SOFTWARE PRODUCT DESCRIPTION

PSCSSH

Version 3.0

The PSCSSH Solution

PSCSSH is the complete SSH networking security extension for OpenVMS VAX, Alpha, Integrity, and X86_64 systems running TCP/IP Services for OpenVMS (sometimes referred to as UCX). PSCSSH turns VAX, Alpha, Integrity, and X86_64 computers into secure application servers in multi-platform environments and integrates OpenVMS systems with virtually any system through industry-standard SSH over TCP/IP.

The De-Facto Standard for Network Security

The SSH protocol is used by millions of users and thousands of organizations all over the world. SSH protocol version 2 is the basis for the Internet Engineering Task Force (IETF) SECSH standard. Process Software implements the F-Secure SSH protocol, which is the only solution that has been certified by the ICSA.

Easy to Install and Operate

Process Software's SSH products integrate cleanly into the OpenVMS environment. PSCSSH supports OpenVMS v5-5.2 and higher, with TCP/IP Services v4.0 (with ECO 5) and higher. It uses the standard TCP/IP Services for OpenVMS BG interface.

PSCSSH is easy to install using the VMINSTAL installation procedure. It takes less than five minutes to configure all services and utilities. You can control PSCSSH by means of a single utility that simplifies network management and allows you to manage IT security.

Configuration Support

PSCSSH supports VAX, Alpha, Integrity, and X86_64 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 PSCSSH files. Only a few system-specific configuration files are required on each machine that runs the software. PSCSSH supports Symmetric Multi-Processing (SMP) for OpenVMS.

Secure Shell (SSH) v1 Client and Server

PSCSSH provides 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.

PSCSSH supports 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 PSCSSH. It is based on WRQ RSIT 6.1.4.0. 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 PSCSSH; TTSSH, F-Secure Secure SSH, Secure CRT(R), and PuTTY on Windows(R)-based systems; and F-Secure SSH, and other SSH programs on UNIX-based systems.

The SSH v1 server is based on F-Secure code version 1.5. 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

PSCSSH also supports protocol SSH v2 client and server. It is based on WRQ RSIT 6.1.4.0. SSH v2 is generally regarded to be more secure than SSH v1.

PROCESS™ SOFTWARE

Although the protocols are incompatible, they may exist simultaneously on a Process Software SSH system. The PSCSSH server front-end identifies which protocol a client desires to use and will create an appropriate server for that client.

The SSH2 server and client are compiled from unaltered cryptographic source which is FIPS 140-2 Level 2 compliant.

The server is authenticated via 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 5, password, keyboard-interactive, and Certificate. With SSH v2, rcp and FTP can be replaced with secure alternatives.

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

SSH Ciphers	SSH v1	SSH v2
3DES (112 bit)	X	X
Arcfour (128 bit)	X	X
BlowFish (128 bit)	X	X
DES (56 bit)	X	X
IDEA (128 bit)	X	
TwoFish (256 bit)		X
AES (128, 192, 256 bit)		X
Cast-128 (128 bit)		X

The Core Features of PSCSSH...

PSCSSH enables remote systems administrators, telecommuters, and other users to access corporate networks without revealing passwords and confidential data to potential eavesdroppers.

* Supports both SSH v1 and SSH v2 protocols in the client and server
* Provides secure file transfer with Secure File Transfer Protocol (SFTP) client and server
* Secure Copy Protocol (SCP) client and server, and 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 email or database access
* Protects all data using strong encryption ciphers
* Supports RSA and DSA authentication
* Provides the ability to start and stop PSCSSH without rebooting the entire system, ensuring 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. (See http://www.process.com/sshclients/index.html for a list of third-party clients that Process Software has tested.)
* A public-key server and assistant have been added to make it easier to manage keys for SSH public key authentication.
* Login/logout events are now logged via the VMS audit server. The user will see a login record created by the SSH server, plus login and logout records for a detached session (the interactive login session).
* Single sign-on support simplifies management by allowing use of existing PKI certificates and Kerberos v5 authentication methods.
* Integrating with Process Software's VMS Authentication Module allows use of LDAP and SecurID authentication.
* The CMPCLIENT utility allows users to enroll certificates by connecting to a CA (certificate authority) and using the CMPv2 protocol to enroll a certificate.
* The CERTVIEW utility allows users to view and validate certificates.
* The CERTTOOL utlity allows the manipulation of X.509 formatted packages.

Secure Copy Protocol v2 (SCPv2)

SCP2 is an evolving file transfer protocol, and not all implementations will offer all levels of functionality. The basic functionality is binary file transfers. PSCSSH supports BINARY and ASCII transfers with SCP2 and will also transfer VMS file characteristics when the remote system has the capability. When operating with systems that do not support the full range of transfer mechanisms that PSCSSH offers, PSCSSH uses various methods to improve the chances that files will be useful upon transfer.

PSCSSH uses the defined extensions in the protocol to transfer information about the OpenVMS file header characteristics such that when a file is transferred between two OpenVMS systems running SSH for OpenVMS, MultiNet v4.4 and higher, or TCPware v5.6 and higher, the file header information will also be transferred and the file will have the same format on the destination system as it had on the source system. Also, when a file is transferred to a non-OpenVMS system, a method has been provided to translate those files that can be translated into a format that will be usable on the remote system. Files that are transferred from non-OpenVMS systems are stored as stream files on the OpenVMS system, which provides compatibility for text files from those systems.

