VPN: Der sichere Transport durchs Netz

VPNs helfen elektronische Werte zu sichern

Autor:	**Dipl.-Ing. Norbert Pohlmann**
	Vorstand Utimaco Safeware AG
☎	0241-963-1426
🖷	0241-963-1390
E-Mail:	norbert.pohlmann@utimaco.de
Internet:	www.utimaco.de

1 Einleitung

Die moderne Informationstechnik arbeitet zunehmend mit verteilten Anwendungen. Das bedeutet, daß Daten an verschiedenen Orten erstellt oder bearbeitet werden, die man dann über Kommunikationsnetze austauscht. Diese Kommunikationstechniken bieten unübersehbare Vorteile in puncto Schnelligkeit, Performance und Flexibilität der Informationsübermittlung. Zugleich aber entstehen nicht zu unterschätzende Sicherheitsrisiken: Die Daten können bei der Übertragung durch Dritte gelesen werden. Zusätzlich können Unbefugte durch die Ankopplung an ein offenes Netz auf die Rechnersysteme des eigenen Netzes zugreifen und Schaden anrichten.

Moderne IT-Sicherheitstechniken ermöglichen es, die Vorteile öffentlicher Kommunikationsinfrastrukturen zu nutzen und bieten zugleich die Vertraulichkeit und Infomationssicherheit eines Privaten Netzwerkes. Man spricht daher von einem sogenannten **Virtual Private Network (VPN)**.

2 Aufbau von Virtual Private Networks

Die grundsätzliche Idee bei Virtual Private Networks (VPNs) ist, die Vorteile einer offenen Kommunikationsinfrastruktur zu nutzen – z.B. die kostengünstige, weltweit verfügbare „shared infrastructure“ des Internet – aber dabei allen Gefährdungen der Informationssicherheit sinnvoll entgegenzuwirken.

Ein VPN soll gewährleisten, daß sensible Daten während der Übertragung über Netzwerke (LANs und WANs) vertraulich übertragen werden, so daß nur die dazu berechtigten Personen auf die sensiblen Daten zugreifen können und keine Fremden in der Lage sind, auf die Rechnersysteme des eigenen Netzes unerlaubt zuzugreifen.

Damit diese Ziele erreicht werden, setzt man kryptographische Verfahren und andere Sicherheitskomponenten ein. Die wesentlichen Sicherheits-mechanismen von VPNs sind:

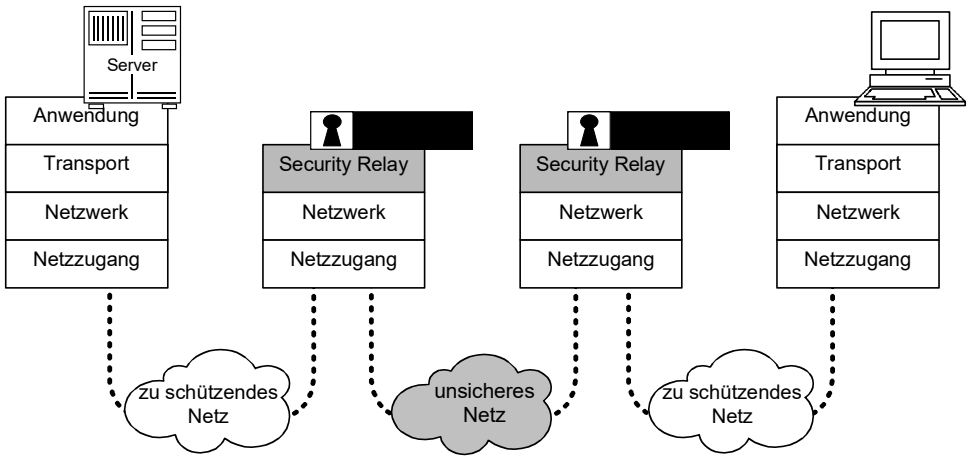
- Verschlüsselung
- Firewalling

2.1 Vertraulichkeit durch Verschlüsselung

Mit der Verschlüsselung der Kommunikationsdaten wird ein besonders wichtiger Teil der Sicherheitsanforderungen an ein VPN erbracht. Ohne Kenntnis des Schlüssels ist es Dritten nicht möglich, abgefangene Daten zu lesen oder unbemerkt zu manipulieren.

