

يـتقـاطـبـ مـادـخـتـسـابـ لـيـغـشـتـ ةـدـاعـاـ نـيـوـكـتـ وـهـجـاـ ةـكـبـشـ ئـلـعـ (NICs)ـ كـلـيـ لـيـنـuxـ

تـايـوـتـ حـمـلاـ

[قـمـدقـمـلاـ](#)

[ايـجـولـوـبـ وـطـ](#)

[تابـلـطـتـمـلاـ](#)

[ةـيـسـاسـأـتـامـوـلـعـمـ](#)

[ذـيـفـنـتـلـلاـ](#)

[نـيـوـكـتـ FTDـ:](#)

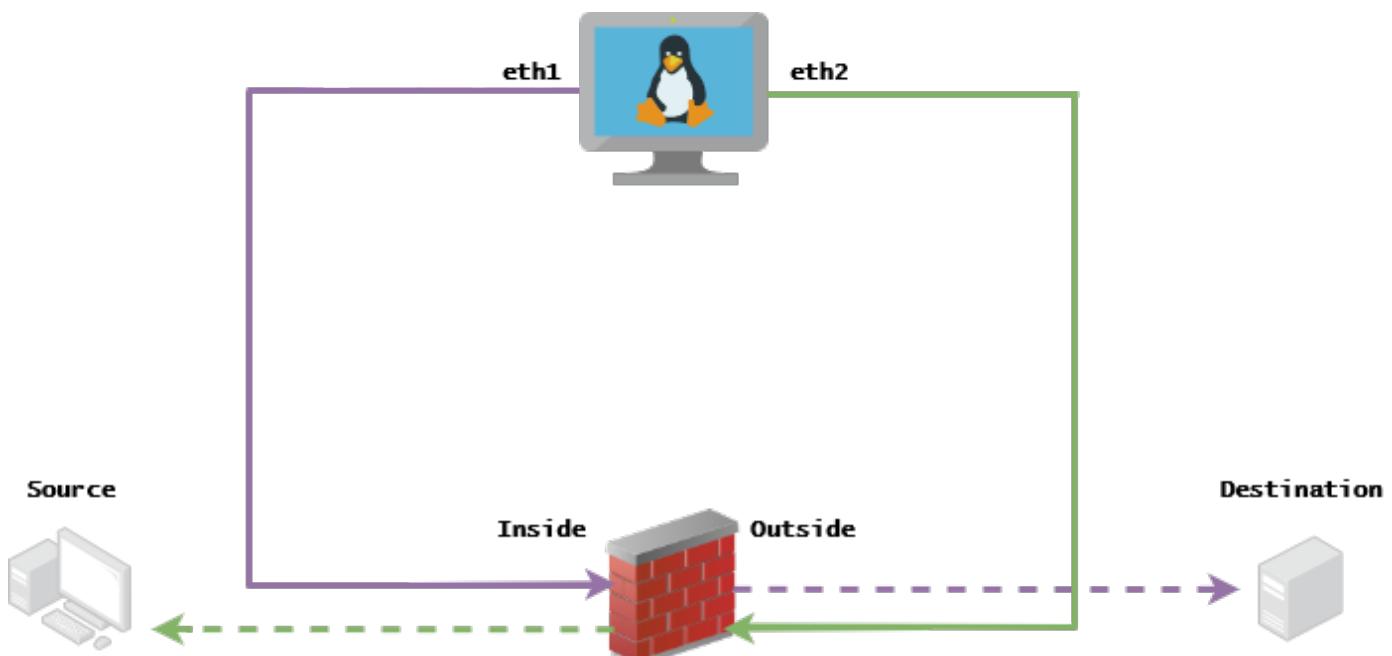
[سـكـونـيـلـ ةـئـيـهـتـ](#)

[قـحـصـلـاـ نـمـ قـقـحـتـلـاـ](#)

قـمـدقـمـلاـ

عـمـ ةـظـوـفـحـمـ PCAPـ تـافـلـمـ نـمـ ةـكـبـشـلـاـ رـوـرـمـ ةـكـرـحـ دـيـعـيـ نـأـ لـيـغـشـتـ ةـدـاعـاـ نـيـوـكـتـ وـهـجـاـ ةـكـبـشـ ئـلـعـ (NICs)ـ كـلـيـ لـيـنـuxـ.

