INSTITUT FÜR INFORMATIK

DER LUDWIG–MAXIMILIANS–UNIVERSITÄT MÜNCHEN

Diplomarbeit

Entwicklung eines Firewall-Konzepts für das Münchner Wissenschaftsnetz (MWN)

Bernhard Wager

Aufgabensteller: Prof. Dr. Heinz-Gerd Hegering

Betreuer: Dr. Gabi Dreo Rodosek
Dr. Victor Apostolescu

Abgabetermin: 15. Oktober 2002

INSTITUT FÜR INFORMATIK
DER LUDWIG–MAXIMILIANS–UNIVERSITÄT MÜNCHEN

Diplomarbeit

Entwicklung eines Firewall-Konzepts für das Münchner Wissenschaftsnetz (MWN)

Bernhard Wager

Aufgabensteller:	Prof. Dr. Heinz-Gerd Hegering
Betreuer:	Dr. Gabi Dreo Rodosek Dr. Victor Apostolescu

Abgabetermin: 15. Oktober 2002

Hiermit versichere ich, dass ich die vorliegende Diplomarbeit selbständig verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel verwendet habe.

München, den 15. Oktober 2002

. . . .
(Unterschrift des Kandidaten)

Zusammenfassung

Am Münchner Wissenschaftsnetz (MWN) sind rund 700 Institute aus unterschiedlichen Bereichen von Hochschule, Forschung und Wissenschaft angeschlossen. Die Institute verteilen sich auf mehrere Standorte im Großraum München. Das MWN vermittelt ihnen den Zugang zum Internet und zu Diensten im MWN selbst. Der Betreiber des MWN ist das Leibniz Rechenzentrum (LRZ). Zwischen dem Betreiber und den Instituten besteht ein Dienstleistungsverhältnis. Das LRZ möchte sein Dienstangebot um einen Firewall-Dienst ergänzen. Bei der Entwicklung des Dienstes sind zwei Dinge zu beachten. Auf der einen Seite stehen die Institute mit sehr unterschiedlichen Sicherheits- und Kommunikationsbedürfnissen. Auf der anderen Seite besitzt das LRZ nur begrenzte Kapazitäten, so dass es nicht jedem einzelnen Wunsch der Institute gerecht werden kann.

Um die Bedürfnisse der Institute zu ermitteln, wurde eine Umfrage durchgeführt. Durch die Umfrage wurden rund zehn Prozent der Institute und 25 Prozent der am MWN angeschlossenen Rechner erfasst. Aus der Auswertung der Umfrage wurden zwei Arten von Profilen herausgearbeitet: Diensteprofile umfassen die von den Instituten genutzten und angebotenen Dienste. Durch Kundenprofile wurden die Kunden hinsichtlich ihrer Sicherheits- und Kommunikationsbedürfnisse gruppiert. Es haben sich fünf Dienste- und vier Kundenprofile ergeben.

Auf dieser Basis konnte der Firewall-Dienst mit vier Dienstklassen (Firewall-Pakete) entwickelt werden. Durch die Firewall-Pakete werden die Dienste- und Kundenprofile abgedeckt. Gleichzeitig ist das LRZ in der Lage, diese vier standardisierten Pakete mit den zur Verfügung stehenden Kapazitäten zu beherrschen. Für die Realisierung des Dienstes wurden Möglichkeiten aufgezeigt. Dazu wurde ein State of the Art aktueller Sicherheitsmechanismen erstellt. Außerdem wurde ein Realisierungsvorschlag für die Firewall-Pakete 1 bis 3 auf der Basis der im MWN eingesetzten Router gemacht. Für das Management des Dienstes wurden Management-Aspekte analysiert, sowie Management-Prozesse identifiziert und beschrieben.

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Kapitel 1

Einleitung

Am Münchner Wissenschaftsnetz (MWN) sind rund 700 Institute aus dem Großraum München angeschlossen. Es ermöglicht die Datenkommunikation untereinander, "vermittelt den Zugang zu Servern bzw. zu Netzdiensten innerhalb des MWN, zum nationalen und internationalen Wissenschaftsnetz und zum allgemeinen Internet" [ApLä 02]. Das MWN steht den Instituten "zur Erfüllung ihrer Aufgaben aus Forschung, Lehre, Verwaltung, Aus- und Weiterbildung, Öffentlichkeitsarbeit und Außendarstellung der Hochschulen und sonstige in Art. 2 des Bayerischen Hochschulgesetzes beschriebenen Aufgaben zur Verfügung" [BADW]. Nutzungsberechtigt sind alle Mitarbeiter und Studenten der angeschlossenen Institute. Im Februar 2002 waren 53500 Benutzer registriert [ApLä 02].

Betreiber des MWN ist das Leibniz-Rechenzentrum der Bayerischen Akademie der Wissenschaften (LRZ). Dem LRZ als Betreiber stehen die 700 am MWN angeschlossenen Institute als Kunden gegenüber. Das LRZ bietet seinen Kunden neben dem Betrieb des MWN weitere Dienstleistungen an, die über das MWN genutzt werden können. Um auch zukünftig eine sichere Nutzung des MWN zu ermöglichen, wurde die Forderung nach neuen Diensten laut.

Ziel dieser Diplomarbeit ist es in diesem Zusammenhang ein Konzept für einen Firewall-Dienst zu entwickeln. Zum Bereich Sicherheit im MWN wurden bereits andere Diplomarbeiten erfolgreich abgeschlossen, so zu den Themen Security-Scanner [Pank 00] und Intrusion Detection Systeme (IDS)[Brüc 00].

1.1 Das Münchner Wissenschaftsnetz (MWN)

1.1.1 Struktur des MWN

Die über 700 am MWN angeschlossenen Institute verteilen sich auf etwa 40 Standorte [ApLä 02] im Großraum München. Die Anbindung der Standorte erfolgt durch angemietete Monomode-Lichtwellenleiter. Die Leitungen sind sternförmig auf das LRZ ausgerichtet. An großen Standorten sind die einzelnen Gebäude und Areale meist sternförmig an einen zentralen Standortverteiler angeschlossen. Dazu wurden vom LRZ eigene Glasfaserverbindungen eingerichtet. In den Gebäuden selber gibt es zwei Arten von Verkabelungen: Eine durchgehend strukturierte Verkabelung oder bei älteren Verkabelungen 10Base5-Leitungen, wobei in der Regel pro Stockwerk ein Segment verlegt ist. Insgesamt sind damit rund 19.000 Räume [ApLä 02] an das MWN angebunden, davon 40 Prozent auf

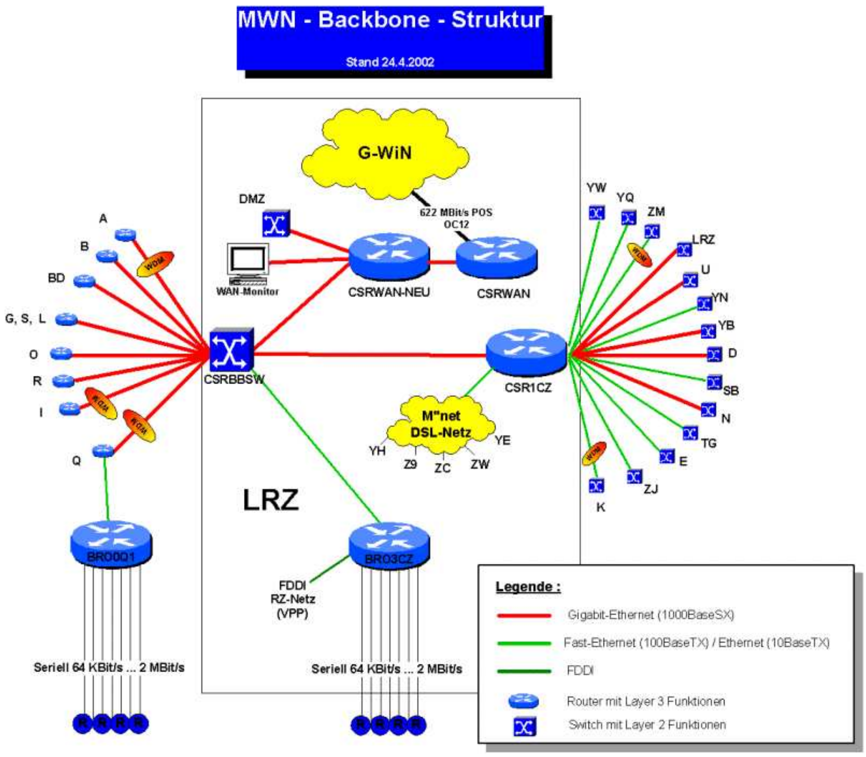

Abbildung 1.1: MWN-Backbone

der Basis von 10Base5. In den nächsten Jahren soll dieses Yellow Cable jedoch durchgehend durch eine strukturierte Verkabelung ersetzt werden.

Das MWN basiert auf der beschriebenen Leitungsinfrastruktur. Die genannten Glasfaserstrecken können durch Wavelength Division Multiplexing (WDM) jedoch nicht nur für das Datennetz, sondern auch für andere Aufgaben (z.B. Kopplung von TK-Nebenstellenanlagen) genutzt werden. Das Backbone des MWN besteht aus Routern an den großen Standorten und einem zentralen Switch im LRZ (siehe Abbildung 1.1). Die Router sind je nach Bedarf mit 100- oder 1000-Mbit/s-Ethernet an den Switch angebunden. Der Anschluss der kleinen Standorte erfolgt über einen Router im LRZ. Die Gebäude- bzw. Arealnetze sind mit dem Standortrouter verbunden. Insgesamt sind ca. 290 Routerinterfaces für diesen Zweck konfiguriert [ApLä 02]. Für die Verteilung im Gebäude sorgt ein Gebäude-Switch. Bei einer durchgehend strukurierten Verkabelung stehen 100 Mbit/s, manchmal auch 1000 Mbit/s zur Verfügung. Bei Gebäuden, in denen noch Yellow Cable zum Einsatz kommt, sind es 10 Mbit/s. In diesem Fall ist es möglich, einzelne Server direkt an den Gebäude-Switch anzuschließen.

Auf der Basis der strukturierten Verkabelung kann mit Hilfe der Switches eine logische Segmentierung vorgenommen werden. Ein auf diese Weise eingerichtetes virtuelles Local Area Network (VLAN) weist alle Eigenschaften eines gewöhnlichen LAN auf. Ein VLAN stellt eine eigene Kollisions- und Broadcastdomäne dar. Verkehr zwischen den VLANs muss deshalb geroutet werden.

Aus der geschilderten Struktur des MWN ergeben sich folgende Probleme und Möglichkeiten, die bei der Konzeption des Firewall-Dienstes zu berücksichtigen sind:

- Mit Hilfe von VLANs lässt sich für jedes Institut ein eigenes Netzsegment einrichten. Darüberhinaus kann das Institutsnetz noch weiter unterteilt werden. Denkbar ist ein eigenes Subnetz für

Server, die Dienste nach außen anbieten.

- Bei einer 10Base5-Verkabelung richtet sich die Segmentierung nicht nach Instituten, sondern nach Stockwerken. Ein eigenes Subnetz für Server lässt sich nur direkt am Gebäude-Switch einrichten.
- Vor kurzem haben sich noch viele vom durchgehenden Einsatz von Switches einen wirksamen Schutz gegen Sniffing versprochen [Rank 00]. Durch Spoofing des Address Resolution Protocols (ARP) und Tools (z. B. dsniff), die einen solchen Angriff einfach durchführbar machen, ist jedoch auch in einem geswitchten Netz Sniffing möglich. Ein wirklicher Schutz kann nur durch eine Verschlüsselung des Datenverkehrs erreicht werden. Allerdings hat dies auch Auswirkungen auf die Filtermöglichkeiten einer Firewall.
- Die im MWN eingesetzten Router (Cisco 6509 [ApLä 02]) besitzen Filtermöglichkeiten, die für das Firewall-Konzept genutzt werden können.

1.1.2 Anbindung des MWN an das Internet

An den Backbone-Switch ist neben den Standort-Routern auch ein Router angeschlossen, über den der Zugang zum Gigabit-Wissenschaftsnetz (G-WiN) des Deutschen Forschungsnetz Vereins (DFN) und damit zum Internet erfolgt. Der Anschluss besitzt eine Bandbreite von 622 Mbit/s. Andere Übergangspunkte zum Internet werden vom LRZ derzeit nicht betrieben. Der Zugang zum Internet ist von Seiten des LRZ also auf einen Punkt konzentriert. An dem Router ist außerdem eine Demilitarisierte Zone (DMZ) angeschlossen – ein eigenes Subnetz mit öffentlich zugänglichen Servern.

Für den Firewall-Dienst ergeben sich daraus folgende zu beachtende Punkte:

- Am Router zum G-WiN wird bereits eine Paketfilterung vorgenommen. Vollständig gesperrt sind die Dienste Simple Network Management Protocol (SNMP), Filesharing (eDonkey, KaZaA, Gnutella und Napster), Tunnel für Internetwork Packet Exchange (IPX) und Netbios (Port 139). Einschränkungen gibt es bei den Diensten Domain Name Service (DNS) und Mail. Außerdem werden Broadcast-Pings und ein Spoofing des Internet Protocols (IP) verhindert [Läpp 02].
- Die Einbeziehung einer zentralen Firewall an der Schnittstelle zum G-WiN macht letztlich nur Sinn, wenn keine anderen Übergänge zum Internet existieren. Das LRZ selber betreibt keine anderen Übergangspunkte. Es muss jedoch davon ausgegangen werden, dass bei den Kunden Modems und Adapter für ISDN (Integrated Services Digital Network) vorhanden sind. Seit der Verbreitung von Dialern ist damit zu rechnen, dass über diese Geräte auch unwissentlich ein Zugang zum Internet hergestellt wird.
- Die vom LRZ betriebene DMZ soll in die Überlegungen mit einbezogen werden.

1.1.3 Institute – Kunden des MWN

Am MWN sind über 700 Institute aus unterschiedlichen Einrichtungen angeschlossen. Ein Großteil der Institute gehört der Bayerischen Akademie der Wissenschaften, der Ludwig-Maximilians-Universität München (LMU), der Technischen Universität München (TUM) sowie der Fachhochschulen München und Weihenstephan an. Weitere Einrichtungen sind die Hochschule für Musik und Theater, Deutsches Herzzentrum, Bayerisches Nationalmuseum, Studentenwerk München und deren

Studentenwohnheime, Max-Planck-Gesellschaft, Landesamt für Forst- und Waldwirtschaft und viele mehr. Der Begriff Institut ist dabei sehr weit gefasst. Darunter können Lehrstühle, Institute oder Fakultäten der Hochschulen fallen, ebenso eine der genannten Einrichtungen oder Teile davon. Auch Studentenwohnheime werden als Institute aufgefasst. Verwaltungseinheiten der Hochschulen bilden ebenfalls eigene Institute. Dadurch muss innerhalb eines Instituts keine Abtrennung des Verwaltungsbereichs erfolgen, was notwendig wäre um Haushalts- und Personaldaten speziell zu schützen.

Auf Grund der Vielfältigkeit der Institute ergeben sich große Unterschiede. Zunächst unterscheiden sich die Institute hinsichtlich ihrer Größe, die an der Zahl der Benutzer des MWN, an der Zahl der angeschlossenen Rechner, dem Umfang des zur Verfügung stehenden IP-Adressbereichs oder der Zahl der vorhandenen Subnetze festgemacht werden kann.

Für den Firewall-Dienst von großer Bedeutung sind die zu erwartenden unterschiedlichen Kommunikationsinteressen der Institute. Neben Klassikern wie World Wide Web (WWW), File Transfer Protocol (FTP) oder E-Mail muss mit einer breiten Palette von Diensten gerechnet werden, die von den Kunden genutzt werden wollen. Gleiches gilt für das Angebot von Diensten. Viele Kunden betreiben aus diesem Grund eigene Server. Das notwendige Know-how für die Konfiguration und Pflege der Server ist umfangreich. Nicht alle Administratoren sind auf dem aktuellsten Kenntnisstand oder es mangelt an den notwendigen Personalkapazitäten.

Einige Institute betreiben bereits eigene Firewalls zum Schutz ihrer Netze. Dies setzt gut informierte und engagierte Mitarbeiter voraus, die nicht bei allen Kunden vorhanden sein können. Auch der Wissensstand über die Gefahren und Probleme bei der Nutzung des Internet ist sehr unterschiedlich. Das Wissen über aktive Inhalte, Cookies, Viren, Würmer, Dialern oder Privacy sowie zu möglichen Schutzmaßnahmen ist sehr unterschiedlich ausgeprägt. Weiterhin ist mit speziellen Schwierigkeiten wie Modems oder offenen Ports bei einzelnen Instituten zu rechnen.

Aus diesen Gründen muss erwartet werden, dass von den Kunden ganz unterschiedliche Anforderungen an den Firewall-Dienst gestellt werden. Diese Anforderungen sind im einzelnen nicht bekannt. Es muss deshalb erst noch festgestellt werden, welche Dienste von den Kunden häufig genutzt bzw. angeboten werden, welche Einschränkungen (die sich aus dem Firewall-Dienst zwangsweise ergeben) akzeptiert werden, in welcher Form die Kunden ihre eigenen Dienstangebote betreiben wollen und welche Schutzmaßnahmen von den Kunden bereits getroffen wurden.

Es muss festgehalten werden, dass der Firewall-Dienst nur einen Beitrag zur Erhöhung der Sicherheit leisten kann. Wollen die Kunden eigene Server betreiben, so muss der Firewall-Dienst den Zugriff darauf gestatten. Auf die Pflege dieser Server hat der Firewall-Dienst keinen Einfluss. Praktisch jede eingesetzte Software weist immer wieder Sicherheitslücken auf. Auch spezielle Sicherheitssoftware wie Secure Shell (SSH) bleibt davon nicht verschont. Als besonders kritisch sind Modems oder ISDN-Adapter in den Instituten zu bewerten, da sie als Nebeneingang zum MWN das gesamte Firewall-Konzept aushebeln können.

1.1.4 LRZ – Betreiber des MWN

Das LRZ ist das gemeinsame Rechenzentrum der LMU, der TUM und der Bayerischen Akademie der Wissenschaften. Es ist der Betreiber des MWN.

1.1.5 Kompetenzenverteilung

Das LRZ ist “grundsätzlich für Planung, Betrieb und Management des MWN bis hin zur Steckdose im Arbeitsraum zuständig” [ApLä 02]. Ausnahmen bestehen in den Bereichen der medizinischen Fakultäten, der Informatik der TU sowie der Fachhochschule (FH) München. Das LRZ koordiniert die Verteilung der IP-Adressen und den Namensraum. Neben den öffentlichen IP-Adressen werden zum Teil auch private IP-Adressen im MWN geroutet.

Auf Seiten der Institute muss ein Netzverantwortlicher als Ansprechpartner für den Betreiber benannt werden. Nach den Netzbenutzungsrichtlinien [Läpp 01] haben die Netzverantwortlichen folgende Aufgaben:

- “Verwaltung der zugeteilten Namens- und Adressräume,
- Führung einer Dokumentation über die ans MWN angeschlossenen Endgeräte bzw. Netze,
- Zusammenarbeit mit dem LRZ bei der Planung und Inbetriebnahme von Erweiterungen der Gebäudenetze (neue Anschlusspunkte, neue Netzstrukturen, Segmentverlängerungen, etc.),
- Mitarbeit bei der Fehlerbehebung (z.B. Durchführen von mit dem LRZ abgestimmten Tests zur Fehlereingrenzung),
- Zusammenarbeit mit dem LRZ bei der Eindämmung missbräuchlicher Netznutzung.”

Es ist sinnvoll bei der Entwicklung des Firewall-Dienstes die Netzverantwortlichen einzubeziehen. Zum einen ist nicht klar, was die Kunden von dem neuen Dienst erwarten. Zum anderen soll der Firewall-Dienst auch der Eindämmung missbräuchlicher Nutzung dienen, woran die Netzverantwortlichen beteiligt sind.

1.1.6 Zugänge zum MWN

Eine Verbindung zum MWN von außerhalb kann über die vom LRZ betriebenen Einwahlserver erfolgen. Es stehen rund 1000 Einwahlzugänge zur Verfügung [ApLä 02]. Dabei ist eine Authentifizierung am Radius-Dienst des MWN notwendig. Neben dem Radius-Server des LRZ existieren 70 weitere Radius-Zonen im MWN. Auch aus dem Internet ist ein Zugang zum MWN per Virtual Private Network (VPN) möglich. Dazu hat das LRZ VPN-Server auf der Basis von PPTP (Point-to-Point Tunneling Protocol) eingerichtet. Die Authentifizierung erfolgt auch in diesem Fall über den Radius-Dienst.

Innerhalb der an das MWN angeschlossenen Gebäude existieren an einigen Orten Zugangsmöglichkeiten für mobilen Endgeräte. Dafür stehen Access-Points für WLANs (Wireless Local Area Network) und entsprechend konfigurierte Datensteckdosen bereit. Diese Zugänge bilden ein separates VLAN. Ein Übergang zum restlichen MWN ist nur über den VPN-Server möglich. Dadurch ergibt sich wiederum die Notwendigkeit der Authentifizierung am Radius-System.

Bei fest angeschlossenen Geräten bestünde die Möglichkeit am Switch die MAC-Adressen (Media Access Control) zu registrieren. Darauf wird auf Grund des hohen Verwaltungsaufwands jedoch verzichtet [ApLä 02]. Deshalb ist sicherzustellen, dass nur berechtigte Nutzer Zugang zu den Rechnern haben. Bei den in öffentlichen Räumen mit Personal Computern (PC) stehenden Geräten muss eine Authentifizierung erfolgen. Im übrigen hat der Netzverantwortliche dafür zu sorgen, dass nur berechtigten Personen der Zugang zu den Rechnern möglich ist. Ob dies durchgehend sichergestellt ist, darf bezweifelt werden. Außerdem muss mit frei zugänglichen Datensteckdosen gerechnet werden. In Zukunft soll deshalb auf der Basis von IEEE (Institute of Electrical and Electronics Engineers) 802.1x und dem Radius-Dienst in allen Bereichen eine Authentifizierung erzwungen werden [ApLä 02].

1.1.7 Weitere Dienstleistungen des LRZ im Zusammenhang mit dem MWN

Bereits eingegangen wurde auf folgende Dienste des LRZ: Betrieb des MWN, Anschluss an das G-WiN, Koordination des Adress- und Namensraums, VPN und Radius. Darüber hinaus bietet das LRZ seinen Kunden eine Vielzahl weiterer Dienstleistungen an. Diese müssen bei der Konzeption des Firewall-Dienstes berücksichtigt werden.

DNS und Dynamic Host Configuration Protocol (DHCP): Von vielen Kunden werden eigene DHCP- und DNS-Server betrieben. Hierbei kommt es immer wieder zu fehlerhaften Konfigurationen. Deshalb bietet das LRZ seinen Kunden an, diese Dienste auf vom LRZ betriebene Server auszulagern. Gerade beim DNS ist es immer zu Betriebsstörungen gekommen. Deshalb können DNS-Anfragen nur an interne Server gerichtet werden. Von diesen haben nur einige die Berechtigung mit Name-Servern im Internet zu kommunizieren.

E-Mail: Das LRZ betreibt Mail-Server, auf denen zur Zeit 19.000 Mail-Boxen eingerichtet sind. Darüber hinaus betreiben viele Institute eigene Mail-Server. Von diesen haben aber nur wenige, zuverlässige Server die Berechtigung Mails direkt aus dem Internet zu empfangen. Dadurch soll der Missbrauch von schlecht konfigurierten Servern als Spam-Relay verhindert werden. Alle Mail-Server, die nicht direkt Mails empfangen können, müssen die Mail-Relays des LRZ benutzen. Dabei wird die Gültigkeit der E-Mail-Adressen überprüft. Attachments mit ausführbaren Inhalten werden gefiltert. Zukünftig soll außerdem eine Überprüfung auf Viren und Würmer stattfinden [Läpp 02].

WWW und FTP: Die Benutzer des MWN haben die Möglichkeit auf vom LRZ betriebenen Rechnern, virtuelle WWW-Server einzurichten (zur Zeit 130 Stück [ApLä 02]). Dadurch wird den Kunden die Konfiguration und Pflege eigener Web-Server erspart. Allerdings kann das LRZ nur Standardkonfigurationen zur Verfügung stellen. Daneben haben die Institute die Möglichkeit anonyme FTP-Server beim LRZ einzurichten.

File- und Backup-Service: Die Daten der WWW- und Mail-Server werden auf einem verteilten Filesystem auf der Basis des Andrew File System (AFS) gespeichert. Der Service wird überwiegend rechenzentrumsintern verwendet, kann aber auch von anderen Stellen im MWN genutzt werden. Dadurch wird der Zugriff auf einen einheitlichen Datenbereich möglich. Mit Tivoli Storage Manager (TSM) wird MWN-weit eine Backup-Dienst angeboten. Täglich werden etwa 650 GB [ApLä 02] an Daten gesichert.

Proxies und Caches: Für die Dienste WWW, FTP und die Streaming-Protokolle RTSP (Real Time Streaming Protocol) und MMS (Microsoft Media Server) betreibt das LRZ Proxies. Darüber hinaus steht ein Socks-Proxy zur Verfügung. Die WWW- und FTP-Proxies sind zusätzlich mit einem Cache ausgestattet. Neben den vom LRZ betriebenen Proxies existieren im MWN weitere, die von verschiedenen Instituten betrieben werden. Zum Großteil handelt es sich dabei um WWW-Proxies. In der Regel dürfen diese Proxies von allen Benutzern des MWN verwendet werden.

Die beschriebenen Angebote des LRZ werden von zentralen Servern erbracht. Auch das Management dieser Dienste erfolgt zentral durch das LRZ. Bei den WWW-Proxies ist hingegen ein anderer Ansatz zu erkennen. Die etwa 25 Proxies sind über das gesamte MWN verteilt. Das Management erfolgt dezentral durch das Institut, das den Proxy aufgestellt hat. Damit andere Institute von den vorhandenen Proxies erfahren können, hat das LRZ eine Liste ins WWW gestellt. Zusätzlich zum dezentralen Management sind also Koordinationsmaßnahmen notwendig, die vom LRZ erbracht werden können.

Ein dezentrales Management ist nicht allen Bereichen sinnvoll. Bei den Diensten E-Mail, DNS und DHCP ist eine Tendenz zu einer stärkeren Zentralisierung zu erkennen. Die Begründung ergibt sich aus dem hohen Koordinationsaufwand und/oder den zahlreichen Fehlkonfigurationen. Durch entsprechende Einschränkungen im Netzverkehr wird eine Nutzung dieser zentralen System zum Teil erzwungen.

Aus dem beschriebenen Dienstleistungsangebot ergeben sich verschiedene Möglichkeiten und Fragestellungen, die im Rahmen des Firewall-Konzepts zu beachten sind.

- Die Kunden haben die Möglichkeit, eigene Dienstangebote auf Server des LRZ auszulagern. Dadurch kann erreicht werden, dass die Institutsnetze vor Zugriffen von außen gänzlich abgeschottet werden können. Zusätzlich ergibt sich für die Kunden der Vorteil, dass die Server vom qualifizierten Personal des LRZ betrieben werden.
- Der Mail-Service des LRZ führt bereits jetzt Filterungen auf der Ebene des Application-Layers durch, zusätzlich erfolgt eine Content-Filterung. Da ein großer Teil der Institute gezwungen ist die Mail-Relays zu verwenden, nutzen viele Kunden in diesem Bereich bereits Firewall-Funktionalitäten. Für eine umfassende Lösung soll der Dienst noch um einen Virenscanner ergänzt werden, der auch in der Lage sein muss, Archive und komprimierte Dateien zu analysieren.
- Für die populären Dienste des Internet stehen im LRZ und auch im übrigen MWN Proxies zur Verfügung. Auf diese Weise kann der Nutzer eines Dienstes sich und seinen Rechner hinter dem Stellvertreter verstecken.
- Für die zukünftigen Funktionen des Firewall-Dienstes muss geklärt werden, ob sie besser durch zentrale oder verteilte Komponenten erbracht werden.
- Das Management des Firewall-Dienstes oder einzelner Teile davon kann zentral oder dezentral erfolgen. Bei einem dezentralen Management ist eine Koordinationsinstanz notwendig, um eine Zusammenarbeit zwischen den Instituten zu ermöglichen und den Betreiber bei anderen Managementaufgaben nicht zu beeinträchtigen.

1.1.8 Vertrauenswürdigkeit des MWN

Auf Grund der unterschiedlichen Kunden sowie der großen Zahl der Benutzer und angeschlossenen Rechner muss das MWN als ein sehr uneinheitliches Netz aufgefasst werden. Das MWN ist im Vergleich zum Internet nicht unbedingt vertrauenswürdiger. Zwar kann wegen der notwendigen Authentifizierung der Verursacher einer Störung schnell identifiziert werden. Allerdings ist der Zwang zur Authentifizierung noch nicht in allen Bereichen sichergestellt und es muss mit einer unerlaubten Nutzung von Zugangskennungen (schwache Passwörter, Social Engineering, Sniffing) gerechnet werden.

