



Primeros pasos con la imagen de Firewall pfSense

Esta página describe los conceptos básicos en torno al Firewall pfSense y cómo configurar el Firewall dentro de la plataforma VDC.

Desplegar el Firewall

El Firewall pfSense debe ser inicialmente desplegado de la misma forma que una imagen de una Máquina Virtual, dicha documentación la encontrará en el video 'Cómo Añadir una Máquina Virtual'. Al llegar a la etapa de añadir sus interfaces de red, es importante asegurarse de que la NIC 0 (interfaz Ethernet 0) es una IP Pública (o la primera IP Pública en el caso que existan más), y que esa NIC 1 sea la interfaz Privada o Externa. La imagen base del Firewall pfSense ha sido pre-configurada para que las interfaces coincidan con la siguiente secuencia.

	IP address	MAC	VLAN
General	213.253.4.82	00:50:56:08:1F:53	Public-VLAN210
Description	192.168.1.1	00:50:56:28:B2:A7	Updater
Network	192.168.1.1	00:50:56:28:B2:A7	Updater
Storage			

Para obtener más información, consulte la sección 'Configurar los recursos de red' de la documentación 'Configuración de Máquinas Virtuales'.

Configurar el Firewall

Es necesario configurar el Firewall para permitir el tráfico desde y hacia el Firewall, también para permitir el tráfico local a Internet y, finalmente, para permitir utilizar el puerto 80 (HTTP al servidor web).

Para configurar el Firewall en primer lugar debe abrir un navegador web - introduzca la dirección IP de la interfaz pública del Firewall que le asignó anteriormente.

NOTA: hay que usar un http seguro, por ejemplo: <https://195.157.12.255> [1]
Ignore el error de certificado, haga clic en 'Continuar al sitio web'. La pantalla que le aparecerá será la siguiente:



The image shows a login interface for a device named 'Sense'. At the top left is the 'Sense' logo, which consists of three interlocking circles (two red, one black) followed by the word 'Sense' in a bold, black, sans-serif font. Below the logo are two input fields. The first is labeled 'Username:' and contains a small blue person icon on the left and a white text box. The second is labeled 'Password:' and contains a small yellow padlock icon on the left and a white text box. Below these fields is the instruction 'Enter username and password to login.' and a 'Login' button with a black border and white text.

El ID de usuario y contraseña predeterminados los encontrará en el apartado 'Datos de acceso a las imágenes proporcionadas por Claranet' de la sección 'Plantillas de MV'. A continuación le aparecerá la página web principal del Firewall.


El primer paso que debe realizar es cambiar la contraseña que viene por defecto para el usuario admin. Mediante su ratón acceda a la opción del menú del sistema en la parte superior izquierda de la página hasta llegar a un cuadro desplegable, a continuación le aparecerán diferentes opciones y deberá seleccionar 'Administrador de usuarios'.



A continuación, le aparecerá la siguiente pantalla:


System: User Manager

Users Groups Settings Servers

Username	Full name	Disabled	Groups
 superuser	superuser	<input type="checkbox"/>	superuser

Additional users can be added here. User permissions for accessing the webConfigurator can be assigned directly or inherited from group memberships. An icon that appears grey indicates that it is a system defined object. Some system object properties can be modified but they cannot be deleted.

Accounts created here are also used for other parts of the system such as OpenVPN, IPsec, and Captive Portal.

Seleccione con el ratón el icono de edición  , situada en la derecha de la línea del usuario admin para editar su contraseña.


A continuación le aparecerá la siguiente pantalla:



System: User Manager


Users Groups Settings Servers



Defined by **USER**

Disabled

Username  superuser

Password 
 (confirmation)

Full name  superuser
User's full name, for your own information only

Expiration date  
Leave blank if the account shouldn't expire, otherwise enter the expiration date in the following format: mm/dd/yy

Group Memberships **Not Member Of** **Member Of**

Escriba una nueva contraseña donde se indica (dos veces). Para continuar con el proceso, desplácese hacia abajo y haga clic en Guardar.

