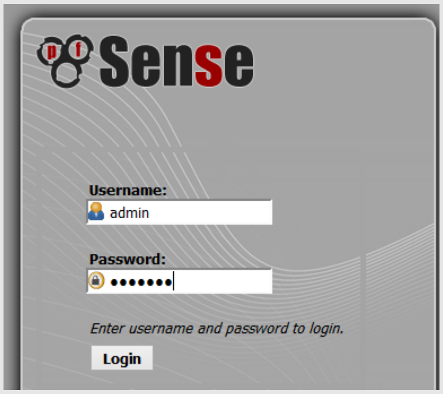
Configuring Interfaces

1. With the URL insert it into the browser and login with username admin and password pfSense.

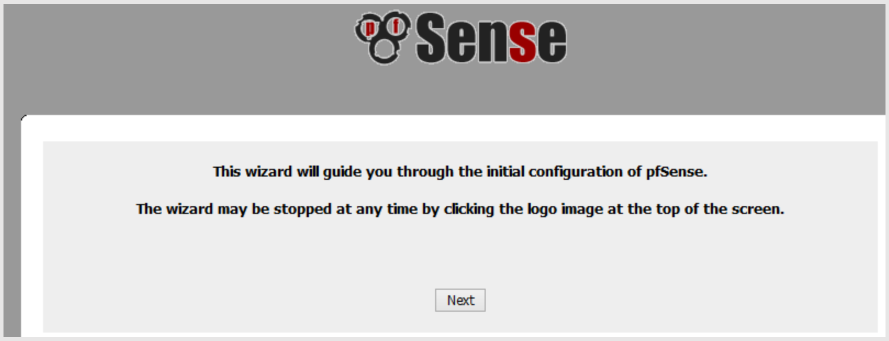


Username: admin

Password: •••••••

Enter username and password to login.

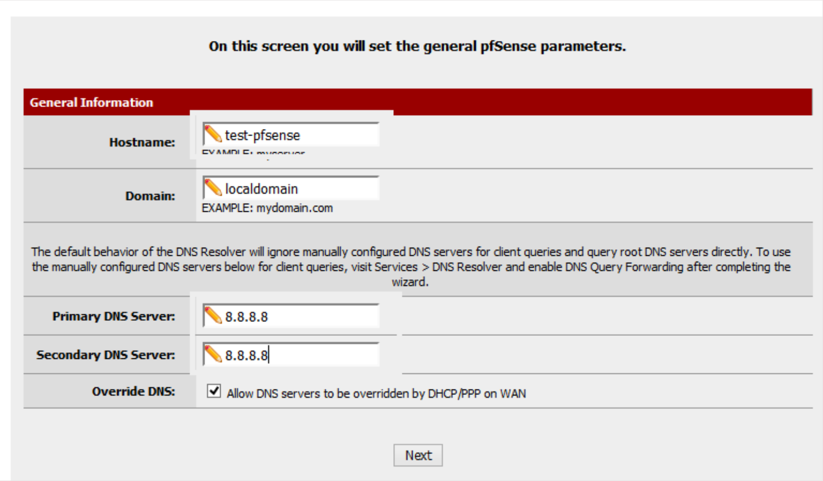
2. After successful login, following wizard appears for the basic setting of pfSense firewall. Click the Next button to start basic configuration process on pfSense firewall.



This wizard will guide you through the initial configuration of pfSense.

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

3. Set the hostname, domain and DNS addresses here.



On this screen you will set the general pfSense parameters.

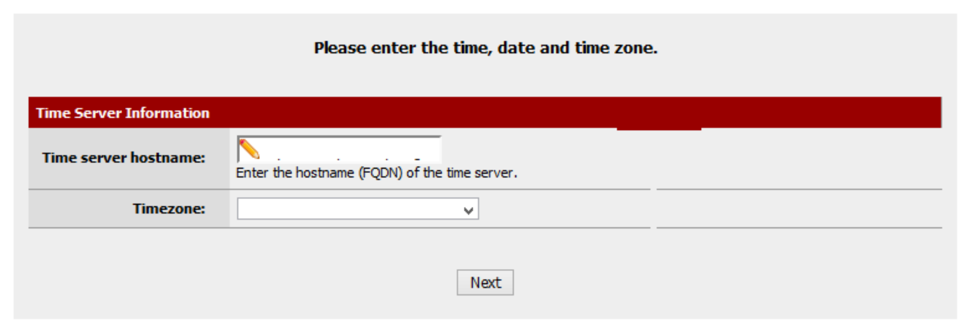
General Information

Hostname:	test-pfsense EXAMPLE: myserver
Domain:	localdomain EXAMPLE: mydomain.com

The default behavior of the DNS Resolver will ignore manually configured DNS servers for client queries and query root DNS servers directly. To use the manually configured DNS servers below for client queries, visit Services > DNS Resolver and enable DNS Query Forwarding after completing the wizard.

Primary DNS Server:	8.8.8.8
Secondary DNS Server:	8.8.8.8
Override DNS:	☑ Allow DNS servers to be overridden by DHCP/PPP on WAN

4. Set the time zone.



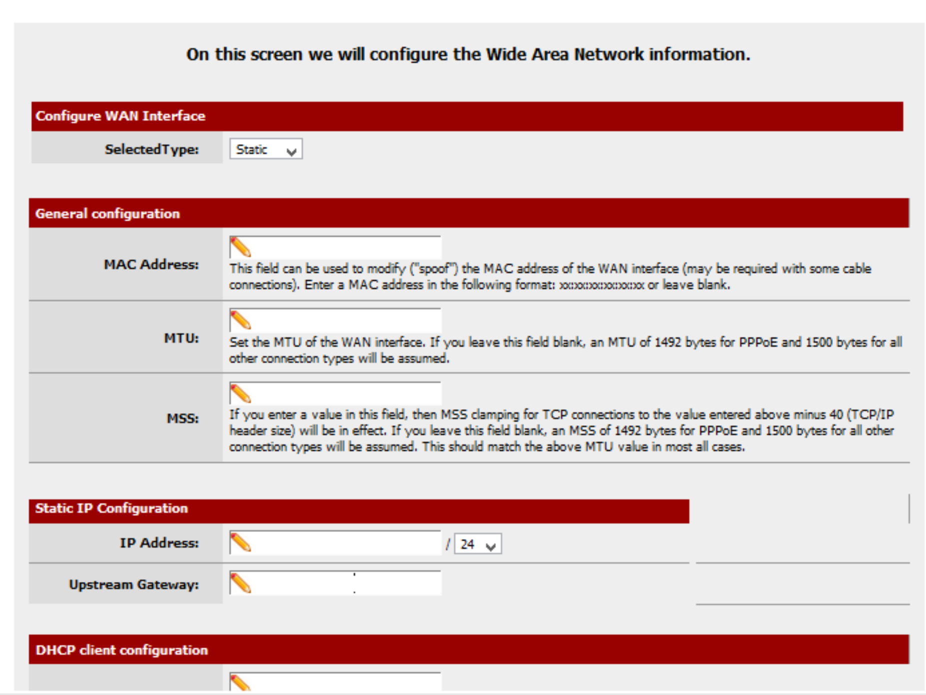
Please enter the time, date and time zone.

Time Server Information

Time server hostname:
Enter the hostname (FQDN) of the time server.

Timezone:

5. Set the WAN interface. By default, pfSense block private networks.



On this screen we will configure the Wide Area Network information.

Configure WAN Interface

SelectedType: Static

General configuration

MAC Address:
This field can be used to modify ("spoof") the MAC address of the WAN interface (may be required with some cable connections). Enter a MAC address in the following format: xx:xx:xx:xx:xx:xx or leave blank.

MTU:
Set the MTU of the WAN interface. If you leave this field blank, an MTU of 1492 bytes for PPPoE and 1500 bytes for all other connection types will be assumed.

MSS:
If you enter a value in this field, then MSS clamping for TCP connections to the value entered above minus 40 (TCP/IP header size) will be in effect. If you leave this field blank, an MSS of 1492 bytes for PPPoE and 1500 bytes for all other connection types will be assumed. This should match the above MTU value in most all cases.

