



Configuring the iptables firewall on trixbox Pro

Document v1.0 - Last edited 1/9/2009 by Chris Sherwood, SureTeq, Inc.

The iptables firewall is included by default in trixbox Pro, however no rules exist, so it is basically disabled. This document will detail the setup and configuration of the iptables firewall on trixbox Pro.

*****NOTE:** This solution is unsupported by Fonality...if you call in asking them to fix your firewall...they won't know what you're talking about!

Let SureTeq provide you with FtOCC certified trixbox Pro and/or trixbox CE **hourly support!** Hourly rates and support contracts are available. For pricing information and contact details, please [click here](#) or contact us!

1.0 - Install Webmin

So, any Linux guru will call me all sorts of funny names for using Webmin to configure the iptables firewall instead of learning the proper syntax and scripting languages...but I say if it makes it much easier and quicker to configure various services...why not utilize the tools available? Why don't we all still milk cows for our breakfast cereal? Because other people have figured out how to make it easier for the rest of us. So with that said...onto the installation of Webmin.

To install Webmin, you need to log in as 'root' and run the following commands in your Linux CLI:

```
cd /usr/src
wget http://prdownloads.sourceforge.net/webadmin/webmin-1.450-1.noarch.rpm
```

```
rpm -ivh webmin-1.450-1.noarch.rpm
```

*****NOTE:** The version of Webmin available at the time this document is being written is v1.450-1. You may have to adjust the lines above if a newer version is available.

*****NOTE:** Sometimes you will get an error when installing Webmin that states 'Port 10000 is already in use.' If you get that error, you can run the following command to see what is using port 10000:

```
lsof -i :10000
```

If you can figure out what is using that port, kill that process until Webmin installation is complete.

Once the install has finished, you can get to your Webmin console by putting the following into a browser that exists on your LAN:

<https://192.168.200.30:10000> (obviously, replace my IP with your trixbox Pro IP, and note that this is HTTPS...not HTTP). The login is root and your root password.

2.0 - iptables configuration

Once inside Webmin, click on 'Networking' followed by 'Linux Firewall.' If you have never touched the Linux firewall, you should see a sort of wizard for the initial configuration of the firewall.

Allow all traffic

Do network address translation on external interface:

Block all incoming connections on external interface:

Block all except SSH and IDENT on external interface:

Block all except SSH, IDENT, ping and high ports on interface:

Block all except ports used for virtual hosting, on interface:

For our purposes, we want to select 'Block all except SSH and IDENT on external interface:' and then drop the box down and select eth0. Click on 'Setup Firewall' and you will be set up with a default set of firewall rules, and you will be taken to the rules configuration page.

Now it is time to add some more rules. This first set of rules is for normal operation of trixbox Pro (ie. the Hybrid-hosted piece). Fonality pushes all updates to the trixbox Pro server through a set of VPN tunnels that are configured as virtual interfaces. Let's first allow all traffic on these interfaces so that Fonality can still get to our server.

Allow access for VPN tunnels:

In the 'Incoming packets (INPUT)' section, click on the 'Add rule' button. Enter in the following information:

Chain and action details section

Rule comment: VTUN 2

Action to take: Accept

Condition details:

Incoming interface: tun0

Click 'Create' at the bottom of the page. Repeat that process one more time, but use 'VTUN 2' as the Rule comment and 'tun1' as the Incoming interface.

Chain and action details

Part of chain Incoming packets (INPUT)

Rule comment VTUN 1

Action to take Do nothing Accept Drop Reject Userspace

Exit chain Log packet Run chain

Reject with ICMP type Default Type icmp-net-unreachable

The action selected above will only be carried out if all the conditions below are met.

Condition details

Source address or network <Ignored>

Destination address or network <Ignored>

Incoming interface Equals tun0

Outgoing interface <Ignored>

Fragmentation Ignored Is fragmented Is not fragmented

Network protocol <Ignored> TCP

Both of your VTUNs should now have full access to the trixbox Pro server.

