Zeitschrift: Bulletin des Schweizerischen Elektrotechnischen Vereins, des Verbandes Schweizerischer Elektrizitätsunternehmen = Bulletin de l'Association suisse des électriciens, de l'Association des entreprises électriques suisses

Herausgeber: Schweizerischer Elektrotechnischer Verein ; Verband Schweizerischer Elektrizitätsunternehmen

Band: 92 (2001)

Heft: 1

Artikel: Sichere Infrastrukturen im Internet-Umfeld

Autor: Weingartner, Hanspeter

DOI: https://doi.org/10.5169/seals-855650

Nutzungsbedingungen

Die ETH-Bibliothek ist die Anbieterin der digitalisierten Zeitschriften auf E-Periodica. Sie besitzt keine Urheberrechte an den Zeitschriften und ist nicht verantwortlich für deren Inhalte. Die Rechte liegen in der Regel bei den Herausgebern beziehungsweise den externen Rechteinhabern. Das Veröffentlichen von Bildern in Print- und Online-Publikationen sowie auf Social Media-Kanälen oder Webseiten ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Mehr erfahren

Conditions d'utilisation

L'ETH Library est le fournisseur des revues numérisées. Elle ne détient aucun droit d'auteur sur les revues et n'est pas responsable de leur contenu. En règle générale, les droits sont détenus par les éditeurs ou les détenteurs de droits externes. La reproduction d'images dans des publications imprimées ou en ligne ainsi que sur des canaux de médias sociaux ou des sites web n'est autorisée qu'avec l'accord préalable des détenteurs des droits. En savoir plus

Terms of use

The ETH Library is the provider of the digitised journals. It does not own any copyrights to the journals and is not responsible for their content. The rights usually lie with the publishers or the external rights holders. Publishing images in print and online publications, as well as on social media channels or websites, is only permitted with the prior consent of the rights holders. Find out more

Download PDF: 12.07.2025

ETH-Bibliothek Zürich, E-Periodica, https://www.e-periodica.ch

Sichere Infrastrukturen im Internet-Umfeld

Einführung und Konzepte für Virtual Private Network (VPN)

Ursprünglich wurden Computer als Stand-alone-Geräte konzipiert, was den Austausch von Daten zwischen den einzelnen Rechnern beschränkte. Vor allem grosse Unternehmen begannen daher schon früh, ihre Computer zu vernetzen. Mit der Vernetzung gehen Firmen allerdings aber auch das Risiko ein, dass Dritte Einsicht in die transferierten Daten erhalten oder diese manipulieren können. Mit verschiedenen Technologien kann die Datensicherheit wesentlich erhöht werden.

Dank immer schnelleren Computern, immer einfacher zu bedienender Software und den damaligen Vernetzungsmöglichkeiten verbreiteten sich in den 90er Jahren private und institutionelle Netzwerke explosionsartig. Diese Netzwerke liessen sich ab Ende der 90er Jahre auch relativ einfach weltweit miteinander verbinden. Das wohl effektivste und kostengünstigste Vernetzungsmedium dafür ist das Internet.

Die Vorteile des Arbeitens mit dem Internet sind enorm: Es lassen sich in kürzester Zeit Informationen finden, für deren Suche man früher Tage oder Wochen benötigt hätte. Nur leider sind auch die Risiken beträchtlich. Jede Person, die Zugriff auf das Internet hat, kann auf die Web-Server eines Netzwerks zugreifen. Sie kann E-Mails verschicken, die auf jeder Harddisk gespeichert werden können. Sobald man mit dem Internet verbunden ist, befindet man sich in einem öffentlich zugänglichen Netzwerk. Dort muss man seine Daten vor unberechtigtem Zugriff schützen, so wie man die Türe des Autos abschliesst, wenn man dieses auf einem öffentlich zugänglichen Parkplatz abstellt.

