

## bintec VPN Access 100

Vielseitig wie Ihr Unternehmen, anspruchsvoll wie Ihre Anforderungen: die VPN Access - Geräte

### VPN Access 100

**Begrüßen Sie eine neue VPN-Generation mit vielfältigen Möglichkeiten**

bintec stellt mit der VPN Access Linie eine Gerätegeneration von VPN Gateways vor, die alle bisherigen Vorteile der bintec Geräte in sich tragen und speziell auf den hochverfügbaren Einsatz im VPN Umfeld optimiert wurden. Stärkere Prozessoren und größerer Speicher stellen die Zukunftsfähigkeit der Produkte eindringlich unter Beweis. IPSec und PPTP Verschlüsselungsfunktionen sind in diesen Geräten bereits vorhanden und müssen nicht mehr separat gekauft und aktiviert werden. Darüber hinaus bieten die Geräte eine Fülle von neuen Funktionen.



#### Load Balancing

Bei allen Geräten der VPN Access-Linie mit drei Ethernet-Interfaces ist es möglich, zwei der drei Interfaces als WAN-Interfaces zu konfigurieren. Damit steht nicht nur mehr Bandbreite zur Verfügung, sondern Sie haben auch die Möglichkeit, den Datenverkehr nach Last oder nach Datenart auf einzelne Leitungen zu verteilen. So kann z.B. eine der Leitungen den gesamten Verkehr ins Internet bewältigen, während die zweite ausschließlich für den VPN Verkehr zuständig ist. Ebenso denkbar ist es, eine der Leitungen für den Betrieb eines Webserverns zu nutzen. Dies kann z.B. eine preisgünstige ADSL-Leitung sein. In Verbindung mit DynDNS ist dann der Webserver trotz dynamischer IP-Adresse stets zu erreichen. Der zweite WAN-Port kann über eine zweite ADSL- oder gar SDSL-Leitung den sonstigen Datenverkehr Ihrer Firma übernehmen.

#### Bintec VPN Access – die Vorteile auf einen Blick:

- High-End-IPSec-Implementierung
- Load Balancing
- viele Backup-Möglichkeiten
- sinnvolle Geräteredundanz

#### Umfassende Backup-Möglichkeiten

Ein VPN hilft Ihnen, geschäftskritische Daten sicher und kostengünstig zwischen verschiedenen Standorten auszutauschen. Umso wichtiger ist es, dass die Kommunikation stets gewährleistet ist. bintec bietet hier eine Fülle von automatischen Mechanismen. Sind z.B. zwei WAN-Leitungen aktiv, kann eine der beiden den gesamten Datentransfer übernehmen, wenn die andere Leitung ausfällt. Falls beide Leitungen ausfallen, kann der VPN-Verkehr automatisch über das integrierte ISDN-Modem geleitet werden. Dieses Umschalten geschieht reibungslos und unmerklich für den Benutzer. Es besteht sogar die Möglichkeit, den Backup-Weg über ein analoges oder ein GSM-Modem zu realisieren.

#### Geräteredundanz

Falls ein Fehler im Gerät selbst vorliegen sollte, lässt sich der Datentransfer automatisch über ein zweites Gerät leiten. Durch unser bintec Router Redundancy Protocol (BRRP) lassen sich zwei Geräte redundant betreiben, die dann im LAN wie ein Gerät agieren. Beide besitzen neben ihrer eigenen IP- und MAC-Adresse pro Interface auch eine gemeinsame virtuelle IP- und MAC-Adresse. Diese wird bei allen

Computern im LAN als Standard-Gateway eingetragen. Die beiden VPN-Geräte kommunizieren über das bintec Protokoll. Fällt eines der Geräte aus, übernimmt automatisch das andere Gerät den gesamten Datenverkehr.

### **Starke Verschlüsselung**

Die bintec IPSec-Implementierung bietet alles, was Kunden wünschen. Neben zahlreichen Verschlüsselungsverfahren wie z.B. dem brandneuen Verfahren AES ("Advanced Encryption Standard") bietet bintec mit der VPN Access-Linie Verschlüsselungen von bis zu 256 Bit Länge. Damit ist Ihr Unternehmen schon heute für die Anforderungen von morgen gerüstet.