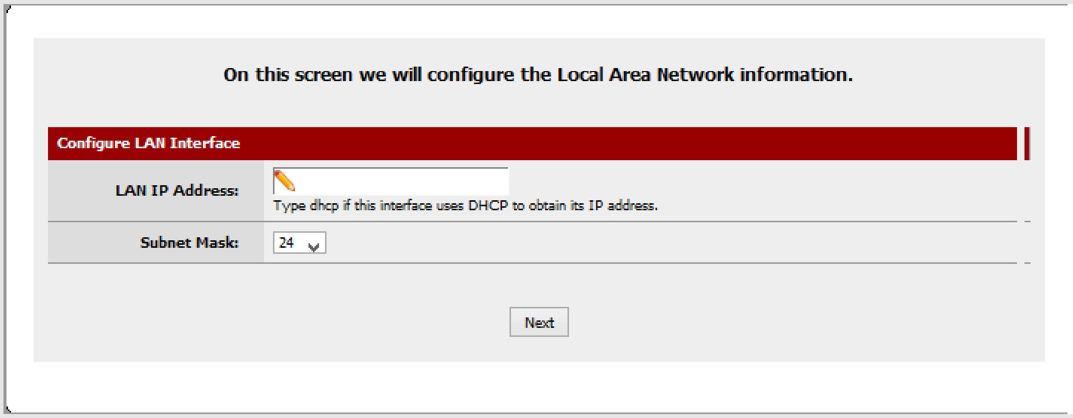
Static IP Configuration

IP Address: / 24

Upstream Gateway:

DHCP client configuration

6. Set the LAN IP address, this is used to access the pfSense web interface.



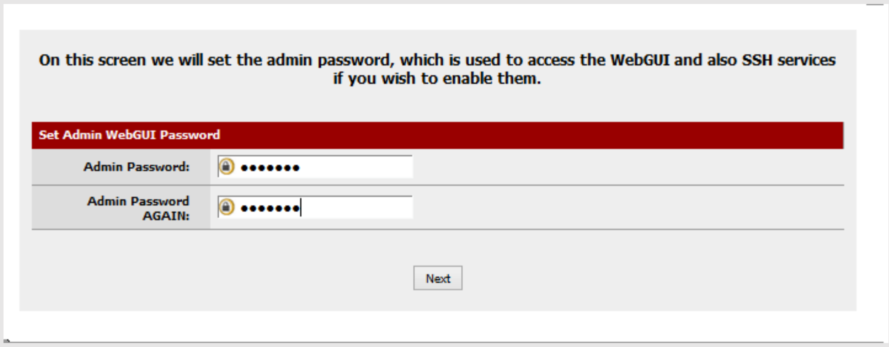
On this screen we will configure the Local Area Network information.

Configure LAN Interface

LAN IP Address:
Type dhcp if this interface uses DHCP to obtain its IP address.

Subnet Mask: 24

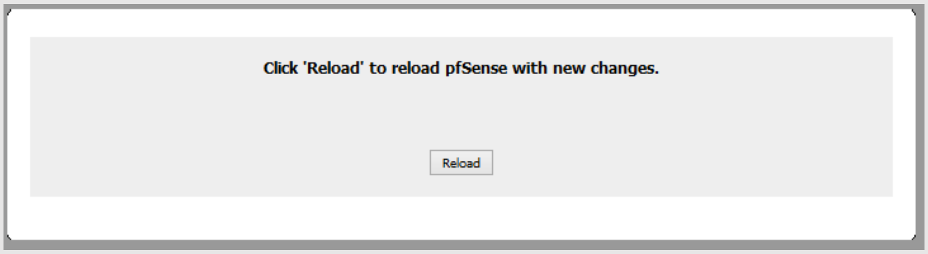
7. By default the web interface password is “pfSense”. Here you can enter a new password for the admin user.



On this screen we will set the admin password, which is used to access the WebGUI and also SSH services if you wish to enable them.

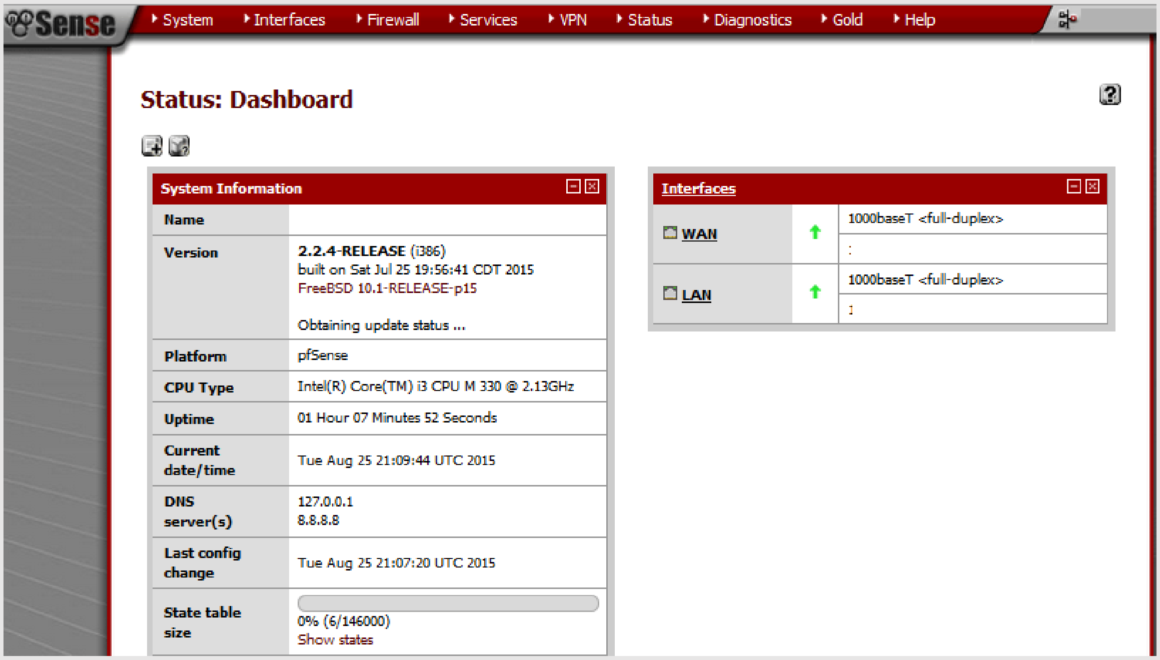
Set Admin WebGUI Password	
Admin Password:	•••••••
Admin Password AGAIN:	•••••••

8. Click the “reload” button to configure the changes.



Click 'Reload' to reload pfSense with new changes.

9. PfSense will display the dashboard and show the system information.



Status: Dashboard

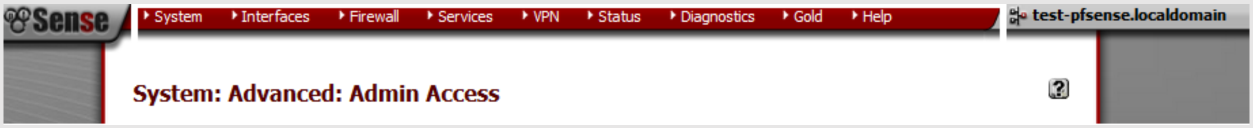
System Information	
Name	
Version	2.2.4-RELEASE (i386) built on Sat Jul 25 19:56:41 CDT 2015 FreeBSD 10.1-RELEASE-p15 Obtaining update status ...
Platform	pfSense
CPU Type	Intel(R) Core(TM) i3 CPU M 330 @ 2.13GHz
Uptime	01 Hour 07 Minutes 52 Seconds
Current date/time	Tue Aug 25 21:09:44 UTC 2015
DNS server(s)	127.0.0.1 8.8.8.8
Last config change	Tue Aug 25 21:07:20 UTC 2015
State table size	0% (6/146000) Show states

Interfaces		
WAN	↑	1000baseT <full-duplex> :
LAN	↑	1000baseT <full-duplex> :

Other Options

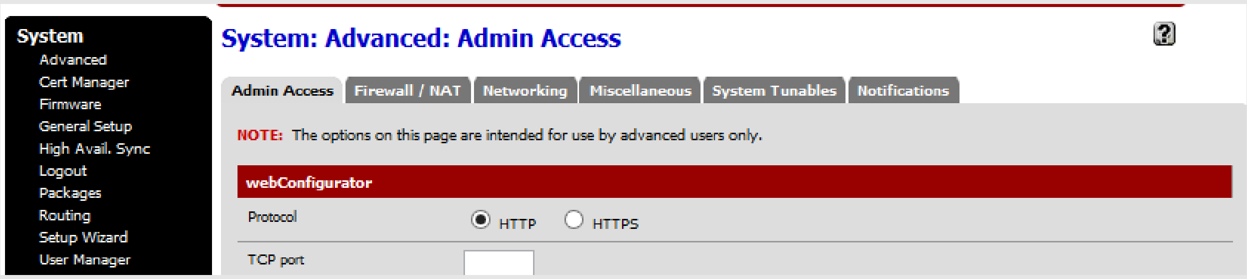
The Menu

The pfSense menu consists of System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help.



System Menu

In the Advanced menu, the user can perform different operations. Like configuring the web interface, firewall/Nat settings, network setting, etc.

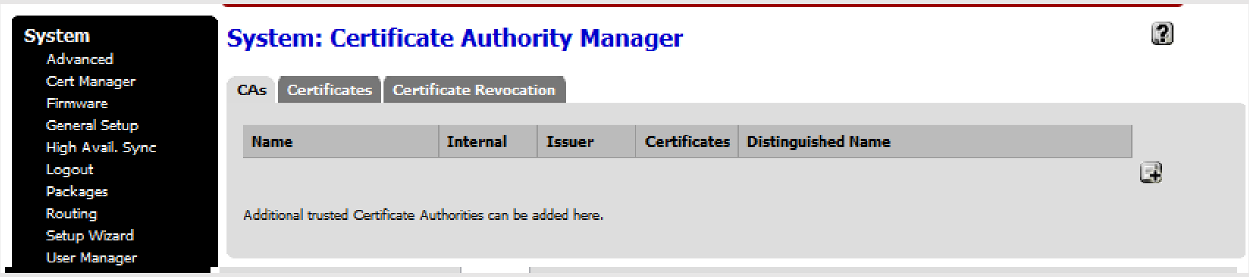


NOTE: The options on this page are intended for use by advanced users only.

