

Sichere Verbindungen

Speziell für mobile oder Telearbeitsplätze konzipiert, bietet der TheGreenBow™ VPN Client eine softwarebasierte IPSec Lösung, welche sichere Verbindungen in Unternehmensnetzwerke über das Internet gewährleistet.

Im Gegensatz zu hardwareabhängigen Lösungen ist der TheGreenBow™ VPN Client kompatibel zu allen gängigen IPSec VPN Gateways. Der TheGreenBow™ VPN Client bietet ein umfassendes Konfigurationsinterface – Das Einrichten eines Virtual Private Networks wird zum Kinderspiel.

Einfache Bedienung

Einfach zu installieren, einfach zu verstehen. Mit dem Konfigurationsassistenten und umfassenden Konfigurationshilfen zu den gängigsten Gateways ist ein VPN schnell aufgebaut. Daher ist der TheGreenBow™ VPN Client eine kosteneffektive Lösung für Systemintegratoren.

Universeller IPSec VPN Client

Der TheGreenBow™ VPN Client läuft unter Microsoft Windows 95, 98, Me, NT4, 2000, XP, Vista und Windows 7 Workstations. Ebenso wird extensiv die Kompatibilität mit allen gängigen IPSec VPN Gateways am Markt getestet. Die ständig erweiterte Liste der unterstützten Gateways finden Sie auf der Internetseite www.thegreenbow.de.

Point-to-Point Tunnel Unterstützung

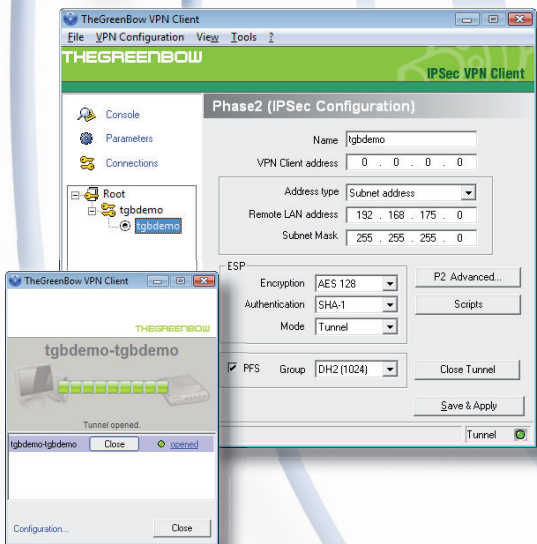
Der TheGreenBow™ VPN Client kann Verbindungen zu anderen TheGreenBow™ VPN Clients aufbauen. Dies ist besonders geeignet für sichere Subnetzwerke innerhalb eines Unternehmens oder für sensitive Wireless LAN Verbindungen.

Management Optionen

Konfigurationseinstellungen und Parameter werden in einer besonderen Dateien abgespeichert. Dies macht Implementierung und Distribution des VPN Clients besonders einfach. Darüber hinaus erlauben diverse Management Tools Administratoren eine erweiterte Kontrolle über den VPN Client.

Skalierbarkeit

Von privaten Nutzern bis zu großen Unternehmen bietet der TheGreenBow™ VPN Client eine effektive und günstige Lösung für alle Projektgrößen.



Key Features

- Kompatibel mit allen IPSec VPN Gateways
- IPSec VPN Tunnel mit DES / 3DES / AES Verschlüsselung
- Internet Key Exchange (IKE) zur Benutzer Authentifizierung
- Unterstützt alle Verbindungsarten: DSL, ISDN, Modem, TCP/IP, WiFi, Kabel, ...
- DPD und Redundant gateway
- Mode-Config (auto, manual)
- USB Stick zur Speicherung der VPN Sicherheitsmerkmale (Konfiguration, Schlüssel, Zertifikate, ...)
- Benutzer Authentifizierung mit X-Auth, PEM oder PKCS#12 Zertifikate, SmartCard, PreShared Key, USB Token, ...
- Unterstützt alle Microsoft Betriebssysteme inklusive Windows 7