### **Zertifikatsunterstützung**

Selbstverständlich arbeiten unsere Geräte nicht nur mit Pre-Shared Keys, sondern auch mit Zertifikaten. Das ermöglicht den Aufbau einer Public-Key-Infrastruktur für höchste Sicherheit bei gleichzeitiger Flexibilität im täglichen Betrieb Ihres VPN. So sind Eingriffe zur Absicherung des Systems – beispielsweise bei Mitarbeiterwechsel oder bei Diebstahl eines VPN-Gerätes – nur noch zentral an einer einzigen Stelle notwendig. Das erleichtert Ihnen die Administration, erhöht die Sicherheit und Zuverlässigkeit und senkt darüber hinaus auch noch die Kosten. (Übrigens: Auch das Bundesministerium für Sicherheit in der Informationstechnologie empfiehlt den Einsatz von Zertifikaten.)

### **VPN mit dynamischen IP-Adressen**

Die bintec IPSec-Implementierung unterstützt von Anfang an den Aufbau von VPN-Tunneln – auch mit dynamischen IP-Adressen. So kann z.B. die Zentrale mit einer statischen IP-Adresse durch kostenloses ISDN-call-back-Verfahren jede Filiale zum Aufbau eines Tunnels veranlassen. Auch kleine Außenstellen sind so stets erreichbar, selbst wenn sie nicht permanent online sind.

Sogar wenn beide VPN-Beteiligten dynamische IP-Adressen haben, steht dank der bintec Lösung der Kommunikation nichts im Wege. Der Austausch der IP-Adressen erfolgt dabei über Dynamic-DNS-Anbieter im Inter- oder Intranet.

### **Kosten sparen durch Datenkompression**

Um Kosten zu sparen, wurde durch Kompression der Datendurchsatz traditioneller ISDN-Leitungen in der Vergangenheit erheblich gesteigert. Dasselbe gilt natürlich für VPN-Verbindungen. Allerdings lassen sich traditionelle Kompressionsverfahren wie VJHC, Stac oder MPPC nicht auf IPSec-Pakete anwenden. Damit würden die Pakete verändert, was die Gegenstelle als Hackerangriff deuten müsste, so dass sie die ankommenden Pakete nicht annehmen würde. Abhilfe schafft hier das Verfahren IPCOMP, das selbstverständlich durch die VPN Access-Produkte von bintec unterstützt wird. IPCOMP erhöht nicht nur die Bandbreite der Verbindungen, sondern reduziert je nach Datenart die Datenmenge um bis zu Faktor zehn. Schon wenn man lediglich von Faktor zwei ausgeht, würde dies bei volumenbasierten Tarifen die Kosten mindestens halbieren.

## ISDN-Schnittstelle

Merkmal	Bezeichnung
ISDN-Protokolle	Euro-ISDN und weitere nationale ISDN-Protokolle
Wahl- und Festverbindungen (S0)	Unterstützte Festverbindungen: D64S, D64S2, TS02, D64S2Y
B-Kanal-Protokolle	Hervorragende Interoperabilität mit anderen Herstellern (Raw-HDLC, CISCO-HDLC, X.75)
PPP, ML-PPP	(Siehe Software)
Multi-CAPI	Optional: CAPI 2.0 mit CAPI-User-Konzept (Passwort für CAPI-Nutzung) ermöglichen direkten Zugriff auf z.B. Fax- und E-Mail-Dienste
Bitraten-Adaption	V.110 (1.200 bis zu 38.400 Bit/s), V.120 bis 57.600 kBit/s (HSCSD) zur Verbindung mit GSM-Teilnehmern

