Universität Rostock

Fakultät für Ingenieurswissenschaften

Fachbereich Elektrotechnik und Informationstechnik

Institut für Nachrichtentechnik und Informationselektronik

Diplomarbeit

Sicherheitskonzept der Informations– und Kommunikationsprozesse in strukturierten Unternehmen anhand des ISO/OSI Referenzmodells

cand. Ing. Bernd Podey

18. Mai 2000

Betreuer

Dr.-Ing. H.-D. Melzer (Universität Rostock, NTIE)

Dipl.-Ing. Th. Kessler (Universität Rostock, NTIE)

Dipl.-Ing H. Becher (Universität Rostock, RZ)

Vorwort

Diese Diplomarbeit wurde mit der Unterstützung einer Vielzahl von Personen erstellt.
Besonderer Dank gilt den Betreuern der Diplomarbeit: Herrn Dr.-Ing. H.-D. Melzer (Universität Rostock, NTIE), Herrn Dipl.-Ing. Th. Kessler (Universität Rostock, NTIE) und Herrn Dipl.-Ing H. Becher (Universität Rostock, Rechenzentrum) für die Themenfindung sowie die konstruktive Zusammenarbeit und Betreuung während der Diplomarbeit.
Für nützliche Anregungen und Hinweise danke ich Herrn Dipl.-Math. M. Riedel (Universität Rostock, Rechenzentrum) und Herrn G. Frisch (Universität Rostock, Rechenzentrum).
Abschließend möchte ich mich bei all denjenigen bedanken, die mir das Studium ermöglicht und dieses zu einem unvergesslichen Erlebnis gemacht haben. Besonderer Dank gilt meinen Eltern, meiner Schwester und meinem Neffen.

Rostock im Mai 2000
Bernd Podey

Kurzreferat

Für ein im internationalen Wettbewerb tätiges Unternehmen ist die Frage nach der Sicherheit der Kommunikation von existenzieller Bedeutung. Vielen Unternehmen fehlt ein Überblick über die Sicherheitsrisiken, die in ihren Netzwerken vorhanden sind. Es entsteht ein Misstrauen gegenüber dem Internet, dass in den meisten Fällen unbegründet ist.

In der vorliegenden Arbeit wird am Beispiel der Teilnetze der Universität Rostock ein Sicherheitskonzept erstellt, dessen Grundlage ein erarbeiteter Fragenkatalog ist. Ausgehend von dem Sicherheitskonzept werden Lösungsvorschläge für die Absicherung einzelner Teilnetze unterbreitet.

Weitere Schwerpunkte der Arbeit sind die Dokumentation der derzeitigen sicherheitsrelevanten Standards, die Darstellung der möglichen Firewallarchitekturen und eine Übersicht über Firewall–Produkte.

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Abkürzungsverzeichnis

AAL	ATM Adaption Layer
AH	Authentication Header
ARP	Address Resolution Protocol
ATM	Asynchronous Transfer Mode
BGP	Border Gateway Protocol
BSI	Bundesamt für Sicherheit in der Informationstechnik
CBC	Cypher Block Chaining
DES	Data Encryption Standard
DES–CBC	Data Encryption Standard Cypher Block Chaining Mode
DH–Verfahren	Diffie–Hellmann Verfahren
DMZ	Demilitarisierte Zone
DNS	Domain Name System
DoS	Denial of Sevice
DSS	Digital Signature Standard
DTL	Designated Transit List
EGP	Exterior Gateway Protocol
EIGRP	Enhanced Interior Gateway Routing Protocol
Email	Electronic Mail
ESP	Encapsulation Security Payload
FDDI	Fiber Distributed Data Interface
FSP	File Service Protocol
HMAC	Keyed Hashing for Message Authentication
HTML	Hyper Text Markup Language
HTTP	Hyper Text Transfer Protocol
IC	Initiator Cokie
ICMP	Internet Control Message Protocol
ICV	Integrity Check Value
IGP	Interior Gateway Protocol
IGMP	Internet Group Management Protocol
IKE	Internet Key Exchange

ILMI	Integrated Local Management Interface
IP	Internet Protocol
IPSec	IP–Security
IRC	Internet Relay Chat
ISAKMP	Internet Security Association and Key Management Protocol
ISDN	Integrated Service Digital Network
ISO	International Standardization Organisation
IuK	Information und Kommunikation
KDC	Key Distribution Center
LAN	Local Area Network
LPR	Line Printer Spooler
LWL	Lichtwellenleiter
MD5	Message Digest Algorithm Nr. 5
MIME	Multipurpose Internet Mail Extensions
MTU	Maximum Transfer Unit
NAT	Network Address Translation
NFS	Network File System
NIS	Network Information System
NNTP	Network News Transfer Protocol
NTP	Network Time Protocol
OSI	Open System Interconnection
OSPF	Open Shortest Path First
PFS	Perfect Forward Secrecy
PNNI	Private Network to Network Interface
POP	Post Office Protocol
PVC	Permanent Virtual Circuit
QOS	Quality Of Service
RC	Responder Cookie
rcp	remote–copy
RFC	Request For Comment
rlogin	remote–login
RIP	Routing Information Protocol

RPC	Remote Procedure Call
RSA	Rivest–Shamir–Adleman–Algorithmus
rsh	remote–shell
RUN	Rostocker Universitäts Netz
S–HTTP	Secure Hyper Text Transfer Protocol
SA	Security Association
SAD	Security Association Database
SDH	Synchrone Digitale Hierarchie
SG	Security Gateway
SHA-1	Secure Hash Algorithm Version 1
SKEME	Secure Key Exchange Mechanism for the Internet
SKIP	Simple Key Management Protocol
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SNP	Sub Network Protocol
SONET	Synchronus Optical Network
SPD	Security Policy Database
SPI	Security Parameters Index
SSL	Secure Socket Layer
SVC	Switched Virual Circuit
TCP	Transfer Control Protocol
TFTP	Trivial File Transfer Protocol
TLS	Transport Layer Security
UDP	User Datagram Protocol
ULP	Upper Layer Protocol
UUCP	Unix to Unix Copy Protocol
VPN	Virtual Private Network
WAIS	Wide Area Information Server
WWW	World Wide Web

Glossar

ActiveX	Ausführbarer Code der in Web–Seiten mit übertragen wird
Admin	Administrator oder Systemverwalter
Bastion Host	Workstation mit 2 Netzwerkkarten, auf dem Applikationsfilter installiert werden
B–Win	Breitband Wissenschaftsnetz – Backbone Netzwerk der Universitäten und Forschungseinrichtungen verwaltet vom DFN auf ATM Basis
Gateway	Zentraler Verbindungspunkt („Tor“) zum Internet
G–Win	Gigabit Wissenschaftsnetz – neues Backbonenetz des DFN löst das B–Win ab, Übertragungstechnologie IP over SONET
Header	„Kopf“ eines Datenpakets, enthält Adress– Status– und andere Protokollinformationen
H.323	Standard für Voice–Over–IP, neuer Standard in der Sprach– und Videoübertragung im Internet
JAVA	ausführbahrer Code, der in Web–Seiten übertragen wird und eine Verbesserung der Bedienbarkeit und des Aussehens einer Webseite bewirkt
Proxy	Stellvertreter für einen, über ein Gateway genutzten, Internet–Dienst. Der Client kommuniziert über diesen Proxy mit dem Internet
Router	Gerät zur Wegfindung in einem Netzwerk
X11	X–Windows: Grafische Benutzeroberfläche auf Unix–Betriebssystemen

Kapitel 1

Motivation

Das Internet hat in den letzten Jahren einen Wandel vom reinen Wissenschaftsnetz hin zu einem, von einem breiten Publikum genutzten, öffentlichen Netz vollzogen. Die sich für ein Unternehmen ergebenden Anwendungen sind Präsentation der eigenen Produkte, preiswerte Verbindung von Unternehmensstandorten über VPNs auch über Ländergrenzen hinweg und Verbindung zu Außendienstmitarbeitern. Durch die Internetanbindung ergeben sich für diese Unternehmen neue Sicherheitsrisiken. Die im Internet verwendeten Protokolle wurden ursprünglich für unternehmensinterne Netzwerke entwickelt, wodurch sich Schwachstellen ergeben, die potentielle Angreifer ausnutzen, um an sicherheitsrelevante Daten zu gelangen. Der Schutz der Daten und des Netzes selbst stellt eine herausfordernde Aufgabe dar. Veröffentlichungen zu diesem Thema enden zumeist mit einer Empfehlung zum Einsatz zumindest eines Application–Level Gateways. Dies ist in Hinblick auf den Datendurchsatz und Kostenfaktor problematisch. Gegenstand dieser Arbeit ist die Erarbeitung alternativer Sicherheitskonzepte an ausgewählten Beispielen, mit deren Hilfe die maximal mögliche Sicherheit bei gleichbleibender Erreichbarkeit, Flexibilität, Zukunftssicherheit und Datenrate angestrebt wird.

Kapitel 2

Informations- und Kommunikationsprozesse in strukturierten Unternehmen

Die Aufgliederung der IUK–Prozesse erfolgt durch die Trennung in Prozesse, die

a) auf Sende–und Empfangsseite zur gleichen Zeit durchgeführt werden müssen (isochrone, bzw. sysnchrone Prozesse)

b) auf der Empfangsseite später durchgeführt werden können(asynchrone Prozesse)

Die Informations– und Kommunikationsprozesse gliedern sich nach Abbildung 2.1. Es folgt eine Analyse der IUK–Prozesse einzelner Unternehmen.

2.1 Universität Rostock–Wissenschaftsnetz

Die derzeitige Struktur der Universität Rostock besteht aus einem Sprach–Netz, das mit Komponenten der Firma Siemens aufgebaut ist, und aus einem Datennetz, das mit Komponenten der Firma CISCO aufgebaut ist. Eine teilweise Verschmelzung wurde mit der Verbindung einzelner Telefonanlagen über ATM erreicht [Lan98]. Die Verbindungen werden direkt über ATM hergestellt und nicht über ein zusätzliches Netzwerkprotokoll. Aus der Verschmelzung ergeben sich die in Kapitel 3.2.1 genannten Sicherheitsprobleme für ATM. Da die Verbindung nur innerhalb der Uiversität erfolgt, und die Zugangskontrolle zum ATM–Netz leicht durchgeführt werden kann, sind die Sicherheitsrisiken als gering einzustufen. Zentrale Angriffspunkte im Sprachnetz sind die Telefonanlagen und die Kabelverteiler. Die Konfiguration der Telefonanlagen muss durch eine Zugriffskon-

<table>
<tr><th colspan="8">IUK-Prozesse</th></tr>
<tr><th colspan="4">isochron</th><th colspan="4">asynchron</th></tr>
<tr><th colspan="2">Sprache</th><th colspan="2">Video</th><th colspan="2">Festbild</th><th colspan="2">Daten</th></tr>
<tr><td>ISDN, analog (PSTN) sicher</td><td>Internet, Intranet (VOIP)</td><td>ISDN (sicher)</td><td>Internet, Intranet</td><td>ISDN (Bildtele-fon)</td><td>Internet, Intranet</td><td>Modem</td><td>Internet, Intranet</td></tr>
<tr><td>Dienst-güte garantiert</td><td>Dienst-güte nicht garantiert</td><td>Dienst-güte garantiert</td><td>Dienst-güte nicht garantiert</td><td colspan="4">Dienstgüte nicht interessant</td></tr>
<tr><td colspan="2">Telefon</td><td colspan="2">Videokonferenzen, Live-Videoübertragung</td><td colspan="2">Bildtelefon</td><td colspan="2">Dateiübertragung, Email, Text, WWW</td></tr>
</table>

Abbildung 2.1: Informations– und Kommunikationsprozesse

trolle vor Angreifern geschützt sein. Die Räume der Telefonanlagen und der Kabelverteiler sind vor unberechtigtem Betreten zu schützen. Werden diese Regeln eingehalten, so ist das Sprachnetz als sicher zu betrachten.

Das Datennetz besteht aus einem ATM–Backbone, aufgebaut mit ATM–Switches, und dem LAN–Bereich, aufgebaut mit den LAN–Switches(Abbildung 7.1). Die Einbindung in den Backbone erfolgt über den ATM–Dienst LAN–Emulation, mit dem virtuelle LANs im gesamten Uni–Bereich verteilt werden können. Über diese virtuellen LANs werden Dienste, wie zum Beispiel Voice–Over–IP, Internetanbindung, Dateitransfer, realisiert. Für jeden dieser Dienste gelten, da alle über das IP–Protokoll kommunizieren, die Sicherheitsprobleme des IP–Protokolls, zum Beispiel Adressfälschungen (siehe Kapitel 3.3). Ein Sicherheitskonzept, das auf die IP–Schicht ausgerichtet ist, macht alle Anwendungen sicherer.

In Forschung und Ausbildung werden in der Universität alle Arten der Kommunikation betrieben. So werden zum Beispiel Videokonferenzen sowohl über ISDN (sicher, da schwer abhörbar), als auch über Internet (unsicher, da prinzipiell abhörbar) durchgeführt. Hinzu kommt die Erprobung neuer Techniken, wie zum Beispiel Voice–Over–IP, was eine Flexbilität in der Konfiguration und im Sicherheitsmanagement erfordert.

Durch die unterschiedlichen Bereiche in der Universität, gibt es Konfigurationen, die den realen Unternehmen gleichzusetzen sind.

2.2 Universität Rostock–Verwaltungsnetz

Die Verwaltung stellt sich wie ein kleines Unternehmen dar, dass die Dienste des Internet eingeschränkt nutzt. Eine beiderseitige Kommunikation über das Internet beschränkt sich auf den Email Austausch. Die Nutzung von WWW und FTP beschränken sich auf Client–Dienste, eigene Server für diese Dienste sind nicht vorgesehen. Durch die festgelegte Nutzer– und Dienststruktur, ist nur eine geringe Flexibilität erforderlich.

isochron	asynchron
Sprache	Daten
ISDN, analog (PSTN)	Internet, Intranet
Dienstgüte garantiert	Dienstgüte nicht interessant
Telefon	Dateiübertragung, Email, Text, WWW

Abbildung 2.2: Informations– und Kommunikationsprozesse im Verwaltungsnetz

2.3 Allgemeines Unternehmen

Das Netz eines Unternehmens ist an seinen Bedürfnissen und Möglichkeiten ausgerichtet. In vielen Unternehmen gab es bereits ein Rechnernetzwerk, bevor eine Verbindung zum Internet hergestellt wurde. Genutzt wird das Internet zur Verbindung mit anderen Unternehmensstandorten, zur Präsentation des Unternehmens im Internet, für kundenspezifische Dienstleistungen, zur Kommunikation per Email und für Recherchen durch die Mitarbeiter. Neue Kommunikationsformen, wie zum Beispiel Internettelefonie und Videokonferenzen über Internet, werden bislang selten eingesetzt. Grund dafür sind

Sicherheitsrisiken, nicht garantierbare Dienstgüte, nicht ausreichende Internetanbindungen und Sicherheitskomponenten, wie zum Beispiel Firewalls, die bestimmte Verbindungstypen nicht passieren lassen. Diese Dienste werden weiterhin über das öffentliche Telefonnetz abgewickelt. Abbildung 2.3 zeigt die IUK–Prozesse in einem strukturiertem Unternehmen.

So groß der Nutzen des Internets auch sein mag, der Anschluss birgt auch Gefahren

isochron			asynchron	
Sprache		Video	Festbild	Daten
ISDN, analog (PSTN)	Intranet (VOIP)	ISDN	ISDN	Internet, Intranet
Dienst-güte garantiert	Dienst-güte nicht garantiert	Dienstgüte garantiert	Dienstgüte nicht interessant für die Bildübertragung	Dienstgüte nicht interessant
Telefon		Videokonferenzen	Bildtelefon	Dateiübertragung, Email, Text, WWW

Abbildung 2.3: Informations– und Kommunikationsprozesse in einem Unternehmen

in sich. Durch die Verbindung von Unternehmensnetz und Internet kann ein Angreifer im ungünstigsten Fall Unternehmens– und Kundendaten ausspionieren. Das Unternehmensnetz muss davor geschützt werden. Bei der Konzeption des Netzes und seiner Sicherheitskomponenten muss eine auf zukünftige Anwendungen ausgerichtete Flexibilität bewahrt bleiben.

Kapitel 3

Sicherheitsrelevante Normen und Standards nach dem ISO/OSI Schichtenmodell

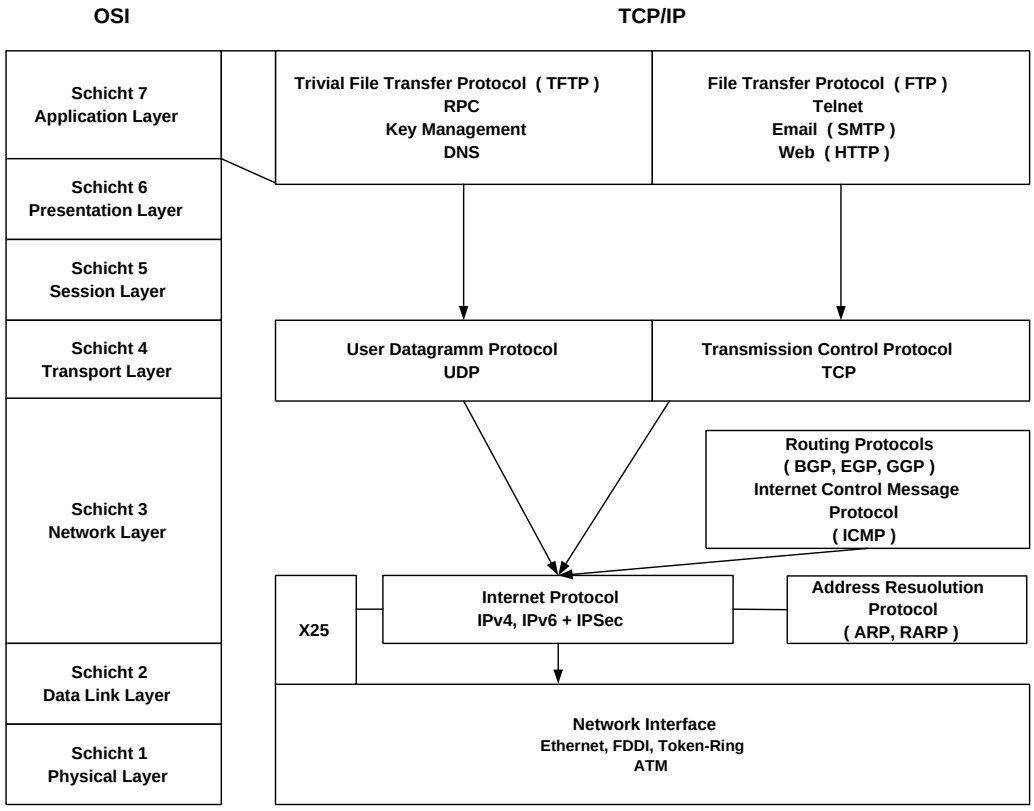


Abbildung 3.1: Das OSI Referenzmodell der ISO / TCP/IP Protokollsuite nach [Mar00]

3.1 Physical Layer – Schicht 1

Die physikalische Verbindung der Netzwerke untereinander findet über Funk, Kupfer– oder Glasfaserkabel statt. Die Schicht 1 übernimmt dabei die Anpassung an das physikalische Übertragungsmedium. Ein Angriff auf dieser Schicht beinhaltet einen direkten Zugriff auf das Übertragungsmedium. Die möglichen Szenerien für die einzelnen Übertragungsmedien werden nachfolgend erläutert.

- Glasfaserkabel
  - Aufteilen einer Verbindung mittels einer LWL–Weiche.
    Hierfür muss ein Zugriff auf eine LWL–Steckverbindung bestehen. Die Steckverbindung wird aufgetrennt und die LWL–Weiche wird eingesetzt.
  - Auskoppeln der Daten durch Überschreitung des Biegeradius der LWL–Faser
    Das LWL–Kabel muss dabei bis auf die Faser entisoliert werden, ohne dabei die Faser selbst zu beschädigen. Danach wird der maximale Biegeradius der LWL–Faser überschritten, und an der Biegestelle kann jetzt das Signal ausgekoppelt werden.
    Beide Varianten führen zu einer Erhöhung der Dämpfung auf dem Kabel, wodurch der Angriff entdeckt werden kann.
- Kupferkabel
  - Zwischenschalten eines Hubs
    Für das Zwischenschalten eines Hubs ist ein Zugriff auf ein Schaltfeld oder einen Switch nötig. Das Anschlusskabel wird aus dem Anschluss entfernt und auf einen Hub gesteckt. Anschließend wird der Uplink des Hubs auf den freien Port gesteckt. Durch die Nutzung des Hubs ist ein Abhören der Verbindung möglich.
  - induktive Auskopplung
    Hierzu wird der Mantel eines Kupferkabels entfernt und die einzelnen Adern mit einem Draht umwickelt. Das ausgekoppelte Signal wird durch das Tiefpassverhalten der Induktivität verfälscht und es kommt zu Übertragungsfehlern, die das Abhören verhindern können. Die Charakteristik des Kabels

selbst ändert sich ebenfalls durch den Eingriff. Die angeschlossenen Stationen bemerken dies nur an Hand von Paketfehlern, die im allgemeinen nicht ausgewertet und bemerkt werden.

- Funk
  Der Funkkanal ist der am leichtesten abhörbare Kanal, da das Medium nicht vor dem physikalischen Zugriff geschützt werden kann. Es muss dafür Sorge getragen werden, dass ein Angreifer aus den abgehörten Bitmustern nicht die ursprünglichen Daten zusammensetzen kann. Dies geschieht durch eine ausreichende Verschlüsselung auf der Übertragungsstrecke.

Insgesamt gestaltet sich der Angriff auf ein Kupfer– oder Glasfaserkabel als schwierig, da ein Zugriff auf die Kabel bzw. die Anschlüsse notwendig ist. Netzschränke lassen sich gut Überwachen, und Kabel sind meist so verlegt, dass unentdeckte Manipulationen nicht möglich sind. Die für den Funkbereich erhältlichen Lösungen werden heute bereits mit Verschlüsselung angeboten. Wird diese mit ausreichender Schlüssellänge eingesetzt, so ist der Funkkanal als sicher zu betrachten. Im weiteren Verlauf wird auf die Angriffsmöglichkeiten auf Layer1 und deren Vermeidung nicht weiter eingegangen.

3.2 Data Link Layer – Schicht 2

Die heute verwendeten Technologien zum Übertragen von IP–Paketen in LAN– und WAN–Netzen sind Ethernet, TokenRing, ATM, FDDI, Frame Relay und neuerdings IP over SONET/SDH.

3.2.1 ATM

Aus Sicht der Anwendungen liegt ATM unterhalb der IP–Schicht. ATM wird als reines Übertragungsmedium genutzt und ist für die IP–Pakete transparent. Daher wird ATM im TCP/IP–Modell auch als Protokoll der Schicht 2.5 eingeordnet. Für die Übertragung der IP–Pakete über ATM wird im allgemeinen der Dienst ATM LAN–Emulation, seltener Classical IP, genutzt. Dieser setzt im ATM Referenzmodell (Abbildung 3.2) auf die AAL–Schicht auf. Die Pakete durchlaufen bis zur Übertragungsschicht alle Schichten des ATM. Das ATM–Referenzmodell ist ein dreidimensionales Modell und nur schwer in das ISO/OSI Modell einzuordnen.

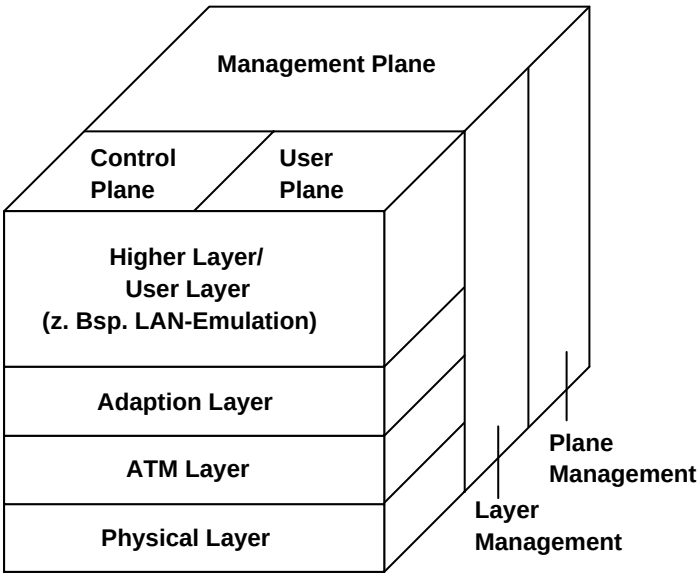


Abbildung 3.2: Das ATM Referenzmodell [Wun97]

Signalisierung

Der Unterschied zwischen ATM und sogenannten „Broadcast LANs“ besteht nach [BE99] darin, dass alle an der Kommunikation beteiligten Komponenten beim Verbindungsaufbau dem Datenaustausch zustimmen müssen. Jede Netzwerkkomponente kann somit Kontrolle über die Verbindung ausüben.
Der Verbindungsaufbau (Abbildung 3.3) ist für eine verteilte Zugriffskontrolle konzipiert worden. Die beim Verbindungsaufbau versandten Informationen dienen bisher der Bestimmung, Festlegung und dem Austausch von Verbindungsparametern für den zu etablierenden SVC. Diesen Vorgang bezeichnet man als betriebsmittelbasierte Zugriffskontrolle. Signalisierungsnachrichten setzen sich aus Informationselementen zusammen, in denen Reservierungswünsche, Protokollinformationen und ATM–Adressen kodiert sind. Alle wesentlichen Informationen sind in der SETUP–Nachricht (Abbildung 3.3) kodiert.

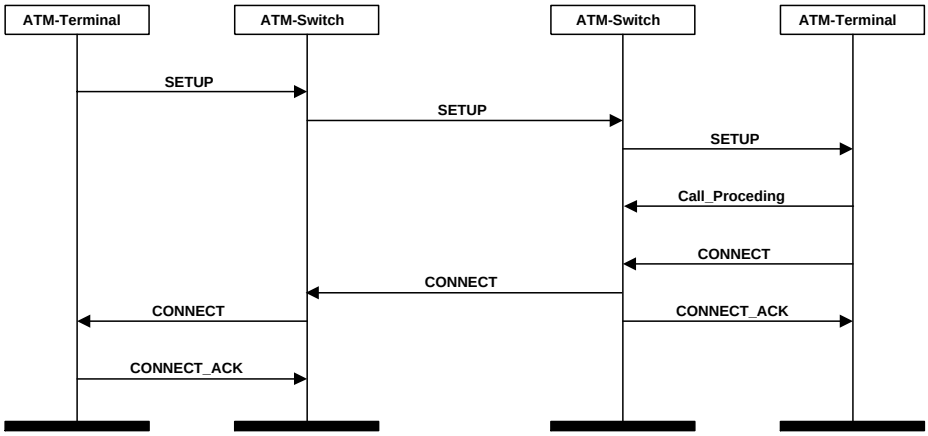


Abbildung 3.3: Standardsignalisierung zwischen zwei ATM–Endgeräten [BE99]

3.2.2 Andere Netzwerktechnologien

FDDI, Ethernet, Token–Ring

Im Gegensatz zu ATM sind FDDI, Ethernet und Token–Ring sogenannte Broadcast LANs. Die Switches, an denen die an der Kommunikation beteiligten Geräte angeschlossen sind, haben als einzige die Möglichkeit den Zugriff auf das Netzwerk zu kontrollieren. Diese Kontrolle kann auf Basis der Switch–Portnummern, der MAC–Adressen oder, bei neueren Switches, auf Basis der IP–Adressen oder der TCP–Ports erfolgen (Layer–4 Switching). Um einen lokalen Angriff durch das Abhören anderer Verbindungen durch `Sniffer` erschweren zu können, ist der Aufbau des Netzes mit Switches dringend notwendig. Durch die physikalische Trennung der Ports, können nicht mehr alle an den Switch angeschlossenen Stationen den Datenverkehr einer anderen Station mithören. Einzelne Verbindungen, wie zum Beispiel zum Server, können weiterhin abgehört werden. Diese Verbindungen müssen besonders geschützt werden, da viele Stationen eines Netzwerkes auf diesen Server zugreifen.
Weiterführende Zugriffskontrollen, wie zum Beispiel Authentisierung der fälschbaren MAC–Adresse, sind bisher nicht vorgesehen.

