

# Table of Contents

---

	1
<b>Index</b>	95

---

# Chapter 1: Initial Configuration

## System



**Hostname**

Name of the firewall host, without domain part

**Domain**

Do not use '.local' as the final part of the domain (TLD). The '.local' domain is **widely used** by mDNS (including Avahi and Apple OS X's Bonjour/Rendezvous/Airprint/Airplay), and some Windows systems and networked devices. These will not network correctly if the router uses '.local'. Alternatives such as '.local.lan' or '.mylocal' are safe.

## DNS Server Settings

<b>DNS Servers</b>	<input type="text" value="208.67.222.222"/>	<input type="text" value="WAN_DHCP - wan - 10.0.2.2"/>	 Delete
	<input type="text" value="1.1.1.1"/>	<input type="text" value="none"/>	 Delete

**Address**  
Enter IP addresses to be used by the system for DNS resolution. These are also used for the DHCP service, DNS Forwarder and DNS Resolver when it has DNS Query Forwarding enabled.

**Gateway**  
Optionally select the gateway for each DNS server. When using multiple WAN connections there should be at least one unique DNS server per gateway.

**Add DNS Server**

**DNS Server Override**  Allow DNS server list to be overridden by DHCP/PPP on WAN

If this option is set, pfSense will use DNS servers assigned by a DHCP/PPP server on WAN for its own purposes (including the DNS Forwarder/DNS Resolver). However, they will not be assigned to DHCP clients.

**Timeservers**

Use a space to separate multiple hosts (only one required). Remember to set up at least one DNS server if a host name is entered here!

**Language**

Choose a language for the webConfigurator

**webConfigurator**

**Theme**

Choose an alternative css file (if installed) to change the appearance of the webConfigurator. css files are located in /usr/local/www/css/

**Top Navigation**

The fixed option is intended for large screens only.

**Hostname in Menu**

Replaces the Help menu title in the Navbar with the system hostname or FQDN.

**Dashboard Columns**

**Interfaces / Interface Assignments**

[Interface Assignments](#) [Interface Groups](#) [Wireless](#) [VLANs](#) [QinQs](#) [PPPs](#) [GREs](#) [GIFs](#) [Bridges](#) [LAGGs](#)

Interface	Network port	
WAN	<input type="text" value="em0 (08:00:27:d7:3c:fc)"/>	
LAN	<input type="text" value="em1 (08:00:27:a3:b4:39)"/>	Delete
<b>Available network ports:</b>	<input type="text" value="em2 (08:00:27:9e:8e:9c)"/>	Add

Save

Interfaces that are configured as members of a lagg(4) interface will not be shown.  
Wireless interfaces must be created on the Wireless tab before they can be assigned.

General Configuration

**Enable**  Enable interface

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

**IPv4 Configuration Type**

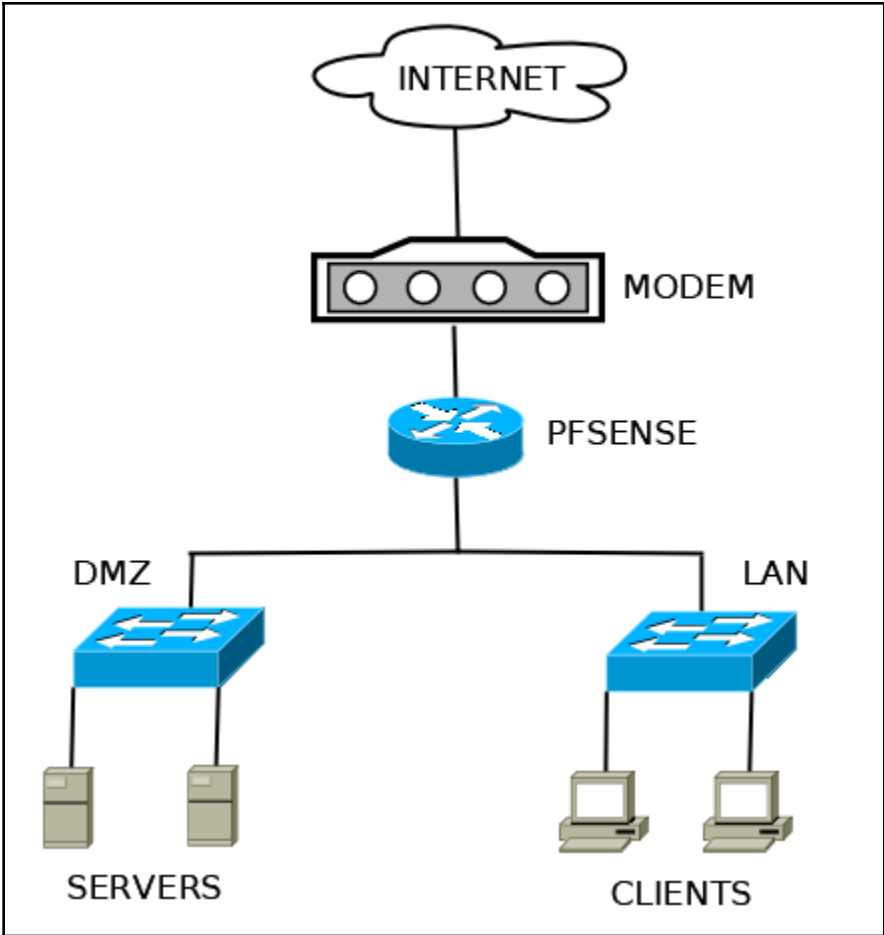
**IPv6 Configuration Type**

**MAC Address**   
This field can be used to modify ("spoof") the MAC address of this interface.  
Enter a MAC address in the following format: xxxxxxxxxx:xx:xx or leave blank.

**MTU**   
If this field is blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary in some circumstances.

**MSS**   
If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 (TCP/IP header size) will be in effect.

**Speed and Duplex**   
Explicitly set speed and duplex mode for this interface.  
WARNING: MUST be set to autoselect (automatically negotiate speed) unless the port this interface connects to has its speed and duplex forced.



**General Configuration**

**Enable**  Enable interface

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

**IPv4 Configuration Type**

**IPv6 Configuration Type**

**MAC Address**   
 This field can be used to modify ("spoof") the MAC address of this interface.  
 Enter a MAC address in the following format: xxxxxxxx:xxxx:xx or leave blank.

**MTU**   
 If this field is blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary in some circumstances.

**MSS**   
 If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 (TCP/IP header size) will be in effect.

**Speed and Duplex**   
 Explicitly set speed and duplex mode for this interface.  
 WARNING: MUST be set to autoselect (automatically negotiate speed) unless the port this interface connects to has its speed and duplex forced.

**Static IPv4 Configuration**

**IPv4 Address**  /

**IPv4 Upstream gateway**  + Add a new gateway

If this interface is an Internet connection, select an existing Gateway from the list or add a new one using the "Add" button.  
 On local area network interfaces the upstream gateway should be "none". Gateways can be managed by [clicking here](#).

**General Configuration**

**Enable**  Enable interface

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

**IPv4 Configuration Type**

**IPv6 Configuration Type**

**MAC Address**   
This field can be used to modify ("spoof") the MAC address of this interface.  
Enter a MAC address in the following format: xxxxxx.xxxxxx or leave blank.

**MTU**   
If this field is blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary in some circumstances.

**MSS**   
If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 (TCP/IP header size) will be in effect.

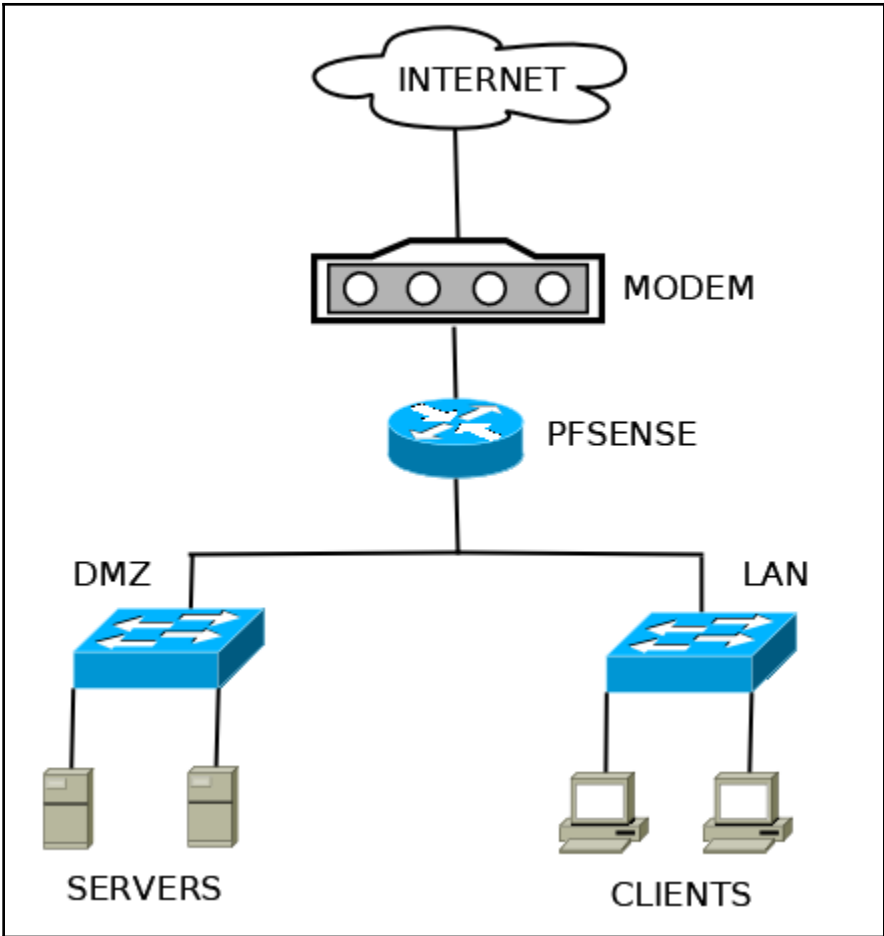
**Speed and Duplex**   
Explicitly set speed and duplex mode for this interface.  
WARNING: MUST be set to autoselect (automatically negotiate speed) unless the port this interface connects to has its speed and duplex forced.

**Static IPv4 Configuration**

**IPv4 Address**  /

**IPv4 Upstream gateway**

If this interface is an Internet connection, select an existing Gateway from the list or add a new one using the "Add" button.  
On local area network interfaces the upstream gateway should be "none". Gateways can be managed by [clicking here](#).



Secure Shell	
Secure Shell Server	<input type="checkbox"/> Enable Secure Shell
SSHd Key Only	Public Key Only <input type="text"/> <p>When set to <i>Public Key Only</i>, SSH access requires authorized keys and these keys must be configured for each <i>user</i> that has been granted secure shell access. If set to <i>Require Both Password and Public Key</i>, the SSH daemon requires both authorized keys <b>and</b> valid passwords to gain access. The default <i>Password or Public Key</i> setting allows either a valid password or a valid authorized key to login.</p>
SSH port	<input type="text" value="22"/> <p>Note: Leave this blank for the default of 22.</p>



File Key Conversions Help

Key  
No key.

Actions

Generate a public/private key pair Generate

Load an existing private key file Load

Save the generated key Save public key Save private key

Parameters

Type of key to generate:  
 RSA     DSA     ECDSA     ED25519     SSH-1 (RSA)

Number of bits in a generated key:

