Kapitel 7

Praktischer Einsatz von Virtual Private Networks

Dieses Kapitel behandelt den praktischen Einsatz von VPN-Systemen. Neben Umsetzungsbeispielen von VPNs für verschiedene Anwendungsfälle wird exemplarisch die Konfiguration zweier gängiger VPN-Lösungen beschrieben.

7.1 Fallstudien

In diesem Abschnitt wird anhand von Praxisbeispielen vorgestellt, wie verschiedene Organisationen mit sehr unterschiedlichen Anforderungen Virtual Private Networks aufgebaut haben, um eine vertrauenswürdige Kommunikation zu gewährleisten.

7.1.1 Sichere Ankopplung von Außendienstmitarbeitern eines Versicherungsunternehmens

Anforderungen

Die Außendienstmitarbeiter greifen auf einen zentralen Server der Versicherung zu, um an aktuelle Informationen zu gelangen. Dies erspart Zeit und ermöglicht den Versicherungsmaklern vor Ort, immer auf aktuelle Daten und Berechnungen zugreifen zu können. Da diese Daten, beispielsweise für Lebensversicherungen (Angaben über Krankheiten des Kunden usw.), sehr sensibel sind, muss die Kommunikation vertrauenswürdig realisiert werden, damit die Versicherung keinen Image-Schaden durch Angriffe erleidet.

Lösung

Zentral wurde ein redundantes, hochverfügbares VPN-Gateway aufgebaut, das über einen X.500-Directory-Service die Zertifikate und Zertifikats-Revokationslisten (CRLs) der einzelnen Außendienstmitarbeiter abrufen kann. Außerdem steht zentral eine PKI für Schlüssel und Zertifikatsmanagement zur Verfügung.

Die einzelnen Außendienstmitarbeiter haben auf ihrem Rechnersystem (Notebook oder Desktop) einen VPN-Client installiert.

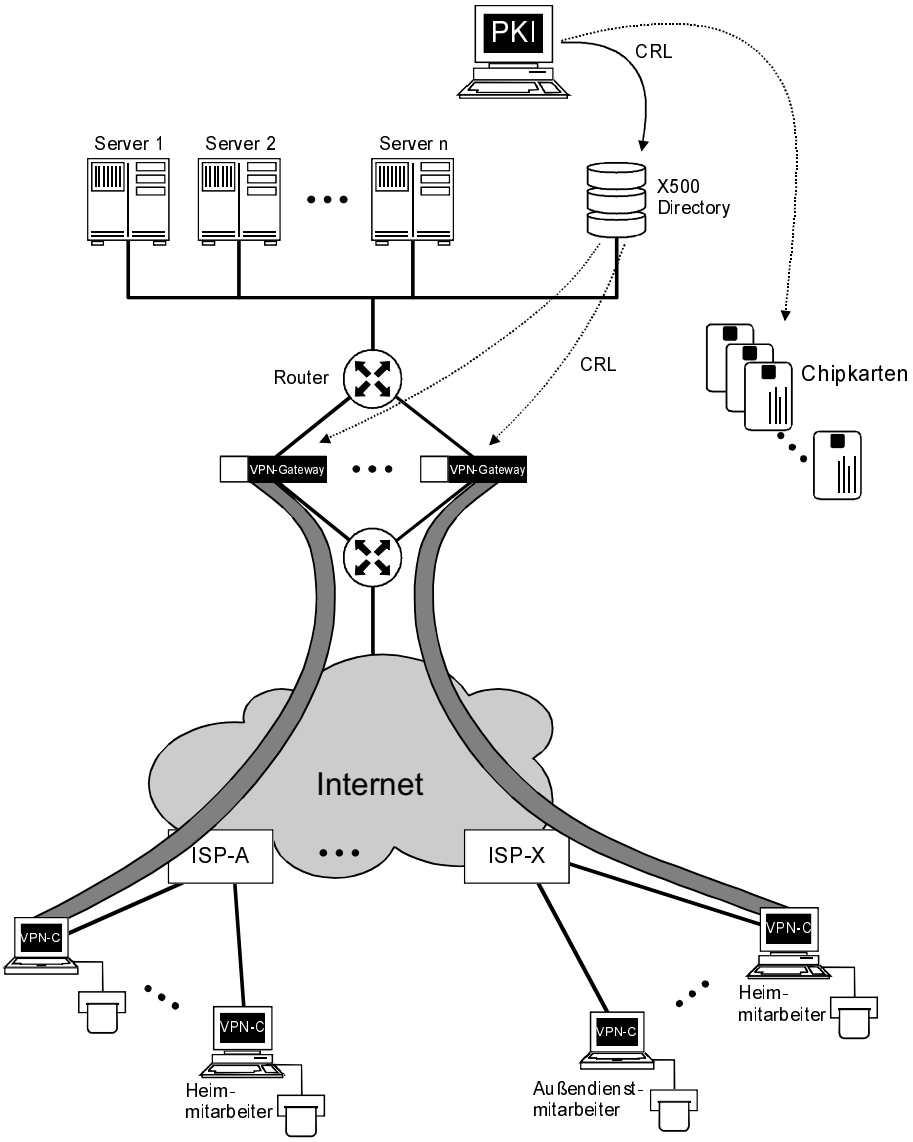

Abb. 7.1: VPN-Anwendung im Außendienst einer Versicherung

Das Hochverfügbarkeitskonzept sorgt dafür, dass beliebig viele VPN-Gateways parallel betrieben werden können, womit eine Performancesteigerung erreicht werden kann. Fallen einzelne VPN-Gateways aus, oder müssen zu Wartungszwecken abgeschaltet werden, werden ihre Verbindungen sofort an andere VPN-Gateways weitergegeben.

