

MULTIPLEX VPN GATEWAY



Das leistungsstarke Central-Site-VPN-Gateway

bintec RXL12500

- 10 x Gigabit-Ethernet, davon 2 x SFP
- 100 IPsec Tunnel (opt. max. 2500 und HW-Beschleunigung)
- 19 Zoll Metallgehäuse
- Integriertes Schaltnetzteil, optionales redundantes Netzteil
- Unterstützung von IPv6
- Extended Routing und NAT (ERN)
- BRRP und Load Balancing



bintec RXL12500

Das leistungsstarke Central-Site-VPN-Gateway

Das Central Site VPN-Gateway bintec RXL12500 eignet sich aufgrund seiner umfangreichen IPSec-Implementierung und der enormen IPSec-Verschlüsselungsleistung für unternehmenskritische Anwendungen in mittleren und großen Unternehmenszentralen.

Produktbeschreibung

Der bintec RXL12500 ist ein leistungsfähiges und durch seine komplette Ausstattung flexibel einsetzbares Central-Site-VPN-Gateway. Mit 19“-Metall-Gehäuse und hocheffizientem internen Schaltnetzteil gewährleistet es langfristige Zuverlässigkeit in unternehmenskritischen Anwendungen. Das Gerät verfügt über 10 Gigabit-Ethernet-Ports (8*RJ45 und 2*SFP), die frei für LAN, WAN oder DMZ konfiguriert werden können.

Ab Werk verfügt das Gerät bereits über eine Lizenz für 100 IPSec-Tunnel, per Lizenzen ist es erweiterbar auf bis zu 2500 Tunnel.

Sowohl die im Gerät integrierte ISDN-Schnittstelle als auch ein am USB-Port angeschlossener UMTS-USB-Stick kann als Remote-Konfigurationszugang verwendet werden. Es besteht zudem die Möglichkeit über die Anschaltung des optionalen Netzzeileinschubes, bintec PSU XL, eine redundante Stromversorgung zu realisieren. Damit ist der bintec RXL12500 selbst für den Einsatz in komplexen Szenarien, als Central-Site-VPN-Gateway in Unternehmenszentralen prädestiniert.

WLAN Controller und HotSpot

Zusätzlich bietet der Router die Option des bintec WLAN Controllers. Der bintec WLAN Controller dient der Konfiguration und Überwachung von kleinen WLAN-Netzen mit bis zu 150 Access Points. Ob Frequenzmanagement mit automatischer Festlegung der Funkkanäle, der Lastverteilung auf mehrere Access Points, die Unterstützung von Virtuellen LANs oder die Verwaltung virtueller Funknetze (Multi-SSID) - mit dem WLAN Controller haben Sie alle fortgeschrittenen Funktionen bequem im Griff. Die Software überwacht dabei permanent das gesamte WLAN und meldet jeden Ausfall und jedes Sicherheitsrisiko.

Das integrierte HotSpot Gateway des Router stellt eine ideale Ergänzung zum WLAN Controller dar und dient zusammen mit der bintec HotSpot Lizenz zur Bereitstellung eines drahtlosen Gästernetz, das eine Authentifizierung des Gastes erfordert. Die sichere Trennung zwischen Gastnetz und Unternehmensnetz wird über den WLAN Controller konfiguriert und mittels virtueller Funknetze umgesetzt.

Funktionen flexibel nutzen

Zur Weiterleitung von Daten zwischen zwei Netzwerken sind nur wenige Funktionen erforderlich. Bintec Gateways verfügen über Leistungsmerkmale, die weit über das reine Routing hinaus gehen und eine Integration in komplexe IT-Infrastrukturen problemlos möglich machen. Funktionen wie Extended Routing und Extended NAT (ERN) erlauben eine exakte Trennung und detaillierte Umsetzung sämtlicher ein- und ausgehender Datenpakete nach genau definierten Kriterien.

Als Routingprotokolle können Sie z. B. RIP, OSPF oder auch das Multicast-Routing-Protokoll

PIM-SM einsetzen – gerade die umfangreiche Multicast-Unterstützung prädestiniert das Gerät für Multimedia- und Streaming-Anwendungen.

