

Seguridad y Auditoria de Sistemas

Ing. Melvin Kalí

5 de noviembre de 2021



Universidad Mariano Gálvez

FACULTAD DE INGENIERÍA EN SISTEMAS

PROYECTO FINAL

Configuración de pfSense Firewall

Integrantes del Grupo:

Rogelio Alfonso Alvarez Girón – 7690-98-2290

Gari Lester Mendoza Bedoya – 7690-17-14228

Selvin Omar Castellanos Solares 7690-17-14269

Noviembre 2021

Parte I

Configurando pfSense

Configuraciones realizadas

A continuación veremos una serie de pasos que nos llevaron a configurar de una forma eficiente y segura el Firewall pfSense en nuestra red físico/virtual.

Instalación del Firewall

Instalando pfSense Firewall:

- Hacemos boot en el equipo y en pocos segundos comienza la carga.
- Aceptamos la licencia de uso y no distribución comercial presionando Enter
- Llegamos al menú de bienvenida y contamos con 3 opciones
 1. Install: Comenzar los pasos de instalación (la que usaremos en este artículo)
 2. Rescue Shell: Caer en el prompt del OS FreeBSD y realizar por comandos tareas de rescate o administración de nuestro cortafuegos
 3. Recover config.xml: Restaurar un config.xml en un pfSense dañado o con problemas. Una forma útil de recuperarnos de un desastre

Presionamos Enter sobre Install

- Veremos un listado de distribuciones de teclado donde por medio del cursor bajaremos y buscaremos la que necesitamos.
- En nuestro caso usaremos Latin American.
- Presionamos Enter para marcarlo
- De regreso al comienzo del listado podemos probar la distribución del teclado.
- Usando la opción Test latinamerican.kbd keymap y despejar alguna duda de si es o no la que necesitamos.
- Para continuar la instalación presionamos ENTER sobre –Continue with latinamerican.kbd keymap–

Parte II

Particionando disco de PfSense

Descripción

El asistente nos da 4 opciones para particionar el disco donde instalaremos

- Auto (UFS): La opción default, más sencilla, solo utilizara un disco
- Manual: Particionaremos de forma manual, ideal para los casos en que compartiremos espacio con otra partición que no queremos eliminar
- Shell: Realizar el particionado por línea de comandos en el shell
- Auto (ZFS): Particionado con filesystem ZFS en 3 o mas discos, alta disponibilidad, mejor performance.

Bajamos con el cursor a Auto (ZFS) y presionamos Enter

La configuracion de ZFS puede parecer intimidante con tantas opciones pero no es de preocuparse, básicamente necesitamos solo decirle cuantos discos usaremos presionando Enter sobre T Pool Type/Disk En la siguiente ventana veremos el listado de modos a elegir uno.

Algo muy útil, si tienes dudas de cual es el que puedes usar, con el cursor al pararte sobre una opción en la parte inferior te dice cuantos discos debes tener para su uso (Nota: los discos deben ser del mismo tamaño, de ponerle un disco mayor vas a malgastar el espacio extra).

Presionamos Enter

-Nos aparece el listado de discos, los marcamos con la tecla Espacio y presionamos Enter sobre OK para continuar

-De regreso a la ventana de configuracion de ZFS Configuration podríamos hacer otros cambios.

La recomendación, a no ser que lo necesiten, es que usen los valores default.

Presionamos Enter sobre Install

-Confirmamos el proceso presionando Enter sobre YES

-Comienza la instalación en disco.

-Si se quiere hacer algún otro cambio se puede hacer desde el shell por medio de comandos?

Presionamos Enter sobre No, para continuar

-Llegamos al final de la instalación.

Presionamos Enter sobre Reboot para reiniciar el equipo.

Quitamos el medio de instalación

Parte III

Configuración IP en pfSense

Descripción

-Apenas reiniciamos nuestro cortafuegos veremos la consola con opciones y las tarjetas de red auto configuradas.

