



User Guide

v1.0

Contents

1	General Configuration	5
1.1	General Configuration Options	5
1.2	Advanced Configuration Options.....	5
2	Network Address Translation	5
2.1	Configuring 1:1 NAT.....	5
2.1.1	Interface.....	5
2.1.2	External subnet.....	6
2.1.3	Internal subnet	6
2.1.4	Description	6
2.1.5	Example single IP 1:1 configuration	6
2.1.6	Example IP range 1:1 configuration.....	6
2.2	Outbound NAT.....	7
2.2.1	Default Outbound NAT Rules.....	7
2.2.2	Static Port.....	7
2.2.3	Disabling Outbound NAT.....	8
2.3	Aliases	8
2.3.1	Configuring Aliases	8
3	Firewall	8
3.1	Firewall Rules	8
3.1.1	Adding a firewall rule.....	9
3.1.2	Editing Firewall Rules.....	10
3.1.3	Deleting Firewall Rules	10
4	Port Forwarding.....	10
4.1	Adding Port Forwards.....	10
4.1.1	Add Port Forward.....	11
4.1.2	Port Forward List.....	12
4.1.3	Port Forward Firewall Rule.....	13
4.2	Traffic Redirection with Port Forwards.....	13
5	Virtual Private Networks (VPNs)	14
5.1	IPSec.....	14

5.1.1	Site to site example configuration	14
5.1.2	Mobile IPSec.....	18
5.1.3	Example Server Configuration	19
5.1.4	Mobile Client Tunnel Creation.....	19
5.1.5	Mobile Client Pre-Shared Key Creation	20
5.2	PPTP.....	21
5.2.1	PPTP Server Configuration	21
5.2.2	IP Addressing	22
5.2.3	Authentication	22
5.2.4	Require 128 bit encryption	22
5.2.5	Save changes to start PPTP server	22
5.2.6	Configure firewall rules for PPTP clients.....	22
5.2.7	Adding Users.....	23
5.2.8	PPTP Logs	24
6	General System Actions.....	25
6.1	Reset to factory defaults.....	25
6.2	Reboot system	25
6.3	Manual Firmware Update	25
6.4	Automatic Update.....	25
6.5	Making Backups	26
6.6	Restoring from Backups	26
6.6.1	Restoring with the WebGUI.....	26
6.6.2	Restoring from the Config History.....	27
6.7	Defining Times for a Schedule	27
6.8	Using the Schedule in a Firewall Rule.....	28
7	Issues.....	28
7.1	Firewall Rule Issues	28
7.2	NAT Rule Issues	29
8	Monitoring.....	29
8.1	RRD Graphs.....	29
8.2	System Graphs	30
8.2.1	Processor Graph.....	30
8.2.2	Throughput Graph.....	30

8.2.3	States Graph.....	30
8.2.4	Traffic Graphs.....	30
8.2.5	Packet Graphs.....	31
8.2.6	Quality Graphs	31
8.2.7	Queue Graphs	31
8.2.8	Settings.....	31
8.2.9	Enable Graphing.....	31
8.2.10	Default Category.....	31
8.2.11	Default Style	31
8.3	Viewing Logs	31

1 General Configuration

1.1 General Configuration Options

Some general system options are found under System->General Setup.

The Hostname and Domain, DNS Servers and the Time zone and NTP Time server can be changed if desired, as covered in the Setup Wizard. Along with the ability to change the DNS Servers, there is another option: Allow DNS server list to be overridden by DHCP/PPP on WAN. This does essentially what it says; if checked, pfSense will use the DNS servers that are assigned dynamically by DHCP or PPP. They will be utilized by the system itself and as the upstream DNS servers for the DNS forwarder. These servers will not be passed on to the DHCP clients behind the pfSense system.

1.2 Advanced Configuration Options

Under System -> Advanced you will find a lot of options that are of a more advanced nature. None of these options should need adjustment for a basic routing/NAT setup, but you may find that some of the changes governed by these options will help in customizing your configuration in beneficial ways.

2 Network Address Translation

2.1 Configuring 1:1 NAT

To configure 1:1 NAT, first add a Virtual IP for the public IP to be used for the 1:1 NAT entry. Then browse to Firewall -> NAT and click the 1:1 tab. Click “add rule” button to add a 1:1 entry.

Firewall: NAT: 1:1: Edit

Interface	<div>WAN</div> <div>Choose which interface this rule applies to. Hint: in most cases, you'll want to use WAN here.</div>
External subnet	<div></div> / <div>32</div> <div>Enter the external (WAN) subnet for the 1:1 mapping. You may map single IP addresses by specifying a /32 subnet.</div>
Internal subnet	<div></div> <div>Enter the internal (LAN) subnet for the 1:1 mapping. The subnet size specified for the external subnet also applies to the internal subnet (they have to be the same).</div>
Description	<div></div> <div>You may enter a description here for your reference (not parsed).</div>

2.1.1 Interface

The interface box is where you select the location of the external subnet. This is almost always your WAN, or an OPT WAN interface in multi-WAN deployments.

2.1.2 External subnet

The external subnet is where you define the public IP address or IP address range for the 1:1 mapping. This can be a single IP address by specifying a /32 mask, or a CIDR range by selecting another mask.

2.1.3 Internal subnet

The internal subnet is where you specify the internal IP address or IP address range for the 1:1 mapping. This IP address or range must be reachable on one of your internal interfaces, whether on a directly attached subnet, or one reachable via static route.

2.1.4 Description

This is an optional field that does not affect the behavior of the 1:1 NAT entry. Fill in something that will allow you to easily identify this entry when working with your firewall in the future.

2.1.5 Example single IP 1:1 configuration

This section will show how to configure a 1:1 NAT entry with a single internal and external IP. In this example, 10.0.0.5 is a Virtual IP on the WAN. In most deployments this will be substituted with one of your public IP addresses. The mail server being configured for this mapping resides on a DMZ segment using internal IP 192.168.2.5. The 1:1 NAT entry to map 10.0.0.5 to 192.168.2.5. A diagram depicting this configuration is Single inside and outside IP.

Firewall: NAT: 1:1: Edit

Interface	<div>WAN</div> <div>Choose which interface this rule applies to. Hint: in most cases, you'll want to use WAN here.</div>
External subnet	<div>10.0.0.5 / 32</div> <div>Enter the external (WAN) subnet for the 1:1 mapping. You may map single IP addresses by specifying a /32 subnet.</div>
Internal subnet	<div>192.168.2.5</div> <div>Enter the internal (LAN) subnet for the 1:1 mapping. The subnet size specified for the external subnet also applies to the internal subnet (they have to be the same).</div>
Description	<div>mail server</div> <div>You may enter a description here for your reference (not parsed).</div>

2.1.6 Example IP range 1:1 configuration

1:1 NAT can be configured for multiple public IPs by using CIDR ranges. This examples covers configuration of 1:1 NAT for a /30 CIDR range of IPs.

External IPs	Internal IPs
10.0.0.64/30	192.168.2.64/30
10.0.0.64	192.168.2.64
10.0.0.65	192.168.2.65
10.0.0.66	192.168.2.66

10.0.0.67	192.168.2.67
-----------	--------------

/30 CIDR mapping — matching final octet

The last octet of the IP addresses need not be the same on the inside and outside, but I recommend doing so whenever possible. For example, as we can see in the next table /30 CIDR mapping — non-matching final octet would also be valid.