Durch integriertes Quality of Service können Sie z. B. den VoIP-Verkehr gegenüber dem normalen Internet-Verkehr priorisieren und auf diese Weise stets ausreichend Bandbreite für Ihre IP-Sprachverbindungen zur Verfügung stellen. Oder Sie räumen dem normalen Datenverkehr gegenüber dem E-Mail-Verkehr Vorrang ein.

Die DNS-Proxy-Funktion unterstützt das LAN bei der Adressumsetzung, und die automatisierte IP-Konfiguration von PCs erfolgt über einen integrierten DHCP-Server.

Umfangreiche IPSec-Implementierung

Die im bintec RXL12500 integrierte IPSec-Implementierung arbeitet nicht nur mit Preshared-Keys, sondern auch mit Zertifikaten. Dies ermöglicht den Aufbau einer Public-Key-Infrastruktur für höchste Sicherheit. (Übrigens: Auch das Bundesministerium für Sicherheit in der Informationstechnologie empfiehlt den Einsatz von Zertifikaten.) Die Zertifikate können ferner bequem und einfach an einem RADIUS-Server verwaltet werden. Die bintec elmeg GmbH bietet dabei sogar eine besondere Funktion, die auch RADIUS-Dial-Out-Lösung ermöglicht. Desweiteren unterstützt die bintec IPSec-Implementierung Sie beim Aufbau von VPN-Verbindungen mit dynamischen IP-Adressen: Auch kleine Außenstellen sind so erreichbar, selbst wenn sie nicht permanent online sein sollten. Sogar wenn beide VPN-Beteiligten lediglich über dynamische IP-Adressen verfügen, steht der vertraulichen Kommunikation nichts im Wege. Der Austausch der IP-Adressen erfolgt dabei entweder über Dynamic-DNS-Anbieter oder direkt über eine ISDN-Verbindung. Dabei wird die eigene dynamische IP-Adresse entweder kostenlos im ISDN-D-Kanal oder, falls dies nicht möglich sein sollte, im B-Kanal (kostenpflichtig) übertragen.

Mittels IKE Config Mode und dem bintec IPSec Multi User besteht zudem die Möglichkeit, IPSec-Dial-In-Lösungen für mehrere Clients mit minimalem Aufwand zu erstellen und zu Verwalten.

XAuth (Extended Authentication) in Kombination mit einer „One Time Password“-Lösung ermöglicht die Absicherung einer Remote Dial In Verbindung auf höchstem Sicherheitsniveau.

Folgende „One Time Password“ Partnerlösung wurde zertifiziert. (SMS PASSCODE ®)



Load Balancing/Redundanz

Der bintec RXL12500 bietet die Möglichkeit, mehrere Interfaces als WAN-Interfaces zu konfigurieren. Damit steht nicht nur mehr Bandbreite zur Verfügung, sondern es besteht die Möglichkeit, den Datenverkehr nach Last oder nach Datenart auf einzelne WAN-Verbindungen zu verteilen. Ebenso können Sie eine Internet-Anbindung mit z. B. 100 Mbit Ethernet für die VPN-Anbindung einer größeren Anzahl von Außenstellen und Außendienstmitarbeitern nutzen und über den zweiten WAN-Port durch eine kostengünstige VDSL-Verbindung den sonstigen Datenverkehr Ihrer Firma sicher stellen.

Durch unser bintec Router Redundancy Protocol (BRRP) lassen sich zwei Geräte so betreiben, dass sie im LAN wie ein Gerät agieren. Beide verfügen neben ihrer eigenen IP- und MAC-Adresse pro Interface auch über eine gemeinsame virtuelle IP- und MAC-Adresse. Diese wird bei allen

Computern im LAN als Standard-Gateway eingetragen. Die beiden auf diese Weise zusammen geschalteten Gateways kommunizieren über das bintec Protokoll, und fällt eines der Geräte aus, übernimmt automatisch das andere Gerät den gesamten Datenverkehr.

Einfache Konfiguration und Wartung

Die Konfiguration des Gateways erfolgt über die Web-GUI, u. a. mit den darin integrierten Konfigurationsassistenten. Die Web-GUI ist eine web-basierte grafische Benutzeroberfläche, die von jedem PC mit einem aktuellen Web-Browser aus über eine HTTP- oder verschlüsselt über eine HTTPS-Verbindung bedient werden kann. Darüber hinaus besteht die Möglichkeit, die Geräte sowohl lokal als auch aus der Ferne über weitere Konfigurationszugänge wie Telnet, SSH und ISDN-Login zu verwalten.

