

Themenschwerpunkte in diesem Artikel sind das Routing und die Sicherheit der Daten. Wir zeigen auf, welche Übertragungsverfahren und Sicherungsmethoden zu einem störungsfreien und planvollen Betrieb zusammenwirken. Die Manipulation von Daten zur Steuerung abgesetzter Produktionsanlagen (M2M, BDE) oder bei der Abwicklung des Zahlungsverkehrs mit Kreditkarten am Point of Sale (POS) kann im Vergleich zum Verlust einer E-Mail mit Geburtstagsgrüßen existenzielle Ausmaße annehmen. Mit multifunktionalen Routern und hochsicheren VPN-Technologien lassen sich schnell und einfach preiswerte Remote-Services realisieren.

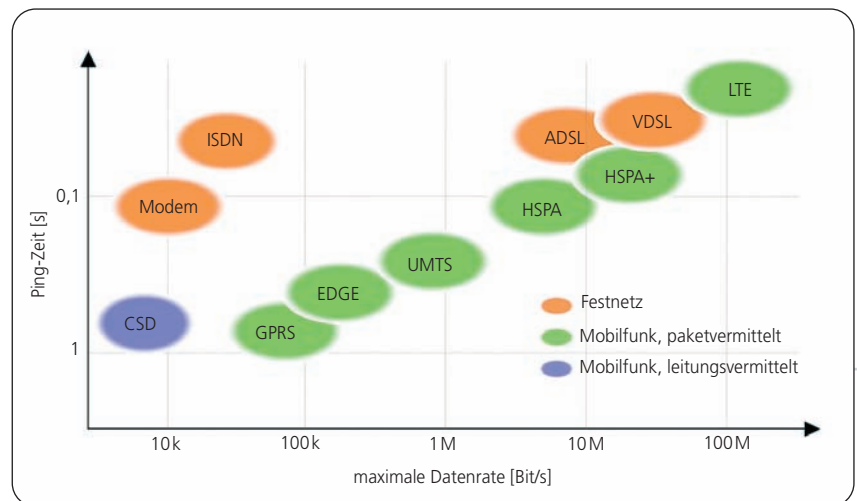
Der Facettenreichtum der Anwendungen in allen Branchen scheint grenzenlos und immer mehr Informationen und Geräte können »online« verfügbar sein. Da werden täglich Ticketverkaufszahlen und Betriebsdaten (BDE) von Liftstationen großräumiger Skigebiete per DSL zur Speicherung und Auswertung an einen zentralen Server übertragen. Im »Internet der Dinge« kommunizieren »aktive Maschinen« miteinander (M2M), um Material nachzubestellen, Mitarbeiter überwachen Prozesse von Fertigungsanlagen und vom Hersteller einer Maschine wird wie selbstverständlich erwartet, dass er zur Inbetriebnahme, Wartung oder Entstörung für sofortige Hilfe mit den passenden Remote-Services parat steht. Mit der Relevanz der Daten für den störungsfreien Betrieb steigt die Notwendigkeit effektiver Sicherungsmaßnahmen bei der Datenübertragung. Deshalb haben Störungen im Datenverkehr eine immer größere Tragweite.

Im Beitrag »In die Ferne schweifen« zur Fernwirktechnik in »de« 1-2/2010 standen der Umbau der traditionellen Telefonnetze zu paketvermittelten Infrastrukturen (NGN), die Datendienste der GSM- und UMTS-Mobilfunknetze sowie die Schnittstellen weit verbreiteter Feldgeräte (RS 232, Ethernet, Zustände von Schaltern) im Vordergrund. Im Vergleich der theoretisch erreichbaren Datenübertragungsraten und Latenzzeiten, s. Bild 1, werden sich die öffentlichen Fest- und Mobilfunknetze zukünftig auf Augenhöhe begegnen. Im November 2009 ergaben Mobilfunk-Feldtests mit HSPA+ auf dem Münchner Marienplatz Datenraten bis zu 15Mbit/s im Download und

# Fernwartung: Aber sicher

## Aspekte und Details zur störungsfreien und gesicherten Datenübertragung

Die wachsende Verfügbarkeit schneller Datennetze zu erschwinglichen Kosten – egal ob leitungsgebunden oder per Funk – beflügelt den Einsatz von Remote-Lösungen. Die modernen Datennetze übernehmen das Routing, die Vermittlung und die Zustellung der Datenpakete. Für die Erfüllung der Schutzziele in der Informationssicherheit wie Vertraulichkeit, Sabotage- und Spionageschutz, Integrität und Verfügbarkeit sind Sender und Empfänger weitgehend selbst verantwortlich.