IP over SONET/SDH

IP over SONET/SDH ist ein neuer Übertragungsstandard für Weitverkehrsnetzwerke und wird als Übertragungstechnologie im G–WIN, dem Nachfolger des B–WIN, benutzt. In den nächsten Jahren wird sich dieses Verfahren aus Kostengründen im WAN–Bereich durchsetzen, da ATM sich im Anwendungsbereich nicht durchsetzen konnte. Die genutzten ATM–Dienste beschränken sich im WAN–Bereich hauptsächlich auf die Übertragung von IP–Paketen, und damit auf IP over ATM over SONET/SDH.

Frame Relay

Frame Relay ist wie ATM ein verbindungsorientiertes Protokoll. Es basiert auf dem X.25 Protokoll [IT93] und enthält zusätzlich Mechanismen zur Flusssteuerung und Fehlersicherung. Frame Relay arbeitet auf der Grundlage von virtuellen Kanälen (PVC und SVC). Frame Relay wird im Backbone–Bereich eingesetzt, da es ein günstiges Verhältnis von Nutzdaten/Protokolldaten hat. Ähnlich zu ATM wird vor dem Austausch von Nachrichten eine Verbindung zwischen den Endpunkten initialisiert. Diese Initialisierung verläuft ohne Autorisierung der Endgeräte auf Basis der bekannten Adressen. Die Sicherung der Verbindung wird den höheren Schichten überlassen. [Uhl00] DoS–Angriffe und Adressfälschungen sind möglich. Auf Grund der Ähnlichkeiten zu ATM sind ähnliche Ansätze für Sicherheitskomponenten wie in Kapitel 5.2.2 denkbar.

3.3 Network Layer – Schicht 3

3.3.1 IPv4

Das Internet–Protokoll ist ein verbindungsloses Protokoll und erlaubt den Austausch von Daten ohne vorherigen Verbindungsaufbau. IP macht die niedrigeren Schichten für die höheren Protokolle unsichtbar. Dies ermöglicht den Anschluss unterschiedlicher Netztypen an ein IP Gateway. IP setzt keine Fehlererkennung der unteren Schichten voraus. Ferner verfügt es über keine Verlässlichkeits- und Flusssteuerungsmechanismen. Diese Probleme werden an die nächsthöhere Schicht, die Transportschicht, abgegeben.

3.3.1.1 IP–Dienste

IP bietet den darüberliegenden Schichten folgende Dienste an:

- Check–Routine für den Internet Header
  Check des Datagramms nach folgenden Kriterien:
  - Ist die Länge des IP–Headers (HLEN) korrekt?
  - Ist die IP–Versionsnummer (VERS) korrekt?
  - Ist die IP–Nachrichtenlänge (TOTAL LENGTH) gültig?
  - Ist die IP–Header–Prüfsumme (HEADER CHECKSUM) gültig?
  - Ist der Wert im Time–to–Live (TTL) Feld gleich Null?
- IP–Source Routing
  Festlegung der Wegewahl durch eine höhere Protokollschicht (Pakete mit dieser Option sollten vom Router aus Gründen der Sicherheit nicht beachtet werden)
- IP–Default Routing
  Es wird dem Router die Wegewahl überlassen. **Standard**
- Routing Operations
  Es wird eine Routing–Liste aufgebaut, an Hand derer die Wegewahl erfolgt. Es gibt statische und dynamische Routing–Tabellen.
- Route Recording
  Jeder Knoten fügt dem Datagramm seine Adresse hinzu, so dass die Route zurückverfolgt werden kann
- Fragmentation and Reassambly
  Wenn ein IP–Packet größer ist als der MTU–Eintrag, so wird das Paket fragmentiert und am Zielort wieder zusammengesetzt.

[BW97]

3.3.1.2 IP–Adressen

Es werden 32 bit Adressen verwendet, um einen Knoten und das Netz, an dem er angeschlossen ist, zu identifizieren. Die bei IP gewählten Adressen ermöglichen eine strukturierte Adressierung unabhängig von den Hardware–Adressen und damit auch unabhängig von der zu Grunde liegenden Netztopologie. Es gibt 4 bereits definierte Adressklassen (Abbildung 3.4), die eine effektive Entscheidung ermöglichen, ob eine Adresse im eigenen oder im fremden Netz liegt [BW97],[Mar00]. Der Mangel an

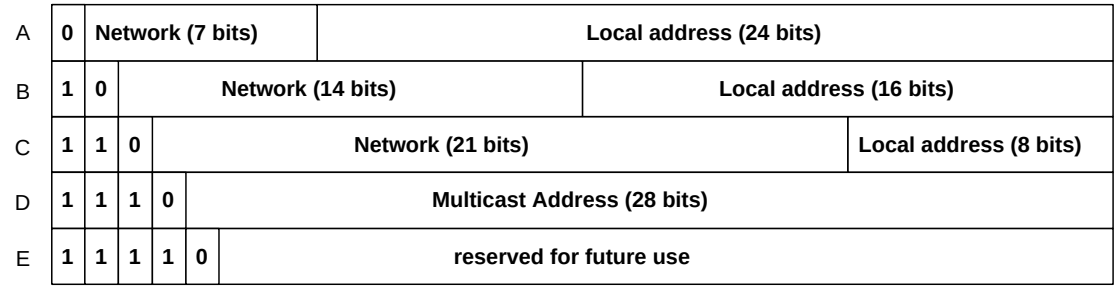


Abbildung 3.4: Adressklassen in IPv4 [BW97]

IP–Adressen erzwingt eine Abkehr von der Vergabepraxis in Class A–, B– oder C–Netzwerke. Heutzutage wird die Zugehörigkeit zu Subnetzen mit der Subnet–Mask festgelegt. Diese auf der Subnetz–Maske basierende Wegewahl wird als IP–Classless Routing bezeichnet. Die Subnetz–Maske ist wie die IP–Adresse 32bit lang und bezeichnet zusammen mit Grundadresse genau einen bestimmten Adressbereich innerhalb der IP–Adressen. Die Größe von Subnetzen wird in Potenzen von 2 festgelegt. Das kleinste Subnetz besteht aus 4 Adressen, die Host– Gateway– Broadcast– und die Grundadresse. Die Eintragung in einer Routertabelle

```
123.456.789.0 // 255.255.255.224
```

bedeutet:

Alle Pakete mit IP–Adressen von 123.456.789.0 (Grundadresse) bis 123.456.789.31 (Broadcastadresse) werden in dieses Subnetz geleitet.

3.3.1.3 IP–Primitive

IP kommuniziert mit der Transport– und der Übertragungsschicht nach dem Prinzip der Primitive.

IP/ULP Primitive

- SEND
  Das übertragende ULP benutzt SEND, um Daten an IP zu übermitteln.
- DELIVER
  IP verwendet DELIVER um dem Ziel–ULP Daten zu übertragen.

IP/SNP Primitive

- SNP_ Send
  wird von IP verwendet, um einen Dienst im SNP zu initiieren
- SNP_ Deliver
  wird von SNP benutzt, um ein Datagramm an IP zu liefern

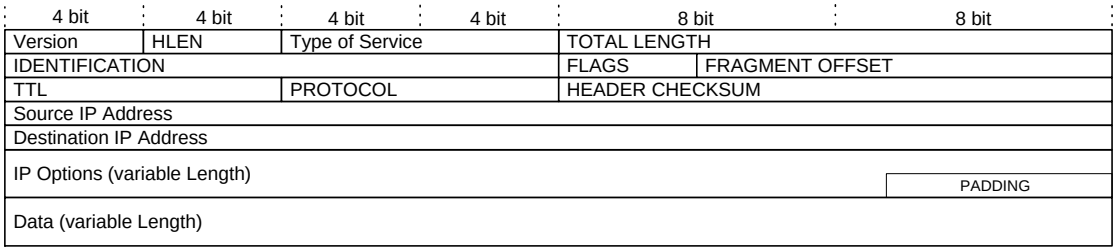
[BW97]

3.3.1.4 IP–Protokolldatenstruktur

Ein IP–Datagramm ist in den IP–Header und die Nutzdaten aufgeteilt. Die Felder eines IP–Datagrammes sind in Abbildung 3.5 dargestellt und erläutert.

3.3.2 IPv6

Die Weiterentwicklung der IP Version 4 ist IP Version 6 (IPv6). Mit der neuen Version sollen Schwachstellen von IPv4 beseitigt werden. Hervorzuheben ist die Implementierung von IPSec, die Vergrößerung des Adressraumes auf 128 bit und die Einbindung von Flusssteuerungsmechanismen. An dem grundlegenden Aufbau von IP als paketvermittelter Dienst hat sich nichts geändert.



Feld	**Bedeutung**
Version	IP Protokollversion
HLEN	Länge des Datagramm–Headers
Type Of Service	Identifikation von Quality of Service Optionen
TOTAL LENGTH	Gesamtlänge des IP–Datagramms
IDENTIFICATION	identifiziert Fragmente eines des Datagramms eindeutig
FLAGS	zeigt an, ob ein Datagramm fragmentiert werden kann
FRAGMENT OFFSET	Angabe der relativen Position des Fragments zum Originaldatagramm
TTL	enthält die Anzahl der Router, die noch überquert werden dürfen. Wird bei jeder Überquerung inkrementiert
PROTOCOL	identifiziert das über IP liegende Protokoll
HEADER CHECKSUM	Genutzt zur Erkennung einer Veränderung am Header
Source IP Address	IP Adresse des Paketabsenders
Destination IP Address	IP Adresse des Zielsystems
IP Options	identifiziert mehrere zusätzliche Dienste
Data	Nutzdaten
PADDING	Auffüllen eines variablen Feldes auf ein vielfaches von 32bit

Abbildung 3.5: Aufbau des IPv4 Datagramms und Bedeutung der Felder [Mar00]

3.3.2.1 IPv6–Header

Der Aufbau des IP–Headers wurde in der Version 6 stark verändert. Es gibt die Möglichkeit von hintereinander verschachtelten Headern, wobei jeder einzelne Header eine andere Funktion hat (Tabelle 3.1). Es wird auf der Übertragungsstrecke nur der gerade benötigte Header ausgewertet, wodurch eine deutliche Verkleinerung des Verarbeitungsaufwandes erreicht wird. Dabei enthält der IPv6 Basis–Header nur die notwendigsten Informationen, die jede zu durchlaufende Station im Internet benötigt (Abbildung 3.6). Im Feld „Next“ eines jeden Headers wird die Art (Protokoll-Identifier in Tabelle 3.1) des darauf folgenden Headers angegeben. So kann sich das Gerät bis zu dem entsprechenden Header durcharbeiten. Eine Aufzählung und eine Reihenfolge der Header ist

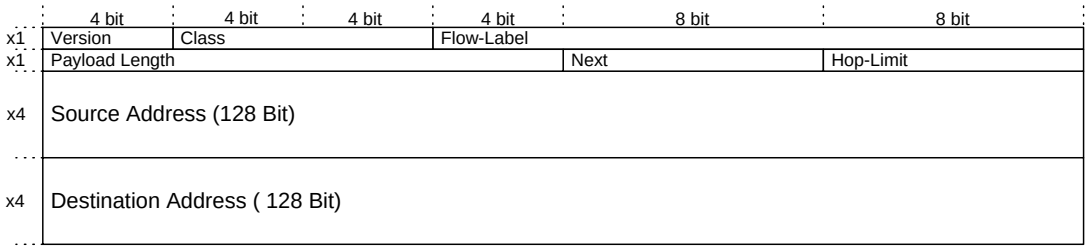


Abbildung 3.6: Aufbau des IPv6 Basisheaders [Dit98]

in Tabelle 3.1 dargestellt, die Header des Datenteils in Tabelle 3.2. Die im Datenteil

Tabelle 3.1: Reihenfolge der IPv6 Header mit Protokoll Identifier [Dit98]

Protokoll–Identifier	**Headertyp**
-	IPv6 Basis–Header
0	Hop–by–Hop–Optionen
60	Ziel–Optionen für jeden Router
43	Header für Routing
44	Header für Fragmentierung
55	Header für Authentisierung
50	Header für Verschlüsselung
60	Ziel–Optionen für Endgerät
siehe Tabelle 3.2	TCP / UDP / andere Nutzdaten

genutzten Protokolle haben unterschiedliche Ident-Nummern.

Tabelle 3.2: Beispiele für Header des Datenteils [Dit98]

Protokoll–Identifier	**Beispiele für Header des Datenteils**
1	ICMP
2	IGMP
4	IPv4–Daten
6	TCP
8	EGP
9	IGP
17	UDP
41	IPv6–Daten in einem Tunnel

Header für das Routing

Der Header für das Routing übernimmt zum großen Teil die Funktionen des Source–Routing der Version 4. Es gilt ebenso wie bei IPv4 die Empfehlung, die Wegewahl durch den Empfänger aus sicherheitstechnischen Gründen zu unterbinden.

Header für die Fragmentierung

Fragmentierung bedeutet Aufteilung des Paketes in mehrere kleine Pakete. Dies geschieht, da nicht auf allen Strecken im Netzwerk mit der gleichen Paketgröße gearbeitet wird. Im Unterschied zur Version 4 darf in Version 6 nicht mehr der Router das Paket aufteilen, sondern nur noch die aussendende Station. Dies bewirkt, dass der Sender Kontrolle über die Aufteilung des Paketes hat. Bei Benutzung des Authentication–Headers der Version 6 ist diese Prozedur zwingend erforderlich, da nur der Absender ein entsprechend authentisiertes Paket erzeugen kann.

Hop–by–Hop–Optionen

Diese Optionen finden Verwendung für den Transport von Optionen, die bei jedem Übertragungsschritt benötigt werden. Bisher definierte Optionen sind Füllbytes zum

Auffüllen des Optionsheaders auf 32bit Grenzen, Jumbo–Payload zum darstellen der Paketgröße wenn die 16bit im normalen Header nicht ausreichen und Router Alarm zur Angabe, wie ein Router mit einem Paket umzugehen hat.

Ziel–Optionen

Zusätzliche Optionen können bei IPv6 entweder als einzelne Header eingeschoben werden, oder zusammengefasst im Header „Ziel–Optionen“ transportiert werden. Im Standard sind bisher nur Füllbytes als Optionen definiert. Der Header „Ziel–Optionen“ stellt eine Vorbereitung für zukünftige Anwendungen (Tunnel, mobile Stationen) dar. Für den Erweiterungsheader „Ziel–Optionen“ gibt es die Besonderheit, dass er mehrfach in der Kette der Header vorkommen kann. Abhängig von der Position des Headers in der Kette gelten die Optionen für das Endgerät oder für die dazwischenliegenden Router.

Verschlüsselung und Authentisierung im Header

Für die Sicherheit der Verbindung wird durch die Verwendung der Header für Authentisierung und Verschlüsselung gesorgt. Mit der Authentisierung lässt sich der Empfänger eindeutig verifizieren und eine Manipulation auf dem Transportweg erkennen. Durch die Verschlüsselung wird das Mitlesen der im Paket vorhandenen Informationen auf dem Übertragungsweg verhindert. (siehe Kapitel 3.3.3)

Flusssteuerung

Das Feld „Flow–Label“ im IPv6–Basis Header (Abbildung 3.6) ist für die Flusssteuerung zuständig. Jedes Paket eines bestimmten Kommunikationstyps erhält den gleichen Wert. Für die Router ist es nun möglich, je nach Kommunikationstyp eine Entscheidung in der Wegewahl zu treffen. Die Benutzung dieses Feldes ist unter anderem für die Übertragung von Video– und Audiodaten in Echtzeit gedacht. Bei welchen Anwendungen Flow–Label in der Praxis genutzt werden, wird sich im Laufe der Jahre zeigen. Es muss speziell darauf geachtet werden, dass nicht der Nutzer selbst die Priorität in der Übertragung ändern kann, ansonsten ist der gesamte Mechanismus wirkungslos.

3.3.3 IPSec

IPSec ist Bestandteil des IPv6–Protokolls und als Erweiterung zu IPv4 vorgesehen. Zu IPSec gehören die Bestandteile Authentication Header, Encapsulation Security Payload, Lokales Security Management und Key–Management.

3.3.3.1 Authentication Header (AH)

Der AH ist entworfen worden, um die Integrität und Authentizität eines IP–Paketes ohne Vertrauen auf die IP–Datagramme zu gewährleisten. Der Mangel an Vertrauen in die IP–Datagramme wird für eine weite Verbreitung von Implementationen des AH im Internet sorgen, gerade in Ländern wo der Ex– und Import von Verschlüsselungstechnologie eingeschränkt ist. Der AH unterstützt Sicherheit zwischen zwei oder mehr Hosts, zwischen 2 oder mehr Security–Gateways, zwischen einem Host und einem Gateway und zwischen einem Host/Gateway und einer Menge von Hosts/Gateways. Bei allen Teilnehmern muss dazu der AH implementiert sein. Ein Security–Gateway ist ein System, dass als Gateway zwischen externen, nicht vertrauenswürdigen Systemen und internen vertrauenswürdigen Systemen fungiert. Falls ein solches Gateway existiert, und alle Hosts im internen Netz vertrauenswürdig sind, kann das Security–Gateway alle Funktionen im Zusammenhang mit dem Authentication Header übernehmen.[Atk95]
Mit dem AH wird durch Verwendung von Sequenznummern Schutz gegen das Wiedereinspielen von Datagrammen erreicht. Der Authentication Header trägt einen Integrity Check Value (ICV), der über die zu schützenden Felder des IP–Pakets berechnet wird. Durch den AH werden IP–Spoofing und darauf aufbauende Angriffe vereitelt. IPv6

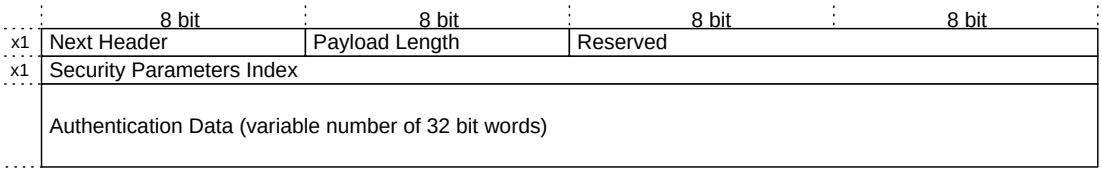


Abbildung 3.7: Aufbau des Authentication–Header [Dit98]

schreibt vor, dass alle Implementierungen die Option zur Authentisierung unterstützen. Es ist im Standard nicht festgelegt, welche Verfahren zur Verschlüsselung verwendet werden, jedoch müssen zumindest die Verfahren HMAC (Keyed Hashing for Message

Authentication siehe RFC 2104) mit MD5 (Message Digest Algorithm Nr.5 siehe RFC 1321) und HMAC mit SHA-1(Secure Hash Algorithm Version 1 des amerikanischen National Institut of Standards and Technology) in jeder Implementierung vorhanden sein. [Dit98]
Es ist abzusehen, dass sicherheitsrelevante Anwendungen in Zukunft Authentisierung vorschreiben werden. Als Beispiel sind das DNS–System und der mobile Einsatz mit IPv6 zu nennen.

3.3.3.2 Encapsulation Security Payload (ESP)

Der IP–ESP ist entworfen worden, um für Integrität, Authentizität und Vertrauen in die IP–Datagramme zu sorgen. ESP unterstützt, wie der AH (Kapitel 3.3.3.1) Sicherheit zwischen zwei oder mehr Hosts, zwischen zwei oder mehr Security–Gateways, zwischen einem Host und einem Gateway und zwischen einem Host/Gateway und einer Menge von Hosts/Gateways. Bei allen Teilnehmern muss dazu ESP implementiert sein. [Atk95] Eine Gateway zu Gateway Verschlüsselung ermöglicht den einfachen und sicheren Aufbau von Virtual Private Networks (VPN).
ESP bietet zum einen die Verschlüsselung der Nutzdaten und zum anderen den Aufbau eines verschlüsselten Tunnels, wobei der gesamte Inhalt eines IP–Pakets inklusive der Header verschlüsselt wird. Die Nutzdatenverschlüsselung wird hauptsächlich bei der Kommunikation von Host zu Gateway/Host bzw. umgekehrt eingesetzt werden. Die Tunnelversion wird beim Einsatz von VPNs, also bei der Kommunikation von Gateway zu Gateway, Verwendung finden. Für die Verschlüsselung sind eine ganze Reihe

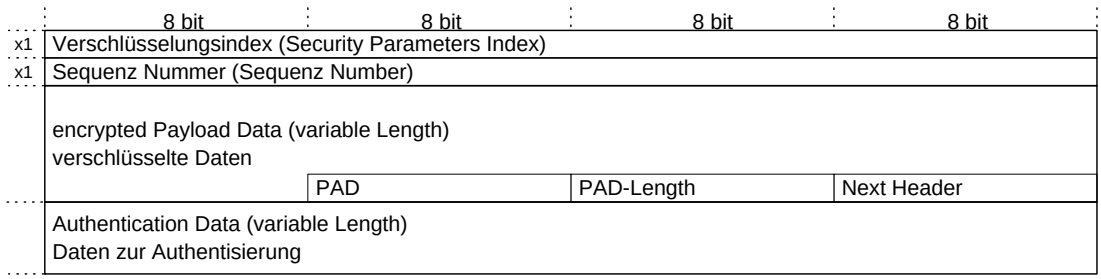


Abbildung 3.8: Aufbau des ESP–Header [Mar00]

von Verfahren wählbar. Bei der Definition des Standards fanden nur symmetrische Ver-

schlüsselungsverfahren Beachtung, da die asymmetrischen Verfahren zu langsam für die heutigen Übertragungsverfahren sind. Es muss nur sichergestellt werden, dass sich Sender und Empfänger auf mindestens ein Verfahren einigen können. Darum sieht der Standard als Mindestanforderung an jede konforme Implementierung das Verfahren DES mit CBC zur Verschlüsselung vor. Bis zum Anfang des Jahres 2000 waren die verwendeten Schlüssellängen dieses Verfahrens durch die Ausfuhrrestriktionen der US–Regierung beschränkt. Diese Einschränkungen wurden teilweise aufgehoben, womit das Standardverschlüsselungsverfahren sicherer wird. Die Schlüsselaustauschverfahren sind in Kapitel 3.3.3.5 beschrieben.

Verschlüsselung mit DES–CBC

Bei der Verwendung des DES–CBC Verfahrens wird eine Datenblocklänge von 64 bit verlangt. Zum Auffüllen auf die 64 Bit Grenze werden Füll–Bits (**PAD** (Abbildung 3.8)) eingefügt. Die Anzahl der eingefügten Bits wird im Feld **PAD–Length** eingetragen. Den verschlüsselten Daten wird ein Initialisierungsvektor vorangestellt. Als Initialisierungsvektor kann ein einfacher Zähler verwendet werden, der mit einer Zufallszahl gestartet wird. Der Verschlüsselungsindex (Abbildung 3.8) dient zusammen mit den IP–Adressen zur Auswahl des Verschlüsselungsverfahrens und des gültigen Schlüssels. [Dit98]

Verschlüsselung mit Triple–DES

Der Unterschied von Triple–DES zu DES–CBC besteht darin, dass der Datenblock dreimal nacheinander mit jeweils einem anderen Schlüssel verschlüsselt wird. [Dit98]

3.3.3.3 Security Association

Das IPSec Paket trägt in seinem Header keine direkte Information in sich, welches Verschlüsselungsverfahren mit welchem Schlüssel gerade benutzt wird. Auf diese zwingend notwendige Information zeigt der Security Parameters Index (SPI) im Header (Abbildung 3.8). Die eigentliche Datenstruktur, die lokal die relevanten Parameter vorhält, ist die Security Association (SA). Eine SA beschreibt eine unidirektionale Verbindung. Sie ist bei IPSec immer auf den Empfänger bezogen, adressiert durch
`[Destination-IP-Address, SPI, Protocol]`.

„Protocol“ bezeichnet die IPSec–Protokolle ESP oder AH und den jeweiligen Modus. Für eine typische Verbindung sind zwei SAs zu etablieren, für jede Verbindungsrichtung eine. Es gibt zwei prinzipielle Modi, den bereits beschriebenen Tunnel–Modus und den Transport–Modus. Im Tunnel–Modus wird ein komplettes IP–Paket inklusive der Header in ein neues Paket verpackt. Im Transport Modus werden die ursprünglichen Header beibehalten.
Weitere Parameter spezifizieren das zu verwendende kryptografische Verfahren sowie von diesem benötigte Schlüssel und Verfahrensparameter. Diese werden der SA in der Security Association Database zugeordnet. Es kann eine bestimmte Gültigkeitsdauer basierend auf Zeit oder verarbeiteter Datenmenge festgelegt werden [Mar00].

3.3.3.4 Lokales Security Management

Security Policy Database

Da IPSec Sicherheitsmechanismen auf Paketebene bereitstellt, muss für jedes dieser Pakete entschieden werden, ob und, wenn ja, wie dieses zu schützen ist. Das administrative Interface für diese Entscheidung bildet die Security Policy Database (SPD). Diese Datenbasis stellt in abstrakter Form die Security Policy eines Computersystems dar. Die SPD muss für jedes „IPSec–Interface“ Regeln definieren, welche Mechanismen auf eingehende– und welche auf ausgehende Pakete angewandt werden sollen („inbound“ rules / „outbound“ rules). Für „normale“ Hosts mit einem Interface stellen diese Regeln die Anforderungen dieses Hosts an den Datenverkehr, der ihn erreicht und der ihn verlässt, dar. Für Security Gateways, die zwei oder mehr Interfaces haben, können aus der Kombination der Regeln für den ankommenden Datenverkehr des einen und den abgehenden Verkehr des anderen Interfaces die Regeln für den überquerenden Datenverkehr gewonnen werden.
Es gibt für das IP–Paket folgende Entscheidungsmöglichkeiten:

- Paket verwerfen
- Paket darf ohne IPSec–Funktionen passieren
- Paket muss IPSec–Mechanismen aufweisen

Im letzten Fall muss mit angegeben werden, welche Sicherheitsmechanismen für das entsprechende Paket eingesetzt werden sollen. Sogenannte Selektoren dienen als Index

zur SAD und kennzeichnen damit die Granularität der entsprechenden Policy [Mar00].

Security Association Database

Die Security Association Database (SAD) enthält eine Liste der gültigen SAs. Eine dynamische Relation zwischen SPD und SAD bietet die Möglichkeit, für eine bestimmte Policy direkt auf eine aktive SA zurückzugreifen bzw. festzustellen, dass eine SA etabliert werden muss.
Die SPD enthält Regeln, wie die Selektoren für den neuen SAD abgeleitet werden. Der Selektor kann dabei

a) direkt aus der SPD kopiert werden oder

b) aus dem auslösenden Paket übernommen werden.

Für ein Security Gateway kann somit zum Beispiel festgelegt werden, ob die resultierende SA für den gesamten Datenverkehr gelten soll, oder ob nur die gleichen im SPD–Eintrag festgelegten Security Services (z.B. ESP mit 3DES) gelten sollen, für jede Hostverbindung jedoch separate SAs, und damit Schlüssel, zu nutzen sind [Mar00].

3.3.3.5 IPSec–Security Association Management/Key Management

Die in den vorherigen Abschnitten beschriebenen Verfahren bieten einen wirksamen Schutz für IP–Pakete. Es stellt sich nun die Frage, wie die einzelnen Hosts, die an der Kommunikation beteiligt sind, untereinander die Informationen über die in einer Security Association gehaltenen Parameter (die eine Art Vertrag über die Sicherheitsparameter darstellen) austauschen. Da in diesem Vertrag geheime symmetrische Schlüssel spezifiziert werden, sind die „Vertragsverhandlungen“ sicher und geheim zu führen. Ohne ein Key Management Protokoll bestünde für Hosts, die mittels IPSec miteinander kommunizieren wollen, die Möglichkeit, diese Schlüssel verhältnismäßig lange vor der Verbindung zum Beispiel per PGP-verschlüsselter Email, per Post oder per Smart–Card zu verbreiten. Dieses Verfahren ist unsicher und unflexibel.
In der IPSec Arbeitsgruppe der IETF ist aus diesem Grund an der Spezifikation geeigneter Key Management Protokolle gearbeitet worden. In der Entwicklung gab es zwei Ansätze [Mar00]:

1. Schlüsselinformationen direkt im IP–Paket durch zusätzliche Headerinformationen mitzuschicken („in–band“):
   Das Key Management bleibt dabei auf derselben Kommunikationsschicht bezogen auf das OSI–Modell.

