PROYECTO FINAL

SERVICIOS DE SEGURIDAD BASADOS EN SDN

UNIVERSIDAD DISTRITAL
FRANCISCO JOSÉ DE CALDAS

NICOLÁS DAVID SABOGAL – 20202020008

LUIS SEBASTIAN MARTINEZ GUERRERO – 20191005153

LUIS MIGUEL POLO – 20182020158

UNIVERSIDAD DISTRITAL FRANCISCO JOSÉ DE CALDAS

INGENIERÍA DE SISTEMAS

REDES DE COMUNICACIONES III

PAULO ALONSO GAONA GARCIA

2024-III

INTRODUCCIÓN

En la era digital actual, la seguridad en las redes de computadoras se ha convertido en un aspecto crítico para garantizar la integridad, confidencialidad y disponibilidad de los datos. Con el aumento de las amenazas cibernéticas y la complejidad de las redes, es esencial implementar mecanismos de seguridad robustos que permitan proteger los recursos y servicios de red. En este contexto, el uso de tecnologías basadas en Software Defined Networking (SDN) y firmwares especializados como VyOS ofrece una solución flexible y eficiente para gestionar y asegurar las redes.

Este proyecto tiene como objetivo principal la configuración de un firmware de enrutamiento basado en Linux, específicamente VyOS, para desplegar mecanismos de seguridad y control de acceso a servicios de red como ICMP, HTTP, FTP y SMTP. A través de este proyecto, se busca aplicar los conocimientos adquiridos en el curso de Redes III, explorando las capacidades de VyOS para la configuración de firewalls, VPNs (GRE e IPSec), y la seguridad en el enrutamiento mediante OSPF. Además, se implementarán servicios de capa de aplicación como DHCP, HTTP y DNS en un entorno virtualizado, con el fin de corroborar el correcto funcionamiento de las configuraciones realizadas.

OBJETIVOS

Objetivo General

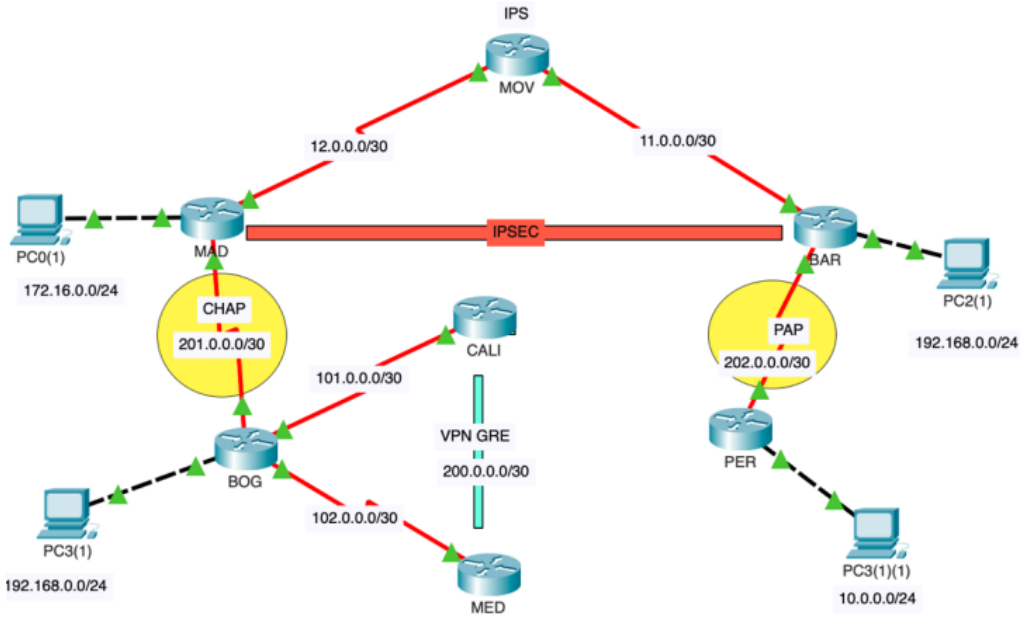
Configurar un firmware de enrutamiento basado en Linux (VyOS) para desplegar mecanismos de seguridad y control de acceso a servicios de red, aplicando los conceptos y conocimientos adquiridos en el curso de Redes III.

Objetivos Específicos

- Configuración de VyOS: Desplegar y configurar VyOS como firmware de enrutamiento, aprovechando sus funcionalidades de firewall, VPN y enrutamiento seguro.
- Implementación de Mecanismos de Seguridad:
    - Configurar un sistema de prevención de intrusiones (IPS) para definir y controlar el tráfico de red (ICMP, HTTP, FTP, SMTP).
    - Establecer conexiones VPN utilizando protocolos GRE e IPSec para garantizar la seguridad y privacidad de las comunicaciones.
    - Asegurar el enrutamiento mediante el protocolo OSPF para realizar el enrutamiento de las conexiones VPN.
- Despliegue de Servicios de Capa de Aplicación:
    - Habilitar y configurar servicios de DHCP, HTTP y DNS en una máquina virtual Linux para probar la conectividad y funcionalidad de la red.
- Validación y Pruebas:
    - Realizar pruebas de conectividad y funcionalidad para verificar el correcto funcionamiento de los servicios implementados.

- Documentar los procedimientos de configuración y los resultados obtenidos, incluyendo diagramas topológicos de red y aspectos de funcionalidad implementada.

ESQUEMA DE TRABAJO



REQUERIMIENTOS

1. Oracle VM VirtualBox. Despliegue de máquinas virtuales.
2. VyOS 1.5. Firmware para enrutamiento.
3. Alpine Linux 3.20.0. Distribución ligera para configuración de un servidor y cliente.
4. Graphical Network Simulator-3 (GNS3). Software para implementación y simulación de redes de comunicación.

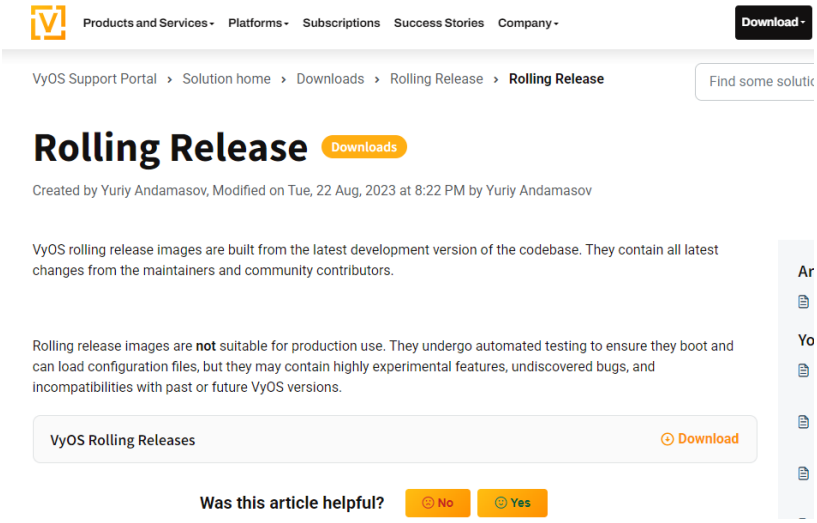
DESARROLLO

CREACIÓN Y CONFIGURACIÓN DE LAS MAQUINAS VIRTUALES

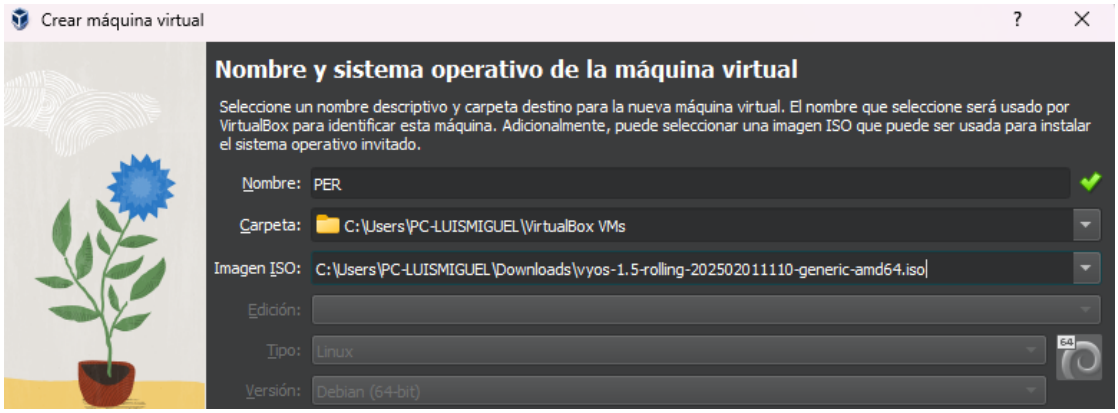
Para este proyecto se utilizaron 9 máquinas virtuales, correspondientes a 7 Routers, 1 Host cliente y 1 Server. Además, se añadieron 2 VPCS básicos de GNS3.

a. Configuración de Routers (máquina virtual)

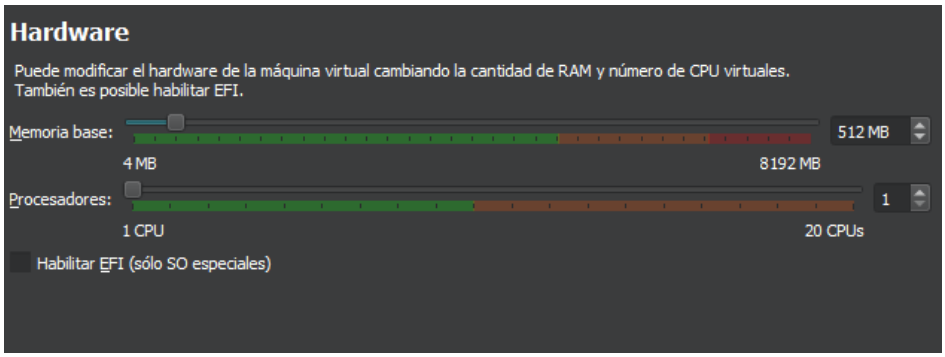
En primer lugar, descargamos la ISO del sistema operativo VyOS 1.5 a través de su sitio web oficial.

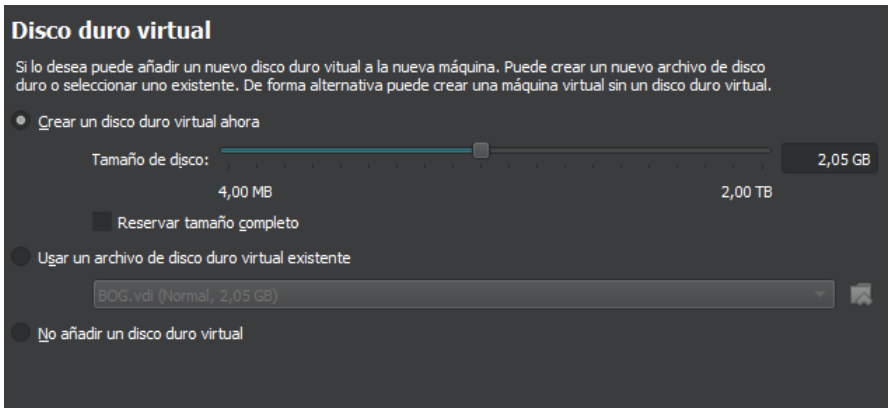


A continuación, creamos una máquina virtual en Oracle VM VirtualBox, asignándole un nombre (en este caso se trata del Router PER), y abajo seleccionamos la imagen ISO de VyOS que acabamos de descargar y le damos en siguiente.



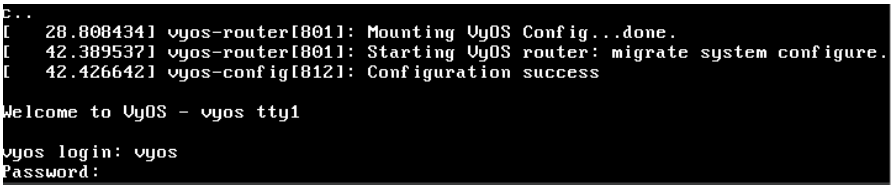
A continuación, seleccionamos las especificaciones de Hardware de la máquina virtual que estamos creando; 512 MB de RAM, 1 Núcleo de procesamiento y 2GB de espacio en disco.





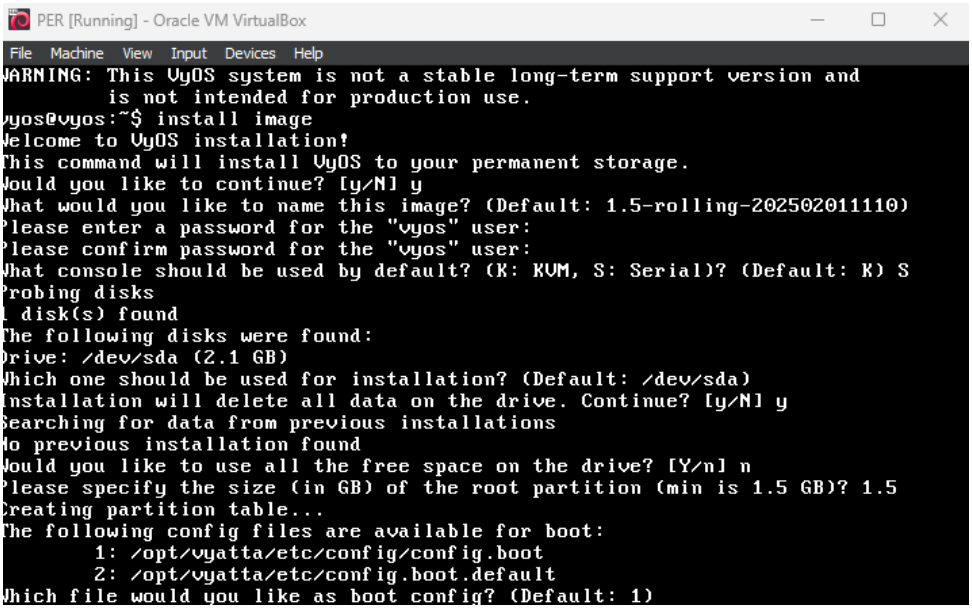
Instalación de la ISO de VyOS

Mediante Oracle VM VirtualBox inicializamos una instancia de la máquina virtual creada, e inciamos sesión con las credenciales predeterminadas de esta ISO; vyos login: vyos y password: vyos.