Werden Server-Dienste betrieben, die aus dem Internet erreichbar sein sollen, ist es möglich dass diese gehackt werden und als Sprungbrett für weitere Angriffe im MWN genutzt werden. Das Hacken von Rechnern ist nicht nur eine theoretische Möglichkeit, sondern in der Vergangenheit auch schon öfters vorgekommen. Auch eine Firewall kann nur begrenzt zwischen einem gutartigen und einem bösartigen Zugriff auf einen Rechner unterscheiden, so dass in Zukunft dieses Problem bestehen bleiben wird.

1.2 Vorgehen

Die einzelnen Schritte zur Entwicklung des Firewall-Konzepts sind in Abbildung 1.2 dargestellt. Zunächst müssen die Anforderungen an den Firewall-Dienst zusammengestellt werden. Sie ergeben sich aus der Problembeschreibung. In der Problembeschreibung wurde u. a. festgestellt, dass sich die 700 am MWN angeschlossenen Institute hinsichtlich Größe, Kommunikationsinteressen und Wissensstand unterscheiden. Deshalb ist zu erwarten, dass von Seiten der Institute sehr unterschiedliche Anforderungen an den Firewall-Dienst gestellt werden. Wie die Anforderungen der Kunden im einzelnen aussehen, ist jedoch noch nicht klar. Dies soll mit Hilfe einer Umfrage ergründet werden. Auf der anderen Seite hat die Analyse der Problemstellung ergeben, dass das LRZ als Betreiber des MWN nur begrenzte Kapazitäten für den Betrieb des Firewall-Dienstes zur Verfügung hat. Aus diesem Grund ist es nicht möglich den Bedürfnissen eines jeden einzelnen Instituts im Detail gerecht zu werden. Deshalb sollen aus den Einzelergebnissen der Umfrage Profile gebildet werden. Durch Diensteprofile sollen die wichtigen und häufig genutzten Dienste zusammengefasst werden. Darüber hinaus werden die befragten Institute in Bezug auf ihre Sicherheitsanforderungen in Gruppen eingeteilt und daraus Kundenprofile entwickelt.

Im dritten Schritt erfolgt die Dienstbeschreibung. Diese wird eine kleine Anzahl standardisierter Paketlösungen umfassen. Diese Firewall-Pakete sollen die in der Anforderungsanalyse herausgearbeiteten Dienste- und Kundenprofile möglichst gut abdecken. Es ist das Ziel, auf diese Weise sowohl einen kundenorientierten, als auch vom LRZ bewältigbaren Dienst zu entwickeln.

Die abschließende vierte Phase umfasst die Realisierung des Dienstes. Es sollen einige für den Firewall-Dienst relevanten Produkte und Konzepte betrachtet werden. Ziel ist es jedoch nicht, eine Evaluation und Produktauswahl vorzunehmen. Vielmehr soll ein Überblick über aktuelle Techniken und Verfahren gewonnen werden (State of the art), die für die Realisierung des Firewall-Dienstes verwendet werden können. Unabhängig vom konkreten Produkt oder Konzept werden daraus Module gebildet, aus denen die entwickelten Firewall-Pakete aufgebaut sein können. Den Abschluss der Arbeit bildet ein für das LRZ geeignetes Betriebskonzept.

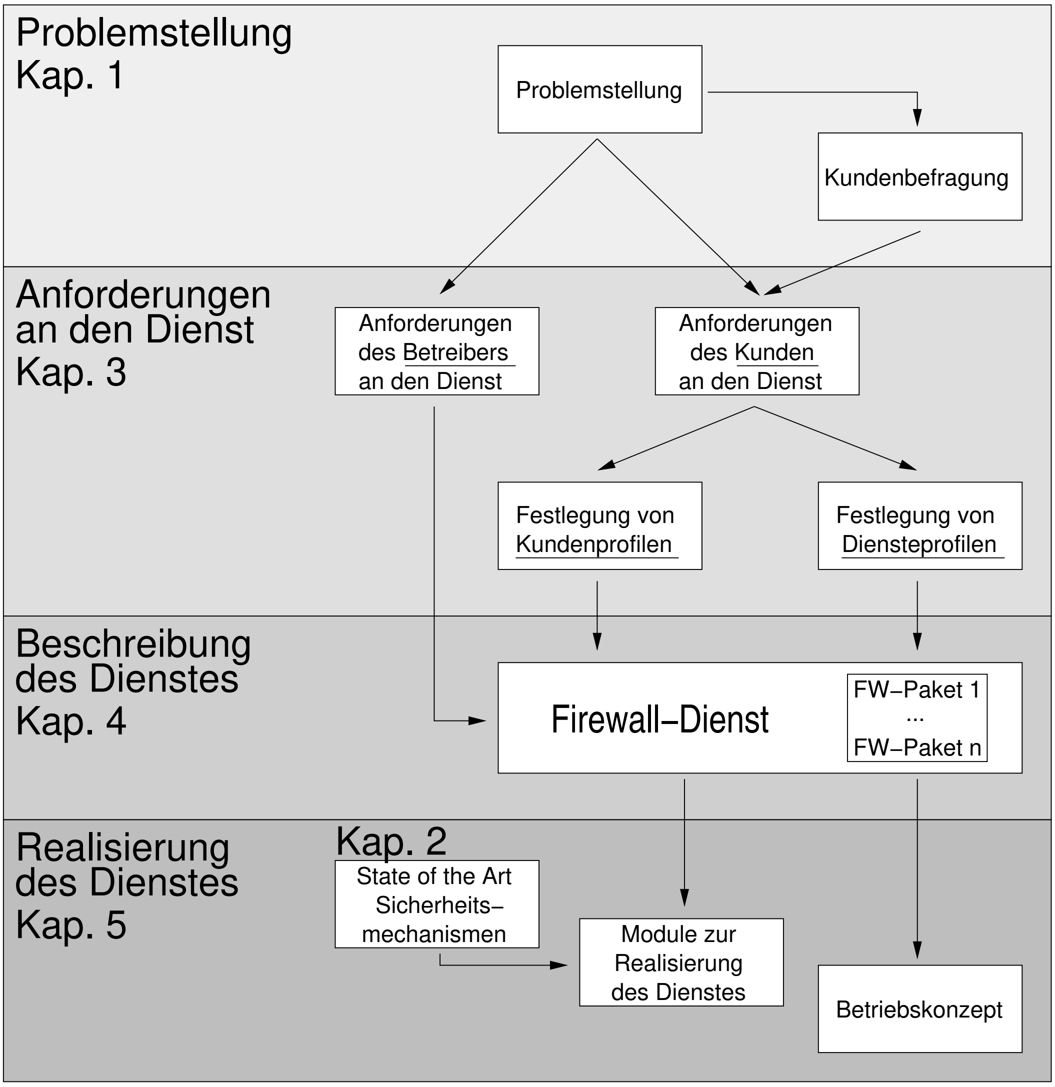

Abbildung 1.2: Vorgehensmodell für die Konzeption des Firewall-Dienstes

Kapitel 2

State of the Art

Da das Ziel dieser Diplomarbeit die Konzeption eines Firewall-Dienstes ist, soll zunächst ein Überblick über aktuelle Sicherheitsmechanismen in Form eines State of the Art gewonnen werden. Dazu werden einige Firewall-Lösungen vorgestellt. Diese Betrachtungen stellen keine Evaluation dar, sondern sollen den aktuellen Stand der Technik wiedergeben und mit den verschiedenen Sicherheitsmechanismen vertraut machen. Zu Beginn des Kapitels (Abschnitt 2.1) werden einige grundlegende Begriffe und Firewall-Architekturen eingeführt.

Viele Firewall-Lösungen werden auf der Basis von Linux aufgebaut. Auch innerhalb des MWN setzen viele Institute auf Linux als Firewall, wie die im nächsten Kapitel vorgestellte Umfrage ergeben hat. Aus diesem Grund werden in Abschnitt 2.2 verschiedene Bestandteile einer Linux-Firewall betrachtet. Die im vorherigen Kapitel vorgenommene Beschreibung des MWN hat gezeigt, dass die Institute über Router vom Typ Cisco Catalyst 6509 an den Backbone des MWN angeschlossen sind. Die Firewall-Mechanismen, die diese Router mitbringen, werden in Abschnitt 2.3 vorgestellt. In Abschnitt 2.4 werden einige “ausgewachsene” Firewall-Lösungen präsentiert: Astaro Security Linux, Firewall-1 von Checkpoint und PIX 500 von Cisco.

Zum Abschluss (Abschnitt 2.5) des Kapitels werden die Firewall-Konzepte der Universitäten Passau und Karlsruhe vorgestellt.

2.1 Grundsätzliches zu Internet-Firewalls

2.1.1 Rechnerzentrierte und netzwerkzentrierte Sicherheit

Grundsätzlich gibt es zwei Ansätze zur Erhöhung der Sicherheit in einem Rechnernetz:

- Rechnerzentrierte Sicherheit,
- netzwerkzentrierte Sicherheit.

Bei der rechnerzentrierten Sicherheit setzt der Schutz auf den einzelnen Rechner selber an. Geeignete Maßnahmen sind beispielsweise Benutzerauthentifizierung am Rechner, Vergabe von Rechten an Ressourcen und die Installation von Virenscannern. Die Schwierigkeit liegt darin, dass jeder Rechner für sich geschützt werden muss. Die Vielfalt der Hardware, Betriebssysteme und Programme vergrößern das Problem. Die Behebung von Fehlern und Sicherheitslücken (beispielsweise in den Implementierungen des Protokoll-Stacks) und die unterschiedlichen Konfigurationen verursachen große Anstrengungen. Der Aufwand steigt mit der Zahl der Rechner.

Im Gegensatz dazu wird bei der netzwerkzentrierten Sicherheit ein Rechnernetz geschützt. Mit Hilfe einer Firewall werden zwei Netze physisch und logisch getrennt. Beispielsweise ein Firmennetz vom Internet oder innerhalb einer Firma das Netz der Personalabteilung vom Netz der Produktion. Der Verkehr zwischen den Netzen wird von der Firewall kontolliert, unerwünschter Verkehr wird gefiltert.

Der Einsatz einer Firewall hat mehrere Vorteile:

- Die Firewall stellt einen zentralen Ort für die Umsetzung von Sicherheitsentscheidungen dar. Die getroffenen Entscheidungen werden an dieser Stelle in konkrete Maßnahme umgesetzt. Die Konsistenz einzelner Sicherheitsentscheidungen ist leichter zu überprüfen.
- Die Firewall ist der einzige Verbindungsknoten zwischen den Netzen. Alle Daten werden über diesen Knoten ausgetauscht. Auf diese Weise können Sicherheitsentscheidungen besser durchgesetzt werden. Verstöße sind leichter zu erkennen.
- Durch die Firewall wird die Angriffsfläche verkleinert. Statt auf die einzelnen Rechner konzentriert sie sich auf die Firewall. Die Angriffsfläche ist besser zu überschauen und zu überwachen.

Eine Firewall hat jedoch auch ihre Grenzen:

- Ein Angriff von innen kann von der Firewall nicht verhindert werden.
- Gibt es weitere Verbindungen zwischen den Netzen, kann die Firewall umgangen werden. Insbesondere ein Modem im geschützten Netz ist problematisch.
- Von dem die Firewall passierenden Verkehr können weiterhin Gefahren ausgehen.

Die Entscheidung welche Daten die Firewall passieren können, basiert häufig auf einem Kompromiss zwischen Sicherheits- und Nutzungsinteressen. Deshalb kann im geschützten Netz nicht vollständig auf eine Sicherung der einzelnen Rechner verzichtet werden. Man kann sich jedoch auf bestimmte Dienste und Rechner konzentrieren. Wird beispielsweise die Entscheidung getroffen, dass Java-Applets grundsätzlich zugelassen sind, so müssen die eingesetzten Browser und Java Virtual Machines auf allen Rechnern regelmäßig aktualisiert werden. Wird auf einem bestimmten Rechner ein SSH-Zugang ermöglicht, so muss der SSH-Dämon auf diesem Rechner gewissenhaft gepflegt werden.

Es werden zwei Grundtypen von Firewalls unterschieden:

- IP-Paket-Filter,
- Proxies.

Eine gute Firewall-Lösungen besteht aus Komponenten beider Grundtypen.

2.1.2 IP-Paket-Filter

Dieser Typ ist häufig auf Routern implementiert und bildet die Grundlage eines jeden Firewall-Produkts. Ein IP-Paket-Filter arbeitet bezogen auf das TCP/IP-Referenzmodell (TCP: Transport Control Protocol) in der Internetschicht. Durch eine Auswertung der Header der Protokolle der Internet- und Transportschicht werden Informationen gewonnen und mit den vorgegebenen Filterregeln verglichen. Trifft eine Regel zu, wird eine konfigurierte Aktion auf das IP-Paket angewandt. Dabei kann es sich z. B. um das Verwerfen oder Loggen des Pakets handeln. Je nach verwendetem Protokoll stehen unterschiedliche Informationen zur Auswertung zur Verfügung. Beispielsweise gibt es bei TCP im Gegensatz zu UDP (User Datagram Protocol) die Möglichkeit die Status-Flags und Sequenznummern mit in die Filterentscheidungen einzubeziehen.

Der Paket-Filter muss darauf vorbereitet sein, dass die Header-Felder der Pakete manipuliert sein können. Beispielsweise kann ein von außen kommendes Paket als Source-Adresse eine Adresse des internen Netzes aufweisen (Spoofing). Die Firewall sollte ein solches Paket verwerfen. Probleme bereiten außerdem fragmentierte Pakete. Da nur das erste Fragment den Header des Transport-Protokolls enthält, können die nachfolgenden Fragmente nicht mehr vollständig überprüft werden. Die Art und Weise, wie eine Firewall fragmentierte Pakete verarbeitet, kann ein Kriterium bei der Auswahl eines Firewall-Produkts sein.

Dynamische Paketfilter

Die IP-Paket-Filter können weiter in statische und dynamische Paketfilter unterteilt werden. Ein statischer Filter trifft bei jedem Paket die Filterentscheidung unabhängig von vorangegangenen Paketen. Dadurch ist er einfach zu implementieren. Die dynamischen Paketfilter versuchen im Gegensatz dazu, den Zustand der einzelnen Verbindungen mit in die Filterentscheidung einzubeziehen. Der Begriff Verbindung bezieht sich in diesem Zusammenhang nicht nur auf TCP, sondern auch auf andere Protokolle, wie UDP und ICMP (Internet Control Message Protocol). Die Anfrage an einen DNS-Server und dessen Antwort wird z. B. auch als Verbindung aufgefasst, obwohl hierbei in der Regel das verbindungslose UDP als Transportprotokoll eingesetzt wird.

Mit dieser Methode kann man z. B. festlegen, dass der Aufbau einer Verbindung nur von innen nach außen erlaubt ist und alle von außen kommenden Pakete von der Firewall abgewiesen werden. Kommt ein Paket aus der erlaubten Richtung an der Firewall an und kann es keiner bestehenden Verbindung zugeordnet werden, so wird angenommen, dass es eine neue Verbindung eröffnet. Die Verbindung wird daraufhin intern gespeichert und der Status "new" zugeordnet. Für die Antwortpakete aus der anderen Richtung wird eine temporäre Öffnungen in der Firewall geschaffen. Es können nun also auch Pakete aus der anderen Richtung passieren, solange die entsprechende Verbindung besteht (deshalb dynamische Paketfilterung). Von außen kommende Pakete werden also nur durch die Firewall gelassen, wenn sie einer Verbindung zugeordnet werden können. Die Verbindung wechselt dann in den Zustand "established".

Die Zuordnung einzelner Pakete zu einer Verbindung geschieht mit Hilfe der Source- und Destination-Adresse sowie des Source- und Destination-Ports. Bei ICMP werden zur Identifizierung einer Verbindung statt Quell- und Zielport andere Informationen verwendet, wie Nachrichtentyp, Code und ID. Bei TCP können die im Protokoll bereits enthaltenen Statusinformationen (Flags und Sequenznummmern) mit einbezogen werden.

Eine Verbindung bleibt höchstens solange bestehen, bis ein Timeout greift. Im Falle von TCP kann das Ende der Verbindung außerdem durch den expliziten Verbindungsabbau festgestellt werden. Dazu werden Status-Flags (FIN, RST) ausgewertet. Bei ICMP gibt es Nachrichten die aus einem Request-Response-Paar bestehen (z.B. echo request, echo response). In diesem Fall kann nach Eingang des Response-Pakets die Verbindung bereits wieder beendet werden.

Bestimmte ICMP Nachrichten dienen dazu einem Host Informationen über den Status einer TCP- oder UDP-Verbindung mitzuteilen. Ein Beispiel ist die Nachricht "Host unreachable", die an den

Ausgangspunkt einer Verbindungsanfrage zurückgeschickt wird, wenn der angefragte Dienst nicht erreichbar ist. Man kann einen dynamischen Paketfilter häufig so konfigurieren, dass er solche ICMP-Pakete passieren lässt, soweit ein Bezug zu einer anderen Verbindung besteht. Der zugehörige Eintrag in der intern verwalteten Verbindungstabelle erhält den Status "related".

Die dynamische Paketfilterung stellt größere Anforderungen an die Implementierung und die Ressourcen, da der Zustand aller Verbindungen intern verwaltet werden muss. Ein dynamischer Paketfilter kann jedoch die Performance verbessern. Bei einem statischen Paketfilter muss für jedes einzelne Paket von neuem der gesamte Regelsatz durchgegangen werden. Bei den dynamischen Paketfiltern ist dies nur für Pakete notwendig, die eine neue Verbindung initiieren. Bei den Folgepaketen reicht die Zuordnung zur entsprechenden Verbindung aus.

Anwendungen mit mehreren TCP-Verbindungen

Bei verschiedenen Internet-Anwendungen werden mehrere TCP-Verbindungen benutzt. Gute dynamische Paketfilter können die Beziehungen zwischen solchen zusammengehörenden Verbindungen erkennen. Ein Kriterium bei der Auswahl eine Paketfilters können die auf diese Weise unterstützten Anwendungen sein.

Das klassische Beispiel ist FTP. Es unterhält neben der Steuerungsverbindung eine oder mehrere Datenverbindungen für den eigentlichen Datentransfer. Beim aktiven FTP werden die Datenverbindungen vom Server aus aufgebaut, also in der zur Steuerungsverbindung entgegengesetzten Richtung. Der Port, auf dem der Server den Client kontaktieren soll, wird dem Server über die Steuerungsverbindung mitgeteilt. Dazu sieht FTP das Port-Kommando vor. Hilfsroutinen von guten dynamischen Paketfiltern können bei manchen Anwendungsprotokollen solche Informationen aus den transportierten Daten entnehmen. Man kann die dynamischen Paketfilter dann so konfigurieren, dass sie auch Pakete durchlassen, die zwar nicht direkt zu einer bestehenden Verbindung gehören, aber zu ihr in Bezug stehen. Die Hilfsroutinen für FTP beispielsweise nehmen dazu in den internen Tabellen des Paketfilters einen Eintrag für eine Datenverbindung vor, sobald sie ein PORT-Kommando in der Steuerungsverbindung feststellen und tatsächlich eine entsprechende Verbindung aufgebaut wird. Diese Verbindung erhält den Status "related".

Die Hilfsroutinen können aber auch in anderer Hinsicht nützlich sein. Bleiben wir beim Beispiel FTP, diesmal aber passives FTP. Angenommen der Paketfilter ist so eingerichtet, dass er nur bestimmte Dienste zulässt. Um FTP zu ermöglichen, muss der Paketfilter Verbindungsanfragen des Clients auf Port 21 zulassen. In Kombination mit der FTP-Hilfsroutine der dynamischen Filterung muss aber kein zusätzlicher Portbereich für die Datenverbindungen geöffnet werden. Der Port, auf dem der Server die Datenverbindung erwartet, wird mit dem PASV-Kommando erfragt. Wie beim aktiven FTP kann diese Information von der Hilfsroutine ermittelt werden und es wird eine zusätzliche "related" Verbindung eingetragen.

Network Address Translation (NAT)

Neben der reinen Filterung ist auch eine Veränderung der Headerinformationen durch den IP-Paket-Filter möglich. Bei NAT werden die Felder Source Address und Destination Address des IP-Headers, sowie Source Port und Destination Port des TCP- und UDP-Headers manipuliert. Je nach nach Art der Änderung spricht man auch von Source NAT (SNAT) und Destination NAT (DNAT). Zwei Formen von NAT sind Masquerading und Port Forwarding.

Masquerading wird verwendet, um ein Netz mit Clients nach außen zu verbergen. Dazu werden von der Firewall die Source-Adressen der Clients durch die Adresse des externen Interfaces der Firewall ersetzt. Nach außen ist auf diese Weise nur noch die IP-Adresse der Firwall sichtbar. Häufig wird Masquerading zusammen mit privaten IP-Adressen eingesetzt. Da private IP-Adressen im Internet nicht geroutet werden, können die Clients von außen nie direkt erreicht werden. Da über die Firewall gleichzeitig Verbindungen mehrerer Clients laufen können, müssen von außen kommende Pakete an den richtigen Client zugestellt werden können. Deshalb wird neben der Source-Adresse auch der Source Port verändert. Für jede Verbindung wird eine neue Portnummer gewählt. Darüber kann die Zuordnung zum richtigen Client sichergestellt werden. Wie bei der dynamischen Paketfilterung müssen deshalb auch bei NAT intern die Verbindungen verwaltet werden.

Port Forwarding kann zum Schutz von Servern eingesetzt werden, die sich hinter der Firewall befinden. Nach außen tritt nur die Firewall in Erscheinung. Alle Dienstanfragen werden an die Firewall gestellt. Je nach angeforderten Dienst leitet sie die Verbindung an den entsprechenden Server weiter. Dazu wird die Destination-Adresse durch die Adresse des entsprechenden Server ersetzt.

2.1.3 Proxies

Proxies können als Bestandteile eines Firewall-Produkts oder in Form eigener Server realisiert sein. In begrenztem Maße finden sich Proxies auch auf Routern. Die Verbindung zwischen Client und Server wird auf dem Proxy unterbrochen. Stattdessen besteht je eine Verbindung zwischen Client und Proxy, sowie zwischen Proxy und Server.

Ein Client im geschützten Netz richtet seine Anfragen nur an den Proxy, der stellvertretend für den Client die Verbindung zum Server herstellt. Ähnlich sieht es aus, wenn im geschützten Netz ein Server betrieben wird, der Dienste für Rechner außerhalb zur Verfügung stellt. Ein Client außerhalb des geschützten Netzes kann nicht direkt mit dem Server in Verbindung treten, sondern muss die Anfrage an den Proxy richten. Der Proxy macht dann selber eine entsrpechende Anfrage an den Server und gibt die erhaltenen Antworten an den Client zurück.

Auf diese Weise ist nach außen nur der Proxy sichtbar. Im Gegensatz zu NAT (auch damit kann das geschützte Netz verborgen werden) erfolgt nicht nur eine Ersetzung der IP-Adressen, sondern die Verbindung wird vollständig unterbrochen. Je nach dem in welcher Schicht des TCP/IP-Referenzmodells der Proxy arbeitet, werden Application Level Gateways (ALG) und Circuit Level Gateways (CLG) unterschieden.

Application Level Gateways

In diesem Fall arbeitet der Proxy in der Anwendungsschicht. Vom Prinzip ist er ein vollwertiger Server, der als einziger Ansprechpartner für das geschützte Netz zur Verfügung steht. Aus diesem Grund muss der Proxy das jeweilige Anwendungsprotokoll vollständig unterstützen. Der Unterschied zu einem Server besteht nur darin, dass der Proxy die Inhalte nicht selbst liefert, sondern dazu den eigentlich angeforderten Server kontaktieren muss. In dieser Rolle fungiert der Proxy als Client. Ist mit dem Proxy ein Cache verknüpft, so relativiert sich diese Aussage. Viele Inhalte müssen dann nicht mehr beim verantwortlichen Server geholt werden, sondern können dem lokalen Cache entnommen werden.

Ein ALG ermöglicht eine Filterung in zweierlei Hinsicht:

- Es kann nach bestimmte Funktionen bzw. Headerinformation des Anwendungsprotokolls gefiltert werden. Beispielsweise kann bei HTTP (Hypertext Transfer Protocol) die PUT-Methode blockiert werden.
- Daneben können die vom Anwendungsprotokoll transportierten Daten gefiltert werden. Um bei HTTP zu bleiben, können beispielsweise alle von einem Script-Tag umschlossenen Teile einer HTML-Seite (Hypertext Markup Language) entfernt werden.

Neben den Filtermöglichkeiten kann mit einem ALG, wie schon erwähnt, ein Cache verknüpft sein. Auch kann für die Benutzung eines Dienstes eine Authentifizierung erzwungen werden.

Die Güte eines ALG hängt mit der Art und Anzahl der unterstützten Anwendungsprotokolle, sowie den damit verbundenen Filtermöglichkeiten zusammen. Bei vielen Anwendungsprotokollen müssen die Clients mit einem Proxy zusammenarbeiten können. Häufig müssen dazu die Clients speziell konfiguriert werden. Ein Proxy der keine Unterstützung auf Seiten der Clients benötigt wird auch als transparenter Proxy bezeichnet. Ein ALG stellt große Anforderungen an Hard- und Software und ist weniger performant als ein Paketfilter. Aus diesem Grund sind ALG selbst anfällig gegenüber Denial-of-Service-Angriffen (DoS-Angriffe). Im Folgenden sind die Vor- und Nachteile noch einmal zusammengefasst dargestellt.

Vorteile:

- Keine direkte Verbindung,
- Verbergen der geschützten Rechner,
- Filtern auf Ebene der Anwendungsprotokolle,
- Zusammenarbeit mit Cache,
- Erzwingen einer Authentifizierung.

Nachteile:

- Eigener Proxy für jedes Anwendungsprotokoll notwendig,
- Unterstützung durch den Client notwendig,
- größere Anforderungen an Hard- und Software,
- größerer Konfigurationsaufwand.

Circuit Level Gateways unterschieden

Ein CLG arbeitet als Proxy in der Transportschicht des TCP/IP-Referenzmodells. Ein CLG stellt eine mögliche Lösung für Anwendungsprotokolle dar, für die es keine speziellen Porxies gibt. Allerdings sind dann keine Filterungen auf der Ebene des Anwendungsprotokolls möglich. Wie bei einem ALG ist auch bei einem CLG eine Unterstützung auf Seiten der Clients notwendig. Häufig findet sich bei einem CLG eine Möglichkeit für die Erzwingung einer Authentifizierung vor Nutzung eines bestimmten Dienstes.

2.2 Eine Firewall auf der Basis von Linux

Der Betriebssystem-Kern von Linux besitzt seit der Version 2.0 einen Paketfilter. Deshalb ist es möglich auf der Basis von Linux ein Firewall-System zu implementieren. Dabei sind die Hardware-Anforderungen des Paketfilters gering, so dass in der Regel schon ein ausrangierter Rechner als Plattform genutzt werden kann. Dies dürfte mit ein Grund sein, warum Linux als Firewall-Lösung am häufigsten bei den Instituten des MWN zu finden ist, wie die durchgeführte Umfrage ergeben hat. (siehe Tabelle 3.13).

In Abschnitt 2.2.2 wird kurz auf die grundlegende Architektur des Paketfilters von Linux eingegangen. Im Abschnitt 2.2.3 wird Stateful Filtering und in Abschnitt 2.2.4 NAT beschrieben.

Linux bietet zudem als Open-Source-Betriebssystem gute Möglichkeiten, den Betriebssystemkern um Sicherheitsfunktionen zu erweitern. Dazu existieren verschiedene Kernel-Patches und -Module, wie beispielsweise:

- Open Wall Patch [openwall] (verhindert das Ausführen von Code aus dem User-Stack),
- Linux Intrusion Detection System [XBB 02] mit Access Control Lists (ACL) für Dateien und Prozesse,
- Paketfilterung mit Ethernet Bridging.

In Abschnitt 2.2.5 werden zwei Möglichkeiten vorgestellt, eine für IP transparente Linux-Firewall einzurichten. Dabei wird auch auf die Möglichkeiten der Paketfilterung zusammen mit der Ethernet-Bridging-Funktion des Linux-Kernel eingegangen.

Zusätzlich kann auf dem Linux-Rechner Software installiert werden, die weitere Firewall-Funktionen hinzufügt. Es existieren zahlreiche Open-Source-Projekte, von denen hier nur einige beispielhaft aufgeführt sind:

- Squid [Chad 02] (HTTP- und FTP-Proxy),
- Server für SMTP (Simple Mail Transfer Protocol) als Mail-Proxy,
- Dante [dante] (SOCKS-Proxy),
- TIS Firewall-Toolkit [Youn 01] (Proxies für verschiedene Protokolle).

In Abschnitt 2.2.6 wird näher auf die Möglichkeiten von Squid eingegangen. Das Zusammenspiel eines SMTP-Servers mit einem Antivirenprogramm wird in Abschnitt 2.2.7 dargestellt.