Ein wesentliches Sicherheitsmerkmal sind die vielfältigen Möglichkeiten das Gateway zu überwachen. Zum einen können Sie sämtliche Konfigurationsparameter sowie Statusinformationen per SNMP abfragen. Zum anderen können diese auch per SNMP-Traps von Gateway an einen SNMP-Manager gesendet werden. Schließlich haben Sie die Möglichkeit Syslog-Meldungen protokollieren zu lassen. Außerdem kann sich der Administrator per E-Mail über bestimmte Ereignisse informieren lassen.

Performance RXL

Leistungsfähigkeit der bintec RXL-Serie

Die in der Regel in der Firmenzentrale eingesetzten neuen bintec-Geräte der RXL-Serie verfügen Dank ihrer integrierten High End Encryption Engine über eine außergewöhnliche Leistungsfähigkeit im Bereich der IPSec-Verschlüsselung. Die konkrete Leistung ist jedoch abhängig von der jeweiligen Paketgröße, dem Verschlüsselungsalgorithmus, der Anzahl der aktiven oder konfigurierten Tunnel, den Firewall-Einstellungen sowie weiteren Faktoren. Aus diesem Grunde ist es schwierig, allgemein gültige Durchsatzwerte anzugeben. Je nach Konfiguration können die tatsächlichen Datenwerte von den angegebenen Werten abweichen.



Getestet wurden die Geräte der bintec RXL-Serie mit Software Version 7.10.1. Die IPSec Werte der RXL12500 wurden mit aktivierter Hardware Verschlüsselung gemessen. Als Messtechnik wurde der Traffic Generator/Analyser "SmartBit 600B" der Firma Spirent verwendet.



IPSec-Performance (AES256)						
Datendurchsatz in Mbit/s pro Paketgröße (byte)						
Gerät	1400	1024	512	256	128	64
bintec RXL12100	130,1	124,1	102,9	77,1	53,33	19,4
bintec RXL12500	793	652,4	389,8	206,3	111,3	62,4

Die Werte der RXL12500 wurden mit aktivierter Hardware Verschlüsselung gemessen.

Routing-Performance						
Datendurchsatz in Mbit/s pro Paketgröße (byte)						
Gerät	1400	1024	512	256	128	64
bintec RXL12100	986,99	980,84	962,40	927,54	615,39	313,73
bintec RXL12500	986,99	980,84	962,40	927,54	615,39	313,73

Varianten

bintec RXL12500 (5510000235)

Zentraleseitiges Enterprise VPN Gateway, 19" Gerät, inkl. 100 aktive IPSec Tunnel (opt. max. aktive 2500 und HW-Encryption), 8 Gigabit Eth. Switch, 2 * SFP Modul Slots, 1 * USB, 1 * ISDN-S0, 1 GB RAM (opt. 4 GB RAM), opt. redundante Stromversorgung

Features

Quality of Service (QoS)

Quality of Service (QoS)

Policy based Traffic Shapping	Dynamisches Bandbreitenmanagement mittels IP Traffic Shaping
Bandbreitenreservierung	Dynamische Reservierung von Bandbreiten, Zuweisung von garantierten und maximalen Bandbreiten
DiffServ	Priority Queuing der Pakete anhand des DiffServ/TOS-Felds
Layer2/3 Tagging	Umsetzen von 802.1p Layer-2-Prioritätsinformation auf Layer 3 Diffserv-Attribute
TCP Download Rate Control	Dient zur Reservierung von Bandbreiten für VoIP-Verbindungen
Gewährleistung	2 Jahre Hersteller-Garantie inklusive Vorabaustauschservice
Software Update	Kostenfreie Software Updates (System Software (BOSS) und Management Software (DIME Manager)

Redundanz / Loadbalancing

BRRP	Bintec Router Redundancy Protocol, dient zur Ausfallsicherung mehrere passiver oder aktiver Geräte mit frei einstellbarer Priorität.
BoD	Bandwidth on Demand (BoD): dynamische Bandbreitenzuschaltung in Abhängigkeit vom Datenaufkommen
Load Balancing	Statische und dynamische Lastverteilung auf mehrere WAN-Verbindungen auf IP-Ebene
VPN Backup	Einfaches VPN Backup über unterschiedlichste Medien. Darüber hinaus ermöglicht das bintec elmeg Interface-basiertes VPN Konzept die Verwendung von Routing-Protokollen für VPN Verbindungen.

