Pragma FortressSSH 5.0

Secure Connectivity Software to Build
a Secure Enterprise Network with SSH
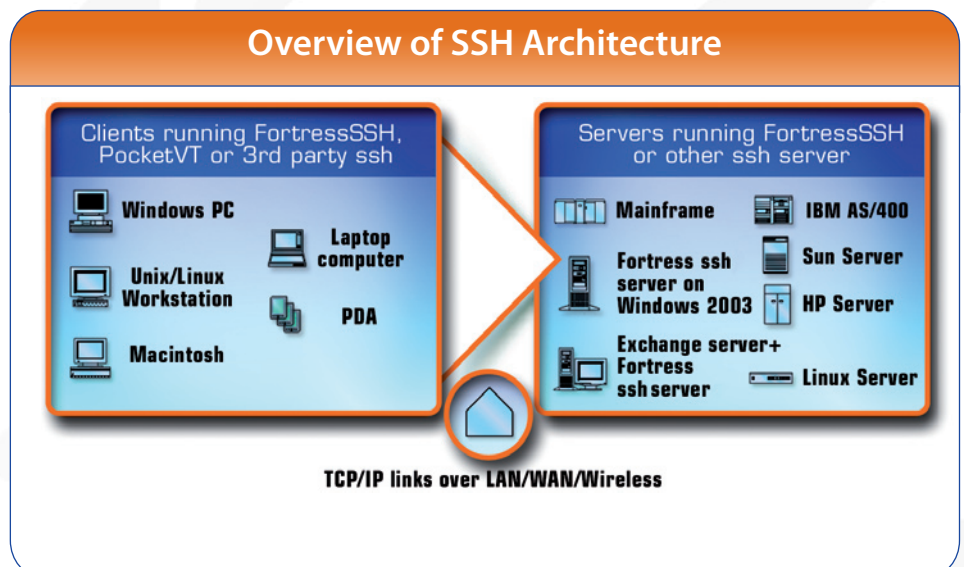
PRAGMA
S Y S T E M S

What is the FortressSSH product line?

Pragma Fortress is a comprehensive secure connectivity product that provides a highly secure encrypted framework to build a secure network environment for your enterprise. This product family was created to meet the growing ney-aed of enterprise security software after years of experience with our large customers and direct feedback from them. The Fortress product line enhances customer's network security against network intrusions, unauthorized data access, hacking, virus and worm attacks. The Fortress product line consists of a series of servers and clients, all of which are highly secure and use encryption for any data or network transfer. For version 5.0, Fortress supports both 64-bit and 32-bit natively. Fortress 5.0's advanced design and architecture allows full 64-bit x64 processor support as well as the proven 32-bit x86 Intel/AMD processors. Fortress 5.0 64-bit allows Windows servers to reach unprecedented scalability and performance level without the 32-bit memory and associated constraints of the 32-bit architecture.

The Fortress line is built with the widely used Secure Shell (SSH) protocol, the de-facto industry standard for secure remote access and file transfer. SSH is now an approved IEEE draft standard. To integrate with Microsoft Windows more effectively, Pragma has added many enhancements to the Fortress line over what other SSH vendors provide. One example is Active Directory based Windows native authentication support (Kerberos & NTLM) in all Fortress servers and clients, which allows single sign-on and seamless secure access to any Windows server or PC. Since Fortress is built using the Secure Shell standard, it is compatible with secure shell clients and servers of other industry vendors like SSH Communications, Attachmate, OpenSSH, Sun, IBM, HP, Apple and Cisco.


Overview of SSH Architecture

Clients running FortressSSH, PocketVT or 3rd party ssh
- Windows PC
- Unix/Linux Workstation
- Laptop computer
- PDA
- Macintosh

Servers running FortressSSH or other ssh server
- Mainframe
- IBM AS/400
- Fortress ssh server on Windows 2003
- Sun Server
- HP Server
- Exchange server + Fortress ssh server
- Linux Server

TCP/IP links over LAN/WAN/Wireless

Secure Connectivity…
Done Right

Fortress is designed with a client-server architecture. The server side consists of Fortress Secure Shell servers (ssh.exe) and Fortress Secure File Transfer servers (sftp-server.exe). The desktop client side is packaged as a single product, "Fortress ClientSuite," and consists of Fortress Secure Shell client (FortressCL.exe and ssh.exe), and Fortress File Transfer Client (FortressFX.exe and sftp.exe). A Fortress client is used to connect to a remote machine running Fortress server and run any character mode programs in the Fortress server. All data, certificates, password and credentials are encrypted in all SSH sessions, thus eliminating virtually any risks associated with remote access.

Pragma Fortress provides access from a wide variety of platforms. Fortress clients are available for any Windows operating system (Windows Vista/2003/XP/2000), PDAs & Mobile Phones (Pocket PC, Windows Mobile, and Windows CE), and Industrial Handhelds (Symbol, Intermec and others). Fortress Servers are available to run in Windows Vista/2003/XP/2000. For platforms that Pragma Fortress does not run on, like Linux, Unix, Mainframe, AS400 and Apple, one can pick servers and clients from many third party providers like OpenSSH, SSH Communications or system vendors like IBM, HP, Sun or Apple. Fortress interoperates seamlessly with any secure shell server or client, thus allowing you to build a secure network of any size. The Secure Shell standard was created in 1995 and is a widely used standard. Servers and clients for secure shell are now available in all major operating systems including Windows, Linux, Unix, Mainframe and Apple MacOS.

