Published on *Cloud Hosting and Virtual Data Centre help* (http://cloudhelp.claranet.com)

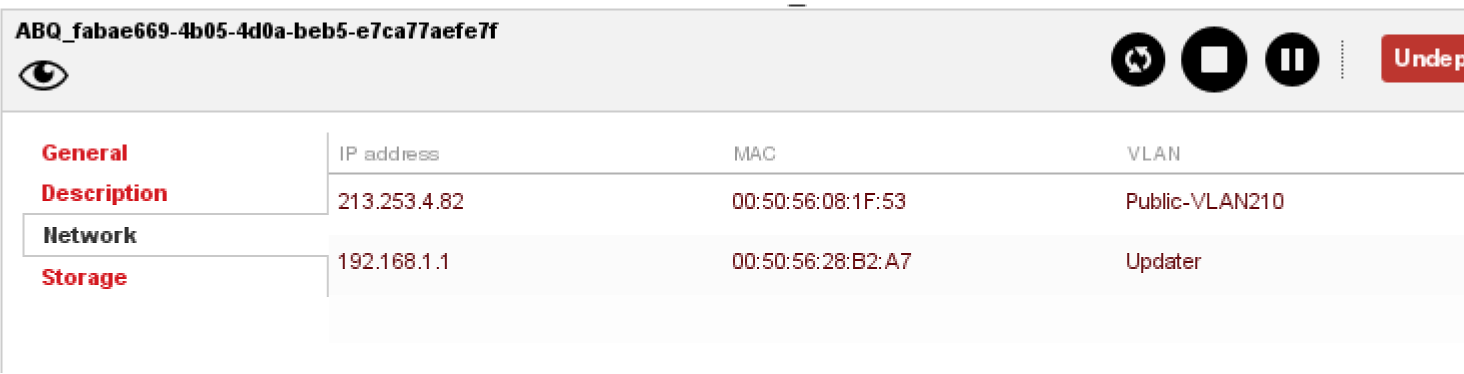
Home > Printer-friendly PDF

Getting Started with the pfSense firewall image

This page outlines the basics around pfSense firewalling and how you configure your firewall within the VDC platform.

Deploying the Firewall

The pfSense firewall should be initially deployed as per a normal Virtual Machine image. When you get to the stage of adding your network interfaces, it is important to ensure that NIC 0 (Ethernet interface 0) is the Public IP (or the first Public IP if there are many), and that NIC 1 is the Private or External interface. The base pfSense image as been preconfigured to expect these interfaces in this sequence.



ABQ_fabae669-4b05-4d0a-beb5-e7ca77aefe7f

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

For more information on how to how to do this, refer to the ?Configure Network Resources? section of the ?Configuring Virtual Machines? documentation

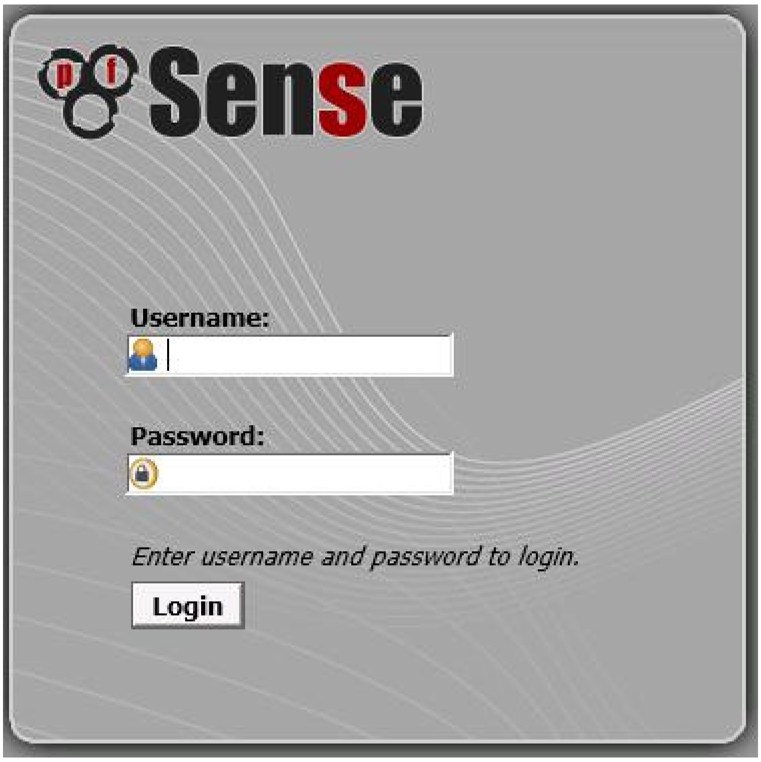
Configure the Firewall

You need to configure the firewall to allow traffic to and from the firewall, as well as allowing traffic from inside to outside and finally allowing port 80 (HTTP to the web server).

Firstly open up a web browser - enter the IP address of the public interface of the firewall that you allocated above.

NOTE: you need to use secure http eg: https://213.253.4.82 [1]

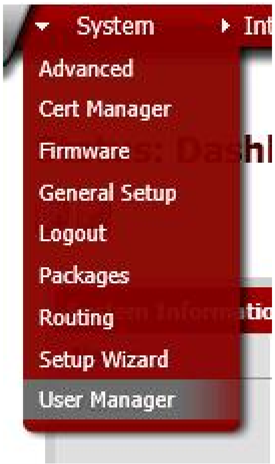
Ignore the certificate error by clicking on ?Continue to web site?. The following screen will appear:



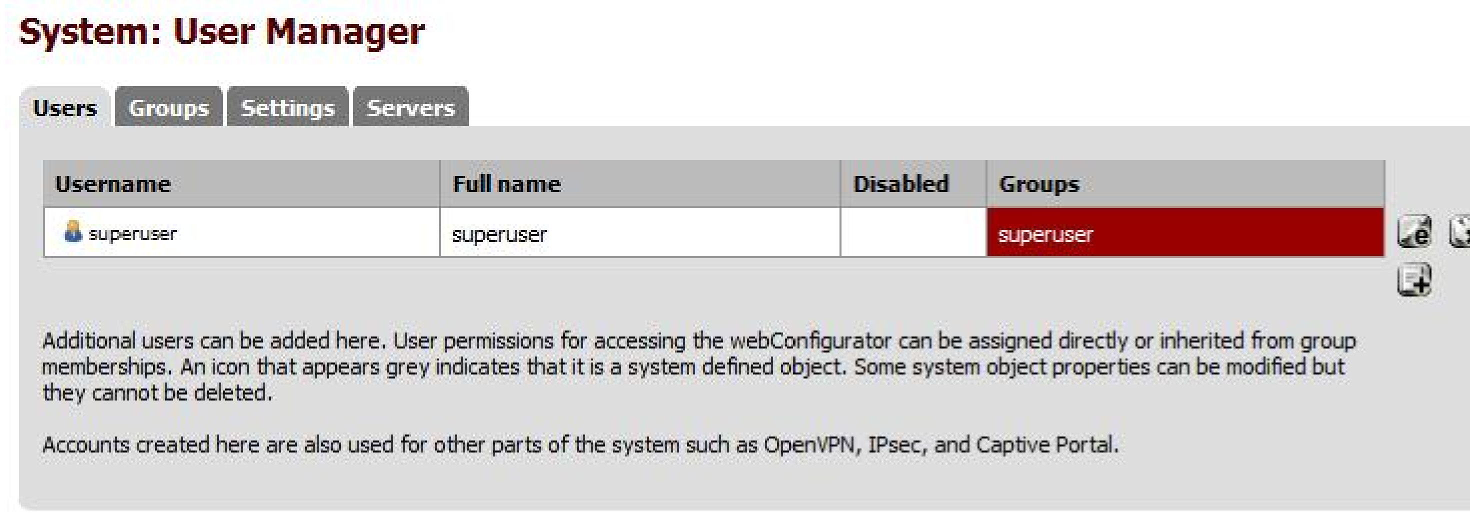
Enter username and password to login.

