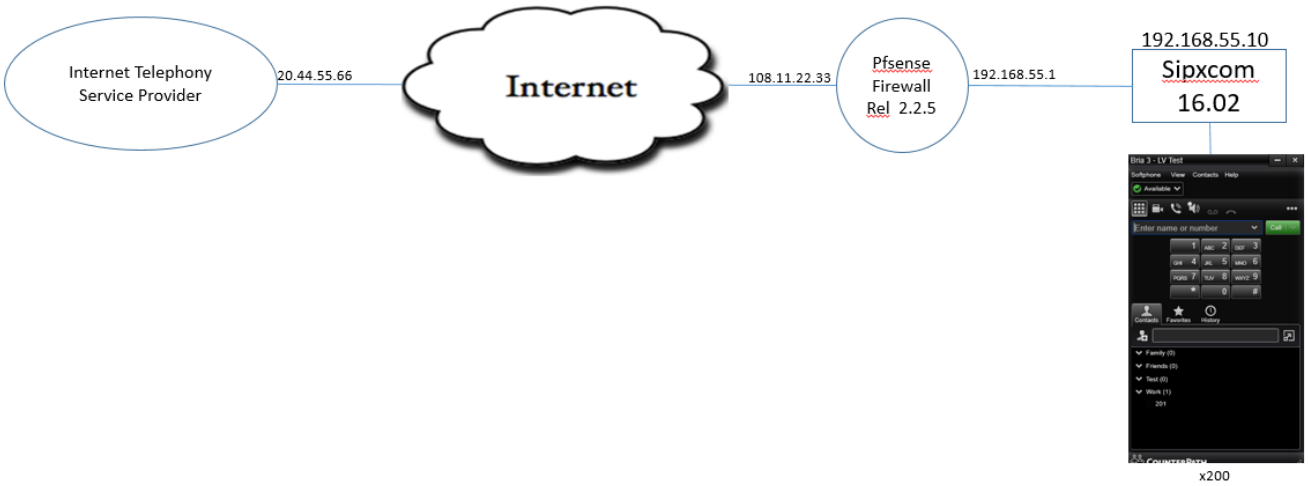
Pfsense Firewall Basic Setup with Sipxcom

