SecurFTP/SSH

File transfer using the SFTP/SSH standard

Today many organizations exchanging data between computer systems via unencrypted FTP are facing serious challenges. User names, passwords, and files are sent across the network in the clear, making FTP tranfers vulnerable against sniffer attacks to spy on or change data during transit across the network. Furthermore, accessing an HPE NonStop system through standard FTP always requires the requesting user to present his system known ID and corresponding password for authentication. Without the ability to restrict specific users from accessing the system through FTP or from accessing specific files, the use of the standard FTP server can cause severe security concerns.

Purpose

SecurFTP/SSH provides secure file transfer for HPE NonStop systems. To protect data confidentiality across the network, it supports file transfers using the SFTP/SSH standard which is especially popular on Unix systems. [Note that SecurFTP is also available supporting the "FTPover SSL" standard; please see the product sheet SecurFTP/SSL for details].

Features

Secure SFTP Transfer
SecurFTP/SSH includes an OSS and a Guardian SFTP client, as well as an SFTP server providing remote SFTP client access to both Guardian and OSS files. All components allow navigating the Guardian file system or specifying files using the OSS or Guardian file name syntax, regardless if OSS is running. Additionally, attributes for target files can be specified like with standard NonStop FTP, allowing direct transfers of structured Guardian files.

Fully compliant to the SSH protocol specification
SecurFTP/SSH is fully compliant to the SSH (Secure Shell) version 2 protocol standard as described in various Internet Draft documents (see www.ietf.org). It cooperates with any SSH solution on UNIX, Windows, or other platforms.

Strong Authentication and multiple cipher suites
SecurFTP/SSH supports Public Key Authentication with key sizes of up to 2048 bits. Various ciphers (such as AES or 3DES) and MACing algorithms can be selected.

Single Sign-on via Kerberos
SecurFTP/SSH supports user and host authentication over SSH, based on the GSSAPI/-Kerberos 5 standards (RFC 4462). Together with comForte's SecurSSO product, this enables single sign-on integration with Microsoft Active Directory and other Kerberos-based SSO solutions.

Built-in user base
A built-in user base allows you to flexibly control who can access your system. Remote users can log on with virtual user names instead of a Guardian UserID, avoiding the exposure of system credentials to file transfer agents. Access can be limited to a part of the file system and to a specific set of operations (e.g. only download).

Central key store
Instead of storing keys in the file system, SecurFTP/SSH includes a key and password store with central access control, providing maximum security for user credentials. This enables easy and secure implementation of batch processes without having to use passwords in batch files.

Requirements

NonStop System:
- G06.27 or later
- H06.15 or later
- J06.11 or later
- L6.05 or later

Partner System:
An SSH2 client or daemon supporting the SFTP protocol

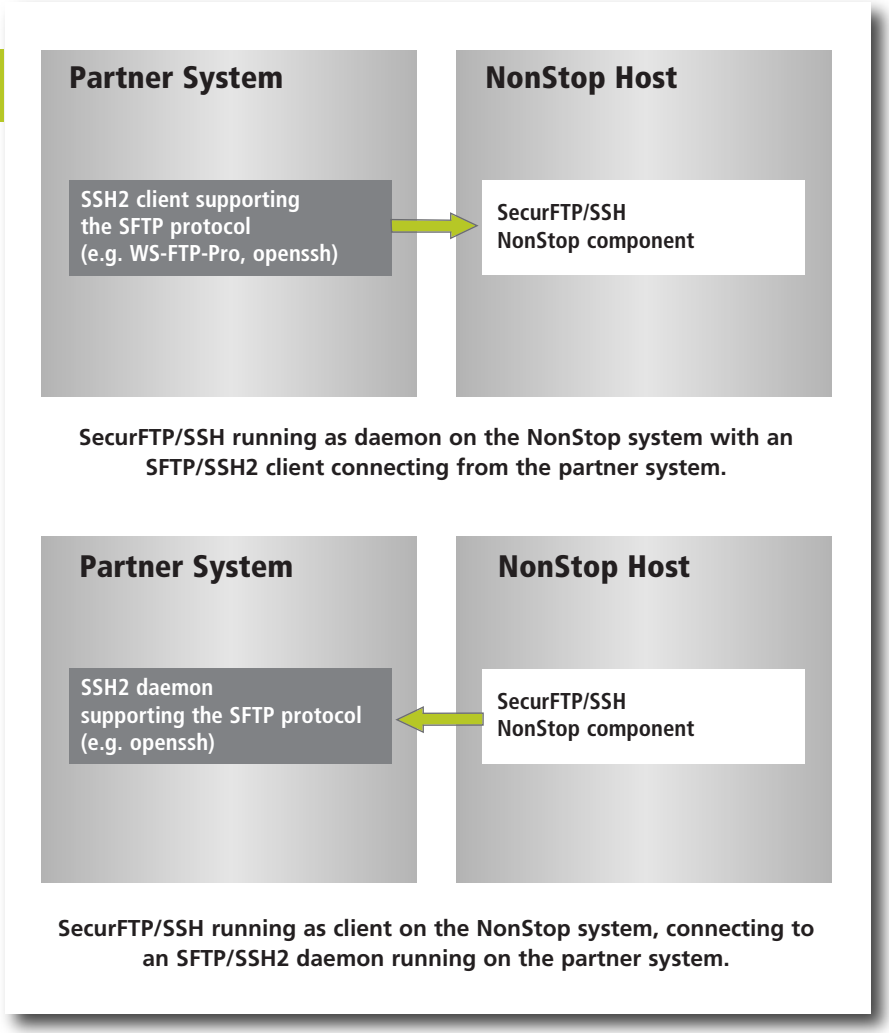
FTP Port forwarding
SecurFTP/SSH also tunnels FTP sessions, securing existing FTP procedures with only minor changes. Both local and remote forwarding are supported.
Advanced Auditing capabilities
An audit file containing all operations initiated from remote clients can optionally be activated. This allows complete tracking of who is accessing your system and what operations are executed.
Leverages NonStop platform fundamentals
To achieve maximum performance and availability, SecurFTP/SSH leverages the platform's native mechanisms for inter-process communication, load balancing and fault tolerance.

Benefits

Because SecurFTP/SSH is standards-compliant, it **will interact with any SFTP/SSH implementation on partner systems.** For instance, SecurFTP/SSH will work with the openssh implementation which is popular on Unix systems as well as with common Windows-based FTP clients supporting the SFTP/SSH protocol such as WS-FTP-Pro or CuteFTP-Pro.

Architecture

On the NonStop platform, SecurFTP/SSH runs in native mode under the Guardian personality, resulting in optimal performance and full leveraging of the NonStop system advantages.
SecurFTP/SSH is available for the HPE Integrity NonStop (Itanium) platform.
OSS is not required to use SecurFTP/SSH, however OSS is fully supported if so desired.



SecurFTP/SSH running as daemon on the NonStop system with an SFTP/SSH2 client connecting from the partner system.

SecurFTP/SSH running as client on the NonStop system, connecting to an SFTP/SSH2 daemon running on the partner system.

SecurFTP/SSH

comforte AG, Germany
phone +49 (0) 611 93199-00
sales@comforte.com

comforte, Inc., USA
phone +1-303 256 6257
ussales@comforte.com

comforte Asia Pte. Ltd., Singapore
phone +65 6808 5507
asiasales@comforte.com

comforte Pty Ltd, Australia
phone +61 2 8197 0272
aussales@comforte.com

www.comforte.com

comforte

For distribution partners in your region visit comforte's homepage www.comforte.com