Lieferumfang

Handbuch	Kurzanleitung Deutsch und Englisch
DVD	DVD mit Systemsoftware, Managementsoftware und Dokumentation
Ethernet Kabel	1 Ethernet Kabel, 3m
Netzkabel	Kaltgerätekabel
Seriellles Kabel	Seriellles Kabel (mini USB - DSUB 9 Female)
USB Kabel	USB Kabel (Type A - Type B)
ISDN-Kabel (BRI/S0)	ISDN (BRI/S0) Kabel, 3m

Layer 2 Funktionalität

Bridging	Unterstützung von Layer 2 Bridging mit der Möglichkeit zur Separierung von Netzwerksegmenten über die Konfiguration von Bridge-Gruppen
VLAN	Unterstützung von bis zu 255 VLAN (Virtual LAN) pro LAN Interface zur Unterteilung des Netzwerkes in unabhängige virtuelle Segmente (Arbeitsgruppen)
Proxy ARP	Erlaubt dem Router ARP-Anfragen für Hosts zu beantworten, die über den Router erreichbar sind. Dadurch ist es möglich, dass Remote Clients eine IP-Adresse aus dem lokalen Netz benutzen.

Optionen

IP-Adress-Übertragung ISDN B/D Kanal	Kostenlose Lizenz für IP-Adress Übertragung im ISDN D oder B Kanal für IPSec Verbindungen; Registrierung unter www.bintec-elmeg.com erforderlich
--------------------------------------	--

Logging / Monitoring / Reporting

Internes System-Logging	Syslog Speicher im RAM, Anzeige über die Web-basierte Konfigurationsoberfläche (http/https), filterbar nach Subsystem, Level, Message
External Systemlogging	Syslog, mehrere Syslog Server mit unterschiedlichen Syslog Level konfigurierbar
E-Mail Alert	Automatischer E-Mail-Versand beim Eintreffen definierbarer Ereignisse
SNMP Traps	SNMP Traps (v1, v2, v3) konfigurierbar
IPSec Monitoring	Anzeige der IPSec-Tunnel und der IPSec-Statistik; Ausgabe über die Web-basierte Konfigurationsoberfläche (http/https)
Interfaces Monitoring	Statistikinformationen aller physikalischen und logischen Schnittstellen (ETH0, ETH1, SSIDx, ...), Ausgabe über die Web-basierte Konfigurationsoberfläche (http/https)
ISDN Monitoring	Anzeige der aktiven und vergangenen ISDN-Verbindungen, Ausgabe über die Web-basierte Konfigurationsoberfläche (http/https)
IP Accounting	Detailliertes IP Accounting, Source, Destination, Port, Interface und Pakete/Bytes-Zähler auch über Syslogprotokoll an Syslog Server übermittelbar
ISDN Accounting	Detaillierte, laufende Aufzeichnung der ISDN-Verbindungsparameter wie Rufnummer und Gebühreninformationen auch über Syslogprotokoll an Syslog Server übermittelbar
RADIUS Accounting	RADIUS Accounting für PPP-, PPTP-, PPPoE- und ISDN-Dialup-Verbindungen
Keep Alive Monitoring	Überwachung von Hosts/Verbindungen via ICMP-Polling
Tracing	Des Weiteren besteht die Möglichkeit, die Traces im PCAP-Format abzulegen, so dass sie anschließend in diversen Opensource Tracetools (z. B. Wireshark) eingelesen werden können.

Administration / Management

RADIUS	Zentrale Überprüfung der Zugangsberechtigung auf einem oder mehreren RADIUS-Servern (PPP, IPSec inklusive X-Auth und Login-Authentifizierung)
RADIUS Dialout	Es besteht die Möglichkeit, die auf einem RADIUS-Server konfigurierten PPP- und IPSec-Verbindungsdaten in das Gateway zu laden (RADIUS Dialout).
TACACS+	Unterstützung von TACACS+-Servern zur Login Authentication und zur Shell-Kommando-Autorisierung
Zeit Synchronisierung	Die Gerätesystemzeit kann sowohl über ISDN als auch von einem SNTP Server bezogen werden (bis zu 3 Time Server konfigurierbar). Die bezogene Zeit kann per SNTP auch an SNTP Clients übertragen werden.
Automatic Time Settings	Die Möglichkeit, Zeitzonenprofile zu konfigurieren, ermöglicht eine automatische Sommer/Winterzeit-Umstellung
Unterstützte Managementsysteme	DIME Manager, XAdmin