**Bild 1:** Trotz der immer noch unverbindlichen Dienstgüte beim QoS-Merkmal »Transferverzögerung« werden die Ping-Zeiten (round trip time) zunehmend tauglicher für zeitkritische Anwendungen

bis zu 2,6Mbit/s im Upload; die Latenzzeiten lagen zwischen 26 ... 58ms. Damit liegt HSPA+ – zumindest unter Feldtestbedingungen – zwischen ADSL und VDSL 25000. LTE (Long Term Evolu-

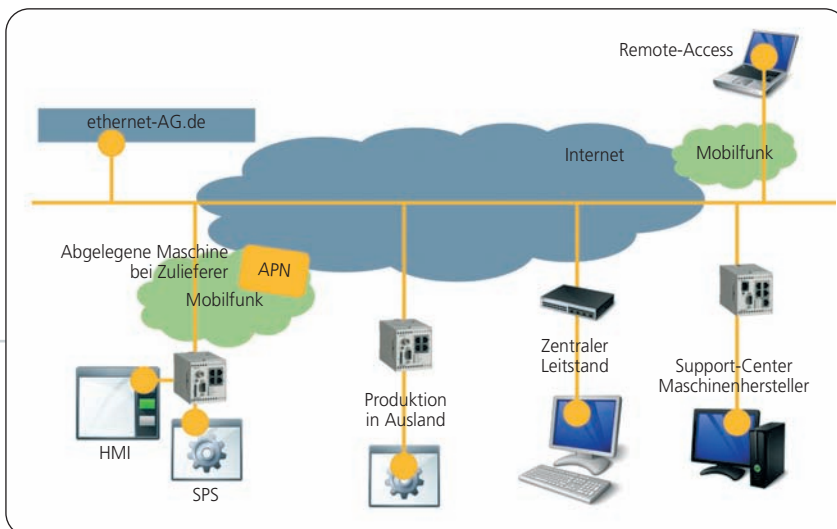
tion; Mobilfunkstandard derzeit noch in Entwicklung) verspricht gar Spitzenraten von 100 ... 300Mbit/s im Downlink und 50 ... 75Mbit/s im Uplink mit Latenzzeiten unter 5ms.

## ERFOLGSFAKTOREN VON M2M-LÖSUNGEN

Eine enge Zusammenarbeit zwischen Lösungspartner, Netzbetreiber und Kunden ist der Schlüssel zu einer unkomplizierten und erfolgreichen Planung und Umsetzung von M2M-Lösungen. Zudem ist der Erfolg einer M2M-Lösung oftmals auch von folgenden Faktoren abhängig:

- Integrationsfähigkeit in bestehende Systeme
- Homogene Infrastrukturen (Netze und Protokolle) schaffen eine Durchgängigkeit von der SPS bis Leitstand und Software Backend

- Ein erweitertes Einsatzspektrum, die finanzielle Planbarkeit der anfallenden Kosten für den Betrieb (Datentarife im Mobilfunk) und die Option auf neuartige Dienstleistungen schaffen Investitionssicherheit
- Einfache Bedienbarkeit als klarer Mehrwert
- Gesellschaftsfähigkeit (Akzeptanz)
- Adäquate Hardware, denn günstige Hardware oder falsche Tarifwahl kann unter Umständen wesentlich höhere Kosten erzeugen.



**Bild 2: Mit multifunktionalen und industrietauglichen Routern, die hochsichere VPN-Technologien beherrschen, lassen sich schnell und einfach preiswerte Remote-Services realisieren**

### Unicast, Multicast und Broadcast

Im Unterschied zu den Datenströmen bei seriellen oder Wählverbindungen, mit physikalisch fest verdrahteten oder vermittelten Punkt-zu-Punkt-Verbindungen, können die Daten in paketvermittelten Infrastrukturen verschiedene Ziele haben. Zum Einsatz kommen folgende Verfahren:

- »Unicast« ist eine logische Punkt-zu-Punkt-Verbindung, die zur Datenübertragung zwischen zwei Endgeräten herstellt.
- »Multicast« wird eingesetzt, wenn eine Information gleichzeitig an mehrere ausgewählte Teilnehmer gesendet werden soll.

rere ausgewählte Teilnehmer gesendet werden soll.

