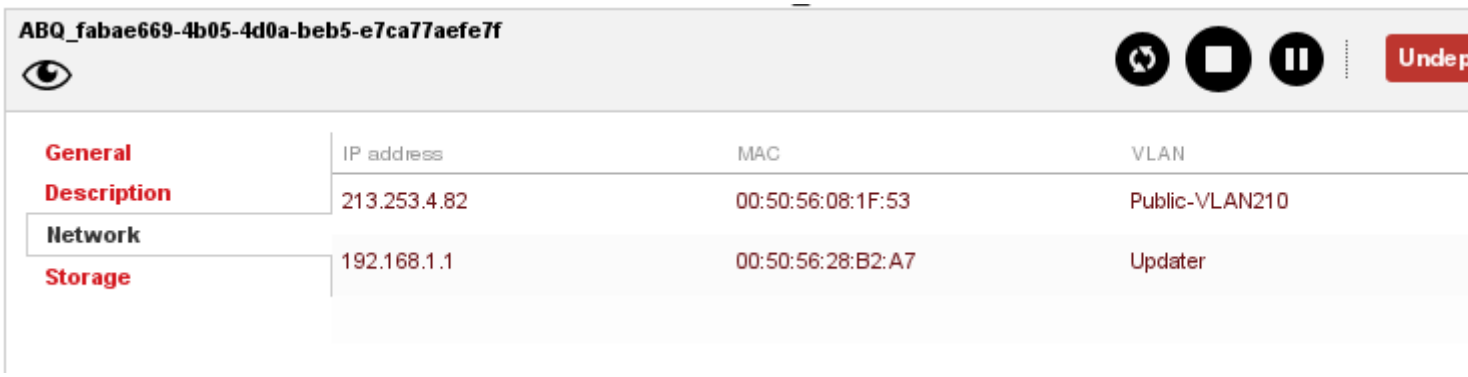
Primeros pasos con la imagen de Firewall pfSense

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.



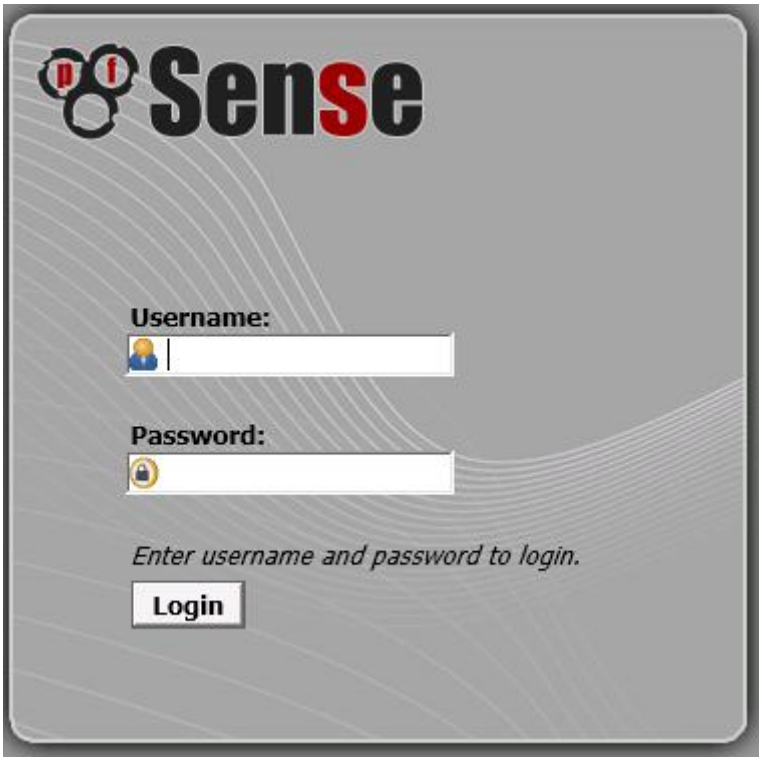
Para obtener más información, consulte la sección 'Configurar los recursos de red' de la documentación 'Configuración de Máquinas Virtuales'.

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.

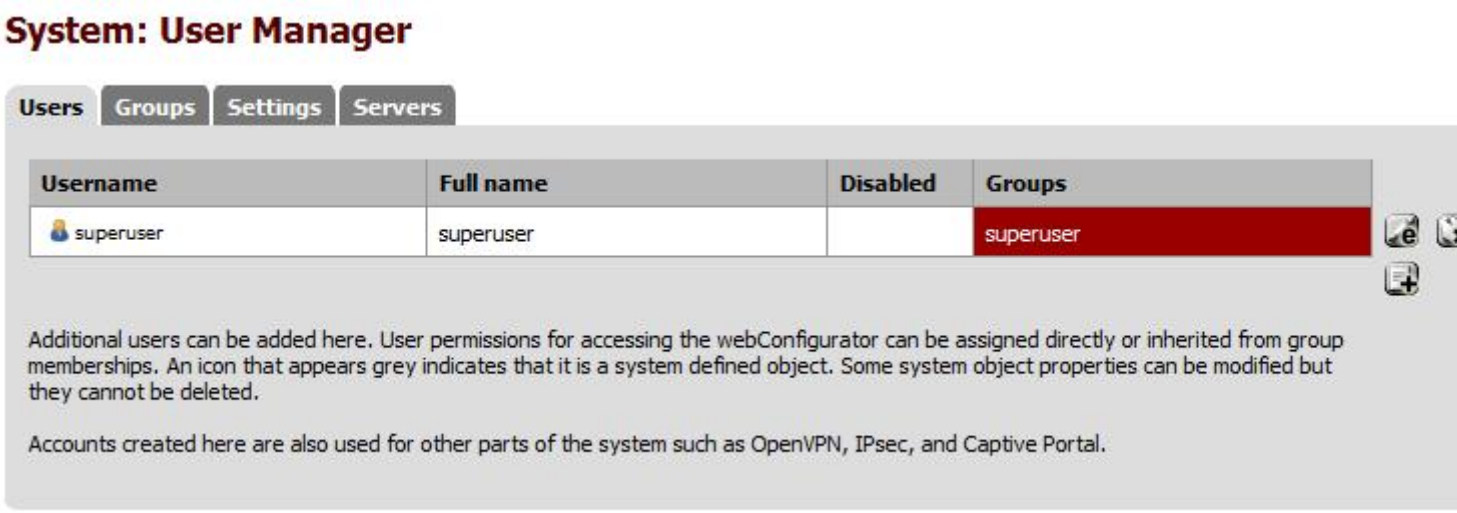
NOTA: hay que usar un http seguro, por ejemplo: https://195.157.12.255 [1]
Ignore el error de certificado, haga clic en 'Continuar al sitio web'. La pantalla que le aparecerá será la siguiente:



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.

