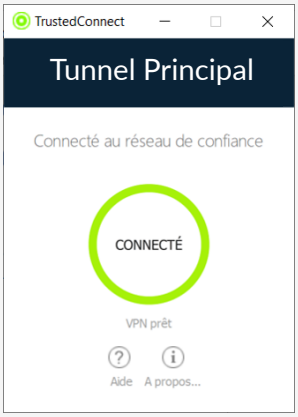
CLIENT VPN WINDOWS ENTERPRISE 7

Le Client VPN de confiance pour toutes les organisations

Facile à déployer et à intégrer dans une infrastructure existante, le Client VPN Windows Enterprise est adapté aux systèmes d'information complexes ou étendus. Disposant d'un visa de sécurité de l'ANSSI dans sa version certifiée, il répond aux exigences de sécurisation des communications des grandes organisations, OIV, OSE et administrations.

Haut niveau de sécurité

Le Client VPN Windows Enterprise a été développé en suivant les recommandations du NIST et de l'ANSSI. Il prend en compte les fonctions d'authentification disponibles sur le système d'information, et inclus à ce titre des mécanismes d'intégration avec les PKI existantes. L'ensemble des protocoles et algorithmes mis en œuvre dans le logiciel en font un client universel pour se connecter à toutes les passerelles VPN du marché, qu'elles soient logicielles ou matérielles, y compris celles qui prennent en charge le référentiel IPsec DR.



Facilité d'installation

En s'appuyant sur les capacités offertes par l'installeur Windows (MSI), les administrateurs peuvent déployer et administrer le Client VPN Windows Enterprise avec des outils de gestion de parc et des groupes d'utilisateurs (GPO). Outre l'installation silencieuse, les scripts, les multiples options de personnalisation et de pré-configuration comme la personnalisation de l'interface utilisateur, le paramétrage des fonctions PKI sont gérables de manière totalement centralisée.

Simplicité d'utilisation

Pour garantir la protection des connexions des utilisateurs, il faut faciliter l'adoption du VPN. C'est pourquoi le Client VPN Windows Enterprise simplifie son usage au maximum en proposant trois modes différents. Le plus simple, le mode « Always-On » propose une interface épurée (TrustedConnect) qui détecte si l'utilisateur est connecté au réseau de confiance. Si ce n'est pas le cas, il monte automatiquement un tunnel sécurisé. Il bascule également de manière transparente du Wi-Fi, à la 4G/5G ou au réseau filaire. Le mode classique permet d'activer le ou les tunnels disponibles. Les utilisateurs accèdent alors aux différentes ressources du réseau distant en fonction de leurs besoins. Enfin l'administrateur bénéficie d'une interface complète lui donnant accès à l'ensemble des paramétrages, notamment pour définir les règles de sécurité à déployer sur les postes.

CARACTÉRISTIQUES TECHNIQUES

Protocoles	• IPsec : IKEv2 • OpenVPN • Réseau : IPv4, IPv6, NAT-Traversal, fragmentation IKE
Authentification	• Détection automatique des certificats sur tous supports • Authentification forte : EAP, X-Auth, PSK, cartes à puce, tokens, PKCS#12… • Gestion des certificats X.509 : DER/PEM ; PFX/P12
Cryptographie	• DH 14-21 & 28, AES-CBC, AES-GCM, AES-CTR (128/192/256), SHA-2 (224/256/384/512) • Prise en charge des RFC 4304 Extended Sequence Number (ESN) et RFC 6023 (Childless IKE Initiation) • Support de l'API Microsoft CNG (Cryptography API: Next Generation) • Méthodes d'authentification : 1, 9, 10, 11, 14, 214 (RFC 4754, 7296, 7427)
Configuration requise	• Windows 10, Windows 11, 64 bits • Processeur x86-64 de 1 GHz • RAM : 2 Go • 40 Mo d'espace disque disponible

Principales fonctionnalités

- Compatible avec les passerelles qui prennent en charge le référentiel IPsec DR
- Mode filtrant, détection de portail captif (CPD) et mode Always-On
- Détection des réseaux de confiance (TND) par balises HTML ou par Active Directory (AD)
- Automatismes d'ouverture de tunnel : sur détection de trafic, insertion du token ou de la carte à puce
- Mode Credential Providers (démarrage avant ouverture de session Windows)
- Interface de configuration dédiée à l'administrateur
- Logs système et administrateur
- Continuité de service : DPD (Dead Peer Detection), passerelle redondante, tunnel de repli
- Fonctions de déploiement avancées : installation et mises à jour silencieuses, personnalisation, scripts
- Gestion avancée des tunnels : tout dans le tunnel, tunnel dans le tunnel, plusieurs tunnels simultanés, blocage du split tunneling