Ablauf

In der PKI – Certification Authority (CA) und Registration Authority (RA) – werden für die Außendienstmitarbeiter und für die VPN-Gateways Identitäten vergeben, Pubic-Key-Schlüsselpaare und passende Zertifikate generiert. Der geheime Schlüssel des Public-Key-Schlüsselpaares und das eigene Zertifikat wird auf den persönlichen Sicherheits-Token (Disketten oder Chipkarten) der Mitarbeiter gespeichert.

Das CA-Zertifikat steht entweder ebenfalls auf dem Sicherheits-Token oder befindet sich in einer Zertifizierungsdatenbank auf dem Client (zum Beispiel im Fall von PKCS#12).

In der PKI werden die aktuellen und ungültigen Zertifikate verwaltet. Mit Hilfe einer CRL werden die ungültigen Zertifikate dem X500-Directory-Service zur Verfügung gestellt.

Um den geheimen Schlüssel auf dem persönlichen Sicherheits-Token nutzen zu können, ist eine Personal Identification Number (PIN) notwendig. Die erste PIN wird dem Außendienstmitarbeiter per PIN-Brief auf eine sichere Art und Weise mitgeteilt. Das persönliche Sicherheits-Token sowie der PIN-Brief werden den Außendienstmitarbeiter separat übermittelt.

Auch in den VPN-Gateways wird der geheime Schlüssel eingeführt. Die VPN-Gateways können die Zertifikate von X.500-Directory Service abrufen. Die VPN Gateways haben, wie die Clients, ebenfalls Sicherheits-Token mit den entsprechenden Informationen.

Wenn alle Komponenten (VPN-Gateways und VPN-Clients mit Sicherheits-Token) personalisiert sind, kann die vertrauenswürdige Kommunikation über das VPN-System beginnen. Die Authentikation der Außendienstmitarbeiter wird zertifikatsbasiert durchgeführt, wobei das entsprechende Sicherheits-Token (Diskette oder Chipkarte) verwendet wird.

Falls ein Außendienstmitarbeiter nicht mehr über das VPN-System auf die Daten und Dienste des Versicherungsunternehmens zugreifen soll, wird das Zertifikat des entsprechenden Außendienstmitarbeiters in eine Revokationsliste (CRL) in der PKI eingetragen und ist damit gesperrt.

7.1.2 Vertrauenswürdige Kommunikation über ein internationales IP-Netzwerk

Anforderungen

Die Kommunikation zwischen den Botschaften und dem Auswärtigen Amt eines Landes soll in vertrauenswürdiger Art und Weise realisiert werden, weil hier Informationen von höchster Sicherheitsrelevanz ausgetauscht werden.

Ähnliche Anforderungen stellen alle zentral organisierten Unternehmen mit sternförmigen Netzwerken.

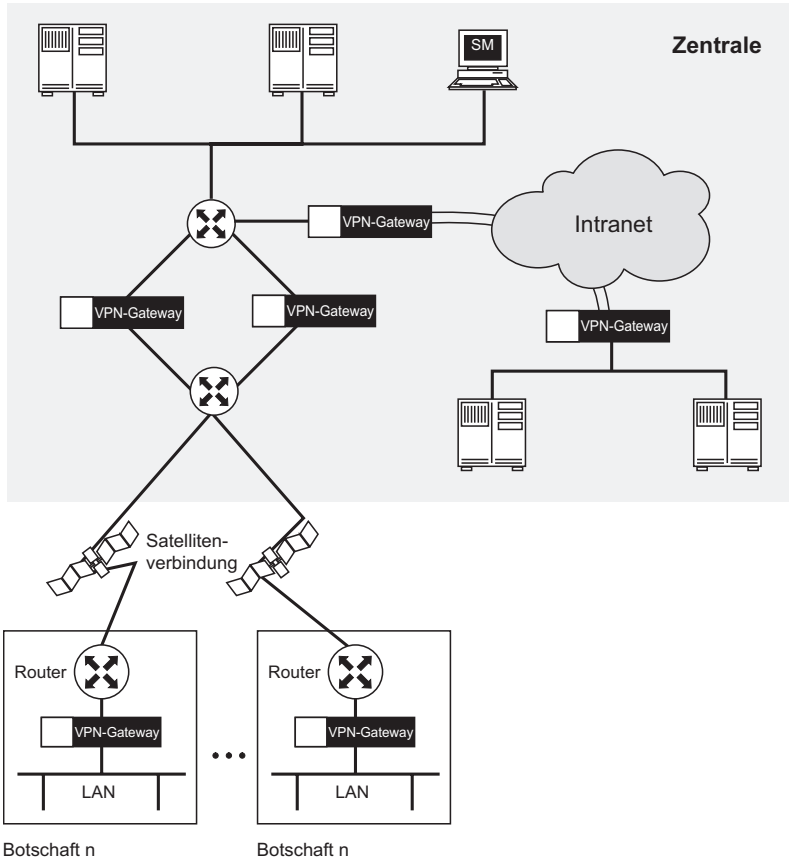

Abb. 7.2: VPN-Anwendung in zentral organisierten Unternehmen oder Behörden

Lösung

In den Botschaften der Länder wird jeweils ein VPN-Gateway vor den Anschluss an das internationale IP-Netzwerk geschaltet. Zentral im Auswärtigen Amt wird ein redundantes, hochverfügbares VPN-Gateway aufgebaut. Die VPN-Gateways sorgen dafür, dass alle Daten vertrauenswürdig über das internationale IP-Netzwerk übertragen werden.

Außerdem wird in der Zentrale ein VPN über das Intranet aufgebaut. Dadurch wird eine vertrauenswürdige Kommunikation zwischen den einzelnen Abteilungen des Auswärtigen Amts sowie zwischen den Abteilungen und den Botschaften gewährleistet.

Die Einrichtung separater VPNs im Intranet und im Extranet dient dazu, dass sowohl die Kommunikation der Abteilungen untereinander und mit den Botschaften als auch der Zugriff der Botschaften auf die Server des Auswärtigen Amts geschützt abläuft.