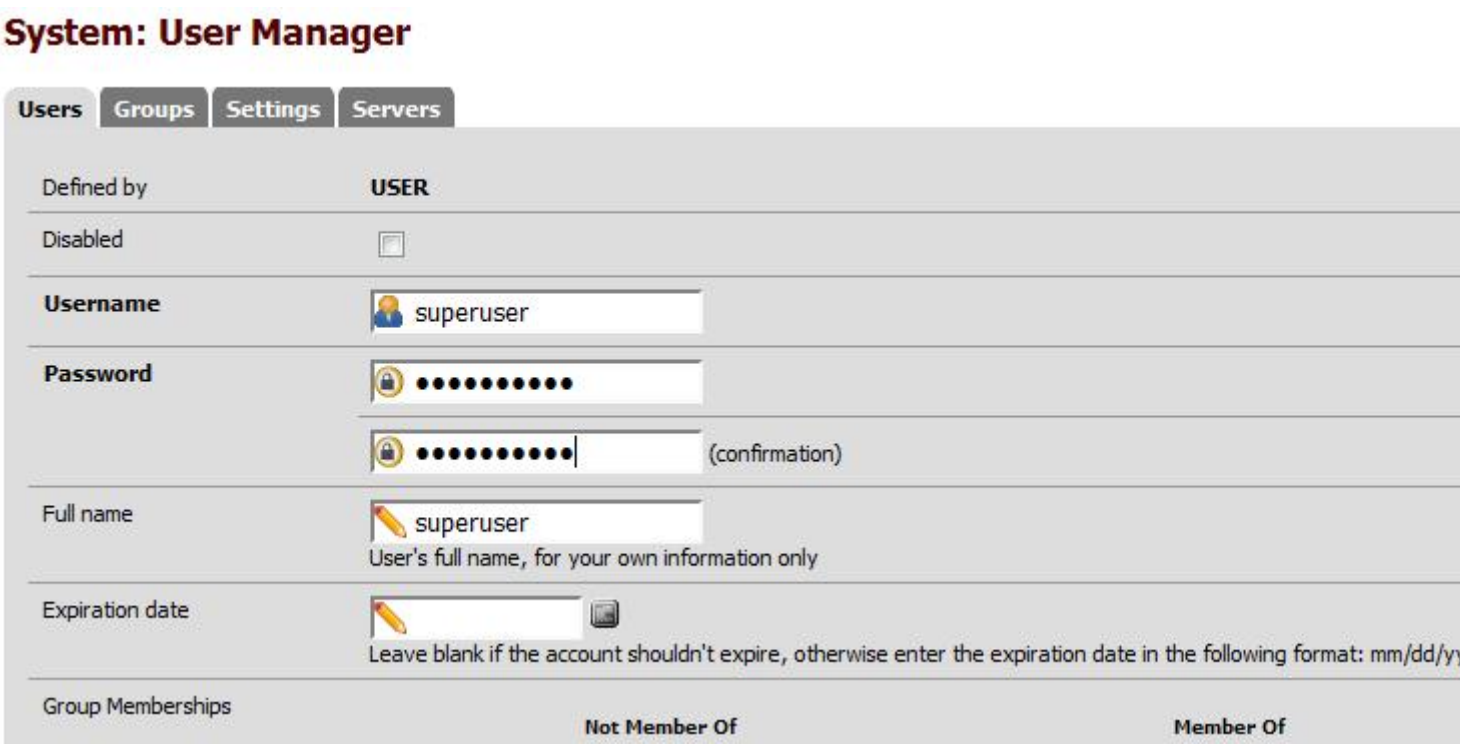
El primer paso que debe realizar es cambiar la contraseña que viene por defecto para el usuario admin. Mediante su ratón acceda a la opción del menú del sistema en la parte superior izquierda de la página hasta llegar a un cuadro desplegable, a continuación le aparecerán diferentes opciones y deberá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

A continuación, le aparecerá la siguiente pantalla:



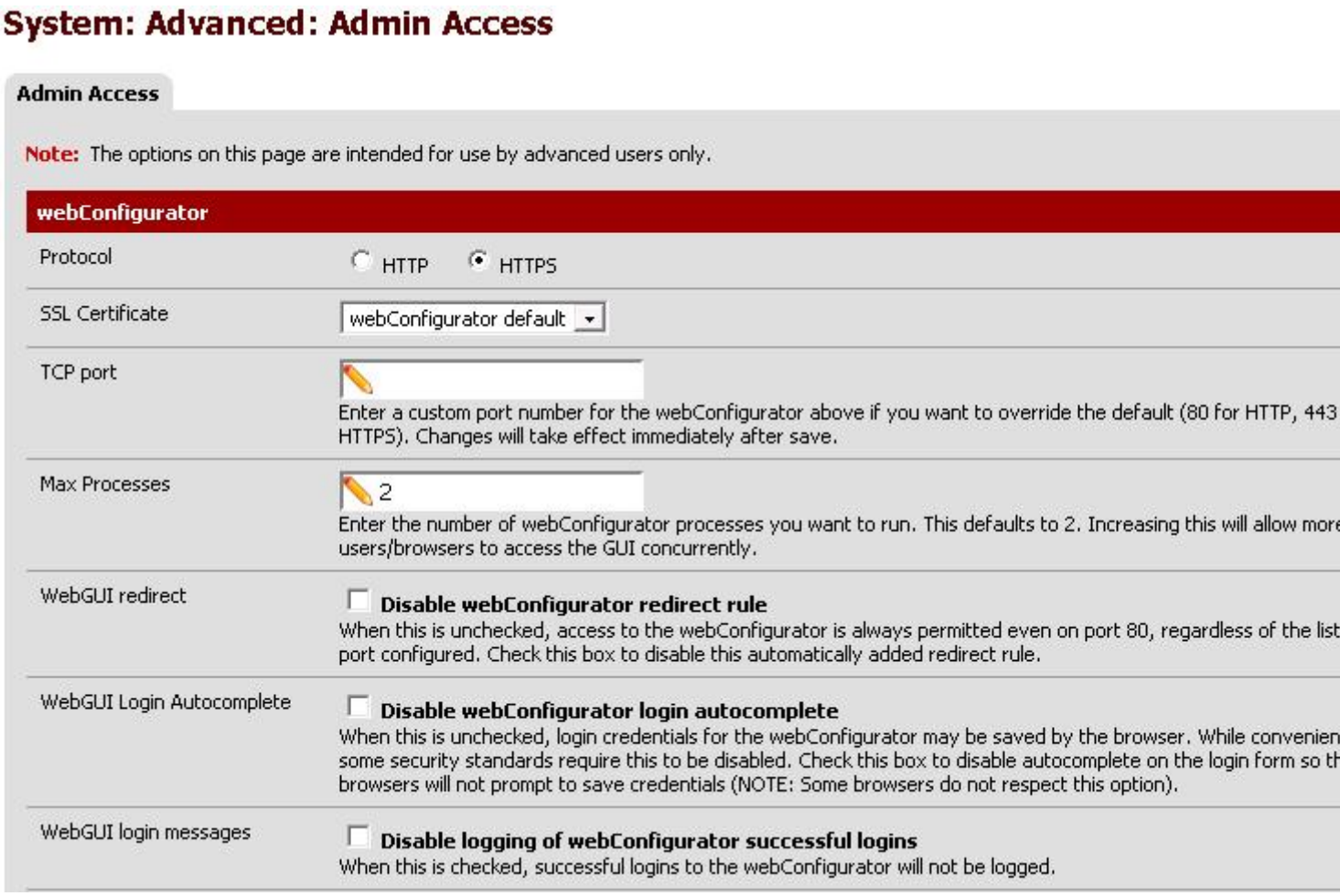
Seleccione con el ratón el icono de edición , situada en la derecha de la línea del usuario admin para editar su contraseña.

