

**Proyecto Final de seguridad y Auditoria**  
**Universidad Mariano Gálvez Sede de Boca del Monte**  
**David Alejandro Serrano Salazar 7690-13-19355**  
**Ervin Gabriel Laferre Guevara 7690-16-10153**  
**Guatemala, 06 de noviembre de 2021**

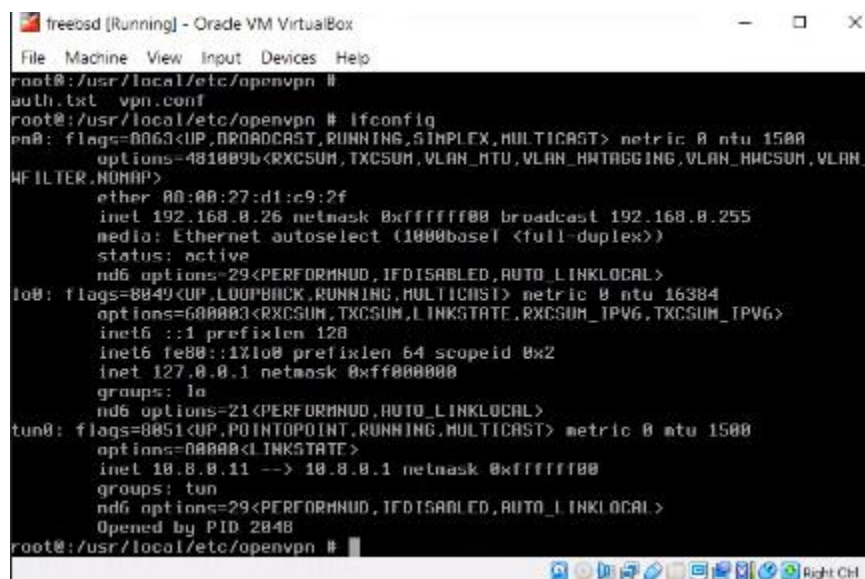
**Configuración de las maquinas asignadas:**

Cada una de las maquinas virtuales que instalamos están relacionadas con una IP estática que se le dio por medio del PFSENSE que actuara tanto como nuestro servidor de VPN como nuestro FIREWALL.