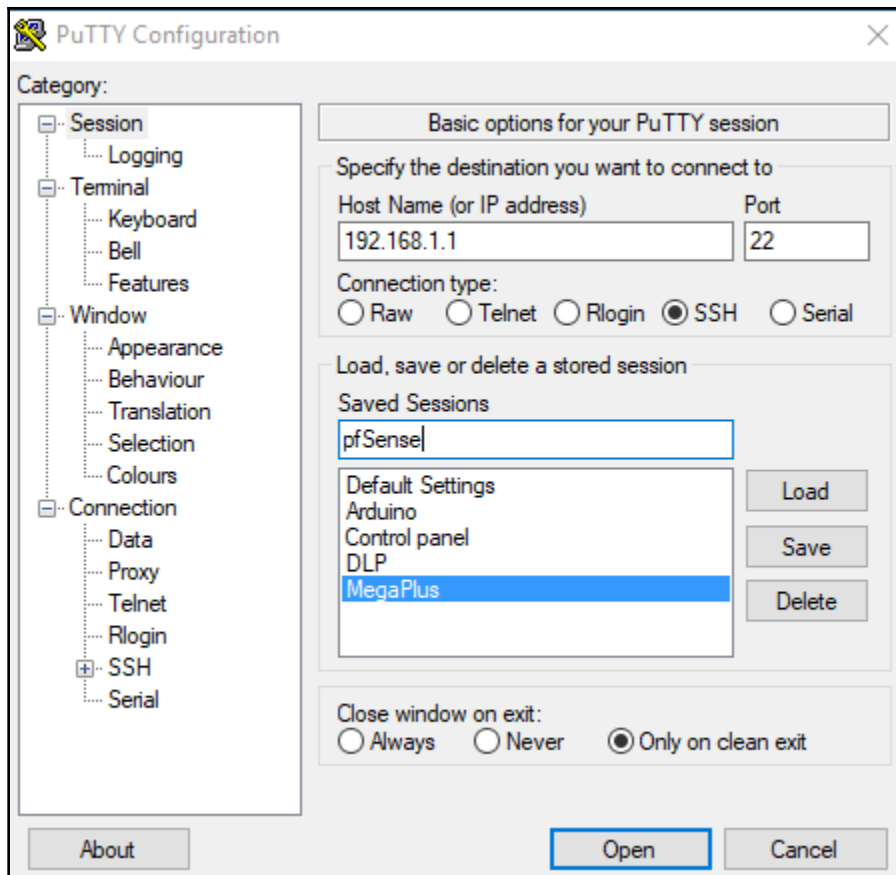
**SSHd Key Only**

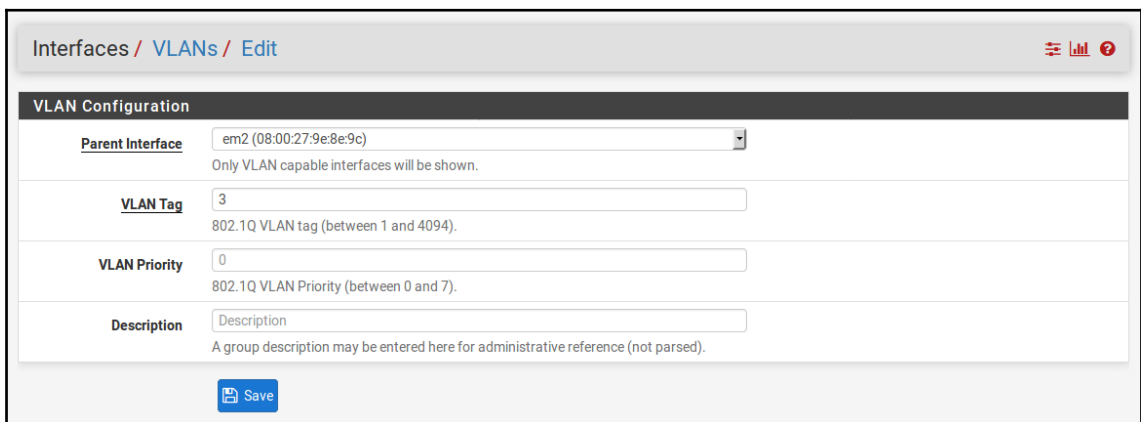
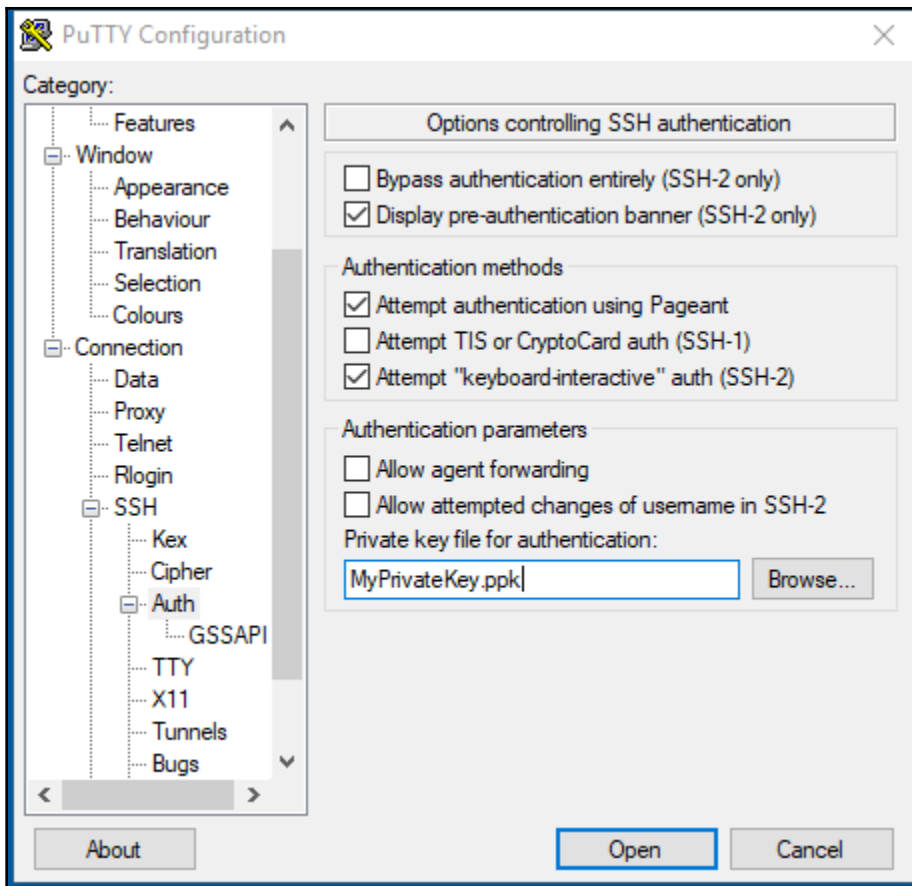
When set to *Public Key Only*, SSH access requires authorized keys and these keys must be configured for each **user** that has been granted secure shell access. If set to *Require Both Password and Public Key*, the SSH daemon requires both authorized keys **and** valid passwords to gain access. The default *Password or Public Key* setting allows either a valid password or a valid authorized key to login.

## Keys

**Authorized SSH Keys**

Enter authorized SSH keys for this user





Interfaces / Interface Assignments 📊 ?

Interface Assignments   Interface Groups   Wireless   VLANs   QinQs   PPPs   GREs   GIFs   Bridges   LAGGs

Interface	Network port	
WAN	em0 (08:00:27:d7:3c:fc)	
LAN	em1 (08:00:27:a3:b4:39)	Delete
OPT1	VLAN 3 on em3 (VLAN for developers)	Delete

Available network ports:

- em0 (08:00:27:d7:3c:fc)
- em1 (08:00:27:a3:b4:39)
- em2 (08:00:27:9e:8e:9c)
- em3 (08:00:27:e5:51:3d)
- VLAN 3 on em2
- VLAN 3 on em3 (VLAN for developers)

[Save](#) [+](#) Add

Interfaces that are configured as members of a lagg(4) in [this list](#)

Wireless interfaces must be created on the Wireless tab before they can be assigned.

```

Do VLANs need to be set up first?
If VLANs will not be used, or only for optional interfaces, it is typical to
say no here and use the webConfigurator to configure VLANs later, if required.

Should VLANs be set up now [y|n]? n

VLAN interfaces:

em2.3          VLAN tag 3, parent interface em2

If the names of the interfaces are not known, auto-detection can
be used instead. To use auto-detection, please disconnect all
interfaces before pressing 'a' to begin the process.

Enter the WAN interface name or 'a' for auto-detection
(em0 em1 em2 em3 em2.3 or a): em0

Enter the LAN interface name or 'a' for auto-detection
NOTE: this enables full Firewalling/NAT mode.
(em1 em2 em3 em2.3 a or nothing if finished): em1

Enter the Optional 1 interface name or 'a' for auto-detection
(em2 em3 em2.3 a or nothing if finished): █

```

---

Available interfaces:

1 - WAN (em0 - dhcp, dhcp6)  
2 - LAN (em1 - static)

Enter the number of the interface you wish to configure: 1

Configure IPv4 address WAN interface via DHCP? (y/n) y

Configure IPv6 address WAN interface via DHCP6? (y/n) y

Do you want to revert to HTTP as the webConfigurator protocol? (y/n) n

Please wait while the changes are saved to WAN...

Reloading filter...

Reloading routing configuration...

DHCPD...

The IPv4 WAN address has been set to dhcp

The IPv6 WAN address has been set to dhcp6

Press <ENTER> to continue. █

---

```
Available interfaces:
```

```
1 - WAN (em0 - dhcp, dhcp6)
2 - LAN (em1 - static)
```

```
Enter the number of the interface you wish to configure: 2
```

```
Enter the new LAN IPv4 address. Press <ENTER> for none:
> 172.16.1.1
```

```
Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
     255.255.0.0   = 16
     255.0.0.0    = 8
```

```
Enter the new LAN IPv4 subnet bit count (1 to 31):
> 16
```

```
For a WAN, enter the new LAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>
```

```
Enter the new LAN IPv6 address. Press <ENTER> for none:
> █
```

```
em0  08:00:27:d7:3c:fc  (up) Intel(R) PRO/1000 Legacy Network Connection 1.
em1  08:00:27:a3:b4:39  (up) Intel(R) PRO/1000 Legacy Network Connection 1.
em2  08:00:27:9e:8e:9c  (down) Intel(R) PRO/1000 Legacy Network Connection 1.
em3  08:00:27:e5:51:3d  (down) Intel(R) PRO/1000 Legacy Network Connection 1.
```

```
Do VLANs need to be set up first?
```

```
If VLANs will not be used, or only for optional interfaces, it is typical to
say no here and use the webConfigurator to configure VLANs later, if required.
```

```
Should VLANs be set up now [y|n]? y
```

```
WARNING: all existing VLANs will be cleared if you proceed!
```

```
Do you want to proceed [y|n]? y
```

```
VLAN Capable interfaces:
```

```
em0  08:00:27:d7:3c:fc  (up)
em1  08:00:27:a3:b4:39  (up)
em2  08:00:27:9e:8e:9c  (up)
em3  08:00:27:e5:51:3d  (up)
```

```
Enter the parent interface name for the new VLAN (or nothing if finished): em2█
```

# Chapter 2: Essential Services

Services / DHCP Server / LAN 🔄 📊 📄 ?

**LAN**

**General Options**

<b>Enable</b>	<input checked="" type="checkbox"/> Enable DHCP server on LAN interface
<b>BOOTP</b>	<input type="checkbox"/> Ignore BOOTP queries
<b>Deny unknown clients</b>	<input type="checkbox"/> Only the clients defined below will get DHCP leases from this server.
<b>Ignore denied clients</b>	<input type="checkbox"/> Denied clients will be ignored rather than rejected. <small>This option is not compatible with failover and cannot be enabled when a Failover Peer IP address is configured.</small>
<b>Ignore client identifiers</b>	<input type="checkbox"/> If a client includes a unique identifier in its DHCP request, that UID will not be recorded in its lease. <small>This option may be useful when a client can dual boot using different client identifiers but the same hardware (MAC) address. Note that the resulting server behavior violates the official DHCP specification.</small>
<b>Subnet</b>	172.16.1.0
<b>Subnet mask</b>	255.255.255.0
<b>Available range</b>	172.16.1.1 - 172.16.1.254
<b>Range</b>	<input type="text" value="172.16.1.100"/> <input type="text" value="172.16.1.200"/>
	From To

**Deny unknown clients**  Only the clients defined below will get DHCP leases from this server.

**DNS servers**

Leave blank to use the system default DNS servers: this interface's IP if DNS Forwarder or Resolver is enabled, otherwise the servers configured on the System / General Setup page.

LAN

DHCPv6 Server Router Advertisements

DHCPv6 Options

**DHCPv6 Server**  Enable DHCPv6 server on interface LAN

**Subnet** fd12:3456:789a::

**Subnet Mask** 48 bits

**Available Range** fd12:3456:789a:: to fd12:3456:789a:ffff:ffff:ffff:ffff

**Range**    
 From To

**Prefix Delegation Range**    
 From To

**Prefix Delegation Size**

A Prefix range can be defined here for DHCP Prefix Delegation. This allows for assigning networks to subrouters. The start and end of the range must end on boundaries of the prefix delegation size.

DHCP Static Mappings for this Interface

Static ARP	MAC address	IP address	Hostname	Description	
	08:00:27:94:0b:84	172.16.1.2		FreeRADIUS server	
	08:00:27:94:0b:83	172.16.1.243	user-VirtualBox	Linux Mint static mapping	
					Add



Services / DHCP Server / LAN / Edit Static Mapping 🔄 ⚙️ 📊 📄 ?

### Static DHCP Mapping on LAN

**MAC Address**  📄 Copy My MAC

MAC address (6 hex octets separated by colons)

**Client Identifier**

**IP Address**

If an IPv4 address is entered, the address must be outside of the pool.  
If no IPv4 address is given, one will be dynamically allocated from the pool.

The same IP address may be assigned to multiple mappings.

**Hostname**

Name of the host, without domain part.

**Description**

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

Services / DHCP Relay ⚙️ 📊 📄 ?

### DHCP Relay Configuration

**Enable**  Enable DHCP relay on interface

**Interface(s)**   LAN

Interfaces without an IP address will not be shown.

**Append circuit ID and agent ID to requests**  
If this is checked, the DHCP relay will append the circuit ID (pfSense interface number) and the agent ID to the DHCP request.

**Destination server**

This is the IPv4 address of the server to which DHCP requests are relayed.

📄 Save
+ Add server

**General DNS Resolver Options**

**Enable**     Enable DNS resolver

**Listen Port**   

The port used for responding to DNS queries. It should normally be left blank unless another service needs to bind to TCP/UDP port 53.

**Enable SSL/TLS Service**     Respond to incoming SSL/TLS queries from local clients

Configures the DNS Resolver to act as a DNS over SSL/TLS server which can answer queries from clients which also support DNS over TLS. Activating this option disables automatic interface response routing behavior, thus it works best with specific interface bindings.

**SSL/TLS Certificate**   

The server certificate to use for SSL/TLS service. The CA chain will be determined automatically.

**SSL/TLS Listen Port**   

The port used for responding to SSL/TLS DNS queries. It should normally be left blank unless another service needs to bind to TCP/UDP port 853.

**Network Interfaces**

- All
- WAN
- LAN
- WAN IPv6 Link-Local
- LAN IPv6 Link-Local

Interface IPs used by the DNS Resolver for responding to queries from clients. If an interface has both IPv4 and IPv6 IPs, both are used. Queries to other interface IPs not selected below are discarded. The default behavior is to respond to queries on every available IPv4 and IPv6 address.

**Outgoing Network Interfaces**

- All
- WAN
- LAN
- WAN IPv6 Link-Local
- LAN IPv6 Link-Local

Utilize different network interface(s) that the DNS Resolver will use to send queries to authoritative servers and receive their replies. By default all interfaces are used.

**Host Overrides**

Host	Parent domain of host	IP to return for host	Description	Actions
------	-----------------------	-----------------------	-------------	---------

Enter any individual hosts for which the resolver's standard DNS lookup process should be overridden and a specific IPv4 or IPv6 address should automatically be returned by the resolver. Standard and also non-standard names and parent domains can be entered, such as 'test', 'mycompany.localdomain', '1.168.192.in-addr.arpa', or 'somesite.com'. Any lookup attempt for the host will automatically return the given IP address, and the usual lookup server for the domain will not be queried for the host's records.

Add

**Domain Overrides**

Domain	Lookup Server IP Address	Description	Actions
--------	--------------------------	-------------	---------

Enter any domains for which the resolver's standard DNS lookup process should be overridden and a different (non-standard) lookup server should be queried instead. Non-standard, 'invalid' and local domains, and subdomains, can also be entered, such as 'test', 'mycompany.localdomain', '1.168.192.in-addr.arpa', or 'somesite.com'. The IP address is treated as the authoritative lookup server for the domain (including all of its subdomains), and other lookup servers will not be queried.

Add

DNS Server Settings	
<b>DNS Servers</b>	<input type="text" value="DNS Server"/> <input type="text" value="none"/>
Address	Gateway
Enter IP addresses to be used by the system for DNS resolution. These are also used for the DHCP service, DNS Forwarder and DNS Resolver when it has DNS Query Forwarding enabled.	Optionally select the gateway for each DNS server. When using multiple WAN connections there should be at least one unique DNS server per gateway.
<b>Add DNS Server</b>	<input type="button" value="+ Add DNS Server"/>
<b>DNS Server Override</b>	<input checked="" type="checkbox"/> Allow DNS server list to be overridden by DHCP/PPP on WAN If this option is set, pfSense will use DNS servers assigned by a DHCP/PPP server on WAN for its own purposes (including the DNS Forwarder/DNS Resolver). However, they will not be assigned to DHCP clients.

## General DNS Resolver Options

**Enable**     **Enable DNS resolver**

<b>Static DHCP</b>	<input checked="" type="checkbox"/> Register DHCP static mappings in the DNS Resolver If this option is set, then DHCP static mappings will be registered in the DNS Resolver, so that their name can be resolved. The domain in <a href="#">System &gt; General Setup</a> should also be set to the proper value.
--------------------	---

Services / [Dynamic DNS](#) / [Dynamic DNS Clients](#) / [Edit](#) ?

---

### Dynamic DNS Client

**Disable**     Disable this client

**Service Type**   

**Interface to monitor**      
If the interface IP address is private the public IP address will be fetched and used instead.

**Hostname**      
Enter the complete fully qualified domain name. Example: myhost.dyndns.org  
 DNS Made Easy: Dynamic DNS ID (NOT hostname)  
 he.net tunnelbroker: Enter the tunnel ID.  
 GleSYS: Enter the record ID.  
 DNSimple: Enter only the domain name.  
 Namecheap, Cloudflare, GratisDNS, Hover, CloudDNS, GoDaddy: Enter the hostname and the domain separately, with the domain being the domain or subdomain zone being handled by the provider.  
 Cloudflare: Enter @ as the hostname to indicate an empty field.

**MX**      
Note: With DynDNS service only a hostname can be used, not an IP address. Set this option only if a special MX record is needed. Not all services support this.

**Wildcards**     Enable Wildcard

**Verbose logging**     Enable verbose logging

Interfaces / **Wireless** 📊 📄 ?

Interface Assignments   Interface Groups   Wireless   VLANs   QinQs   PPPs   GREs   GIFs   Bridges   LAGGs

Wireless Interfaces			
Interface	Mode	Description	Actions
+ Add			

Interfaces / **Wireless** / Edit ?