Protocol ● HTTP ○ HTTPS

TCP port

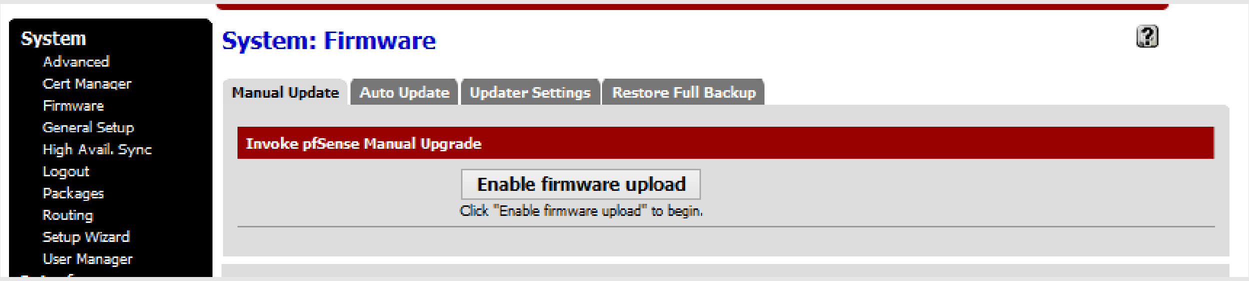
In the Cert manager sub menu, firewall administrator generates certificates for CA and users.



Name	Internal	Issuer	Certificates	Distinguished Name

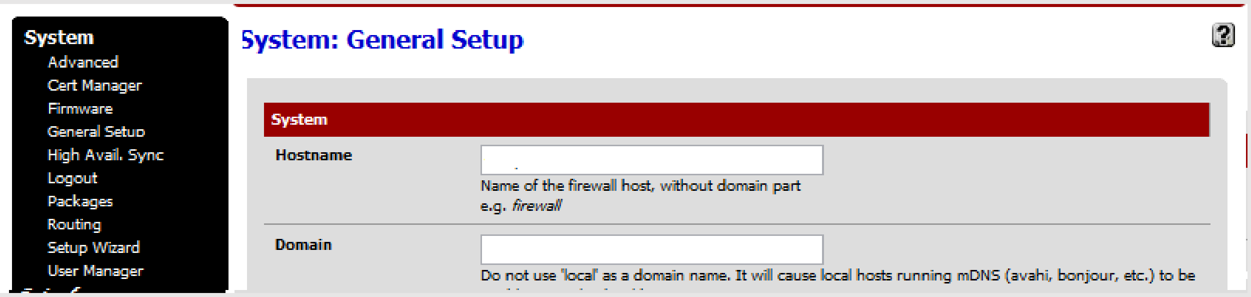
Additional trusted Certificate Authorities can be added here.

In the Firmware sub menu, user can update Pfsense firmware manually/automatically. User can take full backup of Pfsense configurations.



Click "Enable firmware upload" to begin.

In the General Setup sub menu, user can change basic setting such as hostname and domain etc.



System: General Setup

System

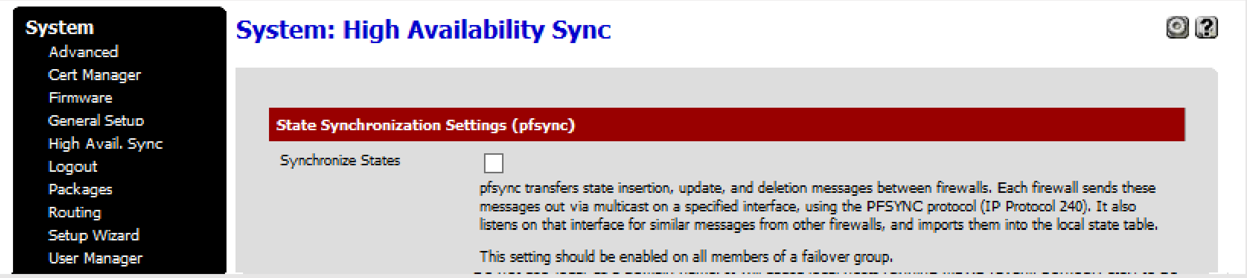
Hostname

Name of the firewall host, without domain part
e.g. *firewall*

Domain

Do not use 'local' as a domain name. It will cause local hosts running mDNS (avahi, bonjour, etc.) to be

As menu title indicates, user can enable/disable high availability feature from this sub menu.



System: High Availability Sync

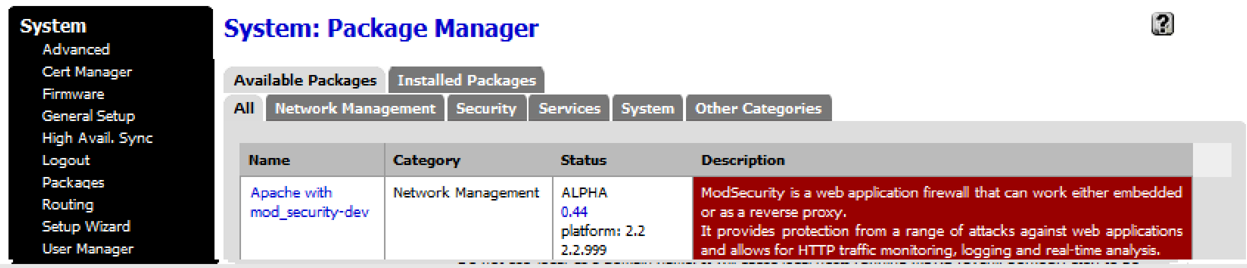
State Synchronization Settings (pfsync)

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.

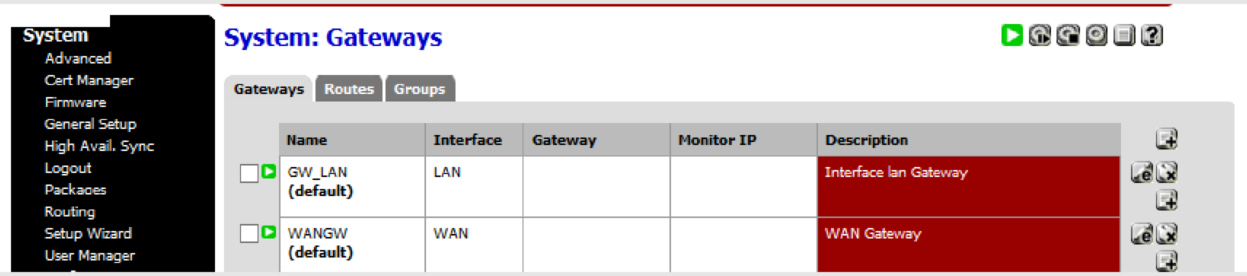
Packages sub menu provides package manager facility in the web interface for Pfsense .



System: Package Manager

Name	Category	Status	Description
Apache with mod_security-dev	Network Management	ALPHA 0.44 platform: 2.2 2.2.999	ModSecurity is a web application firewall that can work either embedded or as a reverse proxy. It provides protection from a range of attacks against web applications and allows for HTTP traffic monitoring, logging and real-time analysis.

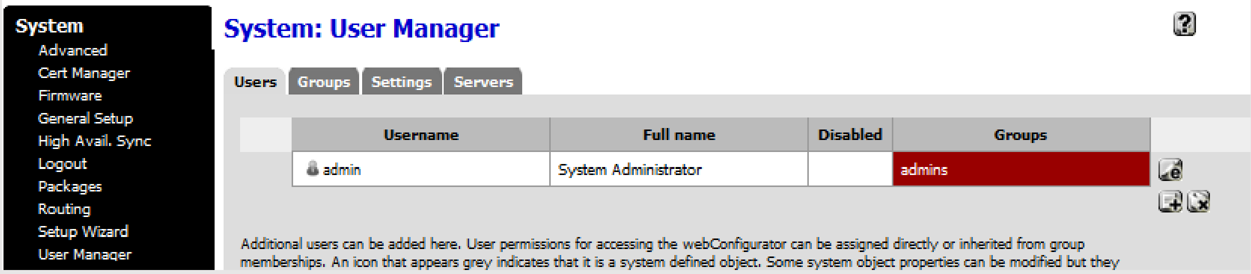
User can perform gateway and route management using Routing sub menu.



System: Gateways

	Name	Interface	Gateway	Monitor IP	Description
☐	GW_LAN **(default)**	LAN			Interface lan Gateway
☐	WANGW **(default)**	WAN			WAN Gateway

Management of user can be done from the User manager sub menu.



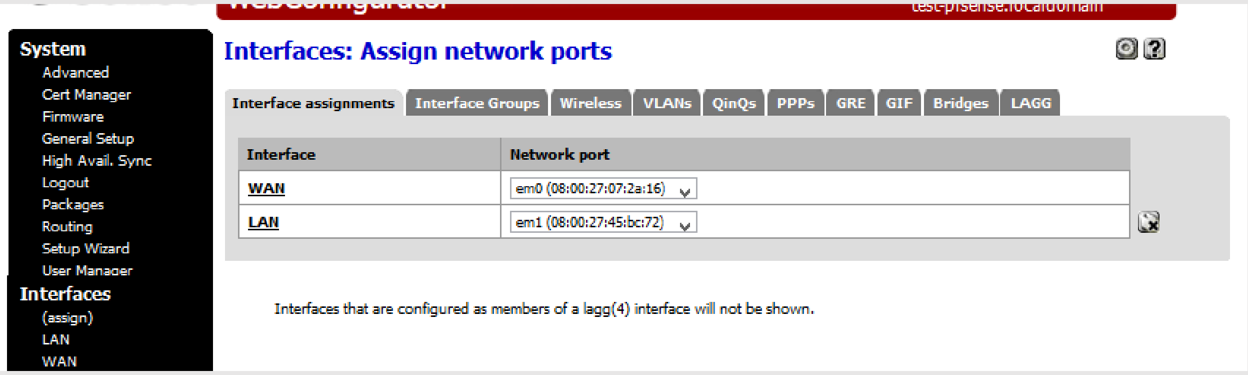
System: User Manager

Username	Full name	Disabled	Groups
admin	System Administrator		admins

Additional users can be added here. User permissions for accessing the webConfigurator can be assigned directly or inherited from group memberships. An icon that appears grey indicates that it is a system defined object. Some system object properties can be modified but they

Interfaces Menu

This menu is used for the assignment of interfaces (LAN/WAN), VLAN setting, wireless and GRE configuration etc.