2. Ein separates und universelles Key Management Protokoll bereitzustellen:
   Dieses kann zwangsläufig nur auf der Anwendungsebene stattfinden und bricht damit mit der „reinen“ Lehre des Schichtenmodells, dass niedrige Schichten für höhere Schichten Dienste erbringen.

Im Laufe der Standardisierungsverfahren hat sich mit ISAKMP/Oakley (IKE) ein universelles Key Management Protokoll durchgesetzt. In jeder standardkonformen Implementation muss damit mindestens IKE unterstützt werden. Nachfolgend werden die wichtigsten Protokolle, die bei der Entwicklung von IKE eine Rolle spielten, näher erläutert [Mar00].

Simple Key Management Protokoll SKIP

SKIP ist ein „in–band“–Key Management, bei dem durch zusätzliche Headerinformationen (SKIP–Header) im Paketheader die Bereitstellung des Schlüsselmaterials erfolgt. Grundsätzlich basiert SKIP auf dem Diffie–Hellman–Verfahren, wobei im Gegensatz zu den später beschriebenen Photuris, Oakley und IKE der öffentliche DH–Exponent eines Hosts ein „langlebiger“ Schlüssel ist, der von einer dritten Instanz zertifiziert oder in einer Art Pre–Shared Key Verfahren (Schlüsselaustausch lange vor der Kommunikation) ausgetauscht wird. Der gemeinsame Schlüssel zwischen zwei beliebigen Instanzen *I* und *J* ergibt sich entsprechend dem DH–Algorithmus aus dem eigenen geheimen Wert sowie dem öffentlichen Exponenten des jeweiligen anderen Kommunikationspartners. Verwendet eine Station SKIP, so wird in jedem Paket ein zusätzlicher Header transportiert [Mar00].

Vorteile

- Unabhängigkeit von einem „Out–of–Band“ Protokoll
- sofortiges Senden geschützter Paket ohne durchlaufen eines Key Management Protokolls
- unkomplizierte Implementierung des Protokolls

- Einhaltung des OSI–Schichtenmodells
- Grundsätzlich keine Speicherung von Statusinformationen nötig

Nachteile

- Paketgröße
  Der zusätzliche SKIP–Header wird in *jedem* Paket transportiert. Dies bedeutet erhebliche Bandbreitenbelastung und Verschlechterung des Verhältnisses von Nutzdaten/Gesatmtdaten im ungünstigsten Fall von 90% auf 84%.
- Austausch/Abgleich von Sicherheitsanforderungen
  Ein Sender weiß im allgemeinen nicht, ob der Empfänger das von ihm gewählte Verfahren beherrscht. In einem solchen Falle werden zusätzliche ICMP–Nachrichten nötig. Ein flexibles Sicherheitsmanagement ist nicht möglich.
- Security Gateways
  SKIP schlägt vor, im Falle des Einsatzes von SGs diesem die geheimen DH–Parameter mitzuteilen. Daraus ergibt sich das Problem, dass das SG eine eventuelle Ende–zu–Ende Verschlüsselung mitlesen kann.

[Mar00]

Photuris

Photuris ist ein Key Management Protokoll, das zur Bereitstellung kurzlebiger (symmetrischer) Session–Keys eingesetzt werden kann und vom Protokolldesign besonders interessant im Hinblick auf die Verhinderung von DoS–Angriffen ist. Dieser Ansatz ist in die Entwicklung von IKE eingeflossen. Photuris besteht aus mehreren Protokollphasen:

1. Cookie Exchange
2. Value Exchange
3. Identification Exchange
4. Weitere optionale Nachrichten

Besonders in der ersten Phase des Protokolls dem Cookie Exchange sind Maßnahmen gegen einen Denial–of–Service Angriff enthalten. Denial–of–Service Angriffe bestehen in dieser Protokollphase aus dem Fluten eines Systems mit Authentisierungsanfragen. Damit einhergehen könnte je nach Protokolldesign:

- Fluten mit Verbindungsaufbauwünschen auf Transportebene und damit Bandbreiten/Systemressourcenverbrauch
- Bindung weiterer Systemressourcen und von Rechenzeit für die Generierung von Protokollnachrichten

Ein intelligenter Angreifer wird versuchen, durch Fälschung seiner IP–Adresse davon abzulenken, dass das System mit Anfragen überflutet wird. IPSec Mechanismen helfen an dieser Stelle noch nicht, Fälschungen zu entdecken, da hierfür erst die Etablierung von SAs notwendig ist, was mit dem Key Management Protokoll stattfindet. Es müssen andere Wege gefunden werden, das Key Management selber vor einem DoS–Angriff zu schützen. Für ein Protokoll, das resistent gegen DoS–Angriffe sein soll, ergibt sich die Hauptanforderung in einem möglichst geringen Verbrauch an Systemressourcen während der Authentisierungsphase. Bezogen auf ein Computersystem sind dies:

- geringer Speicherbedarf: Speicherung nur weniger Statusinformationen
- geringer Rechenzeitbedarf: sparsamer Einsatz kryptografischer Operationen zu Beginn des Protokolls
- geringer Bandbreitenbedarf: möglichst kurze Nachrichten verwenden

Den geringsten Ressourcenverbrauch bezüglich der Übertragung von Nachrichten hat ein zustands-/verbindsloses Protokoll, wie zum Beispiel UDP, welches zum Austausch der Photuris–Nachrichten genutzt wird. In der ersten Phase des Protokolls (Cookie Exchange) werden sogenannte ***Cookies als Pre–Authentisierungstoken*** (Anti–Clogging–Token) verwendet. Als Cookie wird bei Photuris ein 16 Byte langer Header bezeichnet. Initiator und Responder generieren ihre Cookies aus verschiedenen Parametern, so dass die Cookies zusammen genau eine Exchange identifizieren. Der Responder überprüft an Hand der IP–Adresse bei der Generierung seines Cookies ob der Initiator bereits zu viele SPIs hat, ob noch nicht abgeschlossene Photuris–Exchanges in Bearbeitung sind und

ob ein Photuris–SPI mit dem Initiator noch nicht abgelaufen ist. Dieser Mechanismus verhindert folgende Arten von Angriffen:

1. Angreifer, die ihre IP–Adresse nicht fälschen, können leicht durch die responderseitige Begrenzung von „offenen“ Exchanges erkannt werden.

2. Cookie Requests von gefälschten IP–Adressen werden zunächst beantwortet, wobei vom Responder kaum Systemressourcen verbraucht werden.

   - Ohne Routingmanipulation wird die Cookie–Response zum wahren Inhaber der gefälschten IP–Adresse geleitet, der ein ungültiges IC erkennt und die Nachricht verwirft. Der Angreifer kann keine weiteren gültigen Nachrichten erzeugen.
   - Kann der Angreifer das RC abhören (Nachricht führt über sein Netz), kann er weitere gültige Nachrichten erzeugen

3. Ein weiterer Schutzmechanismus ist die Symmetrie der durchzuführenden Rechenoperationen. Beide Parteien müssen gleichmäßig rechenzeitintensive Public–Key–Operationen durchführen. Für einen bezüglich Rechenleistung schwächeren Angreifer, schlägt damit der Angriff fehl.

Dem vorgestellten Cookie Exchange folgen weitere Protokollphasen:

- Value Exchange:
  Es werden entsprechend dem im Cookie–Response ausgewählten Schlüsselaustausch–Schema benötigte Werte sowie unterstütze Verfahren zum Schutz des weiteren Photuris–Exchange ausgetauscht.

- Identification Exchange:
  Im weiteren Verlauf werden durch eine zu wählende Authentisierungsmethode die Identitäten der Parteien ausgetauscht, diese verifiziert und die zuvor ausgetauschten DH–Exponenten authentisiert.

Diese Protokollphasen wurden in die Spezifikation von IKE (Abbildung 3.9) nicht übernommen. [Mar00]

Secure Key Exchange Mechanism for the Internet SKEME

SKEME wurde als Erweiterung von Photuris entwickelt. Folgende Punkte standen dabei im Mittelpunkt:

- Einführung neuer Trustmodelle, zum Beispiel Key Distribution Center (KDC) und manuell verteilte, geheime Schlüssel (Pre–Shared Keys)
- flexiblere Anpassungsfähigkeit zwischen den Sicherheitsanforderungen und dem notwendigen Overhead des Key Exchanges durch Möglichkeit eines schnellen Re–Keying ohne aufwendige Public–Key–Operationen
- explizit keine Unterstützung von Signaturen zur Authentisierung der DH–Parameter, damit keiner der Kommunikationspartner dem jeweilig anderen das Stattfinden einer Kommunikation über die signierten Daten nachweisen kann.

SKEME ist in 3 Phasen unterteilt.

1. SHARE
   Beide Kommunikationspartner senden einen mit dem öffentlichen Schlüssel des anderen verschlüsselten Zufallswert, wobei keine Empfangsbestätigungnen einbezogen sind. Aus den beiden Zufallswerten wird mittels einer Hashfunktion ein gemeinsamer Schlüssel generiert.
2. EXCH
   Die Kommunikationspartner tauschen ihre öffentlichen DH–Exponenten aus.
3. AUTH
   Diese Phase authentisiert die Parameter und damit die Teilnehmer.

Es gibt die Möglichkeit, Kombinationsformen der 3 Phasen anzuwenden. Alle Informationen sind in 3 Nachrichten übertragbar. [Mar00]

Oakley Key Determination Protokoll

Das Oakley Key Determination Protokoll wurde als ein auf dem Diffie–Hellmann Verfahren beruhendes Schlüsselaustauschprotokoll entworfen. Es bietet viele Freiheitsgrade zur optimalen Anpassung an die Erfordernisse der involvierten Parteien [Mar00].
Eigenschaften von Oakley:

- Anti–Clogging–Defense (DoS) mit dem Cookie Mechanismus des Photuris Protokolls
- Etablierung / Abgleich von Verschlüsselungs-, Authentisierungs-, und Schlüsselgenerierungsmethode zwischen den beteiligten Parteien
- Authentisierung der DH–Exponenten durch ein separates Verfahren, um keine zyklischen Abhängigkeiten, ähnlich einem selbstsignierten Zertifikat, zu erzeugen
- DH–Exponentiation braucht nicht vor der Authentisierung stattfinden
- Der generierte Schlüssel hängt nicht nur vom DH–Mechanismus, sondern zusätzlich vom ausgewählten Authentisierungsverfahren, zum Beispiel von einer RSA–Verschlüsselung, ab.
- Eigene DH–Gruppen können genutzt werden

Die Anzahl der auszutauschenden Nachrichten hängt davon ab, wieviele Informationen der Sender pro Protokollschritt preisgibt. Im effizientesten Fall sind 3 Nachrichten auszutauschen. Dieser sogenannte „Aggressive Mode“ bietet bereits Perfect Forward Secrecy (PFS) für das ausgetauschte Schlüsselmaterial und die Geheimhaltung der IDs der Parteien. Im sogenannten „Main Mode“ bietet Oakley zusätzlich DoS Abwehr mit vorgeschalteten Cookie Exchange, PFS für die Geheimhaltung der Identitäten und Signaturen für Nichtabstreitbarkeit der Kommunikationsbeziehung. [Mar00]

ISAKMP

ISAKMP wird als ein universelles Key– bzw. Security–Management–Protokoll für IPSec favorisiert. Streng genommen stellt ISAKMP nur einen Protokollrahmen bereit, in dem mehrere Nachrichtentypen definiert sind. Mit den Protokollnachrichten wird das eigentliche Key–Management–Protokoll aufgebaut. ISAKMP Nachrichten werden mittels UDP ausgetauscht. Vor jeder Nachricht wird ein ISAKMP–Header platziert. Dieser gewährleistet das Halten eines minimalen Verbindungskontextes. Dem Header folgen die unterschiedlichen Nachrichten, je nach Protokollschritt (Tabelle 3.3). ISAKMP ist das erste vorgestellte Protokoll, welches einen 2–Phasen–Ansatz einführt. In Phase 1 wird ein gesicherter Kanal bereitgestellt, über den in Phase 2 Schlüssel für die anfordernden Instanzen ohne aufwendige Public–Key Operationen bereitgestellt werden können.

Tabelle 3.3: Nachrichtendefinitionen in ISAKMP nach [Mar00]

Security Association	-	Aushandlung der Parameter für Sicherheitsdienste und Definierung der Umgebung, Situation, unter der diese Parameter gelten
Proposal	-	Vorschlag von Sicherheitsmechanismen
Transform	-	Definition eines bestimmten Sicherheitsmechanismus
Key Exchange	-	Beliebige Daten, abhängig vom verwendeten Key–Exchange Algorithmus
Identification	-	Daten zur Identifizierung der Teilnehmer, Interpretation abhängig von der Umgebung
Certificate	-	Transport von Public–Key–Zertifikaten oder zertifikatsbezogenen Informationen
Certificate Request	-	explizite Anforderungen von Zertifikaten
Hash	-	Übertragung von Hash–Werten zur Authentisierung und Integritätssicherung in ISAKMP–Nachrichten
Signature	-	Nutzung in einigen Authentisierungs–Schemata zur Nichtabstreitbarkeit der Verbindung
Nonce	-	Zufallsdaten, genutzt für den Schutz vor einem Wiedereinspielen von abgehörten Nachrichten
Notification	-	Informationen über Fehlerzustände
Delete	-	Löschen von einer Security Association

Phase 1

Es finden starke kryptografische Verfahren zur Authentisierung statt. Die kryptografischen Verfahren zum Schutz des ISAKMP–Kanals werden ausgehandelt und die notwendigen Schlüssel etabliert. Dadurch werden Hijacking– und DoS Angriffe verhindert.

Phase2

Der gesicherte Kanal kann genutzt werden, um ein effizienteres Protokoll einzusetzen. Eine Authentisierung und Schlüsseletablierung erfolgt in dieser Phase nun je nach anfordernder Instanz.

Vorteile des 2–Phasen Ansatzes:

1. Nutzung des sicheren Kanals für mehrere Key Exchanges
2. Security Services der ersten Phase schützen die zweite Phase

3. Fehlernachrichten der zweiten Phase bedingen kein völlig neues Aufsetzen des Key Exchanges, da der sichere Kanal weiter besteht. Auch das löschen von SAs erfolgt über den gesicherten Kanal.

[Mar00]
ISAKMP stellt in allen Phasen folgende Exchange Type bereit:

1. Base Exchange
2. Identity Protection Exchange
3. Authentication Only Exchange
4. Aggressive Exchange

[Mar00]

ISAKMP/Oakley (IKE) Key Management Protokoll

Mit Hilfe der in ISAKMP definierten Nachrichten und Exchange Types sowie dem bezüglich kryptografischer Verfahren konkreten „Oakley Key Determination Protocol“ kann ein sehr flexibles Key Management Protokoll aufgebaut werden. Weiterhin fanden noch Verfahren der Protokolle SKEME und Photuris Anwendung. Dieser Zusammenhang ist in Abbildung 3.9 zu erkennen.

Kryptografisch wichtige Funktionen in IKE Nachfolgend werden die wichtigsten Kryptografischen Verfahren erläutert.

- Diffie–Hellmann–Verfahren
  Das DH–Verfahren ist ein Public–Key Verfahren, dessen Sicherheit auf der Schwierigkeit beruht, den diskreten Logarithmus für große Zahlen zu berechnen. Es ist jedoch nur ein reines Schlüsselaustauschprotokoll.
- Asymmetrische Verschlüsselungs– und Signaturverfahren
  RSA oder DSS
- Symmetrische Verschlüsselung mit HMAC
  HMAC ist eine parametrisierbare „Pseudo Random Function“, eine sogenannte Keyed–Hash–Funktion.

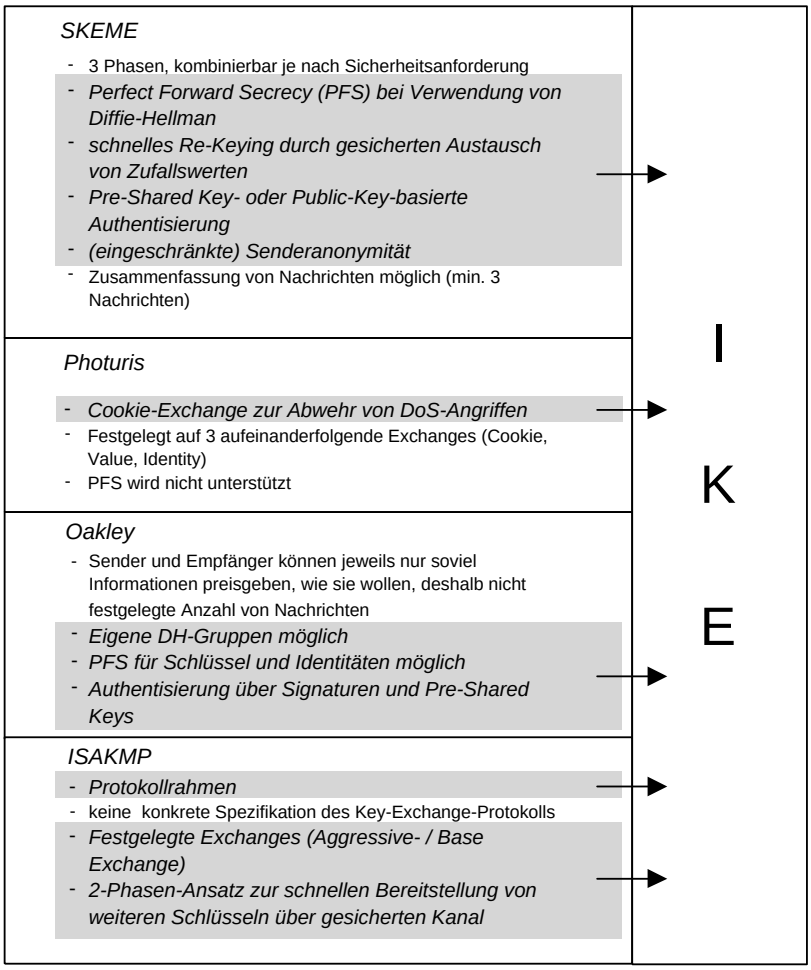


Abbildung 3.9: Übernommene Elemente in das IKE–Protokoll [Mar00]

- Symmetrische Verschlüsselung
  Einsatz zur Verschlüsselung des sicheren Kanals. Mindestanforderung ist Unterstützung des DES–CBC

[Mar00]

Phasen und Modi in IKE In IKE wird der 2–Phasen–Ansatz von ISAKMP aufgegriffen. In Phase 1 werden die Exchange Typen von ISAKMP genutzt. Aus dem Oakley–Protokoll wurden die verschiedenen Modi übernommen, die es den Kommunikationspartnern überlassen, das Verhältnis von Protokolloverhead zu gewünschter Sicherheit festzulegen. Es wurden zwei Modi und damit die Nachrichtenabfolgen und Exchange–

Typen festgelegt. Die Bezeichnungen (Aggressive Mode, Main Mode) wurden ebenfalls aus dem Oakley–Protokoll übernommen.[Mar00]

Tabelle 3.4: Vergleich der Phasen bei IKE [Mar00]

Phase 1	Phase 2
– Authentisierung beider Endpunkte, Auswahl unter unterschiedlich starken Verfahren möglich – Relativ ressourcenintensiv durch große Anzahl an Public Key Operationen (DH, DSS oder RSA) – Keine Möglichkeit des schnellen „Rekeying“ der IKE–SA, stattdessen muss die SA gelöscht und ein völlig neuer Exchange eingeleitet werden – Protokolldesign bietet Schutz vor verschiedenen Angriffsarten – Bidirektionale SA mit gleichen Parametern in beiden Richtungen	– Nur symmetrische Authentisierung von Nachrichten mit Schlüsseln des sicheren Kanals – Optional „Perfect Forward Secrecy“ möglich, mit dem Nachteil rechenintensiver DH–Operationen – Sehr schneller Austausch neuer Schlüssel und / oder Wechsel des Verschlüsselungsverfahrens möglich – Mehrere SAs für einen IKE Clienten gleichzeitig etablierbar

3.4 Transport Layer – Schicht 4

3.4.1 TCP

Das Transmission Control Protocol (TCP) wurde zusammen mit IP entwickelt. Es stellt gesicherte virtuelle Verbindungen bereit. Verlorene oder verstümmelte Pakete werden noch einmal übertragen und die Pakete in der gleichen Folge abgeliefert, wie sie gesendet wurden. TCP ist ein verbindungsorientierter Dienst, der auf IP als Übertragungsprotokoll aufsetzt. Es wird ein Port–Mechanismus genutzt, der die gleichzeitige Aktivität mehrerer Applikationen zulässt. Eine TCP–Verbindung ist gekennzeichnet durch den Vektor `(localhost, localport, remotehost, remoteport)`. Durch diese Kennzeichnung einer Verbindung ist es möglich, dass ein einzelner Port eines Servers mehrere verschiedene Clients bedienen kann.

3.4.1.1 Dienste von TCP

TCP bietet den höheren Schichten folgende Dienste: [Mar00]

- Connection–oriented data management
  TCP speichert Status und Zustandsinformationen eines jeden Datenstroms, der durch das TCP Modul fließt. Ferner ist TCP für den Ende-zu-Ende Transfer von Daten zu einer empfangenden Anwendung durch ein oder mehrere Netze verantwortlich.

- Reliable data transfer
  TCP garantiert einen verlässlichen Datentransfer. Dazu benutzt es Sequenznummern und positive oder negative Bestätigungsflags. TCP setzt dabei Timer und sendet die Daten erneut, wenn bei Ablauf des Timers noch keine Empfangsbestätigung in Form des gesetzten ACK-Bits angekommen ist.

- Stream oriented data transfer
  TCP erhält die Daten eines Upper Layer Protocols (ULP) stromorientiert. Das heißt, es werden einzelne Oktets und keine Blöcke oder Datagramme entgegengenommen. Kommen diese Oktets in der Transportschicht an, so werden sie zu TCP-Segmenten zusammengefasst. Diese werden dann an IP oder ein anderes darunterliegendes Protokoll weitergeleitet. Die Länge der Segmente wird dabei von TCP bestimmt.

- Push function
  Diese Operation wird benutzt, wenn eine Applikation sicher gehen möchte, dass alle Daten, die sie an TCP weitergeleitet hat, auch sofort übertragen werden. Dabei wird TCP durch einen Sendebefehl aufgefordert, den gesamten gepufferten Datenbestand in Form von Segmenten zur Zieladresse zu senden.

- Flow control
  Das Empfänger–TCP–Modul ist in der Lage, den Datenfluss des Senders zu steuern. Dadurch wird ein Pufferüberlauf und eine mögliche Überlastung der Empfängermaschine vermieden. Dem Übertragenden wird ein Fensterwert mitgeteilt. Er kann dann eine bestimmte Anzahl von Bytes innerhalb dieses Fensters versenden. Danach wird das Fenster geschlossen und der Sender muss die Übertragung beenden.

- Resequencing
  TCP verwendet Sequenznummern nicht nur zur Bestätigung, sondern auch zum sogenannten resequencing. Dabei werden diejenigen Segmente zurückgeschickt, die am Zielort zerstört ankommen. Da TCP auf einem verbindungslosen Dienst aufbaut, ist es möglich, dass im Internet Duplikate der Datagramme erstellt und weggeschickt werden (der sogenannte Replay-Attack). Solche Datagramme werden von TCP erkannt und verworfen.

- Multiplexing
  TCP kann mehrere Benutzersitzungen innerhalb eines einzelnen Hostrechners zu den einzelnen ULPs schalten.

- Full–duplex transmission
  TCP bietet volle Duplex–Übertragung zwischen zwei TCP-Instanzen an. Dies erlaubt eine gleichzeitige Zweiweg–Übertragung, ohne dass man auf ein Turnaround-Signal warten muss. Dieses Signal wäre in einer Halb-Duplex Situation notwendig.

- Gracefil close
  TCP schließt eine logische Verbindung zwischen zwei Diensten erst, wenn der gesamte Datenverkehr quittiert wurde.

- Passive and active open
  TCP bietet zwei Formen des Verbindungsaufbaus an. Der passiv–open–Modus ermöglicht den ULPs, TCP mitzuteilen, dass es auf einen Connection Request des fremden Systems warten soll. Empfängt TCP ein solches Connection Request, so wählt das Betriebssystem des Hosts eine Portnummer aus. Die zweite Form des Verbindungsaufbaus ist die des active–open–Modus. Dabei bestimmt das ULP ein socket, durch das die Verbindung aufgebaut werden soll.

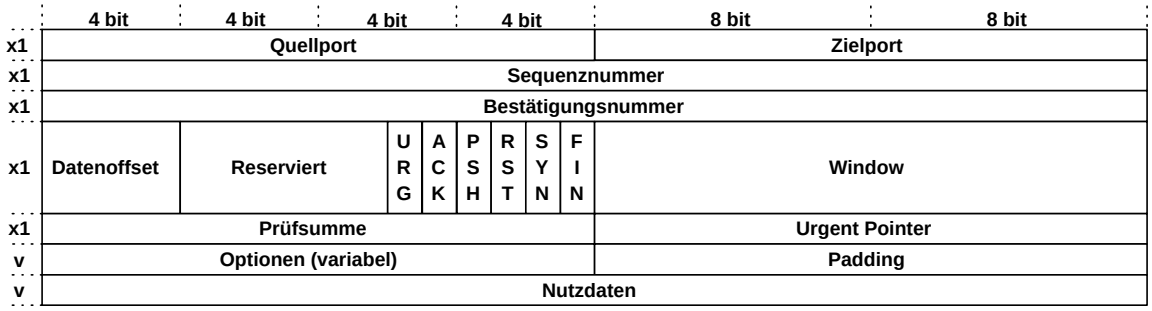
- Transmission Control Blocks (TCB)
  TCP muss einige Informationen der Verbindung speichern. In den TCBs sind unter anderem die remote socket number, Pointer zu den Sende– und Empfängerpuffern, Pointer zur Warteschlange der erneut zu übertragenden Daten, die Sicherheits– und Prioritätspuffer und das derzeitige Segment gespeichert.

3.4.1.2 Steuerkommandos (Dienste–Primitive) und Protokolldatenstruktur

TCP arbeitet wie IP nach dem Konzept der Dienste–Primitive (Tabelle 3.5), um mit den oberen Schichten zu kommunizieren. Die Kommunikation mit den unteren Schichten wird dem IP–Protokoll überlassen.
Der Aufbau eines TCP–Datensegments ist in Abbildung 3.10 dargestellt.

Tabelle 3.5: TCP–Steuerkommandos

Service Request Primitive (ULP zu TCP)	
Befehl	**Parameter**
UNSPECIFIED–PASSIVE–OPEN	Lokaler Port, ULP time-out, time-out Aktion, precedence, security, Optionen
FULL–PASSIVE–OPEN	Lokaler Port, Zielsocket, ULP–time–out, time–out Aktion, precedence, security, Optionen
ACTIVE–OPEN	Lokaler Port, fremder Host, ULP–time–out, time–out Aktion, precedence, security, Optionen
ACTIVE–OPEN–WITH–DATA	Quellport, Zieladresse, ULP–time–out, time–out Aktion, precedence, security, Daten, Datenlänge, Push–Flag, Urgent–Flag
SEND	Lokaler Verbindungsname, Pufferadresse, Byteanzahl, Push–Flag, Urgent–Flag, ULP time–out, time–out Aktion
RECEIVE	Lokaler Verbindungsname, Pufferadresse, Byteanzahl, Urgent–Flag, Push–Flag
ALLOCATE	Lokaler Verbindungsname, Datenlänge
CLOSE	Lokaler Verbindungsname
ABORT	Lokaler Verbindungsname
STATUS	Lokaler Verbindungsname
Service Response Primitive (TCP zu ULP)	
Befehl	**Parameter**
OPEN–ID	Lokaler Verbindungsname, fremder Socket, Zieladresse
OPEN–FAILURE	Lokaler Verbindungsname
OPEN-SUCCESS	Lokaler Verbindungsname
DELIVER	Lokaler Verbindungsname, Pufferadresse, Byteanzahl, Urgent–flag
CLOSING	Lokaler Verbindungsname
TERMINATE	Lokaler Verbindungsname, Beschreibung
STATUS RESPONSE	Lokaler Verbindungsname, Quellport und –adresse, fremder Port, Verbindungszustand, Sende– und Empfangsfenster, Urgent– Modus, time–out, time–out Aktion
ERROR	Lokaler Verbindungsname, Fehlerbeschreibung



Feld	**Bedeutung**
Quellport	Port des Quellsystems
Zielport	Port des Zielsystems
Sequenznummer	Nummer des aktuellen Oktets
Bestätigungsnummer	Sequenznummer des nächsten Oktets
Daten–Offset	Bestimmung, wo das Datenfeld beginnt
Reserviert	Für spätere Verwendung reserviert
URG	Zeigt an, ob das Feld „urgent pointer“ von Bedeutung ist
ACK	Bestätigungsfeld
PSH	Ausführung von Pushfunktionen
RST	Zurücksetzung der Verbindung
SYN	Synchronisierung der Sequenznummern
FIN	Sender hat keine Daten mehr
Window	Angabe, wieviele Oktets der Empfänger zu empfangen bereit ist
Prüfsumme	Zur Bestimmung, ob das Oktet fehlerfrei angekommen ist
Urgent Pointer	Gibt an, in welchem Oktet sich wichtige Informationen befinden
Option	Für Zukünftige Anwendungen
Padding	zum Auffüllen des Headers auf ein Vielfaches von 32bit

Abbildung 3.10: Aufbau eines TCP–Datensegments [CB96]

3.4.2 UDP

Das User Datagram Protocol ist ein verbindungsloses Protokoll der Transportschicht, das prinzipiell als Erweiterung von IP anzusehen ist. Es sind keine Transportquittungen oder andere Sicherheitsmaßnahmen für die Absicherung der Übertragung vorgesehen. UDP enthält 16 bit Portnummern, die unabhängig von den bei TCP verwendeten Portnummern sind. Die Pakete werden im Datenfeld von IP übertragen. UDP findet Verwendung, wenn nicht alle Dienste von TCP benötigt werden. Insbesondere bei Datenabfragen, bei denen die Menge der ausgetauschten Informationen klein ist verglichen mit dem Aufwand eines Verbindungsauf– bzw. –abbaus, wird UDP verwendet. Der Aufbau einer UDP Nachricht ist in Abbildung 3.11 dargestellt.