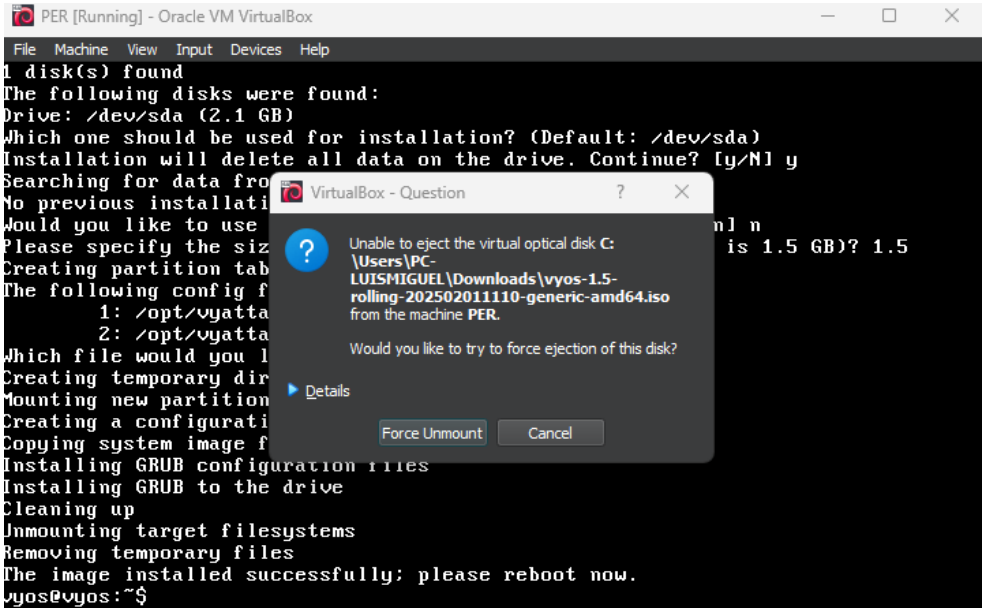


Con el comando `install image` realizamos la instalación de la ISO en la terminal de VyOS. El sistema solicita confirmación para proceder con la instalación, dejamos el nombre por defecto a la imagen y digitamos la contraseña para el usuario “vyos”, en este caso “vyos”.

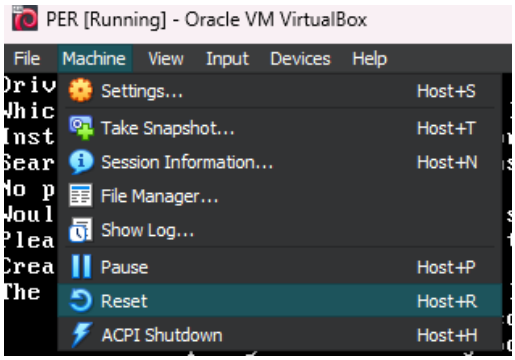
Luego, elegimos la consola predeterminada (en este caso, "S" para Serial). Se identifican los discos disponibles y se muestra /dev/sda con 2.1 GB de espacio y seleccionamos /dev/sda como el disco para la instalación. Se advierte que todos los datos en el disco serán eliminados y se solicita confirmación. Se pregunta si se debe usar todo el espacio del disco (respondemos "n" para especificar un tamaño manualmente) y definimos una partición raíz de 1.5 GB. Se muestran archivos de configuración para el arranque y seleccionamos la configuración predeterminada (config.boot) que corresponde al archivo 1.



Realizamos el retiro de la imagen ISO dando click en Dispositivos, unidades ópticas con la ISO de VyOS marcada y forzar desmontaje.



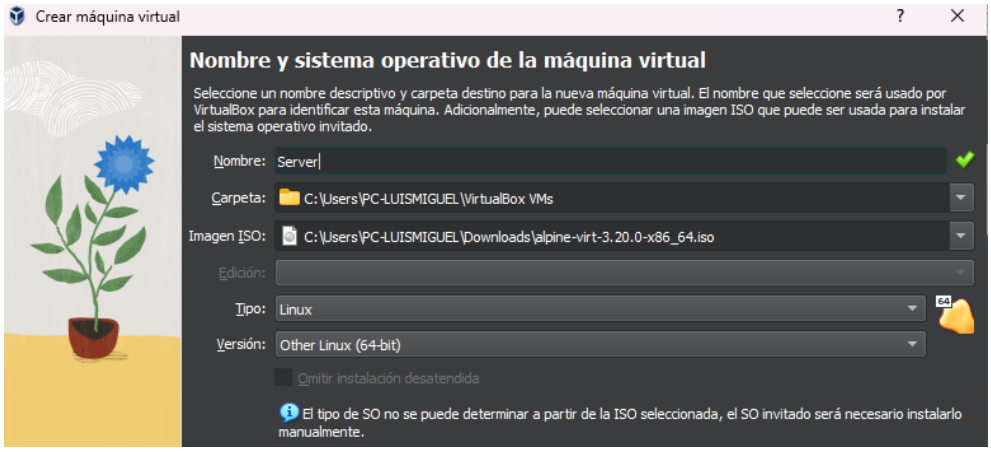
Finalmente reiniciamos la instancia de la máquina virtual



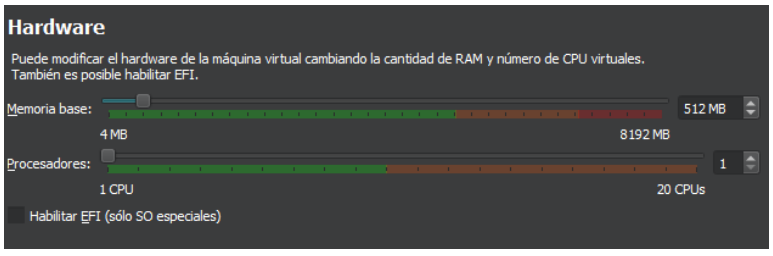
b. Configuración de Server (máquina virtual)

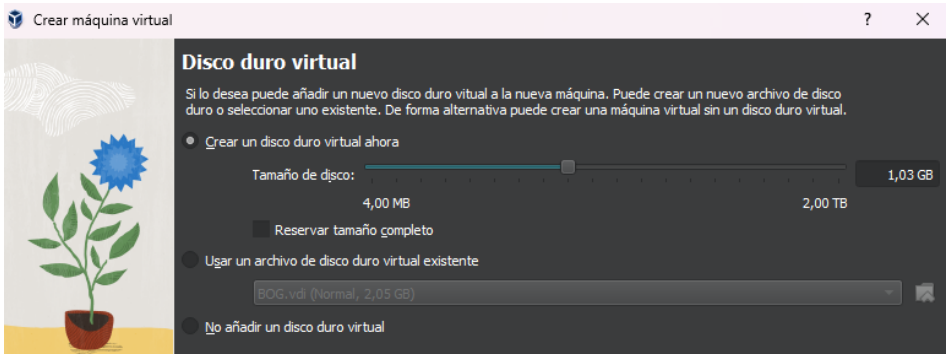
Creamos la máquina virtual "Server" en Oracle VM VirtualBox utilizando la ISO de la distribución Alpine Linux Virtual versión 3.20.0

Seleccionamos abajo el tipo: Linux y la versión: Other Linux (64-bit).

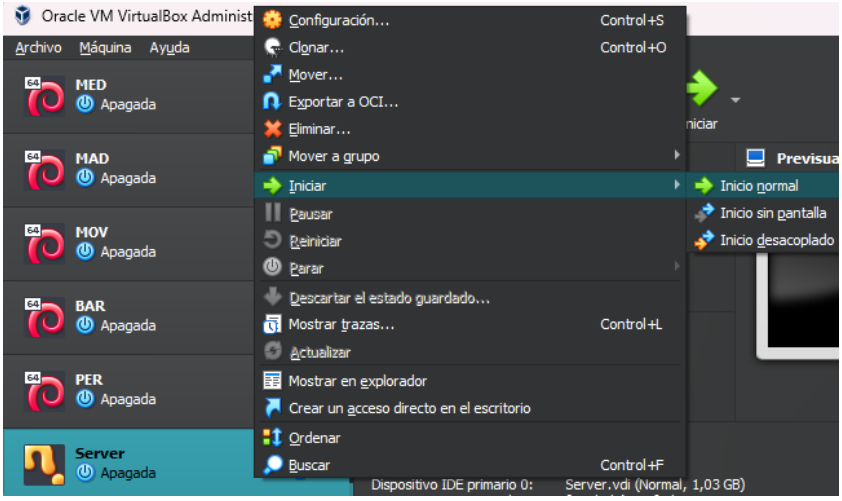


Las especificaciones de Hardware de esta máquina virtual son: 512 MB de RAM, 1 núcleo de procesamiento y 1 GB de espacio en disco.

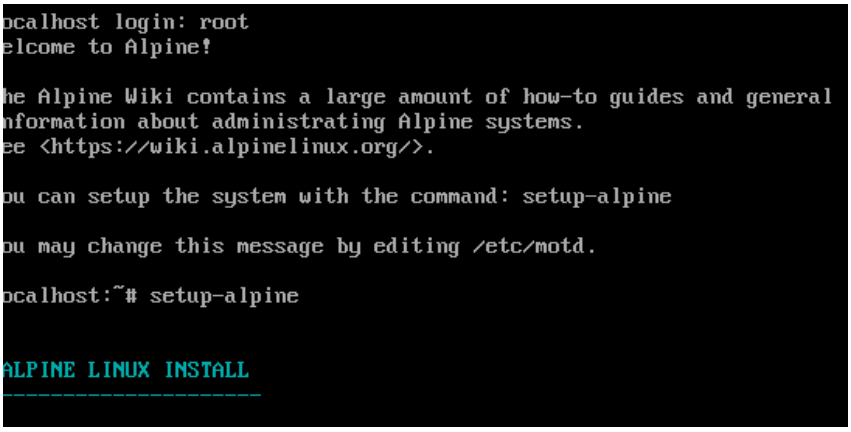




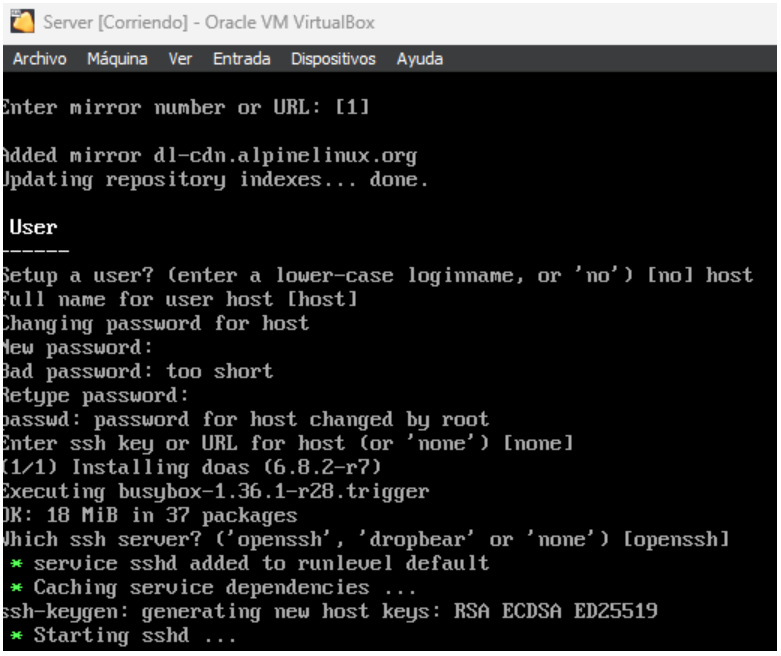
Encendemos la máquina virtual Server para instalar la ISO de Alpine Linux Virtual 3.20.0



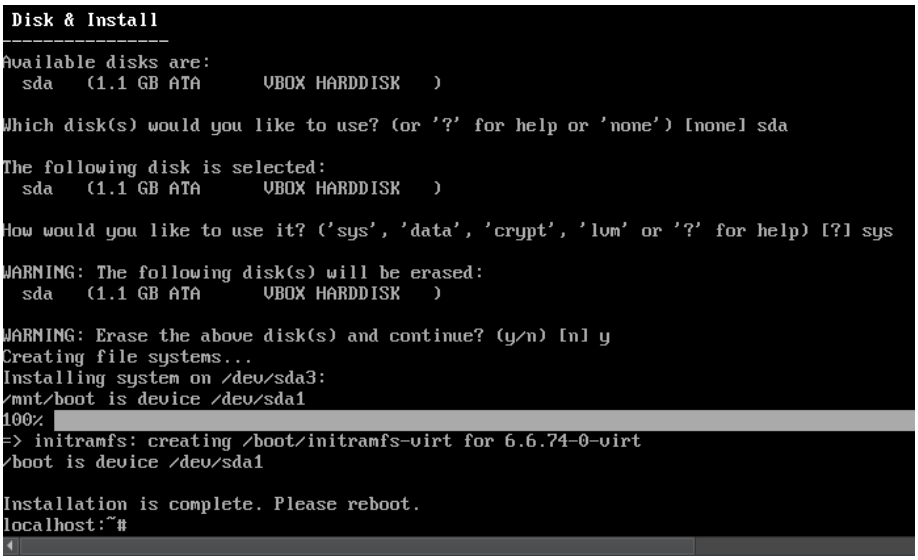
Iniciamos sesión con ‘`root`‘ y escribimos `setup-alpine` para comenzar la instalación.



