Kapitel 2

Notwendigkeiten, Ziele und Anwendungsformen von VPN-Systemen

In diesem Kapitel werden die Notwendigkeiten und allgemeinen Ziele von Virtual Private Networks (VPNs) dargestellt. Die grundsätzliche Idee, die hinter dem Betrieb solcher Systeme steht, wird erläutert und grundlegende Anwendungsformen werden beschrieben.

2.1 Idee und Definition von VPNs

Das Thema VPN hat einen bemerkenswerten Aufschwung erhalten. Leider besteht eine Unschärfe in der Bedeutung des Begriffs.

In der Fachliteratur wird der Begriff VPN in zwei verschiedenen Bedeutungen verwendet:

1. als eine Methode von Bandbreiten-Management und Quality of Service (QoS) oder
2. als Möglichkeit zur Realisierung einer vertrauenswürdigen Kommunikation mit Hilfe von kryptographischen und anderen Sicherheitsfunktionen

In diesem Buch wird der Begriff VPN nur im Sinne der vertrauenswürdigen Kommunikation verstanden und verwendet.

Die grundsätzliche Idee von Virtual Private Networks (VPNs) ist, die Vorteile einer offenen Kommunikationsinfrastruktur zu nutzen – zum Beispiel der kostengünstigen, weltweit verfügbaren »shared infrastructure« des Internet – aber dabei allen Gefährdungen der Informationssicherheit sinnvoll und angemessen entgegenzuwirken.

Ein VPN soll gewährleisten, dass sensible Daten während der Übertragung über verschiedene, sicherheitstechnisch nicht einschätzbare Netzwerke (LANs und WANs, private und/oder öffentliche Netze) vertrauenswürdig übertragen werden, so dass nur die dazu berechtigten Organisationen oder Personen auf die zu schützenden Daten zugreifen können und ihren Informationsgehalt veränder kann.

Definition »V... P... N...«

- »Virtual« bedeutet, dass es sich – aus Anwendersicht – scheinbar um nur »ein« Netzwerk handelt, auch wenn sich viele reale Teilnetzwerke hinter »einem« VPN verbergen.
- »Private« bedeutet, dass die Kommunikation vertrauenswürdig – also nicht öffentlich – durchgeführt und das Risiko eines Schadens bei der Übertragung minimiert wird.
- »Network« bedeutet, dass eine definierte Gruppe von Rechnersystemen miteinander verbunden wird und mit Hilfe eines Protokolls (typischerweise ist das die TCP/IP-Protokollfamilie) kommuniziert.

2.2 Analogien

Um die grundsätzliche Idee eines VPN zu verdeutlichen und so das Verständnis zu erleichtern, werden im Folgenden zwei Analogien erläutert: zum einen ein Sicherheitstransporter und zum anderen eine Pipeline. Beides schützt die zu übertragenden Werte elektronisch vor Diebstahl, Einsichtnahme und Veränderung.

Sicherheitstransporter

Anders als normale LKWs, bei denen die zu transportierenden Werte nicht explizit geschützt sind, dient ein Sicherheitstransporter dazu, die auszutauschenden Werte während des Transports wirkungsvoll gegen Angriffe zu schützen. Dabei nutzen die Organisationen die gemeinsame öffentliche Infrastruktur der Straßen (Landstraßen, Autobahnen etc.), ohne eine eigene Infrastruktur (Privatstraßen) aufbauen zu müssen.

Entsprechend dient ein VPN dazu, Daten (elektronische Werte, so genannte E-Assets) sicher über die öffentliche Infrastruktur von Netzwerken (LANs und WANs) zu transportieren, ohne dass Unbefugte die Daten einsehen oder manipulieren können.

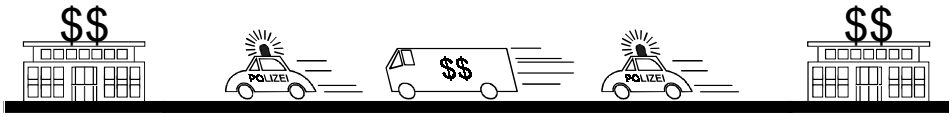

Abb. 2.1: Sicherheitstransporter

Pipeline und Rohrpost

Durch eine Pipeline werden Güter, zum Beispiel Öl, sicher von einem festgelegten Ort zu einem anderen transportiert. Zum Beispiel unterhält die NATO das – in der Öffentlichkeit weitgehend unbekannte – Central European Pipeline System (CEPS); es ist das weltweit umfangreichste und komplizierteste militärische Kraftstoffversorgungssystem.

