VPN-Plattformen

Managen oder managen lassen – das ist hier die Frage

Kai-Oliver Detken

Die Standortkopplung von Unternehmen wird heute wie selbstverständlich über so genannte Virtual Private Networks (VPN) vorgenommen. Dabei wird die Kopplung über sichere verschlüsselte Verbindungen direkt über das Internet vollzogen. Stand zuerst nur die Ablösung vorhandener teurer Standleitungen auf der Tagesordnung, müssen VPNs heute ganz anderen Anforderungen genügen, um auch echtzeitbasierte Dienste wie Voice over IP (VoIP) unterstützen zu können. Zur Realisierung kann ein Unternehmen auf den Provider seiner Wahl zurückgreifen oder selbst die Infrastruktur aufbauen und managen.

Prof. Dr. Kai-Oliver Detken ist Geschäftsführer der Decoit GmbH in Bremen

Virtual Private Networks stellen einem Unternehmen eine virtuelle Kommunikationsplattform zur Verfügung, die einer geschlossenen Benutzergruppe den sicheren Austausch von Informationen ermöglicht. Das heißt, das VPN bietet dieser Benutzergruppe auf Basis eines unsicheren Netzes (dem Internet) die sichere Kommunikation. Dies geschieht auf Basis von Tunneling und Verschlüsselung, was unterschiedlich realisiert werden kann. IP Security (IPsec) nach RFC-4301 hat sich im IP-Umfeld herstellerübergreifend durchgesetzt. Es beschreibt im Wesentlichen die Protokollerweiterungen Authentication Header (AH), Encapsulated Security Payload (ESP) sowie das Internet Key Exchange (IKE) zum Austausch der Schlüssel. Gerade durch das letztgenannte Protokoll, das relativ komplex ist, war eine Kompatibilität zwischen verschiedenen Herstellern anfangs schwierig umzusetzen. Das hat sich aber stark entspannt; auch weil viele Hersteller inzwischen auf eine ähnliche Implementierung (z.B. Open-Source-Projekt Openswan) setzen.

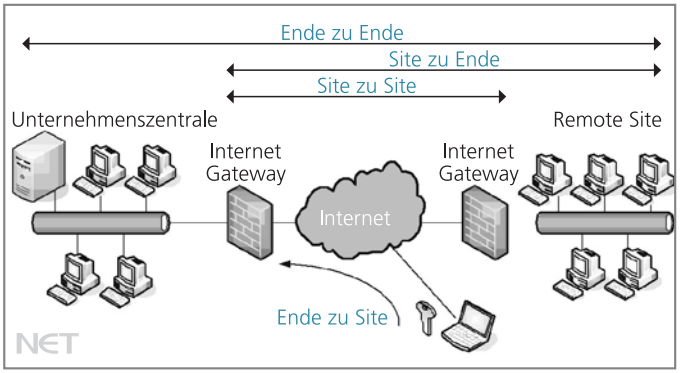

Bild 1: VPN-Anwendungsszenarien

Ein VPN kann durch unterschiedliche Szenarien realisiert werden (*Bild 1*):

- Site zu Ende: ein physisches Netz, in das externe Geräte über ein spezielles VPN-Gateway aufgenommen werden; der externe VPN-Partner wird dadurch zum Bestandteil des zugeordneten Netzes und ist von dort aus direkt adressierbar;
- Site zu Site: zwei zueinander kompatible Netze, die an dem benachbarten Netz (z.B. dem Internet) angrenzen, werden miteinander verbunden, wobei auch hier das dazwischen liegende benachbarte Netz von einer vollkommen anderen Art sein kann;
- Ende zu Ende: es wird unabhängig von den dazwischenliegenden Routern und Firewalls eine VPN-Verbindung zwischen Endgeräten und VPN-Gateway oder -Server aufgebaut;
- Ende zu Site: ein externes Endgerät nimmt direkten Kontakt zu einem VPN-Gateway auf (Roadrunner-Szenario).