Ablauf

Die Architektur erlaubt die vertrauenswürdige Kommunikation zwischen der Zentrale und den Botschaften via Satellit. Auch die Kommunikation der Botschaften untereinander wird via Satellit über die Zentrale und somit über eine vertrauenswürdige Verbindung gelenkt.

Die Kommunikation im Intranet, also zwischen den Abteilungen, wird in diesem Modell ebenfalls vor unbefugten Zugriffen geschützt.

Die Verwaltung erfolgt über das Sicherheitsmanagement (SM) in der Zentrale der Organisation.

7.1.3 Angebot eines vertrauenswürdigen IP-Netzes durch einen Service Provider

Anforderung:

Ein Service Provider möchte nicht nur Kommunikationsmöglichkeiten über das IP-Netz, sondern auch die Möglichkeit *vertrauenswürdiger* Kommunikation anbieten. Dadurch brauchen seine Kunden nicht selbst in entsprechende Sicherheitsmaßnahmen zu investieren.

Lösung:

Der Service Provider rüstet die Unternehmen, die an ein vertrauenswürdiges IP-Netz angekoppelt werden wollen, nicht nur mit Routern, sondern zudem mit VPN-Gateways aus. Diese werden von einem zentralen Management-System beim Service Provider aus verwaltet. Für den Kunden ist diese Lösung völlig transparent; vertraglich ist geregelt, dass die Kommunikation vertrauenswürdig durchgeführt wird und der Service Provider die Verantwortung dafür trägt.

Ablauf:

Der Service Provider installiert die VPN-Gateways bei der Bereitstellung des Anschlusses und verwaltet sie zentral mit Hilfe eines Sicherheitsmanagements.

Er kann seinen Kunden nun vertrauenswürdige Netzwerkverbindungen zwischen deren Unternehmenseinheiten, aber auch zu den anderen am vertrauenswürdigen Netz beteiligten Unternehmen bereitstellen. Nach der Einstellung entsprechender Regeln kann damit eine vertrauenswürdige Kommunikation realisiert werden, die der Service Provider zu einem Mehrpreis anbietet.

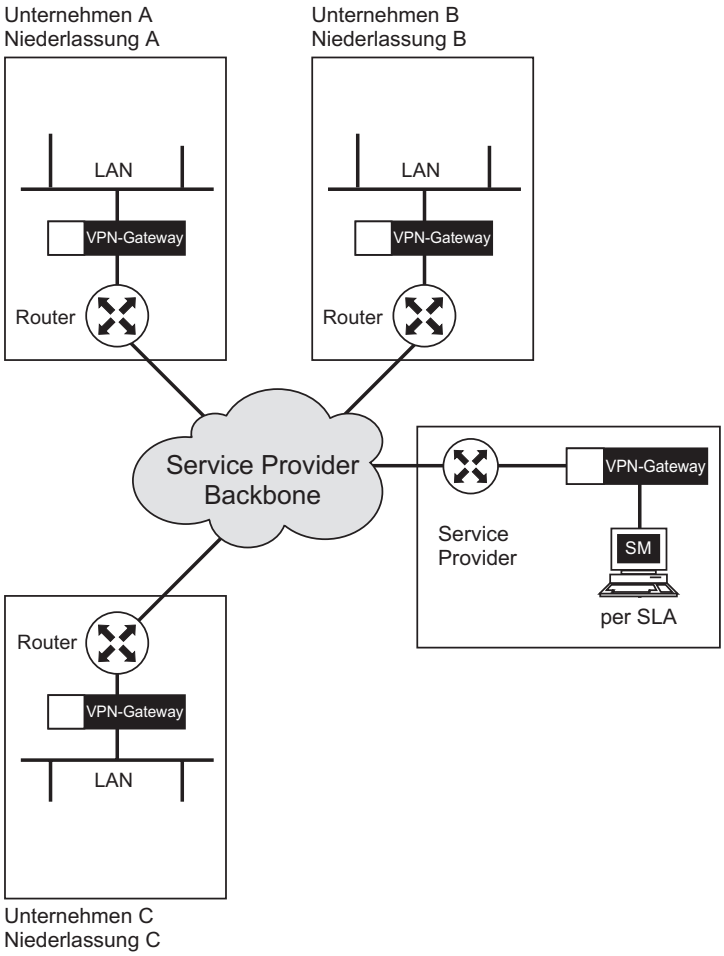

Abb. 7.3: VPN als Angebot eines Service Providers

Betrachtet man diese Lösung im Licht der aktuellen Diskussion um externe IT-Dienstleister, sogenannte Application Service Provider, die auch als Security Service Provider denkbar sind, kann man folgende Ergebnisse festhalten:

- Ein Modell, in dem unterschiedliche Organisationen den gleichen Sicherheits-Dienstleister nutzen, hat den Vorteil, dass durch die Verwendung eines öffentlichen Netzwerks und das Outsourcing der Netzwerkverwaltung und Sicherheitsverwaltung die Kosten deutlich reduziert werden.
- Die Qualität der Sicherheit hängt in diesem Fall von der Qualität und Vertrauenswürdigkeit des Service Providers ab.
- Inwieweit ein Service Provider im Schadensfall zur Rechenschaft gezogen werden kann, sollte vertraglich festgelegt werden.

7.1.4 Vertrauenswürdige Vernetzung von Polizeidienststellen

Anforderung:

Eine Polizeibehörde möchte über das Landesverwaltungsnetz 300 Polizeistationen miteinander vernetzen und hierbei eine vertrauenswürdige Kommunikation gewährleisten. Außerdem soll ein sicherer Zugang zum Internet oder zu anderen zentralen Diensten bereitgestellt werden.

