TDT®

AUSGABE
1/11

SWITCHED

ALEC nutzt TDTs GRE-Tunnel und BGB-Routing

Editorial
Philipp Weinzierl:
35 Jahre Entwicklung sind ein Pfund
(Seite 2)

TDT-Personalien

Josef Zehentbauer - Produktmanager kommt aus den eigenen Reihen
(Seite 4)

Katja Nobis - Controlling und Firmen-Ranking optimieren
(Seite 2)

Die Seite 3 OpenVPN
maechtig, zuverlaessig und flexibel

Seite 4
G5000-Gateway
jetzt auch mit Quad Core und reduntantem Netzteil serienmaessig

C2000 mit bis zu vier 3G/4G Funkmodems

LTE im Anmarsch
TDT stattet seine Geräte mit professionellen LTE Modem Modulen aus

TDT-Produkte auf der CeBit 2011
Vodafone und plustek präsentierten TDT-Equipment für ihre Lösungen

Loadbalancer TDT L3000

NEU:
3G/4G PCI-Modul

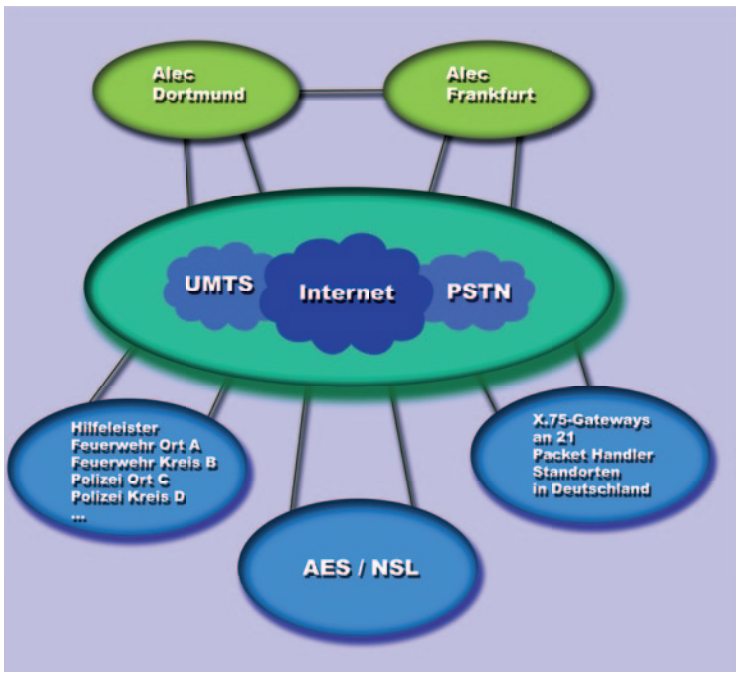
Digitale Festverbindung überflüssig

Andreas Pahne: „TDT-Produkte garantieren schon immer Investitionssicherheit".

Für Deutschlands Wach- und Sicherheitsdienste, die eine innovative Leitstellentechnik benötigen, ist das Dortmunder Unternehmen für Übertragungstechnik, die ALEC GmbH, erste Anlaufadresse. Die seit 1973 operierende Firma plant und betreibt bundesweite Netze, die den Ansprüchen des VdS genügen und in der VdS 2532 gelistet sind.
Dazu werden maßgeschneiderte Soft- und Hardwarelösungen (vom Übertragungsgerät bis zu Alarmempfänger) zur Abrundung einer Komplettlösung gleichfalls mit angeboten. Da die historisch gewachsenen Netze der einzelnen Unternehmen sich als äußerst heterogen erweisen, sind tiefe Kenntnisse im Umgang mit den vielfältigen Netztopologien und deren Protokollen notwendig.

Mit TDT, als bewährtem Partner der ersten Stunde, steht Geschäftsführer Andreas Pahne ein Unternehmen zur Seite, das höchst erfolgreich Router produziert und Netzkonzepte entwickelt. Die Lösungen ermöglichen, dass bestehende Netzarchitekturen von immer teurer werdenden digitalen Festverbindungen ohne Verlust hoher Zuverlässigkeit/Verfügbarkeit ersetzt werden können. Die verschiedensten Übertragungsgeräte routen aus den unterschiedlichsten Netzen über ein Intranet zu den entsprechenden Empfangsstellen.

Wegen der hohen Verfügbarkeit der Netze werden diese nicht nur im Wach- und Sicherheitsgewerbe, die Wert auf eine sehr hohe Verfügbarkeit legen, intensiv genutzt, sondern auch Konzessionäre routen damit entsprechende Meldungen zu einem Hilfeleister, wie z. B. die Feuerwehr (nach DIN 14675:A1). Und es wird gleich dafür gesorgt, dass Brandmeldungen nur bei der Feuerwehr ankommen und die Störungen direkt zum Konzessionär geleitet werden.
Das Netz bindet die neuen Dienste wie GPRS, UMTS oder DSL ein und ist gleichzeitig in der Lage, alte Analog- und ISDN-Anschlüsse, X.25, X.31 und X.75 in das Netz zu integrieren. Dies ist insbesondere in Hinblick auf die neue EN 50518 interessant, da hier Anschlüsse aller Art ohne Rufumleitung innerhalb der BRD verlegt und vernetzt werden können. So kann ein NSL ohne Aufwand – und ohne Mehrkosten – den Meldungsempfang, wie in der Norm gefordert, über eine AES umsetzen und trotzdem Zugriff auf seine Daten behalten. Im Unterschied zu anderen Netzen werden die alten Übertragungstechniken sanft in ein modernes Intranet überführt.
Um den Aufgaben eines modernen Netzes gerecht zu werden und Daten quer durch Deutschland verteilen zu können, hat ALEC eine mächtige Datennetz-Infrastruktur aufgebaut. Diese Infrastruktur basiert aktuell auf 21 Standorten, die bundesweit verteilt – und primär über SDSL zu einem leistungsstarken Intranet verbunden sind. Zur Steigerung der Verfügbarkeit wird jeder Standort zusätzlich über einen weiteren Anschluss, der immer auf einem anderen DSL-Provider beruht, bzw. alternativ über UMTS oder ISDN angebunden ist. Dieses Konzept wurde auch für alle Kundenanschlüsse umgesetzt, wobei aktuell 85 Hilfeleister (Leitstellen) mit mehr als 12.000 Endteilnehmern angebunden sind, deren Daten wie „digitaler Festverbindung" durch das Netz geroutet werden. Im Bereich X.31 ist ALEC bereits heute der zweitgrößte Anbieter in Deutschland. In den moderaten Preisen sind Entstörung innerhalb von 12 Stunden für X.31 enthalten, was wohl einmalig unter den Anbietern von X.31 sein dürfte. Gerade hier bewährt sich eine hohe Verfügbarkeit aller Komponenten und die hochwertige Ausstattung der Anschlussleitungen.