Durch Beobachtung einer Pipeline kann man allenfalls erkennen, wie hoch der absolute Durchfluß ist, nicht aber, woher der Inhalt stammt und wohin er gelangt. Das Transportgut Öl hat keinen Informationsgehalt, sondern lediglich einen materiellen Wert (»Brennwert«).

Bei einem VPN muss zwischen allen Endpunkten sichergestellt sein, dass tatsächlich alle Daten durch die »VPN-Pipeline« laufen, das heißt, dass sie nicht abgezweigt werden können, und dass kein Unbefugter in die »VPN-Pipeline« eindringen kann.

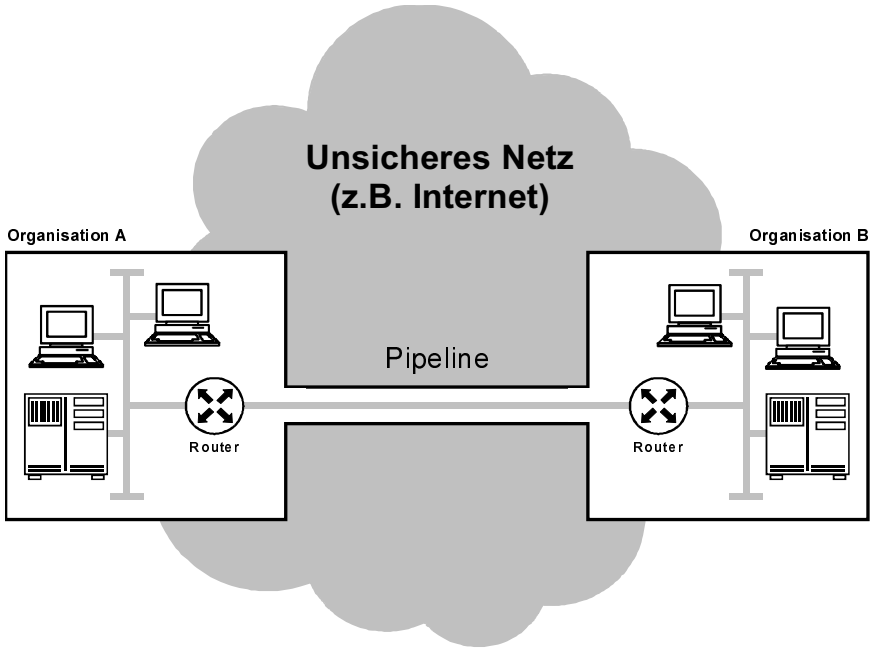

Abb. 2.2: Pipeline

Schon vor mehr als 100 Jahren wurde das Konzept der Pipeline für die gesicherte Übertragung von Schriftgut – also von Information – verwendet: Die Rohrpost in Berlin und anderen Großstädten hatte ihre Blütezeit zwischen 1875 und 1945. Seine größte Ausdehnung hatte das Berliner Netz 1944 mit mehr als 300 offiziellen und rund 100 streng geheimen Kilometern /Arno2000/.

Auch heutzutage befördern Rohrpostanlagen – meist aber nur innerhalb von Unternehmen – Bargeld, Schecks, Dokumente, gefährliche Güter oder auch »nur« Produktionsmittel (übrigens bis 15 kg Gewicht, 30 cm Durchmesser, kilometerweit und bis zu 90 km/h schnell).

Es ist dabei nicht möglich, durch die Beobachtung einer Rohrpost-Hauptleitung zu erkennen, wie sich die Werte bei den Absendern zusammenstellen und bei den Empfängern wieder aufteilen. Außerdem können die Sendungen mit einer Versiegelung der Box zusätzlich geschützt werden.