- »Broadcast« kommt in einem Computernetz vorwiegend dann zum Einsatz, wenn die Adresse des Empfängers noch unbekannt ist; ein Beispiel dafür sind die Protokolle ARP (Adress resolution protocol) und DHCP. Ebenso dient ein Broadcast zur effizienten Übermittlung von Informationen an alle Geräte eines Netzes. Besonderheit: IPv6-Netzwerke (vgl. Artikel »In die Ferne schweiften«) unterstützen keine Broadcasts mehr, sondern verwenden stattdessen Multicasts.

### Routing – das moderne »Fräulein vom Amt« mit innovativen Zusatzfunktionen

Damit jedes Datenpaket schnell und zuverlässig an seinen Empfänger weitergeleitet werden kann, führt es sein Ziel als IP-Adresse mit sich. Router an den Knotenpunkten der Weitverkehrsnetzwerke »kennen« die passenden Verbindungswege und vermitteln alle Datenpakete zum jeweils richtigen Empfänger – insofern ist dies im Ansatz vergleichbar mit dem früheren »Fräulein vom Amt«. »Routing« im Sinn der Verkehrslenkung in Datennetzen wird durch zwei Funktionen charakterisiert:

- erstens durch die Wahl der Zugangswege und
- zweitens durch die Wahl des optimalen Weges für die zu transportierenden Datenpakete von Netzknoten zu Netzknoten unter Verwendung der Ressourcen des Netzes (Forwarding). Das »Routing« liegt mit der Wahl der Zugangswege (leitungsgebundener DSL-Anschluss, Mobilfunknetz etc.) in der Hand des Anwenders. Die Funktion des »Forwarding« leisten Router an den Netzknoten der Datennetze eigenständig auf Basis der vielfältigen Verfahren (statistisch, dynamisch, deterministisch, stochastisch etc.). Damit bestimmen sie, über welchen benachbarten Netzknoten ein Datenpaket weitergeleitet wird.

Wegen dieser unterschiedlichen Wege und wegen unterschiedlicher Laufzeiten durch die vermaschten Netze, können sich Datenpakete »überholen« und beim Empfänger in der verkehrten Reihenfolge ankommen. TCP als Übertragungssteuerungsprotokoll (Schicht 4 im OSI-Modell) sorgt mit der »Sequence Number« (inkrementierte Ordnungsnummer) im TCP-Header nicht nur für die Flusskontrolle, sondern auch dafür, dass die Datenpakete stets in der richtigen Reihenfolge an die empfangsseitige Anwendung übergeben werden.

Als Beispiel für Routing zeigt **Bild 2** eine SPS-Applikation mit HMI als Client im Feld, die sich über das Mobilfunknetz, den APN des Mobilfunkproviders und das Internet mit dem zentralen Leitstand über dessen öffentliche IP-Adresse verbindet. Der Leitstand ist über sein LAN und seinen Firmenrouter, über DSL und seinen Internetprovider, im Internet mit seiner öffentlichen IP-Adresse erreichbar. Dabei kann er im Internet eine »feste« öffentliche IP-Adresse haben oder einen DynDNS-Dienst nutzen, der ihm eine finanziell

## ANGRIFFE AUF PROTOKOLLE/NETZSTRUKTUREN

### Angriffe auf Netzwerkprotokolle

- **Man-in-the-Middle-Angriff:** Wird keine gegenseitige Authentifizierung durchgeführt, kann sich ein Angreifer zwischen die Kommunikationspartner einschalten und dem einen jeweils den anderen vortäuschen (z. B. telnet, rlogin, SSH, GSM, Cisco XAUTH).
- **Unerlaubte Ressourcennutzung:** Ist keine sichere Authentifizierung bzw. sichere Autorisierung vorhanden, kann ein Angreifer unberechtigt Ressourcen nutzen (z. B. rlogin)
- **Mitlesen von Daten und Kontrollinformationen:** Dies betrifft alle unschlüsselten Protokolle (z. B. POP3, IMAP, SMTP, Telnet, rlogin, http)
- **Einschleusen von Daten oder Informationen:** Betroffen sind alle Protokolle ohne ausreichende Nachrichtenaufentifizierung (z. B. POP3, SMTP, Telnet, rlogin, http).

