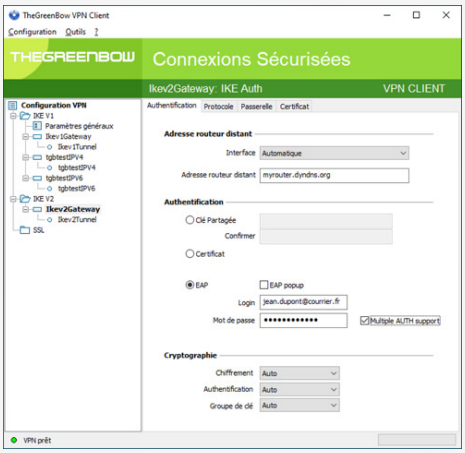
CLIENT VPN WINDOWS STANDARD

Le Client VPN de confiance pour vos connexions à distance

Facile à installer et à utiliser dans une infrastructure existante, le Client VPN Windows Standard est adapté aux systèmes d'information des PME/PMI et TPE. Il répond aux exigences de sécurisation des communications pour le nomadisme digital et le télétravail.

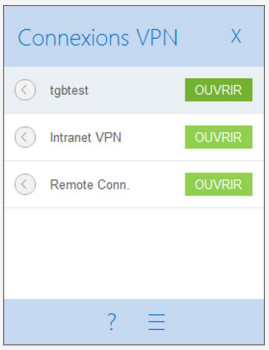
Haut niveau de sécurité

Le Client VPN Windows Standard 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 est compatible avec la majorité des PKI existantes. L'ensemble des protocoles et algorithmes mis en oeuvre dans le logiciel en font un client universel pour se connecter à toutes les passerelles VPN IPsec et OpenVPN du marché, qu'elles soient logicielles ou matérielles.



Facilité d'installation

L'installation sur n'importe quel poste Windows 10 s'effectue de façon guidée en quelques clics de souris.
Le logiciel offre une variété de protocoles, de paramètres et d'options permettant une interopérabilité avec vos équipements.
Pour simplifier l'intégration avec votre passerelle / pare-feu, la configuration de vos connexions VPN est assistée par un Wizard.



Simplicité d'utilisation

Le Client VPN Windows Standard simplifie l'usage du VPN en proposant une interface utilisateur ergonomique pour établir des connexions sécurisées vers votre système d'information.
Les utilisateurs ont une vision directe de l'état des connexions VPN pour vérifier que leurs communications sont bien protégées. Une interface d'administration complète donne accès à l'ensemble des paramétrages pour définir les règles de sécurité à appliquer sur le poste.

CARACTÉRISTIQUES TECHNIQUES

Protocoles	• IPsec : IKEv1, IKEv2 • OpenVPN • Réseau : IPv4, IPv6, NAT-Traversal, fragmentation IKE
Authentification	• Authentification forte : EAP, X-Auth, PSK, tokens et cartes à puce • Gestion des certificats X.509 : DER/PEM ; PFX/P12
Cryptographie	• DH 14-21, AES-CBC, AES-GCM, AES-CTR (128/196/256), SHA-2 (256/384/512) • Extended Sequence Number [RFC 4304] et Childless IKE Initiation [RFC 6023] • Prise en charge des API Microsoft CNG (Cryptography API: Next Generation) et PKCS#11 pour les tokens et cartes à puce • Méthodes d'authentification des certificats: Méthode 1 : RSA Digital Signature with SHA-2 [RFC7296] Méthode 9 : ECDSA «secp256r1» with SHA-256 on the P-256 curve [RFC4754] Méthode 10 : ECDSA «secp384r1» with SHA-384 on the P-384 curve [RCF4754] Méthode 11 : ECDSA «secp521r1» with SHA-521 on the P-521 curve [RCF4754] Méthode 14 : Digital Signature Authentication PKCS1-v1.5 [RCF7427]
Configuration requise	• Windows 10 64 bits • Processeur Intel 1GHz • RAM : 2 Go • 40 Mo d'espace disque disponible

Principales fonctionnalités

- Assistant d'installation et de configuration
- Prise en charge des tokens et cartes à puce
- Gestion des tunnels : full tunneling, split tunneling, plusieurs tunnels simultanés
- Connexion automatique : sur détection de trafic, insertion de clé USB, insertion de token ou de carte à puce
- Association de scripts à l'ouverture / fermeture d'une connexion
- Continuité de service : DPD (Dead Peer Detection), passerelle redondante, tunnel de repli
- Mode Credential Providers (démarrage avant ouverture de session Windows)

THEGREENBOW