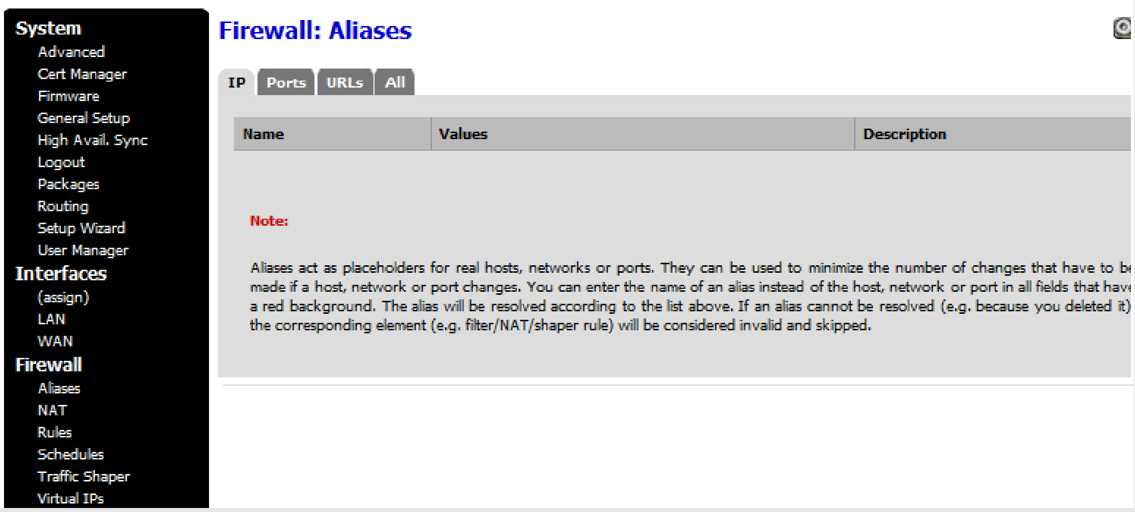
Interfaces: Assign network ports

Interface	Network port
WAN	em0 (08:00:27:07:2a:16)
LAN	em1 (08:00:27:45:bc:72)

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

Firewall Menu

Firewall is the main and core part of pfSense distribution and it provides following features.



Firewall: Aliases

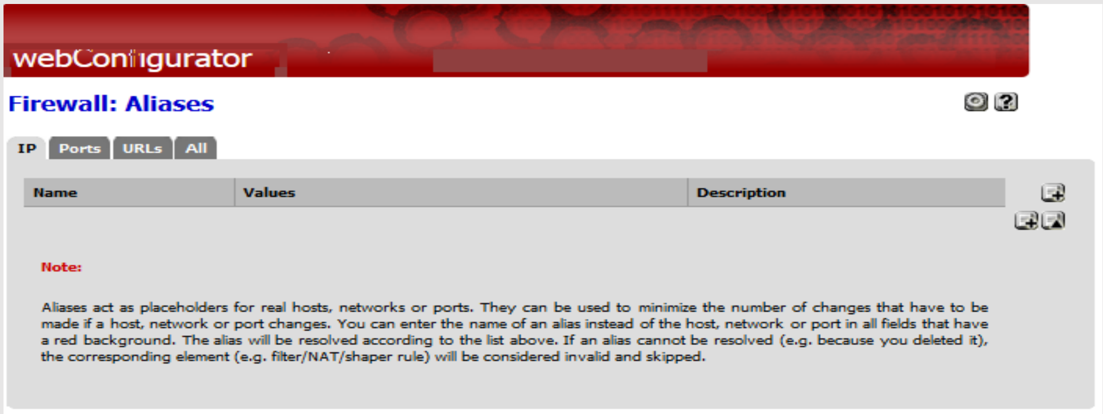
Name	Values	Description

Note:

Aliases act as placeholders for real hosts, networks or ports. They can be used to minimize the number of changes that have to be made if a host, network or port changes. You can enter the name of an alias instead of the host, network or port in all fields that have a red background. The alias will be resolved according to the list above. If an alias cannot be resolved (e.g. because you deleted it) the corresponding element (e.g. filter/NAT/shaper rule) will be considered invalid and skipped.

Aliases

Aliases are defined for real hosts, networks or ports and they can be used to minimize the number of changes.



webConfigurator

Firewall: Aliases

IP | Ports | URLs | All

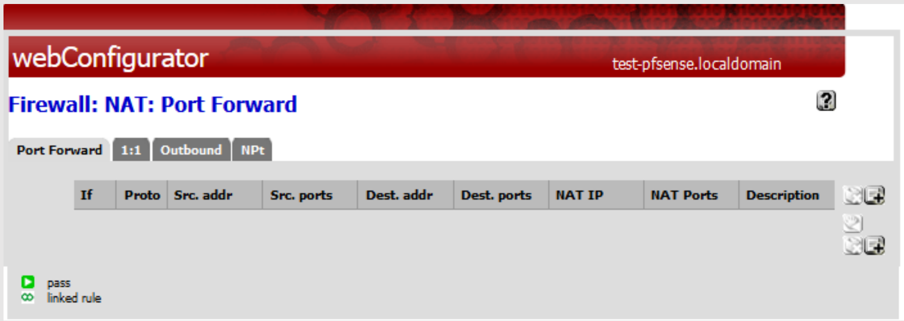
Name	Values	Description

Note:

Aliases act as placeholders for real hosts, networks or ports. They can be used to minimize the number of changes that have to be made if a host, network or port changes. You can enter the name of an alias instead of the host, network or port in all fields that have a red background. The alias will be resolved according to the list above. If an alias cannot be resolved (e.g. because you deleted it), the corresponding element (e.g. filter/NAT/shaper rule) will be considered invalid and skipped.

NAT (Network Address Translation)

NAT binds a specific internal address to a specific external address. Incoming traffic from the Internet to the specified IP will be directed toward the associated internal IP.



webConfigurator test-pfsense.localdomain

Firewall: NAT: Port Forward

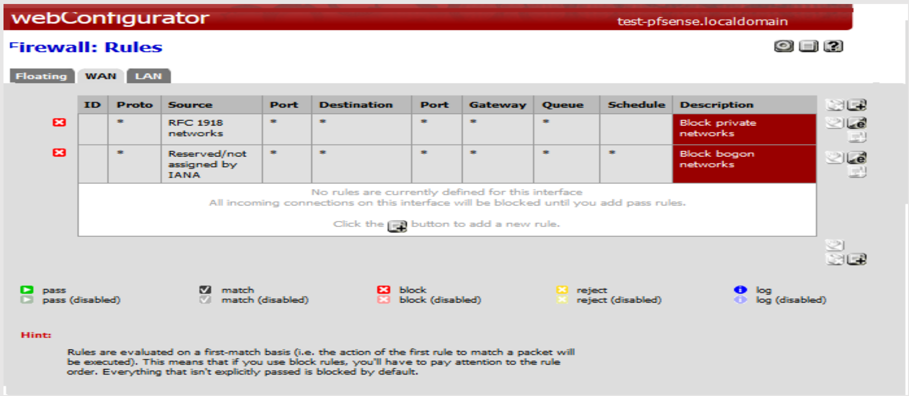
Port Forward | 1:1 | Outbound | NPt

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

🟩 pass
∞ linked rule

Firewall Rules

Firewall rules controls what traffic is allowed to enter an interface on the firewall. After traffic is passed on the interface, it enters an entry in the state table is created.



webConfigurator test-pfsense.localdomain

Firewall: Rules

Floating | WAN | LAN

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

No rules are currently defined for this interface
All incoming connections on this interface will be blocked until you add pass rules.

Click the ⊞ button to add a new rule.

🟩 pass
pass (disabled)

☑ match
match (disabled)

☒ block
block (disabled)

☒ reject
reject (disabled)

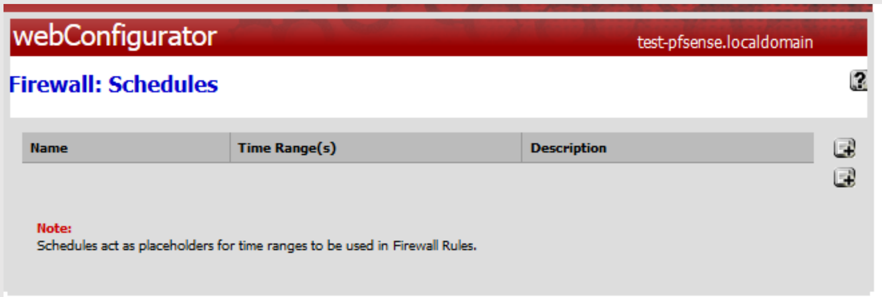
● log
log (disabled)

Hint:

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

Schedules

Firewall rules can be scheduled so that they are only active at certain times of day or on certain specific days or days of the week.



