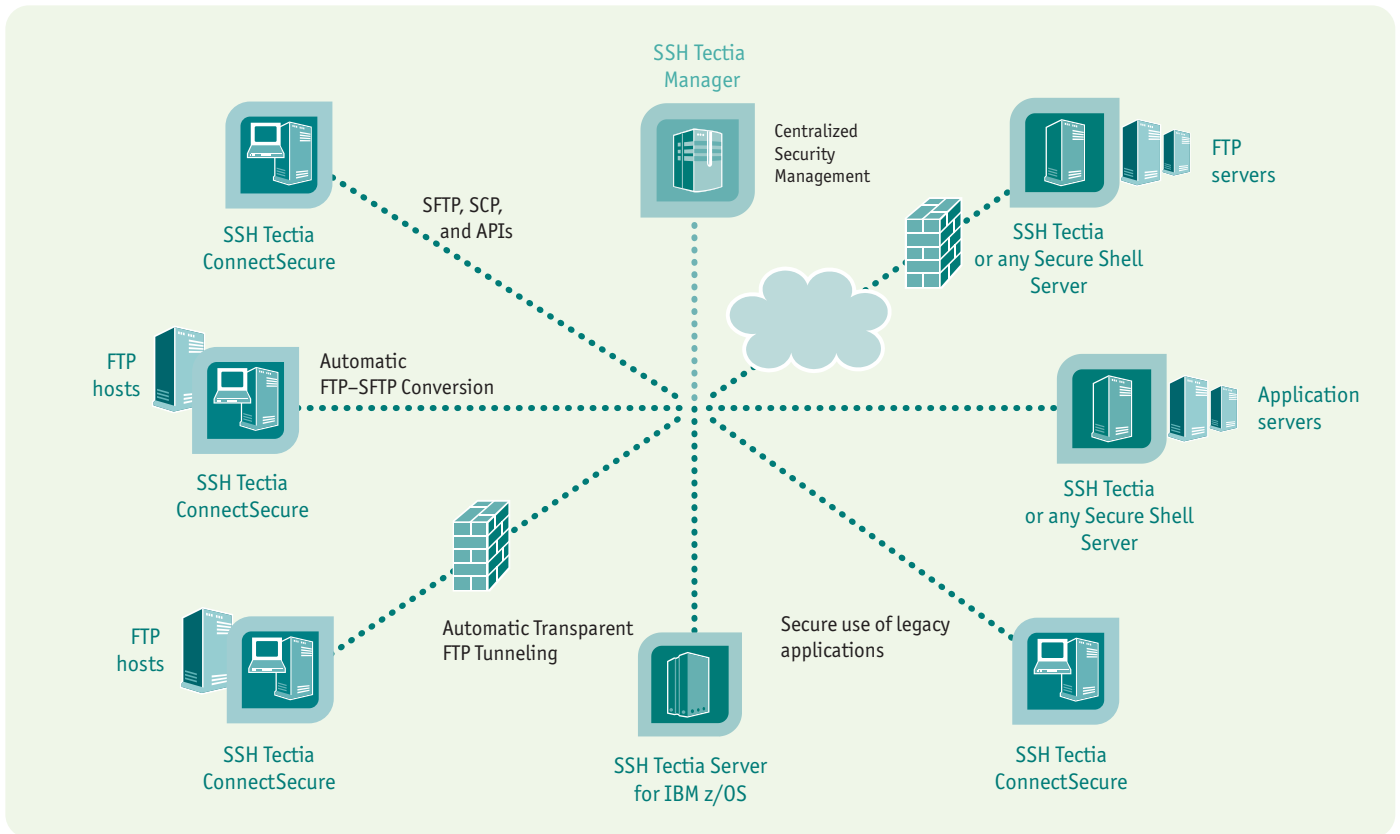




SSH Tectia® ConnectSecure 6.0 Securing File Transfers and Data-in-Transit



SSH Tectia® ConnectSecure is a robust enterprise-class product that enables organizations to quickly and cost-effectively secure any FTP file transfer and data-in-transit without any modification to the existing infrastructure, scripts or applications. SSH Tectia ConnectSecure easily and seamlessly integrates into SSH Tectia Server or other Secure Shell (including OpenSSH) servers to provide enhanced secure file transfer functionality for today's demanding enterprise environments.

