Kapitel 5

Konzepte von Virtual Private Networks

In diesem Kapitel werden verschiedene Konzepte diskutiert, nach denen VPN-Systeme aufgebaut werden können, die zur Sicherstellung einer vertrauenswürdigen Kommunikation genutzt werden.

5.1 Ein VPN-Sicherheitssystem als transparente Lösung

Mit einer Sicherheitsschicht im Kommunikations-Stack kann aus einem »ungesicherten Netzdienst« ein »sicherer Netzdienst« gemacht werden. Hierzu wird im Rechnersystem eine geeignete Sicherheitsschicht (Security Sublayer) in die Kommunikationsarchitektur eingeführt. Eine spezielle und besonders im heterogenen Rechnerumfeld geeignete Möglichkeit, eine solche Sicherheitsschicht zu realisieren, ist zum Beispiel der Einsatz von IPSec in Black-Box-Sicherheitssystemen (siehe Abb. 5.1).

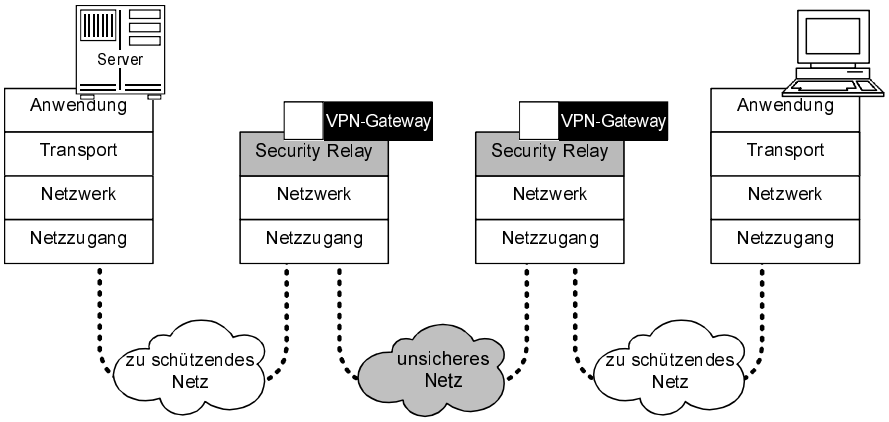

Abb. 5.1: Black-Box-Sicherheitssysteme

5.1.1 Black-Box-Lösung

Black-Box-Lösungen sind handliche Geräte, die auf einfache Weise zwischen Rechnersysteme und Netzwerkanschluss (LAN-Anschluss) geschaltet werden. Das macht sie unabhängig von den jeweiligen Endgeräten und Betriebssystemen und wegen ihrer einfachen Handhabung benutzerfreundlich. In der hochtechnisierten und »intelligenten« High-Tech Black Box spielen sich – unsichtbar für den Benutzer und ohne seine aktive Einwirkung – alle sicherheitsrelevanten Operationen ab.

Im folgenden Kapitel werden die Black Boxes als »VPN-Gateways« bezeichnet.

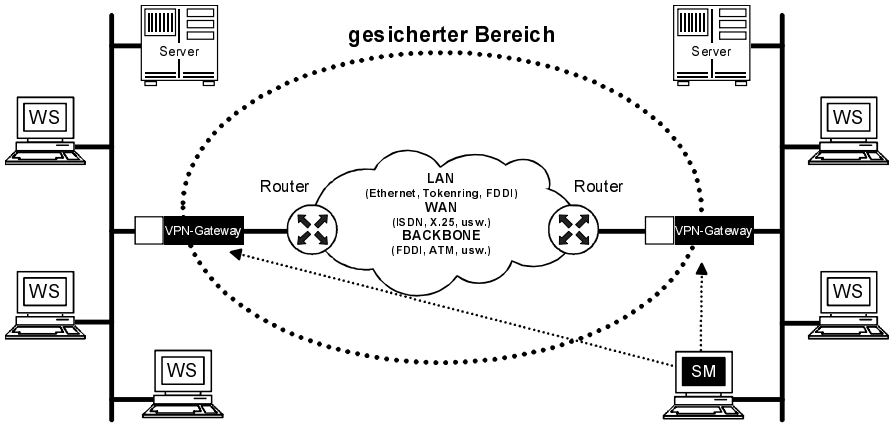

Abb. 5.2: 1:1-VPN mit Black-Box-Lösung

Alle Black Boxes eines Sicherheitssystems sollten von einem Security Management (SM) global gesteuert werden, wobei die Kommunikation – durch kryptographische Funktionen gesichert – über das Netz erfolgen muss.

Vor jedes Rechnersystem oder Subsystem, das geschützt oder über das vertrauliche Daten übertragen werden sollen, wird eine Black Box geschaltet, die sich ähnlich wie eine Bridge verhält. Die Schnittstellen sind beispielsweise zu beiden Seiten (Fast-, Giga-, ...)Ethernet oder Token Ring.

Die Security Black Boxes leisten erweiterte Sicherheitsdienste für das zu schützende Rechnersystem (siehe Abb. 5.2). In Zusammenarbeit mit einer entsprechenden Sicherheitseinrichtung auf der Gegenseite sorgen sie auch für eine kryptographische Sicherung der Kommunikation über das LAN/WAN hinweg.

Vorteile von Black-Box-Lösungen:

- Die Sicherheitseinrichtung Black Box ist unabhängig von Workstations (PCs, UNIX-Systeme, Host-Rechner, ...) und deren Betriebssystemen (Microsoft DOS, Microsoft Windows 95/98/NT/2000/..., OS/2, LINUX, VMS usw.). Das

bedeutet, dass die Black Box auch bei einem Wechsel von Endgeräten oder Workstations weiterhin verwendet werden kann.
- Die Black-Box-Lösung erlaubt die Einrichtung von Sicherheitsfunktionen zwischen Endsystemen, in die ansonsten keine Sicherheitsfunktionen integriert werden könnten (zum Beispiel Terminals oder Routern).
- Bei heterogenen Systemen (unterschiedliche Hardware, Software, Betriebssysteme, ...) kann immer die gleiche Black Box verwendet werden, wodurch sich der notwendige Aufwand verringert.
- Black Boxes sind leichter gesichert zu realisieren als spezielle Software-Lösungen in Rechnersystemen.
- Die Sicherheitseinrichtungen sind hinsichtlich der Sicherheitsqualität unabhängig von anderen Systemkomponenten.
- Die Sicherheit ist anwendungsunabhängig.

Sicherheitsdienste eines VPN-Gateway

Ein VPN-Gateway kann unterschiedliche Sicherheitsdienste bieten:

- Vertraulichkeit,
- Datenintegrität,
- Authentikation (implizit – über die Verschlüsselung – oder explizit mit einem speziellen Authentikationsprotokoll),
- Zugangskontrolle (für Pakete oder Benutzer),
- Rechteverwaltung (für Kommunikationsprotokolle und -dienste),
- Beweissicherung und
- Protokollauswertung.

Dadurch wird erreicht, dass

- Daten nicht im Klartext gelesen werden können,
- keine Manipulation der Daten stattfinden kann,
- nur logische Verbindungen zustande kommen, die erlaubt sind,
- nur Kommunikationsprotokolle und -dienste verwendet werden, die erlaubt sind,
- keine Fremden in der Lage sind, auf Rechnersysteme zuzugreifen, und
- sicherheitsrelevante Ereignisse protokolliert und ausgewertet werden können.

Es gibt gute Gründe für den Einsatz hardwarebasierter VPN-Gateways: Weil die Verschlüsselung unabhängig vom PC- und Netzwerkbetriebssystem durchgeführt wird, beeinträchtigen hardwarebasierte VPNs nicht die Effektivität des Netzwerks. Die Installation erfordert kaum Eingriffe in die vorhandene Netzwerkstruktur und verursacht keinen Aufwand für die mühsame Installation von Software auf einzelnen Rechnern. Weil die Installation relativ einfach vonstatten geht und auf Anwenderseite kaum netzwerktechnisches Know-How vorhanden sein muss, eignet sich die Einrichtung und der Betrieb hardwarebasierter VPN-Gateways auch als Service-Geschäftsmodell für Internet Service Provider.

5.1.2 Security Sublayer im Endgerät: End-to-End-Verschlüsselung

Eine weitere Möglichkeit, die notwendigen Sicherheitsfunktionen einzurichten, ist die Integration einer Sicherheitsschicht in die Rechnersysteme.

Dafür wird zum Beispiel auf den Netzwerkdienst, der von den Netzwerktreibern angeboten wird, ein sogenanntes »Security Sublayer« aufgesetzt. Dieses Security Sublayer bietet der Transportschicht alle Services des Netzwerktreibers – mit dem Unterschied, dass eine Verbindung nur bei Bedarf mit den gewünschten Sicherheitsmerkmalen versehen wird. Aus Sicht des Netzwerktreibers (Netzwerkebene) verhält sich das Security Sublayer wie eine Transportschicht, aus Sicht der Transportschicht verhält es sich wie der Netzwerktreiber. Das Security Sublayer ist somit völlig transparent gegenüber den benachbarten Schichten.

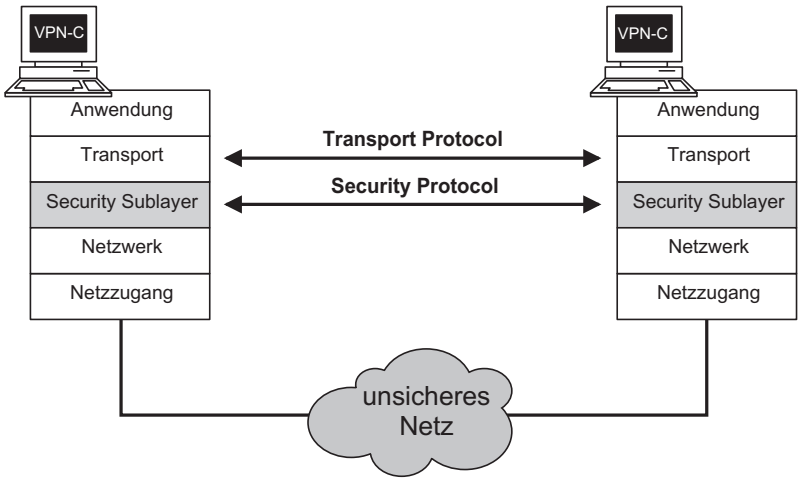

Abb. 5.3: End-to-End-Sicherheit mit PC Security Komponente

In der Praxis wird das Security Sublayer softwaremäßig als transparenter Netzwerktreiber in das Rechnersystem installiert. Wegen der höheren Sicherheit sollte bei einer solchen Lösung unterstützend eine Verschlüsselungskarte verwendet werden, in der die geheimen Schlüssel gespeichert sind.

