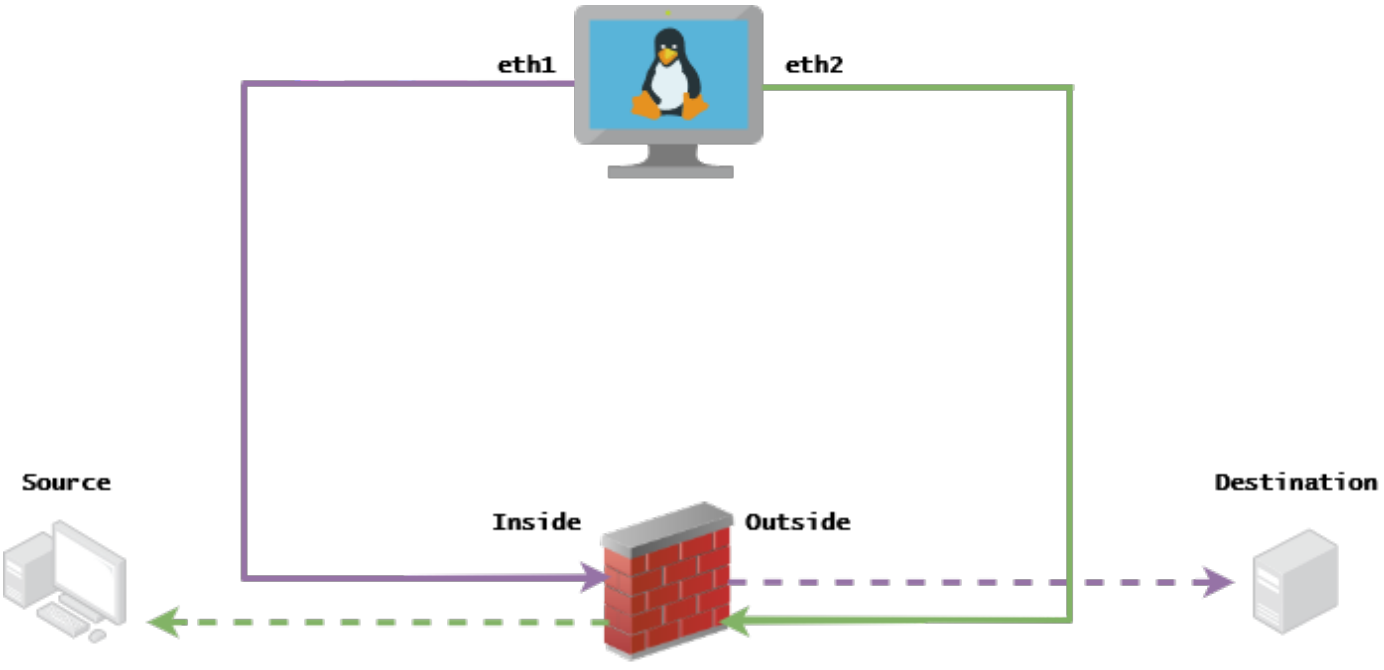
Configuration de la relecture TCP avec 2 cartes réseau sur Kali Linux

Table des matières

Introduction

Ce document décrit la relecture TCP pour relayer le trafic réseau à partir des fichiers PCAP enregistrés avec les outils de capture de paquets.

Topologie



Conditions requises

- VM avec Kali Linux et deux cartes réseau
- FTD (de préférence géré par FMC)
- Connaissance de Linux pour exécuter des commandes.

Informations générales

Réexécution TCPest un outil utilisé pour lire le trafic réseau à partir de fichiers pcap enregistrés avec des outils de capture de paquets tels que wireshark ou TCPdump. Il peut être utile dans les situations où vous devez répliquer le trafic pour tester le résultat sur des périphériques réseau.

