

Datenblatt IPsec Client 2.8.2004

>> IPsec Client



Der IPsec Client von Bintec eignet sich ideal für Geschäftsleute, die häufig reisen oder zu Hause arbeiten. Er bietet ihnen sicheren Fernzugriff über ein bestehendes IPsec-Gateway der Firma oder direkt zu einem IPsec-fähigen Server. Er trägt auch dazu bei, Sicherheitslücken innerhalb des Firmen-LAN zu verhindern. Die flexible Paketfilterfunktion ermöglicht den einfachen Aufbau persönlicher Firewalls zum Schutz der Arbeitsplatzrechner vor unerwarteten vorsätzlichen Angriffen.

Es werden alle gängigen Windows Versionen unterstützt. Die Installation erfolgt über einen Wizard, mit dem die notwendigen Parameter eingegeben werden können.

Die Vorgänge der Verschlüsselung und Authentifizierung sind für den Endanwender vollständig transparent, da die IPsec-Technologie Sicherheit auf der Netzwerkebene bietet, die allen Anwendungen auf Internetbasis gemeinsam ist. Der Anwender verwendet weiterhin die ihm bekannten Anwendungen in gewohnter Weise.

Das Konfigurieren sicherer Verbindungen nimmt der Netzwerkadministrator in einfacher Weise vor. IKE Probing und das mehrschichtige Sicherheitsverfahren ermöglichen das flexible Konfigurieren mehrerer sicherer Verbindungen einschließlich Fernzugriff, LAN, Peer-to-Peer und Client-Server-Konfigurationen. Die zentrale Verwaltung der Konfiguration ermöglicht das Aktualisieren der Sicherheitsrichtlinien im gesamten Unternehmen auf einfache Weise.

Der IPsec Client von Bintec bietet volle PKI-Unterstützung inklusive lokaler LDAP-Fähigkeit (Lightweight Directory Access Protocol) zum Abruf von Zertifikaten und CRLs (Certificate Revocation Lists) sowie Unterstützung für Protokolle mit Common Certificate Online Enrolment. Das Produkt wurde auf seine Verwendbarkeit zusammen mit den meisten bekannten Anwendungsprogrammen getestet.

>> IPsec Client - Übersicht

Der Bintec IPsec Client ermöglicht den Einsatz in beliebigen VPN Umgebungen. Durch seine standardkonforme IPsec Implementierung erlaubt er die Kommunikation mit IPsec Gateways verschiedenster Hersteller und unterstützt zudem alle gängigen Betriebssysteme. Zusätzliche Leistungsmerkmale erlauben die Implementierung einer ganzheitlichen Remote Access VPN Lösung.

Zum Leistungsumfang zählt unter anderem:

- Einwahl über alle Übertragungsnetze
- Kompatibilität mit VPN Gateways unterschiedlicher Hersteller
- Integrierte Personal Firewall
- Höhere Geschwindigkeit durch ISDN Kanalbündelung
- Gebührenersparnis durch Kosten und Verbindungskontrolle
- Hoher Bedienungskomfort durch grafische Oberfläche
- Unterstützung der gängigsten Betriebssystemplattformen
- Unterbindung des Missbrauchs von Dialer-Anwendungen





>> IPsec Client - Technische Daten

LAN-Emulation	Ethernet-Adapter mit NDIS Interface
PC-Betriebssysteme	Windows 98se, Windows NT (V4.0 SP5), Windows 2000, Windows ME, Windows XP Prof.
Netzwerkprotokolle	IP
Unterstützte Mediatypen	ISDN, GSM, GPRS, UMTS, WLAN, LAN, PPTP, PSTN (Modem), xDSL (PPP over Ethernet)
IPsec-VPN	Unterstützung von Pre-Shared-Key und Zertifikaten, Zentrale Konfiguration der IPsec-Proposals, d.h. das zentrale VPN Gateway bestimmt die Richtlinien (für IKE, IPsec-Phase 2) für den Secure Entry Client. IPsec nach RFC 2401-2409, Zur Optimierung in Remote Access-Umgebungen werden zusätzlich die Drafts (XAUTH, IKE-Config, DPD, NAT-T, IP-Comp) unterstützt
Encryption	Triple DES 128, 192 Bit Blowfish 128 Bit AES 128, 192, 256 Bit RSA 1024, 2048 Bit
Hash-Verfahren	SHA1 (Secure Hash Algorithm 1), MD5 (Message Digit 5)
Firewall-Funktionalitäten	IP-NAT (Network Address Translation), Stateful Inspection, LAN-Adapter-Schutz, Schutz des PCs bei VPN-Connection gegenüber Zugriffen von anderen LAN-Benutzern, erweiterte Firewall (Filtering)
PKI	Public Key-Infrastruktur nach X.509 v.3 Standard
- Smart Cards	PKCS#11, TCOS 1.2 und 2.0 (über CT-API oder PC/SC)
- Soft Zertifikat	PKCS#12
- PIN-Richtlinie	Administrative Vorgabe für die Eingabe beliebig komplexer PINs
- Revocation Lists	Überprüfung der CRL (Certificate Revocation List) und ARL (Authority Revocation List)
- Zertifikatsverlängerung	Überprüfung und Hinweis der Gültigkeitsdauer eines Zertifikates
Einmal-Passwort	(One Time Password) Komfortable Eingabe durch Trennung von PIN und Passwort, (RSA-Ready)
Einmal-Passwort	One Time Password in VPN, (RSA-Ready)
DynDNS (Dynamic DNS)	Namensauflösung im Tunnel-Endpoint

IP Adress Allocation	DHCP (Dynamic Host Control Protocol)
Dialer	NCP - Dialer, Alternativ: Microsoft RAS-Dialer für ISP-Einwahl ggf. mit Einwahl-Script
Verbindungsmanagement	Short Hold, Timeout (zeit- und gebührengesteuert)
Kanalbündelung im ISDN	Dynamisch, frei konfigurierbarer Schwellwert
Client Monitor	Grafische Benutzeroberfläche zur Konfiguration des Telearbeitsplatzes, mit Statusanzeigen, Verbindungssteuerung und -überwachung.

>> IPSec Client - Anwendungen

- > Der IPSec Client stellt VPN-Verbindungen zu allen IPSec-fähigen Sicherheitsgateways her und ermöglicht so Außendienstlern sicheren Zugriff auf das interne Firmennetzwerk
- > Durch Einsatz von selbstsignierten Zertifikaten kann sich der Anwender in einfacher Weise eine Reihe von sicheren Peer-to-Peer-Verbindungen definieren und so die wichtigsten IPVerbindungen schützen
- > Sichern eines Local Area Network (LAN) gegen Ausspähen und Sabotage von innen erfolgt einfach und ohne zusätzlichen Leistungsbedarf
- > Die flexible Paketfilterfunktion ermöglicht das einfache Einrichten einer Personal Firewall zum Schutz des Arbeitsplatzrechners vor unerwarteten vorsätzlichen Angriffen