The default user id and password is located in the VM Templates - Login Details for Claranet Images page. You will now be presented with the main web page of the firewall.

The first step we need to complete is changing the default password for the admin user. Move your mouse over the System menu item at the top left hand side of the page until a drop down box appears and select ?User Manager?.



The following screen will appear:



System: User Manager

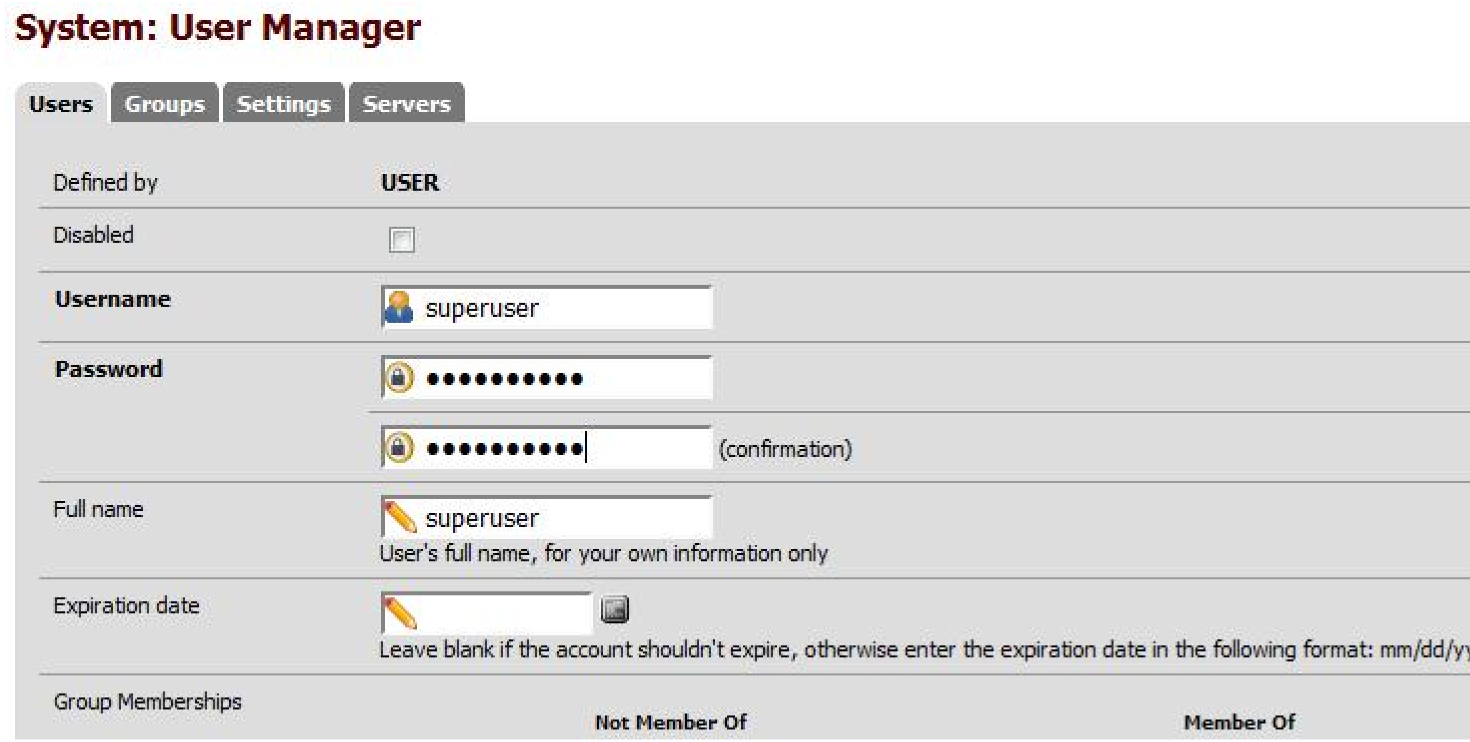
Username	Full name	Disabled	Groups
superuser	superuser		superuser

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.

Move the mouse over the edit icon to the right of the admin user?s line to edit the user.

The following screen will appear:

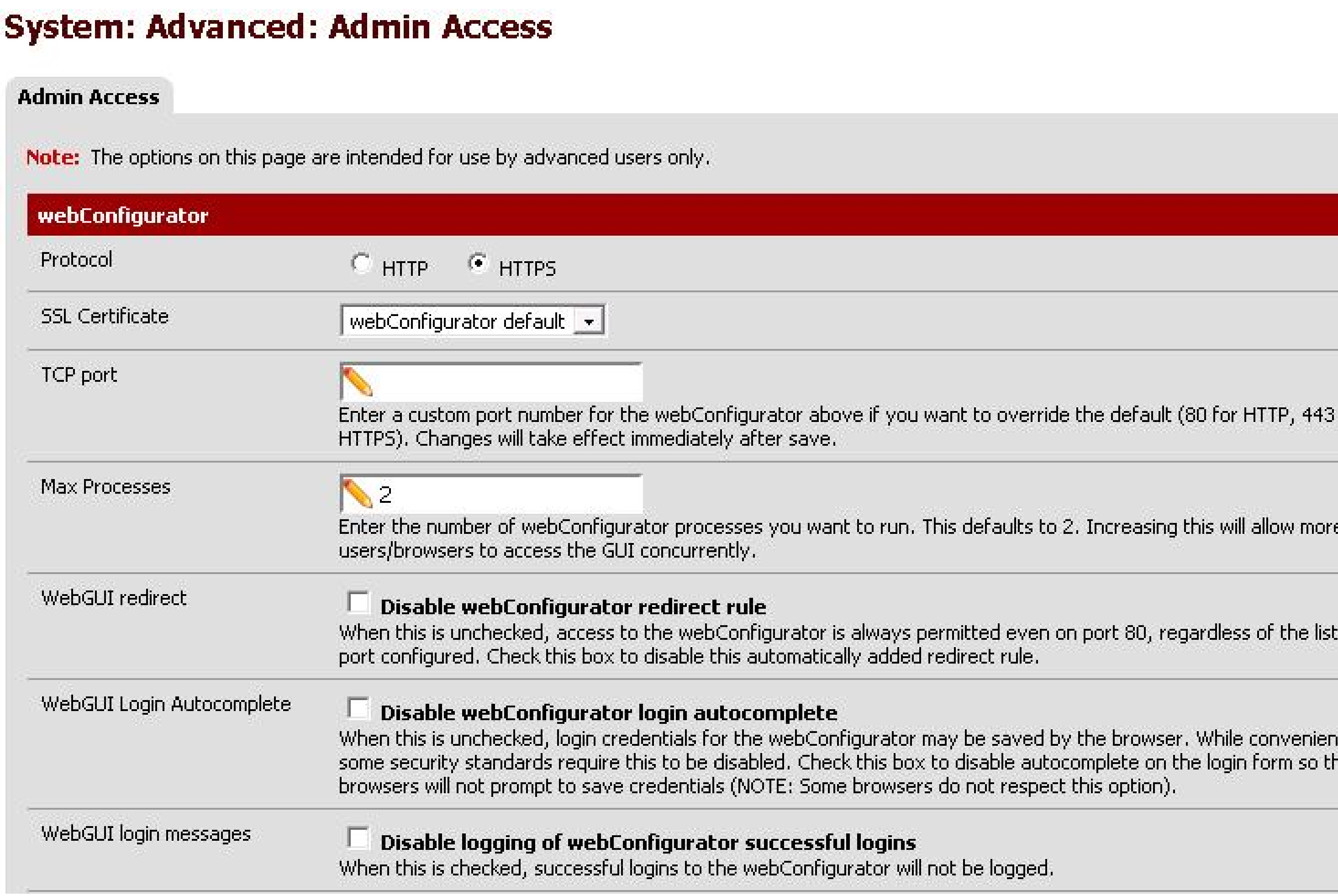


System: User Manager

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/y
Group Memberships	Not Member Of Member Of

Type a new password where indicated (Twice). Scroll down and click save.