Tunnel

Der Vollständigkeit wegen sei hier auch der Begriff »Tunnel« erwähnt, der insbesondere in der amerikanischen Fachliteratur verwendet wird (»tunneling«). Diese Analogie bedeutet »Zugriffsschutz« – wie bei der virtuellen Pipeline durch das Internet.

2.3 Moderne IT-Konzepte und IT-Sicherheit

Wie schon in Kapitel 1 ausgeführt, werden heute die meisten Geschäftsprozesse – Angebotserstellung, Auftragsannahme, Bestellung usw. – mit Hilfe moderner IT-Konzepte abgewickelt. Der Trend zur Globalisierung macht es für fast alle Unternehmen und Organisationen unverzichtbar, immer mehr Arbeitsprozesse über sichere Netzwerke zu realisieren, wenn sie im Wettbewerb bestehen wollen.

Der personelle und materielle Aufwand, der in der Vergangenheit schriftlich auf Papier, mit Hilfe der Post oder durch persönlichen Kontakt abgewickelt wurde, wird also größtenteils durch elektronische Verfahren ersetzt, was weitaus rationeller ist.

Diese Informationsverarbeitungs- und Telekommunikationsprozesse sind zum Beispiel Client-Server-Verbindungen, Web-Systeme und E-Mail-Austausch. Dabei werden in der Regel preiswerte, verfügbare und allgemein zugängliche Kommunikationsinfrastrukturen wie das Internet oder andere öffentlich angebotene Backbones genutzt.

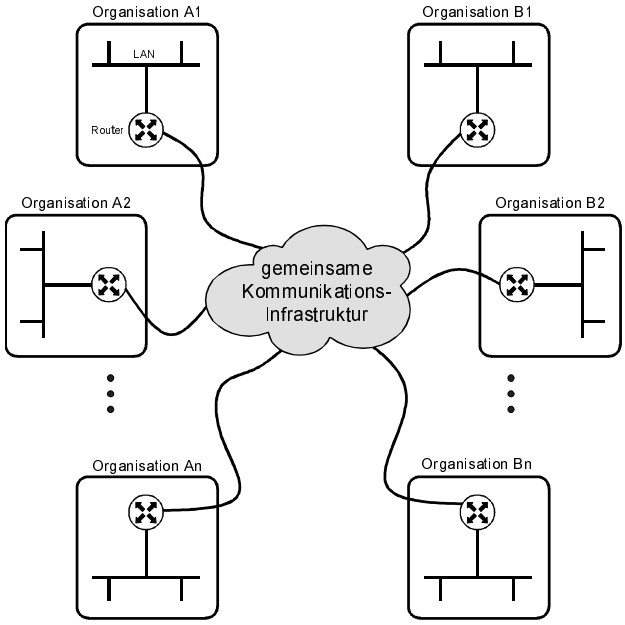

Abb. 2.3: Kopplung von Organisationseinheiten über öffentliche Kommunikationsinfrastrukturen

Technologische Weiterentwicklungen schaffen drastisch höhere Zugangsgeschwindigkeiten zu den öffentlichen Kommunikationsinfrastrukturen.

Während ISDN im Duplex-Betrieb schon bis zu 128 KB pro Sekunde ermöglicht, erreicht die neue ADSL-Technik (Asymmetric Digital Subscriber Line) bis zu 8 MB pro Sekunde – und das mit dem konventionellen Telefonkabel, wie es auf der »letzten Meile« zwischen der Vermittlungsstelle des Telekommunikations-Anbieters und dem Teilnehmeranschluss verlegt ist.

Weitere Entwicklungen stehen bevor, insbesondere Verfahren zur drahtlosen Anbindung.

2.4 Corporate Network versus öffentliche Kommunikationsinfrastruktur

Es gibt zwei unterschiedliche Wege, um die notwendige sichere Kommunikation einer Organisation zur realisieren /Pohl 99b/:

1. Eine Organisation kann für die interne Kommunikation zwischen den einzelnen Organisationseinheiten ein Corporate Network mit eigener Kommunikationsinfrastruktur aufbauen (beispielsweise mit Hilfe von Standleitungen,

ATM-, Frame-Relay- oder X.25-Netzen) und die Kommunikation nach außen – zu Kunden, Lieferanten und Geschäftspartnern – über eine zentrale Stelle realisieren, die an eine öffentliche Kommunikationsinfrastruktur angebunden ist.