Para este artículo en su modo básico (WAN y LAN) vemos que la WAN por default toma ip via DHCP (ideal para un esquema de cable modem o router de un ISP que asigne una ip).

La LAN se configura automáticamente con la 192.168.1.1.

Presionamos 2 y Enter

-Se nos da a elegir cual interfaz de red modificaremos, en este caso para cambiar la LAN elegimos 2 y presionamos Enter.

Seguidamente escribimos la IP que queremos activarle en la LAN. Debes saber que esta sera la ip de puerta de salida o gateway a configurar en los equipos de tu LAN.

Dependiendo de tu esquema de red, elegimos la mascara, en mi caso usare 24 y presionamos Enter

-Como estamos modificando la IP LAN, en el siguiente paso no escribimos nada y presionamos Enter.

Si estuviéramos modificando WAN escribiríamos la ip del gateway o puerta de salida, generalmente una ip del router de nuestro proveedor internet.

Se nos pregunta si queremos revertir el protocolo para conectarnos via web, respondemos que n y presionamos Enter.

-El asistente nos confirma la activación de la nueva IP LAN y nos da el URL al que podemos acceder desde la LAN para su interfaz web.

Acceso al dashboard pfSense

-Para acceder via web a nuestro cortafuegos abrimos un browser y navegamos a su URL `https://IP-LAN-pfSense`.

Recuerda que la ip por default LAN sera 192.168.1.1 pero si la modificaste la puedes confirmar en la consola texto.

Como el certificado SSL es auto firmado (es decir, no esta firmado por una entidad reconocida en internet dedicado a esto) tu navegador te puede dar un error .

No hay problema, damos click a Ocultar detalles avanzados y después a Continuar a 192.168.5.10 (no seguro).

En cualquier otro caso la IP seguramente será otra la ip

-Ingresamos por primera vez via web a pfSense, para eso usaremos los siguientes datos de usuario:

- usuario:
- contraseña:

Y presionamos Enter o damos click al botón Sign in

Parte IV

Setup pfSense

Descripción

-La primera vez que ingresemos via web a pfSense se ejecutara el Wizard pfSense Setup, usted elije si lo desea utilizar.

Este consta de 8 pasos desde el Inicio del wizard pfSense Setup.

1. Ofrecimiento del soporte pago Netgate Global Support
2. Información general de nuestro cortafuegos
3. Activación de zona horaria para fecha y hora
4. Configuración interface WAN
5. Configuración interface LAN
6. Cambio de contraseña del usuario admin
7. Activar cambios.
8. Nuevamente se ofrece el soporte de Netgate finalizando el wizard

Iniciamos el asistente.

Damos click al botón Next.

-En el primer paso se nos ofrece el soporte Netgate.

En caso de interesarte encontraras mas información dando click al botón Learn More.

Damos click al botón Next para continuar.

-Segundo paso, activamos el hostname y dominio de nuestro firewall ademas de los DNS primario y secundario.

Damos click al botón Next

. -Es importante que la fecha y hora de tu firewall estén sincronizados.

Eso lo hacemos en el tercer paso activando nuestra zona horaria en el campo Timezone.

Damos click al botón Next.

-Posiblemente el paso mas importante, el cuarto, donde configuraremos nuestra interfaz WAN.

Dependiendo de tu tipo de conexión sera la configuracion que harás.

Si usas DHCP para conectar tu pfSense Firewall a internet, entonces solo debes hacer ese cambio en el campo SelectType.

En caso de querer configurar otro tipo de conexión, se habilitaran otros campos a configurar.

Damos click al botón Next.

-Quinto paso, solo confirmar la IP LAN y su mascara.

Damos click al botón Next.

-No menos importante, en el sexto paso cambiamos la contraseña de la cuenta admin usada para conectarse al dashboard pfSense.

Damos click al botón Next.

-Realmente son 7 pasos, al llegar al séptimo paso ya habremos terminado, solo nos queda darle click al botón Reload para activar cambios.