Enterprise IT departments are challenged to keep sensitive information confidential, while at the same time facing scarce funding and increased regulatory and audit compliance demands. SSH Tectia ConnectSecure drastically reduces the cost and time needed to secure FTP file transfers and data-in-transit, enabling organizations to reduce risk compliance with laws and regulations, such as PCI DSS, SOX, FISMA, and HIPAA.

SSH Tectia ConnectSecure provides strong authentication, encryption and data integrity across Windows, Linux, and Unix platforms. Supported third-party authentication systems include RSA SecurID®, Entrust® PKI systems, smart cards (including CACs), and hardware tokens.

SECURE FILE TRANSFERS

SSH Tectia ConnectSecure enables organizations to securely transfer files within cross-platform environments, with advanced drop-in functionality, such as Automatic FTP-SFTP Conversion and Transparent FTP Tunneling, which enable users to easily secure file transfers without modifications to existing applications or scripts. Additional

tools, such as the versatile SFTP and SCP command-line tools and secure file transfer APIs, all built on the SSH G3™ architecture with unparalleled SFTP throughput and scalability, are included to meet mission-critical IT security requirements.

SECURING DATA-IN-TRANSIT

For the past decade, computer technology has evolved at great speed, but IT departments have not always been able to modernize software applications at the same rate. As a result, they are forced to support and maintain legacy systems, which often lack adequate security measures.

To cost-effectively extend the useful lifetime of these business-critical systems, SSH provides enterprise IT and security departments with SSH Tectia ConnectSecure, which transparently secures application data-in-transit between workstations and application servers or between servers, all without modifications to the applications or IT infrastructure.

CENTRALLY MANAGED

SSH Tectia ConnectSecure can be centrally managed with SSH Tectia Manager, a cost-effective management solution to pre-configure, deploy, maintain and help audit the SSH Tectia environment from a central location, making it ideal for large enterprises.

SSH Tectia ConnectSecure interoperates with commercially available Secure Shell servers as well as open-source implementations found in many of the leading OSs.

Features

Secure File Transfer

- Transparent, Automatic FTP-SFTP Conversion
- Transparent FTP Tunneling
- Secure peer-to-peer file transfers
- Advanced security options configurable per FTP application executable or script
- Checkpoint/restart, mid-file transfer recovery
- Multi-gigabyte file size support
- Strong data encryption
- Strong file integrity checking
- Streaming for fast performance ⁽¹⁾
- Data stream compression for low-speed connections
- SFTP and SCP command-line tools
- Complete Java and C APIs for SFTP
- Logs and auditing information
- Prefixing to prevent file usage before transfer is complete
- SFTP Extensions for MVS dataset direct streaming ⁽²⁾
- SFTP Extensions for SITE command support ⁽²⁾
- Support for MVS and USS file systems ⁽²⁾
- Automatic EBCDIC-ASCII Character Conversion ⁽²⁾

Secure Data-in-Transit

- Automatic Tunneling
- TCP/IP port forwarding
- Transparent TCP Tunneling ⁽³⁾
- Automatic encryption of data-in-transit
- Comprehensive Filter Rules for tunneling configuration

Security

- Automatic transparent encryption of data-in-transit, including user ID and password
- Firewall-friendly architecture
- Multi-tier security architecture
- Configurable re-keying policies
- Authentication agent functionality
- Multiple channel support
- Compliance with the IETF Secure Shell (secsh) standards

Ease of Implementation

- Automatic connection setup – connection parameters, including user name and destination host captured from FTP datastream
- Configurable FTP fallback option for controlled and phased deployment
- Centralized deployment and management through SSH Tectia Manager

Comprehensive and Flexible Authentication

- Password user authentication
- Public-key authentication (client and server)
- Two-factor user authentication based on smart cards and cryptographic tokens
- Keyboard-interactive interface for easy integration with third-party methods
- Support for GSSAPI/Kerberos
- Support for OpenSSH keys