2. Die gesamte Kommunikation – nach innen wie nach außen – wird über eine öffentliche Kommunikationsinfrastruktur realisiert. Dabei müssen jedoch geeignete IT-Sicherheitsmechanismen eingebunden werden, die den zusätzlich entstehenden Gefahren entgegen wirken.

Im Folgenden werden die Vor- und Nachteile der beiden Möglichkeiten diskutiert.

Corporate Network

Vorteile:

- Die Organisation hat völlige Freiheit bei der Gestaltung der eigenen Kommunikationsinfrastruktur mit allen gewünschten (technisch realisierbaren) Features.
- Da die Kommunikationsinfrastruktur nur von der eigenen Organisation genutzt wird, ist die Sicherheit und zugleich die Verfügbarkeit höher.
- Die eigene Sicherheitspolitik kann auf allen Ebenen eigenverantwortlich umgesetzt werden.

Nachteile:

- Hohe Investitionen, Betriebs- und Wartungskosten müssen selbst getragen werden.
- Innovationen im IT-Bereich zwingen jeweils zu neuen Investitionen.
- Der maximale Durchsatz bestimmt die maximale Bandbreite und damit auch die Kosten.

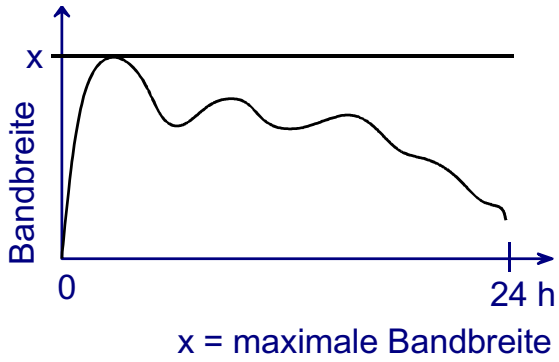

Abb. 2.4: Dimensionierung nach maximaler Bandbreite

Öffentliche Kommunikationsinfrastruktur

Vorteile:

- Innovationen durch die Anbieter stehen den Anwendern unmittelbar zur Verfügung, ohne dass eigene Investitionen notwendig werden.
- Die Kosten für die öffentliche Kommunikationsinfrastruktur sind in der Regel niedriger.
- Die Infrastruktur kann flexibel für die Kommunikation mit Kunden, Lieferanten und Geschäftspartnern benutzt werden.
- Der Anbieter ist verantwortlich für die gleichbleibende Qualität der Dienste in punkto Verfügbarkeit, Geschwindigkeit und Management (Accounting / Billing).
- Die durchschnittliche Bandbreite bestimmt die Kosten, die maximale Bandbreite kann in definierten Bereichen größer sein.

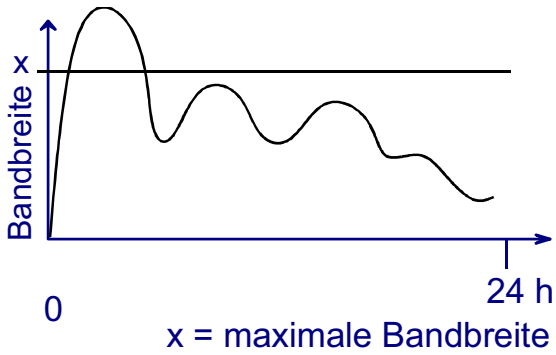

Abb. 2.5: Dimensionierung nach durchschnittlicher Bandbreite

Nachteile:

- Der Anwender ist abhängig vom Anbieter und dessen Sicherheitsstrategie.
- An die öffentliche Kommunikationsinfrastruktur sind auch andere Benutzer angeschlossen, die einen anderen Schutzbedarf haben (Extrembeispiel: Hacker neben professionellen Business-Anwendern).
- Die Security Policy des Anbieters ist nicht immer klar nachvollziehbar und überprüfbar.