-Es importante saber que no es permitido distribuir de forma comercial el software pfSense.

Aceptamos dando click al botón Accept.

-El dashboard web de pfSense Firewall es modular y en forma de bloques que nos irán dando información.

Parte V

Ilustraciones sobre la configuración

Imagen 1

```
Firewall [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
0) Shell
La máquina virtual informa que el SO invitado no soporta integración del ratón en el modo de vídeo actual. Se necesita capturar e
Enter an option:

FreeBSD/amd64 (pfSense.home.arpa) (ttyv0)
VirtualBox Virtual Machine - Netgate Device ID: ab48a3f443202c28a426
*** Welcome to pfSense 2.5.2-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4/DHCP4: 192.168.0.10/24
                v6/DHCP6: ::a00:27ff:fe29:58fb/64

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults    13) Update from console
5) Reboot system               14) Enable Secure Shell (sshd)
6) Halt system                 15) Restore recent configuration
7) Ping host                   16) Restart PHP-FPM
8) Shell

Enter an option: 
```

Figura 1: pfSense corriendo en la máquina virtual

Imagen 2

The screenshot shows the pfSense Community Edition web interface. At the top, there's a navigation bar with the pfSense logo and menu items: System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help. A warning message is displayed: "WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager." Below this, the "Status / Dashboard" section is active. The main content area is divided into two columns. The left column, titled "System Information", contains a table with the following data:

Name	pfSense.home.arpa
User	admin@192.168.0.4 (Local Database)
System	VirtualBox Virtual Machine Netgate Device ID: ab48a3f443202c28a426
BIOS	Vendor: innotek GmbH Version: VirtualBox Release Date: Fri Dec 1 2006
Version	2.5.2-RELEASE (amd64) built on Fri Jul 02 15:33:00 EDT 2021 FreeBSD 12.2-STABLE The system is on the latest version. Version information updated at Sat Oct 23 15:26:20 UTC 2021
CPU Type	Intel(R) Core(TM) i5-7200U CPU @ 2.50GHz AES-NI CPU Crypto: Yes (inactive)

The right column, titled "Netgate Services And Support", shows the "Contract type" as "Community Support". Below this, there's a section for "NETGATE AND pfSense COMMUNITY" with text about purchasing pfSense gateway firewall and access to the "NETGATE RESOURCE LIBRARY". It also mentions upgrading to a Netgate Global Technical Support subscription. At the bottom, there are links for "Upgrade Your Support", "Community Support", "Netgate Global Support FAQ", and "Official Documentation".

Figura 2: pfSense en el navegador

Imagen 3

Create / Edit CA

Descriptive name

VPN_CA

Method

Import an existing Certificate Authority

Trust Store

☐ Add this Certificate Authority to the Operating System Trust Store

When enabled, the contents of the CA will be added to the trust store so that they will be trusted by the operating system.

Randomize Serial

☐ Use random serial numbers when signing certifies

When enabled, if this CA is capable of signing certificates then serial numbers for certificates signed by this CA will be automatically random checked for uniqueness instead of using the sequential value from Next Certificate Serial.

Existing Certificate Authority

Certificate data

-----BEGIN CERTIFICATE-----
MIID/jCCAuagAwIBAgIIXHNW8Fh4Ro4wDQYJKoZIhvcNAQELBQAwWT
EPMA0GA1UE
AxMGVlBOLUNBMQswCQYDVQQGEwJOUDEKMAgGA1UECBMBMzERMA8GA1
UEBxMITGFs

Paste a certificate in X.509 PEM format here.