10.8.0.9	ervin
10.8.0.4	BD
10.8.0.10	david
10.8.0.7	AD

**Servidor FREEDSB**

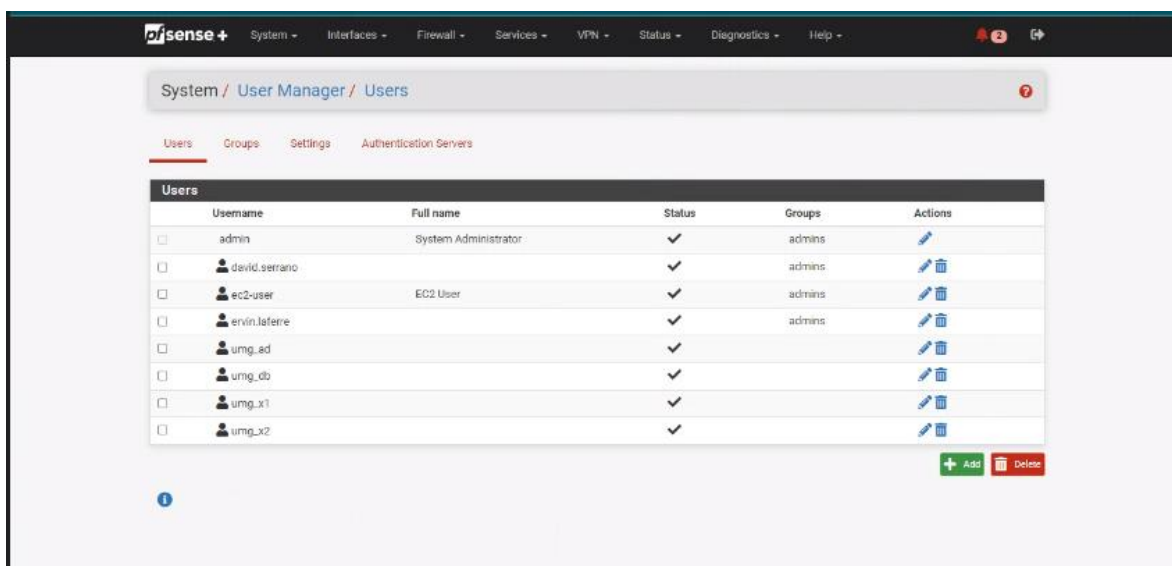
Como vemos tiene una IP asignada por medio de nuestra VPN como su IP local.



```
freebsd [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
root@:/usr/local/etc/openvpn #
auth.txt vpn.conf
root@:/usr/local/etc/openvpn # ifconfig
en0: flags=8063<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
    options=481009b<RXCSUM, TXCSUM, VLAN_MTU, VLAN_HWTAGGING, VLAN_HWCSUM, VLAN_
    AFILTER, NOMAP>
    ether 00:00:27:d1:c9:2f
    inet 192.168.0.26 netmask 0xfffff000 broadcast 192.168.0.255
    media: Ethernet autoselect (1000baseT <full-duplex>)
    status: active
    nd6 options=29<PERFORMNUD, IFDISABLED, AUTO_LINKLOCAL>
lo0: flags=8849<UP,LOOPBACK,RUNNING,MULTICAST> metric 0 mtu 16384
    options=6000003<RXCSUM, TXCSUM, LINKSTATE, RXCSUM_IPV6, TXCSUM_IPV6>
    inet6 ::1 prefixlen 128
    inet6 fe80::1%lo0 prefixlen 64 scopeid 0x2
    inet 127.0.0.1 netmask 0xff000000
    groups: lo
    nd6 options=21<PERFORMNUD, AUTO_LINKLOCAL>
tun0: flags=8051<UP,POINTOPOINT,RUNNING,MULTICAST> metric 0 mtu 1500
    options=00000<LINKSTATE>
    inet 10.8.0.11 --> 10.8.0.1 netmask 0xfffff000
    groups: tun
    nd6 options=29<PERFORMNUD, IFDISABLED, AUTO_LINKLOCAL>
    Opened by PID 2848
root@:/usr/local/etc/openvpn #
```

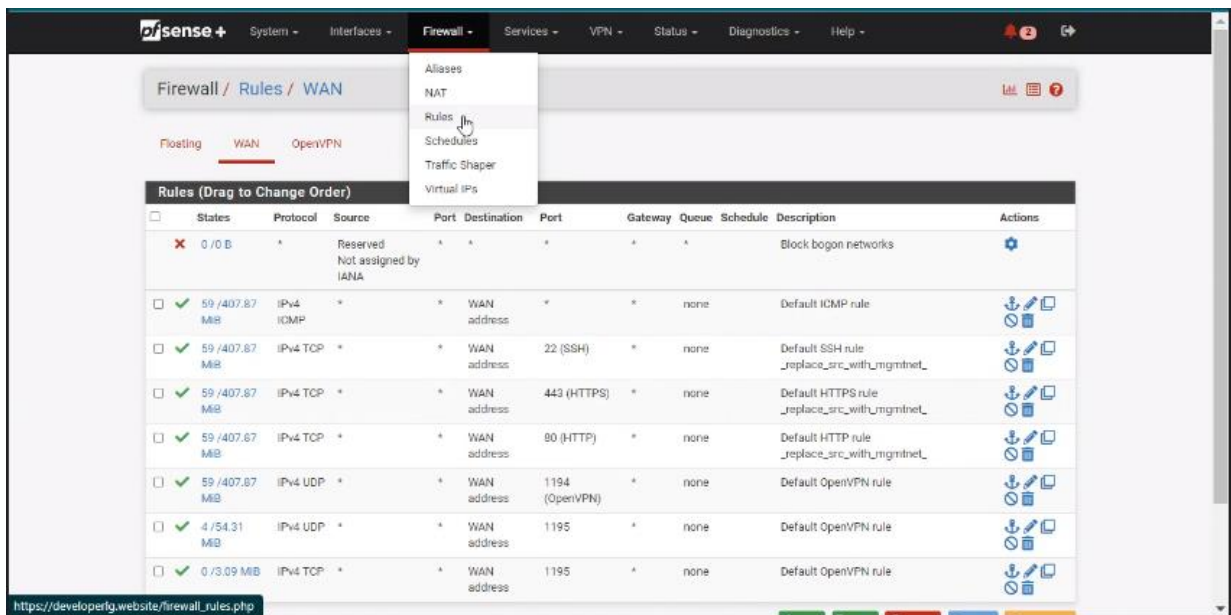
## CONFIGURACION DEL FIREWALL.