SSH technology is extended to Handheld and PDA/Mobile Phone environments by Pragma's PocketVT product offering. This allows mission critical corporate applications to be delivered to mobile devices over wireless securely with PocketVT on the client and Pragma Fortress and other SSH servers on the backend.
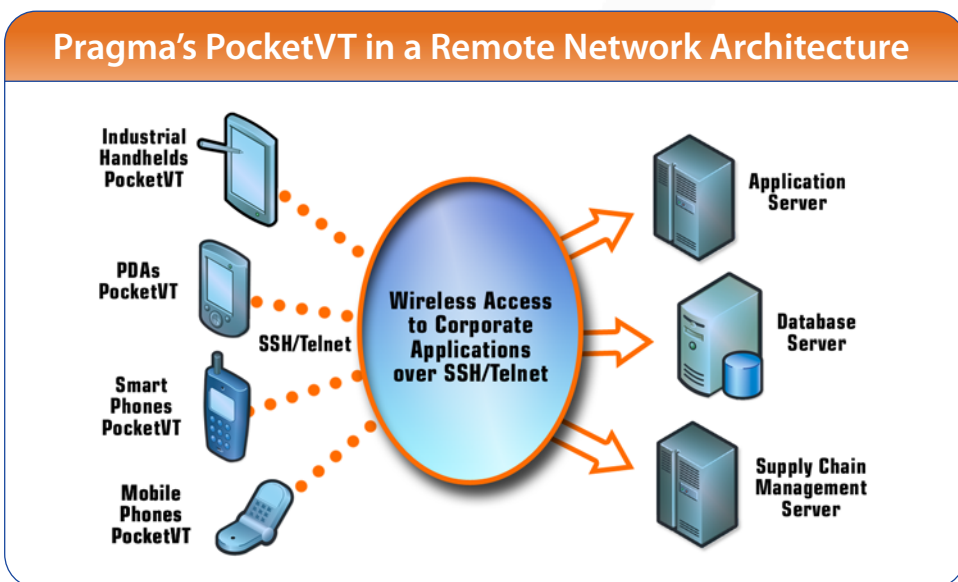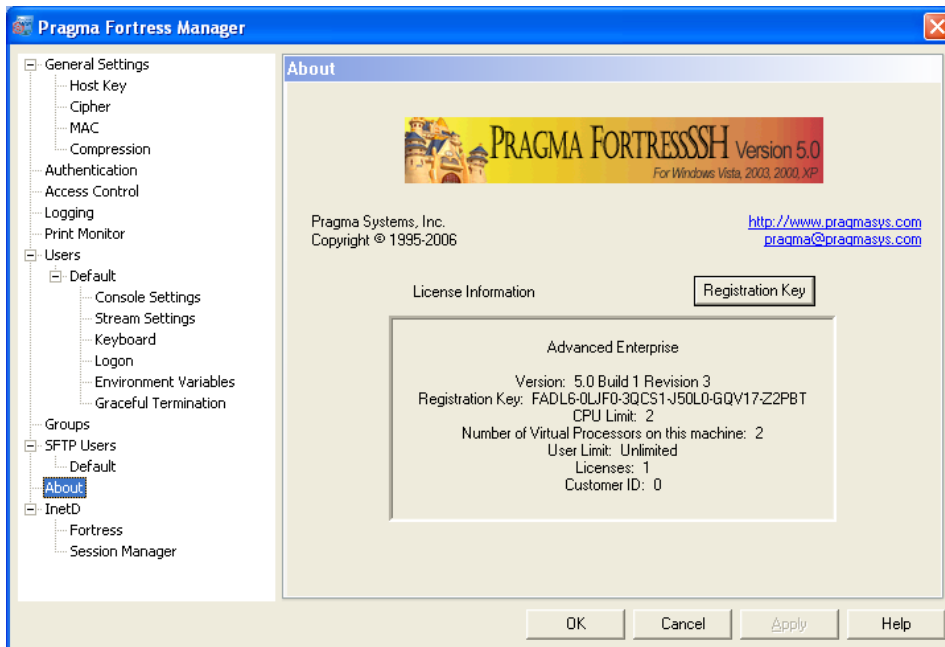
Pragma's PocketVT in a Remote Network Architecture

Pragma FortressSSH 5.0
Secure Connectivity Software to Build
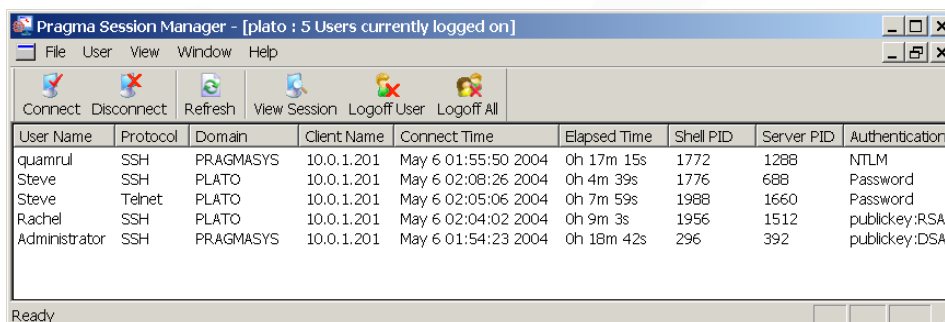## a Secure Enterprise Network with SSH

Secure Connectivity…
Done Right

Pragma Fortress Manager manages all Fortress server configurations as detailed in the below diagram.

