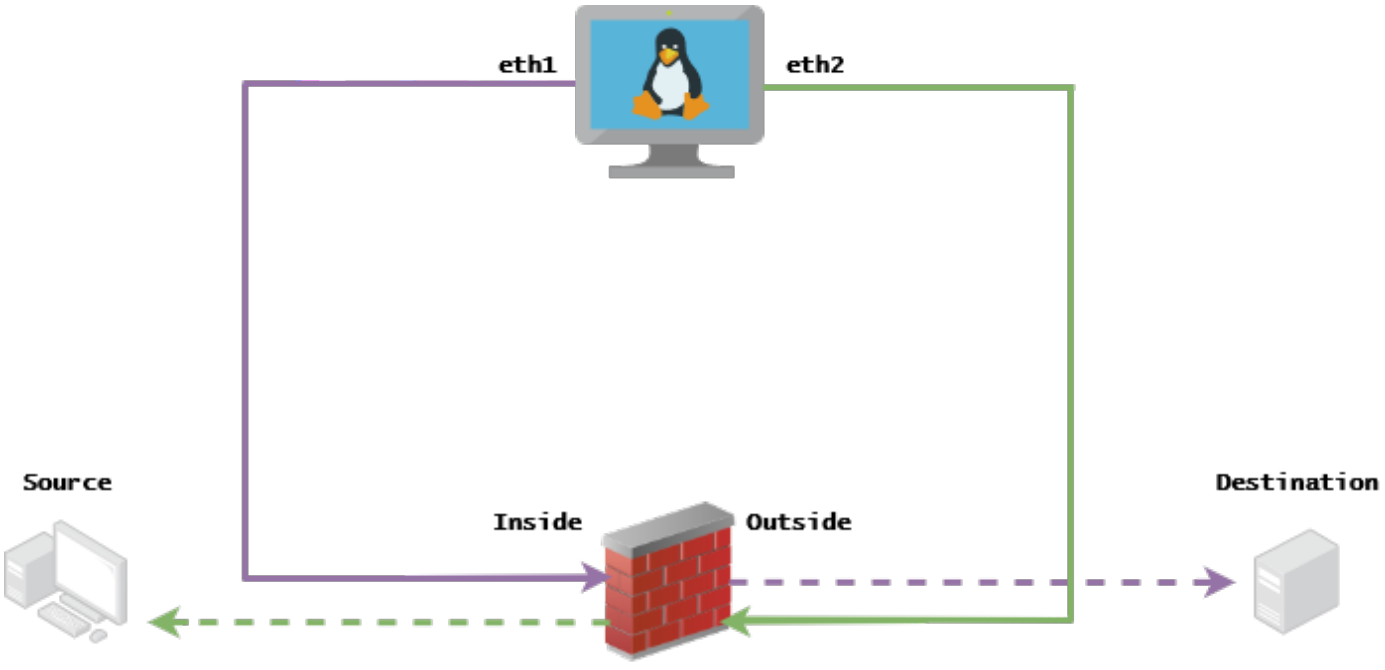
Konfigurieren der TCP-Wiedergabe mit 2 NICs unter Kali Linux

Inhalt

Einleitung

In diesem Dokument wird die TCP-Wiedergabe beschrieben, um den Netzwerkverkehr von PCAP-Dateien wiederzugeben, die mit Paketerfassungs-Tools gespeichert wurden.

Topologie



Voraussetzungen

- VM mit Kali Linux und zwei NICs
- FTD (vorzugsweise von FMC verwaltet)
- Linux-Kenntnisse zum Ausführen von Befehlen.

Hintergrundinformationen

TCP-Wiedergabeist ein Tool, mit dem der Netzwerkverkehr von pcap-Dateien wiedergegeben wird, die mit Paketerfassungstools wie Wireshark oder TCPdump gespeichert wurden. Es kann in Situationen nützlich sein, in denen Sie Datenverkehr replizieren müssen, um das Ergebnis auf Netzwerkgeräten zu testen.

Die grundlegende Funktion der TCP-Wiedergabe besteht darin, alle Pakete aus der bzw. den Eingabedatei(en) mit der Geschwindigkeit, mit der sie aufgezeichnet wurden, bzw. einer bestimmten Datenrate erneut zu senden, und zwar so schnell, wie die Hardware dazu in der Lage ist.