Die Verschlüsselung kann insbesondere im heterogenen Rechnerumfeld mit Hilfe von Black-Boxen einfach und transparent verwirklicht werden.

Als **Black-Box-Lösungen** bezeichnet man Hardware-Geräte, die auf einfache Weise zwischen Rechnersysteme und Netzanschluß (LAN-Anschluß) geschaltet werden. Das macht sie unabhängig von den jeweiligen Endgeräten und Betriebssystemen und wegen ihrer einfachen Handhabung benutzerfreundlich. In der High-Tech Black-Box geschehen alle sicherheits-relevanten Operationen – unsichtbar für den Benutzer und ohne daß er sie eigens veranlassen muß.



Vor jede Organisationseinheit, die über öffentliche Kommunikations-infrastrukturen gesichert kommunizieren möchte, wird dafür eine Black-Box geschaltet. In Zusammenarbeit mit einer entsprechenden Sicherheitseinrichtung auf der Gegenseite sorgt sie für die kryptographische Sicherung der Kommunikation über die öffentliche Kommunikationsinfrastruktur hinweg.

Die folgende Abbildung zeigt, daß mit mehreren Black-Boxes gleichzeitig und unabhängig voneinander beliebig viele VPNs über eine öffentliche Kommunikationsinfrastruktur realisiert werden können.