Administration / Management

Konfigurierbarer Scheduler	Steuerung von Aktionen sowohl zeit- als auch ereignisgesteuert, wie z. B. Reboot Device, Activate/Deactivate Interface, Activate/Deactivate WLAN, Trigger SW Update und Configuration Backup
Configuration Interface (FCI)	Integrierter Webserver für die webbasierte Konfiguration mittels HTTP oder HTTPS (Unterstützung eigener Zertifikate) inkl. Die Benutzeroberfläche ist beim Großteil aller bintec elmeg GmbH-Produkte identisch.
Software Update	Software Updates werden kostenlos bereitgestellt; Update über lokale Dateien, HTTP, TFTP oder per direktem Zugriff auf den bintec elmeg Web Server
Fernwartung	Fernwartung über Telnet, SSL, SSH, HTTP, HTTPS und SNMP (V1,V2,V3)
Konfiguration über Serielle Schnittstelle	Serielle Konfigurationsschnittstelle ist vorhanden
ISDN-Fernwartung	Fernwartung via ISDN-Einwahl mit Rufnummernüberprüfung. Es besteht die Möglichkeit, die ISDN-Fernwartungsverbindung zwischen zwei bintec elmeg-Geräten zu verschlüsseln.
GSM-Fernwartung	Fernwartung via GSM Login (externes USB UMTS Modem erforderlich)
Geräte Discovery Function	Geräte-Discovery über SNMP Multicast.
On The Fly Konfiguration	Kein Neustart nach Umkonfiguration notwendig
SNMP	SNMP (v1, v2, v3), USM Model, VACM Views, SNMP Traps (v1, v2, v3) konfigurierbar, SNMP-IP-Access-Liste konfigurierbar
SNMP Konfiguration	Komplettes Management mit MIB-II, MIB 802.11, Enterprise-MIB
Konfiguration exportieren und importieren	Laden und Speichern der Konfiguration; Speichern der Konfiguration wahlweise verschlüsselt; wahlweise automatisch steuerbar über den Scheduler
SSH Login	Unterstützung von SSH V1.5 und SSH V2.0 für sichere Verbindungen von Terminal Anwendungen
HP OpenView	Einbindung in Network Node Manager
CA SPECTRUM	Einbindung in CA SPECTRUM Infrastructure Manager
XAdmin	Unterstützung vom XAdmin Roll-out- und Konfigurationsmanagement-Tool für größere Router-Installationen (IP+ISDN-GSM)

Schnittstellen

USB 2.0 Host	USB 2.0 Full Speed Host-Port zum Anschluss LTE(4G)- oder UMTS(3G)-USB-Sticks (unterstützte Sticks: siehe www.bintec-elmeg.com)
Ethernet	8 x 10/100/1000 MBit/s Ethernet Twisted Pair, autosensing, Auto MDI/MDI-X, jeder Ethernet-Port kann frei konfiguriert werden (LAN oder WAN).
SFP Slot	2 x SFP Slots für gängige optische 10/100/1000 Mbit/s Ethernet SFP-Module, jeder SFP-Port kann frei konfiguriert werden (LAN, WAN).
Serielle Konsole	Serielle Konsolenschnittstelle / COM-Port (Mini-USB)
USB Konsole	USB Konsolenschnittstelle
ISDN Basic Rate (S0)	1 x S0 (TE), 2 B-Kanäle

Hardware	
19-Zoll	Montierbar in 19-Zoll-Schrank, inkl. 19-Zoll-Einbausatz
Echtzeit Uhr	Auch bei Stromausfall bleibt die Systemzeit einige Stunden erhalten
Umgebungsbedingungen	Temperaturbereich: 0°C bis 40°C; Lagerung: -10°C bis 70°C; Rel. Luftfeuchte 10 - 95% (nicht-kondensierend)
Netzteil	Integriertes Weitbereichsnetzteil 110-240V, mit energieeffizienten Schaltregler
Leistungsaufnahme	Max. 40 Watt, typ. 30 Watt
Abmessungen	Ca. 485,6 mm x 220 mm x 45 mm (Breite x Tiefe X Höhe)
Gewicht	Ca. 2700g
Reset-Knopf	Neustart oder Zurücksetzen auf Werkseinstellung möglich
Status-LEDs	Power, Status, ISDN, 20 * Ethernet
Normen und Zulassungen	R&TTE Directive 1999/5/EG; EN 55022; EN 55024 + EN 55024/A1; EN61000-3-2; EN 61000-3-3; EN 61000-4-4; EN 60950-1; EN 300 328