Lo siguiente que debemos hacer es configurar el puerto SSH, esto le permitirá acceder al servidor Web a través de SSH. Para ello, seleccione 'Sistema' - 'Opciones avanzadas' y aparecerá la siguiente pantalla:

System: Advanced: Admin Access

Admin Access

Note: The options on this page are intended for use by advanced users only.

webConfigurator

Protocol	<input type="radio"/> HTTP <input checked="" type="radio"/> HTTPS
SSL Certificate	<input type="text" value="webConfigurator default"/>
TCP port	<input type="text" value=""/> Enter a custom port number for the webConfigurator above if you want to override the default (80 for HTTP, 443 for HTTPS). Changes will take effect immediately after save.
Max Processes	<input type="text" value="2"/> Enter the number of webConfigurator processes you want to run. This defaults to 2. Increasing this will allow more users/browsers to access the GUI concurrently.
WebGUI redirect	<input type="checkbox"/> Disable webConfigurator redirect rule When this is unchecked, access to the webConfigurator is always permitted even on port 80, regardless of the list of ports configured. Check this box to disable this automatically added redirect rule.
WebGUI Login Autocomplete	<input type="checkbox"/> Disable webConfigurator login autocomplete When this is unchecked, login credentials for the webConfigurator may be saved by the browser. While convenient, some security standards require this to be disabled. Check this box to disable autocomplete on the login form so that browsers will not prompt to save credentials (NOTE: Some browsers do not respect this option).
WebGUI login messages	<input type="checkbox"/> Disable logging of webConfigurator successful logins When this is checked, successful logins to the webConfigurator will not be logged.

Desplácese hacia abajo hasta llegar a la sección SSH:

Secure Shell	
Secure Shell Server	<input type="checkbox"/> Enable Secure Shell
Authentication Method	<input type="checkbox"/> Disable password login for Secure Shell (RSA key only) When enabled, authorized keys need to be configured for each user that has been granted secure shell access.
SSH port	<input type="text"/> Note: Leave this blank for the default of 22.


Haga clic en 'Activar Secure Shell' y configure el puerto SSH en el puerto '8022'. A continuación, desplácese hacia abajo y haga clic en 'Guardar'.

Para seguir con la configuración del Firewall seguiremos con las siguientes reglas:

Permitir SSH en el puerto 8022 para Firewall

Seleccione la opción 'Firewall' y en el desplegable que le aparecerá, seleccione 'Reglas'.



A continuación seleccione 'WAN' y haga clic en el icono  para añadir una nueva regla:

Firewall: Rules: Edit

Edit Firewall rule	
Action	<input type="text" value="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 U... returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is disc...
Disabled	<input type="checkbox"/> Disable this rule Set this option to disable this rule without removing it from the list.
Interface	<input type="text" value="WAN"/> Choose on which interface packets must come in to match this rule.
Protocol	<input type="text" value="TCP"/> Choose which IP protocol this rule should match. Hint: in most cases, you should specify <i>TCP</i> here.
Source	<input type="checkbox"/> not Use this option to invert the sense of the match. Type: <input type="text" value="any"/> Address: <input type="text" value=""/> / <input type="text" value="31"/> <input type="button" value="Advanced"/> - Show source port range
Destination	<input type="checkbox"/> not Use this option to invert the sense of the match.

Para configurar correctamente, rellene el cuadro de dialogo con el contenido que aparece a continuación:

```
Action: Pass
Disabled: not selected
Interface: WAN
Protocol: TCP
Source: any
Destination: Wan Address
Destination Port Range ? From: 8022
Description: SSH to Firewall on Port 8022
```

Haga clic en Guardar y Aplicar cambios. Ahora ya puede usar ssh como herramienta favorita sobre el puerto 8022.

Ejemplos de reglas NAT

La siguiente sección proporciona algunos ejemplos de configuración de NAT.

Ejemplo Regla NAT - Permitir SSH en el puerto 22 del servidor Web

Seleccione 'Firewall' ?'Nat' y a continuación seleccione 'Port Forward':

Firewall: NAT: Port Forward

Port Forward 1:1 Outbound

If	Proto	Src. addr	Src. ports	Dest. addr	Dest. ports	NAT IP	NAT Ports	Description
----	-------	-----------	------------	------------	-------------	--------	-----------	-------------

pass
linked rule

A continuación haga clic en el botón de Agregar Regla de NAT.

Firewall: NAT: Port Forward: Edit

Edit Redirect entry

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

No RDR (NOT)
Enabling this option will disable redirection for traffic matching this rule.
Hint: this option is rarely needed, don't use this unless you know what you're doing.

Interface: WAN
Choose which interface this rule applies to.
Hint: in most cases, you'll want to use WAN here.

Protocol: TCP
Choose which IP protocol this rule should match.
Hint: in most cases, you should specify TCP here.

Source: Advanced - Show source address and port range

Destination: not
Use this option to invert the sense of the match.
Type: WAN address

Para configurar correctamente, rellene el cuadro de dialogo con el contenido que aparece a continuación:

```
Disabled: Not selected
```

```
No RDR (NOT): Not selected
Interface: WAN
Protocol: TCP
Source: Ignore
Destination: Wan Address
Destination Port Range ? SSH
Redirect Target IP Address: 192.168.2.2 (or your webserver IP)
Redirect Target Port: SSH
Description: SSH to Web Server
NAT Reflection: leave as default
Filter Rule Association: Pass
```

Haga clic en Guardar y Aplicar cambios. Ahora ya puede usar SSH en el servidor web (dirección IP como IP Pública en Firewall con el puerto 22), con el nombre de usuario y contraseña del servidor web.