Um diese Infrastruktur aufzubauen, wurde auf Entwicklungen von TDT zurückgegriffen. Das niederbayerische Unternehmen bietet nicht nur Standardprodukte für IP an, sondern passt bestehende Lösungen so an, dass die geforderte Sicherheit (z. B. Verschlüsselung), Verfügbarkeiten (z. B. BGP- Routing mit <10 Sekunden Umroutung) und Kosteneffizenz (z. B. Bevorzugung von DSL vor UMTS) erreicht werden konnte. Fast schon legendär ist der TDT Expert Support, was für einen Betrieb eines höchst komplexen Netzwerkes eine wertvolle Rückversicherung ist, um plötzlich auftauchende Probleme schnell in den Griff zu bekommen.
Die Umstellung auf die Datenübertragung via Intranet mit

TDT-Routern ist seit Januar 2011 vollständig abgeschlossen und erweist sich in seiner Struktur als zukunftsweisend für die „intelligente“ IP-Datenübertragung. Da die Datensicherheit, bzw. das Back-Up-Konzept eine überragende Komponente innerhalb des Konzeptes darstellt, ist folgende Lösung umgesetzt worden.

Die intelligenten Zentralen

Als „Zentralen“ wurden zwei symmetrische Standorte in Dortmund und Frankfurt mit SDSL aufgebaut. Ein dritter Standort in Siegen kommt ab Mai 2011 dazu. Durch diese „Zentralen“ mit je einem alternativen Routing stehen jeweils physisch getrennte Leitungen (jeweils eigener APN) zur Verfügung und als weiterer alternativer Übertragungsweg UMTS. Über die zwei Standorte werden sämtliche Daten geroutet. Pro Standpunkt wird bewusst auf zwei „unabhängige“ Provider gesetzt, um eventuelle Leitungsstörungen sicher umgehen zu können. Aktuell ist „Dortmund“ mit Glas von Vodafone und Kupfer von DOKOM ausgestattet, während in „Frankfurt” Vodafone und QSC das Rennen machten (beide über Glas). Siegen wird mit Glas von der Telekom und Kupfer von Vodafone an den Start gehen. Die ALEC-Philosophie ist anders als die herkömmlicher Rechenzentren, bei der die Außenstellen sich über einen VPN zu einem Rechenzentrum verbinden und dann Daten austauschen. Die Standorte Dortmund, Frankfurt und Siegen sind reine Netz-Gateways, welche die Verbindung zwischen den einzelnen Netzsektoren herstellen. Jede Außenstelle baut dazu permanent je einen VPN nach Dortmund und Frankfurt auf. Dazu setzt das Dortmunder Unternehmen Gateways G5000 von TDT ein. Hinter G5000 steckt die TDT-Garantie, dass bis zu 5.000 Außenstellen über VPN-Tunnel gleichzeitig angebunden werden können. Eine gigantische Anzahl, die bisher von den Kunden nicht annähernd angefordert worden ist. Wie kaum ein anderes Gerät können sie Tunnels verwalten und die Daten-Balance regulieren. Alle Anbindungen werden über IPSec verschlüsselt, da das öffentliche IP-Netz der Transportweg ist und die sensiblen Daten zu hundert Prozent geschützt sein müssen.

Das BGP-Routing

Die ALEC-Netze sind dank der TDT-Router dynamisch. Alle Außenstellen suchen sich über das in den Geräten implementierte BGP-Routing standardmäßig den jeweils bestens geeigneten Weg. Die Stärke des Border Gateway Protocolls liegt darin, verschiedene alternative Routing-Pfade in einer einzigen Routing-Tabelle zu vereinen. Das BGP-Protokoll ermöglicht damit das Routing zwischen autonomen Systemen. Durch all diese Komponenten steckt ein hohes Maß an Intelligenz im Netz, das selbstlernend die Ausfall-Umschaltzeiten auf ein Minimum reduziert. Das BGP-Routing prüft dazu diverse Kriterien bzw. Parameter, wie Laufzeiten und Latenz (Zeitintervall, um das ein Ereignis verzögert wird), um die kürzeste Strecke zu ermitteln. Sobald sich die ausgewählte Strecke gegenüber dem zweiten VPN-Tunnel verschlechtert, wird umgeswitched – natürlich auch bei Streckenausfällen. BGP kann auch innerhalb eines autonomen Systems angewendet werden. Erkennt der G5000 hohe Bitratenfehler, wird auf einen alternativen VPN-Tunnel ausgewichen (der permanent aufgebaut und alle 2 Sekunden mit Nutzdaten getestet wird). Dieser Wechsel erfolgt in der Regel innerhalb von 6–10 Sekunden, womit ALEC unter den kritischen 20 Sekunden der VdS 2471 und der DIN 14675 bleibt. Durch die dauernde Lastverteilung auf die verschiedenen Systeme ist eine permanente Kontrolle aller Übertragungswege und Komponenten zu hundert Prozent sichergestellt. Bei einem herkömmlichen Backup-System, das nur dann eingesetzt wird, wenn etwas ausfällt, kann man nicht sicher sein, ob das Backup beim Ausfall einer Leitung überhaupt noch funktioniert, da es unter Umständen über Jahre nicht eingesetzt werden musste. Dies wäre fatal für ein Sicherheitsunternehmen, das seine Endteilnehmer alle 20 Sekunden auf Verfügbarkeit prüfen muss und ggf. dann mit Störmeldungen „zugeschüttet“ wird.