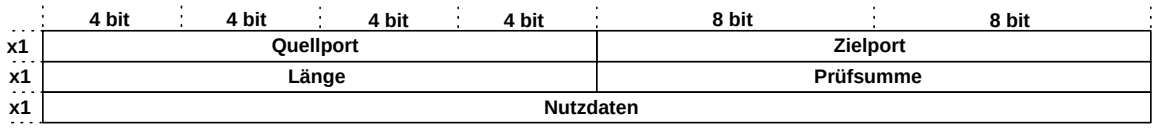
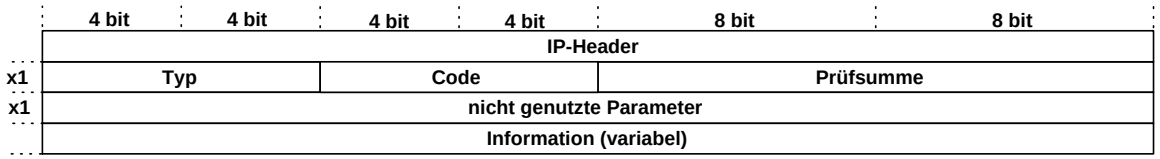


Abbildung 3.11: Aufbau einer UDP Nachricht [CB96]

3.4.3 ICMP

ICMP dient dazu, Fehlermeldungen, Steuerinformationen oder Statusmeldungen zu übertragen. ICMP selbst ist kein eigenständiges Übertragungsprotokoll, sondern nutzt das Datenfeld von IP zur Übertragung. Der Aufbau einer ICMP–Nachricht ist in Abbildung 3.12 dargestellt.



Feld	**Bedeutung**
Typ	Typ der Nachricht
Code	Typ der Fehler oder Statusinformation

Abbildung 3.12: Aufbau einer ICMP Nachricht [BW97]

Es gibt die folgenden ICMP–Services:

Echo Reply	-	Antwort auf einen Echo Request (Ping)
Destination Unreachable	-	gewünschter Host nicht erreichbar
Source quench	-	Router hat keinen Platz mehr für Pakete (Flusssteuerung)
Redirect (change a route)	-	Ändern des Paketweges
Echo Request (Ping)	-	Anforderung eines Echo Reply, um herauszufinden, ob ein Host erreichbar ist
Time Exceed for a Datagram	-	Zeitspanne für den Empfang abgelaufen
Parameter Problem on a Datagram	-	Probleme mit einem Paketheader
Timestamp Request	-	Anforderung eines Zeitstempels
Address Mask Request	-	Anforderung der Adressmaske
Address Mask Reply	-	Antwort auf die Adressmaskenanforderung

3.4.4 Transport Layer Security

Transport Layer Security basiert auf dem von „Netscape Communications“ entwickelten SSL–Protokoll. SSL bietet einen recht allgemeinen Ansatz für die Absicherung von virtuellen Verbindungen auf der Transportebene und kann im OSI–Schichtenmodell oberhalb der Transportschicht eingeordnet werden. Die meisten Anwendungen nutzen die Socket–Schnittstelle als Zugang zu einem TCP/IP–Netzwerk. SSL bedient sich ebenfalls dieser Schnittstelle zum Beispiel zur Übertragung der verschlüsselten Daten. SSL

verhält sich aus Sicht der Socket–Schnittstelle wie jede andere Anwendung. Für die Nutzung der Sicherheitsfunktionen muss die Anwendung explizit die SSL–Funktionen anstatt der Socket–Aufrufe ansprechen. Die SSL–Schicht baut selbstständig eine TCP–Verbindung zur SSL–Schicht des Servers auf, und führt zunächst eine Handshake–Prozedur durch (Abbildung 3.13). Anschließend steht beiden Kommunikationspartnern ein gesicherter Kanal zur Verfügung, der für den Datenaustausch genutzt wird.

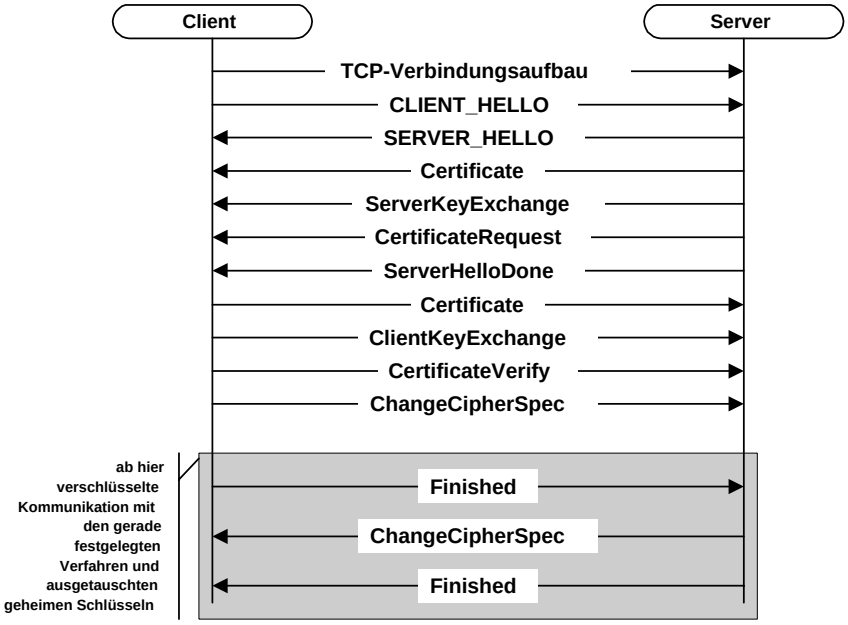


Abbildung 3.13: SSL–Handshakeprozedur [Mar00]

1. **Client_Hello**: Nach einem erfolgreichen TCP–Verbindungsaufbau werden durch den Client zunächst die von ihm unterstützten kryptografischen Verfahren in einer geordneten Liste übergeben.

2. **Server_Hello**: Der Server antwortet mit einem von ihm selektierten Verfahren. Standardmäßig wird das erste Verfahren der Liste genommen, dass der Server unterstützt. Sicherheitsbewusste Clients bzw. Server sollten darauf achten, nur starke Verschlüsselungsverfahren zu benutzen.
   Certificate: Anschließend wird regelmäßig das Serverzertifikat zum Nachweis der Identität an den Client gesendet.

ServerKeyExchange: Ist der in diesem Zertifikat enthaltene Schlüssel nur zum signieren vorgesehen, müssen zusätzlich Parameter für den anschließenden Schlüsselaustausch bereitgestellt werden.
CertificateRequest: Soll sich der Client an Hand eines Zertifikates identifizieren, wird dieses hiermit angefordert.
ServerHelloDone: Abschließend wird dem Client mitgeteilt, dass nunmehr keine weiteren Nachrichten folgen und der Server auf Nachrichten des Clients wartet.

3. **Certificate**: Hat der Server das Clientzertifikat angefordert, wird dieses hiermit bereitgestellt.
   ClientKeyExchange: Der Client wählt die Parameter für den späteren, gemeinsamen Sitzungsschlüssel, die mit dem öffentlichen Schlüssel des Servers kodiert werden. Möglich ist auch die Übermittlung eines öffentlichen DH–Exponenten und eines Zufallswertes.
   ClientVerify: Der Client signiert einen vom Server bereitgestellten Zufallswert zum Nachweis, dass er im Besitz des zum Zertifikat gehörigen geheimen Schlüssels ist.

4. Es stehen beiden Seiten die für die Kommunikation nötigen Verschlüsselungsparameter zur Verfügung.

Der Aufbau eines SSL–Datagramms ist in Abbildung 3.14 zu sehen.

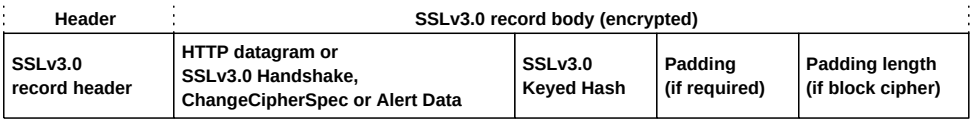


Abbildung 3.14: Aufbau des SSL–Datagramms [Mar00]

3.5 Vergleich der Sicherheitsprotokolle in den TCP/IP–Schichten

Abbildung 3.6 vergleicht die verschiedenen Sicherheitsprotokolle für die Datenübertragung. Es gibt nicht **die** Lösung, die sich gegen alle anderen durchsetzen wird. Wahr-

Tabelle 3.6: Vergleich der Sicherheitsprotokolle [Mar00]

Eigenschaft	*Anwendungsprotokolle*				*Transportschicht*	*Netzwerkschicht*
	S-HTTP	PGP	S/MIME	SSH	SSL (TLS)	IPSec + IKE
Handhabung aus der Sicht des Nutzers	Sehr einfach	Einfach bis schwierig (je nach Clientintegration)	Einfach bis schwierig (je nach Clientintegration)	Sehr einfach	Sehr einfach	Extrem einfach
Anwendungstransparenz	Nicht notwendig	Nicht notwendig	Nicht notwendig	Nicht notwendig	hoch	Extrem hoch
Signaturfunktion (spätere Nichtabstreitbarkeit)	Vorhanden	Vorhanden	Vorhanden	Nicht vorhanden	Nicht vorhanden	Nicht vorhanden
Granularität der Sicherheitsfunktionen	horizontal (innerhalb der Anwendung) hoch, vertikal (Host/Subnetze) nicht vorhanden	Weder horizontal noch vertikal (nur nutzerabhängige Entscheidung)	Weder horizontal noch vertikal (nur nutzerabhängige Entscheidung)	Horizontal nicht; vertikal gering (tunneling)	Horizontal gering Vertikal gering	Horizontal nicht; Vertikal sehr hoch
Unabhängige Integrationsfähigkeit in Hard-- und Software	Nicht möglich	Nicht möglich	Nicht möglich	Nicht möglich	Schwierig / wenn ja, inflexibel	Einfach möglich
Infrastrukturunabhängigkeit	Mittel	Niedrig	Hoch	Gering	Hoch	Mittel
Standardisierung	Hoch	Sehr hoch	Hoch	Hoch	Sehr hoch	Mittel
Verfügbarkeit	Mittel	Sehr hoch	Mittel	Hoch	Sehr hoch	(noch) gering
Verbreitung	Gering	Sehr hoch	Mittel	Mittel	Sehr hoch	(noch) gering
Administrierbarkeit	Einfach	Relativ aufwendig (einfacher mit Key-Servern	Relativ einfach (Zertifikats-verteilung!)	Sehr einfach (!nit. Schlüsselver-teilung)	Abhängig von Infrastruktur (komplex bis einfach)	Komplex bis einfach (je nach Policy)
Mehrseitige Sicherheits-anforderungen in komplexen Netzstrukturen	Nur Ende-zu-Ende Sicherheit	Nur Ende-zu-Ende-Sicherheit	Nur Ende-zu-Ende Sicherheit	Nur Ende-zu-Ende Sicherheit	Rel. Schwierig (ursprünglich nur Ende-zu-Ende)	Extrem flexibel
Anwendungsszenarien	Anwendung im WWW, z. Bsp. Bei Online Bestellungen	Email Verschlüsselung	Sichere Email Übertragung	Sicherer Remote Zugriff z. Bsp. per Telnet	Anwendung für Ende zu Ende Verschlüsselung	Anwendung bei VPNs und zur Authentisierung des Teilnehmers

scheinlich ist eine Koexistenz und Verbindung der verschiedenen Protokolle. So kann zum Beispiel SSL (TLS) für die allgemeine Absicherung des internen Netzes (auch gegen Angriffe von innen) benutzt werden und IPSec für die Verbindung mehrerer Netze über das Internet (VPNs).

Kapitel 4

Erarbeitung eines Sicherheitskonzeptes für ein strukturiertes Unternehmen

4.1 Grundhaltung

Das Sicherheitskonzept einer Firma spiegelt die Haltung zur Sicherheit wieder. Grundlagen des Konzeptes sind die Bedürfnisse des Unternehmens und die Gegenüberstellung der Kosten für das Konzept und der Kosten für eventuelle Einbrüche in das System. Jedes Unternehmen mit einem Internetanschluss muss ein solches Sicherheitskonzept erarbeiten. Bei der Erarbeitung eines Sicherheitskonzeptes sollte eine Liste der von außen zu erreichenden Dienste und eine Liste mit verbotenen Diensten erarbeitet werden. Bei der Auswahl der Dienste ist wieder die Sicherheitsphilosophie von entscheidender Bedeutung. Kernpunkt ist hier die Frage: Verbiete ich alles, was nicht erlaubt ist, oder erlaube ich alles, was nicht verboten ist?
Von den erstellten Listen ausgehend, wird dann die Konfiguration aus Technik und Software aufgestellt.

4.2 Entwicklung eines Sicherheitskonzeptes

Mit Hilfe des folgenden Fragenkataloges kann die Schutzbedürftigkeit des eigenen Netzes festgestellt und ein entsprechendes Sicherheitskonzept entwickelt werden.

1. Von welcher grundlegenden Sicherheitsphilosophie wird ausgegangen?
2. Welche Objekte müssen geschützt werden?
3. Wovor müssen die Objekte geschützt werden?

4. Welche Dienste sollen den Nutzern innerhalb und ausserhalb des Netzes zur Verfügung stehen?
5. Welche Geschwindigkeitsanforderungen bestehen an den Internet–Zugang?
6. Wer und wo sind die potentiellen Angreifer?
7. Worin liegt das Interesse der Angreifer?
8. Wie erfolgen die Angriffe?
9. Kann der Angriff entdeckt werden?
10. Wie groß ist der Schaden bei einem Einbruch?
11. Wie hoch sind die Kosten einer Schutzmaßnahme?
12. Habe ich qualifizierte Mitarbeiter für die Sicherheitstechnik?
13. Wie hoch sind die Einschränkungen für die eigenen Nutzer durch die Sicherheitsmaßnahme?
14. Wie hoch ist das Sicherheitsbewusstsein bei meinen Mitarbeitern?

Ausgehend von diesen Fragen kann das System in eine der ITSEC–Schutzklassen (siehe Tabelle 4.1) eingeordnet werden. Die Definition der Klassen ist aber viel zu ungenau und nur in den seltensten Fällen passend für die eigene Organisation. Eine Einordnung in die ITSEC–Schutzklassen ersetzt nicht die Erarbeitung eines eigenen Sicherheitskonzeptes!
Nach der Erarbeitung eines Sicherheitskonzeptes folgt die Wahl der notwendigen Hard– und Software. Hierbei ist je nach Organisation zu entscheiden, ob ein eigenes System aufgebaut wird, oder ob auf ein kommerzielles Produkt zurückgegriffen wird. Die Entscheidung beruht dabei auf den Kauf- bzw. Administrationskosten.
Beispielhafte Sicherheitskonzepte werden in Kapitel 4.4 beschrieben.

4.3 Sicherheitsanforderungen an Netzwerke

Die allgemeinen Sicherheitsanforderungen richten sich streng nach dem Sicherheitskonzept. Ausgehend von der Einordnung in die verschieden ITSEC–Sicherheitsklassen (Ta-

Tabelle 4.1: Systemanforderungen nach ITSEC–Klassen [BSI92]

ITSEC–Klasse	**wesentliche Forderungen**
D	- geringster Sicherheitsstandard - alle Systeme, die nicht die Anforderungen der höheren Klassen erfüllen
C1	- alle Benutzergruppen befinden sich auf dem selben Sicherheitsniveau - Trennung zwischen Benutzern und Daten
C2	- Überwachung und Speicherung der Operationen der einzelnen Nutzer - individuelle Identifizierung der einzelnen Benutzer - Schutz der Überwachungsdaten vor nicht autorisierten Zugriffen
B1	- Forderungen von C2 - Beseitigung aller bekannten Einbruchsmöglichkeiten in das System - verbindliche Zugangskontrollen - formelle Beschreibung des Sicherheitsmodells - vollständige Dokumentation der Funktionen des Systemverwalters - Markierung aller Objekte durch Geheimhaltungsstufen - Kenntlichmachung von vertraulichen Daten
B2	- Forderungen von B1 - Zugangskontrollen zu allen vom IT–System erreichbaren Komponenten - gesicherter Kommunikationspfad zwischen Benutzer und IT–System - elektromagnetische Abschirmung des IT–Systems nach außen
B3	- Forderungen von B2 - Eintragung aller nicht zugriffsberechtigter Benutzer in Zugangslisten - detaillierte Beschreibung des Sicherheitsmodells - automatische Erfassung von sicherheitsrelevanten Ereignissen - modularer Aufbau des IT–Systems - Verlagerung bestimmter Funktionen in Hardware des IT–Systems - gesicherte Wiederherstellung des Systemzustandes nach Fehlern
A1	- Forderung von B3 - keinerlei Systemerweiterung gegenüber B3 - formelle Beschreibung des Software–Designs - mathematische Eindeutigkeit des Sicherheitsmodells - Nachweis der fehlerfreien Implementierung der Software - Garantie der spezifischen Auslieferung von Hard– und Software

belle 4.1), können die Regeln für den Zugang zum Netz und zu den Netzwerkkomponenten festgelegt werden. Anforderungen speziell an Internet–Firewalls sind im Anhang A dargestellt.

4.4 Beispiele für Sicherheitskonzepte

Für die Erstellung eines Sicherheitskonzeptes werden die Fragen unter Kapitel 4.2 durchgearbeitet. Bei sämtlichen Sicherheitskonzepten wird davon ausgegangen, dass die Bedrohung aus dem externen Netz ausgeht.

4.4.1 Universität Rostock–Wissenschaftsnetz

Das Wissenschaftsnetz der Universität Rostock ist auf die maximale Verfügbarkeit ausgerichtet. Der Anschluss an das B-Win erfolgt zur Zeit mit 155 Mbit/s auf ATM Basis. Das nachfolgende Konzept ist speziell auf das Gateway zum B-Win ausgerichtet. Jeder Fachbereich kann prinzipiell sein eigenes Sicherheitskonzept erarbeiten. Beispiele in der Vergangenheit zeigen, dass teilweise bei Einbrüchen in Server der Universität panische und unüberlegte Reaktionen der Fachbereiche erfolgten. Wenn zum Beispiel ohne ein vorher entwickeltes Konzept einfach nur ein Bastion–Host aufgebaut wird, so ist das Netz hinterher keinesfalls als sicher zu betrachten (siehe Kapitel 5).

1. Von welcher grundlegenden Sicherheitsphilosophie wird ausgegangen?
   Maximale Sicherheit ohne Einschränkung der Verfügbarkeit und der Leistung der benötigten Dienste
   Es ist alles erlaubt, was nicht verboten ist.

2. Welche Objekte müssen geschützt werden?

   - Dateiserver
   - Mailserver
   - Webserver
   - Router
   - Workstations
   - Datenbanken

3. Wovor müssen die Objekte geschützt werden?

   - Denial–Of–Service Angriffe
   - unberechtigter Zugriff auf persönliche Daten
   - Verwüstung der Server

4. Welche Dienste sollen den Nutzern innerhalb und außerhalb des Netzes zur Verfügung stehen und welche müssen gesperrt werden?
   Die Dienste sind in Tabelle 4.2 dargestellt.
   Die Spalte „außerhalb“ beschreibt dabei die Regeln bei der Verbindung mit dem B–Win, „innerhalb“ beschreibt hingegen die Regeln bei der Verbindung der VLANs der Universität untereinander. Die Dienste SNMP und TFTP sind teilweise erlaubt, da ein zeitweiliger Zugriff von außen (zum Beispiel zum Einspielen von Softwareupdates direkt vom Hersteller) nötig ist. Die benötigte Verbindung wird exklusiv für den benötigten Zeitraum in die Filtertabelle eingetragen, und die Verbindung wird überwacht. Die Verbindung zwischen B-Win und Universitätsnetz ist statisch. Die Übertragung von Routinginformationen zwischen B-Win und dem Uni–Netz ist somit nicht erforderlich.

5. Welche Geschwindigkeitsanforderungen bestehen an den Internet–Zugang?
   Die Nutzung von zum Beispiel Videokonferenzen für Ringvorlesungen und die hohe Nutzeranzahl erfordert einen hohen Datendurchsatz beim B–WIN Zugang.

6. Wer und wo sind die potentiellen Angreifer?

   - Studenten oder Mitarbeiter innerhalb des Universitätsnetzes
   - Angreifer aus dem Internet

7. Worin liegt das Interesse der Angreifer?

   - Erlangung von Daten über das Studium zum Beispiel Klausuraufgaben
   - Erlangung von Passworten und damit Zugang zu den Servern um weitergehende Angriffe zu verschleiern und um Speicherplatz für illegale Software zu bekommen
   - Suche nach interessanten Daten

Tabelle 4.2: Erlaubte Dienste innerhalb und außerhalb des Netzes (Wissenschaftsnetz)

Dienst	innerhalb erlaubt	außerhalb erlaubt
DNS	✓	◯
ARP	✓	×
RIP	×	×
BGP	×	×
OSPF	✓	×
EIGRP	✓	×
SNMP	✓	◯
hline NIS	✓	×
NIS+	✓	×
ftp	✓	✓
TFTP	✓	◯
FSP	×	×
GOPHER	✓	✓
HTTP	✓	✓
S–HTTP	✓	✓
SSL	✓	✓
IRC	✓	✓
LPR	✓	×
NFS	✓	×
NTP	✓	✓
NNTP	✓	✓
POP	✓	✓
SMTP	✓	✓
telnet	✓	✓
WAIS	✓	✓
R-Dienste	✓	×
RPC	✓	×
UUCP	✓	×
X11	✓	×
MIME	✓	✓
JAVA	✓	✓
ActiveX	✓	✓

✓– Dienst erlaubt, ◯– Dienst eingeschränkt erlaubt, ×– Dienst gesperrt

- Angriffe aus Interesse (was ist möglich?)

8. Wie erfolgen die Angriffe?

   - Angriffe aus dem Netz
   - Angriff auf der lokalen Maschine

9. Wird der Angriff entdeckt?
   Diese Frage kann nur von dem Administrator der angegriffenen Maschine beantwortet werden. Es gelten die Empfehlungen aus Kapitel 5.1.3.

10. Wie groß ist der Schaden bei einem Einbruch?

    - Kosten für die Wiederherstellung der Ausgangskonfiguration (zeitlicher Aufwand)
    - Umschreiben von z.B. Klausuraufgaben (zeitlicher Aufwand)
    - Vertrauensverlust bei den Nutzern

11. Wie hoch sind die Kosten einer Schutzmaßnahme?
    Die Kosten für eine Schutzmaßnahme setzen sich zusammen aus den Anschaffungskosten für die Hard– und Software, den Kosten für die Installation der Hard– und Software und den Kosten für die Unterhaltung der Anlage sowohl in technischer als auch in administrativer Hinsicht. Der finanzielle und materielle Schaden eines Einbruchs ist gering. Die Kosten für die Lösung sollten daher gering gehalten werden. Die einzelnen Kostenpunkte sind im folgenden genauer aufgeschlüsselt.

    - Kosten für Beschaffung und Installation der Hard– und Software
      Bei Neuanschaffung von Hard– und Software treten hohe Kosten auf.
    - Kosten für Administration der Hard– und Software
      Die Administrationskosten halten sich bei der Universität in Grenzen, da bereits fachkundige Mitarbeiter vorhanden sind, und die Hilfe von Studenten in Anspruch genommen werden kann.
    - Kosten für die technische Unterhaltung der Anlage
      Dieser Punkt ist in einer Universität besonders kritisch, da es vielfach einfacher ist, aus den Geldmitteln neue Hardware zu finanzieren, als Unterhalts-

kosten für ältere Hardware aufzubringen. Die Ursache hierfür ist die Aufteilung der Geldmittel auf verschiedene Haushaltskapitel, zwischen denen nur schwer getauscht werden kann.

12. Habe ich qualifizierte Mitarbeiter für die Sicherheitstechnik?
    In der Universität sind fachlich qualifizierte Mitarbeiter mehrfach vorhanden.

13. Wie hoch dürfen die Einschränkungen für die eigenen Nutzer durch die Sicherheitsmaßnahme sein?
    Die Einschränkungen sollten sich auf ein geringes, nicht bemerkbares Maß beschränken.

14. Wie hoch ist das Sicherheitsbewusstsein bei meinen Mitarbeitern?
    Das Sicherheitsbewusstsein ist bei Studenten im allgemeinen sehr gering. Falls eine Beschränkung des Zugriffs eingeführt wird, muss damit gerechnet werden, dass einige Studenten versuchen werden, diese Mechanismen zu umgehen.
    Bei wissenschaftlichen Mitarbeitern ist das Sicherheitsbewusstsein im allgemeinen höher, allerdings führt eine übermäßige Einschränkung unter Umständen zur Frustration und damit auch zum Versuch der Unterwanderung der Sicherheitsmaßnahmen.

4.4.2 Universität Rostock–Verwaltungsnetz

Bei der Erstellung des Sicherheitskonzeptes wird davon ausgegangen, dass die Bedrohung von ausserhalb des Netzes herrührt. Diese Annahme beruht auf der Tatsache, dass die Verwaltung bereits längere Zeit intern vernetzt ist, und bis jetzt kein Angriff bekannt wurde. Gegen Angriffe von innen helfen nur sichere Passworte und der sorgsame Umgang mit den einzelnen Rechnern.
In einem ersten Schritt sollen den Nutzern nur die notwendigsten Internet–Dienste angeboten werden. Daraus ergeben sich die folgenden Punkte.

1. Von welcher grundlegenden Sicherheitsphilosophie wird ausgegangen?
   Maximale Sicherheit mit Einschränkungen in der Diensteverfügbarkeit
   Es ist alles verboten, was nicht erlaubt ist.

2. Welche Objekte müssen geschützt werden?

- Dateiserver
- Mailserver
- Router
- Workstations
- Datenbanken

3. Wovor müssen die Objekte geschützt werden?

   - Denial–Of–Service Angriffe
   - unberechtigter Zugriff auf persönliche Daten
   - unberechtigter Zugriff auf hochschulinterne Daten
   - Verwüstung der Server

4. Welche Dienste sollen den Nutzern innerhalb und außerhalb des Netzes zur Verfügung stehen und welche müssen gesperrt werden?
   Die Dienste sind in Tabelle 4.3 dargestellt
   Die Spalte „außerhalb“ beschreibt dabei die Regeln bei der Verbindung mit dem Uni–Netz, „innerhalb“ beschreibt hingegen die möglichen Regeln bei der Verbindung der VLANs der Verwaltung untereinander. Da die Verwaltung nur ein VLAN hat, sind die internen Regeln nicht durchsetzbar. Um einen Vergleich mit anderen Netztopologien zuzulassen, ist die Spalte dennoch ausgefüllt. Die Dienste SNMP und TFTP sind teilweise erlaubt, da ein zeitweiliger Zugriff von außen (zum Beispiel zum Einspielen von Softwareupdates direkt vom Hersteller) nötig ist. Die benötigte Verbindung wird exklusiv für den benötigten Zeitraum in die Filtertabelle eingetragen, und die Verbindung wird überwacht.

