

Securing File Transfers and Application Traffic

Tectia ConnectSecure makes file transfer operator's life easier and offers a cost-effective way to reach an advanced security level in the file transfer network.

Is your file transfer and application traffic secure?

If your business applications transfer confidential information, such as customer credit card information, make sure it happens securely. Man-in-the-middle attackers can easily intercept unsecured file transfers and can cause financial and public image losses. With Tectia ConnectSecure you can easily add a secured file transfer layer based on Secure Shell (SSH) to your application architecture.

What to do with all the FTP hosts and file transfer scripts?

Tectia ConnectSecure offers an automated way to move from an unsecured system to a secured system with only small changes to the existing network topology and with no changes to scripts or applications. Tectia ConnectSecure can be placed next to FTP hosts to automatically capture unsecured plaintext data traffic, convert it to SFTP or tunnel it over SSH, and transport the data encrypted. The data is delivered to the destination host secured and safe from man-in-the-middle attackers.

What about unsecured emails and web traffic?

With transparent TCP tunneling, otherwise unsecured TCP-based application traffic, such as emails and web connections, can be encrypted.

“But our network is so complex...”

Tectia ConnectSecure is designed to secure server-to-server connections within heterogenous corporate networks. It can connect to Tectia Server, another Secure Shell server and mainframe computers running Tectia Server for IBM z/OS. Tectia ConnectSecure can be deployed into a cross-platform environment where most commonly Microsoft Windows and different flavors of Unix and Linux operating systems are used.

How to manage Tectia ConnectSecure in the network?

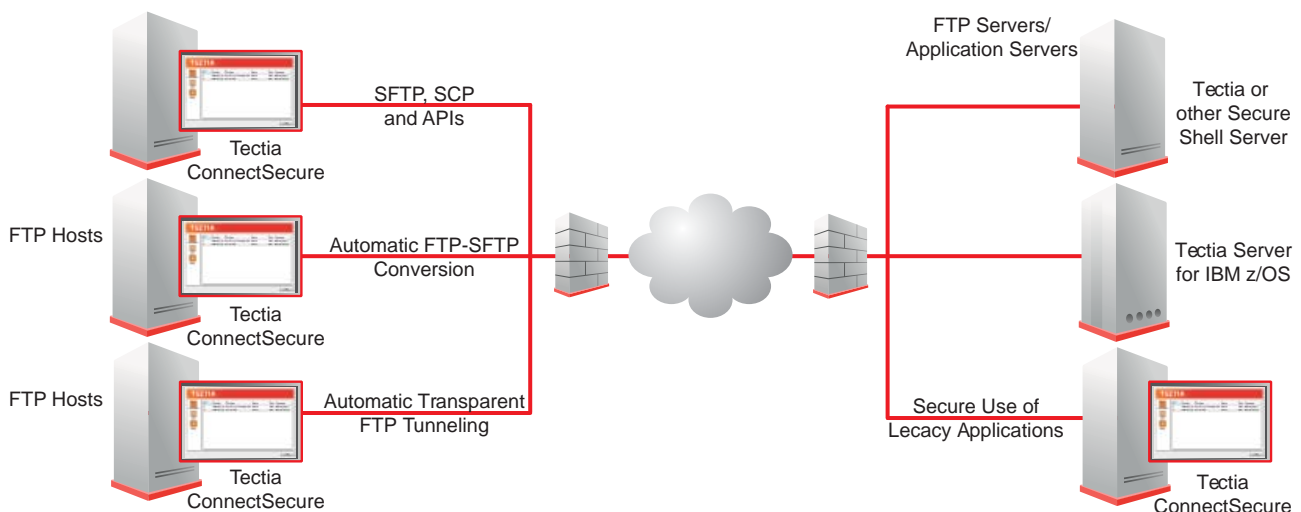
Tectia ConnectSecure hosts can be managed centrally with Tectia Manager. Tectia Manager is a separate product which can be used to upgrade and configure Tectia ConnectSecure remotely and to monitor SFTP operations on the network hosts. Security reports can be produced for compliance audits.

Security Auditors are coming, are you ready?

Tectia ConnectSecure helps your organization to comply with data security regulations and legislation, such as FISMA, HIPAA, PCI-DSS and SOX.

Is that all?