A continuación le aparecerá la siguiente pantalla:

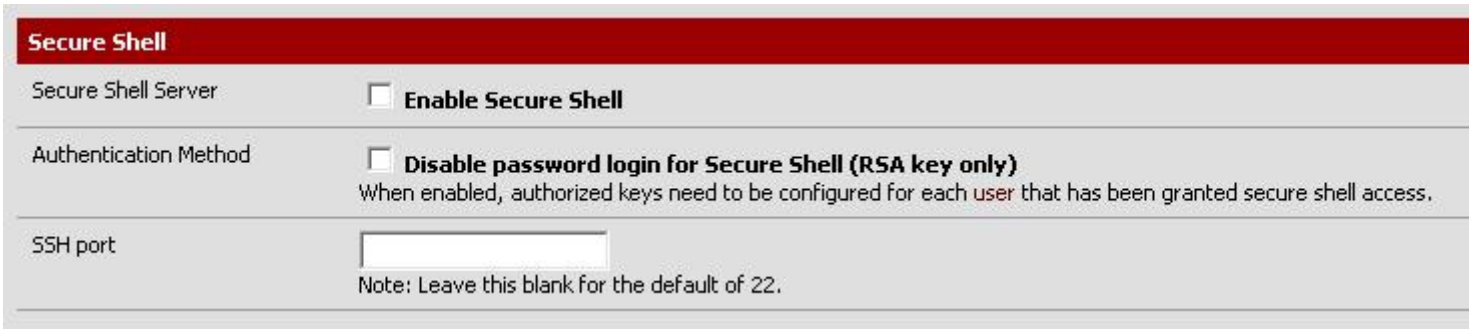


Escriba una nueva contraseña donde se indica (dos veces). Para continuar con el proceso, desplácese hacia abajo y haga clic en Guardar.

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:



Desplácese hacia abajo hasta llegar a la sección SSH:



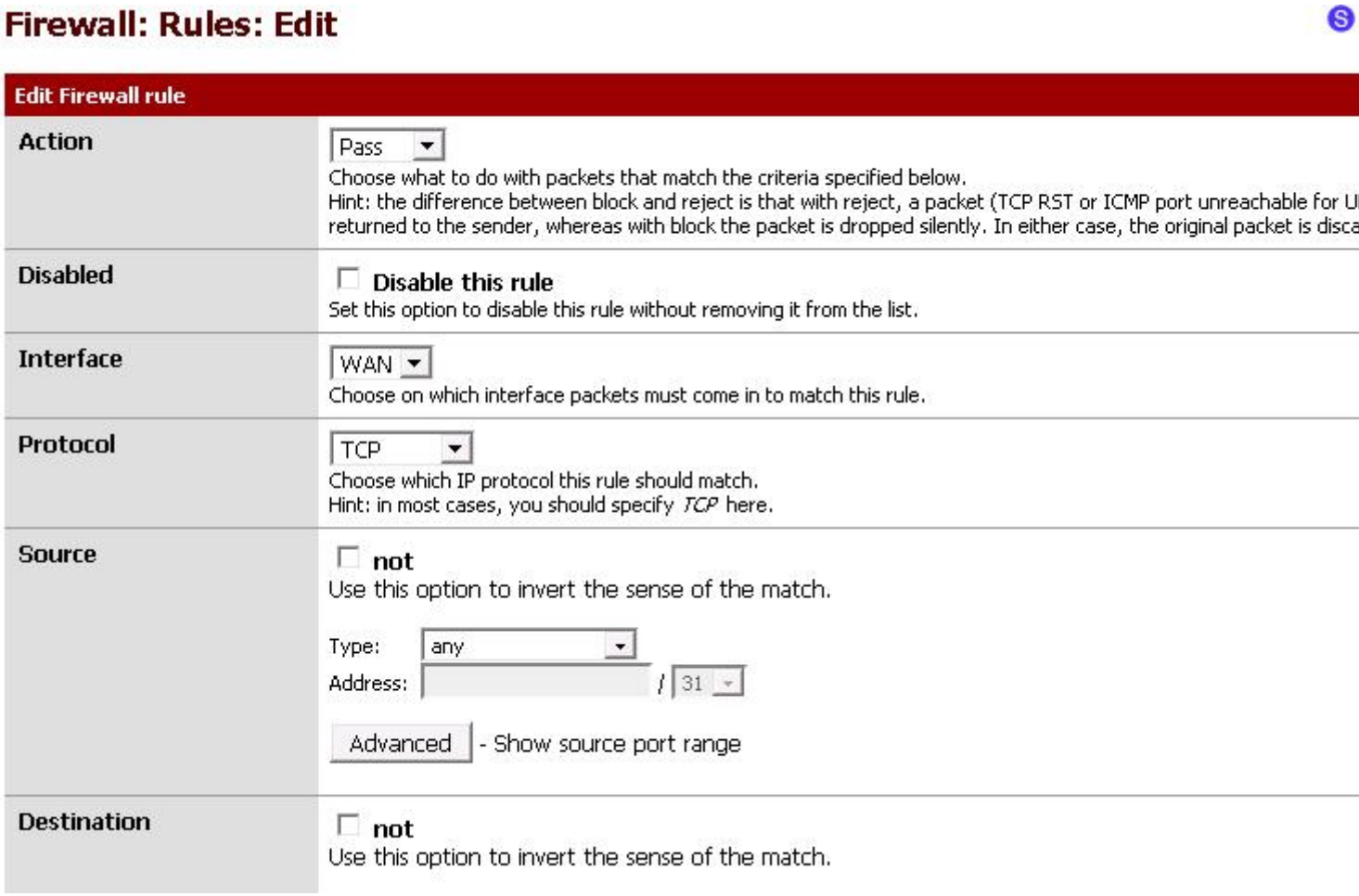
Haga clic en 'Activar Secure Shell' y configure el puerto SSH en el puerto '8022'. A continuación, desplácese hacia abajo y haga clic en 'Guardar'.

