# Configurar Reprodução TCP com 2 NICs no Kali Linux

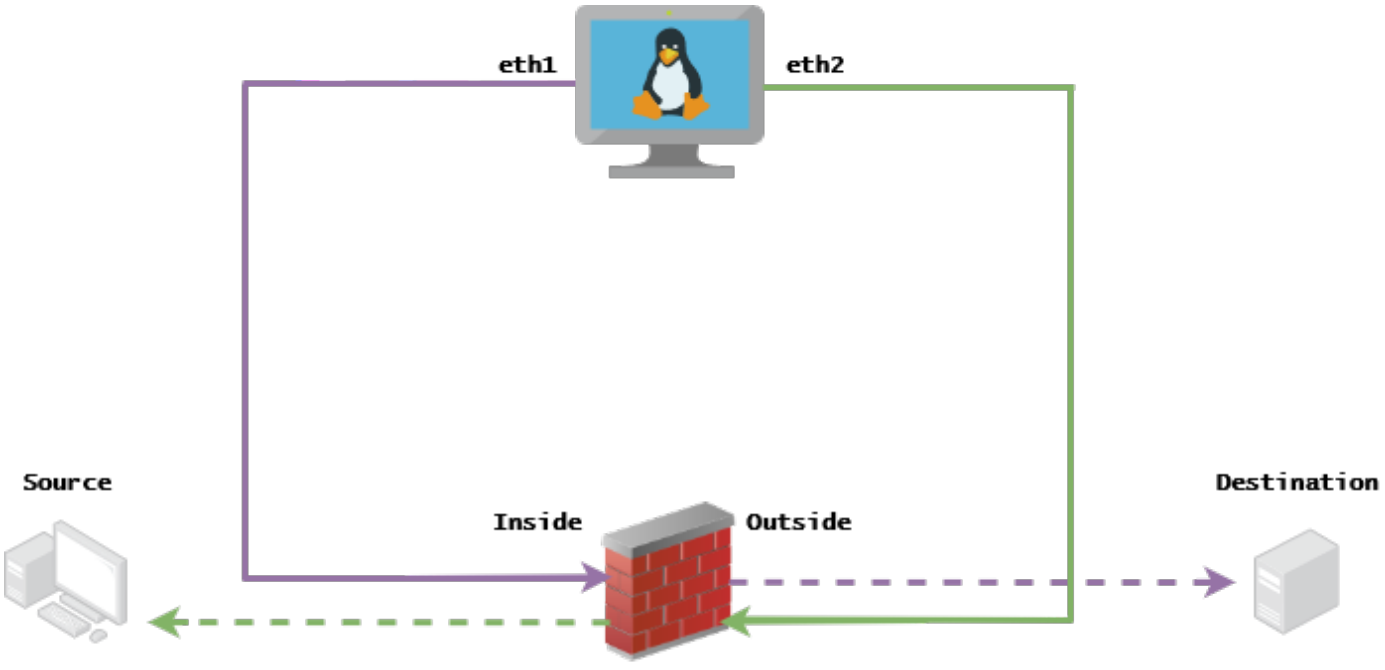
## Contents



## Introduction

Este documento descreve a Repetição de TCP para reproduzir o tráfego de rede de arquivos PCAP salvos com ferramentas de captura de pacotes.

## Topologia




## Requisitos

- VM com Kali Linux e duas NICs
- DTF (de preferência gerido pelo CVP)
- Conhecimento do Linux para executar comandos.

# Informações de Apoio

Reprodução de TCPé uma ferramenta usada para reproduzir o tráfego de rede de arquivos pcap salvos com ferramentas de captura de pacotes como o wireshark ou TCPdump. Ele pode ser útil para situações em que você precisa replicar o tráfego para testar o resultado em dispositivos de rede.

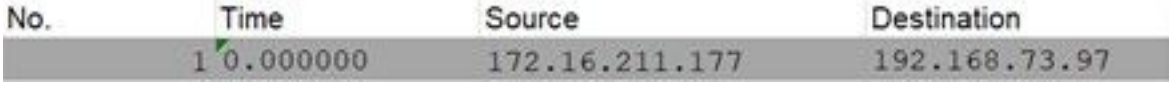
A operação básica do TCP Replay é reenviar todos os pacotes do(s) arquivo(s) de entrada na velocidade em que foram gravados, ou uma taxa de dados especificada, até a velocidade em que o hardware é capaz.

Há outros métodos para executar esse procedimento, no entanto, a finalidade deste artigo é obter a Repetição de TCP sem a necessidade de um roteador do meio.

# Implementação

## Configuração do FTD:

1. Configure as interfaces Internas/Externas com um IP no mesmo segmento que você tem nas capturas de pacotes:




- **Fonte:** 172.16.211.177
- **Destino**: 192.168.73.97

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

> **Dica**: é uma prática recomendada atribuir cada interface a uma VLAN diferente para manter o tráfego isolado.

Running-config (exemplo)

```
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 rotas estáticas dos hosts para seus gateways e falsifique entradas ARP para eles, já que esses são gateways inexistentes.

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

Running-config (exemplo)

```
route Inside 172.16.211.177 172.16.211.100 1
```

```
route Outside 192.168.73.97 192.168.73.100 1
```

Use o backdoor LinaConfigTool para configurar entradas ARP falsas:

1. Faça login na CLI do FTD
2. Ir para o modo especialista
3. Eleve seus privilégios (sudo su)

Exemplo de configuração da 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. Desative a aleatorização do número de sequência igual.

1. Criar uma lista de acesso estendida: **Go to FMC > Objects > Access List > Extended > Add Extended Access List**Crie a ACL com os parâmetros "allow any any"
2. Desabilitar aleatorização de número de sequência: **Go to FMC > Policies > Access Control > Select your ACP > Advanced > Threat Defense Service Policy**Adicionar regra e selecionar **Global** Selecione o que você criou anteriormente **Extended ACL**Desmarcar **Randomize TCP Sequence Number**

Running-config

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

### Configuração do Linux:

1. Configure o IP para cada interface (com base no que pertence à sub-rede interna e à sub-rede externa) ifconfig ethX <ip_address> netmask <mask> exemplo: ifconfig eth1 172.16.211.35 netmask 255.255.255.0
2. (Opcional) Configure cada interface em uma VLAN diferente
3. Transferir o arquivo PCAP para o servidor Linux Kali (Você pode obter o arquivo pcap com tcpdump, capturas no FTD, etc)
4. Crie um arquivo de cache de Repetição TCP com **tcpprep** tcpprep -i input_file -o input_cache -c server_ip/32 exemplo: tcpprep -i stream.pcap -o stream.cache -c 192.168.73.97/32
5. Reescreva os endereços MAC com **tcprewrite** tcprewrite -i input_file -o output_file -c input_cache -C —enet-dmac=<ftd_server_interface_mac>,<ftd_client_interface_mac> exemplo: 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. Conectar NICs ao ASA/FTD
7. Reproduza o fluxo com **tcpreplay** tcpreplay -c input_cache -i <nic_server_interface> -I <nic_client_interface> output_file
   exemplo: tcpreplay -c stream.cache -i eth2 -I eth1 stream.pcap.replay

# Validação

Crie capturas de pacotes no FTD para testar se os pacotes que chegam à interface:

1. Criar captura de pacotes na interface interna cap i interface Inside trace match ip any any

2. Criar captura de pacote na interface externa cap o interface Outside trace match ip any any Execute o tcpreplay e valide se os pacotes chegarem à sua interface:

Cenário de exemplo

```
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
```

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.