Data Sheet

Tectia® ConnectSecure

セキュアなファイル転送とアプリケーショントラフィック

Tectia ConnectSecureはファイル転送オペレーターの業務を簡易化し、ファイル転送ネットワークを高度なセキュリティレベルに到達させる費用対効果の優れた方法を提供します。

あなたのファイル転送とアプリケーションのトラフィックは安全？

ビジネス用途のアプリケーションで顧客のクレジットカード情報等の機密情報を転送する場合、それが安全に実施出来る事を確認する必要があります。マンインザミドル攻撃者は保護されていないファイル転送を容易に傍受する事が可能で、財務損失や企業イメージの損失が発生する可能性があります。Tectia ConnectSecureならば、あなたのアプリケーションのアーキテクチャに対し、Secure Shell（SSH）に基いたセキュアなファイル転送のレイヤを容易に追加出来ます。

全てのFTPホストとファイル転送スクリプトに何をすべきか？

Tectia ConnectSecureは、スクリプトやアプリケーションへの変更を加える事無く、既存のネットワークトポロジへ小規模な変更を行うだけで、セキュアではないシステムをセキュアなシステムに移行させる自動的な手法を提供しています。Tectia ConnectSecureは、セキュアでない平文のデータトラフィックを自動的にキャプチャし、SFTP変換もしくはSSHトンネリングを行い、暗号化されたデータを転送する為、FTPホストの直下のレイヤに配置出来ます。データはマンインザミドル攻撃者から保護され、セキュアに宛先ホストへ配信されます。

セキュアでないEメールおよびウェブトラフィックは？

このようなEメールやウェブ接続などの特にセキュリティで保護されていないTCPベースのアプリケーションのトラフィックは、透過的なTCPトンネリングにより、暗号化することができます。

「しかし、我々のネットワークは複雑である・・・」

Tectia ConnectSecureは、様々な機種が存在する企業ネットワーク内において、サーバー同士の接続をセキュア化するよう設計されています。それはTectia Serverや他社製Secure Shellサーバー、そしてメインフレームコンピュータ上で動作するTectia Server for IBM z/OSとの接続が可能です。

ネットワーク上でTectia ConnectSecureを制御するには？

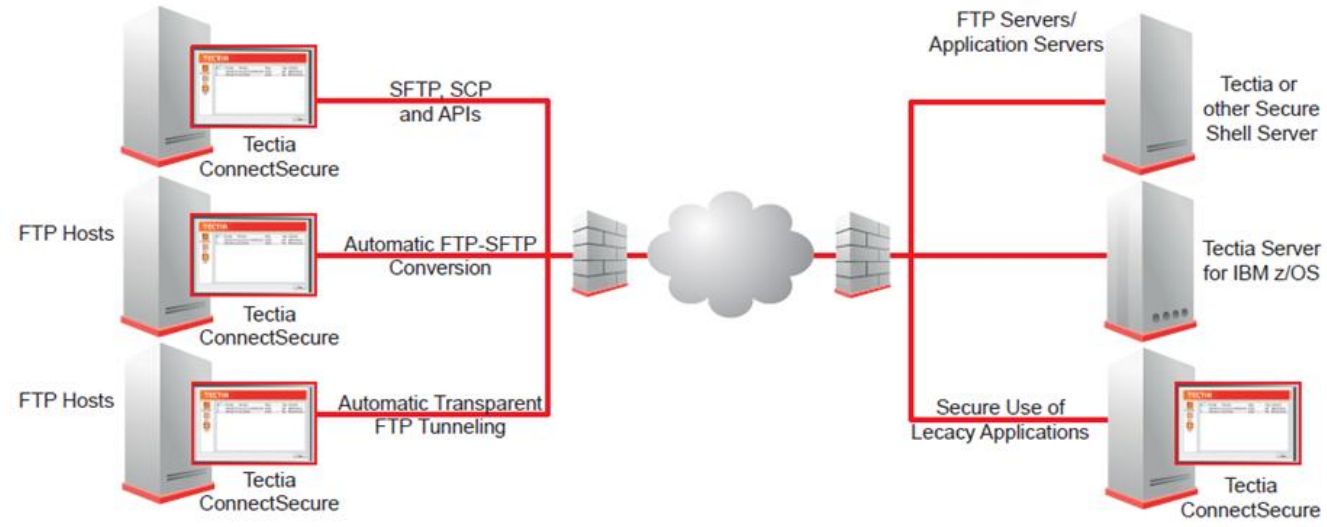
Tectia ConnectSecureのホストはTectia Managerによる集中管理が可能です。Tectia Managerは、リモートからTectia ConnectSecureのアップグレード設定、ネットワークのホスト上でのSFTP操作を監視する別製品です。また、セキュリティレポートをコンプライアンス監査向けに作成出来ます。