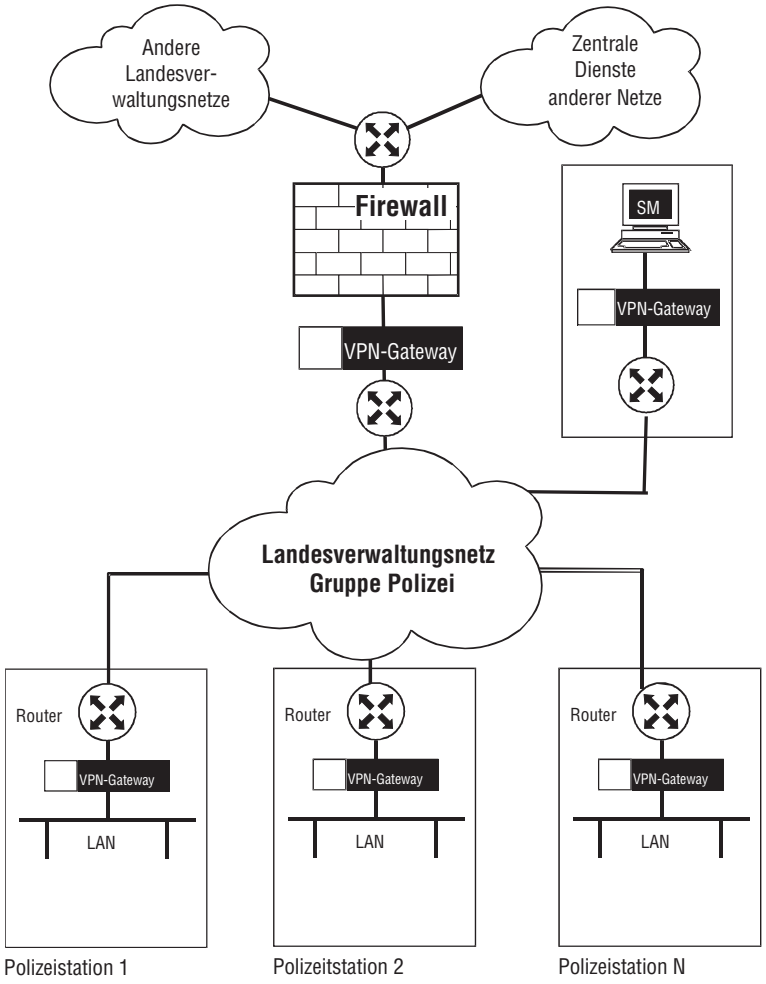

Abb. 7.4: VPN und Firewall-System in einem Landesverwaltungsnetz

Lösung:

Alle Polizeistationen werden mit einem VPN-Gateway ausgerüstet. Das Sicherheitsmanagement wird von einer zentralen Stelle aus durchgeführt. Der Zugang zu den anderen Netzen wird mit einem Firewall-System geschützt, das hinter den VPN-Gateways implementiert wird. Dadurch können die Benutzer in gesicherter Form auf andere Verwaltungsnetze und Netzdienste zugreifen.

Ablauf:

Die Polizeidienststellen sind somit in der Lage, miteinander vertrauenswürdig zu kommunizieren und den geforderten hohen Schutzbedarf zu erfüllen.

Außerdem wird es den Polizeibeamten ermöglicht, mit minimalem Risiko auf Ressourcen in anderen Netzen zuzugreifen. Angriffe aus diesen Netzen werden durch das Firewall-System abgeblockt, so dass Unbefugte keinen Zugriff auf das Netz der Polizei erhalten.

Durch das zentrale Sicherheitsmanagement ist eine einfache Verwaltung der vertrauenswürdigen Kommunikation möglich.

7.2 VPN-Implementierungen

Die praktische Umsetzung von VPN-Konzepten ist keine leichte Sache. Die Vielzahl an Algorithmen, deren unterschiedliche Implementierungen und die nur unzureichende Standardisierung machen die Konfiguration von VPNs oft zu einer mühsamen Angelegenheit. Besonders anspruchsvoll ist die Einrichtung einer VPN-Verbindung, deren Endpunkte von unterschiedlichen Herstellern stammen.

Um ein VPN ohne große »Reibungsverluste« einzuführen, empfiehlt sich deshalb die Beachtung einiger Randbedingungen:

- Die existierenden Standards sollten beachtet werden, d.h., man sollte nur IPSec mit IKE-Schlüsselaustausch benutzen. Wenn alle Stricke reißen, kann bei kleineren VPN-Lösungen ein Pre-Shared Key verwendet werden.
- Möglichst alle VPN-Gateways sollten von demselben Hersteller stammen und in derselben Soft- und Hardwareversion betrieben werden.
- Wenn Schwierigkeiten beim Zusammenspiel der VPN-Gateways auftreten, kann als letzte Möglichkeit eine manuelle IPSec-Konfiguration versucht werden. Dabei müssen alle Details wie eingesetzte Algorithmen oder die Security Association fest definiert werden.

Besonders der zweite Punkt ist in der Praxis kaum einzuhalten. Fusionen von Firmen oder die verschlüsselte Übertragung von Geschäftsdaten zwischen Kooperationspartnern führen zur Nutzung unterschiedlicher Hard- und Software. Hier muss in den meisten Fällen auf die (leider nicht sehr komfortable) Minimallösung »IPSec mit Pre-Shared Key« zurückgegriffen werden.

Nachfolgend werden zwei praktische Beispiele für die Einrichtung von VPNs gegeben. Zuerst wird ein VPN-Gateway auf Linux-Basis vorgestellt, als zweite Lösung kommt eine Firewall vom Typ »Checkpoint Firewall-1« in der Version 4.x mit integriertem VPN-Gateway zum Zuge.

7.2.1 FreeSWAN unter Linux

Zum Umfang einer normalen Linux-Distribution gehört das Freeware-Paket »FreeSWAN«, mit dem ein VPN mittels IPSec aufgebaut werden kann. Im Folgenden soll Schritt für Schritt gezeigt werden, wie ein VPN unter der »SuSE«-Distribution eingerichtet wird.