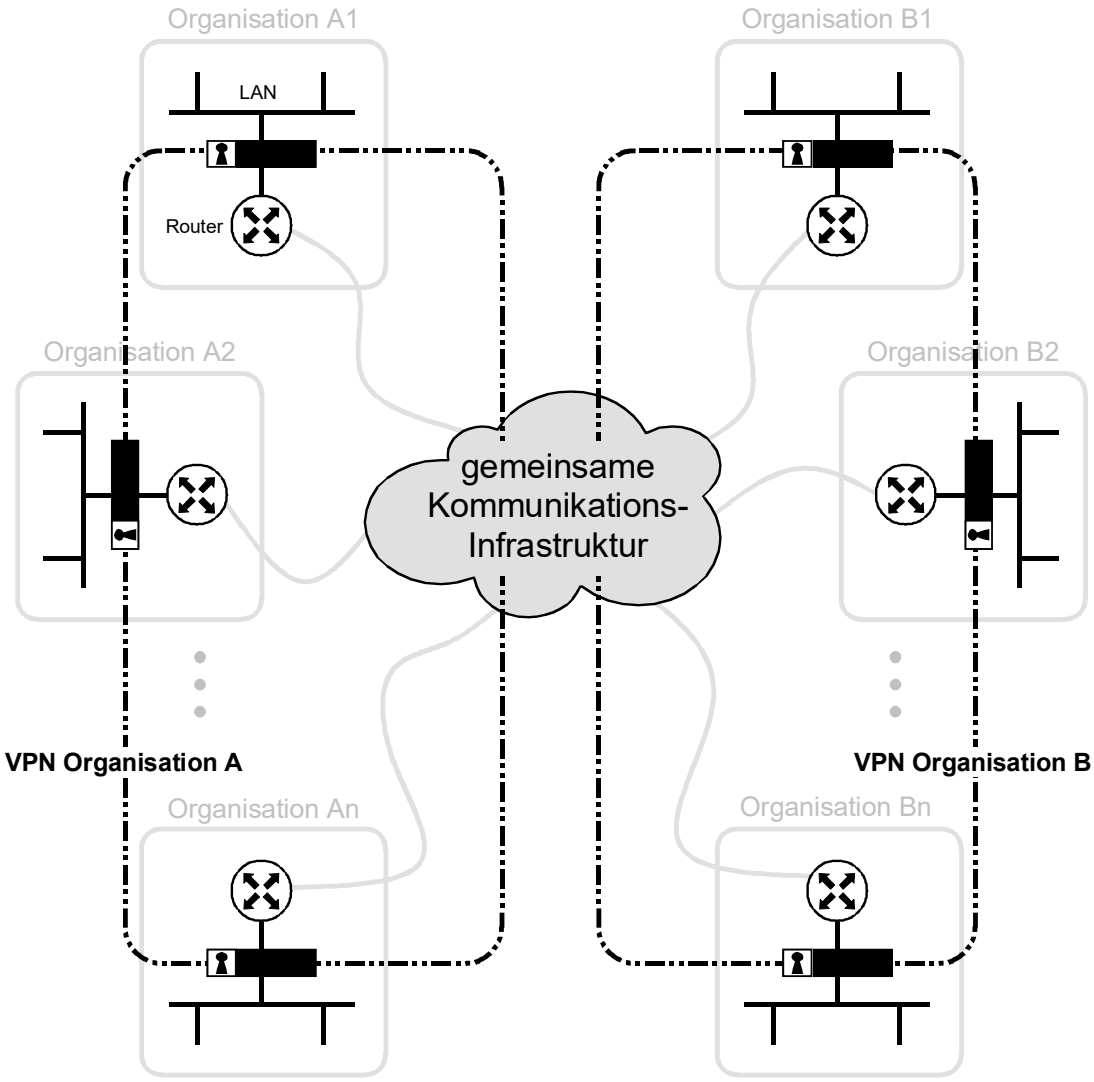


Abbildung 2.1 mehrere VPNs

In der Abbildung 2.1 ist dargestellt, wie zwei VPNs unabhängig voneinander über eine gemeinsame Kommunikationsinfrastruktur (z.B. Internet) realisiert werden können. Die VPN Boxen werden zur Netzwerksicherung vor den Routern positioniert. Es ist auch möglich, daß die unterschiedlichen VPN Realisierungen miteinander eine gesicherte Kommunikationsbeziehung aufbauen. Ein besonderer Vorteil dieser Lösung ist, daß sie auch die Sicherheitsanforderungen für Backup und flexible Bandbreiten erfüllen. Weil die Sicherheit unabhängig vom Übertragungsmedium (ISDN, X25, etc) ist, kann immer ein gleiches Maß an Sicherheit garantiert werden.

2.1.1 VPN-Realisierungen

Hinsichtlich der Realisierung von VPNs existieren unterschiedliche Lösungsansätze. Einige Hersteller haben spezielle Security-Protokolle verwirklicht, die mit einem geschwindigkeitsoptimierten Ansatz arbeiten. Vorteile eines solchen Ansatzes sind absolute Transparenz, sehr geringe Verzögerungszeiten in allen Phasen der Kommunikation, kein Overhead während der Kommunikation und keine Notwendigkeit irgendwelcher Reaktionen seitens der Komponenten, die in den einzelnen Netzen integriert sind. Dieser Ansatz ist besonders bei echtzeitorientierten und Terminal-Anwendungen von besonderer Bedeutung.

IPSec

Im Bereich der Standardisierung hat die Internet Engineering Task Force (IETF) einen Internet-Sicherheitsstandard definiert, der IPSec heißt.
IPSec definiert Mechanismen, um sichere VPNs aufzubauen. IPSec bietet im wesentlichen zwei Mechanismen:

1. den sogenannten Authentication Header und
2. den Encapsulated Security Payload.

Beide Mechanismen können im VPN-typischen Tunnellingmodus betrieben werden. Diese Kombinationen sind die grundsätzlichen Mechanismen, um VPNs aufzubauen.

Tunnelling

Beim Tunneling wird jedes zu sendende Paket in ein neues Paket verpackt (Black Boxes). Dazu wird ein zusätzlicher neuer Header vorgeschaltet. So wird z.B. für IP-basierende Netze ein IP-Header vorangestellt. Weiter kommen zusätzliche Informationen oder Kennzeichen im Body-Teil des Pakets dazu.

Die vorgeschalteten Header charakterisieren die Endpunkte des Tunnels und die eingepackten Header beschreiben die eigentlichen IP-Adressen (Rechnersysteme), zwischen denen die Kommunikation stattfinden soll. Die Adreßbereiche können auch unterschiedlich sein. Mit Tunneling kann aber auch ein beliebiges Paket (z.B. IP oder IPX) verpackt übertragen und am Ziel wieder entpackt werden. Die dazwischenliegenden Router „wissen“ nichts von diesen Mechanismen.

