S-Series Secure Management

This application note describes how to enable the SSH and SSL secure management features on the S-Series platforms.

Version 1.5
June 1, 2006

FORCE10™

Table of Contents

Introduction

Enabling secure management via Secure SHell (SSH) or Secure Sockets Layer (SSL/HTTPS) on the S-Series is a four-step process. SSH and SSL both provide an encrypted transport session between the management station and switch.

1. Generate the SSH keys or SSL certificates offline.
2. Copy the SSH keys or SSL certificates to the switch using TFTP.
3. Enable the secure management server (SSH or HTTPS) on the switch.
4. Disable the insecure version of the management server (Telnet or HTTP).

If you received this document as part of a .zip file, the file should contain two directories: ssh and ssl (the directories are also on the S-Series CD-ROM). If you did not get the entire .zip file, please contact your Force10 account team.

- The ssh directory has example RSA1, RSA2 and DSA keys and a shell script called “generate-keys.sh” that can be used to generate your own SSH keys.
- The ssl directory has example certificates and a shell script called “generate-pem.sh” that can be used to generate your own SSL certificates.

The scripts provided use OpenSSH (http://www.openssh.org/) and OpenSSL (http://www.openssl.org/) for key and certificate generation. Other free and commercial tools exist that can provide the same functionality and you can use them if you like.

For additional options and commands related to the Telnet, SSH and HTTP/HTTPS features, please consult the SFTOS manuals.

Enabling SSH

1. Generate the SSH keys using the script in the ssh directory, or copy the example keys (which end in .key) to your TFTP server.

2. Copy the keys to NVRAM with TFTP as follows from this example, using the IP address of your TFTP server. For SSHv1, copy the RSA1 key. For SSHv2, copy the RSA1, RSA2, and DSA keys, as shown below.

```
SFTOS #copy tftp://192.168.0.10/rsa1.key nvram:sshkey-rsa1

Mode..................................... TFTP
Set TFTP Server IP....................... 192.168.0.10
TFTP Path.....................................
TFTP Filename............................ rsa1.key
Data Type................................ SSH RSA1 key

Management access will be blocked for the duration of the transfer
Are you sure you want to start? (y/n) y

TFTP SSH key receive complete... updating key file...

Key file transfer operation completed successfully
```

```
SFTOS #copy tftp://192.168.0.10/rsa2.key nvram:sshkey-rsa2

Mode..................................... TFTP
Set TFTP Server IP....................... 192.168.0.10
TFTP Path.....................................
TFTP Filename............................ rsa2.key
Data Type................................ SSH RSA2 key

Management access will be blocked for the duration of the transfer
Are you sure you want to start? (y/n) y

TFTP SSH key receive complete... updating key file...

Key file transfer operation completed successfully

SFTOS #copy tftp://192.168.0.10/dsa.key nvram:sshkey-dsa

Mode..................................... TFTP
Set TFTP Server IP....................... 192.168.0.10
TFTP Path.....................................
TFTP Filename............................ dsa.key
Data Type................................ SSH DSA key

Management access will be blocked for the duration of the transfer
Are you sure you want to start? (y/n) y

TFTP SSH key receive complete... updating key file...

Key file transfer operation completed successfully
```

3. Enable the SSH server with this command.

SFTOS Version <= 2.2.1	SFTOS Version >= 2.3.1
`(SFTOS) #ip ssh server enable`	`SFTOS (Config)#ip ssh server enable`

To verify that the server has started, use this command to show the SSH server status and check the log file for the following messages.

```
SFTOS #show ip ssh

SSH Configuration

Administrative Mode: ......................... Enabled
Protocol Levels: ............................. Versions 1 and 2
SSH Sessions Currently Active: ................ 0
Max SSH Sessions Allowed: ..................... 5
SSH Timeout: ................................. 5

SFTOS #show logging buffered

   JAN 01 00:31:54 192.168.0.34-1 UNKN[222273672]: sshd_control.c(444) 15 %% SSHD: sshdListenTask
started
   JAN 01 00:31:54 192.168.0.34-1 UNKN[209305936]: sshd_main.c(596) 16 %% SSHD: successfully
opened file ssh_host_dsa_key
   JAN 01 00:31:54 192.168.0.34-1 UNKN[209305936]: sshd_main.c(609) 17 %% SSHD: successfully
loaded DSA key
   JAN 01 00:31:54 192.168.0.34-1 UNKN[209305936]: sshd_main.c(631) 18 %% SSHD: successfully
opened file ssh_host_rsa_key
   JAN 01 00:31:54 192.168.0.34-1 UNKN[209305936]: sshd_main.c(643) 19 %% SSHD: successfully
loaded RSA2 key
   JAN 01 00:31:56 192.168.0.34-1 UNKN[209305936]: sshd_main.c(353) 20 %% SSHD: Done generating
server key
```

Using an SSH client, connect to the switch and login to verify that the SSH server is working.