## Sicherheit

Merkmal	Bezeichnung
NAT/PAT	Network & Port Address Translation / Stateful Packet Inspection: Abschottung des gesamten Netzes vom öffentlichen Zugang
CLID und Callback	Identifizierung des Anrufers (CLID), Rückruf (Callback)
Access-Listen	Filtern von IP-Paketen nach unterschiedlichen Kriterien (Source, Destination, Port und Interface)
Stateful Inspection Firewall	Filterung mit Überwachung und Interpretation des jeweiligen Status der einzelnen Verbindungen
RADIUS	Zentrale Überprüfung der Zugangsberechtigung auf einem RADIUS-Server (PPP und Login Authentifizierung)
TACACS+	Unterstützung von TACACS-Servern zur Authentifizierung, Autorisierung und Abrechnung (AAA) von Benutzern
Authentisierung	PPP-Mechanismen (siehe Software)
H.323-Proxy	Schutz des Intranets (z.B. durch NAT)
Content Filtering	30 Tage Test-Lizenz
VLAN	Netzwerkknoten lassen sich aus verschiedenen Netzwerksegmenten zu Arbeitsgruppen zusammenfassen
Verschlüsselung für PPP	MPPE bis zu 128 bit, andere bis zu 168 bit
VPN - IPSec	Inklusive mit max. 100 gleichzeitige Tunnels
VPN - IPSec	Starke Verschlüsselung bis 256 Bit (DES, 3DES, CAST, Blowfish, Twofish, AES)
VPN - PPTP	Mit PPTP
VPN - PPTP	Starke Verschlüsselung bis 128 Bit (MPPE), bis zu 168 Bit (DES/3DES, Blowfish)
DynDNS / DynVPN	Router ist trotz dyn. IP-Adresse über das Internet erreichbar
IKE für IPSec	Pre-Shared Keys und Support von X.509-Zertifikaten
X.509	X.509 v1/v3 Zertifikate (PKCS#7/8/10, 12, CLRs, SCEP)
QoS für IPSec	Verfügbar
PKI Support für IPSec	Verfügbar
NAT Traversal für IPSec	Verfügbar
Dynamisches IPSec im B- und	Verfügbar, kostenlose Lizenz erforderlich
IPCOMP	IP Kompression
IPSec / RADIUS	Verfügbar
IPSec Redesign	Policy Manager und Interface-Konzept
L2TP	Layer-2 Tunneling Protokoll für ATM, Ethernet, PPP; Benutzer-Authentifikation
Hardware Verschlüsselung	Für IPSec (DES, 3DES, AES)

## Wartung und Service

Merkmal	Bezeichnung
ISDN-Logging	ISDN Event & System Logging: Aufzeichnung von Systemmeldungen und Ereignissen, z.B. Einbruchsversuchen
SNMP	Komplettes Management mit MIB-II, Enterprise-MIB, inklusive SNMP-Management-Software für Windows (DIME-Tools und -Browser)
SSH Login	Für sichere Verbindungen von Terminal Anwendungen
Lokale / remote Wartung	Komplette Konfiguration und Wartung, lokal und aus der Ferne, über Ethernet, ISDN-login oder serieller Schnittstelle
Trace / Debugging / Monitoring	Traces für ISDN B-/D-Kanal, R-CAPI-Traces, Ethernet-Traces, Grund für Verbindungsabbruch, ISDN-Signalisierungsinformation
Email Alert	Vorhanden
DHCP	Server und Client zur vereinfachten Konfiguration für TCP/IP
Setup-Tool	Integriertes, menü-basierendes, intuitiv zu bedienendes Setup-Programm, einheitlich für das gesamte Bintec Produkt-Portfolio
HTML-Setup-Tool	Grafische Benutzeroberfläche für Browser mit Java Script
HTML Wizard	Browser-basierter Konfigurations-Assistent
H.323-Gatekeeper	Kommunikationskontrolle zwischen Gateway und H.323-Endgeräten
XADMIN	Roll out tool für größere Router-Installationen (IP+ISDN)
Activity Monitor	Kontrolle der Router-Aktivitäten von jedem LAN-PC aus
Dokumentation	Deutschsprachige Dokumentation auf CD
Gewährleistung	2 Jahre Hersteller-Gewährleistung

