THEGREENBOW

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. 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, y compris celles qui prennent en charge le référentiel IPsec DR.

Facilité d'installation

L'installation sur n'importe quel poste Red Hat (par extension AlmaLinux) ou Ubuntu (par extension Debian) 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.

Red Hat ubuntu

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 des certificats : Méthode 1 : RSA Digital Signature avec SHA-2 [RFC 7296] Méthodes 9-11 : ECDSA « secp » avec SHA-2 [RFC 4754] Méthode 14 : RSASSA-PKCS1-v1_5, RSASSA-PSS [RFC 7427] Méthode 214 : ECDSA « BrainpoolP256r1 » avec SHA-2
Configuration requise	• RAM : 2 Go • Red Hat EL 9, Linux Ubuntu 22.04 (avec noyau 5.15) • Processeur Intel 1 GHz • 40 Mo d'espace disque disponible

Principales fonctionnalités

- Compatible avec les passerelles qui prennent en charge le référentiel IPsec DR
- 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