**Wireless Interface Configuration**

**Parent Interface**  ▼


**Mode**  ▼

**Description**

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

 Save

Available network ports:  ▼ + Add

 Save

Interfaces / **OPT6** ☰ 📊 ?

**General Configuration**

**Enable**  Enable interface

**Description**

Enter a description (name) for the interface here.

**IPv4 Configuration Type**  ▼

**IPv6 Configuration Type**  ▼

# Chapter 3: Firewall and NAT

Firewall / Aliases / Edit ?

---

**Properties**

**Name**   
The name of the alias may only consist of the characters "a-z, A-Z, 0-9 and \_".

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

**Type**

---

**Host(s)**

**Hint** Enter as many hosts as desired. Hosts must be specified by their IP address or fully qualified domain name (FQDN). FQDN hostnames are periodically re-resolved and updated. If multiple IPs are returned by a DNS query, all are used. An IP range such as 192.168.1.1-192.168.1.10 or a small subnet such as 192.168.1.16/28 may also be entered and a list of individual IP addresses will be generated.

**IP or FQDN**

Firewall / Aliases / Bulk import ?

---

**IP Alias Details**

**Alias Name**   
The name of the alias may only consist of the characters "a-z, A-Z, 0-9 and \_".

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

**Aliases to import**

Paste in the aliases to import separated by a carriage return. Common examples are lists of IPs, networks, blacklists, etc. The list may contain IP addresses, with or without CIDR prefix, IP ranges, blank lines (ignored) and an optional description after each IP, e.g.:

- 172.16.1.2
- 172.16.0.0/24
- 10.11.12.100-10.11.12.200
- 192.168.1.254 Home router
- 10.20.0.0/16 Office network
- 10.40.1.10-10.40.1.19 Managed switches

Firewall / Rules / LAN

Floating WAN LAN

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓	1 / 505 KiB	IPv4*	LAN net	*	*	*	*	none	Default allow LAN to any rule	
<input type="checkbox"/>	✓	0 / 0 B	IPv6*	LAN net	*	*	*	*	none	Default allow LAN IPv6 to any rule	

Add
 Add
 Delete
 Save
 Separator

Firewall / Rules / Edit

Edit Firewall Rule

**Action**

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 UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

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

**Interface**

Choose the interface from which packets must come to match this rule.

**Address Family**

Select the Internet Protocol version this rule applies to.

**Protocol**

Choose which IP protocol this rule should match.

**Source**

**Source**  Invert match. any Source Address /

⚙ Display Advanced

The **Source Port Range** for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, **any**.

---

**Destination**

**Destination**  Invert match. Single host or alias 207.58.150.178 /

**Destination Port Range** (other)  (other)

From Custom To Custom

Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.

---

**Extra Options**

**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 doing a lot of logging, consider using a remote syslog server (see the [Status: System Logs: Settings](#) page).

**Description** Block Apple Insider rule  
A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.

**Advanced Options** ⚙ Display Advanced

Save



**Schedule Information**

**Schedule Name**   
 The name of the schedule may only consist of the characters "a-z, A-Z, 0-9 and \_".

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

**Month**

**Date**

October_2018						
Mon	Tue	Wed	Thu	Fri	Sat	Sun
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31				

Click individual date to select that date only. Click the appropriate weekday Header to select all occurrences of that weekday.

**Time**      
 Start Hrs Start Mins Stop Hrs Stop Mins

Select the time range for the day(s) selected on the Month(s) above. A full day is 0:00-23:59.

**Time range description**   
 A description may be entered here for administrative reference (not parsed).

**Configured Ranges**

<input type="text" value="Mon - Fri"/>	<input type="text" value="9:00"/>	<input type="text" value="17:00"/>	<input type="text" value="9 to 5"/>	<input type="button" value="Delete"/>
Day(s)	Start time	Stop time	Description	



Firewall / Rules / Floating

Floating WAN LAN

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>		0/0 B	IPv4*	Penalty_List	*	*	*	qOthersLow		Penalty Box	
<input type="checkbox"/>		0/0 B	IPv4*	*	*	*	*	none			

Firewall / Rules / Floating / Edit

Edit Firewall Rule

**Action** 
  
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 UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

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

**Quick**  Apply the action immediately on match.
  
Set this option to apply this action to traffic that matches this rule immediately.

**Interface**

  
LAN
  
DMZ
  
Choose the interface(s) for this rule.

**Direction**

**Address Family** 
  
Select the Internet Protocol version this rule applies to.

**Protocol** 
  
Choose which IP protocol this rule should match.

**Source**

**Source**  Invert match. any Source Address /

⚙ Display Advanced

The **Source Port Range** for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, **any**.

---

**Destination**

**Destination**  Invert match. any Destination Address /

**Destination Port Range** (other)  (other)

From Custom To Custom

Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.

---

**Extra Options**

**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 doing a lot of logging, consider using a remote syslog server (see the [Status: System Logs: Settings](#) page).

**Description** Allow all local interfaces to any rule  
A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.

**Advanced Options** ⚙ Display Advanced

Save

**Firewall / NAT / Port Forward** ?

Port Forward 1:1 Outbound NPT

**Rules**

Interface	Protocol	Source Address	Source Ports	Dest. Address	Dest. Ports	NAT IP	NAT Ports	Description	Actions
<span style="background-color: #28a745; color: white; padding: 2px 5px; border-radius: 3px;">↑ Add</span> <span style="background-color: #28a745; color: white; padding: 2px 5px; border-radius: 3px;">↓ Add</span> <span style="background-color: #dc3545; color: white; padding: 2px 5px; border-radius: 3px;">Delete</span> <span style="background-color: #17a2b8; color: white; padding: 2px 5px; border-radius: 3px;">Save</span> <span style="background-color: #ffc107; color: white; padding: 2px 5px; border-radius: 3px;">+ Separator</span>									

Firewall / NAT / Port Forward / Edit ?

### Edit Redirect Entry

**Disabled**  Disable this rule

**No RDR (NOT)**  Disable redirection for traffic matching this rule  
This option is rarely needed. Don't use this without thorough knowledge of the implications.

**Interface**   
Choose which interface this rule applies to. In most cases "WAN" is specified.

**Protocol**   
Choose which protocol this rule should match. In most cases "TCP" is specified.

**Source**

**Destination**  Invert match.   /   
Type Address/mask

**Destination port range**      
From port Custom To port Custom  
Specify the port or port range for the destination of the packet for this mapping. The 'to' field may be left empty if only mapping a single port.

**Redirect target IP**   
Enter the internal IP address of the server on which to map the ports.  
e.g.: 192.168.1.12

**Redirect target port**    
Port Custom  
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).  
This is usually identical to the "From port" above.

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

**No XMLRPC Sync**  Do not automatically sync to other CARP members  
This prevents the rule on Master from automatically syncing to other CARP members. This does NOT prevent the rule from being overwritten on Slave.

**NAT reflection**

**Filter rule association**   
The "pass" selection does not work properly with Multi-WAN. It will only work on an interface containing the default gateway.

**pfSense** COMMUNITY EDITION System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Help ▾

---

**Firewall / Virtual IPs / Edit** ?

---

**Edit Virtual IP**

**Type**  IP Alias  CARP  Proxy ARP  Other

**Interface** WAN ▾

**Address type** Single address ▾

**Address(es)** 10.1.1.1 / 8 ▾  
The mask must be the network's subnet mask. It does not specify a CIDR range.

**Virtual IP Password**    
Enter the VHID group password. Confirm

**VHID Group** 1 ▾  
Enter the VHID group that the machines will share.

**Advertising frequency** 1 ▾ 0 ▾  
Base Skew  
The frequency that this machine will advertise. 0 means usually master. Otherwise the lowest combination of both values in the cluster determines the master.

**Description** WAN virtual IP  
A description may be entered here for administrative reference (not parsed).



**Edit Advanced Outbound NAT Entry**

**Disabled**  Disable this rule

**Do not NAT**  Enabling this option will disable NAT for traffic matching this rule and stop processing Outbound NAT rules  
In most cases this option is not required.

**Interface**    
The interface on which traffic is matched as it exits the firewall. In most cases this is "WAN" or another externally-connected interface.

**Protocol**    
Choose which protocol this rule should match. In most cases "any" is specified.

**Source**   /     
Type Source network for the outbound NAT mapping. Port or Range

**Destination**   /     
Type Destination network for the outbound NAT mapping. Port or Range

Not   
Invert the sense of the destination match.

**Translation**

**Address**    
Connections matching this rule will be mapped to the specified Address.   
The Address can be an Interface, a Host-type Alias, or a Virtual IP address.



**Edit NAT 1:1 Entry**

**Disabled**  Disable this rule  
When disabled, the rule will not have any effect.

**No BINAT (NOT)**  Do not perform binat for the specified address  
Excludes the address from a later, more general, rule.

**Interface**   
Choose which interface this rule applies to. In most cases "WAN" is specified.

**External subnet IP**   
Enter the external (usually on a WAN) subnet's starting address for the 1:1 mapping. The subnet mask from the internal address below will be applied to this IP address.

**Internal IP**  Not   /   
Invert the sense of the match. Type Address/mask  
Enter the internal (LAN) subnet for the 1:1 mapping. The subnet size specified for the internal subnet will be applied to the external subnet.

**Destination**  Not   /   
Invert the sense of the match. Type Address/mask  
The 1:1 mapping will only be used for connections to or from the specified destination. Hint: this is usually "Any".

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

**NAT reflection**

Save

Firewall / NAT / NPt / Edit ?

### Edit NAT NPt Entry

**Disabled**  Disable this rule

**Interface**  ▼  
 Choose which interface this rule applies to.  
 Hint: Typically the "WAN" is used here.


**Internal IPv6 prefix**  Not  
 Use this option to invert the sense of the match.

**Address**  /  ▼  
 Internal (LAN) ULA IPv6 Prefix for the Network Prefix translation. The prefix size specified for the internal IPv6 prefix will be applied to the external prefix.

**Destination IPv6 prefix**  Not  
 Use this option to invert the sense of the match.

**Address**  /  ▼  
 Global Unicast routable IPv6 prefix

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



Services / UPnP & NAT-PMP 📊 📄 ?

### UPnP & NAT-PMP Settings

**Enable**  Enable UPnP & NAT-PMP

**UPnP Port Mapping**  Allow UPnP Port Mapping  
 This protocol is often used by Microsoft-compatible systems.

**NAT-PMP Port Mapping**  Allow NAT-PMP Port Mapping  
 This protocol is often used by Apple-compatible systems.

**External Interface**  ▼  
 Select only the primary WAN interface (interface with the default gateway). Only one interface may be chosen.

**Interfaces**   
 DMZ  
 WAN  
 loopback  
▼  
 Select the internal interfaces, such as LAN, where UPnP/NAT-PMP clients reside. Use the CTRL or COMMAND key to select multiple interfaces.

# Chapter 4: Additional Services

Services / Captive Portal

### Captive Portal Zones

Zone	Interfaces	Number of users	Description	Actions
Guest_WiFi	LAN	0	WiFi network for customers	

[+ Add](#)

Services / Captive Portal / Guest\_WiFi / Configuration

[Configuration](#) [MACs](#) [Allowed IP Addresses](#) [Allowed Hostnames](#) [Vouchers](#) [File Manager](#)

### Captive Portal Configuration

**Enable**  Enable Captive Portal

**Interfaces**

WAN  
LAN  
DMZ

Select the interface(s) to enable for captive portal.

**Logout popup window**  Enable logout popup window  
If enabled, a popup window will appear when clients are allowed through the captive portal. This allows clients to explicitly disconnect themselves before the idle or hard timeout occurs.

**Pre-authentication redirect URL**   
Use this field to set \$PORTAL\_REDIREURL\$ variable which can be accessed using the custom captive portal index.php page or error pages.

**After authentication Redirection URL**   
Clients will be redirected to this URL instead of the one they initially tried to access after they've authenticated.

### Authentication

**Authentication Method**  No Authentication  Local User Manager / Vouchers  RADIUS Authentication

Select an Authentication Method to use for this zone. One method must be selected.



**Authentication**

**Authentication Method**     No Authentication     Local User Manager / Vouchers     RADIUS Authentication

Select an Authentication Method to use for this zone. One method must be selected.

**HTML Page Contents**

**Portal page contents**        No file selected.

Upload an HTML/PHP file for the portal page here (leave blank to keep the current one). Make sure to include a form (POST to "\$PORTAL\_ACTIONS") with a submit button (name="accept") and a hidden field with name="redirurl" and value="\$PORTAL\_REDIRURL\$". Include the "auth\_user" and "auth\_pass" and/or "auth\_voucher" input fields if authentication is enabled, otherwise it will always fail.

Example code for the form:

```
<form method="post" action="$PORTAL_ACTIONS">
<input name="auth_user" type="text">
<input name="auth_pass" type="password">
<input name="auth_voucher" type="text">
<input name="redirurl" type="hidden" value="$PORTAL_REDIRURL$">
<input name="zone" type="hidden" value="$PORTAL_ZONES">
<input name="accept" type="submit" value="Continue">
</form>
```

**Current Portal Page**               

**Auth error page contents**        No file selected.

The contents of the HTML/PHP file that is uploaded here are displayed when an authentication error occurs. It may include "\$PORTAL\_MESSAGES", which will be replaced by the error or reply messages from the RADIUS server, if any.

**Current Auth Error Page**           

**Logout page contents**        No file selected.

The contents of the HTML/PHP file that is uploaded here are displayed on authentication success when the logout popup is enabled.

**Current Logout Page**           

Services / Captive Portal / Guest\_WiFi / Vouchers 📊 📄 ?

Configuration    MACs    Allowed IP Addresses    Allowed Hostnames    **Vouchers**    File Manager

**Voucher Rolls**

Roll #	Minutes/Ticket	# of Tickets	Comment
0	120	1023	Voucher rolls for captive portal access

**Create, Generate and Activate Rolls with Vouchers**

**Enable**     Enable the creation, generation and activation of rolls with vouchers

### Voucher Rolls

<b>Roll #</b>	<input type="text" value="0"/>	Enter the Roll# (0..65535) found on top of the generated/printed vouchers
<b>Minutes per ticket</b>	<input type="text" value="120"/>	Defines the time in minutes that a user is allowed access. The clock starts ticking the first time a voucher is used for authentication.
<b>Count</b>	<input type="text" value="1023"/>	Enter the number of vouchers (1..1023) found on top of the generated/printed vouchers. WARNING: Changing this number for an existing Roll will mark all vouchers as unused again
<b>Comment</b>	<input type="text" value="Voucher rolls for captive portal access"/>	Can be used to further identify this roll. Ignored by the system.

<b># of Roll bits</b>	<input type="text" value="16"/>	Reserves a range in each voucher to store the Roll # it belongs to. Allowed range: 1..31. Sum of Roll+Ticket+Checksum bits must be one Bit less than the RSA key size.
<b># of Ticket bits</b>	<input type="text" value="10"/>	Reserves a range in each voucher to store the Ticket# it belongs to. Allowed range: 1..16. Using 16 bits allows a roll to have up to 65535 vouchers. A bit array, stored in RAM and in the config, is used to mark if a voucher has been used. A bit array for 65535 vouchers requires 8 KB of storage.
<b># of Checksum bits</b>	<input type="text" value="5"/>	Reserves a range in each voucher to store a simple checksum over Roll # and Ticket#. Allowed range is 0..31.

<b>Idle timeout (Minutes)</b>	<input type="text"/>	Clients will be disconnected after this amount of inactivity. They may log in again immediately, though. Leave this field blank for no idle timeout.
<b>Hard timeout (Minutes)</b>	<input type="text"/>	Clients will be disconnected after this amount of time, regardless of activity. They may log in again immediately, though. Leave this field blank for no hard timeout (not recommended unless an idle timeout is set).