Ejemplo Regla NAT - Permitir HTTP en el puerto 80 al servidor Web

Seleccione 'Firewall' - 'Nat' y a continuación seleccione 'Port Forward':

Firewall: NAT: Port Forward

Port Forward 1:1 Outbound

If	Proto	Src. addr	Src. ports	Dest. addr	Dest. ports	NAT IP	NAT Ports	Description
----	-------	-----------	------------	------------	-------------	--------	-----------	-------------

pass
linked rule

A continuación haga clic en el botón de Agregar Regla de NAT.

Firewall: NAT: Port Forward: Edit

Edit Redirect entry	
Disabled	<input type="checkbox"/> Disable this rule Set this option to disable this rule without removing it from the list.
No RDR (NOT)	<input type="checkbox"/> Enabling this option will disable redirection for traffic matching this rule. Hint: this option is rarely needed, don't use this unless you know what you're doing.
Interface	<input type="text" value="WAN"/> Choose which interface this rule applies to. Hint: in most cases, you'll want to use WAN here.
Protocol	<input type="text" value="TCP"/> Choose which IP protocol this rule should match. Hint: in most cases, you should specify <i>TCP</i> here.
Source	<input type="text" value="Advanced"/> - Show source address and port range
Destination	<input type="checkbox"/> not Use this option to invert the sense of the match. Type: <input type="text" value="WAN address"/>

Para configurar correctamente, rellene el cuadro de dialogo con el contenido que aparece a continuación:

```
Disabled: Not selected
No RDR (NOT): Not selected
Interface: WAN
Protocol: TCP
Source: Ignore
Destination: Wan Address
Destination Port Range ? HTTP
Redirect Target IP Address: 192.168.2.2 (or your webserver IP)
Redirect Target Port: HTTP
Description: HTTP to Web Server
NAT Reflection: leave as default
Filter Rule Association: Pass
```

Haga clic en Guardar y Aplicar cambios. Ahora ya puede ver el servidor de su sitio web a través del servidor web mediante el navegador <http://#public> [2] de su firewall #.

Mapeado NAT 1:1

La siguiente sección proporciona instrucciones sobre cómo configurar mapeo NAT 1:1 con múltiples direcciones IP Públicas.

En este ejemplo, la IP Pública 195.157.13.200 va a ser cambiada a la IP privada 192.168.0.3

Para comprobar la configuración se deben llevar a cabo los siguientes pasos:

- Se necesita una interfaz para cada dirección IP Pública que haga NAT.
- Debe asegurarse que las interfaces con IPs Públicas adicionales han sido numeradas como NIC2 o sucesivas (la primera IP Pública se configura en el NIC 0 y la primera IP

Privada/Externa en NIC 1, como se detalla anteriormente).

- Es necesario establecer NAT 1:1 para esta IP.
- Es necesario crear una regla para abrir el puerto que desee para esta IP.

Asignar interfaz adicional


Siguiendo las instrucciones de configuración de Firewall indicadas anteriormente, su primera interfaz WAN irá asignada a em0 y su LAN en em1:

Interfaces: Assign network ports

Interface assignments Interface Groups PPPs GRE GIF

Interface	Network port
WAN	em0 (08:00:27:ba:f5:7e) ▼
LAN	em1 (08:00:27:ad:a1:87) ▼

Interfaces that are configured as members of a lagg(4) interface will not be shown.

Haga clic en el botón  para asignar una nueva interfaz. OPT1 aparecerá automáticamente junto a em2:

WAN	em0 (08:00:27:ba:f5:7e) ▼
LAN	em1 (08:00:27:ad:a1:87) ▼
OPT1	em2 (08:00:27:d5:82:e5) ▼

Seleccione la opción del menú Interfaces, OPT1.

Seleccione Activar en la parte superior y seleccione en ?Tipo? DHCP. Haga clic en Guardar y Aplicar cambios.

The OPT1 configuration has been changed.




You must apply the changes in order for them to take effect.

Don't forget to adjust the DHCP Server range if needed after applying.

Apply changes

General configuration

Enable Enable Interface



Description  OPT1
Enter a description (name) for the interface here.

