

Virtuelle Privatnetzwerke in der Praxis

Virtuelle Privatnetzwerke erfreuen sich in der Geschäftswelt zunehmender Beliebtheit. Immer mehr Firmen, insbesondere im Segment der kleinen und mittleren Unternehmen, nutzen diese Netzwerktechnologie für die Übertragung firmeninterner Informationen.

Von Dr. Ivan Roman

Der Autor ist Geschäftsführer der Roman Consulting und Engineering AG in Zürich.

2

Der Nutzen der virtuellen Privatnetzwerke (VPN) liegt auf der Hand: Es ist primär der finanzielle Aspekt. Anwendungen für VPN sind meist wesentlich kleiner als für klassische Verbindungen, wie etwa Mietleitungen. Ein weiterer Vorteil liegt in ihrer Flexibilität, lassen sich doch VPN-Verbindungen i.d.R. schnell aufbauen und an neue Gegebenheiten anpassen. Bei der Konfiguration von VPN-Verbindungen sehen sich Anwender jedoch oft mit verschiedenen Problemen konfrontiert. In den nachfolgenden Abschnitten werden einige dieser Probleme diskutiert und entsprechende Lösungsansätze vorgeschlagen. Am Schluss des Artikels wird auf einige Aspekte hingewiesen, die es bei der Planung zu berücksichtigen gilt.

VPN-Problembereiche und Lösungsansätze

VPN zwischen Produkten verschiedener Hersteller

Bei VPN-Verbindungen wird in der Regel das Internet Security Protocol IPsec eingesetzt. Dieses Protokoll umfasst eine Reihe von Standards (RFC), die von der Internet Engineering Task Force (IETF) definiert wurden. Diese Standards bilden ein Rahmenwerk für die Verschlüsselung, Integrität und Authentifizierung sicherheitsrelevanter Daten auf der Netzwerkschicht. IPsec wird heute von den meisten relevanten Herstellern unterstützt und stellt damit de facto den Industriestandard dar. Das Problem steckt jedoch – wie so oft – im Detail: Je nach Hersteller werden nämlich gewisse

Funktionen auf je andere Weise implementiert. Als Folge davon treten nicht selten Kompatibilitätsprobleme auf.

VPN und IP-Adressierung

Bei grossen Firmen ist es üblich, auf beiden Seiten eines VPN-Tunnels so genannte statische Adressen, also fixe IP-Adressen, zu verwenden. Im KMU-Segment dagegen werden oft dynamische, vom Provider zeitlich zugeteilte Adressen eingesetzt. Nutzt einer der Kommunikationspartner im VPN eine dynamische Adresse, der andere jedoch eine statische, muss der Verbindungsaufbau zwingend von der Seite her erfolgen, welcher die dynamische Adresse zugeteilt wurde. Als Steigerung existiert auch die Möglichkeit, beiden Seiten eine dynamische Adresse zuzuweisen. In diesem Fall muss auf die Dienste so genannter dynamischer DNS-Server zurückgegriffen werden, beispielsweise www.dyndns.org. Die dynamischen DNS-Server lösen die statischen Namen in dynamische IP-Adressen auf und ermöglichen somit den Aufbau und Betrieb von VPNs.

Zu beachten ist ferner, dass nicht alle Produkte die Kombination «dynamisch-statisch» und noch weniger die Kombination «dynamisch-dynamisch» unterstützen. Entsprechende Vorabklärungen sind daher unerlässlich. Zu letzterer Variante ist zu bemerken, dass beim Ausfall eines solchen dynamischen DNS-Servers eine VPN-Verbindung nicht möglich ist. Im professionellen Umfeld sollte daher auf die doppel-dynamische Variante eher verzichtet werden.

VPN und NAT

Die Abkürzung NAT steht für Network Address Translation (RFC 3022). NAT

ASPEKTE, DIE ES BEI DER VPN-KONFIGURATION ZU BEACHTEN GILT:

- Wie werden die Adressbereiche der für den VPN-Verkehr zugelassenen Rechner angegeben? (z.B. Address-Ranges oder Subnets)
- Gehören die VPN-Systeme selbst zu diesen Adress-Bereichen?
- Sind die Vorgabe-Werte (Defaults) einzelner Parameter bei beiden VPN-Systemen gleich oder müssen sie angeglichen werden?
- Sind die Eingabeformate (dezimal oder hexadezimal) identisch?
- Sind die verwendeten Terminologien auf beiden VPN-Systemen identisch oder bedeuten gewisse Begriffe je nach Hersteller etwas anderes?
- Sind bereits gewisse Parameter «hard-coded» gesetzt? (Einige Hersteller setzen gewisse Parameter stillschweigend als Default ein.)

