SSH Solutions on OpenVMS

Technical Overview

SSH Solutions

Process Software delivers SSH solutions on OpenVMS as a feature of MultiNet and TCPware TCP/IP stacks or as a standalone product with SSH for OpenVMS. SSH for OpenVMS turns VAX, Alpha and Integrity computers into secure application servers in multi-platform environments, and integrate OpenVMS systems with virtually any other system through industry-standard SSH over TCP/IP.

The De-Facto Standard for Network Security

The SSH protocol is an IETF standard used by millions of people and thousands of organizations all over the world. Process Software's SSH products are based on ICSA-certified code base. The cryptographic library used is compiled from unaltered source code that is FIPS 140-2 compliant, as determined by the Computer Security Division of the National Institute of Science and Technology (NIST). It is widely used by government organizations and large enterprises.

SSH Features

Process Software's SSH products enables remote systems administrators, telecommuters, and other users to access corporate networks without revealing passwords and confidential data to potential eavesdroppers. The main features include:

- Supports both SSH v1 and SSH v2 protocols in the client and server
- Provides secure file transfer with Secure File Transfer Protocol v2 (SFTP v2) client and server, Secure Copy Protocol v2 (SCP v2) client and server, and Secure File Copy Protocol v1 (SCP v1) server.
- Replaces Telnet, FTP, and R services with secure connections
- Encrypts X-11 displays using X-11 forwarding
- Encrypts third-party applications using port forwarding, such as e-mail or database access
- Protects all data using strong encryption ciphers
- Supports RSA and DSA authentication
- Provides the ability to start and stop SSH without rebooting the entire system so that other products remain unaffected
- Data compression improves the network performance when using long distance transmissions or low bandwidth connections
- Operates with most third-party clients and servers
- Single sign-on support simplifies management by allowing use of existing PKI certificates and Kerberos v5 authentication methods.
- A public-key server and assistant have been added to make it easier to manage keys for SSH public key authentication.

- The `CERTENROLL` utility allows users to enroll certificates by connecting to a CA (certificate authority) and using the CMPv2 protocol to enroll a certificate. The `CERTVIEW` allows viewing and validation of certificate contents.
- Provides the ability to convert OpenSSH-format keys to SECSH (SSH2) format.

Easy to Install and Operate

Process Software's SSH products integrate cleanly into the OpenVMS environment. SSH for OpenVMS supports OpenVMS v7.3 and higher, with TCP/IP Services v5.4 and higher. It uses the standard TCP/IP Services for OpenVMS BG interface. MultiNet and TCPware TCP/IP stacks run on OpenVMS v5.5-2 and higher.

Process Software's SSH products are easy to install using the `VMSINSTAL` installation procedure. It takes less than five minutes to configure all services and utilities. You can control Process Software's SSH products by means of a single utility that simplifies network management and allows you to manage the SSH products security.

Configuration Support

The Process Software SSH products support VAX, Alpha and Integrity computers running various versions of OpenVMS. When each node in an OpenVMS cluster shares a common system disk, the cluster needs to store just one copy of most of the SSH product files. Only a few system-specific configuration files are required on each machine that runs the software.

Secure Shell (SSH) v1 Client and Server

Process Software's SSH products provide secure communication over unsecured networks. The SSH client is an application for logging into and executing commands on a remote system replacing rsh, rlogin, rshell, and Telnet applications. Furthermore, X11 connections and arbitrary TCP/IP ports can be forwarded over the secure channel. SSH connects and logs into the specified host. Process Software's SSH products support protocol version 1 client and server. The Secure Shell daemon (SSHD) is the daemon program for SSH v1 that listens for connections from clients. When the SSHD daemon starts, it generates a server RSA key (normally 768 bits). This key is regenerated every hour (the time may be changed in the configuration file) if it has been used, and is never stored on disk. A new daemon is created for each incoming connection.

A client program that allows both SSH1 and SSH2 logins is provided with SSH for OpenVMS. Any SSH client that uses the SSH v1 protocol may be used to access the server. Examples of such programs include FISSH, MultiNet, TCPware, and SSH for OpenVMS Client; TTSSH, F-Secure Secure SSH Client, SecureCRT, and PuTTY on Windows-based systems; and FSecure SSH, and other SSH programs on UNIX-based systems.

The SSH server is authenticated using a combination of public and private keys. Once the server has been authenticated, the user must be authenticated. Process Software offers four options for user authentication: rhosts, rhosts-rsa, rsa challenge-response, and password.

Secure Shell (SSH) v2 Client and Server

Process Software's SSH products also support protocol v2 client and server. SSH v2 is generally regarded as more secure than SSH v1. Although the protocols are incompatible, they may exist simultaneously on a Process Software SSH system. With SSH v2, rcp and FTP can be replaced with secure alternatives. Process Software's SSH server front-end identifies which protocol a client will use, and will create an appropriate server for that client. The server is authenticated using a public key and the Diffie-Hellman key-exchange method. Diffie-Hellman uses a 256-bit random number for the "session key". This key is used to encrypt all further communications in the session. The SSH v2 client authentication offers the following options: host-based, public-key, Kerberos v5, password, keyboard-interactive, and certificate.

