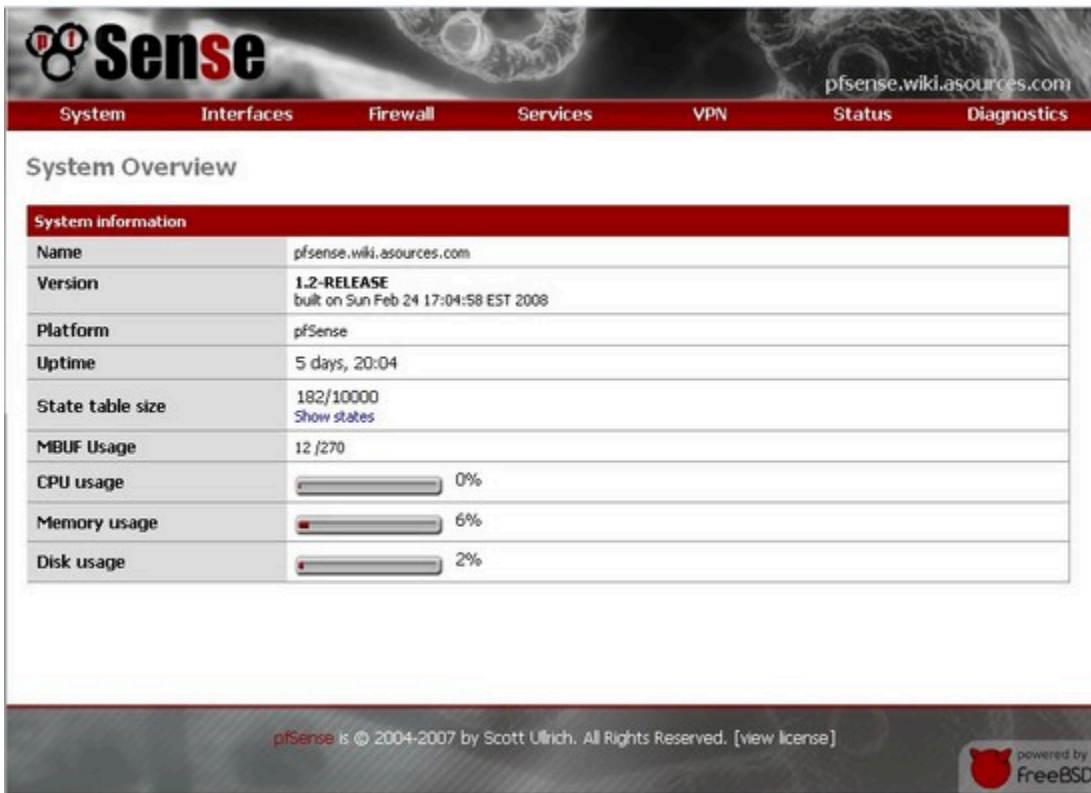





????? pfsense ?????