4. Once you have verified that you can connect to the switch with an SSH client, the Telnet server can be disabled with this command for additional security, if it was enabled. The Telnet server is disabled by default.

SFTOS Version <= 2.2.1	SFTOS Version >= 2.3.1
(SFTOS) #**no ip telnet server enable**	SFTOS (Config)#**no ip telnet server enable**

Enabling SSL/HTTPS

1. Generate the SSL certificates using the script in the ssl directory, or copy the example certificates (which end in .pem) to your TFTP server.

2. Copy the certificates to NVRAM with TFTP as follows from this example, using the IP address of your TFTP server.

```
SFTOS #copy tftp://192.168.0.10/dh512.pem nvram:sslpem-dhweak

Mode..................................... TFTP
Set TFTP Server IP....................... 192.168.0.10
TFTP Path.....................................
TFTP Filename............................ dh512.pem
Data Type................................ SSL DH weak

Management access will be blocked for the duration of the transfer
Are you sure you want to start? (y/n) y

TFTP SSL certificate receive complete... updating certificate file...

Certificate file transfer operation completed successfully

SFTOS #copy tftp://192.168.0.10/dh1024.pem nvram:sslpem-dhstrong

Mode..................................... TFTP
Set TFTP Server IP....................... 192.168.0.10
TFTP Path.....................................
TFTP Filename............................ dh1024.pem
Data Type................................ SSL DH strong

Management access will be blocked for the duration of the transfer
Are you sure you want to start? (y/n) y

TFTP SSL certificate receive complete... updating certificate file...

Certificate file transfer operation completed successfully

SFTOS #copy tftp://192.168.0.10/server.pem nvram:sslpem-server

Mode..................................... TFTP
Set TFTP Server IP....................... 192.168.0.10
TFTP Path.....................................
TFTP Filename............................ server.pem
Data Type................................ SSL Server cert

Management access will be blocked for the duration of the transfer
Are you sure you want to start? (y/n) y

TFTP SSL certificate receive complete... updating certificate file...
```

```
Certificate file transfer operation completed successfully

SFTOS #copy tftp://192.168.0.10/rootcert.pem nvram:sslpem-root

Mode..................................... TFTP
Set TFTP Server IP....................... 192.168.0.10
TFTP Path.....................................
TFTP Filename............................ rootcert.pem
Data Type................................ SSL Root cert

Management access will be blocked for the duration of the transfer
Are you sure you want to start? (y/n) y

TFTP SSL certificate receive complete... updating certificate file...

Certificate file transfer operation completed successfully
```

3. Enable the HTTPS server with this command.

SFTOS Version <= 2.2.1	SFTOS Version >= 2.3.1
(SFTOS) #**ip http secure-server**	SFTOS (Config)#**ip http secure-server enable**

To verify that the server has started, use this command to show the HTTPS server status and check the log file for the following messages.

```
SFTOS #show ip http

Java Mode: Disabled
HTTP Mode (Unsecure): Disabled
HTTP Mode (Secure): Enabled
Secure Port: 443
Secure Protocol Level(s): TLS1 SSL3

SFTOS #show logging buffered

JAN 01 01:16:19 192.168.0.34-1 UNKN[209189968]: sslt_util.c(321) 39 %% SSLT: Successfully
loaded all required SSL PEM files
```

Using a web browser, connect to the switch using an https:// URL and login to verify that the SSL server is working. The padlock icon on your browser should indicate an encrypted connection.

If you used the example certificates, your browser will display a warning that it cannot verify the authenticity of the certificate. This is because the example certificates have not been certified by a Certification Authority. When certificates are acquired from a Certification Authority and loaded on the switch this warning will not occur.

4. Once you have verified that you can connect to the switch with a web browser, the HTTP server can be disabled with this command for additional security if it was enabled previously. The HTTP server is disabled by default.

SFTOS Version <= 2.2.1	SFTOS Version >= 2.3.1
(SFTOS) #**no ip http server**	SFTOS (Config)#**no ip http server enable**

Force10 Networks, Inc.
1440 McCarthy Boulevard
Milpitas, CA 95035
www.force10networks.com

Phone: 408-571-3500
Fax: 408-571-3550
Email: info@force10networks.com