*****NOTE:** The rest of these rules are optional, and should only be opened up if absolutely necessary.

Allow access for SIP connections:

To add SIP connectivity to your server we need to add two rules. In the 'Incoming packets (INPUT)' section, click on the 'Add rule' button. Enter in the following information:

Chain and action details section

Rule comment: SIP 5060

Action to take: Accept

Condition details:

Network protocol: Equals UDP

Destination TCP or UDP port: Equals Port(s): 5060

Click 'Create' at the bottom of the page.

Now we need to add our SIP RTP ports. In the 'Incoming packets (INPUT)' section, click on the 'Add rule' button. Enter in the following information:

Chain and action details section

Rule comment: SIP RTP

Action to take: Accept

Condition details:

Network protocol: Equals UDP

Destination TCP or UDP port: Equals Port Range: 10000 to 20000

Click 'Create' at the bottom of the page.

You should now have two SIP rules in the summary page:

<input type="checkbox"/> Accept	If protocol is UDP and destination port is 5060
<input type="checkbox"/> Accept	If protocol is UDP and destination port is 10000:20000

Allow access for IAX2 trunks:

If you have any incoming IAX2 trunks or if you are using Linked Server, you will want to open up IAX2. In the 'Incoming packets (INPUT)' section, click on the 'Add rule' button. Enter in the following information:

Chain and action details section

Rule comment: IAX2

Action to take: Accept

Condition details:

Network protocol: Equals UDP

Destination TCP or UDP port: Equals Port(s): 4569

Click 'Create' at the bottom of the page.

Allow access for Webmin access:

Since we are using Webmin for configuration, we probably want this to be open. In the 'Incoming packets (INPUT)' section, click on the 'Add rule' button. Enter in the following information:

Chain and action details section

Rule comment: Webmin

Action to take: Accept

Condition details:

Network protocol: Equals TCP

Destination TCP or UDP port: Equals Port(s): 10000

Click 'Create' at the bottom of the page.

Allow access for DNS requests:

You will need DNS open because most likely, your phones use the DNS server of the trixbox Pro. In the 'Incoming packets (INPUT)' section, click on the 'Add rule' button. Enter in the following information:

Chain and action details section

Rule comment: DNS

Action to take: Accept

Condition details:

Network protocol: Equals UDP

Destination TCP or UDP port: Equals Port(s): 53

Click 'Create' at the bottom of the page.

Allow access for DHCP requests:

You will need DHCP open because most likely, your phones use the DHCP server of the trixbox Pro. In the 'Incoming packets (INPUT)' section, click on the 'Add rule' button. Enter in the following information:

Chain and action details section

Rule comment: DHCP

Action to take: Accept

Condition details:

Network protocol: Equals UDP

Destination TCP or UDP port: Equals Port(s): 68

Click 'Create' at the bottom of the page.

Allow access for TFTP:

You will need TFTP open because most likely, your phones use the TFTP server of the trixbox Pro. In the 'Incoming packets (INPUT)' section, click on the 'Add rule' button. Enter in the following information:

Chain and action details section

Rule comment: TFTP

Action to take: Accept

Condition details:

Network protocol: Equals UDP

Destination TCP or UDP port: Equals Port(s): 69

Click 'Create' at the bottom of the page.

Allow access for ICMP:

Using ICMP (ping) is a great tool for network troubleshooting. If you want to allow ICMP, add this rule. In the 'Incoming packets (INPUT)' section, click on the 'Add rule' button. Enter in the following information:

Chain and action details section

Rule comment: ICMP

Action to take: Accept

Condition details:

Network protocol: Equals ICMP

Click 'Create' at the bottom of the page.

3.0 - Applying configuration changes

Now that we have a good set of rules for access to our trixbox Pro server, it is now time to apply those rules. From the Rules Summary page, click 'Apply Configuration' towards the bottom of the screen. The window refreshes, and your firewall is now in place.

Keep in mind that this document assumes that eth0 is the only network card in your server, and that it is the 'external' network. If you have eth0 and eth1, you will want to update your rule set accordingly.