Installation

IPSec benötigt einen Kernel, der das Protokoll unterstützt. Da die neueren Versionen von Linux diese Option per Default aktiviert haben, erübrigt sich die Neukompilation des Kernels mit gesetzten IPSec-Optionen in den meisten Fällen. Mit dem YAST-Installationsprogramm wird zunächst auf allen beteiligten Rechnern die »FreeSWAN«-Software installiert. Anschließend muss (wieder mit dem YAST) die Startvariable START_IPSEC auf den Wert »yes« gesetzt werden. Damit wird das VPN bei jedem Neustart des Rechners ebenfalls gestartet.

Manuell kann IPSec jederzeit mit den folgenden Befehlen hoch- und heruntergefahren werden:

```
ipsec setup --start
ipsec setup --stop
```

Bei gestartetem IPSec ist ein neues Gerät *ipseco* hinzugefügt worden:

```
# ifconfig ipsec0
ipsec0Link encap:Point-to-Point Protocol
inet addr:149.209.1.241  Mask:255.255.255.255
UP RUNNING NOARP  MTU:16260  Metric:1
...
```

Der aktuelle Status von FreeSWAN kann mit dem Kommando

```
ipsec look
```

eingesehen werden.

Konfiguration

Im Verzeichnis */etc* befinden sich zwei Konfigurationsdateien, in denen alle Einstellungen des VPNs angegeben werden:

- Die allgemeine Konfiguration von FreeSWAN wird in der Datei */etc/ipsec.conf* vorgenommen.
- Die Datei */etc/ipsec.secrets* enthält Schlüsselinformationen.

Um unser Beispiel möglichst einfach zu halten, soll ein Pre-Shared Key zum Einsatz kommen.

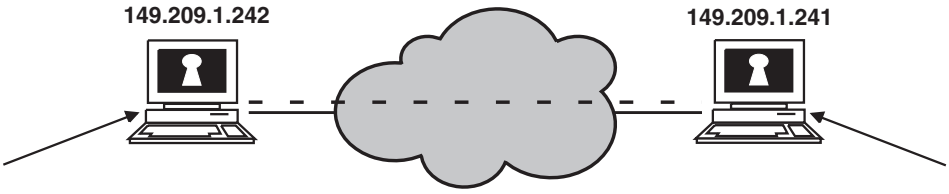

Abb. 7.5: Beispielkonfiguration

Die Konfiguration FreeSWAN geschieht sehr anschaulich über einen »linken« und »rechten« Rechner, wie in Abb. 7.5 angegeben. Bei beiden Rechnern soll die Netzwerkkarte eth0 für das VPN-Gateway genutzt werden.

Die Konfigurationsdateien */etc/ipsec.conf* auf beiden Seiten enthalten in unserem Beispiel die Einträge

```
# basic configuration
config setup
   interfaces="ipsec0=eth0"
   klipsdebug=none
   plutodebug=none
   plutoload="vpn1"
   plutostart="vpn1"
   uniqueids=yes
conn %default
   #authby=rsasig
   #leftrsasigkey=%dns
   #rightrsasigkey=%dns
conn vpn1
   left=149.209.1.242
   leftnexthop=
   right=149.209.1.241
   rightnexthop=
   auto=add
```

Die Schlüsseldatei */etc/ipsec.secrets* enthält auf beiden Seiten einen Pre-Shared Key (PSK).

```
149.209.1.242 149.209.1.241: PSK "1x9presharedkey9a5"
```

Wenn jetzt auf beiden Seiten das VPN gestartet wird (eventuelle Fehlermeldungen in */var/log/messages* beachten!), sollte ein »Ping« zwischen den Rechnern zu den IPSec-Paketen in Abbildung 7.6 führen – hier aufgenommen mit dem Netzwerksniffer »Ethereal«.

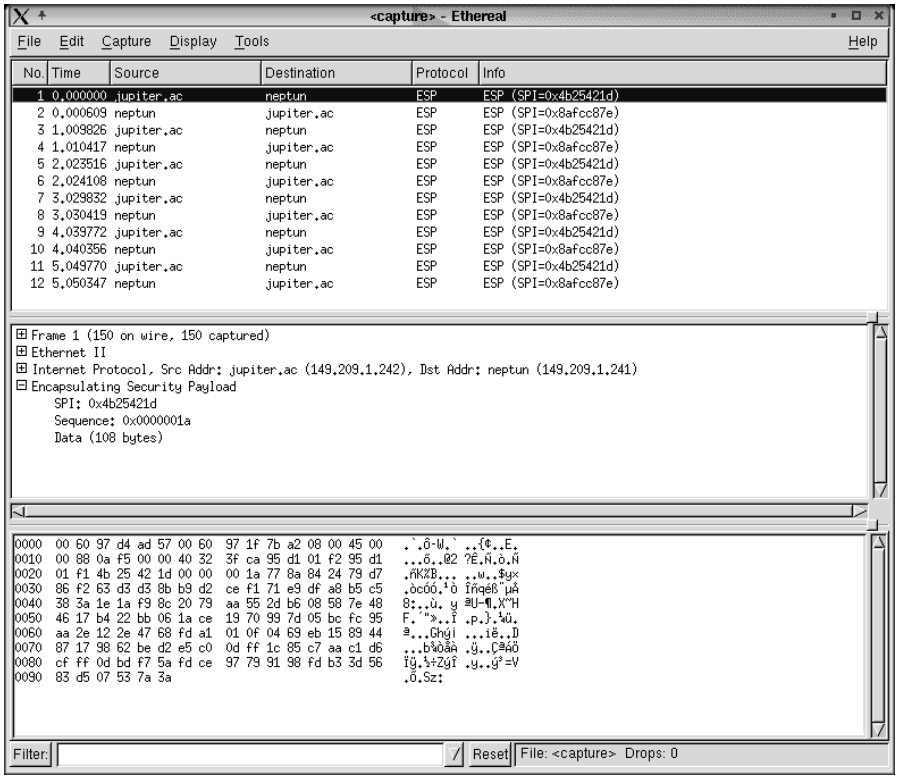

Abb. 7.6: Ping über IPSec

7.2.2 Checkpoint Firewall-1

Im zweiten Beispiel soll ein VPN über zwei NT-Rechner aufgebaut werden. In unserem Beispiel gehen wir von einer Default-Installation von CD aus. Benötigt wird dabei eine »Firewall-1/VPN-1«. Diese Software verfügt über eine ganze Reihe von Verfahren zur Verschlüsselung und zum Schlüsselaustausch, wir beschränken uns wieder auf IPSec mit IKE (siehe auch /LEU01/).