Adresse des Autors
Hanspeter Weingartner, DDS NetCom AG
8320 Fehraltorf, weingartner@dds.ch

Bedrohung für Netzwerke

Wichtige Aspekte für die Datensicherheit sind:

- Authentifizierung: Mit einer Authentifizierung stellt man sicher, dass eine Person, die auf ein privates Netzwerk Zugriff hat und welche mit dessen Servern Daten austauscht, auch tatsächlich diejenige Person ist, für die sie sich ausgibt.
- Vertraulichkeit der Daten: Die Vertraulichkeit der Daten ist sichergestellt, wenn niemand private Daten ohne Berechtigung lesen kann.
- Integrität der Daten: Die Datenintegrität ist sichergestellt, wenn private Daten während der Übertragung über ein öffentlich zugängliches Netzwerk in keiner Weise verändert werden können.

Das heute meist eingesetzte Übertragungsprotokoll ist TCP/IP (Transmission Control Protocol/Internet Protocol). Netzwerke, die mit diesem Protokoll arbeiten, sind ursprünglich nicht so entwickelt worden, dass die drei oben beschriebenen Sicherheitsanforderungen problemlos unterstützt und angeboten werden können. Ohne zusätzlichen Schutz sind die Daten verschiedenen Bedrohungen ausgesetzt, auf deren wichtigste im Folgenden kurz eingegangen wird:

Spoofing

Wie in anderen Netzwerken haben auch die Geräte in IP-Netzwerken eine numerische Adresse. Die Quell- und Zieladresse ist in jedem Datenpaket, das übertragen wird, enthalten. Unter Spoofing wird das unberechtigte Verwenden einer fremden IP-Adresse verstanden, wobei ein Aggressor eine falsche Quell-

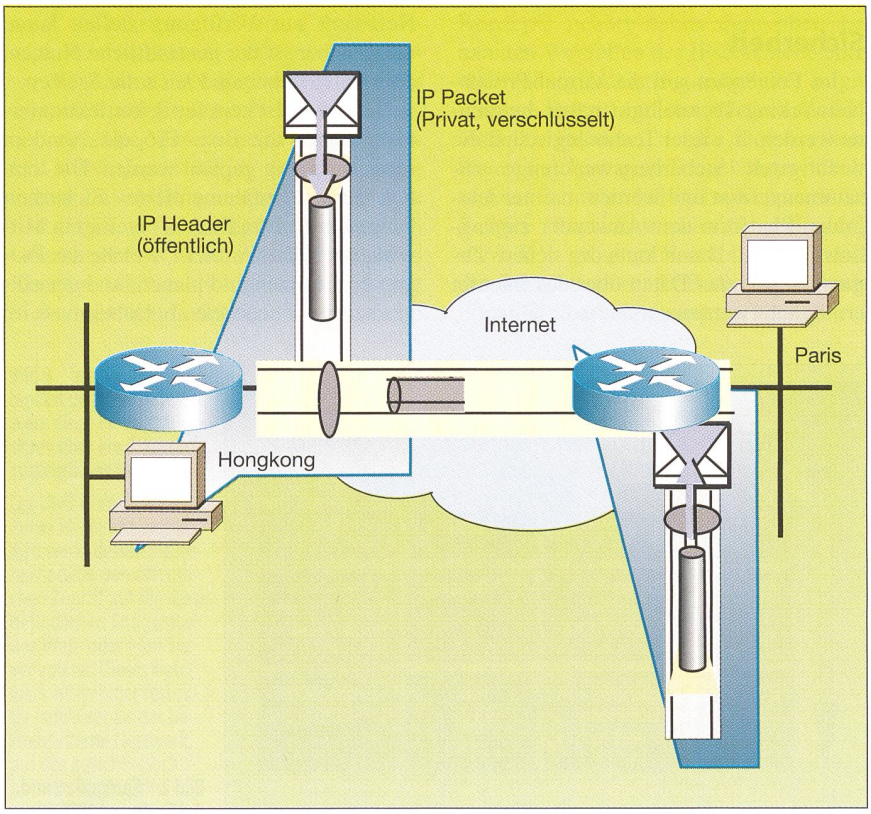

Bild 1 **Prinzip des VPN.** Quelle: Cisco Systems

oder Zieladresse angibt. Spoofing ist die Grundlage von verschiedenen Attacken, wie im Folgenden gezeigt wird.

