Extra NAT con NFTables

A.D.G.

Habiéndonos puesto hoy a resolver problemas de criptografía y buscando decodificadores, se me ocurrió buscar a ver si existe un TRADUCTOR de IPTables que ya hice y envié, a NFTables que no me dió tiempo. Aquí subo el resultado de la forma que encontré y las verificaciones.

Se ha usado las mismas máquinas anteriores de un Ubuntu Server con forwarding activado, y 2 Lubuntu Desktop.
Copiamos las reglas de las IPtables:

```
root@andreidani-servidor:~# iptables-save > iptables_rules.txt
```

Comprobamos que se hayan escrito:

```
root@andreidani-servidor:~# cat iptables_rules.txt
# Generated by iptables-save v1.8.7 on Mon Oct 17 17:58:09 2022
*filter
:INPUT DROP [0:0]
:FORWARD DROP [0:0]
:OUTPUT DROP [12:940]
-A INPUT -i enp0s3 -p icmp -m icmp --icmp-type 0 -j ACCEPT
-A FORWARD -s 192.168.10.0/24 -j ACCEPT
-A FORWARD -s 192.168.20.0/24 -j ACCEPT
-A FORWARD -m state --state ESTABLISHED -j ACCEPT
-A OUTPUT -o enp0s3 -p icmp -m icmp --icmp-type 8 -j ACCEPT
COMMIT
# Completed on Mon Oct 17 17:58:09 2022
# Generated by iptables-save v1.8.7 on Mon Oct 17 17:58:09 2022
*nat
:PREROUTING ACCEPT [0:0]
:INPUT ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
:POSTROUTING ACCEPT [0:0]
-A POSTROUTING -s 192.168.10.0/24 -o enp0s3 -j MASQUERADE
-A POSTROUTING -s 192.168.20.0/24 -o enp0s3 -j MASQUERADE
COMMIT
# Completed on Mon Oct 17 17:58:09 2022
```

Usamos este comando de traducción de IPTables a NFTables, y a la vez lo guardamos en un archivo .nft

```
root@andreidani-servidor:~# iptables-restore-translate -f iptables_rules.txt > nft_ruleset.nft_
```

Podemos verificar que de momento no hay ninguna regla de momento:

```
root@andreidani-servidor:~# nft list ruleset
table ip filter {
	chain INPUT {
		type filter hook input priority filter; policy drop;
	}

	chain OUTPUT {
		type filter hook output priority filter; policy drop;
	}

	chain FORWARD {
		type filter hook forward priority filter; policy drop;
	}
}
table ip nat {
	chain POSTROUTING {
		type nat hook postrouting priority srcnat; policy accept;
	}

	chain PREROUTING {
		type nat hook prerouting priority dstnat; policy accept;
	}

	chain INPUT {
		type nat hook input priority 100; policy accept;
	}

	chain OUTPUT {
		type nat hook output priority -100; policy accept;
	}
}
root@andreidani-servidor:~# _
```

Cargamos las reglas de nft:

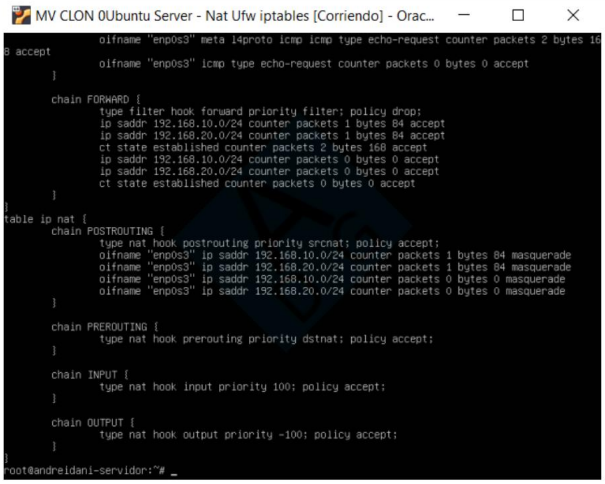
```
root@andreidani-servidor:~# nft -f nft_ruleset.nft
```