Lösungsmassnahmen:

- Lesen der Original-Handbücher beider Kommunikations-Seiten
- Beim IPsec-Verfahren gibt es zwei Methoden für den Schlüsselaustausch: IKE (Internet Key Exchange) und Manual.
- Die IKE-Methode ist bequemer. Das System übernimmt dabei gewisse Funktionen. Bei Kompatibilitätsproblemen funktioniert IKE manchmal nicht. In solchen Situationen ist es hilfreich, die Manual-Methode einzusetzen.
- Auch bei VPNs zwischen zwei Produkten des gleichen Herstellers treten manchmal Probleme auf. Das Angleichen der Firmware-Software-Version minimiert die möglichen Fehlerquellen.

erlaubt eine transparente Umsetzung zwischen den internen Adressen eines LAN und der Adresszuordnung im öffentlichen Netz. Meist wird die NAT-Methode für die Abbildung vieler internen Adressen in eine öffentliche Adresse eingesetzt. Dadurch lässt sich der Bedarf an offiziellen Adressen reduzieren und die Zugangssicherheit erhöhen. Beim Einsatz der NAT-Technik im IPSec-VPN-Umfeld sollte zuerst abgeklärt werden, ob und wie NAT unterstützt wird. Andernfalls muss je nach Betriebsart mit Problemen gerechnet werden.

Die Probleme rühren beispielsweise daher, dass durch die Änderung der IP-Adressen gewisse Prüfsummen (message integrity checks) nicht mehr stimmen. (Detaillierte Informationen sind im RFC Draft «IPsec-NAT Compatibility Requirements», draft-ietf-ipsec-nat-reqts-04.txt, März 2003 auf-

geführt.) Als Lösung wird oft die «ipsec nat transversal»-Funktion verwendet, die den VPN-Durchgang erlaubt. Diese Funktion wird jedoch nicht von allen Geräten unterstützt.

Abwehrmassnahmen

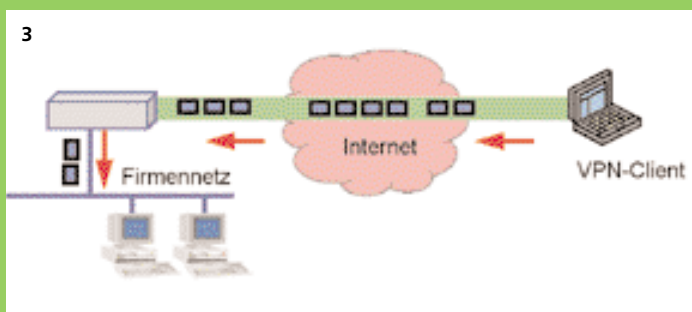
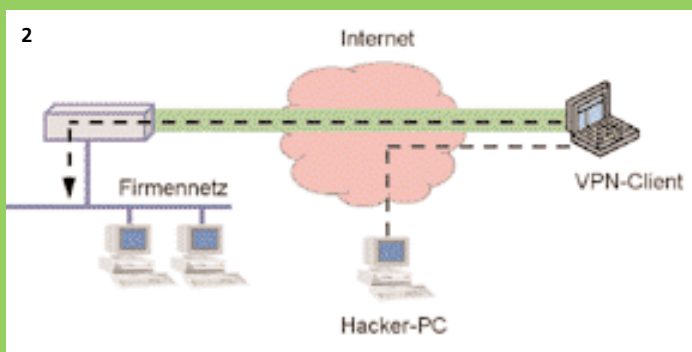
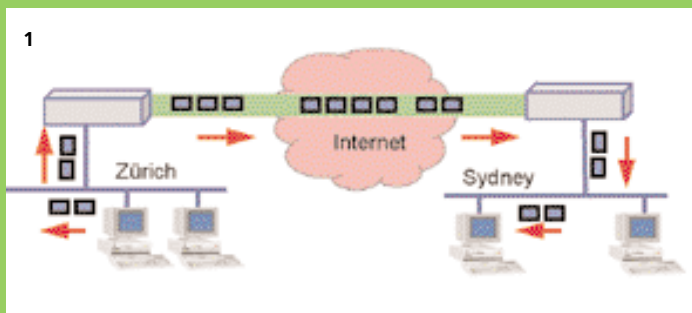
Bei Einsatz der VPN-Software muss die Verträglichkeit der Applikations-Software sorgfältig mit der VPN-Software getestet werden. Die Aspekte der Benutzerfreundlichkeit sollten dabei mit berücksichtigt werden. Bei einer grösseren Anzahl von Clients «im Feld» ist es zudem von Vorteil, die Aktualisierung der Software im voraus zu planen. Auch mit dem Szenario «Diebstahl» muss leider immer gerechnet werden. In diesem Fall darf der Dieb keinen Einblick in gespeicherte Daten und keinen Zugang zum Firmennetzwerk erhalten. Effiziente Authentifizierung (z. B. mittels Smart

