

Reflection® for Secure IT Windows Client est un client SSH sécurisant les fonctions de transfert de fichiers et d'accès terminal, à la fois au format graphique et par ligne de commande. Ce produit fait partie de la gamme Reflection® for Secure IT, serveurs et clients SSH pour Windows et UNIX, spécifiquement conçus pour protéger les données en circulation.

SPÉCIFICATIONS TECHNIQUES

SPÉCIFICATIONS TECHNIQUES

Connectivité

- Protocole SSH2 : SSH2 (IETF SecSh Internet drafts et RFC 4250-4254, 4256, 4462, 4344, 4345 et 4716)
- Protocole SSH1 pour assurer la compatibilité avec d'anciens serveurs de protocoles
- SCP1 (compatibilité serveurs OpenSSH)

Validation cryptographique de librairie

- FIPS 140-2 Level 1 (certificat n° 1027)

Interfaces conviviales

- Interface utilisateur graphique familière
- Scripts batch/ligne de commande (via commandes ssh, sftp et scp)
- NEW** • Configuration adéquate des connexions à sauts multiples

Sécurisation des transferts de fichiers

- SCP :
 - Remplace la commande rcp non sécurisée
 - Prise en charge de SCP1
- SFTP :
 - Remplace le protocole FTP non sécurisé
 - Conforme à draft-ietf-secsh-filexfer
- Utilitaire graphique sécurisé du client FTP :
 - Prise en charge d'un éventail de serveurs FTP par le protocole SFTP, FTP sur SSH, FTP standard (non chiffré), FTP sur SSL/TLS et FTP « Kerberisé » (TLS).
- Serveurs pris en charge :
 - Windows, IBM System z, IBM System i, UNIX, NetWare, Unisys, HP 3000 et OpenVMS
 - Navigation fichier sur mainframes IBM, sans intrusion ni modification sur site
 - Transfert d'un site à l'autre entre serveurs
 - Outils d'automatisation (enregistreur de scripts et automatisation Microsoft OLE)
- NEW** • Conservation de l'horodatage et des attributs lors des transferts SFTP

Tunnels

- Transfert de port TCP (Local/Distant)
- Protocole FTP (à deux canaux)
- Transfert X11
- Port de passerelle

- Protocole RDP (sécurise l'accès au bureau distant Microsoft)

Algorithmes de chiffrement

- Chiffrements :
 - AES (128, 192 et 256 bits CTR)
 - AES (128, 192 et 25 bits CBC)
 - 3DES (clé 3 56 bits CBC)
 - Blowfish (128 bits CBC)
 - CAST (128 bits)
 - Arcfour (128 et 256 bits)
- MAC :
 - HMAC-SHA1 et HMAC-SHA1-96
 - HMAC-SHA256 et HMAC-SHA512
 - HMAC-MD5 et HMAC-MD5-96
 - RIPEMD160
- Échange de clés :
 - RSA
 - Diffie-Hellman

Authentification

- Authentification du serveur :
 - Clé publique (RSA et DSA)
 - Certificats PKI X.509
 - GSSAPI
- Mot de passe d'authentification de l'utilisateur :
 - Local
 - Authentification Domaine Windows (Active Directory)
- Clé publique d'authentification de l'utilisateur :
 - RSA
 - DSA
 - Retransmission d'agent
- NEW** • Prise en charge des cartes à puce pour la retransmission d'agent
- Interaction clavier :
 - RSA SecurID
 - RADIUS
 - Mot de passe interactif clavier
- Certificats PKI X.509 :
 - Gestionnaire de certificats de Reflection
 - Windows Certificate Manager (MSCAPI)
 - Prise en charge du protocole OSCP (Online Certificate Status Protocol)
 - CRL (Certificate Revocation Lists)
 - Recherche LDAP/Active Directory des CRL et certificats CA intermédiaires

FONCTIONNALITÉS DE LA VERSION 7.2

- Prise en charge de Microsoft® Windows 7.
- Prise en charge améliorée des transferts gérés par Attachmate FileXpress.
- Prise en charge améliorée des cartes à puce.
- Accès via des menus au guide d'aide en ligne du produit (disponible en anglais, français, allemand et japonais).
- Prise en charge des protocoles SFTP, FTP sur SSH, FTP standard (non chiffré), FTP sur SSL/TLS et FTP « Kerberisé » (TLS).
- Prise en charge améliorée des certificats, notamment des certificats PKCS #11, CAC (Common Access Card) du Département de la défense des États-Unis, OSCP (Online Certificate Status Protocol), CRL (Certificate Revocation List) et du stockage des certificats intermédiaires via LDAP. Résultat : une authentification stricte.