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:



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.

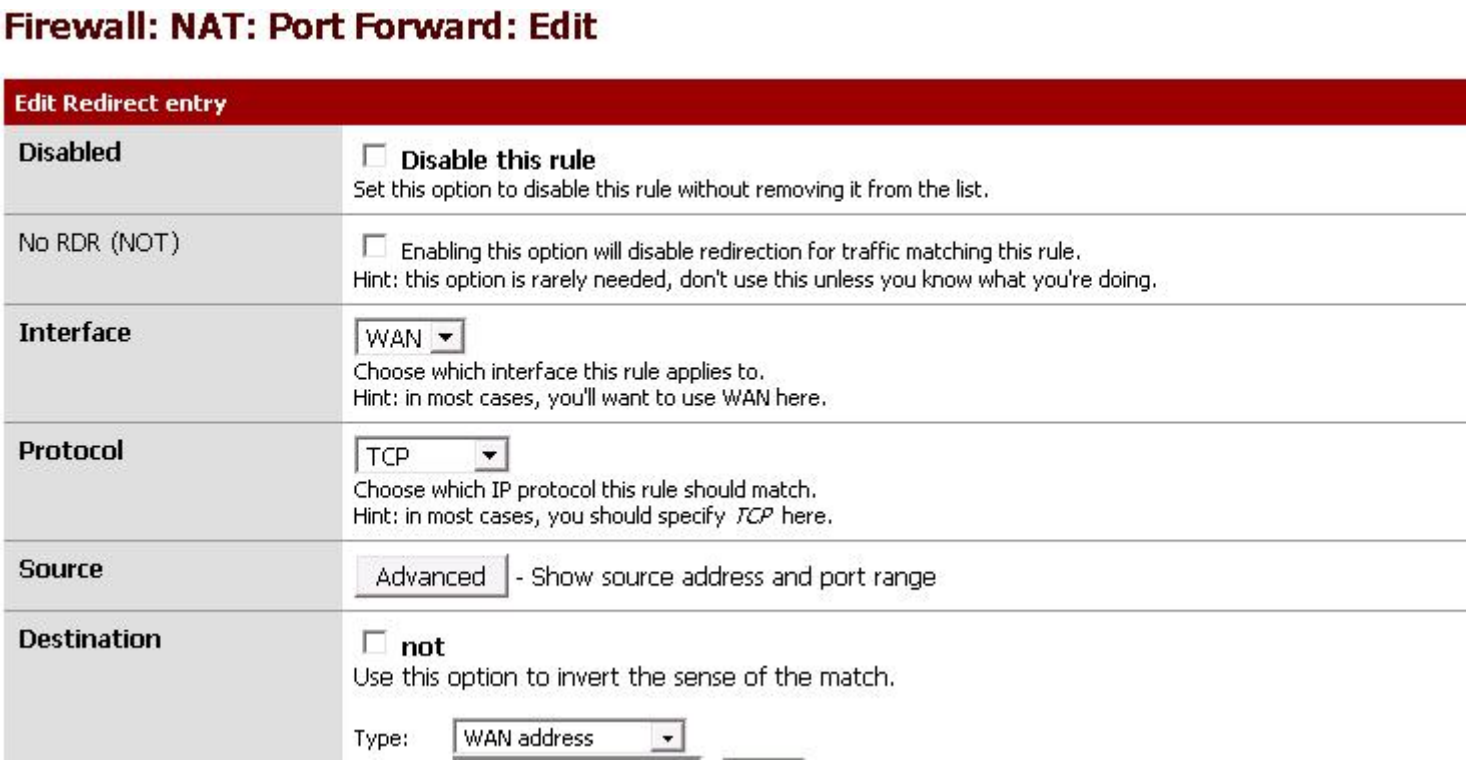
Ejemplos de reglas NAT

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':

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



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

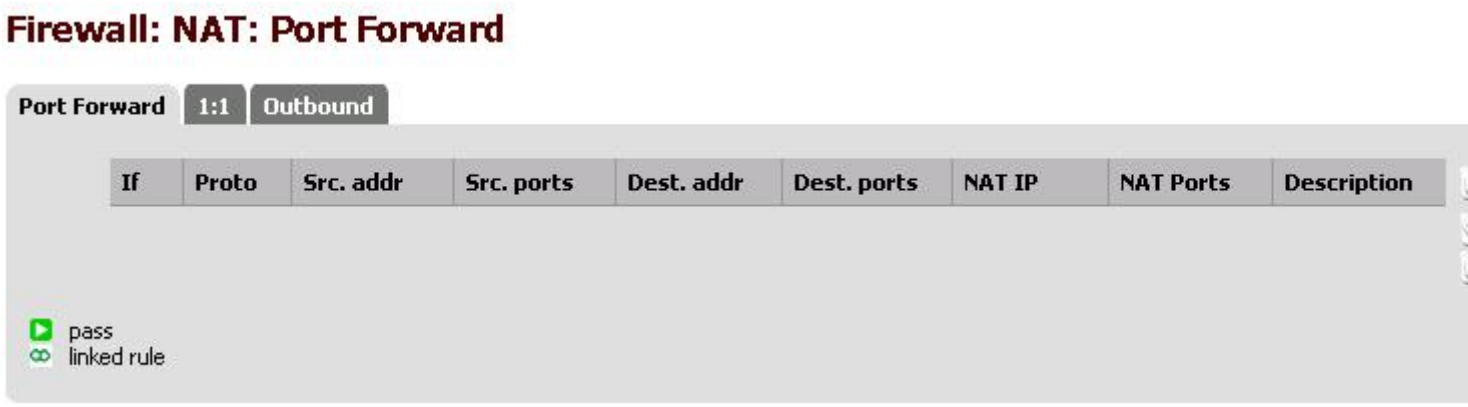
```
Disabled: Not selected
```

```
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
```

