

# SPA100 Firewall / SIP Proxy

## Quick User Installation Guide



# BluegrassNet Voice Firewall/SIP Proxy - SP100



## WAN

defaults to DHCP Client

## LAN

VLAN 1 (untagged) 192.168.1.1

VLAN 100 (tagged) 172.16.100.1

DHCP server running on both VLANs

## *Default login credentials*

Url: <https://192.168.1.1>

Username: admin

Password: pfsense

## *Phone configuration*

SIP server (aka SIP Proxy): IP Address of your SIP registrar (ex. Asterisk server IP)

SIP outbound Proxy: 172.16.100.1

Ethernet VLAN ID: 100

## *Switch LAN ports configuration*

VLAN 1 (default vlan) untagged on all LAN ports

VLAN 100 (voice vlan) tagged on all LAN ports

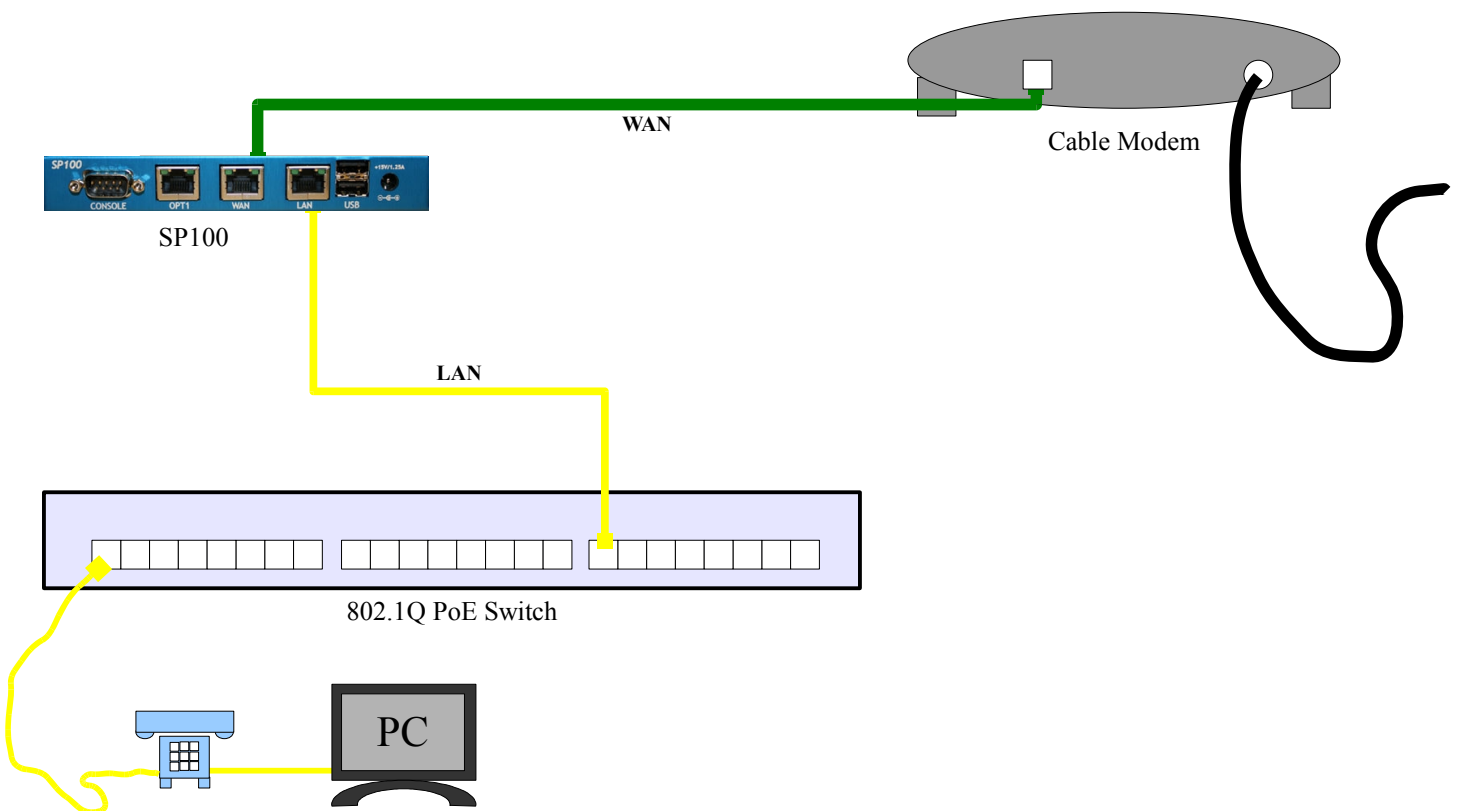
PVID = 1

QoS Method = DSCP

# I

## Installation

1. Connect The LAN port (that which is closest to the power supply) to the LAN segment of your network.
2. Set your network switch to pass VLAN1 untagged and VLAN100 tagged packets for this port. Set the PVID of this port to 1.
3. Connect the WAN port (port next to the LAN port) to the WAN segment of your network. This may consist of a direct connection to a T1 router or cable/dsl modem, a stand alone switch, or even a separate port-based VLAN on the same network switch of step 2.
4. OPT1 is unused by default but can be configured for advanced settings as an additional network segment such as a wireless network or DMZ network.
5. You may now obtain an IP address for your PC/MAC connected to the LAN network and connect to the device at: <https://192.168.1.1>
6. It is suggested you change the default password at this time under **System: General Setup**
7. Configure your remaining LAN ports on your 802.1Q capable switch identical to step 2. CAUTION: If you plan on using a Windows server as your DHCP server you MUST remove VLAN100 from the physical interface the windows server is connected to. Windows' DHCP server is not intelligent enough to realize that VLAN100 packets are a different network and will attempt to deliver VLAN1 IP Addresses to VLAN100 devices rendering your phones non-operational.
