Mit VPNs Kosten sparen

Vor dem Nutzen steht die gründliche Planung und Konzeption

Kai-Oliver Detken

Viele Unternehmen verfügen heute nicht nur über ein LAN, sondern über mehrere LANs – z.B. an unterschiedlichen Produktionsstandorten oder Filialen – , die über das ganze Land oder sogar die ganze Welt verteilt sind. Die notwendige Frage ihrer Verknüpfung wurde oft mit der Lösung beantwortet, teure Standleitungen zu mieten oder auf Frame-Relay-/ATM-Verbindungen zurückzugreifen.
Wegen der hohen Kosten entstand bald die Variante, das vor jedem Firmensitz liegende öffentliche Netz zu nutzen, um Daten günstiger auszutauschen.
Mit dem Internet kamen inzwischen Aufgaben und Probleme hinzu: Gewährleistung von Sicherheit und Performance, wie sie eine Standleitung oder ein Frame-Relay-/ATM-Netz bieten kann.
Das Ergebnis ist das Konzept des Virtual Private Network.

Kai-Oliver Detken ist Senior IT Consultant der Detken Consultancy & Internet Technologies e.K. sowie Dozent und freier Autor in Grasberg

Ein Vorteil von Virtual Private Networks (VPN), die auf dem Internet Protocol (IP) basieren, ist die Nutzung dieser Technologie auch in allen sonstigen Netzen. Es ist also möglich, die Kommunikation in einem Local Area Network (LAN) oder Wide Area Network (WAN) noch sicherer zu gestalten. Dabei ist es durch gemeinsame Standards möglich, auf die verschiedensten Typen (Software-, Hardware-VPN, unterschiedliche Protokolle und Verschlüsselungsverfahren) zurückzugreifen. Durch die schon heute recht mannigfaltigen Komplettangebote an VPN-Lösungen sollte es jedem Unternehmen möglich sein, ein VPN nach seinen individuellen Spezifikationen aufbauen zu können.
Oftmals werden auch VPN-Dienstleistungen von einem Internet Service Provider (ISP) angeboten. Mit der Abgabe dieses Arbeitsbereiches ist es wiederum möglich, Kosten einzusparen. Allerdings muß abgewogen werden, inwieweit man die Sicherheit des Unternehmens in die Hände anderer Unternehmen legen möchte.
Für die Verbindung der einzelnen Außenstellen werden sogenannte Tunneling-Verfahren eingesetzt, mit deren Hilfe sichere, private Verbindungen für Netzapplikationen über ein öffentliches oder ein unsicheres Medium zwischen abgesetzten Netzen und/oder einzelnen PC-Arbeitsplätzen zu einem zentralen Datennetz aufgebaut werden.

Das Thema in Kürze

Der Aufbau eines VPN bedeutet mannigfaltige Anforderungen an die Planung. Die Kostenvorteile gegenüber Standleitungen und die hohe Flexibilität sprechen für sich. Doch sind auch unausgereifte Standards sowie Sicherheitslücken zu bedenken. Der Beitrag geht auf diese verschiedenen Aspekte ein und zeigt darüber hinaus, daß der Wunsch nach höchster Sicherheit und höchster Performance nur in einem Kompromiß münden kann.

Anforderungen an ein VPN

Der Einsatz von Extranets für Unternehmen bedarf der Berücksichtigung unterschiedlicher Anforderungen, die sich in die nachfolgenden Punkte aufgliedern lassen. Diese Anforderungskriterien muß jedes Unternehmen an ein VPN individuell stellen und berücksichtigen, wenn es effektiv, kostensparend, sicher und leistungsfähig eingesetzt werden soll:

- *Flexibilität:*
  Schnelleres und effizienteres Reagieren von sich ändernden Randbedingungen wie Firmenstandorten, Mobilteilnehmern und Telearbeitsplätzen;
- *Security:*
  Hier ist der wichtigste Punkt die machbare Sicherheit einer solchen logischen Infrastruktur, weil die Kommunikation immerhin über ein ungesichertes Netz stattfindet. Dabei darf es nicht möglich sein, von außen auf die internen Firmendaten zuzugreifen;
- *Integration von Sprache und Daten:*
  Die Integration in ein gemeinsames Netz ermöglicht ein einfacheres Management und starke Kostenreduzierung. Ebenso werden keine separaten Telefon- und Datenleitungen mehr benötigt;
- *Mobilität:*
  Der Teilnehmer möchte nicht mehr zwischen dem Fest- und Mobilfunknetz unterscheiden, wenn er auf die Unternehmensdaten oder Dienste und Applikationen zugreift. Ziel ist es, ungebunden von Ort und Zeit mit der Firma oder dem Kunden in Kontakt zu treten;

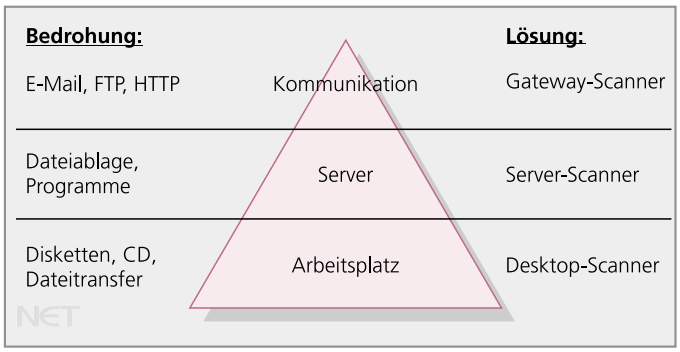

Bild 1: Virenbedrohungen und die jeweiligen Schutzmöglichkeiten

- *Performance:*
  Hiermit ist neben der Leistungsfähigkeit auch die Qualität gemeint, in der der Teilnehmer in der Lage ist, mit einer Gruppe zu kommunizieren. Die Leistungsfähigkeit eines VPN muß sich an der einer Standleitung messen lassen;
- *Verfügbarkeit und Zuverlässigkeit:*
  Die Dienste und Anwendungen müssen immer standortübergreifend verwendet werden können – ohne Verbindungsabbrüche. Durch Einsatz eines Netzwerkmanagementsystems kann z.B. die Verfügbarkeit stark angehoben werden, während der ISP für die Connectivity verantwortlich ist;
- *Transparenz und Kosteneffizienz:*
  Um dies zu erfüllen, muß ein geeignetes Accounting und Billing implementiert sein, das genaue Abrechnungen zuläßt bzw. die eigenen Kosten ständig überprüft, damit man sich nicht aus dem definierten Kostenrahmen bewegt;
- *Offenheit des Systems:*
  Ein Standardkonformes offenes System muß realisiert werden, das zukünftige Entwicklungen mit berücksichtigt. Der Schwerpunkt liegt klar auf dem Internetprotokoll, weshalb auch zukünftig Entwicklungen stark vorangetrieben werden, um das Internet als Dienst-Integrationsplattform zu etablieren.

Absicherung des VPN

Da das VPN als Erweiterung des Intranet über die Organisationsgrenzen hinweg verwendet wird, ist die Sicherheit der wichtigste Punkt der Anforderungen. Bei der Nutzung des Internet als Netz kommt diesem Sachverhalt eine besondere Bedeutung zu, da unternehmensinterne Informationen öffentlich zugänglich werden können. Sicherheit ist besonders kritisch für Organisationen wie Banken und Finanzinstitutionen, die das Netz zur Transaktion von hohen Geldsummen nutzen. Mangelnde Sicherheit in Systemen, Netzen und beim Transport von vertraulichen Daten ist bisher das größte Hindernis.
Wesentliches Kriterium für ein notwendiges Sicherheitskonzept ist daher die Identifikation von Sicherheitslücken in Betriebssystemen und Applikationen, des TCP/IP-Protokolls sowie der unterschiedlichen Angriffstechniken. Dabei muß ein ganzheitlicher Ansatz erfolgen, um das Unternehmen innerhalb eines VPN absichern zu können – angefangen von einem Kommunikationsprofil und der Aufnahme der physischen und logischen Infrastruktur, sind folgende Punkte einzubeziehen:

- Betriebssicherheit;
- Remote Access Points;
- Analyse des Sicherheitsgrades des VPN im Unternehmen;
- Analyse der Sicherheitslücken;
- Anforderungen an das Netz;
- Firewall-Konzeption für die Zugangskontrolle;
- Verschlüsselungssysteme und Authentisierung;
- Viren-Scanner.