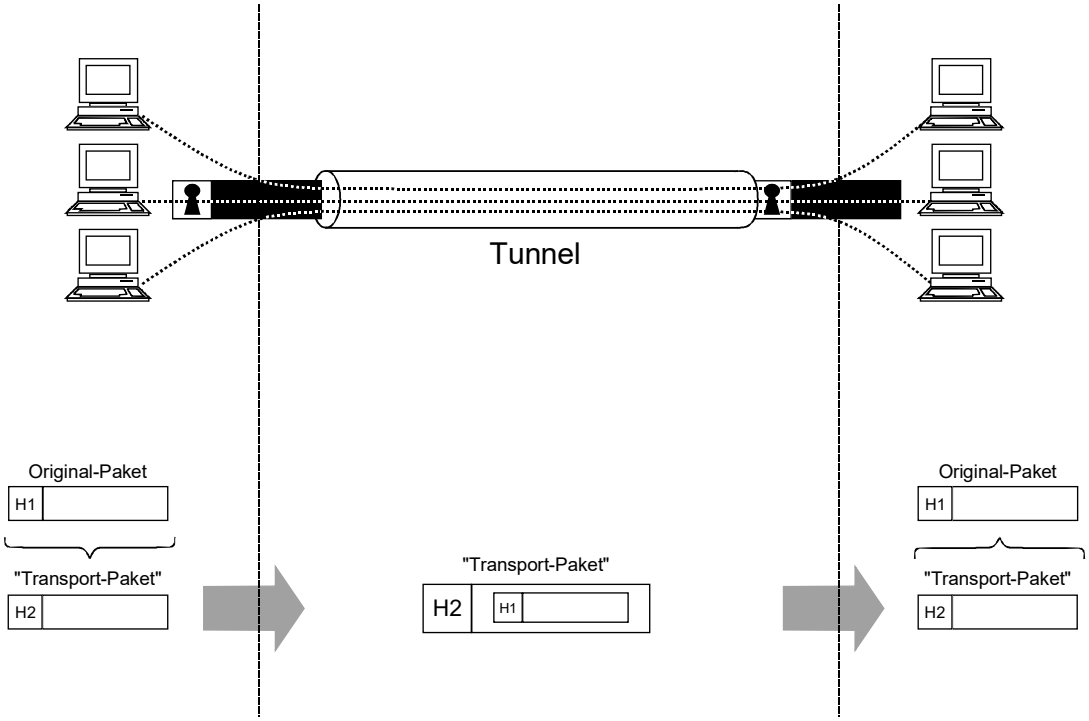


Abbildung 5.4 Tunneling

Vorteil von Tunneling ist, daß, wenn z.B. zwei Organisationen über eine öffentliche Kommunikationsinfrastruktur eine Kommunikation durchführen, immer nur zwei IP-Adressen verwendet werden, unabhängig davon, wie die Kommunikation tatsächlich stattfindet.

Falls die getunnelte Verbindung verschlüsselt wird, kann auch ein gewisser Schutz vor einer Verkehrsflußanalyse gewährleistet werden, da die Quell- und Ziel-Adressen im getunnelten Header verschlüsselt sind und nur die Quell- und Ziel-Adressen der Komponenten, die das Tunneling realisieren, sichtbar werden. Auf der anderen Seite können dann Features wie Prioritätensteuerung nicht mehr verwendet werden.

Key-Management

Als das notwendige Key Management ist bei IPsec das sogenannte ISAKMP-Oakley definiert. Bei dieser Standardisierung sind jedoch noch viele Fragen der Implementierung nicht beantwortet. Auch sind bisher erst wenige Algorithmen zur Authentisierung und Verschlüsselung integriert. Deshalb ist bei vielen heutigen IPSec-Produkten fraglich, ob sie wirklich auf einer gemeinsamen Basis arbeiten und mit Produkten anderer Hersteller zusammenarbeiten können. Dafür ist nicht IPSec verantwortlich, sondern die noch nicht vollständige Umsetzung des Standards.

Auch die bei jeder Verschlüsselung oder Authentikations-Phase entscheidende Frage des Key Management ist noch nicht ausreichend diskutiert. Besonders wichtig beim Key Management ist die Frage einer gemeinsamen Public-Key-Infrastruktur, d.h. einer gemeinsamen Security-Infrastruktur, der die Anwender, die über eine öffentliche Kommunikations-Infrastruktur kommunizieren möchten, wirklich vertrauen können.

Es wird also eine Sicherheitsinfrastruktur benötigt, wo die Generierung eindeutiger Identifikationen, Hinterlegung von Schlüsseln etc. so realisiert ist, daß sich alle Beteiligten auf die Sicherheitsmechanismen absolut verlassen können.