Da das VPN-Gateway in die Firewall integriert ist, muss zunächst die Konfiguration der Firewall durchgeführt werden. Das soll im Folgenden für den »rechten« Rechner in Abbildung 7.5 gezeigt werden, der andere Rechner wird anschließend analog konfiguriert.

Definition der beteiligten Firewalls

Als Erstes wird der eigene Rechner definiert. Wie in Abbildung 7.7 angegeben, muss dieser Rechner als internes Gateway und Management Station definiert werden.

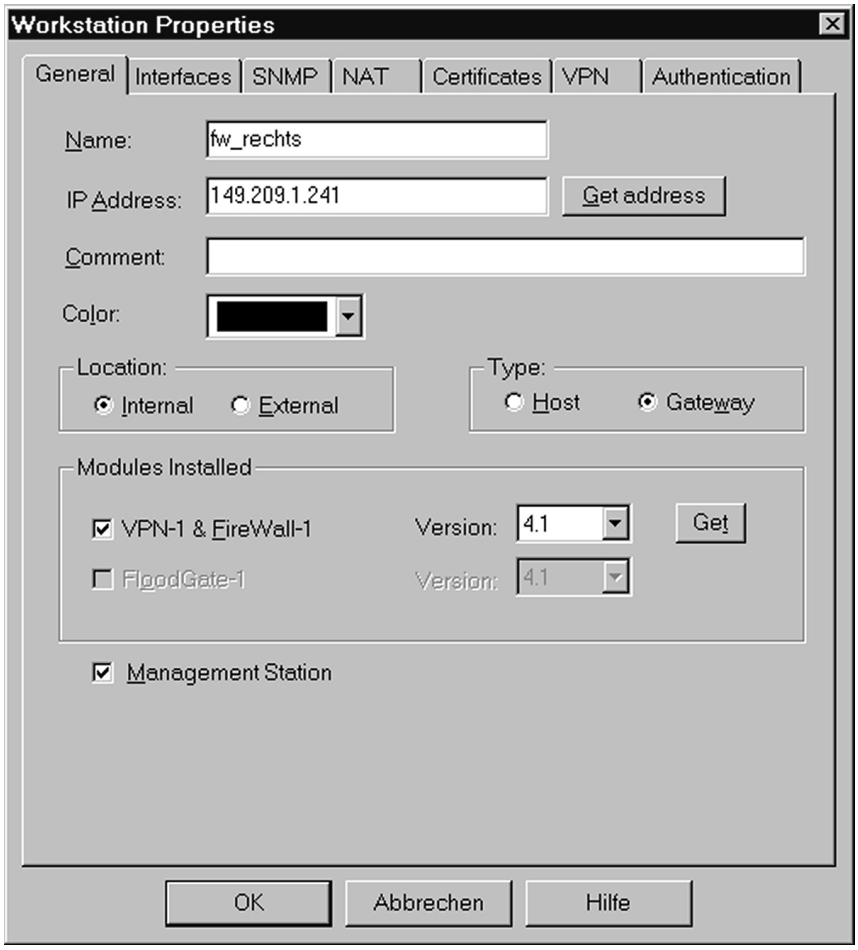

Abb. 7.7: Definition der rechten Firewall

Bei der Konfiguration der Netzwerkkarten (»Interfaces«) ist darauf zu achten, dass Maßnahmen gegen IP-Spoofing getroffen werden (Abb. 7.8). Diese Grundregel gilt natürlich für alle Firewall-Systeme.

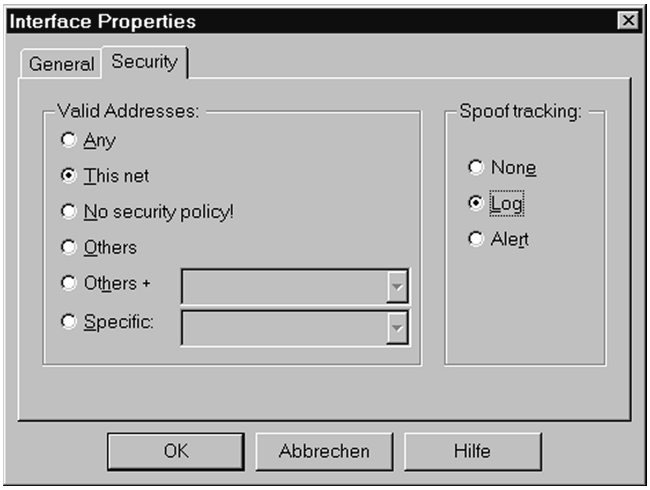

Abb. 7.8: Anti-Spoofing-Optionen

Die zweite Firewall wird als externes Gateway definiert (Abb. 7.9).