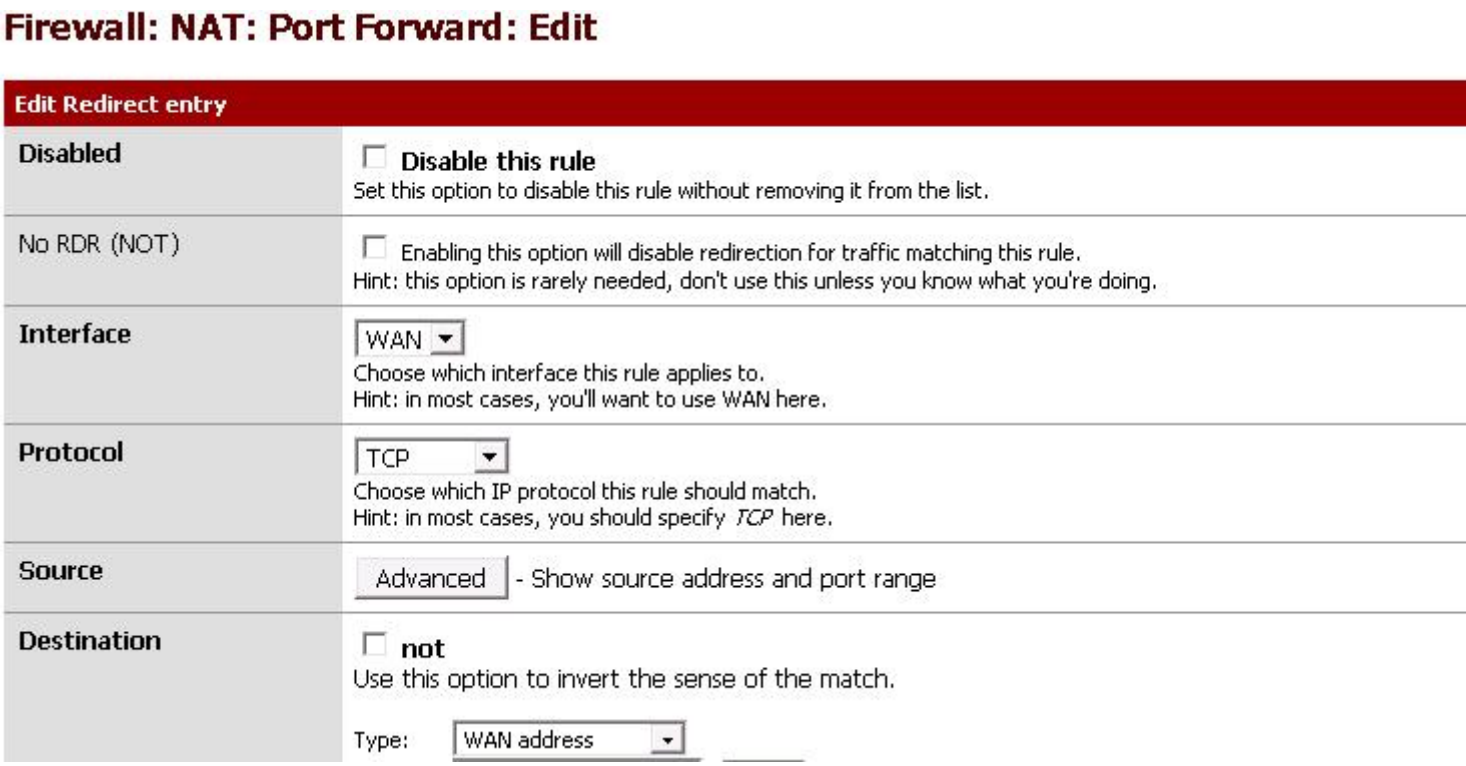
Haga clic en Guardar y Aplicar cambios. Ahora ya puede usar SSH en el servidor web (dirección IP como IP Pública en Firewall con el puerto 22), con el nombre de usuario y contraseña del servidor web.

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

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



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



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:

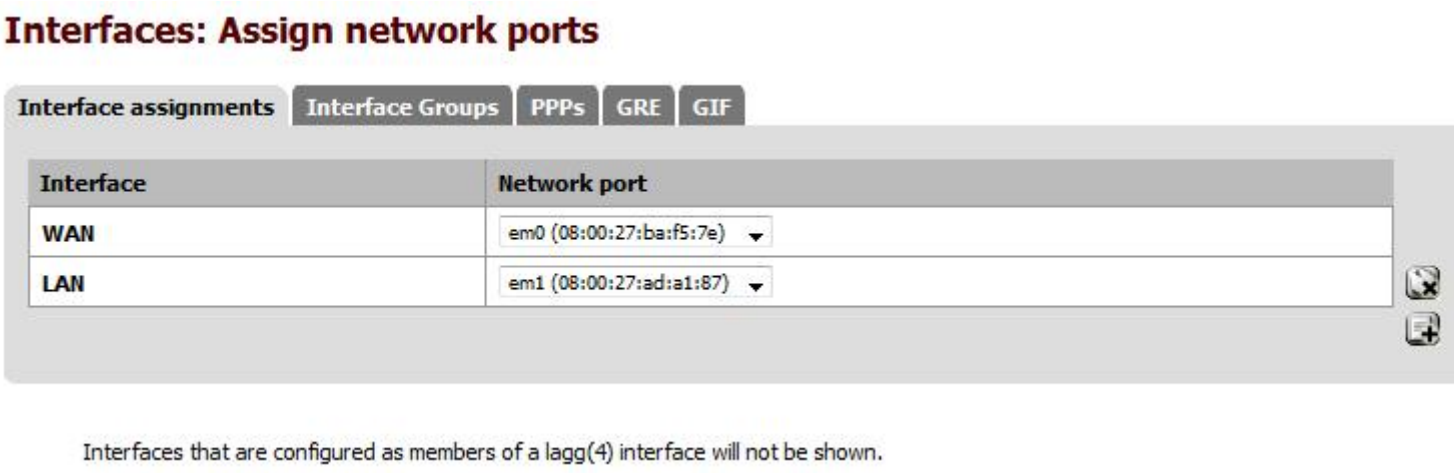
- Se necesita una interfaz para cada dirección IP Pública que haga NAT.
- Debe asegurarse que las interfaces con IPs Públicas adicionales han sido numeradas como NIC2 o sucesivas (la primera IP Pública se configura en el NIC 0 y la primera IP