The following table shows which encryption algorithms are supported by SSH v1 and SSH v2:

SSH Ciphers	**SSHv1**	**SSHv2**
3DES	✓	✓
Arcfour	✓	✓
BlowFish	✓	✓
DES	✓	✓
IDEA	✓	
TwoFish		✓
AES		✓
Cast		✓

Secure Copy Protocol v2 (SCP v2) and Secure File Transfer Protocol v2 (SFTP v2) Client and Server

SCP and SFTP provide secure file transfers. Using SCP v2 and SFTP v2, files can be transferred as ASCII, BINARY, or in OpenVMS format when implementing SSH file transfer protocol v4 (IETF draft). SCP v2 and SFTP v2 also support earlier versions of the SSH file transfer protocol using one specified format: BINARY. Also, the defined syntax for a file specification is UNIX.

Process Software's SSH products use the defined extensions in the SCP and SFTP protocols to transfer information about the OpenVMS file header characteristics. It does this so that the file will have the same format when it is transferred between two OpenVMS systems running SSH for OpenVMS, Process Software MultiNet v4.4 or higher, or Process Software TCPware v5.6 or higher. Also, when a file is transferred to operating systems other than OpenVMS, a method has been provided to translate those files into a format that will be usable on the remote system. Files that are transferred from operating systems other than OpenVMS are stored as stream files on the OpenVMS system, which provides compatibility for text files from those systems. Also, the SFTP user interface is similar to FTP and the SCP user interface is single command line.

Port Forwarding

Port forwarding allows forwarding of TCP/IP connections to a remote machine over an encrypted channel. A local proxy server is created for a remote TCP/IP service. The service can be one of the

Internet protocols: POP, SMTP (used by e-mail software), HTTP (used by Web browsers), TCP/IP connection to an RDBMS server, or almost any other TCP/IP based service provided the port is known via a static assignment. The local proxy server listens for a socket on the desired port, forwards the request and data over the secure channel, and instructs the SSH server to make the connection to the specified service on the remote machine. The only noticeable change is that the client software is configured to connect to the local proxy server rather that the remote server.

X-11 Forwarding

With X11 in use, the connection to the X11 display forwards to the remote side any X11 programs started from the interactive session (or command) through the encrypted channel. Also, the connection to the real X server is made from the local system. Forwarding of X11 connections can be configured on the command line or in configuration files.

The DECW$DISPLAY value set by SSH points to the server system with a display number greater than zero. This is normal and happens because SSH creates a "proxy" X server on the server system for forwarding the connections over the encrypted channel.

SSH sets up “synthetic” Xauthority data on the OpenVMS server (as OpenVMS does not support Xauthority currently). It generates a random authorization cookie, stores it in Xauthority on the server, and verifies that any forwarded connections carry this cookie and replace it by the real cookie when the connection is opened. The real authentication cookie is never sent to the server system (and no cookies are sent unencrypted).

Single Sign-on

Single sign-on support allows use of existing Kerberos v5 and Public Key Infrastructure (PKI) certificates. The Process Software SSH Kerberos v5 requires the operation of HP’s OpenVMS Kerberos v5 v2.0 or greater which contains the KDC. This kit restricts support for Kerberos (and hence, Kerberos V5 support in SSH for OpenVMS) to OpenVMS Alpha v7.3-2 and higher, and OpenVMS I64 v8.2 and higher. When Kerberos v5 support is enabled, authentication may be done via Kerberos password, Kerberos credentials, forwardable TGT, and passing TGT to remote hosts for single sign-on support.

PKI certificates can also be distributed for user authentication of SSH v2 sessions. SSH stores the software certificates in DER binary format. The SSHKEYGEN utility can be used to import and convert PKCS#12 packages into private key/certificate pairs, X.509 format private key into SSH private key, or PKCS#7 into certificates. The CERTENROLL utility may be used to enroll certificates with a Certificate Authority (CA) that supports the CMPv2 protocol, and the CERTVIEW utility may be used to view the contents of those certificates.

Hardware and Software Requirements

SSH for OpenVMS requires at least one network controller supported by TCP/IP Services.

Process Software SSH Solutions:

- MultiNet 5.4 or higher
- TCPware 5.9 or higher
- SSH for OpenVMS 2.3

SSH for OpenVMS supports the following operating systems and TCP/IP Services versions:

- OpenVMS Alpha v7.3 and higher
- OpenVMS Itanium v8.2 and higher
- TCP/IP Services v5.4 or higher
- In order to enable Kerberos v5 authentication in the SSH server, the HP OpenVMS Kerberos v5 product must be installed (see http://h71000.www7.hp.com/openvms/products/kerberos/).

MultiNet and TCPware support the following operating systems:

- OpenVMS VAX v5.5-2 and higher
- OpenVMS Alpha v6.2 and higher
- OpenVMS Itanium v8.2 and higher
- In order to enable Kerberos v5 authentication in the SSH server, the HP OpenVMS Kerberos v5 product must be installed (see http://h71000.www7.hp.com/openvms/products/kerberos/). This restricts support for Kerberos to OpenVMS Alpha v7.2-2 and higher, and OpenVMS I64 v8.2 and higher.

About Process Software

Process Software has been a premier supplier of communications software solutions to mission critical environments for twenty years. We were early innovators of email software and anti-spam technology. Process Software has a proven track record of success with thousands of customers, including many Global 2000 and Fortune 1000 companies.

U.S.A.: (800) 722-7770 • International: (508) 879-6994 • Fax: (508) 879-0042

E-mail: info@process.com • Web: http://www.process.com/