# Stepping Up Security: Migrating from Telnet to SSH

**A WHITE PAPER**

PRAGMA SYSTEMS

## Objective :

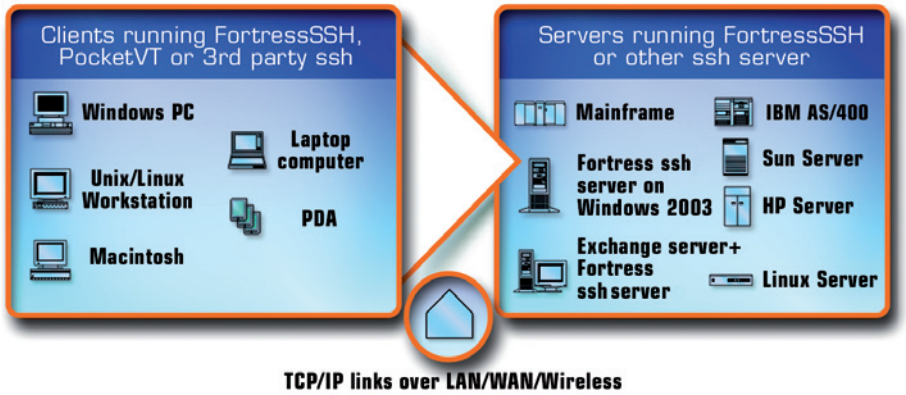
*The objective of this white paper is to examine the need for organizations to migrate from Telnet to the SSH (Secure Shell) protocol; analyze the implications and benefits of adopting SSH; and review the role Pragma Systems and its Fortress SSH product can play in a robust, secure computing environment.*

## Executive Summary

In today's complex business world, companies find it increasingly necessary to venture beyond their own network firewalls to interact electronically with outside vendors, customers or business partners. As they do, administrators and IT officers know only too well that, when it comes to a company's network, security is now as important as – if not more important than – functionality and ease of use.

The natural tension between the demands of day-to-day business and the need for greater system security is prompting many companies to migrate from the straightforward simplicity of Telnet to the heightened level of security that is provided by Secure Shell, or the SSH protocol. And, as they do, Pragma Systems' suite of Fortress products is becoming their platform of choice.

### Overview of SSH Architecture



## Internet Security: Dangers Beyond the Firewall

As company IT directors understand better than anyone, as invaluable as the Internet can be for easing communications with customers, vendors and business partners, it can also be an extremely insecure place. As more and more businesses venture beyond the firewall, anything their employees do online can be readily monitored by unauthorized third parties. If sent without encryption, passwords, account numbers, and mission-critical correspondence can all be recorded for future use by cyber criminals – and third parties with malicious intent can wreak havoc inside the corporate environment.

Given the gradual breakdown of boundaries between internal and external networks, it is easy to see why companies of all sizes are finding it increasingly difficult to protect their networks and systems from a variety of threats. Whether the reason is sophisticated worms or backdoor-based network attacks, legislation or inter-company agreements, security-conscious organizations are increasingly making the decision to migrate from Telnet to the exponentially more secure SSH protocol as part of a comprehensive upgrade for their data-protection and risk-management needs.

## Government Regulation: SOX and Other Data-Protection Mandates

With companies of all sizes, now, security concerns no longer are simply an internal question of business concerns and survival. Layer in state and federal regulatory requirements to keep customer and other sensitive corporate data confidential, and legislators have exponentially raised the security stakes for many organizations. Given the alphabet soup of recent federal regulation – from GLBA (the Gramm-Leach-Bliley Act) to HIPAA (the Health Insurance Portability & Accountability Act) to SOX (Sarbanes Oxley) – protection of a company's financial data increasingly rests with the IT department. The most pressing of these regulatory mandates may be the need for mid-sized and smaller companies to comply in the very near term with the tenets of SOX. While it is true that privately held companies are exempt from the Act's stringent corporate-governance requirements, more and more public and international organizations have begun demanding that their partners and vendors certify compliance in a bid to head off potential legal or regulatory challenges.