GRE-Tunnels

Mit Hilfe des GRE-Tunnels wird quasi eine Ebene eingesetzt, um durch die Tunnel zu routen. Dabei wird neben dem Namen (Adresse) des Interfaces auch die dazugehörigen Tunneladressen mitgeteilt. Somit kann das BGP entscheiden, in welchen Tunnel geroutet werden soll – unter Berücksichtigung der eingestellten Prioritäten. Die Einstellungen der relevanten Routing-Daten sind im Laufe der Zeit von TDT auf ALEC übertragen worden, welche über eine 24-Stunden-Hotline den Betrieb des Netzes sicherstellt. Als Second-Level-Support steht TDT aber weiter an der Seite der ALEC GmbH.

Doppelte Sicherheit

Die „Zentralen” sind neben dem Gateway G5000 zusätzlich mit einem TDT-M3000-Router ausgestattet. Sollte ein G5000-Gerät ausfallen, können die M-Router immer noch die direkte Verbindung zwischen den Standorten aufrecht erhalten. Somit wird nicht nur dem Ausfall von Leitungen Rechnung getragen, sondern auch dem Ausfall von einzelnen Komponenten. Zusätzlich stehen für die Energieversorgung 8 Std. USVs bereit, die durch ein Notstrom-Aggregat unterstützt werden.

Das UMTS-Netz

Mit UMTS steht nicht nur ein physikalisch komplett anderes Übertragungsmedium zur Verfügung, es wird auch die „kritische” letzte Meile zu Kunden, die z. B. durch einen Exklusiv-Vertrag an einen Provider gebunden sind, umgangen. Es wurde ein eigenes, geschlossenes UMTS-Netz aufgebaut, das über eine Leased Line angebunden ist, um die Trennung vom UMTS-Netz zum Internet über die gesamte Strecke sicherzustellen. Dadurch kann jeder beliebige DSL-Ausfall überbrückt werden. Die UMTS-Karten werden durch die ALEC GmbH über ein CDA des UMTS-Providers versorgt. Feste IP-Adressen ermöglichen die Verbindung UMTS auf UMTS ohne Internet und DynDNS. Zur zusätzlichen Sicherheit werden die Daten im UMTS, wie bei den DSL-Anschlüssen über IPSec verschlüsselt. Sicherheit hat eben höchste Priorität.

Die TDT-Netz-Router

Jeder Netz-Router (C-Router oder M3000-Router) einer Außenstelle verfügt über mindestens zwei permanente IPSec-Tunnel (über zwei verschiedene Anschlüsse), je einer nach Dortmund und Frankfurt. In Kürze wird Siegen an das Netz angeschlossen. Die G5000 in den Zentralen, entscheiden mit ihrem BGP-Protokoll, über welchen Weg die Daten übertragen werden. Eine Überwachung von Übertragungsgeräten von Endteilnehmern durch eine Alarmempfangseinrichtung ist ohne Einschränkung möglich, insbesondere, da das Netz extrem schnell Daten nach einem Ausfall umleitet und somit die Alarmempfangseinrichtungen davon im Normalfall nichts mitbekommen.

ALEC, Soft- und Hardwareschmiede

Immer, wenn die Änderungen von Normen neuen Handlungsbedarf erfordern, z. B. die EN 50518, entwickelt ALEC mit seinen Kunden zusammen entsprechende Konzepte und schmiedet, wenn nötig, die dafür notwendigen Hard- und Softwarekomponenten. Dabei sind es fast immer Einzellösungen, da die Unternehmen sehr verschiedene Netze betreiben und unterschiedlich strukturiert sind. Gerade hier bietet der „Rundumversorger” auf Kundenwunsch eine „Lösung aus einer Hand“ an und ist somit erster Ansprechpartner.

Zusatzdienste

Es ist dem Dortmunder Unternehmen auch möglich, über die bestehenden Anschlüsse und Router weitere Funktionalitäten in das Netz zu holen, z. B. die Anbindung von „Fremdnetzen“ dritter Anbieter. Hierbei können z. B. Übertragungsgeräte, die sich in einem kundeneigenen Netz befinden über einen VPN-Tunnel über den bereits vorhandenen DSL-Anschluss und Router angeschaltet werden, ohne dass weitere Kosten entstehen und dieses auch noch, wenn gewünscht, mit weiterreichenden Backup-Möglichkeiten.

Perspektive

Die ALEC GmbH hat in den letzten Jahren das operative Geschäft bis in die Schweiz ausgebaut, da dort ähnliche Strukturen wie in Deutschland vorhanden sind. Und mit TDT steht ein Unternehmen zur Seite, das alle Formen der Datenübertragung nicht nur miterlebt, sondern auch entscheidend mitgestaltet hat. IP wird uns über Jahre begleiten, so Hubert Mirlach von TDT. Alle Unternehmen, die noch „digitale Festverbindungen“, X.31 und X.25 nutzen, können ihre Anschlüsse oder Netze restrukturieren und effizienter und zukunftssicherer machen. „Da wir mit einem eigenen TDT-Kernel programmieren, ist uns Flexibilität auf den Leib geschnitten”. Andreas Pahne wird es für sein nächstes Projekt wieder recht sein.