Unabhängig von den Anwendungsszenarien werden an ein VPN hohe Anforderungen gestellt:

- Flexibilität: Schnelleres und effizienteres Reagieren auf sich ändernde Randbedingungen des Unternehmens wie Firmenstandorte, Mobilteilnehmer und Telearbeitsplätze.
- Sicherheit: Die Flexibilität darf sich auf keinen Fall auf den Sicherheitsgrad auswirken. Die Kommunikation wird über das Internet vorgenommen, das vielen Störeinflüssen ausgesetzt ist. Durch den Einsatz eines VPN darf es für Unbefugte nicht möglich sein, von außen auf die internen Firmendaten zuzugreifen.
- Echtzeitfähigkeit: Es werden heute nicht nur sensible Anwendungen wie Warenwirtschaftssysteme über ein VPN betrieben, sondern es kommen auch immer mehr Sprachdienste zum Einsatz. Daher muss das VPN in der Lage sein, zumindest eine un-

terschiedliche Priorisierung anbieten zu können.

- Mobilität: Mobile Endgeräte sind immer mehr im Einsatz. Waren es früher PDAs, die direkt am Arbeitsplatz synchronisiert wurden, benötigen heute zunehmend Smartphones und Laptops eine direkte Verbindung zum Unternehmensnetz. Das sollte über VPN-Verbindungen ermöglicht werden.
- Performance: Die theoretische Bandbreite sagt noch nicht alles über die wirkliche Leistungsfähigkeit aus. Die Provider garantieren meistens nur für einen Bruchteil der zur Verfügung stehenden Bandbreite.
- Verfügbarkeit und Zuverlässigkeit: Die Dienste und Anwendungen müssen immer standortübergreifend verwendet werden können – ohne Verbindungsabbrüche. Durch Einsatz eines Netzmanagementsystems kann z.B. die Verfügbarkeit stark angehoben werden, während der Provider für die Konnektivität verantwortlich ist.

Die Anforderungen müssen bei einer VPN-Umsetzung berücksichtigt und bei den Anbietern abgefragt werden. Die Provider müssen in jedem Fall mit berücksichtigt werden, unabhängig davon, ob man das VPN selbst oder über den Provider realisieren lassen möchte.

Umsetzungsmöglichkeiten

Ein VPN kann im einfachsten Fall direkt von einem Provider bezogen werden. Mittlerweile bieten alle Internet Service Provider (ISP) diesen Dienst mit an, wobei unterschiedliche Qualitäten zum Einsatz kommen. Ein reines Daten-VPN wird heute ohne jegliche Priorisierung realisiert. Das heißt, es werden DSL-Leitungen (z.B. ADSL, SDSL, VDSL) zur Verfügung gestellt, die keine Garantien für Laufzeiten und Bandbreiten bieten. Die bessere, aber auch teurere Variante, ist eine Realisierung mittels Multi Protocol Label Switching (MPLS). MPLS ermöglicht die verbindungsorientierte Übertragung von Datenpaketen in einem verbindungslosen Netz (wie dem Internet) entlang eines zuvor aufgebauten Verbindungspfades. Das Unternehmen erhält dadurch eine IP-VPN-Konvergenzlösung, die eine gleichzeitige Übertragung verschiedenartiger Anwendungsdaten auf einer Plattform ermöglicht. Dazu erfolgt der Datentransport über verschiedene Verkehrsklassen (abhängig vom Provider), die den Anwendungen die entsprechenden Transportqualitäten bereitstellen. Als Verkehrsklassen kommen definierte QoS-Parameter für anwendungsrelevante technische Eckwerte zum Einsatz. Es erfolgt eine dynamische Zuordnung von Anwendungen zu Verkehrsklassen für eine optimale Ressourcennutzung im Netz bei hoher Kommunikationsqualität der Anwendungen. Zum Teil wird die flexible Nutzung der Verkehrsklassen auch über die reservierte Bandbreite hinaus ermöglicht. Mit der MPLS-Technik ist eine direkte Any-to-Any-Kommunikation zwischen allen Standorten im VPN möglich. Neue Standorte können so leicht mit eingebunden werden.