DoS (Denial of Service)

In den meisten Fällen sendet der Aggressor mit einer falschen Quelladresse eine Vielzahl von Datenpaketen an die mittels Spoofing herausgefundene Zieladresse, so dass die Kommunikationskapazität des Geräts mit der Zieladresse so überlastet wird, dass es sich aus dem Netzwerk abmeldet. Somit ist diese Adresse natürlich auch für berechtigte Nutzer nicht mehr erreichbar, was zu grossen kommerziellen Verlusten oder Imageschäden führen kann.

Session Hijacking

Bei dieser Attacke übernimmt ein Aggressor die Kontrolle über eine aktuelle Verbindung (Session) zwischen zwei Computern, nachdem er die Existenz dieser Session mittels Sniffing (hard- oder softwarebasierender, frei auf dem Markt erhältlicher Protokollanalyser) herausgefunden hat. Dies kann am Ende dazu führen, dass ein Server unbemerkt Unternehmensdaten einem Unberechtigten zur Verfügung stellt. Einen wirksamen Schutz gegen solche Attacken bildet das Verschlüsseln der Daten vor deren Übertragung über das öffentliche (Extranet) oder auch interne (Intranet) Netzwerk.

Sicherheit

Im Folgenden soll die Virtual-Private-Networking-Technologie näher betrachtet werden. In dieser Technologie sind die wichtigsten Sicherheitswerkzeuge zusammengefasst und werden in einer integralen Plattform dem Anwender zugänglich gemacht. Damit kann der sichere Zugang zu privaten Daten über das Internet ermöglicht werden.

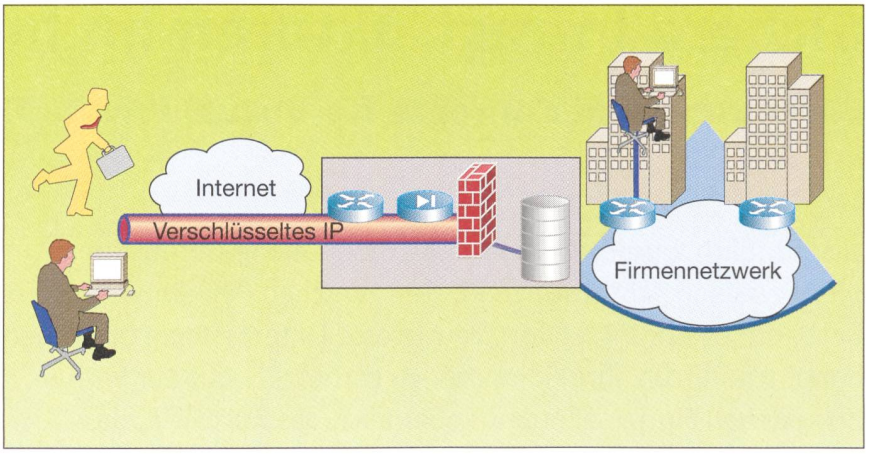

Bild 3 Remote-Access-VPN ermöglichen den Zugriff über ein öffentliches Netzwerk auf ein Intranet oder ein Extranet. Quelle: Cisco Systems

Infolge des Wandels der Geschäftsstrukturen werden immer höhere Anforderungen an Datennetzwerke gestellt, wobei sich diese Modelle immer weniger an den internen Beziehungen, sondern immer mehr an den Kunden- und Partnerbeziehungen orientieren. Dabei ist die schnelle Einführung von neuen Technologien und Diensten sowie die layer- und domänenübergreifende (interne und externe) Vernetzung äusserst wichtig geworden (Layer: OSI-Modell der sieben Kommunikationsschichten nach ISO; Domäne: organisatorische Einheit zur Verwaltung von Endgeräten in grösseren Netzwerken). Je mehr Möglichkeiten ein Netzwerk zur Verfügung stellen kann, umso höher ist der geschäftliche Nutzen, aber umso höher sind auch die Risiken.