Card) erhöht die Zugangssicherheit. Überdies sichert die Verschlüsselung der Daten auf der Festplatte der Notebooks die Vertraulichkeit der Daten.

VPN und Durchsatz

Beim VPN-Einsatz sollten auch Durchsatzaspekte berücksichtigt werden.

Durchsatz und Internet-Anschluss:
Viele Firmen, insbesondere im KMU-Segment, setzen für die Internet-Kommunikation die ADSL-Technologie ein. Der Buchstabe A steht dabei für «asymmetric». Asymmetrisch bedeutet, dass die verfügbare Bandbreite asymmetrisch, also nicht gleichmässig verteilt wird. Ein kleiner Teil der Bandbreite wird für den «Upload», der grössere Teil für «Download» verwendet. Diese Aufteilung ist beim Surfen im Internet sinnvoll. Bei VPN kann die ungleichmässige Bandbreiten-Auftei-



1 – Die Vertraulichkeit der Informationen wird erreicht, indem vor der Übertragung über die öffentliche Infrastruktur die Daten verschlüsselt und nach dem Empfang auf der anderen Seite entschlüsselt werden.

2 – Mittels VPN-Clients lässt sich eine verschlüsselte Verbindung zwischen einem Aussendienstmitarbeiter mit Laptop und dem Firmen-LAN aufbauen.

3 – Beim Einsatz von VPN-Clients ist zu beachten, dass es nicht möglich ist, vom Internet via VPN ins Innere des Firmennetzes zu gelangen.

VPN-CLIENTS

Eine interessante Form von VPNs bilden die so genannten VPN-Clients. Bei dieser Form wird die VPN-Software (z. B.: SafeNet, SoftRemote, SSH Sentinel) direkt auf einem PC, in der Regel einem Notebook, installiert. Auf diese Art lässt sich eine verschlüsselte Verbindung zwischen einem Aussendienstmitarbeiter mit Laptop und dem Firmen-LAN aufbauen (siehe Abbildung 2).

Zu beachten sind folgende Aspekte:

- Verträglichkeit der aktuellen Software mit der VPN-Software.
- Installation und Aktualisierung der VPN-Software, insbesondere bei einer grossen Anzahl der Clients «im Feld».
- Szenario «Diebstahl»
- Kombination VPN- und Internet-Verkehr

lung sinnvoll sein, muss aber nicht. Sie hängt von der Richtung und der Menge der zu übertragenden Daten ab.

Durchsatz und Verschlüsselung:

Die Verschlüsselung hat ebenfalls einen Einfluss auf den Datendurchsatz. Insbesondere die Software-basierende Verschlüsselung kann den Durchsatz verkleinern. Die Hardware-basierende Verschlüsselung ist im Vergleich zu den Softwarelösungen leistungsfähiger. Auch die Wahl des Verschlüsselungsalgorithmus spielt eine Rolle. In der Regel unterstützen die VPN-Systeme den DES- und 3DES-Algorithmus. 3DES ist zweifellos sicherer als der DES-Algorithmus. Diese Sicherheitserhöhung ist aber mit höherem Verarbeitungsaufwand und eventuell mit verminderten Durchsatz verbunden. Im konkreten Fall muss überlegt werden, welche Faktoren überhaupt den Durchsatz limitieren. Eventuell ist dies nämlich die verfügbare Bandbreite und nicht etwa die Verschlüsselung.