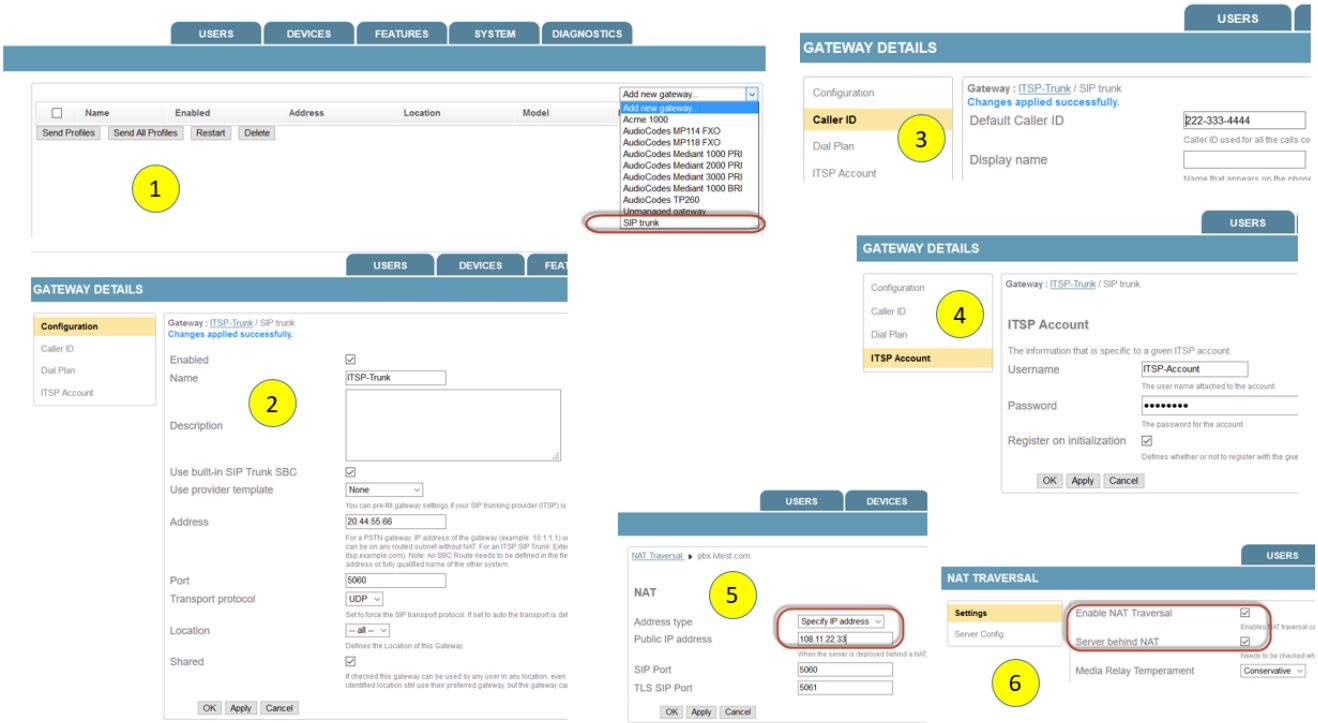
Introduction

The Pfsense opensource firewall is frequently used in network deployments for small and medium enterprises. This document uses the following network topology to illustrate Sipxcom and Pfsense basic configurations for connectivity with an Internet Telephony Service Provider (ITSP). The following assumptions are used in this setup:

1. Pfsense is installed and provides working Internet connectivity to the 19.168.55.x subnet via a LAN interface.
2. Sipxcom is installed with an IP address on the 192.168.55.xx subnet - all services required for SIP trunk and phone connectivity are enabled.
3. The internal SBC application within Sipxcom called **Sipxbridge** is used for SIP trunk connectivity with the ITSP.



Step 1 - Set Up Sipxcom SIP Trunk To the ITSP



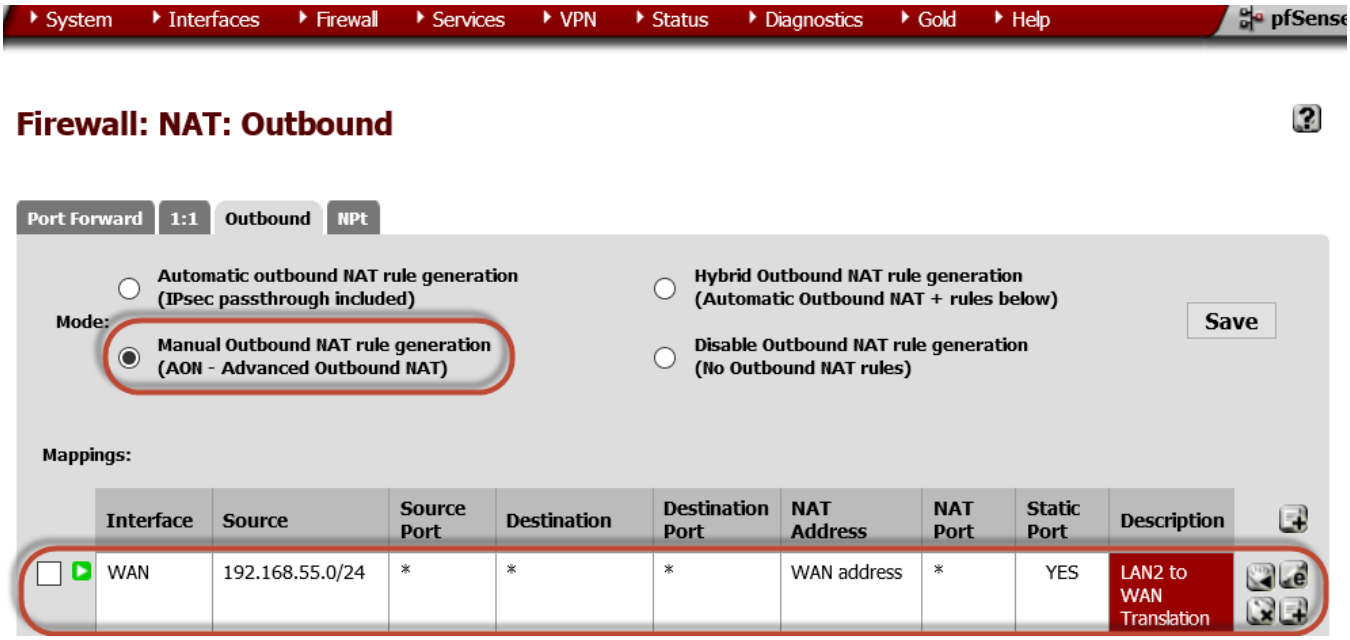
The following steps are used to create a SIP trunk in Sipxcom (each number in the above diagram corresponds to a step number):