5. Welche Geschwindigkeitsanforderungen bestehen an den Internet–Zugang?
   Die Forderung an die Geschwindigkeit ist durch die geringe Nutzeranzahl und die benutzten Dienste relativ niedrig.

6. Wer und wo sind die potentiellen Angreifer?

   - Studenten oder Mitarbeiter innerhalb des Universitätsnetzes
   - Angreifer aus dem Internet

Tabelle 4.3: Erlaubte Dienste innerhalb und außerhalb des Netzes (Verwaltung)

Dienst	innerhalb erlaubt	außerhalb erlaubt
DNS	✓	◯
ARP	✓	×
RIP	✓	×
BGP	✓	×
OSPF	✓	×
EIGRP	✓	×
SNMP	✓	◯
hline NIS	✓	×
NIS+	✓	×
ftp	✓	◯
TFTP	✓	◯
FSP	×	×
GOPHER	×	×
HTTP	✓	✓
S–HTTP	✓	✓
SSL	✓	✓
IRC	×	×
LPR	✓	×
NFS	✓	×
NTP	✓	×
NNTP	✓	×
POP	✓	×
SMTP	✓	◯
telnet	✓	×
WAIS	✓	×
R-Dienste	✓	×
RPC	✓	×
UUCP	✓	×
X11	✓	×
MIME	×	×
JAVA	×	×
ActiveX	×	×

✓– Dienst erlaubt, ◯– Dienst eingeschränkt erlaubt, ×– Dienst gesperrt

7. Worin liegt das Interesse der Angreifer?

   - Erlangung von hochschulinternen Daten wie zum Beispiel Immatrukulationsdaten, Ausschreibungsdaten
   - Angriffe aus Interesse (was ist möglich?)

8. Wie erfolgen die Angriffe?

   - Angriffe aus dem Netz

9. Wird der Angriff entdeckt?
   Ein Angriff **muss** entdeckt werden können. Es sind die in Kapitel 5.1.3 beschriebenen Maßnahmen für die Firewall zu treffen.

10. Wie gross ist der Schaden bei einem Einbruch?

    - Kosten für die Wiederherstellung der Ausgangskonfiguration (zeitlicher Aufwand)
    - Benachrichtigung von an Ausschreibungen beteiligten Firmen und damit verbundener Vertrauensverlust
    - Vertrauensverlust bei den Nutzern

11. Wie hoch sind die Kosten einer Schutzmaßnahme?
    Die Kosten für eine Schutzmaßnahme setzen sich zusammen aus den Anschaffungskosten für die Hard– und Software, den Kosten für die Installation der Hard– und Software und den Kosten für die Unterhaltung der Anlage sowohl in technischer als auch in administrativer Hinsicht. Die Kosten für die Unterhaltung der Anlage müssen gering gehalten werden. Gelder für eine einmalige Anschaffung sind leichter zu bekommen.

    - Kosten für Beschaffung und Installation der Hard– und Software
      Bei Neuanschaffung von Hard– und Software treten hohe Kosten auf. Diese können mittels Förderprogrammen abgefangen werden.
    - Kosten für Administration der Hard– und Software
      Die Administration der Anlage wird zum großen Teil vom Rechenzentrum übernommen.

- Kosten für die technische Unterhaltung der Anlage
  Dieser Punkt ist in einer Universität besonders kritisch, da es vielfach einfacher ist, aus den Geldmitteln neue Hardware zu finanzieren, als Unterhaltskosten für ältere Hardware aufzubringen. Die Ursache hierfür ist die Aufteilung der Geldmittel auf verschiedene Haushaltskapitel, zwischen denen nur schwer getauscht werden kann.

12. Habe ich qualifizierte Mitarbeiter für die Sicherheitstechnik?
    In der Universität sind fachlich qualifizierte Mitarbeiter vorhanden. Die Administration sollte aber nicht viel Zeit verlangern.

13. Wie hoch dürfen die Einschränkungen für die eigenen Nutzer durch die Sicherheitsmaßnahme sein?
    Die Einschränkungen sind so hoch, wie es die Sicherheit erfordert.

14. Wie hoch ist das Sicherheitsbewusstsein bei meinen Mitarbeitern?
    Das Sicherheitsbewusstsein ist bei den Mitarbeitern der Verwaltung hoch einzustufen. Einschränkungen im Zugriff auf das Internet werden aus Sicherheitsgründen akzeptiert werden.

Insgesamt kann das Verwaltungsnetz stark gesichert werden. Einbußen in der Performance stellen für die Mitarbeiter kein Problem dar. Die starken Sicherheitsmaßnahmen werden allerdings Spezialisten anlocken, die aus Interesse versuchen werden, in das System einzubrechen. Es müssen von vornherein geeignete Maßnahmen getroffen werden, diese Angriffe zu erkennen.

4.5 Ergänzungen

Bei der Erarbeitung eines Sicherheitskonzeptes wurde davon ausgegangen, dass der Angriff von einem System außerhalb des Netzes kommt. Bei einem Angriff von außen sind die Ziele des Angriffs vorhersagbar und man weiß genau, wo der Angreifer in das Netz eindringt. Bei Angriffen von innen ist sowohl das Ziel als auch der Angriffspunkt unbekannt. Gegen diese Angriffe helfen Firewalls wenig. Hier kommt es besonders auf den sorgsamen Umgang mit den Passworten an. Ein ausreichend langes, sicheres Passwort nutzt wenig, wenn jeder Mitarbeiter im Unternehmen dieses Passwort kennt. Ein sorgsamer und genau festgelegter Umgang mit den Passwörtern ist unumgänglich. Passworte

dürfen **nie** an Dritte weitergegeben werden, auch wenn es noch so dringend ist. Die Mitarbeiter müssen mit dem Thema Sicherheit vertraut gemacht werden. Die bestehenden Sicherheitsrisiken und die Folgen eines sorglosen Umgangs mit sicherheitsrelevanten Information müssen verdeutlicht werden.
Die Benutzung geswitchter Verbindungen innerhalb des Netzwerkes erschwert ein Abhören von bestehenden Verbindungen durch Dritte. Bei den eingesetzten Switches sollte die Möglichkeit bestehen, eine MAC–Adressen basierte Zugriffskontrolle durchzuführen. Diese Kontrolle verhindert den unberechtigten Zugang von Netzwerkclients.

Kapitel 5

Sicherheitsarchitekturen

5.1 Firewall–Architekturen

Bei den derzeit angewandten Firewalls unterscheidet man zwei prinzipielle Konzepte, den Paketfilter und der Applikationsfilter (Proxy). Die Abbildung 5.1 zeigt eine Übersicht über die verschiedenen Konzepte. In Abbildung 5.2 werden die verschiedenen

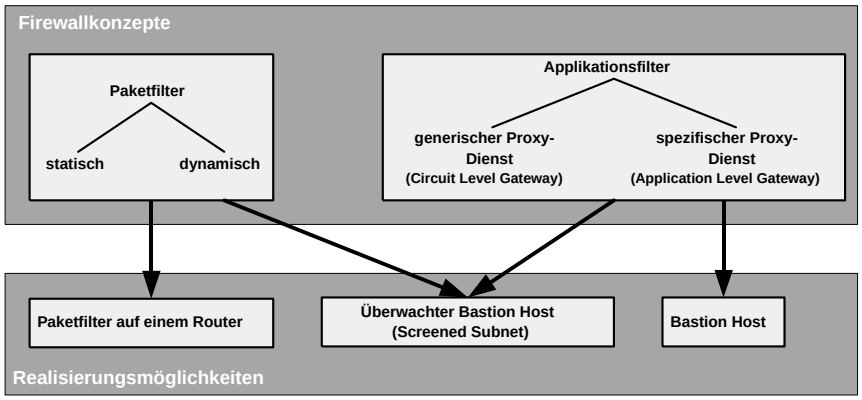


Abbildung 5.1: Firewallkonzepte und deren Realisierungsmöglichkeiten

Konzepte in das ISO/OSI Referenzmodell eingeordnet. Nachfolgend werden die Konzepte erläutert und bewertet. Eine Zusammenfassung ist abschließend in Tabelle 5.1 dargestellt.

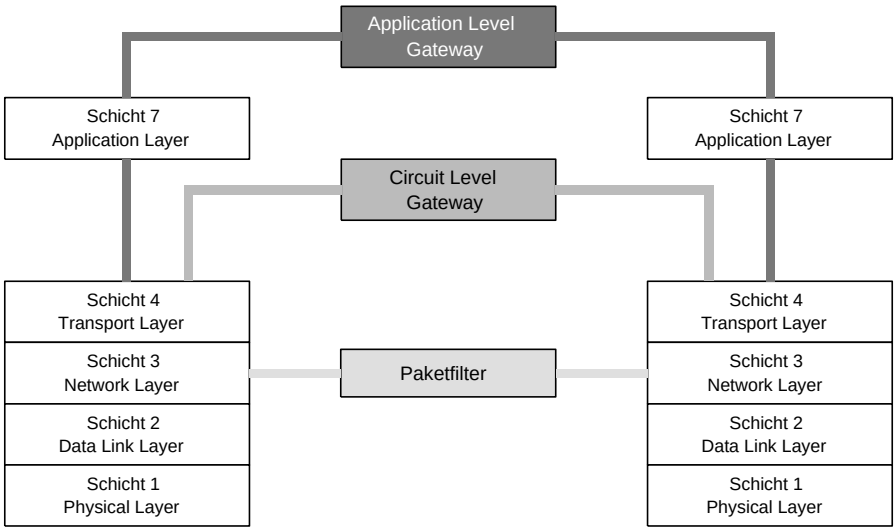


Abbildung 5.2: Einordnung der Firewall–Architekturen [Hab97]

5.1.1 Paketfilter

5.1.1.1 Statische Paketfilter

In der Literatur beschriebene Paketfilter bezeichnen im allgemeinen statische Paketfilter. Da bereits in Routern Paketfilter implementiert sind, stellt dies die preiswerteste Lösung für einen Schutz des eigenen Netzwerkes dar. Paktefilter identifizieren die erlaubten Verbindungen an Hand der Quell- oder Zieladressen sowie der -Ports. Bei statischen Filtern geschieht dies kontextfrei, d.h. nur auf den Inhalt des aktuellen Paketes bezogen. Je nach Art und Konfiguration des Routers erfolgt die Filterung am Eingang und/oder am Ausgang des Routers. In der Konfiguration des Paketfilters werden Positivlisten akzeptabler Maschinen und Dienste sowie Negativlisten von verbotenen Maschinen und Diensten angegeben. Damit sind die Konfigurationsmöglichkeiten auf Adressen und Ports beschränkt. In Abbildung 5.3 ist die Anordnung eines Paketfilters (Router) zu sehen. Ein Router hat mindestens zwei Netzwerkanschlüsse, zwischen denen er vermittelt. Der Paketfilter kann entweder am Punkt (a), am Punkt (b) oder an beiden Punkten im Router installiert werden. Wenn am Ausgang des Routers gefiltert wird, lassen sich Filterentscheidungen mit der Wegewahl koppeln. Problematisch ist in diesem Fall der Verlust der Information, über welchen Port das Paket empfangen wurde. Die Information ist aber wichtig für die Abwehr von Adressfälschungen. IP–Spoofing kann nur von

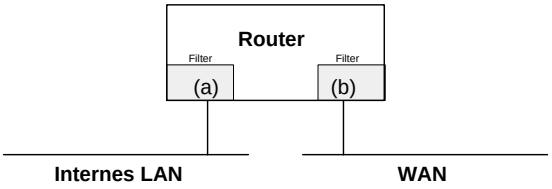


Abbildung 5.3: Router mit Paketfilter

einem Paketfilter verhindert werden, der am Eingang des Routers arbeitet. [BW97]
Für Anwendungen, die auf UDP basieren, sind statische Paketfilter ungeeignet. Da UDP kein Acknowledge–Bit besitzt, kann ein statischer Paketfilter nicht erkennen, ob es sich bei einem UDP–Paket um die Antwort eines externen Servers an einen internen Client handelt, oder ob es eine Anfrage eines externen Clients an einen internen Server ist.

5.1.1.2 Dynamische oder kontextabhängige Paketfilter

Dynamische oder kontextabhängige Paketfilter können Kontext (Verbindungsparameter wie Sequenznummern, Ports, Quell–, Zieladresse, ausgesandte UDP–Pakete, fragmentierte IP–Pakete) auf IP– oder TCP Ebene zwischenspeichern. Dadurch ist es z. Bsp. möglich, nur Antworten auf ausgesandte UDP–Pakete passieren zulassen. Als Antwort werden die Pakete definiert, die von der selben Adresse und dem selben Port kommen, an den das gespeicherte UDP–Paket gesandt wurde. Mittels dieser intelligenten Filter können UDP–Dienste wie zum Beispiel NFS, NIS, RPC granuliert nach Benutzer und Zeit gefiltert werden. Es ist sinnvoll, die Dauer der Kontextspeicherung zu begrenzen. Besteht eine Verbindung über die zeitliche Begrenzung hinaus, so wird sie abgebrochen, bzw. eventuell später eintreffende Pakete werden gefiltert. Ein weiterer Vorteil dynamischer Paketfilter ist die Möglichkeit, fragmentierte Pakete zu Filtern. Die fragmentierten Pakete werden im Router zwischengespeichert, zusammengesetzt und anschließend gefiltert. [BW97]

5.1.2 Applikationsfilter oder Bastion Host

Applikationsfilter ermöglichen die Speicherung protokollabhängiger Informationen auf der Anwendungsebene. Dies geschieht durch Proxy–Dienste auf dem Applikationsfilter. Ist ein Applikationsfilter auf einem sogenannten „multi–homed Host“, das heißt auf

einem Rechner mit 2 oder mehr Netzwerkkarten installiert, so wird dieser Host auch als Bastion–Host bezeichnet, da alle Verbindungen in das externe Netz über ihn führen (Abbildung 5.4). Da der Applikationsfilter Angriffen direkt ausgesetzt ist, sollten die

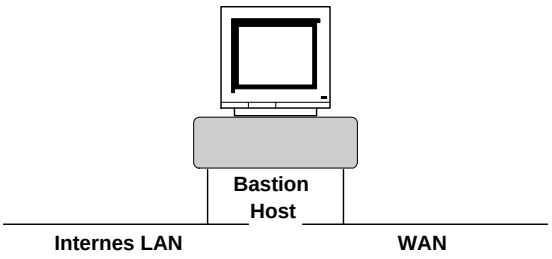


Abbildung 5.4: Bastion–Host

folgenden Sicherheitsvorkehrungen getroffen werden:

- Nach Möglichkeit nur fehlerfreie Software einsetzen
- Nur die notwendigste Software installieren und aktivieren
- Keine Benutzer auf dem Applikationsfilter
- Nur Konsolen– oder Modemzugang.

5.1.2.1 Spezifische Proxy–Dienste

Im Unterschied zum Paketfilter, wo für jedes Paket unabhängig vom Protokoll die selben Filterregeln gelten, ist für jeden angebotenen Dienst über einen Applikationsfilter ein speziell für diesen Dienst entwickelter dedizierter Proxy einzusetzen. Wenn für einen Dienst kein Proxy vorhanden ist, so kann er in den meisten Fällen auch nicht genutzt werden. Dieser Mechanismus ist unflexibel und erschwert die Einführung neuer Technologien.

5.1.2.2 Generische Proxy–Dienste

Wenn für eine gewünschte Anwendung kein dedizierter Proxy existiert, hat man die Möglichkeit, einen generischen Proxy einzusetzen. Dieser arbeitet auf der Transportschicht und wird auch als Circuit–Level–Gateway bezeichnet. Mindestanforderung für

einen generischen Proxy ist ein Satz von Softwarewerkzeugen zur einfachen Konfiguration eines anwendungsspezifischen Proxies. Ein Circuit–Level–Gateway vermittelt zwischen dem Client und dem Server, ohne das Anwendungsprotokoll zu interpretieren. Damit werden dienstespezifische Filterungs– und Protokollmöglichkeiten, wie zum Beispiel das Filtern aktiver Inhalte bei HTTP, nicht zur Verfügung gestellt. Weiterhin sind die Clients bei dem Einsatz von generischen Proxies zu modifizieren, was den Administrationsaufwand in einem Netzwerk erhöht. Der Vorteil eines Circuit–Level Gateways ist die Bereitstellung eines Proxies für unterschiedliche Protokolle.

5.1.3 Überwachter Applikationsfilter (Screened Subnet)

Die Kombination aus Paket– und Applikationsfilter ist der sogenannte überwachte Applikationsfilter (Screened Subnet). Dazu wird einem Applikationsfilter je 1 Paketfilter vor– und nachgeschaltet (Abbildung 5.5).
Eigenschaften des überwachten Applikationsfilters:

- jeglicher Datenverkehr wird über den Applikationsfilter geleitet
- Paketfilter schützen den Applikationsfilter gegen Angriffe aus dem Internet und dem Intranet
- Bei Überwindung des Applikationsfilters steht dem Angreifer noch der interne Paketfilter im Weg
- Die Paketfilter weisen bereits viele Pakete ab, was die Performance des Applikationsfilters erhöht
- Implementation von Diensten wie DNS und SMTP getrennt nach innen und außen, und dadurch Verbergung der inneren Struktur des Netzes möglich

Die Paketfilter sollten grundsätzlich auf anderer Hard– und Software basieren als der Applikationsfilter. Das vermindert das Risiko eines Einbruchs, da anzunehmen ist, dass bei unterschiedlicher Hard– und Software nicht dieselben Sicherheitslücken auftreten. Zusätzlich muss auf der Firewall eine umfangreiche Protokollierung und Überwachung erfolgen, um eventuelle Angriffe sofort entdecken zu können. Hierzu gehört die Überwachung der Änderung an Systemdateien, die Protokollierung sämtlicher Verbindungsversuche und die Abspeicherung sämtlicher Protokolldateien auf einem externen Rechner, der von außen nicht direkt erreichbar ist. Damit werden nachträgliche Änderungen

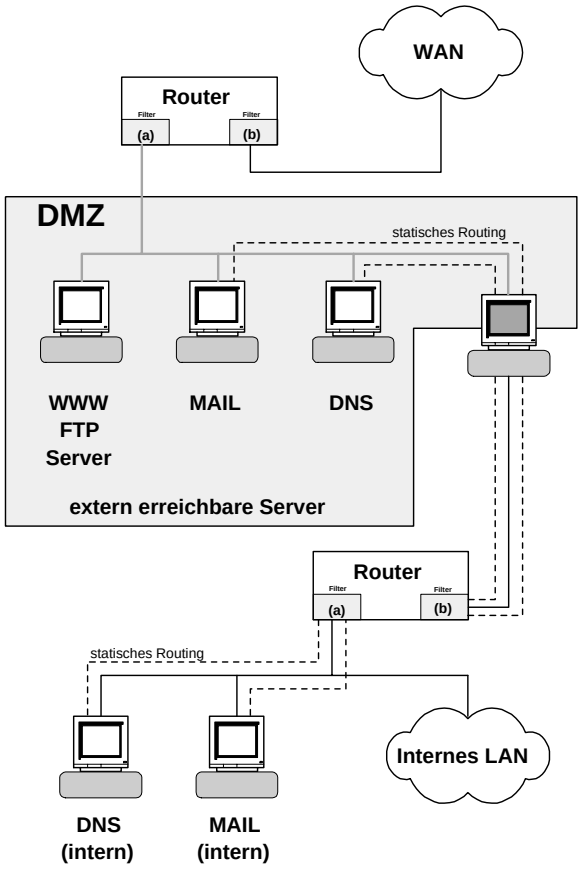


Abbildung 5.5: Überwachter Bastion–Host

an den Protokolldateien unterbunden. Bei einem entdeckten Angriff ist der Administrator sofort auf elektronischem Wege zu benachrichtigen. Dazu gehört die Benachrichtigung per Email auf einen externen und einen internen Server und die Benachrichtigung per SMS auf das Handy.

5.1.4 Vor– und Nachteile der Realisierungsmöglichkeiten

Bei einem Vergleich der Sicherheitskonzepte wird hauptsächlich auf das Verhältnis von Kosten zu Nutzen der Sicherheitslösung geachtet. Paketfilter sind preiswert zu realisieren und haben einen hohen Datendurchsatz, bieten aber einen geringen Schutz des eigenen Netzes vor Angreifern. Applikationsfilter bieten einen größeren Schutz, haben aber einen geringeren Datendurchsatz als ein Paketfilter, und sind als zentraler Punkt selbst angreifbar. Die teuerste, aber auch sicherste Lösung ist eine Kombination aus

Paketfilter und Applikationsfilter. Der Datendurchsatz der Kombination ist der Datendurchsatz des langsamsten Teiles, im allgemeinen des Applikationsfilters. Die einzelnen Vor– und Nachteile der Realisierungsmöglichkeiten sind in Tabelle 5.1 dargestellt.

5.2 ATM–Sicherheitskonzepte

ATM ist als Hochgeschwindigkeitsnetz im Backbone weit verbreitet und hat auch im MAN– und LAN–Bereich an Bedeutung gewonnen. Durch Protokolle, wie zum Beispiel LAN–Emulation, entstehen Sicherheitsrisiken, die bisher keine große Beachtung gefunden haben. ATM bietet andererseits neue Zugriffskontrollmechanismen, die in neue Firewallarchitekturen eingebunden werden können. [BE99]

5.2.1 Angriffsszenarien in ATM–Netzen

Angriffe wenden sich in ATM–Netzen gegen die Vertraulichkeit, Authentizität und Integrität von Daten sowie gegen die Verfügbarkeit des Netzes.

5.2.1.1 Angriffe auf die Vertraulichkeit

Wer die Kontrolle über einen ATM–Switch erlangt, kann diesen so umkonfigurieren, dass der Datenverkehr zu seinem ATM–Anschluss kopiert/umgeleitet wird. Damit erreichen Sniffer–Angriffe eine neue Qualität, da der Angreifer nicht mehr direkten Zugriff auf das physikalische Medium haben muss, um eine Verbindung auszuspionieren. Für den Angrif kann jeder beliebige ATM–Switch auf dem Weg zwischen den Kommunikationspartnern genutzt werden. [BE99]

5.2.1.2 Angriffe auf Authentizität und Integrität

Spoofing–Angriffe können in ATM–Netzen bereits beim Verbindungsaufbau ansetzen. Die beim Verbindungsaufbau ausgesandten Daten, wie zum Beispiel die Absenderadresse, sind nicht authentisiert und können vom Empfänger nicht überprüft werden. Die sich daraus ergebenden Angriffsmöglichkeiten gehen weit über das IP–Spoofing hinaus.
Eine weitere Möglichkeit der Spoofing–Angriffe besteht über das ILMI–Protokoll, welches ein Client benutzt, um seine ATM–Adresse beim Switch zu registrieren. Diese

Tabelle 5.1: Vor– und Nachteile der Firewall–Realisierungsmöglichkeiten [BW97]

Konzept	Vorteil	Nachteil
Paketfiler	- Einfache Handhabung. - Schutz vor IP–Spoofing. - Keine zusätzlichen Anschaffungskosten, da Router paketfilterfähig sind.	- Einschränkung bei Filterregeln auf verbindungsorientierte Verbindungen von innen nach außen mit festen Portnummern. - Keine Einschränkung auf einzelne Benutzer. - Keine Protokollierungsfunktionalität auf Anwendungsebene
Dynamische Paketfilter	- Granulierte Filterung für verbindungs–lose Protokolle und Dienste in Abhängigkeit von z. B. Zeit und Benutzer	- Erhöhter finanzieller Aufwand sowie zeitlicher Aufwand bei der Administration. - Keine Protokollierungsfunktion auf Anwendungsebene
Bastion Host	- Einsatz von Proxies möglich. - Kontextspeicherung möglich. - Benutzerselektion möglich - Zusätzliche Sicherheitsmaßnahmen wie Authentisierung, interaktive Benutzer–nachfrage und Verschlüsselung realisierbar - Protokollierung und Netzüberwachung möglich	- Direkt angreifbar von außen und innen. - Verbergen des inneren Netzes ohne Aufwand nicht möglich - Pro Dienst eigener Proxy notwendig - Geringer Datendurchsatz. - Längere Antwortzeiten - Extra Hardware notwendig (Workstation).
Durch statische Paketfilter überwachter Bastion Host	- Sehr sicher. - Verbergen des inneren Netzes möglich - Bastion Host nicht mehr angreifbar - Internes Netz vor kompromittiertem Bastion Host geschützt	- Erhöhter Ressourcen–Aufwand für Anschaffung, Installation und Wartung - Geringer Datendurchsatz.
Durch dynamische Paketfilter überwachter Bastion Host	- Sehr sicher - Granuliertes Filtern für verbindungslose Protokolle und Dienste in Abhängigkeit von z. B. Zeit und Benutzer schon auf Vermittlungsschicht - Nützlich für kaskadierte Intranets und VPNs mit IPSec	- Erhöhter Ressourcen–Aufwand für Anschaffung, Installation und Wartung. - Geringer Datendurchsatz.

Nachrichten sind ebenfalls nicht authentisiert. Ein Angreifer könnte über ILMI zusätzliche oder fremde Adressen im Switch registrieren, um somit zum Beispiel Filteroptionen zu umgehen. [BE99]

5.2.1.3 Angriffe auf die Verfügbarkeit

Es gibt vielfältige Möglichkeiten von „Denial–of–Service“ Angriffen in ATM–Netzwerken. Zentraler Punkt sind wiederum die ATM–Switche, deren Ausfall die schwer wiegendsten Folgen hat. Die Angriffe können auf folgende Art und Weise stattfinden [BE99]:

- Exzessives Signalisieren
  Die Signalisierung ist in ATM–Switchen häufig ohne spezielle Hardware realisiert und bedeutet somit einen hohen Verarbeitungsaufwand im Switch. Wenn ein Angreifer einen Switch mit Signalisierungen flutet, werden damit andere Teilnehmer im ATM–Netz massiv behindert.
- Aufbrauchen der maximalen Anzahl der virtuellen Verbindungen
  Typische Gerätetreiber für ATM–Schnittstellen ermöglichen nur eine begrenzte Anzahl von virtuellen Verbindungen (z. Bsp. 1024 oder 2048). Durch exzessive Signalisierung kann ein Angreifer diese Anzahl schnell aufbrauchen.
- Reservieren von Betriebsmitteln
- Fremdnutzung der von Dritten reservierten Betriebsmittel
- Manipulation an Zellen
- PNNI–Angriffe

Die aufgeführten Probleme lassen sich größtenteils durch Zugriffskontrollmechanismen (Kapitel 5.2.2) lösen. [BE99]

5.2.2 Zugriffskontrolle in ATM–Netzen

Die nachfolgenden Lösungsvorschläge stammen vom DFN–Firewall–Lab [BE99] und sind keine Standards. Bis jetzt sind keine konkreten Anwendungsfälle dokumentiert oder bekannt geworden.

5.2.2.1 Zugreifbare Informationen bei der Signalisierung

Die SETUP–Nachricht (Kapitel 3.2.1) enthält die meisten Informationen, die eine Firewall–Komponente für die Zugriffskontrolle auswerten kann. Beim Verbindungsaufbau müssen in der SETUP–Nachricht bestimmte IEs angegeben werden. Mit diesen obligatorischen Informationen spezifiziert das ATM-Endgerät die Betriebsmittelanforderungen an das Netz und legt die Empfängeradresse fest. Die an der Signalisierung beteiligten Switches ergänzen gegebenenfalls Informationen über den Weg der virtuellen Verbindung durch das ATM–Netz. Außerdem sind Informationen zur Verarbeitung der Dateneinheiten, die nach dem Verbindungsaufbau über die virtuelle Verbindung übertragen werden sollen, bereits im SETUP vorhanden. Beim Verbindungsaufbau kann angegeben werden, welche Protokolle auf der neuen Verbindung eingesetzt werden sollen. Neben diesen obligatorischen Informationen können weitere Informationen, beispielsweise die Absenderadresse, in der SETUP-Nachricht kodiert werden.
Auf Grundlage der SETUP–Nachricht kann eine Firewall bereits folgende Aktivitäten veranlassen [BE99]:

- **Übermäßige Betriebsmittelanforderung erkennen.**
  Die Firewall–Komponente erkennt anhand des „ATM Traffic Descriptor“ IEs, ob für eine Verbindung zu viele Betriebsmittel reserviert werden. Anhand der „Broadband Bearer Capability“ kann zusätzlich zwischen den Betriebsmittelanforderungen in Abhängigkeit von einer bestimmten Verkehrsklasse unterschieden werden. Beispielsweise ist es für das ATM–Netz weniger kritisch, eine bestimmte Bandbreite an „Unspecified Bit Rate“ (UBR) anzufordern, als durch die Angabe von „Constant Bit Rate“ die gleiche Bandbreite exklusiv zu reservieren.

