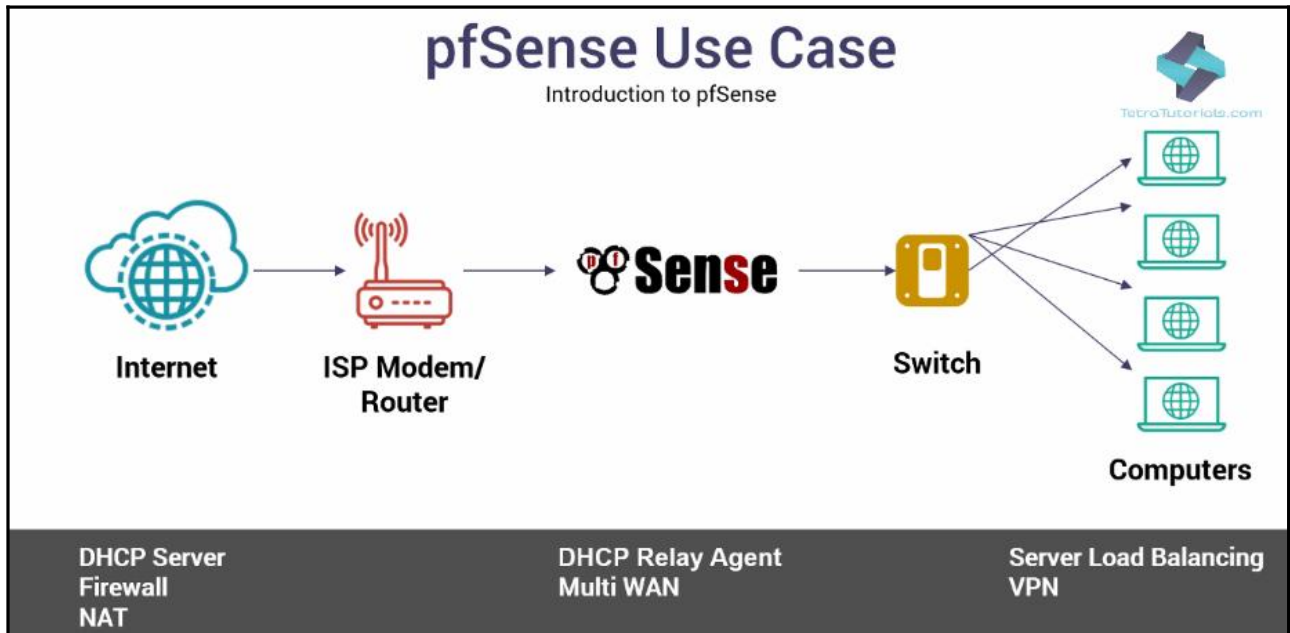
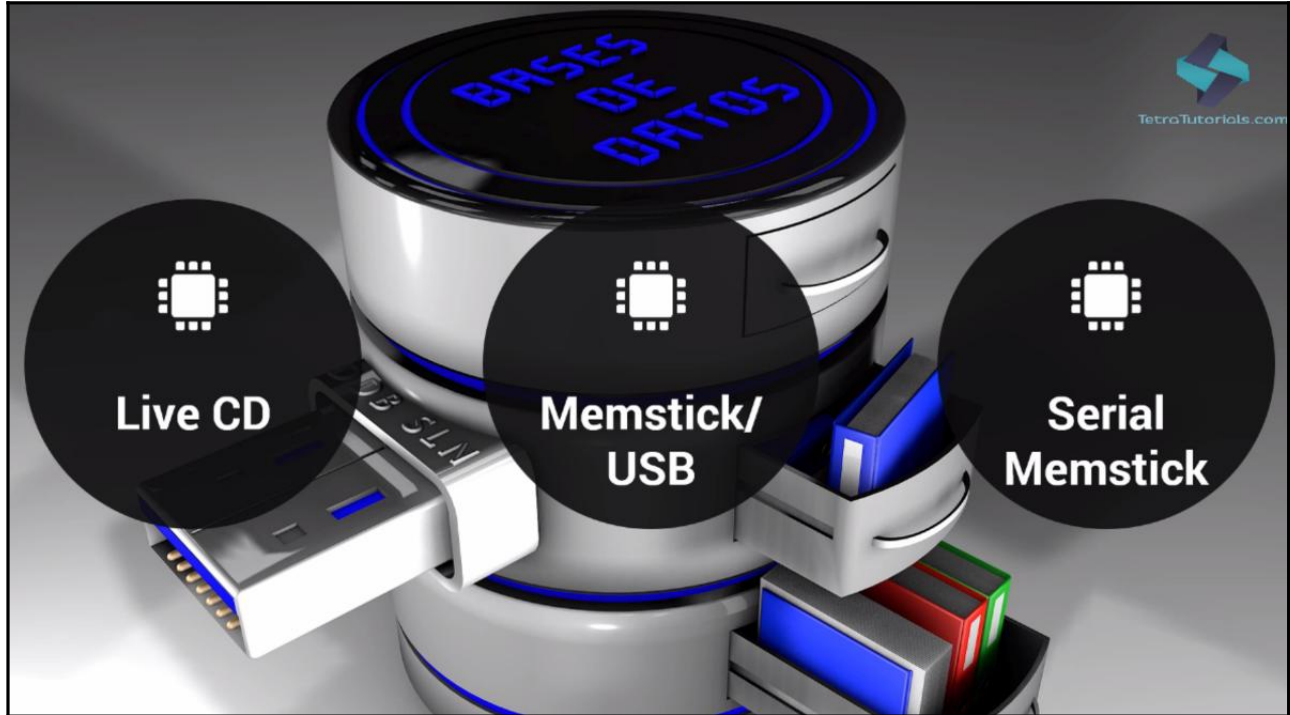


# Chapter 01: Introduction to pfSense



## pfSense Hardware Requirements and Guidance

The following outlines the minimum hardware requirements for pfSense 2.x. Note the minimum requirements are not suitable for all environments. You may be able to get by with less than the minimum, but with less memory you may start swapping to disk, which will dramatically slow down your system.

### General Requirements:

#### Minimum

- CPU - 500 Mhz
- RAM - 512 MB

#### Recommended

- CPU - 1 Ghz
- RAM - 1 GB

### Requirements Specific to Individual Platforms:

#### Full Install

- CD-ROM or USB for initial installation
- 1 GB hard drive

## Hardware Compatibility List

As pfSense is based on FreeBSD, its hardware compatibility list is the same as FreeBSD's. The pfSense kernel includes all FreeBSD drivers.

**PFSENSE 2.4 (FREEBSD 11.1)**

## FreeBSD 11.1-RELEASE Hardware Notes

### The FreeBSD Documentation Project

Copyright © 2000-2017 The FreeBSD Documentation Project

FreeBSD is a registered trademark of the FreeBSD Foundation.

AMD, AMD ATHLON, AMD OPTERON, AMD PHENOM, AMD SEMPRON, AMD TURION, ATHLON, ÉLAN, OPTERON, AND PCNET ARE TRADEMARKS OF ADVANCED MICRO DEVICES, INC.

FUJITSU, THE FUJITSU LOGO, LIFEBOOK, STYLISTIC, PRIMEPOWER, PRIMEQUEST, PRIMECLUSTER, ETERNUS, TRIOLE, ESPRIMO, BioMedCache, Cache, CELLINJECTOR, ISiS, MATERIALS EXPLORER, SYSTEMWALKER, AND INTERSTAGE ARE TRADEMARKS OR REGISTERED TRADEMARKS OF FUJITSU LIMITED IN THE UNITED STATES AND OTHER COUNTRIES.

IBM, AIX, OS/2, POWERPC, PS/2, S/390, AND THINKPAD ARE TRADEMARKS OF INTERNATIONAL BUSINESS MACHINES CORPORATION IN THE UNITED STATES, OTHER COUNTRIES, OR BOTH.

INTEL, CELERON, CENTRINO, CORE, ETHEREXPRESS, i386, i486, ITANIUM, PENTIUM, AND XEON ARE TRADEMARKS OR REGISTERED TRADEMARKS OF INTEL CORPORATION OR ITS SUBSIDIARIES IN THE UNITED STATES AND OTHER COUNTRIES.

SPARC, SPARC64, AND ULTRASPARC ARE TRADEMARKS OF SPARC INTERNATIONAL, INC IN THE UNITED STATES AND OTHER COUNTRIES. SPARC INTERNATIONAL, INC OWNS ALL OF THE SPARC TRADEMARKS AND UNDER LICENSING AGREEMENTS ALLOWS THE PROPER USE OF THESE TRADEMARKS BY ITS MEMBERS.

SUN, SUN MICROSYSTEMS, JAVA, JAVA VIRTUAL MACHINE, JDK, JRE, JSP, JVM, NETRA, OPENJDK, SOLARIS, STAROFFICE, SUNOS AND VIRTUALBOX ARE TRADEMARKS OR REGISTERED TRADEMARKS OF SUN MICROSYSTEMS, INC. IN THE UNITED STATES AND OTHER COUNTRIES.

MANY OF THE DESIGNATIONS USED BY MANUFACTURERS AND SELLERS TO DISTINGUISH THEIR PRODUCTS ARE CLAIMED AS TRADEMARKS. WHERE THOSE DESIGNATIONS APPEAR IN THIS DOCUMENT, AND THE FreeBSD PROJECT WAS AWARE OF THE TRADEMARK CLAIM, THE DESIGNATIONS HAVE BEEN FOLLOWED BY THE "™" OR THE "®" SYMBOL.

Last modified on 2017-06-29 19:38:21 EDT by gjb.

### Table of Contents

#### [1. Introduction](#)

#### [2. Supported Processors and System Boards](#)

##### [2.1. amd64](#)

##### [2.2. i386](#)

##### [2.3. pc98](#)

Download pfSense Community Edition

Secure | <https://www.pfsense.org/download/>

Buy Now | Support Portal | Blog

**pfSense**

Tour | Products | Services | Support | Training | Community | Download

Download Home | Download

### Latest Stable Version (Community Edition)

This is the most recent stable release, and the recommended version for all installations. For upgrade information, see the [Upgrade Guide](#). For pre-configured systems, see the pfSense appliances on [Netgate](#).

[RELEASE NOTES](#) [SOURCE CODE](#)

#### Select Image To Download

Version:

Architecture:

Mirror:

#### Subscribe To The Netgate Newsletter

Product information, software announcements, and special offers. See our [newsletter archive](#) for past announcements.

Email\*

Email Address

## Select Image To Download

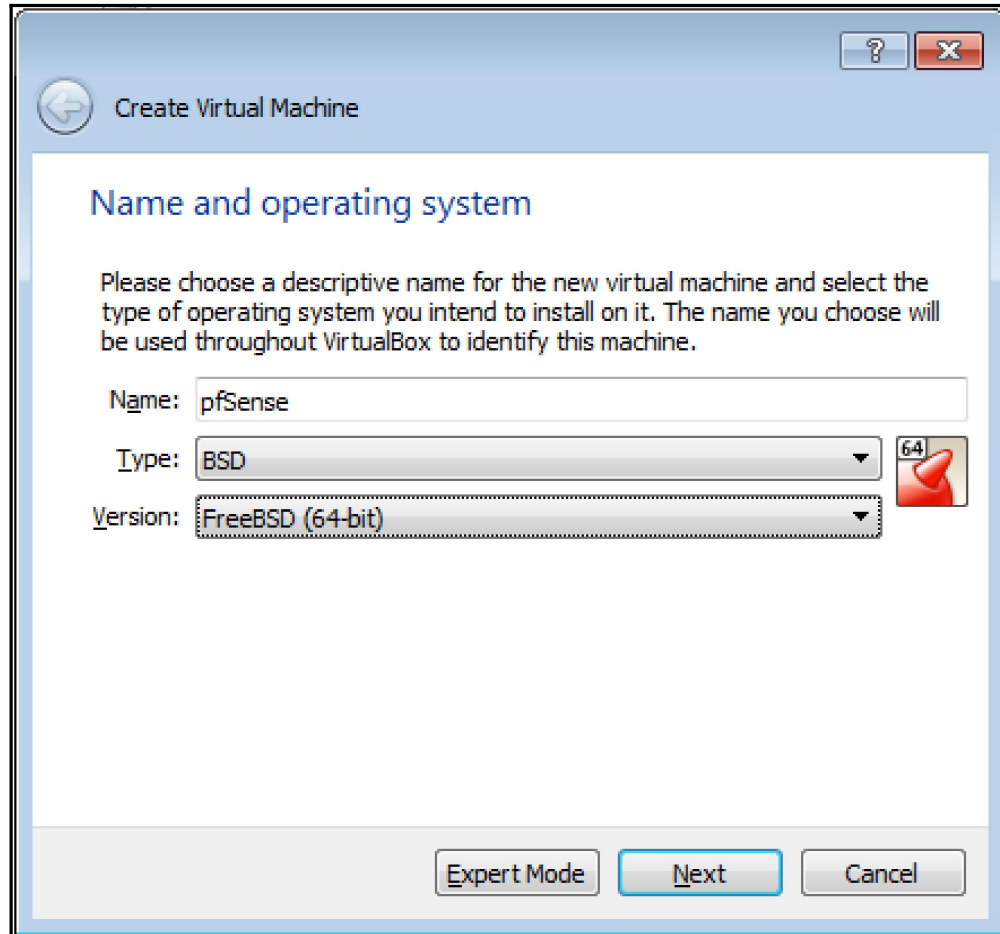
Version:

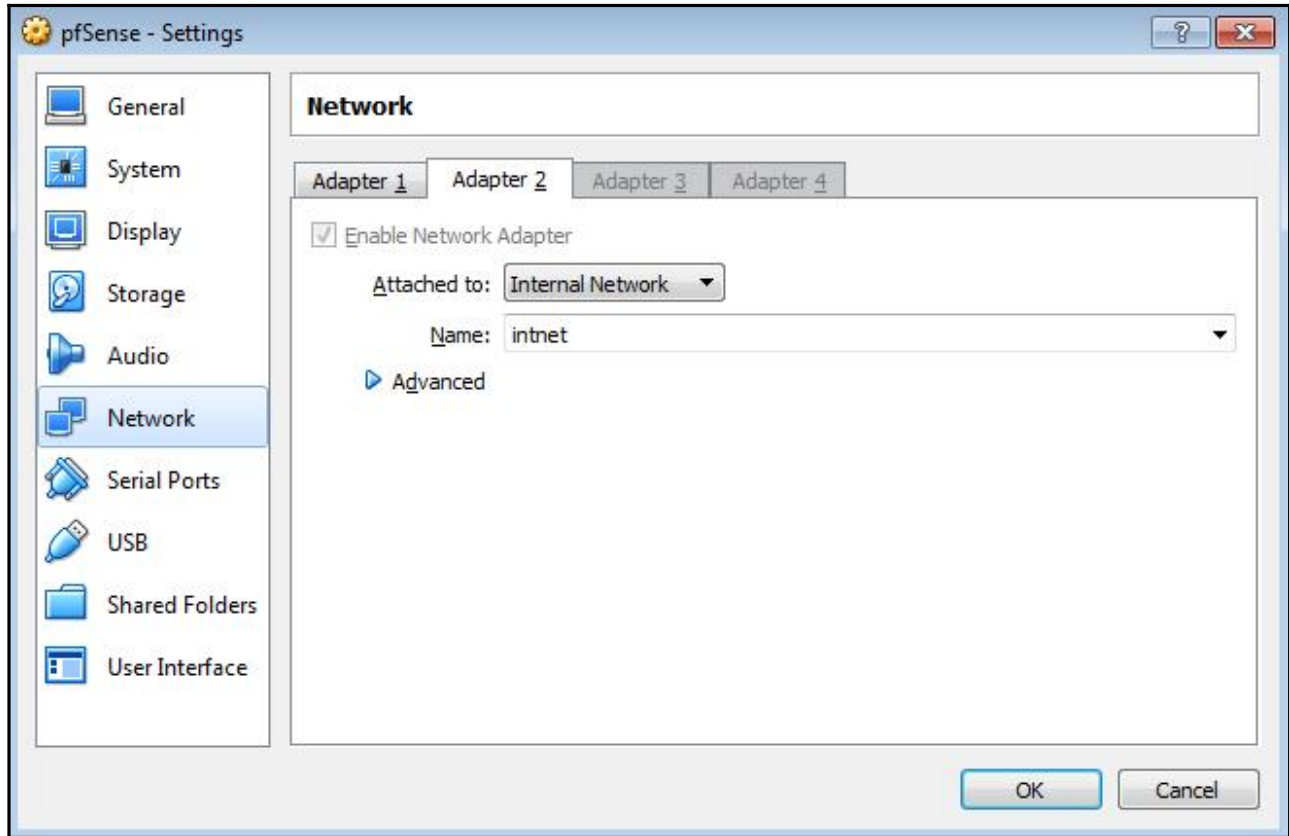
Architecture:

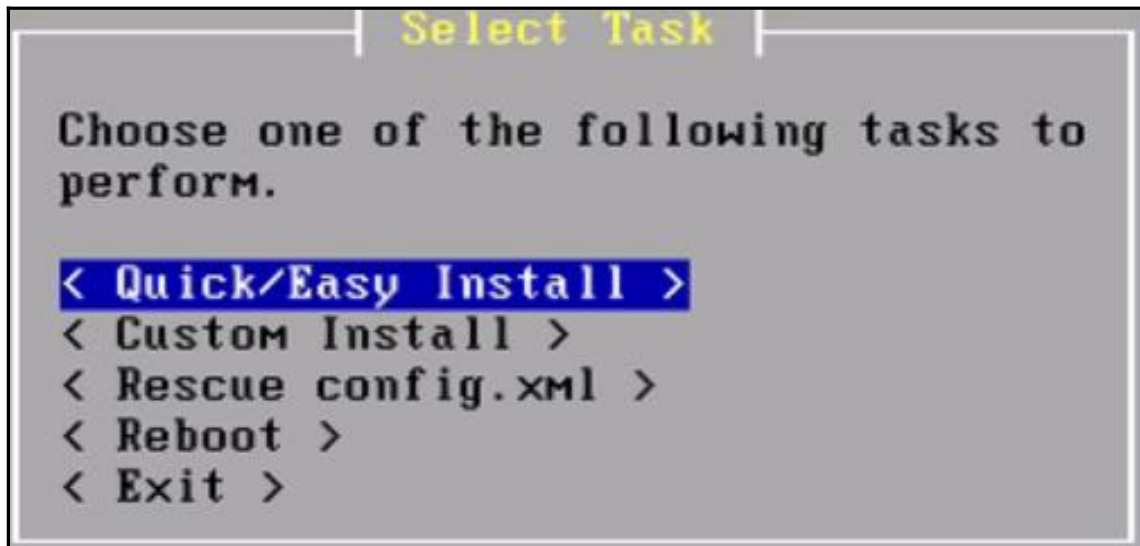
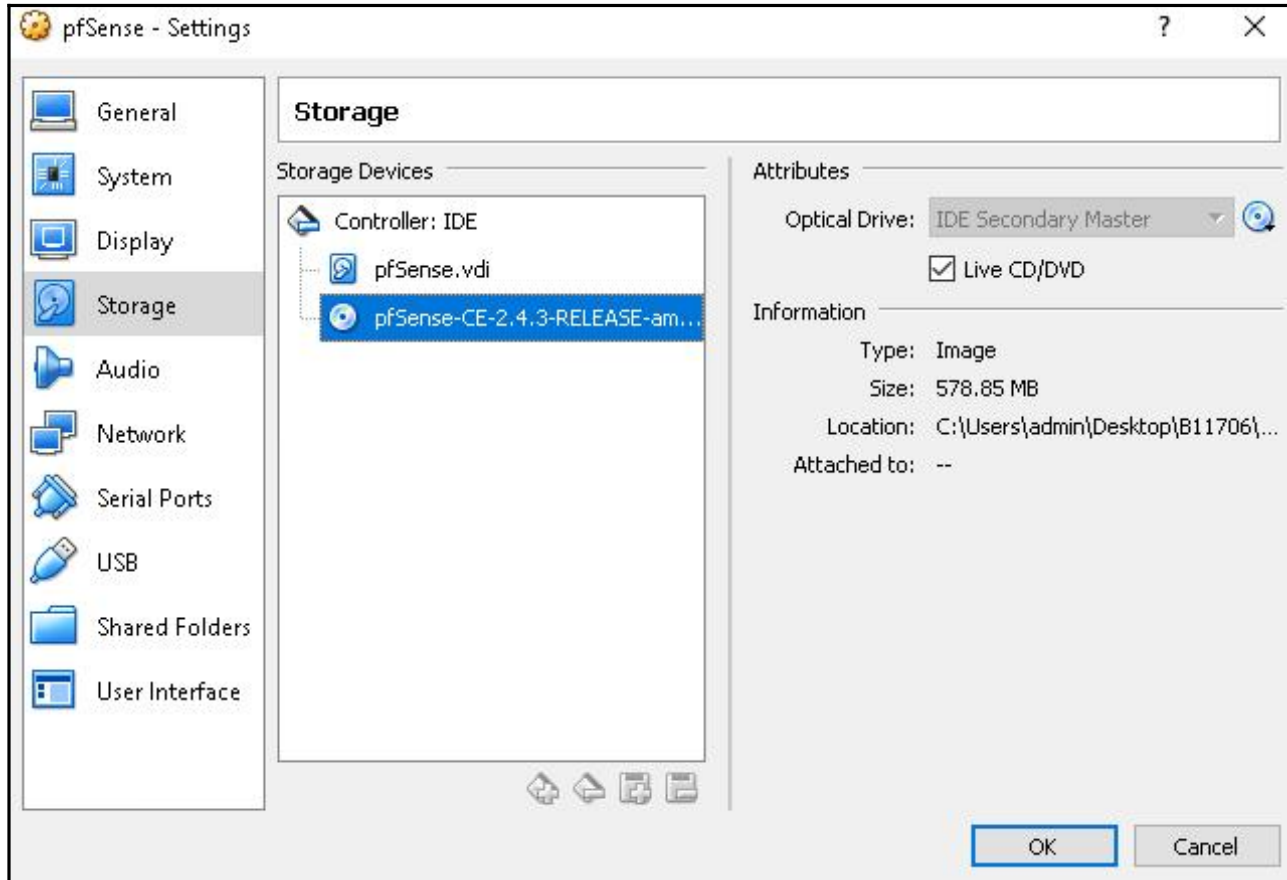
Installer:

Console:

ed by







---

**Install Kernel**

You may now wish to install a custom Kernel configuration.

**< Standard Kernel >**

< Embedded kernel (no UGA console, keyboard) >

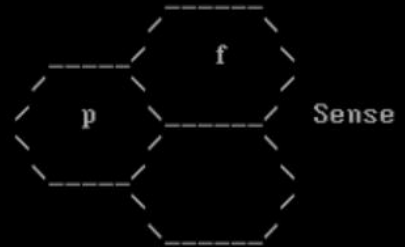
pfSense

Welcome to pfSense

1. Boot Multi User [Enter]
2. Boot [S]ingle User
3. [E]scape to loader prompt
4. Reboot

Options:

5. [K]ernel: kernel (1 of 2)
6. Configure Boot [O]ptions...



Autoboot in 1 seconds. [Space] to pause

<

```
Starting syslog...done.
Starting CRON... done.
pfSense 2.4.3-RELEASE amd64 Mon Mar 26 18:02:04 CDT 2018
Bootup complete

FreeBSD/amd64 (pfSense.localdomain) (ttyv0)

VirtualBox Virtual Machine - Netgate Device ID: 144f98f74a3a1848552f

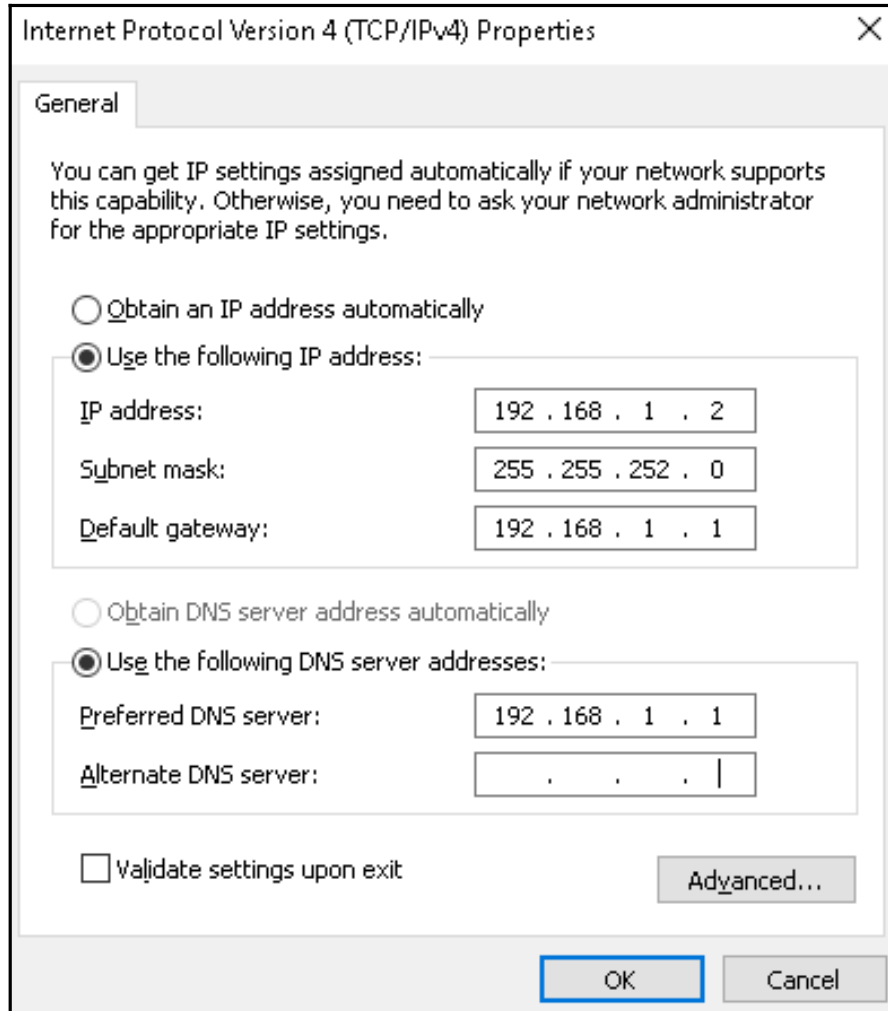
*** Welcome to pfSense 2.4.3-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0          -> v4/DHCP4: 10.0.2.15/24
LAN (lan)     -> em1          -> v4: 192.168.1.1/24

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults  13) Update from console
5) Reboot system             14) Enable Secure Shell (sshd)
6) Halt system               15) Restore recent configuration
7) Ping host                 16) Restart PHP-FPM
8) Shell

Enter an option: █
```





---

```
C:\Users\packt>ping 192.168.1.1 -t
Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Ping statistics for 192.168.1.1:
    Packets: Sent = 17, Received = 17, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
Control-C
^C
C:\Users\packt>
```

---

The screenshot shows the pfSense web interface. At the top, there is a navigation menu with the following items: System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help. The main content area is titled "Wizard / pfSense Setup /" and contains the following text:

**pfSense Setup**

This wizard will provide guidance 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.

[» Next](#)

At the bottom of the page, there is a footer that reads: "pfSense is © 2004 - 2018 by Rubicon Communications, LLC (Netgate). All Rights Reserved. [\[view license\]](#)"



Step 2 of 9

### General Information

On this screen the general pfSense parameters will be set.

**Hostname**

EXAMPLE: myserver

**Domain**

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**

**Secondary DNS Server**

**Override DNS**

Allow DNS servers to be overridden by DHCP/PPP on WAN

» Next

Step 3 of 9

### Time Server Information

Please enter the time, date and time zone.

**Time server  
hostname**

0.pfsense.pool.ntp.org

Enter the hostname (FQDN) of the time server.

**Timezone**

Asia/Kolkata



» Next

Wizard / pfSense Setup / Configure WAN Interface ?

---

Step 4 of 9

### Configure WAN Interface

On this screen the Wide Area Network information will be configured.

**SelectedType**    
  DHCP   
  PPPoE   
  PPTP

#### 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 this field is left blank, an MTU of 1492 bytes for PPPoE and 1500 bytes for all other connection types will be assumed.