ايـجـولـوـبـ وـطـ



تابـلـطـتـمـلاـ

- VM ةـكـبـشـ ةـهـجـاـوـ يـتقـاطـبـوـ kali Linuxـ عـمـ (NICs)
- FMCـ ةـطـسـاـوبـ هـتـرـادـاـ مـتـتـ نـأـ لـضـفـيـ (FTDـ)ـ ةـعـرـسـلـاـ قـيـافـ لـاسـرـالـاـ جـمـانـرـبـ
- رـمـأـوـأـلـاـ لـيـغـشـتـلـ ةـفـرـعـمـ.

ةياس اس ا تامولع

تافلم نم ةكبشلا رورم ةكرح ليغشت ةداعا إل مدخلتست ةادأ وه TCP لىغشت ةداعا PCAP اديفم نوكبي نأ نكمي TCPdump. wireshark لثم مزحلا طاقتلاتاودأ مادرتساب ةظوفحملاء. ةكبشلا ةزهجأ ىلع ةجيتنلا رابتخال رورملا ةكرح خسن ىلإ اهيـ جاتحت يتـ لـ فـ قـ اوـ مـ لـ لـ.

(تافلم) فـلم نـم مـزـحـلا عـيـمـجـ لـاسـرا ةـداعـا يـفـ TCPـ لـيـغـشـتـ ةـداعـا ةـيـسـاسـأـلـا ةـيـلـمـعـلـاـ لـثـمـتـ زـاهـجـلـا ةـرـدـقـ ىـلـاـ لـصـتـ ةـعـرـسـبـ ،ـدـدـحـمـ تـانـاـيـبـ لـدـعـمـ وـأـ اـهـلـيـجـسـتـ ةـعـرـسـبـ لـاخـدـاـلـ.

ةـداعـاـ قـيـقـحـتـ وـهـ ةـلـاقـمـلـاـ هـذـهـ نـمـ ضـرـغـلـاـ نـإـفـ ،ـكـلـذـعـمـوـ ،ـعـارـجـاـلـاـ اـذـهـ ذـيـفـنـتـلـ ىـرـخـأـ قـرـطـ كـانـهـ طـسوـتـمـ جـوـمـ ىـلـاـ ةـجـاحـلـاـ نـوـدـ TCPـ لـيـغـشـتـ.

ذـيـفـنـتـلـاـ

FTDـ نـيـوـكـتـ:

هـكـلـتـمـتـ يـذـلـاـ عـطـقـمـلـاـ سـفـنـ ىـلـعـ IPـ مـاـدـخـتـسـابـ ةـيـجـرـاـخـلـاـ/ـةـيـلـخـاـدـلـاـ تـاهـجـاـوـلـاـ نـيـوـكـتـبـ مـقـ.

| No. | Time | Source | Destination |
|-----|----------|----------------|---------------|
| 1 | 0.000000 | 172.16.211.177 | 192.168.73.97 |

- : ردصمـلـاـ 172.16.211.177
- : 192.168.73.97: ـةـهـجـوـلـاـ

ةـجـاـوـلـكـ رـيـحـتـ > تـاهـجـاـوـلـاـ > ةـزـهـجـأـلـاـ ةـرـادـاـ > ةـزـهـجـأـلـاـ

عاـقـبـاـلـ ةـفـلـتـخـمـ VLANـ ةـكـبـشـ يـفـ ةـهـجـاـوـلـكـ صـيـصـخـتـ تـاسـرـاـمـمـلـاـ لـضـفـاـ نـمـ :ـجـيـمـلـتـ ـةـلـوـزـعـمـ رـوـرـمـلـاـ ةـكـرـحـ.

running-config (لـاثـمـ)

```
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
```

ةـفـيـزـمـلـاـ ARPـ تـالـاخـداـوـ اـهـتـاـبـاـوـبـ ىـلـاـ ةـفـيـضـمـلـاـ ةـزـهـجـأـلـاـ نـمـ ةـتـبـاـثـلـاـ تـارـاـسـمـلـاـ نـيـوـكـتـبـ مـقـ.