Verkehrsklasse	max. Verzögerung (1 Weg)	max. Jitter	max. Paketverlust	Bemerkung
Sprache	25 ms	10 ms	1 %	optimiert für VoIP-Profil (Codec G.729a)
Multimedia	35 ms	20 ms	1 %	laufzeitoptimiert
Premium	45 ms	-	0,1 %	verlustoptimiert
best Effort	-	-	-	keine Zusagen

Tabelle 1: Provider-Verkehrsklassenbeispiele

Provider mit eigener Netzinfrastruktur, die auf MPLS-Basis realisiert sind, können verschiedene Verkehrsklassen innerhalb ihres Netzes anbieten. Dies gilt in keinem Fall für die allgemeine Nutzung des Internet und auch nicht für Provider, die nur Overlay-Netze besitzen (u.a. 1&1, Strato). Overlay-Netze nutzen die physische Infrastruktur eines anderen Providers, um eigene Dienste anbieten zu können. Provider mit eigener Infrastruktur können hingegen unterschiedliche Verkehrsklassen anbieten (z.B. von Best Effort bis Voice, *Tabelle 1*). Durch MPLS lassen sich dann Verzögerungszeiten, Jitter und Paketverluste garantieren, so dass auch echtzeitintensive Anwendungen standortübergreifend genutzt werden können. Für den Transport zwischen Kunden-Router und Point of Presence (POP) des ISP sowie zwischen POP und Kunden-Router erfolgt zur Gewährleistung der Übertragung eine Differenzierung der Verkehrsklassen im Rahmen der zur Verfügung stehenden Bandbreite je Verkehrsklasse. Die Zuordnung der einzelnen IP-Pakete zu den Verkehrsklassen erfolgt über die so genannte Precedence Bits sowie den Diffserv Codepoint (DSCP) im IP-Header der an der Kundenschnittstelle angelieferten IP-Pakete.

Um ein MPLS-Netz in dieser Qualität und Güte aufbauen zu können, sind

Merkmale aus Kundensicht	eigene Realisierung	Remote-Management	gesamtes Management	gehostetes VPN
Standort der Plattform	beim Kunden	beim Kunden	beim Kunden	beim Anbieter
Plattformmanagement	vom Kunden verwaltet	beim externen Anbieter vorhanden und verwaltet	beim Kunden vorhanden, vom Anbieter verwaltet	vom Anbieter komplett verwaltet
Bindung zum Anbieter	nur VPN-Zugänge	nur Managementleistungen	nur Managementleistungen	alle Netzzugänge und Management
Einbindung des Kunden	volle Einbindung	Kunden partizipieren an Entscheidungen	Kunden am Geschäftsablauf involviert	Kunden am Geschäftsablauf involviert
Besitz der Plattform	gehört dem Kunden	gehört dem Kunden	gehört dem Kunden oder wird von ihm finanziert	gehört dem Provider
externer Dienstleistungsanteil	gering	mittel	mittel	hoch
Investitionsaufwand	hoch	hoch	hoch	mittel
Betriebsaufwand	hoch	mittel	mittel	gering
Möglichkeit zum Upgrade	hoch	hoch	hoch	mittel
Kontrolle seitens des Kunden	hoch	mittel	mittel	gering

Tabelle 2: Unterschiedliche Kommunikationslösungen

allerdings zwei Anforderungen zu berücksichtigen:

- Alle Standorte des Unternehmens müssen vom selben Provider erreicht werden können.
- Es müssen an allen Standorten symmetrische Anschlüsse zur Verfügung stehen.

