Configureren van NAT in UFW

Als je gebruik wilt maken van NAT om data van de externe naar de interne netwerk interface te routeren, dan dienen er een aantal configuratiebestanden gewijzigd te worden. Dit zijn etc/default/ufw , /etc/ufw/before.rules en /etc/ufw/sysctl.conf. Open eerst /etc/default/ufw met de editor (bijvoorbeeld nano):

```
nano /etc/default/ufw
```

En wijzig de volgende regel:

```
DEFAULT_FORWARD_POLICY="ACCEPT"
```

Vervolgens dienen we ipv4 forwarding toe te staan. Dit doen we door het bestand /etc/ufw/sysctl.conf te openen in de editor:

```
nano /etc/ufw/sysctl.conf
```

En wijzig de volgende regel:

```
net/ipv4/ip_forward=1
```

Vervolgens openen we /etc/ufw/before.rules in de editor:

```
nano /etc/ufw/before.rules
```

En voeg het volgende toe **voor** de filter regels:

```
# NAT table rules
*nat
:POSTROUTING ACCEPT [0:0]
:PREROUTING ACCEPT [0:0]
-F
# Forward traffic through eth0 - Change to match your out-interface
-A POSTROUTING -s 192.168.1.0/24 -o eth0 -j MASQUERADE
# don't delete the 'COMMIT' line or these nat table rules won't
```

```
# be processed
COMMIT
```

De optie “-F” (Flush) heb ik er ingezet zodat de NAT tabel eerst wordt gewist. Wanneer men UFW uitschakelt en weer inschakelt, komen er dubbele regels in te staan. Hiermee wordt dit voorkomen. Sla het bestand op en herstart UFW met:

```
ufw disable
ufw enable
```

Configureren van Port Forwarding in UFW

Als je bijvoorbeeld verkeer van poort 80 en 443 wilt forwarden naar een server met IP adres 192.168.1.120, dan dien je eerst het bestand /etc/ufw/before.rules te openen in de editor:

```
nano /etc/default/before.rules
```

En wijzig je het bestand als volgt:

```
:PREROUTING ACCEPT [0:0]
-A PREROUTING -i eth0 -p tcp --dport 80 -j DNAT --to-destination 192.168.1.120:80
-A PREROUTING -i eth0 -p tcp --dport 443 -j DNAT --to-destination 192.168.1.120:443
```

Vervolgens herstart je UFW weer met:

```
ufw disable
ufw enable
```

Vervolgens dien je nog wel kenbaar te maken dat tcp verkeer voor poort 80 en 443 toegestaan wordt:

```
ufw allow 80/tcp
ufw allow 443/tcp
```

Bovenstaande regels geven toegang voor **alle** IP adressen van buiten af voor poort 80 en 443. Om dit te beperken tot een specifiek publiek IP adres zou je het volgende kunnen opgeven:

```
ufw allow from <PUBLIEK IP-ADRES> to any port 80 proto tcp
ufw allow from <PUBLIEK IP-ADRES> to any port 443 proto tcp
```

Hier onder volgt nog een voorbeeld van port forwarding waarbij de WAN interface luistert op poort 1999 en vervolgens doorsluist naar poort 80 van de PC met IP-adres 192.168.10.211:

```
-A PREROUTING -i eth0 -p tcp --dport 1999 -j DNAT --to-destination 192.168.10.211:80
```

Bron:

Linuxconfig.org

Revision #2
Created 2023-09-12 13:21:33 UTC by Alex
Updated 2023-09-12 15:47:25 UTC by Alex