External IPs	Internal IPs
10.0.0.64/30	192.168.2.200/30
10.0.0.64	192.168.2.200
10.0.0.65	192.168.2.201
10.0.0.66	192.168.2.202
10.0.0.67	192.168.2.203

I recommend choosing an addressing scheme where the last octet matches, because it makes your network easier to understand and hence maintain.

2.2 Outbound NAT

Outbound NAT controls how traffic leaving your network will be translated. To configure it, visit the Firewall -> NAT page and choose the Outbound tab. There are two configuration options for Outbound NAT in pfSense, Automatic outbound NAT rule generation and Manual outbound NAT generation (Advanced Outbound NAT (AON)). In networks with a single public IP address per WAN, there is usually no reason to enable AON. In environments with multiple public IP addresses, this may be desirable.

2.2.1 Default Outbound NAT Rules

When using the default Automatic outbound NAT, pfSense will automatically create NAT rules translating traffic leaving any internal network to the IP address of the WAN interface which the traffic leaves.

2.2.2 Static Port

By default, pfSense rewrites the source port on all outgoing packets. Many operating systems do a poor job of source port randomization, if they do it at all. This makes IP spoofing easier, and makes it possible to fingerprint hosts behind your firewall from their outbound traffic. Rewriting the source port eliminates these potential (but unlikely) security vulnerabilities.

However, this breaks some applications. There are built in rules when Advanced Outbound NAT is disabled that don't do this for UDP 500 (IKE for VPN traffic) and 5060 (SIP) because these types of traffic will almost always be broken by rewriting the source port. All other traffic has the source port rewritten by default. You may use other protocols, like some games amongst other things, which do not work properly when the source port gets rewritten. To disable this functionality, you need to use the static port option. Click Firewall -> NAT, and the Outbound tab. Click Manual Outbound NAT rule generation (Advanced Outbound NAT (AON)) and click Save. You will then see a rule at the bottom of the page

labeled Auto created rule for LAN. Click the “edit” button to the right of that rule to edit it. Check the Static Port box on that page, and click Save. Apply Changes. After making that change, the source port on outgoing traffic will be preserved.

2.2.3 Disabling Outbound NAT

If you are using public IP addresses on local interfaces, and thus do not need to apply NAT to traffic passing through the firewall, you should disable NAT for that interface. In order to do this, you must first change the Outbound NAT setting to Manual Outbound NAT, and then Save. After making that change, one or more rules will appear in the list on the Outbound NAT screen. Delete the rule or rules for the public IP subnets by clicking each line once (or check the box at the start of the line) and then click the “delete rule” button at the bottom of the list. Click Apply Changes to complete the process.

Once all of the rules have been deleted, outbound NAT will no longer be active for those addresses, and pfSense will then route public IP addresses without translation. To completely disable outbound NAT, delete all of the rules that are present when using Manual Outbound NAT.

2.3 Aliases

Aliases allow you to group ports, hosts, or networks and refer to them by name in your firewall rules, NAT configuration and traffic shaper configuration. This allows you to create significantly shorter and more manageable rulesets. Any box in the web interface with a red background is alias friendly.

Note: Aliases in this context should not be confused with interface IP aliases, which are a means of adding additional IP addresses to a network interface.

2.3.1 Configuring Aliases

To add an alias, go to the Firewall Aliases screen and click the “add alias” button. The following sections describe each type of alias that can be used.

To add new members to an alias, click the “add members” at the bottom of the list of entries on the Firewall -> Aliases -> Edit screen.

3 Firewall

3.1 Firewall Rules

First, browse to Firewall -> Rules. This will bring up the WAN ruleset, which by default has no entries other than those for Block private networks and Block bogon networks if you enabled those. If you click the “edit rule” button to the right of the Block private networks or Block bogon networks rules, it will take you to the WAN interface configuration page, where these options can be enabled or disabled.

Firewall: Rules

LAN WAN OPT1

	Proto	Source	Port	Destination	Port	Gateway	Schedule	Description
	*	RFC 1918 networks	*	*	*	*	*	Block private networks
	*	Reserved/not assigned by IANA	*	*	*	*	*	Block bogon networks

No rules are currently defined for this interface.
All incoming connections on this interface will be blocked until you add pass rules.
Click the button to add a new rule.

Click on the LAN tab to view the LAN rules. By default, this is only the **Default LAN -> any** rule.

Firewall: Rules

LAN WAN OPT1

	Proto	Source	Port	Destination	Port	Gateway	Schedule	Description
	*	LAN net	*	*	*	*		Default LAN -> any

pass
 pass (disabled)

block
 block (disabled)

reject
 reject (disabled)

log
 log (disabled)

Hint:
Rules are evaluated on a first-match basis (i.e. the action of the first rule to match a packet will be executed). This means that if you use block rules, you'll have to pay attention to the rule order. Everything that isn't explicitly passed is blocked by default.

Rules for other interfaces may be viewed by clicking their respective tabs. OPT interfaces will appear with their descriptive names, so if you named your OPT1 interface DMZ, then the tab for its rules will also say DMZ. To the left of each rule is an indicator icon showing the action of the rule — pass, block, or reject. If logging is enabled for the rule, the blue circle containing an i is shown there as well. The same icons are used for disabled rules, except the icon, like the rule, will be grayed out.

3.1.1 Adding a firewall rule

Click either of the “add new rule” buttons on the Firewall: Rules screen to add a new rule. The top and bottom buttons, will add a new rule. The top adds a rule to the top of the ruleset, while the bottom “add new rule” button adds the rule at the bottom.

Firewall: Rules

LAN WAN OPT1

Proto	Source	Port	Destination	Port	Gateway	Schedule	Description
*	LAN net	*	*	*	*		Default LAN -> any

pass pass (disabled) block block (disabled) reject reject (disabled) log log (disabled)

Hint:
Rules are evaluated on a first-match basis (i.e. the action of the first rule to match a packet will be executed). This means that if you use block rules, you'll have to pay attention to the rule order. Everything that isn't explicitly passed is blocked by default.

If you would like to make a new rule that is similar to an existing rule, click the “add a new rule based on this one” button at the end of the row. The edit screen will appear with the existing rule's settings pre-filled, ready to be adjusted. For more information about how to configure the rule that was just added.

3.1.2 Editing Firewall Rules

To edit a firewall rule, click the “edit rule” to the right of the rule, or double click anywhere on the line. You will then be taken to the edit screen for that rule, where you can make any needed adjustments.

3.1.3 Deleting Firewall Rules

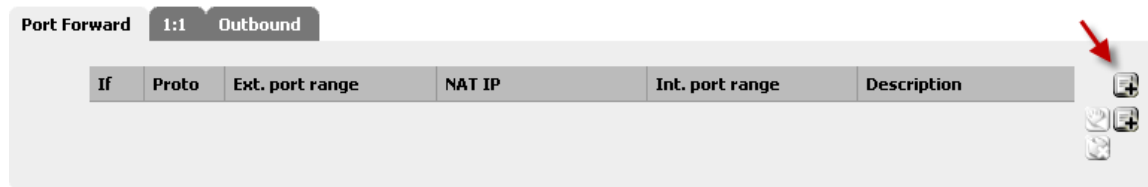
To delete a single rule, click the “delete rule” button to the right of the rule. You will be prompted to confirm the deletion, and if this is what you wanted to do, click OK to actually delete the rule. To delete multiple rules, check the box at the start of the rows that should be removed, then click the “delete selected rules” at the bottom of the list. Rules may also be selected by single clicking anywhere on their line.

4 Port Forwarding

4.1 Adding Port Forwards

Port Forwards are managed at Firewall -> NAT, on the Port Forward tab. The rules on this screen are managed in the same manner as firewall rules. To begin adding a port forward entry, click the “add forward rule” button at the very top or bottom of the list.