Zusätzlich sind die Kosten wesentlich höher als bei einer anderen VPN-Lösung. Wenn die genannten Anforderungen nicht erfüllt werden können (unterschiedliche Provider oder asymmetrische Anschlüsse) und man sich als Unternehmen nicht in die Abhängigkeit eines einzelnen Providers (beispielsweise Tarife, Vertragslaufzeiten, Sicherheit) begeben möchte, ist eine Realisierung über eigene Fachleute oder externe Anbieter durchaus sinnvoll. Dadurch kann auch eine höhere Flexibilität erreicht werden, da einzelne Standorte unterschiedlich angebunden werden können. *Tabelle 2* fasst die Vor- und Nachteile der verschiedenen Realisierungsformen zusammen.

Bei der providerunabhängigen Realisierung sind folgende Anforderungen zu beachten:

- Ausreichende Erreichbarkeit der anzubindenden Standorte über ADSL, SDSL, VDSL usw.;
- eigenes oder externes Netzmonitoring, um alle Verbindungen kontinuierlich überwachen zu können, was durchaus auch bei einer Umsetzung durch einen Provider sinnvoll sein kann, um diesen überwachen zu können;
- IPsec-Realisierung mit ausreichenden Sicherheitsparametern wie AES-Verschlüsselung und Zertifikatseinsatz im Main Mode;
- Vertragsmanagement der einzelnen Standortverträge, um Kosten vergleichen und Laufzeiten der Verträge kontrollieren zu können;
- eigene Priorisierung verschiedener Applikationen am VPN-Router, um Engpässe an den Randbereichen des Netzes Provider-unabhängig zu realisieren.

Hersteller/Anbieter	URL	Produkte
Astaro	www.astaro.de	Astaro Security Gateways (Firewall, VPN, Intrusion Prevention)
Borderware	www.borderware.com	BorderWare SteelGate
Checkpoint	www.checkpoint.com	Connectra Appliance, IPSEC VPN Software Blade, Check Point Power-1 Appliances, Integrated Appliance Solutions (IAS)
Cisco Systems	www.cisco.com	Cisco 800/1700/2600/3600/7100/7200, VPN 3000 Concentrator
McAfee	www.mcafee.com	Snapgear IPSec VPN Gateways
Enterasys Networks	www.enterasys.com	XSR Security Routers
Funkwerk Enterprise Communications	www.funkwerk-ec.com	TR200 Multifunktions-Gateway, R-Serie Bintec, VPN Access Line, X8500 Familie
Linogate	www.linogate.de	Defendo VPN-Gateway
Lucent Technologies	www.alcatel-lucent.com	Lucent VPN Firewall Brick 50/150/700/1200, Security Management Server
Microsoft	www.microsoft.com	ISA Server 2006
NCP	www.ncp-e.com	NCP Secure Enterprise Solution, NCP Secure Entry Clients
Juniper Networks	www.juniper.net	NetScreen-5200, NetScreen-5400
Nortel Networks	www.nortel.com	VPN Router 1750/2700/2750/5000, VPN Gateway 3000 Series, VPN Router Multi-Element Manager
Sonic Wall	www.sonicwall.com/de/	SonicWALL PRO-Serie 1260/2040/3060/4060/4100/5060
Telco Tech	www.liss.de	LiSS 700/1000/2000/3000/5000 Serie
Viprinet	www.viprinet.de	Multichannel VPN-Router 300/1600
Watch Guard	www.watchguard.com	Firebox X e-Serie, Firebox X EDGE

Tabelle 3: Herstellerbeispiele unterschiedlicher VPN-Lösungen

VPN-Endgeräte

Will man als Unternehmen sowohl den Besitz als auch die Verantwortlichkeit des Managements für die Kommunikationsgeräte und -lösungen behalten, muss eine eigene VPN-Plattform aufgebaut werden. Dies kann entweder eigenständig oder durch einen externen Anbieter erfolgen. Bei der Realisierung kann entweder auf hard- oder softwarebasierte Lösungen zurückgegriffen werden (*Tabelle 3*).