2.2.1 Allgemeine Hinweise zu Linux

Die Implementierung von IP unter Linux bietet die Möglichkeit verschiedene sicherheitsrelevante Einstellungen über das proc-Dateisystem vorzunehmen. Im folgenden sind einige dieser Einstellungen aufgelistet:

- rp_filter: (Reverse Path) Verhindert, dass ein Paket mit einer gefälschten Source-Adresse über ein Interface in den Rechner gelangen kann. Es werden alle Pakete abgewiesen, deren Source-Adresse zu einem Rechner hinter einem anderen Interface gehören muss.
- accept_source_route: Über diesen Schalter kann eingestellt werden, ob Pakete mit einer Source-Route an einem Interface akzeptiert werden.
- accept_redirects: Über diesen Eintrag kann die Verarbeitung einer ICMP-Redirect-Nachricht eingestellt werden.
- icmp_echo_ignore_broadcasts: Verhindert Pings an eine Broadcast-Adresse.
- tcp_syncookies: Aktiviert SYN-Cookies, mit deren Hilfe, trotz einer SYN-Flooding-Attacke, berechtigte TCP-Verbindungen noch möglich sind.
- tcp_fin_timeout, tcp_keepalive_time: Über diese Variable können die Timeouts für TCP-Verbindungen justiert werden.

Version	Tool
2.0	ipfwadm
2.2	ipchains
2.4	iptables

Tabelle 2.1: Kommandozeilen-Tools zur Konfiguration der Paketfilter bei den verschiedenen Linux-Versionen

Beim Einrichten einer Firewall unter Linux sollten folgende Punkte beachtet werden:

- Keine unnötigen Software-Pakete auf der Linux-Firewall installieren.
- Keine unnötigen Serverdienste auf der Linux-Firewall laufen lassen. Besonders beachtet werden müssen Dienste, die auf Remote Procedure Call (RPC) beruhen oder über den inetd-Server gestartet werden.
- Keine unnötigen Accounts auf der Linux-Firewall einrichten und die Rechte der Benutzer auf ein Minimum einschränken.
- Keine Kernel-Modul-Unterstützung, da einige Rootkits existieren, die als Kernel-Module arbeiten.

2.2.2 Linux Netfilter

Nach der Linux-Kernel-Version 2.0 wurde in der Version 2.2 und der aktuellen Version 2.4 jeweils ein neues Paketfiltersystem eingeführt. Die verschiedenen Versionen sind nicht zueinander kompatibel. Das gleiche gilt für die Kommandozeilen-Tools über die der Paketfilter konfiguriert wird (siehe Tabelle 2.1). Die Version 2.4 bringt zwar eine Unterstützung für die alten Kommandozeilen-Tools mit, es können damit aber nicht alle Funktionen verwendet werden.

Im folgenden wird näher auf den in Kernel-Version 2.4 integrierten Paketfilter [Fros 01] eingegangen. Für diese Version wurde nicht nur der Paketfilter überarbeitet, sondern die gesamte Architektur der Netzwerkprotokolle. Dabei wurde ein Framework geschaffen und auf eine durchgängige Modularisierung geachtet. Das Framework hat den Namen Netfilter erhalten. Ein wesentlicher Bestandteil ist, dass in den Implementierungen der Netzwerkprotokolle Hooks eingefügt wurden. Diese stellen wohldefinierte Punkte dar, an denen ein Paket auf seiner Reise durch den Protokoll-Stack vorbei kommt. An den Hooks können sich Funktionen registrieren. Erreicht ein Paket einen solchen Hook, so übergibt Netfilter das Paket (zusammen mit der Hook-Nummer) in einer vorgegebenen Reihenfolge an die registrierten Funktionen. Jede Funktion kann dann das Paket untersuchen, verändern, zurückgeben oder verwerfen. Solche Funktionen können beispielsweise zu Paketfilter- oder NAT-Modulen gehören. Die Netfilter-Architektur wurde bisher für IP, IPv6 und DECnet implementiert. Im folgenden beschränkt sich die Darstellung auf IP.

Das Kommandozeilen-Tool ipfilters dient zur Konfiguration des Paketfilters. Darüber hinaus lässt sich damit auch das NAT, und das Paket Mangling einstellen, so dass im Gegensatz zu den vorgegangen Linux-Versionen nur noch ein Tool notwendig ist. Die drei genannten Funktionalitäten werden in Form sog. Tables angeboten:

- Filter-Table: Paketfilterfunktionen einschließlich Stateful Filtering.
- NAT-Table: Alle Formen des NAT einschließlich Masquerading.

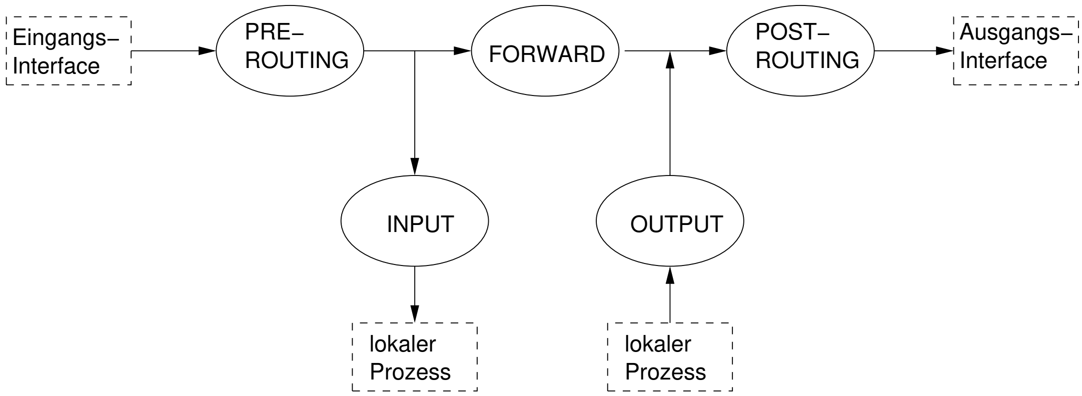

Abbildung 2.1: Standard-Regelketten von ipfilters

Table	Chain
Filter	Input, Forward, Output
NAT	Prerouting, Output, Postrouting
Mangle	Prerouting, Output

Tabelle 2.2: Tables und Chains

- Mangle-Table: Verändern beliebiger Headerfelder z. B. Type-of-Service-Feld (TOS-Feld).

Die Implementierung von IP in Linux enthält fünf Hooks, für die ipfilters jeweils eine Regelkette (Chain) verwaltet. Ein IP-Paket durchläuft die IP-Implementierung wie in Abbildung 2.1 dargestellt. Kommt es an einer Chain vorbei, so müssen die darin enthaltenen Regeln abgearbeitet werden. Ein Paket, das den Protokoll-Stack betritt, durchläuft zunächst die Prerouting-Kette. Als nächstes findet das Routing statt. Ist das Paket für den lokalen Rechner bestimmt durchläuft es noch die Input-Chain und wird dann an einen lokalen Prozess zur Verarbeitung übergeben. Entscheidet das Routing, dass das Paket weitergeleitet werden muss, durchläuft das Paket als nächstes die Forwarding-Chain. Bevor das Paket den Rechner verlässt muss noch die Postrouting-Chain abgearbeitet werden. Ein auf dem lokalen Rechner erzeugtes Paket, muss zunächst die Output-Chain durchlaufen und nach dem Routing-Vorgang ebenfalls die Postrouting-Chain passieren.

Die Regeln in einer Chain werden der Reihe nach abgearbeitet. Jede Regel bezieht sich auf eine Funktion der Filter-, NAT- oder Mangle-Table. Die Funktionen einer Table können nicht aus jeder Kette aufgerufen werden (siehe Tabelle 2.2). Jede Regel besteht aus einem Match- und einem Target-Teil. Der Match-Teil formuliert eine Bedingung. Erfüllt das aktuelle IP-Paket die Bedingung wird die im Target-Teil angegebene Aktion ausgeführt. In Tabelle 2.3 sind einige Targets aufgelistet. Die Targets Accept, Drop und Reject führen dazu, dass das Paket nicht weiter verarbeitet wird. Bei den anderen Targets wird mit der Abarbeitung der Regelkette fortgefahren. Neben den von ipfilters vorgegebenen Regelketten lassen sich auch benutzerdefinierte Regelketten mit beliebigen Namen bilden, die als ein Art Unterprogramm aufgefasst werden können. Der Einstieg in eine benutzerdefinierte Regelkette erfolgt durch die Angabe des Namens als Target. Die Rückkehr aus einer selbstdefinierten Regelkette gelingt mit dem Target Return.

Target	Beschreibung
Accept	Paket wird akzeptiert
Drop	Paket wird kommentarlos verworfen
Reject	Paket wird verwofen und eine Meldung an Absender geschickt
DNAT	Anpassung der Destination Address
SNAT	Anpassung der Source Address
Masq	Masquerading
Log	Meldung an das Syslog ausgeben
Queue	Weitergabe des Pakets an ein Programm ausßerhalb des Kernels

Tabelle 2.3: Targets von ipfilters

2.2.3 Stateful Filtering

Seit der Kernel-Version 2.4 unterstützt Linux dynamische Paketfilterung, bei Linux unter dem Namen Stateful Filtering bekannt. Zu diesem Zweck verwaltet Linux in einer Tabelle den Zustand einzelner Verbindungen. Unter einer Verbindung wird in diesem Zusammenhang nicht nur eine TCP-Verbindung verstanden, sondern auch zusammengehörige UDP- oder ICMP-Datagramme. Zu diesem Zweck verwaltet Linux die Verbindungen in einer internen Tabelle. Dazu werden folgende Informationen registriert:

- Das Transport-Protokoll (TCP oder UDP) bzw. ICMP,
- Status der Verbindung (nur bei TCP, z.B. SYN_SENT, SYN_RECV),
- Timeout bis zum Löschen des Eintrags,
- Quell- und Zieladresse, sowie Quell- und Zielport des losgeschickten Pakets (bei ICMP wird statt der Ports der Typ und Code gespeichert),
- Quell- und Zieladresse, sowie Quell- und Zielport der als Antwort zurückerwarteten Pakete (bei ICMP wird statt der Ports der Typ und Code gespeichert).

Bei jedem Paket wird überprüft, ob in der Tabelle ein zum Paket passender Eintrag bereits vorhanden ist. Ist dies nicht der Fall wird ein neuer Eintrag angelegt. In den Paketfilterregeln kann nun der Zustand einer Verbindung mit in eine Filter-Bedingung einbezogen werden. Folgende Zustände stehen zur Verfügung:

- New: Es existiert kein Eintrag in der Zustandstabelle, die Verbindung ist also neu.
- Established: In der Zustandstabelle existiert bereits ein passender Eintrag.
- Related: Eine Verbindung wird als related angesehen, wenn sie in Beziehung zu einer anderen bereits als established gekennzeichneten Verbindung steht.
- Invalid: Paket kann nicht identifiziert werden. Dies kann auftreten, wenn kein Speicher mehr für die Tabelle zur Verfügung steht oder ein unerwartetes ICMP-Paket eintrifft.

Besonders leistungsfähig wird das Stateful Filtering durch den Related-Zustand. Ein Beispiel ist eine ICMP-Fehlernachricht, die als Folge eines abgelehnten Verbindungsaufbaus verschickt wird. Darüber hinaus können mit dem Related-Zustand Anwendungen unterstützt werden, die mehrere Verbindungen benutzen. Bei FTP werden beispielsweise neben der Steuerungsverbindung, eine oder mehrere

Datenverbindungen verwendet. Um eine FTP-Datenverbindung der zugehörigen Steuerungsverbindung zuordnen zu können, muss das Anwendungsprotokoll von FTP analysiert werden. Bei aktiven FTP muss z. B. das PORT-Kommando ausgelesen werden. Zu diesem Zweck existieren zur Zeit Hilfsmodule für verschiedene Anwendungen:

- FTP – im Standardkernel enthalten,
- IRC (Internet Relay Chat) – im Standardkernel enthalten,
- TFTP (Trivial File Transfer Protocol) – als Patch erhältlich,
- PPTP – als Patch erhältlich,
- Talk – als Patch erhältlich.

2.2.4 Network Address Translation

Der Kernel 2.4 von Linux unterstützt vollständiges NAT. Eine besondere Form des SNAT ist Masquerading. Dadurch werden die Source-Adressen aller hinter der Firewall liegenden Geräte durch die Adresse des externen Interfaces der Firewall ersetzt. Dabei müssen jedoch nicht nur die Source-Adressen, sondern auch die Source-Ports verändert werden. Für jede Verbindung wird die ursprüngliche Source-Adresse, der ursprüngliche Source-Port und der neue Source-Port intern gespeichert. Antwortpakete können dann anhand dieser Informationen an die richtigen Geräte hinter der Firewall weitergegeben werden. Durch das Masquerading erreicht man, dass die Rechner hinter der Firewall nach außen nicht sichtbar sind. Verwendet man im geschützten Netz zusätzlich private IP-Adressen, können die Rechner aus dem Internet zudem nicht direkt erreicht werden.

Das Masquerading eignet sich besonders dann, wenn die Anbindung an das Internet über eine dynamische IP-Adresse erfolgt. Das Masquerading-Modul überprüft dazu vor jeder Adressersetzung die eigene IP-Adresse. Findet die Anbindung an das Internet über eine statische IP-Adresse statt, kann die Überprüfung und der damit verbundene Aufwand eingespart werden, wenn stattdessen das SNAT-Modul eingesetzt wird.

Wie beim Stateful Filtering sind auch beim Masquerading Hilfsroutinen notwendig, um Anwendungen unterstützen zu können, die mehrere Verbindungen benutzen:

- FTP – im Standardkernel enthalten,
- IRC – im Standardkernel enthalten,
- TFTP – als Patch erhältlich,
- PPTP – als Patch erhältlich,
- Talk – als Patch erhältlich,
- SNMP – als Patch erhältlich.

Eine besondere Form des DNAT ist das Redirecting. Mit diesem Modul können Verbindungen, die an einen Web-Server außerhalb gerichtet sind, an einen lokalen Web-Proxy übergeben werden. Auf diese Weise kann beispielsweise mit Squid ein transparenter Proxy auf der Firewall eingerichtet werden. Mit Hilfe des allgemeinen DNAT-Modul ergeben sich weitere Möglichkeiten:

- Transparenter Proxy außerhalb des lokalen Rechner,

- Weiterleiten einer Verbindung an einen hinter der Firewall verborgenen Server (Port Forwarding),
- Lastaufteilung auf mehrere Server hinter der Firewall.

2.2.5 Transparente Firewalls

In diesem Abschnitt werden zwei Möglichkeiten vorgestellt, eine Linux-Firewall in ein bestehendes Netz zu integrieren, ohne dass eine Aufteilung des Netzes in IP-Subnetze nötig wird. Die Firewall ist für die Rechner im Netz auf der Ebene des IP-Protokolls transparent. Daraus ergeben sich folgende Vorteile:

- Der IP-Adressraum des Netz muss nicht aufgeteilt werden,
- es gehen keine IP-Adressen für Broadcast- und Netz-Adressen verloren,
- die im Netz befindlichen Rechner können ihre IP-Konfiguration beibehalten,
- im Fehlerfall kann die Firewall überbrückt werden.

Es existieren allerdings auch Probleme:

- Die Transparenz auf der IP-Ebene erschwert das Auffinden von Fehlern (z. B. “sieht” traceroute die Firewall nicht),
- “möglichst wenig ändern” darf nicht zur Grundlage eines Sicherheitskonzepts werden,
- ein Überbrücken der Firewall könnte bewusst provoziert worden sein (z. B. durch einen DoS-Angriff),
- die Firewall muss Broadcasts und Flooding im Netz berücksichtigen.

Die zwei Möglichkeiten für die Realisierung einer transparenten Firewall basieren auf Funktionen des Linux-Kernel: 802.1d Ethernet Bridging [Buyt 01] und Proxy-ARP [Weis]. Für beide Varianten bietet die Technische Universität Wien eine kostenlose Lösung an, die direkt von einer Diskette lauffähig ist [Selo]. Der Nachteil der Bridging-Lösung ist, dass zur Zeit der Kernel noch gepatched werden muss. Dafür ist die Proxy-ARP-Lösung aufwendiger zu konfigurieren.

Bridging

Das Ethernet-Bridging ist seit der Version 2.4 im Linux-Kernel enthalten. Bei der Version 2.2 musste noch ein Patch eingespielt werden. In beiden Fällen ist damit jedoch noch keine Paketfilterung möglich. Dafür muss ein weiterer Patch installiert sein. Da bei einer auf Version 2.2 basierenden Lösung verschiedene Unzulänglichkeiten (Default-Policy wird nicht berücksichtigt, es muss eine Chain mit dem Namen der Bridge-Interface-Gruppe existieren) vorhanden sind, wird der Einsatz der Kernel-Version 2.4 zusammen mit iptables empfohlen.

Mit Hilfe des Kommandozeilen-Tools brctl können Bridge-Gruppen erzeugt und ihnen Netz-Interfaces zugeordnet werden. Man hat die Möglichkeit einer Bridge-Gruppe eine IP-Adresse zuzuordnen, um beispielsweise einen Management-Zugriff auf das Gerät zu ermöglichen. Den einzelnen Interfaces der Bridge-Gruppe können keine IP-Adressen gegeben werden, die Interface-Namen lassen sich in den Firewall-Regeln jedoch verwenden.

Bei der Definition der Firewall-Regeln sind Dinge zu beachten, die man von einem Paketfilter auf einem Router nicht gewohnt ist. Dazu ein Beispiel: Die Bridge merkt sich intern, welche MAC-Adressen über welchen Bridge-Port erreichbar sind. Auf diese Weise wird eine Verkehrsseparierung möglich. Die Zuordnungen MAC-Adresse zu Bridge-Port muss jedoch erst erlernt werden. Solange für eine MAC-Adresse noch keine Zuordnung besteht, werden die Frames an allen Ports (bis auf den Eingang) ausgegeben (flooding). Ist nun eine Filterregel definiert, die den Verkehr zwischen dem Eingangs-Port und einem anderen Port blockiert, muss richtig reagiert werden. Eine Reaktion der Firewall mit einer Fehlermeldung (ICMP destination unreachable, TCP-Reset) verursacht Probleme, besser ist ein kommentarloses Verwerfen des Pakets.

Wem die Filtermöglichkeiten von iptables nicht ausreichen, kann zusätzlich ebtables [Schu] verwenden. Dazu sind allerdings nochmals ein Kernel-Patch und Kommandozeilen-Tools notwendig. Dann stehen Dinge wie Ethernet Protocol Filtering, ARP Header Filtering, 802.1Q VLAN Filtering, MAC Address NAT und Brouter-Funktionen zur Verfügung.

Proxy-ARP

Mit Hilfe des im Linux-Kernel integrierten ARP-Proxies kann ebenfalls eine transparente Firewall realisiert werden. Im Gegensatz zur Bridge-Lösung arbeitet diese Firewall jedoch weiterhin als Router. Es werden Routing-Entscheidungen getroffen und es findet keine Zuordnung der MAC-Adressen zu den Interfaces statt. Die Transparenz wird dadurch erreicht, dass man der Firewall eine Art Generalvollmacht für die Annahme von IP-Paketen erteilt. Muss ein Host A ein Paket an einen Host B schicken, der an einem anderen Port der Firewall angeschlossen ist, so gibt sich die Firewall als Stellvertreter von Host B aus. Sie nimmt die für Host B bestimmten Pakete entgegen. Wird das Paket entsprechend der Firewall-Policy nicht verworfen, wird es an den echten Host B weitergeleitet.

Die Realisierung erfolgt mit Hilfe von ARP. Host A muss vor dem Senden des IP-Paketes die MAC-Adresse von Host B in Erfahrung bringen. Da Host A der Meinung ist, dass sich Host B im selben Subnetz befindet, wird ein ARP-Request für die IP-Adresse von Host B generiert. Wenn sich Host A und B auf unterschiedlichen Seiten der Firewall befinden, nimmt die Firewall den ARP-Request auf und antwortet mit der eigenen MAC-Adresse. Dazu muss die Firewall jedoch genau wissen, welche Rechner an den einzelnen Netzwerkschnittstellen angeschlossen sind.

Für die Konfiguration sind die iproute2-Programme notwendig. Damit müssen folgende Schritte durchgeführt werden:

- Allen Netz-Interfaces der Firewall muss die selbe IP-Adresse gegeben werden.
- Die Routing-Tabelle muss so angelegt werden, dass ersichtlich ist, welche IP-Adressen über welches Interface erreicht werden können.

2.2.6 Squid

Squid [Chad 02] ist ein HTTP-Proxy für Linux. Er bietet folgende Möglichkeiten:

- Proxy für HTTP und FTP,
- Cache,
- Authentifizierung,

- ACLs für die Zugriffskontrolle auf Sites,
- Betrieb als transparenter Proxy.

Der Betrieb von Squid als transparenter Proxy hat den Vorteil, dass keine Anpassung bei den Clients notwendig ist. Ein entsprechend konfigurierter Paketfilter leitet alle HTTP-Anfragen an den Proxy um, ohne dass der Benutzer darauf Einfluss nehmen kann.

Mit Hilfe von Squid-Guard [BaHå 02] lässt sich die Zugriffskontrolle von Squid noch vereinfachen. Es ist möglich, ganze Sites oder einen Teil einer Site anhand von Uniform Resource Locators (URLs) zu filtern. Auf diese Weise lassen sich beispielsweise unerwünschte Sites komplett unterdrücken oder Bannerwerbung ausblenden. Zusätzlich können Umleitungen auf andere Seiten vorgegeben werden. Neben den URLs können auch IP-Adressen und Benutzernamen in die Filterung mit einbezogen werden. Der größte Vorteil liegt jedoch darin, dass man Listen von unerwünschten Sites nicht selbst anlegen muss, sondern auf für Squid-Guard geeignete und gut gepflegte Listen zurückgreifen kann.

Eine zusätzliche Erweiterung stellt das Squid-Modul für das Pluggable Authentication Modul System (PAM) dar, mit dessen Hilfe die Benutzerauthentifizierung vereinheitlicht werden kann.

2.2.7 SMTP-Proxy

Auf der Basis von Linux lässt sich ein SMTP-Proxy einrichten, der u. a. mit einem Virenscanner zusammenarbeiten kann. Zu diesem Zweck kann das Perl-Programm AMAVIS [BrLi 00] eingesetzt werden. Es arbeitet mit mehreren SMTP-Server (z. B. Postfix, Sendmail) zusammen. AMAVIS ist in der Lage E-Mail-Attachments vom Mail Transfer Agent (MTA) entgegenzunehmen, bei Bedarf Archive zu entpacken und den Inhalt an einen Virenscanner zur Überprüfung weiterzugeben. Stellt der Scanner einen Virus fest, kann die Weiterleitung der Mail gestoppt und stattdessen eine Warnmeldung generiert werden. AMAVIS arbeitet mit Virenscannern vieler Hersteller (z. B. Kaspersky, TrendMicro, F-Secure, NAI, Sophos) zusammen.

Der immer noch weit verbreitete MTA Sendmail [sendmail] unterstützt seit Version 8.10 Milter [milter], ein Application Program Interface (API) für die Filterung von Mails. Mit dieser API lassen sich verschiedene Filtervorgänge vereinfachen:

- Überprüfen von E-Mail-Adressen,
- Modifizieren einer E-Mail,
- Zusammenarbeit mit AMAVIS.

2.3 Sicherheitsmechanismen von Cisco Catalyst 6509

Im MWN werden Router vom Typ Cisco Catalyst 6509 eingesetzt. Dieses Produkt gehört zu einer Familie von modularen Switches mit einer Backplane von bis zu 256 Gbps. Der Catalyst 6509 bietet neun Einschübe, die Switching-Module für Ethernet oder ATM (Asynchronous Transfer Mode), sowie Supervising-Module aufnehmen können. Das Supervising-Modul bietet optional Routerfunktionalität, weshalb hier auch von Level-3-Switching gesprochen wird. Zusätzlich stehen verschiedene Sicherheitsfunktionen zur Verfügung, die in die Realisierung einer Firewall einbezogen werden können. Die Produktbeschreibung [Cis 02a] und andere Dokumente des Herstellers listen u. a. folgende Sicherheitsdienste auf:

- Port Security
- 802.1x
- Access Control Lists innerhalb eines VLAN oder beim Routing zwischen VLANs.
- Reflexive ACL
- Context-Based Access Control
- Lock-and-Key Security
- Network Address Translation (NAT)
- Syslog-Nachrichten bei Sicherheitsverletzungen

2.3.1 Port Security

Ein Switch-Port kann so konfiguriert werden, dass nur berechtigte Rechner über diesen Port Zugang zum Netz erhalten. Die berechtigten Rechner werden über ihre MAC-Adressen identifiziert. Pro Switching-Modul können bis zu 1025 MAC-Adressen registriert werden. Bei einer Verletzung der Port Security können verschiedene Maßnahmen konfiguriert werden, wie Verwerfen von unberechtigten Frames oder Abschalten des Ports.

2.3.2 802.1x

Das im IEEE-Standard 802.1x festgelegte Verfahren ermöglicht es, den Zugang zum Netz erst dann freizuschalten, wenn der Benutzer sich erfolgreich authentifiziert hat. Dazu werden pro Switchport zwei virtuelle Access Points angeboten. Einer davon (unkontrollierte Port) wird ausschließlich für die Authentifizierung offen gehalten. Die Authentifizierung erfolgt an einem Radiusserver. War sie erfolgreich, wird der andere Access Point (kontrollierte Port) freigegeben, womit der normale Zugang zum Netz möglich wird. Dabei kann für jeden Benutzer auf dem Radius-Server ein VLAN eingestellt werden, dem der Switch-Port zugeordnet werden soll. Findet auf dem Port über eine einstellbare Zeit kein Verkehr mehr statt, wird der kontrollierte Port wieder geschlossen.

Durch den 802.1x-Standard, kann eine durchgehende Zugangskontrolle zum Netz realisiert werden. Da die Authentifizierung am Radius-Dienst erfolgt, kann der selbe Benutzer-Account auch für andere Dienste verwendet werden.

2.3.3 Access Control Lists innerhalb eines VLAN oder beim Routing zwischen VLANs

Bei der Cisco Catalyst-Familie hat man einerseits Verkehr, der innerhalb eines VLAN weitergeleitet wird, und andererseits Verkehr, der zwischen VLANs geroutet werden muss. Für beide Arten können Access Control Lists (ACLs) definiert werden, die den Verkehr beeinflussen. Eine ACL, die auf den Verkehr innerhalb eines VLAN wirkt, bezeichnet Ciscos als VLAN ACL (VACL). Eine ACL, die den gerouteten Verkehr kontrolliert, nennt Cisco IOS (Internetwork Operating System) ACL [Cis 02c].

IOS ACLs können beispielsweise für Paketfilterung, NAT, Verschlüsselung oder Policy-based Routing verwendet werden. IOS ACLs werden einzelnen Interfaces zugeordnet und es wird zwischen eingehenden und ausgehenden Paketen unterschieden.

VACLs können für Paketfilterung (IP und IPX), Filterung von MAC-Adressen und Redirecting zu einem bestimmten Port eingesetzt werden. Eine VACL wirkt auch auf Daten, die aus dem VLAN heraus bzw. in das VLAN hinein gelangen. Es wird nicht zwischen eingehenden und ausgehenden Daten unterschieden. Es wird der im VLAN gebridgete Verkehr kontrolliert.

Jede ACL besteht aus einer geordneten Liste von Access Control Entries (ACEs), die nach der vorgegebenen Reihenfolge abgearbeitet werden. Trifft die Bedingung einer ACE zu, so wird die zugehörige Aktion durchgeführt. Werden für ein VLAN-Interface VACLs und IOS ACLs eingerichtet, so werden die zugehörigen ACEs intern zusammengefasst. Bei diesem Vorgang kann die Zahl der ACEs erheblich ansteigen, wenn die VACLs und IOS ACLs ungünstig definiert wurden. Dies kann zu Problemen bei Ressourcen und Performance führen.

2.3.4 Reflexive ACL

Neben statischen Paketfilterregeln werden auch dynamische Paketfilterregeln unterstützt. Dies nennt Cisco Reflexive ACL [Cis 02e]. Laut Cisco wird mit dieser Methode eine Filterung nach Sessions möglich. Der wesentliche Unterschied zu statischen Filtern besteht darin, dass in eine ACL temporäre Einträge vorgenommen werden, die nach einer bestimmten Zeit wieder entfernt werden. Wird beispielsweise eine Session von innen nach außen aufgebaut, so werden temporäre Einträge angelegt, die auch den zur Session gehörenden Verkehr von außen nach innen durchlassen. Dabei wird ganz gezielt nach Quell-, Zieladresse und Ports gefiltert. Bei einer reinen statischen Filterung müssen hingegen immer große Adress- und Portbereiche geöffnet werden, damit die zurückkommenden Pakete passieren können.