Firewall: NAT: Port Forward



If	Proto	Ext. port range	NAT IP	Int. port range	Description
----	-------	-----------------	--------	-----------------	-------------

4.1.1 Add Port Forward

You will now be looking at the Port Forward editing screen. First, select the Interface on which the port to be forwarded resides. In most cases this will be WAN, but if you have an OPT WAN link, or if this will be a local redirect, it may be another interface.

The External Address in most cases should be set to **Interface Address** or an available Virtual IP unless this is a local redirect. The Protocol and External Port Range must be set accordingly for the service being forwarded. For example, to forward VNC you would set Protocol to **TCP** and the External Port Range to **5900**. (Since this is a commonly forwarded port, it is also available in the drop-down list for port selection.)

The NAT IP should be the local IP address to which this external port will forward, and the Local port is where the forwarded port range will begin. If you are forwarding a range of ports, say 19000-19100, you need only specify a local starting point since the ports must match up one to one. This field allows you to open a different port on the outside than the host on the inside is listening on, for example external port 8888 may forward to local port 80 for HTTP on an internal server.

The description field, as in other parts of pfSense, is available for a short sentence about what the port forward does or why it exists. The final option is very important. If you check Auto-add a firewall rule to permit traffic through this NAT rule, then a firewall rule will automatically be created for you that will allow traffic to reach the target port. It is usually best to leave this checked, and then alter the firewall rule afterward if needed. Click Save when finished, then Apply Changes.

Firewall: NAT: Port Forward: Edit

Interface	WAN <small>Choose which interface this rule applies to. Hint: in most cases, you'll want to use WAN here.</small>
External address	Interface address <small>If you want this rule to apply to another IP address than the address of the interface chosen above, select it here (you need to define Virtual IP addresses first). Note if you are redirecting connections on the LAN, select the "any" option.</small>
Protocol	TCP <small>Choose which IP protocol this rule should match. Hint: in most cases, you should specify <i>TCP</i> here.</small>
External port range	from: VNC to: VNC <small>Specify the port or port range on the firewall's external address for this mapping. Hint: you can leave the 'to' field empty if you only want to map a single port</small>
NAT IP	10.0.20.5 <small>Enter the internal IP address of the server on which you want to map the ports. e.g. 192.168.1.12</small>
Local port	VNC <small>Specify the port on the machine with the IP address entered above. In case of a port range, specify the beginning port of the range (the end port will be calculated automatically). Hint: this is usually identical to the 'from' port above</small>
Description	VNC to Sales Server <small>You may enter a description here for your reference (not parsed).</small>
No XMLRPC Sync	<input type="checkbox"/> <small>HINT: This prevents the rule from automatically syncing to other CARP members.</small>

☒ Auto-add a firewall rule to permit traffic through this NAT rule

After clicking Save, you will be taken back to the port forward list, and you will see the newly created entry:

Port Forward

1:1

Outbound

If	Proto	Ext. port range	NAT IP	Int. port range	Description
WAN	TCP	5900 (VNC)	10.0.20.5 (ext.: 192.168.10.5)	5900 (VNC)	VNC to Sales Server







4.1.2 Port Forward List

You may want to double check the firewall rule, as seen under Firewall -> Rules on the tab for the interface upon which the port forward was created. It will show that traffic will be allowed into the NAT IP on the proper port.

LAN

WAN

IPsec

	Proto	Source	Port	Destination	Port	Gateway	Schedule	Description	
<div><div></div><div></div></div>	TCP	*	*	10.0.20.5	5900 (VNC)	*		NAT VNC to Sales Server	<div><div></div><div></div><div></div></div>

4.1.3 Port Forward Firewall Rule

You will want to restrict the **Source** of the automatically generated rule where possible. For things such as mail servers that need to be widely accessible, this isn't practical, but for the VNC example it is likely there are only a small number of hosts that should be able to connect using VNC into a server from across the Internet. Creating an alias of authorized hosts, and changing the source from **any** to the alias is far more secure than leaving the source wide open to the entire Internet. You may want to test first with the unrestricted source, and after verifying it works as desired, restrict the source as desired.

If everything looks right, the port forward should work when tested from outside your network.

4.2 Traffic Redirection with Port Forwards

Another use of port forwards is for transparently redirecting traffic from your internal network. Port forwards specifying the LAN interface or another internal interface will redirect traffic matching the forward to the specified destination. This is most commonly used for transparently proxying HTTP traffic to a proxy server, or redirecting all outbound SMTP to one server. The NAT entry is an example of a configuration that will redirect all HTTP traffic coming into the LAN interface to Squid (port 3129) on the host 172.30.50.10.

Firewall: NAT: Port Forward: Edit

Interface	<div>LAN</div> <div>Choose which interface this rule applies to. Hint: in most cases, you'll want to use WAN here.</div>
External address	<div>any</div> <div>If you want this rule to apply to another IP address than the address of the interface chosen, you need to define Virtual IP addresses first). Note if you are redirecting connections on the LAN, s</div>
Protocol	<div>TCP</div> <div>Choose which IP protocol this rule should match. Hint: in most cases, you should specify <i>TCP</i> here.</div>
External port range	<div>from: HTTP to: HTTP</div> <div>Specify the port or port range on the firewall's external address for this mapping. Hint: you can leave the 'to' field empty if you only want to map a single port</div>
NAT IP	<div>172.30.50.10</div> <div>Enter the internal IP address of the server on which you want to map the ports. e.g. <i>192.168.1.12</i></div>
Local port	<div>(other) 3129</div> <div>Specify the port on the machine with the IP address entered above. In case of a port range, s the range (the end port will be calculated automatically). Hint: this is usually identical to the 'from' port above</div>
Description	<div>Redirect HTTP to Squid</div> <div>You may enter a description here for your reference (not parsed).</div>
No XMLRPC Sync	<div><input type="checkbox"/></div> <div>HINT: This prevents the rule from automatically syncing to other CARP members.</div>

Remember the server you are redirecting to must reside on a different interface than the one used in the port forward, as previously described.

5 Virtual Private Networks (VPNs)

5.1 IPsec

5.1.1 Site to site example configuration

The key to making a working IPsec tunnel is to make sure that both sides have matching settings for authentication, encryption, and so on. Before starting, make a note of the local and remote WAN IP addresses, as well as the local and remote internal subnets that you will be connecting. An IP from the remote subnet to ping is optional, but recommended to keep the tunnel alive.

The system doesn't check for replies, as any traffic initiated to an IP on the remote network will trigger IPsec negotiation, so it doesn't matter if the host actually responds or not as long as it is an IP on the other side of the connection. Aside from the cosmetic tunnel Description and these pieces of information, the other connection settings will be identical. In this example the following settings will be assumed:

Site A		Site B	
Name	Louisville Office	Name	London Office
WAN IP	172.23.1.3	WAN IP	172.16.1.3
LAN Subnet	192.168.1.0/24	LAN Subnet	10.0.10.0/24
LAN IP	192.168.1.1	LAN IP	10.0.10.1

We will start with Site A. First, we must enable IPsec on the router. Navigate to VPN -> IPsec, check Enable IPsec, then click Save:

VPN: IPsec

Tunnels
Mobile clients
Pre-shared keys
CAs

☒ Enable IPsec

Save

Local net	Interface	P1 mode	P1 Enc. Algo	P1 Hash Algo	Description	
Remote net	Remote gw					+

Note:
You can check your IPsec status at [Status:IPsec](#).