## Software-Ausstattung

Merkmal	Bezeichnung
TCP/IP-Routing	Routing-Information-Update und -Verteilung statisch oder dynamisch (RIP v1/v2/triggered, RFC 2091), selektierbar für jedes Interface, ProxyARP, BOOTP/DHCP- Forwarding
Erweitertes IP-Routing	Abhängig von Quell-/Zielpport, Source-IP-Address, TOS ..., d.h. Policy Based Routing
OSPF	Statische/dynamische Aktualisierung und Verteilung von Routing-Informationen
Bridging	Spanning Tree & Transparent Mode
QoS	Quality of Service mit DiffServ und Shaping: Trennung des IP-Datenverkehrs in Klassen mit verschiedenen Prioritäten, optimiertes Queue-Handling und Shaping gemäß diesen Prioritäten
Download QoS	Optimieren des Download Verhaltens für VoIP
BRRP	Bintec Router Redundancy Protocol, Backup eines Router-Services durch einen anderen Router im LAN (Virtual Router)
IP Load Balancing	Bandwidth Management
BoD	Bandwidth on Demand: skalierbare Bandbreite, dynamische Bandbreitenzuschaltung in Abhängigkeit vom Datenaufkommen
AUX Backup	Backup-Möglichkeiten über GSM, GPRS oder Analog-Modem
PPP	Authentisierungsmechanismen (PAP, CHAP, MS-CHAP, MS-CHAP v2), Standard PPP, Kanalbündelung über Multilink-PPP (ML-PPP), transparent Mode, dynamische IP-Adressvergabe (Server- und Client-Modus)
PPPoE	Point to Point Protocol over Ethernet (Client und Server) für High-speed Internet-Zugang über xDSL (RFC 2516)
Dyn. IP-Adressen	Einfacher Internet-Zugang ohne feste IP-Adressen
Artem Access Point Discovery	Auffinden von konfigurierten und unkonfigurierten Artem Access Points im LAN
Betriebssysteme	Unterstützung von DOS, Windows 3.x/95/98/NT/ME/2000/XP, UNIX, Macintosh und Novell
ISDN-Accounting	Detaillierte laufende Aufzeichnung (Call Detail Recording), Rufnummer, Gebühreninformation, ...
IP-Accounting	Source, Destination, Port, Interface, Pakete/Bytes-Zähler
Event Scheduler	volumenabhängige oder zeitbasierte Budgets möglich
Shorthold	Statischer und dynamischer Shorthold spart Verbindungskosten durch automatischen Verbindungsabbau
Keep Alive Monitoring	spart Kosten, indem ein Verbindungsaufbau nur zugelassen wird, wenn konfigurierbare IP-Adressen erreichbar sind
MPPC	Software-Datenkompression auch in Verbindung mit MPPE (Microsoft Point to Point Encryption), kostenlose Lizenz erforderlich
STAC	Kompression für PPP-Verbindungen, kostenlose Lizenz erforderlich
Cost-of-Ownership	Minimal durch z.B. komplette Fernwartbarkeit

## Hardware-Ausstattung

Merkmal	Bezeichnung
RISC Architektur	Motorola 8241 RISC Prozessor mit 32 MB RAM
Flash-ROM	8 MB on board
LAN / WAN	3 x 10/100 MBit/s Ethernet Twisted Pair, autosensing
ISDN	1 x S0, 2 B-Kanäle
Konsole	Serieller Konsole-Port: RS 232 C, 8pol. Mini-DIN, 1.200 Bit/s - 115 kBit/s
Netzteil	Externes Trafo-Netzteil 12 V DC, 1 A
Ein/Aus-Schalter	Vorhanden
Status-LEDs	Power, Status, Ethernet 1, Ethernet 2, Ethernet 3, ISDN-D, ISDN-B, HA, MA
Metall-Gehäuse	Vorhanden
19-Zoll	Optional: montierbar in 19-Zoll-Schrank mit 19-Zoll-Einbau-Rahmen
Abmessungen	Ca. 200 x 30 x 150 mm (B x H x T)
Gewicht	Ca. 900 g