Durchsatz und Anwendungen:

Ein Ernst zu nehmender Faktor (vergleiche Kasten VPN-Planung) sind die eingesetzten Anwendungen. Was will man überhaupt durch den Tunnel «durchschleusen»? Will man bloss gelegentlich eine Offerte oder einige wenige Informationen übermitteln oder will man permanent via VPN-Tunnel ans Firmennetz angeschlossen bleiben und via LAN arbeiten? Einige Anwendungen weisen bezüglich des zeitlichen Verhaltens grosse Sensibilität auf und brechen bei Nicht-Einhalten der entsprechenden «Timers» nicht selten die Sitzungen ab.

Zusammenfassung

VPN ist eine attraktive Technologie, bei der das Internet als Übertragungsmedium zwischen einzelnen Filialen oder zwischen Filialen und einzelnen Mitarbeitern fungiert. Die Verbin-

dung dazwischen wird verschlüsselt und verhindert damit, dass sensitive Daten im Internet gelesen, gefälscht oder modifiziert werden können. Die VPN-Technologie ermöglicht somit, Kosten für Datenleitungen zu sparen. Obschon VPNs heute bereits vielerorts im Einsatz stehen, ist eine Implementierung nicht einfach und sollte – besonders bei grossen Einsätzen – sorgfältig im voraus geplant werden. ◆

VPN-PLANUNG

Viele Probleme lassen sich vermeiden, wenn vor dem VPN-Einsatz eine gute Planung, eine Pilotphase und eine sorgfältige Einführung durchgeführt wird. Insbesondere sollten die Anforderungen an eine zukünftige VPN-Lösung sorgfältig geprüft werden.

In dieser Phase stellen sich folgende Fragen:

- Welche Anwendungen werden eingesetzt?
- Wie zeitsensitiv sind die Anwendungen?
- Wie sehen die Sicherheitsanforderungen bezüglich der Verschlüsselung aus?
- Wie sehen die Verfügbarkeitsanforderungen aus?
- Gibt es Probleme beim Einsatz der Verschlüsselungssoftware in fremden Ländern (z. B. Export- und Einsatzbeschränkungen)?
- Welche Netzwerk-Protokolle (IP, IPX, AppleTalk) werden eingesetzt?
- Welche Durchsätze sind erwünscht/möglich?
- Welche Geschäftsstellen werden eingebunden?
- Wie viele Client-VPNs werden benötigt?
- Wie viele gleichzeitige VPN-Verbindungen werden benötigt?
- Wie werden die VPNs ins Netzwerkmanagement eingebunden?
- Wie sehen die Wachstumsprognosen aus?

HP GEWINNT WEITEREN GROSSAUFTRAG IM IT-OUTSOURCING

HP hat mit Ericsson einen Vertrag über weitgehende Outsourcing-Services abgeschlossen. Im Rahmen des Vertrags mit einer Laufzeit von fünf Jahren übernimmt HP Services die Verantwortung für die globale IT-Infrastruktur von Ericsson. Damit gewinnt HP Services innerhalb von kurzer Zeit einen weiteren Grosskunden für IT-Outsourcing.

TRANSFER VON DIGITALEN INHALTEN

16 führende Hersteller von Unterhaltungselektronik, Computern und mobilen Geräten haben die Gründung der «Digital Home Working Group» (DHWG) bekannt gegeben. Die Gruppe, der unter anderem Fujitsu, HP, Intel, IBM und Nokia angehören, will die gemeinsame Nutzung von digitalen-Inhalten wie digitaler Musik, Fotos und Videos zwischen Unterhaltungselektronik, mobilen Geräten und PCs vereinfachen.

FILENET FÜHREND BEI GESCHÄFTSPROZESS-MANAGEMENT

Analysten des Marktforschungs- und Beratungsunternehmens Gartner Inc. bewerten FileNet bei Lösungen für Business Process Management (BPM) als führend. Dies geht aus einem kürzlich veröffentlichten Bericht mit dem Titel «Magic Quadrant for Pure-Play BPM, 2Q03» hervor.

LCD-MARKT BOOMT

Ein glänzendes Zeugnis stellen die kalifornischen Marktforscher von iSuppli/Stanford Resources dem weltweiten LCD-Markt aus. Dieser hat nach ihren Berechnungen im ersten Halbjahr ein Volumen von 13,7 Mrd. Dollar erreicht und damit gegenüber dem Vorjahr um knapp sieben Prozent zugelegt. Auch für die Zukunft sagen die Marktforscher rosige Zeiten für LC-Displays bei Computer, Fernsehern und Handys voraus.