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

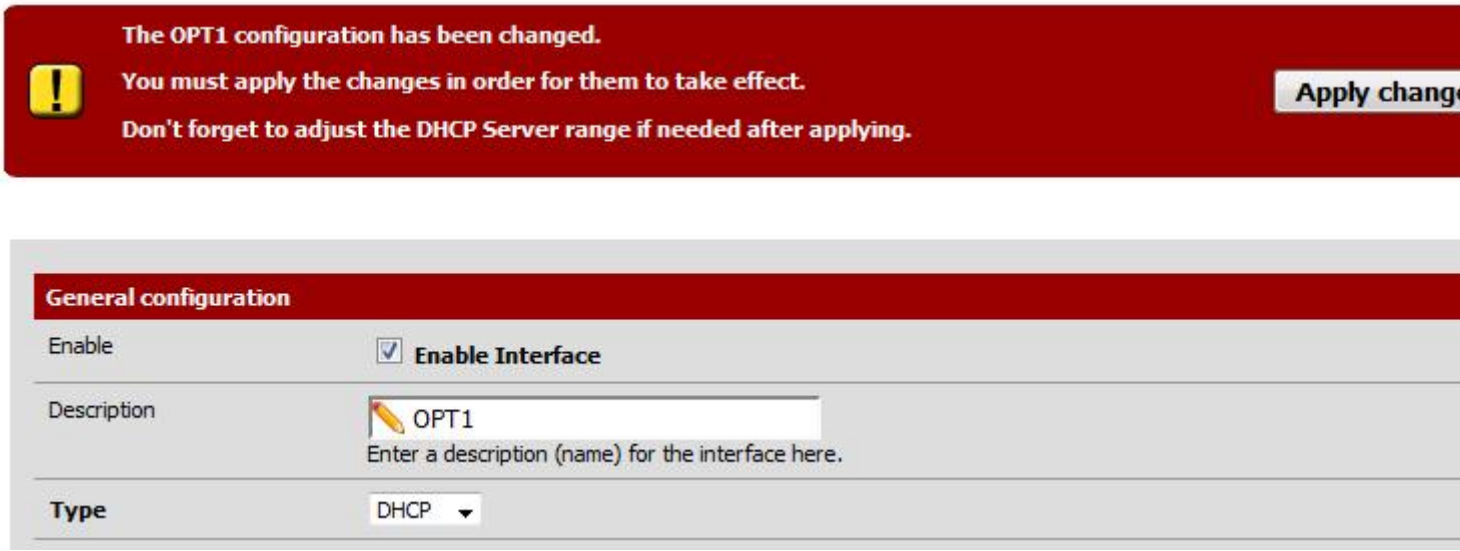
Siguiendo las instrucciones de configuración de Firewall indicadas anteriormente, su primera interfaz WAN irá asignada a em0 y su LAN en em1:



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

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.



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

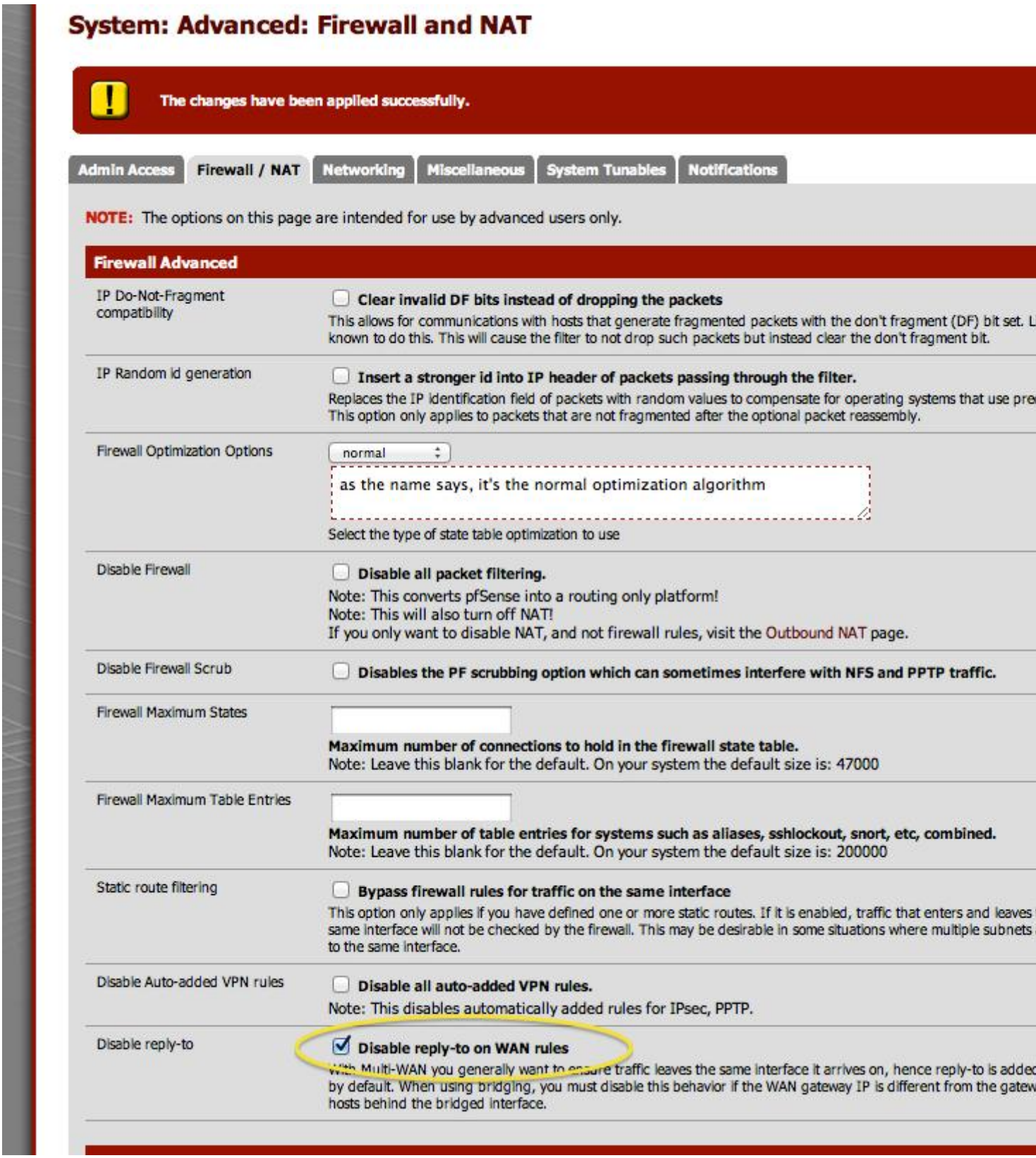
parámetros de configuración adicionales:

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'.