**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. If this field is left 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

Wizard / pfSense Setup / Configure LAN Interface ?

---

Step 5 of 9

### Configure LAN Interface

On this screen the Local Area Network information will be configured.

**LAN IP Address**

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

**Subnet Mask**

---

Wizard / pfSense Setup / Set Admin WebGUI Password ?

Step 6 of 9

**Set Admin WebGUI Password**

On this screen the admin password will be set, which is used to access the WebGUI and also SSH services if enabled.

Admin Password

Admin Password AGAIN

[» Next](#)

Wizard / pfSense Setup / Reload configuration ?

Step 7 of 9

**Reload configuration**

Click 'Reload' to reload pfSense with new changes.

[» Reload](#)

Wizard / pfSense Setup / Wizard completed. ?

Step 9 of 9

**Wizard completed.**

Congratulations! pfSense is now configured.

Remember, we're here to help.

Click [here](#) to learn about Netgate 24/7/365 support.

Click [here](#) to continue on to pfSense webConfigurator.

Status / Dashboard + ?

System Information <span style="float: right;">⚙️ - ✕</span>		Interfaces <span style="float: right;">⚙️ - ✕</span>	
<b>Name</b>	pfSense.packtpub.com	<b>WAN</b>	1000baseT <full-duplex> 10.0.2.15
<b>System</b>	VirtualBox Virtual Machine Netgate Device ID: <b>4b8b02a1e6040908dedb</b>	<b>LAN</b>	1000baseT <full-duplex> 192.168.1.1
<b>BIOS</b>	Vendor: <b>innotek GmbH</b> Version: <b>VirtualBox</b> Release Date: <b>Fri Dec 1 2006</b>		
<b>Version</b>	<b>2.4.3-RELEASE</b> (amd64) built on Mon Mar 26 18:02:04 CDT 2018 FreeBSD 11.1-RELEASE-p7  Version <b>2.4.3_1</b> is available. Version information updated at Wed Jul 18 13:35:02 IST 2018		
<b>CPU Type</b>	Intel(R) Core(TM) i5-6400 CPU @ 2.70GHz AES-NI CPU Crypto: Yes (inactive)		
<b>Kernel PTI</b>	Enabled		
<b>Uptime</b>	01 Hour 31 Minutes 56 Seconds		
<b>Current date/time</b>	Wed Jul 18 13:36:05 IST 2018		

```

Message from syslogd@pfSense at Jul 18 08:04:53 ...
pfSense php-fpm[3331]: /index.php: Successful login for user 'admin' from: 192.16
8.1.2
  
```



**pfSense** System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Help ▾ 🔔 1 🏠

COMMUNITY EDITION

System / [Advanced](#) / [Admin Access](#) ?

[Admin Access](#) [Firewall & NAT](#) [Networking](#) [Miscellaneous](#) [System Tunables](#) [Notifications](#)

---

### webConfigurator

<b>Protocol</b>	<input type="radio"/> HTTP	<input checked="" type="radio"/> HTTPS
<b>SSL Certificate</b>	<input type="text" value="webConfigurator default (5b4e319a1fd3b)"/> ▾	
<b>TCP port</b>	<input type="text"/> <small>Enter a custom port number for the webConfigurator above to override the default (80 for HTTP, 443 for HTTPS). Changes will take effect immediately after save.</small>	
<b>Max Processes</b>	<input type="text" value="2"/> <small>Enter the number of webConfigurator processes to run. This defaults to 2. Increasing this will allow more users/browsers to access the GUI concurrently.</small>	
<b>WebGUI redirect</b>	<input type="checkbox"/> Disable webConfigurator redirect rule <small>When this is unchecked, access to the webConfigurator is always permitted even on port 80, regardless of the listening port configured. Check this box to disable this automatically added redirect rule.</small>	
<b>HSTS</b>	<input type="checkbox"/> Disable HTTP Strict Transport Security <small>When this is unchecked, Strict-Transport-Security HTTPS response header is sent by the webConfigurator to the browser. This will force the browser to use only HTTPS for future requests to the firewall FQDN. Check this box to disable HSTS.</small>	

pfSense System Interfaces Firewall Services VPN Status Diagnostics Help

System / System Hostname Domain

- Advanced
- Cert. Manager
- General Setup
- High Avail. Sync
- Logout (admin)
- Package Manager
- Routing
- Setup Wizard
- Update
- User Manager

### DNS Server Settings

<b>DNS Servers</b>	<input type="text" value="8.8.8.8"/>	<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.	

**Add DNS Server**

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

## System / General Setup ?

### 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="8.8.8.8"/>	<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.

**Add DNS Server** + Add DNS Server

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

### 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.

**Certificate** No private CAs found. A private CA is required to create a new user certificate. Save the user first to import an external certificate.

### Keys

**ojsense** System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Help ▾ 🔔 1 🏠

System / **User Manager** / Users ?

[Users](#) [Groups](#) [Settings](#) [Authentication Servers](#)

Users					
	Username	Full name	Status	Groups	Actions
<input type="checkbox"/>	admin	System Administrator	✓	admins	
<input type="checkbox"/>	packt		✓	admins	

**pfSense** System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Help ▾ 🔔 1

System / User Manager / Users / Edit ?

[Users](#) [Groups](#) [Settings](#) [Authentication Servers](#)

### User Properties

**Defined by** SYSTEM

**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**

System / User Manager / Users ?

[Users](#) [Groups](#) [Settings](#) [Authentication Servers](#)

### Users

	Username	Full name	Status	Groups	Actions
<input type="checkbox"/>	admin	System Administrator	🚫	admins	
<input type="checkbox"/>	packt		✓	admins	

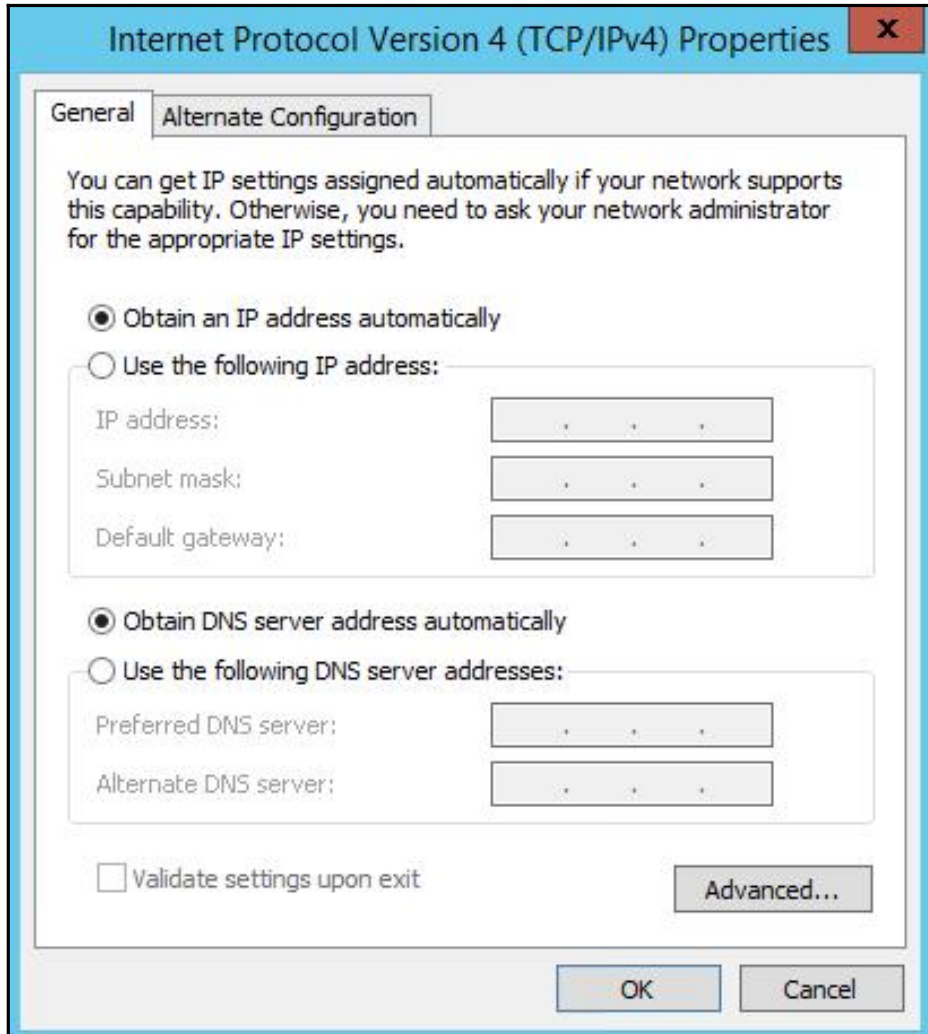
+ Add
🗑 Delete

## 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. This option is not compatible with failover and cannot be enabled when a Failover Peer IP address is configured.
<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. 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.
<b>Subnet</b>	192.168.1.0
<b>Subnet mask</b>	255.255.255.0
<b>Available range</b>	192.168.1.1 - 192.168.1.254
<b>Range</b>	<input type="text" value="192.168.1.100"/> <input type="text" value="192.168.1.199"/>
	From To

---

Servers	
<b>WINS servers</b>	<input type="text" value="WINS Server 1"/>
	<input type="text" value="WINS Server 2"/>
<b>DNS servers</b>	<input type="text" value="192.168.1.1"/>
	<input type="text" value="DNS Server 2"/>
	<input type="text" value="DNS Server 3"/>
	<input type="text" value="DNS Server 4"/>
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.	
Other Options	
<b>Gateway</b>	<input type="text" value="192.168.1.1"/>
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.	
<b>Domain name</b>	<input type="text" value="packtpub.com"/>
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.	
<b>Domain search list</b>	<input type="text"/>
The DHCP server can optionally provide a domain search list. Use the semicolon character as separator.	





```
Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

    Connection-specific DNS Suffix  . : packtpub.com
    Link-local IPv6 Address . . . . . : fe80::f91d:3491:2d51:e158%12
    IPv4 Address. . . . . : 192.168.1.100
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : fe80::1:1%12
                                192.168.1.1

Tunnel adapter isatap.packtpub.com:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : packtpub.com

C:\Users\Administrator>
```

```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\packt>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : packtpub.com
    Link-local IPv6 Address . . . . . : fe80::780c:d57c:aef3:2b13%11
    IPv4 Address. . . . . : 192.168.1.101
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : fe80::1:1%11
                                192.168.1.1
























Tunnel adapter isatap.packtpub.com:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : packtpub.com

C:\Users\packt>
```























Status / Services ?







**Services**

Service	Description	Status	Actions
dhcpcd	DHCP Service	✓	    
dpinger	Gateway Monitoring Daemon	✓	    
ntpd	NTP clock sync	✓	    
syslogd	System Logger Daemon	✓	   
unbound	DNS Resolver	✓	   





Status / Services ?

**Services**

Service	Description	Status	Actions
dhcpcd	DHCP Service	✗	   
dpinger	Gateway Monitoring Daemon	✓	    
ntpd	NTP clock sync	✓	    
syslogd	System Logger Daemon	✓	   
unbound	DNS Resolver	✓	   


Status / DHCP Leases      

**Leases**

	IP address	MAC address	Hostname	Description	Start	End	Online	Lease Type	Actions
✓	192.168.1.101	08:00:27:83:b9:21	packt-PC		2018/07/18 11:31:34	2018/07/18 13:31:34	online	active	 
✓	192.168.1.100	08:00:27:ff:a2:36	WIN-K9084G6EDIO		2018/07/18 10:54:30	2018/07/18 12:54:30	online	active	 

**Leases in Use**

Interface	Pool Start	Pool End	# of leases in use
LAN	192.168.1.100	192.168.1.199	2

 Show all configured leases

```

C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\packt>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : packtpub.com
    Link-local IPv6 Address . . . . . : fe80::780c:d57c:aef3:2b13%11
    IPv4 Address. . . . . : 192.168.1.101
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : fe80::1:1%11
                                192.168.1.1

Tunnel adapter isatap.packtpub.com:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : packtpub.com

C:\Users\packt>

```



Status / DHCP Leases ▶ ⚙ 📊 📄 ?

