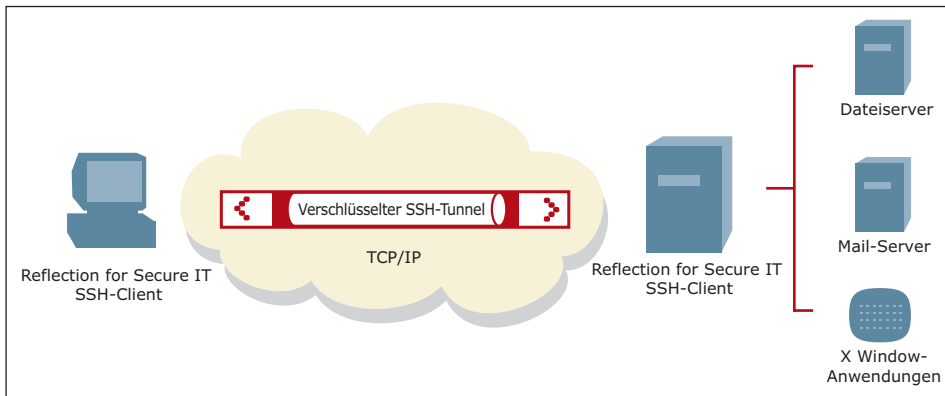


Reflection® for Secure IT Windows Server verwendet das SSH-Protokoll, um sichere Datenübertragungs- und Remoteverwaltungsfunktionen für Windows-Umgebungen zu gewährleisten. Es ist Bestandteil der Reflection for Secure IT-Produktfamilie von SSH-Clients und SSH-Servern für Windows und UNIX, die alle für den Schutz von Daten in einer mobilen Umgebung konzipiert sind.



SSH-Client und SSH-Server bilden zusammen einen sicheren „Tunnel“, durch den die Kommunikation geleitet wird.

Besonderheiten in Version 7.2

- Unterstützung für Microsoft Windows Server 2008 R2 (x86-64)
- Microsoft Cluster Service-Unterstützung
- Verwendung verbundener Laufwerke für den Zugriff auf Netzwerkverzeichnisse bei Terminalsitzungen
- Kontrolle über die pro Benutzer zulässige Anzahl Verbindungen
- Verwendung alternativer Zugangsdaten für den Zugriff auf SFTP-Verzeichnisse (für Datenübertragungen) und verbundene Treiber (für Terminalsitzungen)
- Benutzerdefinierte Speicherorte für Serverkonfigurationsdateien
- Schnellere Active Directory-Domänenauthentifizierung

TECHNISCHE SPEZIFIKATIONEN

Secure Shell-Zugriff

- Sichere Remote-Terminal-Verbindungen:
 - Konfigurierbarer Terminal Provider (z. B. cmd.exe)
 - Konfigurierbares Terminal-Standardverzeichnis

NEU Verwendung verbundener Laufwerke für den Zugriff auf Netzwerkverzeichnisse bei Terminalsitzungen

- Sichere Remote-Befehlsausführung

Sichere Dateiübertragung

- SCP- und SFTP-Protokollunterstützung
- Besondere Funktionen für SCP und SFTP:
 - Smart Copy zum Vermeiden überflüssiger Kopien identischer Quell- und Zieldateien
 - Wiederaufnahme von Dateiübertragungen nach unterbrochenen Downloads
- SCP1-Protokollunterstützung (sorgt für Kompatibilität mit OpenSSH-Clients)
- Unterstützung für virtuelle Verzeichnisse und chroot-Umgebungen

Zugangssteuerung

- Rechtezuweisung (Zulassen oder Verweigern) möglich für:
 - Terminal Shell-Zugriff
 - Ausführungsanforderungen
 - Lokale Anschlussweiterleitung
 - Remote-Anschlussweiterleitung

- SCP1-Zugriff
- SFTP/SCP2-Zugriff
- SFTP-Aktivitäten (Durchsuchen, Herunterladen, Hochladen, Löschen und Umbenennen)

- Zuweisung zu Unterkonfigurationen:

- Global
- Gruppen
- Benutzer
- Per-Client-System (nach IP-Adresse oder Domänenname)

- Verbindungsverweigerung für Benutzer ohne interaktive Windows-Zugriffsrechte möglich

- NEU** • Kontrolle über die pro Benutzer zulässige Anzahl von Verbindungen

- NEU** • Verwendung alternativer Zugangsdaten für den Zugriff auf SFTP-Verzeichnisse (für Datenübertragungen) und verbundene Treiber (für Terminalsitzungen)

Tunneling

- TCP-Anschlussweiterleitung (lokal und remote)
- FTP-Protokoll (aktiver und passiver Modus)
- RDP-Protokoll

Unterstützung folgender Standards:

- Konformität mit IETF SecSh Internet-Drafts und RFCs 4250–4254, 4256, 4462, 4344, 4345 und 4716

Überprüfung der kryptografischen Bibliothek

- FIPS 140-2 Level 1 (Zertifikat Nr. 1027)