### Angriffe auf die Netzstruktur

- **Denial of Service (DoS):** Die Dienstüberlastung wird als DoS-Angriff bezeichnet. Besonders schädigend sind Angriffe, die mit nur einem Paket auskommen (z. B. TCP-SYN-Angriff), denn damit kann die Absenderadresse – und somit die Herkunft – gefälscht werden.

### Begünstigte Angriffe

- **Social Engineering:** Eine Person dazu zu bringen, ein Passwort oder einen Schlüssel zu verraten, wird Social Engineering genannt.
- **»Schwache« Zugangsdaten:** Standardpasswörter können einen Angriff erfolgreich machen.
- **Leichtgläubigkeit:** Von externen Quellen stammende Daten werden ungeprüft als »korrekt« übernommen (Validität, Tainted Data oder Cross-Site Scripting und SQL Injection).

günstigere »dynamische« öffentliche IP-Adresse zuweist. Über den zugehörigen Domainnamen wie z.B. »company.dyndns.org« ist der Leitstand auch mit der wechselnden (dynamischen) IP-Adresse für die Clients im Feld erreichbar.

### NAT und Portforwarding

NAT ist ein Verfahren am Übergang zwischen zwei Datennetzen. Damit können Rechner und andere Ethernet-Geräte eines LAN (privates Netzwerk) auch ohne eigene öffentliche IP über einen Router mit Zielen im Internet (WAN) kommunizieren. Dieser Router stellt als Standard-Gateway den Zugang zum WAN bereit und ersetzt dabei in den Datenpaketen des Absenders dessen private IP-Adresse (z.B. 192.168.200.63) durch seine öffentliche IP-Adresse (z.B. 212.77.187.24). Dies merkt er sich dieses in einer NAT-Tabelle. Durch diese eindeutige Zuordnung können die Geräte des LANs eine Verbindung zu Zielen im Internet aufzubauen und sind für deren Antworten aus dem Internet erreichbar.

Dieses Verfahren wird als Source Network Address Translation (SNAT) bezeichnet. Es hat den Vorteil, dass für Rechner, die innerhalb eines privaten Netzes miteinander kommunizieren müssen, keine öffentlichen IP-Adressen benötigt werden. Ein weiterer Vorteil ist, dass die interne Struktur des Firmennetzwerkes nach außen verborgen bleibt.

Im umgekehrten Fall kann der Router die Datenpakete von eingehenden Verbindungsanfragen von Quellen aus dem Internet, die in seiner NAT-Tabelle nicht bekannt sind, an keinen Rechner im LAN weiterleiten. Dies ist gewollt, um das LAN vor unerwünschten und unsicheren Quellen aus dem Internet zu schützen. Damit bei eingehenden Anfragen eine gewollte Kommunikation stattfinden kann, gibt es »Portforwarding« – nicht zu verwechseln mit dem oben genannten »Forwarding«. Dabei wird der IP-Adresse eines LAN-Teilnehmers (Rechner, SPS: seriell oder Ethernet) bei der Routerkonfiguration ein TCP-Port des Routers zugewiesen. Ein Port ist dabei wie die Durchwahl in einer Telefonanlage. Damit kann der Router auf diesem Port eingehende Datenpakete, wie z.B. an 212.77.178.24: 1194, an das vorbestimmte Gerät im LAN weiterleiten. Das Verfahren bei »Portforwarding« wird als Destination

### SSL HEISST JETZT TLS

Secure Sockets Layer (SSL) oder Transport Layer Security (TLS) ist ein hybrides Verschlüsselungsprotokoll zur Datenübertragung im Internet. SSL wird nun

unter dem Namen TLS weiterentwickelt. TLS 1.0, 1.1 und 1.2 sind die standardisierten Weiterentwicklungen von SSL 3.0 (TLS 1.0 steht neu für SSL 3.1).

### REMOTE SERVICES IM ÜBERBLICK

**Betriebsdatenerfassung (BDE):** operating data logging  
**Ferndiagnose:** remote diagnostics  
**Fernentstörung:** remote debugging

**Fernüberwachung:** remote monitoring  
**Fernwartung:** remote maintenance  
**Fernzugriff:** remote access

Network Address Translation (DNAT) bezeichnet.