Leases									
	IP address	MAC address	Hostname	Description	Start	End	Online	Lease Type	Actions
☑	192.168.1.101	08:00:27:83:b9:21	packt-PC		2018/07/18 11:31:34	2018/07/18 13:31:34	online	active	⊞ ⊕
☑	192.168.1.100	08:00:27:ff:a2:36	WIN- K9084G6EDIO		2018/07/18 10:54:30	2018/07/18 12:54:30	online	active	⊞ ⊕

Leases in Use			
Interface	Pool Start	Pool End	# of leases in use
LAN	192.168.1.100	192.168.1.199	2

⊞ Show all configured leases

```
C:\Users\packt>ipconfig /all
```

```
Windows IP Configuration
```

```
Host Name . . . . . : packt-PC
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : packtpub.com
```

```
Ethernet adapter Local Area Connection:
```

```
Connection-specific DNS Suffix . : packtpub.com
Description . . . . . : Intel(R) PRO/1000 MT Desktop Adapter
Physical Address. . . . . : 08-00-27-83-B9-21
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::780c:d57c:aef3:2b13%11(Preferred)
IPv4 Address. . . . . : 192.168.1.101(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : 18 July 2018 17:07:27
Lease Expires . . . . . : 18 July 2018 19:01:35
Default Gateway . . . . . : fe80::1:1%11
                          192.168.1.1
DHCP Server . . . . . : 192.168.1.1
DHCPv6 IAID . . . . . : 235405351
DHCPv6 Client DUID. . . . . : 00-01-00-01-22-E0-DC-5A-08-00-27-83-B9-21

DNS Servers . . . . . : 192.168.1.1
NetBIOS over Tcpip. . . . . : Enabled
```

```
Tunnel adapter isatap.packtpub.com:
```

```
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . : packtpub.com
Description . . . . . : Microsoft ISATAP Adapter
Physical Address. . . . . : 00-00-00-00-00-00-00-00-E0
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes
```

Control Panel > System and Security > System

Search Control Panel

Control Panel Home

- Device Manager
- Remote settings
- System protection
- Advanced system settings


See also

- Action Center
- Windows Update
- Performance Information and Tools

### View basic information about your computer

**Windows edition**

Windows 7 Professional  
Copyright © 2009 Microsoft Corporation. All rights reserved.  
Service Pack 1  
[Get more features with a new edition of Windows 7](#)



**System**

Rating: [System rating is not available](#)

Processor: Intel(R) Core(TM) i5-6400 CPU @ 2.70GHz 2.71 GHz

Installed memory (RAM): 1.00 GB

System type: 64-bit Operating System

Pen and Touch: No Pen or Touch Input is available for this Display

**Computer name, domain, and workgroup settings**

Computer name: packt-PC [Change settings](#)

Full computer name: packt-PC

Computer description:

Workgroup: WORKGROUP

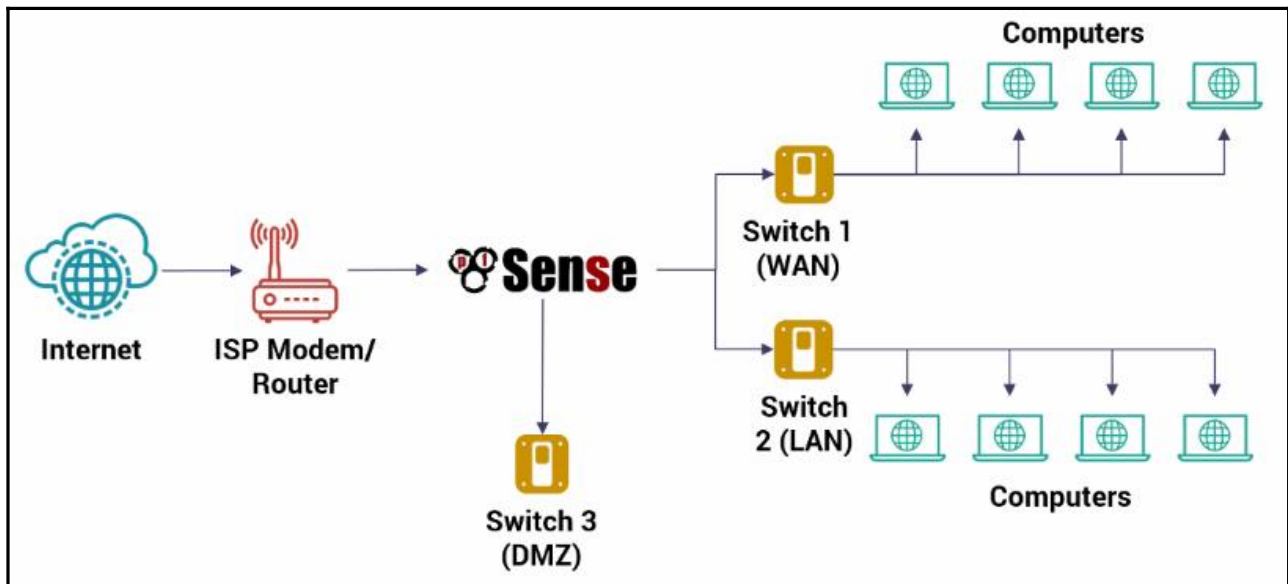
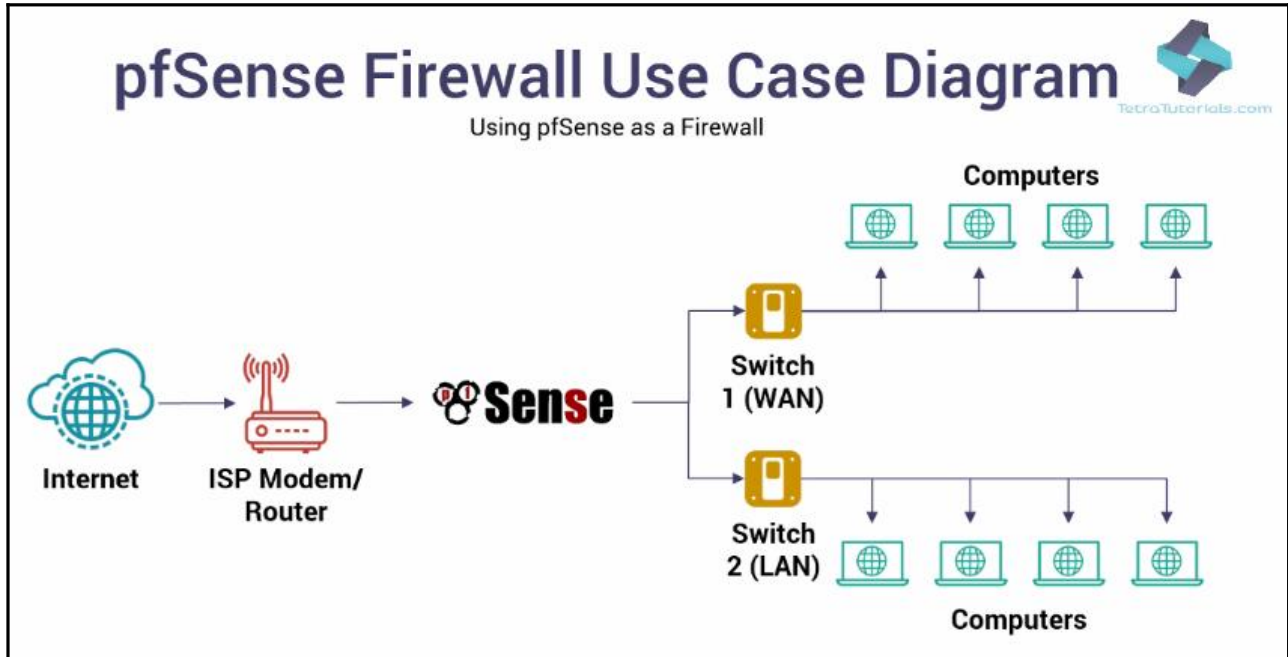
Last 50 DHCP Log Entries. (Maximum 50)

Time	Process	PID	Message
Jul 18 14:54:58	dhcpcd		For info, please visit <a href="https://www.isc.org/software/dhcp/">https://www.isc.org/software/dhcp/</a>
Jul 18 14:54:58	dhcpcd		Config file: /etc/dhcpcd.conf
Jul 18 14:54:58	dhcpcd		Database file: /var/db/dhcpcd.leases
Jul 18 14:54:58	dhcpcd		PID file: /var/run/dhcpcd.pid
Jul 18 14:54:58	dhcpcd		Internet Systems Consortium DHCP Server 4.3.6-P1
Jul 18 14:54:58	dhcpcd		Copyright 2004-2018 Internet Systems Consortium.
Jul 18 14:54:58	dhcpcd		All rights reserved.
Jul 18 14:54:58	dhcpcd		For info, please visit <a href="https://www.isc.org/software/dhcp/">https://www.isc.org/software/dhcp/</a>
Jul 18 14:54:58	dhcpcd		Wrote 1 leases to leases file.
Jul 18 14:54:58	dhcpcd		Listening on BPF/em1/08:00:27:69:28:67/192.168.1.0/24
Jul 18 14:54:58	dhcpcd		Sending on BPF/em1/08:00:27:69:28:67/192.168.1.0/24
Jul 18 14:54:58	dhcpcd		Sending on Socket/fallback/fallback-net

Jul 18 17:01:34 dhcpcd DHCPOFFER on 192.168.1.101 to 08:00:27:83:b9:21 (packt-PC) via em1

Jul 18 17:01:34 dhcpcd DHCPACK on 192.168.1.101 to 08:00:27:83:b9:21 (packt-PC) via em1

# Chapter 02: pfSense as a Firewall



Status / Dashboard + ?

System Information <span style="float: right;">⚙️ - ✕</span>		Interfaces <span style="float: right;">⚙️ - ✕</span>	
<b>Name</b>	pfSense.pactpub.com	<b>WAN</b>	1000baseT <full-duplex> 10.0.2.15
<b>System</b>	VirtualBox Virtual Machine Netgate Device ID: 9e6eeb2755c53e6da6b9	<b>LAN1</b>	1000baseT <full-duplex> 192.168.1.1
<b>BIOS</b>	Vendor: innotek GmbH Version: VirtualBox Release Date: Fri Dec 1 2006	<b>LAN2</b>	1000baseT <full-duplex> 198.168.2.1
<b>Version</b>	2.4.3-RELEASE (amd64) built on Mon Mar 26 18:02:04 CDT 2018 FreeBSD 11.1-RELEASE-p7  Version 2.4.3_1 is available. Version information updated at Fri Jul 20 14:03:08 IST 2018		
<b>CPU Type</b>	Intel(R) Core(TM) i5-6400 CPU @ 2.70GHz AES-NI CPU Crypto: Yes (inactive)		
<b>Kernel PTI</b>	Enabled		
<b>Uptime</b>	03 Hours 10 Minutes 43 Seconds		
<b>Current date/time</b>	Fri Jul 20 14:17:05 IST 2018		

### 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: xx:xx:xx:xx: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.





### webConfigurator

Protocol

HTTP

HTTPS

SSL Certificate

webConfigurator default (5b50e8520e3f2)

TCP port

Enter a custom port number for the webConfigurator above to override the default (80 for HTTP, 443 for HTTPS). Changes will take effect immediately after save.

Max Processes

Enter the number of webConfigurator processes to run. This defaults to 2. Increasing this will allow more users/browsers to access the GUI concurrently.

WebGUI redirect

Disable webConfigurator redirect rule

When this is unchecked, access to the webConfigurator is always permitted even on port 80, regardless of the listening port configured. Check this box to disable this automatically added redirect rule.

HSTS

Disable HTTP Strict Transport Security

When this is unchecked, Strict-Transport-Security HTTPS response header is sent by the webConfigurator to the browser. This will force the browser to use only HTTPS for future requests to the firewall FQDN. Check this box to disable HSTS.

System / [Advanced](#) / [Firewall & NAT](#) ?

Admin Access [Firewall & NAT](#) [Networking](#) [Miscellaneous](#) [System Tunables](#) [Notifications](#)

### Firewall Advanced

**IP Do-Not-Fragment compatibility**  Clear invalid DF bits instead of dropping the packets  
 This allows for communications with hosts that generate fragmented packets with the don't fragment (DF) bit set. Linux NFS is known to do this. This will cause the filter to not drop such packets but instead clear the don't fragment bit.

**IP Random id generation**  Insert a stronger ID into IP header of packets passing through the filter.  
 Replaces the IP identification field of packets with random values to compensate for operating systems that use predictable values. This option only applies to packets that are not fragmented after the optional packet reassembly.

**Firewall Optimization Options**  ▼  
 The default optimization algorithm

**Disable Firewall**  Disable all packet filtering.  
 Note: This converts pfSense into a routing only platform!  
 Note: This will also turn off NAT! To only disable NAT, and not firewall rules, visit the [Outbound NAT](#) page.

**Disable Firewall Scrub**  Disables the PF scrubbing option which can sometimes interfere with NFS traffic.

Firewall / [Rules](#) / [WAN](#) 📊 📄 ?

Floating [WAN](#) [LAN1](#) [LAN2](#)

### Rules (Drag to Change Order)

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✘ 0 / 3 KiB	*	RFC 1918 networks	*	*	*	*	*		Block private networks	⚙️
✘ 0 / 0 B	*	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 pass rules are added. Click the button to add a new rule.

Firewall / Rules / LAN1 ☰ | 📊 | 📄 | ?

Floating WAN LAN1 LAN2

**Rules (Drag to Change Order)**

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	1 / 34.83 MiB	*	*	*	LAN1 Address	443	*	*		Anti-Lockout Rule	⚙️
<input type="checkbox"/>	0 / 45 KiB	IPv4 *	LAN1 net	*	*	*	*	none		Default allow LAN to any rule	📌   ✎   📄   🚫
<input type="checkbox"/>	0 / 0 B	IPv6 *	LAN1 net	*	*	*	*	none		Default allow LAN IPv6 to any rule	📌   ✎   📄   🚫

⬆️ Add
⬇️ Add
🗑️ Delete
💾 Save
➕ Separator



Firewall / Rules / LAN1 ☰ | 📊 | 📄 | ?

The changes have been applied successfully. The firewall rules are now reloading in the background. ✕

[Monitor](#) the filter reload progress.

```
C:\Windows\system32\cmd.exe - ping 192.168.1.1 -t
Tunnel adapter isatap.packtpub.com:
    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  : packtpub.com
C:\Users\packt>ping 192.168.1.1 -t
Pinging 192.168.1.1 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
-
```

```
C:\Windows\system32\cmd.exe - ping 192.168.1.1 -t
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
```

```

C:\Windows\system32\cmd.exe - ping 192.168.1.1 -t
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Request timed out.
Request timed out.

```

Firewall / Rules / LAN1 ≡ | 📊 | 📄 | ?

Floating WAN LAN1 LAN2

**Rules (Drag to Change Order)**

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✓ 0 / 35.72 MiB	*	*	*	LAN1 Address	443 80	*	*		Anti-Lockout Rule	⚙️

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

⬆️ Add
⬇️ Add
🗑️ Delete
💾 Save
➕ Separator

ℹ️

### 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.

**ICMP Subtypes**  ▼

- any
- Alternate Host
- Datagram conversion error
- Echo reply

For ICMP rules on IPv4, one or more of these ICMP subtypes may be specified.

**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.  ▼  /  ▼

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**.

