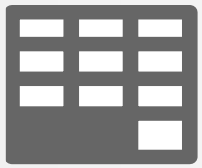
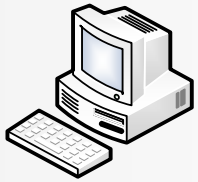
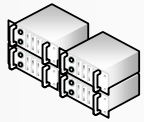
Zentrales VPN Gateway **Netz A**
verbunden mit dem Internet
Zugriff auf **Netze B /C /D /E**

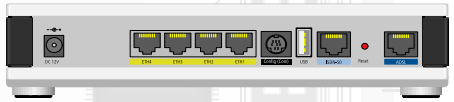




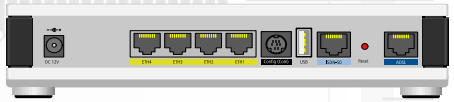


Server / Anwendungen MSR GLT Daten **Netz A bis E**

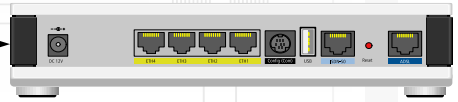
Internet



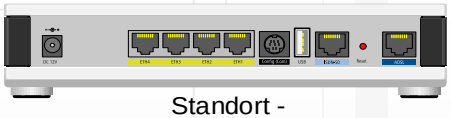
Standort -
VPN Router **Netz B**



Standort -
VPN Router **Netz C**



Standort -
VPN Router **Netz D**



Standort -
VPN Router **Netz E**

Zugriff über
mobile Device
möglich **PIN-Verfahren** zur
Authentisierung
und beim VPN-
Tunnelaufbau

Home Office / Mobiler Mitarbeiter
VPN Client Verbindung zum VPN Gateway Zugriff **Netz A**
verbunden mit dem Internet
Zugriff auf **Netze B /C /D /E (Zugriffskontrolle möglich über Firewall- Regeln)**

VPN Netzwerke (**V**irtuelle **p**rivate **N**etzwerke) gewinnen immer mehr an Bedeutung.

Ihr extrem hoher Sicherheitsstandard (IPSec-VPN) erlaubt die Vernetzung von bis zu 1000 Standorten. Dabei wird ein Verfahren mit AES 256Bit-Verschlüsselung angewandt. Es handelt sich dabei um eine transparente Anbindung der IP-basierten Technik.

Vorteilhaft ist, dass Mitarbeiter jederzeit zentral auf alle angeschlossenen Standorte zugreifen und Systemmeldungen bearbeiten können.

Auch Außendienstmitarbeiter können mit der **VPN Client Software** einen hochsicheren, verschlüsselten Zugang zum Unternehmensnetzwerk herstellen.

IPsec kapselt die ursprünglichen IP-Daten in eigene Pakete ein und versteckt somit alle applikationsbezogenen Informationen im VPN-Tunnel. Ist dieser aufgebaut, können die unterschiedlichsten Formen des IP Datenverkehrs darüber abgewickelt werden, u.a. auch gängige Bussysteme wie Modbus, BACnet und LON, die im Bereich GLT/MSR Technik eingesetzt werden. Dies gilt auch für die Kommunikation zu unterschiedlichen Netzwerkteilnehmern, sofern sie sich hinter einem VPN-Gateway befinden. IPsec schützt die gesamten Verbindungen.

R.T. systemtechnik GmbH