Now, create the tunnel by pressing the “add phase1 entry” button. You will now see a large page that has every setting needed for the tunnel to function. Don't be too discouraged, as many of these settings may be left at their default values.

To get started, fill in the top section that holds the general tunnel information and network Settings. Items in bold are required. Make sure that the Disable this tunnel box is unchecked. The interface setting should likely be **WAN**, but see the note earlier in the chapter on selecting the proper interface if you are unsure. Fill in the Dead Peer Detection (DPD) value with something reasonable, such as **60** seconds. Depending on your needs a lower value may be better, more like **10** or **20** seconds, but a problematic WAN connection on either side might make that too low. For the Local Subnet, is probably best to leave this as **LAN Subnet**. You could also change this to **Network** and fill in the proper values, in this case **192.168.1.0/24**, but leaving it as **LAN Subnet** will ensure that should the network ever be renumbered, this end of the tunnel will follow. Note the other end must be changed manually. The Remote Subnet will be the network at Site B, in this case **10.0.10.0/24**. The Remote Gateway is the WAN address at Site B, **172.16.1.3**. Finally, enter a Description for the tunnel. It is a good idea to put the name of Site B in this box, and some detail about the tunnel's purpose may also help future administration. We'll put "**ExampleCo London Office**" in the description so we have some idea where the tunnel terminates. The defaults

are desirable for most of these settings, and simplifies the process. The most important setting to get right is the Pre-Shared Key. As mentioned in the VPN overview, IPsec using pre-shared keys can be broken if a weak key is used. Use a strong key, at least 10 characters in length containing a mix of upper and lowercase letters, numbers and symbols. The same exact key will need to be entered into the tunnel configuration for Site B later, so you may want to write it down, or copy and paste it elsewhere. Copy and paste may come in handy, especially with a complex key like **aBc123%XyZ9\$7qwErty99**. A Lifetime setting may also be specified, otherwise the default value of **86400** will be used. As we are using a Pre-Shared Key and not certificates, leave all of the certificate boxes empty.

As for Phase 2, there can be a little more variability. The Protocol choice could be **AH** for only authenticated packets, or **ESP** for encryption. ESP is the right choice in all but a few unusual situations. The Encryption algorithms and Hash algorithms can both be set to allow multiple options, and both sides will negotiate and agree upon the settings. In some cases that may be a good thing, but it is usually better to restrict this to the options that you know will be in use. For this example, the only Encryption algorithm selected is 3DES, and the only Hash algorithm selected is SHA1. PFS, or Perfect Forward Secrecy, can help protect against certain key attacks, but is optional. A Lifetime setting may also be specified, otherwise the default value of **3600** will be used.

Phase 2 proposal (SA/Key Exchange)	
Protocol	ESP ▼ ESP is encryption, AH is authentication only
Encryption algorithms	<input type="checkbox"/> DES <input checked="" type="checkbox"/> 3DES <input type="checkbox"/> Blowfish <input type="checkbox"/> CAST128 <input type="checkbox"/> Rijndael (AES) <input type="checkbox"/> Rijndael 256 Hint: use 3DES for best compatibility or if you have a hardware crypto accelerator card. Blowfish is usually the fastest in software encryption.
Hash algorithms	<input checked="" type="checkbox"/> SHA1 <input type="checkbox"/> MD5
PFS key group	off ▼ <i>1 = 768 bit, 2 = 1024 bit, 5 = 1536 bit</i>
Lifetime	3600 seconds

Lastly, you can enter an IP address for a system on the remote LAN that should periodically be sent an ICMP ping. The return value of the ping is not checked, this will only ensure that some traffic is sent on the tunnel so that it will stay established. In this setup, we can use the LAN IP address of the pfSense router at Site B, **10.0.10.1**.

Keep alive	
Automatically ping host	10.0.10.1 IP address

Click the Save button, and then you will need to click Apply changes on the IPsec Tunnels screen.

VPN: IPsec



The IPsec tunnel configuration has been changed.
You must apply the changes in order for them to take effect.

Apply changes

The tunnel for Site A is finished, but now firewall rules are needed to allow traffic from Site B's network to come in via the IPsec tunnel. These rules must be added to the IPsec tab under Firewall -> Rules. See the chapter on Firewall rules for specifics on adding the rules. You may be as permissive as you like, (allow any protocol from anywhere to anywhere), or restrictive (allow TCP from a certain host on Site B to a certain host at Site A on a certain port). In each case, make sure the Source address(es) are Site B addresses, such as **10.0.10.0/24**. The destination addresses should be the Site A network, **192.168.1.0/24**. Now that Site A is configured, it is time to tackle Site B. Repeat the process on Site B's router to enable IPsec and add a tunnel.

Only two parts of this setup will differ from Site A. Those are the general settings and the Keep Alive setting. Make sure that the Disable this tunnel box is unchecked. The interface setting should be **WAN**. Fill in the Dead Peer Detection (DPD) value with the same setting as Site A.. For the Local Subnet, it is probably best to leave this as **LAN Subnet**. You could also change this to **Network** and fill in the proper values, in this case **10.0.10.0/24**. The Remote Subnet will be the network at Site A, in this case **192.168.1.0/24**. The Remote Gateway is the WAN address at Site A, **172.23.1.3**. A Description for the tunnel is still a good idea. We'll put "**ExampleCo Louisville Office**" on this side.

VPN: IPsec: Edit tunnel


Mode	Tunnel
Disabled	<input type="checkbox"/> Disable this tunnel Set this option to disable this tunnel without removing it from the list.
Interface	WAN Select the interface for the local endpoint of this tunnel.
DPD interval	60 seconds Enter a value here to enable Dead Peer Detection (e.g. 60 seconds).
Local subnet	Type: LAN subnet Address: / 0
Remote subnet	192.168.1.0 / 24
Remote gateway	172.23.1.3 Enter the public IP address or hostname of the remote gateway
Description	ExampleCo Louisville Office You may enter a description here for your reference (not parsed).

The Phase 1 and Phase 2 settings must match Site A exactly. Review that section of this example for the details and figures.

The last change is the Keep Alive setting. In this setup, we can use the LAN IP address of the pfSense router at Site A, **192.168.1.1**.

Keep alive		
Automatically ping host	<input type="text" value="192.168.1.1"/>	IP address

Now click the Save button, and then click Apply changes on the IPsec Tunnels screen. As with Site A, you must also add firewall rules to allow traffic on the tunnel to cross from Site A to Site B. Add these rules to the IPsec tab under Firewall -> Rules. This time, the source of the traffic would be Site A, destination Site B. Both tunnels are now configured and should be active. Check the IPsec status by visiting Status -> IPsec. You should see a description of the tunnel along with an indicator icon for its status.

If you do not see a  icon, there may be a problem establishing the tunnel. This soon, the most likely reason is that no traffic has attempted to cross the tunnel. Try to ping a system in the remote subnet at Site B from Site A (or vice versa) and see if the tunnel establishes. Failing that, the IPsec logs will offer an explanation. They are located under Status -> System Logs on the IPsec VPN tab. Be sure to check the status and logs at both sites.

5.1.2 Mobile IPsec

Mobile IPsec will allow you to make a so-called "Road Warrior" style connection, named after the variable nature of anyone who is not in the office that needs to connect back to the main network. It may be a sales person using Wi-Fi on a business trip, the boss from his limo via 3G modem, or a programmer working from their broadband line at home. Most of these will be forced to deal with dynamic IP addresses, and often will not even know the IP address they have. Without a router or firewall supporting IPsec, a traditional IPsec tunnel will not work. In telecommuting scenarios, it's usually undesirable and unnecessary to connect the user's entire home network to your network, and will introduce routing complications. This is where IPsec Mobile Clients come in.