System / User Manager / Groups ?

Users Groups Settings Authentication Servers

### Groups

Group name	Description	Member Count	Actions
admins	System Administrators	1	
all	All Users	4	
captive-portal	User group for captive portal users	2	
vpnguy	User group for VPN	0	

[+ Add](#)

System / User Manager / Groups / Edit ?

Users Groups Settings Authentication Servers

### Group Properties

**Group name**

**Scope**  Warning: Changing this setting may affect the local groups file, in which case a reboot may be required for the changes to take effect.

**Description**   
Group description, for administrative information only

**Group membership**

Not members

- admin
- homer
- john
- vpnguy

Members

-

[> Move to "Members"](#)
[<< Move to "Not members"](#)

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


[Save](#)

### Assigned privileges

System - HA node sync  
User - Config: Deny Config Write  
User - Notices: View  
User - Notices: View and Clear  
User - Services: Captive Portal login  
User - System: Copy files (scp)  
User - System: Copy files to home directory (chrooted scp)  
User - System: Shell account access  
User - System: SSH tunneling  
User - VPN: IPsec xauth Dialin  
User - VPN: L2TP Dialin  
User - VPN: PPPoE Dialin  
WebCfg - AJAX: Get Service Providers  
WebCfg - AJAX: Get Stats  
WebCfg - All pages  
WebCfg - Crash reporter  
WebCfg - Dashboard (all)  
WebCfg - Dashboard widgets (direct access).  
WebCfg - Diagnostics: ARP Table  
WebCfg - Diagnostics: Authentication

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

### Assigned Privileges

Name	Description	Action
User - VPN: IPsec xauth Dialin	Indicates whether the user is allowed to dial in via IPsec xauth (Note: Does not allow shell access, but may allow the user to create SSH tunnels)	

 Add

### User Properties

**Defined by** USER

**Disabled**  This user cannot login

**Username**

**Password**

**Full name**   
User's full name, for administrative information only

**Expiration date**   
Leave blank if the account shouldn't expire, otherwise enter the expiration date as MM/DD/YYYY

**Custom Settings**  Use individual customized GUI options and dashboard layout for this user.

**Group membership**

Not member of

Member of

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

> Move to "Member of" list
<< Move to "Not member of" list

---

### Effective Privileges

Inherited from	Name	Description	Action
captive-portal	User - Services: Captive Portal login	Indicates whether the user is able to login on the captive portal.	<span style="background-color: #4CAF50; color: white; padding: 2px 5px;">+</span> Add

Package / FreeRADIUS: Interfaces / Interfaces ?

[Users](#)   [MACs](#)   [NAS / Clients](#)   [Interfaces](#)   [Settings](#)   [EAP](#)   [SQL](#)   [LDAP](#)   [View config](#)   [XMLRPC Sync](#)

Interface IP Address	Port	Interface Type	IP Version	Description	Action
*	1813	acct	ipaddr	Accounting	<span style="color: blue;">✎</span> <span style="color: red;">✖</span>
*	1812	auth	ipaddr	Authentication	<span style="color: blue;">✎</span> <span style="color: red;">✖</span>
*	1816	status	ipaddr	Status	<span style="color: blue;">✎</span> <span style="color: red;">✖</span>

+ Add

Save

FreeRADIUS: Interfaces / Edit / Interfaces ?

Users   MACs   NAS / Clients   **Interfaces**   Settings   EAP   SQL   LDAP   View config   XMLRPC Sync

---

**General Configuration**


**Interface IP Address**   
 Enter the IP address (e.g. 192.168.100.1) of the listening interface. If you choose \* then it means all interfaces. (Default: \*)

**Port**   
 Enter the port number of the listening interface. Different interface types need different ports. Click Info for details. i

**Interface Type**   
 Enter the type of the listening interface. (Default: Authentication)

**IP Version**   
 Enter the IP version of the listening interface. (Default: IPv4)

**Description**   
 Optionally enter a description here for your reference.



FreeRADIUS: Clients / Edit / NAS / Clients ?

Users   MACs   **NAS / Clients**   Interfaces   Settings   EAP   SQL   LDAP   View config   XMLRPC Sync

---

**General Configuration**

**Client IP Address**   
 Enter the IP address of the RADIUS client. This is the IP of the NAS (switch, access point, firewall, router, etc.).

**Client IP Version**

**Client Shortname**   
 Enter a short name for the client. This is generally the hostname of the NAS.

**Client Shared Secret**   
 Enter the shared secret of the RADIUS client here. This is the shared secret (password) which the NAS (switch, accesspoint, etc.) needs to communicate with the RADIUS server. FreeRADIUS is limited to 31 characters for the shared secret.  
**Warning:** Single quotes in shared secret must be escaped with a backslash (\' ). Backslash must be escaped by using two backslashes (\\ ).

FreeRADIUS: Users / Edit / Users ?

Users **MACs** NAS / Clients Interfaces Settings EAP SQL LDAP View config XMLRPC Sync

### General Configuration

**Username**   
 Enter the username. Whitespace is allowed.  
 Note: May only contain a-z, A-Z, 0-9, underscore, period and hyphen when using OTP.

**Password**   
 Enter the password for this username. Leave empty if you want to use custom options (such as OTP) instead of username/password.

**Password Encryption**   
 Select the password encryption for this user. Default: Cleartext-Password

### Authentication

**Authentication Method**  No Authentication  Local User Manager / Vouchers  RADIUS Authentication  
 Select an Authentication Method to use for this zone. One method must be selected.

**RADIUS protocol**  PAP  CHAP-MD5  MSCHAPv1  MSCHAPv2

### Primary Authentication Source

**Primary RADIUS server**     
IP address of the RADIUS server to authenticate against. RADIUS port. Leave blank for default (1812) RADIUS shared secret. Leave blank to not use a shared secret (not recommended)

**Secondary RADIUS server**     
IP address of the RADIUS server to authenticate against. RADIUS port. Leave blank for default (1812) RADIUS shared secret. Leave blank to not use a shared secret (not recommended)

### Secondary Authentication Source

**Primary RADIUS server**     
IP address of the RADIUS server to authenticate against. RADIUS port. Leave blank for default (1812) RADIUS shared secret. Leave blank to not use a shared secret (not recommended)

**Secondary RADIUS server**     
IP address of the RADIUS server to authenticate against. RADIUS port. Leave blank for default (1812) RADIUS shared secret. Leave blank to not use a shared secret (not recommended)

### Accounting

**RADIUS**  Send RADIUS accounting packets to the primary RADIUS server.

**Accounting Port**   
 Leave blank to use the default port (1813).

**Accounting updates**  No updates  Stop/Start  Stop/Start (FreeRADIUS)  Interim

### RADIUS Options

**Reauthentication**  Reauthenticate connected users every minute  
 If reauthentication is enabled, Access-Requests will be sent to the RADIUS server for each user that is logged in every minute. If an Access-Reject is received for a user, that user is disconnected from the captive portal immediately. Reauthentication requires user credentials to be cached in the captive portal database while a user is logged in; The cached credentials are necessary for the portal to perform automatic reauthentication requests.

**RADIUS MAC Authentication**  Enable RADIUS MAC authentication  
 If this option is enabled, the captive portal will try to authenticate users by sending their MAC address as the username and the password entered below to the RADIUS server.

**MAC authentication secret**

**RADIUS NAS IP Attribute**   
 Choose the IP to use for calling station attribute.

Services / [NTP](#) / [Settings](#) 🔄 📊 📄 ?

[Settings](#) [ACLs](#) [Serial GPS](#) [PPS](#)

### NTP Server Configuration

**Interface**   
 Interfaces without an IP address will not be shown.  
 Selecting no interfaces will listen on all interfaces with a wildcard.  
 Selecting all interfaces will explicitly listen on only the interfaces/IPs specified.

Time Servers	Prefer	No Select	Is a Pool	
<input type="text" value="0.pfsense.pool.ntp.org"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="button" value="Delete"/>
<input type="text" value="Hostname"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="button" value="Delete"/>

**Add**

NTP will only sync if a majority of the servers agree on the time. For best results you should configure between 3 and 5 servers ([NTP support pages recommend at least 4 or 5](#)), or a pool. If only one server is configured, it **will** be believed, and if 2 servers are configured and they disagree, **neither** will be believed. Options:  
**Prefer** - NTP should favor the use of this server more than all others.  
**No Select** - NTP should not use this server for time, but stats for this server will be collected and displayed.  
**Is a Pool** - this entry is a pool of NTP servers and not a single address. This is assumed for \*.pool.ntp.org.





### SNMP Daemon

**Enable**  Enable the SNMP Daemon and its controls

### SNMP Daemon Settings

**Polling Port**

Enter the port to accept polling events on (default 161).

**System Location**

**System Contact**

**Read Community String**

The community string is like a password, restricting access to querying SNMP to hosts knowing the community string. Use a strong value here to protect from unauthorized information disclosure.

### SNMP Traps Enable

**Enable**  Enable the SNMP Trap and its controls

### SNMP Modules

- SNMP modules**
- MibII
  - Netgraph
  - PF
  - Host Resources
  - UCD
  - Regex

# Chapter 5: Virtual Private Networking

VPN / IPsec / Tunnels

Tunnels Mobile Clients Pre-Shared Keys Advanced Settings

### IPsec Tunnels

	IKE	Remote Gateway	Mode	P1 Protocol	P1 Transforms	P1 DH-Group	P1 Description	Actions
<input type="checkbox"/> <span>Disable</span>	V2	WAN 10.0.3.14		AES (256 bits)	SHA256	2 (1024 bit)	Tunnel to satellite office location	
<span>Show Phase 2 Entries (1)</span>								
<input type="checkbox"/> <span>Disable</span>	V1	WAN Mobile Client	aggressive	AES (256 bits)	SHA1	2 (1024 bit)		
<span>Show Phase 2 Entries (1)</span>								

+ Add P1 Delete P1s

VPN / IPsec / Tunnels / Edit Phase 1

Tunnels Mobile Clients Pre-Shared Keys Advanced Settings

### General Information

**Disabled**  Set this option to disable this phase1 without removing it from the list.

**Key Exchange version** IKEv2  
Select the Internet Key Exchange protocol version to be used. Auto uses IKEv2 when initiator, and accepts either IKEv1 or IKEv2 as responder.

**Internet Protocol** IPv4  
Select the Internet Protocol family.

**Interface** WAN  
Select the interface for the local endpoint of this phase1 entry.

**Remote Gateway**  
Enter the public IP address or host name of the remote gateway.

**Description** Phase 1 IPsec peer-to-peer  
A description may be entered here for administrative reference (not parsed).

### Phase 1 Proposal (Authentication)

**Authentication Method** Mutual PSK  
Must match the setting chosen on the remote side.

**My identifier** My IP address

**Peer identifier** Peer IP address

**Pre-Shared Key** supersecretkey  
Enter the Pre-Shared Key string.

---

### Phase 1 Proposal (Encryption Algorithm)

**Encryption Algorithm** AES 256 bits SHA256 2 (1024 bit) Delete

Algorithm      Key length      Hash      DH Group

Note: Blowfish, 3DES, CAST128, MD5, SHA1, and DH groups 1, 2, 22, 23, and 24 provide weak security and should be avoided.

**Add Algorithm** + Add Algorithm

---

**Lifetime (Seconds)** 28800

Firewall / [Rules](#) / [IPsec](#) ⌵ 📊 📄 ?

Floating
WAN
LAN
DMZ
L2TP VPN
IPsec
OpenVPN

#### Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✔	0/0 B	IPv4 *	172.25.0.0/16	*	*	*	*	none		📌 📄 🗑️

↑ Add
↓ Add
🗑️ Delete
📄 Save
+ Separator

📘

Status / IPsec / Overview 🔄 📊 📄 ?

Overview Leases SADs SPDs

### IPsec Status

IPsec ID	Description	Local ID	Local IP	Remote ID	Remote IP	Role	Reauth	Algo	Status
con1000: #4	Tunnel to satellite office location	10.0.3.18	10.0.3.18	10.0.3.14	10.0.3.14	IKEv2 initiator	27851 seconds (07:44:11)	AES_CBC HMAC_SHA2_256_128 PRF_HMAC_SHA2_256 MODP_1024	ESTABLISHED 66 seconds (00:01:06) ago <span style="float: right;">🗑 Disconnect</span>
<a href="#">+ Show child SA entries</a>		10.0.3.18	10.0.3.18	admin@pfsensesetup.com	Unknown	Awaiting connections			

📄

VPN / IPsec / Mobile Clients 🔄 📊 📄 ?

Tunnels Mobile Clients Pre-Shared Keys Advanced Settings

### Enable IPsec Mobile Client Support

IKE Extensions  Enable IPsec Mobile Client Support

### Extended Authentication (Xauth)

User Authentication   
Source

Group Authentication   
Source

### Client Configuration (mode-cfg)

Virtual Address Pool  Provide a virtual IP address to clients

Network configuration for Virtual Address Pool

System / User Manager / Groups / Edit ?

Users **Groups** Settings Authentication Servers

### Group Properties

**Group name**

**Scope**  ▼  
 Warning: Changing this setting may affect the local groups file, in which case a reboot may be required for the changes to take effect.

**Description**   
 Group description, for administrative information only

**Group membership**

<input type="text" value="admin"/> <input type="text" value="homer"/> <input type="text" value="john"/>	<input type="text" value="bart"/> <input type="text" value="comicbookguy"/> <input type="text" value="vpnguy"/>
Not members	Members

> Move to "Members"
<< Move to "Not members"

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

### Assigned privileges

- System - HA node sync
- User - Config: Deny Config Write
- User - Notices: View
- User - Notices: View and Clear
- User - Services: Captive Portal login
- User - System: Copy files (scp)
- User - System: Copy files to home directory (chrooted scp)
- User - System: Shell account access
- User - System: SSH tunneling
- User - VPN: IPsec xauth Dialin
- User - VPN: L2TP Dialin
- User - VPN: PPPoE Dialin
- WebCfg - AJAX: Get Service Providers
- WebCfg - AJAX: Get Stats
- WebCfg - All pages
- WebCfg - Crash reporter
- WebCfg - Dashboard (all)
- WebCfg - Dashboard widgets (direct access).
- WebCfg - Diagnostics: ARP Table
- WebCfg - Diagnostics: Authentication

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



User Properties

Defined by USER

Disabled  This user cannot login

Username

Password

Full name   
User's full name, for administrative information only

Expiration date   
Leave blank if the account shouldn't expire, otherwise enter the expiration date as MM/DD/YYYY

Custom Settings  Use individual customized GUI options and dashboard layout for this user.

Group membership

<input type="text" value="admins&lt;br/&gt;captive-portal&lt;br/&gt;test&lt;br/&gt;vpnusers_"/>	<input type="text" value="vpnusers"/>
---	---------------------------------------

Not member of

Member of

» Move to "Member of" list

« Move to "Not member of" list

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

VPN Site Configuration

General Client Name Resolution Authentication

Remote Host

Host Name or IP Address Port

Auto Configuration ike config pull

Local Host

Adapter Mode

Use a virtual adapter and assigned address

MTU 1380 Obtain Automatically

Address

Netmask

Save Cancel

VPN Site Configuration

Client Name Resolution Authentication Phase

Authentication Method Mutual PSK + XAuth

Local Identity Remote Identity Credentials

Identification Type

User Fully Qualified E

UFQDN String

Save Cancel

---

The image shows a 'VPN Site Configuration' dialog box with a close button in the top right corner. It has four tabs: 'Name Resolution', 'Authentication', 'Phase 1', and 'Phase 2'. The 'Phase 1' tab is selected. Inside the dialog, there is a section titled 'Proposal Parameters' containing several configuration options:

- Exchange Type: aggressive
- DH Exchange: group 2
- Cipher Algorithm: aes
- Cipher Key Length: 256 Bits
- Hash Algorithm: sha1
- Key Life Time limit: 86400 Secs
- Key Life Data limit: 0 Kbytes

Below these parameters is a checkbox labeled 'Enable Check Point Compatible Vendor ID' which is currently unchecked. At the bottom of the dialog are two buttons: 'Save' and 'Cancel'.



