Examples

Inbound file transfers through the secure front ends (SFEs) require RSA SecurID token authentication. Files cannot be transferred directly to the SFEs, so transfers must be done using either SSH passthrough or using scp with the -oProxyCommand option.

Note: While this article covers file transfers through the SFEs only, you can also transfer files through the Secure Unattended Proxy.

To simplify the instructions, the approaches are described in terms of transfers to or from one of the NAS compute resources front ends, such as pfe21, but they also apply to any of the other systems that are in the secure enclave—such as other PFEs, or the Lou front ends (LFEs).

For some of the methods described, two commands are provided. The first command (a) is used if you have identical usernames on your local system and on the NAS systems, or if the usernames are different but you have set up your local ~/.ssh/config file to include the NAS username. To learn how to set this up, download the NAS **ssh_config.txt** template. The second command (b) is used if your usernames are different and you do not include the NAS username in your local ~/.ssh/config file.

File Transfers Using scp with -oProxyCommand

The scp command is not recommended for files over 1 GB; see Remote File Transfer Commands for a comparison of commands. If you have not set up SSH passthrough, you must use scp with the -oProxyCommand option for inbound file transfers through the SFEs.

Note: Because of a formatting issue, the commands in this section are broken into two lines. Each should be on only one line.

Using scp with the -oProxyCommand option to *push* files *out* of your local system:

(a) *your_local_system*% scp -oProxyCommand='ssh sfe6.nas.nasa.gov
ssh-proxy %h' *filename* pfe21.nas.nasa.gov:

or

(b) *your_local_system*% scp -oProxyCommand='ssh *nas_username*@sfe6.nas.nasa.gov
ssh-proxy %h' *filename nas_username*@pfe21.nas.nasa.gov:

Using scp with the -oProxyCommand option to *pull* files *into* your local system:

(a) *your_local_system*% scp -oProxyCommand='ssh sfe6.nas.nasa.gov
ssh-proxy %h' pfe21.nas.nasa.gov:*filename* .

or

(b) *your_local_system*% scp -oProxyCommand='ssh *nas_username*@sfe6.nas.nasa.gov
ssh-proxy %h' *nas_username*@pfe21.nas.nasa.gov:*filename* .

File Transfers Using SSH Passthrough

If you have set up SSH passthrough correctly, you can use scp or shiftc to transfer files between your local system and a NAS host. You can transfer files directly into the NAS host and avoid the need to double-authenticate. The passage through the SFEs is transparent.

Using scp

Using scp to *push* files *out* of your local system:

(a) *your_local_system*% scp *filename* pfe*21*.nas.nasa.gov:

or

(b) *your_local_system*% scp *filename nas_username*@pfe*21*.nas.nasa.gov:

Using scp to *pull* files *into* your local system:

(a) *your_local_system*% scp pfe*21*.nas.nasa.gov:*filename* .

or

(b) *your_local_system*% scp *nas_username*@pfe*21*.nas.nasa.gov:*filename* .

Using shiftc

See Shift File Transfer Overview for shiftc examples.

More About File Transfers

See the list of links in the File Transfer Overview.

You can transfer files between NAS and your local site either by running the transfer command on a PFE or LFE, or by running the command on your local system. Running the command on your local system requires you to go through a secure front end (SFE) or to set up the Secure Unattended Proxy (SUP) or SSH passthrough. Therefore, if your local system is set up to allow direct inbound connections, then starting the transfer from a PFE or LFE will be much simpler than starting the transfer from your local system.

The sample command lines shown below demonstrate how to run the scp or shiftc commands on a PFE to transfer files to or from you local system. You can also apply the commands to other systems in the enclave, such as the LFEs.

Notes:

- The sample command lines use pfe21 as an example.
- Two command lines are provided for each transfer method. Use the first one if your username for your local system is the same as your username for the NAS systems. If the usernames are different, use the second.

Using scp

To push files *out* of a PFE to your local system:

pfe*21*% scp *filename your_local_system*:
pfe*21*% scp *filename local_username@your_local_system*:

To pull files *into* a PFE from your local system:

pfe*21*% scp *your_local_system:filename* .
pfe*21*% scp *local_username@your_local_system:filename* .

Using shiftc

In most cases, it is recommended to initiate remote transfers on the non-NAS side using SUP/Shift since all authentication, firewalls, and shift options have been preconfigured to work correctly. Remote transfers initiated from within NAS, however, are possible if the ssh port of the remote system is accessible and supports the publickey authentication method. The private key must either be loaded in your ssh-agent process or you must use a passphrase-less private key file with --identity set to its full path name. In addition, the file "shift-aux" (obtainable from /usr/local/bin on any pfe or lfe) must be in the default $PATH on the remote system. It is recommended to restrict the list of remote transports to rsync, fish, and shift unless you know which ports are accessible on the remote host and can specify --ports (for either fish-tcp or bbftp) and/or bbftpd is installed on the remote host (for bbftp).

To push files *out* of a PFE to your local system:

pfe*21*% shiftc --remote=rsync,fish,shift *filename your_local_system*:
pfe*21*% shiftc --user=*local_username* --identity=~/.ssh/*your_private_key filename your_local_system*:

To pull files *into* a PFE from your local system:

pfe*21*% shiftc --remote=rsync,fish,shift *your_local_system:filename* .
pfe*21*% shiftc --user=*local_username your_local_system:filename* .

See Shift Command Options for all available options. Transfers may be monitored and stopped/restarted using normal shift methods. See Checking Shift Transfer Status and Restarting Transfers for more information.