Um die Datensicherheit gewährleisten und Angriffe zurückverfolgen zu können, müssen Mechanismen wie Authentifizierung (Nachprüfbarkeit von Benutzern und Daten) und Integrität (Nachprüfbarkeit bzw. Identifikation von Manipulationen der originären Daten) sowie Vertraulichkeit (Datenverschlüsselung) in einem Intranet bzw. VPN unbedingt eingesetzt werden (siehe *Bild 1*).
Um bei Außenarbeitsplätzen die Sicherheit zu erhöhen, muß der Zugangsschutz von Laptops erhöht werden (z.B. durch Smartcards oder biometrische Verfahren wie Fingerabdruckerkennung). Telearbeit wird ebenfalls immer mehr Einfluß auf das Geschäftsleben haben. Der Begriff der Telearbeit läßt sich dabei in Heimarbeit, alternierende und mobile Telearbeit, Satellitenbüros sowie Nachbarschaftsbüros unterteilen.
Zugangsnetze sind GSM-Netze (mobil), ISDN/PSTN (Festnetz, Sprache) und xDSL-Anbindungen (Flate Rate). Die Zugangsarten unterscheiden sich in Performance und Verfügbarkeit, was in einem VPN-Konzept ebenfalls mit berücksichtigt werden muß.

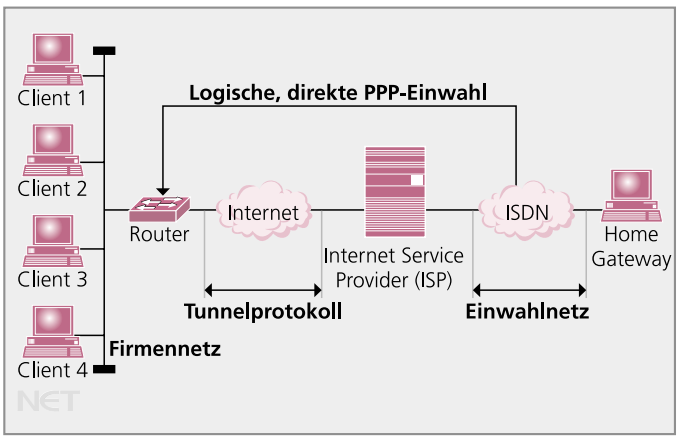

Bild 2: Der Aufbau des VPN über ein Tunnelprotokoll

Tunnel durchs Internet

Eine Absicherung sensitiver Daten ist nicht ohne weiteres möglich. Da die IP-Pakete von zahllosen Systemen transportiert werden, können Unbe-

rechtigte Daten ohne große Probleme mitlesen. Tunnelmechanismen nach RFC-2003 ermöglichen zuallererst die Kopplung von geographisch entfernten Unternehmensnetzen und die Anbindung einzelner Systeme. Die Tunnelmechanismen bieten hierbei den Vorteil eines exklusiven Zugangs unter Vermeidung der Nachteile bei einer üblichen Internet-Anbindung. Das heißt, der Übertragungspfad durch das Internet wird zur virtuellen Verbindung zwischen den jeweiligen Tunnelenden.

Heute wird der Internetzugang meistens über das Point-to-Point-Protocol (PPP) nach RFC-1661 realisiert, um eine Punkt-zu-Punkt-Verbindung vom Endgerät zum Point of Presence (PoP) herzustellen. Das PPP beinhaltet eine Standardmethode zum Transport von Multiprotokoll-Datagrammen und besteht aus drei Komponenten:

- Einkapselung von Multiprotokoll-Datagrammen;
- Link Control Protocol (LCP) zum Etablieren, Konfigurieren und Testen einer Datenverbindung;
- Protokollfamilie des Network Control Protocol (NCP) zum Etablieren und Konfigurieren verschiedener Netzwerkschicht-Protokolle.