---

VPN Site Configuration

Authentication Phase 1 Phase 2 Policy

Proposal Parameters

Transform Algorithm	esp-aes
Transform Key Length	256 Bits
HMAC Algorithm	sha1
PFS Exchange	disabled
Compress Algorithm	disabled
Key Life Time limit	3600 Secs
Key Life Data limit	0 Kbytes

Save Cancel



Create / Edit CA

**Descriptive name**

**Method**

Internal Certificate Authority

**Key length (bits)**

**Digest Algorithm**

NOTE: It is recommended to use an algorithm stronger than SHA1 when possible.

**Lifetime (days)**

**Common Name**

The following certificate authority subject components are optional and may be left blank.

**Country Code**

**State or Province**

**City**

**Organization**

**Organizational Unit**

[CAs](#)  
 [Certificates](#)  
 [Certificate Revocation](#)

### Add/Sign a New Certificate

**Method**

Create an internal Certificate

**Descriptive name**

OpenVPN certificate - server

#### Certificate Attributes

**Attribute Notes**

The following attributes are added to certificates and requests when they are created or signed. These attributes behave differently depending on the selected mode.

For Internal Certificates, these attributes are added directly to the certificate as shown.

**Certificate Type**

Server Certificate

Add type-specific usage attributes to the signed certificate. Used for placing usage restrictions on, or granting abilities to, the signed certificate.

**Alternative Names**

FQDN or Hostname

Type

Value

Enter additional identifiers for the certificate in this list. The Common Name field is automatically added to the certificate as an Alternative Name. The signing CA may ignore or change these values.

Add



MyOpenVPN certificate <i>User Certificate</i> CA: <b>No</b> Server: <b>No</b>	OpenVPN CA ST=US, O=Wayne, L=New Jersey, CN=thewookie.duckdns.org, C=US Valid From: <b>Sun, 21 Oct 2018 04:16:17 +0000</b> Valid Until: <b>Wed, 18 Oct 2028 04:16:17 +0000</b>	ⓘ ⚙️ 🔍 📧 🗑️
MyOpenVPN2 certificate <i>Server Certificate</i> CA: <b>No</b> Server: <b>Yes</b>	OpenVPN CA ST=US, O=Wayne, L=New Jersey, CN=thewookie.duckdns.org Valid From: <b>Sun, 21 Oct 2018 04:23:57 +0000</b> Valid Until: <b>Wed, 18 Oct 2028 04:23:57 +0000</b>	ⓘ ⚙️ 🔍 📧 🗑️

**General Information**

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

**Server mode** Peer to Peer ( SSL/TLS )

**Protocol** UDP on IPv4 only

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

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

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

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

**Cryptographic Settings**

**TLS Configuration**  Use a TLS Key  
 A TLS key enhances security of an OpenVPN connection by requiring both parties to have a common key before a peer can perform a TLS handshake. This layer of HMAC authentication allows control channel packets without the proper key to be dropped, protecting the peers from attack or unauthorized connections. The TLS Key does not have any effect on tunnel data.

Automatically generate a TLS Key.

**Peer Certificate Authority** OpenVPN CA

**Peer Certificate Revocation list** No Certificate Revocation Lists defined. One may be created here: [System > Cert. Manager](#)

**Server certificate** MyOpenVPN2 certificate (Server: Yes, CA: OpenVPN CA)

Firewall / Rules / OpenVPN

Floating WAN LAN PFSYNC IPsec **OpenVPN**

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓	0/0 B	IPv4*	*	*	*	*	none		Allow OpenVPN traffic	

Wizard / OpenVPN Remote Access Server Setup /

Step

**OpenVPN Remote Access Server Setup**

This wizard will provide guidance through an OpenVPN Remote Access Server Setup .

The wizard may be stopped at any time by clicking the logo image at the top of the screen.

**Select an Authentication Backend Type**

Type of Server

**NOTE:** If unsure, leave this set to "Local User Access."

---

Wizard / OpenVPN Remote Access Server Setup / Firewall Rule Configuration ?

Step 10 of 11

**Firewall Rule Configuration**

OpenVPN Remote Access Server Setup Wizard

**Firewall Rule Configuration**

Firewall rules control what network traffic is permitted. Rules must be added to allow traffic to the OpenVPN server's IP and port, as well as allowing traffic from connected clients through the tunnel. These rules can be automatically added here, or configured manually after completing the wizard.

**Traffic from clients to server**

**Firewall Rule**

Add a rule to permit connections to this OpenVPN server process from clients anywhere on the Internet.

**Traffic from clients through VPN**

**OpenVPN rule**

Add a rule to allow all traffic from connected clients to pass inside the VPN tunnel.

[» Next](#)

Wizard / OpenVPN Remote Access Server Setup / Finished! ?

Step 11 of 11

**Finished!**

OpenVPN Remote Access Server Setup Wizard

**Configuration Complete!**

The configuration is now complete.

To be able to export client configurations, browse to System->Packages and install the OpenVPN Client Export package.

[» Finish](#)

OpenVPN Clients		
User	Certificate Name	Export
bart	Use my OpenVPN certificate	- Inline Configurations: <a href="#">Most Clients</a> <a href="#">Android</a> <a href="#">OpenVPN Connect (iOS/Android)</a> - Bundled Configurations: <a href="#">Archive</a> <a href="#">Config File Only</a> - Current Windows Installer (2.4.6-1x02): <a href="#">Windows Vista and Later</a> - Old Windows Installers (2.3.18-1x02): <a href="#">x86-xp</a> <a href="#">x64-xp</a> <a href="#">x86-win6</a> <a href="#">x64-win6</a> - Viscosity (Mac OS X and Windows): <a href="#">Viscosity Bundle</a> <a href="#">Viscosity Inline Config</a>

OpenVPN Connection (pfSense-UDP4-1195-comicbookguy-config) [min] [max] [close]

Current State: Connecting

```
Thu Nov 01 20:23:51 2018 OpenVPN 2.4.6 x86_64-w64-mingw32 [SSL (OpenSSL)] [LZO] [LZ4] [PKCS11] [AE
Thu Nov 01 20:23:51 2018 Windows version 6.1 (Windows 7) 64bit
Thu Nov 01 20:23:51 2018 library versions: OpenSSL 1.1.0h 27 Mar 2018, LZO 2.10
```

pfSense-UDP4-1195-comicbook... [close]

Username:

Password:

Save password

OpenVPN GUI 11.10.0.0/2.4.6



Configuration **Users**

### Enable L2TP

Enable  Enable L2TP server

### Configuration

**Interface** WAN

**Server address** 192.168.1.61

Enter the IP address the L2TP server should give to clients for use as their "gateway". Typically this is set to an unused IP just outside of the client range.

NOTE: This should NOT be set to any IP address currently in use on this firewall.

**Remote address range** 192.168.1.10 / 24

Specify the starting address for the client IP address subnet.

**Number of L2TP users** 1

**Secret** Secret Secret

Specify optional secret shared between peers. Required on some devices/setups.

Confirm

**Authentication type** CHAP

Specifies the protocol to use for authentication.

**Primary L2TP DNS server** 1.1.1.1

**Secondary L2TP DNS server** 1.0.0.1



User

**Username**

**Password**

To change the users password, enter it here.

Confirm

**IP Address**

To assign the user a specific IP address, enter it here.

 Save

---

## Chapter 6: Traffic Shaping

Firewall / Traffic Shaper / Wizards

By Interface    By Queue    Limiters    **Wizards**

**Traffic Shaper Wizards**

Multiple Lan/Wan	<a href="#">traffic_shaper_wizard_multi_all.xml</a>
Dedicated Links	<a href="#">traffic_shaper_wizard_dedicated.xml</a>

Detailed description: This screenshot shows the 'Wizards' tab selected in the 'Traffic Shaper' section of the firewall configuration interface. The breadcrumb path is 'Firewall / Traffic Shaper / Wizards'. Below the breadcrumb, there are four tabs: 'By Interface', 'By Queue', 'Limiters', and 'Wizards', with 'Wizards' being the active tab. A dark header bar contains the text 'Traffic Shaper Wizards'. Below this, there are two entries: 'Multiple Lan/Wan' with a link to 'traffic\_shaper\_wizard\_multi\_all.xml' and 'Dedicated Links' with a link to 'traffic\_shaper\_wizard\_dedicated.xml'.

**Traffic shaper Wizard**

Enter number of WAN type connections   
Number of WAN-type connections (Gateway selected on their interface settings, or dynamic assignment.)

Enter number of LAN type interfaces   
Number of local connections (No gateway selected on their interface settings.)

[» Next](#)

Detailed description: This is the 'Traffic shaper Wizard' configuration page. It has a dark header with the title 'Traffic shaper Wizard'. There are two input fields: 'Enter number of WAN type connections' with the value '1' and 'Enter number of LAN type interfaces' with the value '2'. Below each input field is a descriptive text: 'Number of WAN-type connections (Gateway selected on their interface settings, or dynamic assignment.)' and 'Number of local connections (No gateway selected on their interface settings.)'. At the bottom, there is a blue button with a right-pointing arrow and the text 'Next'.

**Setup connection speed and scheduler information for interface LAN #1**

Interface & Scheduler

Interface & Scheduler

Detailed description: This screenshot shows the configuration for 'Setup connection speed and scheduler information for interface LAN #1'. The header is dark with white text. There are two dropdown menus. The first is labeled 'Interface & Scheduler' and has 'LAN' selected. The second is also labeled 'Interface & Scheduler' and has 'PRIQ' selected.

Setup connection speed and scheduler information for interface WAN#1	
Interface & Scheduler	WAN
Interface & Scheduler	PRIQ
Upload	50
Upload	Mbit/s
Download	100
Download	Mbit/s

Step 2 of 8

### Voice over IP

Voice over IP

**enable**  Prioritize Voice over IP traffic.

### VOIP specific settings

**Provider** Generic (lowdelay)   
Choose Generic if the provider isn't listed.

**Upstream SIP Server**   
(Optional) If this is chosen, the provider field will be overridden. This allows providing the IP address of the remote PBX or SIP Trunk to prioritize. NOTE: A Firewall Alias can also be used in this location.

### Connection WAN #1

**Upload** 15

**Units** Mbit/s

### Connection LAN #1

**Download** 15

**Units** Mbit/s

### Connection LAN #2

**Download** 15

**Units** Mbit/s

[» Next](#)

### Penalty Box

#### Penalty Box

**Enable**  Penalize IP or Alias  
This will lower the priority of traffic from this IP or alias.

### PenaltyBox specific settings

**Address**   
This allows just providing the IP address of the computer(s) to penalize. NOTE: A Firewall Alias can also be used in this location.

**Bandwidth**

**Bandwidth**   
The desired limit to apply.

» Next

### Peer to Peer networking

#### Peer to Peer networking

**Enable**  Lower priority of Peer-to-Peer traffic  
This will lower the priority of P2P traffic below all other traffic. Please check the items to prioritize lower than normal traffic.

### p2p Catch all

**p2pCatchAll**  When enabled, all uncategorized traffic is fed to the p2p queue.

**Bandwidth**

**Bandwidth**   
The desired limit to apply.

### Enable/Disable specific P2P protocols

**Aimster**  Aimster and other P2P using the Aimster protocol and ports

**BitTorrent**  Bittorrent and other P2P using the Torrent protocol and ports

Wizard / pfSense Traffic Shaper / Reload Profile ?

---

Step 7 of 8

### Reload Profile

After pressing Finish the system will load the new profile.  
 Please note that this may take a moment.  
 Also note that the traffic shaper is stateful meaning that only new connections will be shaped.  
 If this is an issue please reset the state table after loading the profile.

[» Finish](#)

Status / Filter Reload ☰ 📊 📄 ?

### Filter Reload

[↻ Reload Filter](#)

Queue Status

#### Reload status

```

Initializing
Creating aliases
Creating gateway group item...
Generating Limiter rules
Generating NAT rules
Creating 1:1 rules...
  
```

<input type="checkbox"/>		0 / 869 B	IPv4 UDP	*	*	*	*	*	qVoIP	DiffServ/Lowdelay/Upload	
<input type="checkbox"/>		0 / 0 B	IPv4 TCP	*	*	*	6881 - 6999	*	qP2P	m_P2P BitTorrent outbound	
<input type="checkbox"/>		0 / 0 B	IPv4 UDP	*	*	*	6881 - 6999	*	qP2P	m_P2P BitTorrent outbound	

Firewall / Rules / Floating / Edit

### Edit Firewall Rule

**Action** 
  
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 UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

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

**Quick**  Apply the action immediately on match.
  
Set this option to apply this action to traffic that matches this rule immediately.

**Interface** 
  
LAN
  
DMZ
  
L2TP VPN
  
Choose the interface(s) for this rule.

**Direction**

**Address Family** 
  
Select the Internet Protocol version this rule applies to.

**Protocol** 
  
Choose which IP protocol this rule should match.

### Destination

**Destination**  Invert match.  Destination Address

**Destination Port Range**    
  
From Custom To Custom
  
Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.

### Extra Options

**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 doing a lot of logging, consider using a remote syslog server (see the Status: System Logs: Settings page).

**Description** 
  
A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.

**Advanced Options**

[snort](#) 3.2.9.8.4 Snort is an open source network intrusion prevention and detection system (IDS/IPS). Combining the benefits of signature, protocol, and anomaly-based inspection.

**Package Dependencies:**

- [snort-2.9.12](#)
- [barnyard2-1.13\\_1](#)

**snort** 3.2.9.8.4 Snort is an open source network intrusion prevention and detection system (IDS/IPS). Combining the benefits of signature, protocol, and anomaly-based inspection. + Install

Package Dependencies:  
[snort-2.9.12](#) [barnyard2-1.13\\_1](#)

Services / Snort / **Global Settings** ?

[Snort Interfaces](#)
[Global Settings](#)
[Updates](#)
[Alerts](#)
[Blocked](#)
[Pass Lists](#)
[Suppress](#)
[IP Lists](#)
[SID Mgmt](#)
[Log Mgmt](#)
[Sync](#)

---

**Snort Subscriber Rules**

**Enable Snort VRT**  Click to enable download of Snort free Registered User or paid Subscriber rules

[Sign Up for a free Registered User Rules Account](#)  
[Sign Up for paid Snort Subscriber Rule Set \(by Talos\)](#)

**Snort Oinkmaster Code**

Obtain a snort.org Oinkmaster code and paste it here. (Paste the code only and not the URL!)

---

**Snort GPLv2 Community Rules**

**Enable Snort GPLv2**  Click to enable download of Snort GPLv2 Community rules

The Snort Community Ruleset is a GPLv2 Talos certified ruleset that is distributed free of charge without any Snort Subscriber License restrictions. This ruleset is updated daily and is a subset of the subscriber ruleset.