ةـدـوـجـوـمـ رـيـغـ تـابـاـوـبـ نـعـ ةـرـابـعـ اـهـنـأـلـ اـرـظـنـ اـهـيـلـاـ.

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

running-config (لـاثـمـ)

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

ةـفـيـزـمـلـاـ ARPـ تـالـاخـداـ نـيـوـكـتـلـ LinaConfigToolـ ةـادـأـلـ يـفـلـخـلـاـ بـاـبـلـاـ مـدـخـتـسـأـ:

1. ب ةصالخا (CLI) رم اوألا رطس ةهجاولى لوط دلار ليجست
 2. عارب خلأ عضو لى لاقتنالا
 3. كب ةصالخا تازايتمالا عفر (sudo su)
- نويوكـتـ لـاثـمـ 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"
```

يـواـسـتـمـلاـ لـسـلـسـتـلـاـ مـقـرـةـيـاـوـشـعـ لـيـطـعـتـبـ مـقـ

1. ءوعـسـوـمـ لـوصـوـمـيـاـقـ عـاشـنـاـ Go to FMC > Objects > Access List > Extended > Add Extended Access List يـأـبـ حـامـسـلـاـ تـامـلـعـمـبـ (ACL) لـوصـوـلـاـ يـفـ مـكـحـتـلـاـ ةـمـيـاـقـ عـاشـنـاـبـ مـقـ
 2. قـبـاسـلـاـ كـأشـنـمـ دـدـجـ Go to FMC > Policies > Access Control > Select your ACP > Advanced > Threat Defense Service Policy Global دـيـدـحـتـوـ دـدـعـاـقـ ةـفـاضـاـيـاـقـ قـقـحـتـلـاـ عـاغـلـاـ ةـمـقـرـةـيـاـوـشـعـ لـيـطـعـتـ
- رـاجـلـاـ نـيـوـكـتـلـاـ (running-config)

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

سـكـونـيـلـ ةـيـهـتـ

1. ةـيـلـخـادـلـاـ ةـيـعـرـفـلـاـ ةـكـبـشـلـاـ لـلـاـ يـمـتـنـيـ دـحـاـوـيـأـ لـلـاـ اـذـهـ دـنـتـسـيـ)ـ ةـهـجـاـوـيـأـ لـلـاـ نـيـوـكـتـ ifconfig ethX <ip_address> netmask <mask> ifconfig eth1 172.16.211.35 netmask 255.255.255.0
2. ةـفـلـتـخـمـ ةـكـبـشـيـفـ ةـهـجـاـوـلـكـ نـيـوـكـتـبـ مـقـ (ـيـرـايـتـخـاـ)
3. مـاـدـخـتـسـاـبـ PCAP فـلـمـ ىـلـعـ لـوـصـحـلـاـ كـنـكـمـيـ (ـKali Linuxـ) مـدـاـخـ لـلـاـ فـلـمـ لـقـنـ tcpdump، FTD، ىـلـعـ طـاقـتـلـاـ
4. مـاـدـخـتـسـاـبـ TCP لـيـغـشـتـ ةـدـاعـاـلـ تـقـفـمـ نـيـزـخـتـ ةـرـكـاـذـ فـلـمـ عـاشـنـاـ tcpprep -i input_file -o input_cache -c server_ip/32 ifconfig eth1 192.168.73.97/32
5. مـاـدـخـتـسـاـبـ MAC نـيـوـانـعـ ةـبـاتـكـ ةـدـاعـاـ tcprewrite tcprewrite -i input_file -o output_file -c input_cache -c —enet-dmac=<ftd_server_interface_mac>,<ftd_client_interface_mac> ifconfig eth1 192.168.73.97/32 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. بـ ةـكـبـشـلـاـ ةـهـجـاـوـتـاـقـاطـبـ لـيـصـوتـ (ـNICـ) ASA/FTD
7. مـاـدـخـتـسـاـبـ tcpreplay tcpreplay -c input_cache -i <nic_server_interface> -o <nic_client_interface> output_file ifconfig eth1 192.168.73.97/32 tcpreplay -c stream.cache -i eth2 -o stream.pcap.replay

ةـحـصـلـاـ نـمـ قـقـحـتـلـاـ

كـبـ ةـصالـخـاـ ةـهـجـاـوـلـاـ لـلـاـ لـصـتـ يـتـلـاـ مـزـحـلـاـ تـنـاـكـ اـذـاـمـ رـابـتـخـاـلـ FTDـ ىـلـعـ مـزـحـ عـاشـنـاـبـ مـقـ

1. ةـقـبـاطـمـ عـبـتـ يـلـخـادـنـرـاقـ i CAP ةـيـلـخـادـلـاـ ةـهـجـاـوـلـاـ ىـلـعـ ةـمـزـحـ طـاقـتـلـاـ عـاشـنـاـ
 2. عـبـتـتـلـاـ قـبـاطـتـ ةـيـجـرـاخـلـاـ o CAP ةـهـجـاـوـلـاـ ةـيـجـرـاخـلـاـ ىـلـعـ ةـمـزـحـ طـاقـتـلـاـ عـاشـنـاـ
- كـ نـرـاقـ لـخـادـلـصـوـ طـبـرـلـاـ نـاـ تـصـحـفـوـ tcpreplayـ لـاـ تـضـكـرـ

ویرانی س لاثم