Unter einer Session können TCP-Verbindungen verstanden werden. Der Beginn der Session wird an Hand des Verbindungsaufbaus festgestellt, worauf entsprechend temporäre Einträge eingerichtet werden. Wird das Ende der TCP-Verbindung registriert oder wird eine bestimmte Zeit der Inaktivität überschritten, so werden die Einträge wieder gelöscht. Reflexive ACL arbeitet auch mit verbindungslosen Protokollen, wie UDP oder ICMP. Bei diesen Protokollen werden temporäre Einträge immer nach einem einstellbaren Timeout entfernt.

Probleme bereiten laut Cisco Anwendungen, bei denen Portnummern während der Sitzung wechseln. Gemeint ist damit beispielsweise aktives FTP, bei dem der Aufbau einer zusätzlichen TCP-Verbindung für die Datenübertragung von außen nach innen versucht wird. Da dafür keine temporären Einträge in die ACL vorgenommen wurden, als die Steuerverbindung von innen nach außen aufgebaut wurde, funktioniert die Datenübertragung nicht.

2.3.5 Context-Based Access Control

Unter Context-Based Access Control (CBAC) werden verschiedene Schutzfunktionen auf verschiedenen Ebenen zusammengefasst [Cis 02d]. Mit Hilfe von CBAC können die Sequenznummern von TCP überprüft werden. Pakete, die nicht im erwarteten Bereich der Sequenznummern liegen, werden dann verworfen. Einige Anwendungsspezifische Befehle können blockiert werden, um bestimmte Angriffe zu unterbinden. Dies ist beispielsweise bei SMTP möglich.

Das bei Reflexive ACLs bestehende Problem mit Anwendungen, die auf mehreren Verbindungen in der Transportschicht beruhen kann zum Teil durch Context-Based Access Control (CBAC) gelöst werden. Informationen zu einer Session werden dabei auch durch Auswertung der Anwendungsprotokolle gewonnen. Unterstützt werden z. B. FTP, Sun-RPC, H.323 und Oracle.

Für Java bietet CBAC die Möglichkeit zwischen sicheren und unsicheren Applets zu unterscheiden. Dazu kann eine Liste vertrauenswürdiger Sites erstellt werden, deren Applets als sicher gelten. Stammt ein Applet nicht von einer vertrauenswürdigen Site wird es blockiert.

Mit Hilfe von CBAC können außerdem verschiedene Arten von DoS-Angriffen unterbunden werden. Es lässt sich beispielsweise eine maximale Anzahl halboffener TCP-Verbindungen vorgeben, um SYN-Flooding zu verhindern. CBAC ist in der Lage mit fragementierten Paketen umzugehen. Fragmente werden blockiert, solange nicht das zugehörige initiale Fragment angekommen ist.

CBAC arbeitet nur mit Anwendungen, die auf TCP oder UDP basieren. Ist der Router als IPsec-Endpunkt definiert, so kann CBAC damit zusammenarbeiten.

2.3.6 Lock-and-Key Security

Lock-and-Key Security wird in der Dokumentation von Cisco manchmal auch Dynamic ACL genannt [Cis 02f]. Durch dieses Feature erhält ein Benutzer die Möglichkeit auch Dienste zu nutzen, die normalerweise blockiert werden. Dazu muss der Benutzer zunächst eine Telnet-Verbindung zum Router aufbauen und sich authentifizieren. Bei einer erfolgreichen Authentifizierung wird die IP-Access-List an dem entsprechenden Interface temporär umkonfiguriert. Nach einem einstellbaren Timeout wird die ursprüngliche Access-List wieder hergestellt.

Für die Authentifizierung können auf dem Router Benutzernamen und Passwörter konfiguriert werden. Darüber hinaus besteht die Möglichkeit die Authentifizierung mit Hilfe eines Radius- oder TACACS+-Server (Terminal Access Controller Access Control System) durchzuführen.

Diese Methode ist anfällig gegen IP-Spoofing. Solange die Öffnung besteht, können auch andere Hosts, die die Adresse des authentifizierten Benutzers spoofen, durch die Firewall hindurch gelangen.

2.3.7 Network Address Translation

Cisco IOS unterstützt mehrere Arten von NAT. Es können statische und dynamische Zuordnungen definiert werden. Außerdem ist es möglich mehrere lokale Adressen auf eine globale IP-Adresse abzubilden. Die interne Zuordnung erfolgt dabei unter Einbeziehung der Portnummern von TCP oder UDP.

2.3.8 Syslog-Nachrichten bei Sicherheitsverletzungen

Meldungen können grundsätzlich an einen Syslog-Server weitergeleitet werden. Der Catalyst unterstützt dafür mehrere Facilities und acht Severity-Stufen. Bei den meisten hier beschriebenen Sicherheitsfunktionen kann das Generieren von Meldungen konfiguriert werden. Im Zusammenhang mit CBAC und SMTP werden sogar rudimentäre IDS-Funktionen geboten. Dazu überwacht CBAC das Syslog und sucht nach speziellen Angriffsmustern. Wird ein solches erkannt, wird die entsprechende SMTP-Session geschlossen.

2.4 Firewall-Produkte

In diesem Abschnitt werden drei eigenständige Firewall-Produkte vorgestellt. Neben dem Marktführer Ceckpoint [FW-1] werden auch die Produkte von Cisco (PIX) [Cis 02b] und Astaro [Astaro] betrachtet. Astaro wurde aus den zahlreichen Linux-Lösungen ausgewählt. Das Astaro-Produkt ist auf Grund der Management-Möglichkeiten eher ein Produkt für den Bereich Small Office/Home Office (SOHO). Checkpoint und Cisco bieten ihre Produkte in unterschiedlichen Versionen an, sowohl für den SOHO-, als auch Enterprise-Markt. Checkpoint hat zudem eine Management-Lösung für einen Security-Provider im Sortiment.

Für die Beschreibung der drei Produkte wurden verschiedene Dokumente der Hersteller und Artikel aus Zeitschriften herangezogen (siehe Literaturliste). Es werden jeweils Architektur, Konfiguration, Logging und Firewall-Funktionen betrachtet. Die Darstellung ist nicht als Ersatz für eine Evaluation gedacht.

2.4.1 Astaro Security Linux

Architektur

Astaro Security Linux 3.2 basiert auf dem Linux-Kernel 2.4. Neben dem Kernel werden noch andere Open-Source-Komponenten (z. B. Apache, Squid) verwendet. Die von Astaro beigesteuerte Teile (Konfiguration, Selbstüberwachung, Update) stehen unter einer proprietären Lizenz. Diese verbietet die Installation zusätzlicher Software, sowie die Modifikation des Systems. Optional sind ein Virenscanner von Kaspersky Labs und eine Hochverfügbarkeit-Lösung erhältlich.

Das System wird auf einer CD ausgeliefert und muss auf eine Festplatte installiert werden. Der Preis richtet sich nach der Anzahl der zu schützenden Rechner. Für privaten Gebrauch kann ein CD-Image kostenlos heruntergeladen werden. Von verschiedenen Herstellern (z. B. Pyramide Computer, Symantec, Dr. Neuhaus) sind Appliances erhältlich.

Die Konfiguration der einzelnen Komponenten (Paketfilter, Squid etc.) erfolgt nicht direkt, sondern über eine Zwischenschicht. Die Konfigurationsdaten werden dazu in einem eigenen Verzeichnis gespeichert. Beim Booten und nach Änderungen werden daraus die notwendigen Konfigurationsdateien und Aufrufoptionen der einzelnen Programme gebildet. Auf diese Weise wird die Administration der Firewall vom darunterliegenden Linux-System entkoppelt. Allerdings sind viele Konfigurationsvorgänge dadurch nicht nachvollziehbar.

Die Sicherheit des Systems wird durch verschiedene Maßnahmen erhöht. Die Proxies laufen in einer Chroot-Umgebung. Außerdem ist der Betriebssystem-Kern um Capabilities erweitert worden. Eine von Astaro entwickelte Komponente zur Selbstüberwachung schützt das System zusätzlich.

Zur Performance gibt Astaro an, dass bei Verwendung einer 1266-MHz-CPU ein Durchsatz von 730 Mbps möglich ist. In Verbindung mit VPN reduziert sich der Wert auf 115 Mbps. Pro Stunde können 6000 E-Mails nach Viren untersucht werden.

Konfiguration

Die Konfiguration kann von einem beliebigen Rechner aus per SSH oder über ein Web-Interface per HTTPS (Hypertext Transfer Protocol Secure) durchgeführt werden. Die vorgenommenen Änderungen an der Konfiguration werden an die schon erwähnte Zwischenschicht weitergegeben. Das System kann über eine Update-Funktion auf dem aktuellen Stand gehalten werden. Das Update kann manuell oder automatisch in regelmäßigen Zeitabständen erfolgen. Der Download der Updates (z. B. Patches, Virenpattern) erfolgt per SSH.

Logging

Für das Logging werden SNMP, Syslog, WELF (WebTrends Enhanced Log Format) und ASCII (American Standard Code for Information Interchange) unterstützt. Das Logging kann out-of-band erfolgen und auch über ein Modem an einen Log-Server geschickt werden. Über das Web-Interface können vorkonfigurierte oder selbst erstellte Reports (z. B. Netzlast, HTTP-Benutzer, Accounting, Filterung, Portscans) erzeugt werden. Neben einer tabellarischen Darstellung ist auch eine graphische möglich. Dazu wird auf das Open-Source-Projekt MRTG zurückgegriffen.

Firewall-Funktionen

Paketfilterung/NAT: Da Astaro den Linux-Kernel 2.4 unterstützt stehen die von Iptables bekannten Möglichkeiten (z. B. Stateful Filtering, NAT) zur Verfügung. Die vom System genutzten TCP-Sequenznummern werden durch einen Zufallsgenerator erzeugt.

Proxies: Für HTTP, HTTPS, DNS, SMTP und Ident werden Proxies angeboten, außerdem steht ein Socks-Proxy zur Verfügung. Nicht enthalten ist ein Proxy für FTP. Der HTTP-Proxy bietet einen Cache und kann auch transparent betrieben werden.

Authentifizierung: Für die Nutzung von HTTP, SMTP und Socks kann eine Authentifizierung erzwungen werden. Die Benutzerverwaltung kann lokal, auf einem Radius-Server oder auf einem Windows-Domain-Controler erfolgen.

Content-Filtering: Für HTTP kann der Zugriff auf Sites mit Hilfe von Black- und Whitelists reguliert werden. Außerdem ist die Astaro-Firewall in der Lage Java, ActiveX und Javascript zu filtern. Für den Schutz der Privatsphäre können Cookies und Web-Bugs verhindert werden. Für die Suche nach Viren in E-Mails wird, wie schon erwähnt, der Virenscanner von Kaspersky Labs eingesetzt. Spam kann durch ein automatisches Überprüfen der Absender-Adresse, sowie durch die Blackhole-Lists unterdrückt werden. Auch ein String-Filter für SMTP ist möglich.

VPN: Astaro Security Linux unterstützt PPTP und IPsec (Internet Protocol Secure).

2.4.2 Firewall-1 von Checkpoint

Architektur

Die Firma Checkpoint hat bereits 1993 mit der Entwicklung der Firewall-1 begonnen. Entsprechend groß ist die Erfahrung der Firma in diesem Bereich. Firewall-1 gilt als Marktführer bei den Firewall-Produkten, nach Angaben von Checkpoint beträgt der Marktanteil 65 Prozent. Firewall-1 wird von Checkpoint als Software-Lösung vertrieben. Die Beschreibung richtet sich nach der Version 4.1. Als zugrundeliegendes Betriebssystem werden Red Hat Linux (6.2, 7.0, 7.2), Solaris (7, 8) und Windows (2000, NT 4.0) unterstützt. Von verschiedenen Herstellern (z. B. Pyramide Computer, Advancetech) werden außerdem Appliances angeboten.

Für die Filterung benutzt Firewall-1 jedoch nicht den Protokoll-Stack des Betriebssystems, sondern eine eigene Implementierung. Dadurch haben Fehler des Betriebssystem-Stacks keine Auswirkungen auf die Schutzwirkung der Firewall. Die Datenpakete werden zwischen der Schicht 2 und 3 abgegriffen und mit der eingestellten Policy verglichen. Wenn keine Verletzung der Policy vorliegt, werden die Pakete wieder an die Schicht 3 des Betriebssystem-Stacks zurückgegeben.

Während des Vergleichs mit der Policy werden Überprüfungen bis auf die Ebene der Anwendungsschicht vorgenommen. Deshalb werden aus den in den Paketen transportierten Daten die Anwendungsprotokolle zurückgewonnen. Auch fragmentierte Pakete werden vor der Filterung zusammengesetzt. Die dabei festgestellten Verbindungen (TCP, UDP, aber nicht ICMP) werden von Firewall-1 in eine Tabelle eingetragen. Dadurch können die Zustände der einzelnen Verbindungen verwaltet und bei der Filterung berücksichtigt werden. Für die Folgepakete einer Verbindung reicht ein Vergleich mit der Verbindungstabelle, statt mit der gesamten Policy aus. Dadurch ergibt sich ein Performance-Gewinn. Checkpoint hat sich dieses sog. Stateful Inspection patentieren lassen.

Für die Firewall-1 gibt es zahlreiche Plugins und Zusatzmodule. Die Verfügbarkeit ist jedoch abhängig vom zugrundeliegende Betriebssystem. Zur Zusammenarbeit mit anderen Produkten wurde von Checkpoint die Open Plattform for Security (OPSEC) ins Leben gerufen. Heute unterstützen rund 300 IT-Firmen OPSEC, darunter Microsoft, Red Hat, Oracle, IBM, Citrix, TrendMicro, Symantec, Siemens, Nokia und Cisco. Den Kern von OPSEC bildet ein SDK, das für Windows, Red Hat Linux, Solaris, HP-UX, AIX und Nokia Ipso verfügbar ist. Über OPSEC können Produkte von Checkpoint und anderen Herstellern Daten austauschen. Es stehen verschiedene Schnittstellen zur Verfügung, beispielsweise:

- Content Vectoring Protocol – z. B. Anbindung eines Virenscanners,
- URL Filtering Protocol – Anbindung eines URL-Filter-Tools,
- Logging Export API – sicherer Export der Firewall-Logs in Management-Tools,
- Suspiscious Activity Monitoring – Anbindung eines IDS,
- User Authority API – Abgleich von Benutzerinformationen, Authentifizierung.

Nach Angaben von Checkpoint ist Firewall-1 in der Lage einen Durchsatz bis zu 3,2 Gbps zu gewährleisten, beim Einsatz von VPN sind es noch 1,2 Gbps. Firewall-1 ist außerdem in der Lage gleichzeitig 1,5 Mio. Verbindungen oder 40.000 VPN-Tunnels zu verwalten. Allerdings finden sich in den Beschreibungen von Checkpoint keine Angaben unter welchen Betriebssystem und auf welcher Hardware diese Performance erreicht werden kann.

Konfiguration

Firewall-1 gibt es in zwei Varianten. Die SmallOffice-Version ist ein einzelnes System, das über ein Web-Interface konfiguriert werden kann. Es ist in dieser Hinsicht mit dem Produkt von Astaro vergleichbar. Die Enterprise-Version besteht aus einem Management-Server und einem oder mehreren Firewall-Modulen. Der Management-Server hat verschiedene Aufgaben, u. a. verteilt er die Konfigurationen an die Firewall-Module, gleicht deren Zustandstabellen ab, nimmt die Logs entgegen, wertet die Logs aus und arbeitet über OPSEC mit anderer Software zusammen. Für Outsorcing-Angebote unterstützt Checkpoint Security-Dienstleister mit Provider-1. Dieses Produkt ersetzt den Management-Server und ist im Gegensatz zu diesem mandantenfähig.

Die Konfiguration von Firewall-1 erfolgt in der Regel von einer Management-Station aus. Dazu steht ein Tool mit GUI (Graphical User Interface) zur Verfügung. Für die Konfiguration wird ein objektorientierter Ansatz verwendet. Daneben gibt es auch ein Kommandozeilen-Programm. Für die Pflege des Firewall-Systems wurde von Checkpoint eine Update-Funktion integriert.

Logging

Die Logs laufen auf dem Management-Server auf. Über die Management-Station können die Logs in Echtzeit oder rückblickend betrachtet werden. Außerdem ist eine Zustandsüberwachung des Firewall-Systems an der Management-Station möglich. Der Management-Server kann die Logs auswerten, Reports erzeugen und Logs über die Logging Export API an Management-Software (z. B. Tivoli) übergeben. Über die Suspiscious-Activity-Monitoring-Schnittstelle ist außerdem ein Austausch mit einem IDS möglich. Alarm-Meldungen können per E-Mail oder SNMP-Traps ausgegeben werden.

Firewall-Funktionen

NAT: Firewall-1 bietet statisches und dynamisches NAT an. Außerdem kann bereits bei der Erzeugung eines entsprechenden Objekts eine NAT-Funktion konfiguriert werden.

Proxies: Es werden für zahlreiche Anwendungen Proxies angeboten. Neben den gängigen Internet-Protokollen werden auch viele Multimedia-, VoIP- und Unternehmensanwendungen unterstützt.

Authentifizierung: Es sind eine ganze Reihe von Authentifizierungs-Verfahren möglich, beispielsweise Radius, TACACS+, S/Key, Betriebssystem, Directory Server. Auch das Anbinden von SmartCards ist möglich.

Content-Filtering: Auch hier gibt es zahlreiche Möglichkeiten, die sich durch Zusatzprodukte erweitern lassen. Bereits in Firewall-1 direkt enthalten sind beispielsweise File Name Matching für FTP, E-Mail Address Translation für SMTP, Filterung von bestimmten Attachment-Typen, Filtern von Javascript-Tags bei HTTP, URL-Filterung bei HTTP. Einige Produkte von Drittanbieter: Virenscanner von F-Secure oder Clearswift, URL-Filtering mit Webwasher Enterprise Edition, Java- und ActiveX-Filterung mit Trendmicro Interscan AppletTrap.

VPN: Für die Realisierung einer VPN-Lösung ist VPN-1 von Checkpoint als Zusatzprodukt erhältlich.

2.4.3 PIX 500 von Cisco

Architektur

Die PIX-500-Familie von Cisco ist im Gegensatz zu den anderen vorgestellten Produkten eine reine Appliance-Lösung. Cisco bietet PIX in verschiedenen Versionen an, die sich hinsichtlich der Performance unterscheiden. Auf der Appliance ist ein von Cisco selbst entwickeltes Betriebssystem (PIX OS) installiert. Die folgende Beschreibung basiert auf der Software-Version 6.2.

Ein wichtiger Bestandteil ist der Adaptive Security Algorithm (ASA). Durch diesen Algorithmus wird ein Stateful Filtering mit Zustandstabellen realisiert. In den Zustandstabellen werden – im Gegensatz zu den anderen vorgestellten Produkten – sogar die TCP-Sequenznummern verwaltet. In PIX ist außerdem ein IDS integriert, mit dessen Hilfe verschiedene Angriffe erkannt und blockiert werden können.

Die leistungsfähigste Version ist PIX 535. Sie ermöglicht einen Durchsatz von 1 Gbps, bei gleichzeitiger Verwendung von VPN noch 95 Mbps. Die PIX 535 kann gleichzeitig 500.000 Verbindungen oder 2000 VPN-Tunnel verwalten.

Konfiguration

Die Konfiguration kann kommandozeilenorientiert über Telnet, SSH oder Konsole erfolgen. Auch eine webbasierte Schnittstelle steht zur Verfügung. Zusätzlich bietet Cisco den PIX Device Manager an, der ein GUI-orientierte Administration ermöglicht. Ansonsten kann die PIX in das Management der anderer Cisco-Komponenten integriert werden. Hier bietet sich der Cisco Secure Policy Manager an. In PIX integriert ist außerdem eine Auto-Update-Funktion.

Logging

Das Logging kann über Syslog oder SNMP an einen zentralen Server übergeben werden. Auch Meldungen des integrierten IDS sind über Syslog zugänglich. Es können Reports und Statistiken zu Traffic, Angriffen, Auslastung usw. erstellt werden.

Firewall-Funktionen

NAT: In PIX sind statische und dynamische NAT-Möglichkeiten vorgesehen.

Proxies: Für zahlreiche Protokolle stehen Proxies zur Verfügung, beispielhaft seien HTTP, FTP, DNS, H.323, SIP (Session Initiation Protocol), RTSP, Oracle SQL (Structured Query Language) und NFS (Network File System) genannt.

Authentifizierung: Eine Authentifizierung kann wie bei anderen Cisco-Produkten üblich per Radius oder TACACS+ erfolgen. Im Zusammenspiel mit Radius können benutzerspezifische ACLs vom Radius-Server heruntergeladen und auf der PIX eingerichtet werden. Durch den sog. Cut-Through-Proxy können nach einer erfolgreichen Authentifizierung alle zur Session gehörenden Pakete ohne weitere Filterung durch den Proxy passieren.

Content-Filtering: Wie bei IOS können Java- und ActiveX-Inhalte aus HTTP herausgefiltert werden. Eine URL-Filterung ist durch Angabe eines Websense- oder N2H2-Server möglich. Wird eine HTTP-Anfrage an einen Web-Server geschickt, erfolgt gleichzeitig eine Überprüfung der URL beim Websense- oder N2H2-Server. Nur bei erfolgreicher Überprüfung werden die Antworten des Web-Server akzeptiert.

VPN: Es werden PPTP, IPSec und Cisco-eigene VPN-Lösungen unterstützt.

2.5 Firewall-Konzepte anderer Universitäten

2.5.1 Firewall-Konzept Passau

Im Vergleich zum MWN handelt es sich beim Passauer Hochschulnetz um ein eher kleines Netz. Am Passauer Hochschulnetz sind etwa 10 Institute der Hochschule, die Verwaltung der Hochschule, die Bibliothek und Wohnheime angeschlossen. Außerdem haben einige Passauer Schulen die Möglichkeit über das Hochschulnetz Zugang zum Internet zu erlangen. Betreiber des Passauer Hochschulnetzes ist das Rechenzentrum der Universität Passau.

An der Universität Passau wurde im Oktober 2000 ein Konzept zur Netzwerksicherheit vorgelegt [Rank 00]. Im Gegensatz zu der für das MWN vorgenommenen Analyse geht das Konzept des Passauer Rechenzentrums davon aus, dass ein globales für alle Bereiche geltendes Sicherheitskonzept umgesetzt werden kann. Es soll nur "in besonderen Fällen notwendig sein, zusätzliche Maßnahmen zur Erhöhung der individuellen Rechnersicherheit zu ergreifen."

Analyse

Aus der Beschreibung des Zustands zum Zeitpunkt der Erstellung des Passauer Konzepts geht hervor, dass der Zugriff aus dem Internet auf das Hochschulnetz ohne Beschränkung möglich war. Zugriffsbeschränkungen mussten zu diesem Zeitpunkt auf den am Hochschulnetz angeschlossenen Rechnern vorgenommen werden. Für berechtigte Benutzer steht ein offizieller Modemzugang für die Verbindung von außen zur Verfügung. Darüber hinaus wird befürchtet, dass in einzelnen Büros weitere Modemzugänge vorhanden sind. Besondere Schwierigkeiten bereitet der Anschluss der Schulen. Dafür gibt es keinen zentralen, sondern mehrere im Hochschulnetz verteilte Übergangspunkte.

Auf dem Unigelände existieren weitere Zugangsmöglichkeiten zum Hochschulnetz. Die Rechner von Mitarbeitern und Lehrstühlen erhalten ohne Authentifizierung Zugang zum Netz. Allerdings werden die an den Switch-Ports gelernten MAC-Adressen regelmäßig gespeichert, wodurch ein Rechner später u. U. identifiziert werden kann. In den Rechnerpools der Universität müssen sich die Benutzer am Rechner anmelden und es findet ebenfalls eine Speicherung der MAC-Adressen statt. Die Rechner und Netzdosen in der Bibliothek sind frei zugänglich, ebenso ein Teil der Anschlüsse in den Hörsälen. In den Studentenwohnheimen besitzt jedes Zimmer eine Netzwerkdose, an die ein Rechner mit einer am Switch fest eingestellten MAC-Adresse angeschlossen werden kann. Der Zugang zum Internet von den Studentenwohnheimen ist nur über Proxies möglich.

Aufgrund der Analyse wurden folgende grundsätzliche Ziele formuliert:

- "Umfangreicher und wirkungsvoller Schutz des Uninetzes und der daran betriebenen Rechner vor Missbrauch – von außerhalb (Internet) und aus dem Uninetz selbst."
- "Bei erfolgtem (oder auch versuchtem) Missbrauch: Identifikation des Rechners, von dem aus der Missbrauch stattgefunden hat. Identifikation der Person, die den Missbrauch ausgeführt hat."

Konzept

Für die Umsetzung des Konzepts wurde eine Neuordnung der Topologie vorgeschlagen. Es sollen nach Möglichkeit Subnetze für bestimmte Aufgaben geschaffen werden (z. B. Servernetz). Am Übergangspunkt zum WiN soll eine zentrale Firewall eingerichtet werden (siehe Abbildung 2.2). Die Firewall ist zweistufig konzipiert. Vom Internet aus bildet ein Cisco-Router 7206 mit Paketfilterfunktionen die erste Stufe. Die zweite Stufe ist das Firewall-Produkt PIX, ebenfalls von Cisco. Dazwischen wird eine DMZ eingerichtet. Der Zugriff vom Internet auf das Hochschulnetz soll nur für bestimmte Anwendungen über Application-Level-Gateways in der DMZ möglich sein. In der DMZ wird zusätzlich ein VPN-Server eingerichtet. Außerdem soll der Zugang der Schulen zentralisiert werden und offene Ports in einem eigenen Subnetz zusammengefasst werden.

Die zentrale Firewall soll den Zugriff von außen nur noch für bestimmte Dienste auf festgelegten Servern zulassen. In einer vorläufigen Liste wurden folgende Dienste genannt: FTP (Port 20, 21), SSH

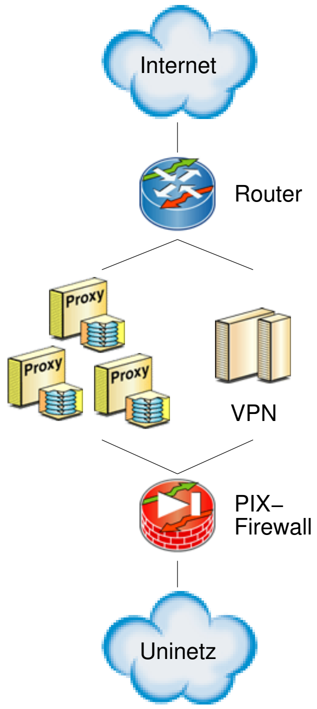

Abbildung 2.2: Firewall-Konzept der Universität Passau

(Port 22), SMTP (Port 25), DNS (Port 53), HTTP (Port 80), POP2 (Post Office Protocol 2, Port 109), POP3 (Port 110), IMAP (Internet Message Access Protocol, Port 143), IMAP3 (Port 220) und HTTPS (Port 443). Andere sicherheitskritische Dienste (z. B. Telnet) sollen gar nicht mehr oder nur über VPN ermöglicht werden. Die Begrenzung auf diese Dienste soll mit Hilfe der Router-Hardware (Cisco 7206) realisiert werden. Es wurde auch auf die Notwendigkeit hingewiesen, den Verkehr innerhalb des Hochschulnetzes zu filtern.

Ein wichtiger Bestandteil des Passauer Konzepts ist eine durchgehende Identifizierung der berechtigten Rechner und Benutzer:

- Für die Rechner in den Pools und Bibliotheken soll eine statische Zuordnung der MAC-Adresse am Switch-Port vorgenommen werden. Bei anderen Rechnern sollen periodisch die aktuellen MAC-Adressen an den Switch-Ports ausgelesen werden (Switch-Polling).
- Bei statischen Rechnern mit einer großen Benutzergruppe soll die Authentifizierung an einem zentralen Gateway erzwungen werden.
- Offene Ports sollen in einem eigenen Subnetz zusammengefasst werden. Benutzer haben sich ebenfalls an dem zentralen Gateway zu authentifizieren.
- Die in den Hörsälen vorhanden Ports sollen physisch gesichert werden.

Auch die Einrichtung eines VPN wird in dem Passauer Konzept diskutiert. Mit Hilfe eines VPN kann vor allem verhindert werden, dass Passwörter im Klartext übertragen werden. Über VPN können Benutzer von außerhalb Zugang zum Hochschulnetz erlangen und so gestellt werden, als ob sie sich innerhalb des Hochschulnetzes befänden.

Ein weitere Thema ist die Abschirmung vor Viren, Trojanern u. ä. Es soll geklärt werden, ob das automatische Scannen von E-Mails, FTP-Downloads etc. rechtlich und technisch möglich ist.