Algorithmen

- Verschlüsselung:
 - AES (128, 192 und 256 Bit CTR)
 - AES (128, 192 und 256 Bit CBC)
 - 3DES (3 56-Bit-Schlüssel EDE)
 - Blowfish (128 Bit)
 - CAST (128 Bit)
 - Arcfour (128 und 256 Bit)
- MACs:
 - HMAC-MD5 (optional MD5-Verweigerung möglich)
 - HMAC-MD5-96
 - HMAC-SHA1
 - HMAC-SHA1-96
 - HMAC-SHA256
 - HMAC-SHA512
 - RIPEMD160
- Schlüsselaustausch:
 - Diffie-Hellman
 - GSS-API-Schlüsselaustausch

Authentifizierung

- Serverauthentifizierung:
 - Öffentlicher Schlüssel (RSA und DSA)
 - PKI X.509-Zertifikate
 - GSSAPI/Kerberos

TECHNISCHE SPEZIFIKATIONEN (Fortsetzung)

- Benutzerauthentifizierung:
 - Kennwort (lokaler Benutzer und Windows-Domänenbenutzer)
 - Öffentlicher Schlüssel:
 - RSA-Benutzerschlüssel
 - DSA-Benutzerschlüssel
 - Kompatibilität öffentlicher Schlüssel mit OpenSSH
 - Interaktiv über Tastatur:
 - RSA SecurID
 - RADIUS
 - Interaktives Kennwort über Tastatur
 - PKI X.509-Zertifikate
 - GSSAPI/Kerberos
- Reflection PKI Services Manager:
 - Zentralisierte Konfiguration und Verwaltung von PKI-Funktionen über mehrere Reflection for Secure IT Windows-Server, UNIX-Server und UNIX-Clients hinweg
 - Eigenständiges Servicemodul, das auf den meisten Plattformen und von Reflection for Secure IT Windows- und UNIX-Servern unterstützt wird
 - NEU - DoD PKI-zertifiziert
 - FIPS 140-2 Level 1-geprüft für die meisten unterstützten Plattformen (Zertifikat Nr. 1048)
- RFCs 2253, 2560 und 3280
- X.509-Zertifikate für Server- und Client-authentifizierung (X.509-Versionen 1-3)
- Version 2 X.509 CRL
- OCSP-Widerrufsprüfungen
- NEU - HSPD-12-Unterstützung
- Unterstützung für LDAP- und HTTP-Zertifikate und CRL-Repositorys
- Unterstützung für Microsoft Windows
- Unterstützte Zertifikaterweiterungen:
 - CDP
 - IDP
 - AIA
 - Richtlinienbeschränkungen
 - Basisbeschränkungen
 - Namensbeschränkungen
 - Erweiterte Schlüsselverwendung
- Benutzerdefinierte Konfiguration unter Verwendung von Trust-Anchors
- Vollständig benutzerdefinierte Zuordnung von SSH-Benutzerkontennamen zu Zertifikaten
- NEU - SOCKS-Proxyunterstützung
- NEU - PKI-Client-Befehlszeilendienstprogramm für die Abfrage von Serviceverfügbarkeit und Zertifikatsgültigkeit

Auditing

- Konfigurierbares Windows-Ereignisprotokolllevel
- Konfigurierbares Debug-Protokoll mit lokalen und UTC-Zeitstempeln
- Benachrichtigung bei Überschreitung der Anzahl zulässiger Kennworteingabeversuche

Verwaltungsprogramme

- NEU • Benutzerdefinierte Speicherorte für Serverkonfigurationsdateien
- Section 508-Unterstützung im Serverkonfigurationsdienstprogramm Reflection for Secure IT Windows

Betriebssysteme

- NEU • Microsoft Windows Server 2008 R2 (x86-64)
- Microsoft Windows Server 2008 (x86 und x86-64)
- Microsoft Windows Server 2003 (x86 und x86-64)
- NEU • Microsoft Cluster Service-Unterstützung

Systemanforderungen

- Alle Systeme, die die Mindestanforderungen für das Microsoft Windows-Betriebssystem erfüllen
- Der Festplattenspeicherplatz variiert je nach installierten Funktionen
- Netzwerkschnittstellenkarte

Über Attachmate

Attachmate ist ein führender Hersteller von fortschrittlichen Softwarelösungen für Terminalemulation, Modernisierung von Legacysystemen, Managed File Transfer (MFT) und Enterprise Fraud Management (EFM). Derzeit nutzen mehr als 65.000 Kunden unsere Technologien, um ihre IT-Ressourcen auf neuartige Weise sinnvoll einzusetzen. www.attachmate.de.



Hauptsitz
 1500 Dexter Avenue North
 Seattle, Washington 98109
 TEL +1 206 217 7500
 FAX +1 206 217 7515

Europäische Zentrale
 Niederlande
 TEL +31 172 50 55 55
 FAX +31 172 50 55 51

Österreich
 TEL +43 1 595 4335 0
 FAX +43 1 595 4335 11
www.attachmate.at
info-at@attachmate.com

Schweiz
 TEL +41 43 399 2090
 FAX +41 43 399 2099
www.attachmate.ch
InfoCH@attachmate.com

Deutschland
 TEL +49 89 99 351 0
 FAX +49 89 99 351 111
 TEL +49 2102 4965 0
 FAX +49 2102 4965 65
www.attachmate.de
info-de@attachmate.com

Weitere Niederlassungen von Attachmate finden Sie unter www.attachmate.de.