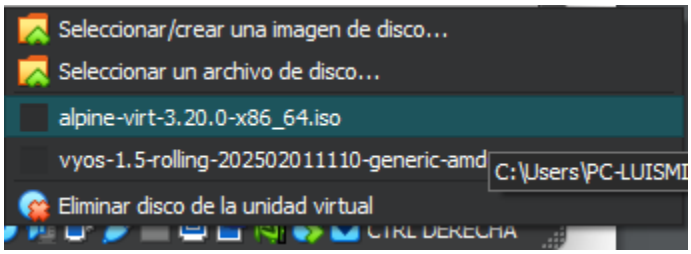
Se continua el proceso de instalación guiado presionando enter hasta que nos pregunte crear el user ‘host’, digitamos la password en este caso ‘root’ y la confirmamos. Seguimos presionando enter hasta que salga el apartado de Disk & Install.

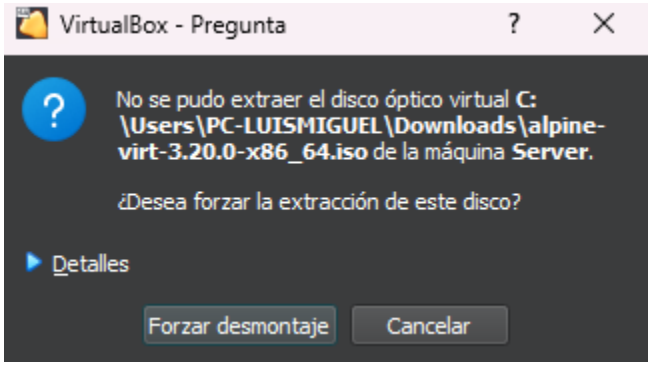


En esta parte escribimos 'sda' para seleccionar el disco y 'sys' como nombre, y finalmente escribimos 'y' para borrar los discos anteriores terminando la instalación.

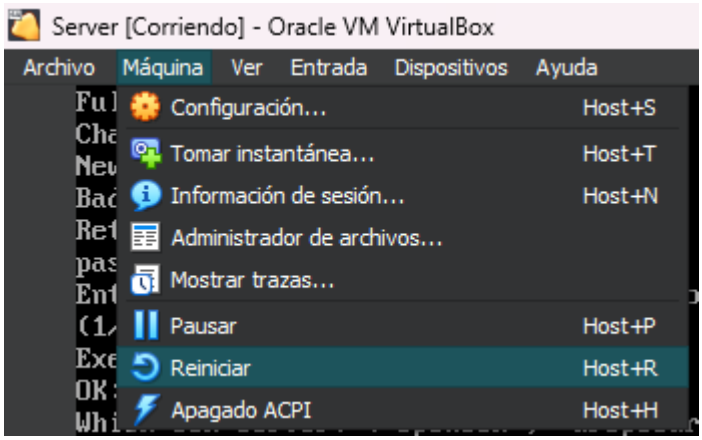


Procedemos a retirar la imagen ISO

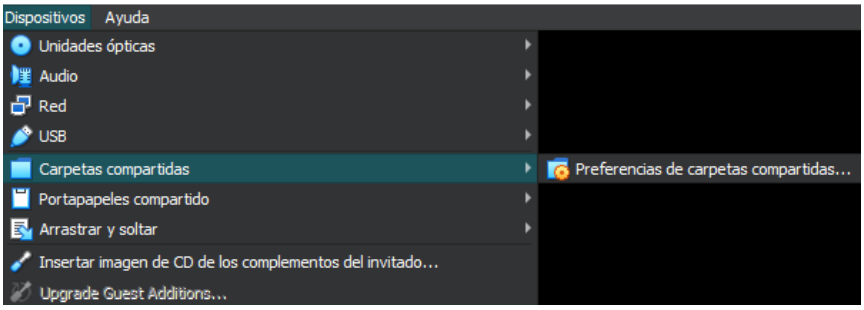


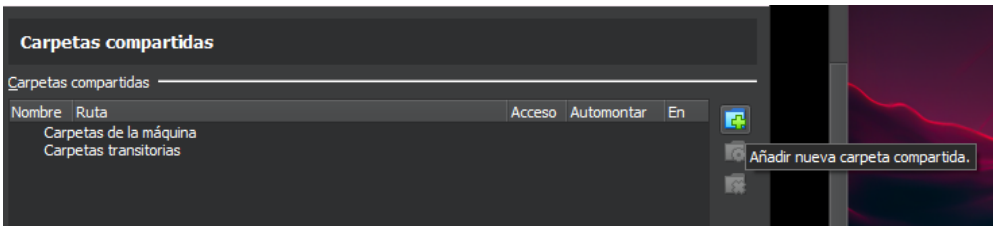


Reiniciamos la máquina virtual Server

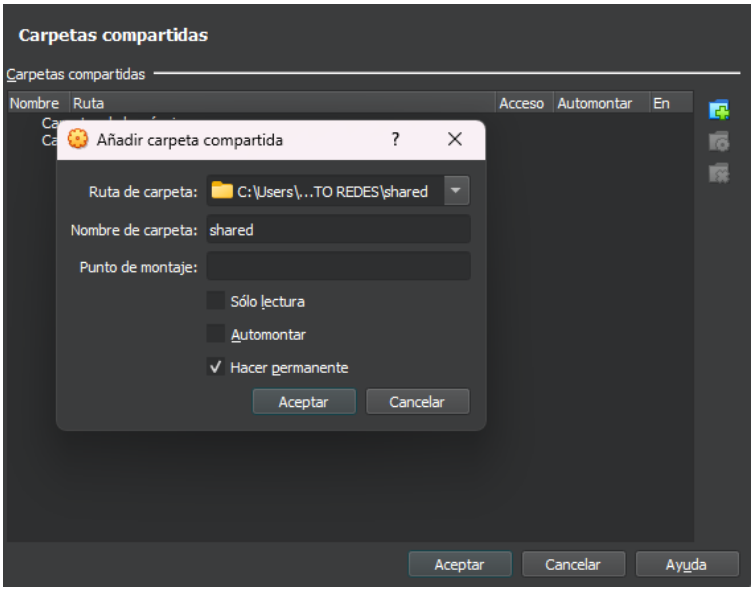


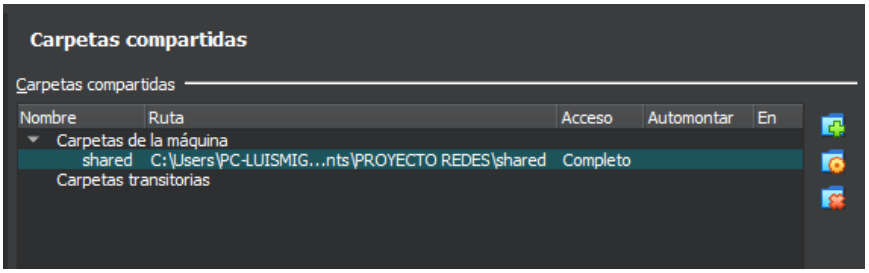
Después de haber reiniciado la máquina virtual, realizamos el vínculo con la carpeta compartida 'shared'



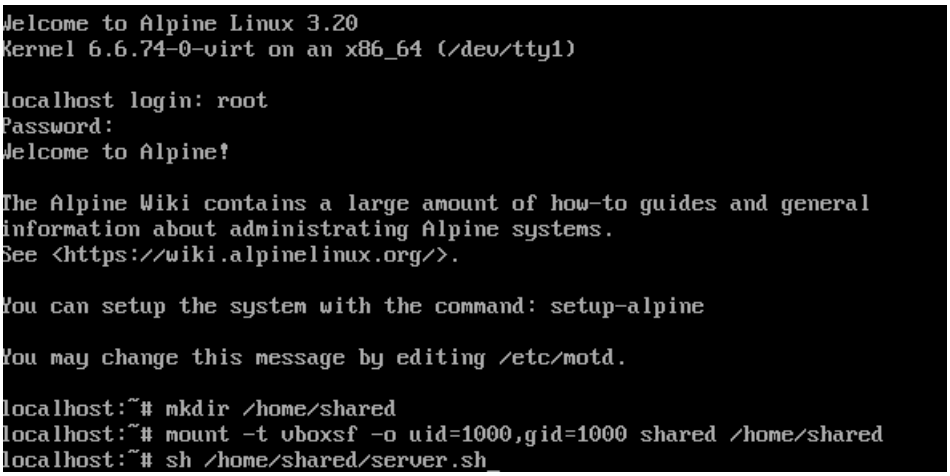


Seleccionamos la ruta de la carpeta y marcamos la opción: hacer permanente y aceptamos.





Entramos nuevamente con la credencial ‘root’ y escribimos los comandos que se observan al final para realizar la configuración; La primera línea crea la carpeta ‘shared’ en home, La segunda línea monta la carpeta compartida en la dirección de la carpeta creada y la última línea ejecuta el script server.sh ubicado en ‘home/shared’.



El script ‘server.sh’ se encarga de configurar la IP estática del servidor, instalar las dependencias necesarias para ofrecer los servicios requeridos y configurarlos.

El comando ‘rc-update add local default’ indica a Alpine Linux que debe ejecutar todo lo contenido en la carpeta ‘/etc/local.d/’ al iniciar el sistema operativo. El comando ‘chmod 775 /etc/local.d/*’ otorga a permisos de ejecución a todo lo contenido ahí.

`/home/shared/server.sh`

```
#!/bin/bash

# Instalar Alpine: setup-alpine

# Instalación de software necesario
apk add bind # named (dns)
apk add dhcp # dhcpd (dhcp)
apk add busybox-extras # httpd (http)

# Configuración
rc-update add local default
cp -a /home/shared/server/* /
chmod 775 /etc/local.d/*

reboot # Reinicar
```

Los archivos contenidos en ‘/etc/local.d/’ son:

`/etc/local.d/shared.start`

Montado de la carpeta compartida.

```
#!/bin/bash

# Configuración Carpeta Compartida
mkdir /home/shared
mount -t vboxsf -o uid=1000,gid=1000 shared /home/shared
```

`/etc/local.d/services.start`

Ejecución de servicios.

```
#!/bin/sh

# Inicio de los servicios
rc-service named start
rc-service dhcpd start
httpd -p 80 -h /home/server/httpd/wwwsite
```

`/etc/local.d/resolvconf.start`

Configuración de servidor DNS en Loopback.

```
#!/bin/sh

# Configuración de DNS en Loopback
echo 127.0.0.1 > /etc/resolv.conf
```

`/etc/network/interfaces`

El archivo de configuración de interfaces

Indica que debe ser iniciada una dirección Loopback en IPv4 y la interfaz Ethernet 0 con direcciones estáticas IPv4.

```
auto lo
iface lo inet loopback

auto eth0
iface eth0 inet static
    address         192.168.0.3/24
    gateway         192.168.0.1
```

Adicionalmente, los procesos instalados son los siguientes:

- **Bind (named):** Un servidor DNS sencillo. Se ejecuta como un servicio Linux (línea 4 de '/etc/local.d/services.start')

`/etc/bind/named.conf`

Habilita servicios DNS de Google para dominios no definidos y define el dominio example.com usando el archivo db.example.com.

```
options {
    forwarders {
        8.8.8.8;
        8.8.4.4;
    };
    directory "/etc/bind";
    allow-query { any; };
    recursion yes;
    dnssec-validation auto;
};

zone "example.com" {
    type master;
    file "/etc/bind/db.example.com";
};
```

`/etc/bind/dh.example.com`

Indica que el dominio solo, o precedido por www deberá ser direccionado a la IP estática del servidor.

```
$TTL    86400
@   IN  SOA example.com. root.localhost. (
              1           ; Serial
              604800      ; Refresh
              86400       ; Retry
              2419200     ; Expire
              86400 )     ; Negative Cache TTL
;
@   IN  NS      example.com.
    IN  A       192.168.0.3
www IN  A       192.168.0.3
```

`/etc/dhcp/dhcpd.conf`

Configura las redes 192.168.0.0/24 y 172.16.0.0/24 con sus respectivos DNS, máscara de red y Gateway, asignando una de 100 direcciones disponibles en cada red.

```
default-lease-time 86400;
max-lease-time 86400;

authoritative;

log-facility local7;

subnet 192.168.0.0 netmask 255.255.255.0 {
    range 192.168.0.100 192.168.0.200;
    option domain-name-servers 192.168.0.3;
    option subnet-mask 255.255.255.0;
    option routers 192.168.0.1;
}

subnet 172.16.0.0 netmask 255.255.255.0 {
    range 172.16.0.100 172.16.0.200;
    option domain-name-servers 192.168.0.3;
    option subnet-mask 255.255.255.0;
    option routers 172.16.0.1;
}
```

- **Busybox-httpd (httpd):** Un servidor HTTP sencillo. Para su despliegue sólo hace falta indicar la ruta de la carpeta que contiene la página web (línea 6 en `/etc/local.d/services`).