Vorteile des VPN-Clients:

- Der VPN-Client ist kostengünstiger als die Black-Box-Lösung.
- Der VPN-Client bietet End-to-End-Sicherheit. Das bedeutet, dass nicht nur die Verbindung zwischen verschiedenen LAN-Segmenten nach außen hin abgeschottet wird, sondern auch jede einzelne Workstation (PC) gegenüber anderen.
- Eine »Person« kann authentisiert werden.

Sicherheitsdienste von PC-Security-Komponenten

Eine VPN-Client bietet unterschiedliche Sicherheitsdienste:

- Vertraulichkeit,
- Datenintegrität,
- Authentikation (implizit – über die Verschlüsselung – oder explizit mit einem speziellen Authentikationsprotokoll),
- Zugangskontrolle (für Pakete),

Dadurch wird erreicht, dass

- Daten nicht im Klartext gelesen werden können,
- keine Manipulation der Daten stattfinden kann,
- nur logische Verbindungen zustande kommen, die erlaubt sind,
- keine Fremden in der Lage sind, auf Rechnersysteme zuzugreifen.

Anwendungsmöglichkeiten und Einsatzvarianten

Mit einem VPN-Gateway und mit einem VPN-Client kann der Sicherheitsdienst Verschlüsselung in unterschiedliche Anwendungsgebiete integriert werden. In LANs können ausgewählte Segmente, bestimmte logische Bereiche oder Anwendungen geschützt werden. Bei der Kopplung von LAN-Segmenten über öffentliche Netze können mit einem VPN-Gateway Angreifer abgewehrt und kryptographisch abgesicherte, vertrauenswürdige logische Netze gebildet werden.

5.1.3 Sicherheit in LAN-Segmenten

Die Integrationsvariante »Sicherheit in LAN-Segmenten« schützt ausgewählte Segmente, logische Bereiche in einem Segment, ausgewählte Rechnersysteme oder Anwendungen innerhalb eines Segments des LAN, beispielsweise die Personalverwaltung (m:n-Topologie).

In den VPN-Gateways stehen Access-Listen und weitere sicherheitsrelevante Informationen. Außerdem stellen sie ein Logbuch zur Verfügung, in dem sicherheitsrelevante Ereignisse protokolliert werden. Die Kommunikationsbeziehungen werden in diesem Anwendungsbeispiel mit Hilfe der Adressen der Netzzugangsebene (MAC-Adressen), die möglichen höheren Protokolle mit Hilfe des Typenfelds bestimmt.

Je nach Einstellung werden die Datenpakete der Netzzugangsebene

- im Klartext durchgelassen,
- in verschlüsselter Form durchgelassen oder
- abgeblockt.

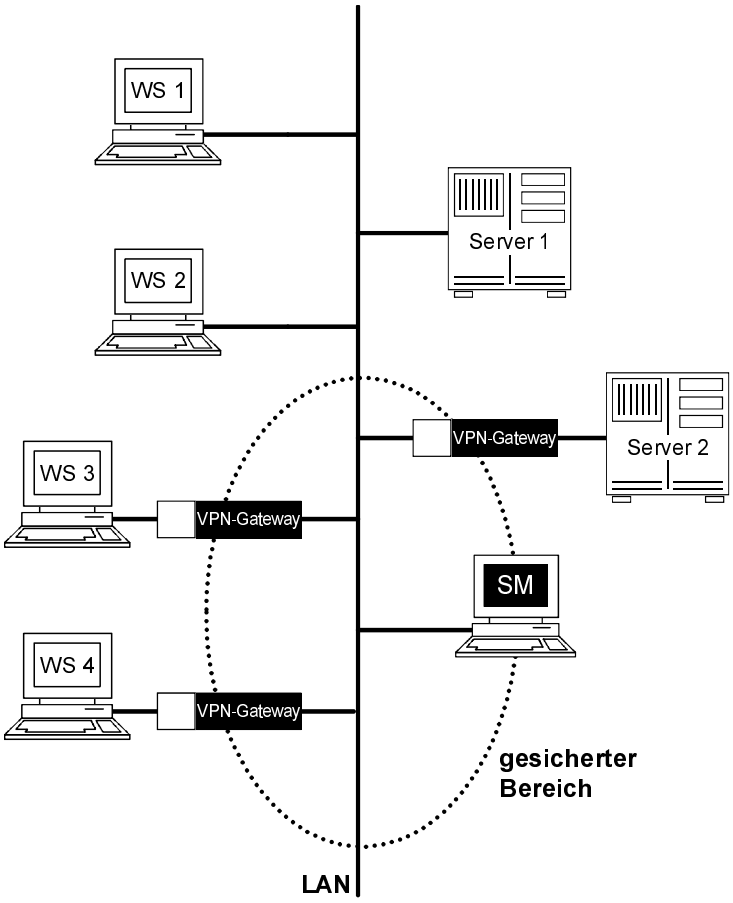

Abb. 5.4: Sicherheit in LAN-Segmenten

In diesem Beispiel (Abb. 5.4) wird dargestellt, wie die Absicherung der Kommunikation der beiden Workstations 3 und 4 mit dem Server 2 gesichert, das heißt verschlüsselt und kontrolliert werden kann. Im LAN-Segment soll niemand in der Lage sein, die übertragenen Daten im Klartext mitzulesen. Falls die Workstation 4 eine Kommunikation mit dem Server 2 durchführen möchte, wird das MAC-Paket von der Workstation 4 an das VPN-Gateway gesendet. Dieses prüft anhand der Access-Liste, ob eine Verbindung zwischen der Workstation 4 und dem Server 2 erlaubt ist (Packet-Filter-Funktion). Im vorliegenden Beispielfall ist eine verschlüsselte Kommunikation erlaubt.

Anschließend wird im VPN-Gateway der Inhalt des MAC-Paketes verschlüsselt und zur Gegenseite übertragen. Das VPN-Gateway vor dem zu schützenden Server 2 liest das MAC-Paket, stellt in seiner Access-Liste fest, dass eine verschlüsselte Kommunikation zwischen der Workstation 4 und dem Server 2 erlaubt ist, und

entschlüsselt das MAC-Paket entsprechend. Anschließend sendet das VPN-Gateway das MAC-Paket im Klartext zum Server 2. Für die Workstation 4 und den Server 2 bleiben die Sicherheitsfunktionen transparent. Die Steuerung des VPN-Gateway wird in gesicherter Form durch ein zentrales Sicherheitsmanagement realisiert.

Möchte die Workstation 4 mit Server 1 kommunizieren, sendet sie dazu ein MAC-Paket auf das LAN-Segment. Im VPN-Gateway der Workstation 4 wird das Paket angenommen. Anhand der Access-Liste wird festgestellt, dass es sich um eine erlaubte Klartextverbindung handelt. Das Paket kann daher das VPN-Gateway im Klartext passieren und gelangt über das LAN zum Server 1.

Wenn die Workstation 2 auf Server 2 zugreifen will, sendet sie das MAC-Paket im Klartext. Das VPN-Gateway von Server 2 nimmt das Paket auf und stellt fest, dass es sich um eine nicht erlaubte Verbindung handelt. Das Paket wird deshalb vom Packet Filter verworfen. Dieses sicherheitsrelevante Ereignis wird entweder im Logbuch gespeichert oder, falls dies so eingestellt ist, als »Spontane Meldung« an das Sicherheitsmanagement (SM) gesendet.

Merkmale der MAC-Verschlüsselung

- Die MAC-Verschlüsselung ist unabhängig vom Netzwerkprotokoll (wie IPX, NLSP, LLC, Netbios, Decnet, SNA usw.).
- Die Verschlüsselung ist unabhängig vom verwendeten Netzwerk-Betriebssystem.
- Die Passworte der Netzwerk-Betriebssysteme (zum Beispiel Netware) werden in verschlüsselter Form übertragen.

5.1.4 Kopplung von LAN-Segmenten mit einer Security Bridge

Bei der Integrationsvariante »Kopplung mehrerer LAN-Segmente« werden zwei LAN-Segmente verbunden (Twisted Pair, Glasfaser usw.), die über einen öffentlich zugänglichen Bereich miteinander gekoppelt sind. Die Kabel in diesem öffentlich zugänglichen Bereich (im vorliegenden Beispiel Gebäudekomplex B, siehe Abb. 5.5) werden mit einem VPN-Gateway als 1:1-VPN gesichert. Dies ist eine einfache Möglichkeit, die notwendige Sicherheit zu garantieren.

Ein Beispiel für die Kopplung mehrerer LAN-Segmente ist die Kommunikation zwischen Bürogebäude und Fertigungshalle: In den Büroräumen (Gebäudekomplex C) steht das Verwaltungssystem (Server). Aus der Fertigungshalle (Gebäudekomplex A) werden Softwarebestände, Seriennummern für die Produkte, Lieferscheine usw. benötigt. Aus diesem Grund müssen die Workstations aus der Fertigungshalle des Gebäudekomplexes A Zugriff auf das Verwaltungssystem (Server) des Gebäudekomplexes C haben.

