AsteriskNow – IPTables Firewall Configuration

In a previous guide I discussed how to setup an AsteriskNow server with Polycom phone support. In this guide I will illustrate how to tighten up your server's security by using the IPTables firewall already installed in the distribution.

IPTables should already be setup and running on the server, however no rules have been applied. You can verify this by doing the following as the root user:

This should report the following:

Verify there are no rules present:

You should see:

Now it's time to add some rules. You can copy the following text to a file and import it into IPTables:

Save the file as iptables.bak and copy it to /etc/iptables.bak

Now import the file into IPTables:

And verify that the rules have been committed:

You should now see:

Now save the new IPTables settings:

That's it! Your server is now blocking all incoming traffic by

default, and only allowing connections to the ports that are necessary to do it’s job. Specifically:

Port 123 UDP for NTP (Time)
Port 69 UDP for TFTP (Phone provisioning)
Port 5060 UDP for SIP (Phone Calls)
Port 10000-20000 UDP for RTP (Phone Calls)
Port 22 TCP for SSH (SSH Connection)
Port 80 & 443 TCP for HTTP/HTTPS (Web)

If you need to open another port just use the following syntax at the command line:

example for SSH over TCP port 22

To specify a range of ports do the following:

example for RTP over UDP ports 10000-20000

You can then save the new configuration by doing:

And if your completely satisfied and want to back up the configuration do: