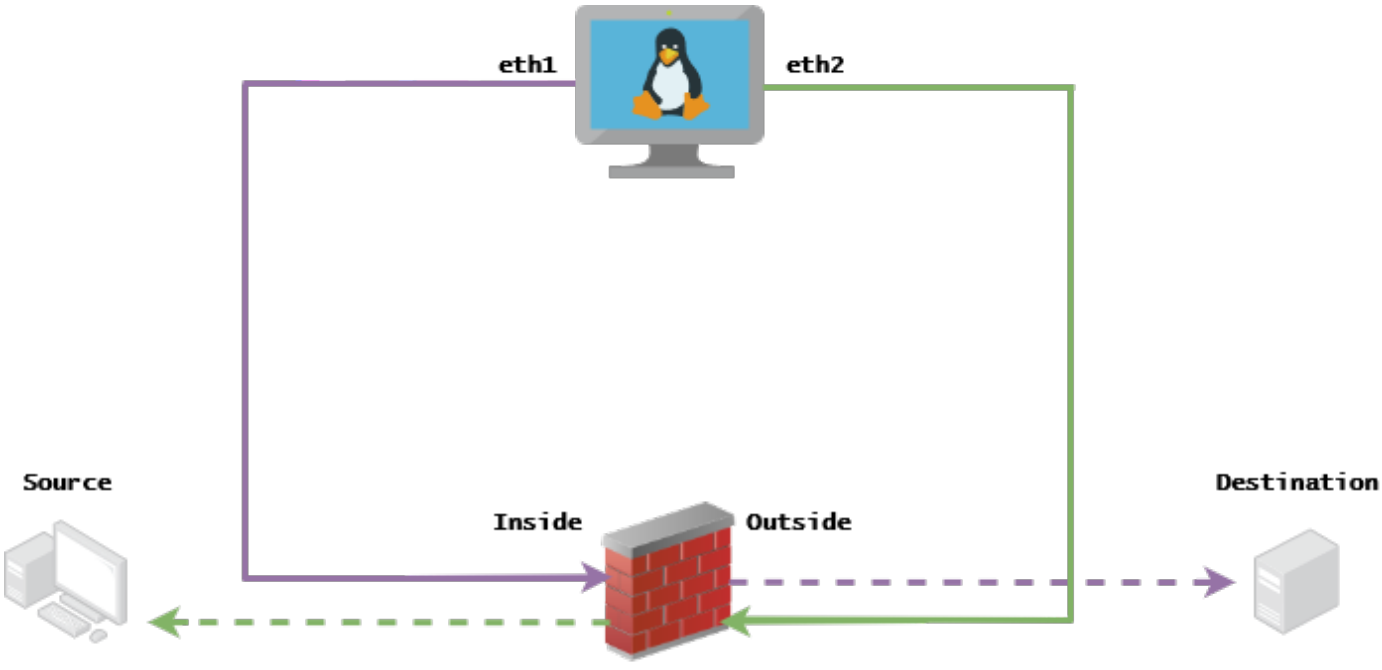
TCP Replay configureren met 2 NIC's op Kali Linux

Inhoud

Inleiding

Dit document beschrijft TCP-terugspelen om netwerkverkeer van PCAP-bestanden die met pakketopnametools zijn opgeslagen, terug te spelen.

Topologie



Vereisten

- VM met Kali Linux en twee NIC’s
- FTD (bij voorkeur beheerd door het VCC)
- Linux kennis om opdrachten uit te voeren.

Achtergrondinformatie

TCP-terugspelenis een gereedschap dat wordt gebruikt om netwerkverkeer van pcap-bestanden die zijn opgeslagen met pakketopnametools zoals wireshark of TCPdump, terug te spelen. Het kan nuttig zijn voor situaties waar u verkeer moet herhalen om het resultaat op netwerkapparaten te testen.