Next we need to move the SSH port, this will allow you to access the Web Server via SSH. Select ?System? ? ?Advanced? and the following screen will appear:



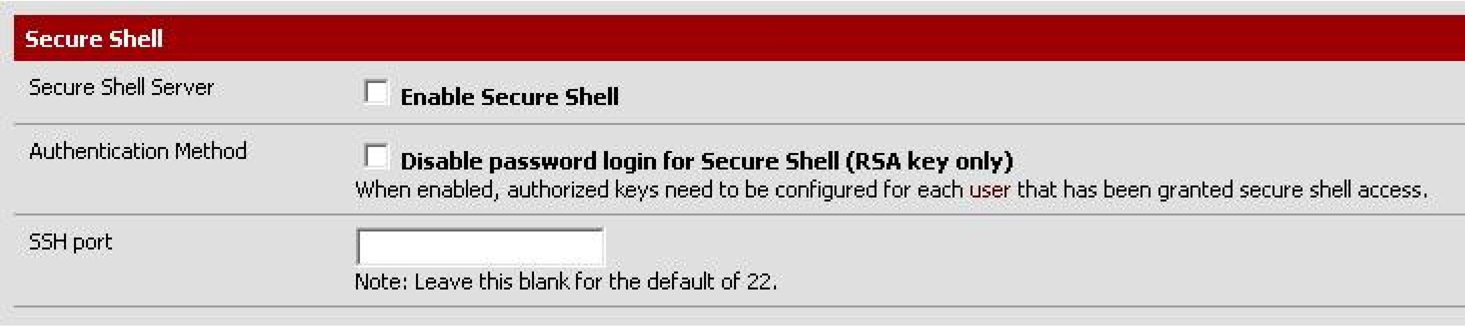
System: Advanced: Admin Access

Admin Access

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

webConfigurator	
Protocol	○ HTTP ● HTTPS
SSL Certificate	webConfigurator default
TCP port	Enter a custom port number for the webConfigurator above if you want to override the default (80 for HTTP, 443 HTTPS). Changes will take effect immediately after save.
Max Processes	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	□ **Disable webConfigurator redirect rule** When this is unchecked, access to the webConfigurator is always permitted even on port 80, regardless of the list port configured. Check this box to disable this automatically added redirect rule.
WebGUI Login Autocomplete	□ **Disable webConfigurator login autocomplete** When this is unchecked, login credentials for the webConfigurator may be saved by the browser. While convenien some security standards require this to be disabled. Check this box to disable autocomplete on the login form so th browsers will not prompt to save credentials (NOTE: Some browsers do not respect this option).
WebGUI login messages	□ **Disable logging of webConfigurator successful logins** When this is checked, successful logins to the webConfigurator will not be logged.

Scroll down to the SSH section:



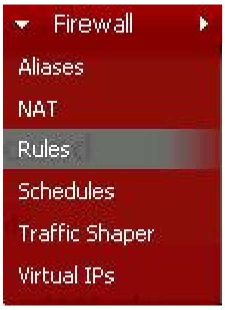
Secure Shell	
Secure Shell Server	□ **Enable Secure Shell**
Authentication Method	□ **Disable password login for Secure Shell (RSA key only)** When enabled, authorized keys need to be configured for each user that has been granted secure shell access.
SSH port	Note: Leave this blank for the default of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

Click to ?Enable Secure Shell? and set the SSH port to ?8022?. Scroll down and click ?Save?.

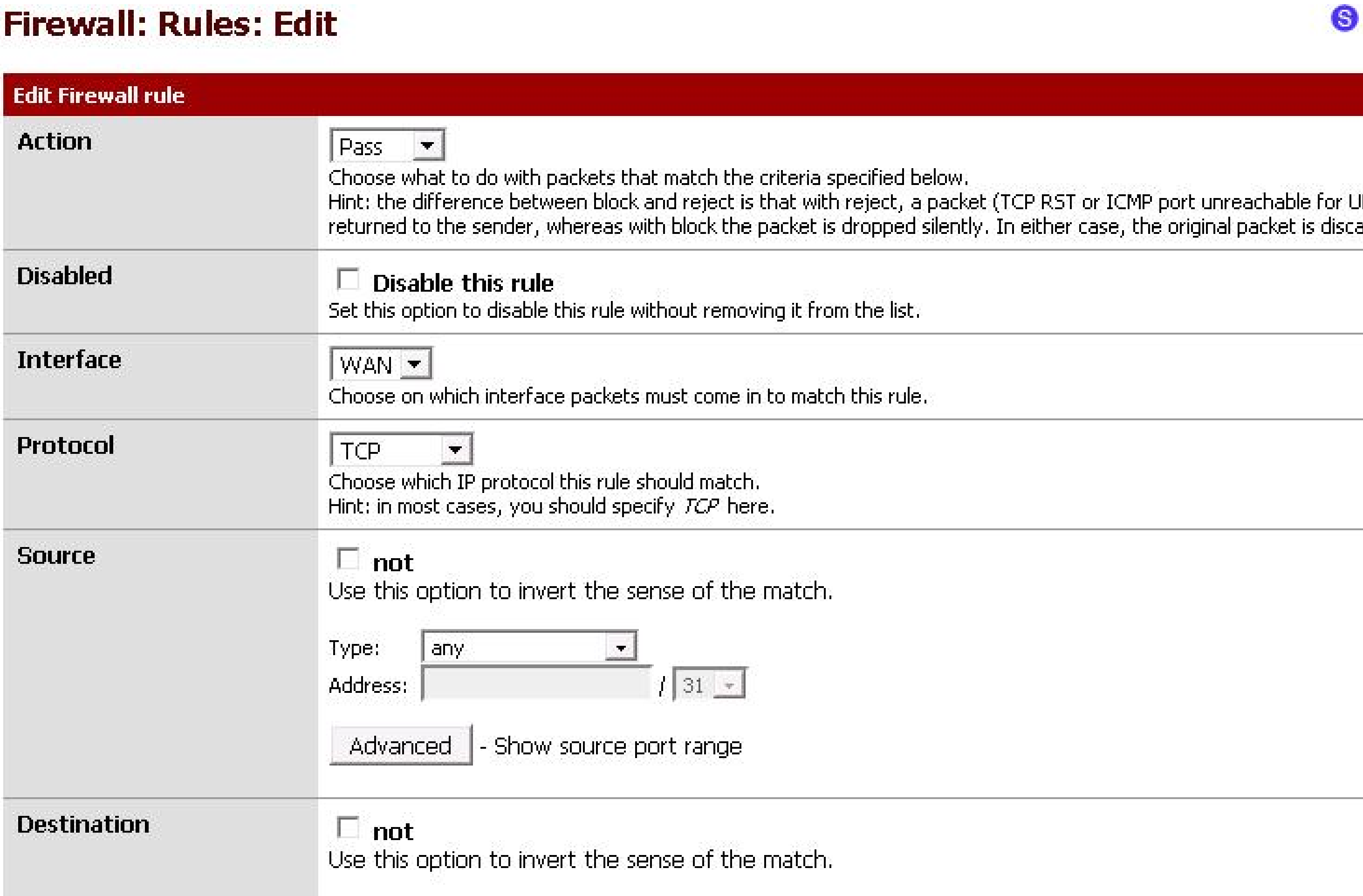
Next we need to configure the firewall with the following rules:

Allow SSH on port 8022 to Firewall

Select ?Firewall? ? ?Rules?



