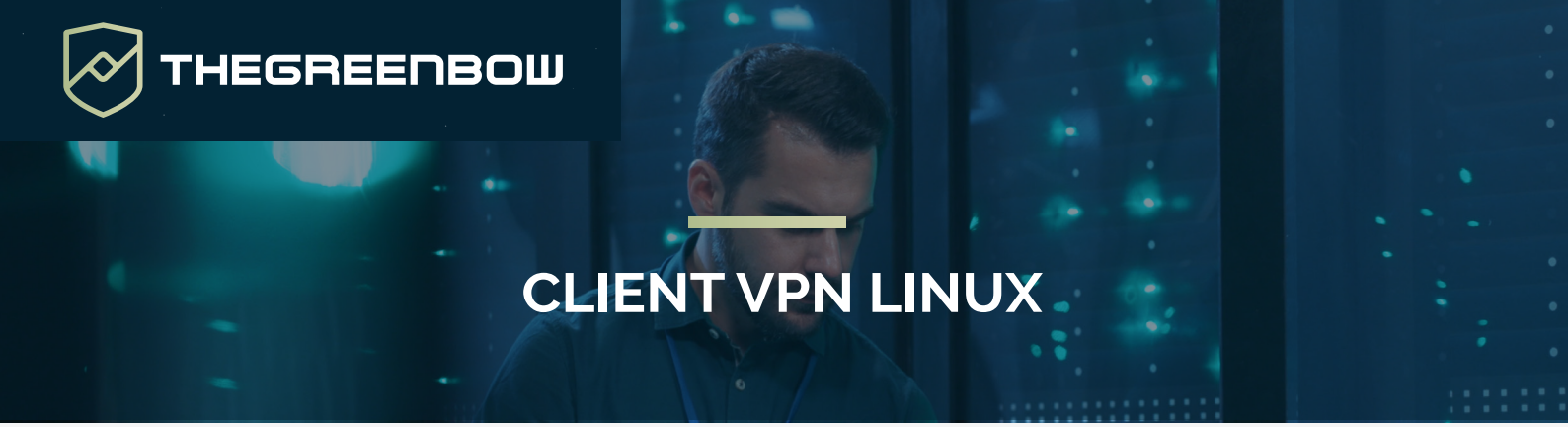


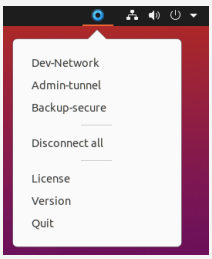
CLIENT VPN LINUX

Le client VPN de confiance pour toutes les organisations

Le Client VPN Linux intègre un driver réseau/IPsec ainsi qu'un module IKE entièrement développés par TheGreenBow, et offre une interface utilisateur simple et efficace. Facile à déployer et à intégrer dans une infrastructure existante, le Client VPN Linux est adapté aux administrateurs en situation de télétravail. Il répond également aux exigences de sécurisation des communications distantes des grandes organisations, OIV, OSE et administrations.

Haut niveau de sécurité

Le Client VPN Linux a été développé en suivant les recommandations du NIST et de l'ANSSI. Il prend en compte les fonctions d'authentification disponibles sur le sytème d'information, et est compatible avec la majorité des PKI existantes.
Pour renforcer l'authentification, il prend en charge les certificats sur les tokens et cartes à puce.



Facilité d'installation

L'installation sur n'importe quel poste Ubuntu, Red Hat ou CentOS est facile à mettre en œuvre en ligne de commande. Le Client VPN Linux est compatible avec les configurations générées pour le Client VPN Windows, et prend en charge de nombreuses options, choix d'algorithmes et fonctions PKI. Interopérable et universel, il se connecte à tous les pare-feux et à toutes les passerelles VPN IKEv2 du marché, qu'elles soient logicielles ou matérielles.

ubuntu Red Hat CentOS

Simplicité d'utilisation

Le Client VPN Linux simplifie l'usage du VPN en proposant une interface utilisateur ergonomique pour établir des connexions sécurisées vers votre système d'information.
Grâce à l'intégration dans la zone de notification de Linux, les utilisateurs ont une vision directe de l'état de la connexion VPN pour vérifier que leurs communications sont bien protégées.

CARACTÉRISTIQUES TECHNIQUES

Protocoles	• IPsec : IKEv2 • Réseau : IPv4, NAT-Traversal, fragmentation IKE
Authentification	• Authentification forte : EAP, PSK, certificats, tokens et cartes à puce • Gestion des certificats X.509 : DER/PEM ; PFX/P12 • Prise en charge de l'API PKCS#11 pour les tokens et cartes à puce
Cryptographie	• DH 14-21, DH 28, AES-GCM, AES-CTR (128/196/256), SHA-2 (256/384/512) • Extended Sequence Number (RFC 4304) • Méthodes d'authentification : 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	• RAM : 2 Go • Linux Ubuntu 18.04, 20.04 (avec GCC v9), Red Hat EL 8, CentOS 8 (avec Xfce ou KDE) • Processeur Intel 1GHz • 40 Mo d'espace disque disponible

Principales fonctionnalités

- Prise en charge des tokens et cartes à puce
- Interface de contrôle dans la zone de notification
- Activation des licences en mode connecté ou avec TheGreenBow Activation Server (TAS)
- Gestion avancée des tunnels : full tunneling, split tunneling
- Continuité de service : DPD (Dead Peer Detection), passerelle redondante
- Logs système et administrateur

TheGreenBow – 14 rue Auber, 75009 Paris, France – sales@thegreenbow.com – +33 1 43 12 39 37
https://www.thegreenbow.com