Sicherheit ist kein fertig konfektioniertes «Out of the Box»-Produkt, sondern muss sorgfältig geplant werden. Die letzten Endes implementierte Sicherheit hängt von den am Projekt beteiligten Mitwirkenden, den Partnern, welche das Projekt konzipieren und planen, und der eingesetzten Technologie ab. Dabei muss im Speziellen auf die Durchgängigkeit, auf die gute Skalierbarkeit, auf ein optimales Kosten-Nutzen-Verhältnis, auf den Investitionsschutz und auf die einfache Umsetzbarkeit der Sicherheitspolitik besonderer Wert gelegt werden.

Virtual Private Networking

Ein Virtual Private Network (VPN) ist ein Netzwerk, das den sicheren Zugriff entfernter Netzwerke oder einzelner Anwender über ein öffentlich zugängliches Medium auf ein anderes Netzwerk ermöglicht. Diese Technologie nützt das öffentlich zugängliche Datennetz, um eine private Verbindung zwischen zwei Netzwerkknoten herzustellen (Bild 1).

VPN können im Internet oder auf dem Backbone eines Service Providers in einer IP-, Frame-Relay- oder ATM-Infrastruktur gebildet werden. Mittels der VPN-Technologie können Daten über ein öffentliches Netzwerk mit einer vergleichbaren Sicherheit wie im internen Netzwerk übertragen werden.

Folgende Technologien machen die Anwendung von VPN überhaupt erst möglich:

- Tunnelling (Bilden einer virtuellen Punkt-zu-Punkt-Verbindung über das Internet)
- Verschlüsselung (Encryption)
- QoS (Quality of Services)
- Umfassende Sicherheit (Statefull Inspection einer Firewall).

Oft wird die Frage gestellt, warum überhaupt ein VPN-Konzept für die Datenübertragung eingesetzt werden soll. Dafür gibt es viele Gründe. Die wichtigsten sind:

- Das Übertragen von Firmendaten ist sicherheitsrelevant. VPN-Konzepte er-

Zeit	Typ	Applikation	Ersatz für	Vorteile
	Remote-Access VPN	Mobile Benutzer, Fernverbindung	vorgegebene Rufwahl, ISDN	Zugang von überall her möglich, tiefe Kosten
	Intranet VPN	Site-to-Site, interne Verbindung	Mietleitung	Erweiterte Verbindungsmöglichkeiten, tiefe Kosten
	Extranet VPN	Business-to-Business, ext. Verbindung	Fax Mail EDI	Ermöglicht E-Commerce

Bild 2 Kategorien und Attribute von VPN. Quelle: Cisco Systems

möglichen das sichere Übertragen von Firmendaten über öffentliche Datennetze.
- Das Übertragen von Firmendaten verursacht Kosten. Der Einsatz des Internets als WAN kann diese Kosten erheblich reduzieren, da teure Infrastrukturen für Mietleitungen oder Frame-Relay-Services reduziert werden können.
- Der sichere Zugriff von mobilen Anwendern ist aufwändig und teuer. Auch diese Kosten können erheblich reduziert werden. Der VPN-Zugriff von mobilen Anwendern auf ein internes Netzwerk wird oft auch als Virtual Private Dial-up Networking (VPDN) bezeichnet.
- Die Verbindungsmöglichkeiten sind vielfältig. Ein VPN kann auf verschiedenen physikalischen Medien wie Cable Modem, DSL, ISDN, analoger Telefonie oder Ethernet aufgebaut und betrieben werden.
- Ein Extranet wird in Zukunft schneller und einfacher zu entwickeln sein. Der Anwender wird sein Extranet ohne fremde Hilfe gestalten und in Betrieb setzen können. Dazu wird eine einfache, leistungsfähige und sichere Übertragungsinfrastruktur benötigt.

Die drei Haupttypen von VPN, nämlich Remote-Access-VPN, Intranet-VPN und Extranet-VPN (Bild 2), sollen nachfolgend vorgestellt werden.