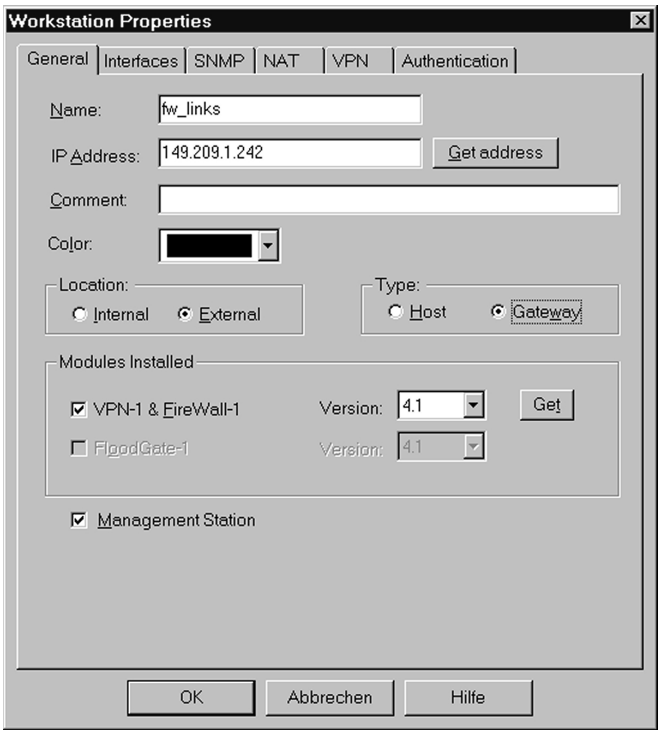

Abb. 7.9: Definition der linken Firewall

Definition der Netzwerke

Anschließend müssen die beteiligten lokalen Netzwerke definiert werden: das eigene Netz als »intern«, das gegenüberliegende Netz als »extern«.

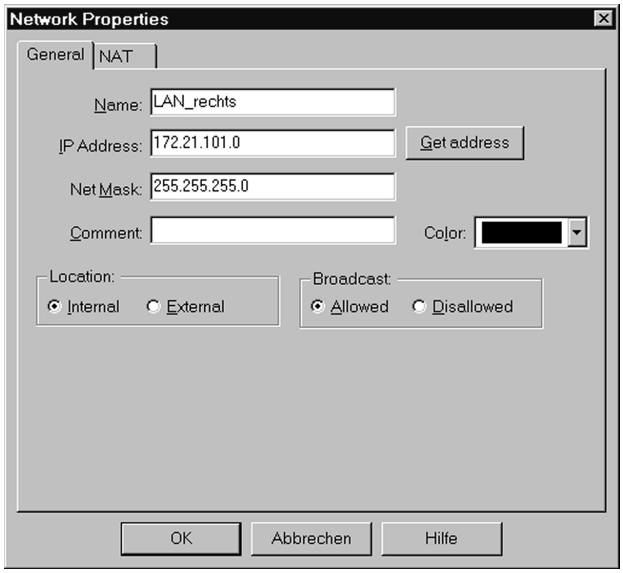

Abb. 7.10: Eigenes Netz

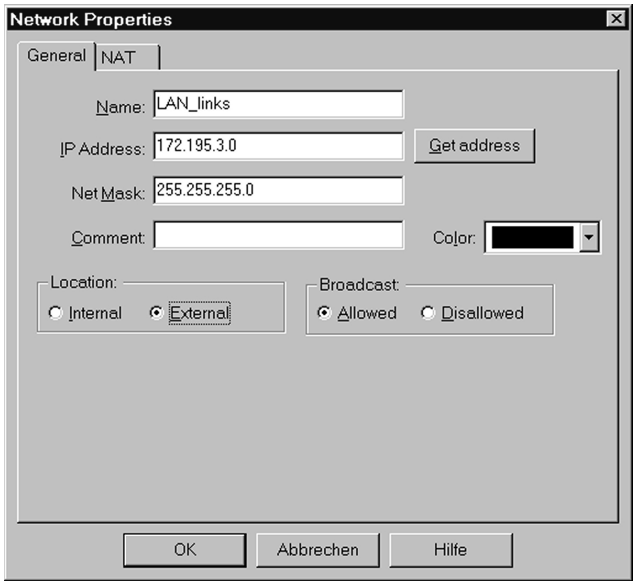

Abb. 7.11: Gegenüberliegendes Netz

Damit ist die Firewall-Konfiguration ohne VPN abgeschlossen. Hier empfiehlt sich ein Test mit der Firewall-Regel »Any Any Accept«. Ist dieser erfolgreich, kann die Konfiguration des VPN-Gateways durchgeführt werden.

Konfiguration von IPSec mit IKE

Nach der Definition der beteiligten Netzwerk-Komponenten kann nun das VPN-Gateway aktiviert werden. Das geschieht über die Konfigurationsmenüs der Firewalls. Dabei werden bei beiden Firewalls die Option IKE und die Verschlüsselungsdomäne des zu der Firewall gehörenden Netzwerks ausgewählt. Bei den Eigenschaften von IKE können dann Algorithmen und die Option »Pre-Shared Secret« (= Pre-Shared Key) ausgewählt werden. Beim Editieren der ersten Firewall kann der Key noch nicht angegeben werden, das ist erst im Menü der zweiten Firewall möglich.