---

**Emerging Threats (ET) Rules**

**Enable ET Open**  Click to enable download of Emerging Threats Open rules

ETOpen is an open source set of Snort rules whose coverage is more limited than ETPro.

**Enable ET Pro**  Click to enable download of Emerging Threats Pro rules

[Sign Up for an ETPro Account](#)  
 ETPro for Snort offers daily updates and extensive coverage of current malware threats.

**Rules Update Settings**

**Update Interval**  Please select the interval for rule updates. Choosing NEVER disables auto-updates.

**Update Start Time**

Enter the rule update start time in 24-hour format (HH:MM). Default is 00:05. Rules will update at the interval chosen above starting at the time specified here. For example, using the default start time of 00:05 and choosing 12 Hours for the interval, the rules will update at 00:05 and 12:05 each day.

**Hide Deprecated Rules Categories**  Click to hide deprecated rules categories in the GUI and remove them from the configuration. Default is not checked.

**Disable SSL Peer Verification**  Click to disable verification of SSL peers during rules updates. This is commonly needed only for self-signed certificates. Default is not checked.



- Snort Interfaces
- Global Settings
- Updates
- Alerts
- Blocked
- Pass Lists
- Suppress
- IP Lists
- SID Mgmt
- Log Mgmt
- Sync

**Installed Rule Set MD5 Signature**

Rule Set Name/Publisher	MD5 Signature Hash	MD5 Signature Date
Snort Subscriber Ruleset	4721db885042640bc27de8b848584887	Sunday, 11-Nov-18 06:09:28 UTC
Snort GPLv2 Community Rules	fcc21191755c1ae641fcd8c98bf54813	Sunday, 11-Nov-18 06:09:28 UTC
Emerging Threats Open Rules	7f1fd01ad05e0ebcc2deabe9404fb1ca	Sunday, 11-Nov-18 12:42:16 UTC
Snort OpenAppID Detectors	Not Enabled	Not Enabled
Snort OpenAppID RULES Detectors	Not Enabled	Not Enabled

**Update Your Rule Set**

Last Update Nov-11 2018 12:42

Result: Success

Update Rules [Update Rules](#)

[Force Update](#)

Click UPDATE RULES to check for and automatically apply any new posted updates for selected rules packages. Clicking FORCE UPDATE will zero out the MD5 hashes and force the download and application of the latest versions of the enabled rules packages.

**General Settings**

**Enable**  Enable interface

**Interface**

Choose the interface where this Snort instance will inspect traffic.

**Description**

Enter a meaningful description here for your reference.

**Snap Length**

Enter the desired interface snaplen value in bytes. Default is 1518 and is suitable for most applications.



---



### Alert Settings

<b>Send Alerts to System Log</b>	<input type="checkbox"/> Snort will send Alerts to the firewall's system log. Default is Not Checked.
<b>Block Offenders</b>	<input checked="" type="checkbox"/> Checking this option will automatically block hosts that generate a Snort alert
<b>Kill States</b>	<input checked="" type="checkbox"/> Checking this option will kill firewall states for the blocked IP. Default is checked.
<b>Which IP to Block</b>	<div style="border: 1px solid #ccc; padding: 2px; display: inline-block;">BOTH</div> Select which IP extracted from the packet you wish to block. Default is BOTH.

<input type="checkbox"/> <a href="#">emerging-netbios.rules</a>	<input type="checkbox"/> <a href="#">snort_file-image.rules</a>	<input type="checkbox"/> <a href="#">snort_protocol-snmp.so.rules</a>
<input checked="" type="checkbox"/> <a href="#">emerging-p2p.rules</a>	<input type="checkbox"/> <a href="#">snort_file-java.rules</a>	<input type="checkbox"/> <a href="#">snort_protocol-tftp.so.rules</a>
<input type="checkbox"/> <a href="#">emerging-policy.rules</a>	<input type="checkbox"/> <a href="#">snort_file-multimedia.rules</a>	<input type="checkbox"/> <a href="#">snort_protocol-voip.so.rules</a>


# Chapter 7: Redundancy, Load Balancing, and Failover

### DNS Server Settings

<b>DNS Servers</b>	<input type="text" value="1.1.1.1"/>	<input type="text" value="WAN_DHCP - wan - 10.0.3.254"/>	 Delete
	<input type="text" value="1.0.0.1"/>	<input type="text" value="OPT_WAN_DHCP - opt2 - 10.0.4.2"/>	 Delete




**Address**  
Enter IP addresses to be used by the system for DNS resolution. These are also used for the DHCP service, DNS Forwarder and DNS Resolver when it has DNS Query Forwarding enabled.

**Gateway**  
Optionally select the gateway for each DNS server. When using multiple WAN connections there should be at least one unique DNS server per gateway.

**Add DNS Server**  Add DNS Server

**Monitor IP**

Enter an alternative address here to be used to monitor the link. This is used for the quality RRD graphs as well as the load balancer entries. Use this if the gateway does not respond to ICMP echo requests (pings).

System / Routing / Gateway Groups / Edit   


### Edit Gateway Group Entry

**Group Name**

**Gateway Priority**

<input type="text" value="OPT_WAN_DHCP"/>	<input type="text" value="Tier 1"/>	<input type="text" value="Interface Address"/>	<input type="text" value="Interface OPT_WAN_DHCP Gateway"/>
<input type="text" value="WAN_DHCP"/>	<input type="text" value="Tier 1"/>	<input type="text" value="Interface Address"/>	<input type="text" value="Interface WAN_DHCP Gateway"/>

Gateway	Tier	Virtual IP	Description
<b>Link Priority</b>	The priority selected here defines in what order failover and balancing of links will be done. Multiple links of the same priority will balance connections until all links in the priority will be exhausted. If all links in a priority level are exhausted then the next available link(s) in the next priority level will be used.		
<b>Virtual IP</b>	The virtual IP field selects which (virtual) IP should be used when this group applies to a local Dynamic DNS, IPsec or OpenVPN endpoint.		
<b>Trigger Level</b>	<input type="text" value="Member Down"/> When to trigger exclusion of a member		
<b>Description</b>	<input type="text" value="Load balancing multi-WAN group"/> A description may be entered here for administrative reference (not parsed).		

 Save

Gateway Groups				
Group Name	Gateways	Priority	Description	Actions
MULTIWAN	OPT_WAN_DHCP WAN_DHCP	Tier 1 Tier 1	Load balancing multi-WAN group	
Add				

Firewall / Rules / Floating / 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 UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

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

**Quick**  Apply the action immediately on match.  
 Set this option to apply this action to traffic that matches this rule immediately.

**Interface** 
 WAN  
LAN  
 PFSYNC  
 OPT\_WAN
   
 Choose the interface(s) for this rule.

**Direction** in

**Address Family** IPv4  
 Select the Internet Protocol version this rule applies to.

**Protocol** Any  
 Choose which IP protocol this rule should match.

**Gateway** MULTIWAN - Load balancing multi-WAN group

Leave as 'default' to use the system routing table. Or choose a gateway to utilize policy based routing.  
 Gateway selection is not valid for "IPV4+IPV6" address family.

Gateways    Gateway Groups

Gateways							
Name	Gateway	Monitor	RTT	RTTsd	Loss	Status	Description
OPT_WAN_DHCP	10.0.4.2	1.0.0.1	16.777ms	9.293ms	0.0%	Online	Interface OPT_WAN_DHCP Gateway
WAN_DHCP	10.0.3.254	10.0.3.254	0.771ms	0.7ms	0.0%	Online	Interface WAN_DHCP Gateway
WAN_DHCP6			Pending	Pending	Pending	Pending	Interface WAN_DHCP6 Gateway

Gateways **Gateway Groups**

Gateway Groups		
Group Name	Gateways	Description
MULTIWAN	<b>Tier 1</b> OPT_WAN_DHCP Online WAN_DHCP Online	Load balancing multi-WAN group

Firewall / Aliases / Edit ?

**Properties**

**Name**   
The name of the alias may only consist of the characters 'a-z, A-Z, 0-9 and \_'.

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

**Type**

**Port(s)**

**Hint** Enter ports as desired, with a single port or port range per entry. Port ranges can be expressed by separating with a colon.

<b>Port</b> <input type="text" value="80"/>	<input type="text" value="HTTP"/>	<input type="button" value="Delete"/>
<input type="text" value="443"/>	<input type="text" value="HTTPS"/>	<input type="button" value="Delete"/>

Firewall / Aliases / Edit ?

---

**Properties**

**Name**   
The name of the alias may only consist of the characters "a-z, A-Z, 0-9 and \_".

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

**Type**

---

**Host(s)**

**Hint** Enter as many hosts as desired. Hosts must be specified by their IP address or fully qualified domain name (FQDN). FQDN hostnames are periodically re-resolved and updated. If multiple IPs are returned by a DNS query, all are used. An IP range such as 192.168.1.1-192.168.1.10 or a small subnet such as 192.168.1.16/28 may also be entered and a list of individual IP addresses will be generated.

IP or FQDN		
<input type="text" value="192.168.2.11"/>	<input type="text" value="WEB SERVER 1"/>	<input type="button" value="Delete"/>
<input type="text" value="192.168.2.12"/>	<input type="text" value="WEB SERVER 2"/>	<input type="button" value="Delete"/>
<input type="text" value="192.168.2.13"/>	<input type="text" value="WEB SERVER 3"/>	<input type="button" value="Delete"/>

### Add/Edit Load Balancer - Pool Entry

**Name**

**Mode**

**Description**

**Port**   
This is the port the servers are listening on. A port alias listed in Firewall -> Aliases may also be specified here.

**Retry**   
Optionally specify how many times to retry checking a server before declaring it down.

---

### Add Item to the Pool

**Monitor**

**Server IP Address**  + Add to pool

---

### Current Pool Members

<p><b>Members</b></p> <div style="border: 1px solid #ccc; height: 40px; width: 100%;"></div> <p>Disabled</p> <div style="text-align: center; margin-top: 5px;"> <span style="background-color: #dc3545; color: white; padding: 2px 5px; border-radius: 3px;">🗑 Remove</span> </div> <div style="text-align: center; margin-top: 5px;"> <span style="background-color: #17a2b8; color: white; padding: 2px 5px; border-radius: 3px;">» Move to enabled list</span> </div>	<div style="border: 1px solid #ccc; height: 40px; width: 100%;"></div> <p>Enabled (Default)</p> <div style="text-align: center; margin-top: 5px;"> <span style="background-color: #dc3545; color: white; padding: 2px 5px; border-radius: 3px;">🗑 Remove</span> </div> <div style="text-align: center; margin-top: 5px;"> <span style="background-color: #17a2b8; color: white; padding: 2px 5px; border-radius: 3px;">« Move to disabled list</span> </div>
--	--

💾 Save

[Pools](#)   [Virtual Servers](#)   [Monitors](#)   [Settings](#)

---

Pool						
Name	Mode	Servers	Port	Monitor	Description	Actions
WEB_SERVER_POOL	loadbalance	192.168.2.11 192.168.2.12 192.168.2.13	WEB_SERVER_PORTS	ICMP	Web server pool	<span style="color: #007bff;">✎</span> <span style="color: #007bff;">🗑</span> <span style="color: #007bff;">📄</span>

+ Add

Services / Load Balancer / Virtual Servers / Edit ⌵ ⌶ ⌷ ⌸ ?

### Edit Load Balancer - Virtual Server Entry

<b>Name</b>	<input type="text" value="WEB_SERVER"/>
<b>Description</b>	<input type="text" value="IP for web server pool"/>
<b>IP Address</b>	<input type="text" value="10.0.3.18"/> <small>This is normally the WAN IP address for the server to listen on. All connections to this IP and port will be forwarded to the pool cluster. A host alias listed in Firewall -&gt; Aliases may also be specified here.</small>
<b>Port</b>	<input type="text" value="80"/> <input type="button" value="↕"/> <small>Port that the clients will connect to. All connections to this port will be forwarded to the pool cluster. If left blank listening ports from the pool will be used. A port alias listed in Firewall -&gt; Aliases may also be specified here.</small>
<b>Virtual Server Pool</b>	<input type="text" value="WEB_SERVER_POOL"/> ⌵
<b>Fall-back Pool</b>	<input type="text" value="None"/> ⌵
<b>Relay Protocol</b>	<input type="text" value="TCP"/> ⌵

Services / Load Balancer / Monitors / Edit ↻ ⌵ ⌶ ⌷ ⌸ ?

### Edit Load Balancer - Monitor Entry

<b>Name</b>	<input type="text" value="WEB_SERVER_HTTP"/>
<b>Description</b>	<input type="text" value="HTTP monitor for web server"/>
<b>Type</b>	<input type="text" value="HTTP"/> ⌵

### HTTP Options

<b>Path</b>	<input type="text" value="/index.html"/>
<b>Host</b>	<input type="text"/> <small>Hostname for Host: header if needed.</small>
<b>HTTP Code</b>	<input type="text" value="200 OK"/> ⌵

### 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 UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

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

**Interface** WAN  
 Choose the interface from which packets must come to match this rule.

**Address Family** IPv4  
 Select the Internet Protocol version this rule applies to.

**Protocol** TCP  
 Choose which IP protocol this rule should match.

---

**Source**

**Source**  Invert match. any Source Address /

[Display Advanced](#)

The **Source Port Range** for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, **any**.

---

**Destination**

**Destination**  Invert match. Single host or alias WEB\_SERVER\_IPS /

**Destination Port Range** (other)  (other)   
 From Custom To Custom

Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.

Floating **WAN** LAN PFSYNC OPT\_WAN

#### Rules (Drag to Change Order)

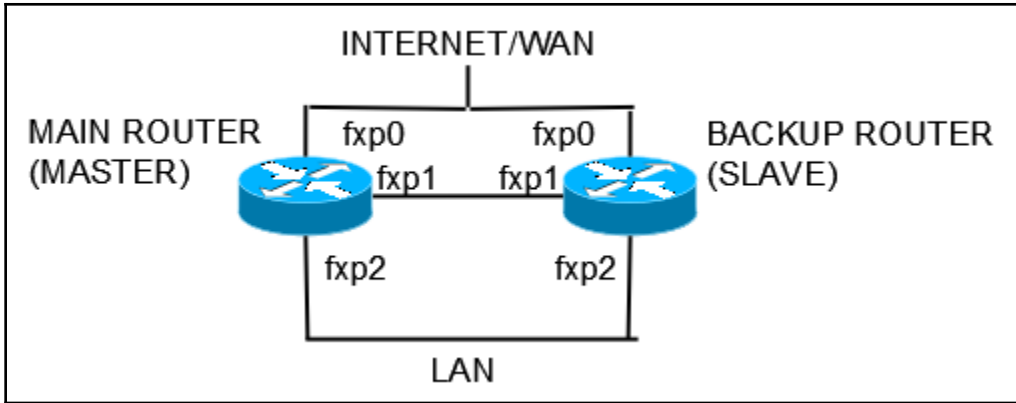
States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✘	0/430 KiB	*	RFC 1918 networks	* *	*	*	*		Block private networks	⚙️
✘	0/656 B	*	Reserved Not assigned by IANA	* *					Block bogon networks	⚙️
<input type="checkbox"/>	✔️	0/0 B	IPv4 TCP	*	*	WEB_SERVER_IPS			Allow web server traffic	📌 🛠️ 🗑️ 📄

Alias details

Value	Description
192.168.2.11	WEB SERVER 1
192.168.2.12	WEB SERVER 2
192.168.2.13	WEB SERVER 3

Add ⬇️ Add 🗑️ Delete 📄 Save ➕ Separator





Firewall / Virtual IPs / Edit

### Edit Virtual IP

Type:  IP Alias  CARP  Proxy ARP  Other

Interface: WAN

Address type: Single address

Address(es): 10.0.3.240 / 8

Virtual IP Password: [Masked] Confirm: [Masked]

VHID Group: 1

Advertising frequency: Base: 1 Skew: 0

Description: WAN virtual IP for CARP

[ Save ]

Virtual IP address	Interface	Type	Description	Actions
172.16.1.240/16 (vhid: 2)	LAN	CARP	LAN virtual IP for CARP	[Edit] [Delete]
10.0.3.240/8 (vhid: 1)	WAN	CARP	WAN virtual IP for CARP	[Edit] [Delete]

[ + Add ]

**General Configuration**

**Enable**  Enable interface

**Description**

Enter a description (name) for the interface here.