Bei der hardwarebasierten Variante werden vorhandene oder neue Router für die VPN-Lösung eingebunden. Viele Hersteller haben aus diesem Grund ihre Router mit zusätzlichen VPN-Funktionen ausgestattet. Wenn die vorhandenen Router weiter genutzt werden können, kann die vorhandene Netzinfrastruktur unangetastet bleiben. Es fallen dann nur Konfigurationsänderungen bzw. die Installation der VPN-Funktionen an. Der Einsatz der VPN-Technik auf dem Router hat jedoch eine erhöhte Prozessorlast zur Folge. Deshalb sollten trotz vorhandener Router-Hardware auch Neuanschaffungen eingeplant werden. Um die Performance in den Griff zu bekommen, da sie auch den normalen Datenverkehr beeinträchtigt, bieten Hersteller teilweise auch VPN-Zusatzmodule an, die die Verschlüsselung übernehmen und dabei die Belastung des Routers minimieren können.

Bei der softwarebasierten Variante wird ein zusätzlicher Dienst auf einem vorhandenen oder neuen Server implementiert und bereitgestellt. Da es sich hierbei um eine installierbare und zu konfigurierende Software handelt, sind eine Vielzahl von Optionen und Funktionen verfügbar. Betriebssysteme wie Windows XP/Vista und Linux-Distributionen bieten ebenfalls bereits in der Grundausstattung VPN-Implementierungen an. Dadurch ist die Sicherheit und Qualität der VPN-Lösung vom Basissystem (Hardware des Servers, Betriebssystem usw.) direkt abhängig. Wenn z.B. das vorhandene Betriebssystem Sicherheitsprobleme aufweist, kann sich dies auch auf die VPN-Lösung auswirken. Deshalb muss das gesamte System immer auf dem neuesten Patch-Stand gehalten werden. Eine Softwarelösung ist zudem von den Hardwarekomponenten des Grundsystems abhängig, denn die VPN-Lösung kann nur die Performance anbieten, die das Grundsystem ver-

Fortsetzung auf Seite 42

Spezifikation erfordern allerdings auch Antennenlösungen der nächsten Generation. Erfreulicherweise erfüllen schon mindestens zwei Industriestandard-Antennenschnittstellen, nämlich CPRI (Common Public Radio Interface) und OBSAI (Open Base Station Architecture Initiative), die Geschwindigkeitsanforderungen von LTE. Bei der CPRI-Schnittstelle reichen die Verbindungsraten von 614,4 Mbit/s bis 2,4 Gbit/s. OBSAI unterstützt Raten von 768 Mbit/s bis 3,07 Gbit/s. Dank der hohen Datenraten bei CPRI und OBSAI können die Datenströme von LTE-Antennen direkt auf den Basisbandprozessor geroutet werden. Auf diese Weise kann der ASIC oder FPGA eingespart werden, der normalerweise die Schnittstelle zwischen den Antennendaten und dem DSP bildet (*Bild 2*). Der TCI6487 enthält eine Sechs-Wege-Antennenschnittstelle und unterstützt die Standards CPRI und OBSAI. Mit Hilfe der Sechs-Wege-OBSAI/CPRI-Antennenschnittstelle lassen sich auch eine Reihe verschiedener Architekturen auf einer Leiterplatte umsetzen, z.B. Stern- und Ringkonfigurationen sowie U-förmige und normale Kettenkonfigurationen (*Bild 3*). Die einzelnen Schnittstellenverbindungen unterstützen wahlweise den Uplink- oder Downlink-Modus mit bis zu 48 Uplink- und 24 Downlink-Datenströmen.

bildung 3. Neue CPRI- bzw. OBSAI-basierte Antennenarchitekturen erlauben direkte Verbindungen zur Backplane

Übergangsstrategien

Beim Übergang von einer Technikgeneration zur nächsten kommt es für gewöhnlich zu Überschneidungen, wenn beide Generationen nebeneinander bestehen. Die Gerätehersteller versuchen deshalb in solchen Phasen, die Bedürfnisse mehrerer Technik flexibel abzudecken, damit sie schnell auf neue Nachfragetrends reagieren können.