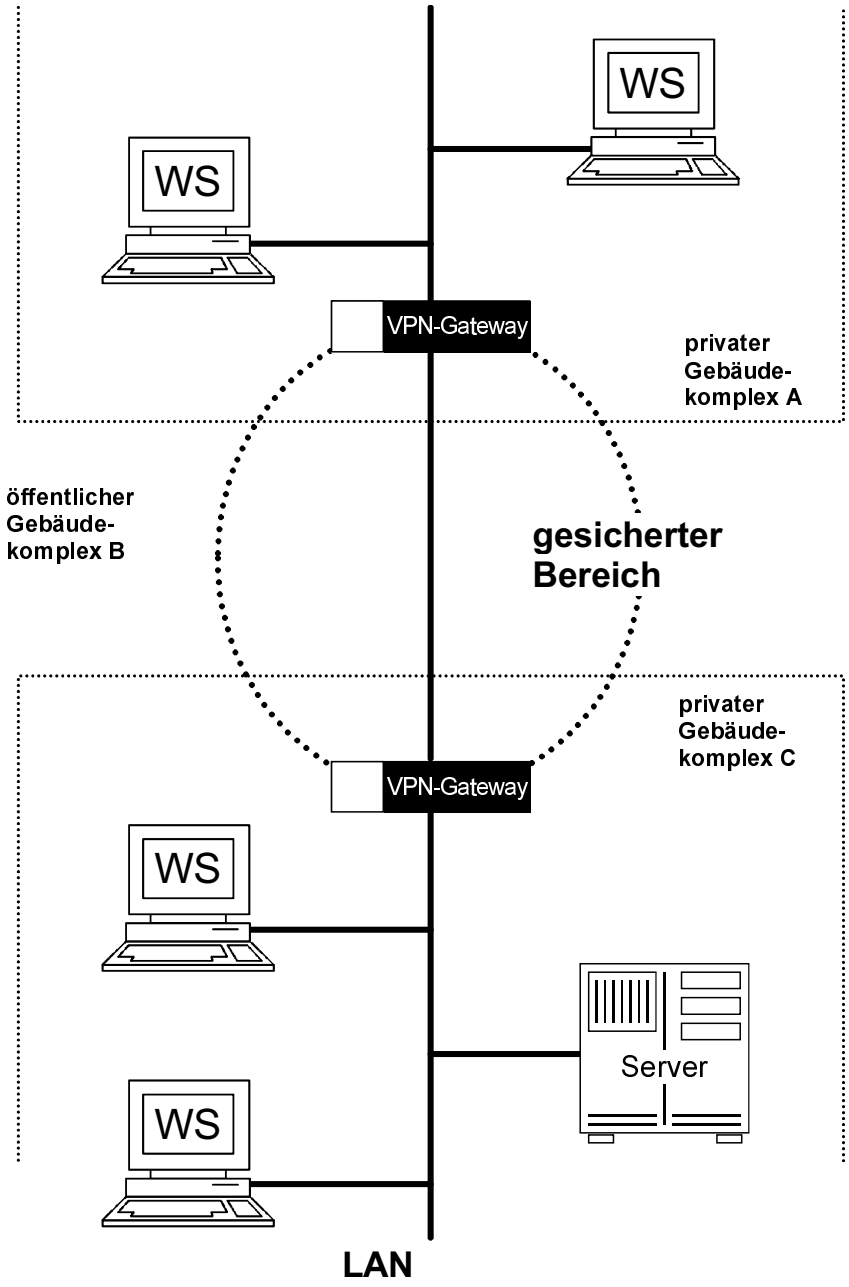

Abb. 5.5: Security Bridge für mehrere LAN-Segmente

In diesem Beispiel ist die Verwendung von VPN-Gateways eine einfache Möglichkeit, die notwendige Sicherheit zu garantieren. Die VPN-Gateways garantieren hier zusätzlich zum »Bridging« die Vertraulichkeit der Daten durch die Verschlüsselung der MAC-Pakete und verhindern, dass Fremde auf das System zugreifen können. Durch die Verschlüsselung wird eine implizite Authentikation erreicht, so dass Fremde nicht in der Lage sind, sinnvolle Pakete in das LAN zu senden.

In dieser Integrationsvariante kann eine solche VPN-Gateway auch als Security Repeater betrieben werden. Dann werden alle Pakete des VPN-Gateways auf der MAC-Ebene ver- bzw. entschlüsselt.

5.1.5 Kopplung von LAN-Segmenten über öffentliche Netze

Mit den folgenden Integrationsvarianten kann die Kommunikation auf der Netzwerkebene, der IP-Ebene, geschützt werden. Dies entspricht zum Beispiel der Bildung von Virtual Private Networks (VPN) nach dem IPSec-Standard.

Anwendungsmöglichkeiten dafür sind

- die Kommunikation aller Rechnersysteme in einem LAN,
- die Kommunikation ausgewählter Rechnersysteme in einem LAN oder
- die Kommunikation über öffentliche Netze beziehungsweise über ein Backbone.

In der folgenden Abbildung 5.6 ist eine Integrationsvariante dargestellt, bei der die Kommunikation über ein öffentliches Netz (ISDN, X.25, Leased Line oder ähnliches), Satellitenübertragung oder ein Backbone (FDDI, ATM usw.) gesichert wird.

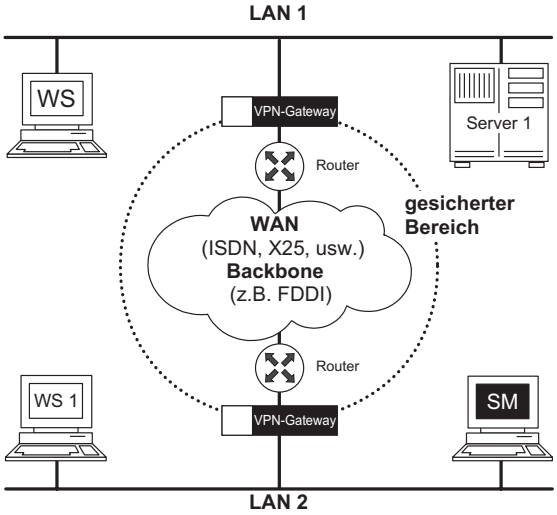

Abb. 5.6: Kopplung von LAN-Segmenten über öffentliche Netze

Die VPN-Gateways werden zur Netzwerksicherung vor den Routern positioniert.

In dieser Integrationsvariante werden die Kommunikationsbeziehungen mit Hilfe der IP-Adressen bestimmt. Je nach Einstellung werden die IP-Pakete von den VPN-Gateways im Klartext oder verschlüsselt durchgelassen oder abgeblockt.

Möchte die Workstation 1 auf Server 1 zugreifen, sendet die Workstation 1 das IP-Paket im Klartext in das LAN. Das VPN-Gateway vor dem Router empfängt das IP-Paket und überprüft in den Access-Listen die Regeln. Falls eine verschlüsselte Verbindung zwischen Workstation 1 und Server 1 erlaubt ist, verschlüsselt das VPN-Gateway das IP-Paket. Der Header des IP-Paketes bleibt unverschlüsselt, damit er vom Router vermittelt werden kann.

In diesem Konzept spielt es aus Sicht des VPN-Gateway keine Rolle, ob die Kommunikation über ISDN, über Satellit, oder über andere Wege erfolgt. Das VPN-Gateway führt in jedem Fall die gleichen Sicherheitsfunktionen aus.

Auf der Gegenseite empfängt das VPN-Gateway das IP-Paket und erkennt in der Access-Liste, dass es sich um eine erlaubte verschlüsselte Kommunikation handelt. Das VPN-Gateway entschlüsselt dann das IP-Paket entsprechend und sendet es im Klartext zum Server 1. Auch hier bleibt die Sicherheit für die beteiligten Komponenten (Workstations, Server, Router usw.) transparent. Die Rechteverwaltung wird zentral von einem Sicherheitsmanagement (SM) realisiert. In einer solchen Konfiguration ist es auch möglich, die Rechteverwaltung sehr einfach zu gestalten. So kann zum Beispiel über die Sub-Adressen der LANs die einfache Regel »Verschlüsselung aller Pakete, die zu den entsprechenden LANs gehören« definiert werden.

Ein besonderer Vorteil dieser Lösung ist, dass sie auch die Sicherheitsanforderungen für Backup und flexible Bandbreiten erfüllt. Weil die Sicherheit unabhängig vom Übertragungsmedium ist, kann immer ein gleich hohes Maß an Sicherheit garantiert werden, auch wenn beispielsweise im Normalbetrieb über eine Standleitung kommuniziert und im Backup-Fall das ISDN-Netz verwendet wird.

Die Funktion eines VPN-Gateways und eines Routers sollte aus sicherheitstechnischer Sicht und aus Gründen der Performance immer von getrennten Komponenten ausgeübt werden.

Router mit IPSec-Funktionalität zeigen meist starke Leistungseinbrüche und bilden daher einen »Flaschenhals«. Aus diesem Grunde stellt der Router die Verbindung zum WAN7-Backbone dar. Zwischen Router und dem LAN-Segment wird das VPN-Gateway positioniert.

Tunneling

Beim Tunneling wird jedes zu sendende Paket in ein neues Paket verpackt. Dazu wird ein zusätzlicher neuer Header vorgeschaltet. So wird beispielsweise für IP-basierte Netze ein IP-Header vorangestellt. Weiterhin kommen zusätzliche Informationen oder Kennzeichen im Body-Teil des Pakets dazu.

Die vorgeschalteten Header charakterisieren die Endpunkte des Tunnels; 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 (zum Beispiel IP oder IPX) verpackt übertragen und am Ziel wieder entpackt werden. Die dazwischenliegenden Router »wissen« nichts von diesen Mechanismen / Pohl99d/.

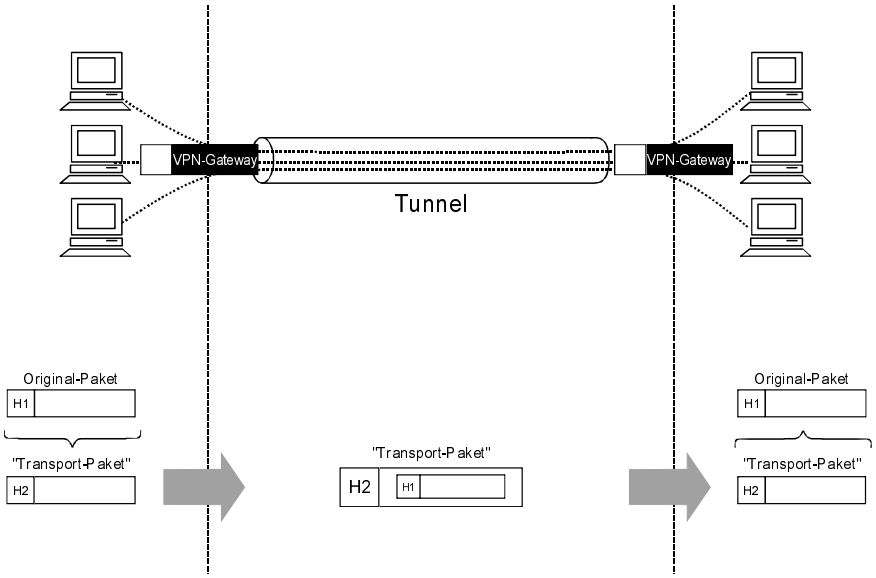

Abb. 5.7: Tunneling

Ein Vorteil von Tunneling ist, dass bei der Kommunikation über eine öffentliche Infrastruktur – beispielsweise zwischen zwei Organisationen – immer nur zwei IP-Adressen verwendet werden, unabhängig davon, über welchen Weg die Kommunikation tatsächlich stattfindet. Im Tunnel können auch nicht routbare Protokolle eingepackt werden.

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 Adressen der Komponenten, die das Tunneling realisieren, sichtbar werden. Andererseits können dann Features wie Prioritätensteuerung nicht mehr verwendet werden.

5.1.6 Bildung von kryptographisch gesicherten logischen Netzen (VPN)

VPN-Gateways können auch vor bestimmten Rechnersystemen platziert werden. Hierdurch wird eine höhere »Tiefe« der »End-to-End-Sicherheit« erreicht.