2.5 Zielsetzung eines VPN

Die moderne Informationstechnik arbeitet zunehmend mit verteilten Anwendungen. Das bedeutet, dass Daten an verschiedenen Orten erstellt oder bearbeitet und dann über Kommunikationsnetze ausgetauscht werden.

Diese Kommunikationstechniken bieten unübersehbare Vorteile im Hinblick auf die Schnelligkeit und Flexibilität der Informationsübermittlung. Zugleich aber entstehen nicht zu unterschätzende Sicherheitsrisiken, die unter Umständen allen Nutzen zunichte machen können:

- Die Daten können durch Dritte gelesen und verändert werden, während sie über öffentliche Netze (Kommunikationsinfrastrukturen) übertragen werden.
- Durch die Ankopplung an ein offenes Netzwerk können Unbefugte auf die Rechnersysteme des eigenen Netzes zugreifen und Schaden anrichten.

Moderne IT-Sicherheitstechniken können die Daten auf ihrem Weg über öffentliche Netze so schützen, dass ihre Vertraulichkeit (Privatheit) gewährleistet bleibt und niemand in der Lage ist, unbefugt auf die eigenen Rechnersysteme zuzugreifen.

Diese Sicherheitsmaßnahmen ermöglichen es, die Vorteile öffentlicher Kommunikationsinfrastrukturen zu nutzen und zugleich die Vertraulichkeit und Informationssicherheit eines privaten Netzwerks zu bewahren.

Damit dieses Ziel erreicht werden kann, müssen kryptographische Verfahren und andere Sicherheitsmechanismen eingesetzt werden.

Dazu zählen zum Beispiel:

- Verschlüsselung
- Authentikation
- Digitale Signaturen für die Unversehrtheit der Daten
- Tunneling
- Firewalling

2.6 Anwendungsformen von VPNs

Verschiedene Anwendungsformen von VPNs stellen spezifische Anforderungen hinsichtlich Connectivity (Verbindlichkeit), Verfügbarkeit, Datendurchsatz, Einsatz von Standards und Schlüsselmangement. Optimal wäre ein VPN, das alle Anforderungen abdeckt und auch den unterschiedlichen Ansprüchen an die Kosten gerecht wird.

Unternehmensweites VPN

Darunter versteht man »private« Netzwerkverbindungen zwischen verschiedenen LAN-Standorten eines Unternehmens (Zentrale und Niederlassungen), die dazu dienen, Unternehmensdaten vertrauenswürdig über ein unsicheres Netz wie das Internet austauschen zu können. Hier spielt die Transparenz der Lösung eine wichtige Rolle.