8. Set your phone network settings so that the phone can participate in VLAN100 while its PC device can remain in VLAN1.



## II Setting up DHCP options

	The default is 7200 seconds.
Maximum lease time	<input type="text"/> seconds This is the maximum lease time for clients that ask for a specific expiration time. The default is 86400 seconds.
Failover peer IP:	<input type="text"/> Leave blank to disable. Enter the REAL address of the other machine. Machines must be using CARP.
Static ARP	<input type="checkbox"/> <b>Enable Static ARP entries</b> <b>Note:</b> Only the machines listed below will be able to communicate with the firewall on this NIC.
Dynamic DNS	<input type="button" value="Advanced"/> - Show Dynamic DNS
NTP servers	<input type="button" value="Advanced"/> - Show NTP configuration
Enable Network booting	<input type="button" value="Advanced"/> - Show Network booting
Time offset	<input type="text"/> Enter the time offset to represent the timezone in which you reside, in seconds. Example: EST is GMT-5, enter -18000 here for EST.
TFTP server name	<input type="text"/> Enter the TFTP server name or IP address here.
<input type="button" value="Save"/>	

Figure 2.1

1. Select Services → DHCP server from the pull-down menu's.
2. Select the voice interface tab
3. Set the NTP servers to ip's you want to use such as your MTE server if its running a time server.
4. Change the time-offset value to represent the timezone you reside. The value is represented in seconds. Do not compensate for daylight savings time (example: EST is GMT -5 even when DST has a -4 offset).
5. Change the tftp-server-name value to the name or ip of the provisioning server your phones will use to fetch their configs. Despite the attribute name referencing tftp this works for tftp, http, https, ftp etc. A URL with username/password and FQDN are all possible as long as your phone devices support such values.
6. Click on 'Save' to save your settings

# III

## Siproxd Settings

Your SP100 comes pre-configured and ready for most SIP applications. Changes can be made from the default values. Briefly, we will walk through some of the settings and explain what they do.