Ansprechpartner: Andreas Pahne
ALEC GmbH
Friedrich-Hölscher-Straße 367
44328 Dortmund
Tel. 0231 22905-0, Fax 0231-22905-10
E-Mail: ap@alec.de

Editorial

Seit fast 35 Jahren entwickelt und produziert TDT Datenkommunikationstechnik für deutsche Unternehmen und für den Weltmarkt.

Der ungewöhnlich lange Erfolg attestiert, dass unsere Entwickler es immer wieder verstehen, den Puls der Zeit zu treffen und neueste Technologien zeitnah zu integrieren. Bei jedem neuen Produkt steckt die gesammelte Erfahrung aus drei Jahrzehnten drin!

Aktuell blickt die ganze Welt erwartungsvoll in Richtung LTE (Long Term Evolution) oder auch 4G genanntes mobile Datennetzwerk. Diese neue Generation mobiler Datenübertragung wird viele weitere Möglichkeiten und Anwendungen mit sich bringen und neue Märkte werden sich erschließen. Wir erwarten Bandbreiten von bis zu 300 Mbps – und das gerade in ländlichen Gebieten, denen bisher der Ausbau von schnellem Internet vorenthalten blieb. Deshalb wird ein „Run” auf die LTE-Endgeräte für die verschiedensten Anwendungen einsetzen, vom Smartphone bis hin zum LTE-fähigen VPN-Router zur mobilen Videoüberwachung.

Wie immer, wenn ein großer neuer Markt entsteht, werden neue Firmen aus dem Boden schießen, um mit Werbeversprechen ein Stück von dem Kuchen abschneiden zu können. TDT weiß jedoch: Zwar bietet das neue Netz viele ungeahnte Möglichkeiten, doch es wird mit den gleichen Alltagsproblemen konfrontiert werden, wie die Vorgängergenerationen. Das Gute daran ist: Mit TDT steht Ihnen ein Partner zur Seite, der die Stärken, aber auch sehr wohl die Schwächen der mobilen Datennetze seit Einführung von GPRS kennt und gerade auf die Unzulänglichkeiten schon reagiert hat, bevor andere Unternehmen von diesen überrascht werden. Aufgrund unserer Erfahrungen und mit unserem Know-how werden wir trotz neuer Technologie wieder ein Produkt anbieten, welches in Punkto Funktionalität und Zuverlässigkeit von Beginn an den Maßstab setzt.

Deshalb ist die Integration von LTE in unsere „mobile Router-Serie” ein weiterer Meilenstein in der TDT-Geschichte, der schon sehr bald realisiert sein wird.

Herzlichst
Ihr Philipp Weinzierl

TDT hat sich mit Katja Nobis Verstärkung für den administrativen Bereich geholt.

Die junge, motivierte Landshuterin arbeitet eng mit Traudl Walter in den Bereichen Buchhaltung, Controlling und Einkauf zusammen. Auf die Frage angesprochen, „warum TDT”, antwortete sie spontan: „Bei der Firma passt einfach alles. Das Image, das Können, die Zielsetzung und vor allem die Chemie unter den Kolleginnen und Kollegen.” Die kommenden Monate werden geprägt sein mit dem Upgrade der neuesten Navision-Software, um noch gezielter Daten für den Vertrieb und Einkauf ermitteln zu können. Dabei zählt sie natürlich auch auf die Erfahrung von Produktionsleiterin Maria Mayer. Die Ergebnisse fließen unter anderem in das interne Lieferanten-Ranking ein.

OpenVPN – mächtig, zuverlässig und flexibel

IPSec hat sich in den letzten Jahren zum De-facto-Standard für den Aufbau von sicheren VPNs entwickelt. So könnte man schnell zu der Überzeugung gelangen, IPSec wäre die alternativlose Lösung schlechthin. Mit **OpenVPN** gibt es aber eine ernst zu nehmende Konkurrenz, welche in einigen Bereichen klare Vorteile gegenüber IPSec verbuchen kann.

Die Konfiguration und Administration von Server und Client gestaltet sich bei OpenVPN wesentlich einfacher. Dies zeigt sich insbesondere bei der Analyse und Fehlersuche in VPN-Netzen. Während es bei IPSec trotz standardisierter Verfahren oftmals zu großen Interoperabilitätsproblemen kommt, sind derartige Probleme bei OpenVPN derzeit undenkbar.

OpenVPN kann problemlos über Firewalls, NAT-Gateways und sogar Proxy-Server kommunizieren, unterstützt dynamische IP-Adressen und bietet eine freie Auswahl an Authentifizierungsmethoden wie Benutzername/Password, Pre-Shared-Keys, X.509-Zertifikate oder Smartcards. Insbesondere die NAT-Problematik bereitet zusammen mit IPSec immer wieder Kopfschmerzen. Unterstützt die jeweilige Implementierung kein NAT-Traversal, lässt sich die Verbindung zwar aufbauen, es ist aber keine Datenübertragung mit ESP/AH möglich.