Bewertung

Ein Hauptaugenmerk des Konzepts liegt in der Schaffung einer durchgängigen Möglichkeit bei Missbrauchsfällen den verursachenden Rechner oder Benutzer zu identifizieren. Deshalb ist in verschiedenen Bereichen die Registrierung von MAC-Adressen vorgesehen. Die Identifizierung der Rechner ist jedoch nicht hundertprozentig sichergestellt, da MAC-Adressen manipuliert werden können. Außerdem verursacht die feste Zuordnung von MAC-Adressen zu Switch-Ports einen hohen Managementaufwand. Die Identifizierung von Benutzern soll bei Rechnern mit einer großen Benutzerzahl oder bei offenen Ports durch einen Authentifizierungs-Gateway realisiert werden. Für ein großes Netz wie das MWN ist die feste Zuordnung von MAC-Adressen auf Grund des hohen Aufwands nur in Ausnahmefällen möglich. Die Schaffung einer erzwungen Authentifizierung ist jedoch auch für das MWN denkbar. Entsprechende Planungen auf Basis von 802.1x und den Radius-Servern gibt es bereits [ApLä 02].

Der Zugriff von außen auf das Hochschulnetz soll in Passau über eine zentrale Firewall abgewickelt werden. Es sollen nur bestimmte Dienste auf bestimmten Servern erreichbar sein. Auch damit ist ein hoher Managementaufwand verbunden, der in dem wesentlich größeren Netz des MWN große Probleme verursacht. Eine zentrale Firewall am Übergang zum WiN hat außerdem den Nachteil, dass der Verkehr zwischen den Instituten nicht kontrolliert wird. Zwar wird im Passauer Konzept angemerkt, dass eine entsprechende interne Kontrolle des Netzverkehrs sinnvoll ist, genauere Angaben finden sich jedoch nicht.

Insgesamt wird im Konzept davon ausgegangen, dass sich im Passauer Hochschulnetz ein einheitliches Sicherheitskonzept durchsetzen lässt, das u. a. vorgibt, welche Dienste von den Instituten nach außen angeboten werden können. Berücksichtigt werden dabei nur die klassischen Dienste WWW, E-Mail und FTP, sowie SSH. In der wesentlich heterogeneren Umgebung des MWN mit den vielen Hochschulen und anderen Einrichtungen ist eine solche globale Vorgabe nicht möglich.

Zwei Details sind noch interessant. Das Passauer Hochschulnetz ist weitestgehend geswitched. Leider wird in der Analyse noch davon ausgegangen, dass dadurch das Abhören des Netzverkehrs nicht möglich ist. Seitdem Tools wie dsniff existieren ist dies nicht mehr gewährleistet. Richtig und auch für das MWN zu befürworten ist das generelle Verbot von Modems in den Instituten. Dadurch wird sichergestellt, dass nur ein Übergang zwischen Internet und Hochschulnetz besteht.

2.5.2 Firewall-Konzept Karlsruhe

Das Hochschulnetz der Universität Karlsruhe mit dem Namen Klick liegt von der Größenordnung zwischen dem Hochschulnetz Passau und dem MWN. Es sind etwa 150 Institute, die am Karlsruher Netz angeschlossen sind. Betrieben wird das Hochschulnetz vom Rechenzentrum der Universität Karlsruhe. In einem Sicherheitskonzept des Rechenzentrums der Universität Karlsruhe wurden im März 2000 “Maßnahmen zur Abwehr von Angriffen auf Rechnersysteme über Netzverbindungen” vorgeschlagen [Lort 00]. Zusätzliche Informationen finden sich in [RZ-KA].

Analyse

Kernstück von Klick ist ein ATM-Backbone. Am Rand des der “ATM-Wolke” befinden sich Switches und Router, über die ein Übergang auf Ethernet möglich ist. Jeder Switch-Port im Klick lässt sich einem VLAN zuordnen. Es existieren mehrere Benutzer-VLANs. Diese bestehen aus mehreren durch

Repeater gekoppelten Segmenten, die jeweils an einem Port des Ethernet-Switch hängen. Für Server sind weitere VLANs eingerichtet, die auch als ATM-Endgeräte angeschlossen sein können. Für die Router existiert ein eigenes VLAN, in dem nur die Routingprotokolle erlaubt sind und benutzt werden. Für das Management der Komponenten existiert ebenfalls ein eigenes VLAN, das sogar auf einer eingenen Verkabelung besteht.

In der ausführlichen Analyse des Sicherheitskonzepts wurde festgestellt, dass Angriffe sowohl von außen, als auch innerhalb des Klick stattfinden können. Auch im Klick wird davon ausgegangen, dass es neben den offiziellen Modem-Zugängen weitere Modems in den einzelnen Instituten gibt. Diese sind dem Rechenzentrum (RZ) meist nicht bekannt und stellen daher nicht kontrollierbare Einwahlpunkte dar. Weiterhin werden "wandernde Geräte" (z. B. Laptops) [RZ-KA] als problematisch angesehen, da sie auch in nicht geschützten Bereichen angeschlossen und dort erfolgreich angegriffen werden können. Schließlich wurde darauf eingegangen, dass sich aus Sicherheit und Konnektivität unterschiedliche Anforderungen ergeben.

Im Sicherheitskonzept der Universität Karlsruhe wurden folgende Ziele vorgegeben:

- "Formulierung der Sicherheitsziele.
- Definitionen von Bereichen mit gleichartigen Sicherheits- und Konnektivitätsanforderungen.
- Schwachstellenanalyse.
- Erstellen eines Sicherheitshandbuchs mit einem öffentlichen und einem RZ-internen Teil."

Konzept

Für die Umsetzung des Sicherheitskonzepts wurden mehrere Sicherheitsbereiche identifiziert. Das Zentralnetz verbindet die einzelnen Institute untereinander und ist selbst in weitere Bereiche mit unterschiedlichen Sicherheitsanforderungen unterteilt. Jedes Institut besitzt ein eigenes Institutsnetz. Daneben gibt es für die Verwaltung der Hochschule ein eigenes Verwaltungsnetz. Innerhalb eines jeden Institutsnetzes gibt es ein Sekretariatsnetz, das für den Schutz der Personal- und Haushaltsdaten zusätzlich gesichert ist. Zwischen den Sekretariatsnetzen und dem Verwaltungsnetz bestehen kryptographische Tunnel zum sicheren Austausch von Daten.

Die einzelnen Sicherheitsbereiche werden durch Firewalls getrennt. "Der Zugang vom Internet und von den Wähleingängen erfolgt über die Hauptpforte" [Lort 00]. Der Übergang vom Zentralnetz zu einem Institutsnetz bzw. zum Verwaltungsnetz erfolgt über eine Institutspforte. Das Sekretariatsnetz innerhalb des Institutsnetz ist durch einen sog. Institutssafe gesichert. Die Merkmale dieser Firewalls werden wie folgt beschrieben:

Hauptpforte: Statischer Filter zur Abwehr primitiver Angriffe, die Konnektivität des Zentralnetzes soll dadurch nicht wesentlich eingeschränkt werden. Die Filter sollen auf dem zentralen Zugangsrouter eingerichtet werden. Da das Zentralnetz dadurch nur schwach geschützt ist müssen kritische Endgeräte besonders gesichert werden.

Institutspforte: Die Institutspforte kann auf mehrere Arten realisiert werden. Ähnlich wie bei der Hauptpforte sind statische Filter möglich, die auf den internen Routern des Klick implementiert werden können. Dadurch kann vor einfachen Angriffen aus anderen Bereichen der Universität geschützt werden. Mehr Sicherheit wird erreicht, wenn ein dezidiertes Firewall-System eingesetzt wird. Dies kann optimal auf die Bedürfnisse eines Instituts ausgerichtet werden. Vom Rechenzentrum soll dafür ein Standardmodell entwickelt werden.

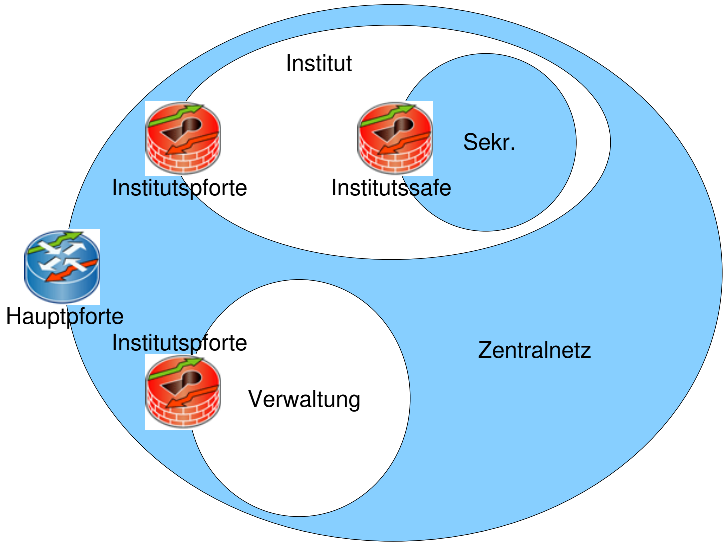

Abbildung 2.3: Firewall-Konzept der Universität Karlsruhe

Institutssafe: Für den Schutz der Sekretariatsnetze soll eine einheitliches und zentral gemanagtes Firewall-System eingesetzt werden. Es besteht die Möglichkeit Institutspforte und Institutssafe auf einem gemeinsamen Firewall-System zu implementieren.

Wie schon erwähnt soll das Zentralnetz in weitere Bereiche unterteilt werden. Diese Bereiche sind alle an der Hauptpforte angeschlossen.

Offenes Netz: Das offene Netz soll im wesentlichen frei zugänglich sein.

Servernetz: Es enthält zentrale Server, die vom Internet und Uninetz angesprochen werden können. Es ist ein offenes Netz, die darin enthaltenen Rechner müssen selbst gut gesichert sein.

Internes Servernetz: Es enthält Server, die nur vom Klick aus angesprochen werden können. Neben den statischen Filterregeln der Hauptpforte sollen für diese Rechner private IP-Adressen verwendet werden.

Internes Netz: Es hat keine Verbindung zum Internet.

Die Wählverbindungen sollten laut Rechenzentrum genau so behandelt werden, wie Zugriffe aus dem Internet. Da jedoch davon auszugehen ist, dass dies von den Instituten nicht akzeptiert wird, sollen sie wie Zugriffe aus dem Klick behandelt werden.

Das Rechenzentrum der Universität Karlsruhe bietet für die Institutspforten eine "Grundkonfigurationen an, die bei Bedarf den speziellen Anforderungen der Institute angepasst werden können" [RZ-KA]. Dabei werden im Institutsnetz zwei Sicherheitsbereiche unterschieden:

Das Mitarbeiternetz für die Arbeitsplatzrechner der Mitarbeiter und für interne Server. Aus dem Mitarbeiternetz ist der Zugriff auf das sichere Servernetz und nach außen möglich. Einschränkungen bestehen nur bei technischen Problemen oder besonders unsicheren Anwendungen. Protokolle, die Klartextpasswörter verwenden sollen nur auf ausdrücklichen Wunsch ermöglicht werden. Ein Zugriff von außen oder aus dem sicheren Servernetz auf das Mitarbeiternetz ist nicht möglich. Lediglich ein Zugriff per SSH kann auf einzelne Rechner ermöglicht werden.

Zugriffsmöglichkeit	Protokolle
Zugriff auf alle Rechner	Finger (TCP 79), Ident (TCP 113), Oracle SQL (TCP 1521 - 1526), Ping (ICMP 8), Real Audio (TCP 7070), SSH (TCP 22), SSH alternativer Port für SSH2 (TCP 24), Whois (TCP 43), WWW (TCP 80)
Zugriff auf alle Rechner, Klartextpasswörter	FTP (TCP 20, 21), Telnet (TCP 23)
Zugriff nur auf einzelne Server	ADSM (ADSTAR Distributed Storage Management)/TSM (TCP 1501 - 1509), DNS (UDP 53, TCP 53), Huelka (TCP 19991 - 19993, 37251), IMAPS (Internet Message Access Protocol, Port 143), TCP 993), NNTP (Network News Transfer Protocol, TCP 119), NTP (Network Time Protocol, UDP 123), SMTP (TCP 25), SPOP3 (Secure Post Office Protocol 3, TCP 995), WWW-Cache (TCP 3128)
Zugriff nur auf einzelne Server, Klartextpasswörter	POP3 (TCP 110)

Tabelle 2.4: Protokolle mit Zugriff vom Mitarbeiternetz nach außen

Zugriffsmöglichkeit	Protokolle
Zugriff auf alle Rechner	ADSM/TSM (TCP 1501 - 1509), DNS (UDP 53, TCP 53), Finger (TCP 79), Ident (TCP 113), Oracle SQL (TCP 1521 - 1526), Ping (ICMP 8), SSH (TCP 22), SSH alternativer Port für SSH2 (TCP 24)
Zugriff auf alle Rechner, Klartextpasswörter	Telnet (TCP 23)
Zugriff nur auf einzelne Server	NTP (UDP 123)

Tabelle 2.5: Protokolle mit Zugriff vom sicheren Servernetz nach außen

Das sichere Servernetz für öffentliche Server (z. B. WWW-Server). Das sichere Servernetz hat keinen Zugriff auf das Mitarbeiternetz und nur beschränkte Zugriffsmöglichkeiten nach außen. Der Zugriff von außen auf das sichere Servernetz soll nur für die notwendigen Serverfunktionen möglich sein. Im wesentlichen sind dies WWW-Server, FTP-Server und der institutseigenen Mailserver.

Die Institutspforte lässt standardmäßig bestimmte Protokolle passieren. Vom Mitarbeiternetz nach außen werden die in Tabelle 2.4 aufgeführten Protolle unterstützt. Bei einigen ist nur der Zugriff auf einzelne Server gestattet, Protokolle mit Klartextpasswörtern werden nur auf Anfrage freigegeben. Ein Zugriff von außen auf das Mitarbeiternetz ist nur auf einzelne Rechner über SSH erlaubt. In Tabelle 2.5 sind die Protokolle aufgeführt, für die ein Zugriff aus dem sicheren Servernetz nach außen möglich ist. Für den Zugriff von außen auf das sichere Servernetz sind dies Ident (TCP 113) und WWW (TCP 80). Auch ein Zugriff vom Mitarbeiternetz auf das sichere Servernetz ist möglich. Im wesentlichen werden dabei die Protokolle aus den ersten beiden Zeilen von Tabelle 2.4 unterstützt, bis auf Oracle SQL und Whois. Bei besonderen Wünschen passt das Rechenzentrum der Universität Karlsruhe diese Konfiguration an.

Für den Zugriff auf externe Dateisysteme über die Firewall hinweg werden NFS und DCE/DFS (Distributed Computing Environment, Distributed File System) als nicht geeignet angesehen. Nur der Zugriff auf Windows-Dateisysteme konnte erfolgreich getestet werden. Dadurch ergeben sich zwei Basismodelle für die Institutspforte:

- “Grundmodell ohne Nutzung von Windowsoperationen über das Firewallsystem.
- Grundmodell mit Nutzung von Windowsoperationen über das Firewallsystem.”

Auf Wunsch können auch Telefonkonferenzen über Netmeeting ermöglicht werden. Ein Verbindungsaufbau von außen ist jedoch nicht möglich. Für den Zugriff auf das Mitarbeiternetz kann neben der SSH-Möglichkeit ein VPN-Zugang eingerichtet werden.

Bewertung

Der Zugriff von außen auf das Hochschulnetz Karlsruhe erfolgt über eine gestaffelte Firewall-Lösung. Es werden verschiedene Sicherheitsbereiche und die einzelne Dienste genau unterschieden. Eine zentrale Firewall am Übergang zum Internet schützt vor primitiven Angriffen. Die einzelnen Institute und innerhalb der Institute die Sekretariate sind zusätzlich geschützt, so dass nicht nur Angriffe von außen, sondern auch von anderen Bereichen im Klick abgewehrt werden können. Innerhalb der Institutsnetze werden neben dem Sekretariatsnetz ein Mitarbeiternetz und ein sicheres Servernetz unterschieden. Ein Unterschied zum MWN besteht darin, dass im MWN die Verwaltungen der Hochschuleinrichtungen als eigene “Institute” angesehen werden und deshalb im Institutsnetz nicht zusätzlich gesichert werden müssen.

Das Firewall-Konzept von Karlsruhe bietet neben einer Grundkonfiguration viele zusätzliche Optionen, wie Freischalten von Protokollen mit Klartextpasswörtern, Ermöglichen von Telefonkonferenzen oder der Zugriff von außen auf einzelne Rechner des Mitarbeiternetzes per SSH. Außerdem werden auf Wunsch weitere Anpassungen vorgenommen. Dies ist für das MWN auf Grund der wesentlich größeren Anzahl der Institute nicht zu leisten.

Die Möglichkeit über Windows-Operationen auf externe Dateisysteme zuzugreifen scheint im MWN nicht notwendig. Die Umfrage bei den Kunden des MWN hat ergeben, dass nur wenige Institute einen Dateizugriff auf Rechner im MWN oder Internet benötigen. Eine Ausnahme stellt der Zugriff auf das Backup-System des LRZ dar, der jedoch über eigene Protokolle abgewickelt wird.

Kapitel 3

Anforderungen an den Firewall-Dienst

Wie bereits erwähnt, sind am MWN sind rund 700 Institute angeschlossen. Bei einer so großen Zahl muss davon ausgegangen werden, dass die Institute sehr unterschiedliche Erwartungen an den Firewall-Dienst haben. Soll durch den Firewall-Dienst ein gewisses Maß an Sicherheit erreicht werden, geht dies nicht ohne Einschränkungen bei der Nutzungen des Internets. Dies bedeutet, dass viele Dienste nicht mehr oder nur noch begrenzt genutzt werden können. Auch das Anbieten von Diensten für das Internet oder das MWN seitens der Institute wird nicht mehr in vollem Umfang möglich sein. Die Institute werden verschiedene Ansichten darüber haben, wo die Grenze zwischen der Sicherheit und den Kommunikationsbedürfnissen zu ziehen ist. Entsprechend unterschiedlich werden die Anforderungen an den Firewalldienst seitens der Institute ausfallen.

Die Institute fordern schon seit längerer Zeit vom LRZ eine Unterstützung bei der Absicherung ihrer Institutsnetze. Die genauen Anforderungen der Institute an einen Firewall-Dienst sind jedoch nicht bekannt. Um den Firewall-Dienst möglichst gut an den Kundenwünschen ausrichten zu können, müssen die Anforderungen der Institute in Erfahrung gebracht werden. Dazu wurde ein Fragebogen erstellt und den Netzverantwortlichen der Institute vorgelegt. Nach den Netzbenutzungsrichtlinien [Läpp 01] waren die Netzverantwortlichen der Institute die richtigen Adressaten für diesen Fragebogen. Außerdem wurde der Fragebogen den Mitgliedern des Arbeitskreis "Firewall" zugesandt, nachdem das Vorhaben im Arbeitskreis vorgestellt worden war. Im Abschnitt 3.1 wird das Konzept des Fragebogens erläutert. Die Ergebnisse der Einzelfragen sind in Abschnitt 3.2 dargestellt.

Ein Problem bei der Entwicklung des Firewall-Dienstes besteht darin, die individuellen Interessen der einzelnen Institute und die Möglichkeiten des LRZ in Einklang zu bringen. Der Firewall-Dienst soll möglichst so gestaltet werden, dass er allen Anforderungen der Institute gerecht wird. Auf der anderen Seite muss der Betrieb des Dienstes durch die Personalkapazitäten des LRZ bewältigbar sein. Eine Firewall für einen Kunden muss schnell und einfach vom LRZ eingerichtet werden können. Die für ein einzelnes Institut notwendige Konfiguration (IP-Adressen, Domain etc.) bei der Einrichtung der Firewall darf nicht zu umfangreich sein. Der Firewall-Dienst kann deshalb nicht auf einzelne Institute, sondern nur auf Gruppen von Instituten ausgerichtet werden. In den Abschnitten 3.3 und 3.4 zu diesem Zweck Dienste- und Kundenprofile erstellt. Der zukünftige Firewall-Dienst soll so gestaltet werden, dass er diesen Profilen weitestgehend entspricht.

In den durch die Firewall getrennten Netzen sollen sich jeweils Rechner mit ähnlichen Sicherheitsanforderungen befinden. Dazu werden in Abschnitt 3.5 Sicherheitszonen innerhalb eines Kundennetzes identifiziert. Außerhalb des Kundennetzes können die Zonen MWN und Internet festgestellt werden.

Die Unterschiede zwischen diesen beiden Zonen werden im Abschnitt 3.6 diskutiert. Die Anforderungen werden schließlich in Abschnitt 3.7 zusammengefasst dargestellt, ergänzt um Punkte die sich aus der Problembeschreibung des letzten Kapitels ergeben.

3.1 Konzept des Fragebogens

3.1.1 Technische Details

Der Fragebogen wurde in HTML erstellt und auf dem öffentlichen Web-Server des LRZ an passender Stelle (http://www.lrz-muenchen.de/services/security/fragebogen/) abgelegt. Die URL wurde durch eine E-Mail den Netzverantwortlichen der Institute mitgeteilt. Außerdem enthielt die Mail einen kurzen Text, der von Seiten des LRZ erstellt wurde und den Sinn des Fragebogens kurz erläuterte.

Um die Bearbeitung des Fragebogens nicht von bestimmten Betriebssystemen oder Webbrowsern abhängig zu machen, wurde weitestgehend der HTML-Standard 3.2 verwendet, der als kleinster gemeinsamer Nenner gelten kann. Außerdem wurde auf Skriptelemente (Javascript) verzichtet. Die Korrektheit wurde mit dem HTML Validation Service des W3C (http://validator.w3.org/) überprüft. Bis auf die Verwendung des Attributs `bcolor` im `tr`-Tag war die Überprüfung erfolgreich. (Dieser Fehler wurde in Kauf genommen, weil so der Fragebogen übersichtlicher gestaltet werden konnte.) Leider stellte sich später heraus, dass der Internet Explorer von Microsoft trotzdem nicht in der Lage war, diese HTML-Seite korrekt zu verarbeiten. Der DOCTYPE-Tag am Anfang der HTML-Seite, der eigentlich den Hinweis auf die verwendete HTML-Version geben soll, erwies sich hier als Stolperstein. So musste dieser Tag entfernt werden, was freilich vom HTML Validator Service moniert wurde.

Für Benutzereingaben in eine Webseite bietet HTML einige Formularelemente an. Die eingegebenen Informationen können dann auf verschiedene Weisen an den Server bzw. an den Auswerter zurück geschickt werden, u. a. als E-Mail. Dies setzt allerdings auf Seiten des Clients ein korrekt eingerichtetes E-Mail-Programm und ein funktionierendes Zusammenspiel zwischen Web Client und Mail Client voraus. Da davon nicht immer ausgegangen werden kann, wurden die Informationen stattdessen per HTTP an ein CGI-Programm (Common-Gateway-Interface-Programm) auf Seiten des Webservers geschickt. Das CGI-Programm (ein sog. Formmailer) packte nun seinerseits die erhaltenen Daten in eine Mail und leitete diese an den Auswerter weiter. Ein entsprechendes CGI-Programm stand auf dem Webserver des LRZ zur Verfügung.

Die Daten in den E-Mails wurden zur Auswertung in eine PostgreSQL-Datenbank übernommen. So weit es möglich war, geschah dies komfortabel mit Hilfe von verschiedenen Skripten. Dies klappte beispielsweise bei Daten, die im Fragebogen per Radio Button oder Checkbox eingegeben werden mussten und so standardisiert waren. An manchen Stellen war jedoch Handarbeit notwendig. Beispielsweise wurde im Fragebogen nach der Anzahl der Rechner im Institut gefragt. Für die Eingabe eignet sich dazu nur ein Textfeld (input type="text"), in das aber auch Eingaben der Form "ca. 100" oder "100 - 110" gemacht werden können.

3.1.2 Aufbau des Fragebogens

Der Fragebogen wurde mit einem kurzen Text eingeleitet und motiviert. Darin wurden drei Studien zum Thema "Internet und Sicherheit" [BMI 01] zitiert und auf jüngste Vorfälle im LRZ hingewiesen. Zusätzlich wurde in der Einleitung herausgestellt, dass für Angriffe heute kein tiefer gehendes

Verständnis der Protokolle und Programme mehr notwendig ist, sondern viele Tools kursieren, die von fast jedem benutzt werden können. Diese zum Teil etwas reißerische Darstellung sollte die angeschriebenen Netzverantwortlichen noch einmal motivieren, an der Umfrage teilzunehmen. Außerdem wurde kurz erläutert, welchen Zweck die Umfrage hat.

Auch wenn nur die Netzverantwortlichen der Institute angeschrieben wurden, so musste doch davon ausgegangen werden, dass verschiedene im Fragebogen vorkommende Begriffe und Abkürzungen nicht allen geläufig sind. Deshalb wurde am Ende des Fragebogens ein kurzes Glossar angehängt.

Insgesamt gab es im Fragebogen 39 Fragen, die auf 6 Blöcke verteilt waren:

- Angaben zum Institut und zum Netzverantwortlichen
- Beschreibung des Institutsnetzes
- Nutzung von Diensten
- Eigene Dienste
- Eigene Maßnahmen zum Schutz des Institutsnetzes
- Fragen zum Firewall-Dienst des LRZ

Ein freies Textfeld am Ende bot Raum für zusätzliche Bemerkungen von Seiten des Ausfüllers. Zu Beginn jedes Frageblocks wurde mit wenigen Worten erklärt, welcher Zusammenhang zwischen den Fragen und dem zukünftigen Firewalldienst des LRZ besteht.

3.1.3 Angaben zum Institut und zum Netzverantwortlichen

Die Eingabe des Institutsnamens ermöglichte die Identifizierung eines Fragebogens. Damit sollten versehentlich mehrmals abgeschickte Fragebögen herausgefiltert werden. Im Zusammenspiel mit der Frage nach der Zugehörigkeit zur LMU, TU, FH oder einer anderen Einrichtung sollte herausgefunden werden, welche Arten von Instituten sich an der Umfrage beteiligten. Name und E-Mail-Adresse des Ausfüllers wurden für eventuelle Rückfragen erfasst.

3.1.4 Beschreibung des Institutsnetzes

Die Fragen in diesem Block dienten dazu, eine Vorstellung von der Größe des Institutsnetzes und von den eingesetzten Betriebssystemen zu erhalten. Dies sollte dazu beitragen, einen eventuellen Zusammenhang zwischen diesen Angaben und Anforderungen an den Firewall-Dienst aufzuzeigen.

Für die Feststellung der Größe des Institutsnetzes wurde nach der Anzahl der zur Verfügung stehenden öffentlichen IP-Adressen, der Verwendung von privaten IP-Adressen, der Anzahl der Subnetze und der Anzahl der angeschlossenen Rechner gefragt. Bei letzterem wurde unterschieden zwischen festen und mobilen Rechnern. Mobile Rechner stellen ein zusätzliches Problem dar, da davon auszugehen ist, dass sie in mehreren Netzen (z. B. auch zu Hause) eingesetzt werden. Die Frage nach der Verwendung privater IP-Adressen hat auch für den Bereich "Eigene Maßnahmen zum Schutz des Institutsnetzes" (siehe Abschnitt 3.1.7) Bedeutung, da ein Rechner mit einer privaten IP-Adresse aus dem Internet nicht direkt erreichbar ist.

Bei der Frage nach den Betriebssystemen wurden vier mögliche Antworten (Windows 95/98/Me, Windows NT/2000/XP, Linux, Solaris) in Form von Checkboxen vorgegeben. Daneben stand ein Textfeld zur Verfügung, in das nicht vorgegebene Betriebssysteme eingetragen werden konnten.

Am Ende dieses Blocks wurden noch zwei Punkte abgefragt, die ein besonderes Sicherheitsproblem darstellen, da sie eine Firewall grundsätzlich aushebeln können: Modems oder ISDN-Adapter, die einen Zugang zu Rechnern oder zum Institutsnetz ermöglichen; frei zugängliche Netzwerksteckdosen.

3.1.5 Nutzung von Diensten

Da das LRZ nicht für alle Dienste gleichermaßen Schutz bieten kann, sollte mit diesen Fragen festgestellt werden, welche Dienste von den Instituten genutzt werden. Dabei wurde unterschieden zwischen Diensten die aus dem MWN oder darüber hinaus aus dem Internet bezogen werden. Es war davon auszugehen, dass die Standarddienste wie WWW, E-Mail oder FTP am meisten genutzt werden. Im Bereich des MWN dürfte aber auch auf Dienste, wie DNS, DHCP oder Proxies verstärkt zugegriffen werden. In beiden Fällen war eine Reihe von voraussichtlich häufig genutzten Diensten vorgegeben, die über Checkboxen ausgewählt werden konnten, dort nicht aufgeführte Dienste konnten in ein Textfeld eingetragen werden.

3.1.6 Eigene Dienste

In den Instituten werden Server betrieben, die Dienste für den Zugriff von außen anbieten. Zum Teil können diese nur aus dem MWN, zum Teil auch aus dem Internet erreicht werden, so dass hier eine entsprechende Unterscheidung notwendig war. Wie im vorherigen Block wurden auch hier mit Checkboxen Vorgaben gemacht, für weitere Dienste stand wieder ein Textfeld zur Verfügung.

Ob die Server, die Dienste nach außen anbieten, in einer DMZ liegen, wurde mit der nächsten Frage geklärt. Diese hätte von der Gliederung des Fragebogens auch im nächsten Block gestellt werden können, auf Grund der inhaltlichen Zusammenhänge schien diese Stelle aber geeigneter.