Select ?WAN? and then click ⊞ to add a new rule:



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 U returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is disca
Disabled	□ **Disable this rule** Set this option to disable this rule without removing it from the list.
Interface	WAN ▾ Choose on which interface packets must come in to match this rule.
Protocol	TCP ▾ Choose which IP protocol this rule should match. Hint: in most cases, you should specify *TCP* here.
Source	□ **not** Use this option to invert the sense of the match. Type: any ▾ Address: / 31 ▾ Advanced - Show source port range
Destination	□ **not** Use this option to invert the sense of the match.

Enter the following:

```
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
```

Click Save and Apply Changes. You are now able to ssh using your preferred tool on port 8022.

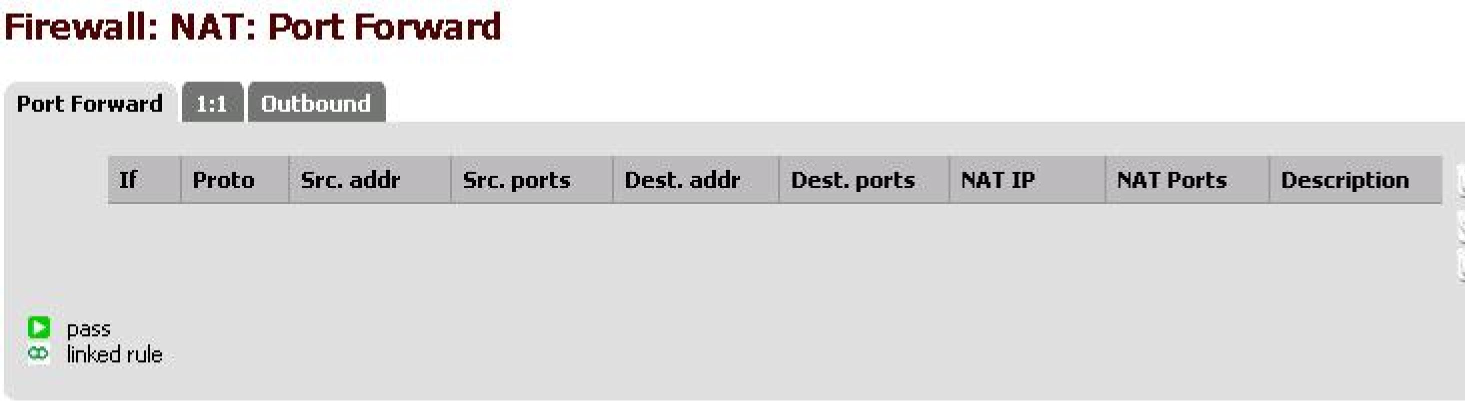
Example NAT rules

Please note: PfSense can only automatically configure outbound NAT if your internal interfaces are statically and not DHCP assigned. If you wish to have DHCP assigned internal interfaces, you must move to hybrid automation and configure the outbound NAT rule yourself.

The following section provides some example NAT configurations

Example NAT rule - Allow SSH on port 22 to Web Server

Select ?Firewall? ? ?Nat? and the select ?Port Forward?:



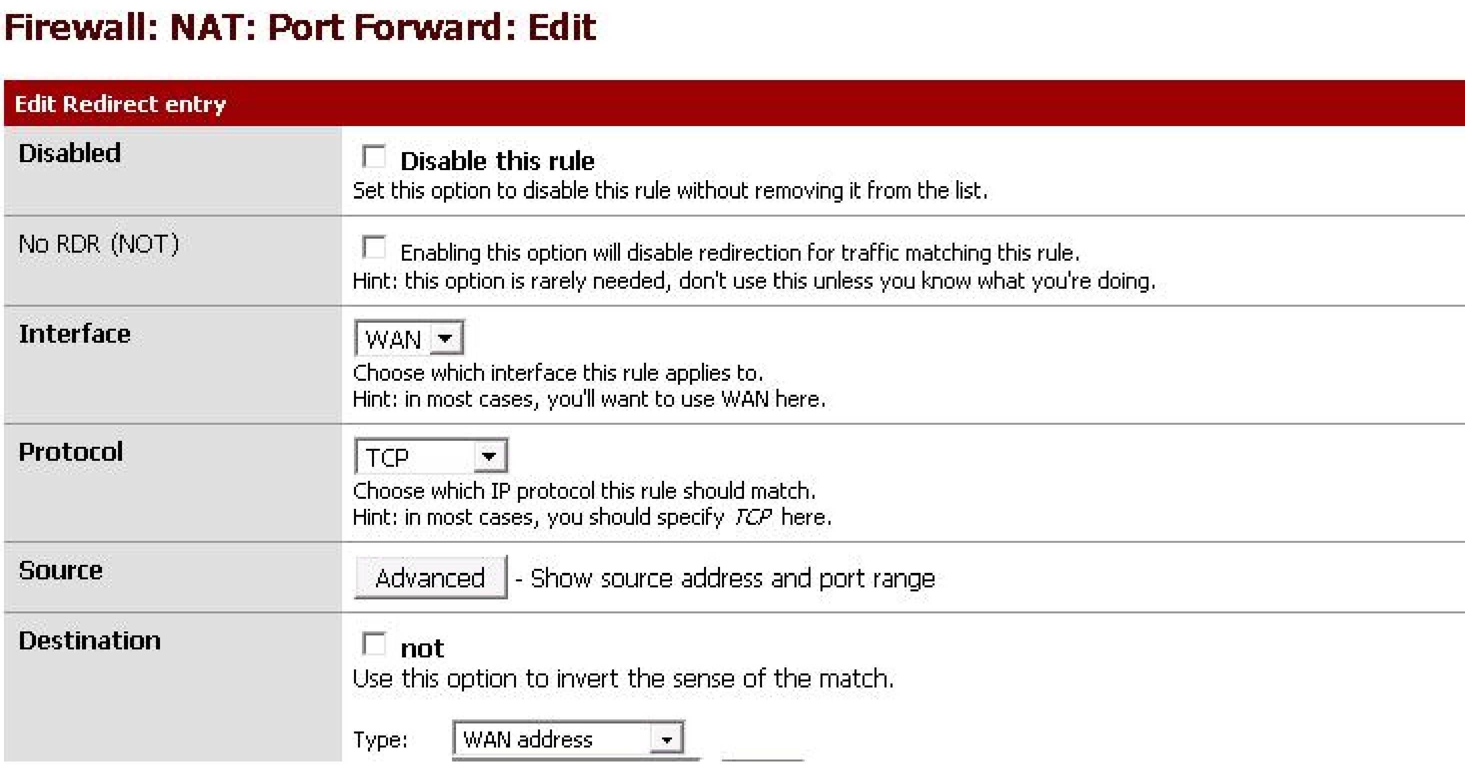
Firewall: NAT: Port Forward

Port Forward | 1:1 | Outbound

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

🟩 pass
∞ linked rule

Click on the Add NAT Rule button



Firewall: NAT: Port Forward: Edit

Edit Redirect entry

Disabled	□ Disable this rule 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 ▾