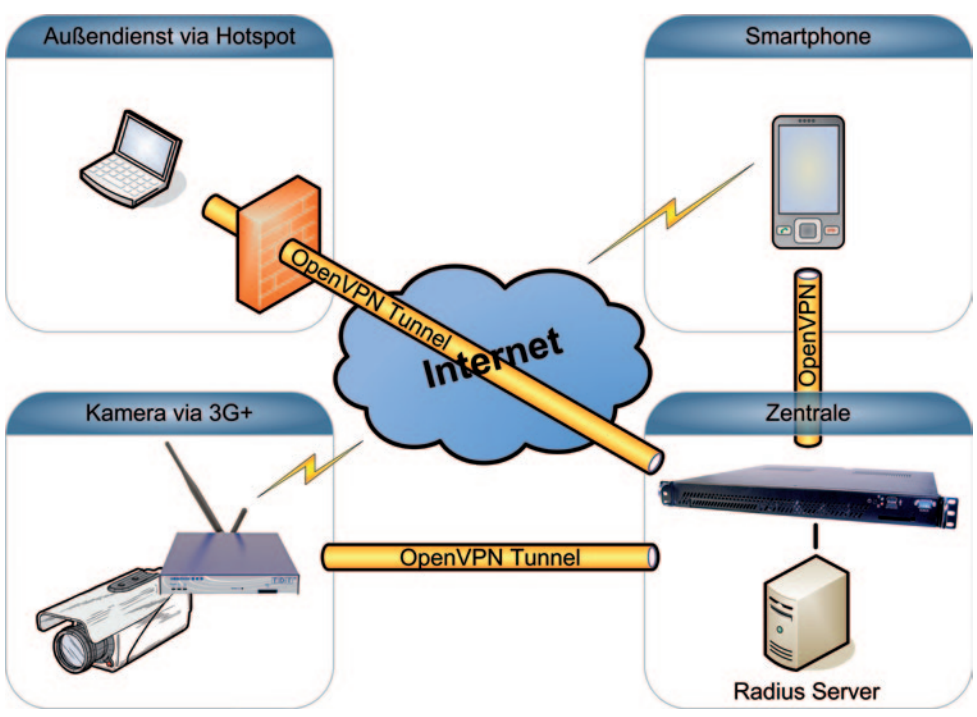
Grundsätzliches zu VPN (Virtual Private Network)

Grundgedanke von VPN ist, wie der Name schon sagt, ein virtuelles privates Netzwerk über ein öffentliches Netzwerk zu realisieren. So kann der Außendienstmitarbeiter als Road-Warrior in das Firmennetz integriert werden, um zentrale Dienste zu nutzen. Es kann aber auch eine komplette Standortvernetzung (LAN-LAN-Kopplung) realisiert werden.

Weiterhin muss ein VPN wichtige Ziele des Datenschutzes sicherstellen:

Vertraulichkeit

Die zu übertragenden Daten müssen vor Abhören und unerlaubtem Zugriff geschützt werden. Eine starke Verschlüsselung trägt hierzu bei, kann aber vor dem Fälschen der Empfängeridentität nicht schützen.



Unveränderbarkeit

Daten dürfen nicht verändert werden. Dem Fälschen der Absenderidentität und der Datenmanipulation kann durch eine starke Prüfsumme (HMAC) vorgebeugt werden.

Nachweisbarkeit

Es muss sichergestellt werden, dass die entsprechenden Daten vom korrekten Absender unverändert ankommen.

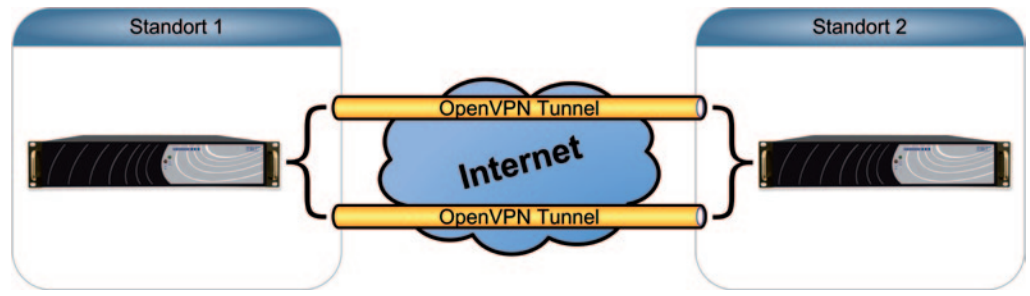
Verfügbarkeit

Der VPN-Dienst muss robust gegen Angriffe wie DoS (Denial-of-Service) sein.

Die Datensicherheit wird in VPN-Netzen durch Verschlüsselung erreicht, wobei OpenVPN eine Fülle an Verschlüsselungsverfahren unterstützt (DES, 3DES, AES, Blowfish, etc.). Authentifizierung wird in modernen Netzen über Zertifikate sichergestellt, aber auch das Pre-Shared-Key-Verfahren kommt noch häufig zum Einsatz. Für die Datenintegrität nutzt man zur Erzeugung von starken Prüfsummen (HMAC) sogenannte Hash-Funktionen, wie MD5 oder SHA-1. Um eine hohe Verfügbarkeit zu erreichen, muss neben dem Schutz vor DoS-Attacken auch die Hardware redundant ausgelegt werden und durch entsprechende Software-Mechanismen wie VRRP und/oder Loadbalancer abgesichert werden.

Mit OpenVPN können die Forderungen an Sicherheit und Verfügbarkeit extrem flexibel umgesetzt werden.

OpenVPN – die Modi



OpenVPN unterstützt die Modi Point-to-Point, Server und Client. Im P2P-Modus verwendet OpenVPN für jede Tunnelverbindung eine eigene Konfiguration sowie einen separaten frei wählbaren TCP- oder UDP-Port. Dieser Modus wird in der Regel nur für die Vernetzung von genau zwei Teilnehmern eingesetzt.

Der Server-Modus erlaubt es mehreren Benutzern, sich gleichzeitig in das Netz einzuwählen. Es ist nur ein Serverprozess für alle Teilnehmer notwendig. Somit wird nur ein einziger TCP- oder UDP-Port benötigt, was die Firewall-Architektur und Sicherheit erhöht.

Das Gegenstück zum Server-Modus ist der Client. Es ist möglich, für eine Verbindung mehrere Server-Instanzen anzugeben. Dies kann für ein priorisiertes Backup-Management sinnvoll sein.