Pragma Fortress Manager

General Settings
- Host Key
- Cipher
- MAC
- Compression
Authentication
Access Control
Logging
Print Monitor
Users
- Default
  - Console Settings
  - Stream Settings
  - Keyboard
  - Logon
  - Environment Variables
  - Graceful Termination
Groups
SFTP Users
- Default
About
InetD
- Fortress
- Session Manager

About

PRAGMA FORTRESSSSH Version 5.0
For Windows Vista, 2003, 2000, XP

Pragma Systems, Inc.
Copyright © 1995-2006
http://www.pragmasys.com
pragma@pragmasys.com

License Information   Registration Key

Advanced Enterprise

Version: 5.0 Build 1 Revision 3
Registration Key: FADL6-0LJF0-3QCS1-J50L0-GQV17-Z2PBT
CPU Limit: 2
Number of Virtual Processors on this machine: 2
User Limit: Unlimited
Licenses: 1
Customer ID: 0

OK   Cancel   Apply   Help

Pragma Fortress Session Manager can view any Fortress server and lists the active sessions and their characteristics.

Pragma Session Manager - [plato : 5 Users currently logged on]

File   User   View   Window   Help

Connect Disconnect Refresh View Session Logoff User Logoff All

User Name	Protocol	Domain	Client Name	Connect Time	Elapsed Time	Shell PID	Server PID	Authentication
quamrul	SSH	PRAGMASYS	10.0.1.201	May 6 01:55:50 2004	0h 17m 15s	1772	1288	NTLM
Steve	SSH	PLATO	10.0.1.201	May 6 02:08:26 2004	0h 4m 39s	1776	688	Password
Steve	Telnet	PLATO	10.0.1.201	May 6 02:05:06 2004	0h 7m 59s	1988	1660	Password
Rachel	SSH	PLATO	10.0.1.201	May 6 02:04:02 2004	0h 9m 3s	1956	1512	publickey:RSA
Administrator	SSH	PRAGMASYS	10.0.1.201	May 6 01:54:23 2004	0h 18m 42s	296	392	publickey:DSA

Ready

Pragma FortressSSH 5.0
Secure Connectivity Software to Build
a Secure Enterprise Network with SSH

Secure Connectivity…
Done Right

Above is a FortressCL ssh client session into a RedHat Linux server named "Einstein". Below is a FortressFX sftp client session into the same Linux server for secure file transfers.

Why is Fortress important

Pragma Fortress includes one of the most feature complete, robust and high-performance Secure Shell server and client implementations in Windows. Remote access of systems is one of the most common tasks performed by most professionals and IT staff. It is very rare in today's network-centric world, for one to work with only one local computer. Quite frequently, an administrator or an end user has to login to other machines and start some task or monitor the progress of other tasks started earlier. These other computers could be in the next room or in multiple locations across a corporate environment.

Pragma FortressSSH 5.0
Secure Connectivity Software to Build
a Secure Enterprise Network with SSH

Secure Connectivity…
Done Right

The Internet and TCP/IP standard for remote access consists of telnet, rsh, rexec or rlogin. But these contain many flaws in that they are not secure because the password is sent in clear text and data is not encrypted. A hacker can simply sniff the data exchanges and capture the password and gain access to sensitive data. Fortress eliminates these security flaws. It introduces a single client and a single server, which can authenticate users based on any of the means used in telnet (password), rsh, rexec (password) and rlogin. It accomplishes this by establishing a secure channel using public key cryptography and strong encryption. Once a secure channel is established, credentials like password and data can be sent without worry as they are all encrypted. Additionally, newer authentication mechanisms such as Kerberos, Windows Active Directory/NTLM, and certificates are supported allowing even greater security in the system using Fortress. Further, with the port forwarding feature of Fortress, a secure tunnel is established between the ssh client and ssh server node over which non-secured TCP/IP applications like SMTP, POP3, Telnet, ftp, X-windows, etc., can be executed making them run securely without any change. All these capabilities make the users task easy and secure when Pragma Fortress is introduced in an organization. Users can continue to perform their everyday tasks, but now in a secure environment. It is designed to replace popular telnet, ftp and Unix/Linux 'r' commands and is able to perform other tasks like tunneling where it secures other protocol traffic, which was not originally designed to be transmitted in a secure manner.

In summary, SSH is a new generation industry standard protocol that allows SSH designers the freedom to architect SSH so that previous flaws of earlier TCP/IP application protocols are eliminated.

Fortress Components

Fortress has four key components:

- Fortress ssh server
- Fortress sftp-server
- FortressCL Terminal Emulation client
- FortressFX File Transfer client