Produkt Spezifikationen

- **Hash Algorithmen**
 MD5-HMAC 128 bit Authentifizierung
 SHA1-HMAC 160 bit Authentifizierung
 SHA2-HMAC 256 bit Authentifizierung
- **Verschlüsselungen**
 DES-CBC 56 bit Verschlüsselung
 3DES-CBC 168 bit Verschlüsselung
 AES 128, 192, 256 bit Verschlüsselung
- **Diffie Hellman Group Unterstützung**
 Group 1: MODP 768
 Group 2: MODP 1024
 Group 5: MODP 1536
 Group 14: MODP 2048
- **Authentifizierungsmechanismen**
 Preshared Key
 X509 Certificate
 X-Auth (mit OTP Tokens)
 Hybrid Authentication Method
 Vista Credential Provider (aka GINA)
- **Zertifikate**
 Flexible Unterstützung von Zertifikaten (PEM, PKCS#12)
 SmartCard & USB Token (RSA,...)
 Windows Certificate Store
- **IKE & IPSec Mode**
 ISAKMP (RFC2408), IKE (RFC2409)
 ESP, Tunnel, Transport
 Main, Aggressive, Quick
 Hybrid Authentication Method
- **Config-Mode**
 Automatisches Abholen von Remote Network, DNS, WINS Server Adressen.
 Manueller Config-Mode wenn Remote Gateway Config-Mode nicht unterstützt.
- **Netzwerk**
 NAT Traversal (Draft1, 2 & 3) erlaubt IPSec Verbindungen durch ein NAT Device. Main mode & aggressive mode.
 NAT Keep Alive, Payload NAT_OA, IP address emulation. Forced NAT-T.
 Multiple Tunnels zu verschiedenen Gateways.
 Dead Peer Detection (DPD) Support.
- **Verbindungsarten**
 DSL, GPRS-Edge-3G, Ethernet, WiFi, ...
- **Redundante Gateways**
 Redundante Gateways wenn das Primäre ausgefallen ist oder nicht antwortet. Nutzt DPD zur Ausfallsicherung.
- **USB Stick Modus**
 Unterstützt alle Formate (SD, MMC, ...) Auto-Schliessen, Auto-Öffnen von IPSec Tunnels beim Ein- oder Ausstecken des USB Stick.
 Sicherheitsmerkmale (Konfiguration, Schlüssel, Zertifikate, ...) kann nicht auf anderen Computern verwendet werden.
- **Peer to Peer**
 Peer to Peer Verbindungen
 Akzeptiert eingehende IPSec Tunnel
- **Blocking Möglichkeiten**
 ‚IPSec only‘ Trafficfilterung
 Blockiert alle Verbindungen außer IPSec VPN.
- **Management Optionen**
 Zugriffskontrolle zum Konfigurations Panel.
 Client Konfiguration in verstecktem Modus.
 Kommandozeilenunterstützung zur einfacheren Implementierung und Verwaltung.
 Scripte beim öffnen oder schließen eines Tunnels starten.
 Neue USB Tokens/Smartcard jederzeit einfügbar.
- **Performance**
 Läuft als Dienst unter Win2K oder XP, hohe Performance, kein System Overhead
- **Anpassbare GUI**
 Optische Anpassungen des User Interface auf Anfrage
- **Unterstützte Plattformen**
 Win2000, WinXP 32-bit, Windows Server 2003 32 bit, Windows Server 2008 32/64 bit, Vista 32/64 bit, Windows 7
- **Unterstützte VPN Gateways**
 TDT VPN Gateways und TDT Router, Astaro, Bewan, Billion, Bintec, Cisco, D-Link, Efficient Network, Fortinet, FreeSwan, OpenSwan, GTA, Hotbrick, Linksys, Microsoft, Netasq, Netgear, Netscreen, Securepoint, Sonicwall, Symantec, Tuxgate, Zyxel, etc...