Configuring Services: SSH Menu

Version: 3408

Table of Contents

Router Installation and Configuration Manual/Configuring Services: SSH Menu....1
Configuring the SSH Service....3
Enabling SSH at Boot-time....4
Disabling SSH at Boot-time....4
Starting the SSH Service....5
Stopping the SSH Service....5
Returning to the Service Configuration Menu....5
Disabling the Telnet Service....6

Router Installation and Configuration Manual/Configuring Services: SSH Menu

This chapter describes how to configure the secure shell (SSH) service on the ImageStream router. The secure shell service allows you to access the ImageStream router across a secure, encrypted link. SSH is generally used as an alternative to telnet and FTP for remote access. This chapter describes the basic configuration of the SSH service, including the port, IP address used by SSH, and other information. More advanced configurations are possible.

This chapter includes the following topics:

- ◊ Configuring the SSH service
- ◊ Enabling SSH at boot-time
- ◊ Disabling SSH at boot-time
- ◊ Starting the SSH service
- ◊ Stopping the SSH service
- ◊ Disabling the Telnet service

After logging in, the main menu is displayed (your menu may look slightly different):

```
ISis-Router main menu
1. Configuration menu
2. Show interface status
3. Advanced
4. Router software management
5. Backup/Restore
6. halt/reboot
0. Log off
```

Select menu option 1, Configuration menu, and press**Enter** to configure the router. The Configuration menu should appear (your menu may look slightly different):

```
Configuration menu
1. AAA (Password) Configuration
2. Global configuration
3. Network interface configuration
4. Firewall and QOS configuration
5. Service configuration
6. Dynamic routing configuration
7. Save configuration to flash
0. ISis-Router main menu
```

Select menu option 5, Service configuration, and press **Enter** to configure the router's service configuration settings. The Service configuration menu will be displayed (again, your menu may look slightly different):

```
Service configuration
1. System scheduler (cron), (running)
2. Dialout PPP, (stopped)
```

```
3. IPSec VPN (Free S/Wan), (stopped)
4. NetFlow exporter (nprobe), (stopped)
5. network interfaces (sand), (running)
6. sconsole (mgetty), (running)
7. snmp (net-snmp), (stopped)
8. ssh (OpenSSH), (running)
0. Configuration menu
```

Select menu option 8, ssh (OpenSSH), (running), and press **Enter** to configure the router's SSH settings. The ssh menu will be displayed (again, your menu may look slightly different):

```
ssh (OpenSSH), (running)
1. Configure ssh (OpenSSH)
2. Enable ssh on boot
3. Disable OpenSSH on boot
4. Start ssh
5. Stop ssh
6. Restore to default configuration
0. Service configuration
```

To configure SSH, select menu option 1, Configure ssh (OpenSSH), and press **Enter**. This will open the default SSH configuration file in your default text editor (your file may look slightly different):

```
# This is ssh server systemwide configuration file.
Port 22
ListenAddress 0.0.0.0
HostKey /etc/ssh/ssh_host_key
ServerKeyBits 768
LoginGraceTime 600
KeyRegenerationInterval 3600
PermitRootLogin yes
StrictModes yes
X11Forwarding no
X11DisplayOffset 10
PrintMotd yes
KeepAlive yes
UseLogin no
#
# Loglevel replaces QuietMode and FascistLogging
#
SyslogFacility AUTH
#LogLevel INFO
#
# For this to work you will also need host keys in /etc/ssh/ssh_known_hosts
#
RhostsRSAAuthentication no
#
# Don't read ~/.rhosts and ~/.shosts files
#
IgnoreRhosts yes
RhostsAuthentication no
#
# Uncomment if you don't trust ~/.ssh/known_hosts for RhostsRSAAuthentication
#
#IgnoreUserKnownHosts yes
RSAAuthentication yes
# To disable tunneled clear text passwords, change to no here! PasswordAuthentication yes
PermitEmptyPasswords no
```

```
HostKey /etc/ssh/ssh_host_rsa_key HostKey /etc/ssh/ssh_host_dsa_key
```

Configuring the SSH Service

ImageStream routers use OpenSSH. OpenSSH is an open source version of the SSH suite of network connectivity tools. Unlike telnet and ftp, ssh and the companion scp tool encrypt all traffic (including passwords) to effectively eliminate eavesdropping, connection hijacking, and other network-level attacks.

The order of the commands entered into this file is not important. In most cases, the default configuration file is sufficient. **Do not make changes to this file unless you are an advanced user experienced with OpenSSH.**

The first step is to configure the port used by the SSH service. By convention, port 22 has been reserved for SSH. Use the Port keyword to specify this value. The syntax for this command is:

```
Port { number }
```

The first part of the entry (Port) specifies the variable to be set. The second part is the value of the variable. Select an unused port. A list of ports is available on the router in the **/etc/services** file.

