Teldat
bintec-elmeg

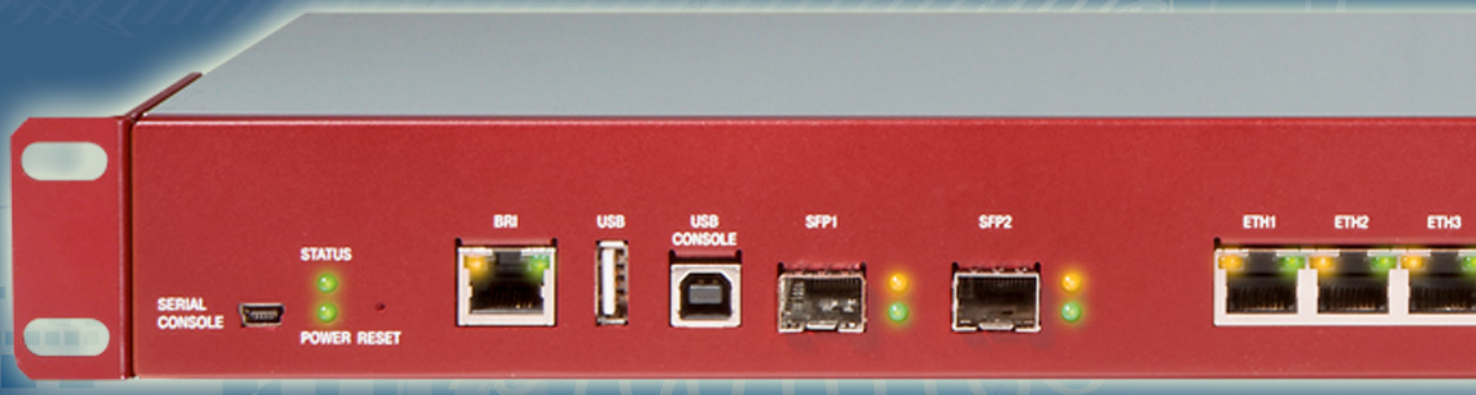
CENTRAL SITE VPN GATEWAY

The high-performance central site VPN Gateway

bintec RXL12500

VPN Gateways certified by:
sms passcode
secure world business

- 10 x Gigabit Ethernet therfrom 2 SFP
- 100 IPSec tunnels (opt. up to 2500 with HW acceleration)
- 19-inch housing
- Integrated power supply (optional redundant)
- IPv6
- Extended Routing and NAT (ERN)
- BRRP and Load Balancing



bintec RXL12500

The high-performance central site VPN Gateway

The bintec RXL12500 central site VPN gateway is, thanks to its comprehensive IPSec implementation and blazing IPSec encryption performance, perfectly suited for mission-critical applications at large and medium-sized corporate headquarters.

Product description

The high-performance bintec RXL12500 central-site VPN gateway offers exceptional flexibility thanks to its comprehensive feature set. With its 19-inch metal housing and highly efficient internal switch mode power supply, the RXL12500 provides long-term reliability for mission-critical applications. The device's ten Gigabit Ethernet ports (8 x RJ45 and 2 x SFP) can be independently configured for use in a LAN, WAN, or DMZ. A license for 100 IPSec tunnels is included and can be expanded to accommodate up to 2500 tunnels.
Administrators can use either the integrated ISDN interface or a UMTS USB stick for remote configuration. The optional bintec PSU XL slide-in power supply module equips the bintec RXL12500 with a redundant power supply, making the central-site VPN gateway a perfect fit for complex environments such as corporate headquarters.

WLAN Controller

The RXL series can also be used in combination with the Teldat WLAN controller.

The Teldat WLAN controller lets you configure and monitor small- and medium-sized WLAN networks with up to 150 access points. No matter whether you need frequency management with automatic channel selection, support for virtual LANs, or virtual wireless network administration (multi-SSID), you'll have every advanced feature at your fingertips with the WLAN Controller. The software continually monitors the entire WLAN, sending a notification for any malfunction or security threat.