Certificate Private Key
(optional)

-----BEGIN PRIVATE KEY-----
MIIEvAIBADANBgkqhkiG9w0BAQEFAASCByggSiAgEAAoIBAQCcx
3HNf6CvSwP
dERI9YNArLFSkzz8oZg6NG7074LjMJ+nGUtrbsCoASf1Z2S/GFUx3
/20D5uc6Cg

Paste the private key for the above certificate here. This is optional in most cases, but is required when generating a Certificate Revocation Li

Next Certificate Serial

3

Enter a decimal number to be used as a sequential serial number for the next certificate to be signed by this CA

Figura 3: Certificado del Servidor para crear nuevos certificados a usuarios

15

Imagen 4





























































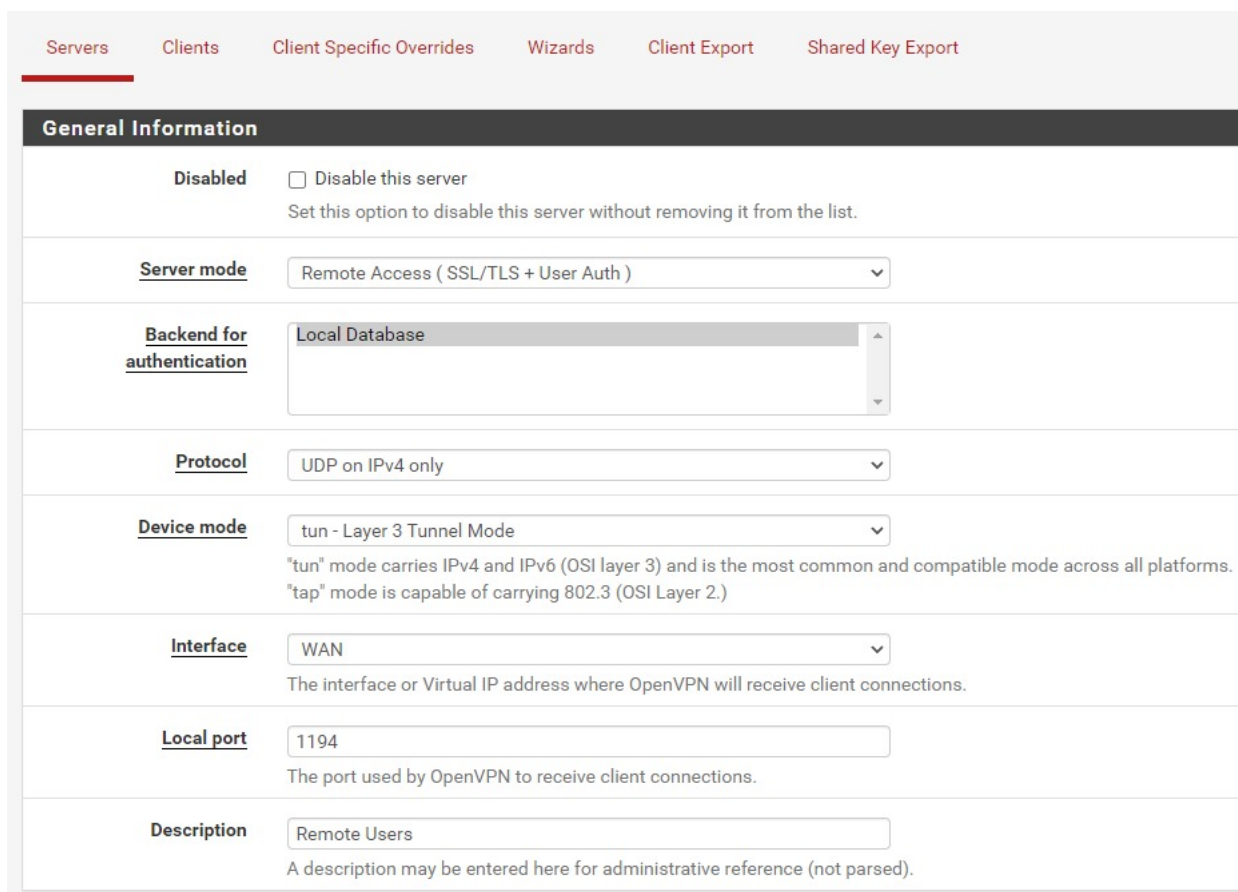
<div> <div>CAs</div> <div>Certificates</div> <div>Certificate Revocation</div> </div>																													
<div> <div>Search</div> <div> <div>Search term</div> <div></div> <div>Both</div> <div>Search</div> <div>Clear</div> </div> <div>Enter a search string or *nix regular expression to search certificate names and distinguished names.</div> </div>																													
<div> <div>Certificates</div> <table> <tr> <th>Name</th><th>Issuer</th><th>Distinguished Name</th><th>In Use</th><th>Actions</th></tr> <tr> <td>webConfigurator default (6172cc2aaf4d0) Server Certificate CA: No Server: Yes</td><td>self-signed</td><td>O=pfSense webConfigurator Self-Signed Certificate, CN=pfSense-6172cc2aaf4d0 Valid From: Fri, 22 Oct 2021 14:35:22 +0000 Valid Until: Thu, 24 Nov 2022 14:35:22 +0000</td><td>webConfigurator</td><td></td></tr> <tr> <td>DEMO_Cert Server Certificate CA: No Server: Yes</td><td>VPN_CA</td><td>ST=3, OU=IT, O=DEMO, L=Laltipur, CN=VPN_Certificate, C=NP Valid From: Fri, 22 Oct 2021 20:39:29 +0000 Valid Until: Mon, 20 Oct 2031 20:39:29 +0000</td><td>OpenVPN Server</td><td></td></tr> <tr> <td>VPN_Client_Cert User Certificate CA: No Server: No</td><td>VPN_CA</td><td>ST=3, OU=IT, O=DEMO, L=Laltipur, CN=demovpn, C=NP Valid From: Fri, 22 Oct 2021 20:58:11 +0000 Valid Until: Mon, 20 Oct 2031 20:58:11 +0000</td><td>User Cert</td><td></td></tr> <tr> <td>VPN_Client_Cert2 User Certificate CA: No Server: No</td><td>VPN_CA</td><td>ST=3, OU=IT, O=DEMO, L=Laltipur, CN=gari, C=NP Valid From: Fri, 22 Oct 2021 21:58:36 +0000 Valid Until: Mon, 20 Oct 2031 21:58:36 +0000</td><td>User Cert</td><td></td></tr> </table> </div>					Name	Issuer	Distinguished Name	In Use	Actions	webConfigurator default (6172cc2aaf4d0) Server Certificate CA: No Server: Yes	self-signed	O=pfSense webConfigurator Self-Signed Certificate, CN=pfSense-6172cc2aaf4d0 Valid From: Fri, 22 Oct 2021 14:35:22 +0000 Valid Until: Thu, 24 Nov 2022 14:35:22 +0000	webConfigurator	    	DEMO_Cert Server Certificate CA: No Server: Yes	VPN_CA	ST=3, OU=IT, O=DEMO, L=Laltipur, CN=VPN_Certificate, C=NP Valid From: Fri, 22 Oct 2021 20:39:29 +0000 Valid Until: Mon, 20 Oct 2031 20:39:29 +0000	OpenVPN Server	    	VPN_Client_Cert User Certificate CA: No Server: No	VPN_CA	ST=3, OU=IT, O=DEMO, L=Laltipur, CN=demovpn, C=NP Valid From: Fri, 22 Oct 2021 20:58:11 +0000 Valid Until: Mon, 20 Oct 2031 20:58:11 +0000	User Cert	    	VPN_Client_Cert2 User Certificate CA: No Server: No	VPN_CA	ST=3, OU=IT, O=DEMO, L=Laltipur, CN=gari, C=NP Valid From: Fri, 22 Oct 2021 21:58:36 +0000 Valid Until: Mon, 20 Oct 2031 21:58:36 +0000	User Cert	    
Name	Issuer	Distinguished Name	In Use	Actions																									
webConfigurator default (6172cc2aaf4d0) Server Certificate CA: No Server: Yes	self-signed	O=pfSense webConfigurator Self-Signed Certificate, CN=pfSense-6172cc2aaf4d0 Valid From: Fri, 22 Oct 2021 14:35:22 +0000 Valid Until: Thu, 24 Nov 2022 14:35:22 +0000	webConfigurator	    																									
DEMO_Cert Server Certificate CA: No Server: Yes	VPN_CA	ST=3, OU=IT, O=DEMO, L=Laltipur, CN=VPN_Certificate, C=NP Valid From: Fri, 22 Oct 2021 20:39:29 +0000 Valid Until: Mon, 20 Oct 2031 20:39:29 +0000	OpenVPN Server	    																									
VPN_Client_Cert User Certificate CA: No Server: No	VPN_CA	ST=3, OU=IT, O=DEMO, L=Laltipur, CN=demovpn, C=NP Valid From: Fri, 22 Oct 2021 20:58:11 +0000 Valid Until: Mon, 20 Oct 2031 20:58:11 +0000	User Cert	    																									
VPN_Client_Cert2 User Certificate CA: No Server: No	VPN_CA	ST=3, OU=IT, O=DEMO, L=Laltipur, CN=gari, C=NP Valid From: Fri, 22 Oct 2021 21:58:36 +0000 Valid Until: Mon, 20 Oct 2031 21:58:36 +0000	User Cert	    																									