The other basic configuration keyword is the **ListenAddress** keyword. By default, the SSH service will respond on all addresses configured on the router. To restrict SSH access to a particular IP address, specify that address using the **ListenAddress** keyword.

The ListenAddress keyword syntax is:

```
ListenAddress { IP address } : [ port ]
```

For example:

```
ListenAddress 192.168.100.1
```

Multiple **ListenAddress** options are permitted. If a port is not specified, the Port keyword described above must appear before the ListenAddress directive.

Many other keywords, both the ones listed in the default configuration and others, are supported. These additional keywords should only be adjusted by experienced administrators. If you have not used OpenSSH or similar SSH implementations, do not change any other values in this file.

Once you have entered all of the configurations for your site in this file, save the file by pressing Control-X. If you have made changes to the file, the router will prompt you to save the file at the bottom of the screen:

```
Save modified buffer (ANSWERING "No" WILL DESTROY CHANGES) ? Y Yes N No    ^C Cancel
```

Press Y on your keyboard to save your configuration. The router will then prompt you for a file name:

```
File Name to write: /etc/ssh/sshd_config ^C Cancel
```

You should accept the default filename. If you choose to save the file in a different location, the router will not automatically locate the file and instate any changes. Press Enter on the keyboard to accept the default. The ^C notation indicates the key combination Control-C. You may press Control-C at any time during the save process to return to the file.

Note: You must save the settings to the router's non-volatile flash memory! If the router is rebooted before saving, your changes will be lost! See Chapter 26, Router Installation and Configuration Manual/Backup/Restore Menu: Managing Configurations for more information.

Once you have saved the file by pressing Enter, the router will return you to the SSH menu:

```
ssh (OpenSSH), (running)
1. Configure ssh (OpenSSH)
2. Enable ssh on boot
3. Disable OpenSSH on boot
4. Start ssh
5. Stop ssh
6. Restore to default configuration
0. Service configuration
```

Enabling SSH at Boot-time

2. Enable ssh on boot

Selecting this menu option enables the SSH service when the router is booted. This does not start the SSH service on the router if it is not running, unless the router is first rebooted. By default, SSH is disabled on boot. To enable SSH at boot-time, select this menu option by pressing 2 and **Enter**. The router will display the following message:

```
ssh enabled on boot.
```

If SNMP has already been enabled on boot, the router will display the message:

```
sssh already enabled on boot.
```

The resulting message will only be displayed for a few seconds, and then you will be returned to the SSH menu.

Disabling SSH at Boot-time

3. Disable ssh on boot

Selecting this menu option disables the SSH service when the router is booted. This does not stop the SSH service if it is running, unless the router is first rebooted. To disable SSH on boot, select this menu option by pressing 3 and **Enter**. The router will display the following message:

```
ssh disabled on boot.
```

If SSH has already been disabled on boot, the router will display the message:

```
ssh already disabled on boot.
```

The resulting message will only be displayed for a few seconds, and then you will be returned to the SSH menu.

Starting the SSH Service

4. Start ssh

Selecting this menu option starts the SSH service on the router. Starting SSH does not automatically enable the SSH service when the router is booted. To start the SSH service, select this menu option by pressing 4 and **Enter**. The router will display the following message:

```
Starting ssh...done.
```

The message will only be displayed for a few seconds, and then you will be returned to the SSH menu.

Stopping the SSH Service

5. Stopping ssh

Selecting this menu option stops the SSH service on the router. Stopping SSH does not automatically disable the SSH service when the router is booted. To stop the SSH service, select this menu option by pressing 5 and **Enter**. The router will display the following message:

```
Stopping ssh...done.
```

The message will only be displayed for a few seconds, and the you will be returned to the SSH menu.

Returning to the Service Configuration Menu

0. Service configuration

Selecting this menu option returns you to the "Service configuration" menu. The router will display the Service configuration menu:

```
Service configuration
1. System scheduler (cron), (running)
2. Dialout PPP, (stopped)
3. IPSec VPN (Free S/Wan), (stopped)
4. NetFlow exporter (nprobe), (stopped)
5. network interfaces (sand), (running)
6. sconsole (mgetty), (running)
7. snmp (net-snmp), (stopped)
8. ssh (OpenSSH), (running)
0. Configuration menu
```

Disabling the Telnet Service

There is no service menu to disable telnet. It has to be commented out via the /etc/inetd.conf file. To do this you'll need to go to the Advanced menu (option 3) then Bash shell (option 1).

- Step 1 Edit the /etc/inetd.conf file:

```
router:/usr/local/sand# pico /etc/inetd.conf
```

Use the arrow keys to go to the end of the file and put a '#' sign in front of the last line like so:

```
#telnet  stream  tcp     nowait  root    /usr/sbin/in.telnetd /usr/sbin/in.telnetd
```

Then hit <control - x> to exit and save out the file.

- Step 2 Restart inetd:

```
router:/usr/local/sand# killall -HUP inetd
```