Eine entsprechende Flexibilität ist besonders für die ersten LTE-Plattformen von Bedeutung, da sich diese momentan zumeist im Laboreinsatz oder Feldversuch befinden. Dank der Flexibilität und Skalierbarkeit des TCI6487 sind Hersteller von Infrastrukturhardware in der Lage, flexibel mehrere verschiedene Protokollstandards und Techniken zu berücksichtigen.

Ist eine Plattform mit mehreren Standards kompatibel, verringert dies die F&E-Kosten des Herstellers und beschleunigt die Markteinführung neuer Produkte. So entwickeln einige Infrastrukturanbieter mit Hilfe des TCI 6487 Multi-Core-DSP-Plattformen, die WCDMA-HSPA und LTE unterstützen; andere wiederum arbeiten an Plattformen für Wimax und LTE.

TI hat eine Bibliothek fertig implementierbarer und ausführlich getesteter LTE-Softwaremodule entwickelt, die

Fortsetzung von Seite 38

arbeiten kann. Daher werden VPN-Gateways meistens als Single-Server-systeme installiert.

Neben der Leistungsfähigkeit ist bei der Auswahl der Geräte darauf zu achten, dass Priorisierung und Traffic Shaping angeboten werden, da kein Einfluss auf das Provider-Netz möglich ist. Durch das Traffic Shaping wird bestimmt, nach welchen Regeln am Ein- oder Ausgangs-Interface der Datenverkehr fließt. Das heißt, ohne Belastung des Interfaces kann 100 % der Leitungskapazität genutzt werden. Bei Nutzung verschiedener Applikationen und Erreichen der oberen Datenratengrenze könnten die letzten 20 % für höher priorisierte Pakete verwendet werden. Die Überlast wird in den internen Puffern zwischengespeichert und nachträglich gesendet oder neu angefordert, während der priorisierte Datenverkehr ohne Verzögerung durchgereicht wird. Anschließend können die Verkehrsklassen für die Applikationen eingerichtet werden, um so die Priorisierung festlegen zu können. Durch die eigenständige Realisierung ist man völlig von denen des Providers unabhängig, kann aber keine durchgängige Qualitätsgarantie schaffen, was aber in den meisten Fällen ausreicht.

Fazit

VPNs werden heute in großem Umfang in allen Unternehmensgrößen eingesetzt. Dabei können sie auch helfen, Kommunikationskosten zu reduzieren. Heutige VPNs sind dabei leistungsfähig genug, um das gesamte Sprach- und Datenaufkommen zu unterstützen. Dabei sollte vorab entschieden werden, ob die VPN-Plattform eigenständig (Provider-unabhängig) aufgebaut oder durch einen Provider der Wahl umgesetzt wer-den sollte. Dies hängt davon ab, welches Know-how im eigenen Unternehmen vorhanden ist und ob überhaupt alle Standorte von einem Provider erreicht werden können. Eine höhere Flexibilität kann man durch die eigenständige Umsetzung oder mit Hilfe eines externen Anbieters erreichen, was sich aber wiederum die Kosten negativ beeinflussen könnte. Das VPN in die Hände eines Providers zu geben, hat hingegen den Vorteil, dass die Wartung, die Einführung neuer Techniken, das Beschaffen neuer Hardware sowie das Management intern eingespart werden können. In jedem Fall stellt die Auswahl eines externen Partners (ob Provider oder neutraler VPN-Anbieter) eine wichtige strategische Unternehmensentscheidung dar, die anhand der eigenen Anforderungen vorab ausreichend überprüft werden sollte. *(bk)*