Figura 4: Certificado existentes

Imagen 5



Servers Clients Client Specific Overrides Wizards Client Export Shared Key Export

General Information

Disabled ☐ Disable this server
Set this option to disable this server without removing it from the list.

Server mode Remote Access (SSL/TLS + User Auth)

Backend for authentication Local Database

Protocol UDP on IPv4 only

Device mode tun - Layer 3 Tunnel Mode
"tun" mode carries IPv4 and IPv6 (OSI layer 3) and is the most common and compatible mode across all platforms.
"tap" mode is capable of carrying 802.3 (OSI Layer 2.)

Interface WAN
The interface or Virtual IP address where OpenVPN will receive client connections.

Local port 1194
The port used by OpenVPN to receive client connections.

Description Remote Users
A description may be entered here for administrative reference (not parsed).

Figura 5: Configuración del Servidor VPN en el Firewall

Imagen 6

VPN / OpenVPN / Clients

Servers Clients Client Specific Overrides Wizards Client Export Shared Key Export

OpenVPN Clients					
Interface	Protocol	Server	Mode / Crypto	Description	Act
WAN	UDP4 (TUN)	3.15.104.133:1194	Mode: Peer to Peer (SSL/TLS) Data Ciphers: AES-256-GCM, AES-128-GCM, CHACHA20-POLY1305, AES-256-CBC Digest: SHA256	VPN_CLIENT	
WAN	UDP4 (TUN)	3.15.104.133:1194	Mode: Peer to Peer (SSL/TLS) Data Ciphers: AES-256-GCM, AES-128-GCM, CHACHA20-POLY1305, AES-256-CBC Digest: SHA256	VPN_CLIENT2	