In addition, for industrial and generic handheld devices, there are clients for PocketPC, Windows Mobile and Windows CE. The three typical uses of Fortress are shown below graphically: remote access, file transfer and tunneling.
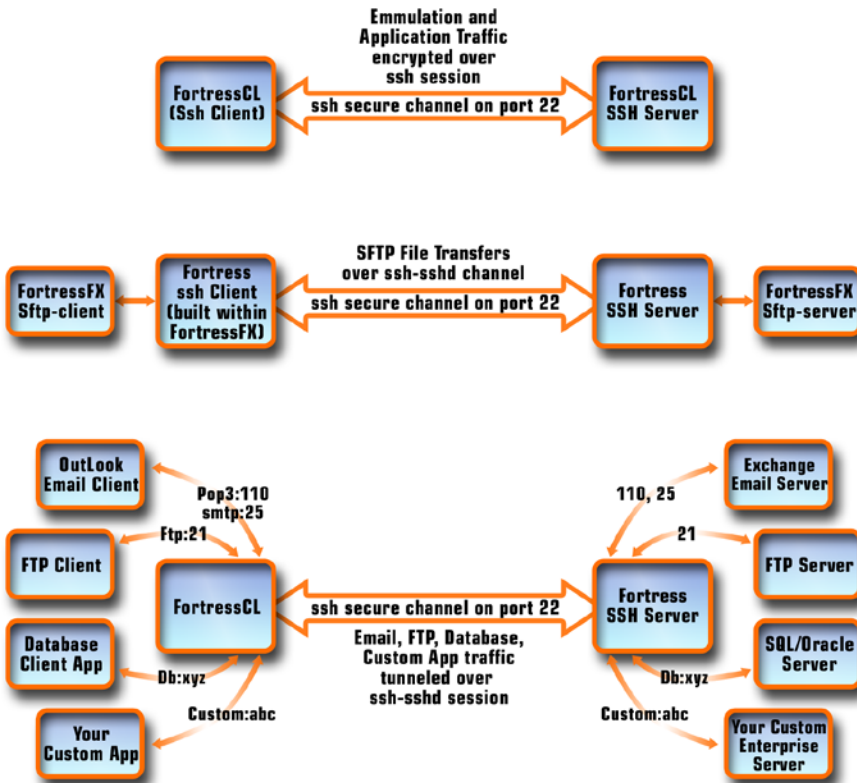
Secure Connectivity…
Done Right

PRAGMA
S Y S T E M S

Common Use Cases for Pragma's FortressSSH Server

Pragma Fortress is designed as a TCP/IP client-server model. The Fortress SecureShell Server (ssh) runs as a service in Windows 2003/2000/XP/Vista, and listens for connections from ssh clients on TCP port 22. A Fortress or ssh client is run to connect to a given ssh server identified by the host name. The client and server exchange RSA/DSA certificates to identify each other and then establish a shared secret key dynamically and securely using RSA/DSA public key encryption. The new shared secret key is then used for encrypting all future data between the ssh and ssh nodes during that session. At this stage, since a secure pathway exists, Windows Active Directory credentials, password or other authentication information can be transferred safely for user authentication.

Pragma FortressSSH 5.0
Secure Connectivity Software to Build
a Secure Enterprise Network with SSH

Secure Connectivity…
Done Right

Once the user authentication is complete, the ssh server typically provides the command shell of the operating system to the ssh client. The ssh client can type any command into this shell and get its output interactively. All input and output data are encrypted and optionally compressed during transit on the network. The session ends when a shell terminating command like "exit" or "logout" is typed on the ssh client. Thus, ssh access works very much like telnet access. If one has used telnet, rsh, rexec or rlogin, they will be at ease using the Fortress ssh client. In addition to interactive sessions, command line versions of clients are provided so that batch files and scripts can be written to fully automate regularly performed tasks without any human operator.

Another important use of Fortress is to use an ssh-sshd session as a secure tunnel to pass data from non-secure protocols like SMTP, POP3, FTP, TELNET, etc. to make them run in a secure manner without any change. In these cases, ports of the protocols to be protected are forwarded by proxy, listing them when a FortressCL or ssh client session is started.

Fortress Highlights

- First in the industry with full native 64-bit x64 support in both SSH servers and clients
- Pragma Wrap technology to allow all console/character programs to run in FortressSSH session
- Pragma Advanced Console technology which avoids screen scraping, avoids console and stream mode dichotomy to allow unlimited command history viewing in console mode similar to Unix/Linux
- Single sign-on for all your network access
- Enterprise wide deployment ability with Kerberos authentication working across Windows, Unix, Linux and all other major platforms
- Active Directory based Windows Authentication in Fortress servers and clients
- Auto Loading of Certificates at first logon for fully automatic Certificate login support; this allows great ease in setup of certificate base access to Fortress servers from any ssh client, be it Unix/Linux or Fortress client
- Remote access, file transfer, application delivery all occurs through a single port – port 22
- Latest US Government/NIST approved encryption standards like AES (Advanced Encryption Standard) are included
- Full management via graphical and command line management tools
- Full integration with Microsoft Windows environment
- High performance with maximum sessions support (700 in 32-bit and thousands in 64-bit)

Pragma FortressSSH 5.0
Secure Connectivity Software to Build
a Secure Enterprise Network with SSH

Secure Connectivity…
Done Right

How Pragma Fortress works

Pragma Fortress package contains a full implementation of the ssh server and ssh client in a Windows environment. Both the client and server run in Windows Vista/2003/XP/2000.

Pragma Fortress ssh server is a native, true multi-threaded implementation in Windows. We do not use Unix emulation on Windows like CYGWIN as they are a low performance interim solution not designed for the enterprise. Pragma's versions are written directly to the Microsoft Win32 API interface giving you maximum performance and feature compatibility throughout the Windows environment.

For Fortress ssh, Pragma uses its Inetd server to listen for the ssh designated port 22 (this is configurable for other ports, as well). Inetd server comes with Fortress and is built as a service in Windows, so it is always running in the background. When a ssh client connects to a ssh port (generally port 22), the Inetd server accepts the connection and then starts the ssh.exe secure shell server process to serve this particular ssh client. Inetd passes the socket handle of the remote client (ssh client in this case) to a started process (ssh.exe in this case) via a well known environment variable "PRAGMA-SYS_INETD_SOCK". Inetd server then continues to listen for the next client connection.