Bei beiden Verfahren wissen weder der Rechner im LAN noch der Host im Internet von der NAT-Tabelle im Router und dem Tausch der IP-Adressen. Für LAN-Geräte ist der Router als Standard-Gateway der Empfänger der Datenpakete. Für den Host im Internet scheinen die Pakete vom Router mit NAT-Funktion direkt zu kommen – er weiß nicht, dass »hinter dem Router« ein LAN und/oder LAN-Teilnehmer wie SPS oder Workstation existieren

### Multifunktionale Router für heterogene IT-Szenarien

Im professionellen und industriellen Bereich stellen gewachsene IT- und Kommunikationsstrukturen vielfältige Anforderungen an universell einsetzbare Router. Neben der kompakten Ausführung zur Hutschienenmontage in Schaltschränken sollen sie sehr einfach in bestehende Systeme und Anla-

gen integriert werden können und damit mittel- und langfristig homogene Infrastrukturen (Netze und Protokolle), von der SPS bis zum Backend (Hard- und Software) im Leitstand schaffen. Multifunktionale Router sollen »nach innen« die klassische serielle Schnittstelle für ältere SPS-Installationen oder Sensoren ebenso bedienen können wie moderne Ethernetschnittstellen mit einem Mehrportswitch, sollen DHCP-Server sein und die Adresse des DNS-Servers kennen (DNS-Relay). Die Kommunikation »nach außen« soll wahlweise über ein Modem am analogen Telefonanschluss, über ISDN, direkt über ein DSL-Modem ins Internet (WAN) oder eines der modernen Mobilfunknetze erfolgen. Im besten Fall kann ein Router über die verschiedenen Standards wie CSD, GPRS, EDGE, HSDPA der GSM- und UMTS-Netze kommunizieren. CSD (Circuit Switched Data) ist der leitungsvermittelte Datenübertragungsdienst in GSM-Netzen mit 9,6 Kbit/s; siehe Bild 1.

### NORMEN ZUR SICHERHEIT IN DATENNETZEN

Bei Wählverbindungen und Standleitungen innerhalb der öffentlichen Fest- und Mobilfunk-Telefonnetze ist die sichere Datenübertragung durch das Übertragungssystem selbst gegeben. Bei der Nutzung des unsicheren Internets für professionelle Anwendungen – wenn auch nur als Teilstrecke des Übertragungsweges – ist die Notwendigkeit für den Schutz der Daten inzwischen unbestritten.

Zudem ist die Sicherheit von Computernetzen Gegenstand internationaler Normen zur Qualitätssicherung. Wichtige Normen in diesem Zusammenhang sind vor allem die amerikanische TCSEC und die europäischen ITSEC-Standards sowie der neuere Common Criteria Stan-

dard. Die Zertifizierung der Sicherheit erfolgt in Deutschland in der Regel durch das Bundesamt für Sicherheit in der Informationstechnik. International spielen Vorschriften wie Basel II und der Sarbanes-Oxley Act eine wichtige Rolle.

Nicht zuletzt lassen sich Verpflichtungen zur Informationssicherheit im deutschsprachigen Raum aus verschiedenen Gesetzen zum Gesellschaftsrecht, Haftungsrecht, Datenschutz, Bankenrecht usw. herleiten.

Das war allerdings nicht immer so: Seit des Anfängen des Internets wurden und werden in aller Öffentlichkeit »vor den Augen der Internetgemeinde« ungeschützt Daten übertragen und brisante Zugangsdaten per E-Mail verschickt.

**SCHUTZZIELE – INFORMATIONSSICHERHEIT**

- 1. Vertraulichkeit**  
Beschränkter Empfänger/Empfängerkreis, Weitergabe und Veröffentlichung unerwünscht
- 2. Sabotage- und Spionageschutz**  
Absichtliche Störung eines Ablaufs, gewaltsame Beschädigung/Zerstörung von Geräten und Infrastrukturen
- 3. Integrität**  
Daten über einen bestimmten Zeitraum vollständig und unverändert »Schutz vor Verlust« und »Schutz vor vorsätzlicher Veränderung« durch verschlüsselte Prüfsumme
- 4. Verfügbarkeit**  
eines technischen Systems: das Maß/die Wahrscheinlichkeit, bestimmte Anforderungen innerhalb eines bestimmten Zeitrahmens zu erfüllen. Ist Qualitätskriterium:  
Verfügbarkeit = (Gesamtzeit – Gesamtausfallzeit) / Gesamtzeit

Die industrietauglichen Dial-in- und Dial-out-Router wie der MoRoS-UMTS von Insys Microelectronics erfüllen alle diese Anforderungen: Sie sind Modem, Router und Switch in einem Gerät. NAT, Port-Forwarding und ein 4+1-Port-Switch sind ebenso integriert sowie die Nutzung redundanter Verbindungswege zur Minimierung des Ausfallrisikos bei kritischen Anwendungen. Bereits in der Standardversion lassen sich zwei SIM-Karten unterschiedlicher Provider einsetzen. Die Fallback-Optionen auf alternative Verbindungen decken alle erforderlichen Leitungswege ab – notfalls spricht man ein externes Modem an.

