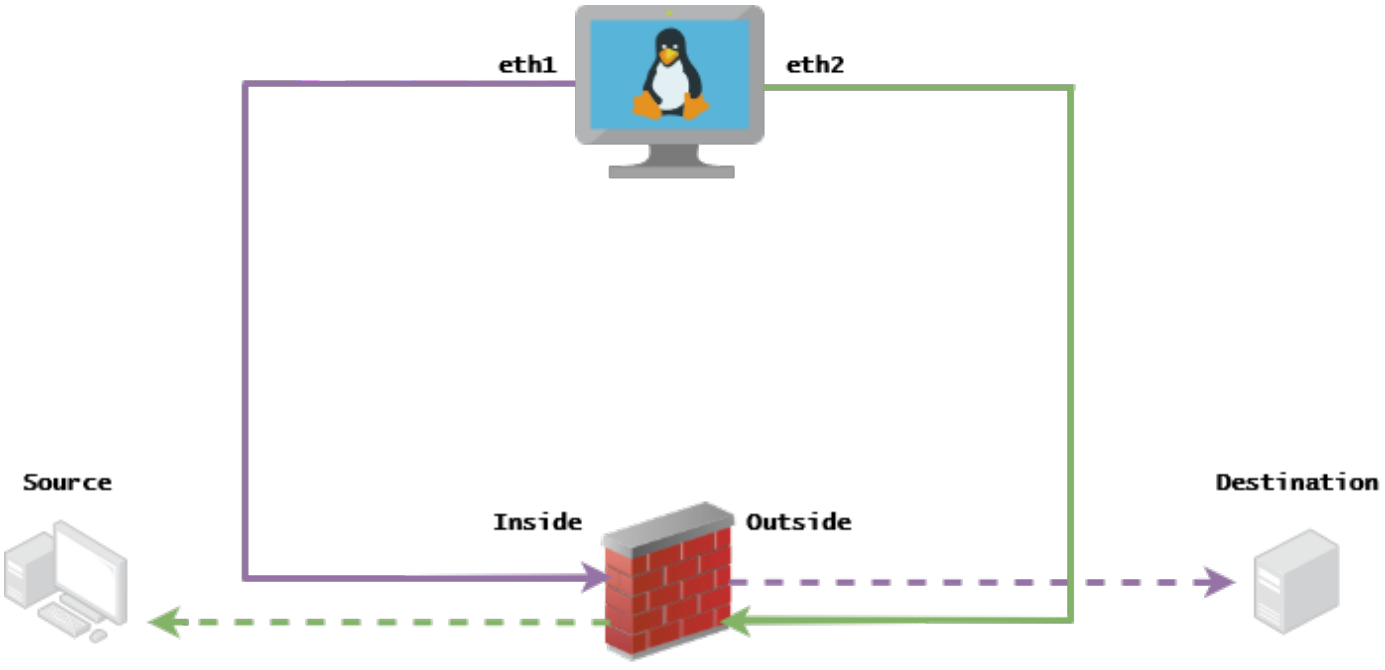
Configuración de TCP Replay con 2 NIC en Kali Linux

Contenido

Introducción

Este documento describe TCP Replay para reproducir el tráfico de red de los archivos PCAP guardados con las herramientas de captura de paquetes.

Topología



Requisitos

- VM con Kali Linux y dos NIC
- FTD (gestionado preferiblemente por el CSP)
- Conocimiento de Linux para ejecutar comandos.

Antecedentes

Reproducción de TCPes una herramienta utilizada para reproducir el tráfico de red de los archivos pcap guardados con herramientas de captura de paquetes como wireshark o TCPdump. Puede resultar útil en situaciones en las que necesite replicar tráfico para probar el resultado en dispositivos de red.