There is only one definition for Mobile IPsec on pfSense, so you may be wondering how to setup multiple clients. Instead of relying on a fixed address for the remote end of the tunnel, a unique Identifier/Pre-Shared Key pair is used, much like a username and password. This allows the clients to be authenticated and distinguished from one another.

Before you begin configuring clients, you may want to choose an IP address range they will be using. This is not controlled on the server side, so some care will be needed to ensure that IP addresses do not overlap when setting up client software. The IP addresses must differ from those in use at the site hosting the mobile tunnel. In this example, *192.168.111.0/24* will be used, but it can be any unused subnet that you desire. Alternatively, you aren't required to specify an IP address. The clients can be configured so they pass through the local IP address of the connecting client. This will be a private IP

where the client is behind NAT, and a public IP where one is directly assigned to the client. If you will be filtering based on the source IP on the IPsec interface, you will want to specify an IP for each client so you always know the source IP and it will not change. Not specifying the source IP may also create routing difficulties, where the client is on a local network conflicting with one of your internal networks.

5.1.3 Example Server Configuration

There are two components to the server configuration for mobile clients: Creating the tunnel, and creating the Pre-Shared Keys.

5.1.4 Mobile Client Tunnel Creation

First, we must enable IPsec on the router if you haven't done so already. Navigate to VPN -> IPsec, check Enable IPsec, then click Save. With IPsec enabled, mobile client support must also be turned on. From VPN -> IPsec, click on the Mobile clients tab. Check the Allow mobile clients box, and then continue on to the next set of options.

VPN: IPsec: Mobile

Tunnels	Mobile clients	Pre-shared keys	CAs
---------	----------------	-----------------	-----

☒ Allow mobile clients

Phase 1 proposal (Authentication)	
Negotiation mode	aggressive <small>Aggressive is faster, but less secure.</small>
My identifier	My IP address
Encryption algorithm	3DES <small>Must match the setting chosen on the remote side.</small>
Hash algorithm	SHA1 <small>Must match the setting chosen on the remote side.</small>
DH key group	2 <small>1 = 768 bit, 2 = 1024 bit, 5 = 1536 bit Must match the setting chosen on the remote side.</small>
DPD Interval	120 <small>Dead Peer Detection interval in seconds. Leave this empty to only respond to DPD requests and not send any requests.</small>
Lifetime	86400 seconds
Authentication method	Pre-shared key <small>Must match the setting chosen on the remote side.</small>

A Phase 1 proposal must now be configured for Authentication, as shown in the picture above. When dealing with mobile clients, it is best to use safe, widelycompatible settings. Using **aggressive** for the Negotiation mode will allow for using a wider range of identifier types, such as the e-mail address style that are used in this example setup. Since this side should have a static address, using **My IP address** for the My identifier option should be safe. The Encryption algorithm, **3DES** and the Hash algorithm **SHA1** are secure and well-

supported. A DH key group of **2** is a good, safe, middle ground as well. Due to the large variance in connection types that will be dealt with, a higher DPD value of around **120** seconds is more likely to ensure that connections are not dropped prematurely. The Lifetime can be set much lower if you'd like, but **86400** should still be acceptable. We will be using **Pre-Shared Key** for the Authentication method, since in this example we want everyone to have individual Identifiers and Pre-Shared Keys.

The Phase 2 options for the mobile tunnels. Since encrypted traffic is important in this case, the Protocol should be set for **ESP**. The Encryption algorithms for Phase 2 can be set for as many as needed. You may find that certain software clients behave better than others using different algorithms. A safe choice is to at least check **3DES**, but others may be used. For Hash algorithms, you can choose both **SHA1** and **MD5**, or just one of the two. PFS is optional, and depending on the client software involved it may be best to leave this **off**. The default Lifetime of **3600** is probably still a good idea here. Now click Save and move on.

Phase 2 proposal (SA/Key Exchange)	
Protocol	ESP <small>ESP is encryption, AH is authentication only</small>
Encryption algorithms	<input type="checkbox"/> DES <input checked="" type="checkbox"/> 3DES <input checked="" type="checkbox"/> Blowfish <input checked="" type="checkbox"/> CAST128 <input checked="" type="checkbox"/> Rijndael (AES) <input type="checkbox"/> Rijndael 256 <small>Hint: use 3DES for best compatibility or if you have a hardware crypto accelerator card. Blowfish is usually the fastest in software encryption.</small>
Hash algorithms	<input checked="" type="checkbox"/> SHA1 <input type="checkbox"/> MD5
PFS key group	off <small>1 = 768 bit, 2 = 1024 bit, 5 = 1536 bit</small>
Lifetime	3600 seconds
<div>Save</div>	

After clicking Save, the settings must be applied before they will take effect. Click Apply changes and then the tunnel setup for mobile clients is complete.

VPN: IPsec: Mobile

 The IPsec tunnel configuration has been changed.
You must apply the changes in order for them to take effect.

Apply changes

5.1.5 Mobile Client Pre-Shared Key Creation

The next part of the mobile client setup is to enter Identifiers and Pre-Shared Keys for the individual clients. From VPN -> IPsec, click on the Pre-shared keys tab. This will list all of the currently created Identifier/PSK pairs. Since we just started, this is likely empty. To create a new pair, click the “add pre-shared key” button.

VPN: IPsec: Keys

Tunnels Mobile clients **Pre-shared keys** CAs

Identifier	Pre-shared key	
		 

A screen with two fields will appear. One for the Identifier, and one for the Pre-shared key. In the first box, enter an e-mail address for this client. It does not have to be a real, valid, address, it need only resemble one. As mentioned in the VPN overview, IPsec using pre-shared keys can be broken if a weak key is used. Use a strong key, at least 10 characters in length containing a mix of upper and lowercase letters, numbers and symbols. Click Save when finished.


VPN: IPsec: Edit pre-shared key

Identifier	<input type="text" value="fieldtech@lvx.example.com"/> <small>This can be either an IP address, fully qualified domain name or an e-mail address.</small>
Pre-shared key	<input type="text" value="PSk33##44\$\$55%%789"/>

Save




As with the tunnel settings, after altering key settings, the changes will need to be applied. The Identifier and Pre-shared key just created should also be listed on this screen. If there are more Identifier/PSK pairs to add, click and repeat the above step. Otherwise, click Apply changes to complete the IPsec setup.

VPN: IPsec: Keys

 The IPsec tunnel configuration has been changed.
You must apply the changes in order for them to take effect.

Apply changes

Tunnels Mobile clients **Pre-shared keys** CAs

Identifier	Pre-shared key	
fieldtech@lvx.example.com	PSk33##44\$\$55%%789	  

5.2 PPTP

5.2.1 PPTP Server Configuration

To configure the PPTP server, first browse to VPN -> PPTP. Select Enable PPTP server.

5.2.2 IP Addressing

You will need to decide what IP addresses to use for the PPTP server and clients. The Remote address range is usually a portion of your LAN subnet, such as 192.168.1.128/28 (.128 through .143). Then select an IP address outside of that range for the Server address, such as 192.168.1.144.

Server address	<input type="text" value="192.168.1.144"/> Enter the IP address the PPTP server should use on its side for all clients.
Remote address range	<input type="text" value="192.168.1.128"/> / 28 Specify the starting address for the client IP address subnet. The PPTP server will assign 16 addresses, starting at the address entered above, to clients.