Optionale Ziele und individuelle Parameter sind über ein leicht zu bedienendes Webinterface komfortabel konfigurierbar. Kundenspezifische Einstellungen können auf Wunsch bereits ab Werk konfiguriert werden. Die 2G- und 3G-Router im kompakten Hutschienengehäuse besitzen eine Firewall, beherrschen neben OpenVPN auch IPsec und

verfügen über ein redundantes WAN-Interface mit vorgegebener Priorisierung. Eine Desktopvariante ist als Baureihe MLR verfügbar.

Wie sich Daten durch einen VPN-Tunnel sicher und »incognito« durchs Internet transportieren lassen, erfahren Sie im nächsten Abschnitt.

**Virtual Private Network – zentrale Lösung mit geringem Verwaltungsaufwand**

Private Unternehmen und öffentliche Einrichtungen sind in vielen Bereichen – innerhalb ihrer Standorte oder weltweit – von Datenübertragung abhängig. Deshalb ist die Datensicherheit ein Baustein des Risikomanagements zu den Aspekten Betrug, Diebstahl, Systemausfall, Sabotage und Spionage dar. Details dazu sind im Kasten »Schutzziele« zusammengefasst.

Mit den mannigfaltigen Kombinationsmöglichkeiten verschiedener Übertragungswege und -geräte wird die Pla-

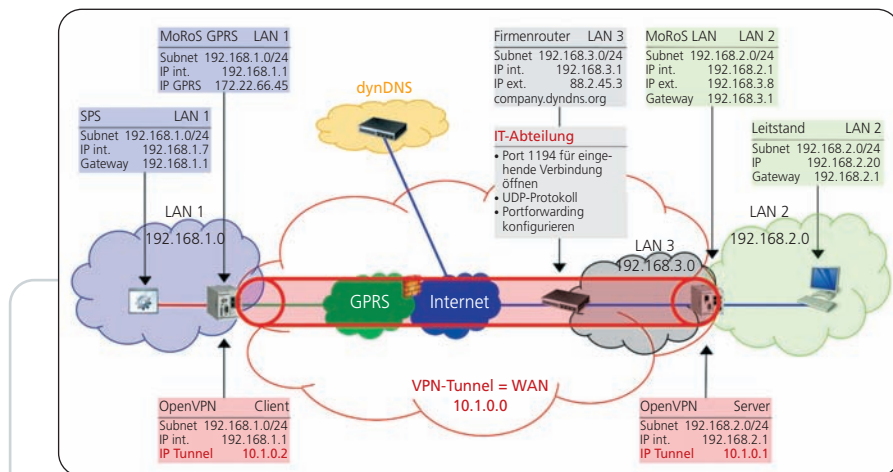
nung der Infrastrukturelemente zur Datenübertragung zunehmend aufwändiger. Allerdings ist die Steigerung der Datensicherheit auch ohne große Hürden für die Benutzer und mit moderatem Aufwand realisierbar. Die Vorsorgemaßnahmen für eine sichere und von Dritten nicht lesbare Kommunikation über ein unsicheres Netzwerk wie dem Internet sind ebenso vielfältig wie die Angriffsmöglichkeiten (siehe Kasten »Angriffe auf Protokolle/Netzstrukturen«). Dabei geht es im Grund um diese beiden Aspekte:

- hinreichende Verschlüsselung der Daten und
- Authentifizierung der beteiligten Kommunikationspartner.