Abschließend wurde nach Diensten gefragt, die zwar im Institut genutzt werden, von außen aber auf keinen Fall erreichbar sein sollen. In diesem Zusammenhang wurde u. a. an Datei- und Druckdienste gedacht. Auch hier wurden wieder einige Dienste durch Checkboxen zur Auswahl gestellt, andere konnten in einem Textfeld angegeben werden.

3.1.7 Eigene Maßnahmen zum Schutz des Institutsnetzes

Schon in den vorherigen Abschnitten sind Fragen aufgetaucht, die sich auf eigene Schutzmaßnahmen der Institute bezogen haben. So wurde beispielsweise nach der Verwendung privater IP-Adressen oder dem Vorhandensein einer DMZ gefragt. In diesem Block wurde darüber hinaus nach dem Einsatz spezieller Software gefragt: Firewalls, Desktop-Firewalls und Antiviren-Produkte. Zur Frage nach dem Einsatz von Firewalls gab es zusätzlich ein Textfeld, in dem das verwendete Firewallprodukt eingetragen werden konnte.

3.1.8 Fragen zum Firewalldienst des LRZ

Die bisherigen Fragen bezogen sich auf den momentanen Zustand in den Instituten. Die folgenden elf Fragen hingegen waren dem zukünftigen Firewall-Dienst gewidmet. Mit den ersten drei Fragen sollte festgestellt werden, in wie weit die Institute Einschränkungen bei der Nutzung von Diensten akzeptieren würden:

- Beschränkung des Zugriffs auf ausgewählte Dienste
- Filterung von Java-Applets und anderen aktiven Inhalten
- Filterung von URLs, um z. B. den Zugriff auf bestimmte Seiten zu unterbinden

Eine Möglichkeit, um ein Institutsnetz vor unberechtigten Zugriffen von außen zu schützen, ist es gar keine mehr zuzulassen. In zwei Fragen wurde abgeklärt, ob auf Zugriffe aus dem Internet bzw. aus dem MWN auf das eigene Institutsnetz verzichtet werden kann. In Zusammenhang damit Stand die folgende Frage nach der Notwendigkeit eines Remote-Zugangs zum Institutsnetz. So wäre zwar der Zugriff aus dem Internet oder dem MWN unterbunden, berechtigte Personen könnten aber remote auf das Institutsnetz zugreifen, um beispielsweise von zu Hause aus Daten aus dem Institut zu nutzen.

Manche Institute werden auch zukünftig eigene Server betreiben wollen. Um das übrige Institutsnetz wirksam schützen zu können, ist es notwendig, die Server in ein eigenes Subnetz (DMZ) auszulagern. Der Zugriff von außen könnte dann auf dieses Subnetz beschränkt werden. Neben dieser Beschränkung sind u. U. auch Umstrukturierungen im Institutsnetz notwendig. In zwei Fragen wurde abgeklärt, ob die Institute mit entsprechenden Maßnahmen einverstanden wären, wobei wieder unterschieden wurde zwischen Zugriffen aus dem Internet und aus dem MWN. Dem Thema Umstrukturierungen widmete sich auch eine Frage, nach einer möglichen Änderung der IP-Adressierung im Institutsnetz. Dahinter stand der Gedanke verstärkt private IP-Adressen einzusetzen.

Wer eigene Dienste nach außen anbieten will, kann dazu auch Serverkapazitäten des LRZ nutzen. Das LRZ bietet für viele Dienste entsprechende Server an. Mit einer ersten Frage sollte zunächst geklärt werden, ob den Verantwortlichen der Institute dieses Angebot des LRZ überhaupt bekannt ist. Die anschließende Frage versuchte dann zu ergründen, ob die Institute bereit sind, statt ihrer eigenen Server zukünftig verstärkt die Kapazitäten des LRZ zu nutzen.

3.2 Auswertung der Fragebögen

3.2.1 Vorbemerkungen

Im Fragebogen wurde nach den Betriebssystemen, Diensten und Firewalls gefragt, die in den Instituten eingesetzt werden. Bei den Betriebssystemen und Diensten gab es zur Arbeitserleichterung einige Vorgaben in Form von Checkboxen, die einfach angeklickt werden konnten. Dort nicht aufgeführte Betriebssysteme und Dienste, sowie die Firewalls konnten in ein Textfeld eingegeben werden. Die auf diese Weise erfassten, nicht einheitlichen Daten mussten vor der eigentlichen Auswertung zusammengefasst werden. Bei den Diensten sind so 23 Dienstgruppen entstanden, die zum Teil mehrere unterschiedliche Protokolle umfassen. Beispielsweise sind in der Gruppe E-Mail Protokolle, wie POP3, SMTP oder IMAP enthalten. Manche Gruppen umfassen sehr unterschiedliche Anwendungen, unter Druck- und Dateidienste fallen z. B. rsync, AFS oder LPR (Line Printer).

Bei den Fragen nach dem Einsatz von Desktop-Firewalls und Antiviren-Software wurde eigentlich erwartet, dass jeweils die Anzahl der Rechner angegeben wird, auf denen solche Software installiert ist. Leider waren die Antworten hier manchmal zu ungenau oder es wurde statt einer Anzahl das verwendete Produkt genannt. Aus diesem Grund wurde statt einer Anzahl nur noch ein boolscher Wert in die Auswertung übernommen, je nach dem ob eine solche Software eingesetzt wird oder nicht.

	angeschriebene Institute	eingegangene Fragebögen	gewertete Fragebögen
Anzahl	ca. 650	59	56

Tabelle 3.1: Anzahl der Fragebögen

Vor der Auswertung wurden die Fragebögen nach Widersprüchen durchsucht. Häufig aufgetreten sind folgende Widersprüche:

- Es ist gar kein Subnetz vorhanden.
- Eine DMZ ist vorhanden, aber nur ein Subnetz.
- Es wird ein DHCP-Server im Internet genutzt, aber kein DNS-Server.

Der Grund für solche Widersprüche ist dabei weniger darin zusehen, dass ein Fragebogen mutwillig falsch oder nicht gewissenhaft ausgefüllt wurde. Vielmehr muss davon ausgegangen werden, dass es bei manchen Ausfüllern vielleicht doch Schwierigkeiten mit der Terminologie gegeben hat, auch wenn nur die Netzverantwortlichen der Institute angeschrieben wurden. Um die Hürde nicht zu hoch zu legen, wurde ein Fragebogen erst bei zwei entdeckten Widersprüchen aus der Auswertung herausgenommen. Schließlich kann eine Frage auch mal versehentlich falsch ausgefüllt oder missverstanden werden.

Dass mehrfach eingegangene Fragebögen nur einmal gewertet wurden, versteht sich von selbst. Interessant sind jedoch zwei Fragebögen, die zwar vom selben Institut gekommen sind, aber von unterschiedlichen Personen bearbeitet wurden. Dabei sind sich beide nicht in allen Punkten einig. Beispielsweise wurde von ihnen unterschiedlich beurteilt, ob eine Einschränkung bei den nutzbaren Diensten akzeptabel sei oder nicht. Auch bei der Bereitschaft die Serverkapazitäten des LRZ verstärkt zu nutzen, gingen die Ansichten auseinander. Hier wurde ein allgemeines Problem dieser Umfrage deutlich. Die Antworten spiegelten nicht die Meinung des gesamten Instituts wider, sondern nur die des angeschriebenen Netzverantwortlichen. Dabei darf spekuliert werden, ob der Netzverantwortliche auf Grund zunehmenden “Leidensdruck” zu weitreichenderen Einschränkungen bei der Nutzung des Internet bereit ist als die übrigen Mitarbeiter des Instituts. Auf der anderen Seite ist zu hoffen, dass die Meinung des Netzverantwortlichen bei Fragen, die das Institutsnetz betreffen, ein gewisses Gewicht hat. Von den beiden genannten Fragebögen wurde übrigens der gewertet, der mehr Details zu den genutzten Diensten, Betriebssystemen und Firewalls enthielt.

3.2.2 Beteiligung an der Umfrage

Nach dem Ablegen des Fragebogens auf dem Server des LRZ wurden ca. 650 Institute angeschrieben. Auf Antworten wurde einen Monat gewartet. In diesem Zeitraum sind 59 Fragebögen (ohne doppelte) eingegangen, von denen 3 auf Grund zu vieler Wiedersprüche nicht gewertet wurden (siehe Tabelle 3.1).

Die verbleibenden 56 Fragebögen machen rund neun Prozent der angeschriebenen Institute aus. Diese Institute repräsentieren jedoch rund 11.700 am MWN angeschlossene Rechner. Bei geschätzten insgesamt 40.000 Rechnern [ApLä 02] sind dies 29 Prozent. Der große Anteil lässt sich dadurch erklären, dass fünf große (mehr als 316 Rechner) und einige mittelgroße (101 – 316 Rechner) Institute an der Umfrage teilgenommen haben (siehe Tabelle 3.4). Bei den Instituten, die nicht auf das Anschreiben reagiert haben, dürfte es sich folglich vor allem um mittlere und kleinere Institute (bis zu

	LMU	TU	FH	andere
Fragebögen nach Einrichtung	13	32	4	7

Tabelle 3.2: Beteiligung an der Umfrage nach Hochschulen und anderen Einrichtungen

	Ingenieur- u. Naturwissenschafften	andere	nicht zuordenbar
Fragebögen nach Fachgebiet	43	10	3

Tabelle 3.3: Beteiligung an der Umfrage nach Fachgebiet

100 Rechner) handeln. Dies lässt sich vielleicht dadurch erklären, dass es bei einem kleinen Institut schwieriger ist einen Netzverantwortlichen zu finden, der über gute Kenntnisse im Bereich Rechner- und Netzwerksicherheit, sowie über ein entsprechendes Problembewusstsein verfügt. Deshalb sollten gerade diese Institute durch den zukünftige Firewall-Dienst profitieren.

An der Umfrage haben sich, wie Tabelle 3.2 zeigt, vor allem Institute der Technischen Universität beteiligt. Dies kann u. U. dadurch erklärt werden, dass bei diesen Instituten eine größere Affinität zu technischen Themen besteht. Dieser Verdacht wird bekräftigt, wenn man sich anschaut, aus welchen Fachgebieten die teilnehmenden Institute stammen. Rund drei Viertel der Institute, die den Fragebogen beantwortet haben, stammen aus dem Bereich der Ingenieur- und Naturwissenschaften (siehe Tabelle 3.3).

3.2.3 Größe der Institutsnetze

Für die Bestimmung der Größe eines Institutsnetzes standen drei Werte zur Auswahl:

- Anzahl der verwendeten Rechner (mobile und feste Rechner)
- Anzahl der zur Verfügung stehenden öffentlichen IP-Adressen
- Anzahl der Subnetze

Am besten dafür geeignet ist die Anzahl der Rechner. Sie ergibt sich aus der Summe der fest angeschlossenen und der mobilen Rechner. Es wurden vier Größenkategorien gebildet (siehe Tabelle 3.4), die Intervallgrenzen wurden logarithmisch gewählt ($10^{1,5}$, 10^2, $10^{2,5}$).

Die Anzahl der zur Verfügung stehenden öffentlichen IP-Adressen ergibt sich aus der Frage nach dem IP-Adressbereich, den das Institut vom LRZ erhalten hat. Wie aus Tabelle 3.5 ersichtlich ist, besteht zwischen der Anzahl der Rechner und der Anzahl der zur Verfügung stehenden öffentlichen IP-Adressen eine Korrelation. Dabei zeigt sich, dass die Institute, die eine größere Anzahl Rechner besitzen, in der Regel auch mehr öffentliche IP-Adressen haben. Trotzdem ist die Wahl der Rechneranzahl als Größenkriterium besser geeignet. Die Zahl der IP-Adressen liegt, wie die Auswertung zeigt, immer deutlich über der Rechneranzahl. Zusätzlich kann das Bild durch die Verwendung von privaten IP-Adressen und NAT-Gateways verfälscht werden.

Die Anzahl der Subnetze ist zur Größenunterscheidung nicht geeignet, da zwei Drittel der Institute scheinbar nur ein oder zwei Subnetze haben. Die Frage nach der Anzahl der Subnetze ist oft auch falsch beantwortet worden. Wie schon erwähnt, war ein häufiger Fehler beim Ausfüllen des Fragebogens, dass zwar nur ein Subnetz angegeben wurde, trotzdem aber eine DMZ vorhanden sein sollte.

Größe des Instiutsnetzes	Fragebögen
insgesamt	56
1 - 32 Rechner	12
33 - 100 Rechner	22
101 - 316 Rechner	17
mehr als 316 Rechner	5

Tabelle 3.4: Größe der Institutsnetze nach Anzahl der Rechner

Anzahl öffentlicher IP-Adressen	1 - 128	129 - 256	257 - 512	¿512
insgesamt	16	23	10	7
1 - 32 Rechner	7	5	0	0
33 - 100 Rechner	7	12	1	2
101 - 316 Rechner	1	5	8	3
mehr als 316 Rechner	1	1	1	2

Tabelle 3.5: Zusammenhang zwischen der Anzahl der Rechner und der Anzahl öffentlicher IP-Adressen

3.2.4 Eingesetzte Betriebssysteme

Neben der Unterscheidung der Institute nach ihrer Größe war außerdem vorgesehen, eine Unterscheidung nach den eingesetzten Betriebssystemen vorzunehmen. Dies konnte nicht durchgeführt werden, da in fast allen Instituten ein Mix aus unterschiedlichen Betriebssystemen eingesetzt wird. Nur vier befragte Institute setzen ausschließlich Windows NT/2000/XP ein. Jedoch die Hälfte der Institute nutzen gleichzeitig Windows 95/98/Me, Windows NT/2000/XP und Linux in ihrem Netz. Tabelle 3.6 gibt einen Überblick über die eigensetzten Betriebssysteme. Dabei wird keine Aussage darüber getroffen, auf wievielen Rechnern ein Betriebssystem installiert ist, sondern nur, ob ein Betriebssystem überhaupt im Institut eingesetzt wird.

3.2.5 Sicherheitsaspekte

Bei der Frage nach der Anzahl der am Institutsnetz angeschlossenen Rechner wurde unterschieden zwischen festen (Desktop, Server etc.) und mobilen (Notebooks etc.) Rechnern. Der Anteil der mobilen Rechner an der Gesamtzahl beträgt dabei zwölf Prozent. Bei den kleinen Instituten mit bis zu 32

Betriebssystem	Nennungen
Win 95/98/Me	38
Win NT/2000/XP	52
Linux	42
Solaris	11
andere Unixe	20
MacOS	12
andere	9

Tabelle 3.6: Eingesetzte Betriebssysteme

Anteil mobiler Rechner	%
insgesamt	12
1 - 32 Rechner	16
33 - 100 Rechner	11
101 - 316 Rechner	11
mehr als 316 Rechner	3

Tabelle 3.7: Anteil mobiler Rechner (Laptops) an der Gesamtzahl der Rechner im Durchschnitt der Institute

	ja	nein	k. Ang.
Modem- oder ISDN-Zugang	9 (16%)	46 (82%)	1 (2%)
frei zugängliche Netzwerkanschlüsse	30 (54%)	26 (46%)	0

Tabelle 3.8: Anzahl der Institute mit Modems und frei zugängliche Netzwerkanschlüssen

Rechnern liegt er sogar bei 16 Prozent (siehe Tabelle 3.7).

Das Firewall-Konzept soll den Übergang vom MWN bzw. Internet zum Institutsnetz schützen. Dabei ist eine einzige, zentrale Übergangsstelle im Netz zu schaffen, die von einer Firewall überwacht werden kann. Andere Zugänge zum Institutsnetz darf es nicht geben. Modems oder ISDN-Adapter stellen in diesem Zusammenhang ein großes Problem dar, da sie als "Nebeneingänge" missbraucht werden können. Gerade wenn eine Firewall die Nutzung von Diensten zukünftig beschränkt, muss davon ausgegangen werden, dass die Modems von "schwarzen Schafen" als Ersatzverbindungen genutzt werden. Dies würde das Firewallkonzept ad absurdum führen. Seit der Verbreitung von Dialern besteht zusätzlich die Gefahr, dass auch ohne Wissen der Benutzer ein zusätzlicher Zugang zum Institutsnetz geschaffen wird. Ein nicht unerheblicher Teil der Institute (16 Prozent) setzen Modems oder ISDN-Adapter als Zugangsmöglichkeit ein (siehe Tabelle 3.8). Es darf angezweifelt werden, ob diese Anzahl tatsächlich notwendig ist.

Eine Firewall kann nur vor Angriffen von außen schützen. Da viele Institute öffentlich zugänglich sind, muss davon ausgegangen werden, dass nicht kontrollierbare Netzwerkanschlüsse vorhanden sind, die Angriffe von innen ermöglichen. Dies wird durch die Umfrage bestätigt. Mehr als die Hälfte der Institute geben in der Umfrage an, dass bei ihnen frei zugängliche Netzwerkanschlüsse vorhanden sind (siehe Tabelle 3.8).

3.2.6 Maßnahmen der Institute zum Schutz des Institutsnetzes

Die Auswertung hat gezeigt, dass in vielen Instituten bereits verschiedene Schutzmaßnahmen ergriffen wurden. Dies nährt die Hoffnung, dass ein gewisses Sicherheitsbewusstsein bei den Verantwortlichen in den Instituten vorhanden ist. Eine erste Maßnahme zum Schutz der Institute ist die Verwendung von privaten IP-Adressen zusammen mit einem NAT-Gateway. Nach außen ist nur der NAT-Gateway sichtbar, die Struktur des abgeschirmten Netzes bleibt verborgen. Bereits 41 Prozent verwenden private IP-Adressen, bei den kleinen Instituten besteht hier allerdings noch Nachholbedarf (siehe Tabelle 3.9). Allerdings gibt die Umfrage keinen Aufschluss darüber, in welchem Umfang private IP-Adressen verwendet werden.

Dienste, die von außen erreichbar sein müssen, sollten auf eigenen Servern in einem extra eingerichteten Subnetz untergebracht werden. Etwa ein Drittel der befragten Institute hat bereits eine solche

Verwendung priv. IP-Adressen	ja	nein	k. Ang.
insgesamt	23 (41%)	33 (59%)	0
1 - 32 Rechner	3 (25%)	9 (75%)	0
33 - 100 Rechner	8 (36%)	14 (64%)	0
101 - 316 Rechner	7 (41%)	10 (59%)	0
mehr als 316 Rechner	5 (100%)	0	0

Tabelle 3.9: Anzahl der Institute, die private IP-Adressen verwenden (aufgeschlüsselt nach der Größe der Institutsnetze)

DMZ vorhanden	ja	nein	k. Ang.
insgesamt	16 (32%)	33 (66%)	1 (2%)
1 - 32 Rechner	0	9 (100%)	0
33 - 100 Rechner	6 (32%)	12 (63%)	1 (5%)
101 - 316 Rechner	6 (35%)	11 (65%)	0
mehr als 316 Rechner	4 (80%)	1 (20%)	0

Tabelle 3.10: Anzahl der Institute, die eine demilitarisierte Zone eingerichtet haben (aufgeschlüsselt nach der Größe der Institutsnetze). Berücksichtigt sind nur die 50 Institute, die aus dem Internet zugängliche Server betreiben.

demilitarisierte Zone (DMZ) eingerichtet (siehe Tabelle 3.10). Dabei wurden nur Institute berücksichtigt, die nach eigenen Angaben aus dem Internet zugängliche Server betreiben. Ein großer Unterschied zeigt sich hinsichtlich der Größe der Institute. Von den kleinen Instituten (bis zu 32 Rechnern) hat kein einziges befragtes Institut eine DMZ, bei den großen (ab 316 Rechner) sind es 80 Prozent.

Der Einsatz von Antivirensoftware ist weit verbreitet. Bis auf drei Institute, gaben alle an, dass sie entsprechende Produkte einsetzen. Desktopfirewalls sind neuere Produkte, deshalb auch noch nicht so bekannt (elf Prozent der befragten Institute machten zu dieser Frage keine Angaben) und nicht so weit verbreitet. Von den befragten Instituten setzen aber immerhin schon 43 Prozent solche Software ein (siehe Tabelle 3.11). Leider konnte nicht ausgewertet werden, auf wieviel Prozent der Institutsrechner Antivirenprogramme bzw. Desktopfirewalls tatsächlich installiert sind. Auch gibt die Umfrage keinen Aufschluss darüber, wie regelmäßig Updates vorgenommen werden.

Besonders interessant war die Frage nach dem Einsatz eigener Firewalls. Etwa 40 Prozent der Institute, die an der Umfrage teilgenommen haben, gaben an, dass sie eine Firewall betreiben. Wie schon bei anderen Fragen zeigte sich auch hier, dass die kleinen Institute hinter dem allgemeinen Durchschnitt zurückliegen (siehe Tabelle 3.12). Als Firewalls werden vor allem Lösungen auf der Basis von Linux eingesetzt. Aus der Tabelle 3.13 kann außerdem herausgelesen werden, dass meist eigene Lösungen an Stelle von fertigen Produkten verwendet werden. Dies setzt einen entsprechend engagierten und kenntnisreichen Mitarbeiter voraus. Kleine Institute sind in dieser Hinsicht offensichtlich benachtei-

	ja	nein	k. Ang.
Einsatz von Antivirensoftware	53 (95%)	1 (2%)	2 (4%)
Einsatz von Dektopfirewalls	24 (43%)	26 (46%)	6 (11%)

Tabelle 3.11: Anzahl der Institute, die Antivirensoftware und Desktopfirewalls einsetzen

Firewall vorhanden	ja	nein
insgesamt	23 (41%)	33 (59%)
1 - 32 Rechner	4 (33%)	8 (67%)
33 - 100 Rechner	6 (27%)	16 (73%)
101 - 316 Rechner	9 (53%)	8 (47%)
mehr als 316 Rechner	4 (80%)	1 (20%)

Tabelle 3.12: Anzahl der Institute, die eine Firewall betreiben (aufgeschlüsselt nach der Größe der Institutsnetze)

Firewallart	Nennungen
Filter der Cisco-Router	1
eigene Lösung auf Basis von FreeBSD	1
eigene Lösung auf Basis von Linux	15
spezielle Linux-Firewall-Distribution	3
andere Firewallprodukte	4

Tabelle 3.13: Eingesetzte Firewallarten in den Instituten

ligt.

3.2.7 Genutzte und angebotene Dienste

Für ein kundennahes Firewallkonzept ist es wichtig herauszubekommen, welche Dienste von den Instituten genutzt werden und welche Dienste sie selber für den Zugriff von außen anbieten. Dabei wurde jeweils unterschieden zwischen Internet und MWN. Schließlich wurde noch gefragt, welche intern genutzten Dienste nicht von außen erreichbar sein sollen.

Bei den genutzten Diensten führen erwartungsgemäß die Klassiker E-Mail, FTP und WWW. Von sehr vielen werden außerdem Proxies im MWN genutzt – gemeint sind Proxies des LRZ und anderer Institute. Es werden auch Proxies im Internet genutzt, wobei nicht klar ist, welcher Art diese Proxies sind.

Etwas erschreckend ist der hohe Anteil von Telnet. Immerhin noch ein Drittel der befragten Institute nutzt nach eignen Angaben Telnet, um auf Server im Internet zuzugreifen. Auch der Zugriff per Telnet auf das Institutsnetz ist bei manchen noch möglich. Allerdings hat SSH hier einen deutlich größeren Anteil.

Die neueren Dienste des Internet aus den Bereichen Messaging, Multimedia, VPN und Filesharing spielen hingegen fast keine Rolle. Unter den Begriff Multimedia-Dienste wurden Nennungen wie Videokonferenz und Streaming zusammengefasst. Nur wenige Institute gaben an, welche Videokonferenz-Software sie einsetzen. Genannt wurden Netmeeting und Mbone. Für VPN werden IPsec, IPv6 (über IPv4) und PPTP eingesetzt. Der Bereich Bereich Datei- und Druckdienste umfasst die vom LRZ angebotenen Dienste AFS und TSM. Weiterhin wurden Dienste wie LPR oder rsync genannt.

Von den in Tabelle 3.14 aufgeführten 23 Dienstgruppen, werden 13 häufiger genutzt. Unter häufiger genutzten Dienstgruppen werden solche verstanden, die mindestens in einer Spalte der Tabelle auf über zehn Prozent kommen. Beschränkt man die Analyse auf die kleinen Institute (siehe Tabelle 3.15),

Dienst/ Anwendung	Nutzung im Internet	Nutzung im MWN	Angebot für das Internet	Angebot für das MWN	kein Zugriff von außen
DHCP	2 (4%)	17 (30%)	0	0	0
DNS	0	43 (77%)	16 (29%)	22 (39%)	14 (25%)
Kerberos	0	0	0	1 (2%)	0
LDAP	0	0	0	1 (2%)	0
Radius	0	1 (2%)	0	1 (2%)	0
RPC (NIS, NFS)	0	1 (2%)	0	1 (2%)	31 (55%)
Time (NTP)	15 (27%)	32 (57%)	0	0	0
E-Mail (SMTP etc.)	46 (82%)	51 (91%)	39 (70%)	41 (73%)	0
FTP	40 (71%)	51 (91%)	27 (48%)	31 (55%)	10 (18%)
WWW (HTTP, HTTPS)	49 (88%)	50 (89%)	44 (79%)	45 (80%)	4 (7%)
Usenet	18 (32%)	34 (61%)	2 (4%)	4 (7%)	0
Telnet	19 (34%)	28 (50%)	6 (11%)	10 (18%)	30 (54%)
SSH	29 (52%)	43 (77%)	34 (61%)	37 (66%)	3 (5%)
Filesharing	1 (2%)	0	1 (2%)	0	0
Messaging (ICQ, IRC)	1 (2%)	2 (4%)	0	0	0
Multimedia (Mbone etc.)	4 (7%)	2 (4%)	3 (5%)	2 (4%)	0
Datei-/Druckdienste	1 (2%)	6 (11%)	4 (7%)	31 (55%)	0
SMB/CIFS	0	1 (2%)	0	2 (4%)	29 (52%)
Proxy-Dienste	12 (21%)	47 (84%)	0	0	0
VPN (PPTP, IPsec etc.)	1 (2%)	1 (2%)	4 (7%)	2 (4%)	1 (2%)
Appeltalk over IP	0	1 (2%)	0	0	0
RDP	0	0	0	1 (2%)	0
andere Anwendungen	4 (7%)	5 (9%)	2 (4%)	4 (7%)	1 (2%)

Tabelle 3.14: Häufigkeit genutzter und angebotener Dienste (Abkürzungen siehe Abkürzungsverzeichnis)

so stellt man fest, dass von ihnen – bis auf eine Ausnahme – nur diese 13 Dienstgruppen genutzt werden. Bei der Ausnahme handelt es sich um ein Institut, das per VPN von außen auf das eigene Netz zugreifen möchte.

3.2.8 Akzeptanz zukünftiger Einschränkungen

Etwas überraschend ist die Bereitschaft vieler Institute, Einschränkungen bei der Nutzung von Internetdiensten zu akzeptieren. Mehr als die Hälfte der Institute wäre laut Umfrage damit einverstanden, wenn der Zugriff auf das Internet zukünftig auf bestimmte Dienste beschränkt wäre. Dabei ist festzustellen, dass vor allem kleine Institute (mit bis zu 32 Rechner) mit dieser Einschränkung leben könnten, während mit zunehmender Größe des Instituts diese Bereitschaft sinkt (siehe Tabelle 3.17). Ähnlich groß ist die Zustimmung zu einer eventuellen Filterung der URLs (siehe Tabelle 3.16). Hier gibt es jedoch keine signifikanten Unterschiede hinsichtlich der Größe der Institute. Ablehnender wird das Content-Filtering bewertet. Nur knapp ein Viertel der befragten Institute würde eine solche Beschränkung akzeptieren.