Both the ssh client and the ssh server from Pragma fully adhere to the SSH level protocol. This allows for full compatibility with any SSH level clients and servers available from other vendors in the industry for any operating system. The SSH standard uses RSA/DSA public key cryptography to negotiate securely a symmetric key that is used for encrypting and decrypting all communications between two machines. SSH1 is the original protocol which now has been replaced by the newer SSH2 version. Pragma Fortress 5.0 supports SSH2 protocols in its servers and clients (for both SSH1 and SSH2 support use Fortress 4.0).

Pragma Fortress client and server supports a port forwarding feature that allows any TCP/IP based programs to run over ssh-sshd secure channel. This creates a secure environment by using our Fortress package without additional software. Our solution is SSH standard based, so it is compatible with any other vendor's SSH port forwarding feature.
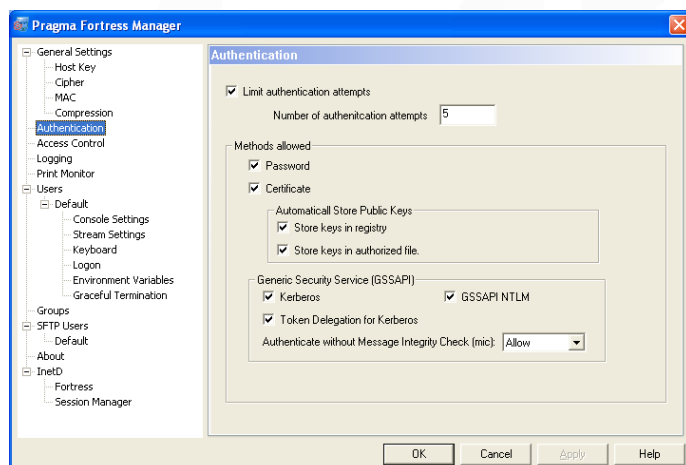
Secure Connectivity…
Done Right

Authentication

Authentication methods supported by Pragma Fortress are:

- Kerberos (using GSSAPI)

- Windows NTLM (using GSSAPI)

- Certificate based logins

- Password

Pragma Fortress provides comprehensive authentication support in both its servers and clients, allowing enterprises to choose the authentication methods suitable for its particular environment. All authentications are integrated with Windows Active Directory, allowing full use of Windows user accounts and security policy enforcements. SSH standard recommended GSSAPI (Generic Security Services Application Provider Interface) methodology is used to implement Kerberos and Windows NTLM authentication in Fortress. This allows interoperability between a Windows platform and Unix, Linux, Apple MacOS and other operating systems using any of these authentication methods. Kerberos authentication is the most advanced, is widely available, and is suitable for enterprises of any size. Kerberos is used in Windows Vista/2003/XP/2000 and can be the basis for building networks consisting of mixed operating systems. NTLM is used in Windows NT. The use of Kerberos allows single sign-on capability as the currently logged on user is able to login to Fortress server (ssh or sftp-server) without having to type in any credential information or password. Certificate based logins allow a user to login to their account if the public part of their certificate is stored in a well known location, typically their home directory. A site can change the configuration to suit their security requirement, limiting authentications or allowing all methods to be available. The screen below shows the Authentication selection screen within Pragma Fortress Manager.

Programs in Fortress packages

Pragma Fortress 5.0 supports operating systems Windows Vista/2003/XP/2000. For Windows NT support, customers can utilize our Pragma Fortress 4.0 product. The primary programs included with Pragma Fortress 5.0 product family are:

Inetdsrv.exe	Inetd server (similar to Inetd in Unix/Linux) for Vista/2003/XP/2000. Listens for incoming connections and starts ssh when a connection is established
sshd.exe	SecureShell server for Vista/2003/XP/2000
sftp-server.exe	Secure File Transfer server for Vista/2003/XP/2000
ssh.exe	Command line Secure Shell Client for Vista/2003/XP/2000. VT and WYSE emulations are supported
sftp.exe	Command line secure file transfer client for Vista/2003/XP/2000. Use in place of ftp client
sshkeygen.exe	SSH RSA/DSA key generator for Vista/2003/XP/2000
PragmaMgr.exe	Graphical Pragma Fortress Manager to modify Fortress server configurations
SessionMgr.exe	Graphical Pragma Fortress Session Manager to manage all sessions into Fortress servers
FortressCL.exe	Graphical Fortress ssh client that performs VT emulation and tunneling. Runs in Windows Vista/2003/XP/2000
FortressFX.exe	Graphical Fortress sftp client that performs secure encrypted file transfer. Runs in Windows Vista/2003/XP/2000
Pragmaftp.exe	Command line Pragma ftp client for Vista/2003/XP/2000 that supports passive mode of FTP needed to transfer files using FTP over ssh sessions

Pragma Fortress Client Suite includes FortressCL and FortressFX programs and adds many essential command line tools to manage systems into a single all encompassing package. One license of the Fortress Client Suite is included with each Fortress Server to evaluate the client in your enterprise. The Client software can be installed in the server machine or another PC. Additional client licenses can be purchased based on the number of client seats your enterprise needs. Pragma Fortress Client Suite is the single product that can meet the emulation and file transfer needs of the client side for Fortress or in an SSH environment.

Pragma Fortress comes in four packages:

- Pragma Fortress Server (32 bit)
- Pragma Fortress Server x64
- Pragma Fortress ClientSuite (32 bit)
- Pragma Fortress ClientSuite x64

Pragma Fortress is available in native 64-bit x64 format of AMD64 and IntelEMT64 64-bit processors. For the 64-bit versions, 64 is added to some binary names listed above, for example, ssh64.exe, Inetdsrv64.exe.