Type DHCP ▼

Si utiliza varias interfaces con NAT 1:1 para cada una, tendrá que añadir los siguientes

parámetros de configuración adicionales:

En primer lugar, tendrá que abrir las opciones adicionales de configuración de Firewall. A continuación vaya al menú 'Sistema', 'Gestor de usuarios', y luego haga clic en la etiqueta 'Grupos'.

Haga clic en el botón Editar  situado junto al grupo 'súper usuario'. A continuación, desplácese hacia abajo hasta la parte inferior en la sección 'Asignación de privilegios' y haga clic en el icono  para añadir nuevos privilegios.

En la página de añadir Privilegios, haga clic en 'Seleccionar todo' y luego en 'Guardar'.

Ahora tendrá que deseleccionar Reply-To. Seguidamente vaya al Menú 'Sistema' 'Avanzado' y haga clic en la etiqueta 'Firewall / NAT'. Finalmente haga clic en la casilla de verificación 'Desactivar respuesta a las normas sobre WAN'.

System: Advanced: Firewall and NAT



The changes have been applied successfully.

Admin Access

Firewall / NAT

Networking

Miscellaneous

System Tunables

Notifications

NOTE: The options on this page are intended for use by advanced users only.

Firewall Advanced

IP Do-Not-Fragment compatibility

Clear invalid DF bits instead of dropping the packets

This allows for communications with hosts that generate fragmented packets with the don't fragment (DF) bit set. Known to do this. This will cause the filter to not drop such packets but instead clear the don't fragment bit.

IP Random id generation

Insert a stronger id into IP header of packets passing through the filter.

Replaces the IP identification field of packets with random values to compensate for operating systems that use predictable values. This option only applies to packets that are not fragmented after the optional packet reassembly.

Firewall Optimization Options

normal

as the name says, it's the normal optimization algorithm

Select the type of state table optimization to use

Disable Firewall

Disable all packet filtering.

Note: This converts pfSense into a routing only platform!

Note: This will also turn off NAT!

If you only want to disable NAT, and not firewall rules, visit the [Outbound NAT](#) page.

Disable Firewall Scrub

Disables the PF scrubbing option which can sometimes interfere with NFS and PPTP traffic.

Firewall Maximum States

Maximum number of connections to hold in the firewall state table.

Note: Leave this blank for the default. On your system the default size is: 47000

Firewall Maximum Table Entries

Maximum number of table entries for systems such as aliases, sshlockout, snort, etc, combined.

Note: Leave this blank for the default. On your system the default size is: 200000

Static route filtering

Bypass firewall rules for traffic on the same interface

This option only applies if you have defined one or more static routes. If it is enabled, traffic that enters and leaves the same interface will not be checked by the firewall. This may be desirable in some situations where multiple subnets exist on the same interface.

Disable Auto-added VPN rules

Disable all auto-added VPN rules.

Note: This disables automatically added rules for IPsec, PPTP.

Disable reply-to

Disable reply-to on WAN rules

With Multi-WAN you generally want to ensure traffic leaves the same interface it arrives on, hence reply-to is added by default. When using bridging, you must disable this behavior if the WAN gateway IP is different from the gateway IP of hosts behind the bridged interface.

Para ejecutar los cambios haga clic en 'Guardar'. A continuación, vaya al menú 'Sistema', 'Avanzado' y haga clic en el menú 'Red'. Deseleccione la casilla 'Suprimir mensajes ARP':

System: Advanced: Networking

Admin Access

Firewall / NAT

Networking

Miscellaneous

System Tunables

Notifications

NOTE: The options on this page are intended for use by advanced users only.

IPv6 Options

Allow IPv6

Allow IPv6

All IPv6 will be blocked unless this box is checked.

IPv6 over IPv4 Tunneling

Enable IPv4 NAT encapsulation of IPv6 packets

This provides an RFC 2893 compatibility mechanism that can be used to tunneling IPv6 packets over IPv4 routing infrastructure. If enabled, don't forget to add a firewall rule to permit IPv6 packets.

IP address :

Network Interfaces

Device polling

Enable device polling

Device polling is a technique that lets the system periodically poll network devices for new data instead of relying on interrupts. This prevents your webConfigurator, SSH, etc. from being inaccessible due to interrupt floods when under extreme load. Generally this is not recommended. Not all NICs support polling; see the pfSense homepage for a list of supported cards.

Hardware Checksum Offloading

Disable hardware checksum offload

Checking this option will disable hardware checksum offloading. Checksum offloading is broken in some hardware, particularly some Realtek cards. Rarely, drivers may have problems with checksum offloading and some specific NICs.

Hardware TCP Segmentation Offloading

Disable hardware TCP segmentation offload

Checking this option will disable hardware TCP segmentation offloading (TSO, TSO4, TSO6). This offloading is broken in some hardware drivers, and may impact performance with some specific NICs.