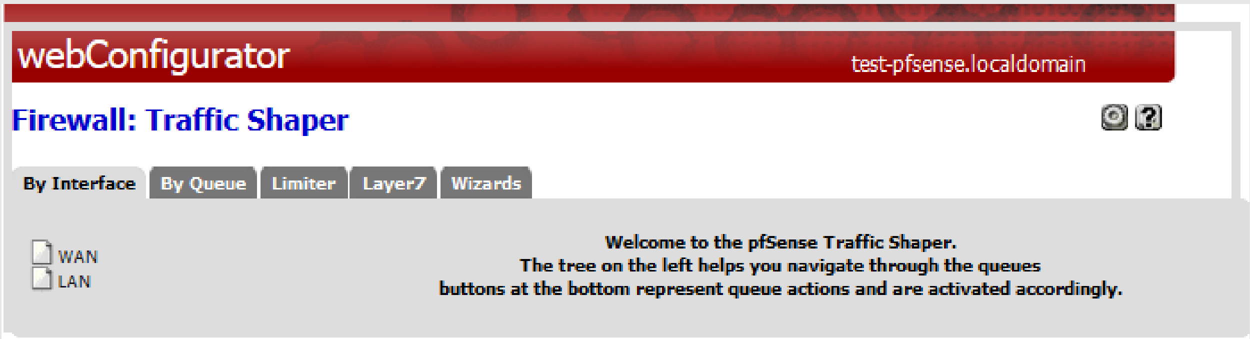
Firewall: Schedules

Name	Time Range(s)	Description

Note:
Schedules act as placeholders for time ranges to be used in Firewall Rules.

Traffic Shaper

Traffic shaping is the control of computer network traffic in order to optimize performance and lower latency.

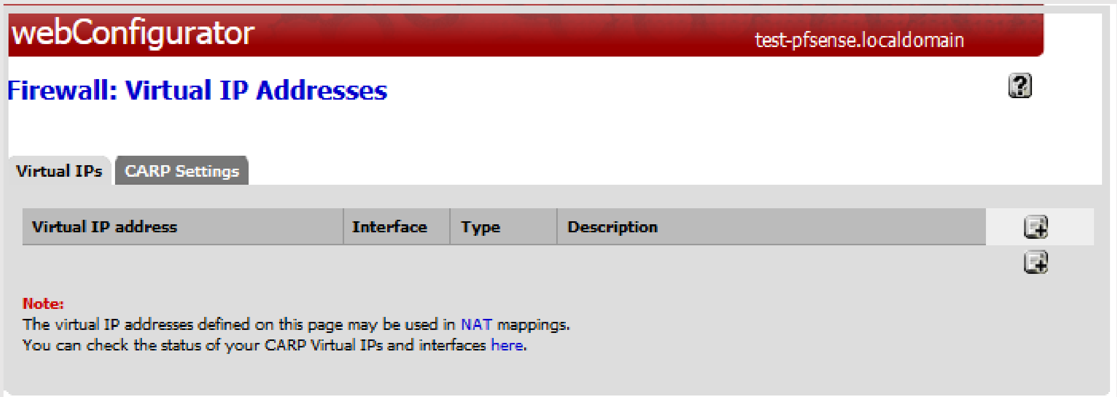


Firewall: Traffic Shaper

Welcome to the pfSense Traffic Shaper.
The tree on the left helps you navigate through the queues
buttons at the bottom represent queue actions and are activated accordingly.

Virtual IPs

Virtual IPs add knowledge of additional IP addresses to the firewall that are different from the firewall's real interface addresses.



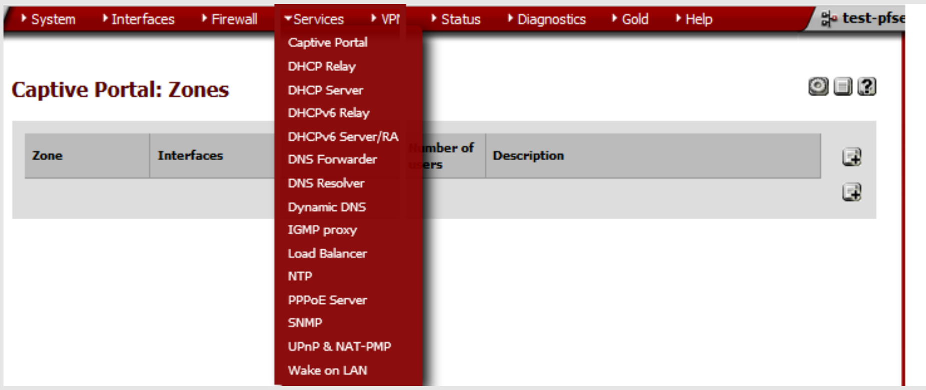
Firewall: Virtual IP Addresses

Virtual IP address	Interface	Type	Description

Note:
The virtual IP addresses defined on this page may be used in NAT mappings.
You can check the status of your CARP Virtual IPs and interfaces here.

Services Menu

Services menu shows services which are provided by the pfSense distribution along firewall. New program/software installed for some specific service is also shown in this menu such as snort. By default, following services are listed in services menu.

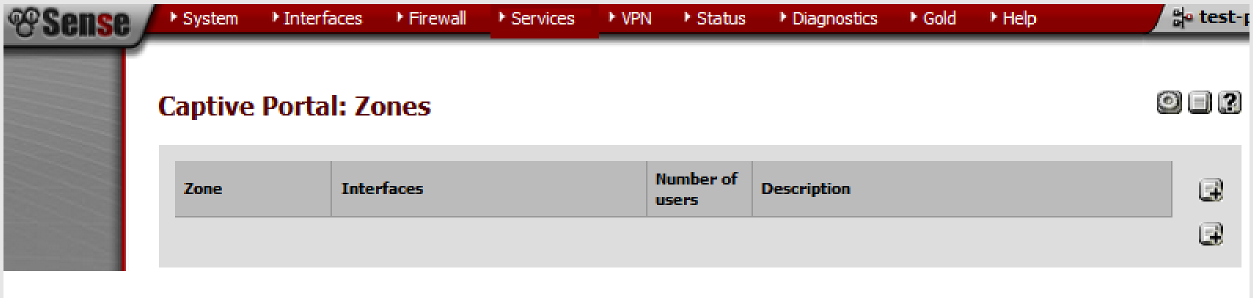


Captive Portal: Zones

Zone	Interfaces	Number of users	Description

Captive portal

The captive portal functionality in pfSense allows securing a network by requiring a username and password entered on a portal page.

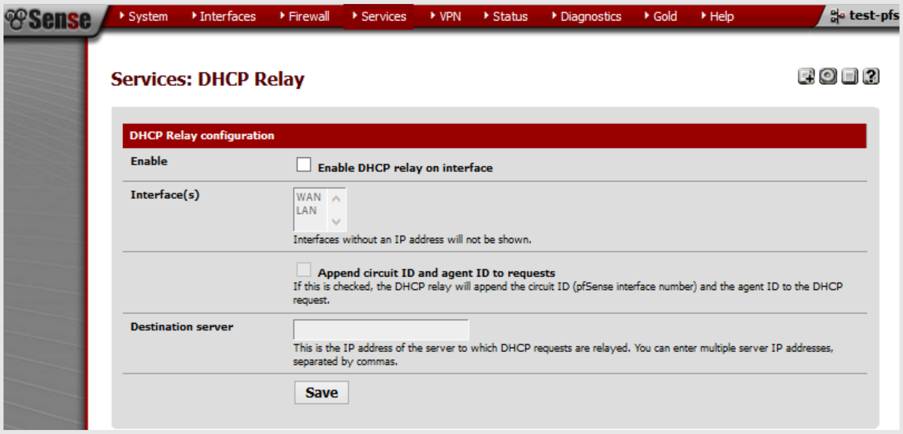


Captive Portal: Zones

Zone	Interfaces	Number of users	Description

DHCP Relay

The DHCP Relay daemon will relay DHCP requests between broadcast domains for IPv4 DHCP.



Services: DHCP Relay

DHCP Relay configuration

Enable: ☐ Enable DHCP relay on interface

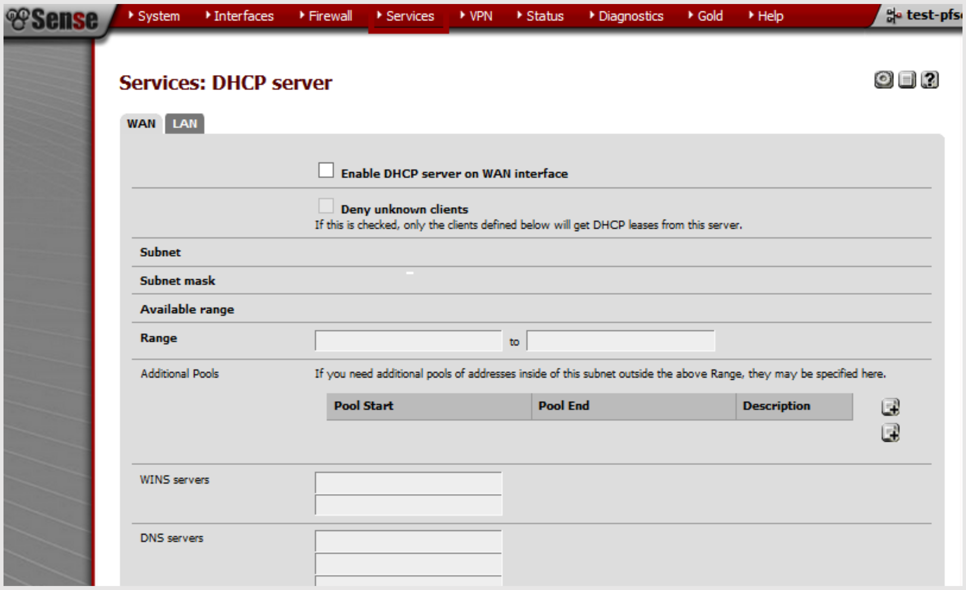
Interface(s): WAN LAN
Interfaces without an IP address will not be shown.