- Clé PKCS #12 et stockage de certificat
- Prise en charge des cartes à puce PKCS #11

- NEW** • Emplacement de stockage des certificats autorisés partagés
- GSSAPI/Kerberos :
 - Client Kerebos Reflection
 - Attributs de référence d'ouverture de session Microsoft SSPI
 - Support des authentifications site et utilisateur avec GSSAPI

Types d'émulation

- VT500 et VT420
- VT320, VT220 et VT100
- VT-UTF8
- Console Linux
- BBS-ANSI et SCO-ANSI
- QNX
- xterm

Prise en charge internationale

- Français
- Allemand
- Anglais
- Japonais

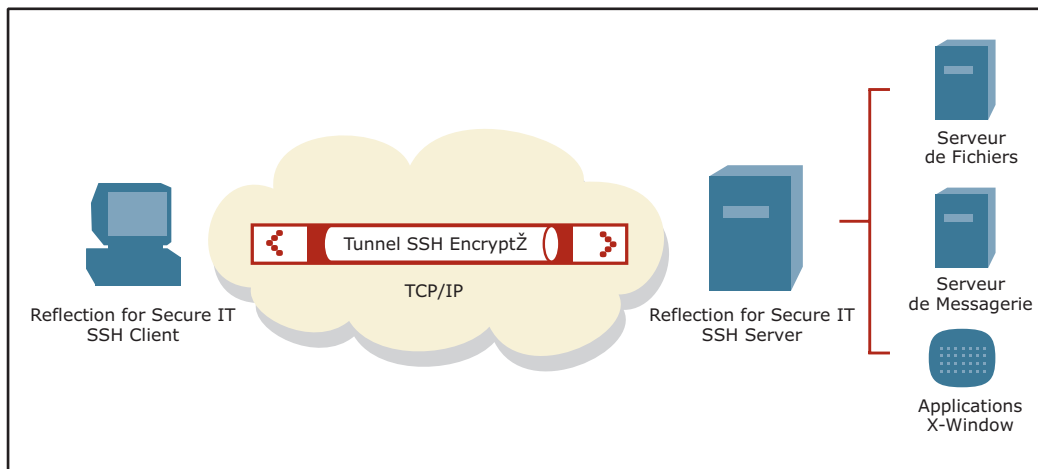
Systèmes d'exploitation

- NEW** • Microsoft Windows 7
- Microsoft Windows Vista (Service Pack 2)
- Microsoft Windows XP (Service Pack 3)
- Microsoft Windows Server 2003
- Microsoft Windows Server 2008 (y compris R2)
- Windows Terminal Server
- Citrix XenApp

SPÉCIFICATIONS TECHNIQUES

Configuration système requise

- Tout système compatible avec la configuration minimale requise par le système d'exploitation Microsoft Windows
- L'espace disque varie selon les fonctions installées
- Carte d'interface réseau



Le couplage du client et du serveur SSH constitue un tunnel sécurisé à travers lequel circulent toutes les communications.

À propos d'Attachmate

Attachmate commercialise des logiciels avancés d'émulation de terminal, de modernisation des sites centraux et de transferts de fichiers administrés. Sa « Business Unit » NetIQ développe des solutions d'automatisation des processus et de gestion de la performance, de la sécurité et de la conformité en environnements distribués. Grâce aux technologies Attachmate, plus de 65 000 entreprises dans le monde maximisent la création de valeur de leurs systèmes d'information en mettant leurs ressources au service de l'innovation et de la performance. www.attachmate.fr



Siège Social
 1500 Dexter Avenue North
 Seattle, Washington 98109
 États-Unis
 TEL +1 206 217 7500
 FAX +1 206 217 7515

Siège Social EMEA
 Pays-Bas
 TEL +31 172 50 55 55
 FAX +31 172 50 55 51

Siège France
 France
 TEL +33 1 46 04 10 10
 FAX +33 1 49 09 05 59

WEB www.attachmate.fr
 EMAIL marketfr@attachmate.com

Pour les informations relatives aux bureaux locaux, visitez le site www.attachmate.fr