ssh®
Securing the path to your information assets

Data Sheet

Tectia® SSH Server for IBM z/OS

Secure File Transfers for Mainframes

In large and medium-sized enterprises, mainframes are still relied upon as the most trusted, secure repository for Big Data. Because the mainframe technology itself is a vault for core systems and databases, encryption of the connections coming to and from it needs to be emphasized as much as data-at-rest. Unsecure FTP is still prevalent in many environments, which puts your backend data at risk. Today, compliance - internal and external, government regulations and PCI concerns mandate that data-in-transit is encrypted and protected at all ends of the enterprise and cloud. The mainframe is no longer alone. SSH Communications Security can provide solutions that prevent security breaches, brand damage and financial losses that can have detrimental effect on enterprises' reputation and trust.

Data-in-Transit Solutions from the Company that Invented the SSH Protocol

Tectia SSH Server for IBM z/OS is a turnkey, enterprise class Secure Shell (SSH) server that enables secure transfer of large amounts of mission critical business information without modification or scripts, FTP file transfer jobs, applications, or IT infrastructure.

Tectia SSH Server for IBM z/OS includes SSH Communications Security client and server tools, delivering unmatched data integrity and strong authentication with both drag-and-drop and automated secure file transfers.

Tectia SSH Server for IBM z/OS supports direct MVS data set access, interactive MVS data set listing, interfacing with JES, I/O streaming, confi gurable ASCII/EBCDIC code set conversions, checkpoint/restart, and FTP compatibility commands, such as the SITE command.

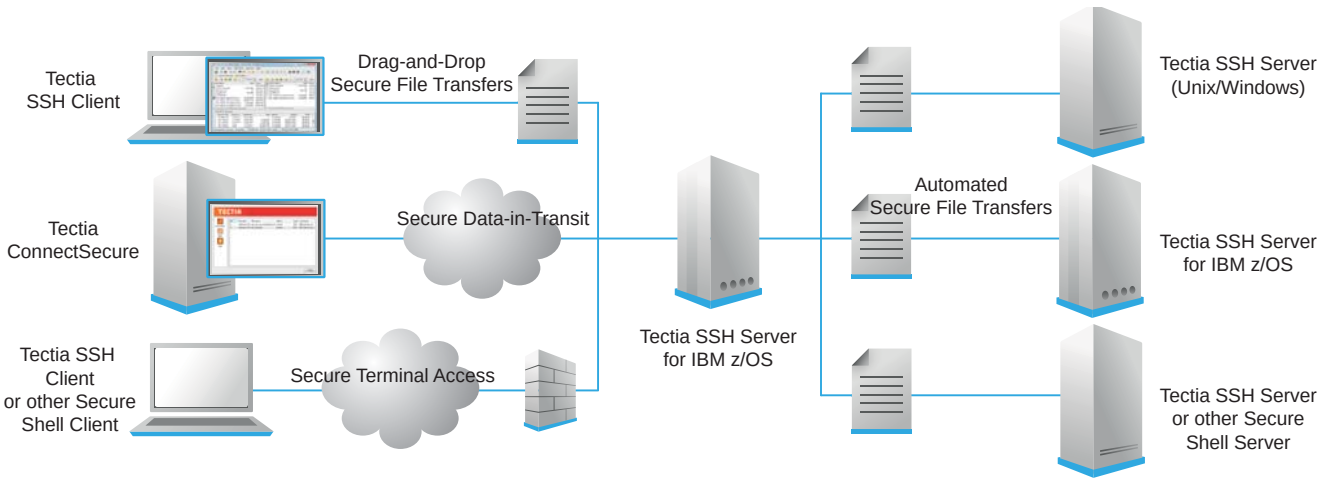
Eliminate Unsecured FTP File Transfers

Fortune 1000 companies still utilize FTP to transfer sensitive business information - including customer credit cards and personally identifi able information. Cyber-criminals know that if they can breach the perimeter they can easily capture massive amounts of high value data traveling unsecured via FTP from the mainframe.

Tectia SSH Server for IBM z/OS greatly reduces security risks inherent to unsecured FTP file transfers by providing automated FTP-SFTP conversion and transparent FTP tunneling.

Meet or Exceed Regulation Mandates

Tectia SSH Server for IBM z/OS helps organizations of all types and sizes meet internal and external compliance requirements including PCI-DSS, SOX, HIPAA, FIPS, FISMA, and many others.



Features

Ease of Use

- Configurable FTP fallback option for controlled and phased deployment
- System-wide and user-specific file transfer profiles
- Transparent application tunneling with Tectia ConnectSecure
- Listing of MVS data sets as files and folders for easy interactive command line

User and Server Authentication

- Authentication and access control through SAF calls to RACF, ACF2, and TSS
- User authentication with passwords
- User and server authentication with X.509 certificates
- User and server authentication with public keys
- Logging and auditing using SMF records and Syslogd facilities

Secure File Transfer

- Transparent, automatic FTP-SFTP conversion
- Transparent FTP tunneling
- Checkpoint/restart, mid-file transfer recovery
- Multi-gigabyte file size support
- Strong encryption of data
- Strong packet-by-packet file integrity checking
- SFTP and SCP command-line tools for interactive and unattended use
- Logging and auditing using SMF records and Syslogd facilities
- SFTP Extensions for SITE command support
- Support for MVS and USS file systems
- Automatic EBCDIC-ASCII character conversion
- Interactive MVS data set listing capability
- Interfacing z/OS Job Entry Subsystem (JES)

Security

- Automatic transparent encryption of data-in-transit, including user ID and password
- Strong confidentiality and data integrity
- Hardware acceleration of cryptographic operations
- Support for U.S. NIST FIPS 140-2 Certified hardware acceleration
- Firewall-friendly architecture
- Multi-tier security architecture
- Configurable re-keying policies
- Multi-channel support – multiple secure sessions are multiplexed to a single TCP/IP connection
- Compliance with the IETF Secure Shell standards

Secure Application Connectivity

- Automatic tunneling
- TCP/IP port forwarding
- Automatic encryption of data-intransit
- Transparent TN3270 security with Tectia Client or Tectia ConnectSecure

Supported Platforms

IBM z/OS versions 1.12, 1.13 and 2.1

Specifications

Supported Cryptographic Algorithms

Hardware-supported:
- AES (128 bit)
- 3DES (168 bit)
- SHA-1 and SHA-2 hash algorithm

Software-supported:
- AES (128 / 192 / 256 bit)
- 3DES (168 bit)
- DSA and RSA public-key algorithms
- HMAC MD5, HMAC SHA1, HMAC SHA224, HMAC SHA256, HMAC SHA384 and HMAC SHA512 data integrity algorithms
- Support for OpenPGP keys
- Diffie-Hellman (SHA-1 and SHA-2 methods) key exchange algorithms

Supported Cryptographic Algorithms

Full utilization through ICSF for:
- CCF
- PCICA
- PCICC
- PCIXCC
- CPACF
- CryptoExpress2

Supported Authentication Mechanisms

- RACF
- ACF2
- Top Secret

SSH Communications Security | sales@ssh.com | www.ssh.com