Tectia ConnectSecure also offers SFTP, SCP and SSH command-line tools for versatility. To integrate secure file transfer capability to existing applications, SFTP APIs are also available.



Features

Secure File Transfer

- Native SFTP functionality for secured end-to-end file transfers
- Transparent FTP tunneling
- Transparent, automatic FTP-SFTP conversion
- SFTP, SCP & SSH command line tools
- Checkpoint/restart, mid-file transfer recovery
- Streaming for fast performance (1)
- Data stream compression for low-speed connections
- Prefixing to prevent file usage before transfer is complete
- Multi-gigabyte file size support
- Strong data encryption
- Strong file integrity checking
- Complete SFTP APIs for C & Java (2)

With Tectia Server for IBM z/OS:

- SFTP extension for MVS dataset direct streaming
- SFTP extensions for SITE command support
- Support for MVS and USS file systems

- Automatic EBCDIC-ASCII character conversion
- Interfacing z/OS Job Entry Subsystem (JES)

Secure Data-in-Transit

- Support for connections to standard Secure Shell v2 servers
- Transparent TCP tunneling
- Automatic tunneling
- TCP/IP port forwarding
- Automatic encryption of data in transit
- Comprehensive filter rules for tunneling configurations
- IPv6 support

Security

- Logs and auditing information
- Automatic transparent encryption of data-in-transit, including user ID and password
- Firewall-friendly architecture
- Multi-tier security architecture
- Authentication agent functionality
- Multi-channel support
- Compliance with IETF Secure Shell

(secsh) standard

Ease of Use

- Automatic connection setup - connection parameters, including user name and destination host, can be captured from the FTP data stream
- Configurable FTP fallback option for controlled and phased deployment, in case SFTP fails, FTP can be used for the instance
- Possibility for centralized deployment and management with Tectia Manager
- Terminal and file transfer UI for end users and configuration UI for administrators

Flexible Authentication

- Public-key authentication (client and server)
- User authentication with passwords
- Two-factor user authentication based on smart cards, tokens and Tectia MobileID
- Keyboard-interactive interface for easy integration with 3rd party methods, such as LDAP
- Support for GSSAPI/Kerberos
- Support for OpenSSH keys

Specifications

Supported Cryptographic Algorithms

Asymmetric (Public-Key) Algorithms:

- DSA and RSA

Symmetric (Session Encryption)

Algorithms:

- AES (128 / 192 / 256 bit)
- 3DES (168 bit)

Data Integrity Algorithms:

- HMAC MD5, HMAC SHA-1, HMAC SHA224, HMAC SHA256, HMAC SHA384, HMAC SHA 512

Key Exchange Algorithms:

- Diffie-Hellman (SHA-1 and SHA-2 methods)

Certifications

- FIPS 140-2 certified cryptographic module

Supported PKI Specifications

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

Supported Third-Party Authentication Products

- Tectia MobileID
- Entrust Authority™ Security Manager
- Microsoft CA
- Windows domain authentication through GSSAPI
- RSA SecurID®
- SafeWord® through PAM
- Centrify Direct Control

Supported Platforms

Tectia products can run on any standard hardware capable of running the supported operating system versions:

- HP-UX 11iv1, 11iv2, 11iv3 (PA-RISC)
- HP-UX 11iv2, 11iv3 (IA-64)
- IBM AIX 5.3, 6.1, 7.1 (POWER)
- Microsoft Windows XP, Server 2003, Server 2003 R2, Vista, Server 2008, 7 (x86)
- Microsoft Windows Server 2003, Server 2003 R2, Vista, Server 2008, Server 2008 R2, 7 (x64)
- Red Hat Enterprise Linux 4, 5, 6 (x86)
- Red Hat Enterprise Linux 4, 5, 6 (x86-64)
- Oracle Solaris 9, 10 (SPARC)
- Oracle Solaris 10, 11 (x86-64)
- SUSE Linux Enterprise Desktop 10, 11 (x86)
- SUSE Linux Enterprise Server 9, 10, 11 (x86)
- SUSE Linux Enterprise Desktop 10, 11 (x86-64)
- SUSE Linux Enterprise Server 10, 11 (x86-64)

(1) With Tectia Server

(2) C API is for all platforms, Java API is for Linux, Solaris and Windows