Figura 6: Clientes creados en la VPN

Imagen 7

System / User Manager / Users

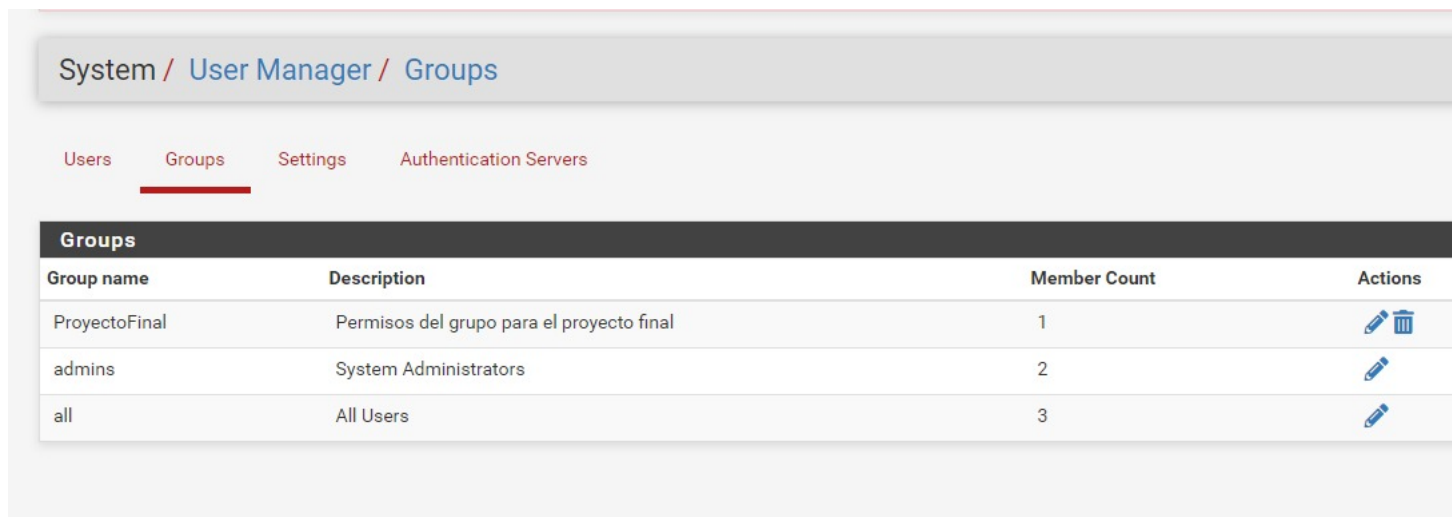
UsersGroupsSettingsAuthentication Servers

Users					
	Username	Full name	Status	Groups	Actions
<input type="checkbox"/>	admin	System Administrator	✓	admins	
<input type="checkbox"/>	demovpn	Demo VPN	✓	admins	
<input type="checkbox"/>	gari	Gari Mendoza	✓	ProyectoFinal	

Add

Figura 7: Usuarios creados

Imagen 8



System / User Manager / Groups

Users Groups Settings Authentication Servers





Groups			
Group name	Description	Member Count	Actions
ProyectoFinal	Permisos del grupo para el proyecto final	1	 
admins	System Administrators	2	
all	All Users	3	

Figura 8: Creación del grupo de Proyecto Final para el control de permisos limitados a usuarios

Imagen 9

Users

Groups

Settings

Authentication Servers

Group Properties

Group name

ProyectoFinal

Scope

Local

Description

Permisos del grupo para el proyecto final

Group membership

admin

demovpn

gari

>> Move to "Members"

<< Move to "Not members"

Not members

Members

Hold down CTRL (PC)/COMMAND (Mac) key to select multiple items.

Assigned Privileges

Name	Description
WebCfg - Dashboard widgets (direct access).	Allow direct access to all Dashboard widget pages, required for some widgets using AJAX.