**Source Port Range**  ▼  Custom  ▼  Custom

From Custom To Custom

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

Floating WAN LAN1 LAN2

---

### Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	0 / 35.98 MiB	*	*	*	LAN1 Address	443	*	*		Anti-Lockout Rule	
<input type="checkbox"/>	0 / 0 B	IPv4 TCP/UDP	LAN1 net	80 (HTTP)	*	*	*	none			 
<input type="checkbox"/>	0 / 0 B	IPv4 ICMP any	LAN1 net	*	*	*	*	none			 
<input type="checkbox"/>	0 / 0 B	IPv4 TCP/UDP	LAN1 net	21 (FTP)	*	*	*	none			 

```
C:\Windows\system32\cmd.exe - ping 192.168.1.1 -t
```

```
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
```

```

C:\Windows\system32\cmd.exe - ping 192.168.1.1 -t
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64

```

Floating WAN LAN1 LAN2

**Rules (Drag to Change Order)**

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✓ 0 / 35.98 MiB	*	*	*	LAN1 Address	443	*	*		Anti-Lockout Rule	
☐ ✓ 0 / 8 KIB	IPv4 ICMP any	LAN1 net	*	*	*	*	none			
☐ ✓ 0 / 0 B	IPv4 TCP/UDP	LAN1 net	53 (DNS)	*	*	*	none			
☐ ✓ 0 / 0 B	IPv4 TCP/UDP	LAN1 net	80 (HTTP)	*	*	*	none			
☐ ✓ 0 / 0 B	IPv4 TCP/UDP	LAN1 net	443 (HTTPS)	*	*	*	none			

Add
 Add
 Delete
 Save
 Separator



Floating WAN LAN1 **LAN2**

**Rules (Drag to Change Order)**

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓ 0 / 0 B	IPv4 ICMP any	LAN2 net	*	*	*	*	none			
<input type="checkbox"/>	✓ 0 / 0 B	IPv4 TCP/UDP	LAN2 net	53 (DNS)	*	*	*	none			

Add
 Add
 Delete
 Save
 Separator

Floating WAN LAN1 **LAN2**

**Rules (Drag to Change Order)**

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
	✓ 2 / 36.09 MiB	*	*	*	LAN1 Address	443 80	*	*		Anti-Lockout Rule	
<input type="checkbox"/>	0 / 0 B	IPv4 TCP/UDP	LAN1 net	*	LAN2 net	*	*	none			
<input type="checkbox"/>	✓ 0 / 8 KiB	IPv4 ICMP any	LAN1 net	*	*	*	*	none			
<input type="checkbox"/>	✓ 0 / 0 B	IPv4 TCP/UDP	LAN1 net	53 (DNS)	*	*	*	none			
<input type="checkbox"/>	✓ 0 / 0 B	IPv4 TCP/UDP	LAN1 net	80 (HTTP)	*	*	*	none			
<input type="checkbox"/>	✓ 0 / 0 B	IPv4 TCP/UDP	LAN1 net	443 (HTTPS)	*	*	*	none			

Add
 Add
 Delete
 Save
 Separator

Floating WAN LAN1 LAN2

Rules (Drag to Change Order)

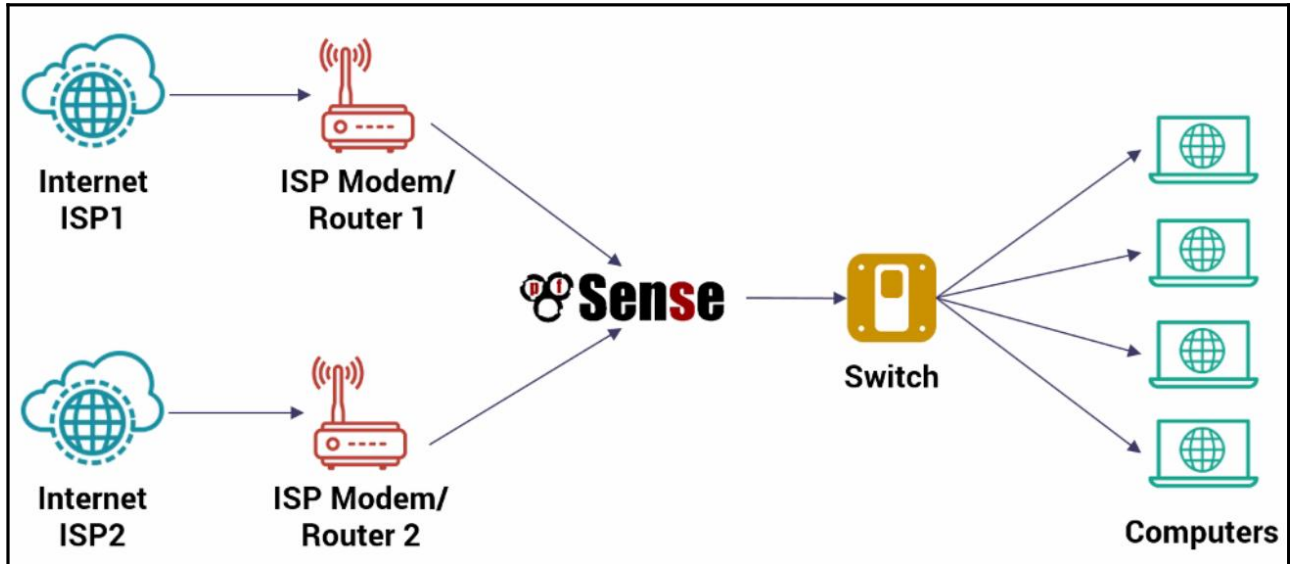
	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>		0 / 0 B	IPv4 *	LAN2 net	*	LAN1 net	* *	none			
<input type="checkbox"/>		0 / 0 B	IPv4 ICMP any	LAN2 net	*	*	* *	none			
<input type="checkbox"/>		0 / 0 B	IPv4 TCP/UDP	LAN2 net	53 (DNS)	*	* *	none			
<input type="checkbox"/>		0 / 0 B	IPv4 TCP/UDP	LAN2 net	80 (HTTP)	*	* *	none			

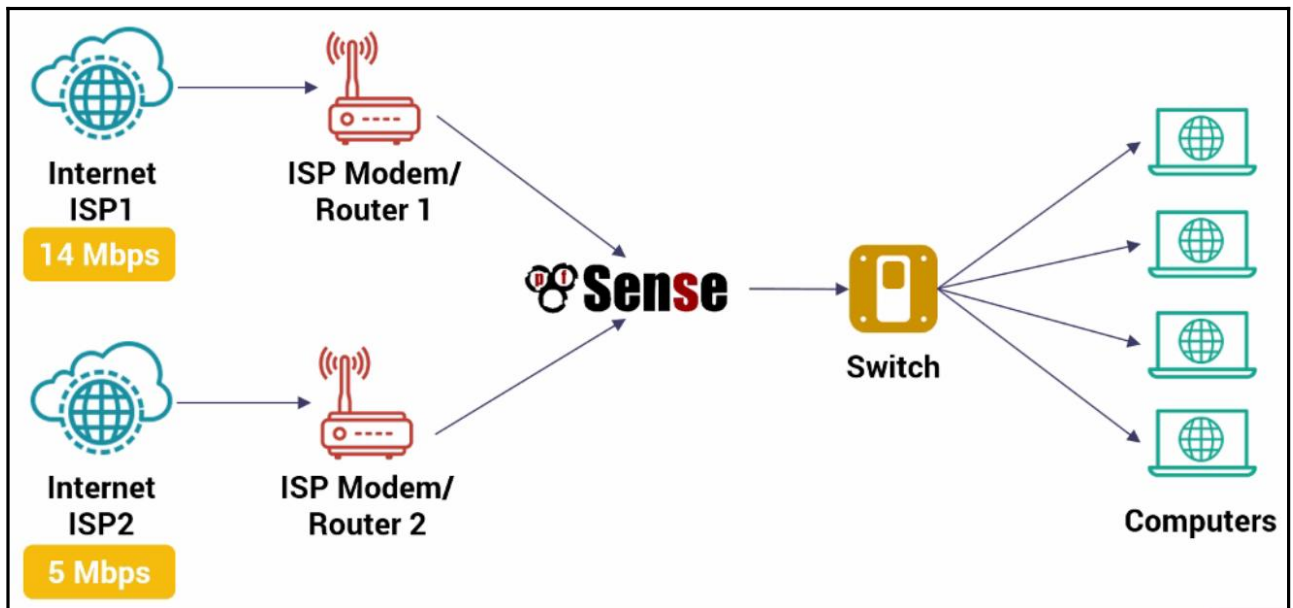
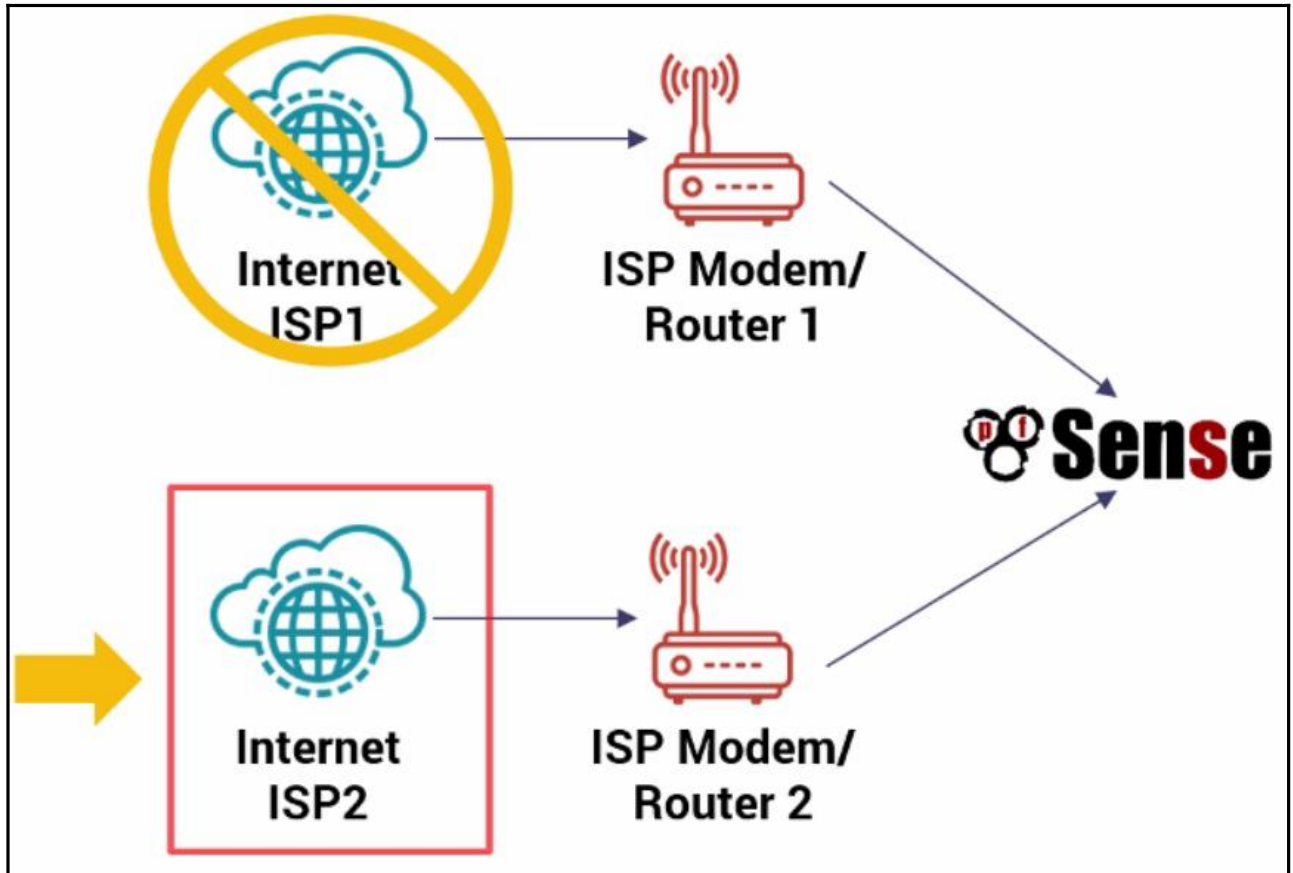
Add Add Delete Save Separator

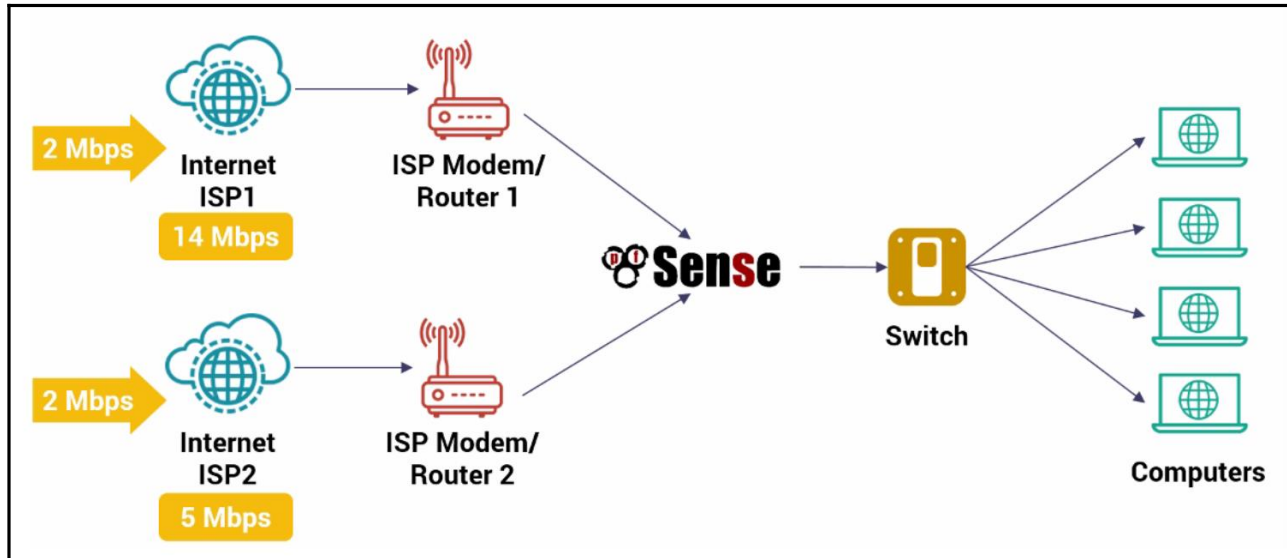
<input type="checkbox"/>		0 / 0 B	IPv4 TCP/UDP	LAN1 net	443 (HTTPS)	*	* *	none			
--------------------------	--	---------	-----------------	-------------	----------------	---	-----	------	--	--	--

---

# Chapter 03: pfSense as a Failover and Load Balancer







Enter an option: restart

\VirtualBox Virtual Machine - Netgate Device ID: 9e6eeb2755c53e6da6b9

\*\*\* Welcome to pfSense 2.4.3-RELEASE (amd64) on pfSense \*\*\*

WAN (wan)	-> em0	-> v4/DHCP4: 10.0.2.15/24
LAN1 (lan)	-> em1	-> v4: 192.168.1.1/24
WAN2 (opt1)	-> em2	-> v4/DHCP4: 192.168.1.103/24

- |                                   |                                  |
|-----------------------------------|----------------------------------|
| 0) Logout (SSH only)              | 9) pfTop                         |
| 1) Assign Interfaces              | 10) Filter Logs                  |
| 2) Set interface(s) IP address    | 11) Restart webConfigurator      |
| 3) Reset webConfigurator password | 12) PHP shell + pfSense tools    |
| 4) Reset to factory defaults      | 13) Update from console          |
| 5) Reboot system                  | 14) Enable Secure Shell (sshd)   |
| 6) Halt system                    | 15) Restore recent configuration |
| 7) Ping host                      | 16) Restart PHP-FPM              |
| 8) Shell                          |                                  |

Enter an option: █

Status / Dashboard + ?

