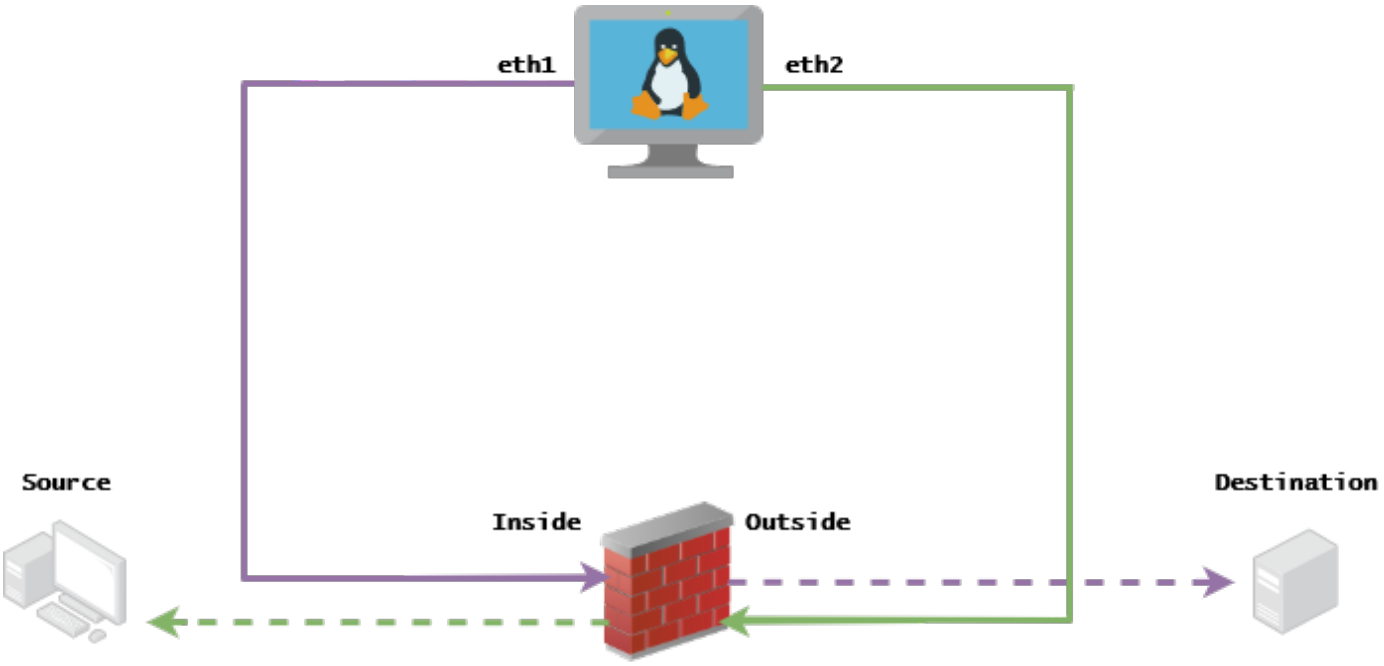
Kali Linux에서 2개의 NIC로 TCP 재생 구성

목차

소개

이 문서에서는 패킷 캡처 툴을 사용하여 저장된 PCAP 파일의 네트워크 트래픽을 재생하는 TCP 재생에 대해 설명합니다.

토폴로지



요구 사항

- Kali Linux 및 2개의 NIC가 있는 VM
- FTD(FMC에서 관리하는 것이 좋음)
- 명령을 실행하는 Linux 지식

배경 정보

TCP 재생wireshark 또는 TCPdump와 같은 패킷 캡처 툴로 저장된 pcap 파일의 네트워크 트래픽을 재생하는 데 사용되는 툴입니다. 네트워크 디바이스에서 결과를 테스트하기 위해 트래픽을 복제해야 하는 경우에 유용할 수 있습니다.