Es gibt andere Methoden, um dieses Verfahren durchzuführen, aber der Zweck dieses Artikels ist es, TCP-Wiedergabe ohne die Notwendigkeit eines mittleren Routers zu erreichen.

Implementierung

FTD-Konfiguration:

1. Konfigurieren Sie die internen/externen Schnittstellen mit einer IP auf dem gleichen Segment, das Sie auf Ihrer Paketerfassung haben:

No.	Time	Source	Destination
1	0.000000	172.16.211.177	192.168.73.97

- **Quelle:** 172.16.211.177
- **Zielort**: 192.168.73.97

FMC > Devices > Device Management > Interfaces > Edit each interface

> **Tipp:** Es empfiehlt sich, jede Schnittstelle einem anderen VLAN zuzuweisen, um den Datenverkehr isoliert zu halten.

Running-config (Beispiel)

```
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. Konfigurieren Sie statische Routen von den Hosts zu ihren Gateways und gefälschte ARP-Einträge, da diese Gateways nicht vorhanden sind.

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

Running-config (Beispiel)

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

Verwenden Sie die LinaConfigTool-Backdoor, um gefälschte ARP-Einträge zu konfigurieren:

1. An der FTD-CLI anmelden
2. Zum Expertenmodus wechseln
3. Erhöhen Sie Ihre Berechtigungen (sudo su)

LinaConfigTool - Konfigurationsbeispiel

```
/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. Deaktivieren Sie die Zufallssteuerung der Sequenznummer "Gleich".

1. Erstellen einer erweiterten Zugriffsliste: **Go to FMC > Objects > Access List > Extended > Add Extended Access List**Erstellen Sie die ACL mit den Parametern "allow any any" (Beliebige zulassen)
2. Zufällige Sequenznummern deaktivieren: **Go to FMC > Policies > Access Control > Select your ACP > Advanced > Threat Defense Service Policy**Regel hinzufügen und auswählen **Global** Wählen Sie Ihre zuvor erstellte **Extended ACL**Deaktivieren **Randomize TCP Sequence Number**

Ausführungskonfiguration

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

Linux-Konfiguration:

1. Konfigurieren Sie die IP-Adresse für jede Schnittstelle (diese basiert darauf, welche Schnittstelle zum internen und zum externen Subnetz gehört). ifconfig ethX <IP-Adresse> netmask <Maske> Beispiel: ifconfig eth1 172.16.211.35 netmask 255.255.255.0
2. (Optional) Konfigurieren Sie jede Schnittstelle in einem anderen VLAN.
3. Übertragen Sie die PCAP-Datei in den Kali Linux-Server (Sie können die pcap-Datei mit tcpdump, Aufnahmen auf der FTD, etc. erhalten)
4. Erstellen einer TCP-Wiedergabe-Cachedatei mit **tcpprep** tcpprep -i input_file -o input_cache -c server_ip/32 Beispiel: tcpprep -i stream.pcap -o stream.cache -c 192.168.73.97/32
5. Umschreiben der MAC-Adressen mit **tcprewrite** tcprewrite -i input_file -o output_file -c input_cache -C —enet-dmac=<ftd_server_interface_mac>,<ftd_client_interface_mac> Beispiel: 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. Verbinden von NICs mit ASA/FTD
7. Wiedergabe des Streams mit **tcpreplay** tcpreplay -c input_cache -i <nic_server_interface> -I <nic_client_interface> output_file
   Beispiel: tcpreplay -c stream.cache -i eth2 -I eth1 stream.pcap.replay

Validierung

Erstellen Sie Paketerfassungen auf Ihrem FTD, um zu testen, ob die Pakete, die an Ihre Schnittstelle ankommen:

1. Erstellung der Paketerfassung über die interne Schnittstelle cap i interface Inside trace match ip any any
2. Erstellung der Paketerfassung auf der externen Schnittstelle Obergrenze der Schnittstelle Außerhalb trace match ip any any

Führen Sie tcpreplay aus, und überprüfen Sie, ob die Pakete an Ihre Schnittstelle gelangen:

Beispielszenario

```
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
```

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.