Flexible functionality

Forwarding data between two networks only requires basic functionality. Bintec gateways however offer features that go far beyond mere routing to allow seamless integration into even the most complex IT infrastructures. Functions such as extended routing and extended NAT (ERN) enable detailed implementations to strictly separate all incoming and outgoing packets according to precisely defined criteria.
For routing, you can use RIP, OSPF or the multicast routing protocol PIM-SM. Comprehensive multicast support makes this gateway an excellent choice for multimedia and streaming applications.
Integrated quality of service allows you to prioritize your data. Put VoIP traffic ahead of normal Internet traffic to ensure your IP voice applications have sufficient bandwidth at all times. Or use the QoS functionality to give regular data priority over e-mail traffic.
The DNS proxy feature supports address translation on the LAN and the integrated DHCP server automates IP configuration on client PCs.

Comprehensive IPSec implementation

The RXL12500's IPSec implementation goes beyond preshared keys. We've also given you the ability to use certificates, as Germany's Federal Office for Information Security recommends. This lets you build a public key infrastructure for maximum security. Administrators can manage certificates conveniently and easily with a RADIUS server. Teldat even provides special functionality that makes it possible to implement a RADIUS dial-out solution.
Using the IKE Config Mode and Bintec IPSec Multi-User features, administrators can implement and administer IPSec dial-in solutions for a large number of clients with minimal effort.
IKE-X-Auth (extended authentication) lets you secure connections using a one-time password to achieve the highest level of security possible. The bintec IPSec implementation also assists you in establishing VPN connections with dynamic IP addresses, extending connectivity to small branch locations that may not be online all the time. Even if both VPN participants have dynamic IP addresses, they can still take advantage of secure communications. A dynamic DNS provider or a direct ISDN connection can facilitate the exchange of IP addresses. The dynamic IP address is sent either over the ISDN D-channel at no cost or, if this is not possible, over the B-channel (carrier charges may apply).

Load balancing / Redundancy

With the bintec RXL12500, you can configure multiple interfaces for WAN access. This not only provides more bandwidth, but also makes it possible to distribute data across individual WAN connections according to loads or data types. You can for instance use one internet connection on a 100 Mbps Ethernet port to establish VPNs for numerous branch locations and external staff members. A second WAN port can then provide cost-effective VDSL internet access for the rest of the company.
Our bintec Router Redundancy Protocol allows two routers to function on the LAN as if they were a single device. In addition to each unit having its own unique IP and MAC addresses for every interface, the two units are also assigned a shared virtual IP and MAC address. This virtual address is then entered as the standard gateway on all the computers on the LAN. The two linked gateways communicate with each other using the bintec protocol. If one of the units goes down, the other one automatically takes over and handles all the traffic.

Simple configuration and maintenance

Administrators can configure the gateway using the configuration assistants that are integrated into the Configuration Interface (FCI). The FCI is a web-based graphical user interface that can be accessed via HTTP or the encrypted HTTPS protocol from any PC with a current Web browser. Administrators can configure the RXL12500 locally or remotely using telnet, SSH, or an ISDN login.
The gateway's numerous monitoring options represent one of its main security features. You can query all the configuration parameters and status information via SNMP. You can also have this information sent from the Gateway to an SNMP manager via SNMP traps or create log files of syslog messages. Administrators can also choose to receive e-mail notifications of specific events.

bintec RXL-Series Performance

Frequently used at large and medium-sized corporate headquarters, the new bintec RXL-series devices boast exceptional IPSec encryption performance thanks to the integrated High End Encryption Engine.

The performance in a specific scenario, however, depends on packet size, the encryption algorithm, the number of active or configured tunnels, the firewall settings, and other factors. That makes it difficult to provide universally valid data transfer speeds. Depending on the configuration, the actual data rates can vary from specifications.

The information provided represents net transfer rates before taking into consideration any overhead resulting from TCP and UDP headers, Ethernet frames, etc.

The bintec RXL series devices were tested with software version 7.10.1. The IPSec Measurements of the RXL12500 were performed with activated Hardware Encryption. Measurements were performed using the SmartBits 600B network performance analysis system from Spirent.