```
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
```

هـ لـ وـ لـ جـ رـ تـ لـ اـ هـ ذـ هـ

ةـ يـ لـ آـ لـ اـ تـ اـ يـ نـ قـ تـ لـ اـ نـ مـ مـ جـ مـ وـ عـ مـ اـ دـ خـ تـ سـ اـ بـ دـ نـ تـ سـ مـ لـ اـ اـ ذـ هـ تـ مـ جـ رـ تـ
لـ اـ عـ لـ اـ ءـ اـ حـ نـ اـ عـ يـ مـ جـ يـ فـ نـ يـ مـ دـ خـ تـ سـ مـ لـ لـ مـ عـ دـ ئـ وـ تـ حـ مـ يـ دـ قـ تـ لـ ةـ يـ رـ شـ بـ لـ اـ وـ
اـ مـ كـ ةـ قـ يـ قـ دـ نـ وـ كـ تـ نـ لـ ةـ يـ لـ آـ ةـ مـ جـ رـ تـ لـ ضـ فـ اـ نـ اـ ةـ ظـ حـ اـ لـ مـ ئـ جـ رـ يـ .ـ صـ اـ خـ لـ اـ مـ هـ تـ غـ لـ بـ
يـ لـ خـ تـ .ـ فـ رـ تـ حـ مـ مـ جـ رـ تـ مـ اـ هـ دـ قـ يـ يـ تـ لـ اـ ةـ يـ فـ اـ رـ تـ حـ اـ لـ اـ ةـ مـ جـ رـ تـ لـ اـ عـ مـ لـ اـ حـ لـ اـ وـ
ىـ لـ إـ أـ مـ ئـ اـ دـ عـ وـ جـ رـ لـ اـ بـ يـ صـ وـ تـ وـ تـ اـ مـ جـ رـ تـ لـ اـ هـ ذـ هـ ةـ قـ دـ نـ عـ اـ هـ تـ يـ لـ وـ ئـ سـ مـ
(رـ فـ وـ تـ مـ طـ بـ اـ رـ لـ اـ)ـ يـ لـ صـ أـ لـ اـ يـ زـ يـ لـ جـ نـ إـ لـ اـ دـ نـ تـ سـ مـ لـ اـ).