5.2.3 Authentication

You can authenticate users from the local user database, or via RADIUS. RADIUS allows you to connect to another server on your network to provide authentication. This can be used to authenticate PPTP users from Microsoft Active Directory as well as numerous other RADIUS capable servers.

If using RADIUS, check the Use a RADIUS server for authentication box and fill in the RADIUS server and shared secret. For authentication using the local user database, leave that box unchecked. You will have to add your users on the Users tab of the VPN -> PPTP screen unless using RADIUS. See Section “Adding Users” below for more details on the built in authentication system.

5.2.4 Require 128 bit encryption

You should require 128 bit encryption where possible. Most PPTP clients support 128 bit encryption, so this should be fine in most environments. PPTP is relatively weak at 128 bit, and significantly more so at 40 and 56 bit. Unless you absolutely must, you should never use anything less than 128 bit with PPTP.

5.2.5 Save changes to start PPTP server

After filling in the aforementioned items, click Save. This will save your configuration and launch the PPTP server. If you are authenticating your users with the local user database, click the Users tab and enter your users there.

5.2.6 Configure firewall rules for PPTP clients

Browse to Firewall -> Rules and click the PPTP VPN tab. These rules control what traffic is permitted from PPTP clients. Until you add a firewall rule here, all traffic initiated from connected PPTP clients will be blocked. Traffic initiated from your LAN to the PPTP clients is controlled using your LAN firewall rules. Initially you may want to add an allow all rule here for testing purposes, and once you verify functionality, restrict the ruleset as desired.

WAN

WLAN

PPTP VPN

Proto	Source	Port	Destination	Port	Gateway	Schedule	Description
*	*	*	*	*	*		temporary allow all rule for testing

5.2.7 Adding Users

Adding users via RADIUS will vary from one implementation to another. This fact makes it beyond the scope of this section, but should be covered in the documentation for the particular RADIUS server being employed.

Adding users to pfSense's built-in PPTP users system is quite easy. First, click on VPN -> PPTP, and then the Users tab. You will be presented with an empty users screen. Click the button "add user" to add a user.

VPN: PPTP: Users

Configuration **Users**

Username	IP address
<div>   </div>	

After clicking the button , the user editing page will appear. Fill it in with the username and password for a user, You may also enter a static IP assignment if desired.

VPN: PPTP: User: Edit

Username	<input type="text" value="salesguy"/>
Password	<input type="password" value="....."/> <input type="password" value="....."/> (confirmation)
IP address	<input type="text"/> <small>If you want the user to be assigned a specific IP address, enter it here.</small>
<input type="button" value="Save"/>	

Click Save, and then the user list will return, but before the change will take effect, the Apply Changes button must first be clicked.





VPN: PPTP: Users



The PPTP user list has been modified.
You must apply the changes in order for them to take effect.
Warning: this will terminate all current PPTP sessions!

Apply changes

Configuration Users

Username	IP address	
salesguy		   

















Repeat that process for each user you would like to add, eventually you will have a rather full looking user list.

VPN: PPTP: Users



The changes have been applied successfully. You can also [monitor](#) the filter reload progress.

Configuration Users

Username	IP address	
ceo		   
fieldtech	192.168.1.126	   
msmarketing		   
salesguy		   

If you need to edit an existing user, click “edit user” button . Users may be deleted by clicking “delete user” button.

5.2.8 PPTP Logs

A record of login and logout events is kept on Status -> System Logs, on the PPTP tab.

Last 150 PPTP VPN log entries			
Time	Action	User	IP address
Jul 17 12:46:26	◀	rick	
Jul 17 12:08:52	▶	rick	192.168.130.128
Jul 17 12:04:04	▶	rick	

As you can see, each login and logout should be recorded with a timestamp and username, and each login will also show the IP address assigned to the PPTP client.

6 General System Actions

6.1 Reset to factory defaults

In the WebGUI at Diagnostics -> Factory defaults

6.2 Reboot system

This will cleanly shutdown the pfSense system and restart the OS. You go in the WebGUI Diagnostics -> Reboot

6.3 Manual Firmware Update

Browse to <http://www.pfsense.org> and click the Downloads link. On the Downloads page, click the link for Upgrades. This will lead to the mirror selection page. Pick a mirror geographically close to your location for best performance. Once a mirror has been selected, a directory listing will appear with update files for the current pfSense release. Download the .tgz file, (e.g. pfSense-Full-Update-1.2.3.tgz) and the accompanying To install the update file, visit the pfSense WebGUI. Click System -> Firmware. Click Enable Firmware Upload. Click the Browse button next to Firmware Image File. Locate the update file downloaded in the previous step, and click Open. Finally, click the Upgrade Firmware button. The update will take a few minutes to upload and apply, depending on the speed of the connection being used for the update and the speed of the target system. The firewall will reboot automatically when finished.

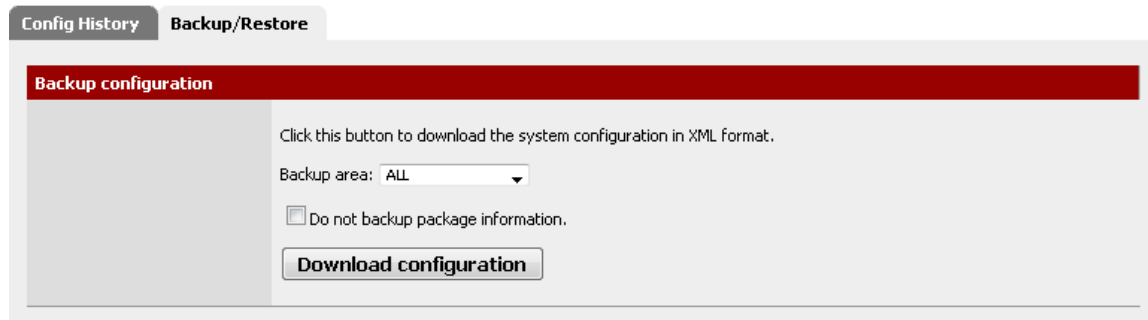
6.4 Automatic Update

Automatic Update is a new feature that will contact a pfSense.com server and determine if there is a newer released version than the one being run currently. This check is performed when you visit the Automatic Updates page found under System -> Firmware, then click the Auto Update tab in the WebGUI. If a new update is available, it will be listed. Click the button to install the update. The update will take a few minutes to download and apply, depending on the speed of the Internet connection being used and the speed of the target system. The firewall will reboot automatically when finished. By default, the update check only pertains to officially released versions of pfSense, but it is also possible to use this method to track snapshots as well. The update version can be changed by visiting the Updater Settings tab, located immediately to the right of the Auto Update tab. It is safest to use the released versions, as they see the most testing and should be reasonably safe and trouble-free. However, as with any upgrade, you should first visit the pfSense website and read the update notes for that release.

6.5 Making Backups

Making a backup in the WebGUI is quite simple. Just visit Diagnostics -> Backup/Restore. In the Backup Configuration section of the page, ensure that Backup Area is set to **ALL**, (the default choice) then click Download Configuration

Diagnostics: Backup/restore



The screenshot shows the 'Backup/Restore' tab in the pfSense WebGUI. The 'Backup configuration' section is active. It contains a red header bar with the title 'Backup configuration'. Below the header, there is a text instruction: 'Click this button to download the system configuration in XML format.' A dropdown menu labeled 'Backup area:' is set to 'ALL'. Below the dropdown is a checkbox labeled 'Do not backup package information.' which is unchecked. At the bottom of the section is a button labeled 'Download configuration'.