Como vemos existen varios usuarios que se crearon para tener distintos accesos y niveles de seguridad dependiendo el tipo de usuario que tengamos, asimismo se entablaron grupos que son administrador para que se puedan modificar desde cualquier maquina y no solo se dependa de una persona para realizar dicha configuración, en esta pantalla para agregar permisos bastaría con agregar (botón verde) y la ventana que levanta ingresar los datos requeridos y seleccionar si es administrador o no.



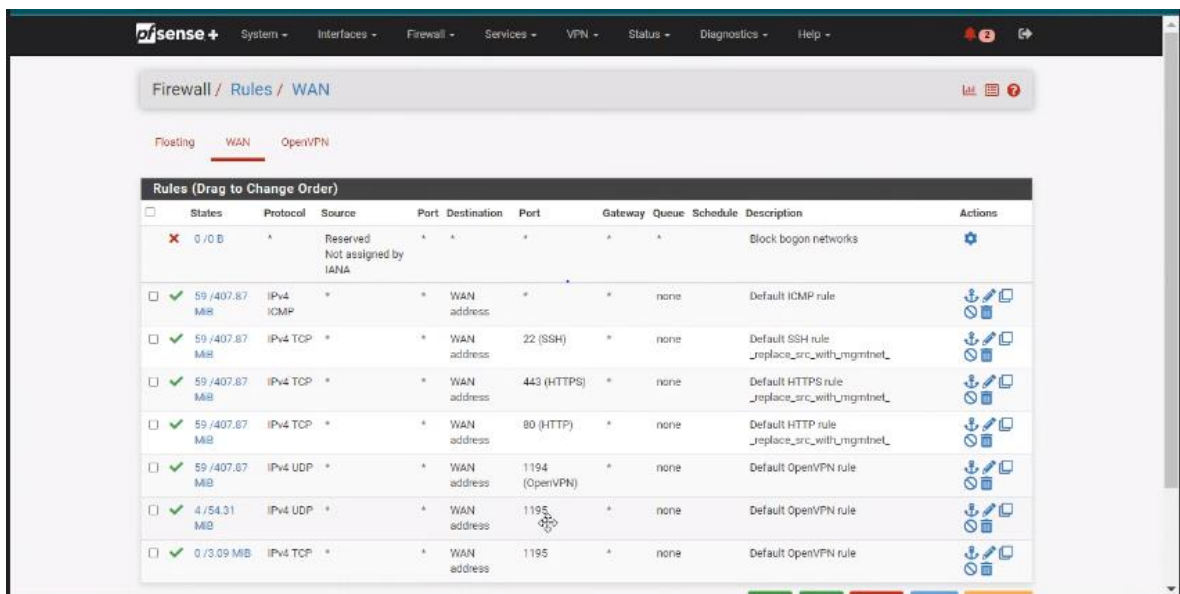
## CONFIGURACION DE REGLAS.