Routing und Bridging

Hier liegt bei IPSec in der Tat der Hase im Pfeffer. Eine IPSec-SA (Security Association) ist im IPSec-Tunnel-Modus für die Kopplung von genau zwei Subnetzen definiert. Es erlaubt somit kein Next-Hop-Routing. Um derartige Szenarien mit IPSec zu realisieren, muss entweder für jedes zu routende Netz ein IPSec-Tunnel etabliert werden, oder es wird eine hochkomplexe Transport-Mode-Sitzung mit darüber liegendem L2TP mit PPP aufgebaut. Letzteres ist übrigens in den meisten Implementierungen nicht für Routing-Szenarien, sondern lediglich für Road-Warrior berücksichtigt.

OpenVPN bietet hier erheblich flexiblere Möglichkeiten. So kann im Routed-Modus eine beliebige Anzahl von Subnetzen durch ein Next-Hop-Routing auf Ebene 3 über einen einzigen Tunnel miteinander verbunden werden. Der Bridged-Modus gestattet sogar eine Anbindung auf Layer 2 (MAC-Ebene). Grundsätzlich ist dieser Modus für Road-Warrior-Verbindungen gedacht.Durch eine Erweiterung von TDT, dem **MCC*** (Multi-Channel-Connection) wird der Bridged-Modus zum wahren Künstler! So können mehrere Tunnels von ein und demselben Client zu einer einzigen logischen Schnittstelle gebündelt werden. Dies führt ähnlich wie bei RAID-Systemen wahlweise zur Erhöhung des Durchsatzes oder der Ausfallsicherheit. Des weiteren ist ein VPN-Client im Bridged-Modus gleichzeitig Teilnehmer der zentralseitigen Broadcast-Domain, was viele Anwendungsgebiete überhaupt erst möglich macht.

TCP und UDP

Im Gegensatz zu vielen anderen VPN-Lösungen können bei OpenVPN das Transportprotokoll (TCP oder UDP) als auch der Port frei gewählt werden. Sehr schnell und flexibel arbeitet OpenVPN standardmäßig auf dem UDP-Port 1194. Wird für die Verbindung beispielsweise TCP mit Port 80 verwendet, muss meist nicht einmal die Firewall umgestellt werden. Obendrein kann OpenVPN sogar über Proxy-Server arbeiten.

Authentifizierung mit OpenVPN

Die wohl wichtigste Funktion innerhalb eines VPN ist die Authentifizierung der Teilnehmer. Durch die Authentifizierung wird die Identität von Sender und Empfänger sichergestellt. Darauf aufbauend werden Sitzungsschlüssel für Verschlüsselung generiert, sowie ein Hash-Verfahren zur Bildung einer starken Prüfsumme vereinbart. Für den Verbindungsaufbau verwendet OpenVPN das SSL/TLS-Verfahren, wobei TLS (Transport Layer Security) den Nachfolger von SSL (Secure Socket Layer) bezeichnet.

Zur Authentifizierung stehen die Verfahren Username-Password, Pre-Shared-Key (PSK), Public-Key mit X.509-Zertifikaten oder auch Smartcards zur Verfügung.

Das PSK-Verfahren ist aufgrund seiner einfachen Konfiguration sehr beliebt und entsprechend weit verbreitet. Es muss lediglich ein Schlüssel für je zwei Teilnehmer erzeugt und an diese verteilt werden. Hierin liegt aber auch schon die Hauptproblematik dieses Verfahrens. Zum einen muss ein sicherer Weg zur Übermittlung des Schlüssels gefunden werden und zum anderen muss die Vertraulichkeit an den Endpunkten gewährleistet sein. Gelangt der Schlüssel in falsche Hände, liegt der gesamte Datenverkehr offen. Für professionell genutzte VPNs ist dieses Verfahren nicht zu empfehlen, wobei es sowieso den P2P-Implementierungen vorbehalten ist.

Für jegliche Client-Server-Konstellationen ist der Einsatz von X.509-Zertifikaten mindestens auf Serverseite Pflicht. Der Client kann sich wahlweise mit einem Zertifikat oder Benutzername/Passwort anmelden. Mit Hilfe der Anmelde-Informationen kann OpenVPN zusätzlich mit einem Radius-Server gekoppelt werden. Dies ermöglicht das zentrale Speichern von Anmeldeinformationen, zugehörigen Attributen wie IP-Adresse oder Routing, sowie das Sammeln von Accounting-Daten. Das Public-Key-Verfahren mit X.509-Zertifikaten beschreibt ein asymmetrisches Verschlüsselungsverfahren. Jeder Teilnehmer besitzt dabei ein Schlüsselpaar, das aus einem privaten geheimen Schlüssel und einem öffentlichen Schlüssel besteht.

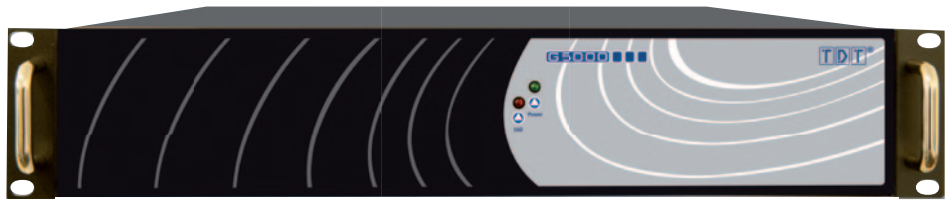
Um die Teilnehmer mit X.509-Zertifikaten ausstatten zu können, ist eine sogenannte PKI (Public Key Infrastructure) erforderlich. Die PKI dient der Erstellung und Verwaltung von Zertifikaten. Die übergeordnete CA (Certificate Authority) fungiert als vertrauenswürdige Stammzertifizierungsstelle und signiert die ausgestellten Zertifikate. Durch Einsatz einer sogenannten CRL (Certificate Revocation List) können nicht mehr vertrauenswürdige Zertifikate zur Laufzeit als ungültig erklärt werden. Die CRL ist öffentlich und für den OpenVPN-Server erreichbar. So können dynamisch Aktualisierungen vorgenommen werden.