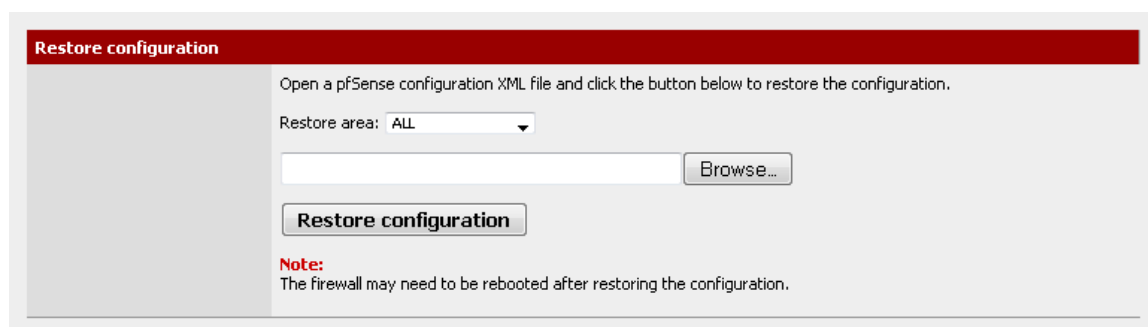
Your web browser will then prompt you to save the file somewhere on the PC being used to view the WebGUI. It will be named config-*<hostname>-<timestamp>*.xml, but that may be changed before saving the file.

6.6 Restoring from Backups

Backups won't do you much good without a means to restore them, and by extension, test them. pfSense offers several means for restoring configurations. Some are more involved than others, but each should have the same end result: a running system identical to what was there when the backup was made.

6.6.1 Restoring with the WebGUI

The easiest way for most people to restore a configuration is by using the WebGUI. Navigate to Diagnostics -> Backup/Restore, and look at the Restore configuration section. To restore the backup, select the area to restore (typically **ALL**), then click Browse. Locate the backup file on your PC, and then click the Restore configuration button. The configuration will be applied, and the firewall will reboot with the settings obtained from the backup file.











The screenshot shows the 'Restore configuration' section in the pfSense WebGUI. It has a red header bar with the title 'Restore configuration'. Below the header, there is a text instruction: 'Open a pfSense configuration XML file and click the button below to restore the configuration.' A dropdown menu labeled 'Restore area:' is set to 'ALL'. Below the dropdown is a text input field for the file path, followed by a 'Browse...' button. At the bottom of the section is a button labeled 'Restore configuration'. Below this button is a red 'Note:' section that states: 'The firewall may need to be rebooted after restoring the configuration.'

6.6.2 Restoring from the Config History

For minor problems, one of pfSense's internal backups may be the easiest way to back out a change. From the Diagnostics -> Backup/Restore page, click the Config History tab. The previous 30 configurations are stored, along with the current running configuration. To switch to one of these previous configurations, click the beside its entry.

Diagnostics: Configuration History

Config History		Backup/Restore
Date	Configuration Change	
6/24/09 20:04:13	/services_dhcp.php made unknown change	Current
6/24/09 19:56:30	/services_dhcp.php made unknown change	 
6/18/09 10:49:11	/firewall_rules_edit.php made unknown change	 
6/18/09 10:45:29	/vpn_ipsec_edit.php made unknown change	 
6/17/09 14:00:55	An OpenVPN server has been created/modified	 

The configuration will be switched, but a reboot is not automatic where required. Minor changes do not require a reboot, though reverting some major changes will. To be safe, you may want to reboot the router with the new configuration by going to Diagnostics -> Reboot System and click Yes. Previously saved configurations may be deleted by clicking "Remove this backup" button, but you need not delete them by hand to save space; the old configuration backups are automatically deleted when new ones are created. You may want to remove a backup from a known-bad configuration change to ensure that it is not accidentally restored.

6.7 Defining Times for a Schedule

To add a schedule from Firewall -> Schedules, click the "add schedule" button. That should bring up the schedule editing screen, as seen in Figure 6.23, "Adding a Time Range". The first field on this screen is for the Schedule Name. This setting is the name that will appear in the selection list for use in firewall rules. Much like alias names, this name must only contain letters and digits, and no spaces. For this example, we'll put in **BusinessHours**. Next in the Description box, enter a longer free-form description of this schedule, such as **Normal Business Hours**. Since a schedule is made up of one or more time range definitions, you must next define a time range before you can save the schedule. A schedule can apply to specific days, such as July 20, 2012, or to days of the week, such as Monday-Wednesday. To select any given day within the next year, choose the Month from the drop-down list, then click on the specific day or days on the calendar. To select a day of the week, click its name in the column headers. For our example, click on Mon, Tue, Wed, Thu, and Fri. This will make the schedule active for any Monday-Friday, regardless of the month. Now select the time in which this schedule should be active, in 24-hour format. Our business hours will be **9:00** to **17:00** (5pm). All times are given in the local time zone. Now enter a Time Range Description, like **Work Week**, then click Add Time. If there are more times to define, repeat that process until you are satisfied with the results. For example, to expand on this setup, there may be a half day on Saturday to define, or maybe the shop opens late on Mondays. In that case, define a time range for the identical days, and then another range for each day with different times. This collection of time ranges will be the full schedule.

When all of the necessary time ranges have been defined, click Save. This schedule will now be available for use in firewall rules.

Name	Time Range(s)	Description
BusinessHours	Mon - Fri 9:00-17:00 Work Week	Normal Business Hours

6.8 Using the Schedule in a Firewall Rule




To create a firewall rule employing this schedule, you must add a rule on the desired interface. For our example, add a rule to block TCP traffic on the LAN interface from the LAN subnet, to any destination on the HTTP port. When you get to the Schedule setting choose the schedule we just defined, **BusinessHours**.

Schedule

BusinessHours ▼

Leave as 'none' to leave the rule enabled all the time.

After saving the rule, the schedule will appear in the firewall rule list, along with an indication of the schedule's active state. As you can see this is a block rule, but the schedule column is indicating that the rule is currently not in its active blocking state because it is being viewed at a time that is outside of the scheduled range. If you hover over the schedule name, it will show the times defined for that schedule. If you hover over the schedule state indicator, it will tell you descriptively how the rule is behaving at that point in time. Since this is being viewed outside of the times defined in our BusinessHours schedule, this will say "Traffic matching this rule is currently being allowed". Had we used a pass rule, the opposite would be true.

	Proto	Source	Port	Destination	Port	Gateway	Schedule	Description
 	TCP	LAN net	*	*	80 (HTTP)	*	 BusinessHours	Block Web Access during Business Hours

Now that the rule is defined, be sure to test it both inside and outside of the scheduled times to ensure that the desired behavior is enacted.

7 Issues

7.1 Firewall Rule Issues

If the default "LAN to Any" rule has been changed or removed from the LAN interface, traffic attempting to reach the Internet from client PCs via the pfSense router may be blocked. This should be easily confirmed by browsing to Status -> System Logs, and looking at the Firewall tab. If there are entries there that show blocked connections from LAN PCs trying to reach Internet hosts, revisit your LAN ruleset at Firewall -> Rules, then the LAN tab and make the necessary adjustments to allow that traffic.