Para configurar las reglas dentro del firewall nos vamos a la barra de menú y encontraremos la parte de FIREWALL, pinchamos en ella. Y nos desplegara una tabla con todas las reglas configuradas a cada uno de los usuarios, donde hemos podido denegar el trafico especifico a una página, así como a una sección de IPS para prohibir el uso de redes sociales, la cual esta regla se puede activar a una cantidad infinita de usuario, también hemos permitido el acceso y denegar el acceso a la pagina de la UMG con la finalidad de probar esta.



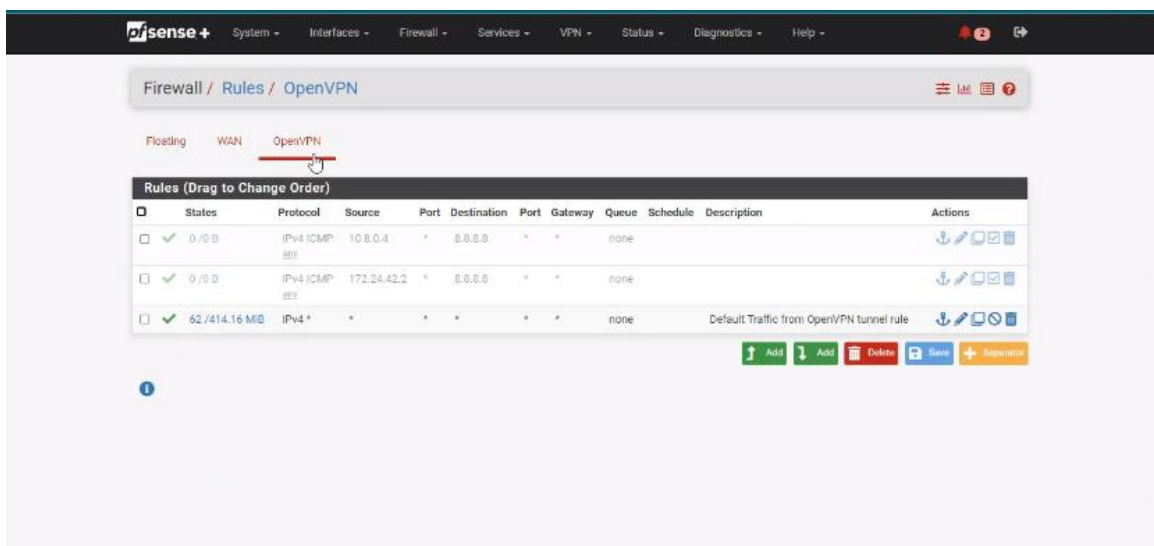
## CONFIGURACION DE IP PUBLICA

La configuración de cada una de estas IPS es necesaria para el funcionamiento de la VPN, con la cual, una nos servirá para la red interna que creará la VPN y la otra nos servirá para la salida del internet.