Die TDT-PKI erlaubt durch entsprechende Sub-CA's die Implementierung von kundenspezifischen autarken Stammzertifizierungsstellen, womit das diesbezüglich weitgreifende Know-how einfach ausgelagert werden kann.

Ein Beitrag von
Jürgen Büttner/Josef Zehentbauer

*MCC siehe auch Seite 4

Das VPN Gateway G5000 jetzt mit Quad Core und redundantem Netzteil serienmäßig



Der G5000 ist ein Central Site VPN Gateway und Loadbalancer, mit einer Kapazität von bis zu 5.000 IPSec und 2.400 OpenVPN-Tunnel. Das heißt, bis zu 5.000/2.400 Außenstellen können gesichert und authentifiziert an die Hostumgebung angebunden werden.

Die modulare und damit hoch flexible Architektur des G5000 erlaubt die Konfiguration mit zusätzlichen Schnittstellen, wie ISDN, Ethernet, Fiber, etc.

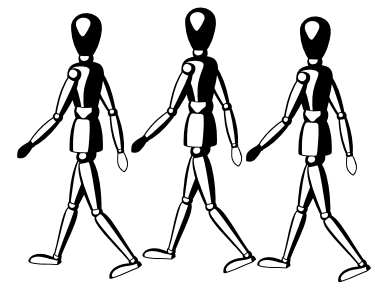
Ein intelligentes Backup Management, ein komplexes Firewall-System mit Statefull Inspection und Intrusion Detection/Prevention sorgen für eine sichere Netzanbindung der Host-Systeme.

Als Standard ist der G5000 jetzt mit redundanten Netzteilen ausgestattet. Dies garantiert zusammen mit VRRP (Virtual Router Redundancy Protokol) eine hohe Ausfallsicherheit. Die Netzteileinheiten sind mit stabilen Handgriffen ausgestattet und im Fehlerfalle bequem zu tauschen, auch während des Betriebs (Hot Sappable).

Der G5000 kommt im 19“-Design und ist mit einem Rail Mount System zur komfortablen Installation in einem Rack ausgestattet.

LTE IM ANMARSCH

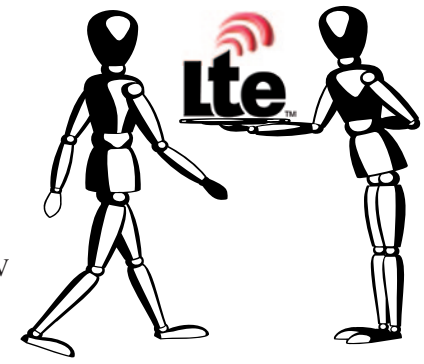
Das neue Mobilfunk-Netz wird Realität



Die ersten Zellen sind installiert und in Betrieb. TDT wird in Kürze die Router Modelle C15xx mit professionellen LTE Modem Modulen ausstatten. TDTs C2000 sowie eine PCI-Karte.

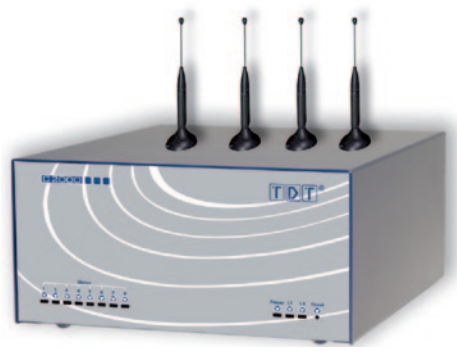
Vorteile von LTE für den Anwender:

- 10-fache Geschwindigkeit gegenüber HSPA bei Datenübertragungen
  - bis zu 100Mbit/s Download/Downlink
  - bis zu 50 Mbit/s Upload/Uplink
- 10 bis 20-mal schnellerer Verbindungsaufbau als HSPA
- Bessere Energieeffizienz der Endgeräte
- Komplett IP-basierte Umgebung
- Koexistenz und Zusammenarbeit mit GSM/GPRS/EDGE, UMTS/HSPA/HSPA+
- Ermöglicht zeitkritische Anwendungen, z. B. IP-Telefonie, Videoübertragung, HDTV



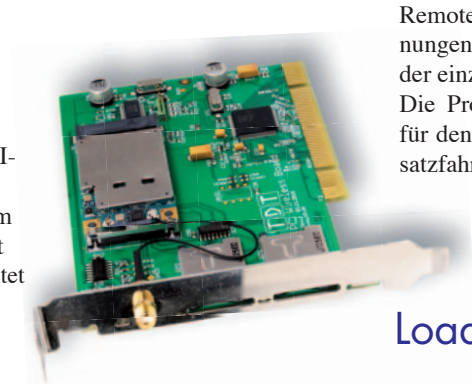
C2000 mit bis zu vier 3G/4G Funkmodems

Immer wieder wurden wir von unseren Kunden gefragt, ob es denn nicht möglich sei, zwei oder mehr UMTS-Verbindungen gleichzeitig herzustellen. Dabei war eine häufig angefragte Anwendung, die Verwendung von zwei Videokameras, die jeweils eine eigene Verbindung mit voller Bandbreite nutzen sollten.