- **Unerwünschte Zieladressen erkennen.**
  Die „Called Party Number“ (Empfängeradresse) muss beim SETUP angegeben werden, um die Signalisierung durch ein ATM–Netz zu vermitteln. Die Firewall-Komponente kann hierauf Adressfilter anwenden, die bestimmte ATM-Adressen erkennen. Neben dieser Selektion kann bei erkannten Diensten eine Lastverteilung durch Manipulation der Empfangsadresse durchgeführt werden.

- **Kontextinformationen sammeln.**
  Bei einem SETUP für eine Punkt–zu–Mehrpunktverbindung muss die Firewall–Komponente alle benötigten Informationen aus dem SETUP für spätere Auswer-

tungen von ADD_PARTY– und DROP_PARTY–Nachrichten speichern. Bei dieser initialen Signalisierung für eine Punkt–zu–Mehrpunkt–Verbindung werden alle Dienstgüteparameter und „Bearer Capabilities“ für die nachfolgenden ADD_PARTY–Signalisierungen festgelegt.

- **Erzwingen optionaler Informationen.**
  Einige optionale Informationen können unter Sicherheitsgesichtspunkten durchaus erforderlich sein. Eine Firewall–Komponente kann prüfen, ob diese Informationen vom ATM–Endgerät angegeben werden. So ist es beispielsweise denkbar, die Angabe der optionalen Absenderadresse durch den Firewall zu erzwingen.

5.2.2.2 Signalisierungskontroller für richtlinienbasierte Zugriffskontrolle

Die im vorigen Abschnitt beschriebenen Zugriffskontrollen gehen weit über die bisher in ATM–Switchen implementierten hinaus. Auf Basis einer Zugriffskontrolle bei der Etablierung einer Verbindung wird eine neue Firewallkomponente eingeführt, der Signalisierungskontroller. [BE99] Nachfolgend werden die wichtigsten Szenerien einer Kontrolle der ATM–Signalisierung vorgestellt.

Ablehnung des Verbindungsaufbaus

Die SETUP–Nachricht wird vom Signalisierungskontroller abgefangen und nach Auswertung nicht weitergeleitet. Statt dessen wird ein RELEASE_COMPLETE an den Initiator der Verbindung zurückgesandt.

Selektive Ablehnung bestimmter Empfänger

Bei einer Punkt–zu–Mehrpunkt–Verbindung gibt es ein zusätzliches Szenario für die Ablehnung einer Verbindung.
In der ersten Phase (Herstellung einer virtuellen Verbindung zum ersten Teilnehmer) verläuft die Signalisierung wie im vorher genannten Beispiel. Zusätzlich kann in der 2. Phase (Ansprechen weiterer Empfänger) verhindert werden, dass bestimmte Teilnehmer mit der ADD_PARTY–Nachricht an der Kommunikation teilnehmen können.
Durch eine Ablehnung einer Verbindungsetablierung in der zweiten Phase wird die Punkt–zu–Mehrpunkt–Verbindung nicht abgebrochen.

Verdrängen von Verbindungen bei priorisierter Signalisierung

In typischen ATM–Netzen ist die Vergabe der Ressourcen nach dem Prinzip „First Come – First Serve“ geregelt. Im einfachsten Fall kann eine einzige Verbindung sämtliche Ressourcen belegen. Diese Strategie ist in vielen Produktionsnetzen inakzeptabel. Ähnlich den hochpriorisierten Prozessen bei Betriebssystemen kann ein Signalisierungskontroller für die Priorisierung wichtiger Verbindungen eingesetzt werden. Etablierte Verbindungen mit niedriger Priorität werden dabei zugunsten von Verbindungen mit hoher Priorität abgebaut. Denkbar ist zum Beispiel die Bevorzugung von Telofongesprächen gegenüber Videoübertragungen und die Priorisierung interner Datenübertragung gegenüber der externen Datenübertragung. Zur Durchführung der Priorisierung ist es notwendig, auf Basis der Informationselemente in der SETUP–Nachricht Prioritätsklassen zu definieren. Diese bilden die Basis für die Entscheidungen des Signalisierungskontrollers.
[BE99]

5.2.2.3 Weitergehende Zugriffskontrollkonzepte auf Basis des Signalisierungskontrollers

Im vorhergehenden Abschnitt agierte der Signalisierungskontroller im wesentlichen als Filter, der auf Grund der in der Signalisierungsnachricht vorhandenen Information die Nachricht entweder abfängt oder weiterleitet. Darüber hinaus gibt es erweiterte Ansätze, in denen der Signalisierungskontroller gezielt Informationselemente der Signalisierungsnachrichten verändert, um Sicherheitsrichtlinien durchzusetzen. [BE99]

Einschleifen von Sicherheitskomponenten

Das Einschleifen von Sicherheitskomponenten (Abbildung 5.6) kann ohne Änderung der PNNI–Nachricht erfolgen, wenn vom Signalisierungskontroller der Aufbau einer virtuellen Verbindung zur Sicherheitskomponente und wieder zurück veranlasst werden kann. Da der Signalisierungskontroller am Anfang und am Ende des Weges steht, kann der Umweg vor anderen Switches verborgen werden. [BE99]

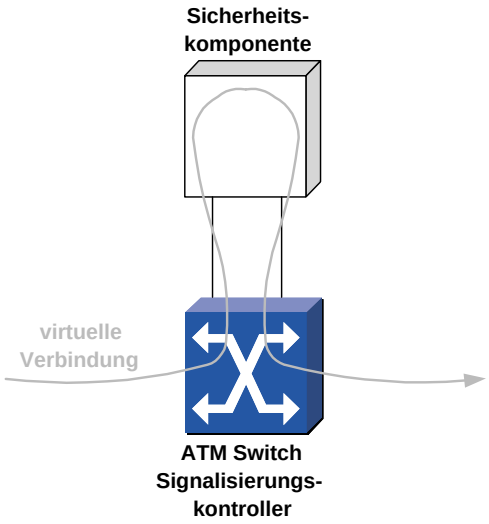


Abbildung 5.6: „Einschleifen“ einer Sicherheitskompnente durch den Signalisierungskontroller [BE99]

Einfügen von Sicherheitskomponenten durch Ersetzen der Empfängeradresse

Ein Signalisierungskontroller kann durch Änderung der Empfänger–Adresse („Called Party Number“) in einer SETUP–Nachricht erreichen, dass eine Sicherheitskomponente direkt angesprochen wird. Das die Verbindung initiierende ATM–Gerät bemerkt die Veränderung nicht, da bei der CONNECT–Nachricht keine Adressen der beteiligten Systeme mehr verwendet werden. Ohne Änderungen in der Signalisierung würde hierbei allerdings die Adresse des ursprünglichen Empfängers verloren gehen. Zur Vermeidung dieses Umstandes hat der Signalisierungskontroller drei Möglichkeiten [BE99]:

- Transport der Information in zusätzlichen Informationselementen der SETUP–Nachricht an die Sicherheitskomponente
- Benutzung des bereits spezifizierten Informationselementes der „Called Party Subaddress“, in dem normalerweise die Empfängeradresse übertragen wird, wenn beim Verbindungsaufbau über ein öfentliches Netz E.164–Adressen verwendet werden und die Adresse des gewünschten Empfängers nach einem anderen Schema vergeben wurde. Die Benutzung dieses Feldes ist nur möglich, wenn dieses IE nicht bereits für die Adressierung der Sicherheitskomponente benötigt wird
- Senden der Informationen über eine eigene Verbindung vom Signalisierungskon-

troller zur Sicherheitskomponente. Dies ist sinnvoll, da über diese Verbindung andere notwendige Informationen (Lastinformationen, Anweisungen) mit ausgetauscht werden können.

Einfügen von Sicherheitskomponenten durch Ergänzung der DTL

PNNI legt mit einer „Designated Transit List“ (DTL) den Pfad zum Empfänger fest. Eine DTL wird bereits von dem Switch erzeugt, an den das die Verbindung eröffnende Gerät angeschlossen ist. Der Signalsierungskontroller verändert die PNNI–Nachrichten dahingehend, dass die DTL die Sicherheitskomponente enthält. Die normale Verarbeitung der DTL resultiert dann in einem Pfad, der über die Sicherheitskomponente führt. Dabei ist es nicht mehr zwingend notwendig, dass der Pfad von der Sicherheitskomponente wieder zum Signalisierungskontroller zurückführt. [BE99]

5.2.2.4 Virtuelle Netze

Der Einsatz von Signalisierungskontrollern ermöglicht das Einrichten mehrerer virtueller Netze auf demselben ATM–Netz. Durch den Einsatz von Signalisierungskontrollern auf jedem Switch des internen Netzes können Systeme nach Sicherheitsanforderungen gruppiert und in jeweils eigenen virtuellen Netzen zusammengeschlossen werden. Die Konfigurierung der virtuellen Netze ist unabhängig von der physischen Verkabelung in einem Netzwerk. Über einen Signalisierungskontroller kann festgelegt werden, zwischen welchen ATM–Adressen virtuelle Verbindungen aufgebaut werden dürfen. Da die Filterregeln auf ATM–Adressen basieren, besteht grundsätzlich die Gefahr durch „Spoofing“–Angriffe. Wenn die Kontrolle des Signalisierungskontrollers jedoch innerhalb eines jeden Switches erfolgt, kann der Versuch eines Endgerätes, eine ATM–Adresse zu fälschen, bereits von dem Switch erkannt werden, an dem der Angreifer angeschlossen ist.
Das Konzept der virtuellen Netze ist für alle ATM–basierten Protokolle einsetzbar.
Die Konfiguration der Filterregeln ist sehr aufwendig und fehleranfällig. Die Unterstützung durch automatisierte Verfahren zur Verteilung der Filterregeln auf verschiedene Switche eines Netzes ist daher zwingend notwendig. [BE99]

5.2.2.5 Verbinden virtueller Netze über Firewalls

Die Verbindung mehrerer virtueller Netze mit unterschiedlichen Sicherheitsanforderungen erfolgt, wie bei herrkömmlichen Netzen, über eine Firewall. Der Vorteil bei der Konzeption virtueller Netze besteht darin, dass für den Einsatz mehrerer Firewalls im internen Netz die bestehende Verkabelung nicht geändert werden muss. Die Firewall befindet sich nicht mehr am Übergang vom öffentlichen zum internen Netz, sondern am Übergang von einem virtuellen Netz zum anderen. Eine solche Konfiguration sichert das Netzwerk nicht nur gegen Angriffe aus dem öffentlichen Netz, sondern auch gegen Angriffe aus anderen internen Teilnetzen. [BE99]

Dezentrale Firewalls

Vorteile	**Nachteile**
– Schutz vor kompromittierter Firewall	– schlechte Performance durch Überqueren mehrerer Firewalls – keine nennenswerte Erhöhung der Sicherheit – mehrfache Konfiguration unterschiedlicher Firewalls

Zentrale Firewalls

Vorteile	**Nachteile**
– Konfiguration nur an zentraler Stelle erforderlich	– Darstellung eines „Single Point Of Failure“– eines zentralen Fehler– und Angriffspunktes
– Es muss maximal eine Firewall überquert werden	– Aufteilung in virtuelle Netze bringt bei einem erfolgreichen Angriff keine Vorteile mehr

Virtuell zentraler Firewall

Vorteile

- Lastverteilung auf mehrere replizierte Komponenten, die nicht an zentraler Stelle plaziert sein müssen und die durch die Signalisierungskontroller eingebunden werden
- Vermeidung unnötiger Umwege, da die Kommunikation zwischen räumlich benachbarten Systemen nicht zwangsläufig über die zentrale Firewall führen muss

Nachteile

- wie beim Zentralen Firewall

[BE99]

Kapitel 6

Sicherheitsprodukte

Es gibt inzwischen eine Vielzahl von Firewall–Produkten auf dem Markt. Diese werden in reine Softwareprodukte und in kombinierte Soft–/Hardware Produkte unterschieden. Speziell für kleinere Unternehmen sind freie Softwareprodukte, die zum Beispiel für Linux angeboten werden, in Zusammenhang mit den preiswerten PC–Kosten eine Alternative für den Kauf einer Komplettkonfiguration. Nachteilig ist die anspruchsvolle Konfiguration der Software, die von Fachunkundigen nur schwierig durchzuführen ist. Eine Alternative sind die angebotenen Komplettprodukte, die sowohl Hard– als auch Software beinhalten. Diese sind meist einfacher zu konfigurieren, bzw. werden mit Hersteller– bzw. Konfigurationssupport angeboten. Nachfolgend werden einige Produkte genauer betrachtet. Ein Test ausgewählter Firewall–Produkte ist in [BW97] durchgeführt worden. Eine Übersicht über die vorgestellten Firewall Produkte gibt Tabelle 6.1

6.1 Software–Produkte

6.1.1 Checkpoint FireWall–1

Checkpoint ist Marktführer im Bereich der Firewallprodukte. FireWall–1 ist ein Softwareprodukt, das für unterschiedliche Plattformen (x86, SPARC, PowerPC) und unterschiedliche Betriebssysteme (HP–UX, IBM–AIX, Solaris, WindowsNT) angeboten wird. Die Checkpoint Firwall–1 Software staffelt sich in verschiedene Produkte und Zusatzmodule, wodurch eine höchstmögliche Flexibilität auch in wachsenden Umgebungen erreicht wird. [Che00]
Komponenten der FireWall–1:

Internet Gateway

Für Netzwerke bis zu 25, 50, 100, 250 IP–Adressen.
Es enthält das FireWall–1 Modul und die Management–Konsole, die auf dem Gateway selbst installiert werden müssen. Der Remote–Zugriff auf die Management–Konsole per mitgelieferten GUI ist möglich. FireWall–1 ist ein Applikationsfilter mit zentralem Management, Zugriffskontrolle, Client/Session/User authentication, NAT, Auditing, und Content–Security Unterstützung. In Zusammenarbeit mit einem VPN–Produkt der Firma Checkpoint können sichere VPNs aufgebaut werden. Diese sind mit DES, Triple-DES oder IPSec/IKE abgesichert.
Zu einem FireWall–1 Modul gehören ein „Inspection Modul“ genannter dynamischer Paketfilter, sogenannte Security–Server für HTTP, FTP, TELNET, RLOGIN und SMTP, ein Graphical User Interface und ein Management Server.
FireWall–1 Inspection Modul
Jedes einkommende Paket wird auf Einhaltung der Security–Policies kontrolliert, bevor es weiter verarbeitet wird. Für den Fall, dass eine Kontrolle des Datenteils des Paketes benötigt wird, kann das Inspection Modul dieses Paket an einen der Security–Server weiterleiten.
Security–Server
Der Security–Server gliedert sich in Authentifizierung und Content–Security. Authentifizierung gibt es für Verbindungen über HTTP, FTP, TELNET, und RLOGIN. Das Inspection–Modul gibt dafür das Paket an den Security–Server weiter. Dieser führt die Authentifizierung durch und gibt, falls die Authentifizierung erfolgreich war, die Verbindung frei. Der Inhalt einer Verbindung kann mit Content–Security überprüft werden. Zu dieser Überprüfung gehören Adressfilterung, Befehlsüberprüfung, Anit–Virus Inspektion und Java/ActiveX Filterung. Das Firewall–Modul beinhaltet Content–Security für HTTP, FTP und SMTP. Der Security–Server arbeitet prinzipiell als Proxy für die angebotenen Dienste. Im Unterschied zu anderen Proxies muss der Client allerdings keine extra Verbindung zum Proxy aufbauen. Die Umleitung des Datenstroms wird vom Inspection Modul der FireWall–1 übernommen. Die Verbindung wird dabei aufgetrennt und ein Umweg über den Security–Server eingeschleust. Diese Umleitung wird von keinem der beiden Kommunikationspartner bemerkt. Im Verlaufe der Überprüfung kann der Security Server einen extenen Proxy–Server für die Filterung der Pakete einbinden. Die URL–Filterung und das Viren–Scanning werden durch Produkte anderer

Herrsteller übernommen. Hierfür stehen definierte Schnittstellen und Funktionsaufrufe zur Verfügung, mit den der jeweilige Security Server den externen Server (Proxy) kontaktieren kann. Diese Schnittstellen (APIs) können dazu benutzt werden, zusätzliche Applikationen in die Benutzung der Content–Security einzubinden (zum Beispiel X11). Mit Benutzung der APIs wird sichergestellt, dass sich alle Komponenten der Firewall zentral konfigurieren lassen.

Enterprise Center

Zentrales Management beliebig vieler FireWall–1 Module mittels der Enterprise Security Console und Unterstützung einer unbegrenzten Anzahl interner IP–Adressen mit dem FireWall–1 Modul unlimited. Die Konsole kann auf einem separatem Rechner installiert werden und als zentrale Management–Station für die FireWall–1 Module fungieren. Das Enterprise Center enthält ein FireWall–1 Modul unlimited mit den unter `Internet Gateway` genannten Funktionen.

Networking Security Center

Das `Networking Security Center` ist ein um die `unlimited Open Security Section` erweitertes `Enterprise Center unlimited`. Die `Open Security Extension` ermöglicht das Managen von Drittprodukten (Paketfilter und Access Listen), wie Cisco–, Bay– und 3Com Router Access Listen, Cisco PIX Firewall und Microsoft Steelhead Router Firewall, von der Management–Konsole der FireWall–1 aus. Durch das zentrale Management erfolgt eine Aufwands– und Fehlerreduktion in der Konfiguration der Komponenten eines Firewall Systems.

Enterprise Security Console

Die bereits unter `Enterprise Center` genannte `Enterprise Security Console` ist nur die zentrale Management Konsole und wird hier ohne FireWall–1 Module ausgeliefert.

FireWall Encryption Modul

Die `Checkpoint Encryption Services` ermöglichen eine sichere Datenkommunikation über das Internet, garantieren Datenschutz und ermöglichen Echtheitszerti-

fikate und Vollständigkeit.

6.1.2 Raptor Firewall

Die `Raptor` Firewall von Axent Technologies ist aus dem Produkt Eagle–Firewall der Firma Raptor Systems hervorgegangen. Mit der `Raptor` erwirbt man ein Softwareprodukt, das auf den Betriebssystemen WindowsNT oder Solaris basiert. Es beinhaltet einen Applikationsfilter, der sich gut für den Einsatz in einem Screened Subnet eignet, und eine komfortable Management–Konsole. Auf dem Applikationsfilter können mehrere dedizierte Proxies für die unterschiedlichsten Dienste eingesetzt werden. Wenn für einen Dienst kein spezifischer Proxy existiert, so kann ein generischer Proxy die Filterung und Weiterleitung dieses Dienstes übernehmen. Die folgenden Dienste werden von der Firewall unterstützt [Axe00]:

- Support for Microsoft LAN Manager file and printer sharing services
- SQL*Net
- Telnet
- FTP
- SMTP - Secure e-mail
- HTTP-Enhanced with support for ratings, and HTTP v1.1 features including connection persistency and request pipelining.
- HTTP-FTP
- HTTP-Gopher
- HTTP-HTTPs
- H.323–Voice–Over–IP
- Ping (ICMP)
- NNTP-News service with ratings support
- Java filtering-Using optional third-party application

- Gopher+ - with URL ratings support
- RealAudio® and RealVideo®
- DNS - graphically configurable name server with built-in support for split-DNS
- NTP (Network Time Protocol)

Weiterhin erlaubt die Firewall Authentifizierung, NAT, Nutzung von IPSec/IKE und den Aufbau von VPNs.

6.1.3 Gauntlet Internet Firewall

Die `Gauntlet Internet Firewall` ist ein ursprüngliches Produkt der Firma Trusted Information Systems, die auch das unter Kapitel 6.1.5 vorgestellte Produkt `Firewall Toolkit` entwickelt hat. Nach der Übernahme des Produktes von Network Associates wird es dort weiterentwickelt und vertrieben. `Gauntlet` ist eine Erweiterung des `Firewall Toolkit`. Das Produkt beinhaltet eine komplette Firewall–Lösung mit integrierter VPN Funktionalität und integriertem McAffee Virenscanning. Es ist verfügbar für die Betriebssysteme Solaris, HP–UX, und WindowsNT. Die nachfolgenden Dienste werden auf der Firewall angeboten [Net00]:

- TELNET–, Rlogin–, FTP–, HTTP–, GOPHER–, SMTP–, NNTP–, RSH–, SQL Proxy
- Generischer Proxy
- X11 Gateway
- JAVA Guard
- Secure Server(FTP, HTTP), SHTTP, SSL
- E-mail Gateway
- URL–Screening (URL–Filter)
- DNS–Server
- RealAudio® Support

- integrierte McAffee Virus–Scanning Maschine
- VPNs mit IPSec/IKE
- Multiprozessor Support

Ähnlich der Checkpoint FireWall–1 gibt es eine zentrale Managementkonsole, die Komponenten anderer Hersteller in die zentrale Sicherheitskonfiguration einbeziehen kann.

6.1.4 Linux–Firewall

Linux ist ein im Quellcode verfügbares Betriebssystem, an dem Entwickler aus der ganzen Welt arbeiten. Es ist das am besten dokumentierte und getestete Betriebssystem, das auf dem Markt erhältlich ist. Damit erfüllt sich eine Anforderung an eine Firewall, die von keiner anderen kommerziellen Lösung erreicht wird, die Forderung nach umfangreicher Dokumentation des Quellcodes jedes auf der Firewall eingesetzten Programmes. Die Programmteile der Firewall selbst sind ebenfalls im Quellcode verfügbar. Der Aufbau einer Firewall ist unter Nutzung eines PC und Linux als Betriebssystems mit geringen finanziellen Mitteln möglich.
Verfügbare Dienste sind:

- Paketfilter
  Im Kernel enthalten, Konfiguration mit `ipchains`
- generische Proxies
  socks
- spezifische Proxies
  - TIS FWTK
    Das leistungsfähigste frei verfügbare Firewallpaket (Kapitel 6.1.5)
  - Apache HTTP
    Ein HTTP Server und Proxy
  - SQUID Proxy
    Ein Proxy für HTTP, FTP, GOPHER, SSL und WAIS
- NAT
  Network Address Translation, IP–Masquerading

6.1.5 TIS–Firewall Toolkit

Das Firewall Toolkit der Firma Trusted Information Systems (TIS) ist eine im Quellcode frei erhältliche Sammlung von Dienstprogrammen zum Aufbau einer eigenen Firewall. Das Toolkit ist für Unix–Betriebssysteme, die TCP/IP mit Berkeley Socket unterstützen, erhältlich. Der Einsatz mit dem freien Betriebssystem Linux ist dabei besonders hervorzuheben. Das Toolkit geht dabei weit über die mit Linux erhältlichen Firewall–Komponenten hinaus. Das Paket enthält Proxies für `Telnet, FTP, Rlogin, SMTP-Mail, HTTP, Gopher, X11` und ein `plug-gw`, das als transparenter Proxy für viele TCP–Dienste einsetzbar ist. Zusätzlich enthalten sind die Programme `netacl` für die Zugriffskontrolle auf Layer 3 und `authsrv` zur Netzwerkauthentisierung. [Tru00]

6.2 Hard– und Software–Produkte

6.2.1 Cisco Secure PIX Firewall Series

Cisco bietet mit seiner PIX–Firewall Serie eine Komplettlösung an. Diese besteht aus einem Rechner im 19 Zoll Gehäuse und der dazugehörigen Firewall Software, die von Cisco entwickelt wurde. Im Gegensatz zu den meisten anderen Firewall–Lösungen, die Unix als Betriebssystem nutzen, setzt die Cisco Software auf ein eigenes rudimentäres Betriebssystem auf. Dieses ist mit nur minimalen Funktionen ausgestattet und damit sicherer als ein aus vielen Zeilen Quellcode bestehendes Betriebssystem. Das Betriebssystem ist für den Einsatz als Firewall optimiert, was die Performance zusätzlich erhöht. Kernstücke der PIX Firewall sind ein „Cut–Through Proxy“, der die Authentifizierung und Autorisierung der Benutzer im laufenden Betrieb vornimmt, und der Adaptive Security Algorithm, der einen dynamischen Paketfilter darstellt. Die Management Konsole ist JAVA–basiert und unterstützt das zentrale Management aller Cisco PIX in einem Netzwerk. [Cis00]

Adaptive Security Algorithm (ASA)

ASA basiert auf der IP–Quell– und –Zieladresse, den zufälligen TCP Sequenz Nummern, TCP Port Nummern und zusätzlichen TCP Flags in jedem Paket. Alle ankommenden und ausgehenden Pakete werden mit den Einträgen in der Verbindungstabelle

verglichen.

Cut–Through Proxy

Anders als ein Proxy Server, der jedes Datenpaket einer Verbindung auf Anwendungsebene analysiert, sendet die PIX Firewall zunächst eine Anfrage an eine TACACS+ oder RADIUS Datenbank. Wenn die Verbindung authorisiert und mit der Sicherheitspolitik vereinbar ist, werden die jetzigen und nachfolgenden Datenpakete dieser Verbindung ohne weitere Überprüfung übertragen. Diese Prozedur erhöht den Datendurchsatz erheblich, da nicht jedes Paket überprüft werden muss. Die Daten der Verbindung werden, wie bei dynamischen Paketfiltern üblich, zwischengespeichert, und nachfolgende Pakete daran identifiziert.

6.2.2 Kryptokom: KryptoWall

Die `KryptoWall` der Firma Kryptokom besteht aus den Komponenten Bastion–Host, zwei KryptoGuard LAN–Boxen(Beinhalten die Paketfilter), Information Server und Security Management. Die Komponenten realisieren das Konzept eines Screened Subnet. [Kry00]

Bastion–Host

Der Bastion Host besteht aus einer Unix basierten Workstation mit zwei Netzwerkanschlüssen. Auf dem Bastion–Host ist ein Applikationsfilter installiert, der wiederum für jeden benötigten Dienst einen Proxy bereitstellt. Angebotene Proxies sind zum Beispiel für `Telnet, FTP, SMTP-Mail, HTTP, WAIS` verfügbar. Zusätzlich gibt es einen generischen Proxy, der an zukünftige Anwendungen angepasst werden kann.

KryptoGuard LAN–Boxen

Mit den LAN–Boxen kann eine Verschlüsselung mit dem DES–Algorithmus mit maximal 112 Bit in Hardware realisiert werden. Zusätzlich ist in den LAN–Boxen ein Paketfilter implementiert. Die Filterregeln werden so definiert, dass jede IP–Verbindung von innen und außen über den Bastion–Host führt. Einzige Ausnahme bilden DNS– und Informationsanfragen aus dem unsicheren äußeren Netz. Diese Anfragen werden direkt

zum Informationsserver geroutet. Der Paketfilter kontrolliert die Pakete nach Diensten/Portnummern (TCP und UDP) und ob der Zugriff in einem definierten Zeitraum durchgeführt wird. Darüberhinaus wird der Bastion–Host vor fragmentierten Paketen geschützt. Ein Verstoß gegen die in der Access Liste definierten Regeln wird protokolliert und, wenn definiert, eine sofortige Meldung an das Management gesendet.

Information Server

Informationen, die öffentlich zugänglich sein sollen, können auf einem (oder mehreren) Information Server dem Nutzer aus dem INTERNET zur Verfügung gestellt werden. Dieser Information Server befindet sich in der DMZ zwischen Bastion–Host und dem äußeren Paketfilter. Für Teilnehmer aus dem unsicheren Netz können auf FTP–, WWW–, NNTP(News)–, Mail– und Nameservern Daten zur Verfügung gestellt werden. Die Zugänge zu den Diensten des Information Servers werden durch den äußeren Paketfilter kontrolliert.