Das PPP wurde zum Verbindungsaufbau und zur Authentifizierung entwickelt. Zusätzlich findet eine Überwachung der physischen Verbindung über Protokolle höherer Schichten (z.B. IP), die Vergabe von IPX- bzw. IP-Adressen und das Übertragen von IPX-/IP-Paketen statt. PPP ist aber heute der Quasi-Standard für ISDN-Verbindungen unter Microsoft Windows geworden und findet deshalb am meisten Anwendung. PPP läßt sich unterteilen in das Password Authentication Protocol (PAP) und Challenge Handshake Authentication Protocol (CHAP), die zur Bestätigung und Überprüfung der Identität eingesetzt werden.

Das Zugangssystem ist über ein LAN oder WAN mit dem dahinterliegenden Netz verbunden und leitet die Pakete über PPP zum jeweiligen Zielrechner weiter. Bei der Tunnellösung packt das Zielsystem die vom Teilnehmer empfangenen PPP-Pakete in ein definiertes Tunnelprotokoll ein und transportiert es über das Internet zum Zielsystem. Durch das Tunnelverfahren verhält sich das System so, als ob sich der Teilnehmer direkt eingewählt hätte. Zusätzlich wird der externe Teilnehmer autorisiert, es werden eine IP-Adresse zugewiesen und die IP-/IPX-Pakete entpackt, um sie zum Zielrechner weiterzuleiten. Endgerät für das Tunnelprotokoll kann ein Access Router sein oder ein Server, der in der Lage ist, Tunnelmechanismen zu implementieren. Durch die logische Zugehörigkeit des eingeloggten Teilnehmers entsteht ein VPN (siehe *Bild 2*).

Hersteller/Anbieter	URL	Produkte
Astaro	www.astaro.com	Astaro Security Linux
Avaya	www.avaya.com	VSU5, VSU100R, VSU2000, VSU5000, VSU7500, VSU10000
Bintec	www.bintec.de	X1200, X2300i, X3200, X4100, X4300, X8500
Borderware	www.borderware.com	IPSec Option für Firewall Server
Centrinity	www.centrinity.com	First Class
Checkpoint	www.checkpoint.com	VPN-1 Internet Gateway, VPN-1, VPN-1 Pro, VPN-1 Net
Cisco Systems	www.cisco.com	Cisco 800, Cisco 1710, Cisco 1760, Cisco 2600 Serie, Cisco 3600 Serie, Cisco 3700 Serie, Cisco 7100 Serie, Cisco 7200 Serie, Pix Firewall, VPN 3000 Concentrator-Serie
Cyber Guard	www.cyberguard.com	Cyber Guard IPSec VPN Gateway
D-Link	www.dlink.de	DI-804V
Enterasys Networks	www.enterasys.com	XSR1805
F-Secure	www.f-secure.com	VPN+, VPN+ Gateway
Open IT	www.open-it.com	Free S/WAN
Linogate	www.linogate.de	Defendo
Lucent Technologies	www.lucent.com	Lucent VPN Firewall
Microsoft	www.microsoft.com	ISA Server 2000
NCP	www.ncp.de	Secure VPN/PKI Gateway
Net Screen	www.netscreen.com	Net Screen-5XP Elite, Net Screen-25a, Net Screen-50, Net Screen-100a, Net Screen-208, Net Screen-500, Net Screen-1000, Net Screen-Remote
Nokia	www.nokia.com	Crypto Cluster CC500, IP330
Nortel Networks	www.nortelnetworks.com	Contivity 600, Contivity 1010, Contivity 1050, Contivity 1100, Contivity 1600, Contivity 1700, Contivity 2600, Contivity 2700, Contivity 4600
PGP Corporation	www.pgp.com	PGP Enterprise Tool, PGP Mobile, PGP PersonalPGP SDK
SecGo Solutions	www.secgo.com	Secgo Crypto IP, Secgo Crypto IP v3
Secure Computing	www.securecomputing.com	Sidewinder
Sonic Wall	www.sonicwall.com	GX250, GX650, Pro 100, Pro 200, Pro 300, Soho 3/10, Soho 3/50, Tele 3, Tele 3 TZ
Suse	www.suse.de	Suse Firewall on CD VPN
Symantec	www.symantec.com	Firewall + VPN Appliance 100, Firewall + VPN Appliance 200(R), Firewall/VPN 200 R, Gateway Security Appliance 5110, Gateway Security Appliance 5200, Gateway Security Appliance 5300, Veloci Raptor 500, Veloci Raptor 700, Veloci Raptor 1000
Watch Guard	www.watchguard.com	Firebox