Secure File Transfer Protocol v2 (SFTP2)

SFTP2 is an FTP-like client that can be used to transfer files over a network. SFTP2 transfers the files through ssh2 connections to ensure that the file transport is secure. In order to connect using SFTP2, you need to make sure that sshd2 is running on the remote host that you are connecting to.

SFTP2 is an evolving file transfer protocol, and not all implementations will offer all levels of functionality. The basic functionality is binary file transfers. PSCSSH supports BINARY and ASCII transfers with SFTP2 and will also transfer VMS file characteristics when the remote system has the capability. When operating with systems that do not support the full range of transfer mechanisms that PSCSSH offers, PSCSSH uses various methods to improve the chances that files will be useful upon transfer.

Publickey Assistant

The publickey assistant can be used to add, remove, and list SSH v2 public keys that are stored on a remote server.

CMPCLIENT

Allows users to enroll certificates by connecting to a CA (certification authority) and using the CMPv2 protocol for enrolling a certificate. The user may supply an existing private key when creating the certification request or allow a new key to be generated.

CERTVIEW

Allows users to view and validate certificates, and, optionally, to output the information from a certificate that is formatted correctly to use when creating the SSH certificate mapping configuration.

CERTTOOL

The CERTTOOL utility is used for different needs concerning X.509 certificates in PKCS#10 and PKCS#12 format. The CERTVIEW tool can be used for certificate viewing and validation.

For PKCS#10, CERTTOOL creates certificate requests, allowing the user to specify specific keyUsage and extendedKeyUsage flags.

For PKCS#12, CERTTOOL creates a PKCS#12 package containing any number of private keys and certificates. The final PFX package is encoded with an HMAC and by default contains one password protected safe, which contains all the other objects in an unshrouded format.

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 email 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 than the remote server.

X11 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 sever 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 “fake” 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 with the real cookie when the connection is opened. The real authentication cookie is never sent to the server system (and no cookies are 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 T2.0 or greater, which contains the KDC. This kit restricts support for Kerberos (and hence, Kerberos v5 support in PSCSSH) to OpenVMS Alpha v7.2-2 and higher, and OpenVMS I64. 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 support the CMPv2 protocol.

In addition, SSH v2 can be integrated with Process Software's VMS Authentication Module to provide LDAP authentication for SSH.

Standards and RFCs

The PSCSSH product conforms to the following Internet Requests for Comments (RFCs):

Request for Comments Title	RFC No.
Basic Socket Interface Extensions for IPv6	3493
The Secure Shell (SSH) Protocol Assigned Numbers	4250
The Secure Shell (SSH) Protocol Architecture	4251
The Secure Shell (SSH) Authentication Protocol	4252
The Secure Shell (SSH) Transport Layer Protocol	4253
The Secure Shell (SSH) Connection Protocol	4254
Generic Message Exchange Authentication for the Secure Shell Protocol (SSH)	4256
The Secure Shell (SSH) Transport Layer Encryption Modes	4344
Improved Arcfour Modes for the Secure Shell (SSH) Transport	4345
Diffie-Hellman Group Exchange for the Secure Shell (SSH) Transport Layer Protocol	4419
RSA Key Exchange for the Secure Shell (SSH) Transport Layer Protocol	4432
The Secure Shell (SSH) Public Key File Format	4716

Services, Documentation, and Ordering Information

Technical Services

Process Software's Technical Services Program has a well-deserved reputation for excellence. Services include consulting, software maintenance, support, and online resources. In short, everything you need to keep your Process Software products and your network operating at peak efficiency.

Consulting

A comprehensive suite of programs is available on a host of topics, including PSCSSH installation and configuration, DNS setup and use, network security, troubleshooting, and others.

Hot Line Support

Networking experts are available by telephone and email.

Updates

All maintenance customers with current service contracts receive automatic software and documentation updates of major releases.

Documentation

Comprehensive documentation for PSCSSH includes an administration and user's guide that provides installation and configuration information, along with product release notes that contain late-breaking product information. Documentation is provided in HTML and PDF formats on the Process Software Web site (https://www.process.com).

Ordering Information

PSCSSH is downloaded from the Process Software website. Contact sales@process.com or request a free evaluation at:

https://
www.process.com/tcipip/sshreq.asp.

Software Warranty

Process Software warrants all products for 90 days from the date of delivery.

Hardware and Software Requirements

PSCSSH requires at least one network controller supported by TCP/IP Services.

PSCSSH supports the following operating systems and TCP/IP Services versions:

* OpenVMS VAX V5.5-2 and later
* OpenVMS Alpha V6.2 and later
* OpenVMS I64 V8.2 and later
* OpenVMS X86_64 V9.2 and later
* Any version of TCP/IP Services supported by VSI or HPE

Note: To enable Kerberos v5 authentication in the SSH server, the HPE OpenVMS Kerberos v5 product must be installed.

About Process Software

Process Software is a premier supplier of communications software solutions to mission critical environments. We deliver customer-centric and innovative IP-based technologies to our customers worldwide and provide them with superior customer support and service.

Process Software
P.O. Box 922
Framingham, MA 01701

Telephone:
U.S./Canada 1-(800) 722-7770
International 1-(508) 879-6994

Web: https://www.process.com

Email: sales@process.com