Im Rahmen des Signaturgesetzes wird in Deutschland eine solche kontrollierte Sicherheitsinfrastruktur aufgebaut und eine gemeinsame Security Policy definiert; das ist ein vielversprechender Ansatz.

Im Rahmen des Sicherheitsmanagement wird immer wieder die Aushandlung von Verfahrensweisen, Algorithmen, Parametern und Schlüssellängen usw. diskutiert. In der Praxis wird es sich als Sicherheitsrisiko erweisen, daß die Komponenten, in die IPSec integriert werden soll, nicht sinnvoll entscheiden können, ob eine Kommunikation nun verschlüsselt werden soll oder nicht.

Außerdem gibt es bei IPSec noch weitere Aspekte, die noch einer eingehenderen Untersuchung bedürfen. Dazu gehören z.B. Flow-Control-Funktionen, die bezogen auf Ports bestimmte Prioritäten gewährleisten können. Diese würden bei einer IPSec-Relisierung nicht mehr zur Verfügung gestellt werden können.
Auch wirkt sich die Realisierung von IPSec negativ auf die Routing Performance aus. Die zusätzlichen Bytes belasten die Kommunikation, was zur Folge hat, daß die Nettodatenrate in einem IP-Paket sinkt, so daß die IP-Pakete weniger Nutzdaten transportieren. Im schlimmsten Fall bedeutet das, daß die Router gezwungen sind zu fragmentieren. Das ist ein zusätzlicher Aufwand, der den Datendurchsatz deutlich schrumpfen läßt.

Anderseits bietet IPSec in Zukunft die Chance für einen allgemeinen Sicherheitsstandard, sofern die entsprechenden vertrauenswürdigen Sicherheitsinfrastrukturen geschaffen werden.
Zwei wichtige Aufgaben, die eine gemeinsame sichere Infrastruktur dabei realisieren müßte, sind Identifikationsfestlegung und Generierung von verbindlichen Zertifikaten.

2.2 Firewall-Systeme

Der Sicherheitsmechanismus Verschlüsselung wirkt nur gegen die unerlaubte Einsicht der Informationen während der Kommunikation. Zusätzlich muß noch mit Hilfe von Firewall-Systemen das zweite Hauptrisiko: der unerlaubte Zugriff auf die eigenen Rechnersysteme verhindert werden

Firewall-Systeme werden als Schranke zwischen ein zu schützendes Netz und ein unsicheres Netz geschaltet, so daß der gesamte Datenverkehr zwischen den beiden Netzen nur über das Firewall-System möglich ist.

Ein Firewall-System ist somit das elektronische Äquivalent zu einem Pförtner. Es überprüft, wer aus dem unsicheren Netz auf das zu schützende Netz der Organisation zugreifen darf, und kontrolliert, über welche Protokolle und Dienste zugegriffen wird und mit welchen Rechnersystemen kommuniziert werden darf.

Auf dem Firewall-System werden Sicherheitsmechanismen implementiert, die diesen Übergang sicher und beherrschbar machen. Dazu analysiert das Firewall-System die Kommunikationsdaten, kontrolliert die Kommunikationsbeziehungen und Kommunikationspartner, reglementiert die Kommunikation gemäß der Sicherheitspolitik des Unternehmens, protokolliert sicherheitsrelevante Ereignisse und alarmiert bei starken Verstößen den Security-Administrator.

Ein Angreifer darf nicht in der Lage sein, die Firewall zu überwinden.

Allgemeine Ziele eines Firewall-Systems sind:

- Zugangskontrolle auf der Netzwerkebene

  Es wird überprüft, welche Rechnersysteme (IP-Adressen) über das Firewall-System miteinander kommunizieren dürfen.

- Zugangskontrolle auf Benutzerebene

  Das Firewall-System überprüft, welche Benutzer über das Firewall-System eine Kommunikationsverbindung aufbauen dürfen. Dazu wird die Echtheit (Authentizität) des Benutzers verifiziert.

- Rechteverwaltung

  Im Rahmen der Rechteverwaltung wird festgelegt, mit welchen Protokollen und Diensten und zu welchen Zeiten über das Firewall-System eine Kommunikation stattfinden darf.