Hardware Large Receive Offloading

Disable hardware large receive offload

Checking this option will disable hardware large receive offloading (LRO). This offloading is broken in some hardware drivers, and may impact performance with some specific NICs.

ARP Handling

Suppress ARP messages


This option will suppress ARP log messages when multiple interfaces reside on the same broadcast domain

Save


Haga clic en 'Guardar' para finalizar.

Configurar NAT 1:1

Haga clic en 'Firewall' y 'NAT'. Seleccione la pestaña 1:1.

Seleccione el icono  para añadir la nueva regla y configurar la interfaz a OPT1, Subred Externa en la dirección IP Pública (la subred debe ser /32 si sólo desea configurar NAT en una única dirección IP).

Firewall: NAT: 1:1: Edit

Edit NAT 1:1 entry	
Disabled	<input type="checkbox"/> Disable this rule Set this option to disable this rule without removing it from the list.
Interface	OPT1 ▾ Choose which interface this rule applies to. Hint: in most cases, you'll want to use WAN here.
External subnet IP	195.157.13.200 Enter the external (usually on a WAN) subnet's starting address for the 1:1 mapping. The subnet mask from the internal address below will be applied to this IP address. Hint: this is generally an address owned by the router itself on the selected interface.
Internal IP	<input type="checkbox"/> not Use this option to invert the sense of the match. Type: Single host ▾ Address: 192.168.0.3 / 31 ▾ Enter the internal (LAN) subnet for the 1:1 mapping. The subnet size specified for the internal subnet will be applied to the external subnet.
Destination	<input type="checkbox"/> not Use this option to invert the sense of the match. Type: any ▾ Address: / 31 ▾ The 1:1 mapping will only be used for connections to or from the specified destination. Hint: this is usually 'any'.
Description	 NAT1 You may enter a description here for your reference (not parsed).
NAT reflection	use system default ▾

Configure la IP interna en la dirección IP Privada del host.

Establezca una descripción para esta regla NAT y haga clic en Guardar y Aplicar los cambios en el sistema.

Aplique una regla de firewall

Seleccione el menú FIREWALL y seleccione REGLAS.

Seleccione la etiqueta OPT1. Seguidamente seleccione  para crear nueva regla.

Firewall: Rules: Edit

Edit Firewall rule	
Action	<input type="text" value="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 U) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.
Disabled	<input type="checkbox"/> Disable this rule Set this option to disable this rule without removing it from the list.
Interface	<input type="text" value="OPT1"/> Choose on which interface packets must come in to match this rule.
Protocol	<input type="text" value="TCP"/> Choose which IP protocol this rule should match. Hint: in most cases, you should specify <i>TCP</i> here.
Source	<input type="checkbox"/> not Use this option to invert the sense of the match. Type: <input type="text" value="any"/> Address: <input type="text" value=""/> / <input type="text" value="31"/> <input type="button" value="Advanced"/> - Show source port range
Destination	<input checked="" type="checkbox"/> not Use this option to invert the sense of the match. Type: <input type="text" value="Single host or alias"/> Address: <input type="text" value="192.168.0.3"/> / <input type="text" value="31"/>
Destination port range	from: <input type="text" value="SSH"/> <input type="text" value=""/> to: <input type="text" value="SSH"/> <input type="text" value=""/> Specify the port or port range for the destination of the packet for this rule. Hint: you can leave the 'to' field empty if you only want to filter a single port
Log	<input type="checkbox"/> Log packets that are handled by this rule Hint: the firewall has limited local log space. Don't turn on logging for everything. If you want to do a lot of logging, consider using a remote syslog server (see the Diagnostics: System logs: Settings page).
Description	<input type="text" value="Rule1-NAT1"/> You may enter a description here for your reference.

Asegúrese de que la interfaz está en 'OPT1' o con el nombre de interfaz que esté utilizando para esta dirección IP Pública.

En el campo Tipo de Destino indique 'dirección única' y especifique la dirección IP Privada del host al que se quiere conectar, en este caso 192.168.0.3

Configure el rango de puerto de destino, en este caso SSH. Escriba una breve descripción para esta regla.

A continuación seleccione Guardar y Aplicar los cambios.

Con estos cambios, ahora debería ser capaz de establecer una conexión ssh con la dirección IP Pública 195.157.13.200 redirigida a 192.168.0.3

Source URL: <http://cloudhelp.claranet.com/es/content/primeros-pasos-con-la-imagen-de-firewall-pfsense>

Links:

[1] <https://195.157.12.255>

[2] <http://#public>