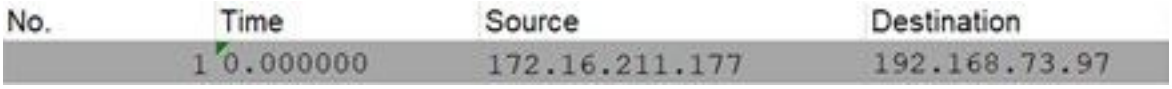
La operación básica de TCP Replay es reenviar todos los paquetes desde los archivos de entrada a la velocidad a la que fueron grabados, o una velocidad de datos especificada, hasta la velocidad que el hardware sea capaz.

Existen otros métodos para realizar este procedimiento, sin embargo, el propósito de este artículo es lograr la Reproducción TCP sin la necesidad de un router intermedio.

Instrumentación

Configuración de FTD:

1. Configure las interfaces interna/externa con una IP en el mismo segmento que tiene en sus capturas de paquetes:



No.	Time	Source	Destination
1	0.000000	172.16.211.177	192.168.73.97

- **Fuente:** 172.16.211.177
- **Destino**: 192.168.73.97

FMC > Dispositivos > Gestión de dispositivos > Interfaces > Editar cada interfaz

> **Sugerencia**: se recomienda asignar cada interfaz a una VLAN diferente para mantener el tráfico aislado.

Running-config (ejemplo)

```
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. Configure rutas estáticas desde los hosts a sus gateways y entradas ARP falsas a ellos, ya que estas son gateways inexistentes.

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

Running-config (ejemplo)

```
route Inside 172.16.211.177 172.16.211.100 1
```

```
route Outside 192.168.73.97 192.168.73.100 1
```

Utilice la puerta trasera LinaConfigTool para configurar entradas ARP falsas:

1. Inicio de sesión en la CLI de FTD
2. Ir al modo experto
3. Aumentar sus privilegios (sudo su)

Ejemplo de configuración 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. Desactive la aleatorización de números de secuencia iguales.

1. Crear una lista de acceso ampliada: **Go to FMC > Objects > Access List > Extended > Add Extended Access List**Cree la ACL con los parámetros "allow any any"
2. Deshabilitar aleatorización de números de secuencia: **Go to FMC > Policies > Access Control > Select your ACP > Advanced > Threat Defense Service Policy**Agregar regla y seleccionar **Global** Seleccione el archivo creado anteriormente **Extended ACL**Desmarcar **Randomize TCP Sequence Number**

Running-config

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

Configuración de Linux:

1. Configure la IP para cada interfaz (se basa en cuál pertenece a la subred interna y a la subred externa) ifconfig ethX <ip_address> netmask <mask> ejemplo: ifconfig eth1 172.16.211.35 netmask 255.255.255.0
2. (Opcional) Configure cada interfaz en una VLAN diferente
3. Transferir el archivo PCAP al servidor Kali Linux (puede obtener el archivo pcap con tcpdump, capturas en el FTD, etc)
4. Cree un archivo de caché de reproducción TCP con **tcprep** tcpprep -i archivo_entrada -o caché_entrada -c ip_servidor/32 ejemplo: tcpprep -i stream.pcap -o stream.cache -c 192.168.73.97/32
5. Reescriba las direcciones MAC con **tcprewrite** tcprewrite -i input_file -o output_file -c input_cache -C —enet-dmac=<ftd_server_interface_mac>,<ftd_client_interface_mac> ejemplo: 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. Conexión de NIC al ASA/FTD
7. Reproduzca la secuencia con **tcpreplay** tcpreplay -c input_cache -i <nic_server_interface> -I <nic_client_interface> output_file
   ejemplo: tcpreplay -c stream.cache -i eth2 -I eth1 stream.pcap.replay

Validación

Cree capturas de paquetes en su FTD para probar si los paquetes que llegan a su interfaz:

1. Crear captura de paquetes en la interfaz interna cap i interface Inside trace match ip any any
2. Crear captura de paquetes en la interfaz externa cap o interface Outside trace match ip any any

Ejecute tcpreplay y valide si los paquetes llegan a su interfaz:

Situación de ejemplo

```
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
```

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).