- Kontrolle auf der Anwendungsebene

  Es wird überprüft, ob Kommandos genutzt oder Dateiinhalte übertragen werden, die nicht zu der durch die Anwendung definierten Aufgabenstellung gehören.

- Entkopplung von Diensten

  Dienste werden entkoppelt, damit Implementierungsfehler, Schwachstellen und Konzeptionsfehler der Dienste keine Möglichkeit für Angriffe bieten.

- Beweissicherung und Protokollauswertung

  Verbindungsdaten und sicherheitsrelevante Ereignisse werden protokolliert und können für die Beweissicherung von Handlungen der Benutzer und für die Erkennung von Sicherheitsverletzungen ausgewertet werden.

- Alarmierung

  Besonders sicherheitsrelevante Ereignisse werden an ein Security Management gesendet, damit bei Sicherheitsverletzungen schnell reagiert werden kann.

- Verbergen der internen Netzstruktur

  Die Kenntnis der Kommunikationswege erleichtert Hackern die Arbeit. Daher ist es wichtig, die Struktur des zu schützenden Netzes gegenüber dem unsicheren Netz geheimzuhalten. Das Firewall-System schirmt die Struktur des zu schützenden Netzes nach außen hin ab. Es soll aus dem unsicheren Netz nicht sichtbar sein, ob im zu schützenden Netz 10, 100, 1.000 oder 10.000 Rechnersysteme vorhanden sind.

2.2.1 Aktive Firewall-Elemente

Bei Firewall-Elementen wird unterschieden zwischen Elementen, die aktiv in die Kommunikation zwischen dem zu schützenden und dem unsicheren Netz eingreifen, und dem Security Management, das für die Verwaltung des aktiven Firewall-Elementes verantwortlich ist, indem die Sicherheitspolitik einer Organisation in Form eines Regelwerkes definiert wird.
In der Praxis haben sich die aktiven Firewall-Elemente **Packet Filter** und **Application Gateway** herauskristallisiert, die einen unterschiedlichen Ansatz bei der Einbindung in das Kommunikationssystem und bei den Möglichkeiten der Analyse und Protokollierung haben *(siehe auch: Norbert Pohlmann, Firewall-Systeme, 3. Auflage 2000, 549 S., MITP-Verlag, ISBN 3-8266-4040-6).*

2.2.2 High-level Security Firewall-System

In der Praxis gibt es eine Vielzahl von Kombinationsmöglichkeiten von Firewall-Systemen (nur Packet Filter, nur Application Gateway, Packet Filter und Application Gateway, usw.). Ein High-level Security Firewall-System faßt mehrere aktive Firewall-Elemente intelligent zusammen – nämlich zwei Packet Filter als Screened Subnet und ein dual-homed Application Gateway – und garantiert so ein Höchstmaß an Sicherheit.