☐ 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 IP address of the server to which DHCP requests are relayed. You can enter multiple server IP addresses, separated by commas.

DHCP Server

User can run DHCP service on the firewall for the network devices.



Services: DHCP server

WAN | LAN

□ Enable DHCP server on WAN interface

□ Deny unknown clients
If this is checked, only the clients defined below will get DHCP leases from this server.

Subnet

Subnet mask

Available range

Range ______ to ______

Additional Pools — If you need additional pools of addresses inside of this subnet outside the above Range, they may be specified here.

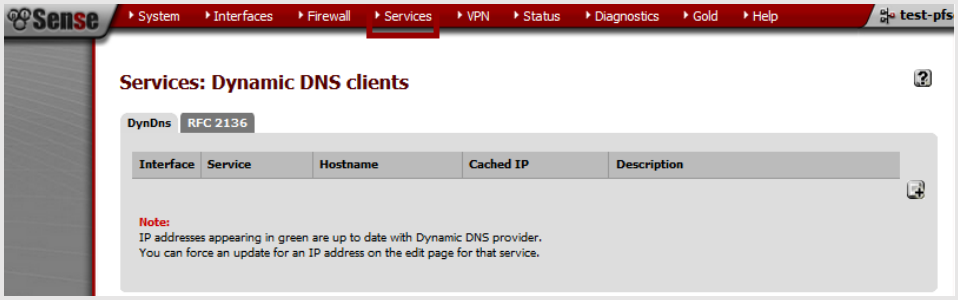
Pool Start	Pool End	Description

WINS servers

DNS servers

DNS Forwarder/Resolver/Dynamic DNS

DNS different services can be configured on the pfSense firewall.

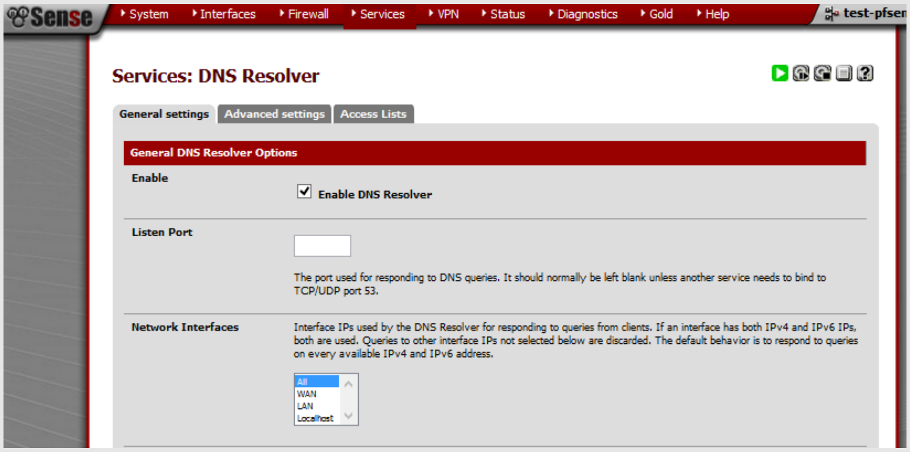


Services: Dynamic DNS clients

DynDns | RFC 2136

Interface	Service	Hostname	Cached IP	Description

Note:
IP addresses appearing in green are up to date with Dynamic DNS provider.
You can force an update for an IP address on the edit page for that service.



Services: DNS Resolver

General settings | Advanced settings | Access Lists

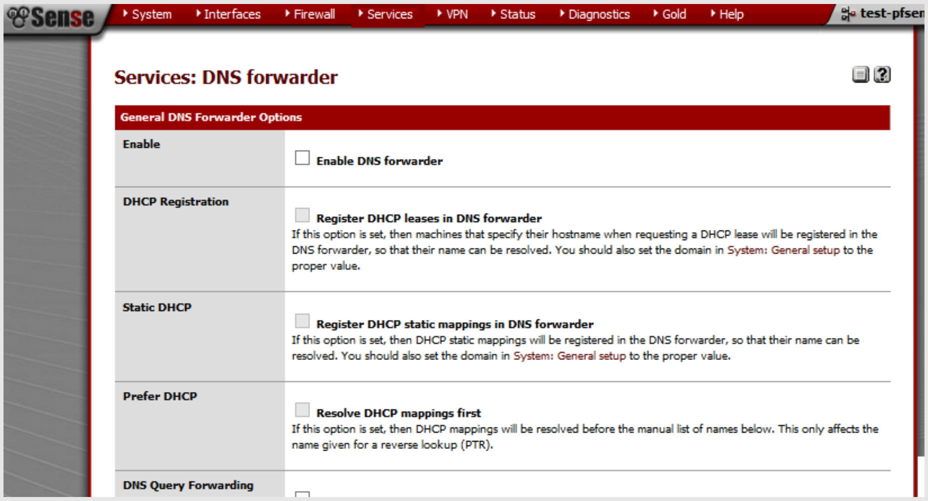
General DNS Resolver Options

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.

Network Interfaces — 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.

All
WAN
LAN
Localhost



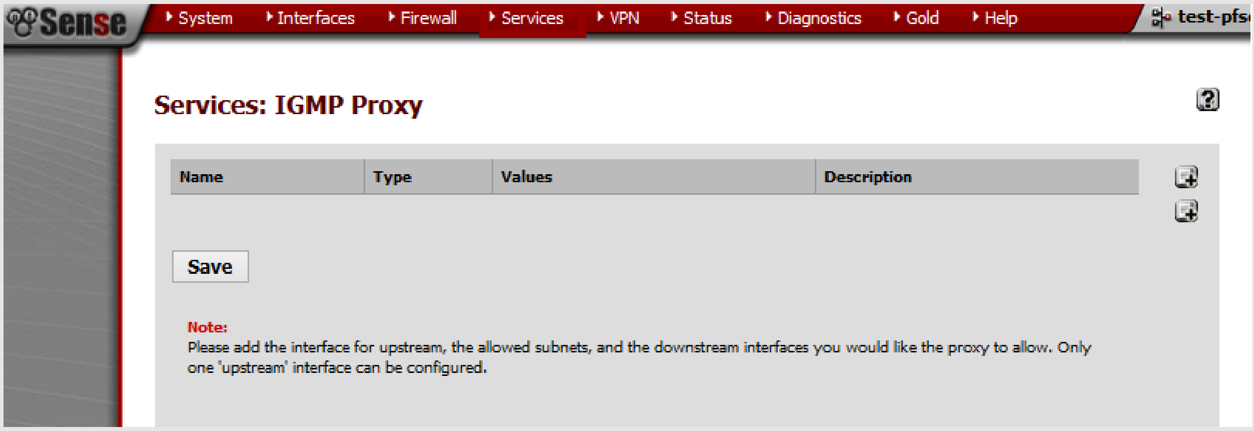
Services: DNS forwarder

General DNS Forwarder Options

Enable	□ Enable DNS forwarder
DHCP Registration	□ Register DHCP leases in DNS forwarder If this option is set, then machines that specify their hostname when requesting a DHCP lease will be registered in the DNS forwarder, so that their name can be resolved. You should also set the domain in System: General setup to the proper value.
Static DHCP	□ Register DHCP static mappings in DNS forwarder If this option is set, then DHCP static mappings will be registered in the DNS forwarder, so that their name can be resolved. You should also set the domain in System: General setup to the proper value.
Prefer DHCP	□ Resolve DHCP mappings first If this option is set, then DHCP mappings will be resolved before the manual list of names below. This only affects the name given for a reverse lookup (PTR).
DNS Query Forwarding	□

IGMP Proxy

User can configure IGMP on the pfSense firewall from services menu.



Services: IGMP Proxy

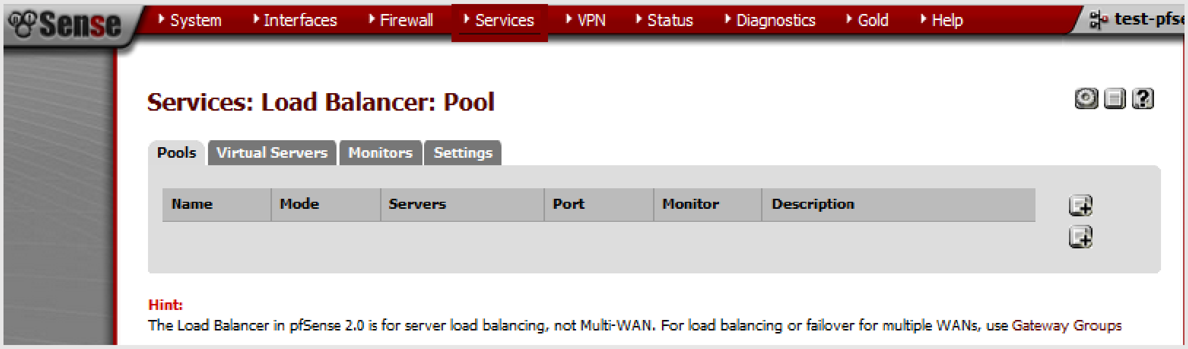
Name	Type	Values	Description

Save

Note:
Please add the interface for upstream, the allowed subnets, and the downstream interfaces you would like the proxy to allow. Only one 'upstream' interface can be configured.