Manage keys with sshkeygen.exe

Every Fortress SecureShell node, be it client or server, needs to have a RSA/DSA key. This key, which is actually a pair of keys: one public and one private, is generated by the sshkeygen.exe program at install time or later if necessary. The public part of the key can be distributed widely so that other machines can talk to this machine. The private part of the key must be stored in a secure manner. Like other ssh vendors, our Fortress ssh key implementation is also file based. The Public part of the key is one file and the Private part of the key is another file. Typically, these files are named in pairs. If you specify the key name "mymachine" to sshkeygen program, it will store the public part of the key in "mymachine.pub" file and the private part of the key in "mymachine" file.

To avoid manual work, our install package automatically generates the private and public key pairs for the machine during install using the sshkeygen.exe program and stores them in a secure directory location. The machine's private key is stored in the "\Windows\System32\Drivers\etc\pragma_ssh_host_key" file and the public key is stored in the "\Windows\System32\Drivers\etc\pragma_ssh_host_key.pub" file. During uninstall of Fortress, only these two files are left intact so that next

time Fortress is installed, the machine's host key does not change. Using Pragma Manager's graphical program, administrators can change the host key or its directory location.

To simplify key distribution, ssh automatically sends the public part of the invocation key of a machine if it is not located in its information base. This public key information base is stored in the text file known_hosts and is located in the home directory of the user logging on typically "\Documents and Settings\Username\Application Data\PragmaSSH". As an administrator, you do not have to manually distribute machine public keys to other machines. Fortress can automatically build the public key information base as it encounters new machines in the network.

Like machines, each individual user who uses the Fortress ssh client, will need to have a RSA/DSA key pair, generated by sshkeygen.exe program and stored in:

 "\Documents and Settings\Username\Application Data\PragmaSSH" directory.

This RSA/DSA key file name is what you specify in "ssh –i mykey" part of the invocation command line or in the GUI clients. If no key name is given with "-i" option, then the key in "\Documents and Settings\Username\Application Data\PragmaSSH\id_rsa" is used as the keyfile name. During installation of Fortress client, the install program automatically generates this key pair: id_rsa and id_rsa. pub to represent the current logged on user. Also generated are the id_dsa/id_dsa.pub key pairs for use in an SSH2 environment as DSA keys and identity/identity.pub for SSH1 environment. Additional key sets to represent other users can be generated at any time by running the sshkeygen. exe program or the 'generate key' option in the graphical programs.

Note: It is very critical to guard files which are the private part of any RSA/DSA key. Private Key Files such as id_dsa, id_rsa and pragma_ssh_host_key must be protected by NTFS permissions so that only authorized individuals have read or access permission into it. For this reason, we recommend you to install Fortress packages in secured NTFS file systems.
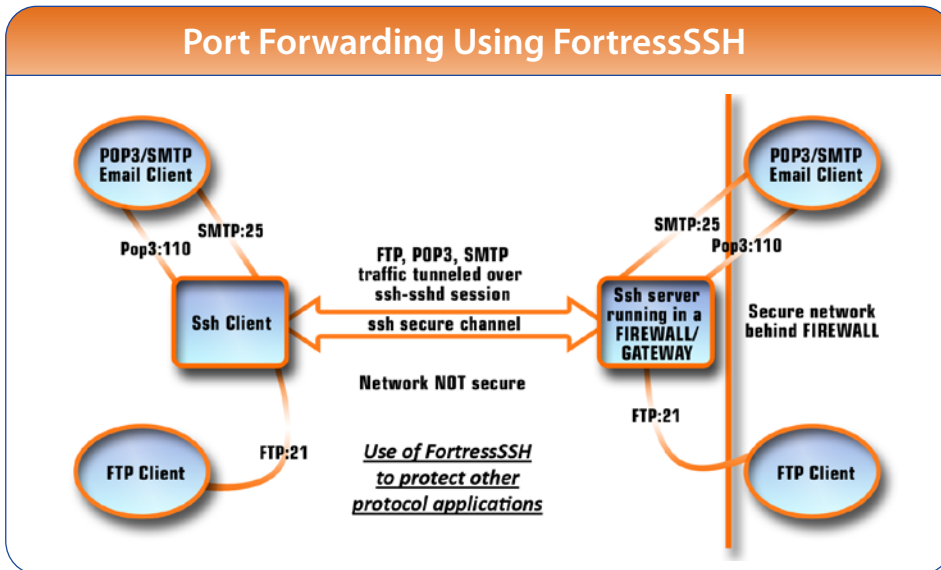
Port Forwarding secures other TCP/IP programs

The port forwarding feature of Fortress allows any TCP or UDP application to be secure by passing their data over the secure ssh-sshd session without any changes to the application. This creates a secure application environment by using ssh technology. The diagram below shows its use where ftp, smtp and pop3 traffic are passed through a ssh-sshd session.