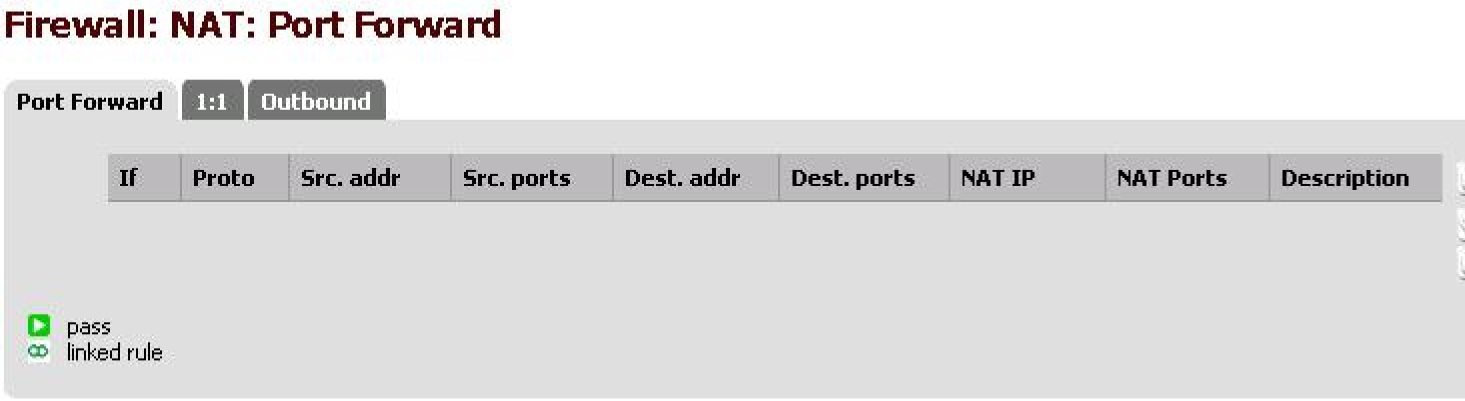
Configure the following:

```
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
```

Click on Save and then apply rule. You can now SSH into the web server (IP address as public IP on firewall with port 22), with user the username and password details of the webserver.

Example NAT rule - Allow HTTP on port 80 to Web Server

Select ?Firewall? ? ?Nat? and the select ?Port Forward?:

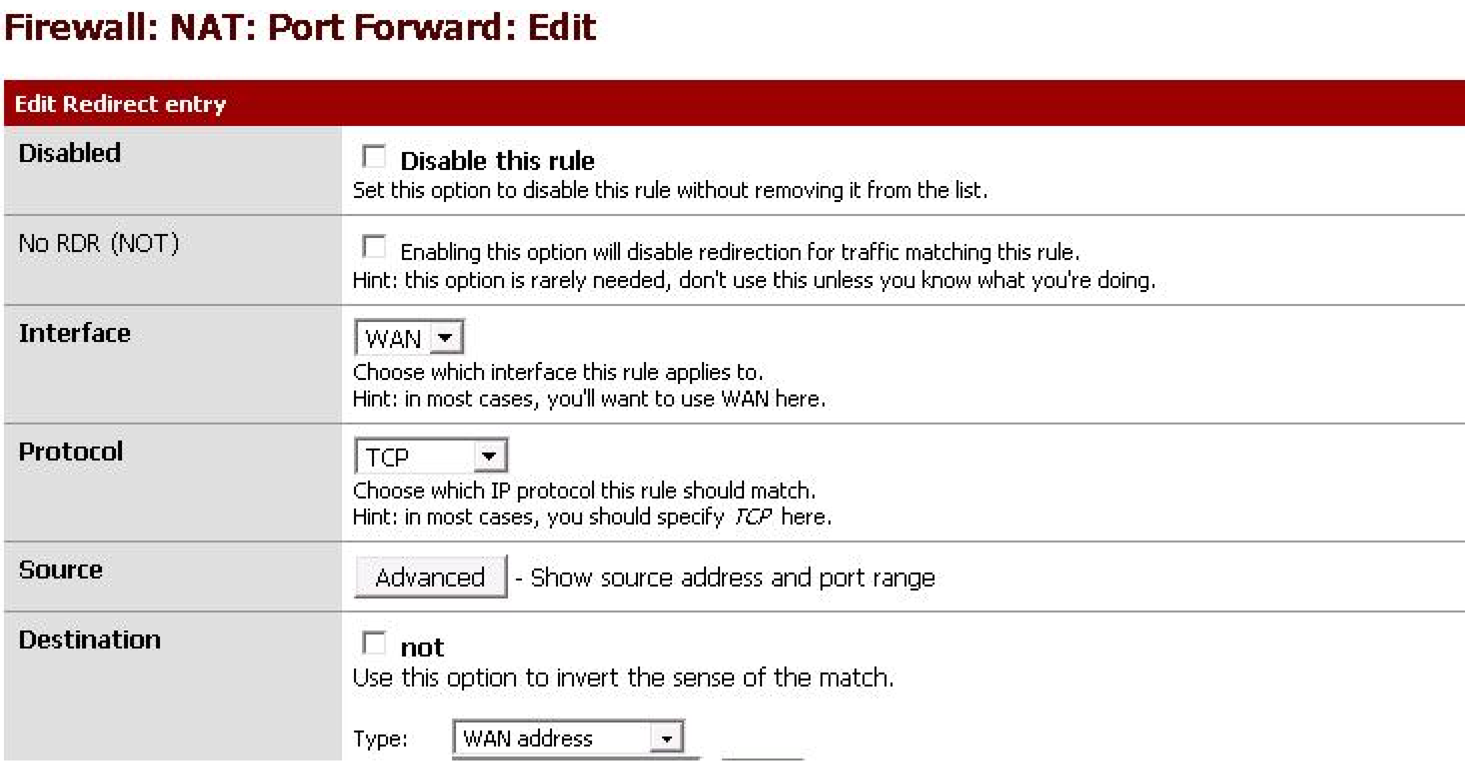


Firewall: NAT: Port Forward

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

▶ pass
∞ linked rule

Click on the Add NAT Rule button



Firewall: NAT: Port Forward: Edit

Edit Redirect entry	
Disabled	□ Disable this rule 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 ▾

Configure the following:

```
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
```

Click on Save and then apply rule. You should now be able to view a webpage served from your webserver by browsing to http://#public [2] IP of your firewall#.

1:1 NAT mapping

The following section provides instructions on how to configure 1:1 NAT mapping with multiple public IP addresses.

In this example, a Public IP of 195.157.13.200 was to be made to NAT to Private address of 192.168.0.3

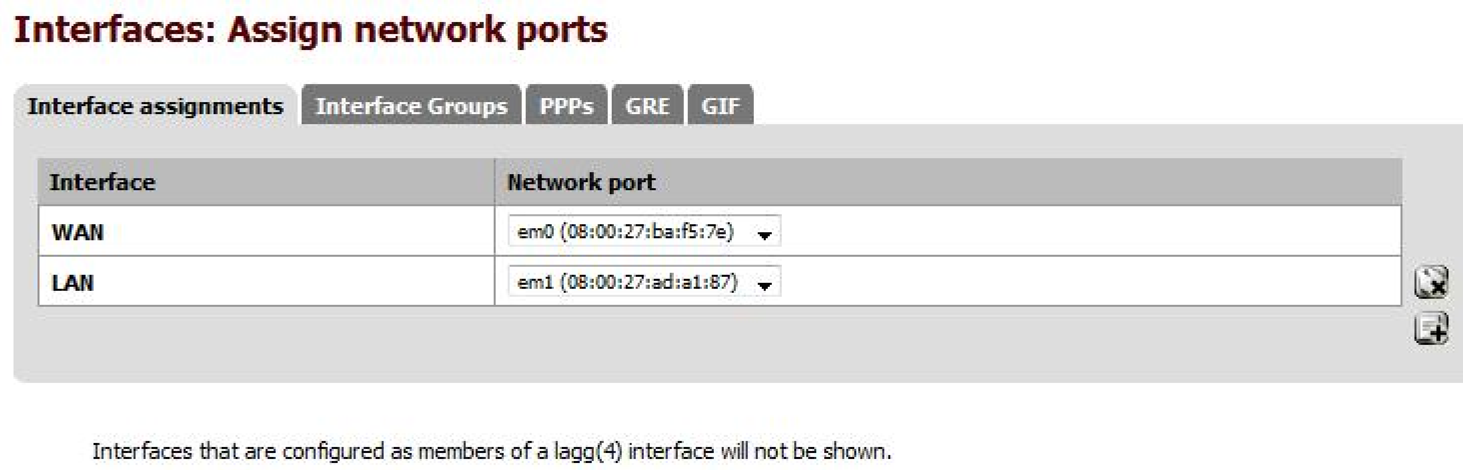
Things you have to do to make this work:

- You need a public IP interface for each public IP address you want to NAT.