Last year, the U.S. Securities and Exchange Commission (SEC) granted a brief extension to companies with a market valuation of $75 million or less. By December 2007, however, all companies covered by the act, regardless of size, must report on the effectiveness of their own internal controls – and by end-2008, must complete external audits of their security measures. As the SEC moves toward full compliance with the Act, then, private and small to-mid-sized firms are likely to face increasing pressure to, at a minimum, effect comprehensive security improvements – and stepped-up security begins with an upgrade from Telnet to SSH.

PRAGMA SYSTEMS

## Telnet: The Good, the Bad and the Insecure

Telnet debuted in the late 1960s, when the concept of networking computers was new, and there were a limited number of computers even in existence. Then, as today, its simplicity was one of its selling points – and it is the main reason it continues to be one of the most popular ways of working on the Internet. Telnet essentially allows users to open a session on a remote server and work in the file system as though they were working in front of a machine – but Telnet's simplicity is, at once, its greatest strength and greatest weakness. With Telnet, whatever text a user types and sends travels across the network essentially unchanged. That means that, since users are typically required to log into remote computers, their user names and passwords get sent across the network in plain text.

It is a process roughly analogous to writing a name on a piece of paper and passing it to someone who shouts the name across a crowded room to someone else who writes it down on another piece of paper, repeating this process in a chain until the name reaches the intended recipient. Telnet's simplicity requires that businesses trust all of the computers and people along that chain – any one of which could record user name and passwords and use them to log onto the same remote computers.

Telnet's lack of encryption, even for passwords, is, arguably, its biggest inherent limitation – flanked by its inability to prevent "man-in-the-middle" attacks, where information being passed between two parties is intercepted by a third party without the knowledge of the other two. Telnet is unable to authenticate user identities because this ability was not needed when it was first developed, when the Internet was used primarily for government, academic and research purposes. As the Internet became available to the general public, Telnet became increasingly vulnerable – and is, in fact, no longer recommended for any person or organization utilizing a public-access portal to the Internet or requiring additional computer security.

## SSH: Securing the Network

In its simplest form, SSH is a straightforward replacement for Telnet, RSH and rlogin. It's important to note that SSH is a protocol, not a product; as such, it is a specification of how to conduct secure communication over a network. The SSH protocol covers authentication, encryption, and the integrity of data transmitted over a network. SSH was developed in 1995 to correct many of the security problems with Telnet, and has gradually been replacing Telnet ever since. The advantage of SSH, which is now an RFC standard (RFC 4251, 4254, 4256, 4252, 4344, 4462 and 4253), is that it can handle all the same things Telnet can, but steps up computing security by using both encryption and public key authentication.

SSH offers organizations the same basic capabilities as Telnet, providing command-line interfaces to remote computers in a virtually identical way. The main difference: SSH encrypts all text in a

way that only the two computers supposed to be involved in the conversation can understand. This means the likelihood of an unauthorized party gaining access to company machines or data is minimal. (As a further security measure, many organizations also limit SSH connections to specific IP addresses, denying anyone attempting to access the network from outside the set of permitted IPs, even if they have the appropriate log-in information.)

To summarize, SSH protects against:

- Eavesdropping of data transmitted over the network
- Manipulation of data at intermediate points – for example, routers – within the network
- IP address spoofing where an attack hosts pretends to be a trusted host by sending packets with the source address of the trusted host
- DNS spoofing, where an attacker forges name server records
- Interception of cleartext passwords and other data by intermediate hosts
- Manipulation of data by people in control of intermediate hosts
- Attacks based on listening to X authentication data and spoofed connection to the X11 server

The SSH protocol can be used to login securely into another computer over a network, execute commands on a remote machine, and copy files from one machine to another. What's more, SSH provides strong authentication and secure communications over insecure channels – and, in addition to facilitating secure X11 connections, is an ideal replacement for rlogin, rsh, and rcp.