Diese Eigenschaften können geeignete Protokolle (z.B. SSH, HTTPS, SFTP) dezentral erfüllen. Alternativ kann eine zentrale Stelle unabhängig von den einzelnen Anwendungen diese Sicherheitseigenschaften bereitstellen. Die Vorteile des zentralen Ansatzes liegen auf der Hand: die einmalige Implementierung der Sicherheitsfunktionen und der geringere Wartungsaufwand. Ein Virtual Private Network (VPN) ist eine solche zentral bereitgestellte Sicherung. OpenVPN ist eine von vielen Implementierungen eines VPNs zur sicheren Datenübertragung durch öffentliche Datennetze und kann mit weiteren Vorteilen punkten: Die OpenVPN-Software ist kostenlos und legt als Open-Source (lizenziert unter GPL 2) den Quellcode zur Prüfung durch jedermann offen. Vorkompilierte Programmpakete gibt es für verschiedene Betriebssysteme wie z.B. Linux, Solaris, OpenBSD, FreeBSD, NetBSD, Mac OS-X, und Windows 2000/XP/ Vista.

**VPN-Tunnel als Tarnkappe**

Ein VPN-Tunnel verbindet Rechner oder LANs über bereits bestehende Netzwerke. Beispiele für bestehende Netzwerke sind das Internet oder paketorientierte Datenübertragungsdienste von Mobilfunknetzen wie GPRS, EDGE, HSPA und UMTS. Die LANs an den beiden Tunnelenden haben dabei unterschiedliche IP-Adressbereiche wie z.B. 192.168.1.0/24 und 192.168.2.0/24; vgl. Bild 3. Damit lässt sich jedes Gerät an den beiden Enden des VPN-Tunnels vom jeweils anderen LAN aus eindeutig adressieren. Denkbar sind VPN-Verbindungen auch innerhalb eines Firmennetzes zur sicheren Übertragung von



**Bild 3: Ein VPN-Tunnel verbindet zwei LANs durch beliebig viele lokale und Weitverkehrsnetze für geschützte Datenkommunikation, wie ein langes Netzwerkkabel zur exklusiven Nutzung**

geheimen Daten im Bereich der Geschäftsleitung oder der Entwicklung.

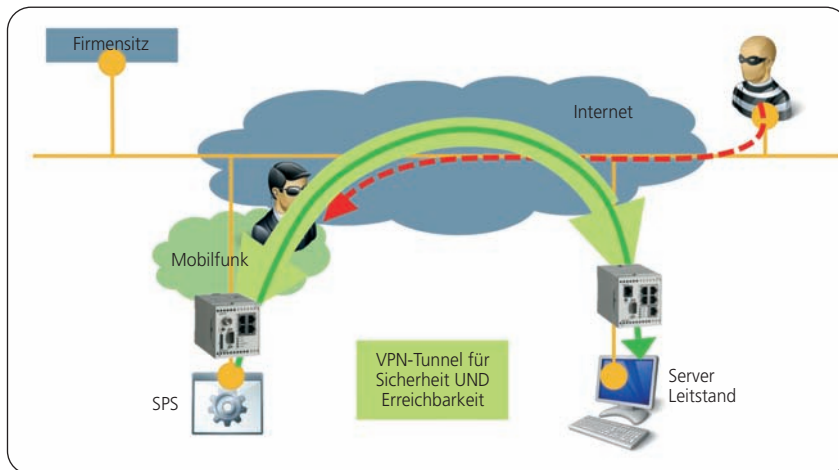
Zur Errichtung eines VPN ist grundsätzlich keine spezielle VPN-Hardware erforderlich. Die spezielle VPN-Software wiederum lässt sich auf Computern installieren oder ist bereits in Netzwerkkomponenten wie den Routern der MoRoS-Produktfamilie von Insys im Controller integriert. Weil dieser Tunnel eine logische Verknüpfung von Netzwerkkomponenten zur exklusiven und geschützten Nutzung darstellt, spricht man von »virtuell«. »Privat« ist ein VPN-Tunnel deshalb, da anderen Netzteilnehmern – egal ob Freund (Internetprovider) oder Feind (Hacker) – der Zugriff auf die im Tunnel übertragenen Daten verwehrt bleibt, siehe Bild 4.

Ein weiteres und mächtiges Merkmal eines VPN-Tunnels ist die Verschlüsselung der gesamten Verbindung zwischen zwei Punkten: dem VPN-Server und einem VPN-Client. Alle durch den Tunnel übertragenen Daten werden automatisch verschlüsselt. Damit entfällt die aufwendige Verschlüsselung jedes einzelnen Dienstes wie z.B. FTP. Deshalb vergleicht man ein VPN-Tunnel mit einer »geschlossenen Gesellschaft«: Nur ausgewählte Personen (Autorisierte) dürfen teilnehmen und erhalten nur durch Vorlage ihres Ausweises (Zertifikat) einen Zutritt.