Tabelle: Eine Übersicht von Herstellern bzw. Anbietern des VPN-Marktes (Auswahl)

Es gibt unterschiedliche Möglichkeiten, Tunnel für VPNs aufzusetzen bzw. realisieren zu lassen:

- *Inhouse:*
  Das Unternehmen setzt eigenverantwortlich einen Tunnel durch das Internet auf, um ein globales VPN realisieren zu können. Dabei befindet sich ein Tunnel-Server im eigenen Intranet. Auf den Clients muß spezielle Software vorhanden sein, um auf das Netz zugreifen zu können;
- *Outsourcing:*
  Der Internet Service Provider nimmt dem Kunden das Problem der Reali-

sierung ab. Dadurch lassen sich Kosten einsparen sowie die Verantwortung an den ISP abgeben. Die Unternehmen am VPN sind mittels einer Wähl- oder Mietleitung mit dem ISP verbunden. Zusätzlich ist keine weitere Software notwendig;

- *Hybride Lösung:*
  Diese Variante unterteilt die Realisierung in den Bereich ISP und Unternehmen. Auch hier ist der ISP für den Aufbau und das Management des Tunneling verantwortlich. Der Tunnel-Server steht hingegen beim Unternehmen.

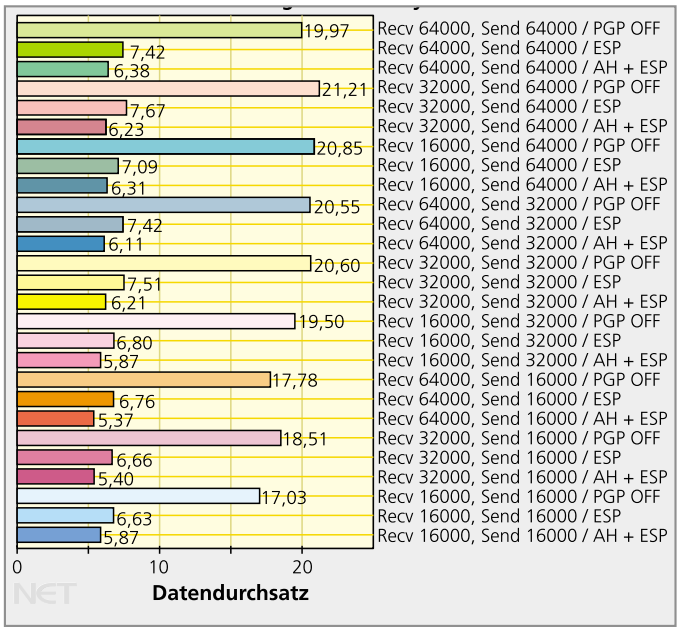

Bild 3: Der Datendurchsatz in einem konkreten Test bei Paketen mit 1500 Byte

Unterschiede gibt es sowohl bei den Mechanismen als auch bei der Realisierung auf den jeweiligen Schichten. Ist beispielsweise der Client für den Aufbau eines Tunnels verantwortlich, muß der Client als Tunnel-Server auch über die notwendige Software verfügen. Wird hingegen der Aufbau einer Verbindung durch einen Remote Access Server (RAS) vorgenommen, ist dieser für alle Verbindungen zuständig. Die Clients benötigen dabei kein Software-Upgrade.