## Drivers for Change

As organizations move, then, to migrating from a Telnet server environment to an SSH protocol, their key reasons include:

- The fact that SSH is an encrypted protocol. All data sent over the network from computer to server and vice-versa is encrypted
- The SSH protocol allows for a wide range of security options when logging into user accounts, including passphrase authentication, certificate login, X forwarding, compression and even more secure restrictions
- SSH is a proven, established protocol that has been used by companies worldwide for more than a decade
- The availability of a broad range of mature SSH clients and servers for Windows, Macintosh, Unix and other operating systems

# Secure Connectivity...
## Done Right

PRAGMA SYSTEMS

### Why Pragma Systems?

Pragma Systems provides remote access and connectivity solutions that fundamentally solve the security challenges associated with remote management, file transfer, and application delivery across a networked environment.

The corporation of today is faced with constant challenges in providing secure and reliable access, control, and management capabilities across its network and computing infrastructure. With these challenges come seemingly endless requests for more information, more access, and more productivity.

Unfortunately, more and more solutions providers are offering generic, one-size-fits-all, one-stop networking, infrastructure, and security solutions. And that is where Pragma Systems comes in. Pragma Systems is laser-focused on providing the most secure, fast, scalable and reliable solutions for corporate SSH connectivity needs.

### The Pragma Fortress 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 needs 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 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 levels without the associated constraints of the 32-bit architecture. The Fortress line is built with the widely used SSH protocol, the de facto industry standard for secure remote access and file transfer. SSH is now an approved IEEE draft standard.

# Secure Connectivity…
## Done Right

*The following chart breaks down, capability by capability, why so many companies are turning to Pragma's Fortress line to upgrade from Telnet and shows the competitive advantages of Pragma's SSH offerings:*

| | Pragma | SSH Comm. | Van Dyke |
|---|---|---|---|
| **Product Name** | **FortressSSH** | **Tectia** | **VShell** |
| Windows SSH Server | ✓ | ✓ | ✓ |
| Windows SSH Client | ✓ | ✓ | ✓ |
| Native 64-bit | ✓ | | |
| Native 32-bit | ✓ | ✓ | ✓ |
| Console Mode Support | ✓ | | ✓ |
| Console Mode with Command History | ✓ | | |
| Can Run All Character Mode Applications | ✓ | | |
| Can Run Apps like Microsoft Resource kit, vi | ✓ | | |
| Run Oracle, CA Ingress Database Command Line Programs | ✓ | | |
| SAP Console Application Support | ✓ | | |
| Kerberos/GSSAPI Support | ✓ | ✓ | ✓ |
| Stream Mode Support | ✓ | ✓ | |
| Centralized Configuration Management | ✓ | ✓ | |
| Remote Session Management | ✓ | | |
| Command Line Clients Bundled | ✓ | | |
| Handheld Client Support | ✓ | | |
| Windows Mobile Support | ✓ | | |
| Number of Connections Supported in 32-bit Server | 1000+ | 60 | 70 |
| Number of Connections Supported in 64-bit Server | 1000+ | no 64-bit ver. | no 64-bit ver. |
| Secure File Transfer | ✓ | ✓ | ✓ |
| Unattended/Scripted Install | ✓ | | |
| GUI Configuration Manager | ✓ | | |
| NTLM Logon | ✓ | | |
| Public Key Logon | ✓ | ✓ | ✓ |
| Nested Session Support | ✓ | | ✓ |
| Proven Years of Windows Server Experience (Telnet) | ✓ | | |
| High-Performance Multi-Threaded Design | ✓ | | |
| Optimized with Overlapped I/O, Winsock | ✓ | | |
| Performance | Best/Fastest | Good | Very Good |
| Port Forwarding | ✓ | ✓ | ✓ |
| VT Terminal Support | ✓ | ✓ | ✓ |
| Wyse, IBM ASCII Terminal Support | ✓ | | |
| Windows Vista Support | ✓ | | |
| Windows 2008 Server (Longhorn support) | ✓ | | |