`/home/server/httpd/wwwsite/styles.css`

y por último una página muy sencilla con un anuncio de prueba enlazada a una hoja de estilos.

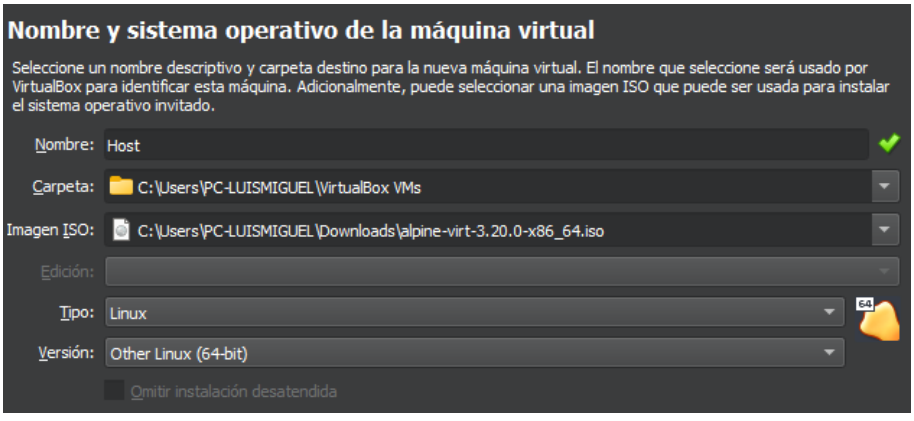
```
<!DOCTYPE html>
<html lang="es">
<head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <title>Página de Prueba</title>
    <link rel="stylesheet" href="styles.css">
</head>
<body>
    <div class="container">
        <h1>¡Hola! ¡Soy Alpine Linux Server!</h1>
        <p>Esta es una página de prueba desplegada en un servidor HTTP de BusyBox en Alpine Linux.</p>
    </div>
</body>
</html>
```

```css
body {
    font-family: Arial, sans-serif;
    background-color: #f4f4f9;
    margin: 0;
    display: flex;
    justify-content: center;
    align-items: center;
    height: 100vh;
    color: #333;
}

.container {
    text-align: center;
    background: #fff;
    padding: 20px;
    border-radius: 8px;
    box-shadow: 0 0 10px rgba(0, 0, 0, 0.1);
}

h1 {
    color: #0073e6;
    margin-bottom: 10px;
}

p {
    font-size: 1.2em;
}
```

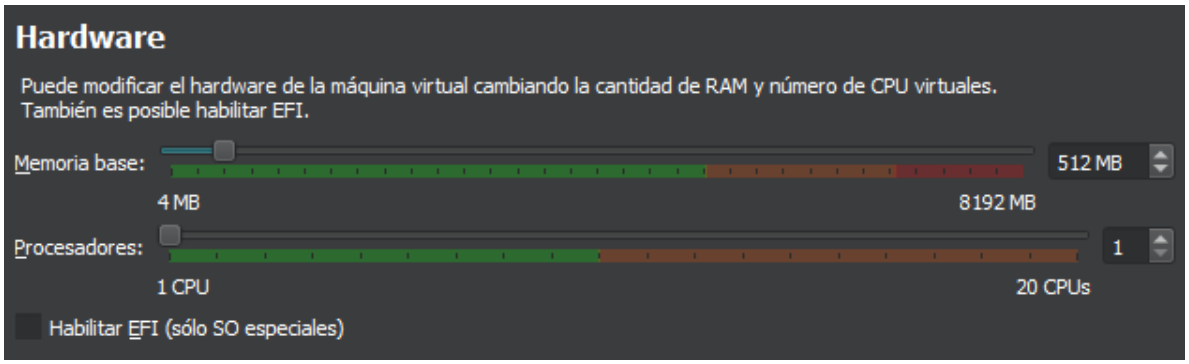
c. Configuración de Cliente (máquina virtual)

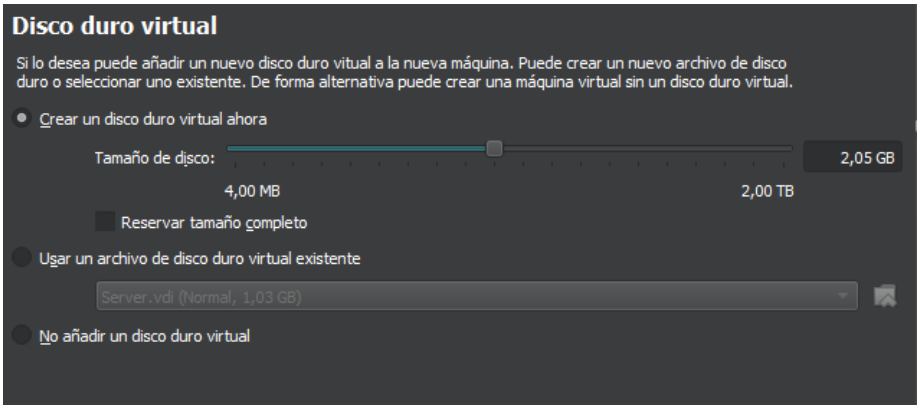
Después de configurar “Server”, creamos la máquina virtual “Host” en Oracle VM VirtualBox reutilizando la ISO de la distribución Alpine Linux Virtual 3.20.0

Volvemos a seleccionar en la parte inferior el tipo: Linux y la versión: Other Linux (64-bit).

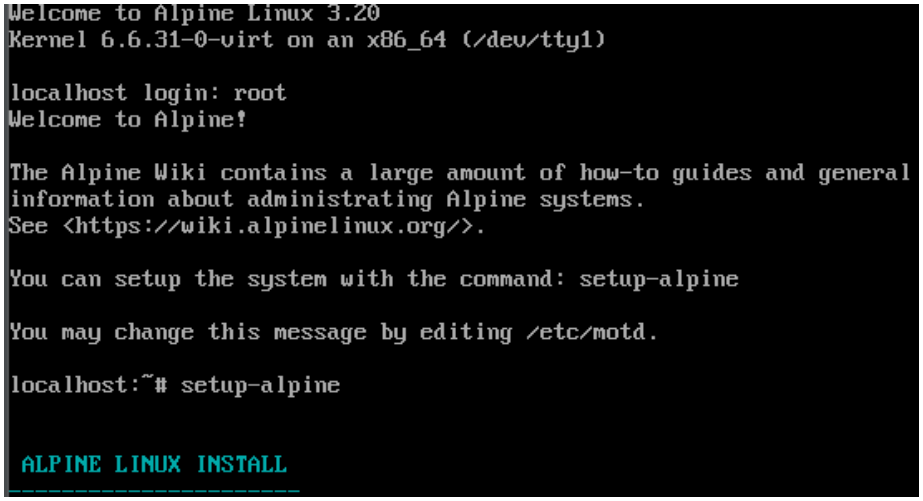


Las especificaciones de Hardware de “Server” son: 512 MB de RAM, 1 núcleo de procesamiento y 2 GB de espacio en disco.





Una vez iniciada la instancia de “Host” repetimos el proceso realizado con la máquina virtual “Server” para realizar la instalación.



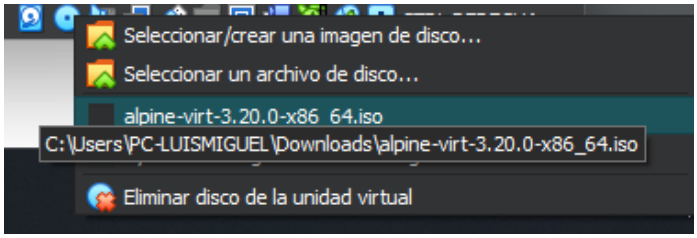
Esta vez el nombre de usuario es ‘host’ y digitamos la contraseña.

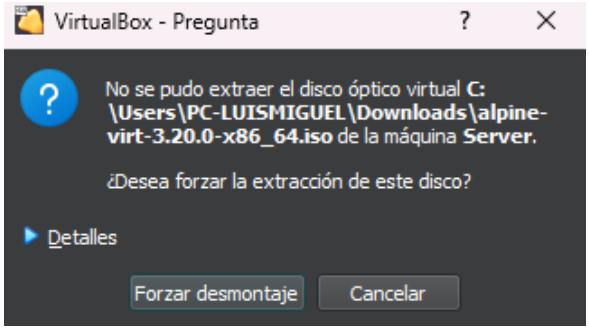
```
User
------
Setup a user? (enter a lower-case loginname, or 'no') [no] host
Full name for user host [host]
Changing password for host
New password:
Bad password: too short
Retype password:
passwd: password for host changed by root
```

Repetimos lo anteriormente realizado en “Server” para esta parte.

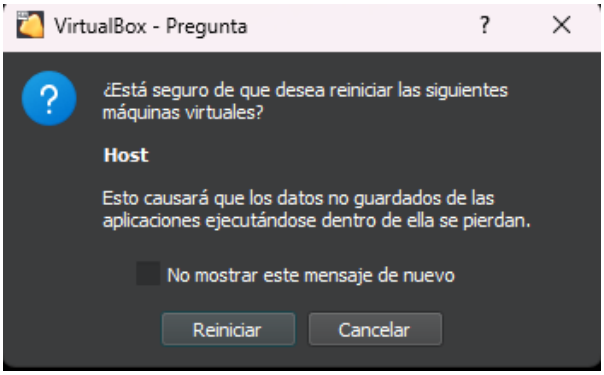
```
Disk & Install
----------------
Available disks are:
  sda    (2.2 GB ATA      VBOX HARDDISK   )

Which disk(s) would you like to use? (or '?' for help or 'none') [none] sda

The following disk is selected:
  sda    (2.2 GB ATA      VBOX HARDDISK   )

How would you like to use it? ('sys', 'data', 'crypt', 'lvm' or '?' for help) [?] sys

WARNING: The following disk(s) will be erased:
  sda    (2.2 GB ATA      VBOX HARDDISK   )

WARNING: Erase the above disk(s) and continue? (y/n) [n] y
Creating file systems...
Installing system on /dev/sda3:
/mnt/boot is device /dev/sda1
91%
```

Retiramos la Imagen ISO

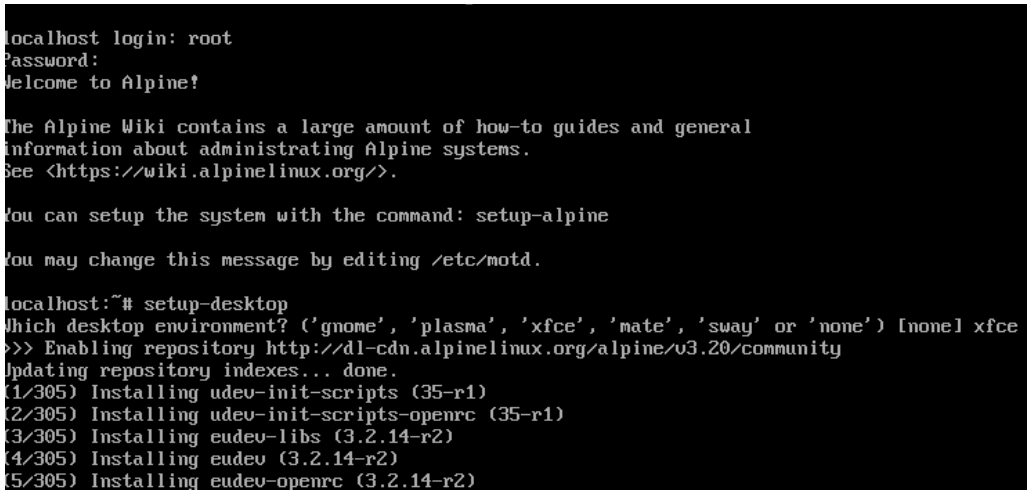




Y reiniciamos la máquina virtual “Host”

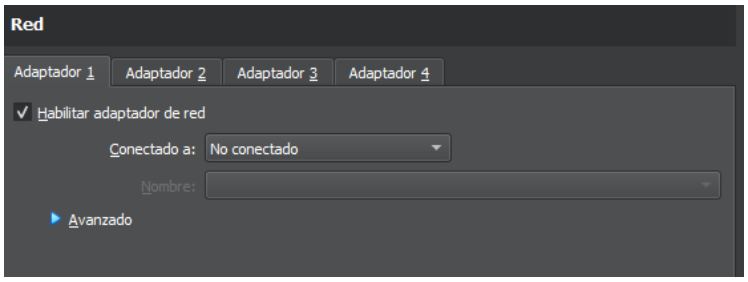


Después de reiniciar la máquina virtual, iniciamos sesión nuevamente con ‘root’ y escribimos ‘setup-desktop’ para instalar el gestor de ventanas, escribimos ‘xfce’ para seleccionar el entorno de escritorio y finalizamos la instalación.