Dienst/ Anwendung	Nutzung im Internet	Nutzung im MWN	Angebot für das Internet	Angebot für das MWN	kein Zugriff von außen
DHCP		3 (25%)			
DNS		9 (75%)			1 (8%)
RPC (NIS, NFS)					1 (8%)
Time (NTP)	3 (25%)	4 (33%)			
E-Mail (SMTP etc.)	10 (83%)	10 (83%)	5 (42%)	5 (42%)	
FTP	4 (33%)	11 (92%)	3 (25%)	3 (25%)	
WWW (HTTP, HTTPS)	10 (83%)	9 (75)	7 (58%)	6 (50%)	1 (8%)
Usenet	2 (17%)	6 (50%)			
Telnet	1 (8%)	8 (67%)	2 (17%)	1 (8%)	
SSH	1 (8%)	9 (75%)	2 (17%)	3 (25%)	
Datei-/Druckdienste		1 (8%)	1 (8%)	3 (25%)	
SMB/CIFS					1 (8%)
Proxy	2 (17%)	9 (75%)			
VPN (PPTP, IPsec etc.)			1 (8%)	1 (8%)	

Tabelle 3.15: Häufigkeit genutzter und angebotener Dienste bei kleinen Instituten (bis zu 32 Rechner)

	ja	nein	k. Ang.
Beschränkung der Dienste	31 (55%)	20 (36%)	5 (9%)
Content-Filtering	13 (23%)	42 (75%)	1 (2%)
URL-Filtering	30 (54%)	24 (43%)	2 (4%)

Tabelle 3.16: Bereitschaft der Institute Einschränkungen bei den Diensten hinzunehmen

Beschränkung der Dienste	ja	nein	k. Ang.
insgesamt	31 (55%)	20 (36%)	5 (9%)
1 - 32 Rechner	8 (67%)	2 (17%)	2 (17%)
33 - 100 Rechner	12 (55%)	8 (36%)	2 (9%)
101 - 316 Rechner	9 (53%)	7 (41%)	2 (6%)
mehr als 316 Rechner	2 (40%)	3 (60%)	0

Tabelle 3.17: Bereitschaft der Institute den Zugriff auf bestimmte Dienste zu beschränken (aufgeschlüsselt nach der Größe der Institutsnetze)

	ja	nein	k. Ang.
kein Zugriff aus dem Internet	15 (27%)	39 (70%)	2 (4%)
kein Zugriff aus dem MWN	11 (20%)	44 (79%)	1 (2%)
Remotezugang notwendig	50 (89%)	5 (9%)	1 (2%)

Tabelle 3.18: Bereitschaft der Institute den Zugriff auf das Institutsnetz von außen zu unterbinden; Notwendigkeit eines Remotezugangs

kein Zugriff aus dem Internet	ja	nein	k. Ang.
insgesamt	15 (27%)	39 (70%)	2 (4%)
1 - 32 Rechner	5 (42%)	6 (50%)	1 (8%)
33 - 100 Rechner	7 (32 %)	14 (64%)	1 (5%)
101 - 316 Rechner	3 (18%)	14 (82%)	0
mehr als 316 Rechner	0	5 (100%)	0

Tabelle 3.19: Bereitschaft der Institute den Zugriff aus dem Internet auf das Institutsnetz zu unterbinden (aufgeschlüsselt nach der Größe der Institutsnetze)

Etliche Institute kämen offensichtlich auch damit zu Recht, wenn zukünftig kein Zugriff von außen auf das Institutsnetz mehr möglich ist (siehe Tabelle 3.18). Trotz dieser recht drastischen Maßnahme, würden laut Umfrage bei Zugriffen aus dem Internet immerhin 27 Prozent, bei Zugriffen aus dem MWN 20 Prozent einen solchen Schritt hinnehmen. Dabei gilt weitestgehend, dass die Institute die auf Zugriffe aus dem MWN verzichten können, auch keine Zugriffe aus dem Internet benötigen. Diese Teilmengenbeziehung wird nur durch zwei Institute gestört: Ein Institut machte unvollständige Angeben. Das andere benötigt eine Möglichkeit ein VPN mit einem Institut in den USA zu bilden, ist aber ansonsten auf keine Zugriffe angewiesen. Ein Großteil der Institute besteht ohnehin darauf, dass ein Remotezugang möglich ist, um beispielsweise zu Hause Daten im Institut nutzen zu können. Auch hier zeigt sich, dass kleine Institute eher bereit sind Einschränkungen zu akzeptieren. 42 Prozent der befragten Institute, die bis zu 32 Rechner haben, würden auf die Möglichkeit verzichten können, dass aus dem Internet auf ihr Netz zugegriffen werden kann. Bei den großen Instituten sinkt dieser Wert deutlich (siehe Tabelle 3.19).

Etwas weniger drastisch ist die Maßnahme die Dienste, die von außen erreichbar sein müssen, in einer demilitarisierte Zone zusammenzufassen. Drei Viertel der Befragten wären mit einer damit verbundenen Umstrukturierung des eigenen Netzes einverstanden (siehe Tabelle 3.20). Bei Diensten, die nur aus dem MWN erreicht werden müssen, liegt dieser Wert bei 66 Prozent und damit etwas niedriger. Anzumerken ist, dass alle Institute, die bereit sind eine DMZ für das MWN einzurichten, auch eine DMZ für das Internet einrichten würden.

In vielen Fällen kann auch eine weitgehende Verwendung von privaten statt öffentlichen IP-Adressen eine Verbesserung der Sicherheit bringen. Es wurde zunächst befürchtet, dass der damit verbundene Aufwand in vielen Instituten zu groß ist und deshalb nicht akzeptiert wird. Diese Befürchtung scheint jedoch unbegründet, da 80 Prozent der befragten Netzverantwortlichen eine solche Veränderung bei der Adressierung für möglich halten.

Für viele Dienste, die von außen erreichbar sein sollen, gibt es außerdem die Möglichkeit sie auf Servern des LRZ zu betreiben. Erfreulicherweise wissen 93 Prozent der Befragten von dieser Möglichkeit. Im Zusammenhang mit einer Firewall-Lösung wären etwa die Hälfte der Institute laut Umfrage bereit, diese Möglichkeit verstärkt zu nutzen (siehe Tabelle 3.21). Auch hier zeichnet sich ab, dass

	ja	nein	k. Ang.
neue Adressierung	45 (80%)	10 (18%)	1 (2%)
DMZ für Zugriff aus Internet	42 (75%)	13 (23%)	1 (2%)
DMZ für Zugriff aus MWN	37 (66%)	17 (30%)	2 (4%)

Tabelle 3.20: Bereitschaft der Institute ihre Netze umzustrukturieren und DMZ einzurichten

	ja	nein	k. Ang.
Wissen um Auslagerungsmglkt.	52 (93%)	3 (5%)	1 (2%)
Bereitschaft zum Auslagern	31 (55%)	23 (41%)	2 (4%)

Tabelle 3.21: Möglichkeit bestimmte Dienste, die von außen erreichbar sein sollen, auf Server des LRZ auszulagern

kleine Institute diese Möglichkeit eher nutzen würden als große (siehe Tabelle 3.22).

3.3 Diensteprofile

3.3.1 Herausarbeitung der Diensteprofile

Im Abschnitt 3.2.7 wurden die Antworten auf die Fragen nach den im Internet und MWN genutzten und angebotenen Diensten ausgewertet. Dabei hat sich herausgestellt, dass 13 Dienstgruppen häufiger – sprich vom mindestens zehn Prozent der befragten Institute – genannt wurden. Da das LRZ keine maßgeschneiderten, sondern nur standardisierte Firewall-Lösungen anbieten kann, ist es sinnvoll den Schwerpunkt auf diese Dienste zu legen und sie in die Diensteprofile aufzunehmen.

Zusätzlich müssen in den Profilen Dienste berücksichtigt werden, die zwar seltener genannt wurden, aber für das MWN eine wichtige Rolle spielen:

- Über Radius wird die Authentifizierung an den Wähl- und VPN-Zugängen abgewickelt. Zur Zeit gibt es etwa 70 Radius-Server.
- Für den Backup- und Archiv-Dienst wird Tivoli Storage Management (TSM) eingesetzt.
- Der Network-Attached-Storage-Dienst basiert auf AFS.
- Für die Bildung von VPNs muss die Nutzung von IPsec und PPTP ermöglicht werden.

Dadurch ergeben sich folgende Diensteprofile:

Bereitschaft zum Auslagern	ja	nein	k. Ang.
insgesamt	31 (55%)	23 (41%)	2 (4%)
1 - 32 Rechner	10 (83%)	2 (17%)	0
33 - 100 Rechner	11 (50%)	9 (41%)	2 (9%)
101 - 316 Rechner	9 (53%)	8 (47%)	0
mehr als 316 Rechner	1 (20%)	4 (80%)	0

Tabelle 3.22: Bereitschaft der Institute bestimmte Dienste auf Server des LRZ auszulagern (aufgeschlüsselt nach der Größe der Institutsnetze)

passende Institute	Profil 1	Profil 2	Profil 3	Profil 4	Profil 5
insgesamt	45 (80%)	46 (82%)	46 (82%)	45 (80%)	48 (86%)
1 - 32 Rechner	12 (100%)	12 (100%)	11 (92%)	12 (100%)	11 (92%)
33 - 100 Rechner	20 (91%)	18 (82%)	19 (86%)	17 (77%)	19 (86%)
101 - 316 Rechner	11 (65%)	13 (76%)	13 (76%)	14 (82%)	15 (88%)
mehr als 316 Rechner	2 (40%)	3 (60%)	3 (60%)	2 (40%)	3 (60%)

Tabelle 3.23: Anzahl der Institute, die zu den Diensteprofilen passen.

Profil 1 umfasst Dienste, die im Internet genutzt werden. Im einzelnen sind dies E-Mail (POP3, SMTP, IMAP), FTP, Time (NTP), Proxy-Dienste, Telnet, SSH, Usenet und WWW (HTTP, HTTPS). Bei caching Proxies wie für WWW oder FTP muss es ausreichen, den Proxy-Verbund des MWN zu nutzen. Andere Arten wie Proxies zur Anonymisierung arbeiten in der Regel transparent für das jeweilige Protokoll. Eine besondere Berücksichtigung von Proxies (beispielsweise in Form freigegebener Ports) scheint deshalb nicht notwendig.

Profil 2 beinhaltet Dienste, die im MWN genutzt werden. Neben den Diensten aus Profil 1 sind dies DHCP, DNS und Dateidienste. Zu letzteren zählen AFS und TSM. Im Gegensatz zu Profil 1 müssen für den Zugriff auf die Proxies im MWN verschiedene Ports freigegeben werden (z.B. proxy.lrz-muenchen.de:8080).

Profil 3 enthält Dienste, die vom Institut für den Zugriff aus dem Internet angeboten werden. Im einzelnen sind dies E-Mail (POP3, SMTP, IMAP), FTP, Telnet, SSH, WWW (HTTP, HTTPS), DNS und VPN (IPsec, PPTP).

Profil 4 sind Dienste die für das MWN angeboten werden. Zu den in Profil 3 genannten Diensten kommen hier noch Datei- und Druckdienste sowie Radius hinzu.

Profil 5 umfasst die Dienste, die innerhalb des Institutsnetzes notwendig sind, auf die aber von außen nicht zugegriffen werden darf. Dies sind FTP, Telnet, DNS, SMB/CIFS und RPC-Dienste (NIS, NFS). Da FTP, Telnet und DNS auch in den Profilen 3 und 4 genannt wurden, kann eine entsprechende Filterung nur für das interne Netz des Instituts, nicht aber für eine eventuelle DMZ vorgenommen werden.

3.3.2 Eignung der Diensteprofile

Die Diensteprofile wurden so erstellt, dass sie alle häufig genannten und einige für das MWN wichtigen Dienste umfassen. Im folgenden wird nun überprüft, ob diese Profilbildung den Bedürfnissen der Institute tatsächlich gerecht wird. Dabei zeigt Tabelle 3.23, dass bei allen Kommunikationsbeziehungen für mindestens 80 Prozent der befragten Institute die Berücksichtigung dieser Dienste ausreichen würden. Die anderen Institute benutzen Dienste, die zu selten genannt wurden oder für das MWN zu wenig Bedeutung haben, als dass sie in einer einheitlichen Lösung berücksichtigt werden könnten. Auffällig ist, dass vor allem die kleinen Institute gut mit dieser Profilbildung zurecht kommen würden, bei den Profilen 1, 2 und 4 sind es sogar alle der befragten, kleinen Institute. Nicht verwunderlich ist, dass mit zunehmender Größe der Institute die Passgenauigkeit abnimmt. In Tabelle 3.24 werden die verschiedenen Profile kombiniert. Selbst wenn man alle gleichzeitig nimmt, passen immer noch mehr als die Hälfte der Institute zu den Diensteprofilen.

Kombinationen	1 - 5	1 und 2	3 und 4
insgesamt	31 (55%)	40 (71%)	41 (73%)
1 - 32 Rechner	10 (83%)	12 (100%)	11 (92%)
33 - 100 Rechner	13 (59%)	18 (82%)	16 (73%)
101 - 316 Rechner	8 (47%)	9 (53%)	12 (71%)
mehr als 316 Rechner	0	1 (20%)	2 (40%)

Tabelle 3.24: Anzahl der Institute, die zu Kombinationen der Diensteprofile passen.

Beschränkung der Dienste	ja	nein	k. Ang.
insgesamt	21 (38%)	15 (27%)	4 (7%)
1 - 32 Rechner	8 (67%)	2 (17%)	2 (17%)
33 - 100 Rechner	9 (41%)	7 (32%)	2 (9%)
101 - 316 Rechner	4 (24%)	5 (29%)	0
mehr als 316 Rechner	0	1 (20%)	0

Tabelle 3.25: Antwort der Institute, die zu den Diensteprofilen 1 und 2 passen, auf die Frage nach Einschränkung der nutzbaren Dienste. Der prozentuale Anteil bezieht sich auf die Gesamtzahl der befragten Institute.

Es besteht die Absicht, dass sich der zukünftige Firewall-Dienst des LRZ an den herausgearbeiteten Diensteprofilen ausrichtet. Es stellt sich die Frage, wie sich die Profile auf die in Abschnitt 3.2.8 betrachteten Einschränkungen auswirken. Bei der Nutzung von Diensten ist bei vielen Instituten die Bereitschaft vorhanden gewesen, Einschränkungen auf bestimmte Dienste zu akzeptieren. Welche Dienste dies sein sollen, ist nicht gesagt worden. Jetzt sollen konkret die Dienste aus den Profilen 1 und 2 genommen werden. Tabelle 3.25 zeigt, dass 38 Prozent der befragten Institute eine Beschränkung der Dienste akzeptieren und zugleich zu den genannten Profilen passen. Dieser Anteil rechtfertigt es, dass eine Nutzungsbeschränkung auf die in den Profilen 1 und 2 aufgeführten Dienste im zukünftigen Firewall-Angebot als Option enthalten sein sollte.

Bezüglich des Angebots von Diensten ist bei vielen Instituten die Bereitschaft vorhanden gewesen, eine DMZ für die eigenen Server einzurichten oder das Dienstangebot auf fremde Server auszulagern. Es ist nichts darüber ausgesagt worden, um welche Dienste es sich dabei handelt. Jetzt sollen dafür die Dienste aus den Profilen 3 und 4 genommen werden. Tabelle 3.26 zeigt, dass 54 Prozent der befragten Institute bereit sind eine DMZ einzurichten und gleichzeitig zu den genannten Diensteprofilen passen. Aus Tabelle 3.27 ist zu entnehmen, dass 43 Prozent der befragten Institute eine Auslagerung ihrer Dienste vornehmen wollen und gleichzeitig zu den genannten Profilen passen. Auf Grund dieser Ergebnisse ist es sinnvoll, das Einrichten einer DMZ bzw. das Auslagern von Diensten als Möglichkeiten im zukünftigen Firewalldienst zu berücksichtigen.

3.4 Kundenprofile bezüglich Zugriffen von außen

Bisher wurden die einzelnen Ergebnisse aus der Umfrage zum zukünftigen Firewall-Dienst des LRZ weitestgehend unabhängig voneinander betrachtet. Im folgenden sollen jetzt mehrere Antworten kombiniert und Gruppen gebildet werden, denen die Institute – die Kunden des LRZ – zugeordnet werden können. Aus der Gruppenbildung sollen Kundenprofile gewonnen werden, die den später noch zu

Einrichtung einer DMZ	ja	nein	k. Ang.
insgesamt	30 (54%)	10 (18%)	1 (2%)
1 - 32 Rechner	10 (83%)	1 (8%)	0
33 - 100 Rechner	10 (45%)	5 (23%)	1 (5%)
101 - 316 Rechner	8 (47%)	4 (24%)	0
mehr als 316 Rechner	2 (40%)	0	0

Tabelle 3.26: Antwort der Institute, die zu den Diensteprofilen 3 und 4 passen, auf die Frage nach der Einrichtung einer DMZ (für Zugriffe aus dem MWN). Der prozentuale Anteil bezieht sich auf die Gesamtzahl der befragten Institute.

Bereitschaft zum Auslagern	ja	nein	k. Ang.
insgesamt	24 (43%)	15 (27%)	2 (4%)
1 - 32 Rechner	9 (75%)	2 (17%)	0
33 - 100 Rechner	8 (36%)	6 (27%)	2 (9%)
101 - 316 Rechner	6 (35%)	6 (35%)	0
mehr als 316 Rechner	1 (20%)	1 (20%)	0

Tabelle 3.27: Antwort der Institute, die zu den Diensteprofilen 3 und 4 passen, auf die Frage nach der Bereichtschaft zur Auslagerung des eigenen Dienstangebots. Der prozentuale Anteil bezieht sich auf die Gesamtzahl der befragten Institute.

entwickelnden Klassen des Firewall-Dienstes zugeordnet werden sollen. Dabei sind durchaus m:n-Beziehungen möglich – in eine Firewall-Klasse können mehrere Kundenprofile fallen, genauso wie ein Profil auf mehrere Firewall-Klassen passen kann.

Zunächst sollen Profile gebildet werden, die sich auf den Zugriff von außen auf vom Institut angebotene Dienste beziehen. Für die Gruppenbildung wurden die folgenden sechs Fragen herangezogen:

- “Angenommen, der Zugriff aus dem Internet auf das Institutsnetz würde vollständig unterbunden. Dies würde bedeuten, dass kein Rechner Ihres Institutsnetzes aus dem Internet erreichbar wären. Ein Remote-Zugang (z.B. für den Datei-Zugriff) wäre noch möglich. Wäre Ihr Institut mit dieser Maßnahme einverstanden?
- Angenommen, der Zugriff aus dem MWN auf das Institutsnetz würde vollständig unterbunden. Dies würde bedeuten, dass kein Rechner Ihres Institutsnetzes von anderen Instituten aus erreichbar wären. Ein Remote-Zugang (z.B. für den Datei-Zugriff) wäre noch möglich. Wäre Ihr Institut mit dieser Maßnahme einverstanden?
- Angenommen, der Zugriff aus dem Internet auf das Institutsnetz wäre auf ein Subnetz (Demilitarisierte Zone) beschränkt. In diesem könnten alle Server zusammengefasst werden, die aus dem Internet erreichbar sein sollen (z.B. WWW-Server mit öffentlichen Informationen). Wäre Ihr Institut mit dieser Maßnahme einverstanden?
- Angenommen, der Zugriff aus dem MWN auf das Institutsnetz wäre auf ein Subnetz (Demilitarisierte Zone) beschränkt. In diesem könnten alle Server zusammengefasst werden, die aus dem MWN erreichbar sein sollen (z.B. Datei-Server für den Remote-Zugriff). Wäre Ihr Institut mit dieser Maßnahme einverstanden?
- Angenommen, der Firewall-Dienst würde eine Änderung der IP-Adressierung in Ihrem Institutsnetz nötig machen, wäre es in Ihrem Institut möglich, diese Änderungen vorzunehmen?

- Befinden sich die Server-Rechner, die Dienste für das MWN oder das Internet anbieten, in einem eigenen Subnetz?”

Von den ersten vier Fragen sind je zwei nahezu identisch. Sie unterscheiden sich nur darin, ob ein Zugriff auf das Institutsnetz aus dem Internet oder dem MWN erfolgt. Deshalb wird im Folgenden die Gruppenbildung zunächst getrennt für Zugriffe aus dem Internet und dem MWN vorgenommen. In einem weiteren Schritt werden die erhaltenen Gruppen zusammengeführt. Die Gruppenbildung wurde wie folgt vorgenommen:

Gruppe 1 wurden alle Institute zugeordnet, die auf Zugriffe von außen (aus dem Internet bzw. MWN) verzichten können. Dies ist die radikalste Form, um Zugriffe von außen einzuschränken. Für die Zuordnung zu dieser Gruppe waren allein die ersten beiden Fragen maßgeblich. Einschränkend wurde bei beiden Fragen ein Remote-Zugang von außen in Aussicht gestellt. Deshalb ist nicht verwunderlich, dass die Institute, die dieser Gruppe zugeordnet werden können, nahezu alle einen Remote-Zugang fordern.

Gruppe 2 wurden die Institute zugeordnet, die auf einen Zugriff von außen nicht verzichten können (Verneinung der ersten bzw. zweiten Frage), aber bereit sind, eine Demilitarisierte Zone (DMZ) einzurichten (Bejahung der dritten bzw. vierten Frage). Eine solche DMZ enthält alle Server die von außen erreichbar sein sollen, andere Subnetze des Instituts sind von außen nicht erreichbar. Auch der Remote-Zugang ist auf Server in der DMZ beschränkt. Darauf wurde in der Frage durch das Anführen eines Beispiels ausdrücklich hingewiesen. Remote Access, um z. B. auf einen Datei-Server in der DMZ zuzugreifen, ist von mehr als 90 Prozent der dieser Gruppe zuordenbaren Institute erwünscht. Alle Institute, die dieser Gruppe zugeordnet wurden, mussten außerdem einer Änderung der IP-Adressierung zustimmen oder bereits eine DMZ eingerichtet haben. Inwieweit Institute mit bereits eingerichteter DMZ und eventuell auch eigener Firewall bereit sind, auf den zukünftigen Firewall-Dienst des LRZ umzusteigen, wurde durch die Umfrage nicht untersucht. An dieser Stelle geht es deshalb nur darum Institutsprofile herauszuarbeiten, damit der Firewall-Dienst möglichst gut an die Bedürfnisse der Institute angepasst und so von möglichst vielen genutzt werden kann.

Gruppe 3 umfasst alle Institute, die auf einen Zugriff von außen nicht verzichten können (Verneinung der ersten bzw. zweiten Frage) und keine DMZ einrichten wollen (Verneinung der dritten bzw. vierten Frage). Ob für diese Gruppe eine geeignete Firewall-Klasse gefunden werden kann, darf schon an dieser Stelle bezweifelt werden.

Gruppe 4 enthält alle Institute, deren Angaben unvollständig oder fehlerhaft sind. So wollen beispielsweise zwei Institute eine DMZ für Zugriffe aus dem Internet einrichten. Da sie bisher keine DMZ haben, müsste die Einrichtung eines eigenen Subnetzes und damit Verbunden eine Veränderung der bisherigen IP-Adressierung erfolgen. Dies lehnen die beiden Institute jedoch ab. Da keine Antworten priorisiert werden können, wurden die beiden Institute dieser Gruppe zugeordnet.

3.4.1 Gruppierung der Institute bei Zugriffen aus dem Internet

Hinsichtlich von Zugriffen aus dem Internet konnten der ersten Gruppe 15 Institute, der zweiten Gruppe 25 Institute zugeordnet werden (siehe Tabelle 3.28). Dies entspricht 27 bzw. 45 Prozent der befragten Institute. Zugriffsmöglichkeit aus dem Internet, aber keine DMZ wollen zwölf Institute (21 Prozent). Fehlerhaft oder unvollständig waren die Angaben von vier Instituten (7 Prozent).

	Gruppe 1	Gruppe 2	Gruppe 3	Gruppe 4
Zugriffe aus dem Internet	15 (27%)	25 (45%)	12 (21%)	4 (7%)
davon kleine Institute (bis zu 32 Rechner)	5 (42%)	5 (42%)	1 (8%)	1 (8%)
Zugriffe aus dem MWN	11 (20%)	26 (46%)	17 (30%)	2 (4%)
davon kleine Institute (bis zu 32 Rechner)	5 (42%)	6 (50%)	1 (8%)	0

Tabelle 3.28: Gruppierung der Institute, unterschieden nach Zugriffen aus dem Internet und dem MWN und unter besonderer Berücksichtigung der kleinen Institute

Obwohl für Institute, die keine Zugriffsmöglichkeiten aus dem Internet benötigen (Gruppe 1), keine Veränderung der IP-Adressierung notwendig ist, wären doch alle mit einer solchen Maßnahme einverstanden. Diese Tatsache kann genutzt werden, um das Institutsnetz durch die Umstellung auf private IP-Adressen und Masquerading nach außen zu verbergen. Zugriffe von außen sind dann deshalb schon nicht mehr möglich, weil private IP-Adressen im Internet nicht geroutet werden. Allerdings muss überlegt werden, ob dieses Mittel im Zusammenhang mit einem Remote-Zugang eingesetzt werden kann.

Von den Instituten der Gruppe 1 bieten zur Zeit noch zwölf Institute Dienste an, die aus dem Internet erreicht werden können. Da der Zugriff aus dem Internet auf das Institutsnetz in dieser Gruppe unterbunden werden soll, wären diese Dienste nicht mehr erreichbar. Die Institute haben jedoch die Möglichkeit die Serverkapazitäten des LRZ oder anderer Einrichtungen zu nutzen. Von dieser Möglichkeit wissen 14 der 15 Institute dieser Gruppe. Von den zwölf Instituten, die zur Zeit noch Dienste anbieten, wären acht bereit, diese Möglichkeit auch zu nutzen. Was die übrigen vier Institute tun wollen, konnte durch die Umfrage nicht festgestellt werden. Denkbar wäre, dass die Institute zukünftig auf diese Dienste verzichten oder sie nur noch über den Remote-Zugang nutzen.

Für die Institute, die ihre Dienste für das Internet zukünftig aus einer DMZ anbieten wollen (Gruppe 2), stellt sich die Frage, welche Dienste dies sind. Von den 25 Instituten dieser Gruppe passen zwei nicht in das im Abschnitt 3.3 entwickelte Diensteprofil. Das eine Institut möchte einen aus dem Internet zugänglichen AFS-Server betreiben, das andere Terminal Services anbieten. Ob diese Dienste von einer Firewall-Klasse unterstützt werden können ist fraglich.

Die Analyse der einzelnen Antworten der Umfrage hat ergeben, dass sich kleine Institute meist deutlich von der Gesamtheit abheben. Wie sieht dies nun bei den Institutsgruppen aus? Bis auf zwei Institute mit bis zu 32 Rechnern können alle den Gruppen 1 und 2 zugeordnet werden (siehe Tabelle 3.28). Von den zwei anderen Instituten waren bei einem die Angaben unvollständig, das zweite Institut wünscht keine Einschränkung bei Zugriffen aus dem Internet.

3.4.2 Gruppierung der Institute bei Zugriffen aus dem MWN

Zugriffe aus dem MWN auf das Institutsnetz generell unterbinden (Gruppe 1) wollen elf Institute, den Zugriff auf eine DMZ beschränken (Gruppe 2) wollen 26 Institute (siehe Tabelle 3.28). Dies sind 20 bzw. 46 Prozent der befragten Institute. Keine Einschränkungen dieser Art wollen 17 Institute (30 Prozent) und fehlerhafte oder unvollständige Antworten kamen von zwei Instituten (4 Prozent). Es fällt auf, dass im Vergleich zu Zugriffen aus dem Internet die Zahl der Institute, die generell keine Zugriffe auf das Institutsnetz zulassen wollen geringer ist. Gleichzeitig ist die Zahl derer, die keine Einschränkungen beim Zugriff von außen wollen, größer. Insgesamt lässt sich also die Tendenz zu einem niedrigeren Sicherheitslevel bei Zugriffen aus dem MWN gegenüber Zugriffen aus dem Internet feststellen.

Die Gruppe der Institute, die keinen Zugriff aus dem MWN ermöglichen wollen (Gruppe 1), würden bis auf ein Institut auch einer Veränderung der IP-Adressierung zustimmen. Dies ist hier zwar nicht notwendig, eröffnet aber wie bei den Zugriffen aus dem Internet die Möglichkeit private IP-Adressen und Masquerading einzusetzen.

Von den elf Instituten der Gruppe 1 bieten zur Zeit acht Dienste für das MWN an. Diese Dienste können nach den Bedingungen der Gruppe 1 aus dem MWN nicht mehr erreicht werden. Die Institute habe die Möglichkeit diese Dienste auf Server des LRZ oder anderer Einrichtungen auszulagern – davon wissen alle Institute. Von den acht Instituten, die zur Zeit Dienste anbieten, sind fünf bereit, diese Möglichkeit auch zu nutzen. Den übrigen drei Instituten bleibt die Einstellung des Dienstes oder die Beschränkung auf den Remote-Zugang.

Bei den Instituten die zukünftig ihre Dienste für das MWN aus einer DMZ heraus anbieten wollen (Gruppe 2), stellt sich wiederum die Frage, welche Dienste dies sind. Von den 26 Instituten bieten nur zwei Institute Dienste an, die nicht in das in Abschnitt 3.3 aufgestellte Diensteprofil passen. Dies ist einmal der Zugriff auf eine Oracle-DB, zum anderen die Nutzung von Terminal Services.

Betrachtet man wiederum nur die kleinen Institute mit bis zu 32 Rechnern, ergibt sich das selbe Bild wie bei den Zugriffen aus dem Internet. Nur ein Institut kann nicht in die Gruppen 1 oder 2 eingeordnet werden (siehe Tabelle 3.28). Dabei handelt es sich um das Institut, das schon keine Einschränkungen bei Zugriffen aus dem Internet gewünscht hat.