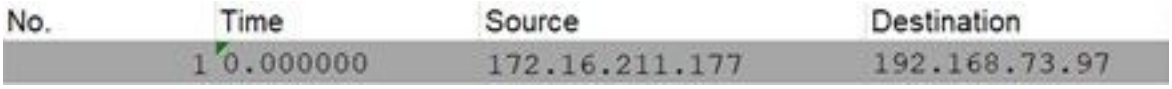
De basisbediening van TCP Replay is om alle pakketten van het invoerbestand of de invoerbestanden opnieuw te verzenden met de snelheid waarmee ze zijn opgenomen of met een opgegeven gegevenssnelheid, tot zo snel als de hardware mogelijk is.

Er zijn andere methoden om deze procedure uit te voeren, maar het doel voor dit artikel is om TCP Replay te bereiken zonder de noodzaak van een middenrouter.

Implementatie

FTD-configuratie:

1. Configureer de interfaces binnen/buiten met een IP op hetzelfde segment dat u op uw pakket hebt opgenomen:



No.	Time	Source	Destination
1	0.000000	172.16.211.177	192.168.73.97

- **Bron:** 172.16.211.177
- **Bestemming**: 192 168 73 97

FMC > Apparaten > Apparaatbeheer > Interfaces > Elke interface bewerken

> **Tip**: het is de beste praktijk om elke interface in een ander VLAN toe te wijzen om het verkeer te isoleren.

Config (voorbeeld)

```
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. Configureer statische routes van de hosts naar hun gateways en nep ARP ingangen naar hen omdat dit niet-bestaande gateways zijn.

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

Config (voorbeeld)

```
route Inside 172.16.211.177 172.16.211.100 1
```

```
route Outside 192.168.73.97 192.168.73.100 1
```

Gebruik de achterdeur van LinaConfigTool om valse ARP-vermeldingen te configureren:

1. Aanmelden bij de FTD CLI
2. Ga naar expert-modus
3. Verhoog je rechten (sudo su)

Configuratievoorbeeld van LinaconfiguratieTool

```
/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. Schakel de randomisatie van het evenaarsnummer uit.

1. Een uitgebreide toegangslijst maken: **Go to FMC > Objects > Access List > Extended > Add Extended Access List**Maak de ACL met parameters "toestaan om het even welk"
2. Schakel randomisatie van sequentienummer uit: **Go to FMC > Policies > Access Control > Select your ACP > Advanced > Threat Defense Service Policy**Voeg regel toe en selecteer **Global** Selecteer uw eerder gemaakte afbeelding **Extended ACL**Uitschakelen **Randomize TCP Sequence Number**

Config

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

Linux-configuratie:

1. Configureer het IP voor elke interface (dit is gebaseerd op welke interface tot het binnen- en het buitennetwerk behoort) ifconfig ethX <ip_address> netmask <masker> voorbeeld: ifconfig eth1 172.16.211.35 netmask 255.255.255.0
2. (Optioneel) Configureer elke interface in een ander VLAN
3. Transfer PCAP-bestand naar de Kali Linux-server (u kunt het pcap-bestand met tcpdump krijgen, vangt op de FTD, etc)
4. Maak een TCP Replay cache bestand met **tcprep** tcprep -i input_file -o input_cache -c server_ip/32 voorbeeld: tcpprep -i stream.pcap -o stream.cache -c 192.168.73.97/32
5. Herschrijf de MAC-adressen met **tcprewrite** tcprewrite -i input_file -o output_file -c input_cache -C —enet-dmac=<ftd_server_interface_mac>,<ftd_client_interface_mac> voorbeeld: 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. Sluit NIC's aan op de ASA/FTD
7. De stream opnieuw afspelen met **tcpreplay** tcpreplay -c input_cache -i <nic_server_interface> -I <nic_client_interface> output_file
   voorbeeld: tcpreplay -c stream.cache -i eth2 -I eth1 stream.pcap.replay

Validatie

Maak pakketopnamen op uw FTD om te testen of de pakketten die in uw interface aankomen:

1. Maak pakketopname op de Inside interface. cap in interface Inside trace match ip elke

willekeurige

2. Maak pakketopname op de buiteninterface buiten afstemmen ip elk gewenst

Draai de tcpreplay en bevestig als de pakketten in uw interface aankomen:

Voorbeeldscenario

```
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
```

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.