Load Balancer

Load Balancing is one of the important feature which is also supported by the pfSense firewall.



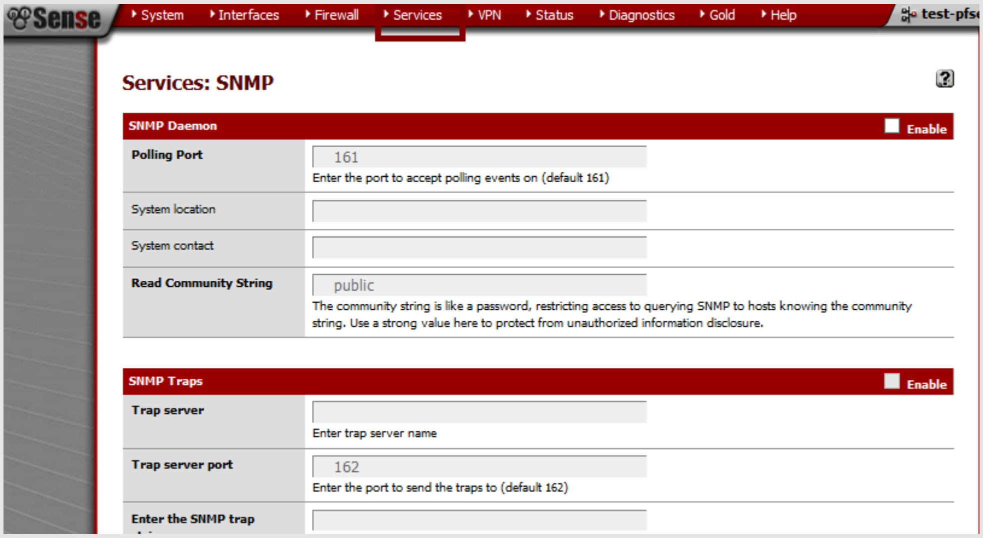
Services: Load Balancer: Pool

Name	Mode	Servers	Port	Monitor	Description

Hint:
The Load Balancer in pfSense 2.0 is for server load balancing, not Multi-WAN. For load balancing or failover for multiple WANs, use Gateway Groups

SNMP (Simple Network Management Protocol)

pfSense supports all versions of snmp for remote management of firewall.



Services: SNMP

SNMP Daemon □ Enable

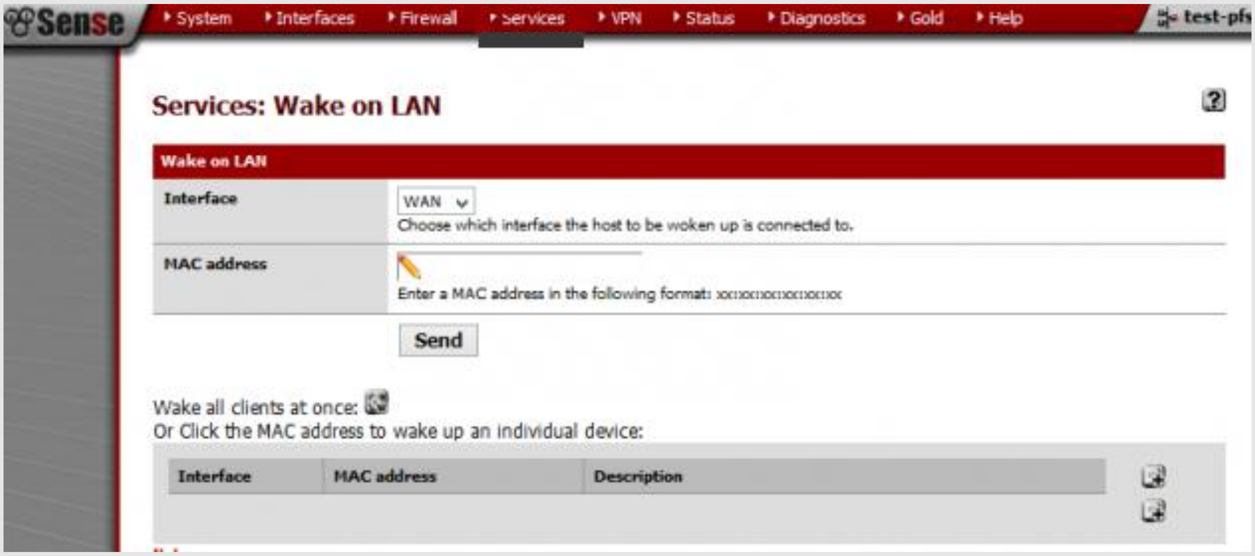
Polling Port	161 Enter the port to accept polling events on (default 161)
System location	
System contact	
Read Community String	public The community string is like a password, restricting access to querying SNMP to hosts knowing the community string. Use a strong value here to protect from unauthorized information disclosure.

SNMP Traps □ Enable

Trap server	Enter trap server name
Trap server port	162 Enter the port to send the traps to (default 162)
Enter the SNMP trap	

Wake on Lan

Using this feature packet sent to a workstation on a locally connected network which will power on a workstation.



Services: Wake on LAN

Wake on LAN

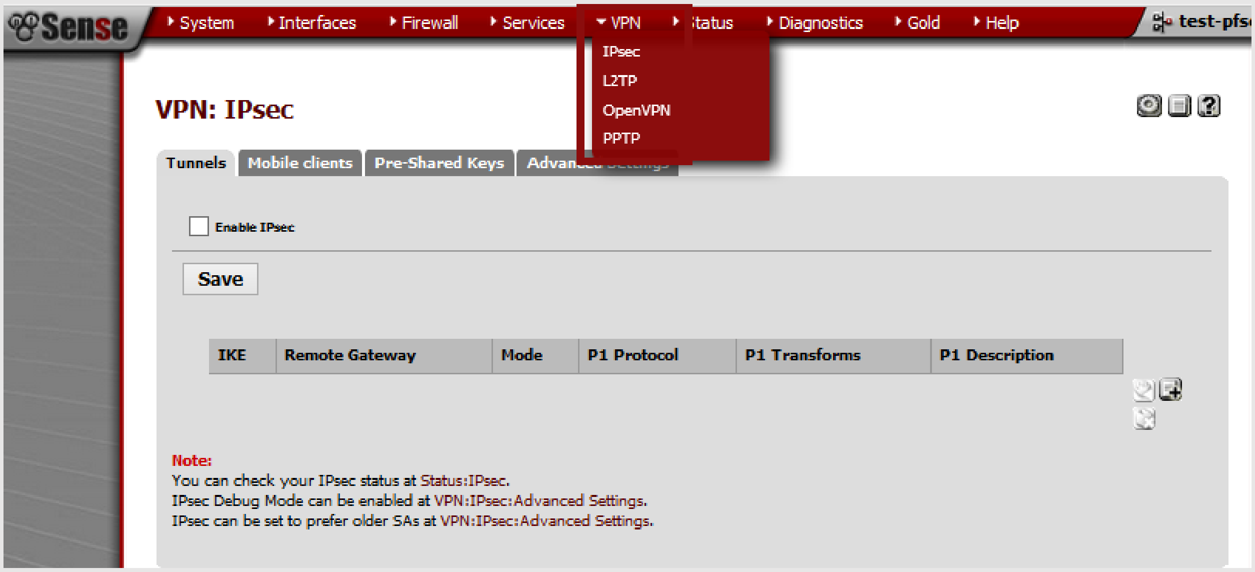
Interface	WAN Choose which interface the host to be woken up is connected to.
MAC address	Enter a MAC address in the following format: xx:xx:xx:xx:xx:xx

Wake all clients at once:
Or Click the MAC address to wake up an individual device:

Interface	MAC address	Description

VPN IPsec

IPsec is a standard for providing security to IP protocols via encryption and/or authentication.