Remote-Access-VPN

Remote-Access-VPN (Bild 3) ermöglichen den externen Zugriff über ein öffentlich zugängliches Netzwerk wie das Internet auf ein Intranet oder ein Extranet. Sie verwenden analoge oder digitale Wählleitungen, ISDN, DSL, Mobile IP und Cable-Modem-Technologien für den Aufbau einer sicheren Verbindung von mobilen Anwendern, Heimwerkern und Verkaufsbüros zu einem firmeninternen Netzwerk. Sie sind auf geringe Datenaufkommen ausgelegt und ermöglichen externen Mitarbeitern oder Organisationen, sich zu jeder Zeit und von jedem Ort aus über eine öffentliche Netzwerkinfrastruktur in das Firmennetzwerk einzuwählen, wobei dieselbe Sicherheitspolitik wie für das interne Netzwerk angewendet werden kann.

In einer Remote-Access-VPN-Umgebung ist der wichtigste Sicherheitsaspekt die genaue Identifikation eines Benutzers als berechtigtes Mitglied des Netzwerks. Zwecks dieser Identifikation wird ein sogenannter Tunnel-zum-Home-Gateway aufgebaut, über den die Identifikation, die Autorisierung und die Buchführung abgewickelt wird. Diese Funktionalität wird auf der internen Netzwerkseite von einem AAA-Server (Authentication, Authorisation, Accounting) bereitgestellt.

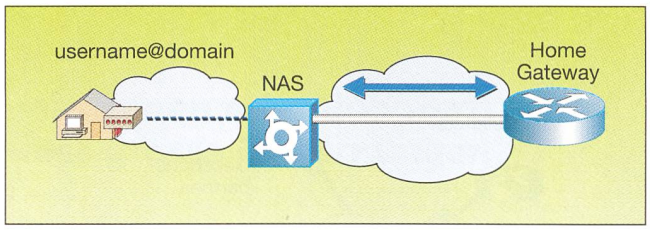

Bild 4 NAS(Network Access Server)-initialisiertes VPN. Quelle: Cisco Systems

Grundsätzlich werden zwei Typen von Remote-Access-VPN unterschieden: das dedizierte oder benutzerinitialisierte VPN (Client initiated VPN) und das NAS-initialisierte VPN (Network Access Server initiated VPN).

Bei einem von einem Benutzer initialisierten VPN befindet sich die entsprechende Software auf dem Personalcomputer des Benutzers. Diese Software baut einen sicheren IP-Tunnel über das Netzwerk eines Internet Service Providers (ISP) zum Host auf (End-to-End Security). Diese Anwendung ist ideal für Homebanking oder andere sensitive Geschäftstransaktionen über das Internet. Der Client hat in diesem Fall eine IPsec-Client-Software (IPsec ist ein standardisierter Sicherheitszusatz zum derzeit gültigen Internet-Protokoll IPv4) auf seinem Personalcomputer installiert, die ihm den sicheren Zugang zum gewünschten Netzwerk gewährleistet. Diese Client-Software baut zusammen mit dem AAA-Server die sichere VPN-Verbindung über das öffentlich zugängliche Netzwerk (Internet) auf. Die Vorteile beim Client initiated VPN liegen darin, dass die sogenannte Last Mile vom Benutzer bis zum PoP (Point of Presence) des Service Providers ebenfalls sicher ist und dass dieses Konzept sehr stabil funktioniert, da die Sicherheitsfunktionalität bereits beim Client implementiert ist. Dadurch ist diese Funktionalität (Tunneling, Encryption) auch einfacher skalierbar. Als Nachteile zu nennen sind der Verwaltungsaufwand für die IPsec-Clients und die Tatsache, dass die Sicherheitsfunktionalität durch den Client aufgebaut werden muss.