- You need to ensure additional Public IP Interfaces are numbered NIC2 or higher (preserving the 1st Public IP on NIC 0 and First Private/External IP on NIC 1 as detailed earlier)
- You need to set up 1:1 NAT for this IP
- You need to create a rule to allow the port you want for this IP.

Assign additional interface

Following the firewall setup instructions earlier, your first WAN interface will be assigned to em0, and your LAN to em1:

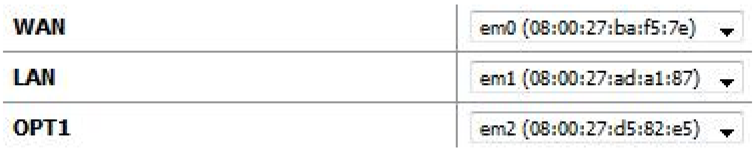


Interfaces: Assign network ports

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.

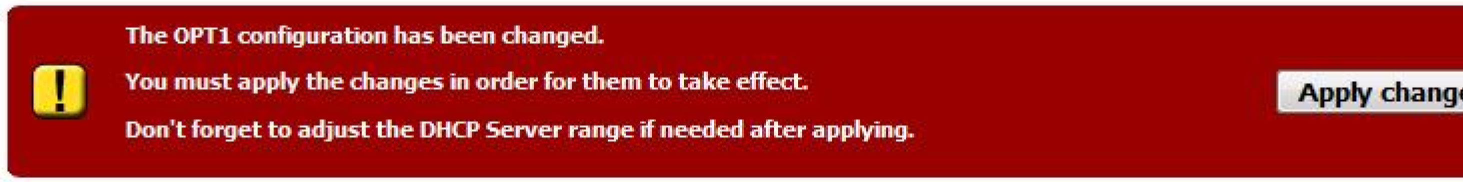
Click the ⊞ button to assign a new interface. OPT1 will automatically appear attached to em2:



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

Select Interfaces menu item, OPT1

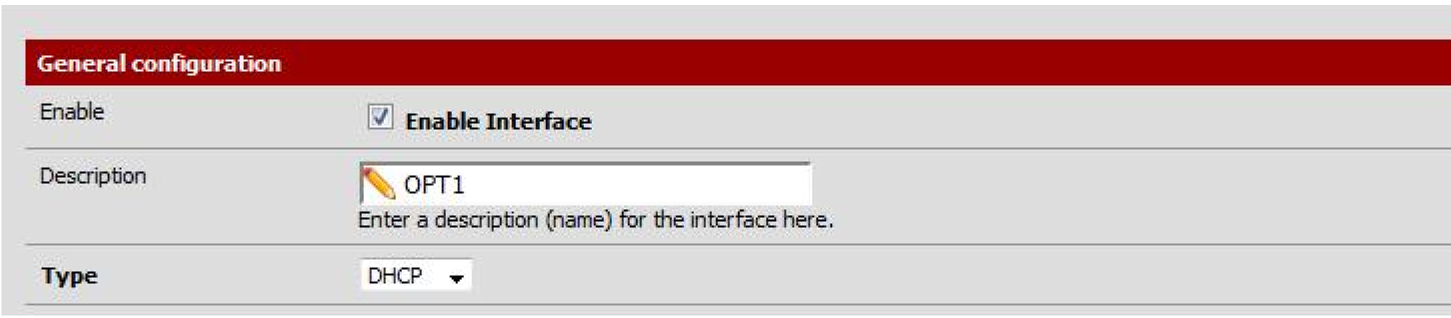
Select Enable at the top and set type to DHCP. Save changes and click Apply changes



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.



General configuration

Enable	☑ Enable Interface
Description	OPT1 Enter a description (name) for the interface here.
Type	DHCP

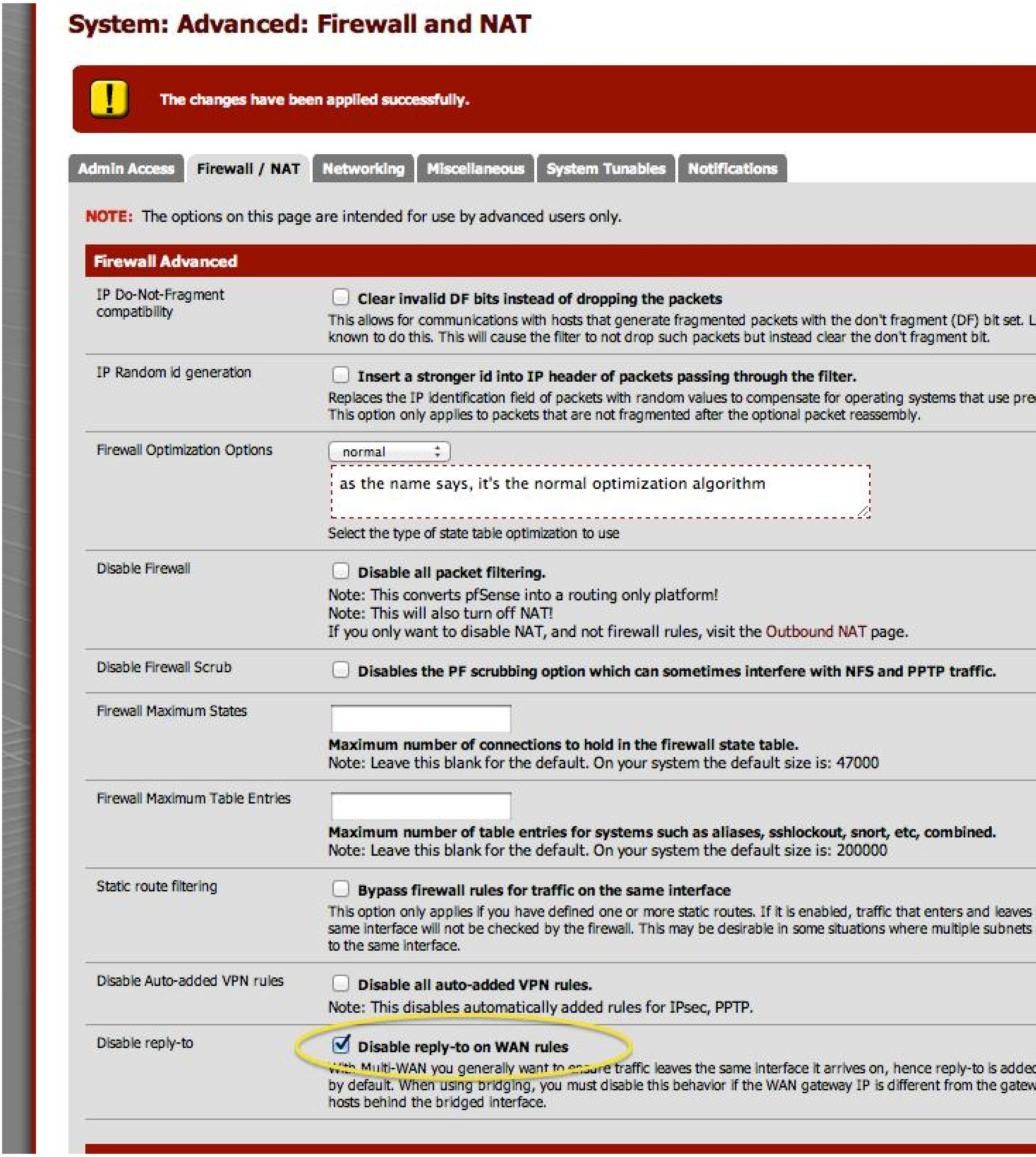
If you are using multiple interfaces with 1:1 NAT mapping to each, you will need to add the following additional configuration parameters:

Firstly, you'll need to open up the additional firewall config options. Go to the 'System' menu, 'User Manager', then click on the 'Groups' tag.

