



Techotopia

Safari Power Saver
Click to Start Flash Plug-in

THIS CHRISTMAS, GIVE **SHELTER**.

\$ Enter Amount

HELP A CHILD
IN NEED NOW



DOING THE
MOST GOOD

AdChoices

[Download SSH](#)

[Download Install](#)

[SSH Server](#)

[Remote Access](#)

Configuring Ubuntu Linux Remote Access using SSH

Like 7 people like this.

From Techotopia

2



SHARE

Previous
Managing Ubuntu
Linux Users and
Groups

Table of Contents

Next

Remote Access to the
Ubuntu Linux Desktop

Purchase and download the fully updated Ubuntu 10.10 version of this eBook in PDF & ePub formats for only \$9.99

PDF/ePub version contains 40 chapters and over 225 pages. Download preview.

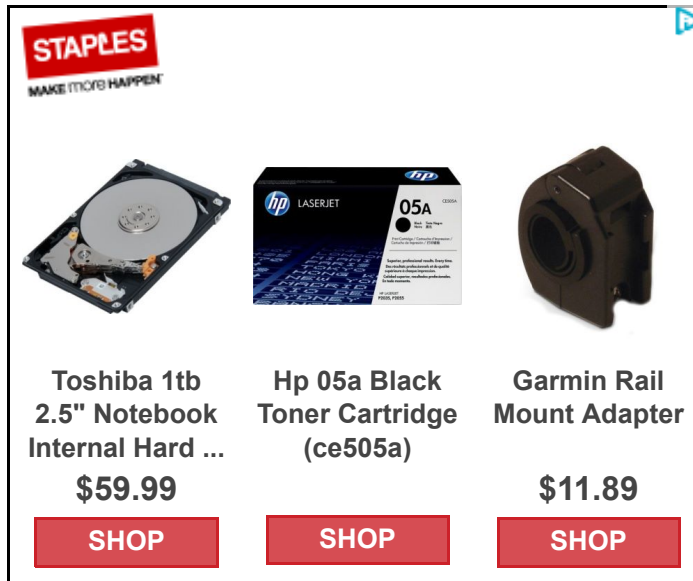
[Buy Now](#)

SSH is a TCP/IP service that provides a secure mechanism for remotely logging into one system over either a local network or the internet into another system. SSH also provides the ability to transfer files between remote systems. When a user logs into a remote system using SSH, they receive a command prompt allowing them to enter commands on the remote system as if they were sitting at the remote system and had opened a terminal session.

In this chapter we will cover the steps necessary to configure an Ubuntu Linux system to accept SSH connections. This involves installing the SSH server on the local systems and configuring the firewall to allow SSH connections.

Contents

- 1 Installing SSH on an Ubuntu Linux System
- 2 Configuring the Ubuntu Linux Firewall to Allow SSH Connections
- 3 Using SSH on Ubuntu Linux
- 4 Copying files using SSH
- 5 Disabling the SSH Server



Product	Price	Action
Toshiba 1tb 2.5" Notebook Internal Hard Drive	\$59.99	SHOP
Hp 05a Black Toner Cartridge (ce505a)		SHOP
Garmin Rail Mount Adapter	\$11.89	SHOP



iOS 8 App Development Essentials

iOS 8 App Development Essentials eBook

\$14.99

[Buy eBook](#)

eBookFrenzy.com

Safari Power Saver
Click to Start Flash Plug-in

Installing SSH on an Ubuntu Linux System

In order for a system to accept SSH connections the system must first be running the SSH server. By default, Ubuntu does not install the SSH server so the first step is to ensure that the server is installed. This can be performed using either the Synaptic Package Manager or the apt-get command-line tool.

To install using the Synaptic Package Manager, select the *System* desktop menu and then click on *Synaptic Package Manager* in the *Administration* sub-menu. Enter your password when prompted to do so. Click on the Search button in the toolbar and search for *openssh-server*. After the search completes, you will see *openssh-server* in the package list. Simply click on the check box next to this item and follow the instructions to install the SSH server package. When you are ready to initiate the installation, click the *Apply* button in the Synaptic toolbar.