Beim NAS-initialisierten VPN entfällt diese IPsec-Client-Software. Ein externer Benutzer wählt sich über ein normales Modem via PPP/SLIP in den PoP seines Service Providers ein. Der PoP übernimmt die Authentifizierung und erstellt bis zum internen Netzwerk eine sichere Verbindung über das öffentlich zugängliche Datennetz. Dabei ist die gesamte Funktionalität des VPN im Netzwerk des Service Providers implementiert. Der Nachteil ist dabei offensichtlich der Mangel an Sicherheit bis zum Einwählpunkt des Service Providers. Dafür entfällt der Verwaltungsaufwand für die IPsec-Client-Software. In einer Remote-VPN-Umgebung muss immer zwischen Verwaltungsaufwand und Sicherheit abgewägt werden. Zu den Vorteilen dieses Konzepts gehört neben dem oben genannten Wegfallen der IPsec-Client-Software der gleichzeitig mögliche, ungeschützte Zugriff auf das Internet. Zudem wird der gesamte, sichere Datenverkehr über einen einzigen Tunnel abgewickelt, welcher in vielen Fällen im Netzwerk des Service Providers prioritär behandelt wird. Den grössten Nachteil bildet heute die Restriktion auf PoP, die diese Funktionalität überhaupt anbieten können.

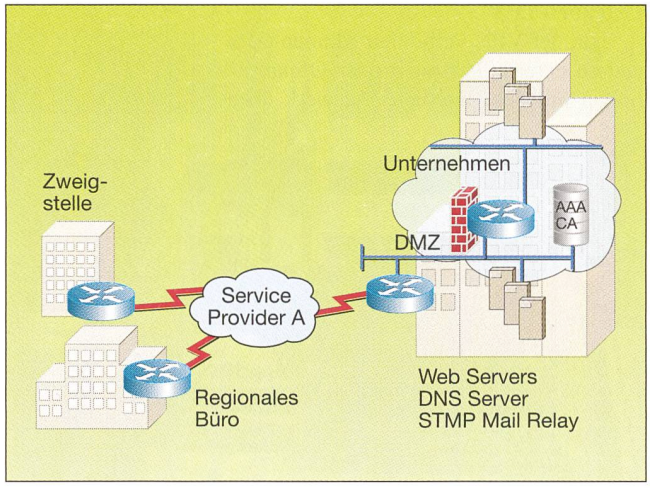

Bild 5 Intranet-VPN verbinden das interne Netzwerk eines Firmenhauptsitzes über ein öffentlich zugängliches Netzwerk.

Die DMZ (demilitarisierte Zone) ist ein autonomes Netzwerk, dessen Sicherheitspolitik den öffentlichen Zugriff auf die darin befindlichen Endgeräte wie Web- oder Mail-Server zulässt. Dieses Netzwerk ist weniger restriktiv geschützt als das betriebsinterne Netzwerk, auf das ausschliesslich Mitarbeiter Zugriffsrechte besitzen. Quelle: Cisco Systems

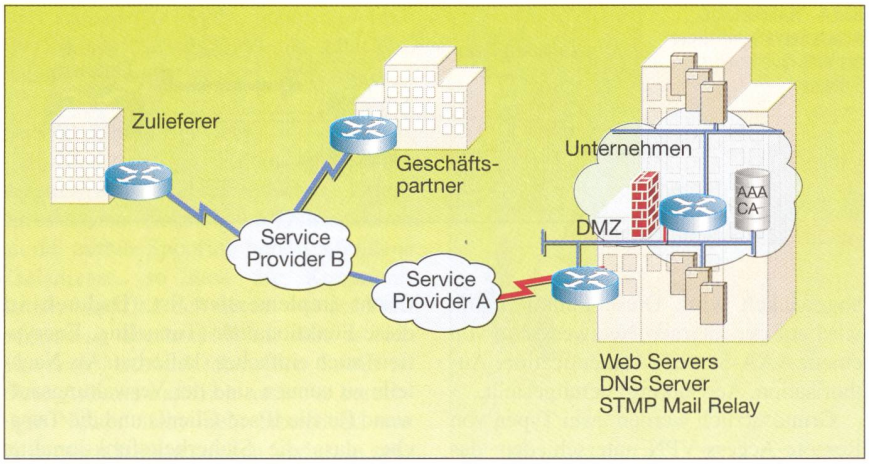

Bild 6 Extranet-VPN verbinden Dritte mit dem internen Netzwerk über ein öffentlich zugängliches Netzwerk.
Quelle: Cisco Systems