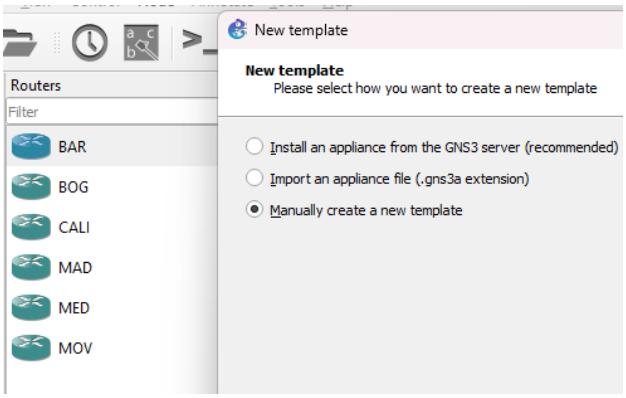


CONSTRUCCIÓN DE TOPOLOGÍA EN GNS3

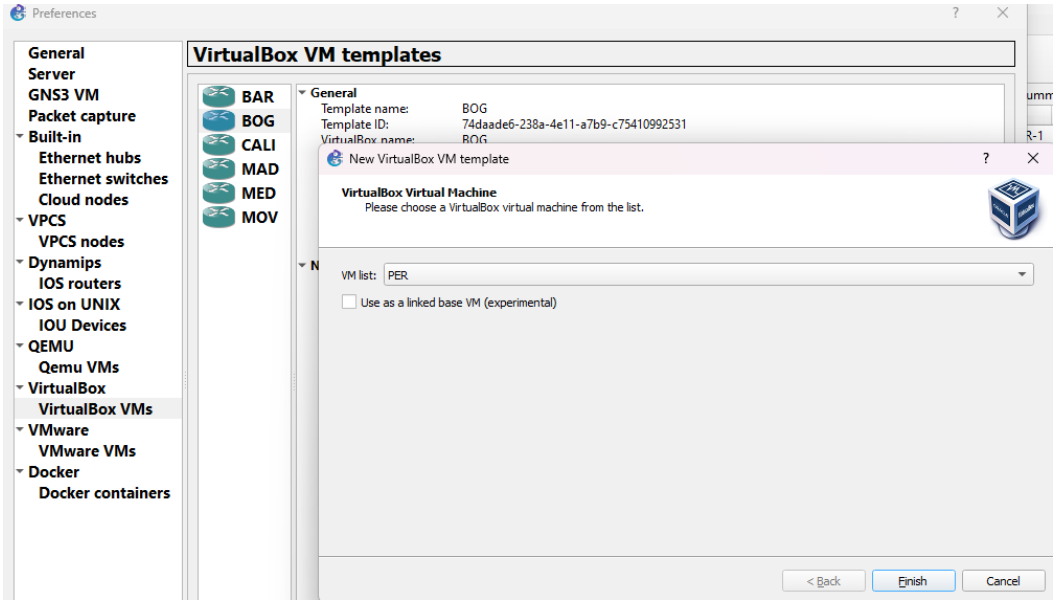
Una vez realizada la creación y configuración de las máquinas virtuales a utilizar, es importante desconectar las cuatro interfaces de red en Oracle VM VirtualBox marcando la opción de habilitar el adaptador de red de cada una. Esto se debe hacer con todas las máquinas virtuales creadas.



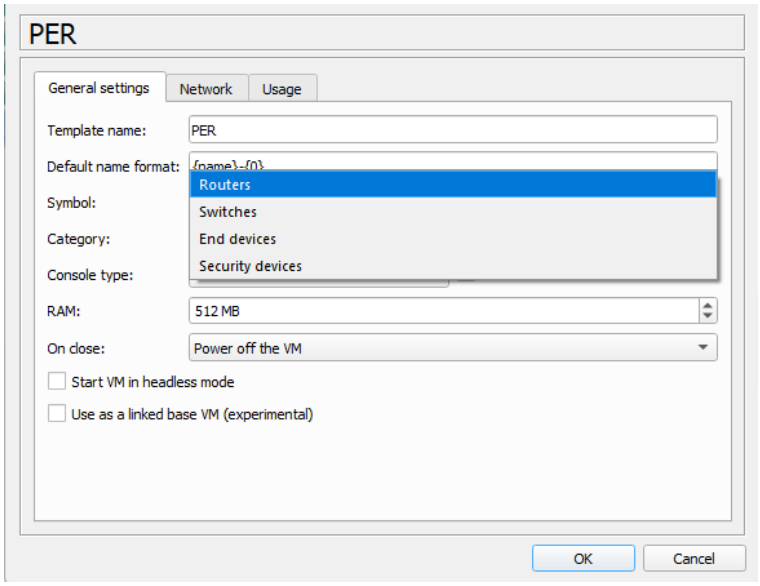
A continuación, en GNS3 añadimos los templates de las máquinas virtuales, seleccionamos la opción de crear manualmente un nuevo template.



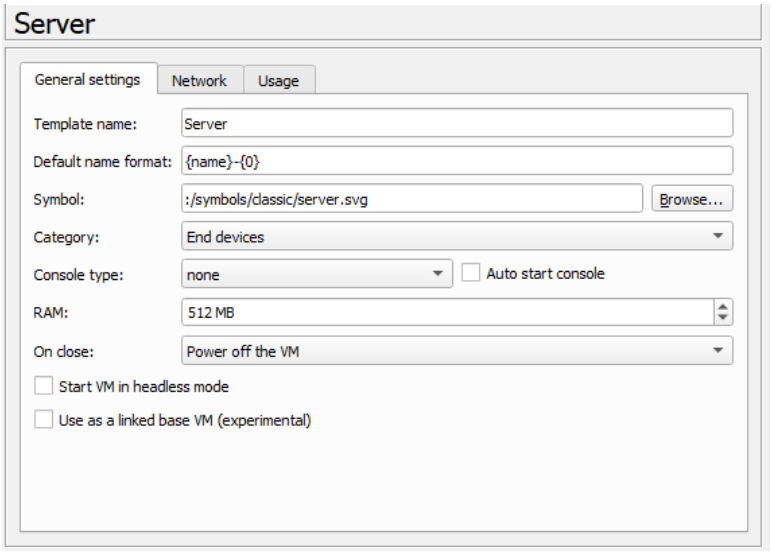
Seleccionamos VirualBox VM templates, new y automáticamente se selecciona una de las máquinas virtuales creadas en VirtualBox. Una vez hecho damos click sobre la template para configurarla.



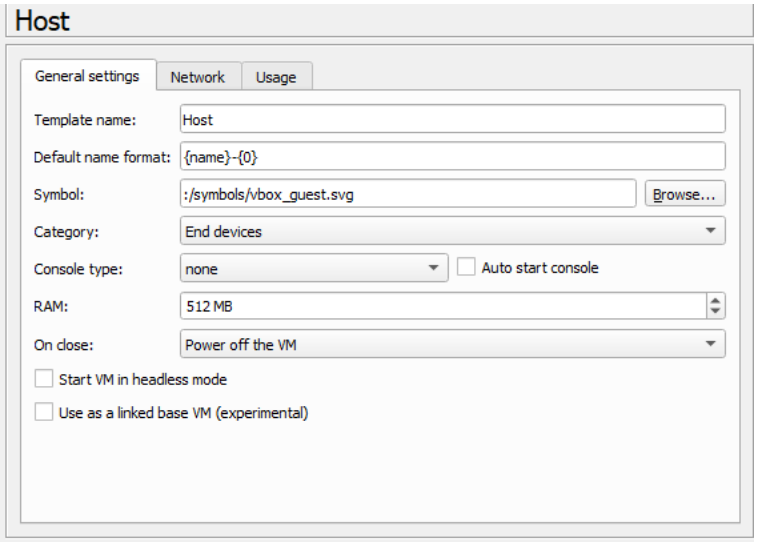
Para los routers escogemos como categoría: Routers, seleccionamos su símbolo en Classic y en Network definimos 4 adaptadores.



Para la máquina virtual Server cambiamos su categoría a End devices y seleccionamos su símbolo en Classic.



Finalmente, para la máquina virtual Server también cambiamos su categoría a End devices y dejamos su símbolo por defecto.



Una vez creados los templates de cada máquina virtual en GNS3 se ensambla la topología del enunciado, teniendo en cuenta el siguiente esquema de conexión de interfaces.

MOV:

eth0: MAD

eth1: BAR

MAD:

eth0: MOV

eth1: BOG

eth2: Host-1

BOG:

eth0: MAD

eth1: CALI

eth2: MED

eth3: PC1

BAR:

eth0: MOV

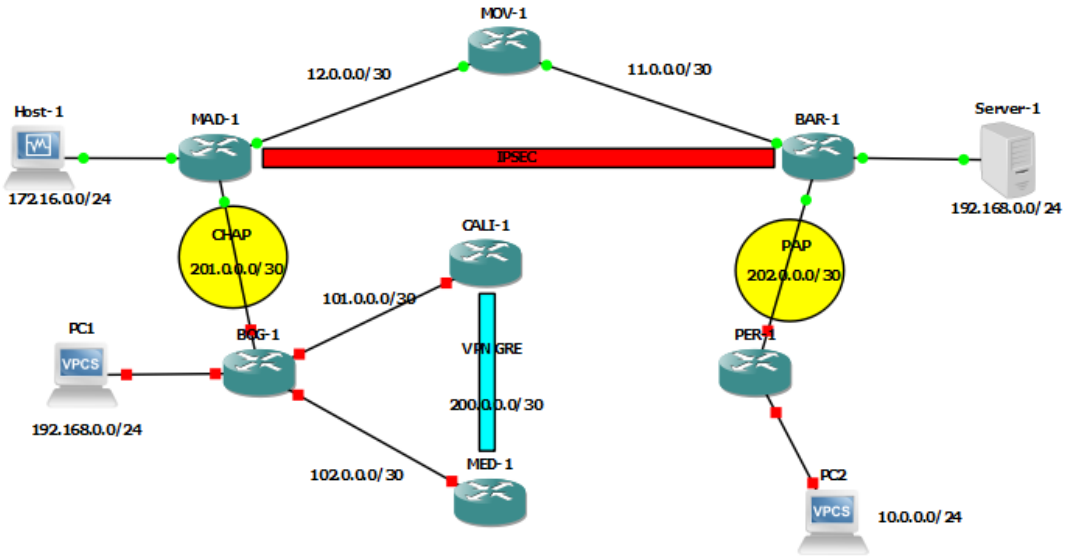
eth1: PER

eth2: Server-1

PER:

eth0: BAR

eth1: PC2.



CONFIGURACIÓN DE ROUTERS VyOS EN GNS3

Cambio del host-name

Se cambia el host-name de cada máquina virtual, para poder facilitar así su futura identificación

ROUTER MOV-1

```
vyos@vyos# set system host-name MOV
[edit]
```

ROUTER MAD-1

```
vyos@vyos# set system host-name MAD
[edit]
```

ROUTER BAR-1

```
vyos@vyos# set system host-name BAR
[edit]
```

ROUTER BOG-1

```
vyos@vyos# set system host-name BOG
[edit]
```

ROUTER PER-1

```
vyos@vyos# set system host-name PER
```

ROUTER CALI-1

```
vyos@vyos# set system host-name CALI
[edit]
```

ROUTER MED-1

```
vyos@vyos# set system host-name MED
[edit]
```

Configuración de interfaces

Según la topología se definen las interfaces de cada maquina virtual, donde algunas direcciones IP las asignamos de manera estática, y en los otros casos como BOG y PER una interfaz en especifico se asigna automáticamente desde un servidor DHCP.

ROUTER MOV-1

```
vyos@vyos# set interfaces ethernet eth0 address 12.0.0.1/30
[edit]
vyos@vyos# set interfaces ethernet eth1 address 11.0.0.1/30
```

ROUTER MAD-1

```
vyos@vyos# set interfaces ethernet eth0 address 12.0.0.2/30
[edit]
vyos@vyos# set interfaces ethernet eth1 address 201.0.0.1/32
[edit]
vyos@vyos# set interfaces ethernet eth2 address 172.16.0.1/24
[edit]
```

ROUTER BAR-1

```
vyos@vyos# set interfaces ethernet eth0 address 11.0.0.2/30
[edit]
vyos@vyos# set interfaces ethernet eth1 address 202.0.0.1/32
[edit]
vyos@vyos# set interfaces ethernet eth2 address 192.168.0.1/24
[edit]
```

ROUTER BOG-1

```
vyos@vyos# set interfaces ethernet eth0 address dhcp
[edit]
vyos@vyos# set interfaces ethernet eth1 address 101.0.0.1/30
[edit]
vyos@vyos# set interfaces ethernet eth2 address 102.0.0.1/30
[edit]
vyos@vyos# set interfaces ethernet eth3 address 192.168.0.1/24
[edit]
```

ROUTER PER-1

```
vyos@vyos# set interfaces ethernet eth0 address dhcp
[edit]
vyos@vyos# set interfaces ethernet eth1 address 10.0.0.1/24
[edit]
```

ROUTER CALI-1

```
vyos@vyos# set interfaces ethernet eth0 address 101.0.0.2/30
[edit]
```

ROUTER MED-1

```
vyos@vyos# set interface ethernet eth0 address 102.0.0.2/30
[edit]
```

Configuración de enrutamiento

En este caso vamos a utilizar OSPF, donde vamos a definir que todas las maquinas virtuales van a pertenecer al área 0.