7.2 NAT Rule Issues

If the outbound NAT rules have been changed from their defaults, it may also be possible that traffic attempting to reach the Internet does not have NAT properly applied. Navigate to Firewall -> NAT, and go to the Outbound tab. Unless you are sure that you need it set to manual, change the setting to Automatic outbound NAT rule generation (IPsec passthrough) and then try to reach the Internet from a client PC again. If that did not help a PC on the LAN to get out, then the issue is likely elsewhere. If you have this set to Manual Outbound NAT rule generation (Advanced Outbound NAT (AON)), and it works from LAN but not from an OPT interface, you will need to manually set a rule that matches traffic coming from there. Look at the existing rule for LAN and adjust it accordingly, or refer to the NAT chapter for more information on creating outbound NAT rules. The same applies for traffic coming from VPN users: PPTP, OpenVPN, IPsec, etc. If these users need to reach the Internet via this pfSense router, they will need outbound NAT rules for their subnets.

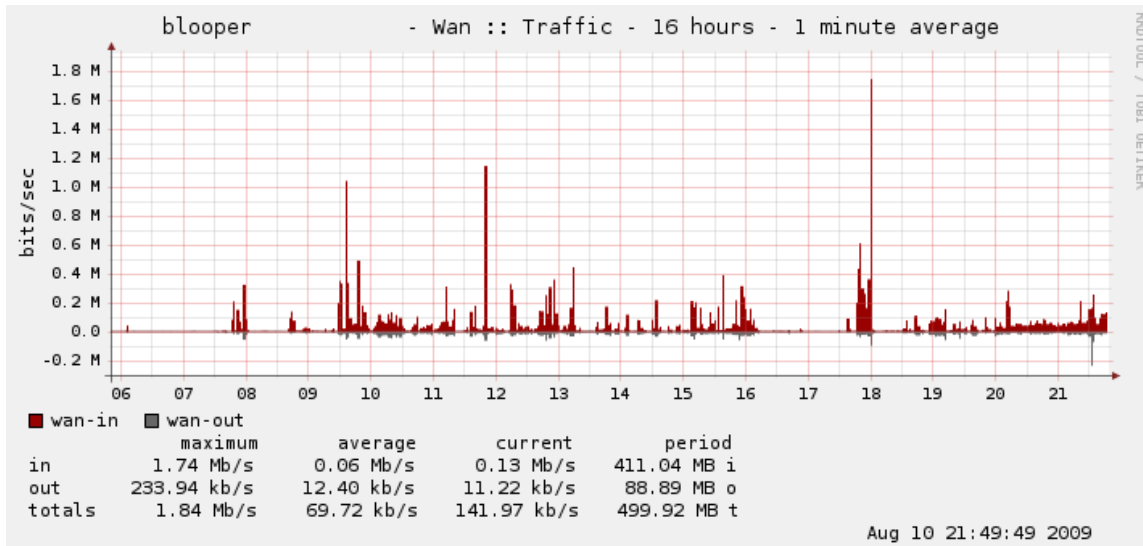
8 Monitoring

8.1 RRD Graphs

RRD Graphs are another useful set of data provided by pfSense. While the router is running it keeps track of various bits of data about how the system performs, and then stores this data in Round-Robin Database (RRD) files. Graphs of this data are available from Status -> RRD Graphs. On that screen there are six tabs, each of which are covered in this section: System, Traffic, Packets, Quality, Queues, and Settings. Each graph is available in several times spans, and each of these is averaged over a different period of time based on how much time is being covered in a given graph. Also on each graph will be a legend and a summarization of the data being shown (minimums, averages, maximums, current values, etc.). Graphs are available in a 4 hour range with a 1 minute average, a 16 hour range with a 1 minute average, a 2 day range with a 5 minute average, a 1 month range with a 1 hour average, a 6 month range with a 12 hour average, and a 1 year range with a 12 hour average.

Many graphs can be viewed in Inverse style or Absolute style. With Inverse style, the graph is split down the middle horizontally and incoming traffic is shown going up from the center, and outgoing traffic is shown going down from the center. With Absolute style, the values are superimposed.

As you can see that it is a 16 hour inverse graph of traffic on the WAN, which has had a maximum use of 1.74Mbit/s average during a 1 minute period.



8.2 System Graphs

The graphs under the System tab show a general overview of the system utilization, including CPU usage, total throughput, and firewall states.

8.2.1 Processor Graph

The processor graph shows CPU usage for user and system processes, interrupts, and the number of running processes.

8.2.2 Throughput Graph

The throughput graph shows the incoming and outgoing traffic totalled up for all interfaces.

8.2.3 States Graph

The states graph is a bit more complex. It shows the number of system states but also breaks down the value in several ways. It shows the filter states from firewall rules, NAT states from NAT rules, the count of unique active source and destination IP addresses, and the number of state changes per second.

8.2.4 Traffic Graphs

Traffic graphs will show the amount of bandwidth used on each available interface in bits per second notation, and there is also an All graphs choice which will show all of the traffic graphs on a single page.

8.2.5 Packet Graphs

The packet graphs work much like the traffic graphs, except instead of reporting based on bandwidth used, it reports the number of packets per second (pps) passed.

8.2.6 Quality Graphs

The quality graph tracks the quality of WAN or WAN-like interface (those with a gateway specified, or using DHCP). Shown on these graphs are the response time from the gateway in milliseconds, as well as a percentage of lost packets. Any loss on the graph indicates connectivity issues or times of excessive bandwidth use.

8.2.7 Queue Graphs

The queue graphs are a composite of each traffic shaper queue. Each individual queue is shown, represented by a unique color. You can view either the graph of all queues, or the graph representing the drops from all queues.

8.2.8 Settings

The RRD graphs can be customized to better suit your preferences. You can even turn them off if you prefer to use some external graphing solution instead. Click Save when finished making changes.

8.2.9 Enable Graphing

Check the box to turn on graphing, or remove the check to disable graphing.

8.2.10 Default Category

The Default Category option picks which tab will show up first when you click on Status -> RRD Graphs.





8.2.11 Default Style

The Default Style option picks which style of graphs to use by default, Inverse or Absolute.

8.3 Viewing Logs

The firewall logs may be found under Status -> System Logs, on the Firewall tab. You can view either parsed logs, which are easier to read, or the raw logs, which have more detail if you understand PF's logging format. There is also a setting for the system logs which will show these entries in forward or reverse order.

The parsed WebGUI logs are in 6 columns: Action, Time, Interface, Source, Destination, and Protocol. Action shows what happened to the packet which generated the log entry, either pass, block, or reject. Time is the time that the packet arrived. Interface is where the packet entered pfSense. Source is the source IP address and port. Destination is the destination IP address and port. Protocol is the protocol of the packet, be it ICMP, TCP, UDP, etc.

Act	Time	If	Source	Destination	Proto
	Jul 16 20:54:05	WAN	0.0.0.0:68	255.255.255.255:67	UDP
	Jul 16 20:56:05	WAN	0.0.0.0:68	255.255.255.255:67	UDP
	Jul 16 21:05:05	WAN	0.0.0.0:68	255.255.255.255:67	UDP
	Jul 16 21:06:05	WAN	0.0.0.0:68	255.255.255.255:67	UDP

The action icon is a link which will lookup and display the rule which caused the log entry. More often than not, this simply says "Default Deny", but when troubleshooting rule issues it can help narrow down the suspects. If the protocol is TCP, you will also see extra fields here that represent TCP flags present in the packet. These indicate various connection states or packet attributes. Some of the more common ones are:

S — SYN Synchronize sequence numbers. Indicates a new connection attempt when only SYN is set.

A — ACK Indicates ACKnowledgment of data. As discussed earlier, these are replies to let the sender know data was received OK.

F — FIN Indicates there is no more data from the sender, closing a connection.

R — RST Connection reset. This flag is set when replying to a request to open a connection on a port which has no listening daemon. Can also be set by firewall software to turn away undesirable connections.