To install from the command line, begin by opening a terminal window by selecting the *Applications* menu and selecting *Terminal* from the *Accessories* menu. In the terminal window enter the following command and press enter to execute it:

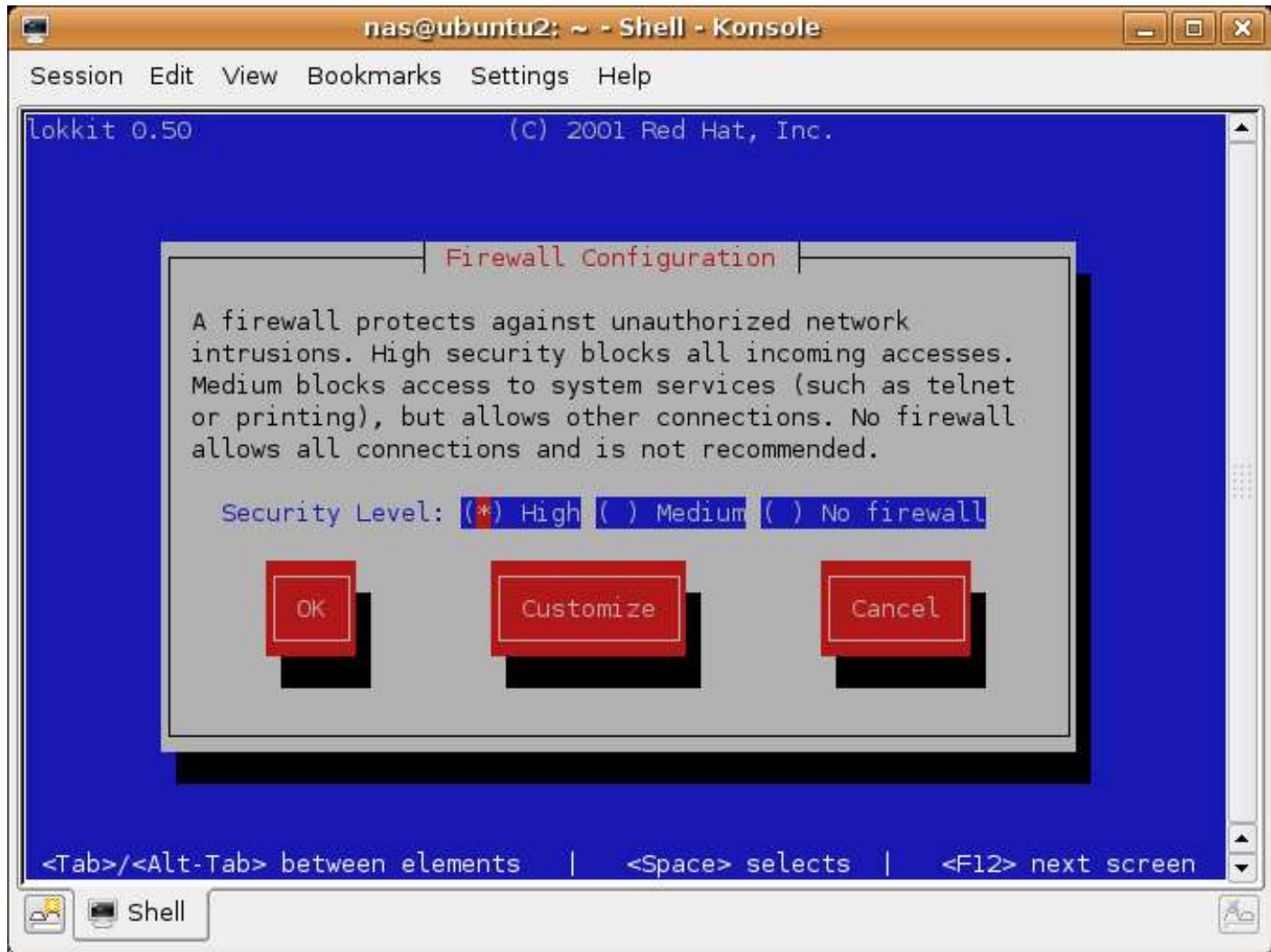
```
sudo apt-get install openssh-server
```

The installation process will download the SSH server, install it and start the service running in the background. You may now attempt to connect from a remote system (see below for details of how to do this). If you receive a "connection refused" message when you try to connect you may need to configure the firewall to allow SSH connections to be established to this system.