ISDN	
CAPI	CAPI 2.0 mit CAPI-User-Konzept (Passwort für CAPI-Nutzung)
ISDN-Protokolle	Euro-ISDN (Mehrgeräte und Anlagenanschluss), 1TR6 und weitere nationale ISDN-Protokolle
ISDN-Autokonfiguration	Automatische Erkennung und Konfiguration des ISDN-Protokolls
ISDN-Festverbindungen	Unterstützte Festverbindungen: D64S, D64S2, TS02, D64S2Y
B-Kanal-Protokolle	Hervorragende Interoperabilität mit anderen Herstellern (Raw-HDLC, CISCO-HDLC, X.75)
X.31 over CAPI	Unterstützung vieler verschiedener Verbindungswege: X.31/A für ISDN-D-Kanal, X.31/A+B für ISDN-B-Kanal, X.25 innerhalb des ISDN-B-Kanals (auch Mietleitungen)
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

VPN	
IPSec Algorithmen	DES (64 Bit), 3DES (192 Bit), AES (128,192,256 Bit), CAST (128 Bit), Blowfish (128-448 Bit), Twofish (256 Bit); MD-5, SHA-1, SHA-2 (256,384,512), RipeMD160, Tiger192 Hashes
Anzahl der PPTP Tunnel	Inklusive 100 aktiver PPTP Tunnel, optional erweiterbar auf bis zu 1000 PPTP Tunnel
Anzahl der L2TP/GRE Tunnel	Inklusive 1000 aktiver L2TP und GRE Tunnel (auch in Kombination möglich)
IPSec	Internet Protocol Security für den Aufbau von VPN-Verbindungen
Anzahl der IPSec Tunnel	Inklusive 100 aktiver IPSec Tunnel, optional erweiterbar auf bis zu 2500 IPSec Tunnel
IPSec Hardwarebeschleunigung	Optional Hardwarebeschleunigung für IPSec Verschlüsselungsalgorithmen DES, 3DES, AES und Hardwarebeschleunigung für die MD-5, SHA-1 Hash Generierung
IPSec IKE	IPSec-Schlüsselaustausch über Preshared Keys oder Zertifikate
IPSec IKE Config Mode	IKE Config Mode Server ermöglicht die dynamische Zuteilung von IP-Adressen aus dem Adressbereich des Unternehmens. IKE Config Mode Client ermöglicht es dem Router, sich dynamisch eine IP-Adresse zuweisen zu lassen.

VPN	
IPSec IKE XAUTH (Client/Server)	Internet Key Exchange Protocol Extended Authenticaion Client zur Anmeldung an XAUTH Server und XAUTH Server zur Anmeldung von XAUTH Clients
IPSec IKE XAUTH (Client/Server)	Inklusive der Weiterleitung an einen RADIUS-OTP (One Time Password) Server (unterstützte OTP Lösungen siehe www.bintec-elmeg.com).
IPSec NAT-T	Unterstützung von NAT-Traversal (Nat-T) für den Einsatz auf VPN Strecken mit NAT
IPSec IPComp	IPSec IPComp-Datenkompression für höheren Datendurchsatz mittels LZS
IPSec Zertifikate (PKI)	Unterstützung von X.509 mehrstufigen Zertifikaten kompatibel zu Microsoft und Open SSL CA Server; Upload von PKCS#7/8/10/12 Dateien über TFTP, HTTP, LDAP, File Upload und manuell über FCI
IPSec SCEP	Zertifikatsmanagement mittels SCEP (Simple Certificate Enrollment Protocol)
IPSec Certificate Revocation Lists (CRL)	Unterstützung von Remote CRLs auf einem Server via LDAP oder lokaler CRLs
IPSec Dead Peer Detection (DPD)	Sorgt für eine kontinuierliche Überwachung der IPSec-Verbindung
IPSec Dynamic IP via ISDN	Übertragung von dynamischen IP-Adressen über ISDN D-Kanal oder ISDN B-Kanal (kostenlose Lizenz erforderlich)
IPSec Dynamic DNS	Ermöglicht die Registrierung dynamischer IP-Adresse bei einem Dynamic DNS Provider für den Aufbau einer IPSec-Verbindung.
IPSec RADIUS	Authentifizierung von IPSec-Verbindungen an einem RADIUS Server. Zusätzlich besteht die Möglichkeit, die auf einem RADIUS Server konfigurierten IPSec Peers in das Gateway zu laden (RADIUS Dialout).
IPSec Multi User	Ermöglicht die Einwahl mehrerer IPSec Clients über einen einzigen IPSec-Peer-Konfigurationseintrag
IPSec QoS	Es besteht die Möglichkeit, Quality of Service (Traffic Shaping) innerhalb eines IPSec-Tunnels zu betreiben
IPSec NAT	Durch das Aktivieren von NAT auf einer IPSec-Verbindung ist es möglich, mehrere Remote Locations mit gleichen lokalen IP-Adress-Netzen auf unterschiedliche IP-Netze für die VPN Verbindung umzusetzen.