Click on the edit button next to the 'Superuser' group. Next scroll down to the bottom of the 'Assigned Privileges' section, and click to add some new privileges.

On the Add Privileges page, click 'Select all', and then 'Save'.

Now you'll need to disble Reply-To. Go to the 'System' menu, 'Advanced' and click the 'Firewall / NAT' tab. Click the 'Disable reply-to on WAN rules' check box.



System: Advanced: Firewall and NAT

The changes have been applied successfully.

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. L
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 pre
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
same interface will not be checked by the firewall. This may be desirable in some situations where multiple subnets
to the same interface.

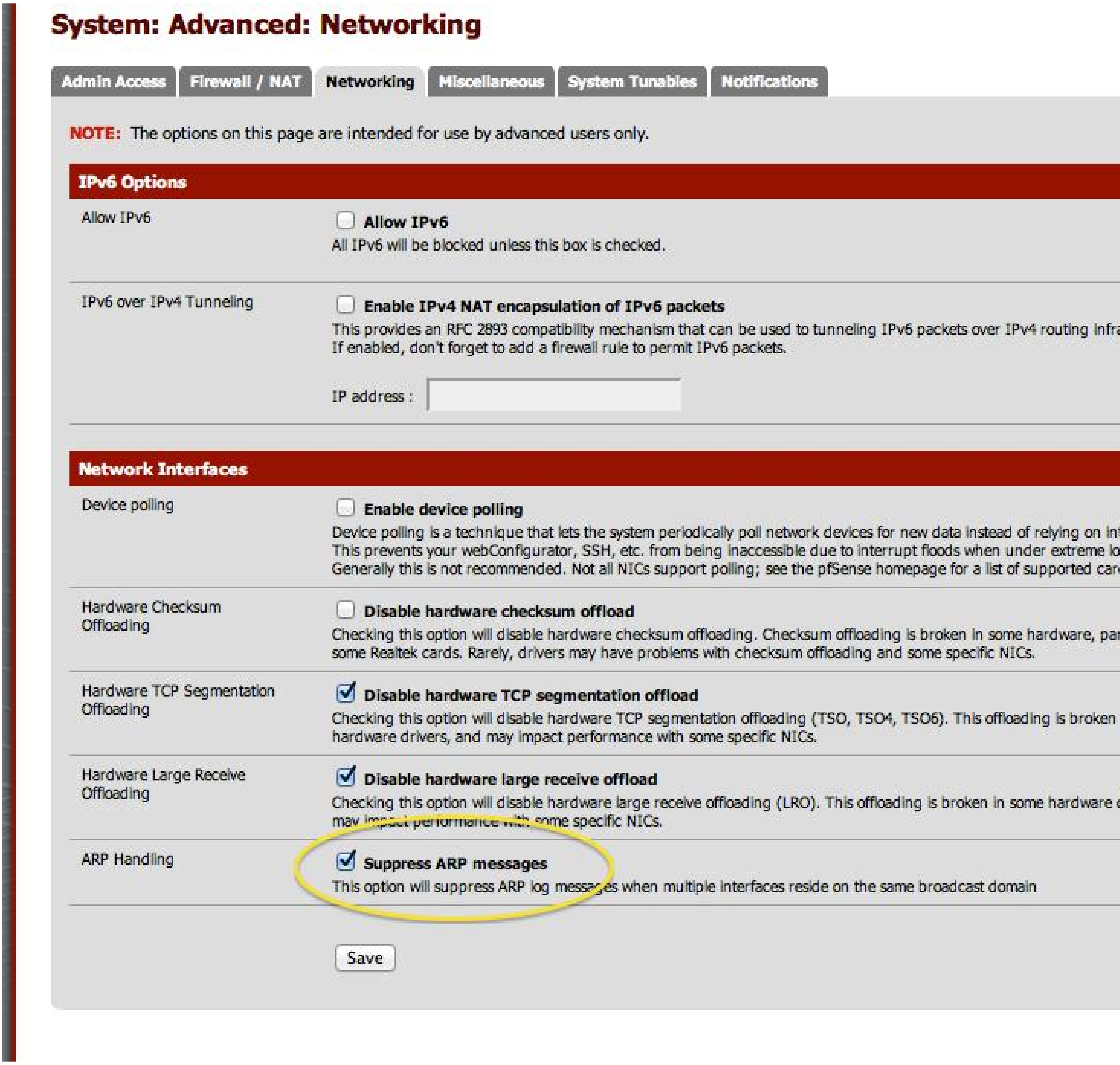
Disable Auto-added VPN rules

□ **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 addec
by default. When using bridging, you must disable this behavior if the WAN gateway IP is different from the gatew
hosts behind the bridged interface.

Click 'Save'. Next, go to the 'System' menu, 'Advanced' and click on the 'Networking' tab. Click 'Suppress ARP messages':



System: Advanced: Networking

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 infra
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 int
This prevents your webConfigurator, SSH, etc. from being inaccessible due to interrupt floods when under extreme lo
Generally this is not recommended. Not all NICs support polling; see the pfSense homepage for a list of supported car

Hardware Checksum Offloading — □ **Disable hardware checksum offload**
Checking this option will disable hardware checksum offloading. Checksum offloading is broken in some hardware, par
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
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 d
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