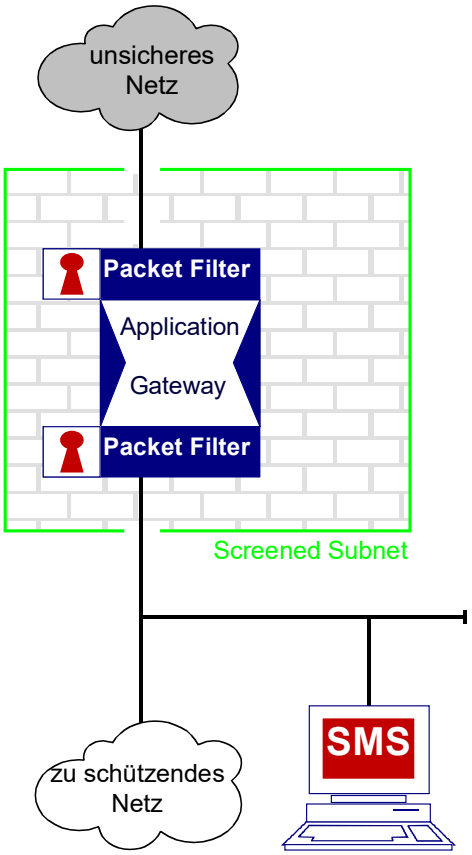


Abbildung 5.2 High-level Security Firewall-System

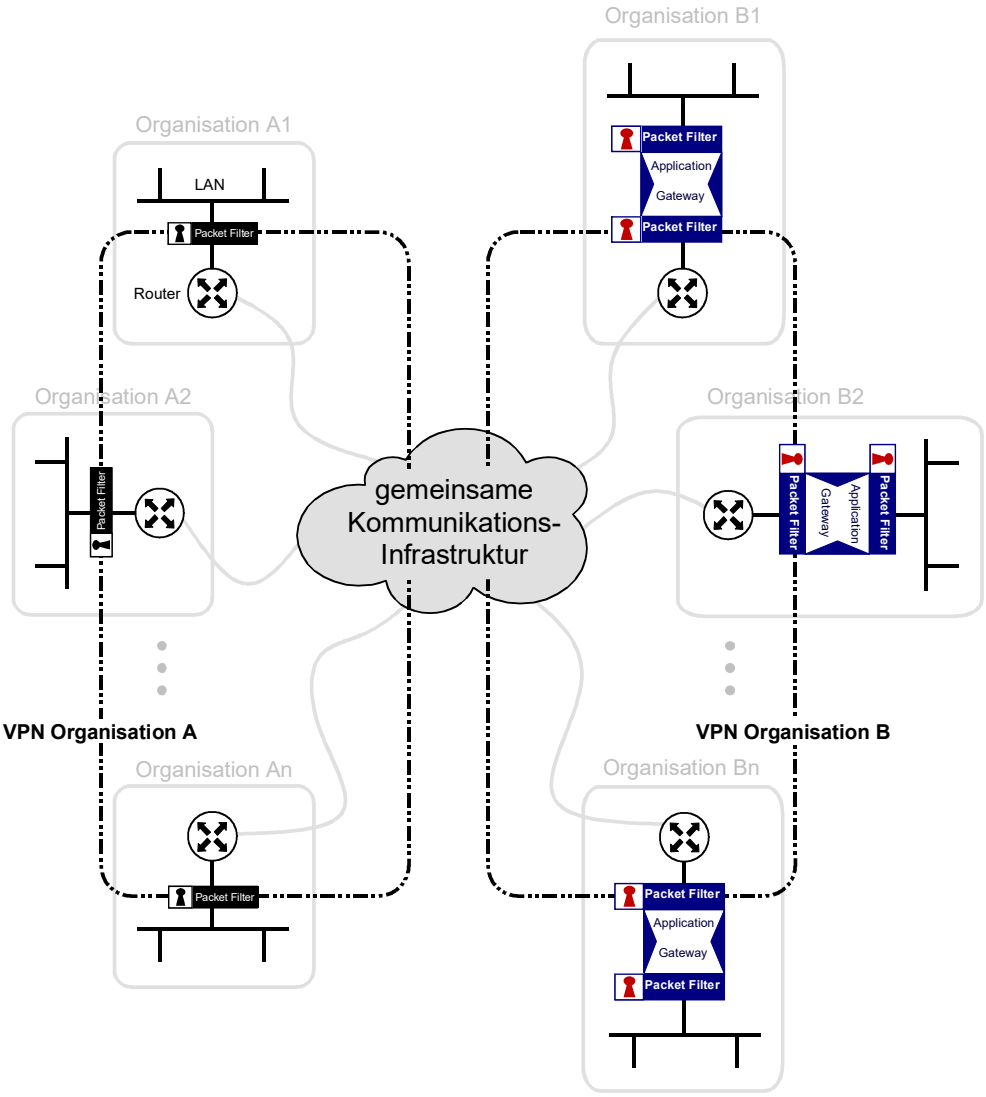


Abbildung 2.3 Integration von Firewall-Systemen in VPNs

2.2.3 Unterschiedliche Firewall-Konzepte:

Packet Filter, Application Gateway oder aber ein High-level Firewall-Konzept haben unterschiedliche Wirksamkeiten, wie sie die Kommunikation nach außen kontrollieren und wie sie einen Übergriff aus einem fremden auf das eigene Netz verhindern können.
Welches Firewall-Konzept nun bei der Etablierung eines VPN über öffentliche Kommunikationsinfrastrukturen verwendet werden sollte, hängt auch von der Kommunikationinfrastruktur selber ab. Wenn die Kommunikationsinfrastruktur an sich schon ein Höchstmaß an Sicherheit und Vertrauenswürdigkeit bietet, d.h. alle angeschlossenen Teilnehmer haben ungefähr die gleichen Sicherheitsbedürfnisse, kann auch mit einer einfachen Firewall-Lösung (z.B. einem Packet-Filter) eine ausreichende Sicherheit erreicht werden.
Wird aber z.B. ein VPN über das Internet realisiert, wo beliebig viele Teilnehmer mit äußerst heterogenen Zielen die gleiche Kommunikationsinfrastruktur benutzen, sollte ein Teilnehmer mit einem hohen Schutzbedarf auf jeden Fall einen hohen Widerstand (mit einem High-level Security Firewall-System) bei der Ankoppelung realisieren.