**IPv4 Configuration Type**

**IPv6 Configuration Type**

**MAC Address**

This field can be used to modify ("spoof") the MAC address of this interface.  
Enter a MAC address in the following format: xxxxxxxx:xxxx:xx or leave blank.

**MTU**

If this field is blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary in some circumstances.

**MSS**

If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 (TCP/IP header size) will be in effect.

**Speed and Duplex**

Explicitly set speed and duplex mode for this interface.  
WARNING: MUST be set to autoselect (automatically negotiate speed) unless the port this interface connects to has its speed and duplex forced.

**Static IPv4 Configuration**

**IPv4 Address**  /

**IPv4 Upstream gateway**  [+ Add a new gateway](#)

**State Synchronization Settings (pfsync)**

**Synchronize states**  pfsync transfers state insertion, update, and deletion messages between firewalls.

Each firewall sends these messages out via multicast on a specified interface, using the PFSYNC protocol (IP Protocol 240). It also listens on that interface for similar messages from other firewalls, and imports them into the local state table. This setting should be enabled on all members of a failover group. Clicking "Save" will force a configuration sync if it is enabled! (see Configuration Synchronization Settings below)

**Synchronize Interface**

If Synchronize States is enabled this interface will be used for communication. It is recommended to set this to an interface other than LAN! A dedicated interface works the best. An IP must be defined on each machine participating in this failover group. An IP must be assigned to the interface on any participating sync nodes.

**pfsync Synchronize Peer IP**

Setting this option will force pfsync to synchronize its state table to this IP address. The default is directed multicast.

**Configuration Synchronization Settings (XMLRPC Sync)**

**Synchronize Config to IP**

Enter the IP address of the firewall to which the selected configuration sections should be synchronized.

XMLRPC sync is currently only supported over connections using the same protocol and port as this system - make sure the remote system's port and protocol are set accordingly!  
Do not use the Synchronize Config to IP and password option on backup cluster members!

**Remote System Username**

Enter the webConfigurator username of the system entered above for synchronizing the configuration. Do not use the Synchronize Config to IP and username option on backup cluster members!

**Remote System Password**

Enter the webConfigurator password of the system entered above for synchronizing the configuration. Do not use the Synchronize Config to IP and password option on backup cluster members!

Confirm

**Select options to sync**

- User manager users and groups
- Authentication servers (e.g. LDAP, RADIUS)
- Certificate Authorities, Certificates, and Certificate Revocation Lists
- Firewall rules
- Firewall schedules
- Firewall aliases
- NAT configuration
- IPsec configuration
- OpenVPN configuration
- DHCP Server settings
- WoL Server settings
- Static Route configuration
- Load Balancer configuration
- Virtual IPs
- Traffic Shaper configuration
- Traffic Shaper Limiters configuration
- DNS Forwarder and DNS Resolver configurations
- Captive Portal

Toggle All

**Translation**

**Address**

Connections matching this rule will be mapped to the specified **Address**.  
The **Address** can be an Interface, a Host-type Alias, or a **Virtual IP** address.

**Port or Range**   Static Port

Enter the external source **Port or Range** used for remapping the original source port on connections matching the rule.

Port ranges are a low port and high port number separated by ":".  
Leave blank when **Static Port** is checked.

**Other Options**

**Gateway**   
 The default is to use the IP on this interface of the firewall as the gateway. Specify an alternate gateway here if this is not the correct gateway for the network. Type "none" for no gateway assignment.

**Domain name**   
 The default is to use the domain name of this system as the default domain name provided by DHCP. An alternate domain name may be specified here.

**Domain search list**   
 The DHCP server can optionally provide a domain search list. Use the semicolon character as separator.

**Default lease time**    
 This is used for clients that do not ask for a specific expiration time. The default is 7200 seconds.

**Maximum lease time**    
 This is the maximum lease time for clients that ask for a specific expiration time. The default is 86400 seconds.

**Failover peer IP**   
 Leave blank to disable. Enter the interface IP address of the other machine. Machines must be using CARP. Interface's advskew determines whether the DHCPd process is Primary or Secondary. Ensure one machine's advskew < 20 (and the other is > 20).

**Rules (Drag to Change Order)**

<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓	0/0/B	IPv4*	*	*	*	*	none		PFSYNC rule to be overwritten	

**Status / CARP**

**CARP Interfaces**

CARP Interface	Virtual IP	Status
LAN@2	172.16.1.240/16	▶ MASTER
WAN@1	10.0.3.240/8	▶ MASTER

**pfSync Nodes**

pfSync nodes:

```

0b82a8ec
1c34b355
20c0c376
789490e9
9ca10926
b48b58ca
e9857c7e
  
```

# Chapter 8: Routing and Bridging

Interfaces / Bridges / Edit

### Bridge Configuration

**Member Interfaces**

- WAN
- LAN
- PFSYNC
- DMZ

Interfaces participating in the bridge.

**Description**

LAN-DMZ bridge

**Advanced Options**

Hide Advanced

### Advanced Configuration

**Cache Size**

Set the size of the bridge address cache. The default is 2000 entries.

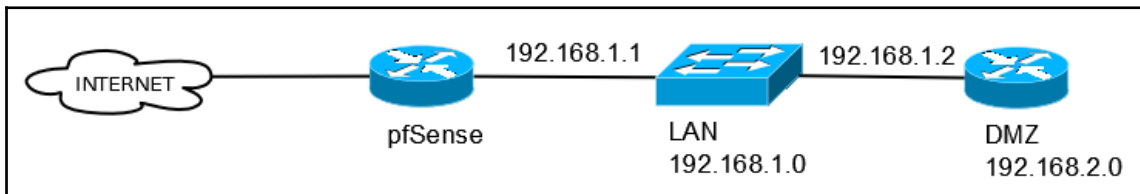
**Cache expire time**

Set the timeout of address cache entries to this number of seconds. If seconds is zero, then address cache entries will not be expired. The default is 1200 seconds.

**Span Port**

- WAN
- LAN
- PFSYNC
- DMZ

Add the interface named by interface as a span port on the bridge. Span ports transmit a copy of every frame received by the bridge. This is most useful for snooping a bridged network passively on another host connected to one of the span ports of the bridge. The span interface cannot be part of the bridge member interfaces.



### Edit Gateway

**Disabled**  **Disable this gateway**  
Set this option to disable this gateway without removing it from the list.

**Interface**   
Choose which interface this gateway applies to.

**Address Family**   
Choose the Internet Protocol this gateway uses.

**Name**   
Gateway name

**Gateway**   
Gateway IP address

**Gateway Monitoring**  **Disable Gateway Monitoring**  
This will consider this gateway as always being up.

**Gateway Action**  **Disable Gateway Monitoring Action**  
No action will be taken on gateway events. The gateway is always considered up.

**Monitor IP**   
Enter an alternative address here to be used to monitor the link. This is used for the quality RRD graphs as well as the load balancer entries. Use this if the gateway does not respond to ICMP echo requests (pings).

**Force state**  **Mark Gateway as Down**  
This will force this gateway to be considered down.

**Description**   
A description may be entered here for reference (not parsed).

[⚙️ Display Advanced](#)

System / Routing / Static Routes / Edit
🏠 📊 📧 ?

### Edit Route Entry

**Destination network**  /   
Destination network for this static route

**Gateway**   
Choose which gateway this route applies to or [add a new one first](#)

**Disabled**  **Disable this static route**  
Set this option to disable this static route without removing it from the list.

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

[💾 Save](#)



ROUTED Settings

General Options

**Enable RIP**  Enables the Routing Information Protocol daemon.

**Interfaces**

LAN  
PFSYNC  
DMZ  
WAN

Select the interfaces that RIP will bind to. You can use the CTRL or COMMAND key to select multiple interfaces.

**RIP Version** RIP Version 2

**RIPv2 password** delpennew

Specify a RIPv2 password. This password will be sent in the clear on all RIPv2 responses received and sent.

**no\_ag**  Turns off aggregation of subnets in RIPv1 and RIPv2 responses.

**no\_super\_ag**  Turns off aggregation of networks into supernets in RIPv2 responses.

Save



General Options

**Enable**    Enable OSPF Routing

**Log Adjacency Changes**    If set to yes, adjacency changes will be written via syslog.

**Router ID**     
Specify the Router ID. RID is the highest logical (loopback) IP address configured on a router.  
For more information on router identifiers see [wikipedia](#).

**Area**     
OSPFd area for this instance of OSPF.  
For more information on Areas see [wikipedia](#).

**Disable FIB updates (Routing table)**     
Disables the updating of the host routing table (turns into stub router).

**Redistribute**    Redistribute connected networks    Redistribute Kernel routing table (pfSense static routes)

Redistribute BGP Routes to OSPF Neighbors    Redistribute a default route to this device    Redistribute FRR static routes

**SPF Hold Time**     
Set the SPF holdtime in milliseconds. The minimum time between two consecutive shortest path first calculations.  
The default value is 5 seconds; the valid range is 1-5 seconds.

**SPF Delay**     
Set SPF delay in milliseconds. The delay between receiving an update to the link state database and starting the shortest path first calculation.  
The default value is 1; valid range is 1-10 seconds.

---

# Chapter 9: Services and Maintenance

### Wake-on-LAN

**Interface**

Choose which interface the host to be woken up is connected to.

**MAC address**

Enter a MAC address in the following format: xx:xx:xx:xx:xx:xx

Send

### Edit WOL Entry

**Interface**

Choose which interface this host is connected to.

**MAC address**

Enter a MAC address in the following format: xx:xx:xx:xx:xx:xx

**Description**

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

Save

### Wake-on-LAN Devices

Click the MAC address to wake up an individual device.

Interface	MAC address	Description	Actions
LAN	<a href="#">08:00:27:94:0b:83</a>	Old Lenovo for Bitcoin mining	

Add Wake All Devices

Services / PPPoE Server 🔍 ?

PPPoE Server				
Interface	Local IP	Number of users	Description	Actions
<span style="background-color: #28a745; color: white; padding: 2px 5px; border-radius: 3px;">+ Add</span>				

Services / PPPoE Server / Edit ☰ 📄 ?

### PPPoE Server Configuration

**Enable**  Enable PPPoE Server

**Interface**

**Total User Count**   
The number of PPPoE users allowed to connect to this server simultaneously.

**User Max Logins**   
The number of times a single user may be logged in at the same time.

**Server Address**   
Enter the IP address the PPPoE server should give to clients for use as their "gateway". Typically this is set to an unused IP just outside of the client range.  
NOTE: This should NOT be set to any IP address currently in use on this firewall.

**Remote Address Range**   
Specify the starting address for the client IP address subnet.

**Subnet mask**   
Hint: 24 is 255.255.255.0

**Description**

**DNS Servers**   
  
If entered these servers will be given to all PPPoE clients, otherwise LAN DNS and one WAN DNS will go to all clients.

**RADIUS**  Use RADIUS Authentication  
Users will be authenticated using the RADIUS server specified below. The local user database will not be used.

User table	admin	●●●●●●●●●●	172.16.1.102	Delete
	chris	●●●●●●●●	172.16.1.110	Delete
	Username	Password	IP Address	
<input type="button" value="+ Add user"/>				

### Remote Logging Options

**Enable Remote Logging**  Send log messages to remote syslog server

**Source Address**  This option will allow the logging daemon to bind to a single IP address, rather than all IP addresses. If a single IP is picked, remote syslog servers must all be of that IP type. To mix IPv4 and IPv6 remote syslog servers, bind to all interfaces.  
NOTE: If an IP address cannot be located on the chosen interface, the daemon will bind to all addresses.

**IP Protocol**  This option is only used when a non-default address is chosen as the source above. This option only expresses a preference; if an IP address of the selected type is not found on the chosen interface, the other type will be tried.

**Remote log servers**

**Remote Syslog Contents**

- Everything
- System Events
- Firewall Events
- DNS Events (Resolver/unbound, Forwarder/dnsmasq, filterdns)
- DHCP Events (DHCP Daemon, DHCP Relay, DHCP Client)
- PPP Events (PPPoE WAN Client, L2TP WAN Client, PPTP WAN Client)
- Captive Portal Events
- VPN Events (IPsec, OpenVPN, L2TP, PPPoE Server)
- Gateway Monitor Events
- Routing Daemon Events (RADVD, UPnP, RIP, OSPF, BGP)
- Server Load Balancer Events (relayd)
- Network Time Protocol Events (NTP Daemon, NTP Client)
- Wireless Events (hostapd)

Syslog sends UDP datagrams to port 514 on the specified remote syslog server, unless another port is specified. Be sure to set syslogd on the remote server to accept syslog messages from pfSense.



### Ping

**Hostname**

google.com

**IP Protocol**

IPv4

**Source address**

Automatically selected (default)

Select source address for the ping.

**Maximum number of pings**

3

Select the maximum number of pings.



### Results

```
PING google.com (172.217.9.238): 56 data bytes
64 bytes from 172.217.9.238: icmp_seq=0 ttl=52 time=34.301 ms
64 bytes from 172.217.9.238: icmp_seq=1 ttl=52 time=16.211 ms
64 bytes from 172.217.9.238: icmp_seq=2 ttl=52 time=16.277 ms

--- google.com ping statistics ---
3 packets transmitted, 3 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 16.211/22.263/34.301/8.512 ms
```

**Traceroute**

**Hostname**


**IP Protocol**   
Select the protocol to use.

**Source Address**   
Select source address for the trace.

**Maximum number of hops**   
Select the maximum number of network hops to trace.

**Reverse Address Lookup**   
When checked, traceroute will attempt to perform a PTR lookup to locate hostnames for hops along the path. This will slow down the process as it has to wait for DNS replies.

**Use ICMP**   
By default, traceroute uses UDP but that may be blocked by some routers. Check this box to use ICMP instead, which may succeed.



