Table des matières

Collecteur nfdump

Le collecteur de Flux nfdump permet de capturer le flux réseaux (netflow) au format nfcapd et de les conserver pour etre traité par la suite.

Pour ce LAB nous prendrons 3 VM.

1. VM routeur
2. VM Collecteur
3. VM Client (qui simulera du trafic sur le réseau)

VM Routeur

Conf réseau

```
# The primary network interface Patte FW
allow-hotplug enp8s0
iface enp8s0 inet dhcp

#Patte LAN
allow-hotplug enp9s0
iface enp9s0 inet staic
  address 10.200.20.1/28
  gateway 10.200.20.1
  dns-nameservers 1.1.1.1 8.8.8.8
  dns-domain poc.test
```

Activer l'Ip forwarding sur la VM

```
nano /etc/sysctl.conf
décommenter net.ipv4.ip_forward=1
```

Relancer la conf

```
sysctl -p /etc/sysctl.conf
```

Activer NAT

installer iptables: apt install iptables

```
iptables -t nat -A POSTROUTING -o enp8s0 -j MASQUERADE
```

sauvegarde de la règle:

```
iptables-save > /etc/iptables-rules.save
```

Ajouter dans /etc/network/interfaces :

```
post-up iptables-restore < /etc/iptables-rules.save
```

pour être charger à chaque boot en même temps que les paramètre de l'interface.

Installation Sonde

Conf fprobe:

```
apt-get install fprobe
```

Modifier la configuration de la sonde:

```
nano /etc/default/fprobe
```

command line:

```
 /usr/sbin/fprobe -ienp9s0 -fip 10.200.20.2:2055
```

Editer de le fichier de conf

```
nano /etc/default/fprobe
#fprobe default configuration file

INTERFACE="enp9s0"
FLOW_COLLECTOR="10.200.20.2:2055"

#fprobe can't distinguish IP packet from other (e.g. ARP)
OTHER_ARGS=""
```

relancer le service a pres chaque modif de config

```
sudo service fprobe restart
```

VM Client

Network

Éditer la conf réseau:

```
#The primary network interface
allow-hotplug enp1s0
iface enp7s0 inet staic
  address 10.200.20.2/28
  gateway 10.200.20.1
  dns-nameservers 10.200.20.1
  dns-domain poc.test
```

Le poste simulera du traffic par le biais de sa passerelle

VM Collecteur

Network

```
nano /etc/network/interface
The primary network interface
allow-hotplug enp1s0
iface enp7s0 inet staic
  address 10.200.20.2/28
  gateway 10.200.20.1
  dns-nameservers 10.200.20.1
  dns-domain poc.test
```

NFDUMP

Installer NFdump:

```
apt install nfdump
```

controle version nfdump -V : NSEL-NEL1.6.22

---

commande line:
afficher le cache complet:

```
nfdump -R /var/cache/nfdump/ -o long
```

```
Date first seen          Duration Proto      Src IP Addr:Port          Dst
IP Addr:Port     Flags Tos  Packets    Bytes Flows
2022-06-21 18:16:29.227     0.000 UDP      162.159.200.1:123   ->
10.200.20.2:123   ........   0        1       76     1
2022-06-21 18:16:29.214     0.000 UDP        10.200.20.2:123   ->
```

```
162.159.200.1:123   ........ 184        1       76     1
2022-06-21 18:16:39.213     0.000 UDP        10.200.20.2:123   ->
82.64.84.116:123   ........ 184        1       76     1
2022-06-21 18:16:39.227     0.000 UDP       82.64.84.116:123   ->
10.200.20.2:123   ........ 184        1       76     1
2022-06-21 18:17:15.288     0.001 UDP      192.168.122.1:53    ->
10.200.20.3:40888 ........   0        2      228     1
2022-06-21 18:17:15.358     0.000 UDP        10.200.20.3:60900 ->
192.168.122.1:53    ........   0        2      118     1
2022-06-21 18:17:16.283     0.000 UDP      192.168.122.1:53    ->
10.200.20.3:40650 ........   0        2      232     1
2022-06-21 18:17:15.539     0.000 UDP      192.168.122.1:53    ->
10.200.20.3:40918 ........   0        2      232     1
2022-06-21 18:17:15.552     0.000 UDP        10.200.20.3:38797 ->
192.168.122.1:53    ........   0        2      126     1
2022-06-21 18:17:16.195     0.000 UDP        10.200.20.3:53495 ->
192.168.122.1:53    ........   0        2      122     1
2022-06-21 18:17:15.323     0.879 TCP     216.58.198.196:443   ->
10.200.20.3:34330 ...AP.S.   0       70   217508     1
2022-06-21 18:17:15.370     0.000 UDP      192.168.122.1:53    ->
10.200.20.3:46356 ........   0        1      110     1
2022-06-21 18:17:15.303     0.008 UDP      192.168.122.1:53    ->
10.200.20.3:45494 ........   0        2      164     1
2022-06-21 18:17:15.563     0.000 UDP      192.168.122.1:53    ->
10.200.20.3:38797 ........   0        2      242     1
2022-06-21 18:17:16.252     0.283 TCP     216.58.214.163:443   ->
10.200.20.3:55008 ...AP..F   0        6     3495     1
2022-06-21 18:17:16.252     0.273 TCP        10.200.20.3:55008 ->
216.58.214.163:443   ...AP..F   0        9      570     1
2022-06-21 18:17:15.264     0.000 UDP        10.200.20.3:40888 ->
192.168.122.1:53    ........   0        2       98     1
Summary: total flows: 24094, total bytes: 27.3 G, total packets: 8.0 M, avg
bps: 281590, avg pps: 10, avg bpp: 3426
Time window: 2022-06-20 12:10:00 - 2022-06-30 17:29:15
Total flows processed: 24094, Blocks skipped: 0, Bytes read: 1415744
Sys: 0.158s flows/second: 152211.4   Wall: 0.511s flows/second: 47145.4
```

analyse toutes les sources nfdump
Visualiser le cache:

```
ls -lh /var/cache/nfdump
```

Sepcifier une date de recherche:

```
nfdump -R /var/cache/nfdump -t 2022/6/21-2022/6/21.23:59:59
```

Pour rechercher en fonction d'une ip (sommes agrgées)

```
nfdump -R /var/cache/nfdump -t 2022/6/21-2022/6/21.23:59:59 -s 10.200.20.3 -
O bytes
```