Intranet-VPN

Intranet-VPN verbinden das interne Netzwerk eines Firmenhauptsitzes meistens über Standleitung zum nächsten PoP des Internet Service Providers über ein öffentlich zugängliches Netzwerk wie das Internet mit seinen Aussenstellen oder Verkaufsbüros (Bild 5). Dabei gilt dieselbe Sicherheitspolitik, wie wenn sich diese externen Benutzer im internen Netzwerk befinden würden. Zu diesem Netzwerk haben ausschliesslich Firmenmitarbeiter Zugriff. Meist wird ein Intranet-VPN anstelle einer Mietleitung eingesetzt. Diese Verbindungen sind sicher, ermöglichen Quality of Services (QoS), können leicht verwaltet werden und sind äusserst zuverlässig.

Die Vorteile eines Intranet-VPN sind primär die Kostenreduktion für WAN-Verbindungen (keine Kosten für Mietleitungen, Frame-Relay-Services usw.) und das einfache Anbinden von neuen Standorten. Allerdings sollten mit dem entsprechenden Service Provider garantierte Datenraten verhandelt und festgelegt werden.

Extranet-VPN

Extranet-VPN verbinden Kunden oder andere externe Personen oder Organisationen mit dem internen Netzwerk über ein öffentlich zugängliches Netzwerk wie beispielsweise das Internet (Bild 6). Sie unterscheiden sich von Intranet-VPN dadurch, dass sie den Zugriff von Personen oder Organisationen steuern, die sich organisatorisch ausserhalb der eigenen Firma befinden. Typischerweise ersetzt ein Extranet-VPN den Datenaustausch durch E-Mail und/oder Fax und erleichtert somit das E-Business.

Externen Partnern die Anbindung an das eigene Netzwerk zu ermöglichen, war früher teuer und schwierig. Teure Mietleitungen zum Geschäftspartner mussten beschafft, Netzwerkmanagement und Sicherheit abgestimmt und unterhalten werden. In vielen Fällen mussten beide Partner über die gleiche Hardware verfügen. Wollten sich dazu noch einige mobile Benutzer einwählen, mussten zusätzlich komplizierte separate «Dial Domains» eingerichtet und unterhalten werden. Auf Grund dieser Komplexität verzichteten viele Firmen darauf, ihre Partner direkt in das firmeneigene Netzwerk einzubinden. Daraus entstanden komplizierte Abläufe und somit eine reduzierte Effektivität der Geschäftsbeziehungen.

Grosse Vorteile des Extranet-VPN sind seine einfache Implementation und das einfache Verwalten. In einem Extranet-VPN werden dieselben Protokolle wie in den beiden anderen VPN-Konzepten verwendet. Der einzige Unterschied ist, dass firmenexternen Benutzern der geschützte, kontrollierte Zugriff auf das firmeninterne Netzwerk erlaubt wird.

Schlussfolgerung

Zusammenfassend lässt sich sagen, dass Virtual Private Networks die Vernetzbarkeit verbessern, die Datensicherheit und die Flexibilität bezüglich des externen Zugriffs erhöhen, zuverlässig arbeiten und vor allem die Kosten für den Datenaustausch reduzieren.

Des infrastructures sûres en environnement Internet

Introduction et concept pour Virtual Private Network (VPN)

A l'origine, les ordinateurs étaient conçus comme appareils autonomes, ce qui limitait l'échange de données entre eux. Mais les grandes entreprises surtout ont commencé très tôt à interconnecter leurs ordinateurs. Ce faisant, elles courent cependant le risque que des tiers puissent voir les données transférées ou les manipuler. Diverses technologies permettent d'accroître considérablement la sécurité des données.