ROUTER MOV-1

```
vyos@vyos# set protocols ospf area 0 network 12.0.0.0/30
[edit]
vyos@vyos# set protocols ospf area 0 network 11.0.0.0/30
[edit]
```

ROUTER MAD-1

```
vyos@vyos# set protocols ospf area 0 network 12.0.0.0/30
[edit]
vyos@vyos# set protocols ospf area 0 network 172.16.0.0/24
```

ROUTER BAR-1

```
vyos@vyos# set protocols ospf area 0 network 11.0.0.0/30
[edit]
vyos@vyos# set protocols ospf area 0 network 192.168.0.0/24
[edit]
```

ROUTER BOG-1

```
vyos@vyos# set protocols ospf area 0 network 101.0.0.0/30
[edit]
vyos@vyos# set protocols ospf area 0 network 102.0.0.0/30
[edit]
vyos@vyos# set protocols ospf area 0 network 192.168.0.0/24
[edit]
```

ROUTER CALI-1

```
vyos@vyos# set protocols ospf area 0 network 101.0.0.0/30
[edit]
```

ROUTER MED-1

```
vyos@vyos# set protocols ospf area 0 network 101.0.0.0/30
[edit]
```

Configuración túnel MAD-BAR

El túnel entre **MAD** y **BAR** se establece utilizando **IPsec**, un protocolo que proporciona seguridad en la comunicación a través de redes públicas como Internet, ambos routers configuran un túnel **site-to-site** utilizando **Internet Key Exchange (IKE) y Encapsulating Security Payload (ESP)** para cifrar los datos.

- Establecimiento de la conexión con IKE
    - Se usa **AES-256** para cifrado de clave.

    - Se usa **SHA-256** para verificar la integridad de los paquetes.
    - Se usa **Diffie-Hellman Group 14** para el intercambio seguro de claves.
    - Se establece un **lifetime de 3600 segundos** para renovar la clave.
- Protección del tráfico con ESP
    - Se usa **AES-256** para cifrado de los datos.
    - Se usa **SHA-256** para garantizar la integridad de los paquetes.
    - Se establece un **lifetime de 3600 segundos**.
- Pre-Shared Secret (PSK)
    - Se usa una clave precompartida (`vyos secret vyos`) para autenticación entre **MAD** y **BAR**.

ROUTER MAD-1

```
vyos@vyos# set vpn ipsec ike-group IKE-GROUP proposal 1 encryption aes256
[edit]
vyos@vyos# set vpn ipsec ike-group IKE-GROUP proposal 1 hash sha256
[edit]
vyos@vyos# set vpn ipsec ike-group IKE-GROUP proposal 1 dh-group 14
[edit]
vyos@vyos# set vpn ipsec ike-group IKE-GROUP lifetime 3600
[edit]
vyos@vyos# set vpn ipsec esp-group ESP-GROUP proposal 1 encryption aes256
[edit]
vyos@vyos# set vpn ipsec esp-group ESP-GROUP proposal 1 hash sha256
[edit]
vyos@vyos# set vpn ipsec esp-group ESP-GROUP lifetime 3600
[edit]
vyos@vyos# set vpn ipsec authentication psk vyos id 11.0.0.2
[edit]
vyos@vyos# set vpn ipsec authentication psk vyos id 12.0.0.2
[edit]
vyos@vyos# set vpn ipsec authentication psk vyos secret vyos
vyos@vyos# set vpn ipsec site-to-site peer BAR authentication mode pre-shared-se
cret
[edit]
vyos@vyos# set vpn ipsec site-to-site peer BAR local-address 12.0.0.2
[edit]
vyos@vyos# set vpn ipsec site-to-site peer BAR remote-address 11.0.0.2
[edit]
vyos@vyos# set vpn ipsec site-to-site peer BAR ike-group IKE-GROUP
[edit]
vyos@vyos# set vpn ipsec site-to-site peer BAR tunnel 1 esp-group ESP-GROUP
[edit]
vyos@vyos# set vpn ipsec site-to-site peer BAR tunnel 1 local prefix 172.16.0.0/
24
[edit]
vyos@vyos# set vpn ipsec site-to-site peer BAR tunnel 1 remote prefix 192.168.0.
0/24
[edit]
```

ROUTER BAR-1

```
vyos@vyos# set vpn ipsec ike-group IKE-GROUP proposal 1 encryption aes256
[edit]
vyos@vyos# set vpn ipsec ike-group IKE-GROUP proposal 1 hash sha256
[edit]
vyos@vyos# set vpn ipsec ike-group IKE-GROUP proposal 1 dh-group 14
[edit]
vyos@vyos# set vpn ipsec ike-group IKE-GROUP lifetime 3600
[edit]
```

```
vyos@vyos# set vpn ipsec esp-group ESP-GROUP proposal 1 encryption aes256
[edit]
vyos@vyos# set vpn ipsec esp-group ESP-GROUP proposal 1 hash sha256
[edit]
vyos@vyos# set vpn ipsec esp-group ESP-GROUP lifetime 3600
[edit]
```

```
vyos@vyos# set vpn ipsec authentication psk vyos id 11.0.0.2
[edit]
vyos@vyos# set vpn ipsec authentication psk vyos id 12.0.0.2
[edit]
vyos@vyos# set vpn ipsec authentication psk vyos secret vyos
[edit]
```

```
vyos@vyos# set vpn ipsec site-to-site peer MAD authentication mode pre-shared-se
cret
[edit]
vyos@vyos# set vpn ipsec site-to-site peer MAD local-address 11.0.0.2
[edit]
vyos@vyos# set vpn ipsec site-to-site peer MAD remote-address 12.0.0.2
[edit]
vyos@vyos# set vpn ipsec site-to-site peer MAD ike-group IKE-GROUP
[edit]
vyos@vyos# set vpn ipsec site-to-site peer MAD tunnel 1 esp-group ESP-GROUP
[edit]
vyos@vyos# set vpn ipsec site-to-site peer MAD tunnel 1 local prefix 192.168.0.0
/24
[edit]
vyos@vyos# set vpn ipsec site-to-site peer MAD tunnel 1 remote prefix 172.16.0.0
/24
[edit]
```

Configuración túnel CALI-MED

El túnel entre CALI y MED se establece utilizando GRE (Generic Routing Encapsulation) sobre IPsec, El túnel entre **MAD** y **BAR** se establece utilizando **IPsec**, un protocolo que proporciona seguridad en la comunicación a través de redes públicas como Internet, ambos routers configuran un túnel **site-to-site** utilizando **Internet Key Exchange (IKE) , Encapsulating Security Payload (ESP)** para cifrar los datos y **Generic Routing Encapsulation (GRE)** encapsulando tráfico de distintos protocolos dentro de paquetes IP, permitiendo el enrutamiento entre redes privadas.

- GRE Tunnel
    - Se crea una **interfaz de túnel GRE** llamada `tun0`.
    - Se define **101.0.0.2** (CALI) como la dirección de origen y **102.0.0.2** (MED) como la dirección de destino.
    - La IP del túnel en CALI será **200.0.0.1/30** y en MED será **200.0.0.2/30**.
- Establecimiento de la conexión con IKE
    - Se usa **AES-256** para cifrado de clave.
    - Se usa **SHA-256** para verificar la integridad de los paquetes.

    - Se usa **Diffie-Hellman Group 14** para el intercambio seguro de claves.
    - Se establece un **lifetime de 3600 segundos** para renovar la clave.
- Protección del tráfico con ESP
    - Se usa **AES-256** para cifrado de los datos.
    - Se usa **SHA-256** para garantizar la integridad de los paquetes.
    - Se establece un **lifetime de 3600 segundos**.
- Pre-Shared Secret (PSK)
    - Se usa una clave precompartida (`vyos secret vyos`) para autenticación entre **MAD** y **BAR**.

ROUTER CALI-1

```
vyos@vyos# set interfaces tunnel tun0 encapsulation gre
[edit]
vyos@vyos# set interfaces tunnel tun0 source-address 101.0.0.2
[edit]
vyos@vyos# set interfaces tunnel tun0 remote 102.0.0.2
[edit]
vyos@vyos# set interfaces tunnel tun0 address 200.0.0.1/30
[edit]
```

```
vyos@vyos# set vpn ipsec ike-group IKE-GROUP proposal 1 encryption aes256
[edit]
vyos@vyos# set vpn ipsec ike-group IKE-GROUP proposal 1 hash sha256
[edit]
vyos@vyos# set vpn ipsec ike-group IKE-GROUP proposal 1 dh-group 14
[edit]
vyos@vyos# set vpn ipsec ike-group IKE-GROUP lifetime 3600
[edit]
```

```
vyos@vyos# set vpn ipsec esp-group ESP-GROUP proposal 1 encryption aes256
[edit]
vyos@vyos# set vpn ipsec esp-group ESP-GROUP proposal 1 hash sha256
[edit]
vyos@vyos# set vpn ipsec esp-group ESP-GROUP lifetime 3600
[edit]
```

```
vyos@vyos# set vpn ipsec authentication psk vyos id 101.0.0.2
[edit]
vyos@vyos# set vpn ipsec authentication psk vyos id 102.0.0.2
[edit]
vyos@vyos# set vpn ipsec authentication psk vyos secret vyos
[edit]
```

```
vyos@vyos# set vpn ipsec site-to-site peer MED authentication mode pre-shared-se
cret
[edit]
vyos@vyos# set vpn ipsec site-to-site peer MED local-address 101.0.0.2
[edit]
vyos@vyos# set vpn ipsec site-to-site peer MED remote-address 102.0.0.2
[edit]
vyos@vyos# set vpn ipsec site-to-site peer MED ike-group IKE-GROUP
[edit]
vyos@vyos# set vpn ipsec site-to-site peer MED tunnel 0 esp-group ESP-GROUP
[edit]
vyos@vyos# set vpn ipsec site-to-site peer MED tunnel 0 protocol gre
[edit]
```

ROUTER MED-1

```
vyos@vyos# set interfaces tunnel tun0 encapsulation gre
[edit]
vyos@vyos# set interfaces tunnel tun0 source-address 102.0.0.2
[edit]
vyos@vyos# set interfaces tunnel tun0 remote 101.0.0.2
[edit]
vyos@vyos# set interfaces tunnel tun0 address 200.0.0.2/30
[edit]
vyos@vyos# set vpn ipsec ike-group IKE-GROUP proposal 1 encryption aes256
[edit]
vyos@vyos# set vpn ipsec ike-group IKE-GROUP proposal 1 hash sha256
[edit]
vyos@vyos# set vpn ipsec ike-group IKE-GROUP proposal 1 dh-group 14
[edit]
vyos@vyos# set vpn ipsec ike-group IKE-GROUP lifetime 3600
[edit]
vyos@vyos# set vpn ipsec esp-group ESP-GROUP proposal 1 encryption aes256
[edit]
vyos@vyos# set vpn ipsec esp-group ESP-GROUP proposal 1 hash sha256
[edit]
vyos@vyos# set vpn ipsec esp-group ESP-GROUP lifetime 3600
[edit]
vyos@vyos# set vpn ipsec authentication psk vyos id 101.0.0.2
[edit]
vyos@vyos# set vpn ipsec authentication psk vyos id 102.0.0.2
[edit]
vyos@vyos# set vpn ipsec authentication psk vyos secret vyos
[edit]
vyos@vyos# set vpn ipsec site-to-site peer CALI authentication mode pre-shared-s
ecret
[edit]
vyos@vyos# set vpn ipsec site-to-site peer CALI local-address 102.0.0.2
[edit]
vyos@vyos# set vpn ipsec site-to-site peer CALI remote-address 101.0.0.2
[edit]
vyos@vyos# set vpn ipsec site-to-site peer CALI ike-group IKE-GROUP
[edit]
vyos@vyos# set vpn ipsec site-to-site peer CALI tunnel 0 esp-group ESP-GROUP
[edit]
vyos@vyos# set vpn ipsec site-to-site peer CALI tunnel 0 protocol gre
[edit]
```

Configuración dhcp-relay

En el router MAD, se configura un DHCP Relay, que permite reenviar solicitudes de clientes DHCP desde una red donde no hay un servidor DHCP directo hacia otro servidor DHCP en otra red.

```
vyos@vyos# set service dhcp-relay server 192.168.0.3
[edit]
vyos@vyos# set service dhcp-relay listen-interface eth2
[edit]
vyos@vyos# set service dhcp-relay upstream-interface eth0
[edit]
```

Se indica que el servidor DHCP está en la dirección 192.168.0.3, MAD enviará todas las solicitudes DHCP recibidas en su red local a este servidor, eth2 tiene la dirección 172.16.0.1/24 la cual es la interfaz de la red donde están los clientes que necesitan obtener direcciones IP, eth0 es la interfaz con la dirección 12.0.0.2/30, conectada a otra red donde está el servidor DHCP.

Configuración dhcp-server

El servidor DHCP permite asignar direcciones IP automáticamente a los dispositivos en la red.

ROUTER BOG-1

```
vyos@vyos# set service dhcp-server shared-network-name LAN subnet 192.168.0.0/24
 subnet-id 1
[edit]
vyos@vyos# set service dhcp-server shared-network-name LAN subnet 192.168.0.0/24
 option default-router 192.168.0.1
[edit]
vyos@vyos# set service dhcp-server shared-network-name LAN subnet 192.168.0.0/24
 range 0 start 192.168.0.10
[edit]
vyos@vyos# set service dhcp-server shared-network-name LAN subnet 192.168.0.0/24
 range 0 stop 192.168.0.100
[edit]
```

LAN es el nombre de la red administrada por el servidor DHCP, donde se especifica la red donde se asignarán direcciones IP en este caso 192.168.0.0/24 y se define un rango de direcciones que el servidor DHCP puede asignar a los clientes, empieza en 192.168.0.10 y termina en 192.168.0.100 por lo tanto las direcciones fuera de este rango no serán asignadas automáticamente.

