SECURSH

Enterprise-class Secure Shell for HPE NonStop Servers

Today many organizations exchanging data between computer systems via shared communication lines are facing serious challenges. User names, passwords, files and sensitive application data are sent across the network in the clear, making it vulnerable against sniffer attacks to spy on or change data during transit across the network.

SecurSH is designed to help your organization to effectively manage security risks, and comply with external and internal security policies.

Purpose

SecurSH is an enterprise security solution to provide secure shell connectivity for HPE NonStop servers. It provides end-to-end communications security, strong authentication and auditing for system administration, file transfer, and applications connectivity. SecurSH is designed to address the most critical security requirements of large enterprises, financial institutions and government agencies.

Features

Fully compliant to the SSH protocol specification. SecurSH 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. SecurSH supports Public Key Authentication with key sizes of up to 2048 bit are supported. Various ciphers (such as AES or 3DES) and MACing algorithms can be selected.

Single Sign-on via Kerberos. SecurSH 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.

Support of full screen terminal access. Unlike other solutions, SecurSH supports pseudo terminals on the NonStop platform, allowing SSH clients to execute full screen applications such as emacs or vi within the secure shell.

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 to expose the system credentials to file transfer clients. 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, SecurSH includes a key and password store with central access control, providing maximum security for user credentials. This enables easy and secure imple-mentation of batch processes without having to use passwords in batch files.

Secure SFTP Transfer. SecurSH 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.

System Requirements

NonStop System

- H06.15 or later
- J06.04 or later
- L16.05 or later

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

comforte, Inc., USA
phone +1 646 438 5716
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

TCP and FTP Port forwarding. TCP port forwarding allows secure tunneling of Telnet sessions, as well as other connections. SecurSH also tunnels FTP sessions, securing existing FTP procedures with only little changes. Both local and remote forwarding are supported.

TCP/IP version 6 support. SecurSH supports TCP/IP version 4 and version 6, as well as dual mode, i.e. mixed IPv6/IPv4.

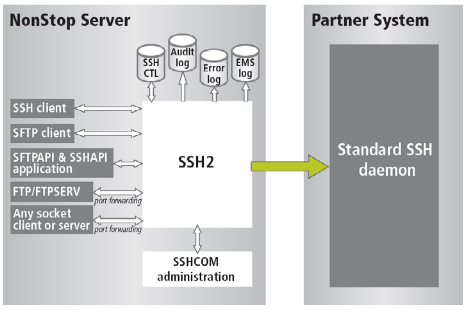
Advanced Auditing capabilities. An audit file containing all operations initiated from remote clients can optionally be activated. This allows to fully keep track of who is accessing your system and what operations are executed.
Leverages NonStop platform fundamentals. SecurSH leverages the platform's native mechanisms for inter-process communication, load balancing and fault tolerance for maximum performance and availability.

Benefits

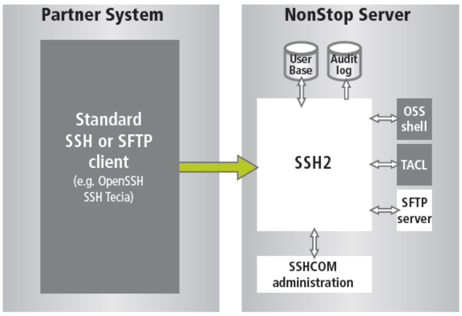
Because SecurSH is standards-compliant, it will interact with any SSH implementation on partner systems such as OpenSSH.
With its native platform support, outstanding performance, easy manageability, advanced access control, single sign-on and auditing capabilities, SecurSH provides a comprehensive, enterpriseclass SSH solution for HPE NonStop suiting the most advanced requirements "out of the box".

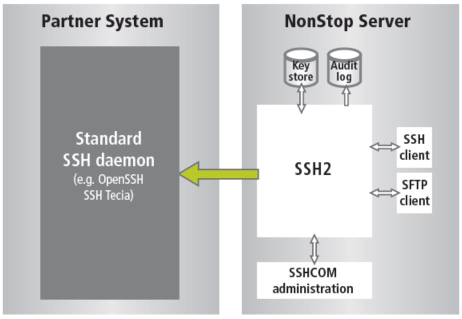
Architecture

On the NonStop platform, **SecurSH** runs in native mode under the Guardian personality, optionally as a nonstop or persistent process. While OSS is not required to use SecurSH,it is fully supported if so desired.



SSHLIB as optional extra describes the external interface offered by the SSH application program interface (API). SSHLIB is used for launching an SSH object and controlling it automatically by an application via the SSH API. SSHLIB can simplify the task of controlling status or resources on a remote host. It is also helpful to automate setup scripts for duplicating softwarepackage installations on different servers. Using this library unlocks the powerful Tcl Expect like pattern matching that has been built into SSHLIB.


Partner System
Standard SSH or SFTP client
(e.g. OpenSSH SSH Tecia)
NonStop Server
User Base
Audit log
SSH2
OSS shell
TACL
SFTP server
SSHCOM administration


Partner System
Standard SSH daemon
(e.g. OpenSSH SSH Tecia)
NonStop Server
Key store
Audit log
SSH2
SSH client
SFTP client
SSHCOM administration