Configuration de base VyOS

VyOS est un OS de routeur virtuel à placer dans une VM ou sur une petite 1u

Le lien de téléchargement de Vyos :

https://downloads.vyos.io/?dir=rolling/current/amd64

Configuration minimale

```
conf
set interfaces ethernet eth0 description WAN
set interfaces ethernet eth0 address dhcp
set interfaces ethernet eth1 description LAN
set interfaces ethernet eth1 address 192.168.2.1/24

set service dhcp-server shared-network-name dhcpproc authoritative
set service dhcp-server shared-network-name subnet 192.168.2.0/24 default-router 192.168.2.1
set service dhcp-server shared-network-name subnet 192.168.2.0/24 dns-server 192.168.2.1
set service dhcp-server shared-network-name subnet 192.168.2.0/24 range 0 start 192.168.2.10
set service dhcp-server shared-network-name subnet 192.168.2.0/24 range 0 stop 192.168.2.200

set nat source rule 99 description LAN2WAN
set nat source rule 99 outbound-interface eth0
set nat source rule 99 source address 192.168.2.0/24
set nat source rule 99 translation address masquerade

commit
save
```

Configuration simple

```
sudo dpkg-reconfigure keyboard-configuration # Tant qu'a faire, autant mettre le clavier en français...
conf

set interfaces ethernet eth0 address '192.168.1.253/24'
set interfaces ethernet eth0 description 'WAN'
set interfaces ethernet eth1 address '192.168.2.1/24'
set interfaces ethernet eth1 description 'LAN'

set nat source rule 100 outbound-interface 'eth0'
set nat source rule 100 source address '192.168.2.0/24'
set nat source rule 100 translation address 'masquerade'

set service dhcp-server disabled 'false'
set service dhcp-server shared-network-name LAN authoritative 'disable'
set service dhcp-server shared-network-name LAN subnet 192.168.2.0/24 default-router '192.168.2.1'
set service dhcp-server shared-network-name LAN subnet 192.168.2.0/24 dns-server '192.168.2.1'
set service dhcp-server shared-network-name LAN subnet 192.168.2.0/24 domain-name 'lan-interne'
set service dhcp-server shared-network-name LAN subnet 192.168.2.0/24 lease '86400'
set service dhcp-server shared-network-name LAN subnet 192.168.2.0/24 start 192.168.2.128 stop
'192.168.2.255'
set service dns forwarding cache-size '0'
set service dns forwarding listen-on 'eth1'
set service dns forwarding name-server '9.9.9.9'
set service dns forwarding name-server '1.1.1.1'
set service snmp community public authorization 'ro'
set service snmp community public network '192.168.2.0/24'
set service snmp community public network '192.168.1.0/24'
set service snmp contact 'Somebody <someone@somewhe.re>'
set service snmp listen-address 0.0.0.0 port '161'
set service snmp location 'Some hypervisor'
set service ssh port '22'

set system gateway-address '192.168.1.1'
set system host-name 'routeur-NAT'
set system login user vyos authentication plaintext-password 'un mot de passe, pour changer...'
set system login user vyos level 'admin'
set system ntp server '0.pool.ntp.org'
set system ntp server '1.pool.ntp.org'
set system ntp server '2.pool.ntp.org'
set system time-zone 'Europe/Paris'
```

```
set firewall all-ping 'enable'

set firewall broadcast-ping 'disable'

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'


# On crée une règle pour autoriser les connexions http https et ssh a arriver depuis le WAN

set firewall name OUTSIDE-IN default-action 'drop'

set firewall name OUTSIDE-IN rule 10 action 'accept'

set firewall name OUTSIDE-IN rule 10 state established 'enable'

set firewall name OUTSIDE-IN rule 10 state related 'enable'

set firewall name OUTSIDE-IN rule 20 action 'accept'

set firewall name OUTSIDE-IN rule 20 destination port '80'

set firewall name OUTSIDE-IN rule 20 protocol 'tcp'

set firewall name OUTSIDE-IN rule 20 state new 'enable'

set firewall name OUTSIDE-IN rule 21 action 'accept'

set firewall name OUTSIDE-IN rule 21 destination port '443'

set firewall name OUTSIDE-IN rule 21 protocol 'tcp'

set firewall name OUTSIDE-IN rule 21 state new 'enable'

set firewall name OUTSIDE-IN rule 22 action 'accept'

set firewall name OUTSIDE-IN rule 22 destination port '22'

set firewall name OUTSIDE-IN rule 22 protocol 'tcp'

set firewall name OUTSIDE-IN rule 22 state new 'enable'


# On crée une règle pour autoriser les connexions déjà établies ainsi que ping ntp et ssh a se connecter au routeur

set firewall name OUTSIDE-LOCAL default-action 'drop'

set firewall name OUTSIDE-LOCAL rule 10 action 'accept'

set firewall name OUTSIDE-LOCAL rule 10 state established 'enable'

set firewall name OUTSIDE-LOCAL rule 10 state related 'enable'

set firewall name OUTSIDE-LOCAL rule 20 action 'accept'

set firewall name OUTSIDE-LOCAL rule 20 icmp type-name 'echo-request'

set firewall name OUTSIDE-LOCAL rule 20 protocol 'icmp'

set firewall name OUTSIDE-LOCAL rule 20 state new 'enable'

set firewall name OUTSIDE-LOCAL rule 30 action 'drop'

set firewall name OUTSIDE-LOCAL rule 30 destination port '22'

set firewall name OUTSIDE-LOCAL rule 30 protocol 'tcp'
```

```
set firewall name OUTSIDE-LOCAL rule 30 recent count '4'
set firewall name OUTSIDE-LOCAL rule 30 recent time '60'
set firewall name OUTSIDE-LOCAL rule 30 state new 'enable'
set firewall name OUTSIDE-LOCAL rule 31 action 'accept'
set firewall name OUTSIDE-LOCAL rule 31 destination port '22'
set firewall name OUTSIDE-LOCAL rule 31 protocol 'tcp'
set firewall name OUTSIDE-LOCAL rule 31 state new 'enable'
set firewall name OUTSIDE-LOCAL rule 40 action 'accept'
set firewall name OUTSIDE-LOCAL rule 40 destination port '161'
set firewall name OUTSIDE-LOCAL rule 40 protocol 'udp'
set firewall name OUTSIDE-LOCAL rule 40 state new 'enable'


set interfaces ethernet eth0 firewall in name 'OUTSIDE-IN'
set interfaces ethernet eth0 firewall local name 'OUTSIDE-LOCAL'


commit
save
```

Script de sauvegarde de configuration

```
#!/bin/vbash
source /opt/vyatta/etc/functions/script-template


run show configuration commands > $HOME/$(date +%Y%m%d)-$(hostname)-vyos.conf.txt
```