### OpenVPN – kostenlose und NAT-Router-freundliche Open-Source-Lösung

Für die Verschlüsselung und Authentifizierung verwendet OpenVPN die OpenSSL-Bibliothek und nutzt dabei wie IPsec X.509-Zertifikate. Allerdings geht OpenVPN bei der Nutzung von TLS (siehe Kasten »SSL heißt jetzt TLS«) einen speziellen Weg und kann damit IP-Pakete und Ethernet-Frames inklusiv aller darüber liegenden Protokolle tunneln. OpenVPN bevorzugt für die Datenübertragung im Tunnel UDP, ein Protokoll ohne Flusskontrolle. Der Grund: Eine nochmalige Flusssteuerung der im VPN-Tunnel eingekapselten TCP/IP-Daten ist nicht erforderlich. Mit dieser Strategie vermeidet OpenVPN unerwünschten Overhead und spart damit kostenpflichtigen Datenverkehr (Traffic).

Auf der Empfängerseite arbeitet OpenVPN alle Schritte in umgekehrter Reihenfolge ab und leitet die Pakete weiter. Bei TLS wird der gesamte Verkehr über einen einzigen UDP-Port



**Bild 4: VPN-Tunnel mit dreifachem Nutzen: Sichere Datenübertragung durchs Internet, keine Chance für böswillige Angreifer und Erreichbarkeit der Mobilfunk-Feldgeräte**

abgewickelt. Dazu multiplext der Server – sowohl den TLS-Handshake als auch die verschlüsselten Pakete – auf eine Verbindung. Da OpenVPN weder die IP-Adresse noch die UDP-Portnummer des Paketes authentifiziert, bereiten NAT-Router auf dem Weg zum Empfänger keine Probleme. Clients mit dynamischen IP-Adressen (Road Warrior) bedient OpenVPN klaglos. Selbst der Server darf eine dynamische IP-Adresse haben. Dem Client reicht zum Erreichen des Servers beispielsweise die Angabe dessen DynDNS-Namens. Eine vollständige Beispiel-Konfiguration zeigt Bild 3.

Bevor allerdings ein OpenVPN-Tunnel aufgebaut werden kann, muss ein OpenVPN-Client seine Echtheit und Berechtigung gegenüber dem OpenVPN-Server nachweisen. Im Gegenzug kann auch der OpenVPN-Client eine Echtheitsprüfung des OpenVPN-Servers durchführen.

### Authentifizierung prüft Echtheit und Berechtigung

Jedes Gerät der MoRoS-Produktfamilie von Insys Microelectronics lässt sich in der PRO-Ausführung als OpenVPN-

Client oder OpenVPN-Server konfigurieren. Die Art der Authentifizierung für eine OpenVPN-Verbindung (ohne Authentifizierung, mit statischem Schlüssel oder mit zertifikatsbasierter Authentifizierung) legt man in der Konfiguration des OpenVPN-Servers fest.

Bei der zertifikatsbasierten Authentifizierung hat jeder Teilnehmer ein öffentliches Zertifikat und einen geheimen Schlüssel. So wie die Gäste der oben genannten »geschlossenen Gesellschaft« nur mit Autorisierung und Zertifizierung Zutritt erhalten, kann sich ein OpenVPN-Client in der Variante »Zertifikatsbasierte Authentifikation« erst nach dem erfolgreichen Absolvieren dieser Prozeduren, wie oben beschrieben, mit einem OpenVPN-Server verbinden und Daten übertragen.

Im praktischen Einsatz ist OpenVPN mit der zertifikatsbasierten Authentifizierung die derzeit einfachste Lösung für eine sichere Datenübertragung.

Dipl.-Ing. (FH) Robert Torscht,  
Insys Microelectronics GmbH

## MEHR INFOS

### Weiterführende Artikel

- »In die Ferne schweifen«, »de« Heft 1–2/2010

### Links

- Entwickler und Lizenzgeber von OpenVPN ist OpenVPN Technologies, Inc.: [www.openvpn.eu](http://www.openvpn.eu)

- OpenVPN e. V.: [www.openvpn.net](http://www.openvpn.net)
- Insys Microelectronics GmbH: [www.insys-tec.de](http://www.insys-tec.de)

### Noch Fragen?

Sigurd Schobert  
Telefon: (089) 12607-244  
[schobert@de-online.info](mailto:schobert@de-online.info)