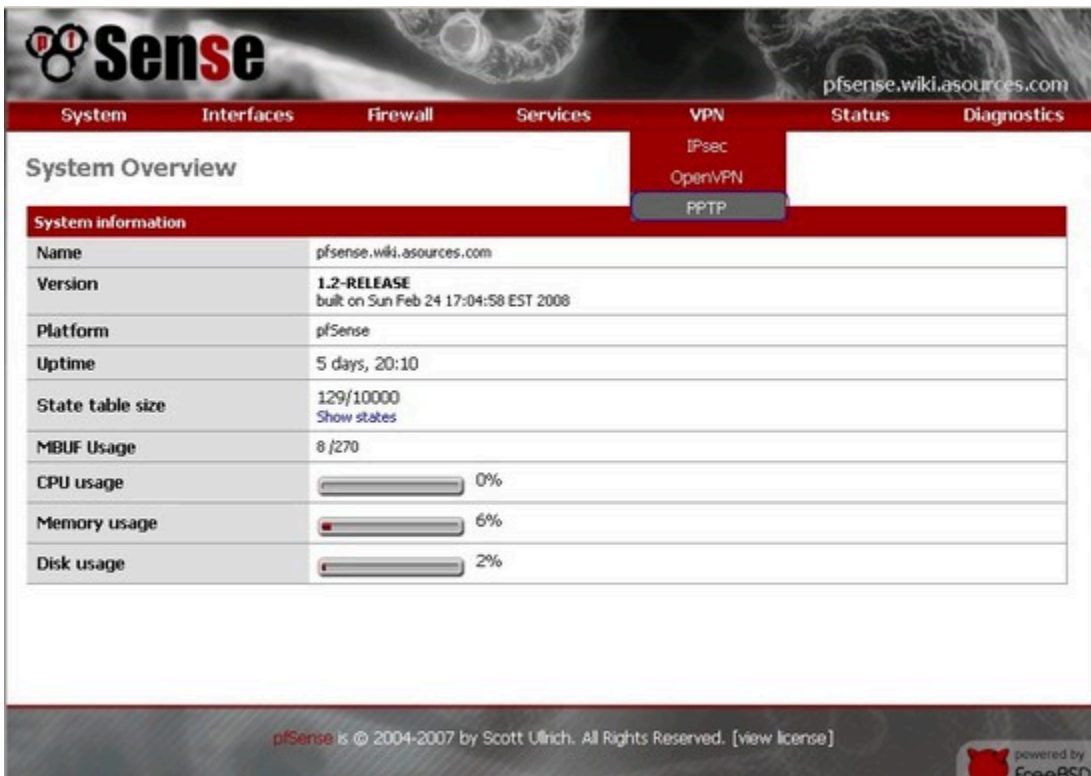


The screenshot shows the pfSense System Overview page. The top navigation bar includes System, Interfaces, Firewall, Services, VPN, Status, and Diagnostics. The System Overview section contains a table with the following data:




System information	
Name	pfsense.wiki.asources.com
Version	<b>1.2-RELEASE</b> built on Sun Feb 24 17:04:58 EST 2008
Platform	pfSense
Uptime	5 days, 20:04
State table size	182/10000 <a href="#">Show states</a>
MBUF Usage	12 /270
CPU usage	 0%
Memory usage	 6%
Disk usage	 2%

At the bottom, there is a copyright notice: "pfSense is © 2004-2007 by Scott Ulrich. All Rights Reserved. [view license]" and a logo for "powered by FreeBSD".

?? VPN--->PPTP



The screenshot shows the pfSense VPN configuration page. The top navigation bar includes System, Interfaces, Firewall, Services, VPN, Status, and Diagnostics. The VPN section is active, showing sub-options: IPsec, OpenVPN, and PPTP. The System Overview section contains a table with the following data:

System information	
Name	pfsense.wiki.asources.com
Version	<b>1.2-RELEASE</b> built on Sun Feb 24 17:04:58 EST 2008
Platform	pfSense
Uptime	5 days, 20:10
State table size	129/10000 <a href="#">Show states</a>
MBUF Usage	8 /270
CPU usage	 0%
Memory usage	 6%
Disk usage	 2%

At the bottom, there is a copyright notice: "pfSense is © 2004-2007 by Scott Ulrich. All Rights Reserved. [view license]" and a logo for "powered by FreeBSD".

????????? Configuration ????WAN ? IP ? VPN ???? IP ?????????????? Save, ??????? Apply changes ???????

???? Users ????? + ????? VPN ??

????ID????? Save?

**Sense** pfsense.wiki.asources.com

System Interfaces Firewall Services VPN Status Diagnostics

**VPN: PPTP: Users**

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

Configuration Users

Username	IP address
00	

pfsense is © 2004-2007 by Scott Ulrich. All Rights Reserved. [view license] powered by

?????? Firewall--->Rules

**Sense** pfsense.wiki.asources.com

System Interfaces Firewall Services VPN Status Diagnostics

**System Overview**

System information

- Aliases
- NAT
- Rules**
- Schedules
- Traffic Shaper
- Virtual IPs

Name	pfsense
Version	1.2-bulk
Platform	pfSense
Uptime	5 days, 20:06
State table size	185/10000 <a href="#">Show states</a>
MBUF Usage	12 /270
CPU usage	<input type="text" value="0%"/>
Memory usage	<input type="text" value="6%"/>
Disk usage	<input type="text" value="2%"/>

pfsense is © 2004-2007 by Scott Ulrich. All Rights Reserved. [view license] powered by **freeBSD**

???????? PPTP VPN ????????

**Firewall: Rules**

LAN WAN **PPTP VPN**

Proto	Source	Port	Destination	Port	Gateway	Schedule	Description
<input type="checkbox"/>							
<input type="checkbox"/>							

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

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

pfSense is © 2004-2007 by Scott Ulich. All Rights Reserved. [view license]

?????????? PPTP ? TCP/IP????? LAN

**Firewall: Rules: Edit**

**Action** Pass  
 Choose what to do with packets that match the criteria specified below.  
 Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded. Reject only works when the protocol is set to either TCP or UDP (but not "TCP/UDP") below.

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

**Interface** PPTP  
 Choose on which interface packets must come in to match this rule.

**Protocol** TCP/UDP  
 Choose which IP protocol this rule should match.  
 Hint: in most cases, you should specify TCP here.