System Information <span style="float: right;">⚙️ - ✕</span>		Interfaces <span style="float: right;">⚙️ - ✕</span>	
<b>Name</b>	pfSense.packtpub.com	<b>WAN</b> <span style="color: green;">↑</span>	1000baseT <full-duplex> 10.0.2.15
<b>System</b>	VirtualBox Virtual Machine Netgate Device ID: <b>9e6eeb2755c53e6da6b9</b>	<b>LAN1</b> <span style="color: green;">↑</span>	1000baseT <full-duplex> 192.168.1.1
<b>BIOS</b>	Vendor: <b>innotek GmbH</b> Version: <b>VirtualBox</b> Release Date: <b>Fri Dec 1 2006</b>	<b>WAN2</b> <span style="color: green;">↑</span>	1000baseT <full-duplex> 192.168.1.103
<b>Version</b>	<b>2.4.3-RELEASE</b> (amd64) built on Mon Mar 26 18:02:04 CDT 2018 FreeBSD 11.1-RELEASE-p7  Version <b>2.4.3_1</b> is available. <a href="#">⬇️</a> Version information updated at Fri Jul 20 18:33:20 IST 2018 <a href="#">🔄</a>		
<b>CPU Type</b>	Intel(R) Core(TM) i5-6400 CPU @ 2.70GHz AES-NI CPU Crypto: Yes (inactive)		
<b>Kernel PTI</b>	Enabled		
<b>Uptime</b>	07 Hours 36 Minutes 39 Seconds		
<b>Current date/time</b>	Fri Jul 20 18:43:01 IST 2018		

Interfaces <span style="float: right;">⚙️ - ✕</span>			
<b>WAN1</b> <span style="color: green;">↑</span>	1000baseT <full-duplex>	10.0.2.15	
<b>LAN1</b> <span style="color: green;">↑</span>	1000baseT <full-duplex>	192.168.1.1	
<b>WAN2</b> <span style="color: green;">↑</span>	1000baseT <full-duplex>	192.168.1.103	

```

C:\Users\packt>ping google.com -t

Pinging google.com [216.58.220.174] with 32 bytes of data:
Reply from 216.58.220.174: bytes=32 time=54ms TTL=52
Reply from 216.58.220.174: bytes=32 time=43ms TTL=52
Reply from 216.58.220.174: bytes=32 time=50ms TTL=52
Reply from 216.58.220.174: bytes=32 time=41ms TTL=52
Reply from 216.58.220.174: bytes=32 time=44ms TTL=52
Reply from 216.58.220.174: bytes=32 time=40ms TTL=52
Reply from 216.58.220.174: bytes=32 time=40ms TTL=52
Reply from 216.58.220.174: bytes=32 time=40ms TTL=52
Reply from 216.58.220.174: bytes=32 time=41ms TTL=52
Reply from 216.58.220.174: bytes=32 time=40ms TTL=52
Reply from 216.58.220.174: bytes=32 time=39ms TTL=52
Reply from 216.58.220.174: bytes=32 time=40ms TTL=52

```

System / Routing / Gateways 🔄 📊 📄 ?

Gateways Static Routes Gateway Groups

Gateways						
Name	Interface	Gateway	Monitor IP	Description	Actions	
☑ WAN1_DHCP (default)	WAN1	10.0.2.2	10.0.2.2	Interface WAN1_DHCP Gateway		
☑ WAN2_DHCP	WAN2	192.168.1.1	192.168.1.1	Interface WAN2_DHCP Gateway		
☑ WAN1_DHCP6 (default)	WAN1	dynamic		Interface WAN1_DHCP6 Gateway		
☑ WAN2_DHCP6	WAN2	fe80::1:1	fe80::1:1	Interface WAN2_DHCP6 Gateway		

+ Add

System / Routing / Gateway Groups 📊 📄 ?

Gateways Static Routes Gateway Groups

Gateway Groups				
Group Name	Gateways	Priority	Description	Actions

+ Add

System / Routing / Gateway Groups / Edit 🔍 📊 📄 ?

### Edit Gateway Group Entry

**Group Name**

**Gateway Priority**

WAN1_DHCP	Never	Interface Address	Interface WAN1_DHCP Gateway
WAN2_DHCP	Never	Interface Address	Interface WAN2_DHCP Gateway
WAN1_DHCP6	Never	Interface Address	Interface WAN1_DHCP6 Gateway
WAN2_DHCP6	Never	Interface Address	Interface WAN2_DHCP6 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>	Member down		
	When to trigger exclusion of a member		

System / Routing / Gateway Groups / Edit 🔍 📊 📄 ?

### Edit Gateway Group Entry

**Group Name**

**Gateway Priority**

WAN1_DHCP	Tier 1	Interface Address	Interface WAN1_DHCP Gateway
WAN2_DHCP	Tier 1	Interface Address	Interface WAN2_DHCP Gateway

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.



**Source**

Source  Invert match. LAN1 net  Source Address /

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)  From Custom To (other)  Custom

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

**Gateway** 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.

Firewall / Rules / LAN1 ⌵ ⏏️ 📄 ?

Floating WAN1 LAN1 WAN2

**Rules (Drag to Change Order)**

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	✓ 0 / 49.04 MiB	*	*	*	LAN1 Address	443 80	*	*		Anti-Lockout Rule	⚙️
<input type="checkbox"/>	✓ 0 / 0 B	IPv4 TCP	LAN1 net	*	*	*	WAN_Group	none			⚓ 🖋️ 📄 🗑️
<input type="checkbox"/>	✓ 0 / 0 B	IPv4 TCP	LAN1 net	*	*	*	WAN_Group	none			⚓ 🖋️ 📄 🗑️
<input type="checkbox"/>	👉 0 / 0 B	IPv4 *	LAN1 net	*	WAN2 net	*	*	none			⚓ 🖋️ 📄 ✓ 🗑️
<input type="checkbox"/>	✓ 0 / 381 KiB	IPv4 ICMP any	LAN1 net	*	*	*	*	none			⚓ 🖋️ 📄 🗑️
<input type="checkbox"/>	✓ 0 / 0 B	IPv4 TCP/UDP	LAN1 net	53 (DNS)	*	*	*	none			⚓ 🖋️ 📄 🗑️
<input type="checkbox"/>	✓ 0 / 0 B	IPv4 TCP/UDP	LAN1 net	80 (HTTP)	*	*	*	none			⚓ 🖋️ 📄 🗑️

Status / Gateways / Gateway Groups 📊 📄 ?

Gateways Gateway Groups

### Gateway Groups

Group Name	Gateways	Description
WAN_Group	<div style="border: 1px solid #ccc; padding: 5px;"> <p>Tier 1</p> <p>WAN1_DHCP Online</p> <p>WAN2_DHCP Online</p> </div>	

```
C:\Users\packt>ping google.com -t

Pinging google.com [216.58.220.174] with 32 bytes of data:
Reply from 216.58.220.174: bytes=32 time=54ms TTL=52
Reply from 216.58.220.174: bytes=32 time=43ms TTL=52
Reply from 216.58.220.174: bytes=32 time=50ms TTL=52
Reply from 216.58.220.174: bytes=32 time=41ms TTL=52
Reply from 216.58.220.174: bytes=32 time=44ms TTL=52
Reply from 216.58.220.174: bytes=32 time=40ms TTL=52
Reply from 216.58.220.174: bytes=32 time=40ms TTL=52
Reply from 216.58.220.174: bytes=32 time=40ms TTL=52
Reply from 216.58.220.174: bytes=32 time=41ms TTL=52
Reply from 216.58.220.174: bytes=32 time=40ms TTL=52
Reply from 216.58.220.174: bytes=32 time=39ms TTL=52
Reply from 216.58.220.174: bytes=32 time=40ms TTL=52
```

System / Routing / Gateway Groups 📊 📄 ?

Gateways Static Routes Gateway Groups

### Gateway Groups

Group Name	Gateways	Priority	Description	Actions
WAN_Group	WAN1_DHCP WAN2_DHCP	Tier 1 Tier 1		

+ Add

Gateways

Name	Interface	Gateway	Monitor IP	Description	Actions
<input checked="" type="checkbox"/> WAN1_DHCP (default)	WAN1	10.0.2.2	10.0.2.2	Interface WAN1_DHCP Gateway	
<input checked="" type="checkbox"/> WAN2_DHCP	WAN2	192.168.1.1	192.168.1.1	Interface WAN2_DHCP Gateway	
<input checked="" type="checkbox"/> WAN1_DHCP6 (default)	WAN1	dynamic		Interface WAN1_DHCP6 Gateway	
<input checked="" type="checkbox"/> WAN2_DHCP6	WAN2	fe80::1:1	fe80::1:1	Interface WAN2_DHCP6 Gateway	

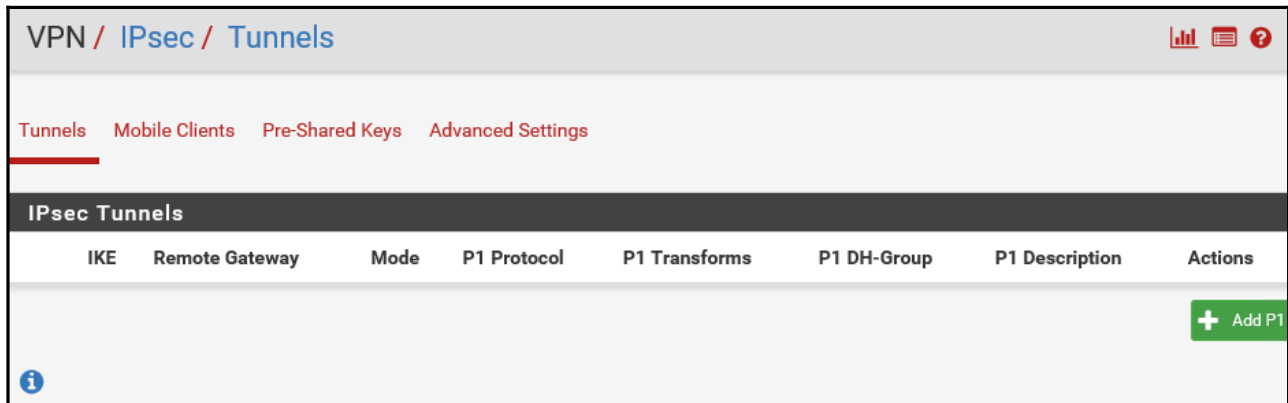
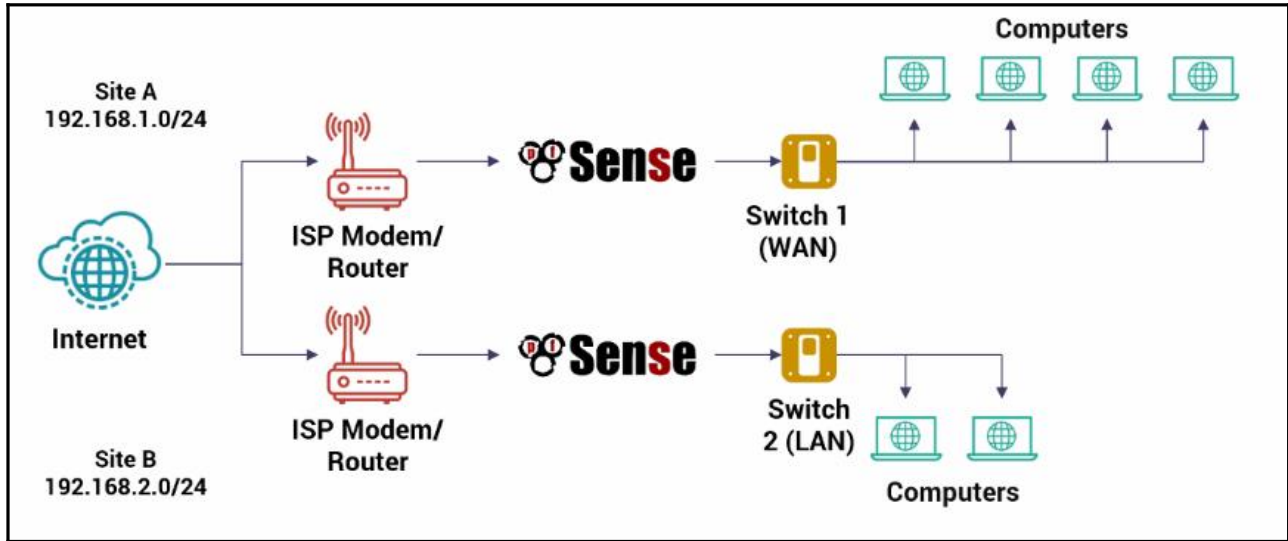
+ Add

**Force state**

Mark Gateway as Down

This will force this gateway to be considered down.

# Chapter 04: Remote Connectivity with pfSense and IPsec



**General Information**

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

**Key Exchange version** IKEv1  
 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** WAN1  
 Select the interface for the local endpoint of this phase1 entry.