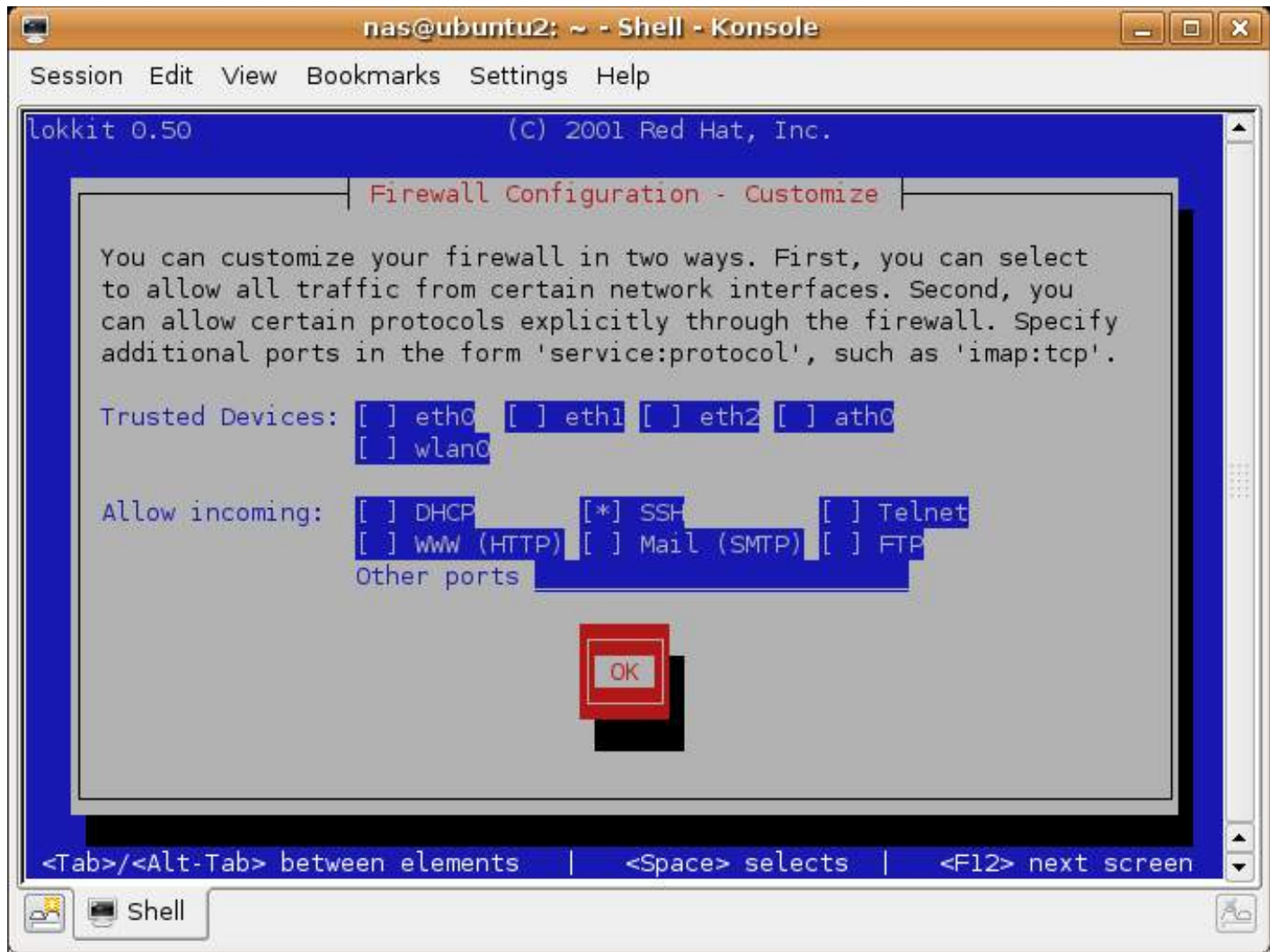
Configuring the Ubuntu Linux Firewall to Allow SSH Connections

If you are using a firewall to protect your system you will need to allow SSH connections before you be able to connect from a remote system. If you are using the basic firewall configuration (see Basic Ubuntu Linux Firewall Configuration) you can allow SSH connections using the *lokkit* tool.