Security	
NAT/PAT	Symmetrische Network und Port Address Translation (NAT/PAT) mit zufallsgenerierten Ports inklusive Multi NAT (1:1-Übersetzen ganzer Netzwerke)
Policy based NAT/PAT	Network und Port Address Translation anhand von unterschiedlichen Kriterien wie IP-Protokollen, Source/Destination IP Address, Source/Destination Port
Policy based NAT/PAT	Sowohl für eingehende als auch ausgehende Verbindungen für jedes Interface unterschiedlich konfigurierbar
Stateful Inspection Firewall	Richtungsabhängige Paketfilterung mit Überwachung und Interpretation des jeweiligen Status der einzelnen Verbindung
Paket Filter	Filtern von IP-Paketen anhand von unterschiedlichen Kriterien wie IP-Protokollen, Source/Destination IP Address, Source/Destination Port, TOS/DSCP, Layer-2-Priorität für jedes Interface unterschiedlich konfigurierbar

Routing

Policy based Routing	Erweitertes Routing (Policy Based Routing) abhängig von unterschiedlichen Kriterien wie IP-Protokollen (Layer4), Source/Destination IP Address, Source/Destination Port, TOS/DSCP, Source/Destination Interface und Destination Interface Status
Multicast IGMP	Unterstützung vom Internet Group Management Protocol (IGMP v1, v2, v3) für die gleichzeitige Verteilung von IP-Paketen an mehrere Stationen
Multicast IGMP Proxy	Dient zur einfachen Weiterleitung von Multicast-Paketen über dedizierte Interfaces
Multicast Routing Protokoll PIM SM	Protocol Independent Multicast (PIM) dient zur Informationsverteilung über einen zentralen Rendezvous Point Server. Beim unterstützten PIM Modus Sparse Mode (SM) werden nur Pakete an Gruppen weitergeleitet, welche die Pakete bestellt haben.
Multicast inside IPSec Tunnel	Ermöglicht die Übertragung von Multicast Paketen über einen IPSec-Tunnel
RIP	Unterstützung von RIPv1 und RIPv2, getrennt einstellbar für jedes Interface
Extended RIP	Triggerd RIP Updates nach RFC 2091 und 2453, Poisoned Reverse für eine bessere Verteilung der Routen, des Weiteren die Möglichkeit, RIP Filter für jedes Interface eingeständig zu definieren.
OSPF	Unterstützung vom dynamischen Routing Protokoll OSPF