Mit dieser Integrationsvariante können sichere logische Netze in einem Gesamtnetz realisiert werden. Es ist auch möglich, mehrere logische Netze parallel oder geschachtelt zu betreiben. Ein VPN-Gateway kann dann auch zu mehreren logischen Netzen gehören.

Damit können bestimmte, besonders sicherheitsrelevante Bereiche (der arbeitsmedizinische Bereich, die Personalabteilung, Geschäftsführung, Forschungs- oder Marketing-Abteilung) geschützt werden (m:n-Topologie). Alle Daten, die zwischen den Rechnersystemen ausgetauscht werden, sind verschlüsselt.

In den beschriebenen Virtual Private Networks (VPNs) können verschiedene Strategien verfolgt werden. So kann zum Beispiel festgelegt werden, dass die Kommunikation zwischen den Workstations 1, 2 und 3 immer verschlüsselt wird und alle anderen Kommunikationsverbindungen im Klartext ablaufen. Eine andere Strategie könnte vorsehen, dass nur eine Kommunikation zwischen den Workstations 1, 2 und 3 möglich ist, und das auch nur in verschlüsselter Form.

Merkmale der IP-Verschlüsselung

Die IP-Verschlüsselung ist unabhängig vom Übertragungsmedium und bietet daher einen hohen Investitionsschutz. Die Vertraulichkeit der Daten wird gewährleistet, auch die der Passworte wie beispielsweise bei Telnet, FTP oder rlogin.

Der Zugriff von Angreifern aus öffentlichen Netzen auf Rechnersysteme wird abgewehrt. Außerdem ist es mit einem solchen Sicherheitssystem möglich, Security Domains zu bilden.

5.1.7 VPN-Client

Ein VPN -Client kann eine Softwarelösung oder eine Kombination aus Software- und Hardwarelösung sein, die in das Rechnersystem integriert wird. Es handelt sich um ein Security Sublayer, das erweiterte Kommunikationssicherheitsdienste wie Verschlüsselung und Zugangskontrolle zur Verfügung stellt. Durch die Verwendung sicherer Hardware kann die vertrauliche Speicherung von geheimen

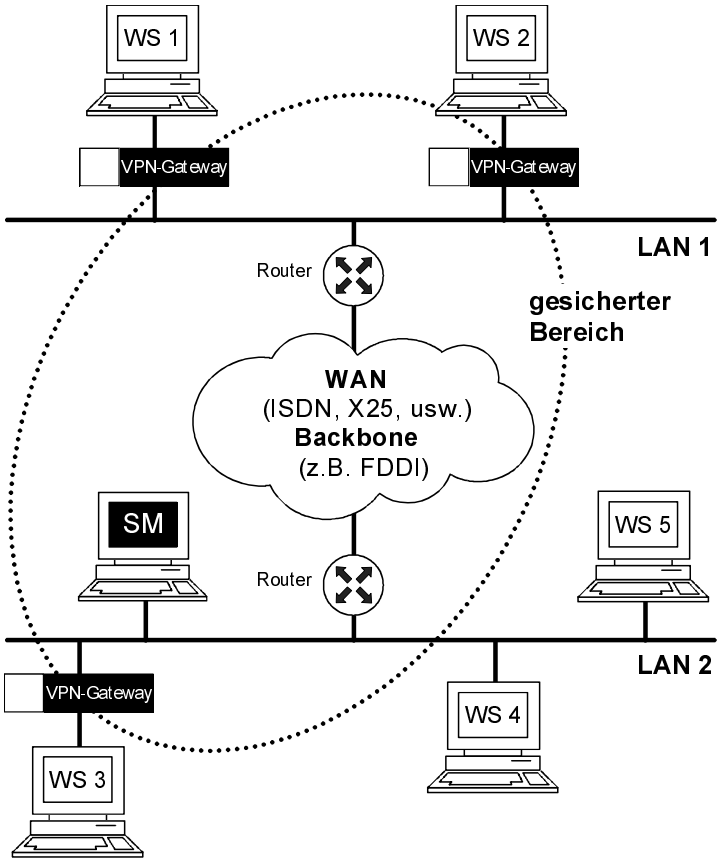

Abb. 5.8: End-to-End-Sicherheit

Schlüsseln gewährleistet werden. Mit Hilfe eines VPN-Clients kann die Verschlüsselung zwischen PCs, aber auch die Verschlüsselung zwischen einem PC und einem VPN-Gateway realisiert werden.

Wenn eine Workstation ohne VPN-Client mit dem Server-System 1 kommuniziert, kann dies über das Packet Filter anhand der festgelegten Protokolle und Dienste kontrolliert werden. Mit Hilfe des Sicherheitsmanagements können der VPN-Client sowie die VPN-Gateways gesteuert und verwaltet werden.

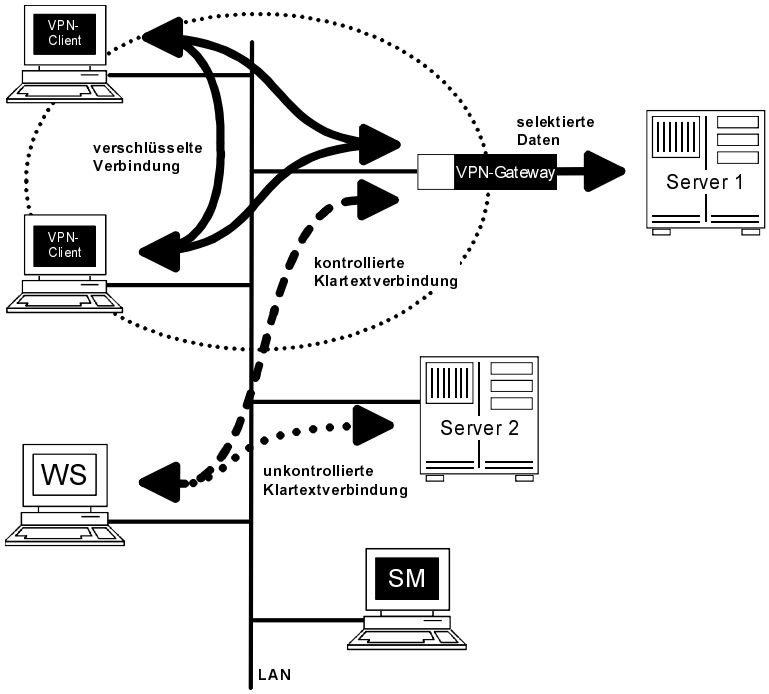

Abb. 5.9: VPN-Client

5.1.8 Anwendungsfälle

Die Notwendigkeit, Rechnersysteme »remote« an das lokale Netz einer Organisation anzukoppeln, wird zunehmend größer. Für Außendienstmitarbeiter wird es immer wichtiger, direkt auf Preislisten und Lieferzeiten zugreifen und Bestellungen eingeben zu können, damit der Arbeitsvorgang effektiv und ohne Medienbruch durchgeführt werden kann. Im Hinblick auf gesellschaftspolitische Entwicklungen und die Verfügbarkeit von Know-how wird es immer dringlicher, auch Heimarbeitsplätze anzubieten, die »remote« an das System angekoppelt sind. Die Eintrittswahrscheinlichkeit eines Angriffs ist aber gerade in der Umgebung von Remote-Rechnern besonders hoch einzustufen, so dass bei der Remote-Ankoppelung eine hohe Gefahr des Missbrauchs besteht.

Kopplung von mobilen Rechnersystemen (Notebooks)

Notebooks können z. B. mit einem Modem über die Telefonleitung oder mit einem Mobiltelefon über das Mobilfunknetz (z. B. GSM, GPRS, UMTS) an ein Server-System gekoppelt werden. Die Kombination von VPN-Client und VPN-Gateway bietet ein einfaches Konzept, das die notwendige hohe Sicherheit zur Verfügung stellt.

Im folgenden Beispiel (Abb. 5.10) werden die IP-Pakete vom Notebook in verschlüsselter Form über das Fernsprechnetz oder Mobilfunknetz gesendet und vom VPN-Gateway entsprechend entschlüsselt.

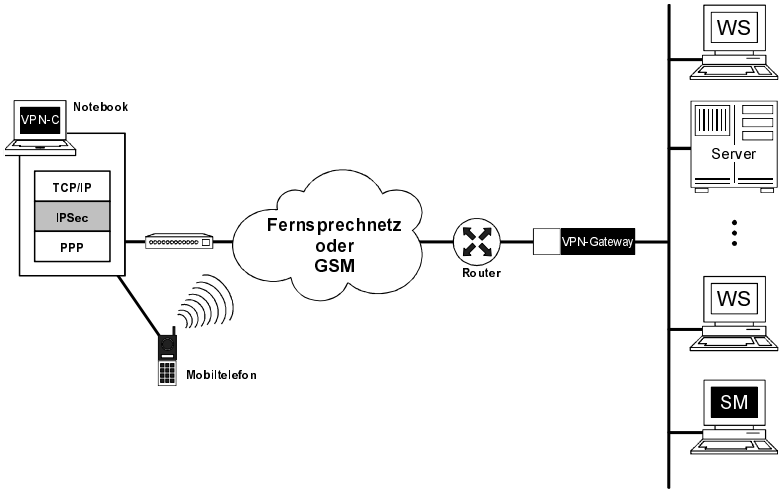

Abb. 5.10: Kopplung mobiler Rechnersysteme

Durch das VPN-Gateway kann bestimmt werden, welcher Benutzer auf welches Rechnersystem zugreifen darf, um beispielsweise Arbeiten abzuliefern oder neue Aufträge zu holen.

Kopplung von Tele-Arbeitsplätzen

Für die Einrichtung von Telearbeitsplätzen ist die Ankopplung über ISDN besonders interessant. ISDN ist in Deutschland flächendeckend verfügbar und inzwischen sind viele Millionen Anschlüsse darauf umgestellt; die Akzeptanz ist so hoch wie in keinem anderen Land.

Über das ISDN-Netz können IP-Pakete verschlüsselt und in gesicherter Form übertragen und auf der Seite der Zentrale durch das VPN-Gateway entschlüsselt werden. Das VPN-Gateway sorgt für eine effektive Abschottung, so dass kein Hacker in der Lage ist, auf die zu schützenden Rechnersysteme zuzugreifen.

Tele-Arbeitsplätze können so nicht nur durch die Verschlüsselung, sondern auch durch Überwachung und Kontrolle mit Packet-Filter-Funktionalität geschützt werden.