Security Management Station

Mit Hilfe des Security Managements werden die Zugangskontroll–Tabellen verwaltet und in die LAN–Boxen sowie den Bastion–Host geladen. Die Logbücher der Paketfilter und des Bastion–Hosts können gelesen und ausgewertet werden. Das Security Management versorgt die Komponenten mit sicherheitsrelevanten Informationen wie zum Beispiel Schlüsseln. Die Kommunikation erfolgt dabei über einen kryptografisch sicheren Kanal.

6.3 Überblick

Tabelle 6.1 gibt einen Überblick über die vorgestellten Firewall–Produkte. Die Informationen hierzu wurden aus Testszenarien und Internetveröffentlichungen gewonnen. Technisch relevante Informationen sind auf den Internetseiten der Firmen schwer erhältlich.
Für das in Kapitel 5.5 vorgestellte Konzept des Screened Subnet eignet sich aus Sicherheits– und Performance Gründen die Kombination von der Checkpoint FireWall–1 mit mehreren externen Proxies (z. Bsp. auf der Gauntlet–Firewall) als Applikationsfilter, und die vorhandenen Router als Paketfilter. Diese Lösung hat den Vorteil, dass sie für

Tabelle 6.1: Übersicht über die Firewall Produkte

	Checkpoint	Raptor	Gauntlet	Linux	FWTK	Cisco PIX	Krypto Wall
Produktart	Software	Software	Software	Software	Software	Soft+Hardware	Soft+Hardware
stat. Paketfilter				X	X [4]		
dyn. Paketfilter	X					X	X
gen. Proxy	X	X	X	[2]	X	X [3]	X
spez. Proxy	für HTTP, FTP, SMTP [1]	Telnet, HTTP, FTP, SMTP, Real Audio/ Video, Gopher, SQL, VOIP	Telnet, HTTP, FTP, SMTP, Real Audio/ Video, Gopher, SQL, RSH, Rlogin, NNTP	[2]	Telnet, HTTP, FTP, SMTP, Gopher, Rlogin	-	Telnet, FTP, SMTP, HTTP, WAIS
X11	generisch	generisch	X11-Gateway	[2]	X11-Gateway	generisch	generisch
Management-konsole	X	X	X	[2]	-	X	X
Management von Fremdprodukten	mit der Komponente Networking Security Center	-	im Softwarepaket enthalten	[2]	-	-	-
Virus Scanning	nein	nein	integrierte McAffee Scan Maschine	[2]	nein	nein	nein
Verschlüsselung	**Nur mit Firewall-Encryption Modul** IPSec, TLS, 3DES, DES, SSL, RSA, MD-5, SHA-1	IPSec, SSL, TLS, S-HTTP, HTTPS	IPSec, SSL, TLS, S-HTTP, HTTPS, S-MIME, PGP, DES, 3DES	[2]	-	IPSec, SSL,	IPSec, DES, 3DES, Keyed MD5, SSL, SHTTP, HTTPS
Betriebssystem	HP-UX, IBM-AIX, Solaris, WindowsNT	HP-UX, Solaris, Sinix, WindowsNT	WindowsNT, Unix	Linux	Unix-System mit Berkeley Socket, z. B. Linux	eigener Betriebssystem-kernel	eigenes Betriebssystem
transparenter Betrieb	ja	nein	nein	[2]	nein	ja	nein

[1] kein Proxy im herrkömmlichen Sinne , [2] abhängig von der eingesetzten Software , [3] Cut-Through Proxy

[4] im Linux-Kernel enthalten

die Kommunikationspartner transparent ist, und eine Änderung in den Anwendungsprogrammmen nicht notwendig ist. In der Konfiguration der Adressumsetzung kann ausgewählt werden, ob der externe Kommunikationspartner die IP–Adresse des Applikationsfilters, die originale IP–Adresse des Absenders oder eine IP–Adresse aus dem Adressenpool der NAT als Rücksendeadresse erhält.
Für eine Lösung, die ausschließlich aus einem Paketfilter besteht, ist die Cisco Secure PIX Firewall wegen der hohen Anzahl möglicher Verbindungen und des Datendurchsatzes die optimale Wahl.

Kapitel 7

Lösungskonzept am Beispiel der Universität Rostock

7.1 Stand des Auf– und Ausbaus des Universitätsnetzes

Das RUN wurde in den Jahren 1996/1997 auf der „grünen Wiese“ errichtet. Die Basis bildet ein ATM–Backbone, der mit jeweils 155 Mbit/s zwischen den Standorten ausgebaut ist. Die örtlichen Ethernet–Switche sind über einen ATM–Uplink an diesen Backbone angeschlossen. Für die Übertragung der Ethernet–Pakete über ATM wird der ATM–Dienst LAN–Emulation benutzt. Dieser Aufbau ermöglicht eine flexible Gestaltung der einzelnen Subnetze, da jedem Port auf einem Switch ein anderes Subnetz zugeordnet werden kann. Der Aufbau verteilter Arbeitsgruppen ist somit ohne Probleme möglich. Der Anschluss an das B-WIN erfolgt derzeit mit 65 Mbit/s über einen 155 Mbit/s Link. Geplant ist, im Jahr 2000 den Anschluss zum neuen G-WIN herzustellen. Dieser ermöglicht Übertragungsraten bis 2,5 Gbit/s auf Basis der IP over SONET Technologie. ATM–Dienste werden in Zukunft vom DFN nur auf Anforderung zur Verfügung gestellt. Mit dieser Entwicklung müssen alle Überlegungen, die in früheren Arbeiten, zum Beispiel zur Übertragung von Ferngesprächen über das ATM–Netz, neu getätigt werden. Insgesamt wird ATM auch im Backbone–Bereich durch Gigabit–Ethernet aus Kostengründen verdrängt. Nachteil dieser Entwicklung ist die Verringerung der Flexibilität in dem Aufbau der Subnetze. Das Universitätsnetz teilt sich in 3 Bereiche, das Hochschul–(Wissenschafts–) Netz, das Verwaltungsnetz und das Medizinnetz. Der derzeitige logische Aufbau des Universitätsnetzes ist in Abbildung 7.1 dargestellt.

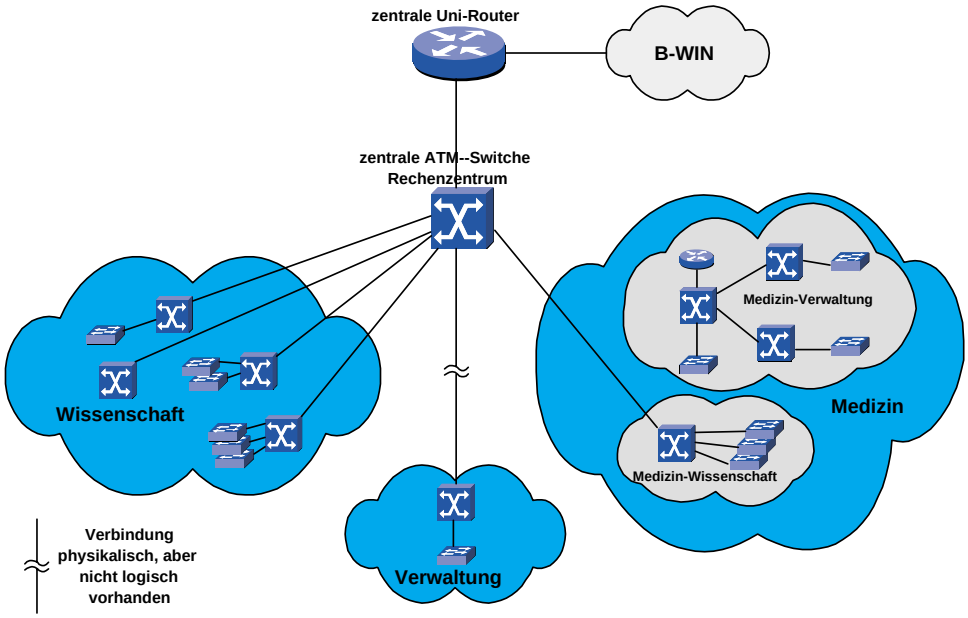


Abbildung 7.1: Logischer Aufbau des RUN

7.2 Lösungskonzepte

7.2.1 Das Wissenschaftsnetz

Der Aufbau des RUN wurde in Kapitel 7.1 erläutert. Ausgangspunkt für die Erstellung des Lösungskonzeptes ist das in Kapitel 4.4.1 erarbeitete Sicherheitskonzept im Zusammenhang mit den in Kapitel 5 vorgestellten Sicherheitsarchitekturen. Als Grundvoraussetzung für die einzusetzende Hardware wurden Flexibilität, Zukunftssicherheit, Performance und niedrige Kosten herausgestellt. Zusammen mit den geringen Sicherheitsanforderungen ergab sich der Paketfilter als optimales Sicherheitskonzept. In den Routern werden bereits Paketfilter zur Filterung bestimmter Dienste eingesetzt, so dass nur die Konfiguration der Paketfilter geändert werden muss. Mit Hilfe der Tabelle 4.2 und [CB96] wurden die zu sperrenden Dienste definiert (Tabelle 7.1). Das interne Netz steht hierbei für die Routerkonfiguration zwischen den einzelnen LAN–Segmenten des RUN. Als externe Verbindung wird alles definiert, was aus dem RUN in das B-WIN gesendet bzw. aus dem B-Win empfangen wird.

Tabelle 7.1: Paketfilterkonfiguration im Wissenschaftsnetz

Zugang	Quelle	Port	Ziel	Port	Attribute	Kommentar
blockiert	intern	*	intern	*		Verhinderung von IP–Spoofing am Routereingang
blockiert	extern	*	Router	*		Verhinderung des Zugangs zum Router
erlaubt	RESERVE	*	UNSER–DNS	53		Zugang für Reserve–Name–Server
blockiert	*	*	*	53		sonst keine DNS–Zonentransfers
erlaubt	*	*	*	53	UDP	UDP–DNS–Anfragen zugelassen
erlaubt	NTP.ext.	123	NTP.int.	123	UDP	externe NTP–Anfragen
blockiert	*	*	*	67	UDP	bootp gesperrt
blockiert	*	*	*	69	UDP	kein Zugriff auf den tftpd
blockiert	*	*	*	87		link–Dienst wird häufig missbraucht
blockiert	*	*	*	111		weder TCP–RPC
blockiert	*	*	*	111	UDP	noch UDP–RPC
blockiert	*	*	*	161,162	UDP	SNMP gesperrt
blockiert	*	*	*	177	UDP	xdmcp, keine X11–Logins
blockiert	*	*	*	2049	UDP	noch UDP–NFS
blockiert	*	*	*	2049		und TCP–NFS erlaubt
blockiert	*	*	*	512		„r–Befehle“
blockiert	*	*	*	513		dito
blockiert	*	*	*	514		dito
blockiert	*	*	*	515		kein externer lpr
blockiert	*	*	*	512	UDP	biff–Dienst
blockiert	*	*	*	513	UDP	who–Dienst
blockiert	*	*	*	514	UDP	syslog

Zugang	Quelle	Port	Ziel	Port	Attribute	Kommentar
blockiert	*	*	*	520	UDP	route–Keine Manipulation an den Routing–Tabellen
blockiert	*	*	*	540		kein uucp
blockiert	*	*	*	2000	openwin–analog X11	
blockiert	*	*	*	6000-6100		keine ausgehende X11–Verbindungen
erlaubt	*	*	*	6667		IRC erlaubt
erlaubt	*	*	*	*		sonstiger TCP ist ok
erlaubt	*	*	*	*	UDP	sonstiger UDP ist erlaubt

7.2.2 Verwaltung

Die Verwaltung hat nach dem Sicherheitskonzept in Kapitel 4.4.2 einen viel höheren Schutzbedarf als das Wissenschaftsnetz. Die Benutzung eines reinen Paketfilters scheidet damit von vornherein aus. Applikationsfilter alleine sind direkt von aussen und innen angreifbar und können die innere Struktur eines Netzes nicht ohne Sicherheitsrisiko verbergen. Als Lösung ergibt sich eine aus einem Applikationsfilter mit jeweils einem vor– und nachgeschalteten Paketfilter, auch Screened Subnet genannt (Abbildung 5.5), bestehende Konfiguration. Die Paketfilter fungieren als Sicherung für den Applikationsfilter, und sie entlasten den Applikationsfilter durch eine Vorfilterung der ankommenden Pakete.

7.2.2.1 Angepasster Firewall–Aufbau

Trotz der Übereinstimmungen mit dem Konzept „Screened Subnet“ müssen einige Änderungen und Definitionen vorgenommen werden. Der genaue Aufbau des Lösungskonzeptes ist in Abbildung 7.2 dargestellt. Der innere DNS– und der innere Mail–Server sind bereits vorhanden und werden weiter benutzt.

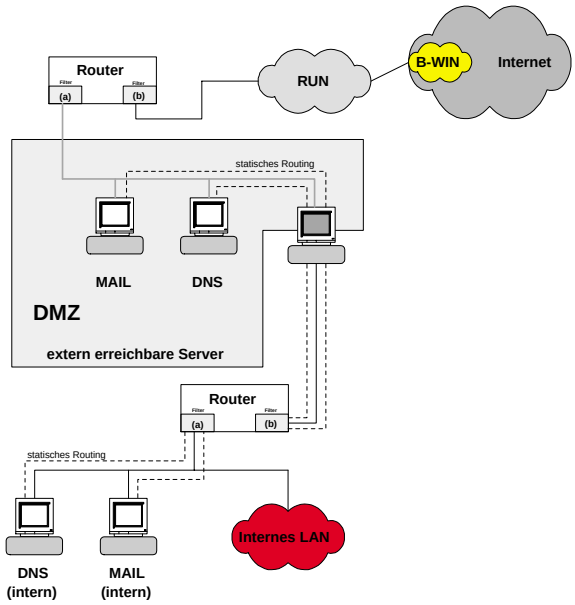


Abbildung 7.2: Lösung für die Verwaltung

7.2.2.2 Paketfilterkonfiguration

Wie in Abbildung 7.2 erkennbar ist, schützen die Paketfilter den Bastion–Host vor Angriffen und das innere Netz vor einem kompromittierten Bastion–Host. Der äußere Paketfilter kann nicht erwünschte Pakete abwehren, so dass der Bastion–Host entlastet wird. Der innere Paketfilter wird so konfiguriert, dass Hosts aus dem internen LAN nur Verbindung mit dem Bastion–Host erlangen können. Unerwünschte Protokolle werden abgewiesen. Zu empfehlen ist der Einsatz von dynamischen Paketfiltern, die einen Bastion–Host zusätzlich vor fragmentierten Paketen schützen. Die Paketfilter sind besonderer Angriffspunkt und müssen daher besonders geschützt werden. Dazu gehört:

- Nur Konsolen– oder Modemzugang zulassen
- Keine Nutzer auf dem Paketfilter
- Managementport deaktivieren

Interner Paketfilter

Der interne Paketfilter schützt das interne Netz vor einem kompromittierten Applikationsfilter und diesen wiederum vor Angriffen aus dem internen Netz. Auf Grund der

beschränkten Routenauswahl kann ARP eingeschränkt werden. Für statische Konfigurationen, dass heißt bei nicht veränderlichen IP–Adressen, ist es möglich, statische Routingtabellen aufzubauen, und das ARP im Router komplett zu deaktivieren. Sämtliche Gateway Protokolle (IGP, EGP, BGP) sind zu deaktivieren, da der gesamte ausgehende Verkehr über das Gateway geleitet wird. In Tabelle 7.2 ist die Konfiguration des internen Paketfilters, so weit das ohne genaue Kenntnis der später eingesetzten Hardware möglich ist, dargestellt. Es ist möglich, den internen Paketfilter mit einem Telnet–Zugang auszurüsten. Aus dem externen Bereich muss ein Angreifer den äußeren Router und das Gateway überwinden, um an den Router heranzukommen. Um einen Angriff von innen abzuwehren sollte der Router so konfiguriert werden, dass Verbindungen zum Telnet–Port nur vom Administrator oder vom Administratornetz zugelassen werden. Für eine Fern–Administration ist der Router mit einem Modemzugang ausauszustatten, da eine Telnetverbindung zu unsicher ist.
Der Aufbau des internen Netzes sollte mittels statisch vergebenen IP–Adressen vorgenommen werden. Für diesen Fall können die Tabellen für das Routing im Router fest vorgegeben werden. Bei jeder Änderung in der Adressvergabe bzw. bei Änderungen der Rechnerkonfiguration (wechseln der IP–Adresse, Austausch der Netzwerkkarte, Austausch des kompletten Rechners) müssen diese Tabellen geändert werden.

externer Paketfilter

Der externe Paketfilter hat die Aufgabe, die eintreffenden IP–Pakete vorzufiltern und bestimmten Diensten den Aus– bzw. Zugang zu erlauben oder zu verwehren. Eine gründliche Konfiguration erspart den folgenden Geräten Arbeit und der Datendurchsatz steigt. Der externe Router, auf dem der externe Paketfilter installiert ist, übernimmt Aufgaben wie zum Beispiel Adresszuordnungen und Routenwahl. Pakete mit Source–Routing Option sollten vom Router bereits am Eingang abgewiesen werden, ebenso wie Pakete mit internen IP–Adressen, die am externen Port ankommen. Als Ziele sind einzig Geräte in der DMZ zu definieren. Andere IP–Adressen sollten gesperrt werden. Die Konfiguration eines Beispiel–Paketfilters ist in Tabelle 7.3 dargestellt.

7.2.2.3 Konfiguration des Bastion–Host

Auf dem Bastion–Host sind für die wichtigsten Dienste die Application–Proxies installiert. Zusätzlich kann ein generischer Proxy installiert werden, der weiteren TCP–

Tabelle 7.2: Konfiguration des internen Paketfilters

Zugang	Quelle	Port	Ziel	Port	Attribute	Kommentar
erlaubt	intern	*	Gateway	80		Kontakt vom Client zum Gateway–HTTP–Proxy
erlaubt	Gateway	80	intern	*		Verbindungen vom Gateway–HTTP Proxy zum Client
erlaubt	int. DNS	*	ext. DNS	53	UDP	DNS–Anfragen an externen DNS
erlaubt	ext. DNS	*	int. DNS	53	UDP	Anfragen an internen DNS
erlaubt	intern	*	Gateway	21		Anfrage zum Verbindungsaufbau an Gateway–FTP–Proxy
erlaubt	Gateway	21	intern	*		Antwort des Gateway–FTP–Proxies auf Verbindungsanfrage
erlaubt	Gateway	20	intern	*		Einrichten des Datenkanals für interne FTP–Anfrage
erlaubt	intern	*	Gateway	20		Antworten auf dem FTP–Datenkanal
erlaubt	Gateway	*	intern	$\geq$1024	ACK	Antworten für die Clients
erlaubt	intern	$\geq$1024	Gateway	≥ 1024	a	Verbindungen z.Bsp. FTP Passive–Transfer–Modus
erlaubt	Admin	*	Gateway	23		Telnet–Verbindung zum Gateway nur vom Admin bzw. Admin–Netz
erlaubt	Gateway	23	Admin	*	ACK	und zurück
erlaubt	Admin	*	Router int.	23		Telnet–Verbindung zum internen Router nur vom Admin bzw. Admin–Netz
erlaubt	Router int.	23	Admin	*	ACK	und zurück

a – außer im ersten Paket Acknowledge (ACK) Bit gesetzt

Zugang	Quelle	Port	Ziel	Port	Attribute	Kommentar
erlaubt	Mail.int.	*	Mail.ext.	25		Zugang zum externen Mailserver
erlaubt	Mail.ext.	*	Mail.int.	25		und zum internen Mailserver
erlaubt	Mail.ext.	*	Mail.int.	*	ACK	Rückantworten für Mailserver
erlaubt	Mail.int.	*	Mail.ext.	*	ACK	dito
erlaubt	intern	123	Gateway	123	UDP	NTP–Zeitabfrage
erlaubt	Gateway	123	intern	123	UDP	dito
blockiert	*	*	*	6000-6100		X11–Verbindungen zum Server
blockiert	*	*	*	*		Sonst kein TCP erlaubt
blockiert	*	*	*	*	UDP	Sonst kein UDP erlaubt

Datenverkehr über das Gateway schleust. Der generische Proxy muss nicht allzu umfangreich konfiguriert sein, da die beiden Paketfilter den Zugang regeln können. Im Applikationsfilter wird weiterhin die Adressumsetzung für die Network–Address–Translation vorgenommen. Hierzu tauscht der Applikationsfilter die „echte“ IP–Adresse gegen eine IP–Adresse aus dem Pool der NAT aus. Somit weiß nur der Applikationsfilter, von welchem Rechner das Paket stammt. Die Topologie des inneren Netzes kann dadurch verborgen werden. Zur Entlastung des Gateways können einige Dienste und Proxies ausgelagert werden. So wird in [Fir99] vorgeschlagen, den HTTP– und FTP–Proxy mit Virus–Filterung auf eine externe Machine auszulagern, die in der DMZ beheimatet ist. Da der Proxy nicht auf einem Bastion–Host installiert ist, muss sichergestellt werden, dass sämtlicher entsprechender Datenverkehr über den Proxy geleitet wird. Die Zugangslisten zum Gateway und die Paketfilter werden dahingehend umkonfiguriert. Auf dem Gateway selbst wird dann entweder ein generischer Proxy oder ein in seinen Filterfunktionen beschränkten HTTP– bzw. FTP–Proxy eingesetzt. Eine komplette Deaktivierung der Proxies auf dem Gateway würde das Gateway–Konzept unterwandern und ist nicht empfehlenswert.

Tabelle 7.3: Konfiguration des externen Paketfilters

Zugang	Quelle	Port	Ziel	Port	Attribute	Kommentar
blockiert	intern	*	intern	*		IP–Spoofing verhindern
blockiert	intern	*	intern	*	UDP	dito
erlaubt	Proxy	$\geq$1024	*	80		Kontakt vom Proxy zu einem externen HTTP–Server
erlaubt	*	80	Proxy	$\geq$1024	ACK	Antworten auf HTTP–Anfragen
erlaubt	Reserve	*	ext.DNS	53		Zugang für Reserve–Name–Server
erlaubt	*	*	ext.DNS	53	UDP	ankommende DNS–Anfragen
erlaubt	ext.DNS	53	*	*	UDP	und Antworten
erlaubt	ext.DNS	*	*	53	UDP	ausgehende DNS–Anfragen
erlaubt	*	53	ext.DNS	*	UDP	und Antworten
erlaubt	Proxy	*	*	21		Anfrage zum Verbindungsaufbau FTP–Server
erlaubt	*	21	Proxy	*	ACK	Antwort des FTP–Servers auf Verbindungsanfrage
erlaubt	*	20	Proxy	*		Einrichten des Datenkanals für FTP–Anfrage
erlaubt	Proxy	*	*	20		Antworten auf dem FTP–Datenkanal
erlaubt	Proxy	$\geq$ 1024	*	$\geq$ 1024	a*	Einrichten eines Datenkanals FTP–passiver Modus
erlaubt	*	$\geq$ 1024	Proxy	$\geq$ 1024	ACK	Antworten bei FTP–passiver Modus

* – außer im ersten Paket Acknowledge (ACK) Bit gesetzt

Zugang	Quelle	Port	Ziel	Port	Attribute	Kommentar
blockiert	*	*	*	*		Sonst kein TCP erlaubt
blockiert	*	*	*	*	UDP	Sonst kein UDP erlaubt

7.2.3 Zentrales Firewall–System

In der Universität gibt es Bereiche, die einen Schutz ihres Netzes beim Zugang zum Internet benötigen. Einige dieser Bereiche (Medizin, Verwaltung) benötigen einen dauerhaften Schutz. Andere brauchen Schutz für eine bestimmte Zeit, so zum Beispiel wissenschaftliche Projekte und Forschungen, die in Zusammenarbeit mit Firmen bearbeitet werden. Die Anforderungen der zu schützenden Bereiche unterscheiden sich teilweise stark. So ist zum Beispiel bei der Verwaltung nur der Schutz vor dem Internet als Forderung anzusehen. Wissenschaftliche Projekte in Zusammenarbeit mit Firmen erfordern eventuell die Einrichtung eines VPN. Um alle diese Forderungen abdecken zu können, ist der Einsatz eines zentralen Firewall–Systems aus Kostengründen sinnvoll. Derzeit befindet sich ein solches System in der Projektierungsphase [Fir99]. Unmittelbare Voraussetzung für ein zentrales System ist das Vorhandensein eines ATM–Backbones, da nur damit eine dynamische Zuordnung von Netzwerkanschlüssen an LAN–Segmente erfolgen kann und keine direkte physikalische Verbindung zwischen den LAN–Segmenten und der Firewall vorhanden sein muss. Es ergeben sich folgende Forderungen (mit [Fir99]):

- Flexible Konfigurationsmöglichkeiten des Applikationsfilters und der Paketfilter in Hinblick auf Zugehörigkeit und Schutzbestimmungen
- Keine Beeinträchtigung der Sicherheit der dauerhaft geschützten Bereiche durch die temporär geschützten Bereiche
- Bestehende Adressen in den geschlossenen Teilnetzen sollen weiterhin verwendbar sein. Bei der Nutzung der Dienste soll das Zentrale Firewall-System für den Anwender transparent sein.
- Ein großer Funktionsumfang bei der Zugriffskontrolle und eine umfangreiche Protokollierung muss gewährleistet sein. Die Zugriffskontrolle soll anwendungs-,

richtungs-, nutzer- und zeitbezogene Zugriffskontrollisten enthalten. Unregelmässigkeiten sollen schnell und sicher erkannt werden und durch ein Alarmierungssystem sofort weitergeleitet werden können.

- Die Administration des Zentralen Firewall-Systems soll über eine GUI (Graphical User Interface) erfolgen, wobei auch eine remote Administration mit gesicherter Datenübertragung möglich sein soll. Prinzipiell soll eine Delegierung von administrativen Aufgaben, angepasst an die Sicherheitskonzepte der Teilbereiche, möglich sein.

Die Forderung eines GUI zur Administration direkt auf dem Applikationsfilter ist äußerst problematisch, da dieses mit Sicherheitsproblemen ausgestattet sein wird. Jedes heute benutzte GUI hat seine Schwachstellen. Einzige Lösung dieses Problems ist die Benutzung eines GUI auf einem Internen Rechner und der Zugriff auf die Firewall über eine authentifizierte und geschützte Verbindung. Generell sollte der Zugriff auf die Administrationsports der Firewall nur von einer begrenzten Anzahl von Clients möglich sein. Diese müssen explizit in Zugangslisten festgelegt sein.

7.2.3.1 Firewall–Aufbau

Die Auswahl des Firewall–Aufbaus richtet sich nach dem Bereich, der den meisten Schutz benötigt. Diese Bereiche sind in der Universität die Verwaltung und die Medizin. Als Konzept kommt nur das „Screened Subnet“ in Frage. Es gibt einige Ergänzungen zu dem unter Kapitel 7.2.2 vorgestellten Konzept. Dies betrifft in erster Linie einen in der DMZ zur Verfügung gestellten WWW– und FTP–Server.

7.2.3.2 Konfiguration

Die Firewallkonfiguration und –administration kann an zentraler Stelle erfolgen. Eine zentrale Firewall bedeutet nicht, dass alle angeschlossenen Netze den gleichen Sicherheitsbeschränkungen unterliegen müssen. Für jedes angeschlossene Netz sind separate Konfigurationen möglich. Weiterhin stellt die Firewall sicher, dass die unterschiedlichen Netze auch voreinander geschützt sind. Dabei ist sicherzustellen, dass das Application Gateway besonders geschützt ist, da ein Einbruch in dieses System den Zugang zu allen gesicherten Netzen möglich macht. Zur Verringerung des Risikos eines Einbruchs sollten die einzelnen Komponenten der Firewall von unterschiedlichen Softwareherstellern

stammen. Das bezieht sich sowohl auf die Programmteile der Firewall–Lösung als auch auf das zugrundeliegende Betriebssystem.