**Source**  **not**  
 Use this option to invert the sense of the match.  
 Type: any  
 Address: / 31  
 Advanced - Show source port range

**Source OS** OS Type: any  
 Note: this only works for TCP rules

**Destination**  **not**  
 Use this option to invert the sense of the match.  
 Type: any  
 Address: / 31



**Destination port range** from: any to: any

Specify the port or port range for the destination of the packet for this rule.  
Hint: you can leave the to field empty if you only want to filter a single port

**Log**  **Log packets that are handled by this rule**  
Hint: the firewall has limited local log space. Don't turn on logging for everything. If you want to do a lot of logging, consider using a remote syslog server (see the Diagnostics: System logs: Settings page).

**Advanced Options**  - Show advanced options

**State Type**  - Show state

**No XMLRPC Sync**   
HINT: This prevents the rule from automatically syncing to other carp members.

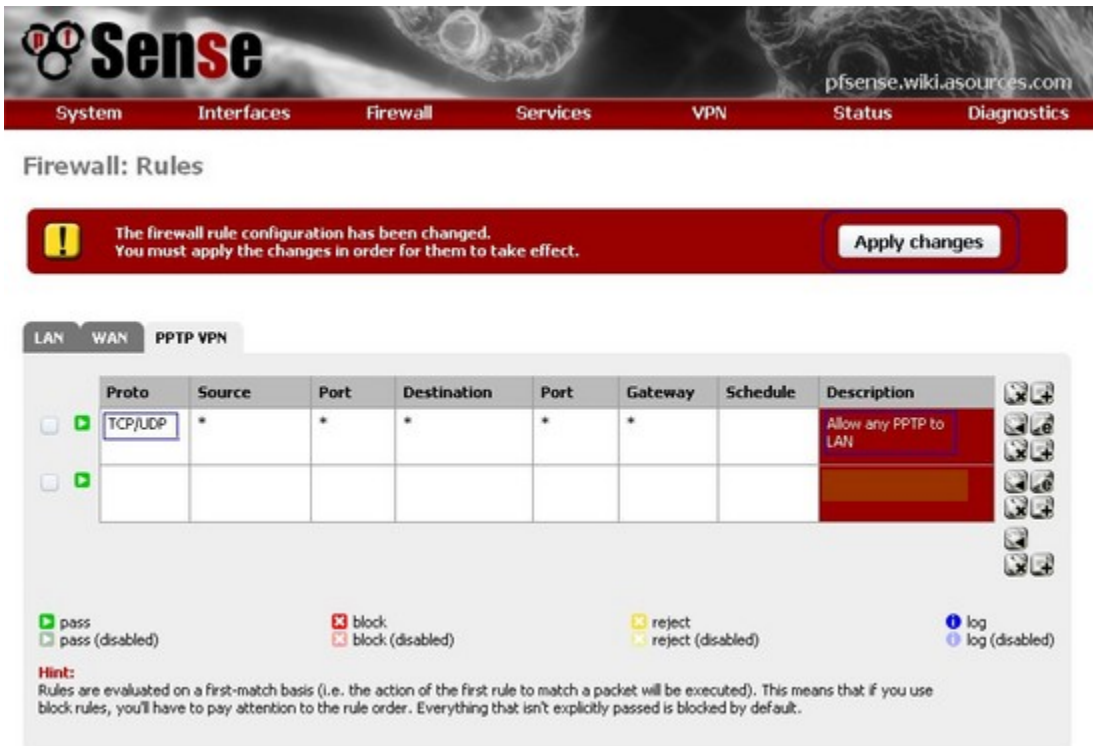
**Schedule** none  
Leave as 'none' to leave the rule enabled all the time.  
NOTE: schedule logic can be a bit different. Click here for more information.

**Gateway** default  
Leave as 'default' to use the system routing table. Or choose a gateway to utilize policy based routing.

**Description**  對此 rules 的描述  
You may enter a description here for your reference (not parsed).

Notes: ?? Destination -> any?PPTP ???????? LAN ?????? WAN????? PPTP ?????? LAN???? Destination -> LAN subnet?

save????????????????? Apply changes ??



The screenshot shows the Sense Firewall configuration interface. At the top, there is a navigation bar with links for System, Interfaces, Firewall, Services, VPN, Status, and Diagnostics. Below this is the 'Firewall: Rules' section. A red notification banner states: 'The firewall rule configuration has been changed. You must apply the changes in order for them to take effect.' with an 'Apply changes' button. The main area shows a table of firewall rules. The first rule is selected and highlighted in red. It has the following configuration: Proto: TCP/UDP, Source: \*, Port: \*, Destination: \*, Port: \*, Gateway: \*, Schedule: (empty), and Description: 'Allow any PPTP to LAN'. Below the table, there are checkboxes for 'pass' and 'pass (disabled)', and buttons for 'block', 'block (disabled)', 'reject', and 'reject (disabled)'. A 'log' button is also present. A 'Hint' section at the bottom explains that rules are evaluated on a first-match basis.

OK?PPTP VPN server ??????