⁽¹⁾ When used with SSH Tectia Server

⁽²⁾ When used with SSH Tectia Server for IBM z/OS

⁽³⁾ With Windows

Specifications

Supported Cryptographic Algorithms

Asymmetric (Public-Key) Algorithms

- Diffie-Hellman, DSA, and RSA

Symmetric (Session Encryption) Algorithms

- AES (128 / 192 / 256 bit)
- 3DES (168 bit)
- Arcfour (128 bit)
- Blowfish (128 bit)
- SEED (128 bit)
- Twofish (128 / 192 / 256 bit)
- Cryptocore Rabbit Stream Cipher (128 bit)

Data Integrity Algorithms

- HMAC MD5 and HMAC SHA-1
- Cryptocore Badger MAC

Certifications

- FIPS 140-2

Supported PKI Specifications

- X.509 v3 certificate support
- X.509 v2 CRL fetching via HTTP, LDAP, offline
- OCSP
- PKIX CMPv2 support
- PKCS#7 and PKCS#12 import
- PKCS#8 and PKCS#11 key support
- MSCAPI support on Windows

Supported Third-Party Authentication Products

- Entrust Authority™ Security Manager 7.1-7.2
- RSA Keon®
- Microsoft CA
- Windows domain authentication through GSSAPI
- RSA SecurID®
- SafeWord® through PAM
- Microsoft IAS through RADIUS
- FreeRADIUS
- Centrify Direct Control 3.0

Supported Platforms *

- HP-UX 11i v1, 11i v2, 11i v3 (PA-RISC)
- HP-UX 11i v2, 11i v3 (IA64)
- IBM AIX 5.3 (POWER)
- Microsoft Windows 2000, XP, Server 2003 (x86)
- Red Hat Enterprise Linux 3, 4, 5, 5.1 (x86)
- Red Hat Enterprise Linux 3, 4, 5, 5.1 (x86-64)
- Sun Solaris 8, 9, 10 (SPARC)
- Sun Solaris 10 (x86-64)
- SUSE Linux Enterprise Desktop 10 (x86)
- SUSE Linux Enterprise Server 9, 10 (x86)
- SUSE Linux Enterprise Desktop 10 (x86-64)
- SUSE Linux Enterprise Server 9, 10 (x86-64)



* The SSH Tectia products can run on any standard hardware capable of running the supported operating system versions.

FINLAND

Valimotie 17
FI-00380 Helsinki
Tel: +358 20 500 7000
Fax: +358 20 500 7001
sales.fi@ssh.com
www.ssh.com

GERMANY

Lintorfer Str. 7
De-40878 Ratingen
Tel: +49 2102 30979 0
Fax: +49 2102 30979 0
sales.de@ssh.com
www.de.ssh.com

USA

20 William Street G35
Wellesley, MA 02481
Tel: +1 781 247 2100
Fax: +1 781 431 0864
sales.americas@ssh.com
www.ssh.com

JAPAN

sales.jp@ssh.com
www.ssh.com/jp/

UNITED KINGDOM

SoanePoint, 6–8 Market Place
Reading, Berkshire
RG1 2EG
Tel.: +44 (0) 1189 255 580
Fax: +44 (0) 1189 255 586
sales.uk@ssh.com
www.ssh.com



© 2008 SSH Communications Security Corp. All rights reserved. ssh® and Tectia® are registered trademarks of SSH Communications Security Corp in the United States and in certain other jurisdictions. The SSH and Tectia logos are trademarks of SSH Communications Security Corp and may be registered in certain jurisdictions. RSA, RSA Secured, and SecurID are either registered trademarks or trademarks of RSA Security Inc. in the United States and/or other countries. Entrust is a trademark of Entrust, Inc. in the United States and/or other countries. Entrust is a registered trademark of Entrust, Inc. in the United States and other countries. In Canada, Entrust is a registered trademark of Entrust Technologies Limited. All Entrust product and program names are trademarks of Entrust, Inc. All other names and marks are the property of their respective owners. FIPS 140-2 Validated™: A Certification Mark of NIST, which does not imply product endorsement by NIST, the U.S. or Canadian Governments.