**Remote Gateway** 192.168.2.1  
 Enter the public IP address or host name of the remote gateway.

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

Phase 1 Proposal (Authentication)	
<b>Authentication Method</b>	<input type="text" value="Mutual PSK"/> Must match the setting chosen on the remote side.
<b>Negotiation mode</b>	<input type="text" value="Aggressive"/> Aggressive is more flexible, but less secure.
<b>My identifier</b>	<input type="text" value="My IP address"/> <input type="text"/>
<b>Peer identifier</b>	<input type="text" value="Peer IP address"/> <input type="text"/>
<b>Pre-Shared Key</b>	<input type="text" value="packtpub@123"/> Enter the Pre-Shared Key string.
<b>My Certificate</b>	<input type="text" value="webConfigurator default (5b50e8520e3f2)"/> Select a certificate previously configured in the Certificate Manager.
<b>Peer Certificate Authority</b>	<input type="text" value="PacktPubDC"/> Select a certificate authority previously configured in the Certificate Manager.

Phase 1 Proposal (Encryption Algorithm)					
<b>Encryption Algorithm</b>	<input type="text" value="AES"/> Algorithm	<input type="text"/> Key length	<input type="text" value="SHA256"/> Hash	<input type="text" value="2 (1024 bit)"/> DH Group	<input type="button" value="Delete"/>
<b>Add Algorithm</b>	<input type="button" value="+ Add Algorithm"/>				
<b>Lifetime (Seconds)</b>	<input type="text" value="28800"/>				

### Advanced Options

**Disable rekey**  Disables renegotiation when a connection is about to expire.

**Margintime (Seconds)**   
How long before connection expiry or keying-channel expiry should attempt to negotiate a replacement begin.

**Disable Reauth**  Whether rekeying of an IKE\_SA should also reauthenticate the peer. In IKEv1, reauthentication is always done.

**Responder Only**  Enable this option to never initiate this connection from this side, only respond to incoming requests.

**NAT Traversal**   
Set this option to enable the use of NAT-T (i.e. the encapsulation of ESP in UDP packets) if needed, which can help with clients that are behind restrictive firewalls.

**MOBIKE**   
Set this option to control the use of MOBIKE

**Split connections**  Enable this to split connection entries with multiple phase 2 configurations. Required for remote endpoints that support only a single traffic selector per child SA.

**Dead Peer Detection**  Enable DPD

**Delay**   
Delay between requesting peer acknowledgement.

**Max failures**   
Number of consecutive failures allowed before disconnect.

VPN / IPsec / Tunnels 🔄 📊 📄 ?

[Tunnels](#) [Mobile Clients](#) [Pre-Shared Keys](#) [Advanced Settings](#)




The changes have been applied successfully. ✕

#### IPsec Tunnels

	IKE	Remote Gateway	Mode	P1 Protocol	P1 Transforms	P1 DH-Group	P1 Description	Actions
<input type="checkbox"/>	<span style="background-color: orange; padding: 2px;">Disable</span>	V1 WAN1 192.168.2.1	aggressive	AES	SHA256	2 (1024 bit)	Site A	

+ Show Phase 2 Entries (0)

+ Add P1
🗑 Delete P1s

IPsec Tunnels																						
	IKE	Remote Gateway	Mode	P1 Protocol	P1 Transforms	P1 DH-Group	P1 Description	Actions														
<input type="checkbox"/>	<span style="background-color: orange; color: white; padding: 2px;">Disable</span>	V1 WAN1 192.168.2.1	aggressive	AES	SHA256	2 (1024 bit)	Site A	  														
<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th>Mode</th> <th>Local Subnet</th> <th>Remote Subnet</th> <th>P2 Protocol</th> <th>P2 Transforms</th> <th>P2 Auth Methods</th> <th>P2 actions</th> </tr> </thead> <tbody> <tr> <td colspan="7" style="text-align: center;"><span style="background-color: green; color: white; padding: 5px;">+ Add P2</span></td> </tr> </tbody> </table>									Mode	Local Subnet	Remote Subnet	P2 Protocol	P2 Transforms	P2 Auth Methods	P2 actions	<span style="background-color: green; color: white; padding: 5px;">+ Add P2</span>						
Mode	Local Subnet	Remote Subnet	P2 Protocol	P2 Transforms	P2 Auth Methods	P2 actions																
<span style="background-color: green; color: white; padding: 5px;">+ Add P2</span>																						
						<span style="background-color: green; color: white; padding: 2px;">+ Add P1</span>	<span style="background-color: red; color: white; padding: 2px;">Delete P1s</span>															

### General Information

**Disabled**  Disable this phase 2 entry without removing it from the list.

**Mode** Tunnel IPv4 ▼

**Local Network** LAN1 subnet ▼  / 0 ▼

Type Address

**NAT/BINAT translation** None ▼  / 0 ▼

Type Address

If NAT/BINAT is required on this network specify the address to be translated

**Remote Network** Network ▼ 192.168.2.0 / 24 ▼

Type Address

**Description** Site B

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



### Phase 2 Proposal (SA/Key Exchange)

**Protocol**  ▼  
 ESP is encryption, AH is authentication only.

**Encryption Algorithms**

AES  ▼

AES128-GCM  ▼

AES192-GCM  ▼

AES256-GCM  ▼

Blowfish  ▼

3DES

CAST128

Use 3DES for best compatibility or for a hardware crypto accelerator card. Blowfish is usually the fastest in software encryption.

**Hash Algorithms**  MD5  SHA1  SHA256  SHA384  SHA512  AES-XCBC

**PFS key group**  ▼

**Lifetime**   
 Seconds

Tunnels **Mobile Clients** Pre-Shared Keys Advanced Settings

The changes have been applied successfully. ×

### IPsec Tunnels

	IKE	Remote Gateway	Mode	P1 Protocol	P1 Transforms	P1 DH-Group	P1 Description	Actions																
<input type="checkbox"/>	<span>Disable</span>	V1 WAN1 192.168.2.1	aggressive	AES	SHA256	2 (1024 bit)	Site A																	
<table border="1"> <thead> <tr> <th></th> <th>Mode</th> <th>Local Subnet</th> <th>Remote Subnet</th> <th>P2 Protocol</th> <th>P2 Transforms</th> <th>P2 Auth Methods</th> <th>P2 actions</th> </tr> </thead> <tbody> <tr> <td><input type="checkbox"/></td> <td><span>Disable</span></td> <td>tunnel LAN1</td> <td>192.168.2.0/24</td> <td>ESP</td> <td>AES (256 bits)</td> <td>SHA256</td> <td> </td> </tr> </tbody> </table> <p><span>+</span> Add P2</p>										Mode	Local Subnet	Remote Subnet	P2 Protocol	P2 Transforms	P2 Auth Methods	P2 actions	<input type="checkbox"/>	<span>Disable</span>	tunnel LAN1	192.168.2.0/24	ESP	AES (256 bits)	SHA256	
	Mode	Local Subnet	Remote Subnet	P2 Protocol	P2 Transforms	P2 Auth Methods	P2 actions																	
<input type="checkbox"/>	<span>Disable</span>	tunnel LAN1	192.168.2.0/24	ESP	AES (256 bits)	SHA256																		

+ Add P1 🗑️ Delete P1s

Firewall / Rules / WAN1 📊 📄 ?

Floating WAN1 LAN1 WAN2 IPsec

**Rules (Drag to Change Order)**

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✘	0 /45 KIB	*	RFC 1918 networks	*	*	*	*	*		Block private networks	⚙️
✘	0 /0 B	*	Reserved Not assigned by IANA	*	*	*	*	*		Block bogon networks	⚙️
<input type="checkbox"/>	✔️ 0 /0 B	IPv4 TCP	*	*	WAN1 address	1194 (OpenVPN)	*	none		OpenVPN wizard	📌 🗑️

⬆️ 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.

Firewall / Rules / IPsec

Floating WAN1 LAN1 WAN2 **IPsec**

Rules (Drag to Change Order)

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

Add Add Delete Save Separator

Firewall / NAT / Outbound

Port Forward 1:1 **Outbound** NPT

Outbound NAT Mode

Mode

Automatic outbound NAT rule generation. (IPsec passthrough included)

Hybrid Outbound NAT rule generation. (Automatic Outbound NAT + rules below)

Manual Outbound NAT rule generation. (AON - Advanced Outbound NAT)

Disable Outbound NAT rule generation. (No Outbound NAT rules)

Save

Mappings

Interface	Source	Source Port	Destination	Destination Port	NAT Address	NAT Port	Static Port	Description	Actions
									Add  Add  Delete  Save

**Source**   /

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


**Misc**

No XMLRPC Sync






Prevents the rule on Master from automatically syncing to other CARP members. This does NOT prevent the rule from being overwritten on Slave.





Description

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



 Save


### Mappings

	Interface	Source	Source Port	Destination	Destination Port	NAT Address	NAT Port	Static Port	Description	Actions
<input type="checkbox"/>	 WAN1	192.168.1.0/24	*	*	*	WAN1 address	*		NAT for IPSec	  

 Add
  Add
  Delete
  Save

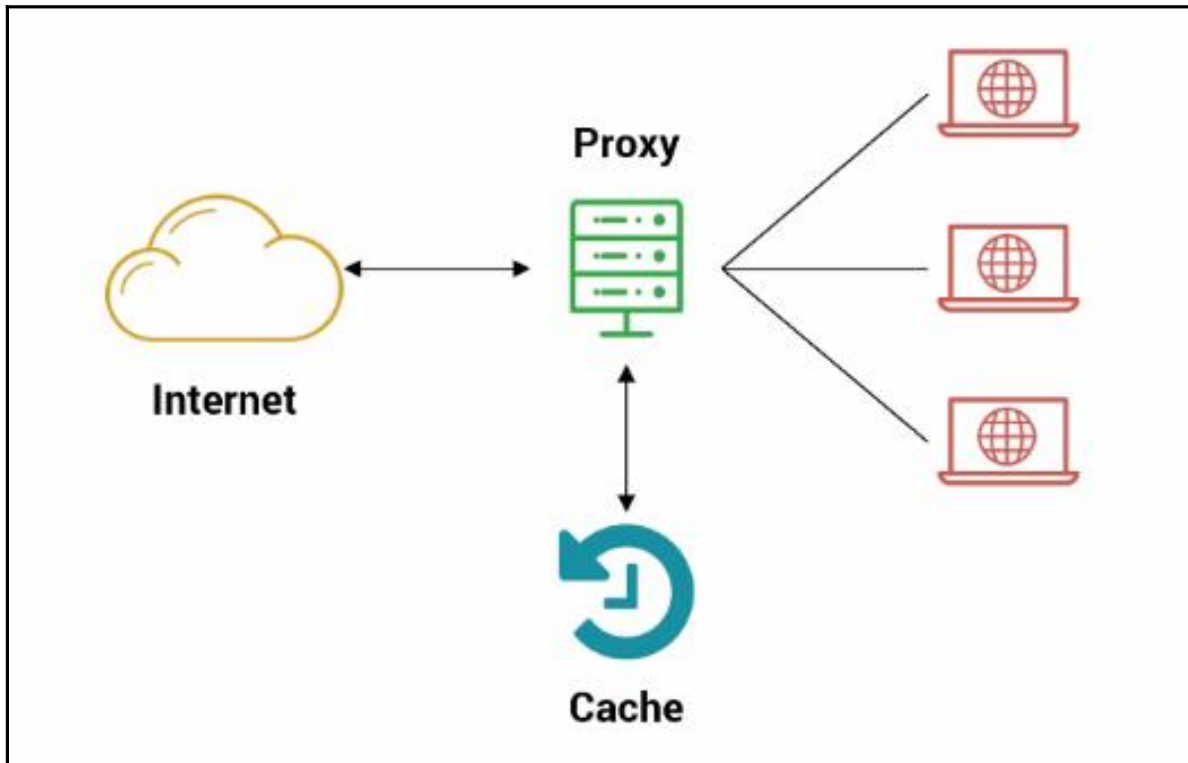
### Automatic Rules:

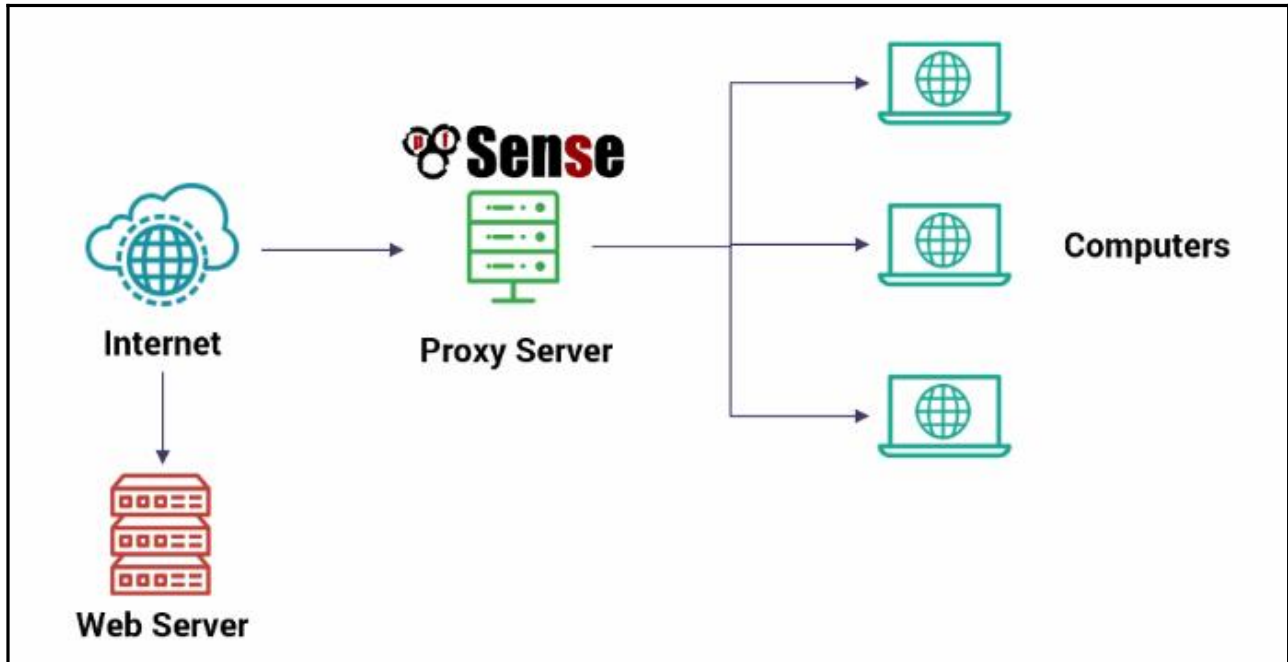
	Interface	Source	Source Port	Destination	Destination Port	NAT Address	NAT Port	Static Port	Description
<input checked="" type="checkbox"/>	WAN1	127.0.0.0/8 192.168.1.0/24	*	*	500	WAN1 address	*	<input checked="" type="checkbox"/>	Auto created rule for ISAKMP
<input checked="" type="checkbox"/>	WAN1	127.0.0.0/8 192.168.1.0/24	*	*	*	WAN1 address	*		Auto created rule
<input checked="" type="checkbox"/>	WAN2	127.0.0.0/8 192.168.1.0/24	*	*	500	WAN2 address	*	<input checked="" type="checkbox"/>	Auto created rule for ISAKMP
<input checked="" type="checkbox"/>	WAN2	127.0.0.0/8 192.168.1.0/24	*	*	*	WAN2 address	*		Auto created rule



---

## Chapter 05: Using pfSense as a Squid Proxy Server





System / [Package Manager](#) / [Package Installer](#) ?