IPSec-Performance (AES256) Data Throughput in Mbit/s per paket size (byte)						
Device	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

The Measurements of the RXL12500 were performed with activated Hardware Encryption.

Routing-Performance Data Throughput in Mbit/s per paket size (byte)						
Device	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

Variants

bintec RXL12500 (5510000235)	Central site enterprise VPN gateway, 19 inch rack, incl. 100 active IPSec tunnels (opt. max. active 2500 and HW encyption), 8 Gigabit Eth. switch, 2 * SFP module slots, 1 * USB, 1 * ISDN BRI, 1 GB RAM (opt. 4 GB RAM), opt. redundant power supply

Features

ISDN	
CAPI	CAPI 2.0 with CAPI user concept (password for CAPI use)

ISDN	
ISDN protocols	Euro-ISDN (Point-to-mulitpoint/Point-to-point), 1TR6 and other national ISDN protocols
ISDN auto-configuration	Automatic recognition and configuration of ISDN protocols
ISDN leased lines	Supported leased lines: D64S, D64S2, TS02, D64S2Y
B channel protocols	Excellent interoperability with other manufacturers (Raw HDLC, CISCO HDLC, X.75)
X.31 over CAPI	Support for various connection paths: X.31/A for ISDN D-channel, X.31/A+B for ISDN B-channel, X.25 within ISDN B-channel (also leased lines)
Bit rate adaption	V.110 (1,200 up to 38,400 bps), V.120 up to 57,600 kbps (HSCSD) for connection to GSM subscribers

VPN	
Number of PPTP tunnels	Inclusive 100 active PPTP tunnels, optional up to 1000 PPTP tunnels
Number of L2TP/GRE tunnels	Inclusive 1000 active L2TP and GRE v.0 tunnels (also in combination possible)
IPSec	Internet Protocol Security establishing of VPN connections
Number of IPSec tunnels	Inclusive 100 active IPSec tunnels, optional up to 2500 IPSec tunnels
IPSec Algorithms	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, RipeMD160, Tiger192 Hashes
IPSec hardware acceleration	Optional hardware acceleration for IPSec encryption algorithms DES, 3DES, AES and hardware acceleration for MD-5, SHA-1 Hash generation
IPSec IKE	IPSec key exchange via preshared keys or certificates
IPSec IKE Config Mode	IKE Config Mode server enables dynamic assignment of IP addresses from the address pool of the company. IKE Config Mode client enables the router, to get assigned dynamically an IP address.
IPSec IKE XAUTH (Client/Server)	Internet Key Exchange protocol Extended Authenticaion client for login to XAUTH server and XAUTH server for loging of XAUTH clients
IPSec IKE XAUTH (Client/Server)	Inclusive the forwarding to a RADIUS-OTP (One Time Password) server (supported OTP solutions see www.teldat.de).
IPSec NAT-T	Support of NAT-Traversal (Nat-T) for the application at VPN lines with NAT
IPSec IPComp	IPSec IPComp data compression for higher data throughput via LZS
IPSec certificates (PKI)	Support of X.509 multi-level certificates compatible to Micrososft and Open SSL CA server; upload of PKCS#7/8/10/12 files via TFTP, HTTP, HTTP, LDAP, file upload and manual via FCI
IPSec SCEP	Certificates management via SCEP (Simple Certificate Enrollment Protocol)
IPSec Certificate Revocation Lists (CRL)	Support of remote CRLs on a server via LDAP or local CRLs
IPSec Dead Peer Detection (DPD)	Continuous control of IPSec connection
IPSec dynamic IP via ISDN	Transmission of dynamic IP address in ISDN D or B channel; free-of-charge licence necessary
IPSec dynamic DNS	Enables the registering of dynamic IP addresses by a dynamic DNS provider for establishing a IPSec connection.
IPSec RADIUS	Authentication of IPSec connections at a RADIUS server. Additionally the IPSec peers, which were configured on a RADIUS server, can be loaded into the gateway (RADIUS dialout).