1. Select **Services: siproxd** from the main menu. (figure 3.1)

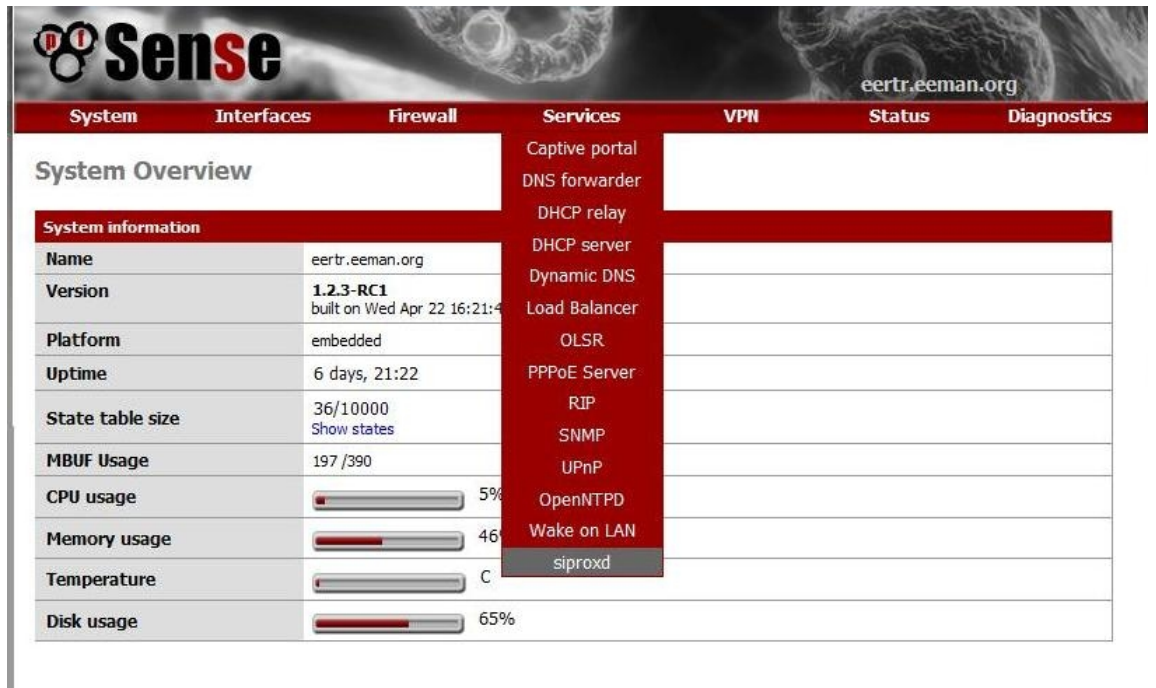


Figure 3.1

2. Set the Inbound interface to the VOICE interface. Set the Outbound interface to the WAN interface. See Figure 3.2 for examples.