ROUTER PER-1

```
vyos@vyos# set service dhcp-server shared-network-name LAN subnet 10.0.0.0/24 su
bnet-id 1
[edit]
vyos@vyos# set service dhcp-server shared-network-name LAN subnet 10.0.0.0/24 op
tion default-router 10.0.0.1
[edit]
vyos@vyos# set service dhcp-server shared-network-name LAN subnet 10.0.0.0/24 ra
nge 0 start 10.0.0.10
[edit]
vyos@vyos# set service dhcp-server shared-network-name LAN subnet 10.0.0.0/24 ra
nge 0 stop 10.0.0.100
[edit]
```

LAN es el nombre de la red administrada por el servidor DHCP, donde se especifica la red donde se asignarán direcciones IP en este caso 10.0.0.0/24 y se define un rango de direcciones que el servidor DHCP puede asignar a los clientes, empieza en 10.0.0.10 y termina en 10.0.0.100 por lo tanto las direcciones fuera de este rango no serán asignadas automáticamente.

Configuración pppoe-server

PPPoE (Point-to-Point Protocol over Ethernet) permite a los clientes conectarse a Internet o a una red privada mediante autenticación. VyOS puede actuar como un servidor PPPoE para asignar direcciones IP dinámicas a los clientes.

Se crea un usuario y una contraseña con la cual los clientes tendrán que autenticarse para poder conectarse al servidor PPPoE, se especifica el protocolo de autenticación que en el caso de BAR es PAP y en MAD es CHAP (CHAP es mas seguro que PAP, ya que PAP envía la contraseña en texto plano), se define un grupo de direcciones IP, para que el router las asigne automáticamente a cada cliente PPPoE, así mismo se define la interfaz por la que se recibirá las conexiones PPPoE de los clientes, y por ultimo se define el gateway que usaran los clientes.

ROUTER MAD-1

```
vyos@vyos# set service pppoe-server authentication local-users username vyos pas
sword vyos
[edit]
vyos@vyos# set service pppoe-server authentication protocols chap
[edit]
vyos@vyos# set service pppoe-server authentication mode local
[edit]
vyos@vyos# set service pppoe-server client-ip-pool IP-POOL range 201.0.0.1/30
[edit]
vyos@vyos# set service pppoe-server default-pool IP-POOL
[edit]
vyos@vyos# set service pppoe-server interface eth1
[edit]
vyos@vyos# set service pppoe-server gateway-address 201.0.0.1
[edit]
```

ROUTER BAR-1

```
vyos@vyos# set service pppoe-server authentication local-users username vyos pas
sword vyos
[edit]
vyos@vyos# set service pppoe-server authentication protocols pap
[edit]
vyos@vyos# set service pppoe-server authentication mode local
[edit]
vyos@vyos# set service pppoe-server client-ip-pool IP-POOL range 202.0.0.1/30
[edit]
vyos@vyos# set service pppoe-server default-pool IP-POOL
[edit]
vyos@vyos# set service pppoe-server interface eth1
[edit]
vyos@vyos# set service pppoe-server gateway-address 202.0.0.1
[edit]
```

Configuración interfaces PPPOE

Las interfaces PPPoE (Point-to-Point Protocol over Ethernet) permiten que un router actúe como cliente PPPoE para conectarse a un servidor PPPoE y obtener acceso a la red o a Internet.

A cada router se le define el usuario y la contraseña para la autenticación, el servidor verificará estas credenciales para otorgar acceso, y así mismo se define la interfaz por la cual se conectará físicamente al servidor PPPoE

ROUTER BOG-1

```
vyos@vyos# set interfaces pppoe pppoe0 authentication username vyos
[edit]
vyos@vyos# set interfaces pppoe pppoe0 authentication password vyos
[edit]
vyos@vyos# set interfaces pppoe pppoe0 source-interface eth0
[edit]
```

ROUTER PER-1

```
vyos@vyos# set interfaces pppoe pppoe0 authentication username vyos
[edit]
vyos@vyos# set interfaces pppoe pppoe0 authentication password vyos
[edit]
vyos@vyos# set interfaces pppoe pppoe0 source-interface eth0
[edit]
```

Sin embargo, en esta versión de VyOS (1.5.x) existe un bug sin resolver relacionado al funcionamiento de PPPoE que resulta en un reinicio de los servicios VRF, imposibilitando el enrutamiento OSPF. La distribución de VyOS no es libre, únicamente la versión actual (Rolling reléase) es de libre acceso, en cambio, versiones anteriores requieren de una subscripción.

Configuración FIREWALL

Esta configuración en VyOS define reglas de firewall para bloquear todo el tráfico ICMP, que incluye ping y otros mensajes de control de red.

Se crea una Lista de Control de Acceso (ACL) llamada ACL-ICMP:

- Regla 10: Bloquea todo el tráfico ICMP.
- Se aplica a cualquier origen y cualquier destino (`0.0.0.0/0`).
- Cubre todos los tipos de mensajes ICMP (ping, traceroute, TTL expirado, etc.).

Se aplica el Firewall a Tráfico de Entrada (Input Filter)

Regla 10 en el input filter:

- Cualquier tráfico que intente ingresar al router MOV será evaluado por la ACL `ACL-ICMP`.
- Resultado: Todo tráfico ICMP que intente llegar al router será bloqueado.

Aplica el Firewall a Tráfico de Reenvío (Forward Filter)

Regla 10 en el forward filter:

- Todo tráfico ICMP que pase a través de MOV hacia otras redes será evaluado por `ACL-ICMP`.
- Resultado: MOV no permitirá que el tráfico ICMP pase entre redes conectadas a él.

ROUTER MOV-1

```
vyos@MOV# set firewall ipv4 name ACL-ICMP rule 10 action drop
[edit]
vyos@MOV# set firewall ipv4 name ACL-ICMP rule 10 protocol icmp
[edit]
vyos@MOV# set firewall ipv4 name ACL-ICMP rule 10 destination address 0.0.0.0/0
[edit]
vyos@MOV# set firewall ipv4 name ACL-ICMP rule 10 source address 0.0.0.0/0
[edit]
vyos@MOV# set firewall ipv4 name ACL-ICMP rule 20 action accept
[edit]
vyos@MOV# set firewall ipv4 input filter rule 10 action jump
[edit]
vyos@MOV# set firewall ipv4 input filter rule 10 jump-target ACL-ICMP
[edit]
vyos@MOV# set firewall ipv4 forward filter rule 10 action jump
[edit]
vyos@MOV# set firewall ipv4 forward filter rule 10 jump-target ACL-ICMP
[edit]
```

VERIFICACIÓN DE CONFIGURACIONES VyOS REALIZADAS

VPN GRE

En ROUTER CALI-1 la VPN GRE está establecida correctamente con el host remoto 102.0.0.2. Se ha configurado una conexión IKEv1/2 (MED) y un túnel GRE (MED-tunnel-0). La seguridad está garantizada mediante cifrado AES de 256 bits y autenticación SHA2-256.

ROUTER CALI-1

```
vyos@CALI:~$ show vpn ipsec connections
Connection    State    Type     Remote address    Local TS    Remote TS    Local
 id    Remote id    Proposal
------------  -------  -------  ----------------  ----------  -----------  -----
-----  -----------  ------------------------------------
MED           up       IKEv1/2  102.0.0.2         -           -
      %any          AES_CBC/256/HMAC_SHA2_256_128/MODP_2048
MED-tunnel-0  up       IPsec    102.0.0.2         dynamic     dynamic
      %any          AES_CBC/256/HMAC_SHA2_256_128/None
vyos@CALI:~$
```

Igualmente, en MED-1 se observa que la conexión CALI también está en estado up y utiliza el protocolo IKEv1/2 con un par remoto en la dirección 101.0.0.2. Además, hay un túnel GRE (CALI-tunnel-0), también en estado up.

ROUTER MED-1

```
vyos@MED:~$ show vpn ipsec connections
Connection     State    Type     Remote address    Local TS    Remote TS    Loca
l id    Remote id    Proposal
-------------  -------  -------  ----------------  ----------  -----------  ----
------  -----------  ----------------------------------------
CALI           up       IKEv1/2  101.0.0.2         -           -
       %any         AES_CBC/256/HMAC_SHA2_256_128/MODP_2048
CALI-tunnel-0  up       IPsec    101.0.0.2         dynamic     dynamic
       %any         AES_CBC/256/HMAC_SHA2_256_128/None
vyos@MED:~$
```

Al realizar un ping desde alguno de los routers asegurados hacia la interfaz protegida del otro, se puede verificar que el tráfico está siendo protegido usando el protocolo ESP desde la perspectiva de BOG al monitorear el tráfico.

ROUTER CALI-1

```
PING 200.0.0.2 (200.0.0.2) 56(84) bytes of data.
64 bytes from 200.0.0.2: icmp_seq=1 ttl=64 time=3.23 ms
64 bytes from 200.0.0.2: icmp_seq=2 ttl=64 time=2.15 ms
```

ROUTER BOG-1

```
vyos@BOG:~$ monitor traffic interface eth1
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eth1, link-type EN10MB (Ethernet), snapshot length 262144 bytes
13:50:44.941191 IP 101.0.0.2 > 102.0.0.2: ESP(spi=0xc4b220a2,seq=0x5d), length 1
52
13:50:44.942344 IP 102.0.0.2 > 101.0.0.2: ESP(spi=0xca664c86,seq=0x5d), length 1
52
```

VPN IPSEC

En MAD-1 VPN IPsec está correctamente establecida con el host remoto 11.0.0.2, utilizando una conexión IKEv1/2 (BAR) y un túnel IPsec (BAR-tunnel-1). La configuración permite la comunicación segura entre las subredes 172.16.0.0/24 (local) y 192.168.0.0/24 (remota), garantizando la protección del tráfico. Se emplea cifrado AES de 256 bits y autenticación SHA2-256, asegurando un alto nivel de seguridad.

ROUTER MAD-1

```
vyos@MAD: $ show vpn ipsec connections
Connection    State    Type     Remote address    Local TS        Remote TS
 Local id    Remote id    Proposal
------------  -------  -------  ----------------  -------------  --------------
 ----------  -----------  ---------------------------------------
BAR           up       IKEv1/2  11.0.0.2          -              -
             %any         AES_CBC/256/HMAC_SHA2_256_128/MODP_2048
BAR-tunnel-1  up       IPsec    11.0.0.2          172.16.0.0/24  192.168.0.0/24
             %any         AES_CBC/256/HMAC_SHA2_256_128/None
vyos@MAD:~$ _
```

En BAR-1 se observa que la conexión MAD también está en estado up, utilizando el protocolo IKEv1/2 con un par remoto en la dirección 12.0.0.2. Además, el túnel MAD-tunnel-1 también está en estado up, utilizando IPsec con tráfico entre la red local 192.168.0.0/24 y la red remota 172.16.0.0/24.

ROUTER BAR-1

```
vyos@BAR:~$ show vpn ipsec connections
Connection    State    Type     Remote address    Local TS        Remote TS
 Local id    Remote id    Proposal
------------  -------  -------  ----------------  -------------  --------------
 ----------  -----------  ---------------------------------------
MAD           up       IKEv1/2  12.0.0.2          -              -
             %any         AES_CBC/256/HMAC_SHA2_256_128/MODP_2048
MAD-tunnel-1  up       IPsec    12.0.0.2          192.168.0.0/24  172.16.0.0/24
             %any         AES_CBC/256/HMAC_SHA2_256_128/None
vyos@BAR:~$ S_
```

Al realizar un ping desde alguno de los routers asegurados hacia la interfaz protegida del otro, se puede verificar que el tráfico está siendo protegido usando el protocolo ESP desde la perspectiva de MOV al monitorear el tráfico.

ROUTER BAR-1

```
PING 172.16.0.1 (172.16.0.1) 56(84) bytes of data.
64 bytes from 172.16.0.1: icmp_seq=1 ttl=64 time=3.00 ms
64 bytes from 172.16.0.1: icmp_seq=2 ttl=64 time=2.23 ms
```

ROUTER MOV-1

```
vyos@MOV:~$ monitor traffic interface eth1
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eth1, link-type EN10MB (Ethernet), snapshot length 262144 bytes
14:00:18.397783 IP 11.0.0.2 > 12.0.0.2: ESP(spi=0xc16e2020,seq=0x14), length 136
14:00:18.398930 IP 12.0.0.2 > 11.0.0.2: ESP(spi=0xc1ffc2da,seq=0x14), length 136
```

FIREWALL

En MOV existe un firewall que desecha absolutamente todo el tráfico que use el protocolo ICMP (ping), tanto entrante, como saliente, a través de la redirección de ambos hacia el firewall ACL-ICMP que filtra todo el tráfico ICMP desde cualquier origen hacia cualquier destino (0.0.0.0/0). Esto puede ser verificado al hacer ping desde alguno de los routers adyacentes hacia el otro sin usar una interfaz protegida por Ipsec.

ROUTER BAR-1

```
vyos@BAR:~$ ping 12.0.0.1
PING 12.0.0.1 (12.0.0.1) 56(84) bytes of data.
^C
--- 12.0.0.1 ping statistics ---
18 packets transmitted, 0 received, 100% packet loss, time 17393ms
```

ROUTER MOV-1

```
vyos@MOV:~$ monitor traffic interface eth1
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eth1, link-type EN10MB (Ethernet), snapshot length 262144 bytes
^C14:08:07.568328 IP 11.0.0.1 > 224.0.0.5: OSPFv2, Hello, length 48

1 packet captured
25 packets received by filter
16 packets dropped by kernel
```

Prueba de conectividad Server-1

El servidor está conectado correctamente a la red, pues puede realizar un ping a la red LAN del router MAD. Además, está ejecutando correctamente los servicios.