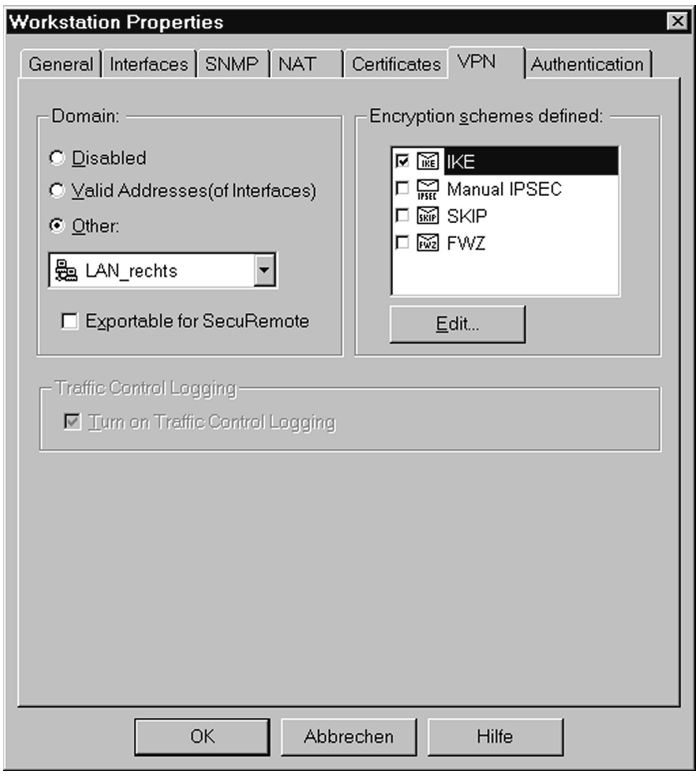

Abb. 7.12: Rechtes VPN-Gateway

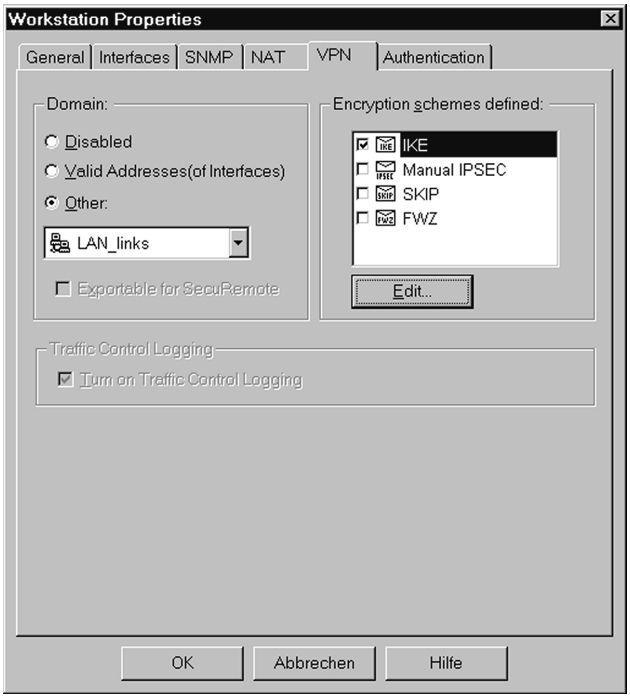

Abb. 7.13: Linkes VPN-Gateway

Abb. 7.14: Eigenschaften von IKE

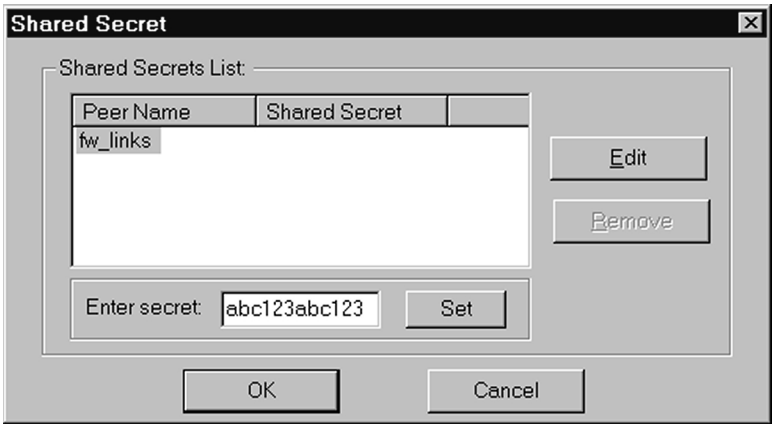

Abb. 7.15: Definition des Pre-Shared Keys

Damit ist die Konfiguration der Firewall-Objekte abgeschlossen.

Filterregeln für das VPN-Gateway

Auch die Definition der Filterregeln für das VPN-Gateway ist ein komplexer Vorgang. Insgesamt sind fünf Regeln zu definieren, die in Abbildung 7.16 angegeben sind:

- Regel 1 erlaubt als Kommunikation zwischen den beiden Firewalls ausschließlich die Dienste IKE, AH und ESP. Damit wird das IPSec-Protokoll zwischen den Endpunkten der VPN-Strecke zugelassen.
- Regel 2 verwirft alle anderen Pakete, die von außen auf das VPN-Gateway treffen.
- Die Regeln drei und vier beschreiben die Kommunikation zwischen den beiden hinter den Gateways liegenden lokalen Netzwerken. Hier muss »Encrypt« angegeben werden, um IPSec auch wirklich zu nutzen.
- Regel fünf ist ein »Any Any Drop«, allerdings im Gegensatz zu der impliziten letzten Regel »Any Any Drop« mit ausführlicher Protokollierung.

Zu guter Letzt müssen noch die Eigenschaften der beiden »Encrypt«-Einträge angepasst werden. Dabei sollte als »Allowed Peer Gateway« die gegenüberliegende Firewall angegeben werden (Abb. 7.17).

Dieselben Arbeiten müssen spiegelbildlich auf der anderen Firewall durchgeführt werden. Anschließend steht der verschlüsselten Kommunikation der beiden Netzwerke nichts mehr im Weg. Eine Beobachtung der Logbuch-Einträge der »Firewall-1« führt bei Fehlern meist schnell auf die richtige Spur.

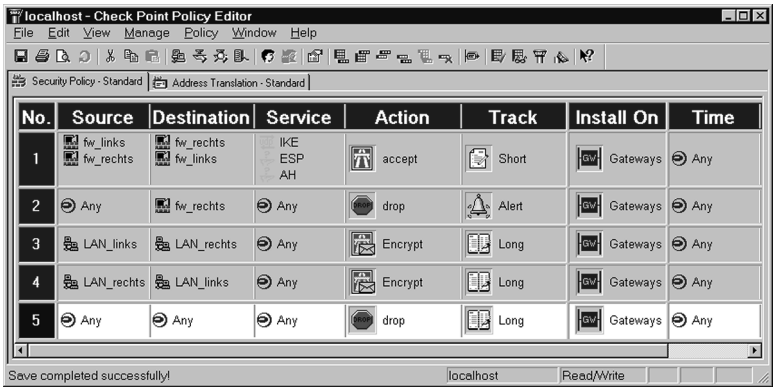

Abb. 7.16: Filterregeln für das rechte VPN-Gateway

Abb. 7.17: Weitere IKE-Eigenschaften