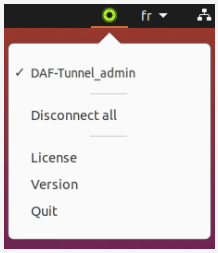
CLIENT VPN LINUX

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.

Simplicité d'utilisation

Le Client VPN Linux propose à la fois une interface en ligne de commande et une interface graphique simple 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 : signature numérique RSA avec SHA-2 [RFC7296] Méthode 9 : ECDSA « secp256r1 » avec SHA-256 sur courbe P-256 [RFC4754] Méthode 10 : ECDSA « secp384r1 » avec SHA-384 sur courbe P-384 [RCF4754] Méthode 11 : ECDSA « secp521r1 » avec SHA-512 sur courbe P-521 [RCF4754] Méthode 14 : signature numérique PKCS1-v1.5 avec SHA-2 [RCF7427]
Configuration requise	• RAM : 2 Go • Linux Ubuntu 18.04, 20.04 (avec GCC v9), Red Hat EL 8 & 9, CentOS 8 (avec Xfce ou KDE) • Processeur Intel 1 GHz • 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