

# SFTP and SCP: Secure File Transfer Protocols

SFTP (SSH File Transfer Protocol) and SCP (Secure Copy Protocol) are both secure file transfer protocols that operate as subsystems of SSH-2 (Secure Shell version 2). These protocols provide encrypted and authenticated methods for transferring files between systems.

## SFTP (SSH File Transfer Protocol)

SFTP is a robust and versatile protocol that offers secure file transfer capabilities:

- It operates over an encrypted SSH connection, typically on port 22.
- SFTP provides strong encryption and authentication to protect against various attacks.
- It supports a wide range of file operations, including uploading, downloading, and remote file manipulation.

### Key Features:

- Encryption of data during transit.
- Simplified use with a single port connection.
- Support for advanced features that most other file-transfer protocols don't have.

## SCP (Secure Copy Protocol)

SCP is another secure file transfer protocol that, like SFTP, operates as an SSH-2 subsystem:

- It is designed specifically for securely copying files between hosts on a network.
- SCP uses the same authentication and security mechanisms as SSH.

### Comparison to SFTP:

- SCP is simple to use in scripts, but lacks many of SFTP's advanced features.
- SFTP offers more functionality, including the ability to resume interrupted transfers and perform remote file system operations.

**Poison pill:** in order to fill the functionality gap between SFTP and SCP, some SCP clients attempt to use a parallel SSH-2 Shell to perform some of the operations the SCP protocol lacks, but in doing so they create a potential side-channel for attacks. If all you need are secure file-transfers, and SCP is requesting to perform Shell operations, the safest choice is

to drop SCP altogether and switch to SFTP. Do not allow Shell just because SCP may ask for it, unless you know exactly how to keep it safe.

## SSH-2 Subsystems

It's important to note that SFTP and SCP are not the only subsystems of SSH-2. The SSH-2 protocol is a versatile framework that supports various subsystems:

1. **File Transfer:** SFTP and SCP.
2. **Remote Command Execution:** Allows running individual commands on the remote system.
3. **Shell Access:** Provides a full interactive shell session on the remote machine.

This flexibility makes SSH-2 a powerful tool for secure remote system management and file transfer, but - as all powerful tools - it requires careful configuration from a knowledgeable administrator.

## Security Considerations

Both SFTP and SCP offer significant security advantages over traditional, unencrypted file-transfer protocols:

- They use strong encryption to protect data in transit.
- They provide authentication mechanisms to verify the identity of both the client and server.
- They ensure data integrity, preventing unauthorized modifications during transfer.

## Choosing Between SFTP and SCP

When deciding between SFTP and SCP, consider:

- **Functionality:** SFTP offers more advanced file management features.
- **Compatibility:** SCP might be the only choice in old/legacy environments where SFTP support is limited or absent.
- **Fitness:** In most modern scenarios, SFTP is the preferred choice due to its broader feature set and widespread support.

---

Revision #1

Created 25 November 2024 23:32:07 by DevTeam

Updated 25 November 2024 23:45:04 by DevTeam