VPN: IPsec

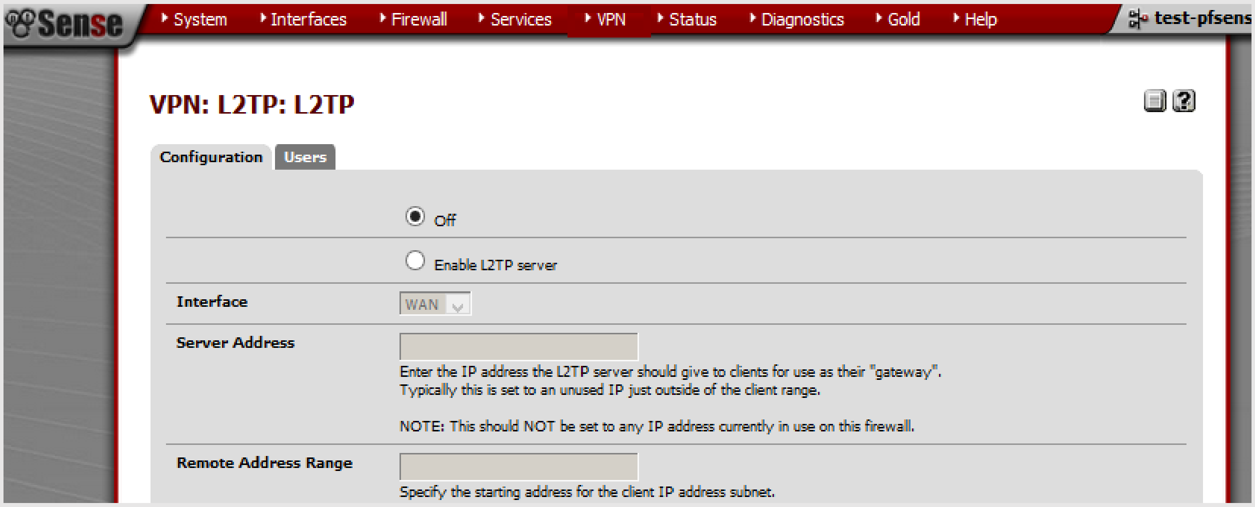
☐ Enable IPsec

IKE	Remote Gateway	Mode	P1 Protocol	P1 Transforms	P1 Description

Note:
You can check your IPsec status at Status:IPsec.
IPsec Debug Mode can be enabled at VPN:IPsec:Advanced Settings.
IPsec can be set to prefer older SAs at VPN:IPsec:Advanced Settings.

L2TP IPsec

L2TP/IPsec is a common VPN type that wraps L2TP, an insecure tunneling protocol, inside a secure channel built using transport mode IPsec.



VPN: L2TP: L2TP

● Off

○ Enable L2TP server

Interface: WAN

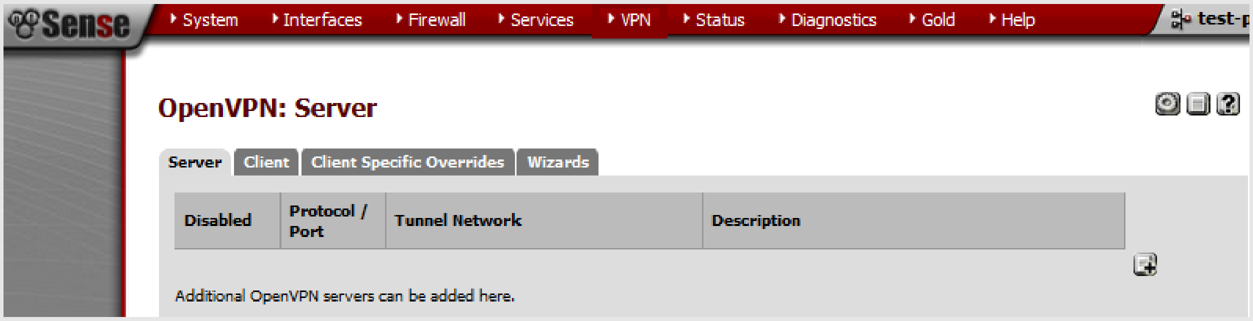
Server Address: Enter the IP address the L2TP server should give to clients for use as their "gateway".
Typically this is set to an unused IP just outside of the client range.

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

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

OpenVPN

OpenVPN is an Open Source VPN server and client that is supported on pfSense.



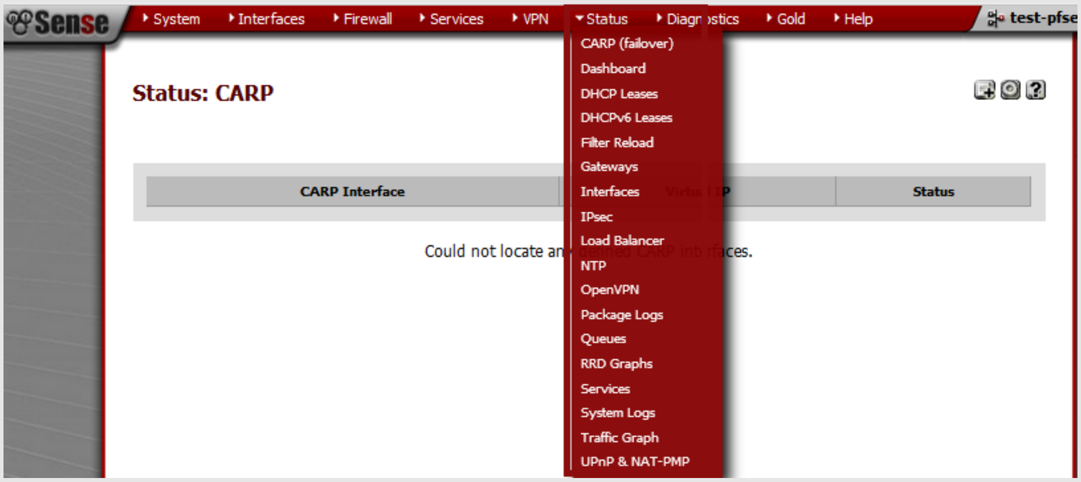
OpenVPN: Server

Disabled	Protocol / Port	Tunnel Network	Description

Additional OpenVPN servers can be added here.

Status Menu

It shows the status of services provided by pfSense such as dhcp server, ipsec and load balancer etc.



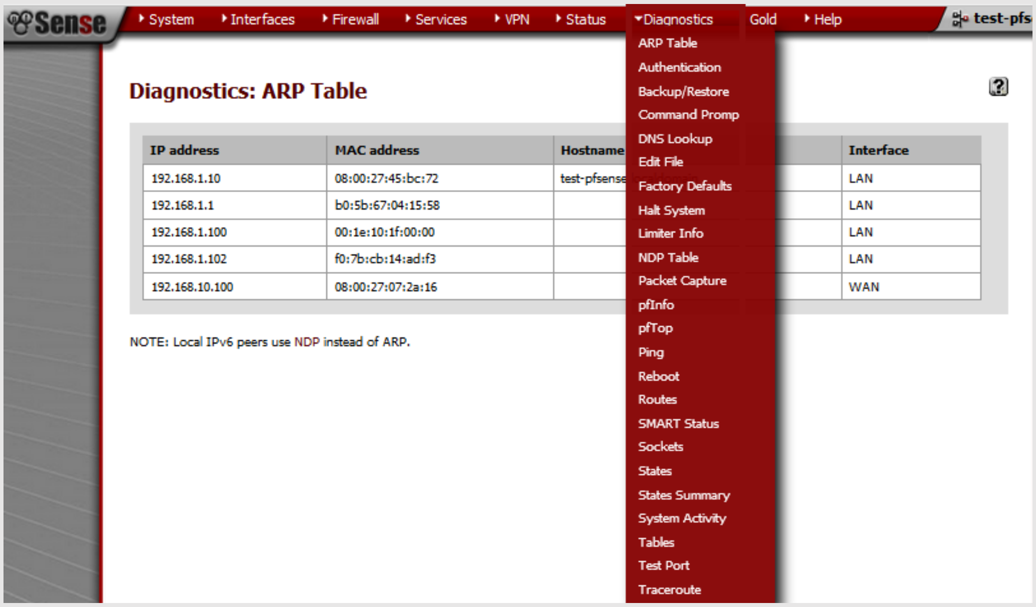
Status: CARP

CARP Interface	Virtual IP	Status

Could not locate any defined CARP interfaces.

Diagnostic Menu

This menu helps administrator/user for the rectification of pfSense issues or problems.

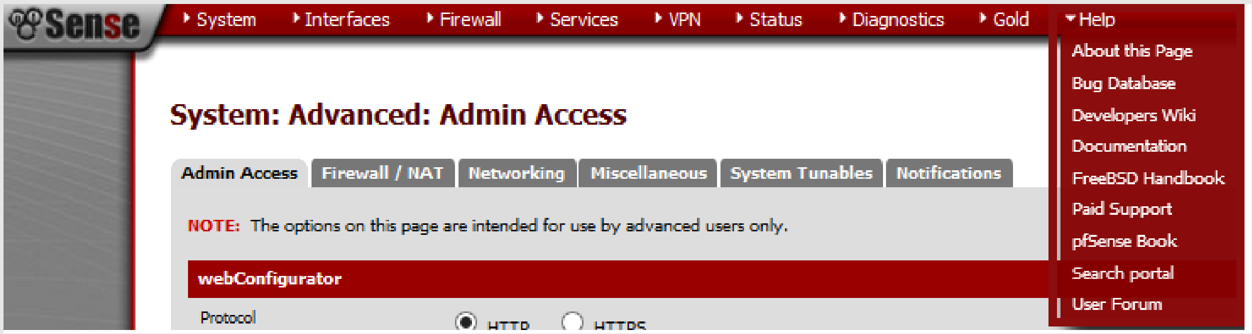


Diagnostics: ARP Table

IP address	MAC address	Hostname	Interface
192.168.1.10	08:00:27:45:bc:72	test-pfsense	LAN
192.168.1.1	b0:5b:67:04:15:58		LAN
192.168.1.100	00:1e:10:1f:00:00		LAN
192.168.1.102	f0:7b:cb:14:ad:f3		LAN
192.168.10.100	08:00:27:07:2a:16		WAN

NOTE: Local IPv6 peers use NDP instead of ARP.

Help Menu



System: Advanced: Admin Access

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

webConfigurator

Protocol ● HTTP ○ HTTPS