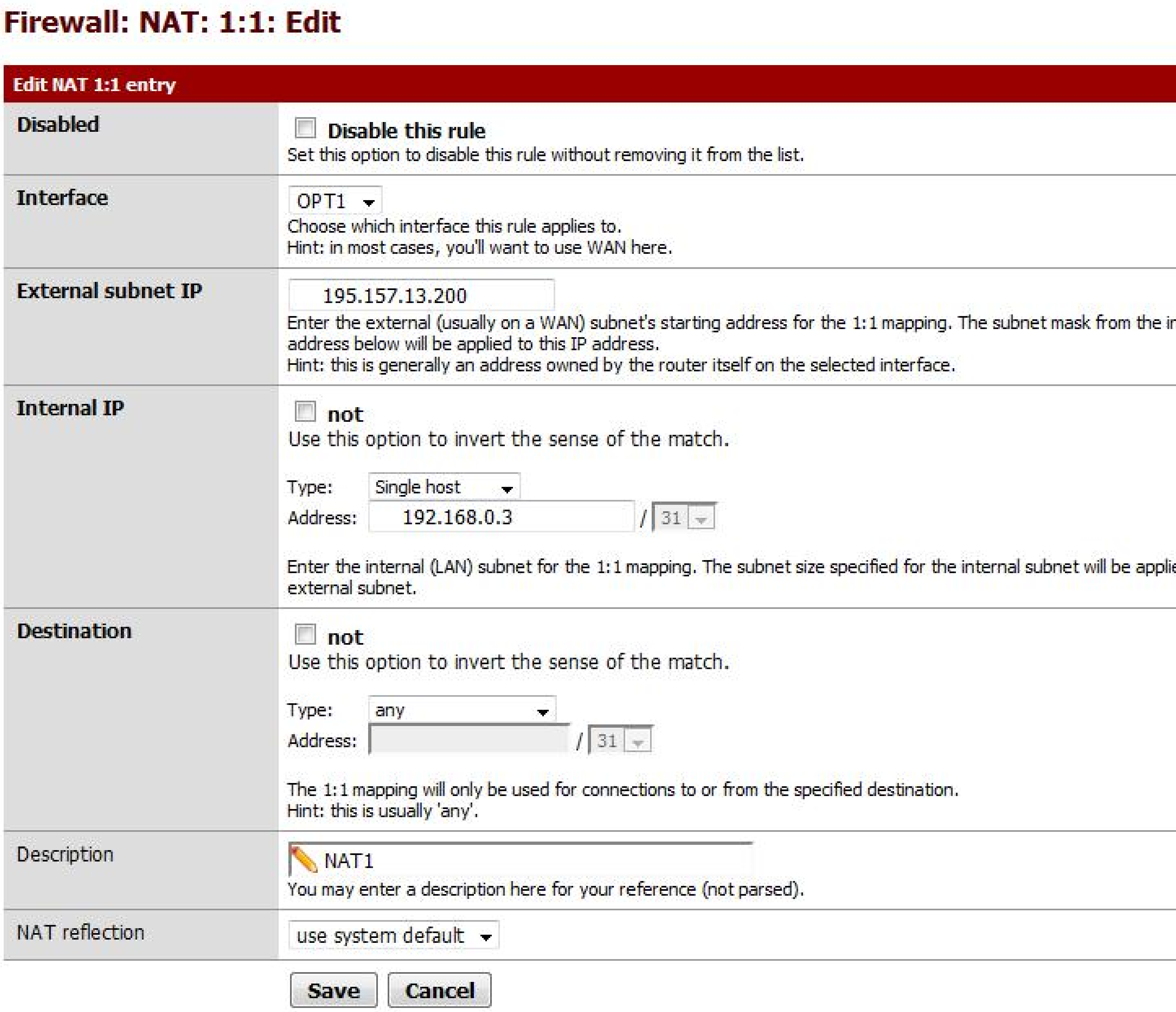
Save

Click 'Save' to finish.

Configure 1:1 NAT

Click ?FIREWALL? and ?NAT?. Select the 1:1 tab.

Select ⊞ to add new rule and set Interface to OPT1, External Subnet to the public IP address (subnet should be 32 if it is just a single IP address you want to NAT).



Firewall: NAT: 1:1: Edit

Edit NAT 1:1 entry	
Disabled	□ **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 ir 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	□ **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 applie external subnet.
Destination	□ **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

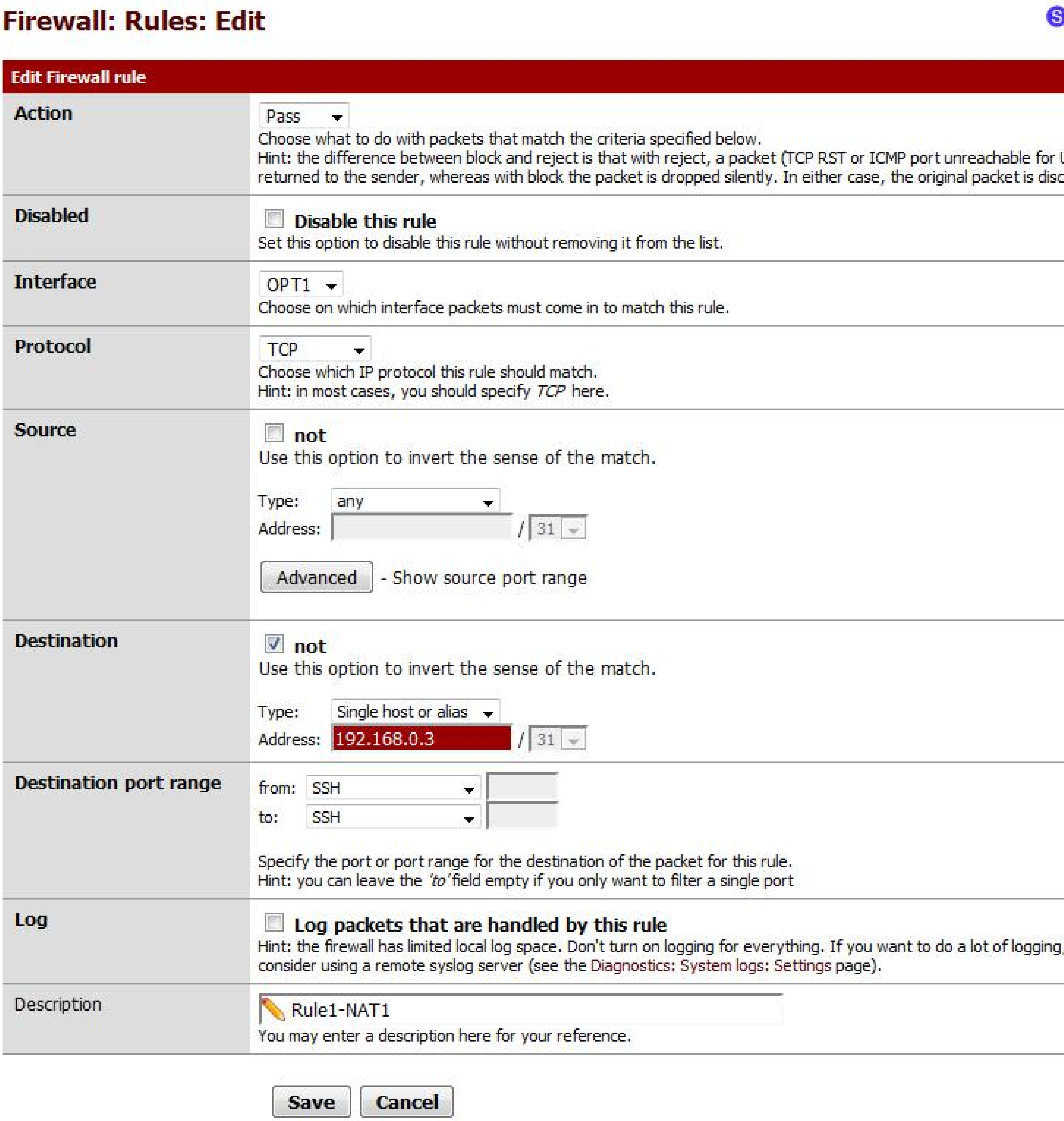
Set the Internal IP to the private IP address of the host you want to reach.

Set a description for this NAT rule and SAVE. Apply changes to the system.

Apply a firewall rule

Select the menu option FIREWALL and select RULES

Select OPT1 tab. Select ⊞ to create new rule



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 U returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is disc
Disabled	□ **Disable this rule** Set this option to disable this rule without removing it from the list.
Interface	OPT1 Choose on which interface packets must come in to match this rule.
Protocol	TCP Choose which IP protocol this rule should match. Hint: in most cases, you should specify *TCP* here.
Source	□ **not** Use this option to invert the sense of the match. Type: any Address: / 31 Advanced - Show source port range
Destination	☑ **not** Use this option to invert the sense of the match. Type: Single host or alias Address: 192.168.0.3 / 31
Destination port range	from: SSH to: SSH 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	□ **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	Rule1-NAT1 You may enter a description here for your reference.

Make sure interface is set to 'OPT1' or whatever interface name you are using for this public IP address. Set

Destination type to 'single address' and specify the private IP address of host you want to reach, in this case 192.168.0.3

Set the destination port range, in this case SSH. Set a description for this rule.

Save changes and apply changes.

You should now be able to make an ssh connection to the public IP address on 195.157.13.200 and this should be redirected to 192.168.0.3.

Source URL: http://cloudhelp.claranet.com/content/getting-started-pfsense-firewall-image

Links:
[1] https://213.253.4.82
[2] http://#public