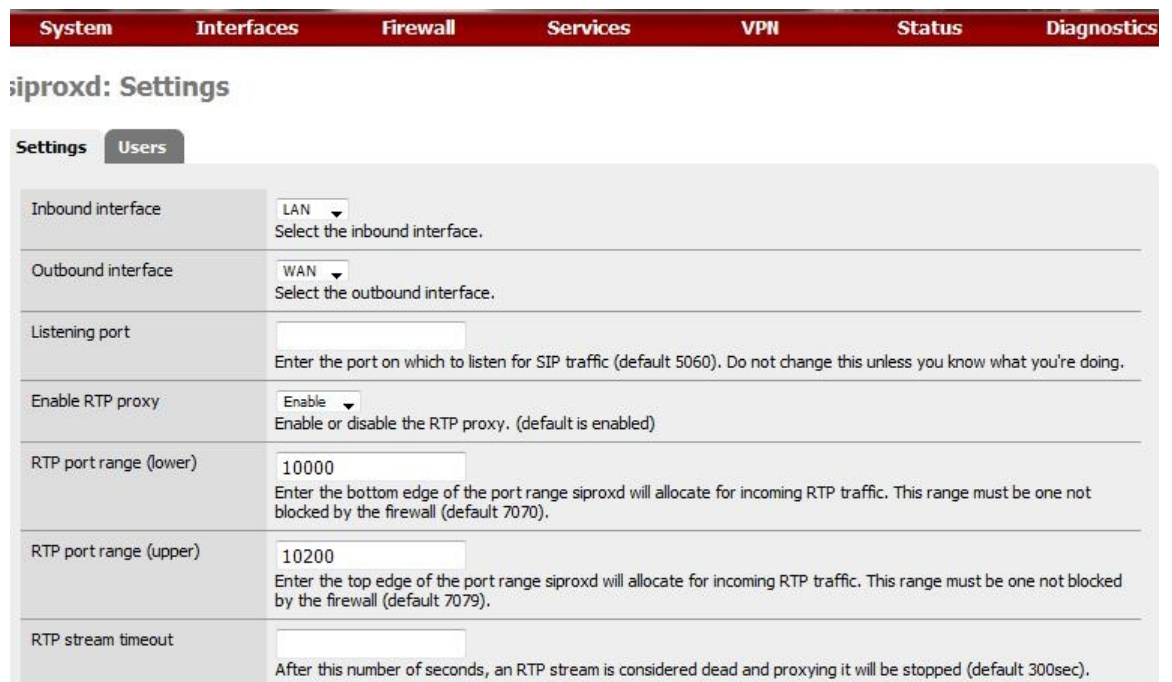


Figure 3.2

3. Normally the Listening port can be left blank (defaulting to 5060). This is the standard port for SIP signalling.
4. Enable RTP Proxy: This should be enabled if you want to proxy the media stream in order to avoid NAT-isms.
5. RTP Port range: This sets up the negotiation of what ports to use for the RTP media stream. Each conversation requires 2 ports for RTP and RTCP data. By narrowing the range to say 10000 – 10200 you narrow the opening in your firewall and restrict the calls to 100.
6. RTP stream timeout. This defaults to 300 seconds (5 min). You probably wont have to change this setting.

Default expiration timeout	<input type="text"/>	If a REGISTER request dose not contain an Expires header or expires= parameter, this number of seconds will be used and reported back to the UA in the answer.
Enable proxy authentication	<input type="checkbox"/>	If this is checked, clients will be forced to authenticate themselves at the proxy (for registration only).
Outbound proxy hostname	<input type="text"/>	Enter the hostname of an outbound proxy to send all traffic to. This is only useful if you have multiple masquerading firewalls to cross.
Outbound proxy port	<input type="text"/>	Enter the port of the outbound proxy to send all traffic to. This is only useful if you have multiple masquerading firewalls to cross.
Expedited Forwarding	<input checked="" type="checkbox"/>	This service is designed to allow ISPs to offer a service with attributes similar to a "leased line". This service offers the ULTIMATE IN LOW LOSS, LOW LATENCY AND LOW JITTER by ensuring that there is always sufficient room in output queues for the contracted expedited forwarding traffic.

Figure 3.3

7. Default expiration timeout : you should really never have a need to set this unless your registrar is sending faulty headers.
8. Enable proxy authentication : This is used of the proxy is going to act like a registrar for the sip devices instead of a proxy. This is not normal.
9. Outbound proxy hostname / port : If your proxy must send its calls to yet another proxy before reaching the server you may specify the hostname and port here.
10. Expedited Forwarding : This sets the DSCP headers of your RTP media stream to Expedited Forwarding (EF), aka 0xb8, aka decimal 46, aka binary 101110. This is vital for networks that prioritize voice traffic based on such markings.

## IV

# Enabling the Traffic Shaper

1. Perform 3 speed tests from <http://www.speedtest.net/> . Record your slowest upload and download speeds of the 3 tests.
2. Select **Firewall: Traffic Shaper** from the main menu

3. After being presented with a warning about overwriting current settings click next to begin the setup wizard.

4. Using the speeds recorded from step 1 populate the upload and download field network speeds. Make sure to record in Kbits (1Mbps = 1024 Kbits). The relationship of Download and LAN vs. Upload and WAN may appear backwards upon first glance. This is simply because packets can only be limited as they leave an interface. There is no way to restrict the rate at which packets are received after they have already been sent.