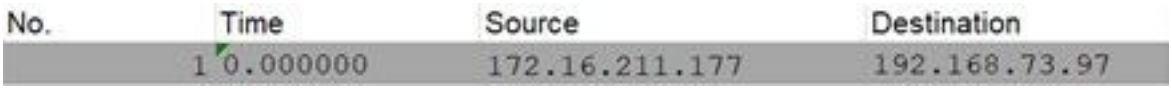
L'opération de base de la relecture TCP consiste à renvoyer tous les paquets du ou des fichiers d'entrée à la vitesse à laquelle ils ont été enregistrés, ou à un débit de données spécifié, jusqu'à la vitesse maximale autorisée par le matériel.

Il existe d'autres méthodes pour effectuer cette procédure, cependant, l'objectif de cet article est d'effectuer une relecture TCP sans avoir besoin d'un routeur intermédiaire.

Mise En Oeuvre

Configuration FTD :

1. Configurez les interfaces internes/externes avec une adresse IP sur le même segment que celui que vous avez sur vos captures de paquets :



No.	Time	Source	Destination
1	0.000000	172.16.211.177	192.168.73.97

- **Source :** 172.16.211.177
- **Destination** : 192.168.73.97

FMC > Périphériques > Gestion des périphériques > Interfaces > Modifier chaque interface

> **Conseil** : il est recommandé d'affecter chaque interface à un VLAN différent pour isoler le trafic.

Running-config (exemple)

```
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. Configurez des routes statiques depuis les hôtes vers leurs passerelles et des entrées ARP factices vers ces hôtes, car il s'agit de passerelles inexistantes.

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

Running-config (exemple)

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

Utilisez la porte dérobée LinaConfigTool pour configurer de fausses entrées ARP :

1. Connexion à l'interface de ligne de commande FTD
2. Passez en mode expert
3. Augmentez vos privilèges (sudo su)

Exemple de configuration de 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. Désactivez la randomisation des numéros de séquence égaux.

1. Créer une liste d'accès étendue : **Go to FMC > Objects > Access List > Extended > Add Extended Access List**Créez la liste de contrôle d'accès avec les paramètres « allow any any »
2. Désactiver la randomisation des numéros de séquence : **Go to FMC > Policies > Access Control > Select your ACP > Advanced > Threat Defense Service Policy**Ajouter une règle et sélectionner **Global** Sélectionnez le fichier créé précédemment **Extended ACL**Décocher **Randomize TCP Sequence Number**

running-config

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

Configuration Linux :

1. Configurez l'adresse IP pour chaque interface (en fonction de celle qui appartient au sous-réseau interne et au sous-réseau externe) ifconfig ethX <adresse_ip> masque_réseau <masque> exemple : ifconfig eth1 172.16.211.35 netmask 255.255.255.0
2. (Facultatif) Configurez chaque interface dans un VLAN différent
3. Transférer le fichier PCAP dans le serveur Kali Linux (Vous pouvez obtenir le fichier pcap avec tcpdump, les captures sur le FTD, etc)
4. Créer un fichier cache de relecture TCP avec **tcpprep** tcpprep -i fichier_entrée -o cache_entrée -c ip_serveur/32 exemple : tcpprep -i stream.pcap -o stream.cache -c 192.168.73.97/32
5. Réécrivez les adresses MAC avec **tcprewrite** tcprewrite -i fichier_entrée -o fichier_sortie -c cache_entrée -C —enet-dmac=<ftd_server_interface_mac>,<ftd_client_interface_mac> exemple : 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. Connexion des cartes réseau à l'ASA/FTD
7. Relire le flux avec **tcpreplay** tcpreplay -c input_cache -i <interface_serveur_carte_réseau> -I <interface_client_carte_réseau> output_file
   exemple : tcpreplay -c stream.cache -i eth2 -I eth1 stream.pcap.replay

Validation

Créez des captures de paquets sur votre FTD pour tester si les paquets qui arrivent dans votre interface :

1. Créer une capture de paquets sur l’interface interne cap i interface Inside trace match ip any any
2. Créer une capture de paquets sur l'interface externe cap o interface Outside trace match ip any any

Exécutez la lecture anticipée et validez si les paquets arrivent dans votre interface :

Exemple de scénario

```
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
```

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.