VPN	
IPSec Multi User	Enables the Dial-in of several IPSec clients via a single IPSec peer configuration entry
IPSec QoS	The possibility to operate Quality of Service (traffic shaping) inside of an IPSec tunnel
IPSec NAT	By activating of NAT on an IPSec connection it is possible, to implement several remote locations with identical local IP addess networks in different IP nets for the VPN connection

Security	
NAT/PAT	Symmetric Network and Port Address Translation (NAT/PAT) with randomly generated ports inclusive Multi NAT (1:1 translation of whole networks)
Policy based NAT/PAT	Network and Port Address Translation via different criteria like IP protocols, source/destination IP Address, source/destination port
Policy based NAT/PAT	For incoming and outgoing connections and for each interface variable configurable
Stateful Inspection Firewall	Packet filtering depending on the direction with controling and interpretation of each single connection status
Packet Filter	Filtering of IP packets according to different criteria like IP protocols, source/destination IP address, source/destination port, TOS/DSCP, layer 2 priority for each interface variable configurable

Routing	
Policy based Routing	Extended routing (Policy Based Routing) depending of diffent criteria like IP protocols (Layer4), source/destination IP address, source/destination port, TOS/DSCP, source/destination interface and destination interface status
Multicast IGMP	Support of Internet Group Management Protocol (IGMP v1, v2, v3) for the simultaneous distribution of IP packets to several stations
Multicast IGMP Proxy	For easy forwarding of multicast packets via dedicated interfaces
Multicast Routing Protocol PIM SM	Protocol Independent Multicast (PIM) distributes information via a central Rendezvous Point Server. PIM Modus Sparse Mode (SM) forwards only packets to groups which have been requested
Multicast inside IPSec tunnel	Enables the transmission of multicast packets via an IPSec tunnel
RIP	Support of RIPv1 and RIPv2, separated configurable for each interface
Extended RIP	Triggerd RIP updates according RFC 2091 and 2453, Poisened Rerverse for a better distribution of the routes; furthermore the possibility to define RIP filters for each interface.
OSPF	Support of the dynamic routing protocol OSPF
BGP4	On request

Protocols / Encapsulations	
PPP/MLPPP	Support of Point to Point Protocol (PPP) for establishing of standard PPP connections, inclusive the Multilink extension MLPPP for the bundeling of several connections
PPPoE (Server/Client)	Point-to-Point Protocol over Ethernet (Client and Server) for establisching of PPP connections via Ethernet/DSL (RFC 2516)

Protocols / Encapsulations

MLPPPoE (Server/Client)	Multilink extension MLPPPoE for bundeling several PPPoE connections (only if both sides support MLPPPoE)
DNS	DNS client, DNS server, DNS relay and DNS proxy
DYN DNS	Enables the registering of dynamic assigned IP addresses at adynamic DNS provider, e.g. for establishing of VPN connections
DNS Forwarding	Enables the forwarding of DNS requests of free configurable domains to assigned DNS server.
DHCP	DHCP Client, Server, Proxy and Relay for siplified TCP/IP configuration
Packet size controling	Adaption of PMTU or automatic packet size controling via fragmentation

Quality of Service (QoS)

Policy based Traffic Shapping	Dynamic bandwidth management via IP traffic shaping
Bandwidth reservation	Dynamic reservation of bandwidth, allocation of guaranteed and maximum bandwidths
DiffServ	Priority Queuing of packets on the basis of the DiffServ/TOS field
Layer2/3 tagging	Conversion of 802.1p layer 2 priorisation information to layer 3 diffserv attributes
TCP Download Rate Control	For reservation of bandwidth for VoIP connections

Redundancy / Loadbalancing

BRRP	Bintec Router Redundancy Protocol for backup of several passive or active devices with free selectable priority
BoD	Bandwidth on Demand: dynamic bandwidth to suit data traffic load
Load Balancing	Static and dynamic load balancing to several WAN connections on IP layer
VPN backup	Simple VPN backup via different media. Additional enables the Teldat interface based VPN concept the application of routing protocols for VPN connections.