Secure Connectivity...
Done Right

PRAGMA
SYSTEMS

Port Forwarding Using FortressSSH

POP3/SMTP
Email Client

SMTP:25
Pop3:110

FTP, POP3, SMTP
traffic tunneled over
ssh-sshd session

ssh secure channel

Ssh Client

Network NOT secure

FTP:21

*Use of FortressSSH
to protect other
protocol applications*

FTP Client

POP3/SMTP
Email Client

SMTP:25
Pop3:110

Ssh server
running in a
FIREWALL/
GATEWAY

Secure network
behind FIREWALL

FTP:21

FTP Client

Interoperability with Unix/Linux

Pragma Fortress ssh programs are fully standard compliant. Our ssh server in Windows can be accessed by any ssh client running in any operating system. Similarly, our ssh client, running in Windows, can access any ssh server running in any operating system. In actual tests, Pragma Fortress running on Windows have been accessed from SSH clients of HP-UX, Linux, Solaris, AIX, MacOS, OpenSSH, SSH Communication, Attachmate Secure IT, and many other third party ssh clients. Our Windows Fortress ssh/sftp clients has accessed SSH servers of HP-UX, Linux, Solaris, AIX, MacOS, OpenSSH, Attachmate Secure IT, and SSH Communication. Kerberos Authentication has been tested between Pragma Fortress in Windows Active Directory and OpenSSH implementation across Linux and other platforms. As long as the SSH conforming protocol is used, Fortress is compatible with any vendor's ssh server or client, including all authentication mechanisms.

Pragma FortressSSH 5.0
Secure Connectivity Software to Build
a Secure Enterprise Network with SSH

Secure Connectivity…
Done Right

Sample use cases for Pragma Fortress

Secure remote access and running of applications

Instead of telnet, rsh or rexec, one would use a ssh client to connect to a ssh server, get a Windows command shell session, and then run any console mode or character mode applications or commands. Edit, vi, emacs, net, ps, pstat, netstat, ping, ipconfig, kill, shutdown, net view, net use, passwd, dir, cl, link and debug commands can be run over ssh session. All regular applications thus run securely.

Secure remote systems management

An administrator can initiate ssh sessions into systems that need management or monitoring. These management nodes can now be Windows servers running Pragma Fortress server. Many Windows management tools have command line access. Process status (ps), event log monitoring, process kill (kill), performance monitoring (pstat), file editing (edit), network monitoring (net), system shut-down and reboot (shutdown), user addition (net user), and active directory management are many of the daily admin tasks that can be performed securely over an ssh session. No Windows password will be compromised. With ssh, Linux, Solaris, HP-UX, AIX, Windows servers, Windows client nodes can be managed from a single ssh client console.

Secure email access

Fortress provides two choices for secure email access. You can install Fortress in your email server or put it in some other machine and use it as a gateway to go to your email server. For email you have to redirect two ports, pop3:110 for mail retrieval and SMTP:25 for sending mail.

Secure Email Access Across Fortress
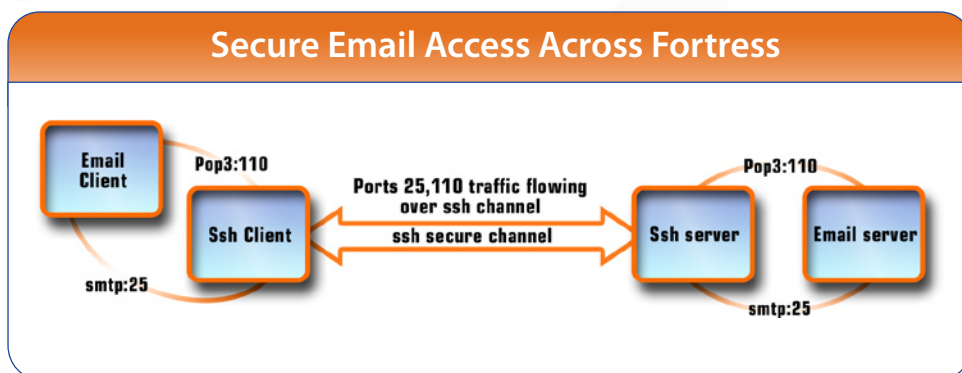
SSH –g –L 25:email.company.com:25 –L 110:email.company.com:110
email.company.com

Configure Outlook/Eudora/emailclient to use localhost as the SMTP
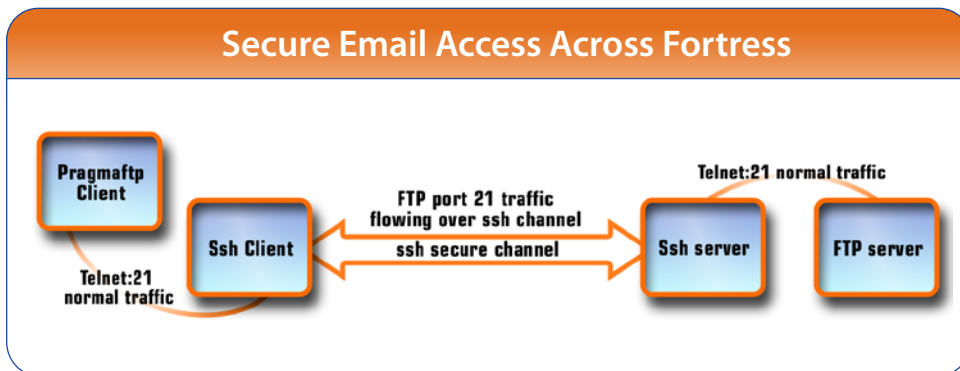and POP3 server name

Pragma FortressSSH 5.0
Secure Connectivity Software to Build
a Secure Enterprise Network with SSH

Secure file transfer via FTP

Fortress provides two choices for secure file transfer via FTP. You can install the Fortress server in your ftp server or install it in some other machine and use it as a gateway to go to your ftp server.

