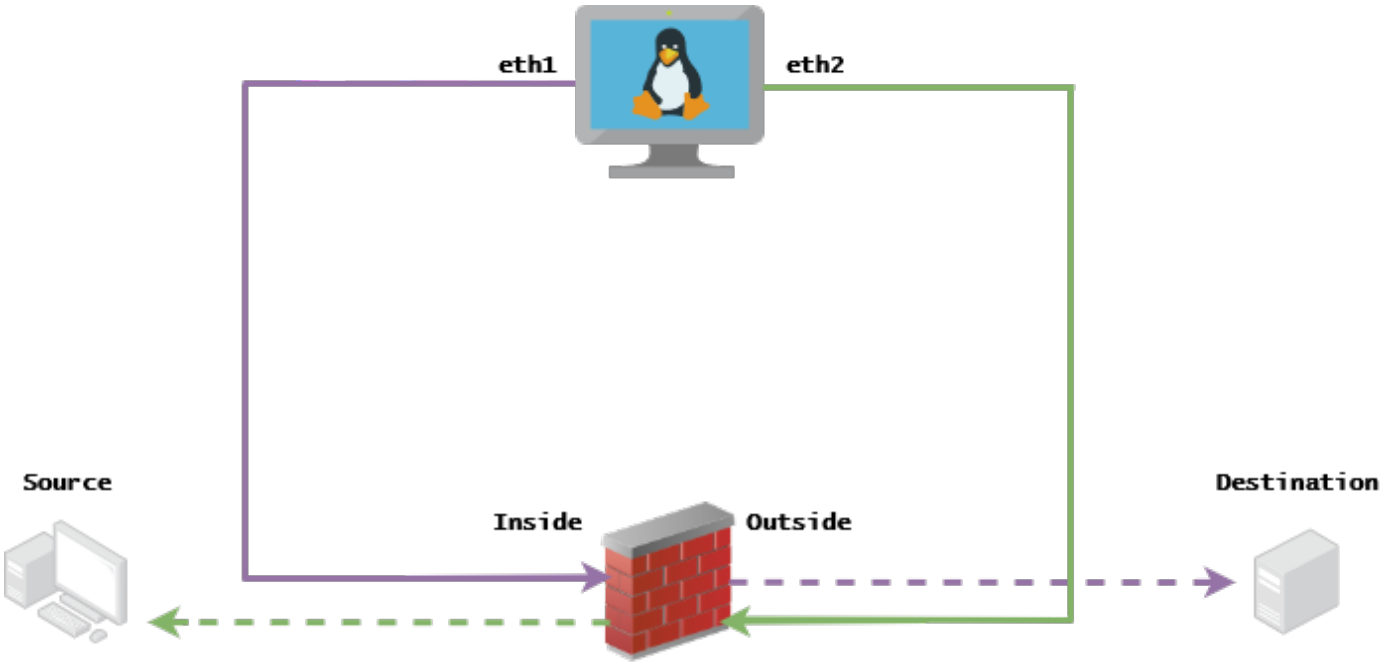
Kali Linuxで2つのNICを使用したTCPリプレイの設定

内容

概要

このドキュメントでは、パケットキャプチャツールで保存されたPCAPファイルからネットワークトラフィックをリプレイするためのTCPリプレイについて説明します。

トポロジ



必要条件

- Kali Linuxと2つのNICを搭載したVM
- FTD（FMCによる管理が望ましい）
- コマンドを実行するためのLinuxの知識。

背景説明

TCPリプレイは、WiresharkやTCPdumpなどのパケットキャプチャツールで保存されたpcapファイルからネットワークトラフィックをリプレイするために使用されるツールです。これは、ネットワークデバイスで結果をテストするためにトラフィックを複製する必要がある状況で役立ちます。

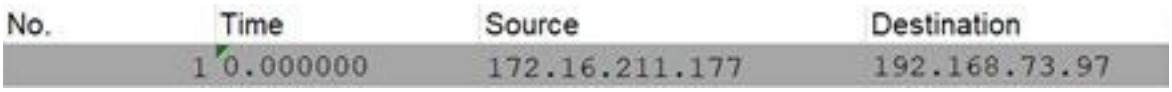
TCPリプレイの基本的な動作は、入力ファイルからのすべてのパケットを、記録された速度または指定されたデータレートで、ハードウェアが可能な限り高速に再送信することです。

この手順を実行する方法は他にもありますが、この記事の目的は、中間ルータを必要とせずにTCPリプレイを実現することです。

実装

FTD設定：

1.パケットキャプチャと同じセグメント上にIPを持つ内部/外部インターフェイスを設定します。



- Source:172.16.211.177
- Destination:192.168.73.97

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

> **ヒント**：トラフィックを隔離しておくために、各インターフェイスを異なるVLANに割り当てることをお勧めします。

Running-config（例）

```
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.ホストからそのゲートウェイへのスタティックルートを設定し、それらのゲートウェイには存在しないゲートウェイであるため、偽のARPエントリを設定します。

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

Running-config（例）

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

LinaConfigToolバックドアを使用して、偽のARPエントリを設定します。

1. FTD CLIにログインします。
2. エキスパートモードに移行する
3. 権限の昇格(sudo su)

LinaConfigToolの設定例

```
/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. equals sequence number randomizationを無効にします。

1. 拡張アクセスリストを作成します。 **Go to FMC > Objects > Access List > Extended > Add Extended Access List**パラメータ「allow any any」を使用してACLを作成します。
2. シーケンス番号のランダム化を無効にする： **Go to FMC > Policies > Access Control > Select your ACP > Advanced > Threat Defense Service Policy**ルールを追加して選択 **Global** 以前作成したオブジェクトを選択します。 **Extended ACL**オフ **Randomize TCP Sequence Number**

running-config

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

Linux 設定:

1. 各インターフェイスのIPを設定します（これは、内部サブネットと外部サブネットのどちらに属するかに基づきます）。 ifconfig ethX <ip_address> netmask <mask> 例：ifconfig eth1 172.16.211.35 netmask 255.255.255.0
2. （オプション）各インターフェイスを異なるVLANに設定します
3. PCAPファイルをKali Linuxサーバに転送します（tcpdumpを使用してpcapファイルを取得したり、FTDでキャプチャしたりできます）。
4. **tcpprep**を使用したTCPリプレイキャッシュファイルの作成 tcpprep -i input_file -o input_cache -c server_ip/32 例：tcpprep -i stream.pcap -o stream.cache -c 192.168.73.97/32
5. **tcprewrite**でMACアドレスを書き換えます。 tcprewrite -i input_file -o output_file -c input_cache -C —enet-dmac=<ftd_server_interface_mac>,<ftd_client_interface_mac>
   例： 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. NICのASA/FTDへの接続
7. tcpreplayでストリームを再**再生** tcpreplay -c input_cache -i <nic_server_interface> -I <nic_client_interface> output_file
   例： tcpreplay -c stream.cache -i eth2 -I eth1 stream.pcap.replay

検証

FTDでパケットキャプチャを作成し、インターフェイスに着信するパケットをテストします。

1. 内部インターフェイスでのパケットキャプチャの作成 cap i interface Inside trace match ip any any
2. Outsideインターフェイスでのパケットキャプチャの作成 cap o interface Outside trace match ip any any

tcpreplayを実行し、パケットがインターフェイスに到着したかどうかを確認します。

シナリオ例

```
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
```

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。