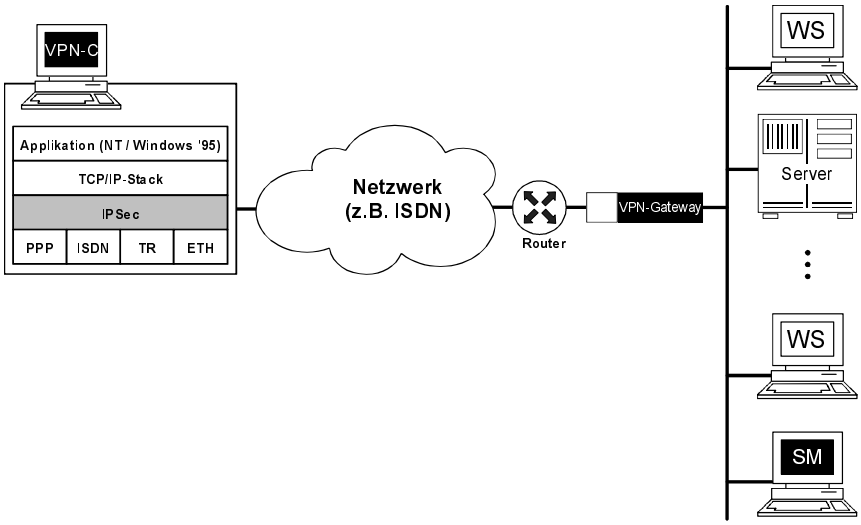

Abb. 5.11: Kopplung von Tele-Arbeitsplätzen

Mit Hilfe der Packet-Filter auf der zentralen Seite kann kontrolliert werden, auf welches Server-System und mit welchen Protokollen die Tele-Arbeitsplätze zugreifen dürfen. Außerdem kann genau festgelegt werden, zu welcher Zeit der Zugriff erlaubt wird.

VPN-Realisierungen

Hinsichtlich der Realisierung von VPNs existieren unterschiedliche Lösungsansätze. Einige Hersteller haben spezielle Sicherheitsprotokolle 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 Anwendungen und bei Terminal-Anwendungen von besonderer Bedeutung.

5.2 Topologien von VPNs

Ein VPN fasst eine Menge von Netzwerk-Knoten zu einem Netzwerk zusammen, das durch krytographische Methoden vor dem Zugriff Außenstehender abgeschottet ist. Dabei spielt es keine Rolle, ob die Kommunikations-Strecken über öffentli-

che Netze (Telefon, Internet) geführt werden oder ob Teile eines internen LAN miteinander kommunizieren sollen. Abhängig davon, zwischen wie vielen Partnern die Verschlüsselung aufgebaut werden muss, kommen VPN-Strukturen 1:1, 1:n und m:n zur Anwendung.

Die Entscheidung, welche dieser Topologien zum Einsatz kommt, ergibt sich aus der Anforderungs-Analyse der über das Netzwerk abzuwickelnden Aufgaben und ihres Sicherheitsbedarfs. Da ein späterer Wechsel auf eine andere VPN-Topologie oft nur mit erheblichen Aufwand möglich ist, kommt dieser grundsätzlichen Auswahl eine besondere Bedeutung zu.

5.2.1 Die 1:1-Topologie

Bei dieser Topologie sind nur zwei Systeme an der Bildung eines VPN beteiligt. Zwischen ihnen wird die verschlüsselte Kommunikation abgewickelt, die von Unbefugten nicht abgehört werden kann. Fast immer handelt es sich bei diesen Systemen um VPN-Gateways, die verschiedene Standorte einer größeren Firma oder Institution miteinander verbinden. Will ein Rechner am Standort A über das VPN mit einem Rechner am Standort B kommunizieren, gelangen seine Netzwerkpakete zunächst unverschlüsselt über das lokale Netz A bis zum VPN-Gateway. Von dort gehen sie über den verschlüsselten und authentisierten Tunnel bis zum VPN-Gateway B auf der anderen Seite. Ab da bewegen sie sich wieder unverschlüsselt durch das Netz B zum Zielrechner. Da im Normalfall mehrere Rechner aus Netz A gleichzeitig mit Rechnern aus Netz B kommunizieren wollen, können über den VPN-Tunnel mehrere logische Kanäle geöffnet werden, die jeweils den einzelnen Kommunikations-Strecken zugeordnet sind. Bei den VPN-Gateways kann es sich um dezidierte Systeme oder auch um Firewall-Systeme oder Router handeln, bei denen eine zusätzliche VPN-Software installiert wurde. Abbildung 5.12 zeigt ein Beispiel.

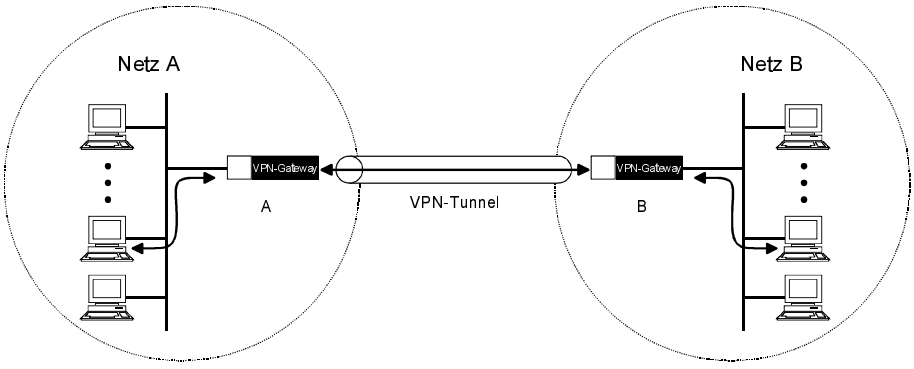

Abb. 5.12: VPN in der 1:1-Topologie

Charakteristisch für ein 1:1-VPN ist die starre Zuordnung der Tunnel zu den VPN-Gateways und ihren festen IP-Adressen. Deshalb wird auch die in Abbildung 5.13 angegebene Topologie aus drei gekoppelten Netzwerken als (in diesem Fall: dreifaches) 1:1-VPN bezeichnet. Es sind insgesamt drei Tunnel vorhanden, über die die Kommunikation zwischen den Standorten A, B und C abgewickelt wird.

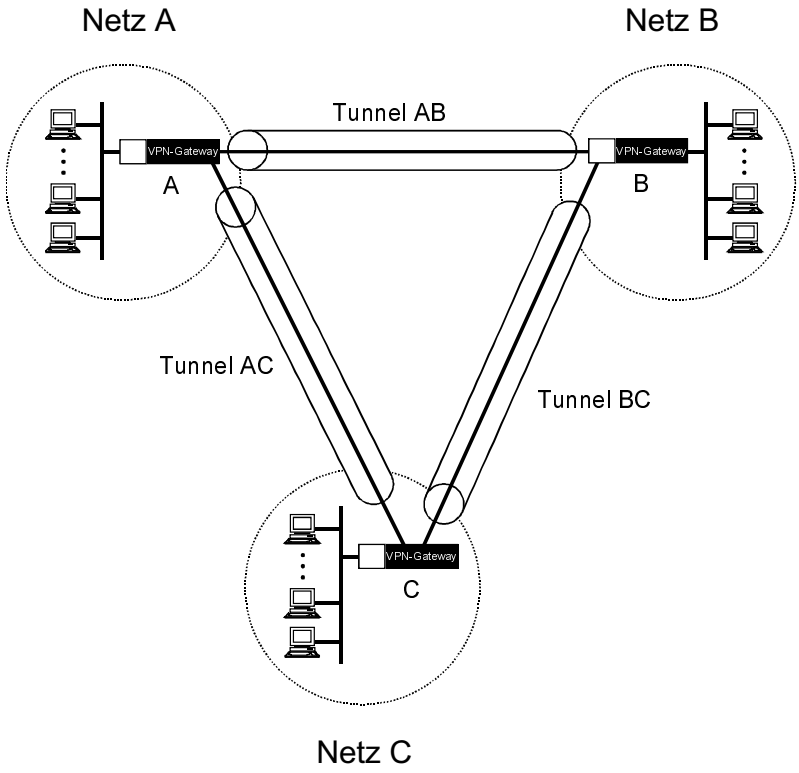

Abb. 5.13: Drei Standorte mit 1:1-Topologie

5.2.2 Die 1:n-Topologie

In vielen Fällen reicht die Zuordnung von VPN-Strecken zu festen Tunneln nicht aus. Geschäftsreisende wie zum Beispiel Außendienst-Mitarbeiter müssen sich von beliebigen Standorten aus über unterschiedliche Provider in das interne Netz einwählen können. Geschieht diese Kommunikation über ein öffentliches Netz wie das Internet, haben sie praktisch keinen Einfluss auf die ihnen vom Provider zur Verfügung gestellte Netzwerk-Adresse. Das VPN-Gateway auf der anderen Seite muss nach erfolgter Authentikation eine VPN-Strecke zu der jeweiligen (temporären) Adresse des Benutzers aufbauen. Hinter dem VPN-Gateway befindet sich wieder das firmeninterne Netz, über das die weitere Kommunikation mit dem Ziel-

rechner unverschlüsselt abgewickelt wird. Da die gesicherten Verbindungen jeweils vom VPN-Gateway zu den diversen Netzknoten reichen, trägt diese Topologie den Namen 1:n-VPN.

Im Gegensatz zu den sicheren Tunneln bei einem 1:1-VPN, über die jeweils mehrere Rechner durch unterschiedliche logische Kanäle miteinander kommunizieren können, besteht beim 1:n-VPN eine gesicherte Peer-to-Peer-Verbindung zwischen den Endknoten der Kommunikation. Abbildung 5.14 gibt ein Beispiel.

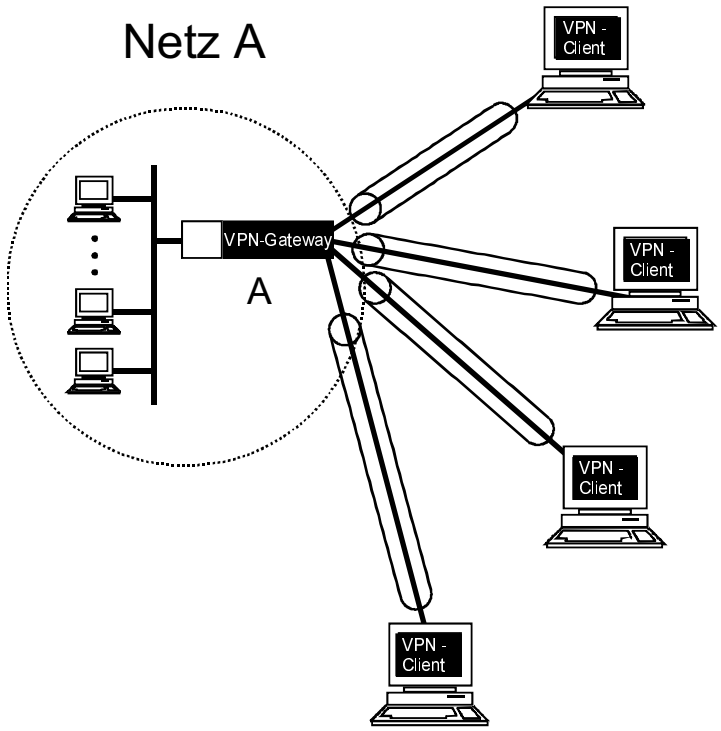

Abb. 5.14: VPN in der 1:n-Topologie

5.2.3 Die m:n-Topologie

Die beiden bisher beschriebenen Topologien decken die meisten VPN-Anwendungsfälle ab. Insbesondere die Kommunikation über das Internet lässt sich fast immer durch eine der beiden Varianten implementieren. Dennoch gibt es Anforderungen, bei denen eine mehr oder weniger willkürliche Gruppierung von Netzwerk-Knoten zu logischen Netzen mit erhöhtem Sicherheitsbedarf erforderlich ist.

