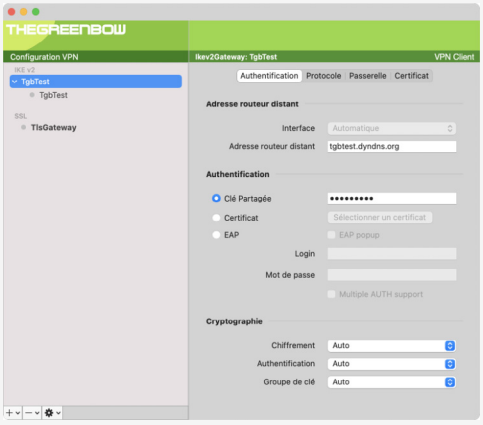
CLIENT VPN MACOS

Le client VPN de confiance pour vos connexions depuis un Mac.

Facile à installer et à utiliser dans une infrastructure existante, le Client VPN macOS est adapté aux systèmes d'information des petites et des grandes entreprises. Il répond aux exigences de sécurisation des communications pour le nomadisme digital et le télétravail.

Haut niveau de sécurité

Le Client VPN macOS a été développé en suivant les recommandations du NIST et de l'ANSSI. 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 macOS 10.15 (Catalina) ou supérieur 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 votre passerelle / pare-feu et votre PKI.

Simplicité d'utilisation

Le Client VPN macOS 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, ou à déployer sur d'autres postes.

CARACTÉRISTIQUES TECHNIQUES

Protocoles	• IPsec IKEv2 • OpenVPN • Réseau : IPv4, IPv6, NAT-Traversal, fragmentation IKE
Authentification	• Authentification : EAP, PSK, certificats • 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) • Méthodes d'authentification des certificats : Méthode 1 : RSA Digital Signature
Configuration requise	• macOS 10.15 ou supérieur • 20 Mo d'espace disque disponible

Principales fonctionnalités

- Panneau de configuration
- Gestion des tunnels : full tunneling, split tunneling
- Continuité de service : DPD (Dead Peer Detection), passerelle redondante
- Obtention des paramètres réseau depuis la passerelle (mode CP)
- Configuration et établissement de connexion SSL (OpenVPN)