

THEGREENBOW



TheGreenBow VPN Client

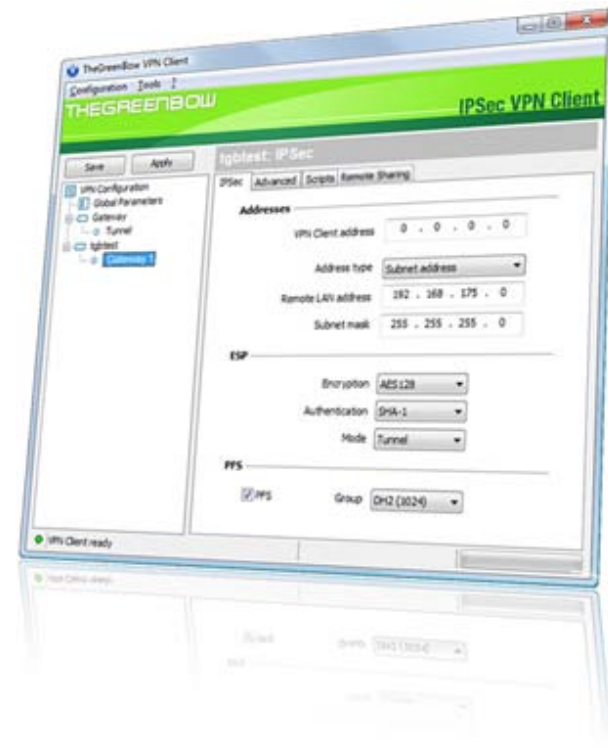
Secure, Strong, Simple

Client VPN IPSec



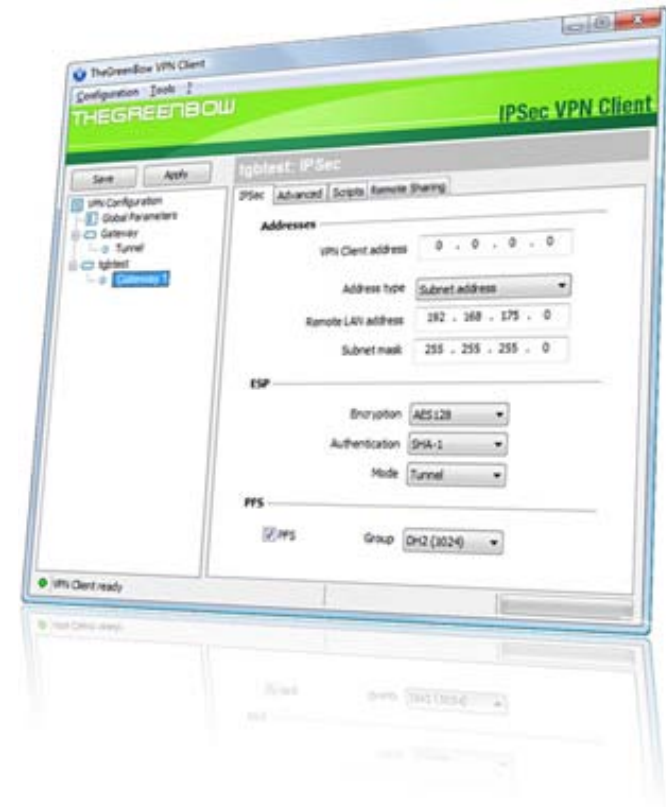
Authentification et Chiffrement

- Algorithmes de chiffrement et de hachage
 - Authentification MD5-HMAC 128 bit
 - Authentification SHA1-HMAC 160-bit
 - Cryptage DES-CBC 56 bit
 - Cryptage 3DES-CBC 168 bit
 - Cryptage AES 128, 192, 256 bit
- Diffie Hellman Group Support
 - Group 1 : MODP 768
 - Group 2 : MODP 1024
 - Group 5 : MODP 1536
 - Group 14 : MODP 2048
- Mécanisme d'authentification
 - Clé pré-partagée
 - Certificats X509
 - X-Auth
 - Cartes à puce et Token (Aladdin, ..)
 - Prise en charge flexible de certificat (PEM, PKCS#12, ...)
- Gestion des clés
 - ISAKMP (RFC2408)
 - IKE (RFC2409)
- IKE & IPSec Mode
 - ESP, Tunnel, Transport
 - Principal, agressif, rapide
 - Méthode d'authentification hybride
- Config-Mode