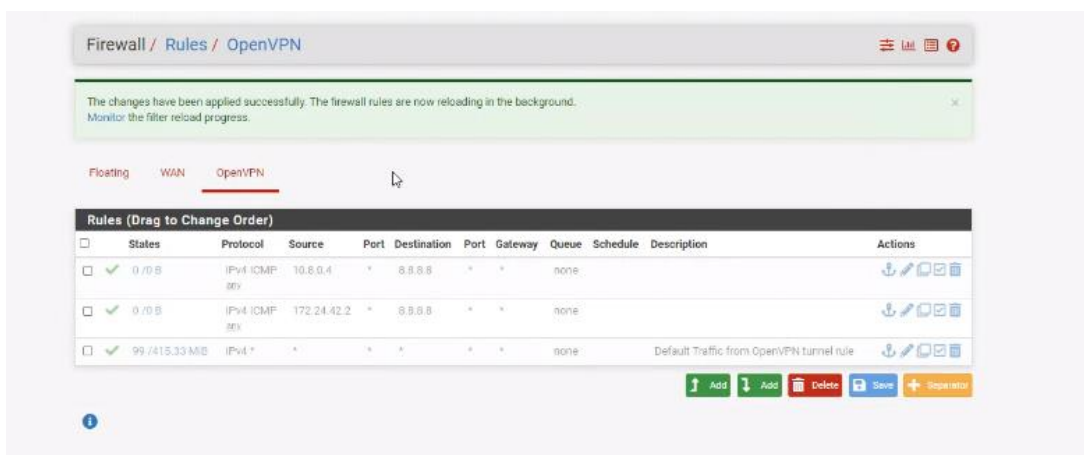
## CONFIGURACION DE IP PRIVADA

Ya una vez dentro creamos reglas de comportamiento. Una sola regla activa para todos lados de ida y vuelta la configuración, como puede ser el caso del internet, o puertos específicos para conexiones, tal es el caso de algunos servicios como Microsoft Teams, Meet, Skype entre otros.



## CONFIGURACION DE IP PRIVADA

Cada vez que realizamos una actualización del firewall sin importar la acción que estemos realizando nos encontraremos con el siguiente escenario al momento de darle guardar para activar las reglas nos saldrá un mensaje de confirmación para validar que estemos de acuerdo y si lo estamos nos saldrá el mensaje que vemos a continuación, indicando que la reglas han sido aplicadas inmediatamente se puede visualizar en los clientes estos cambios.



## PRUEBAS DE LAS REGLAS IMPLEMENTADAS

Como describimos en la parte de arriba el servidor tiene la IP con terminación 7 en las reglas del FIREWALL, indicamos que se podía enviar paquetes ICMP, como podemos visualizar en la siguiente imagen

```
C:\Users\dserrano>ping 10.8.0.7

Haciendo ping a 10.8.0.7 con 32 bytes de datos:
Respuesta desde 10.8.0.7: bytes=32 tiempo=333ms TTL=127
Respuesta desde 10.8.0.7: bytes=32 tiempo=320ms TTL=127
Respuesta desde 10.8.0.7: bytes=32 tiempo=326ms TTL=127
Respuesta desde 10.8.0.7: bytes=32 tiempo=345ms TTL=127

Estadísticas de ping para 10.8.0.7:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 320ms, Máximo = 345ms, Media = 331ms
```

Luego de esto realizamos una actualización de esta regla activando una restricción completa a la red que no puedan enviar este tipo de paquetes, como vemos en la imagen continua no ha recibido ningún paquete, todos se perdieron.

```
C:\Users\dserrano>ping 10.8.0.7

Haciendo ping a 10.8.0.7 con 32 bytes de datos:
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.

Estadísticas de ping para 10.8.0.7:
    Paquetes: enviados = 4, recibidos = 0, perdidos = 4
    (100% perdidos),
```

## CREACION DE REGLAS DENTRO DEL FIREWALL

En el apartado de Firewall, existe un botón color verde que indica agregar (ADD), en el cual nos dará una ventana donde podemos configurar las reglas que creamos necesarias e indicar el usuario o los usuarios que afectará esta regla, en la imagen siguiente, veremos el ejemplo de la creación de una de estas para que la cualquier IP pueda visualizar el SERVIDOR ADD.

Firewall / Rules / Edit

### Edit Firewall Rule

**Action** Pass  
Choose what to do with packets that match the criteria specified below.  
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

**Disabled** ☒ Disable this rule  
Set this option to disable this rule without removing it from the list.

**Interface** OpenVPN  
Choose the interface from which packets must come to match this rule.

**Address Family** IPv4  
Select the Internet Protocol version this rule applies to.

**Protocol** ICMP  
Choose which IP protocol this rule should match.

**ICMP Subtypes** Any  
Alternate Host  
Datagram conversion error  
Echo reply  
For ICMP rules on IPv4, one or more of these ICMP subtypes may be specified.

---

**Source**

Source ☐ Invert match Single host or alias 10.8.0.10 /

**Destination**

Destination ☐ Invert match Single host or alias 10.8.0.7 /

**Extra Options**

**Log** ☒ Log packets that are handled by this rule  
Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the Status: System Logs: Settings page).