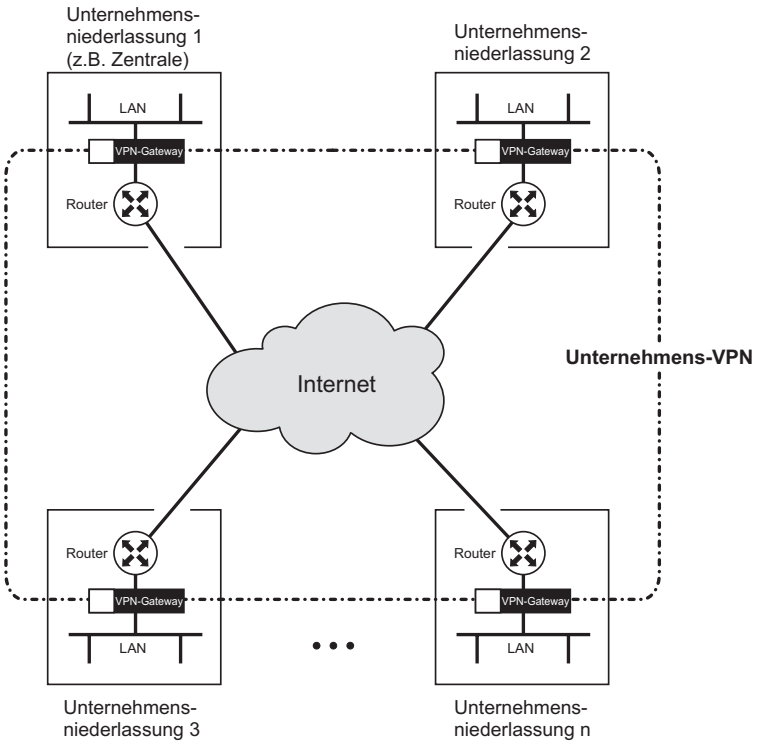

Abb. 2.6: Unternehmensweites VPN

Sichere Remote-Ankopplung

Heim- und/oder Mobil-Arbeitsplätze greifen innerhalb eines VPN über ein öffentliches Netzwerk (zum Beispiel das Internet) geschützt auf die zentral gespeicherten Unternehmensdaten zu. Hier spielt die Identifikation und Authentikation des Nutzers, der auf die Daten zugreifen möchte, eine besondere Rolle.

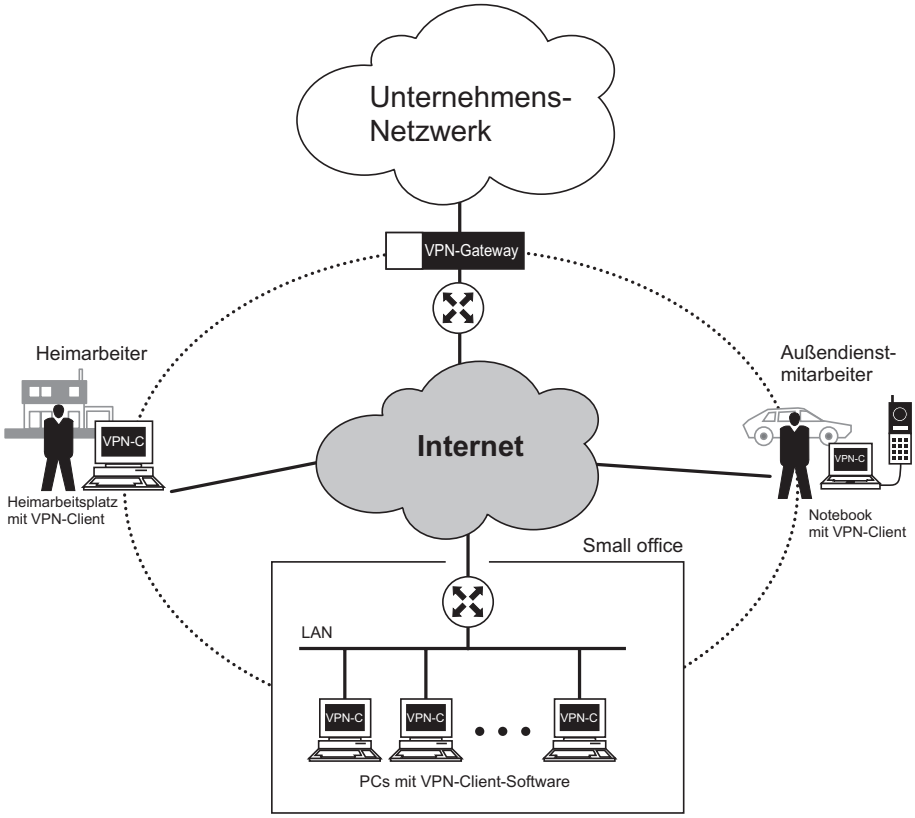

Abb. 2.7: Remote-Ankoppelung mit Hilfe eines VPN

VPN zwischen verschiedenen Unternehmen

In einer definierten Gruppe von Unternehmen – beispielsweise von Automobilherstellern und -zulieferern – können alle Partner miteinander mit Hilfe von VPNs eine vertrauenswürdige, untereinander und nach außen hin geschützte Kommunikation realisieren. Hier spielt das unternehmensübergreifende Sicherheitsmanagement eine besondere Rolle.