Kapitel 8

Fazit

Als Ergebnis der Arbeit ist ein Katalog zur Erarbeitung eines Sicherheitskonzeptes entstanden (Kapitel 4). Dieser Katalog umfasst die wichtigsten Fragen, die für die Sicherheitskonzeption geklärt werden müssen. Für Teilnetze der Universität Rostock ist mit Hilfe des Kataloges ein Sicherheitskonzept erarbeitet worden. Es wurden verschiedene Firewallarchitekturen in ihren Vor– und Nachteilen beleuchtet (Kapitel 5). Abschließend wurden Lösungsvorschläge für Teilnetze der Universität auf Basis der Sicherheitskonzeption und der vorgestellten Firewall–Architekturen erarbeitet (Kapitel 7). Es bleibt festzustellen, dass der Einsatz einer Firewall den Administrator nicht von seiner Sorgfaltspflicht in der Administration der einzelnen Rechner im Netzwerk entbindet. Zur Vorbeugung eines Angriffes ist es sinnvoll, sich in Security–Mail–Listen, wie zum Beispiel CERT eintragen zu lassen. Die Angriffsmöglichkeiten, die auf die eigenen Maschinen zutreffen, sind in den meisten Fällen bereits dort dokumentiert und Updates sind verfügbar. Für die Akzeptanz einer Sicherheitsmaßnahme ist der Grad der Einschränkung im Vergleich mit dem Nutzen für jeden einzelnen Nutzer entscheidend. So ist zum Beispiel ein PC, der nicht ständig am Netz ist, und der eventuell eine veränderliche IP–Adresse hat, nicht das normale Ziel eines Angriffes. Bei Servern und Workstations, die ständig erreichbar sind, und die Nutzerdaten enthalten, stellt sich die Sache anders dar. Diese sind durch die gleichbleibende und ständig erreichbare IP–Adresse einer höheren Gefährdung ausgesetzt. Diese Gefährdung kann durch ein Bündel an Maßnahmen stark verringert werden. Dazu gehören:

- Benutzung sicherer Passworte
  Die Passworte müssen sorgfältig ausgewählt werden. Das Passwort sollte ausreichend lang sein, und nicht aus einem Wörterbuch stammen, bzw. keine Kombination verschiedener Worte sein. Am besten sind Passwörter, die durch ein Programm zufällig zusammengestellt wurden.

- Umfangreiche Protokollierung und Überwachung aller Prozesse und Login– Versuche
  Durch die Protokollierung und Überwachung wird ein Einbruch in das System frühzeitig erkannt, was größere Schäden verhindert. Weiterhin kann dadurch der Ursprung des Angriffs ermittelt werden.

- Benachrichtigung des Administrators
  Bei der Entdeckung eines Einbruchs ist der Administrator sofort per Email und zusätzlich, wenn möglich, per SMS zu informieren. Als Indikator kann dabei die unerlaubte Veränderung von Systemdateien, wie zum Beispiel Nutzerdatenbank, Protokolldatei, etc., dienen.

- Regelmäßige Sicherung der lokalen Daten
  Durch eine regelmäßige Datensicherung wird der Schaden eines Einbruchs minimiert. Durch eine zusätzliche Sicherung des kompletten Grundsystems vor dem Anschalten an das Netz kann jederzeit die Grundkonfiguration wiederhergestellt werden. Diese „Erstsicherung“ sollte für immer aufgehoben und nicht überspielt werden.

- Informationen und Sicherheitsupdates beziehen
  Durch die Mitgliedschaft in Mailinglisten, zum Beispiel DFN–CERT, wird man rechtzeitig über Sicherheitslöcher in seinem System informiert. Die von den Herstellern bereitgestellten Updates sollten umgehend eingespielt werden.

Viel schwieriger zu erkennen und zu überwachen sind Angriffe, die innerhalb des Netzes stattfinden. Gegen diese Art des Angriffes helfen sichere Passworte, regelmäßige Sicherheitsupdates und eine Zugangskontrolle zu Workstations. Für eine Zugangskontrolle sollten Bios– und Bildschirmschonerpassworte, sowie Betriebssysteme mit einer sicheren Anmeldeprozedur verwendet werden. Die Vergabepraxis der Passworte ist ebenfalls zu überdenken. Ein X–Stellen langes sicheres Passwort nutzt wenig, wenn jeder Mitarbeiter im Unternehmen dieses Passwort kennt. Ein sorgsamer und genau festgelegter Umgang mit den Passwörtern ist unumgänglich. Die Mitarbeiter müssen mit dem Thema Sicherheit vertraut gemacht werden. Die bestehenden Sicherheitsrisiken und die Folgen eines sorglosen Umgangs mit sicherheitsrelevanten Information müssen verdeutlicht werden. Für den Administrator gilt, dass er die Mitarbeiter ermutigt, sich bei Unregelmäßigkeiten sofort bei ihm zu melden. Wachsame Mitarbeiter können helfen,

die Verbreitung von Viren zu verhindern oder aber einen Einbruch zu erkennen.
Die Benutzung geswitchter Verbindungen innerhalb des Netzwerkes erschwert ein Abhören von bestehenden Verbindungen durch Dritte. Bei den eingesetzten Switches sollte die Möglichkeit bestehen, eine MAC–Adressen basierte Zugriffskontrolle durchzuführen. Diese Kontrolle verhindert den unberechtigten Zugang von Netzwerkclients.

Anhang A

Sicherheitsanforderungen an Internet–Firewalls [BW97]

Die nachfolgenden Forderungen wurden durch das Bundesamt für Sicherheit in der Informationstechnik BSI aufgestellt und in dieses Dokument übernommen. Diese Forderungen sind häufig bereits Bestandteil des eigenen Sicherheitskonzeptes, so dass die nachfolgenden Kapitel nicht von diesem losgelöst betrachtet werden können.

A.1 Bisherige Sicherheitsanforderungen an Internet– Firewalls des BSI

A.1.1 Forderungen zur Abwehr von Angriffen auf die Firewall–Anordnung

1. Identifikation und Authentisierung für Administrator und Revisor nur über einen vertrauenswürdigen Pfad.

2. Die Defaulteinstellung der Rechte muss sicherstellen, dass die Rollen Administrator und Revisor realisiert sind.

3. Bei einem Ausfall der Protokollierungskomponente muss eine Warnung ausgegeben werden, die ein unverzügliches Eingreifen des Administrators ermöglicht. Es muss möglich sein, die Firewall so zu konfigurieren, dass bei einem Ausfall der Protokollierungskomponenten jegliche nicht administrative Nutzung (im Sinne von 1) der Firewall unterbunden wird.

4. Integritätstests der eingesetzten Programme und Dateien mindestens einmal täglich.

Es muss möglich sein, die Firewall so zu konfigurieren, dass bei einer Integritätsverletzung jegliche nicht administrative Nutzung der Firewall (im Sinne von 1) unterbunden wird. Die für den Integritätstest notwendigen Programme und Dateien müssen auf einem Medium speicherbar sein, welches hardwaremäßig gegen Schreibzugriffe gesichert werden kann. Es muss protokolliert werden, welche Änderungen (mit Datum und Uhrzeit) an der Konfiguration der Firewall vorgenommen wurden.

5. Es muss möglich sein, die Firewall so zu konfigurieren, dass bei einem Systemabsturz jegliche nicht administrative Nutzung der Firewall (im Sinne von 1) unterbunden wird.

6. Auf den eingesetzten Komponenten darf nur Software vorhanden sein, die für die Funktionsfähigkeit der Firewall nötig ist. Die benutzte Software (inkl. aller Konfigurationsdateien) muss ausführlich dokumentiert und begründet werden.

A.1.2 Forderungen zur Abwehr von Angriffen auf das zu sichernde Netz

A.1.2.1 Obligatorische Forderungen

7. Die Firewall–Anordnung muss für den Fall des hohen und sehr hohen Schutzbedarfs aus mindestens zwei getrennten Filtern bestehen. Die Filter müssen hintereinander angeordnet sein, so dass für eine Verbindung zwischen den beiden beteiligten Netzen beide Filter passiert werden müssen. Die Filter müssen mit unterschiedlicher Hard– und Software (Betriebssystem) arbeiten und unterschiedliche Formate für die Beschreibung der Filterregeln benutzen.

8. Die Einstellung der Filterregeln bei einer Erstinstallation und die Anordnung der Komponenten muss sicherstellen, dass alle Verbindungen, die nicht explizit erlaubt sind, abgewiesen werden. Auch bei einem völligen Ausfall der Firewall–Komponenten dürfen nur Verbindungen durchgelassen werden, die explizit erlaubt worden sind.

9. Die Struktur des zu schützenden Netzes muss verdeckt werden können, d.h. dass keine internen Informationen wie Benutzernamen, Rechnernummern, –namen und

Mailadressen nach außen gelangen können.

10. Die Verwaltung der Komponenten muss übersichtlich sein (grafisches Interface).

11. Die Verwaltung der Komponenten muss zentral über einen vertrauenswürdigen Pfad (z.B. ein separates Netz oder über eine verschlüsselte Verbindung) erfolgen.

12. Der Aufbau von Verbindungen auf der Anwendungsschicht durch die Firewall muss benutzerabhängig und zeitabhängig erlaubt oder verboten werden können.

13. Zur Benutzer–Identifikation müssen starke Authentisierungsmethoden benutzt werden.

14. Es muss möglich sein, mehrere Benutzer zu einer Gruppe zusammenzufassen.

15. Die Filterregeln müssen auf ihre Widerspruchsfreiheit überprüft werden.

16. Es müssen die Protokolle Telnet, FTP, SMTP, DNS, NNTP und HTTP unterstützt werden.

17. Für Telnet-Verbindungen vom Internet zur Firewall (kommende Verbindungen) muss durch zusätzliche Prozesse eine Verschlüsselung der übertragenen Nutzinformationen durchgeführt werden.

18. Für Verbindungen auf der Anwendungsschicht müssen zusätzlich alle Befehle, die den Import von Daten in das zu schützende Netz (z.B. ein retr bei FTP) oder den Export von lokalen Daten ins Internet (z.B. ein post bei HTTP) bewirken, benutzerabhängig und zeitabhängig erlaubt oder verboten werden können.

19. Für jede aufgebaute– und abgewiesene Verbindung auf der Anwendungsschicht muss eine Protokollierung von Benutzer–Identifikation, IP–Adresse des Quell– und Zielrechners, Portnummer, Zeit und Datum durchgeführt werden, wobei auch Einschränkungen auf bestimmte Verbindungen möglich sind.

20. Spezielle, einstellbare Protokollmeldungen müssen zu einer unverzüglichen Warnung führen.

21. Die Protokollinformationen müssen über einen vertrauenswürdigen Pfad an eine zentrale Stelle geschickt werden können.

22. Bei der Benutzung von FTP muss es möglich sein, den Verbindungsaufbau für die Datenverbindung (FTP–DATA) von der Firewall ins Internet durchführen zu lassen (Benutzung des PASV–Kommandos).

A.1.2.2 Zusätzliche Forderung bei Verwendung von Filtern auf Layer drei (IP) und vier (TCP, UDP)

23. Die Weiterleitung von Paketen muss abhängig von

    (a) IP–Quell– und IP–Zieladresse einzelner Rechner oder kompletter Teilnetze und

    (b) Quell– und Zielport für TCP und UDP

    erlaubt oder verboten werden können. Dies wird in Filterregeln festgelegt. (Der Quell–Port ist z.B. für einen Zone-Transfer zwischen den UDP-Ports 53 zweier DNS-Server wichtig.

24. Die Filterung gemäß voriger Forderung muss getrennt für jedes Interface möglich sein.

25. Die Reihenfolge der Filterregeln darf nicht automatisch von der Firewall verändert werden.

26. Wenn mehr als zwei Interfaces vorhanden sind, muss eine Filterung getrennt für kommende und gehende Pakete möglich sein.

27. Bei TCP-Paketen muss eine Unterscheidung, ob ein Verbindungsaufbau stattfindet oder eine bestehende Verbindung benutzt wird, d.h. eine Unterscheidung zwischen ACK und ACK-losen Paketen, möglich sein.

28. Protokollierung von IP-Nummer, Dienst, Zeit und Datum für jedes Paket, wobei auch Einschränkungen auf bestimmte Pakete (z.B. nur Pakete mit einer speziellen Quell-Adresse) möglich sind.

29. Im Falle der Kombination der Firewall mit einem Router darf die Sicherheit der Firewall nicht durch eine Veränderung der Routing-Einträge gefährdet werden. Es muss statisches Routing benutzt werden.

30. Source-Routing Informationen müssen standardmäßig abgewiesen werden.

A.2 Zusätzliche Sicherheitsanforderungen an Internet–Firewalls

A.2.1 Paket–Filterung / Reglementierung

31. Firewalls sollten eine Mindestgröße an Fragmentlänge verlangen.
32. Firewalls sollten ein Minimum an Fragment-Offset vorschreiben.
33. Firewalls sollten die ICMP-Meldung Destination Unreachable filtern können.
34. Firewalls sollten die ICMP-Meldung Redirect filtern können.
35. DNS-Spoofing sollte abgewiesen werden können.
36. Zonen-Transfer-Requests von einem unbekannten Host sollten mit Refused beantwortet werden können.
37. ARP-Tabellen sollten fixiert werden können.
38. Das automatische Ablaufen von ARP sollte unterbunden werden können.
39. Die FTP-Befehle CWD, CDUP, RETR, STOR, LIST, NLIST, SYST sollten an eine Rechteverwaltung gekoppelt werden können. Der FTP-Befehl SITE sollte abgewiesen werden können.
40. Eingehende Telnet-Daten sollten auf Port 23 gefiltert werden können.
41. S-HTTP-Daten sollten vom HTTP-Proxy abgewiesen werden können.
42. Paket-Filter sollten Kontext speichern können
43. Die folgenden Netzobjekte sollten für die Filterung definiert werden können: Host, Domain, Subnet, Group, IP-Range, VPN-Objekte

A.2.2 Abwendung von Standardangriffen

44. Ein Spoof-Checking sollte durchgeführt werden.
45. Ping-to-Death sollte abgefangen werden.
46. TCP-SYN-Flooding sollte verhindert werden können.
47. Anti-Virus Checking sollte unterstützt werden können.
48. Paket-Reassemblierung sollte durchgeführt werden.
49. Session Hijacking sollte verhindert werden können.
50. TCP-Sequence-Number-Guessing sollte verhindert werden können.
51. Es sollte möglich sein, im internen Netz die gleichen IP-Adressen zu verwenden, wie im externen Netz.

A.2.3 Administration

52. Die Administration der Firewall sollte durch starke Authentisierungsmechanismen geschützt sein. (z.B. durch Chipkarte)
53. IP–Forwarding sollte auch nach einem Neustart noch abgeschaltet sein.
54. Eine Remote–Administration sollte mittels starker Authentisierung und Verschlüsselung geschützt sein.

A.2.4 Verschlüsselung/Authentisierung

55. Die Schlüssellänge bei Verschlüsselungsalgorithmen sollte unbeschränkt sein. (Z.B. durch Exportbeschränkungen.)
56. Das Schlüsselmanagement sollte ausreichend sicher sein.
57. Remote und Mobile Access Control sollten mittels starker Authentisierung und Verschlüsselung geschützt sein.
58. Für Telnet, FTP und HTTP sollte eine erweiterte Login–Prozedur zur Verfügung stehen.

59. Eine Client Authentication zur Authentisierung von Benutzern beliebiger Anwendungen sollte möglich sein. (Sowohl TCP, UDP, als auch RPC-basiert)

60. Die Authentisierung bei kritischen Protokollen sollte transparent sein.

61. Eine Authentisierung sollte pro Sitzung möglich sein.

62. Es sollten die wesentlichen kryptographischen Algorithmen implementiert sein.

63. Sitzungsschlüssel sollten je nach Schlüssellänge mit ausreichender Häufigkeit gewechselt werden können.

A.2.5 sonstige Anforderungen

64. Folgende Dienste sollten angeboten werden können und nicht schlicht abgewiesen werden: NFS, NIS, RPC, RIP, OSPF, r–Kommandos, DNS, WAIS.

65. Die BGP–Meldung Notification sollte abgewiesen werden können.

66. Die RIP–Meldung Loose-Source-Routing sollte abgewiesen werden.

67. Die Firewall sollte transparent betrieben werden können.

68. Eine On–line Hilfe sollte vorhanden sein.

69. Für den Betrieb der Firewall sollte keine proprietäre Hardware notwendig sein.

70. Der Aufwand für die Installation sollte nicht zu hoch sein.

71. Der Aufwand für die Anschaffung sollte nicht übermäßig sein.

72. Der Aufwand für das Betreiben der Firewall sollte angemessen niedrig sein.

73. Support in Installation und Training sollte angeboten werden.

74. Versionspflege sollte angeboten werden

A.3 Zusätzliche Funktionen der Produkte

A.3.1 Filterung und Proxyauswahl

75. Folgende Regelarten sollten angeboten werden: allow, deny, drop.

76. Mindestens eines der folgenden Protokolle sollte durch dedizierte Proxies behandelt werden. : Oracle SQL*Net, Netscape CoolTalk, Microsoft NetMeeting, Citrix, IntelPhone, RealAudio, X11, Sybase, Finger, whois, syslog,

A.3.2 Protokollierung/Alarmierung

77. Die Alarmierung des Administrators sollte mindestens über Email und Audio möglich sein.

78. Protokollinformationen sollten an einen externen Host gesendet werden können. (z.B. automatisch per Email)

A.3.3 Plattform

79. Mindestens eine der folgenden Plattformen sollte unterstützt werden: Windows95, Windows NT, SINIX, SunOS und Solaris, HP–UX, BSD, AIX, DEC–UNIX, OSF1, LINUX

80. Router sollten unterstützt werden.

81. Für folgende Netze sollten Interfaces vorgesehen sein: SLIP, PPP, Ethernet, Fast Ethernet, Token Ring, X.25, FDDI, ATM

A.3.4 Authentisierung

82. Mindestens eines der folgenden Verfahren sollte bei der Authentisierung unterstützt werden: Access Key, APOP, Defender Security System, Digipass, Safeword Authentication Server, SecureNet, SecurID, S/Key, Digital Pathways SNK, Cryptocard, Reusable Passwords, Kerberos, Racal WatchWord Keys, TACACs+, RADIUS

A.3.5 sonstige Merkmale

83. Modem–Verbindungen sollten gesichert werden können.

84. Andere Protokolle wie IPX oder DECNET sollten unterstützt werden.

85. Network Address Translation (NAT) sollte unterstützt werden.

A.4 Zukünftige Anforderungen an Internet– Firewalls

A.4.1 Ausführbarer Code

86. An ausführbarem Code sollte mindestens JAVA, JAVAScript, MIME und ActiveX gefiltert werden können.

87. Ausführbarer Code sollte auch in FTP erkannt und gefiltert werden.

88. Es sollte ein Protokoll unterstützt werden, das es erlaubt, externe und third–party Inhaltsuntersuchungsprogramme (wie z.B. automatische Audit-Tools) zu integrieren.

89. Logfiles sollten automatisch ausgewertet werden können.

A.4.2 VPN / Sicherungsdienste / Key Management

90. VPNs sollten durch IPSec, TLS/SSL oder proprietär geknüpft werden können.

91. Falls eine Firewall eines VPNs ausfällt, sollte deren Aufgabe durch eine andere übernommen werden können.

92. Mehrere Firewalls sollten von einer zentralen Stelle aus verwaltet werden können.

93. Die Kommunikation mit einer Zertifizierungsstelle sollte unterstützt werden.

94. Mindestens die aktuellen Standards IPSec, ISAKMP/Oakley, TLS/SSL, RADIUS, TACACS+ sollten unterstützt werden.

A.4.3 Sonstige Anforderungen

95. Neue Protokolle sollten hinzugefügt werden können. (z.B. durch generische Proxies)

96. Die eingesetzten Programme sollten gut dokumentiert sein.

97. Eine Änderung der Software im zu schützenden Netz oder im unsicheren Netz durch die Installation oder den Betrieb der Firewall sollte nicht notwendig sein.

98. Multicast–Pakete sollten unterstützt werden.

A.5 Produkttests

In [BW97] wurden Firewallprodukte verschiedener Hersteller nach den aufgestellten Kriterien getestet und bewertet.

Anhang B

Feste TCP– und UDP Port–Nummern in den IP–Paketen

Die nachfolgende Tabelle gibt einen auszugsweisen Überblick über TCP– und UDP–Portnummern in IP–Paketen.

Tabelle B.1: TCP– und UDP–Ports

Port	Protokoll	Name	Beschreibung
1	TCP	tcpmux	Der TCP–Port–Multiplexer. Wenig verbreitet.
7	UDP,TCP	echo	Ein Echo–Server; nützlich um zu sehen, ob eine Maschine „lebt“; eine höhere Art ICMP Echo(ping).
9	UDP,TCP	discard	Das `/dev/null` des Internet. Harmlos.
11	TCP	systat	Gelegentlich (aber selten) mit *netstat*, *w* oder *ps* vebunden
13	UDP,TCP	daytime	Uhrzeit, Format für menschliche Augen. Harmlos.
15	netstat	siehe `systat`	
19	UDP,TCP	chargen	Ein Zeichenstromgenerator. Manche lesen so etwas gerne. Harmlos.
20	TCP	ftp–data	FTP–Datenkanal. Schwierig zu filtern.
21	TCP	ftp	FTP–Kontrollkanal
23	TCP	telnet	*Telnet* Zugang
25	TCP	SMTP	*sendmail* Zugang
37	UDP	time	Uhrzeit in maschinenlesbarer Form

Port	Protokoll	Name	Beschreibung
43	TCP	whois	liefert Kontaktinformationen, befragte whois–Server sind meist NIC.DDN.MIL und RS.INTERNIC.NET, selten gibt es einen eigenen whois–Server
53	UDP,TCP	domain	DNS–Port
67	UDP	bootp	
69	UDP	tftp	TFTP Zugang. Gefährlich!
70	TCP	gopher	Informationsprotokoll GOPHER. Gefährlich, aber nützlich.
79	TCP	finger	Auskunftsserver für Computer– bzw. Nutzerinformationen. Kann leicht zum ausspionieren von Nutzerverhalten oder zum Erraten von Passwörtern genutzt werden
80	TCP	http	Port zum HTTP–Server, auch als WWW bekannt. Gefährlich, aber nützlich
87	TCP	link	Außer durch Hacker kaum genutzt. Guter Port für einen Alarm.
88	UDP	kerberos	Der offizielle Kerberos–Port dient dem Schlüsselaustausch und der Authentifikation bei authentifizierten Logins
95	TCP	supdup	Außer durch Hacker kaum genutzt, noch ein Port für einen Alarm.
109	TCP	pop–2	Zugang zum POP–2 Mailserver.
110	TCP	pop–3	Zugang zum POP–3 Mailserver.
111	UDP,TCP	sunrpc	*portmapper*; Einzig fester Port des RPC–Dienstes, merkt sich die RPC–Service Nummern der von dem Server über RPC angebotenen Dienste.
113	TCP	auth	Genutzt zur Authentisierung des Sendesystems, und damit zur Erkennung von gefälschten IP–Adressen. Nicht sehr aussagekräftig.

Port	Protokoll	Name	Beschreibung
119	TCP	nntp	Zugang zum NNTP–Server, ähnlich SMTP, Dient zur Übertragung von Newsartikeln
123	UDP	ntp	Zugang zum NTP–Protokoll, sicher falls NTPs eigene Zugangskontrollen genutzt werden
144	TCP	NeWS	Ein Window–System – wie X11 behandeln
161	UDP	snmp	Zugang zum SNMP. Gefährlich da keine Authentisierung
162	UDP	snmp–trap	dito
177	UDP	xdmcp	X11–Remote Logins. Gefährlich.
512	TCP	exec	
513	TCP	login	*rlogin* Zugang. Sehr gefährlich, da Zugang ohne Authentisierung möglich
514	TCP	shell	*rsh, rcp* Zugang. Gefährlich wie 513
515	TCP	printer	*lpr* Zugang. Es gibt kaum einen Grund diesen Zugang über eine Firewall zu lassen
512	UDP	biff	
513	UDP	who	
514	UDP	syslog	Protokollierung
517	UDP	talk	Talk–Protokoll, das eigentliche Protokoll läuft zwischen zufälligen TCP–Ports ab
518	UDP	n–talk	dito
520	UDP	route	RIP–Port für Broadcasts und Anfragen
540	TCP	uucp	UUCP–Port, Gefährlich da ohne Authentisierung. Funktionalität wird durch andere Protokolle übernommen
1025	TCP	listener	üblicher Port für den Listener–Dienst
2000	TCP	openwin	Analog X11
2049	TCP,UDP	nfs	NFS–Port, problematisch durch Sicherheitslücken
2766	TCP	listen	Der Listener, wie tcpmux, aber mit mehr Diensten
6000-6xxx	TCP	X11	X11 (X–Windows) Ports, Gefährlich
6667	TCP	irc	IRC–Port

Literaturverzeichnis

[Atk95] ATKINSON, R.: *Security Architecture for the Internet Protocol*. Standards Track RFC 1825, Naval Research Laboratory, August 1995. Internet Draft.

[Axe00] AXENT TECHNOLOGIES: *Produktbeschreibungen Raptor Firewall*. Webseiten der Firma Axent Technologies, 2000. http://www.axent.com.

[BE99] BENECKE, CARSTEN und UWE ELLERMAN: *Zugriffskontrolle in ATM–Netzen (Innovative Firewall–Konzepte für virtuelle Netze)*. DFN–Bericht Nr. 87, DFN–FireWall–Lab und POB Business Consulting GmbH, März 1999. Bericht zum 6. Workshop „Sicherheit in vernetzten Systemen“ Hamburg 1999.

[BSI92] BSI: *Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik(ITSEC)*. Bundesamt für Sicherheit in der Informationstechnik, Köln, 1992.

[BW97] BONNARD, ANDREAS und CHRISTIAN WOLFF: *Gesicherte Verbindungen von Computernetzen mit Hilfe einer Firewall*. Siemens AG ZT IK3, München, 1997. Studie im Auftrag des Bundesamtes für Sicherheit in der Informationstechnik.

[CB96] CHESWICK, WILLIAM R. und STEVEN M. BELLOVIN: *Firewalls und Sicherheit im Internet*. Addison–Wesley, 1996. Deutsche Übersetzung von Firewall and Internet Security.

[Che00] CHECKPOINT TECHNOLOGIES: *Produktbeschreibungen Checkpoint FireWall–1*. Webseiten der Firma Checkpoint Technologies, 2000. http://www.checkpoint.com.

[Cis00] CISCO SYSTEMS: *Produktbeschreibungen Cisco Secure PIX Firewall*. Webseiten der Firma Cisco Systems, 2000. http://www.cisco.com.

[Dit98] DITTLER, HANS PETER: *IPv6 – Das neue Internet–Protokoll*. dpunkt.verlag, 1998.

[Fir99] *Zentrales Firewall-System für die Universität Rostock*, 1999. Studie des Rechenzentrums der Universität Rostock.

[Hab97] HABERMANN, THOMAS: *Struktur, Netzdesign und Leistungsbestimmung des ATM–Backbone–Netzes der Universität Rostock.* Diplomarbeit, Universität Rostock, Jan 1997.

[IT93] ITU-T: *X.25: Interface between Data Terminal Equipment (DTE) and Data Circuit-Terminating Equipment (DCE) for Terminals operating in the Packet Mode and connected to Public Data Networks by Dedicated Circuit*. Standard X.25, International Telecommunication Union, März 1993. Recommendation.

[Kry00] KRYPTOKOM: *Produktbeschreibungen KryptoKom KryptoWall*. Webseiten der Firma KryptoKom, 2000. http://www.kryptokom.de.

[Lan98] LANGE, CHRISTOPH: *Technische und wirtschaftliche Untersuchungen eines Kommunikationsverbundes auf ATM–Technologie*. Diplomarbeit, Universität Rostock, Mai 1998.

[Mar00] MARTIUS, KAI: *Sicherheitsmanagement in TCP/IP–Netzen*. Vieweg, Januar 2000.

[Net00] NETWORK ASSOCIATES ABTEILUNG PGP SECURITY: *Produktbeschreibungen Gauntlet Firewall*. Webseiten der Firma Network Associates Abteilung PGP Security, 2000. http://www.pgp.com.

[Tru00] TRUSTED INFORMATION SYSTEMS: *Produktbeschreibungen TIS Firewall Toolkit*. Webseiten der Firma Trusted Information Systems, 2000. http://www.tis.com.

[Uhl00] UHLIG, FRANK: *Frame Relay*. http://www.frankuhlig.de, März 2000.

[Wun97] WUNDERLICH, FREDERICK: *Integration von ATM in bestehende LANs*. Diplomarbeit, Universität Rostock, Jan 1997.

Erklärung

Hiermit versichere ich, die vorliegende Arbeit selbständig angefertigt und keine weiteren als die angegebenen Quellen benutzt zu haben.

Rostock den 30.05.2000