If you do not already have a terminal window open start one by selecting *Terminal* from the *Accessories* sub-menu of the desktop *Applications* menu. The *lokkit* screen will appear as follows:



Use the Tab key to move the *Customize* button and press *Enter*. On the Customize screen Tab to the SSH entry and press space so that an asterisk (*) appears next to the setting to show it is enabled. The screen should now appear as follows:



Tab to the *OK* button and press *Enter* to return to the main screen. Tab once again to the *OK* button and press enter to exit *lokkit*.

If you have configured your firewall using the Firestarter tool you will need to set up an incoming connection policy to allow connections to the SSH service. Configuring Firestarter is covered in detail in [Using Firestarter to Configure an Ubuntu Linux Firewall](#).

Using SSH on Ubuntu Linux

SSH can be used to log into your system from a remote system. It is also possible to test that the SSH server is running and accessible from the local machine. SSH connections are established using the *ssh* client utility.

To connect from your local machine back to itself use the following command:

```
ssh -l username ipaddresss
```

Where *username* is the name of the user you wish to log in as and *ipaddress* is the IP address of your system. You can also substitute the hostname of the system in place of the IP address. If you do not know the IP address run the *ipconfig*

command in a terminal window. This will output information similar to:

```
eth0      Link encap:Ethernet  HWaddr 00:13:72:0B:14:57  
          inet addr:192.168.2.21  Bcast:192.168.2.255  Mask:255.255.255.0  
          inet6 addr: fe80::213:72ff:fe0b:1457/64 Scope:Link  
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1  
          RX packets:4261067 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:4409081 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:100  
          RX bytes:2068332349 (1.9 GiB)  TX bytes:2408187471 (2.2 GiB)  
          Base address:0xcce0 Memory:fe3e0000-fe400000
```

In the above output the IP address is shown as *inet addr:*, in this case 192.168.2.21. Similarly, the hostname may be obtained by running the *hostname* tool at a terminal command prompt.

To connect from a remote system perform the same steps above using either the IP address or host name of the remote host to which you connect. Enter your password when prompted and you will find yourself logged into the remote system.

Copying files using SSH

The SSH service provides a mechanism for copying files to and from a remote system. Copying is performed using the *scp* utility. To copy a file to a directory on a remote system, execute the following command:

```
scp myfile.txt username@192.168.2.21:/home/demo
```

Where *myfile.txt* is the name of the file to be uploaded to the remote system, *username* is the name of user account to be used to log into the remote system, 192.168.2.1 is replaced by the real IP address or hostname of the system and /home/demo represents the directory into which the file should be copied.

The above file could similarly be copied from the remote system to the local system as follows:

```
scp username@192.168.2.21:/home/demo/myfile.txt .
```

The above command will copy the remote file to the current directory on the local system.

Disabling the SSH Server

Having configured the system to run the SSH server we can now look at how to disable it. As mentioned previously, the SSH server runs in the background as a service. In order to disable SSH we need to turn off the SSH service. This can be achieved using the *Services* tool. To launch the services tool click on the desktop *System* menu and select *Services* from the *Administration* sub-menu. By default, the configuration options in the Services tool are read-only. In order change these settings, click on the *Unlock* button and enter your password.

The Services tool will appear containing a list of all available services. Scroll down to find the *Remote shell server* entry as shown below:

Safari Power Saver
Click to Start Flash Plug-in

Looking for
open houses
nearby?

Zillow

LEGAL



Uncheck the box next to the SSH entry and click on the *Close* button. The SSH server is now disabled. To re-enable the server, repeat the above steps and check the box next to *Remote shell server* to enable the service.



Purchase and download the fully updated Ubuntu 10.10 version of this eBook in PDF & ePub formats for only \$9.99

PDF/ePub version contains 40 chapters and over 225 pages. Download preview.

[Buy Now](#)

Retrieved from "http://www.techotopia.com/index.php/Configuring_Ubuntu_Linux_Remote_Access_using_SSH"

Flash Player Power Saver
Click to Start Flash Plug-in

A winter scene with two people walking in the snow. One person is carrying a large box, and the other is wearing a Santa hat. There are bare trees and a house in the background.

**Big Brands. Big Savings.
Made Easy.**

Discover Deals™

[Shop Deals](#)

- This page was last modified 18:21, 11 May 2009.
- Copyright 2014 Payload Media. All Rights Reserved.