Performancevergleich

Durch den Einsatz von Verschlüsselungsverfahren (symmetrisch, asymmetrisch) werden die Tunnel für die Daten erst abgesichert. Asymmetrische Verschlüsselungsverfahren sind etwa um den Faktor Tausend langsamer im Vergleich zur symmetrischen Variante. Beide Verfahren sind allerdings notwendig, um Authentisierung und Verschlüsselung gleichermaßen zu betreiben. Kryptografische Algorithmen, auf Hardware implementiert, können die Performance erheblich steigern. Hier muß letztendlich zwischen Kosten/Nutzen bzw. Leistung/Sicherheit entschieden werden. Wenn man eine höhere Sicherheit, sprich Verschlüsselung, erhalten will, muß man Einschränkungen in der Performance hinnehmen.

In einem konkreten Beispiel wurden Performance-Messungen zwischen zwei Windows-2000-Plattformen vorgenommen. Die Ausstattung bestand dabei aus einem 600-MHz-Prozessor AMD K7 Athlon, PCI-32-Bus sowie 256 Mbyte RAM. Die Messungen wurden mit den Parametern Receive-/Send-Socket 16, 32 und 64 kbyte durchgeführt.

Bild 3 zeigt dabei die optimale Paketgröße von 1500 Byte, die verwendet wurde, da sie unfragmentiert weitergeleitet wird. Zur Verschlüsselung und zum Tunnelaufbau wurde das Tool PGPnet (www.pgp.com) verwendet, das standardmäßig IPsec (Layer-3-Protokoll) mit CAST (Verschlüsselung) nutzt.

Wie man an der Meßabbildung erkennen kann, sind durch die Verschlüsselung klare Performance-Einbußen zu verzeichnen. Dabei nimmt eine Authentifizierung plus Verschlüsselung mehr auf die Datenrate Einfluß, als wenn man ausschließlich eine Authentifizierung vornimmt. Die Sende- und Empfangspuffer an den jeweiligen Endgeräten lassen ebenfalls eine unterschiedliche Datenrate erkennen, die aber tolerierbar ist.

Resümee

Der Aufbau eines VPN bedeutet auch mannigfaltige Anforderungen an die Planung und Konzeption. Die Kostenvorteile gegenüber Standleitungen und die hohe Flexibilität sprechen als Vorteile für sich. Allerdings erschweren noch unausgereifte Standards sowie Sicherheitslücken die Akzeptanz. Aus diesem Grund sollte man möglichst noch auf einen Hersteller für die gesamte Lösung zurückgreifen und diese vor dem Produktivbetrieb ausgiebig testen.

Weiterhin sind heutige Lösungen (Software, Hardware) stark von den verwendeten Block-Chiffrier-Algorithmen abhängig. Sie besitzen eine erhebliche Abhängigkeit von der Prozessorleistung, so daß teilweise nur noch ein kleiner Teil der eigentlich möglichen Übertragungsgeschwindigkeit der Netzhardware erreicht wird.

Bei der Performance sind Algorithmen wie CAST als auch 3DES als nachteilig für Applikationen mit hohem Datendurchsatz zu werten. Hier läßt sich die höchste Performance nur durch Hardware-Lösungen erreichen. Dies bedeutet, daß Server, die mit z.B. IPsec arbeiten sollen, entsprechend ausgelegt werden müssen, damit diese den geplanten Clients noch eine ausreichende Performance zur Verfügung stellen können.

Die gesteigerte Sicherheit geht im Normalfall zu Lasten der Netz-Performance. Dies zeigt auch, daß nicht jedes System in der Lage ist, IPsec-gesicherten Verkehr zu unterstützen. Hierzu zählen insbesondere Mikrocontroller mit TCP/IP-Stack, die allein die nötige Rechenleistung nicht aufbringen können, um z.B. Echtzeitdatenströme darüber zu übertragen.

(we)