Ein besonderer Aspekt bei Firewall-Systemen ist, daß sie lokal verwaltet werden können, das heißt, bezogen auf die Kommunikationsmöglichkeiten und Protokollierung kann die eigene lokale Sicherheitspolitik realisiert werden, und dies unabhängig von Anderen.

Vorbehalte gegen Softwarelösungen

Vielfach wird angenommen, auch mit einer reinen Softwarelösung, die z.B. auf Windows-NT läuft, sei bereits ein genügend sicheres VPN realisierbar. Das ist auf gar keinen Fall möglich, denn NT zum Beispiel ist kein sicheres Betriebssystem.

3 Kriterien für die Auswahl von VPN-Lösungen

Die wichtigsten Sicherheitskriterien für die Auswahl einer VPN-Lösung sind:

- die Offenheit und Transparenz der Sicherheit,
- der Nachweis, daß es sich um geprüfte Sicherheit handelt und
- die Gewißheit, daß die Sicherheitsleistung nicht durch staatliche Restriktionen beeinträchtigt wird.

3.1 Offenheit und Transparenz der Sicherheit

Eine VPN-Lösung soll nicht nur die Sicherheitsdienste erfüllen, für die sie angeschafft wurde, sondern in der Praxis „verhindern, was nicht gewollt ist“.
Aus diesem Grund ist die **Vertrauenswürdigkeit in eine VPN-Lösung** von besonderer Bedeutung. Dies ist äquivalent zu einem Pförtner, dem eine Organisation vertrauen können muß, damit die Sicherheitspolitik einer Organisation umgesetzt werden kann.

Offene und transparente Sicherheit

Die Art und Weise der eingesetzten Sicherheitsmechanismen müssen offengelegt werden, damit für den Betreiber eine Virtual Private Networks das erreichbare Sicherheitsniveau überschaubar ist.
Die in einem VPN verwendeten Algorithmen für die Verschlüsselung sollen standardisierte Sicherheitsmechanismen sein, die allgemein bekannt und grundlegend durch Fachleute erforscht sind, damit die Sicherheitsleistung nachweisbar und transparent ist.
Außerdem sollten die Designkriterien für die VPN-Elemente dargestellt werden.

3.2 Geprüfte, nachweisbare Sicherheit

Analog zu den Sicherheitsmechanismen in anderen Bereichen (z.B. Airbag in einem Auto) müssen die VPN-Sicherheitsmechanismen überprüft sein, aber nicht von jedem einzelnen Benutzer (Autofahrer), sondern von unabhängigen Fachleuten (dem TÜV).
Evaluierungen, z.B. durch IT-SEC, dienen dazu, die Qualität von IT-Sicherheitsprodukten zu bestätigen,.

3.3 Sicherheit ohne staatliche Restriktionen

Die Wirksamkeit der Sicherheitsmechanismen darf keinerlei staatlichen Beschränkungen unterliegen, damit ein VPN-System wirklich sicher realisiert werden kann. Mit geeigneter Schlüssellänge für kryptographische Sicherheitsmechanismen wie Verschlüsselung und Authentikation und ohne den Einbau irgendwelcher Sicherheitslücken für Geheimdienste oder andere staatliche Stellen, wie:

- reduzierte Schlüssellängen
- Key Recovery (Möglichkeit zur Rückgewinnung von Schlüsseln)
- Key Escrow-Mechanismen (zwangsweise Schlüsselhinterlegung bei staatlichen Treuhandstellen)
- oder sogar Trapdoors (eingebaute Einstiegsmöglichkeiten).

Bei einer möglichen Bedrohung durch internationale Wirtschaftsspionage muß daher überlegt werden, ausschließlich Sicherheitsprodukte zu verwenden, die diesen Restriktionen nicht unterliegen.