

Vyos

Router Vyos

- [Instalación](#)
- [Comandos Vyos](#)
- [Configuración inicial Vyos Movistar FTTH](#)
- [Configuración Base Vyos](#)
- [Vyos reglas firewall básicas](#)

Instalación

La instalación de un router con Vyos, es bastante sencilla, tan solo hay que arrancar la imagen ISO que se descarga desde la web de [Vyos](#). Una vez descargada, arrancamos desde la ISO y el sistema presentará la pantalla de login, usando como user vyos con password vyos nos aparecerá el prompt

```
The programs included with the Debian GNU/Linux system are free software; the exact
distribution terms for each program are described in the individual files in
/usr/share/doc/*/copyright.
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
vyos@vyos: ~$
```

desde aquí procederemos a instalarlo en el disco de nuestra máquina con el comando *install image*

```
vyos@vyos: ~$ install image
Welcome to the VyOS install program. This script will walk you through the process of
installing the VyOS image to a local hard drive.
Would you like to continue? (Yes/No) [Yes]: Yes Probing drives: OK
Looking for pre-existing RAID groups...none found.
The VyOS image will require a minimum 2000MB root.
Would you like me to try to partition a drive automatically
or would you rather partition it manually with parted? If
you have already setup your partitions, you may skip this step
Partition (Auto/Parted/Skip) [Auto]:
I found the following drives on your system:
sda    94294MB
Install the image on? [sda]:
This will destroy all data on /dev/sda.
Continue? (Yes/No) [No]: Yes
How big of a root partition should I create? (2000MB - 4294MB) [4294] MB:
Creating filesystem on /dev/sda1: OK
Done!
Copying /opt/vyatta/etc/config.boot.default to sda. Enter password for administrator account
Enter password for user 'vyos':
Retype password for user 'vyos':
I need to install the GRUB boot loader.
```

I found the following drives on your system:

sda 94294MB

Which drive should GRUB modify the boot partition on? [sda]:

Setting up grub: OK

Done!

vynos@vynos: ~\$

Una vez instalado procederemos a reiniciar con *reboot*

Comandos Vyos

En el más alto nivel tenemos los comandos set y show, si tecleamos tabulador, nos aparecerá una lista de opciones de cada comando

```
vyos@vyos: ~$ s[ tab]
set    show
```

```
vyos@vyos: ~$ show [ tab]
Possible completions:
arp          Show Address Resolution Protocol (ARP) information
bridge      Show bridging information
cluster     Show clustering information
configuration Show running configuration
conntrack   Show conntrack entries in the conntrack table
conntrack-sync
              Show connection syncing information
date        Show system date and time
dhcp        Show Dynamic Host Configuration Protocol (DHCP) information
dhcpv6      Show status related to DHCPv6
disk        Show status of disk device
dns         Show Domain Name Server (DNS) information
file        Show files for a particular image
firewall    Show firewall information
flow-accounting
              Show flow accounting statistics
hardware    Show system hardware details
history     show command history
host        Show host information
incoming    Show ethernet input-policy information
: q
```

Entrar en modo configuración

```
vyos@vyos: ~$ configure
[edit]
```

Configuración inicial Vynos

Movistar FTTH

Comandos de configuración básicos de un router Vynos

Habilitamos que suene el altavoz interno al arrancar, el nombre del router, el acceso por SSH, el NTP y la zona horaria

```
set system option startup-beep
set system host-name router-1.ateinco.net
set service ssh port 22
set system ntp server 150.214.94.5
set system time-zone Europe/Madrid
set system console device ttyS0 speed '115200'
```

Interfaces

Suponemos que nuestra interfaz LAN va a ser la eth1 y la WAN la eth0

```
set interfaces ethernet eth1 vif 6 description "Movistar_Data"
set interfaces ethernet eth1 vif 3 description "Movistar_VoIP"
set interfaces ethernet eth1 vif 2 description "Movistar_IPTV"
set interfaces ethernet eth1 description 'WAN'
set interfaces ethernet eth0 address 10.200.200.1/24
set interfaces ethernet eth0 description 'LAN'
set service dhcp-server shared-network-name LAN subnet 10.200.200.0/24 default-router 10.200.200.1
set service dhcp-server shared-network-name LAN subnet 10.200.200.0/24 name server 1.1.1.1
set service dhcp-server shared-network-name LAN subnet 10.200.200.0/24 range 0 start 10.200.200.64
set service dhcp-server shared-network-name LAN subnet 10.200.200.0/24 range 0 stop 10.200.200.128
set service dhcp-server shared-network-name LAN subnet 10.200.200.0/24 lease 86400
```

Habilitar WAN Movistar

```
set nat source rule 100 outbound-interface eth1.6
set nat source rule 100 source address "10.200.200.0/24"
set nat source rule 100 translation address masquerade
set interfaces pppoe pppoe0 description "Movistar_ppoe"
set interfaces pppoe pppoe0 source-interface eth1.6
set interfaces pppoe pppoe0 authentication user "adslppp@telefonicanetpa"
set interfaces pppoe pppoe0 authentication password "adslppp"
set interfaces ethernet eth1 vif 6 address dhcp
set protocols static route 0.0.0.0/0 interface pppoe0
```

Habilitar Movistar VoIP

```
set interfaces ethernet eth1 vif 3 address dhcp
```

Esto nos dará una IP dinámica para la VoIP

Habilitar IPTV

En este caso la habilitaremos, pero en la TV, se nos asigna un IP estos datos aparecen en la config original del router

```
set interfaces ethernet eth1 vif 2 address 10.X.X.X/8
```

Configuración Base Vyos

Habilitamos que suene el altavoz interno al arrancar, el nombre del router, el acceso por SSH, el NTP, la zona horaria, la velocidad de la consola (si existe), el nivel de syslog y las fuentes de actualización

```
set system option startup-beep
set system host-name router-1.ateinco.net
set service ssh port 22
set system ntp server 150.214.94.5
set system time-zone Europe/Madrid
set system console device ttyS0 speed '115200'
set system syslog global facility all level 'notice'
set system syslog global facility protocols level 'debug'
```

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'
```