Cremos la carpeta para meter las reglas, ejecutando como root:

```
mkdir -p /root/NFTables/
```

Ahora creamos las reglas para la tabla NAT, ejecutando como root:

```
nano /root/NFTables/TablaNAT
```

…y agregamos el siguiente texto:

```
table inet nat {

  chain prerouting {

    type nat hook prerouting priority 0; policy accept;

    # Por forwarding del puerto 80
    iifname "eth0" tcp dport 80 counter dnat ip to 192.168.1.10:80

  }

  chain postrouting {

    type nat hook postrouting priority 100; policy accept;

    # Cambiar la IP de salida a toda la subred 192.168.1.0/24
    oifname "eth0" ip saddr 192.168.1.0/24 counter masquerade

  }

}
```

A continuación, creamos las reglas para la tabla filter, ejecutando como root:

```
nano /root/NFTables/TablaFilter
```

… y agregamos el siguiente texto:

```
table inet filter {

  # eth2 es la pata DMZ
  chain ingresseth2 {
    type filter hook ingress device eth2 priority -1; policy accept;

    # Bloquear el acceso a la subred de la LAN.
    ip daddr 192.168.1.0/24 counter drop

  }

  chain input {
    type filter hook input priority 0; policy drop;
    ct state related,established counter accept;
  }

  chain forward {
    type filter hook forward priority 0; policy accept;
  }

  chain output {
    type filter hook output priority 0; policy accept;
  }

}
```

Ahora, modificamos el archivo **/etc/nftables.conf** dejándolo sólo con este texto:

```
#!/usr/sbin/ nft -f

flush ruleset

include "/root/NFTables/TablaNAT"
include "/root/NFTables/TablaFilter"
```

Finalmente, cada vez que queramos que las reglas se carguen, ejecutamos como root:

`nft --file /etc/nftables.conf`

Entonces, cada vez que esa línea se ejecute como root, se borrará toda la configuración existente de NFTables y se cargarán únicamente las reglas de ambos archivos.

Una buena práctica es ejecutar esa carga de reglas antes de que se levante la interfaz loopback. Esto lo hacemos editando /etc/network/interfaces, de la siguiente manera:

```
auto lo
iface lo inet loopback
  pre-up nft --file /etc/nftables.conf
```