**Results**

1	10.0.3.254	0.562 ms	0.423 ms	0.256 ms
2	10.0.2.2	0.696 ms	0.665 ms	0.650 ms
3	192.168.2.1	1.654 ms	1.589 ms	2.157 ms
4	10.240.163.109	10.614 ms	9.896 ms	9.338 ms
5	67.59.242.66	14.477 ms	10.564 ms	10.221 ms
6	67.83.248.146	13.399 ms	14.763 ms	13.144 ms
7	67.59.239.235	21.236 ms	16.151 ms	14.660 ms
8	64.15.3.250	15.000 ms	16.222 ms	15.283 ms
9	* 4.35.80.5	16.646 ms	15.210 ms	
10	* * 4.69.150.206	21.985 ms		
11	64.125.13.29	25.790 ms	23.843 ms	16.512 ms
12	64.125.27.196	27.209 ms	23.200 ms	25.348 ms
13	64.125.29.31	25.487 ms	25.791 ms	31.508 ms
14	64.125.30.249	23.098 ms	23.110 ms	23.083 ms
15	64.125.29.123	22.862 ms	22.781 ms	22.277 ms
16	64.125.192.142	22.797 ms	23.880 ms	21.847 ms
17	208.80.154.224	21.663 ms	20.242 ms	21.867 ms

## Diagnostics / Command Prompt



### Shell Output - netstat -a

Active Internet connections (including servers)

Proto	Recv-Q	Send-Q	Local Address	Foreign Address	(state)
tcp4	0	0	pfSense.https	172.16.1.102.48426	ESTABLISHED
tcp4	0	0	pfSense.utime	172.16.1.2.50256	ESTABLISHED
tcp4	0	0	pfSense.utime	*.*	LISTEN
tcp6	0	0	*.http	*.*	LISTEN
tcp4	0	0	*.http	*.*	LISTEN
tcp6	0	0	*.https	*.*	LISTEN
tcp4	0	0	*.https	*.*	LISTEN
tcp4	0	0	localhost.rndc	*.*	LISTEN
tcp4	0	0	*.domain	*.*	LISTEN
tcp6	0	0	*.domain	*.*	LISTEN

## Diagnostics / pfTop



### pfTop Configuration

View

Filter expression

[click for filter help](#)

Sort by

Maximum # of States

### Output

pfTop: Up State 1-3/3 (28), View: default, Order: bytes

PR	DIR	SRC	DEST	STATE	AGE	EXP	PKTS	BYTES
tcp	In	172.16.1.102:48408	172.16.1.1:443	ESTABLISHED:ESTABLISHED	00:04:25	24:00:00	1756	1848456
tcp	In	172.16.1.2:50256	172.16.1.1:519	ESTABLISHED:ESTABLISHED	01:37:13	23:59:59	7761	450772
tcp	Out	172.16.1.2:50256	172.16.1.1:519	ESTABLISHED:ESTABLISHED	01:37:13	23:59:59	0	0

Diagnostics / Command Prompt ?

Shell Output - tcpdump -c 10

```

tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on em0, link-type EN10MB (Ethernet), capture size 262144 bytes
16:25:00.966519 IP 10.0.3.18 > 10.0.3.254: ICMP echo request, id 61873, seq 35232, length 8
16:25:00.967259 IP 10.0.3.254 > 10.0.3.18: ICMP echo reply, id 61873, seq 35232, length 8
16:25:00.985021 IP 10.0.3.18 > vrrp.mcast.net: VRRPv2, Advertisement, vrid 1, prio 240, authtype none, intvl 1s, length 36
16:25:01.486536 IP 10.0.3.18 > 192.168.2.11: ICMP echo request, id 14312, seq 1, length 64
16:25:01.486749 IP 10.0.3.18 > 192.168.2.12: ICMP echo request, id 14312, seq 2, length 64
16:25:01.487066 IP 10.0.3.18 > 192.168.2.13: ICMP echo request, id 14312, seq 3, length 64
16:25:01.487425 IP 10.0.3.18 > 192.168.2.11: ICMP echo request, id 14312, seq 4, length 64
16:25:01.487474 IP 10.0.3.18 > 192.168.2.12: ICMP echo request, id 14312, seq 5, length 64
16:25:01.487539 IP 10.0.3.18 > 192.168.2.13: ICMP echo request, id 14312, seq 6, length 64
16:25:01.488025 IP 10.0.3.18 > 10.0.3.254: ICMP echo request, id 61873, seq 35233, length 8
10 packets captured
160 packets received by filter
0 packets dropped by kernel

```

Execute Shell Command

tcpdump -c 10

⏪ Execute ⏩ Clear

## Appendix A: Backing Up and Restoring pfSense

Diagnostics / Backup & Restore / Backup & Restore ?

Backup & Restore Config History

---

**Backup Configuration**

Backup area









































Skip packages  Do not backup package information.

Skip RRD data  Do not backup RRD data (NOTE: RRD Data can consume 4+ megabytes of config.xml space!)

Encryption  Encrypt this configuration file.

[Download configuration as XML](#)



 Diff	Date	Version	Size	Configuration Change	Actions
<input type="radio"/>	11/24/18 11:13:01	18.9	28 KiB	(system): Upgraded config version level from 18.5 to 18.9	Current configuration
<input type="radio"/>	11/24/18 11:03:04	18.5	28 KiB	admin@172.16.1.102: Saved system update settings.	  
<input type="radio"/>	11/24/18 10:25:59	18.5	28 KiB	(system): Overwrote previous installation of FRR.	  
<input type="radio"/>	11/24/18 10:25:58	18.5	25 KiB	(system): Intermediate config write during package install for FRR.	  
<input type="radio"/>	11/24/18 10:25:55	18.5	26 KiB	(system): Intermediate config write during package removal for frr.	  
<input type="radio"/>	11/24/18 10:25:45	18.5	28 KiB	(system): Overwrote previous installation of routed.	  
<input type="radio"/>	11/24/18 10:25:44	18.5	27 KiB	(system): Intermediate config write during package install for routed.	  
<input type="radio"/>	11/24/18 10:25:42	18.5	27 KiB	(system): Intermediate config write during package removal for routed.	  
<input type="radio"/>	11/24/18 10:25:11	18.5	28 KiB	(system): Configured default pkg repo after restore	  
<input type="radio"/>	11/18/18 18:07:12	18.5	27 KiB	admin@172.16.1.102: /interfaces.php made unknown change	  
<input type="radio"/>	11/18/18 18:05:44	18.5	28 KiB	admin@172.16.1.102: Gateways: removed gateway 0	  
<input type="radio"/>	11/18/18 18:05:17	18.5	29 KiB	admin@172.16.1.102: Gateway Groups: removed gateway group 0	  
<input type="radio"/>	11/18/18 18:00:18	18.5	29 KiB	admin@172.16.1.102: Enter CARP maintenance mode	  
<input type="radio"/>	11/18/18 17:59:57	18.5	29 KiB	admin@172.16.1.102: Leave CARP maintenance mode	  

## Configuration Diff from 11/24/18 10:25:59 to 11/24/18 11:13:01

```

-- /conf/backup/config-1543055159.xml 2018-11-24 11:03:04.806337000 +0000
+++ /conf/config.xml 2018-11-24 11:13:01.260058000 +0000
@@ -1,6 +1,6 @@
<?xml version="1.0"?>
<pfsense>
- <version>18.5</version>
+ <version>18.9</version>
  <lastchange></lastchange>
  <system>
    <optimization>normal</optimization>
@@ -62,6 +62,10 @@
    <dns1gw>WAN_DHCP</dns1gw>
    <dns2gw>OPT_WAN_DHCP</dns2gw>
    <pkg_repo_conf_path>/usr/local/share/pfSense/pkg/repos/pfSense-repo-devel.conf</pkg_repo_conf_path>
+ <gitsync>
+   <repositoryurl></repositoryurl>
+   <branch></branch>
+ </gitsync>
  </system>
  <interfaces>
    <wan>
@@ -485,7 +489,7 @@
    <month>*</month>
    <wday>*</wday>
    <who>root</who>
-   <command>/usr/bin/nice -n20 /usr/local/sbin/expirable -v -t 3600 sshlockout</command>
+   <command>/usr/bin/nice -n20 /usr/local/sbin/expirable -v -t 3600 sshguard</command>
  </item>
  <item>
    <minute>*/60</minute>
@@ -647,8 +651,8 @@
    <dnssecstripped></dnssecstripped>
  </unbound>
  <revision>

```

---

### Restore Backup

Open a pfSense configuration XML file and click the button below to restore the configuration.

**Restore area**

**Configuration file**  No file selected.

**Encryption**  Configuration file is encrypted.

The firewall will reboot after restoring the configuration.

---

### Package Functions

Click this button to reinstall all system packages. This may take a while.

**System Update**   **Update Settings**

---

### Firmware Branch

**Branch**

Please select the branch from which to update the system firmware.  
Use of the development version is at your own risk!

---

### Updates

**Dashboard check**  Disable the Dashboard auto-update check

**Confirmation Required to update pfSense system.**

Branch

Latest development snapshots (Experimental 2.4.x DEVEL)

Please select the branch from which to update the system firmware.  
Use of the development version is at your own risk!

Current Base System 2.4.4

Latest Base System 2.4.5.a.20181120.0925

Confirm Update

 Confirm**Updating System**

Number of packages to be installed: 3




Number of packages to be upgraded: 32

The process will require 14 MiB more space.

69 MiB to be downloaded.

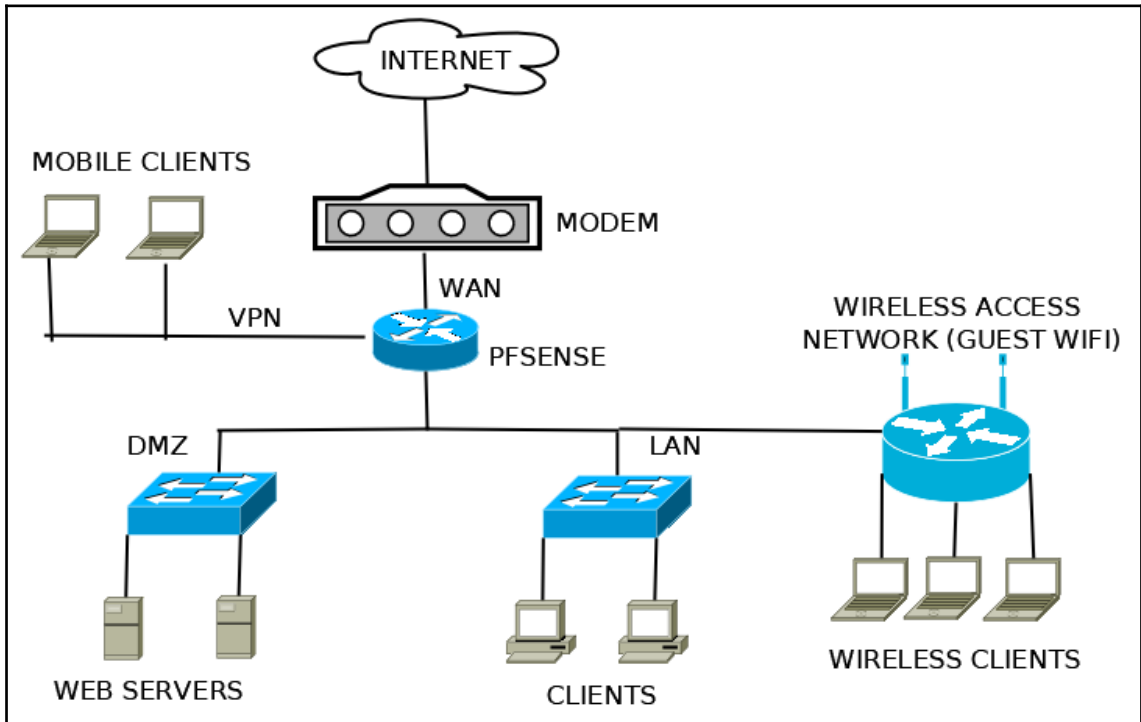
```
[1/35] Fetching wpa_supplicant-2.6_3.txz: ..... done
[2/35] Fetching sqlite3-3.25.1.txz: ..... done
[3/35] Fetching smartmontools-6.6_2.txz: ..... done
[4/35] Fetching relayd-5.5.20140810_3.txz: ..... done
[5/35] Fetching py27-setuptools-40.0.0.txz: ..... done
[6/35] Fetching php72-pear-XML_RPC2-1.1.4.txz: ..... done
[7/35] Fetching php72-pear-Net_Smtp-1.8.1.txz: .. done
[8/35] Fetching pfSense-rc-2.4.5.a.20181121.0459.txz: .. done
[9/35] Fetching pfSense-kernel-pfSense-2.4.5.a.20181121.0459.txz: ..... done
[10/35] Fetching pfSense-default-config-2.4.5.a.20181121.0459.txz: .. done
[11/35] Fetching pfSense-base-2.4.5.a.20181121.0459.txz: ..|
```

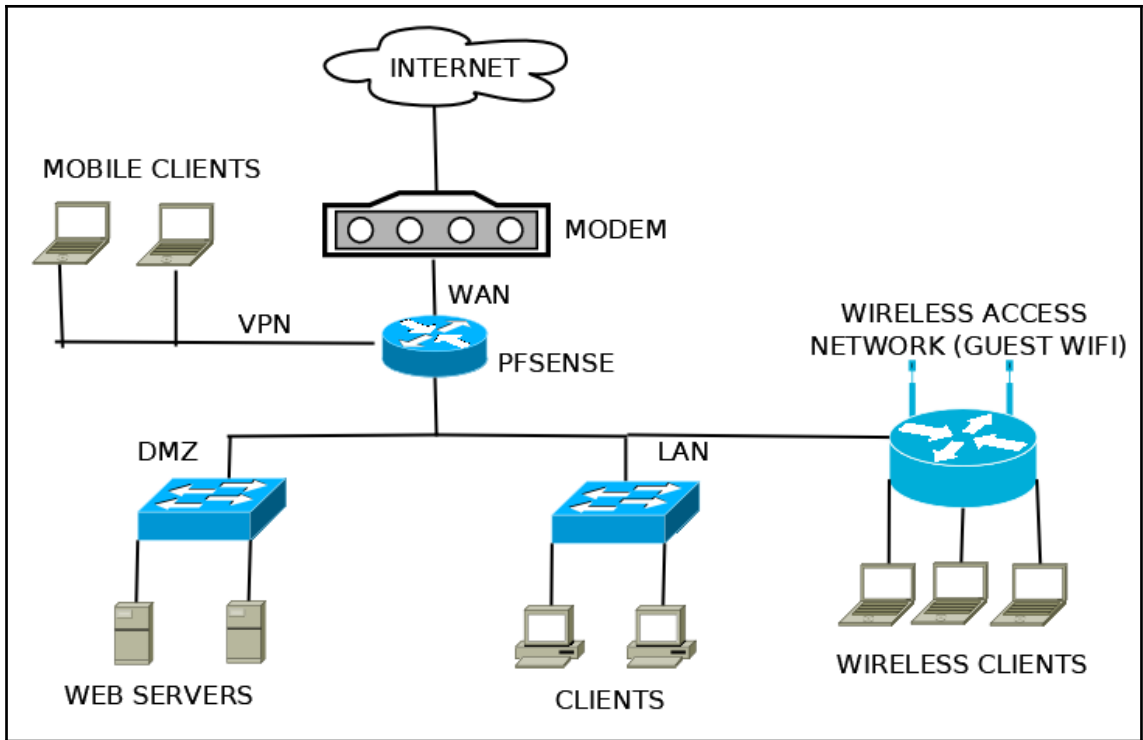
---

System Information  	
<b>Name</b>	pfSense.thewookie.duckdns.org
<b>User</b>	admin@172.16.1.102 (Local Database)
<b>System</b>	VirtualBox Virtual Machine Netgate Device ID: <b>700d2b83652bb90e4e01</b>
<b>BIOS</b>	Vendor: <b>innotek GmbH</b> Version: <b>VirtualBox</b> Release Date: <b>Fri Dec 1 2006</b>
<b>Version</b>	<b>2.4.5-DEVELOPMENT</b> (amd64) built on Wed Nov 21 05:00:12 EST 2018 FreeBSD 11.2-RELEASE-p4  <b>The system is on the latest version.</b> Version information updated at Sat Nov 24 7:23:19 EST 2018 

---

## Appendix B: Determining Hardware Requirements





# Index