Figura 9: Propiedades del grupo

Imagen 10

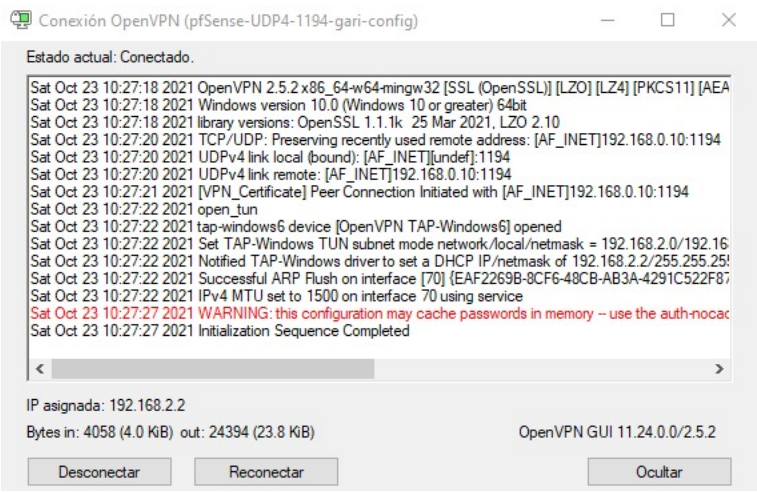


Figura 10: Usuarios conectados con el usuario Gary y enlazados a la VPN

Imagen 11

Firewall / Rules / WAN

Floating WAN OpenVPN

Rules (Drag to Change Order)

<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	5 / 53 K/s	*	*	*	WAN Address	80	*	*		Anti-Lockout Rule	
<input checked="" type="checkbox"/>	0 / 0 B	*	Reserved Not assigned by IANA	*	*	*	*	*		Block bogon networks	
<input type="checkbox"/>	0 / 0 B	IPv6 TCP	*	*	2607:f8b:0:4008:8da::200e	*	*	none			
<input type="checkbox"/>	0 / 0 B	IPv4 UDP	*	*	WAN address	1194 (OpenVPN)	*	none		OpenVPN Remote Users wizard	

Add Add Delete Save Separation

Figura 11: Regla para bloquear Google

Imagen 12

Firewall / Rules / OpenVPN

Floating WAN OpenVPN

Rules (Drag to Change Order)

<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	0 / 0 B	IPv4 *	*	*	pfB_PRI1_v4	*	*	none		pfB_PRI1_v4 auto rule	
<input type="checkbox"/>	0 / 0 B	IPv6 TCP	*	*	2607:f8b0:4008:80a::200e	*	*	none			
<input type="checkbox"/>	0 / 0 B	IPv4 *	*	*	*	*	*	none		OpenVPN Remote Users wizard	

Add Add Delete Save Separator

Figura 12: Reglas para clientes que se conectan por la VPN

Imagen 13

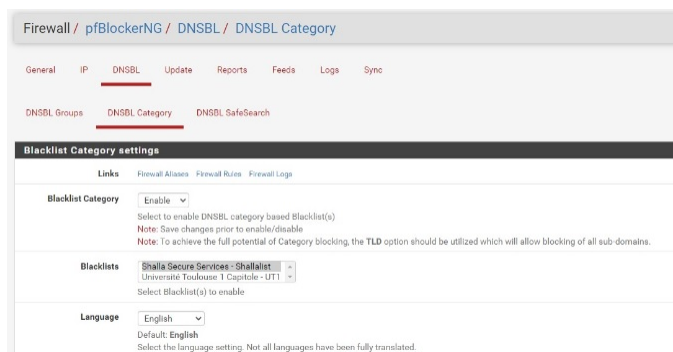


Figura 13: pfBlockerNG elemento para bloquear paginas Web

Imagen 14

<input checked="" type="checkbox"/>	URL shortener	Sites offering short links for URLs.
<input type="checkbox"/>	Violence	Sites about killing and harming people. Covers anything about brutality and beastiality.
<input type="checkbox"/>	Warez	Collection of sites offering programs to break licence keys, licence keys themselves, cracked software and other copyrighted material.
<input type="checkbox"/>	Weapons	Sites offering all kinds of weapons or accessories for weapons
<input checked="" type="checkbox"/>	Webmail	Sites that offer web-based email services.
<input type="checkbox"/>	Web Phone	Sites that enable user to phone via the Internet. Any site where users can voice-chat with each other.
<input type="checkbox"/>	Web Radio	Sites that offer listening to music and radio live streams.
<input type="checkbox"/>	Web TV	Sites offering TV streams via Internet.
<div><input checked="" type="checkbox"/> Enable All <input type="checkbox"/> Disable All</div>		

Figura 14: Bloqueo de links que sean cortos