Layer 2 Functionality

Bridging	Support of layer 2 bridging with the possibility of separation of network segment via the configuration of bridge groups
VLAN	Support of up to 255 VLAN (Virtual LAN) per LAN Interface for segmentation of the network in independent virtual segments (workgroups)
Proxy ARP	Enables the router to answer ARP requests for hosts, which are accessible via the router. That enables the remote clients to use an IP address from the local net.

Logging / Monitoring / Reporting

Logging / Monitoring / Reporting

Internal system logging	Syslog storage in RAM, display via web-based configuration user interface (http/https), filter for subsystem, level, message
External system logging	Syslog, several syslog server with different syslog level configurable
E-Mail alert	Automatic E-Mail alert by definable events
SNMP traps	SNMP traps (v1, v2, v3) configurable
Activity Monitor	Sending of information to a PC on which Brickware is installed
IPSec monitoring	Display of IPSec tunnel and IPSec statistic; output via web-based configuration user interface (http/https)
Interfaces monitoring	Statistic information of all pysical and logical interfaces (ETH0, ETH1, SSIDx, ...), output via web-based configuration user interface (http/https)
ISDN monitoring	Display of active and past ISDN connections; output via web-based configuration user interface (http/https)
IP accounting	Detailed IP accounting, source, destination, port, interface and packet/bytes counter, transmission also via syslog protocol to syslog server
ISDN accounting	Detailed ongoing recording of ISDN connection parameter like calling number and charging information, transmission also via syslog protocol to syslog server
RADIUS accounting	RADIUS accounting for PPP, PPTP, PPPoE and ISDN dialup connections
Keep Alive Monitoring	Control of hosts/connections via ICMP polling
Tracing	Detailed traces can be done for different protocols e.g. ISDN, PPPoE, ... generation local on the device and remote via DIME Manager
Tracing	Traces can be stored in PCAP format, so that import to different open source trace tools (e.g. wireshark) is possible.

Administration / Management

RADIUS	Central check of access authorization at one or several RADIUS server, RADIUS (PPP, IPSec inclusive X-Auth and login authentication)
RADIUS dialout	On a RADIUS server configured PPP und IPSec connection can be loaded into the gateway (RADIUS dialout).
TACACS+	Support of TACACS+ server for login authentication and for shell comando authorization
Time synchronization	The device system time can be obtained via ISDN and from a SNTP server (up to 3 time server configurable). The obtained time can also be transmitted per SNTP to SNTP clients.
Automatic Time Settings	Time zone profiles are configurable. That enables an automatic change from summer to winter time.
Supported management systems	DIME Manager, XAdmin
Configurable scheduler	Configuring of time and event controlled tasks, e.g. reboot device, activate/deactivate interface, activate/deactivate WLAN, trigger SW update and configuration backup

Administration / Management

Configuration Interface (FCI)	Integrated web server for web-based configuration via HTTP or HTTPS (supporting self created certificates). This user interface is by most of Teldat GmbH products identical.
Software update	Software updates are free of charge; update via local files, HTTP, TFTP or via direct access to the Teldat web server
Remote maintenance	Remote maintenance via telnet, SSL, SSH, HTTP, HTTPS and SNMP (V1,V2,V3)
Configuration via serial interface	Serial configuariton interface is available
ISDN remote maintenance	Remote maintenance via ISDN dial-in with checking of the calling number. The ISDN remote maintenance connection between two Teldat devices can be encrypted.
ISDN remote maintenance	A transparent mode enables transmissions of configurations and software updates respectively
GSM remote maintenance	Remote maintenance via GSM login (external USB UMTS (3G) modem required)
Device discovery function	Device discovery via SNMP multicast.
On The Fly configuration	No reboot after reconfiguration required
SNMP	SNMP (v1, v2, v3), USM model, VACM views, SNMP traps (v1, v2, v3) configurable, SNMP IP access list configurable
SNMP configuration	Complete management with MIB-II, MIB 802.11, Enterprise MIB
Configuration export and import	Load and save configurations, optional encrypted; optional automatic control via scheduler
SSH login	Supports SSH V1.5 and SSH V2.0 for secure connections of terminal applications
HP OpenView	Integration into Network Node Manager
CA Spectrum	Integration into CA SPECTRUM Infrastructure Manager
XAdmin	Support of XAdmin roll out and configuration managemant tool for larger router installations (IP+ISDN+GSM)