So könnte es beispielsweise nötig sein, die über das gesamte Firmennetz verteilten Rechner einer Forschungs-Abteilung logisch vom Rest des Netzwerks abzukop-

peln, obwohl die Pakete physikalisch ganz oder teilweise über dieselben Leitungen gesendet werden. Auch die Zusammenstellung dezidierter Rechner aus verschiedenen physikalischen Netzwerken (beispielsweise Zulieferer und Endfertiger) zu einem »privaten« Netz ist denkbar. Bei einem solchen Konzept ist die beliebige Zusammenstellung der einzelnen Rechner zu einem oder mehreren VPNs möglich, was die Bezeichnung m:n-VPN erklärt (Abb. 5.15).

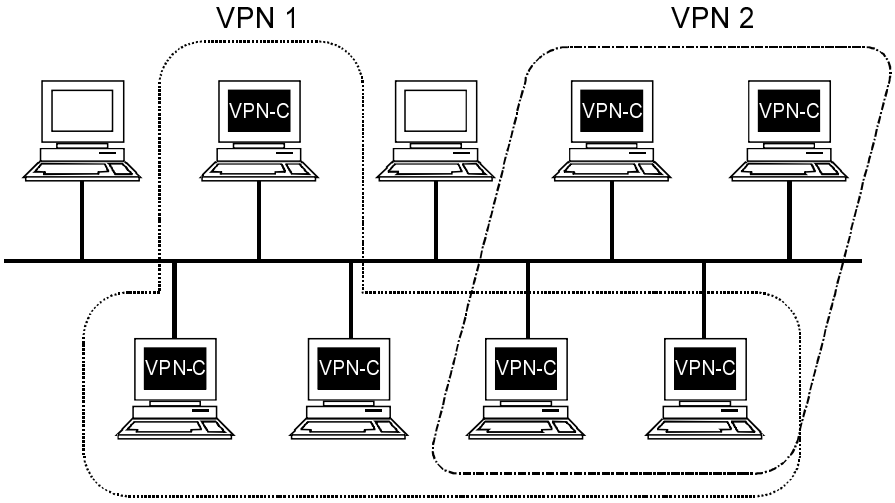

Abb. 5.15: VPN in der m:n-Topologie

Der organisatorische Aufwand zur Implementierung und Wartung der m:n-Topologie ist deutlich größer als bei den anderen Varianten, da sich durch die im Betrieb üblichen organisatorischen Maßnahmen die Zuordnung der einzelnen Rechner zu den VPNs häufiger als bei den anderen Topologien ändert und die VPN-Struktur tagesaktuell nachgezogen werden muss.

5.3 Sicherheitsmanagement für VPN-Systeme

Mit Hilfe eines Sicherheitsmanagements sollte eine einfache, zuverlässige und nachprüfbare Verwaltung eines VPN-Systems möglich sein.

5.3.1 Anforderungen an ein Sicherheitsmanagement

Das Sicherheitsmanagement muss selbst gegen Angriffe resistent sein, weil sonst Angreifer über das Sicherheitsmanagement die Sicherheitsfunktionen der VPN-Gateways und VPN-Clients ausschalten können. Dazu sollte das Sicherheitsmanagement selbst Sicherheitsmechanismen wie Identifikation und Authentikation,

Rollen-Verteilung, Protokollierung mit Audit-Möglichkeiten sowie Verschlüsselung der sicherheitsrelevanten Informationen im Sicherheitsmanagement bieten.

Ein Sicherheitsmanagement für VPN-Systeme soll mindestens die Voraussetzungen »Benutzerfreundlichkeit« und »Widerspruchsfreiheit von Regeln« erfüllen.

- Benutzerfreundlichkeit: Die Menüführung des Sicherheitsmanagements soll einfach und zuverlässig sein. Außerdem sollen keine redundanten Eingaben notwendig sein.
- Widerspruchsfreiheit der Regeln: Fehleingaben in den Eingabefeldern (zum Beispiel für IP-Adressen) sollten nicht möglich sein. Hier sollte eine syntaktische Überprüfung stattfinden.
- Filterregeln sollten nur für die entsprechende Protokollschicht einstellbar sein. Benutzer sollten beispielsweise nicht gleichzeitig als »aktiv« und als »gesperrt« für einen Dienst eingetragen werden können. Mehrfach-Einträge sollen eliminiert werden. Ferner sollte eine semantische Überprüfung der Filterregeln erfolgen.

Damit eine hohe Gesamtsicherheit des gesamten VPN-Systems gewährleistet werden kann, müssen zusätzlich die Sicherheitsfunktionen Zugangskontrolle, Rechteverwaltung, Verschlüsselung und Protokollierung zur Verfügung gestellt werden.

- Zugangskontrolle im Sicherheitsmanagement: Hier soll eine Identifikation und Authentikation der Benutzer durchgeführt werden, damit Unberechtigte das Sicherheitsmanagement nicht nutzen können.
- Rechteverwaltung (Rollen) im Sicherheitsmanagement: Um einen sicheren Betrieb des Sicherheitsmanagement zu gewährleisten, sollten möglichst die folgenden Rollen im Sicherheitsmanagement angeboten werden: Security Administrator, Operator, Editor, Observer und Auditor.
  - Der Security Administrator ist beispielsweise für die Personalisierung des Sicherheitsmanagements, die Vergabe der Zugriffsrechte für das Sicherheitsmanagementnd für das Erstellen und Wiedereinspielen von Backups verantwortlich.
  - Der Operator hat die Aufgabe, die Nutzungsrechte gemäß der Sicherheitspolitik seiner Organisation einzugeben.
  - Ein Editor ist für die Datenerfassung von nicht sicherheitskritischen Daten wie Benutzernamen, Rechnersystemen, Profilen etc. verantwortlich. Er kann keine Rechte vergeben oder entziehen.
  - Der Observer hat die Aufgabe, den Betrieb des VPN-Systems zu beobachten und gegebenenfalls Probleme zu analysieren. Er kann keine Rechte vergeben oder entziehen.
  - Der Auditor übernimmt die Aufgabe, die Logbuchdaten des Sicherheitsmanagement auf sicherheitskritische Aktionen zu überprüfen. Er kann keine Rechte vergeben oder entziehen.

Für besonders sicherheitskritische Aktionen im Sicherheitsmanagement kann ein Mehr-Augen-Prinzip verlangt werden, bei dem zwei oder mehr Personen nur gemeinsam, beispielsweise durch die Eingabe ihres Passworts, eine Aktion auslösen dürfen.

Die sicherheitsrelevanten Informationen, zum Beispiel Passworte oder Schlüssel für die Authentikation, sollten im Sicherheitsmanagement in verschlüsselter Form abgespeichert werden, damit kein Missbrauch dieser Informationen stattfinden kann.

Die verschiedenen Funktionen im Sicherheitsmanagement sollten in separaten Logbüchern protokolliert werden. Zu diesem Zweck sollte das Sicherheitsmanagement beispielsweise folgende Logbücher zur Verfügung stellen:

- Funktions-Logbuch: Hierin werden alle Aktionen festgehalten, die mit Hilfe des Sicherheitsmanagement durchgeführt werden, zum Beispiel die Vergabe der Rechte für die Benutzer, das Löschen von Logbüchern usw. In diesem Logbuch können die Handlungen der Benutzer des Sicherheitsmanagements (Security Administrator, Operator usw.) festgehalten werden.
- Login-Logbuch: Dort werden alle Logins in das Sicherheitsmanagement festgehalten.
- Fehler-Logbuch: Darin werden alle Fehler festgehalten, die im Sicherheitsmanagement erkannt werden.
- Backup-Logbuch: Es werden alle Backup-Aktionen festgehalten, die der Security Administrator im Sicherheitsmanagement durchführt.

Weitere Anforderungen

- Kopplung an ein Netzwerkmanagement-System (NMS):
  Die besonders hohe Verfügbarkeit von VPN-Systemen macht es in der Regel erforderlich, bestimmte »Spontane Meldungen« der VPN-Gateways oder VPN-Clients, die Auskunft über die Verfügbarkeit des Systems geben, an das Netzwerkmanagement zu senden, weil dieses in größeren Organisationen häufig eine 24-Stunden-Besetzung hat und bei Ausfällen schnell reagieren kann. Dazu sollte das Sicherheitsmanagement in der Lage sein, SNMP-Traps und einfache Get-Befehle mit Hilfe eines SNMP Proxy mit dem Netzwerkmanagement auszutauschen.

- Kommunikationsschutz für das Sicherheitsmanagement:
  In vielen Systemanordnungen ist es sinnvoll, das Sicherheitsmanagement mit Hilfe eines Firewall-Systems abzuschotten. Dies kann dann der Fall sein, wenn in den unterschiedlichen Organisationseinheiten lokale Security Manager tätig sind, die auf ein zentrales Sicherheitsmanagement zugreifen

5.3.2 Systeme zum Sicherheitsmanagement

Das Sicherheitsmanagement größerer VPNs wird in der Regel mit Hilfe von zentralen Software-Systemen durchgeführt. Kommerzielle Management-Systeme sind proprietäre Produkte einzelner Hersteller, der mit ihnen gebotene Komfort liefert starke Argumente für den Kauf eines bestimmten Systems.