Secure Email Access Across Fortress

SSH –g –L 21:ftp.company.com:21 ftp.company.com

Pragmaftp localhost

>passive

>cd /pub/docs

>get afile

>put afile

>quit

SSH –g –L 21:ftp.company.com:21 gateway.company.com

Pragmaftp localhost

>passive

>cd /pub/docs

>get afile

>put afile

>quit

Secure Connectivity…
Done Right

Securing Telnet

Fortress provides two choices for securing Telnet. You can install the Fortress ssh server in the machine running telnet server or install it in some other machine and use it as a gateway to go to your telnet server.

Securing Telnet Across Fortress
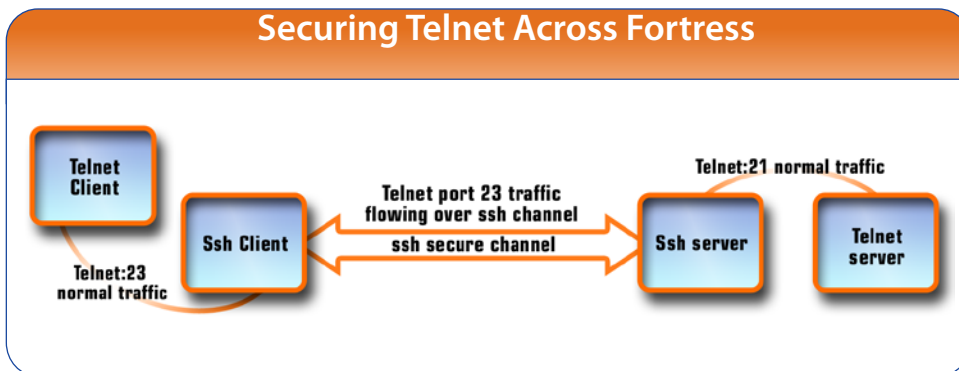
SSH –g –L 23:ahost.company.com:23 ahost.company.com

telnet localhost

Configuring Pragma Fortress

Pragma leverages the ease of use typically associated with Windows based programs. Complex option settings common in Unix ssh are replaced by graphical dialog boxes where most configuration options can be easily selected or modified. A single graphical program called "Pragma Fortress Manager" allows all configuration changes. Settings are also stored in Windows registries for easy maintenance and control. Registry items are stored under "HKEY_LOCAL_MACHINE\SOFTWARE\ PragmaSystems".

Configuring Pragma Fortress Clients

Pragma Fortress clients (FortressCL, FortressFX and command line ssh.exe, sftp.exe) perform their configuration settings within their own programs. GUI Clients FortressCL and FortressFX provide easy graphical configuration changes and store them in Windows registry for later uses. For command line versions, we have maintained the switches as they are in Unix ssh/sftp clients. Running any command line program, like ssh or sftp, without any parameters lists the options switches allowed in that command.

Pragma PocketVT extends Fortress to handhelds

Pragma's PocketVT product line extends Fortress client reach to industrial and generic handheld devices. Handhelds from Symbol, Intermec, LXE, Techlogix, PSC and others are supported. Most industrial devices running Microsoft PocketPC, Windows Mobile or Windows CE operating systems are supported. PocketVT is customized for most devices so that the advantages of a device, like built-in scanner, RFID, keypads are fully available to the users. VT emulations are supported and both ssh and

Secure Connectivity…
Done Right

telnet protocols are available. This allows customers with current telnet deployments to quickly and seamlessly transition over enterprise applications to SSH. PocketVT is fully industry compliant and it's ssh/telnet client works with Pragma's ssh/telnet servers and any industry compliant ssh/telnet servers of other vendors.

State of the Industry

Security is a big concern for the generally open access oriented TCP/IP protocols, on top of which Internet and IT networks are built. In a rapid pace, enterprise computing and IT activities are taking place over the Internet and the Web. Security has become a paramount issue. Without secured access and secured protection of resources and transactions, the net is a hacker's paradise. Pragma Fortress can help make an enterprise and the net more secure. SSH has been widely adopted in the Unix and Linux community. With the full featured Fortress Server for Windows 2000/2003/XP/Vista from Pragma, Windows nodes can now be securely accessed and managed using the proven ssh standard. The ssh standard will now be more widely adopted since all three core enterprise platforms of the net age: Unix, Windows 2003/2000 and Linux, can be securely accessed and managed by ssh.

In addition, PKI (Public Key Infrastructure) is continuing to gain support in the industry. Authentication via cryptographic certificate, Active Directory and other identity management packages will supplant the password based authentication that is still common. Pragma Fortress supports these key authentication methods and thus can be widely deployed in the enterprise to build all Windows networks or one based on a mix of Windows, Unix, Linux and Mainframe systems.

Resources

*   A book. SSH – The Secure Shell. By Daniel J. Barrett & Richard E. Silverman. Publisher: O'Reilly. 2001. The definitive guide for Secure Shell protocol and its use in many platforms.

*   A book. Unix Secure Shell. By Anne Carasik. Publisher: McGraw Hill. 1999. Discusses Secure Shell protocol and its use in Unix.

*   User Guide for Pragma Fortress. Covers Pragma's Windows 2000/2003/XP/Vista Secure Shell servers and clients. Available from Pragma as part of Pragma Fortress product. www.pragmasys.com/Fortress

*   Web site of SSH Communications Security, the creator of SSH protocols. They provide ssh servers for Unix/Linux/Windows and ssh clients for Unix/Linux, Windows and Macintosh. www.ssh.com

*   www.ietf.org/html.charters/secsh-charter.html

Copyright © 2006, Pragma Systems, Inc. All rights reserved.

Pragma FortressSSH 5.0
Secure Connectivity Software to Build
a Secure Enterprise Network with SSH

17