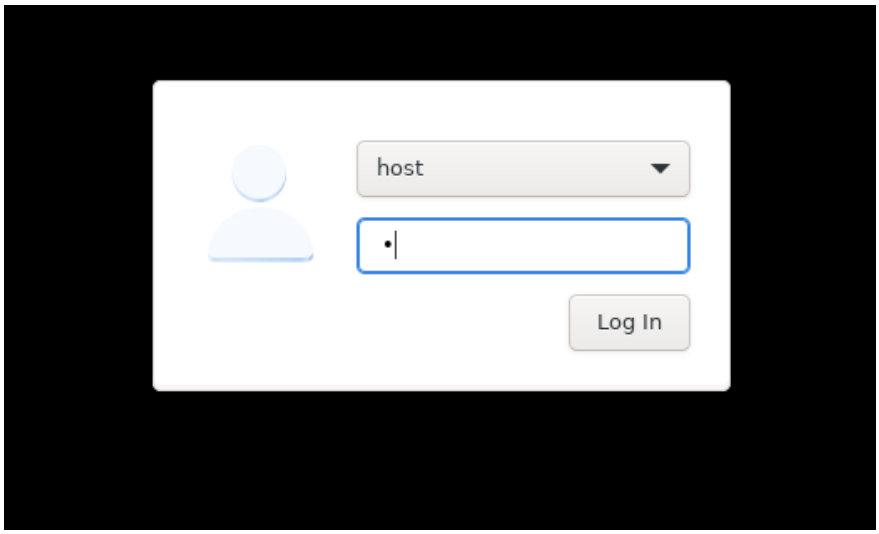
Servidor Server-1

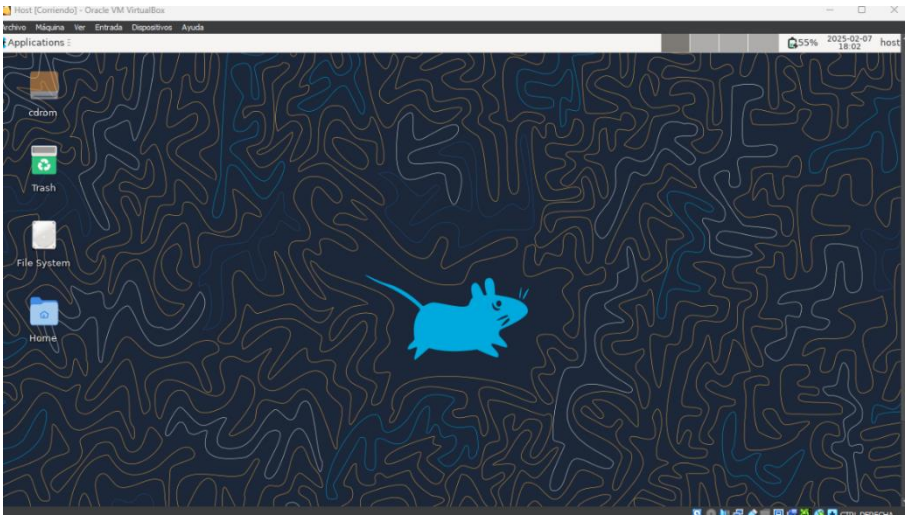
```
localhost:~# rc-service named status
 * status: started
localhost:~# rc-service dhcpd status
 * status: started
localhost:~# httpd status
httpd: bind: Address in use
localhost:~# ping 172.16.0.1
PING 172.16.0.1 (172.16.0.1): 56 data bytes
64 bytes from 172.16.0.1: seq=0 ttl=63 time=46.598 ms
64 bytes from 172.16.0.1: seq=1 ttl=63 time=4.448 ms
64 bytes from 172.16.0.1: seq=2 ttl=63 time=4.402 ms
64 bytes from 172.16.0.1: seq=3 ttl=63 time=13.590 ms
```

Prueba de conectividad Host-1

El cliente está correctamente configurado. Cuenta con una interfaz gráfica a través de la cual puede accederse a la página web ofrecida por el servidor.

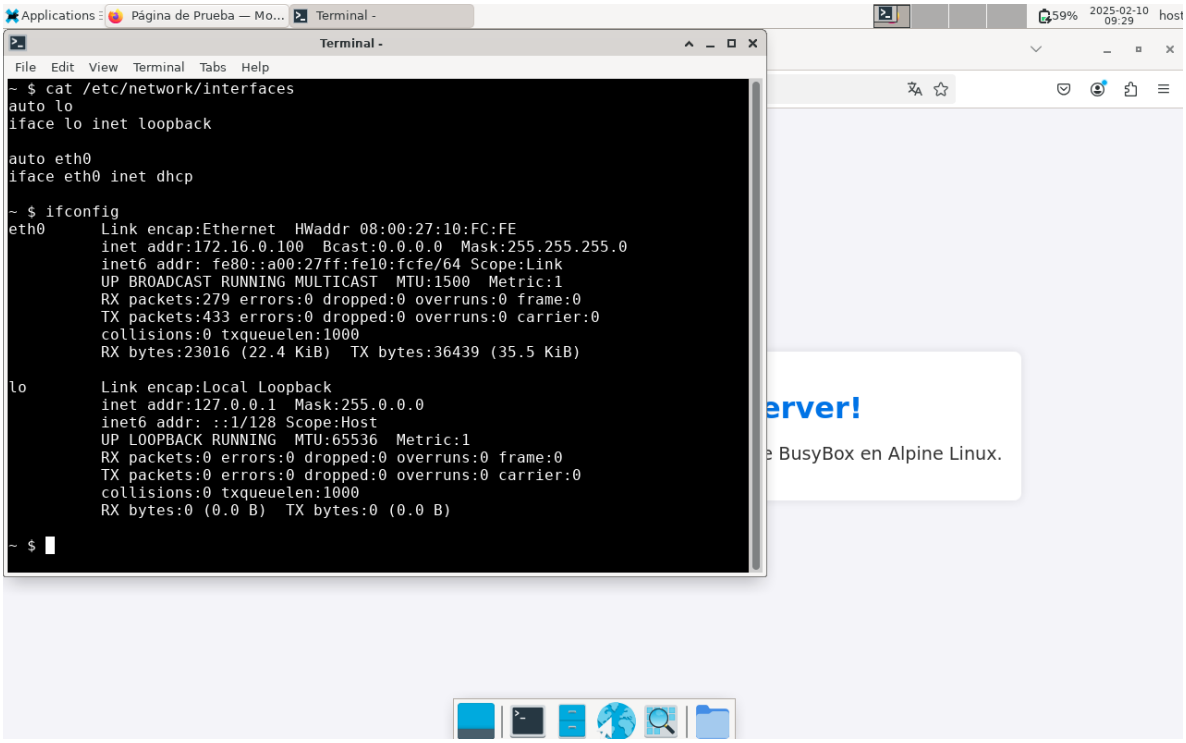
Cliente Host-1

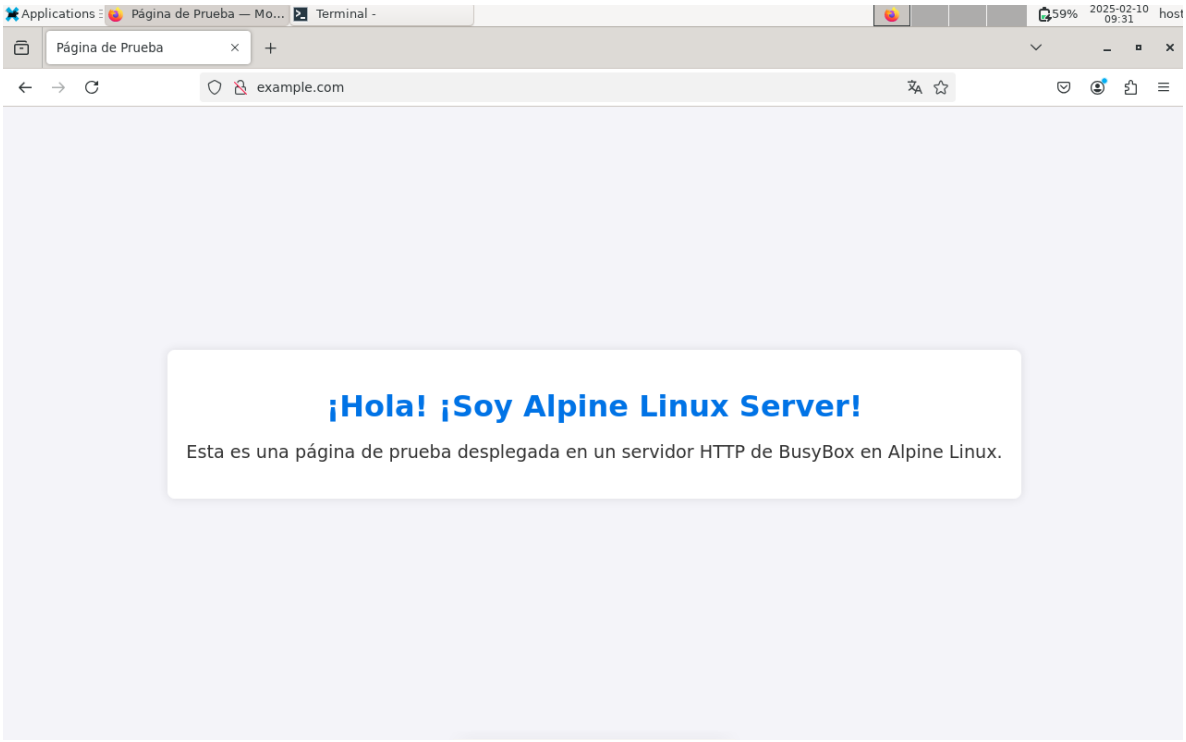




Al ejecutar los comandos `cat /etc/network/interfaces` y `ifconfig` es posible verificar que la interfaz eth0 está configurada para recibir una dirección IP a través del protocolo DHCP y que ha recibido la dirección 172.16.0.100, el Gateway 172.168.0.1 y el DNS 192.168.0.3. Al visitar la página example.com, ofrecida por el servidor, se puede verificar el correcto funcionamiento de los servicios DNS y HTTP ofrecidos por el servidor.

Cliente Host-1





CONCLUSIONES

La implementación de una topología protegida utilizando VyOS y Alpine Linux permitió validar la configuración y el funcionamiento de diferentes mecanismos de seguridad y control de

acceso en redes. La integración de firewalls, VPNs y protocolos de enrutamiento como OSPF son efectivos para la segmentación y protección del tráfico, asegurando la integridad de las comunicaciones.

El uso de túneles GRE sobre IPsec permitió establecer conexiones seguras entre redes remotas, garantizando la confidencialidad de los datos. Asimismo, la configuración de servidores DHCP y DNS en Alpine Linux facilitó la gestión de direcciones IP y la resolución de nombres en la red, comprobando su operatividad mediante pruebas de conectividad y acceso a servicios web.

Sin embargo, se identificaron limitaciones en la implementación de PPPoE en VyOS 1.5.x, ya que un error en esta versión ocasiona la interrupción de los servicios VRF, afectando el enrutamiento OSPF. Esta situación evidencia la importancia del acceso libre a versiones anteriores del software, ya que la restricción impuesta por VyOS a sus versiones estables dificulta la implementación en entornos educativos y de prueba. De manera similar, la última versión de Alpine Linux no permite la configuración de un servidor DHCP, lo que obligó a utilizar una versión anterior para el despliegue del laboratorio.

Por último, el proyecto permitió aplicar los conocimientos adquiridos en el curso de Redes III en un entorno práctico, fortaleciendo la comprensión de los mecanismos de seguridad en redes basadas en SDN. La experiencia adquirida en la configuración y gestión de VyOS, junto con el uso de herramientas de simulación como GNS3, proporciona una base sólida para el desarrollo de infraestructuras de red seguras y eficientes en futuros escenarios profesionales.

RECURSOS

[1] Sistema Operativo VyOS. Disponible en https://github.com/vyos/vyos-rolling-nightly-builds/releases

[2] Software de simulación GNS3. Disponible en https://www.gns3.com/software/download
[3] Gestor de máquinas virtuales Oracle VM VirtualBox. Disponible en https://www.virtualbox.org/wiki/Downloads

[4] Distribución Alpine Linux Virtual 3.20.0 Disponible en https://dl-cdn.alpinelinux.org/alpine/v3.20/releases/x86_64/alpine-virt-3.20.0-x86_64.iso

BIBLIOGRAFÍA

[5] Guía de Usuario de VyOS. Disponible en https://docs.vyos.io/es/latest/

[6] Túnel — documentación de VyOS - 1.5.x (circinus). VyOS User Guide — VyOS 1.4.x (sagitta)documentation. Disponible en https://docs.vyos.io/es/latest/configuration/interfaces/tunnel.html#generic-routing-encapsulation-gre

[7] PPPoE — documentación de VyOS - 1.5.x (circinus). VyOS User Guide — VyOS 1.4.x (sagitta) documentation. Disponible en https://docs.vyos.io/es/latest/configuration/interfaces/pppoe.html

[8] OSPF — documentación de VyOS - 1.5.x (circinus). VyOS User Guide — VyOS 1.4.x (sagitta) documentation. Disponible en https://docs.vyos.io/es/latest/configuration/protocols/ospf.html

[9] IPv4 Firewall Configuration — documentación de VyOS - 1.5.x (circinus). VyOS User Guide — VyOS 1.4.x (sagitta) documentation. Disponible en https://docs.vyos.io/es/latest/configuration/firewall/ipv4.html

[10] Configuring pppoe dial-up, ospf cannot be opened. VyOS Forums. Disponible en https://forum.vyos.io/t/configuring-pppoe-dial-up-ospf-cannot-be-opened/15889