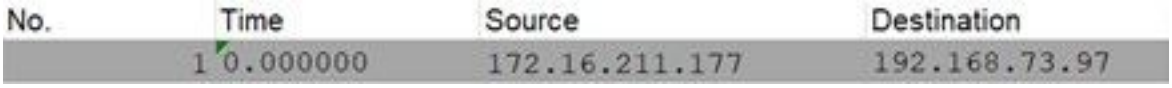
TCP Replay의 기본 작업은 하드웨어가 가능한 한 빨리 기록된 속도 또는 지정된 데이터 속도로 입력 파일에서 모든 패킷을 재전송하는 것입니다.

이 절차를 수행하는 다른 방법도 있지만 이 문서의 목적은 중간 라우터가 필요 없는 TCP 재생을 달성하는 것입니다.

구현

FTD 구성:

1. 패킷 캡처에 있는 세그먼트에서 IP를 사용하여 내부/외부 인터페이스를 구성합니다.



- **출처:** 172.16.211.177
- **대상**: 192.168.73.97

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

팁: 트래픽을 격리하려면 각 인터페이스를 다른 VLAN에 할당하는 것이 좋습니다.

Running-config(예)

```
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. 호스트에서 게이트웨이로의 고정 경로와 존재하지 않는 게이트웨이인 위조된 ARP 항목을 구성합니다.

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

Running-config(예)

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

LinaConfigTool 백도어를 사용하여 위조 ARP 항목을 구성합니다.

1. FTD CLI에 로그인
2. 전문가 모드로 이동
3. 권한 상승(sudo su)

LinaConfigTool 구성 예

```
/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. 등호 시퀀스 번호 임의 설정을 비활성화합니다.

1. 확장 액세스 목록 만들기: **Go to FMC > Objects > Access List > Extended > Add Extended Access List**"allow any any" 매개변수를 사용하여 ACL을 생성합니다.
2. 시퀀스 번호 임의 설정을 비활성화합니다. **Go to FMC > Policies > Access Control > Select your ACP > Advanced > Threat Defense Service Policy**규칙 추가 및 선택 **Global** 이전에 만든 항목을 선택하십시오 . **Extended ACL**선택 취소 **Randomize TCP Sequence Number**

실행 구성

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

Linux 구성:

1. 각 인터페이스에 대한 IP를 구성합니다(내부 서브넷 및 외부 서브넷에 속한 IP를 기준으로 함). ifconfig ethX <ip_address> netmask <mask> 예: ifconfig eth1 172.16.211.35 넷마스크 255.255.255.0
2. (선택 사항) 각 인터페이스를 다른 VLAN으로 구성합니다
3. Kali Linux 서버로 PCAP 파일 전송(tcpdump, FTD의 캡처 등을 사용하여 pcap 파일을 가져올 수 있음)
4. tcpprep를 사용하여 TCP 재생 캐시 파일 **생성** tcpprep -i input_file -o input_cache -c server_ip/32 예: tcpprep -i stream.pcap -o stream.cache -c 192.168.73.97/32
5. MAC 주소를 tcprewrite로 다시 **씁니다** tcprewrite -i input_file -o output_file -c input_cache -C —enet-dmac=<ftd_server_interface_mac>,<ftd_client_interface_mac>
   예: 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. ASA/FTD에 NIC 연결
7. tcpreplay로 스트림 **재생** tcpreplay -c input_cache -i <nic_server_interface> -I <nic_client_interface> output_file
   예: tcpreplay -c stream.cache -i eth2 -I eth1 stream.pcap.replay

검증

FTD에서 패킷 캡처를 생성하여 인터페이스에 도착하는 패킷을 테스트합니다.

1. 내부 인터페이스에서 패킷 캡처 생성 cap i interface 내부 추적 ip any match
2. 외부 인터페이스에서 패킷 캡처 생성 cap o interface 외부 추적 ip any match

tcpreplay를 실행하고 패킷이 인터페이스에 도착하는지 확인합니다.

예제 시나리오

```
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
```

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.