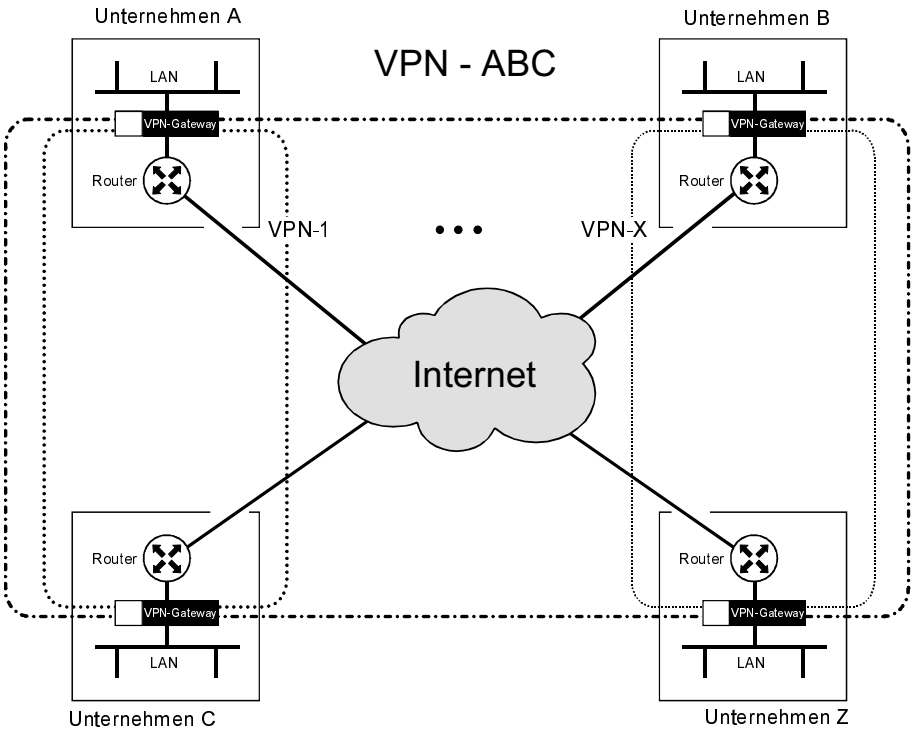

Abb. 2.8: Kooperatives VPN verschiedener Unternehmen

Kombinationen der Anwendungsformen

Natürlich gibt es auch Kombinationen der oben beschriebenen Anwendungsformen. Hier spielt die Verwendung eines einheitlichen Standards und die Möglichkeit eines flexiblen und unternehmensübergreifenden Sicherheitsmanagements eine besondere Rolle.

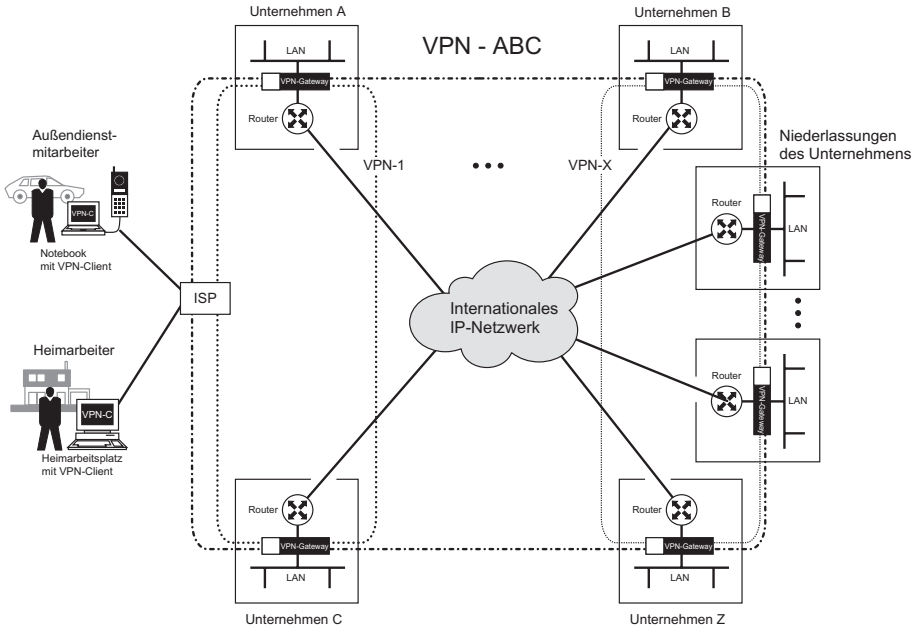

Abb. 2.9: VPN-Kombinationen