5. Enable the 'Prioritize Voice over IP Traffic' option (Figure 4.3).

6. Choose your provider type from the list or choose Generic if your type is not listed.

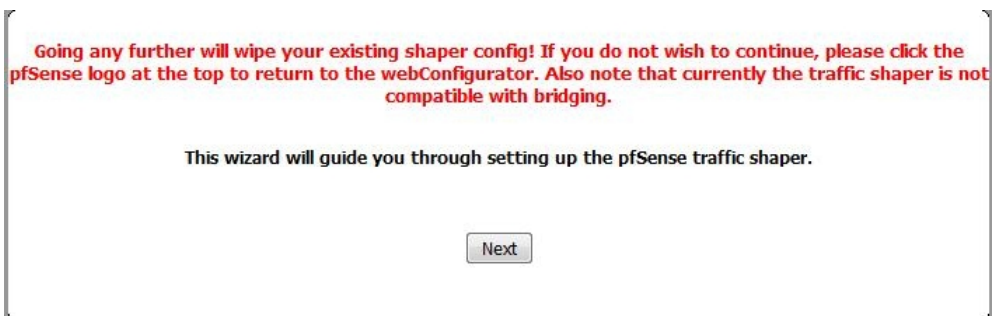


Figure 4.1

Shaper configuration

pfSense Traffic Shaper Wizard

Setup network speeds

Inside:	LAN	This is usually the LAN interface Inside interface for shaping your download speeds
Download:	1536	The download speed of your WAN link in Kbits/second. Note: PPPOE users should take into account PPPOE overhead and put a lower speed here.
Outside:	WAN	This is usually the WAN interface Outside interface for shaping your upload speeds
Upload:	1536	The upload speed of your WAN link in Kbits/second. Note: PPPOE users should take into account PPPOE overhead and put a lower speed here.

Next

Figure 4.2

Voice over IP

pfSense Traffic Shaper Wizard

Enable:  Prioritize Voice over IP traffic  
This will raise the priority of VOIP traffic above all other traffic.

Next

VOIP specific settings

Provider: Asterisk  
Choose Generic if your provider isn't listed.

Address: (Optional) If this is chosen, the provider field will be overridden. This allows you to just provide the IP address of the VOIP adaptor to prioritize. NOTE: You can also use a Firewall Alias in this location.

Bandwidth: 256Kbits/sec Total bandwidth guarantee for VOIP phone(s)

Next

Figure 4.3

7. Additionally you could put the specific address of your device in the Address field. This would only prioritize traffic to and from that IP.
8. Bandwidth : Calculate the number of concurrent calls you can conservatively expect to conduct at one time. Each G.729 call is 29k, each G.711u (ulaw) call is 80k, and each T.38 fax is 100k. Total the bandwidth and record here. This bandwidth will be reserved from your upload bandwidth and not be used even when no calls are in use.

9. The penalty box screen allows you to rate limit traffic to and from a specific IP on your network. You can leave this disabled if you do not need to make use of this at this time.
10. The Peer-to-Peer screen allows you to lower the priority of p2p traffic and even limit its throughput similar to the way the penalty box screen works. You can also specify which p2p protocols you want to enable/disable on your network.
11. Network gaming screen : These settings exist primarily for home users or offices that still participate in 'team building exercises'
12. Other network protocols : by selecting this option, you can raise or lower the priority of each protocol listed. None will be ranked higher than VoIP.
13. After clicking Next on the 'other network protocols' screen, a final confirmation screen will appear. Click Finish and a 'Filter Reload Status' screen will appear. Upon completion, a notification that the rules have been reloaded will now appear. See Figures 4.4 and 4.5

Congratulations! You have now successfully setup your traffic shaping rules. Try running another speed test while conducting a VoIP call. If you set things up correctly you should have a clean call despite the bandwidth testing. Did your upload speed report a lower value? This is likely due to reserving traffic for VoIP.

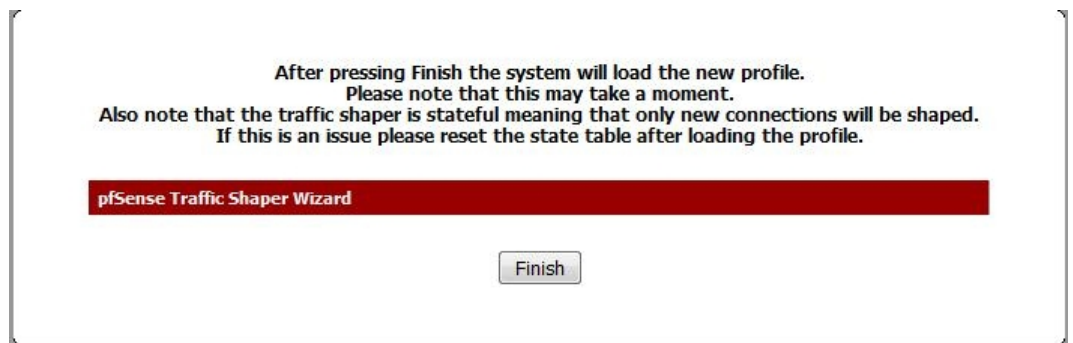


Figure 4.4



Figure 4.5