**Description** Permiso a David de acceso al AD  
A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.

**Advanced Options** [Display Advanced](#)

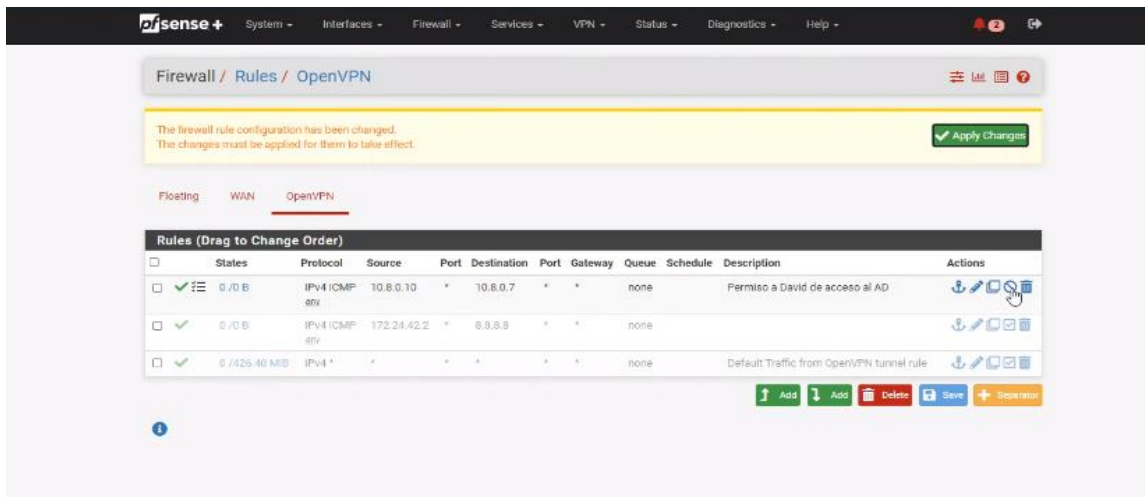
---

**Rule Information**

Tracking ID	1636142713
Created	11/5/21 20:05:13 by admin@181.174.106.84 (Local Database)
Updated	11/5/21 20:09:40 by admin@181.174.106.84 (Local Database)

[Save](#)

Una vez llenamos todos los campos que hemos visto en la imagen, pinchamos en el botón de guardar, y nos regresara a la pantalla anterior donde estarán todas las reglas listadas dentro de la tabla, está actualmente creada aparecerá desactivada y lo único que tendríamos que realizar es la activación de dicha regla, para que este vigente.



Como vimos anteriormente el mensaje de aplicar cambios nos aparecerá y luego se activará, otro ejemplo que pudimos realizar es la restricción de internet a la IP que se conecte en este caso bloqueamos la IP de Google.

```
C:\Users\dserrano>ping www.google.com

Haciendo ping a www.google.com [142.250.64.196] con 32 bytes de datos:
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.

Estadísticas de ping para 142.250.64.196:
    Paquetes: enviados = 4, recibidos = 0, perdidos = 4
    (100% perdidos),
```

Luego la desactivamos y vemos que es sencillo realizar reglas en el firewall para limitar el acceso a internet o algún segmento específico de la red.

```
C:\Users\dserrano>ping www.google.com

Haciendo ping a www.google.com [142.250.64.196] con 32 bytes de datos:
Respuesta desde 142.250.64.196: bytes=32 tiempo=231ms TTL=101
Respuesta desde 142.250.64.196: bytes=32 tiempo=223ms TTL=101
Respuesta desde 142.250.64.196: bytes=32 tiempo=237ms TTL=101
Respuesta desde 142.250.64.196: bytes=32 tiempo=231ms TTL=101

Estadísticas de ping para 142.250.64.196:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 223ms, Máximo = 237ms, Media = 230ms
```