Der **C2000** bietet jetzt die Möglichkeit bis zu vier 3G/4G Funkmodems zu installieren und damit vier unabhängige Verbindungen herzustellen. Dabei kann jedes Funkmodem als Backup zwei SIM-Karten bedienen, folglich zwei unabhängige Netzbetreiber unterstützen. Eine Besonderheit, die alle TDT 3/4G Router unterstützen, ist das **TDT MCC** (Multi-Channel-Connection)**.** Hierbei bestehen zwei identische Daten-Verbindungen zu einer Gegenstelle, z. B. zwei identische Video-Streams. Ist eine Verbindung gestört oder fällt sie aus, wird unterbrechungs- und verlustfrei auf die zweite Verbindung umgeschaltet. Eine weitere Besonderheit des TDT MCC ist die Multiplikation der Bandbreite. Beliebige Schnittstellen können quasi parallel geschaltet werden, so auch zwei oder mehr Funk-Schnittstellen und damit eine Verdoppelung oder Verdreifachung der Bandbreite erwirken. Einzige Forderung ist die Installation eines TDT Routers auf beiden Seiten.

NEU: 3G/4G PCI-Modul



Zum Einbau in eine beliebige Hardware-Plattform mit PCI-Schnittstelle bietet TDT jetzt eine 3G/4G Lösung. Das PCI-Modul hostet ein professionelles 3G/4G* Funkmodem und unterstützt dabei zwei SIM Karten Slots. Bestückt mit zwei SIM-Karten unterschiedlicher Netzprovider gewährleistet das Modul eine hohe Ausfallsicherheit und Zuverlässigkeit.

*Sobald 4G-Modems verfügbar sind.

TDT auf der CeBIT 2011

vodafone und plustek präsentierten TDT-Equipment für ihre Lösungen

Auf dem CeBIT-Stand von Vodafone präsentierte Lotto Niedersachsen live sein „neues Datennetz“, auf höchstem Sicherheitsniveau und höchster Verfügbarkeit bei gleichzeitig geringsten Betriebskosten. Erreicht wurde dies durch den konsequenten Einsatz modernster 3G-Router-Technik von TDT.
TDT entwickelte die Systemlösung, die Migration und den Roll Out, zusammen mit Lotto Niedersachsen und Vodafone als Netzprovider.

Auch bei plustek war TDT vertreten. Die Firma produziert unter anderem Netzwerkvideorecorder, die ein intelligentes Aufzeichnen von Videos ermöglichen. In Verbindung mit dem TDT C1500 VPN Router kann per Remote auf die Recorder und die Aufzeichnungen zugegriffen werden. Eine Steuerung der einzelnen Kameras ist zudem gegeben.
Die Produktserie beinhaltet auch Recorder für den Fahrzeugeinbau, z. B. für BOS-Einsatzfahrzeuge, Züge, Busse und Taxen. Hier setzt plustek auf den TDT ELW-Router, der durch die E-Zulassung für diesen Einsatzzweck optimiert wurde. Dank der mittlerweile höchst zuverlässigen UMTS-Anbindung können Videos sowie die aktuellen Geo-Daten jederzeit abgerufen werden.
Die Live-Demos fanden großes Interesse bei den Vertretern der Behörden und bei den Installationspartnern von plustek.

Typisch TDT: Produktmanager kommt aus den eigenen Reihen

Schnörkellos und geradlinig verläuft die Karriere von Josef Zehentbauer im Hause TDT. Nach seiner erfolgreichen verkürzten Ausbildungszeit zum IT System-Elektroniker war es TDT-Chef Michael Pickhardt klar, welches Potential in ihm steckt. Durch seine Arbeit im TDT-Expert Support konnte er seine Fähigkeiten voll ausnutzen. Neben der Kundenbetreuung realisierte er Datennetze, zum Beispiel für ALDI und die ALEC GmbH.

Schon bald sind Entwicklungsarbeiten hinzu gekommen.
Begleitend zu seiner Arbeit studiert Josef Zehentbauer Elektrotechnik und erreichte im Vordiplom die Gesamtnote 1,6. Das ideale Gerüst, um als TDT-Produktmanager erfolgreich zu sein. „Das sichere Gespür, welche neuen Entwicklungen und Trends in der Kommunikationstechnik eingesetzt werden und der bekannte Tick, schneller zu sein, als die Mitbewerber, macht die Aufgabe äußerst interessant”, so Josef Zehentbauer. „Bei allen Entwicklungen muss neben der Hard- und Software der Support von Anfang an im Gesamtkonzept berücksichtigt sein.” Das wird die neuen Router-Modelle mit professionellen LTE-Modulen auszeichnen. Und eine weitere gute Nachricht zum Schluss: Router, die bereits im Einsatz sind, können dank bewährtem TDT-Design „upgegradet” werden.

Loadbalancer TDT L3000

Loadbalancing wird immer dann interessant und gefordert, wenn große Lastaufkommen auf mehrere Server verteilt werden müssen. Dabei kann das Verteilen der Last innerhalb einer Serverfarm, oder verteilt im WWW gesteuert werden.
Die Lastverteilung erfolgt über einen weiten Bereich von konfigurierbaren Kriterien, angefangen vom einfachen Round Robin und gewichteten RR-Algorithmus bis hin zu SSL offload und der Verteilung von Requests auf Anwender Ebene (Layer 7 Content Switching).
Mit dem TDT L3000 Loadbalancer sind Sie gerüstet, für erhöhten Durchsatz bietet TDT den L5000.

IMPRESSUM

Herausgeber
TDT GmbH
Michael Pickhardt
Geschäftsführer

Siemensstraße 18
84051 Essenbach
Tel. 08703 929-00
Fax 08703 929-201

E-Mail: info@tdt.de
web: www.tdt.de

Verantwortlich für den Inhalt: H. J. Büttner
Leiter Vertrieb und Marketing

Auflage 50.000

Gesamtproduktion:
MCW GbR
Ulmenstraße 21
84051 Essenbach

Tel. 08703-91360
jwimmer@rze.de