1. Go to **Devices->Gateways** and select SIP trunk from the pull-down menu
2. The SIP Trunk configuration menu will be displayed - assign a name to the trunk, provision the public IP address or FQDN for the ITSP, port number, and transport protocol. Hit the **Apply** button.
3. Assign a default **caller-id** to the trunk.

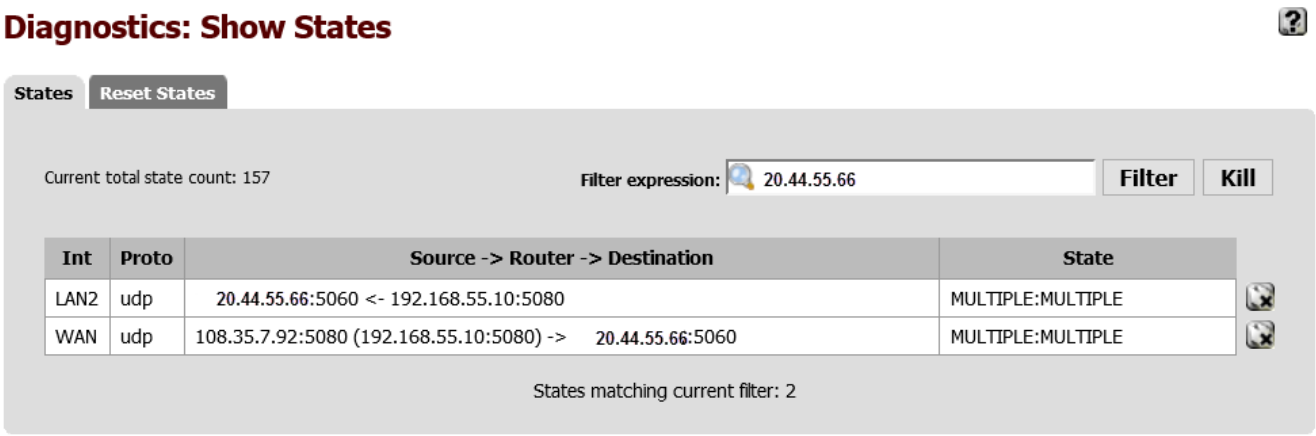
4. Go to ITSP Account menu - if the ITSP is providing a registered SIP trunk, then provision the SIP trunk account name / password information and enable the **Register on Initialization** option. Hit **OK** to create the SIP trunk gateway profile. After 30 seconds or so, Sipxbridge will register the SIP trunk with the ITSP - go to **Diagnostics->SIP Trunk Statistics** and ascertain that the trunk is registered and authenticated. If the ITSP SIP trunk is static (no registration is required), then leave the ITSP account information blank for the Sipxcom SIP trunk gateway. Static SIP trunks are not listed when the **Diagnostics->SIP Trunk Statistics** menu is displayed.
5. Go to **System-NAT Traversal->Server Config** , specify the **Address type** as static, and provision the **Public IP address** with the IP address assigned to the WAN interface in Pfsense. Hit Apply. Although calls will work properly when STUN is enabled, specifying a static public IP address in the NAT traversal field allows calls to work properly in the event that DNS is not available.
6. **Go to System-NAT Traversal->Settings** and ascertain that the **Enable NAT Traversal** and **Server behind NAT** options are enabled.