Réseau

- Réseau
 - NAT traversal (Draft1, 2 y 3) permite la conexión VPN a través de un dispositivo NAT. Mode principal et agressif.
 - NAT Keep Alive, NAT_OA Payload, émulation d'adresse IP.
 - NAT-T forcé.
 - Plusieurs tunnel pour plusieurs passerelles.
 - Dead Peer Detection (DPD)
- Technologies de connexion
 - DSL, dial-up modem, GPRS-Edge-3G, Ethernet, PCMCIA cards, WIFI, etc...
- Passerelle redondante
 - Passerelle redondante quand la principale est en panne ou ne répond pas. Utilisez le DPD pour le basculement.
- Peer to Peer
 - Connections en Peer to Peer.
 - Accepte les tunnels IPsec entrants.
- Capacités de blocage
 - Filtrage du trafic 'Seulement IPsec'.
 - Peut bloquer toutes les connexions autres que les connexions VPN.
- Remote Desktop Sharing (RDP session)
 - Plusieurs sessions de partage de bureau à distance
 - Le tunnel VPN s'ouvre automatiquement, et une session Remote Desktop Sharing est lancé pour atteindre la machine distante.
 - A voir dans la [vidéo ici](#).



Déploiement

- **Mode Clé USB**
 - Tous les formats sont supportés(SD, MMC, ...).
 - Auto fermeture, ouverture automatique des tunnels IPSec lors du branchement ou du retrait de la clé USB.
 - Elements de sécurité (e.g. configuration réseau, clé partagée, certificat, ..) ne peuvent être utilisés sur d'autres ordinateurs.
- **Config-Mode**
 - Récupération automatique du réseau DNS distant , et de l'adresses du serveur WINS.
 - Peer to Peer .
 - Connexions en Peer to Peer.
 - Accepte les tunnels IPSec entrants.
- **Capacités de blocage**
 - Filtrage du trafic 'Seulement IPSec'.
 - Peut bloquer toutes les connexions autres que les connexions VPN.
- **Options de gestion**
 - Contrôle d'accès pour le panneau de configuration
 - Peut fonctionner de manière totalement invisible pour les utilisateurs (mode caché)
- **Jeu de lignes de commande pour faciliter le déploiement et la gestion**
 - Possibilité de se lancer avant la connexion.
 - Lancement de script quand un tunnel s'ouvre ou se ferme.



Ecosystem

- Plates-formes supportées

- Windows Server 2003/2008, XP, Vista 32/64-bit, Seven 32/64-bit.
- Windows Mobile 5.0, Mobile 6 & 6.5



- Plus de 100 passerelles VPN supportés

- Astaro, Bewan, Billion, Bintec, Cisco, D-Link, Efficient Network, Fortinet, FreeSwan, OpenSwan, GTA, Hotbrick, Linksys, Microsoft, Netasq, Netcelo, Netgear, Netscreen, Securepoint, Sonicwall, Speedtouch, Symantec, Tuxgate, Zyxel,...

- USB Tokens & SmartCards supportés

- ActivIdentity, Aladdin, Alios, Gemalto, Oberthur, Safenet, ...

- Langues supportés

- Allemand, Anglais, Arabe, Chinois (simplifié), Danois, Espagnol, Farsi, Finlandais, Français, Grec, Hindi, Hongrois, Italien, Japonais, Néerlandais, Norvégien, Polonais, Portugais, Russe, Slovénien, Serbe (latin), Tchèque, Thaï & Turc.

- Solution Partenaires





Secure, Strong, Simple

TheGreenBow Logiciels de sécurité

[▶ Telecharger](#)