Ein Management-System besteht im Allgemeinen aus drei Komponenten (Abb. 5.16):

- Der Management-Server ist ein dezidierter Rechner, dessen Kernstück eine Datenbank mit der gesamten Konfiguration des VPN ist. Er dient als zentrales Logging-System und bedient die externen Schnittstellen zu anderen Systemen, wie etwa einem Netzwerkmanagement-System.
- Die eigentliche Administration findet über ein grafisches Benutzer-Interface statt, das auf dem Management-Server oder den Arbeitsplatz-Rechnern der verschiedenen Administratoren laufen kann. Dieses Interface wird meist als Graphical User Interface (GUI) bezeichnet (Abb. 5.17)
- Die unterste Ebene in der Hierarchie wird durch die VPN-Gateways beziehungsweise VPN-Clients gebildet, die ihre Konfigurations-Daten vom Management-Server erhalten.

Die Kommunikation zwischen den einzelnen Komponenten verlangt ein Höchstmaß an Sicherheit, so dass starke Verfahren zu Authentikation und Verschlüsselung zum Einsatz kommen. Bei VPN-Clients, die in der Regel offline sind (zum Beispiel Desktops, Notebooks), ist eine automatische Konfiguration über den Management-Sever nicht möglich. Änderungen der Konfiguration müssen manuell übertragen beziehungsweise eine automatische Re-Konfiguration manuell gestartet werden.

Firewall-Systeme mit intergriertem VPN bieten ein gemeinsames Sicherheitsmanagement beider Komponenten. Die VPN-Strecke erscheint dann sehr übersichtlich als »Filterregel« in der Firewall-Konfiguration.

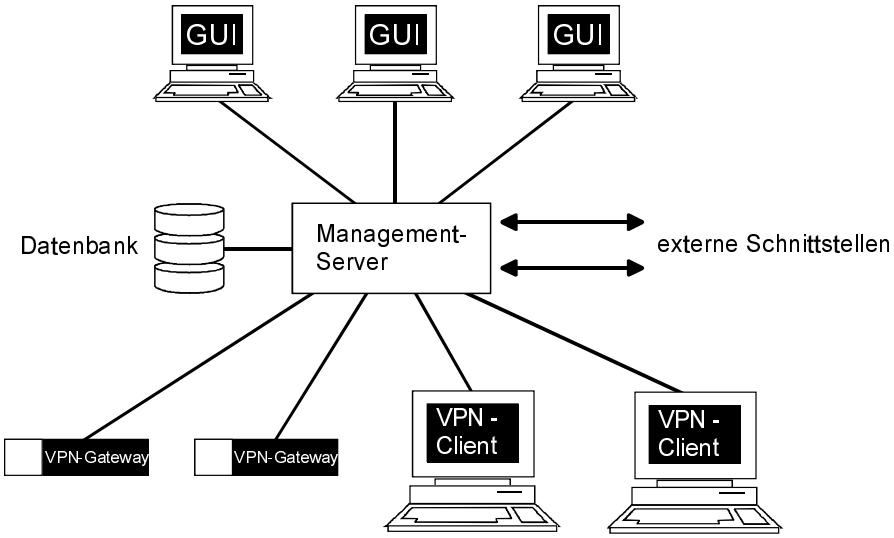

Abb. 5.16: Sicherheitsmanagement

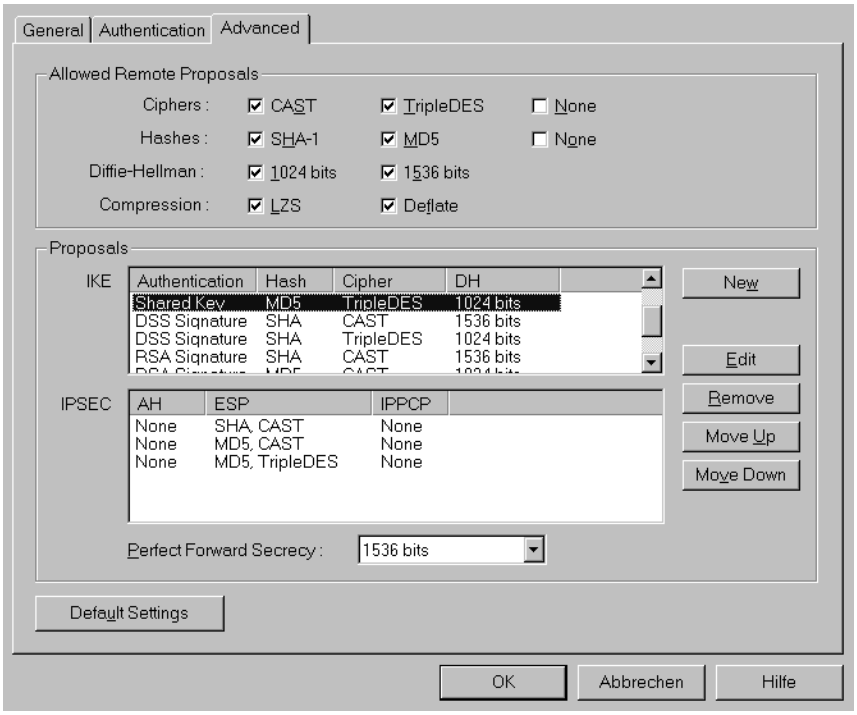

Abb. 5.17: Konfiguration eines VPN

5.3.3 Zertifizierungs-Systeme

Ein zentrales Element von VPN-Systemen ist die gegenseitige Authentikation. Damit belegt jeder Teilnehmer, dass er tatsächlich der angegebene Kommunikationspartner ist. Nur bei kleinen VPNs ist es möglich, die mit der Authentikation verbundenen Aufgaben manuell zu lösen. Eine automatische Authentikation bedarf einer Infrastruktur, die in der Praxis durch die in Kapitel 4 beschriebenen Zertifizierungs-Systeme geschaffen wird. Da Zertifikate neben dem Nachweis der Authentizität durch eine digitale Signatur auch kryptographische Verfahren und die dazu benötigten Schlüssel enthalten, sind die zu ihrer Verwaltung implementierten Systeme hochkomplexe und von der Administration her oft gewöhnungsbedürftige Produkte.

Ein Zertifizierungs-System enthält folgende Komponenten:

- Mit einem PKI-Editor (Public Key Infrastructure) wird die in Kapitel 4 angesprochene hierarchische Struktur aus Certification Authorities (CA) und Registration Authorities (RA) definiert.
- Mit dem Policy-Editor wird für einen Typ von Zertifikaten verbindlich festgelegt, wie der Nachweis der Identität erfolgt, welche kryptographischen Algorithmen benutzt werden und wie die Gültigkeit des Zertifikates geregelt werden soll.
- Grafische Frontends (GUIs) stellen die Schnittstelle für die Personen dar, die innerhalb der CAs und RAs mit der Erstellung und Administration der Zertifikate betraut sind.

In komplexen Zertifizierungs-Systemen findet eine Arbeitsteilung zwischen den Institutionen CA, RA sowie den dort arbeitenden Personengruppen CA-Operatoren (CAO) und RA-Operatoren (RAO) statt. Die Beziehungen zwischen diesen sind wie folgt definiert (Beispiel Abb. 5.18):

- Die Aufgabe einer Certification Authority CA ist die Bearbeitung von Anfragen der RA nach Zertifikaten, die innerhalb der CA erstellt, in einer Datenbank abgespeichert und schließlich ausgeliefert werden.
- Ein CAO definiert die ihm zugeordneten RA und RAO, definiert die für die verschiedenen Typen von Zertifikaten benötigten Policies, leitet diese an seine RAs weiter und ruft Zertifikate zurück, die vorzeitig aus dem Verkehr gezogen werden müssen.
- Innerhalb der RA werden die (Benutzer-)Anfragen nach Zertifikaten angenommen und an die zugeordnete CA weitergeleitet.
- Ein RAO setzt die vom CAO definierte Policy um, das heißt, er kontrolliert die Authentizität der Personen oder Systeme, die ein Zertifikat erhalten sollen, signiert die Anfrage und sendet sie an seine CA weiter.

PKI-Editor

Der erste Schritt bei der Erstellung einer Zertifizierungs-Infrastruktur ist die Definition der beteiligten Instanzen und ihrer Abhängigkeiten. Dabei wird ein grundsätzlicher Rahmen für die Erstellung von Zertifikaten definiert, der Algorithmen, Verfahren zum Schlüsselaustausch, Regelungen für die Gültigkeitsdauer von Zertifikaten und Mechanismen zum vorzeitigen Zurückziehen von Zertifikaten über Sperrlisten (Certification Revocation List, CRL) enthält.

Da bei der Erstellung der Infrastruktur eine Fülle von Aufgaben zu bewältigen ist, wurden Software-Systeme entwickelt, die Unterstützung leisten können. Abbildung 5.18 zeigt einen PKI-Editor mit grafischer Benutzeroberfläche.

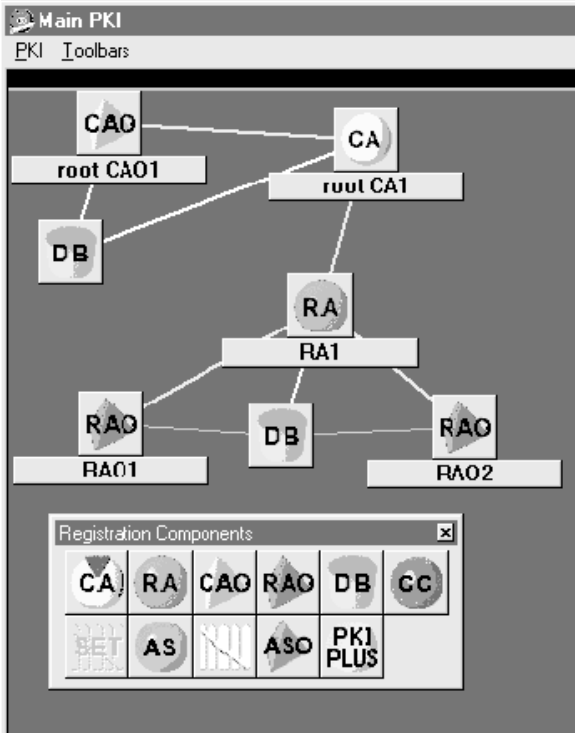

Abb. 5.18: PKI-Editor

Anschließend werden die so definierten CAs, CAOs, RAs und RAOs konfiguriert. Abbildung 5.19 gibt ein Beispiel.