To facilitate more effective integration with Microsoft Windows, Pragma has added many enhancements to the Fortress line over what other SSH vendors provide. One example of its efforts is the Active Directory based Windows native authentication support (Kerberos & NTLM) that comes with all Fortress servers and clients, which allows single sign-on and seamless secure access to any Windows server or PC. And, since Fortress is built using the SSH standard, it is compatible with the SSH clients and servers of other vendors, including SSH Communications, Attachmate, OpenSSH, Sun, IBM, HP, Apple and Cisco.

Fortress has been designed from the ground up utilizing 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 sshd.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.

## Data Encryption

With Fortress, 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 (Motorola/Symbol, Intermec, LXE, PsionTekLogix and others).

Fortress Servers are available to run in Windows Vista/2003/XP/2000. Fortress interoperates seamlessly with any secure shell server or client, including Linux, Unix and Apple, 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.

With Fortress, SFTP (Secure File Transfer Protocol) – part of the SSH protocol set offering -- replaces the non-secure FTP (File Transfer Protocol), and SCP (secure copy) replaces the non-secure "rcp" (remote copy) command. SSH also comprises a port-forwarding capability, in which standard applications like e-mail and other corporate applications can be made to run securely by passing all data from these applications over secure SSH channels.

# Secure Connectivity…
## Done Right

PRAGMA SYSTEMS

## Mobile Network Solutions

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 offers its customers a unique, 2:1 combination of Telnet and SSH technologies that work across a company's server and clients – including most industry standard mobile and handheld devices. That is because Pragma stands alone in providing innovative, cost-effective solutions that enable secure, seamless and speedy remote management, data and file transfer, and customized application support.

As Pragma Systems Vice President of Sales & Marketing Andrew Tull points out, the strongest and most flexible secure connectivity solutions work with your existing environment and utilize management systems that support today's toughest standards: 802.11i, WPA2, AES encryption, RFID, and more. "We have designed our Pragma solution specifically to help companies facing vertical supply-chain management challenges meet their connectivity needs in the most secure, reliable way possible," explains Tull. "Pragma's server and client technology solutions give you the cost-effective tools you need to securely manage your systems throughout your Windows based network."

## Pragma Systems Delivers

A long line of companies have come to rely on Pragma's outstanding performance, superior customer service and across-the-board reliability. Companies like McKesson, Micron Technology, Marshfield Clinic, Biogen, Sandia National Lab and many more have migrated from Telnet to Pragma FortressSSH solutions.

Call Pragma today, and learn how we can help your company by providing:

- Reliable, proven enterprise-grade secure connectivity software for all Windows® environents:
    - That's highly-secure – even offering a protocol for secure remote login and other secure network services over an insecure network;
    - Facilitates data and system management;
    - Allows secure file transfers; and
    - Provides consistent, reliable application delivery
- Gives you and your company a powerful, convenient approach to protecting communications on a computer network
- Superior and responsive customer service – both throughout the sales process and during lifetime of usage
- Offers peace of mind

## To Contact Pragma Systems

Pragma Systems, Inc.
13809 Research Blvd.
Suite 675
Austin, Texas 78750
Corporate: 512.219.7270
Sales: 800.224.1675
FAX: 512.219.7110

sales@pragmasys.com

www.pragmasys.com

## Additional Resources:

For information on SSH servers and products:

www.pragmasys.com

For a copy of the Sarbanes-Oxley Act of 2002, or detailed information on compliance requirements:

www.sec.gov

For a link to discussion forums on SOX:

http://www.sarbanes-oxley-forum.com/

For more information in IEEE:

http://www.ieee.org/portal/site

For more information on the Internet Engineering Task Force and RFC standards:

http://www.ietf.org/