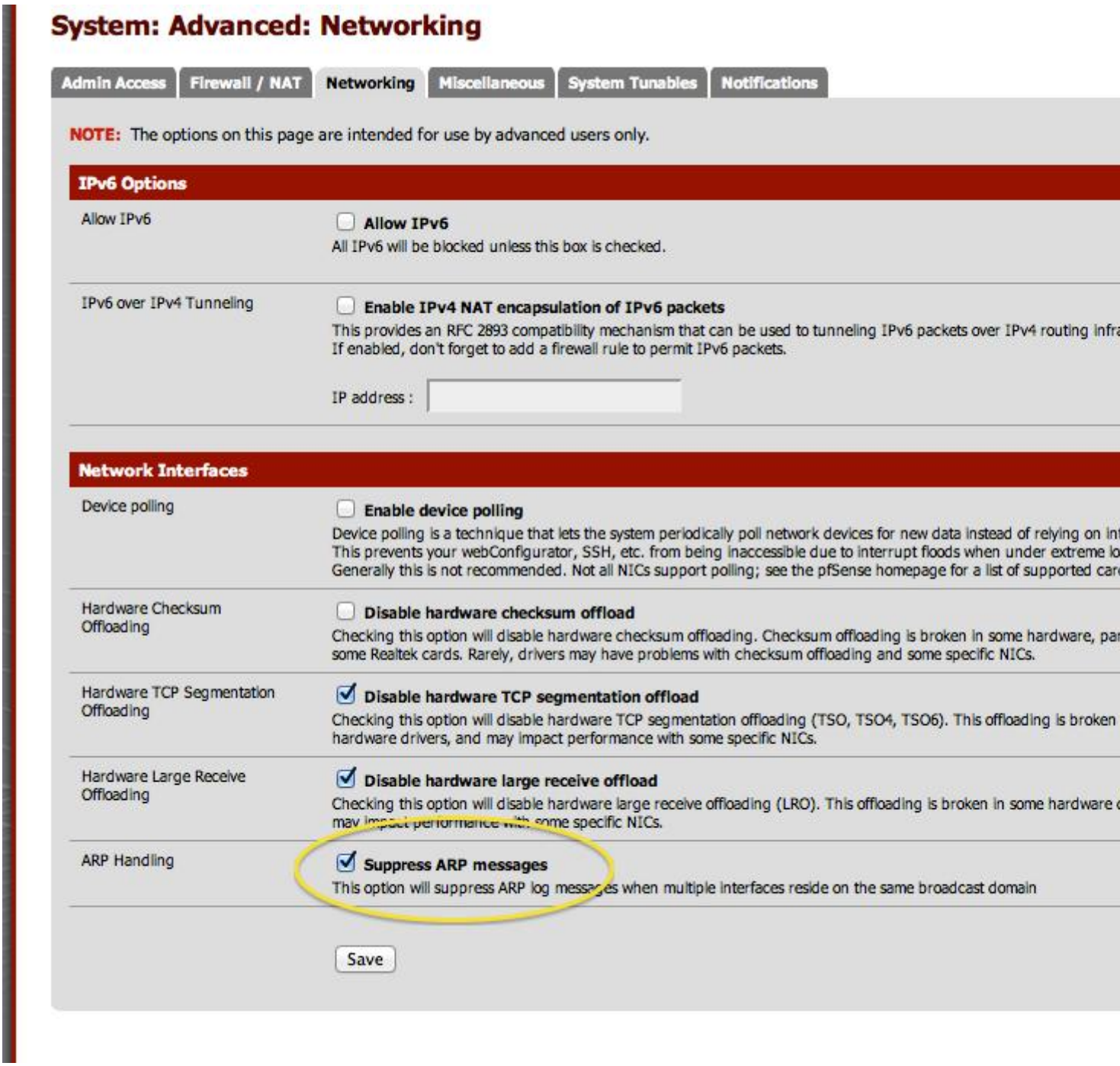
Haga clic en el botón Editar  situado junto al grupo 'súper usuario'. A continuación, desplácese hacia abajo hasta la parte inferior en la sección 'Asignación de privilegios' y haga clic en el icono  para añadir nuevos privilegios.

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'.



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':

