Vyos reglas firewall básicas

Suponemos nuestra red en el rango 192.168.1.0/24 (para la regla de nat).

Las reglas de firewall aceptan ping, y los relacionados con IPSEC y Wireguard en la parte WAN.
Suponemos que nuestra interfaz WAN es la eth0 y la LAN la eth1

```
###
## Establecemos la base
###
set interfaces ethernet eth0 description 'WAN'
set interfaces ethernet eth0 firewall in name 'WAN-FW'
set interfaces ethernet eth0 firewall local name 'WAN-LOCAL'
###
# Reglas basicas de firewall
###
set firewall all-ping 'enable'
set firewall broadcast-ping 'disable'
set firewall config-trap 'disable'
set firewall ipv6-receive-redirects 'disable'
set firewall ipv6-src-route 'disable'
set firewall ip-src-route 'disable'
set firewall log-martians 'enable'
set firewall receive-redirects 'disable'
set firewall send-redirects 'enable'
set firewall source-validation 'disable'
set firewall syn-cookies 'enable'
set firewall twa-hazards-protection 'disable'
## Politicas desde WAN (Red publica) al Firewall
set firewall name WAN-FW default-action 'drop'
set firewall name WAN-FW rule 10 action 'accept'
set firewall name WAN-FW rule 10 state established 'enable'
set firewall name WAN-FW rule 10 state related 'enable'
## Politicas desde WAN (Red publica) a los dispositivos internos
set firewall name WAN-LOCAL default-action 'drop'
set firewall name WAN-LOCAL 'enable-default-log'
set firewall name WAN-LOCAL rule 10 action 'accept'
set firewall name WAN-LOCAL rule 10 state established 'enable'
```

```
set firewall name WAN-LOCAL rule 10 state related 'enable'
set firewall name WAN-LOCAL rule 20 action 'accept'
set firewall name WAN-LOCAL rule 20 icmp type-name 'echo-request'
set firewall name WAN-LOCAL rule 20 protocol 'icmp'
set firewall name WAN-LOCAL rule 20 state new 'enable'
set firewall name WAN-LOCAL rule 30 action 'drop'
set firewall name WAN-LOCAL rule 30 destination port '22'
set firewall name WAN-LOCAL rule 30 protocol 'tcp'
set firewall name WAN-LOCAL rule 30 recent count '4'
set firewall name WAN-LOCAL rule 30 recent time '60'
set firewall name WAN-LOCAL rule 30 state new 'enable'
set firewall name WAN-LOCAL rule 31 action 'accept'
set firewall name WAN-LOCAL rule 31 destination port '22'
set firewall name WAN-LOCAL rule 31 protocol 'tcp'
set firewall name WAN-LOCAL rule 31 state new 'enable'
## Acepta Ipsec
set firewall name WAN-LOCAL rule 40 action 'accept'
set firewall name WAN-LOCAL rule 40 ipsec 'match-ipsec'
## Acepta Wireguard en el puerto 51820
set firewall name WAN-LOCAL rule 50 action 'accept'
set firewall name WAN-LOCAL rule 50 description WireGuard_IN
set firewall name WAN-LOCAL rule 50 destination port 51820
set firewall name WAN-LOCAL rule 50 log enable
set firewall name WAN-LOCAL rule 50 protocol 'udp'
set firewall name WAN-LOCAL rule 50 source
###
#  NAT
###
set nat source rule 100 outbound-interface 'eth0'
set nat source rule 100 source address '192.168.1.0/24'
set nat source rule 100 translation address 'masquerade'
```

Revision #8
Created 14 August 2022 07:39:32 by Admin
Updated 14 August 2022 07:55:30 by Admin