Protokolle / Encapsulation

PPP/MLPPP	Unterstützung des Point to Point Protokolls (PPP) zum Aufbau von Standard-PPP-Verbindungen, inklusive der Multilink-Erweiterung MLPPP für die Bündelung von mehreren Verbindungen
PPPoE (Server/Client)	Point to Point Protokoll over Ethernet (Client/Server) für den Aufbau von PPP-Verbindungen über Ethernet/DSL (RFC2516)
MLPPPoE (Server/Client)	Multilink-Erweiterung MLPPPoE für das Bündeln mehrerer PPPoE-Verbindungen (nur möglich, wenn beide Seiten MLPPPoE unterstützen)
DNS	DNS Client, DNS Server, DNS Relay und DNS Proxy
DYN DNS	Ermöglicht die Registrierung von dynamisch zugeteilten IP-Adressen bei einem Dynamic DNS Provider z. B. zum Aufbau von VPN-Verbindungen
DNS Forwarding	Ermöglicht es, DNS-Anfragen von frei konfigurierbaren Dömanen zur Auflösung an bestimmte DNS Server weiterzuleiten.
DHCP	DHCP Client, Server, Proxy und Relay zur vereinfachten TCP/IP-Konfiguration
Paketgrößensteuerung	Anpassung der PMTU oder automatische Paketgrößensteuerung über Fragmentierung

IPv6

IPv4/ IPv6 Dual Stack	Parallelbetrieb von IPv4/ IPv6 unterstützt
DHCPv6	DHCP Server und Client
NDP	Neighbor Discovery Protocol: Router Discovery, Prefix Discovery, Parameter Discovery, Address Resolution, Static configuration of neighbors, IPv6 Router Advertisement Option for DNS Configuration (through ND)
ULA	Unique Local IPv6 Unicast Addresses
IPv6 Addressing	IPv6 Stateless address auto-configuration (SLAAC), Manual address configuration, General-prefix support for address configuration (user and prefix delegation DHCPv6), Duplicate Address Detection

IPv6

ICMPv6 (router & host)	Destination Unreachable, Packet too big, Time exceeded, Echo Request
Routing Protocols	Static Routes
Multicast	Multicast for IPv6
Firewall	Firewall via IPv6
IPSec	IPSec for IPv6

Zubehör

WLAN Controller

License WLAN Contr. 6AP (5500000943)	WLAN Controller Lizenz für 6 APs oder für die Erweiterung um 6 APs passend für die Geräte RS123x, RS353xx, Rxxx2 und RXL12x00
---	---

Software Lizenzen

RSxx3/Rxx02/RTxx02/RXL-IPSEC25 (5500000781)	Lizenz für 25 zusätzliche IPSec Tunnel bei den Geräten der RSxx3, Rxx02, RTxx02 und RXL12xxx Serie
RXL12xxx-HW-ENC (5500001161)	Lizenz für die RXL12500 zur Aktivierung der IPSec Hardware Encryption
RXL12xxx-IPSEC100 (5500001162)	Lizenz für 100 zusätzliche aktive IPSec Tunnel für die bintec RXL Serie
RXL12xxx-IPSEC400 (5500001163)	Lizenz für 400 zusätzliche aktive IPSec Tunnel für die bintec RXL12500 Serie
RXL12xxx-IPSEC1000 (5500001164)	Lizenz für 1000 zusätzliche aktive IPSec Tunnel für die bintec RXL12500 Serie
RXL12xxx-PPTP25 (5500001203)	Lizenz für 25 zusätzliche aktive PPTP Tunnel für die bintec RXL Serie

Pick-up Service / Garantieverlängerung

Service Package 'extra large' (5500001187)	Garantieverlängerung um 3 Jahre auf insgesamt 5 Jahre, inkl. Vorabaustausch für bintec elmeg Produkte der Kategorie 'extra large'. Übersicht der Kategoriezuordnung / detaillierte Beschreibung unter www.bintec-elmeg.com/servicepackages
---	--

Zubehör

bintec SFP-LC-SX (5530000189)	1000Base-SX SFP-Modul für die bintec RS123x u. bintec RXL-Serie zum Anschluss an Glasfaser. Unterstützt 62,5 µm und 50 µm Multimode Fiber (MMF). Wellenlänge 850nm. Max. Entfernung 275m bzw. 550m
bintec SFP-LC-TX/LX/LH (5530000190)	1000Base-LX SFP-Modul für die bintec RS123x u. bintec RXL-Serie zum Anschluss an Glasfaser. Unterstützt 9 µm Singlemode Fiber (SMF). Wellenlänge 1310nm. Max. Entfernung 10km
bintec 4GE-LE (5530000119)	LTE (4G)/UMTS (3G) Erweiterungsgerät für Router; 1x Gbit Eth; Simkarten Slot; Wandhalterung; PoE Injector inklusive

Stromversorgung

bintec PSU XL (5510000294)

Externe redundante Stromversorgung für bis zu 2 bintec RXL12xxx, 19" Gerät