Las reglas ahora sí aparecerían y serían estas, las abro con editor nano ya que con el comando posterior se muestra poco en la captura:

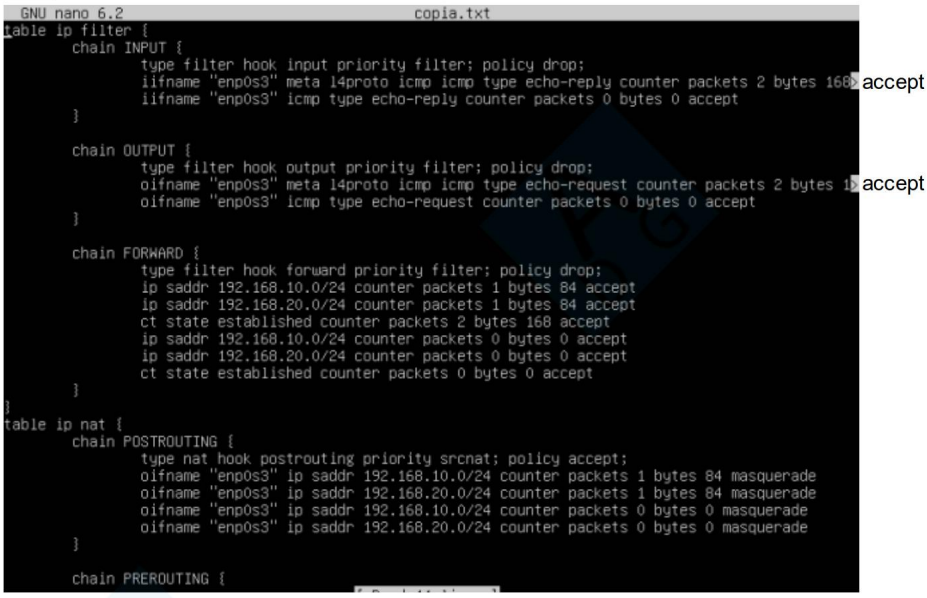
```
  GNU nano 6.2                                   nft_ruleset.nft
# Translated by iptables-restore-translate v1.8.7 on Mon Oct 17 18:02:34 2022
add table ip filter
add chain ip filter INPUT { type filter hook input priority 0; policy drop; }
add chain ip filter FORWARD { type filter hook forward priority 0; policy drop; }
add chain ip filter OUTPUT { type filter hook output priority 0; policy drop; }
add rule ip filter INPUT iifname "enp0s3" icmp type echo-reply counter accept
add rule ip filter FORWARD ip saddr 192.168.10.0/24 counter accept
add rule ip filter FORWARD ip saddr 192.168.20.0/24 counter accept
add rule ip filter FORWARD ct state established  counter accept
add rule ip filter OUTPUT oifname "enp0s3" icmp type echo-request counter accept
add table ip nat
add chain ip nat PREROUTING { type nat hook prerouting priority -100; policy accept; }
add chain ip nat INPUT { type nat hook input priority 100; policy accept; }
add chain ip nat OUTPUT { type nat hook output priority -100; policy accept; }
add chain ip nat POSTROUTING { type nat hook postrouting priority 100; policy accept; }
add rule ip nat POSTROUTING oifname "enp0s3" ip saddr 192.168.10.0/24 counter masquerade
add rule ip nat POSTROUTING oifname "enp0s3" ip saddr 192.168.20.0/24 counter masquerade
# Completed on Mon Oct 17 18:02:34 2022
```

Verificamos las reglas importadas:

```
root@andreidani-servidor:~# nft list ruleset_
```



En esta siguiente vista Nano hay la parte de arriba que no se veía en la izquierda:



Pings desde un cliente a internet y al otro cliente respectivo.