادم Kali Linux (يمكنك الحصول على ملف PCAP باستخدام tcpdump، التقاط على FTD، وما إلى ذلك)
4. إنشاء ملف ذاكرة تخزين مؤقت لإعادة تشغيل TCP باستخدام **TCPPREP** tcpprep -i input_file -o input_cache -c server_ip/32 مثال: tcpprep -i stream.pcap -o stream.cache -c 192.168.73.97/32
5. إعادة كتابة عناوين MAC باستخدام **tcprewrite** tcprewrite -i input_file -o output_file -c input_cache -c —enet-dmac=<ftd_server_interface_mac>،<ftd_client_interface_mac> مثال: tcprewrite -i stream.pcap -o stream.pcap.replay -c stream.cache -c —enet-dmac=00:50:56:b3:81:35،00:50:56:b3:63:f4
6. توصيل بطاقات واجهة الشبكة (NIC) ب ASA/FTD
7. إعادة تشغيل التدفق باستخدام **tcpreplay** tcpreplay -c input_cache -i <nic_server_interface> -i <nic_client_interface> output_file مثال: tcpreplay -c stream.cache -i eth2 -i eth1 stream.pcap.replay

التحقق من الصحة

قم بإنشاء حزم على FTD لاختبار ما إذا كانت الحزم التي تصل إلى الواجهة الخاصة بك:

1. إنشاء التقاط حزمة على الواجهة الداخلية CAP i داخل قران تتبع مطابقة ip any
2. إنشاء التقاط حزمة على الواجهة الخارجية واجهة CAP o الخارجية طابقة التتبع IP any

تذكر أن tcpreplay وتصفحها إن الربط وصل داخل قران ك:

وي ران ي س ل اث م

```
firepower# show cap
capture i type raw-data trace interface Inside interface Outside [Capturing - 13106 bytes]
match ip any any
capture o type raw-data trace interface Outside [Capturing - 11348 bytes]
match ip any any
firepower# show cap i

47 packets captured

1: 00:03:53.657299 172.16.211.177.23725 > 192.168.73.97.443: S 1610809777:1610809777(0) win 8192
```

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).