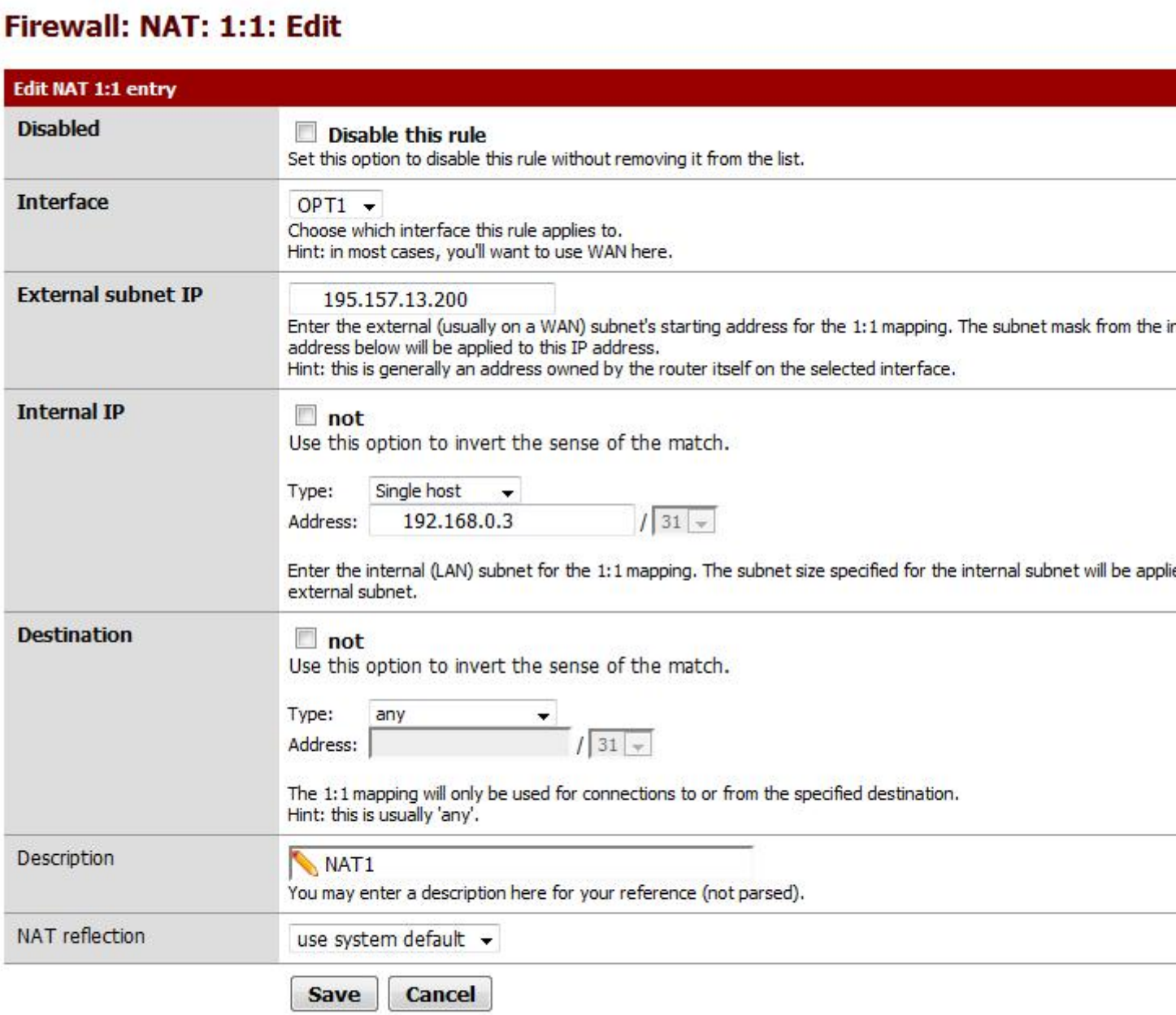


Haga clic en 'Guardar' para finalizar.

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).



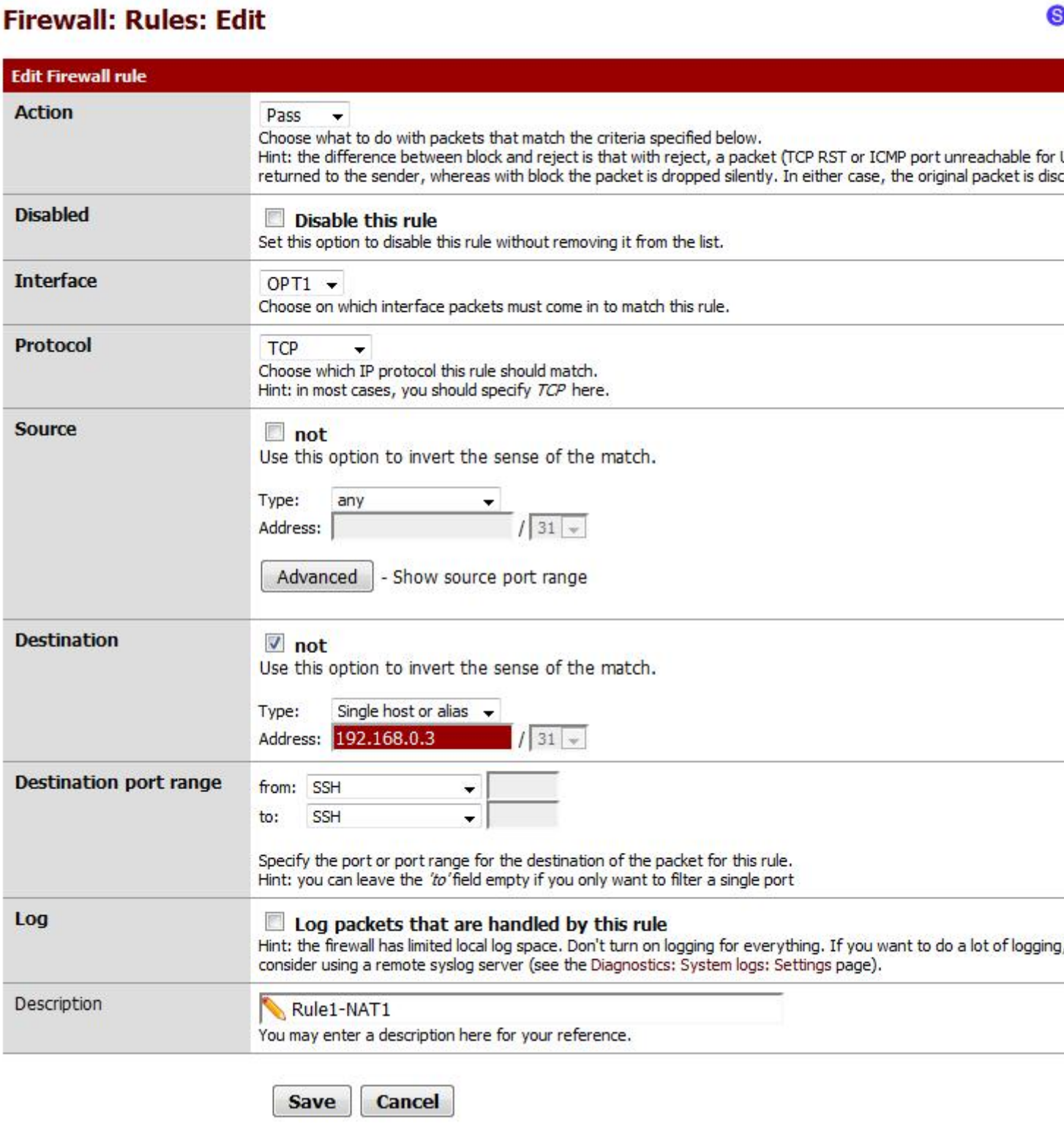
Configure la IP interna en la dirección IP Privada del host.

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.



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

Links:
[1] https://195.157.12.255
[2] http://#public