セキュリティ監査人の受け入れ準備は整っていますか？

Tectia ConnectSecureは、企業がFISMA、HIPAA、PCI－DSSやSOX等のようなデータセキュリティに関する規制や法律への準拠するための補助となります。

更なる機能

また、Tectia ConnectSecureはSFTP、SCP、そして汎用性のためのSSHのコマンドラインツールを提供しています。既存アプリケーションへセキュアなファイル転送機能を統合する為のSFTPのAPIも用意されています。



特徴

セキュアなファイル転送

- セキュアなエンドツーエンドのファイル転送の為のネイティブなSFTP機能
- 透過的なFTPトンネリング
- 透過的な自動FTP-SFTP変換
- SFTP/STPコマンドラインツール
- チェックポイント/リスタート：中断されたファイル転送の復旧
- ストリーミング機能による高速転送　※1
- 低速接続時のストリームデータ圧縮
- 転送完了前のデータ利用を防ぐプレフィックシング
- ギガバイトサイズのファイルをサポート
- 強力なデータ暗号化
- 強力なファイル完全性チェック
- C/JAVAに対応したSFTP API　※2
- Tectia Server for IBM z/OSとの併用
- MVSデータセット・ダイレクト・ストリーミングに対応する為のSFTP拡張
- SITEコマンドをサポートする為のSFTP拡張
- MVS及びUSSファイルシステをサポート
- 自動EBCDIC-ASCIIキャラクター変換

セキュアなデータ通信

- 標準のSecure Shell v2サーバーへの接続をサポート
- 透過的なTCPトンネリング
- 自動トンネリング
- TCP/IPポートフォワーディング
- データ通信の自動暗号化
- トンネリング設定の為の包括的なフィルタルール

セキュリティ

- ログ及び監査証跡情報
- IDとパスワードを含むデータ通信の自動的で透過的な暗号化
- ファイアウォールに適したアーキテクチャ
- 多層セキュリティアーキテクスチャ
- 認証エージェント機能
- 複数のチャネルをサポート
- IETF Secure Shell(SecSh)標準に準拠

導入の容易さ

- 自動接続セットアップ：ユーザ名と接続先ホストを含む接続パラメータをFTP通信から取得可
- 計画的、段階的な構築に便利なFTPフォールバックオプション
- Tectia® Managerによる一元的な展開と管理が可能
- エンドユーザ向けファイル転送ターミナルUI及び管理UI

柔軟な認証

- 公開鍵認証（クライアント及びサーバ）
- パスワードによるユーザ認証
- スマートカード、トークン及びTectia MobileIDによる二要素認証
- LDAP等の他社製品との統合を容易にするキーボードインタラクティブインターフェイス
- GSSAPI/Kerberosのサポート
- OpenSSH鍵のサポート

仕様

暗号化アルゴリズムのサポート

- 非対称アルゴリズム(公開鍵)
- DSA/RSA

対称アルゴリズム(セッション暗号)

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

データー貫性アルゴリズム

- 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)

認証

- FIPS140-2 certified cryptographic module

PKI機能のサポート

- X.509 v3 証明書をサポート
- HTTP, LDAP, offlineでのX.509 v2 CRL フェッチ
- OCSP
- SCEP
- PKCS#7 / PKCS#12 インポート
- PKCS#8 / PKCS#11 鍵サポート
- WindowsでのMSCAPIサポート

他社認証製品のサポート

- Tectia MoileID
- Entrust Authority™ Security Manager
- Microsoft CA
- Windows ドメイン認証(GSSAPI経由)
- RSA SecurID ®
- SafeWord ®(PAM使用)
- Centrify Direct Control

対応プラットフォーム

Tectia製品はサポートOSに対応する標準のHWプラットフォームで動作可能です。

- 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 ,Vista, Server 2008, 7 (x86)
- Microsoft Windows Server 2003,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 (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　Tectia® Serverとの併用時
※2　C用APIは全てのプラットフォームに対応
JAVA用APIはLinux、Solaris、Windowsのみ対応

販売代理店：株式会社ディアイティ
TEL:03-5634-7653　Mail:info@dit.co.jp　URL:http://www.dit.co.jp