Interfaces

USB 2.0 host	USB 2.0 full speed host port for connecting LTE(4G) or UMTS(3G) USB sticks (supported sticks: see www.teldat.org)
Ethernet	8 x 10/100/1000 Mbps Ethernet Twisted Pair, autosensing, Auto MDI/MDI-X, all Ethernet ports can be configured as LAN or WAN.
SFP Slot	2 x SFP slots for conventional optical 10/100/1000 Mbps Ethernet SFP module, all SFP ports can be configured as LAN or WAN.
USB console	USB console interface
Serial console	Serial console interface / COM port (mini USB)
ISDN Basic Rate (BRI)	1 x BRI (TE), 2 B channels

Hardware

19 inch	Mountable in 19 inch rack, incl. 19 inch rack mount kit
Realtime clock	System time persists even at power failure for some hours.

Hardware

Environment	Temperature range: Operational 0°C to 40°C; storage -10°C to 70°C; Max. rel. humidity 10 - 95% (non condensing)
Power supply	Integrated wide range power supply 110-240V, with energy efficient swiching controller
Power consumption	Max. 40 Watt, typ. 30 Watt
Housing	19 inch 1 high unit metal case, screw-on 19 inch mounting-angle, LEDs and network connectors at front side
Dimension	Ca. 485.6 mm x 220 mm x 45 mm (W x H x D)
Weight	Ca. 2700g
Reset button	Restart or reset to factory state possible
Status LEDs	Power, Status, ISDN, 20 * Ethernet
Standards and certifications	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

Content of Delivery

Manual	Quick Installation Guide in German and English
DVD	DVD with system software, management software and documentation
Ethernet cable	1 Ethernet cable, 3m
Network cable	Power cable
Serial cable	Serial cable (mini USB - DSUB 9 female)
USB cable	USB cable (Type A - Type B)
ISDN (BRI/S0) cable	ISDN (BRI/S0) cable, 3m

Service

Warranty	2 year manufacturer warranty inclusive advanced replacement
Software Update	Free-of-charge software updates for system software (BOSS) and management software (DIME Manager)

Options

IP address ISDN B/D channel license	Free of charge license for IP address transmission in ISDN D or B channel for IPSec connections; registering under www.teldat.de required.

Accessoires

WLAN Controller

License WLAN Contr. 6AP (5500000943)	WLAN Controller license for 6 Access Points (APs) or for the extension with 6 APs for the products: Rxxx2 and RXL12x00.

Software Licenses

Rxx02/RTxx02/RXL12xxx-IPSEC25 (5500000781)	Additional 25 IPSec tunnel license for Rxx02, RTxx02 and RXL12xxx series
RXL12xxx-HW-ENC (5500001161)	RXL12500 license to activate IPSec hardware encryption
RXL12xxx-IPSEC100 (5500001162)	RXL series license for 100 additional active IPSec tunnels
RXL12xxx-IPSEC400 (5500001163)	RXL12500 series license for 400 additional active IPSec tunnels
RXL12xxx-IPSEC1000 (5500001164)	RXL12500 series license for 1000 additional active IPSec tunnels
RXL12xxx-PPTP25 (5500001203)	RXL series license for 25 additional active PPTP tunnels

Pick-up Service / Warranty Extension

Service Package 'extra large' (5500001187)	Warranty extension of 3 years to a total of 5 years, including advanced replacement for Teldat products of the category 'extra large'. Please find a detailed description as well as an overview of the categories on www.teldat.de/servicepackages.

Power Supply

bintec PSU XL (5510000294)	External redundant power supply unit for up to 2 bintec RXL12xxx, 19 inch rack