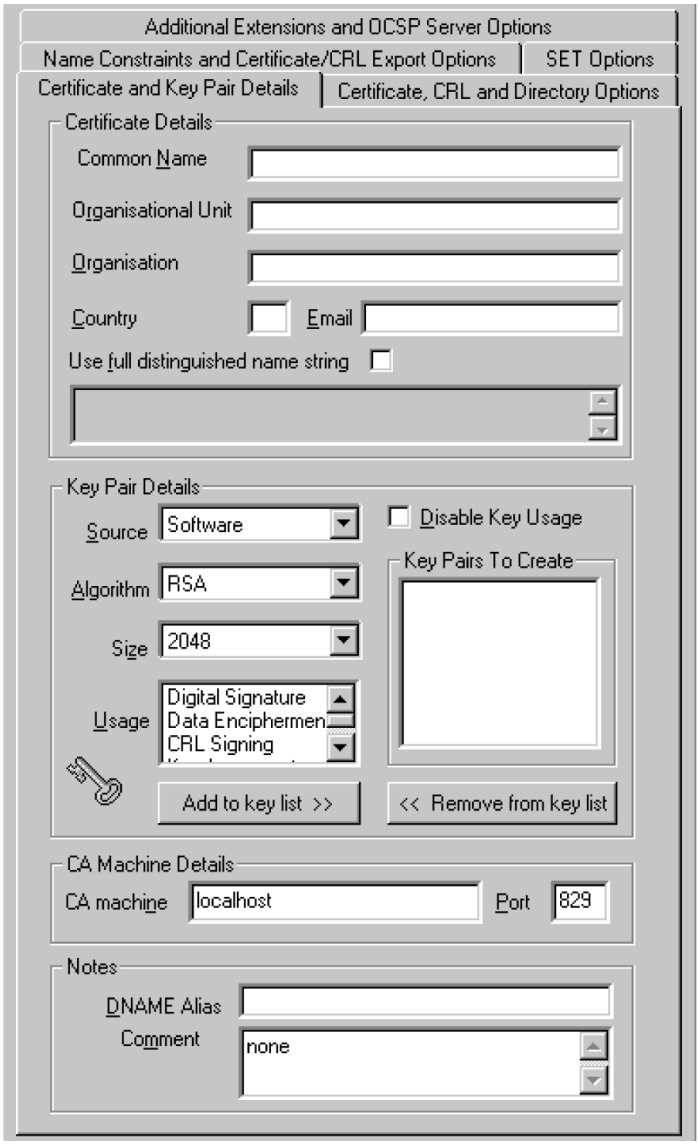

Abb. 5.19: Konfiguration einer CA

Policy-Editor

Mit diesem Tool werden die Mechanismen festgelegt, nach denen der Antrag für ein Zertifikat bearbeitet wird. Abhängig von der Sicherheits-Klasse des Zertifikats sind dabei bestimmte Anforderungen zu erfüllen. Mit der Definition einer Policy werden die bei der Definition der PKI festgelegten Rahmenbedingungen für Verfahren usw. »mit Leben erfüllt«. Auch hier existieren grafische Oberflächen (Abb. 5.20). Der CAO legt hier wie auf einem Formblatt die Randbedingungen für die Ausstellung von Zertifikaten fest.

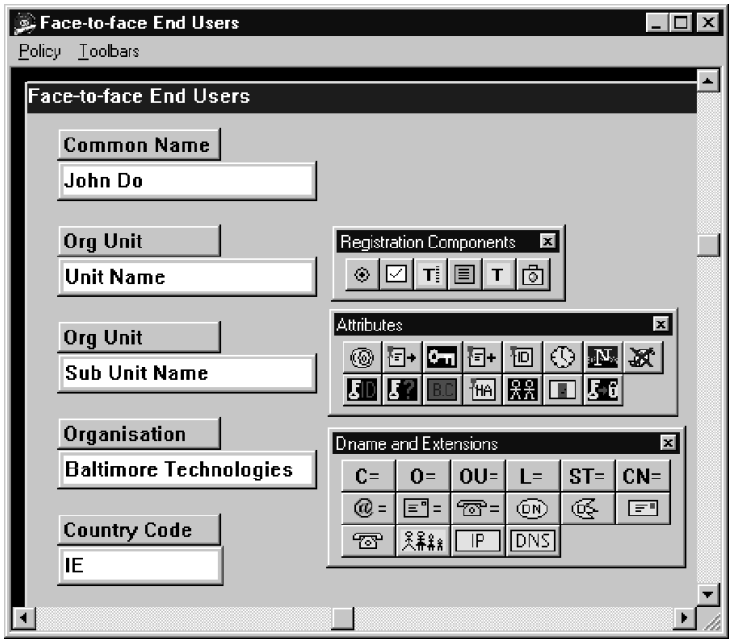

Abb. 5.20: Policy-Editor

5.3.4 Directory-Service

Innerhalb einer VPN-Infrastruktur spielt der schnelle Zugriff auf Sicherheitsinformationen eine entscheidende Rolle. Da die Verhandlungen der an der Kommunikation beteiligten Partner online ablaufen, muss auch der Zugriff auf Zertifikate und Listen mit abgelaufenen Zertifikaten mit einer adäquaten Geschwindigkeit erfolgen. Bei kleinen VPNs können Änderungen manuell auf die einzelnen Komponenten übertragen werden. In den meisten Fällen muss ein Verzeichnis-Dienst (Directory-Service) eingerichtet werden, der die automatische Verteilung von Informationen und den Zugriff darauf regelt.

Ein VPN-Verzeichnis-Dienst ist im Grunde nichts anderes als eine Datenbank, in der Informationen über Zertifikate und die in diesen abgelegten öffentlichen Schlüsseln verwaltet werden. Der Zugriff auf die Datenbank geschieht über die Angabe von Namen, IP-Adressen oder anderen eindeutigen Kriterien. Verzeichnis-Dienste sind meist hierarchisch aufgebaut, so dass die Verbreitung der Informationen (Replikation) innerhalb der Hierarchie transparent und effizient erfolgt. Die Software der VPN-Gateways oder VPN-Clients greift beim Aufbau einer neuen Verbindung auf den Verzeichnis-Dienst zu, falls die gewünschten Informationen nicht lokal verfügbar sind. Moderne VPN-Management-Systeme verfügen über eine Verzeichnis-Schnittstelle nach der LDAP-Spezifikation. Die anfallenden Konfigurations-Arbeiten können dann wahlweise auf dem LDAP-Server oder innerhalb des VPN-Management-Systems durchgeführt werden.

Zur Konfiguration und Administration eines Verzeichnis-Dienstes existieren grafisch orientierte Tools, die den Administratoren die Arbeit erleichtern (Abb. 5.21).

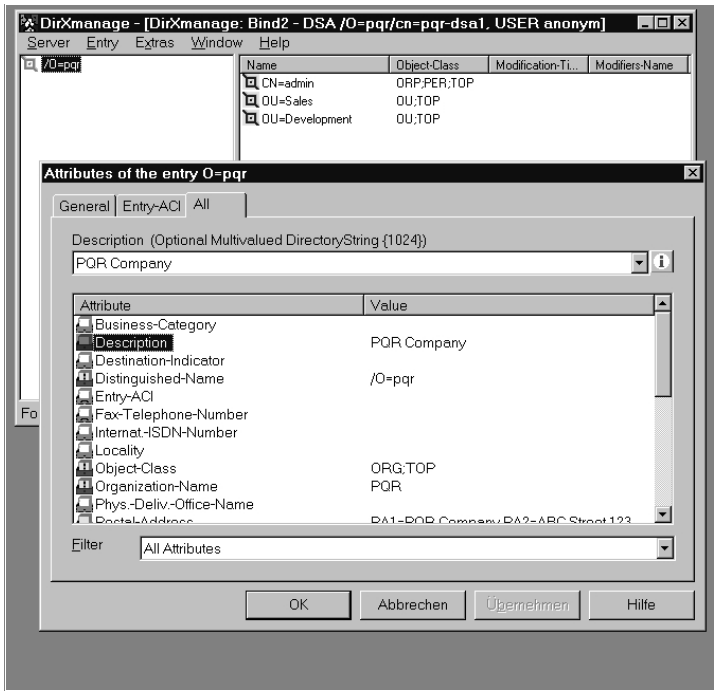

Abb. 5.21: Konfiguration eines Verzeichnis-Dienstes

5.3.5 Schlüssel-Management

VPNs nutzen die hybride Verschlüsselungstechnik: Für die Übertragung der Nutzdaten wird symmetrische Verschlüsselung genutzt, für die Übertragung des symmetrischen Schlüssels hingegen asymmetrische Verschlüsselung. Während die symmetrischen Schlüssel meist von Zufallsgeneratoren erzeugt werden, müssen die für die asymmetrische Verschlüsselung benutzten Paare aus privaten und öffentlichen Schlüsseln vor Beginn der Kommunikation bereit stehen. Dabei muss von der eingesetzten Infrastruktur sowohl die Geheimhaltung des privaten Schlüssels als auch die Authentizität des öffentlichen Schlüssels garantiert werden.

Kommt ein Zertifizierungs-System mit Verzeichnis-Dienst (z. B. LDAP) zum Einsatz, wird das Management der Schlüssel über diesen vorgenommen. Von der CA gelangt der private Schlüssel abgesichert zum Empfänger, oft wird er auch direkt beim Empfänger erzeugt. Die Echtheit des öffentlichen Schlüssels wird über ein Zertifikat oder eine Kette von Zertifikaten nachgewiesen. Sollen Schlüsselpaare zurückgezogen werden, wird das dazugehörige Zertifikat in die Certification Revocation List (CRL) eingetragen. Die Veröffentlichung neuer Schlüssel beziehungsweise Zertifikate geschieht über einen Verzeichnis-Dienst, ebenso wie die Bekanntgabe ungültiger Schlüssel.

Der Einsatz eines kompletten Zertifizierungs-Systems ist allerdings keine notwendige Bedingung zum Betrieb eines VPN. Im Extremfall können die öffentlichen Schlüssel manuell auf die an der Kommunikation beteiligten Systeme gebracht werden. Bei größeren VPNs scheidet diese Variante allerdings wegen des hohen administrativen Aufwands aus. Als Mittelweg zwischen manuellem Schlüsselaustausch und Zertifizierungs-System kann der Einsatz eines Key-Servers angesehen werden, auf den die öffentlichen Schlüssel nach ihrer Erstellung kopiert werden. Von diesem Rechner beziehen dann alle am VPN beteiligten Knoten die benötigten öffentlichen Schlüssel, der Einsatz eines komplexen Verzeichnis-Dienstes erübrigt sich.

Sind an der Bildung eines VPNs nur wenige Knoten beteiligt (z. B. 1:1-Topologie mit drei Standorten), ist der manuelle Schlüsselaustausch die geeignete Methode. Sind aber remote Benutzer (1:n-Topologie) zu versorgen oder ist in der nächsten Zeit mit einem Wachstum der am VPN beteiligten Rechner zu erwarten, sollte konsequent auf einen LDAP Verzeichnis-Dienst gesetzt werden. Für große VPNs stellt sich die Frage nach dem Verzeichnis-Dienst nicht, dieser wird außer für das VPN auch für die Administration von Firewalls oder Authentikations-Systemen benötigt.