Configuring SSH (Secure Shell) for Remote Login on a Cisco Router

Prior to the introduction of SSH in the Cisco IOS, the only remote login protocol was Telnet. Although quite functional, Telnet is a non-secure protocol in which the entire session, including authentication, is in clear text and thus subject to snooping. (See the soundtraining.net YouTube video on Protocol Analysis with Wireshark for a demonstration.)
SSH is both a protocol and an application that replaces Telnet and provides an encrypted connection for remote administration of a Cisco network device such as a router, switch, or security appliance.
The Cisco IOS includes both an SSH server and an SSH client. This document is concerned only with the configuration of the SSH server component.

Prerequisites

Software

The SSH server component requires that you have an IPSec (DES or 3DES) encryption software image from Cisco IOS Release 12.1(1)T or later installed on your router. Advanced IP services images include the IPSec component. This document was written using c2800nm-advipservicesk9-mz.123-14.T5.bin and c870-advipservicesk9-mz.124-15.T6.bin.

Pre-configuration

You must configure a hostname and a domain name on your router. For example:

```
router01#
router01#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
router01(config)#hostname router01
router01(config)#ip domain-name soundtraining.net
router01(config)#
```

You must also generate an RSA keypair for your router which automatically enables SSH. In the following example, note how the keypair is named for the combination of hostname and domain name that were previously configured. The modulus represents the key length. Cisco recommends a minimum key length of 1024 bits (even though the default key length is 512 bits):

```
router01(config)#
router01(config)#crypto key generate rsa
The name for the keys will be: router01.soundtraining.net
Choose the size of the key modulus in the range of 360 to 2048 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys ...[OK]

router01(config)#
```

Finally, you must either use an AAA server such as a RADIUS or TACACS+ server or create a local user database to authenticate remote users and enable authentication on the terminal lines. For the purpose of this document, we'll create a local user database on the router. In the following example, the user "donc" was created with a privilege level of 15 (the maximum allowed) and given an encrypted password of "p@ss5678". (The command "secret" followed by "0" tells the router to encrypt the following plaintext password. In the router's running configuration, the password would not be human readable.) We also used line configuration mode to tell the router to use its local user database for authentication (login local) on terminals lines 0-4.

```
router01(config)#
router01(config)#username donc privilege 15 secret 0 p@ss5678
router01(config)#line vty 0 4
router01(config-line)#login local
router01(config-line)#
```

Enabling SSH

To enable SSH, you must tell the router which keypair to use. Optionally, you can configure the SSH version (it defaults to SSH version 1), authentication timeout values, and several other parameters. In the following example, we told the router to use the previously created keypair and to use SSH v 2:

```
router01(config)#
router01(config)#ip ssh version 2
router01(config)#ip ssh rsa keypair-name router01.soundtraining.net
router01(config)#
```

You can now log on to your router securely using an SSH client. The SSH client we recommend is TeraTerm (http://ttssh2.sourceforge.jp/).

Soundthinking point: To delete the RSA key-pair, use the global configuration command **crypto key zeroize rsa**. Deleting the RSA key-pair automatically disables the SSH server.

Viewing SSH Configurations and Connections

You can use the privileged mode commands "view ssh" and "view ip ssh" to view SSH configurations and connections (if any). In the following example, the SSHv1 configuration from a Cisco 871 router is verified using "show ip ssh" and a single SSHv1 connection is displayed using the command "show ssh". Notice that we did not enable SSHv2 on this router, so it defaulted to SSH version 1.99. Also note in the output of the "show ssh" command that SSH version 1 defaults to 3DES. SSHv2 supports AES, a more robust and efficient encryption technology. SSHv2 is also not subject to the same security exploits as SSHv1. soundtraining.net recommends the use of SSHv2 and disabling a dropback to SSHv1. Enabling SSHv2 disables SSHv1. This example is included only to demonstrate backwards compatibility:

```
router04#
router04#show ip ssh
SSH Enabled - version 1.99
Authentication timeout: 120 secs; Authentication retries: 3
router04#
router04#show ssh
Connection      Version Encryption      State                   Username
2               1.5     3DES            Session started         donc
%No SSHv2 server connections running.
router04#
```

Student Exercise: Enabling SSH on a Cisco Router for Secure Remote Login

1. Ensure you have a hostname configured on your router that corresponds with your position on the classroom network diagram:
   Router#**conf t**
   Router(config)#**hostname router23**
2. You must also configure a domain name:
   Router(config)#**ip domain-name soundtraining.class**
3. Generate an RSA keypair with a key length of 1024 bits using the following sequence of commands:
   router(config)#
   router(config)#**crypto key generate rsa**
   The name for the keys will be: routerXX.soundtraining.class (where XX is your router number)
   Choose the size of the key modulus in the range of 360 to 2048 for your
   General Purpose Keys. Choosing a key modulus greater than 512 may take
   a few minutes.
   How many bits in the modulus [512]: **1024**
   % Generating 1024 bit RSA keys ...[OK]
4. Create a username in the router's local database for SSH authentication using the following command (for the purpose of the exercise, use the username "user15"):
   router01(config)#**username user15 privilege 15 secret 0 p@ss5678**
5. Enable login authentication against the local database when logging in to a terminal line with the following commands:
   router01(config)#**line vty 0 4**
   router01(config-line)#**login local**
6. Enable SSHv2 and the previously configured keypair with the following commands:
   router01(config)#**ip ssh version 2**
   router01(config)#**ip ssh rsa keypair-name routerXX.soundtraining.class** (where XX is your router number)
7. Attempt to login to your router using the TeraTerm SSH client. (If you haven't already downloaded and installed it, it's available on the classroom website. Ask your instructor for assistance, if necessary.)