Step 2 - Provision Pfsense Firewall

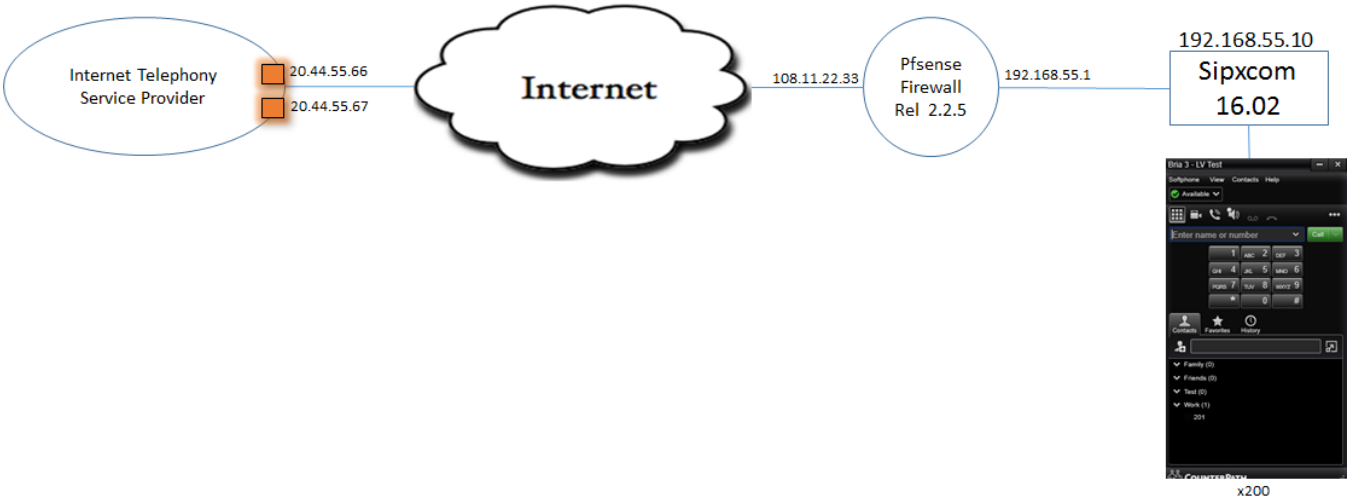
When setting up Pfsense, the following **Firewall->NAT->Outbound** manual outbound NAT rule should of been already defined (assumption 1 in the Introduction). This rule translates private addresses in the 192.168.55.xx subnet to the public IP address assigned to the Pfsense WAN interface (and vice-versa).



If the SIP trunk from the ITSP is a static trunk with no registration parameters, then ascertain that the ITSP sends SIP signaling to the public IP address of Pfsense using port 5080 and not port 5060. For both registered and non-registered trunks, Sipxbridge will ping the ITSP address every 20 seconds, as specified in the **Devices->SIP Trunk SBCs->sipXbridge-1** *Signaling keep-alive interval* setting - this keeps the 5080 firewall port open to receive incoming calls from the ITSP. The Pfsense **Diagnostics->Show States** command is useful in troubleshooting the firewall states, and which ports are open.



Sometimes an ITSP has two or more 'edge servers' for redundancy and load-sharing, with each edge server having the ability to issue incoming external calls to Sipxcom (e.g. see following diagram).



The ITSP edge server with IP address 20.44.55.66 is defined in the SIP trunk - the 20 second heartbeat from Sipxbridge keeps firewall state alive to allow incoming invites from this ITSP edge server. However, a Pfsense **NAT->Port Forwarding** rule must be defined to allow Invites from the 20.44.55.67 to be forwarded to to Sipxcom - the rule is defined here:

System | Interfaces | Firewall | Services | VPN | Status | Diagnostics | Gold | Help

Firewall: NAT: Port Forward

Port Forward | 1:1 | Outbound | NPt

	If	Proto	Src. addr	Src. ports	Dest. addr	Dest. ports	NAT IP	NAT Ports
☐	WAN	TCP/UDP	20.44.55.67	5060 (SIP)	WAN address	5080	192.168.55.10	5080

A Pfsense NAT port forward rule must be defined for every ITSP server beyond the primary server defined in the SIP trunk gateway when an ITSP has multiple edge servers that can issue SIP invites to Sipxcom.