---

pfSense-pkg-squid installation successfully completed.

[Installed Packages](#)
[Available Packages](#)
[Package Installer](#)

---

**Package Installation**

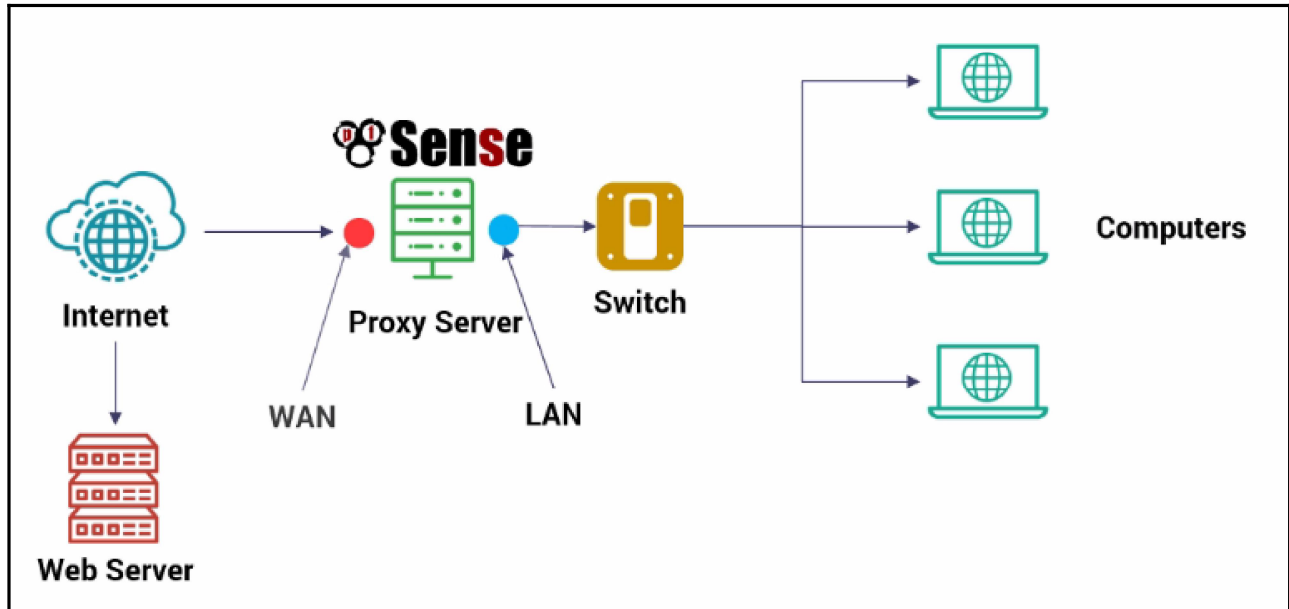
```

/usr/local/etc/squid/squid.conf.documented is a fully annotated
configuration file you can consult for further reference.

Additionally, you should check your configuration by calling
'squid -f /path/to/squid.conf -k parse' before starting Squid.
Message from pfSense-pkg-squid-0.4.43_1:

Please visit Services - Squid Proxy Server menu to configure the package and enable the proxy.
>>> Cleaning up cache... done.
Success

```



General Remote Cache Local Cache Antivirus ACLs Traffic Mgmt Authentication Users Real Time Sync

---

### Squid General Settings

**Enable Squid Proxy**  Check to enable the Squid proxy.  
**Important:** If unchecked, ALL Squid services will be disabled and stopped.

**Keep Settings/Data**  If enabled, the settings, logs, cache, AV defs and other data will be preserved across package reinstalls.  
**Important:** If disabled, all settings and data will be wiped on package uninstall/reinstall/upgrade.

**Proxy Interface(s)**   
 LAN1  
 WAN2  
 WAN1  
 loopback  
 The interface(s) the proxy server will bind to. Use CTRL + click to select multiple interfaces.

**Proxy Port**   
 This is the port the proxy server will listen on. Default: 3128

**ICP Port**   
 This is the port the proxy server will send and receive ICP queries to and from neighbor caches. Leave this blank if you don't want the proxy server to communicate with neighbor caches through ICP.

**Allow Users on Interface**  If checked, the users connected to the interface(s) selected in the 'Proxy interface(s)' field will be allowed to use the proxy.  
 There will be no need to add the interface's subnet to the list of allowed subnets.

### Transparent Proxy Settings

**Transparent HTTP Proxy**  Enable transparent mode to forward all requests for destination port 80 to the proxy server. [i](#)

Transparent proxy mode works without any additional configuration being necessary on clients.  
**Important:** Transparent mode will filter SSL (port 443) if you enable 'HTTPS/SSL Interception' below.  
**Hint:** In order to proxy both HTTP and HTTPS protocols **without intercepting SSL connections**, configure WPAD/PAC options on your DNS/DHCP servers.

**Transparent Proxy Interface(s)**

The interface(s) the proxy server will transparently intercept requests on. Use CTRL + click to select multiple interfaces.

**Bypass Proxy for Private Address Destination**  Do not forward traffic to Private Address Space (RFC 1918) destinations.  
Destinations in Private Address Space (RFC 1918) are passed directly through the firewall, not through the proxy server.

**Bypass Proxy for These Source IPs**

Do not forward traffic from these **source** IPs, CIDR nets, hostnames, or aliases through the proxy server but let it pass directly through the firewall.  
**Applies only to transparent mode.** Separate entries by semi-colons (;)

**Bypass Proxy for These Destination IPs**

Do not proxy traffic going to these **destination** IPs, CIDR nets, hostnames, or aliases, but let it pass directly through the firewall.  
**Applies only to transparent mode.** Separate entries by semi-colons (;)

### SSL Man In the Middle Filtering

**HTTPS/SSL Interception**  Enable SSL filtering.

### Logging Settings

**Enable Access Logging**  This will enable the access log.  
**Warning:** Do NOT enable if available disk space is low.

**Log Store Directory**

The directory where the logs will be stored; also used for logs other than the Access Log above. Default: /var/squid/logs  
**Important:** Do NOT include the trailing / when setting a custom location.

**Rotate Logs**

Defines how many days of logfiles will be kept. Rotation is disabled if left empty.

**Log Pages Denied by SquidGuard**  Makes it possible for SquidGuard denied log to be included on Squid logs.  
Click Info for detailed instructions. [i](#)



---

## Headers Handling, Language and Other Customizations

**Visible Hostname**

This is the hostname to be displayed in proxy server error messages.

**Administrator's  
Email**

This is the email address displayed in error messages to the users.

**Error Language**

 ▼

Select the language in which the proxy server will display error messages to users.

**X-Forwarded  
Header Mode**

 ▼

Choose how to handle X-Forwarded-For headers. Default: on 

**Disable VIA Header**

If not set, Squid will include a Via header in requests and replies as required by RFC2616.

**Do Not Cache**

Enter domain(s) and/or IP address(es) that should never be cached. Put each entry on a separate line.

**Enable Offline Mode**

Enable this option and the proxy server will never try to validate cached objects.

Offline mode gives access to more cached information than normally allowed (e.g., expired cached versions where the origin server should have been contacted otherwise).

### Squid Hard Disk Cache Settings

<b>Hard Disk Cache Size</b>	<input type="text" value="100"/>	Amount of disk space (in megabytes) to use for cached objects.
<b>Hard Disk Cache System</b>	<input type="text" value="ufs"/>	This specifies the kind of storage system to use. <a href="#">i</a>
<b>Clear Disk Cache NOW</b>	Hard Disk Cache is automatically managed by swapstate_check.php script which is scheduled to run daily via cron. <a href="#">i</a> If you wish to clear cache <b>immediately</b> , click this button <b>once</b> : <input type="button" value="Clear Disk Cache NOW"/>	
<b>Level 1 Directories</b>	<input type="text" value="16"/>	Specifies the number of Level 1 directories for the hard disk cache. <a href="#">i</a>
<b>Hard Disk Cache Location</b>	<input type="text" value="/var/squid/cache"/>	This is the directory where the cache will be stored. Default: /var/squid/cache <a href="#">i</a>
<b>Minimum Object Size</b>	<input type="text" value="0"/>	Objects smaller than the size specified (in kilobytes) will not be saved on disk. Default: 0 (meaning there is no minimum)
<b>Maximum Object Size</b>	<input type="text" value="4"/>	Objects larger than the size specified (in megabytes) will not be saved on disk. Default: 4 (MB) <a href="#">i</a>

### Squid Memory Cache Settings

<b>Memory Cache Size</b>	<input type="text" value="64"/>	Specifies the ideal amount of physical RAM (in megabytes) to be used for In-Transit objects, Hot Objects and Negative-Cached objects. Minimum value: 1 (MB). Default: 64 (MB) <a href="#">i</a>
<b>Maximum Object Size in RAM</b>	<input type="text" value="256"/>	Objects greater than this size (in kilobytes) will not be attempted to kept in the memory cache. Default: 256 (KB)
<b>Memory Replacement Policy</b>	<input type="text" value="Heap GDSF"/>	The memory replacement policy determines which objects are purged from memory when space is needed. Default: heap GDSF <a href="#">i</a>

## Dynamic and Update Content

### Cache Dynamic Content

Select to enable caching of dynamic content.

With [dynamic cache](#) enabled, you can also apply refresh\_patterns to sites like [Windows Updates](#). [i](#)

### Custom refresh\_patterns

Enter custom refresh\_patterns for better dynamic cache usage.

**Note:** These refresh\_patterns will only be included if 'Cache Dynamic Content' is enabled.

[General](#) [Remote Cache](#) [Local Cache](#) [Antivirus](#) [ACLs](#) [Traffic Mgmt](#) [Authentication](#) [Users](#) [Real Time](#) [Sync](#)

## ClamAV Anti-Virus Integration Using C-ICAP

### Enable AV

Enable Squid antivirus check using ClamAV.

### Client Forward Options

Send both client username and IP info (Default)

Select what client info to forward to ClamAV.

### ClamAV Database Update

never

Optionally, you can schedule ClamAV definitions updates via cron. Select the desired frequency here. [i](#)

**Important:** Set to 'every 1 hour' if you want to use Google Safe Browsing feature.

Click the button below **once** to force the update of AV databases immediately. **Note:** This will take a while. Check freshclam log on the 'Real Time' tab for progress information.

### Squid Access Control Lists

#### Allowed Subnets

Enter subnets that are allowed to use the proxy in CIDR format. All the other subnets won't be able to use the proxy. Put each entry on a separate line.

**When 'Allow Users on Interface' is checked on 'General' tab, there is no need to add the 'Proxy Interface(s)' subnet(s) to this list.**

#### Unrestricted IPs

Enter unrestricted IP address(es) / network(s) in CIDR format. Configured entries will NOT be filtered out by the other access control directives set in this page.

Put each entry on a separate line. [i](#)

#### Banned Hosts Addresses

Enter IP address(es) / network(s) in CIDR format. Configured entries will NOT be allowed to use the proxy. Put each entry on a separate line.

<b>Whitelist</b>	<input type="text"/> <p>Destination domains that will be accessible to the users that are allowed to use the proxy. Put each entry on a separate line. You can also use regular expressions.</p>
<b>Blacklist</b>	<input type="text"/> <p>Destination domains that will be blocked for the users that are allowed to use the proxy. Put each entry on a separate line. You can also use regular expressions.</p>
<b>Block User Agents</b>	<input type="text"/> <p>Enter user agents that will be blocked for the users that are allowed to use the proxy. Put each entry on a separate line. You can also use regular expressions.</p>

General Remote Cache Local Cache Antivirus ACLs Traffic Mgmt Authentication Users Real Time Sync

---

**Squid Traffic Management Settings**

<b>Maximum Download Size</b>	<input type="text" value="0"/> X <p>Limit the maximum total download size to the size specified here (in kilobytes). Set to 0 to disable.</p>
<b>Maximum Upload Size</b>	<input type="text" value="0"/> <p>Limit the maximum total upload size to the size specified here (in kilobytes). Set to 0 to disable.</p>
<b>Overall Bandwidth Throttling</b>	<input type="text" value="0"/> <p>This value specifies the bandwidth throttle for downloads (in kilobytes per second). Users will gradually have their download speed decreased according to this value. Set to 0 to disable.</p>
<b>Per-Host Throttling</b>	<input type="text" value="0"/> <p>This value specifies the download throttling per host. Set to 0 to disable.</p>
<b>Throttle Unrestricted IPs</b>	<input type="checkbox"/> If enabled, even 'Unrestricted IPs' configured on the ACLs tab are subject to throttling.

```
C:\Users\packt>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::780c:d57c:aef3:2b13%11
    IPv4 Address. . . . . : 192.168.1.2
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : fe80::1:1%11
                                192.168.1.1

Tunnel adapter isatap.<D17026F3-1D71-4EF0-B8F0-E3D4285DCA7B>:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

C:\Users\packt>_
```

**Banned Hosts Addresses**

Enter IP address(es) / network(s) in CIDR format. Configured entries will NOT be allowed to use the proxy.  
Put each entry on a separate line.

**Administrator's Email**

This is the email address displayed in error messages to the users.

**Blacklist**

Destination domains that will be blocked for the users that are allowed to use the proxy.  
Put each entry on a separate line. You can also use regular expressions.

**Per-Host Throttling**

This value specifies the download throttling per host. Set to 0 to disable.