3.4.3 Kundenprofile für den Zugriff aus dem Internet und dem MWN

Nachdem in den beiden vorangegangenen Abschnitten die Gruppierung getrennt für Zugriffe aus dem Internet und aus dem MWN vorgenommen wurde, sollen daraus nun Schnittmengen gebildet werden. Für einen Großteil der Institute – die Kunden des LRZ – gilt, dass sie sowohl für Zugriffe aus dem Internet, als auch für Zugriffe aus dem MWN die gleichen Einschränkungen akzeptieren. Keinen Zugriff aus dem Internet und dem MWN auf das Institutsnetz wünschen neun Kunden (16 Prozent), die Beschränkung auf eine DMZ 21 Institute (38 Prozent) und gar keine Einschränkungen 12 Institute (21 Prozent). Von den übrigen Kunden wollen die meisten für Zugriffe aus dem MWN eine weniger einschränkende Zugriffsmöglichkeit als für Zugriffe aus dem Internet (siehe Tabelle 3.29). So wollen fünf Institute aus dem Internet keine Zugriffe, aus dem MWN Zugriffe beschränkt auf eine DMZ zulassen. Desweiteren gibt es drei Institute, die den Zugriff aus dem Internet auf eine DMZ, Zugriffe aus dem MWN uneingeschränkt ermöglichen wollen.

Übrig bleiben Einzelfälle bzw. fehlerhafte oder unvollständige Antworten. Unter den Einzelfällen findet sich ein Institut, das zwar keine Dienste für das Internet und das MWN anbietet, aber mit einem Institut auf einem anderen Kontinent via Internet ein VPN bilden möchte. Dazu wird der Zugang aus dem Internet auf eine DMZ benötigt, während Zugriffe aus dem MWN vollständig unterbunden werden können.

Bei dem geschilderten Einzelfall handelt es sich außerdem um ein kleines Institut (bis zu 32 Rechner). Die übrigen kleinen Institute wünschen sich von zwei Ausnahmen abgesehen – ein Institut möchte keine Einschränkung, bei einem zweiten waren die Angaben unvollständig – alle eine Beschränkung des Zugriffs aus dem Internet und dem MWN auf ihr Institutsnetz.

<table>
<tr><th>Internet
MWN</th><th>Gruppe 1</th><th>Gruppe 2</th><th>Gruppe 3</th><th>Gruppe 4</th></tr>
<tr><td>Gruppe 1</td><td>9 (16%)</td><td>1 (2%)</td><td>0</td><td>1 (2%)</td></tr>
<tr><td>Gruppe 2</td><td>5 (9%)</td><td>21 (38%)</td><td>0</td><td>0</td></tr>
<tr><td rowspan="2">Gruppe 3</td><td>1 (2%)</td><td>3 (5%)</td><td>12 (21%)</td><td>1 (2%)</td></tr>
<tr><td colspan="3">16 (28%)</td><td></td></tr>
<tr><td>Gruppe 4</td><td>0</td><td>0</td><td>0</td><td>2 (4%)</td></tr>
</table>

Tabelle 3.29: Schnittmengen aus den für Zugriffe aus dem Internet und dem MWN gebildeten Gruppen. Die als Profile gewählten Schnitte sind fett gedruckt.

Abschließend kann festgestellt werden, dass es drei Kundenprofile bezüglich Zugriffe von außen gibt. Diese Profile sollen später den Firewall-Klassen zugeordnet werden können.

Profil 1 umfasst Kunden, die weder Zugriffe aus dem Internet, noch aus dem MWN wünschen. Diese Gruppe umfasst 16 Prozent der befragten Institute. Die einzige Zugangsmöglichkeit soll durch Remote Access sichergestellt werden. Dies wird von allen Instituten aus diesem Profil gewünscht. Die mit der Verwendung von privaten IP-Adressen und Masquerading notwendigen Umstellungen bei der IP-Adressierung würde ebenfalls von allen Kunden akzeptiert werden.

Profil 2 beinhaltet die Kunden, die zwar keine Zugriffe aus dem Internet ermöglichen, jedoch Zugriffe aus dem MWN auf eine DMZ anbieten wollen. Hier handelt es sich um 9 Prozent der Institute. Alle diese Institute akzeptieren eine Umstellung der IP-Adressierung und wären damit auch einer Verwendung von privaten IP-Adressen und Masquerading aufgeschlossen. Bis auf ein Institut passen alle Institute in das Diensteprofil aus Abschnitt 3.3. Dies sind 7 Prozent der befragten Institute.

Profil 3 schließt die Kunden ein, die sowohl für Zugriffe aus dem Internet, wie auch für Zugriffe aus dem MWN eine DMZ einrichten wollen. Hier handelt es sich um 38 Prozent der Institute. Ein Teil der Institute hat bereits eine DMZ eingerichtet und will deshalb auch keine Umstellung der IP-Adressierung. Bei den angebotenen Diensten passen zwei Institute nicht in das Diensteprofil aus Abschnitt 3.3. Unter Berücksichtigung dieses Aspekts umfasst das Profil 3 dann noch 34 Prozent.

Profil 4 enthält die Kunden, die für Zugriffe aus dem MWN und zum Großteil auch aus dem Internet keine Beschränkung wünschen. Insgesamt umfasst diese Gruppe 28 Prozent der befragten Institute.

Zum Profil 4 ist anzumerken, dass der Zugriff aus dem Internet auf das gesamte Institutsnetz nicht im Sinne eines Sicherheitskonzeptes sein kann. Auch dann nicht, wenn die zugreifbaren Dienste auf das Diensteprofil aus Abschnitt 3.3 eingeschränkt würden. Dies muss ebenso für Zugriffe aus dem MWN gelten. Zwar kann die Vertrauenswürdigkeit von Zugriffen aus dem MWN etwas besser eingeschätzt werden, dies rechtfertigt aber noch nicht, das gesamte Institutsnetz offen zu legen. Zudem ist die Zahl der Institute, die einen uneingeschränkten Zugriff aus dem MWN kombiniert mit Einschränkungen für Zugriffe aus dem Internet wollen, verhältnismäßig klein.

Übrig bleiben ein Einzelfall (wie oben beschrieben) und vier Institute, deren Angaben ungenügend waren.

Zone	internes Netz	MWN-Server	Internet-Server
Profil 1	x		
Profil 2	x	x	
Profil 3	x	x	x

Tabelle 3.30: Beziehung zwischen den Sicherheitszonen und den Kundenprofilen zum Angebot von Diensten

3.5 Sicherheitszonen in einem Institut

Da die Verwaltungen in der Regel als eigene Institute aufgefasst werden, ist in den Instituten keine spezielle Verwaltungszone notwendig. Die hier betrachteten Zonen können sicher nicht die Situation in allen Instituten abdecken. U. U. gibt es in manchen Instituten weitere Sicherheitszonen, die ein eigenes Subnetz und eine zusätzliche Abschirmung notwendig machen. Da das Firewall-Konzept aber nur eine Standardlösung bietet, kann auf solche Sonderfälle nicht eingegangen werden. In den meisten Instituten sind folgende Sicherheitszonen zu erwarten:

Internes Netz: Im internen Netz befinden sich die Mitarbeiterrechner und Server, die nur innerhalb des internen Netzes genutzt werden können. Von außen kann nicht auf dieses Netz zugegriffen werden. Von außen erreichbare Server stellen ein potentielles Angriffsziel dar. Ein erfolgreiches Eindringen in einen solchen Rechner würde das gesamte interne Netz korrumpieren. Da auch die gängigen SSH-Server in der Vergangenheit Sicherheitslücken aufgewiesen haben, kann auch deren Verwendung nicht empfohlen werden.
Der Zugriff vom internen Netz auf Dienste des MWN oder Internet ist möglich. Dafür vorgesehen ist standardmäßig die Verwendung eines dynamischen Paketfilters. Als Option kann zusätzlich ein statischer Filter geschaltet werden, der den Zugriff auf ausgewählte Dienste begrenzt.

MWN-Server: Diese Zone enthält Server mit Angeboten für das MWN. Im einfachsten Fall ist dies nur ein SSH-Server, der den Zugang für berechtigte Nutzer in das Institutsnetz gestattet. Dieser Server kann dann als Remote-Server genutzt werden. Unter Verwendung von SCP könnte damit ein Dateiserver realisiert werden. Vom SSH-Server aus lässt sich außerdem auf andere sonst nicht zugängliche Dienste zugreifen. Weiterhin sind in dieser Zone Server erlaubt, die auf das MWN begrenzte Dienste anbieten. Soll der Zugriff auf einen bestimmten Personenkreis eingeschränkt werden, kann dies jedoch nur durch zusätzliche Maßnahmen erreicht werden. Der Zugriff von außen wird durch einen statischen Paketfilter auf bestimmte Dienste begrenzt. Diese Dienste sind im Diensteprofil 4 (siehe Abschnitt 3.3) aufgeführt.

Internet-Server: Diese Zone enthält alle Server, die aus dem Internet erreichbar sein sollen. Der Zugriff von außen wird durch einen statischen Paketfilter auf bestimmte Dienste begrenzt. Diese Dienste sind im Diensteprofil 3 aufgeführt.

Im Abschnitt 3.4 wurden aus den Ergebnissen der Umfrage Kundenprofile herausgearbeitet. Institute des Profils 1 benötigen nur die Zone “internes Netz”, Institute des Profils 2 benötigen die Zonen “internes Netz” und “MWN-Server” und die Institute des Profils 3 benötigen alle Zonen (siehe Tabelle 3.30). Das Realisieren der Zonen “MWN-Server” und “Internet-Server” in zwei getrennten Subnetzen bedeutet einen erhöhten Aufwand und scheint deswegen nicht ratsam. Auf Seiten des LRZ müsste ein zusätzliches VLAN eingerichtet werden. Mit häufigen Wechseln der Server zwischen den Zonen ist zu rechnen, was den Administrationaufwand erhöht. Auf Seiten der Institute müsste bei zwei getrennten Subnetzen zusätzliche Rechner angeschafft und konfiguriert werden.

Unter Berücksichtigung der Kunden- und Betreiberanforderungen wird deshalb vorgeschlagen, die Zonen "MWN-Server" und "Internet-Server" in einem gemeinsamen Subnetz zu realisieren. Der Zugriff auf Dienste, die ausschließlich dem MWN vorbehalten sind (z. B. DNS), kann durch Filterregeln gewährleistet werden. Bei Servern, die getrennte Angebote für das MWN und das Internet anbieten, muss dies durch eine entsprechende Serverkonfiguration sichergestellt werden. Zusätzlich kann bei einzelnen Diensten (z. B. WWW) durch die Verwendung von zwei Ports eine Unterscheidung getroffen werden.

Zusammenfassend ergeben sich zwei Teilnetze:

- Internes Netz,
- Servernetz.

Verbindungen von außen sind nur auf das Servernetz möglich und dort auch nur auf die angebotenen Dienste. Das interne Netz ist von außen nicht erreichbar. Da damit zu rechnen ist, dass ein Server im Servernetz gehackt wird, sollte auch vom Servernetz aus nicht auf das interne Netz zugegriffen werden können. Für den Zugriff aus dem internen Netz auf das Servernetz können unter Umständen zusätzliche Dienste genutzt werden, die aus dem Internet nicht erreichbar sind. Beispielsweise wäre ein SSH-Zugang für Konfigurationsaufgaben denkbar.

3.6 MWN und Internet aus der Sicht der Institute

Als Institute werden in diesem Zusammenhang einzelne Lehrstühle, Institute, Fakultäten, Verwaltungen der Fakultäten und Universitäten, Bibliotheken, Wohnheime, Krankenhäuser etc. verstanden. Da die Verwaltungen überwiegend als eigene Institute organisiert sind, ist es nicht notwendig innerhalb eines Instituts eine Trennung von Forschungsbereich/Lehrbereich und Verwaltungsbereich zum Schutz von Personal- und Haushaltsdaten vorzunehmen [Lort 00]. Die meisten Institute bieten nach außen Dienste an. Dazu zählen WWW-Server mit Angeboten für das Internet oder beschränkt auf das MWN, Datei-Server mit Zugriffsmöglichkeiten aus dem MWN, Radius-Server für die Authentifizierung im MWN und vieles mehr.

Aus der Sicht der Institute gibt es neben dem eigenen Institutsnetz, das MWN und dahinter das Internet. Entsprechend gibt es zwei Übergangspunkte – vom Internet zum MWN, vom MWN zum Institutsnetz. Das MWN unterscheidet sich vom Internet dadurch, dass es nur von einem geschlossenen Benutzerkreis genutzt werden kann. Dies sind die Mitarbeiter und Studenten der Universitäten, Fachhochschulen und anderer Einrichtungen. Zur Zeit sind beim LRZ 53.523 Benutzer registriert [ApLä 02]. Der Zugang zum MWN ist von den angeschlossenen Instituten, über Einwahl-Server und einen VPN-Server möglich. Der VPN-Server wird genutzt für die WLAN-Zugänge und als Möglichkeit, sich von anderen Teilen des Internet aus in das MWN einzuloggen. Beim Einwahl- und VPN-Server ist eine Authentifizierung notwendig. Dies erfolgt durch ein verteiltes System von Radius-Servern. Da dabei keine festen IP-Adressen verwendet werden, werden die Zugangsdaten zur Zeit 10 Tage gespeichert [Läpp 02]. Schon jetzt sollte zur Nutzung des MWN durchgehend eine Authentifizierung Pflicht sein. Garantiert werden kann dies zur Zeit aber nur für die Zugänge in den öffentlichen Räumen, für die Einwahl-Server und für den VPN-Zugang. In anderen Bereichen ist es möglich auch ohne Authentifizierung das MWN zu nutzen. Nach der Umfrage bei den Netzverantwortlichen der Institute gibt es bei rund der Hälfte der Institute frei zugängliche Netzwerksteckdosen. Zukünftig soll nach einem Software-Update der Switches eine durchgehende Authentifizierung nach IEEE 802.1x möglich werden [ApLä 02]. Ein zusätzliches Problem stellen eigene Modems oder ISDN-Adapter der Institute dar, die bei etwa 15 Prozent der Institute vorhanden sind.

Wie die Umfrage bei den Netzverantwortlichen der Institute gezeigt hat, bringen die Institute dem MWN mehr Vertrauen entgegen als dem Internet:

- 15 Institute wären bereit Zugriffe aus dem Internet auf ihr Institutsnetz vollständig zu unterbinden. Davon akzeptieren jedoch nur neun die selbe Einschränkung für das MWN.

- Eine Demilitarisierte Zone (DMZ) für Angebote, die aus dem Internet genutzt werden können, befürworten 42 Institute. Eine DMZ für Angebote in das MWN hingegen nur 37 Institute.

- Server, die Datei- und Druckdienste anbieten, sollen bei 31 Instituten aus dem MWN erreichbar sein, bei nur sechs aus dem Internet.

Allein die Tatsache, dass sich die Benutzer des MWN authentifizieren müssen oder über feste IP-Adressen identifizierbar sind, kann dieses Vertrauen nicht rechtfertigen. Ein Kunde von T-Online würde wohl kaum (zumindest nicht wissentlich) einen Datei- oder Druck-Server den anderen Nutzern von T-Online zugänglich machen wollen. Worin unterscheidet sich nun das MWN von den Netzen anderer Provider?

Nach den Benutzerrichtlinien [BADW] darf das MWN nur für Zwecke der "Forschung, Lehre, Verwaltung, Aus- und Weiterbildung, Öffentlichkeitsarbeit und Außendarstellung" genutzt werden. Die Benutzer des Netzes sind aufgefordert das MWN "verantwortungsvoll und ökonomisch" zu verwenden. Zum "Problemkreis einer nicht zulässigen Nutzung" [Hege 01] zählen Filesharing-Dienste, Missbrauch von anonymen FTP-Servern, durch Hackerangriffe manipulierte Server und Netzspiele. Neben dem zentralen Management des MWN durch das LRZ, sind einige Aufgaben auch dezentral organisiert. So muss jedes Institut einen Netzverantwortlichen benennen. Zu dessen Aufgaben gehören die Verwaltung des zugewiesenen Namens- und Adressraums, Dokumentation des Institutsnetz, Mitwirkung bei der Fehlerbehebung und Mitwirkung bei der Eindämmung missbräuchlicher Nutzung [Läpp 01].

Diese Regelungen alleine erlauben jedoch nur im beschränktem Maße, dem MWN ein größeres Vertrauen entgegenzubringen als dem übrigen Internet. Dazu ist die Gefahr von gehackten Rechnern und offenen Ports zu groß. Auch die große Zahl berechtigter Nutzer, lässt einige schwarze Schafe erwarten. Aus diesem Grund ist die Unterscheidung zwischen Internet und MWN weniger aus sicherheitstechnischer Sicht zu betrachten. Bei Diensten, die nur für das MWN angeboten werden, muss damit gerechnet werden, dass auch unberechtigte Person Zugriff darauf erlangen können. Beispielsweise gibt es in manchen Instituten Prüfungsprotokolle. Diese werden von manchen Studenten nach der Prüfung angefertigt und können dann von weiteren Kandidaten zur Prüfungsvorbereitung genutzt werden. Es gibt dabei die Übereinkunft zwischen Prüfern und Studenten, diese Unterlagen nur den Angehörigen des MWN zugänglich zu machen. Einen möglichen unberechtigten Zugriff nehmen beide Seiten in Kauf. Dienste, die aber garantiert nur einem begrenzten Benutzerkreis zugänglich sein sollen, müssen zusätzlich abgesichert werden. Das Firewall-Konzept mit seinen standardisierten Lösungen kann dies jedoch nicht leisten. Es kann nur eine Hürde aufbauen, in dem auf solche Dienste nur aus dem MWN zugegriffen werden kann. Diese Hürde ist aber überwindbar.

3.7 Zusammenstellung der Anforderungen

3.7.1 Anforderungen des Dienstes

Aus der in Kapitel 1.1 geschilderten Problematik ergab sich die Notwendigkeit für die Bereitstellung eines Firewall-Dienstes. Dieser soll die Situation hinsichtlich einer sicheren Nutzung des Internet und des MWN verbessern. In diesem Abschnitt sind die Anforderungen dargestellt, die sich aus dem Dienst selbst ergeben. In den beiden folgenden Abschnitten werden weitere Anforderungen aufgezählt, die aus der Sicht des Betreibers (LRZ) und der Kunden (Institute) zu berücksichtigen sind. Dabei sind Konflikte zwischen einzelnen Anforderungen möglich.

Kontrolle des Datenverkehrs: Es muss sowohl der Verkehr zwischen Internet und Institut, als auch zwischen MWN und Institut kontrolliert werden. Aus diesem Grund ist eine Firewall-Lösung, die nur den Verkehr am Übergangspunkt zwischen G-WiN und MWN filtert, nicht ausreichend. Es muss sichergestellt werden, dass auch innerhalb des MWN eine Kontrolle stattfindet, also im Netzverkehr zwischen den einzelnen Instituten des MWN. Für eine wirkungsvolle Filterung ist es notwendig, dass der Übergang vom/zum Institut auf eine Stelle konzentriert wird. Weitere Zugänge erhöhen den Konfigurationsaufwand und die Fehleranfälligkeit. Besonders problematisch sind Zugänge in Form von Modems, ISDN-Adaptern etc. und sollten deshalb weitestgehend untersagt werden.

Zugriffe aus dem Internet und dem MWN: Zugriffe von außen müssen auf die notwendigen Dienste und erlaubte Operationen beschränkt werden. Außerdem sollen nur Rechner erreichbar sein, die einen Dienst anbieten. Die sicherste Methode ist es, für diese Rechner ein eigenes Subnetz (DMZ) anzulegen. Die anderen Teile des Institutsnetzes sollen von außen nicht erreichbar sein.

Nutzung von Diensten: Den Benutzungsrichtlinien für das MWN [BADW] ist zu entnehmen, dass das MWN für "Forschung, Lehre, Verwaltung, Aus- und Weiterbildung, Öffentlichkeitsarbeit und Außendarstellung der Hochschulen und für sonstige in Art. 2 des Bayerischen Hochschulgesetzes beschriebene Aufgaben zur Verfügung" steht. Aus diesem Grund kann eine Beschränkung auf sinnvolle Dienste notwendig werden. Eine missbräuchliche Nutzung sollte unterbunden werden. Dazu zählt z. B. der Austausch von urheberrechtlich geschütztem Material über Filesharing-Dienste.

Erschweren von Scans: Die für die Vorbereitung eines Angriffs notwendige Informationsbeschaffung soll erschwert werden. Dazu muss die interne Struktur der Netze verborgen werden. Informationen, die auf verwendete Betriebssysteme, Anwendungen und Firewalls schließen lassen, müssen so weit wie möglich unterdrückt werden.

Erschweren von Hacks: Die von außen erreichbaren Server müssen gut gepflegt sein, um ein Eindringen in das System zu unterbinden. Dazu gehören das Vornehmen regelmäßiger Updates und das sofortiges Anwenden von Sicherheits-Patches.

Filterung der Anwendungsdaten: Die durch die Anwendungsprotokolle transportierten Daten sollen nach schädlichem Inhalt gefiltert werden. Beispielsweise können Mail-Attachments Viren, Trojaner oder Würmer enthalten, durch aktive Inhalte des WWW (Java-Applets, Active-X-Controls etc.) können unberechtigte Operationen ausgeführt werden. Aber nicht nur eingehende Daten sind für eine Filterung interessant. Bei ausgehenden Verbindungen kann es z. B. sinnvoll sein, personenbezogene Daten zu entfernen.

Schutz vor sonstigen Angriffen: Neben den bereits genannten Maßnahmen, ist ein Schutz vor weiteren Arten von Angriffen notwendig. Dazu zählen Denial-of-Service oder Spoofing.

3.7.2 Anforderungen des Betreibers

Aus der in Kapitel 1.1 geschilderten Struktur und Organisation des MWN ergeben sich aus der Sicht des Betreibers weitere Anforderungen.

Kosten des G-WiN-Zugangs: Die Kosten des G-WiN-Zugangs beliefen sich 2001 auf 1,4 Mio DM [Hege 01]. Die Kosten richten sich nach der Bandbreite des Anschlusses (622 Mbit/s) und dem Transfervolumen (25 TByte pro Monat). Das LRZ übernimmt die Bezahlung des Zugangs. Um die Kosten in diesem Rahmen halten zu können, muss eine missbräuchliche Nutzung unterbunden werden. Besonders Dienste, die große Transfervolumen verursachen und nicht den Statuten des MWN entsprechen (z. B. Filesharing), sind zu unterbinden.

Berücksichtigung der vorhandenen Infrastruktur: Im MWN ist noch nicht in allen Bereichen eine strukturierte Verkabelung vorhanden. In den Gebäuden wird in etwa 40 Prozent der Fälle noch eine Verkabelung basierend auf 10Base5 betrieben. Allerdings soll in nächster Zeit auch in diesen Bereichen auf eine strukturierte Verkabelung umgestellt werden [ApLä 02]. Bis dahin muss dieses Situation vom Firewall-Dienst berücksichtigt werden. Das LRZ betreibt bis auf wenige Ausnahmen alle Netzkomponenten des MWN. Beim Einrichten einer Firewall muss deshalb sichergestellt werden, dass hinter einer Firewall befindliche Komponenten für das LRZ erreichbar und managebar bleiben [Wimm 01].

Nutzung vorhandener Kapazitäten: Das LRZ ist nicht in der Lage zusätzliches Personal für den Firewall-Dienst einzustellen. Aus diesem Grund können nur einige wenige standardisierte Firewall-Pakete angeboten werden. Für die Einarbeitung in neue Produkte und für deren Betrieb werden Personalkapazitäten gebunden. Deshalb muss geprüft werden, ob bereits vorhandene Geräte, Software und Dienste für den Firewall-Dienst herangezogen werden können. Als Beispiele denkbar sind die Nutzung der Filtermöglichkeiten der Router oder die Erweiterung des schon vorhandenen Mail-Service um einen Virenscanner. Die dabei eingesetzten Komponenten sind bereits bekannt und bewährt.

Betrieb des Dienstes: Für den Firewall-Dienst ist die Erstellung eines Betriebskonzept notwendig. Bestehende Betriebsabläufe und Managementprozesse müssen unter Umständen angepasst werden. Der Firewall-Dienst muss beim Störungsmanagement, der Netzdokumentation und beim Netz- und Systemmanagement berücksichtigt werden.

3.7.3 Anforderungen des Kunden

Die rund 700 Institute treten hinsichtlich des Firewall-Dienstes als Kunden auf. Die Institute unterscheiden sich in Größe, Struktur, und Tätigkeit. Zudem besteht ein unterschiedlicher Wissensstand darüber, welche Gefahren bei der Nutzung des Internet existieren, welche Maßnahmen zum Schutz des eigenen Netzes sinnvoll sind und wie diese umgesetzt werden können. Daraus ergeben sich auf Seiten der Institute entsprechend unterschiedliche Anforderungen an den Firewall-Dienst. Wie diese Anforderungen im einzelnen aussehen war jedoch nicht bekannt. Aus diesem Grund wurden mit Hilfe der Umfrage Dienste- und Kundenprofile entwickelt.

Diensteprofile: Aus der Umfrage konnte ermittelt werden, welche Dienste von den Instituten häufig genutzt und angeboten werden. Weiter wurden Dienste berücksichtigt die für das MWN eine wichtige Rolle spielen (z. B. Radius). Dabei wurden fünf Kommunikationsbeziehungen unterschieden. Dem entsprechend wurden fünf Diensteprofile (siehe Abschnitt 3.3) herausgearbeitet. Der Firewall-Dienst muss diese Profile berücksichtigen, um den Kommunikationsinteressen möglichst vieler Institute gerecht zu werden. Ergänzend muss sichergestellt werden, dass die Server vom Institutsnetz aus verwaltet werden können.

Nutzung von Diensten: Die von den Kunden häufig genutzten Dienste sind in den Diensteprofilen 1 und 2 aufgelistet. Da 38 Prozent der Institute (siehe Abschnitt 3.25) eine Nutzungsbeschränkung auf diese Dienste befürworten, soll der Firewall-Dienst eine entsprechende Möglichkeit anbieten.

Content-Filtering: Ein weiteres Ergebnis der Umfrage war, dass einige Institute Content-Filtering akzeptieren. Auf die Frage, ob mit Hilfe von Content-Filtering Java-Applets und andere aktive Inhalte des WWW blockiert werden sollen, antworteten 23 Prozent mit ja. Die Frage nach einer Beschränkung des Zugriffs auf bestimmte Sites (URL-Filtering) im Internet befürworteten sogar 54 Prozent (siehe Tabelle 3.16). Aus diesem Grund muss untersucht werden, ob im Firewall-Dienst entsprechende Filtermöglichkeiten realisiert werden können.

Kundenprofile: Bei der Auswertung der Umfrage wurde untersucht, ob und in welcher Form die Institute zukünftig Dienste für das Internet und MWN anbieten wollen. Daraus wurden vier Kundenprofile (siehe Abschnitt 3.4.3) gewonnen. Die für den Firewall-Dienst zu entwickelnden Paket-Lösungen müssen diese Profile berücksichtigen.

Kapitel 4

Dienstbeschreibung

Für die Beschreibung des Dienstes wird das in “A Framwork for IT-Service Management” [DR 02] eingeführte Modell verwendet. Das Service Model wird mit Hilfe von UML dargestellt. Methodisch erfolgt die Spezifikation in drei Schritten: Beschreibung aus dienstzentrierter Sicht, aus providerzentrierter Sicht und aus kundenzentrierter Sicht. Von Schritt zu Schritt wird die Spezifikation ergänzt und verfeinert. Auf diese Weise entsteht ein umfassendes UML-Klassendiagramm mit vorgegebenen Klassen, Attributen, Assoziationen und Vererbungen. Im folgenden wird für die Beschreibung des Firewall-Dienstes dieses Klassenmodell in Teilen instantiiert (siehe Abbildung 4.1).

4.1 Firewall: Service

Name: Firewall

Trennung des Kundennetz vom übrigen MWN und vom Internet. Sämtlicher Verkehr zwischen den Netzen läuft über die Firewall. Der Verkehr wird so eingeschränkt, dass er den Sicherheitsanforderungen genügt.

Eine Firewall ist ein Konzept zur physischen und logischen Trennung zweier oder mehrerer Teilnetze mit unterschiedlichen Sicherheitsanforderungen. Der Firewall-Dienst des MWN trennt ein Kundennetz vom übrigen MWN und vom Internet. Zusätzlich ist eine Unterteilung des Kundennetzes in einzelne Subnetze möglich, die ebenfalls durch den Firewall-Dienst getrennt werden. Für die Wirksamkeit des Dienstes wird sichergestellt, dass sämtlicher Verkehr über die Firewall läuft.

Der Firewall-Dienst wurde auf die Erfüllung der in Abschnitt 3.7 zusammengestellten Anforderungen ausgerichtet. Zugriffe aus dem Internet und dem MWN auf das Kundennetz können durch die Firewall eingeschränkt werden. Eine Beschränkung bei der Nutzung von Diensten und Filtern von Anwendungsdaten ist ebenfalls möglich. Durch den Firewall-Dienst sollen das Scannen und Hacken von Rechnern sowie andere Angriffe erschwert werden.

Im übrigen ergibt sich die Funktionalität des Firewall-Dienst aus den folgenden Functional Building Blocks (FBB).

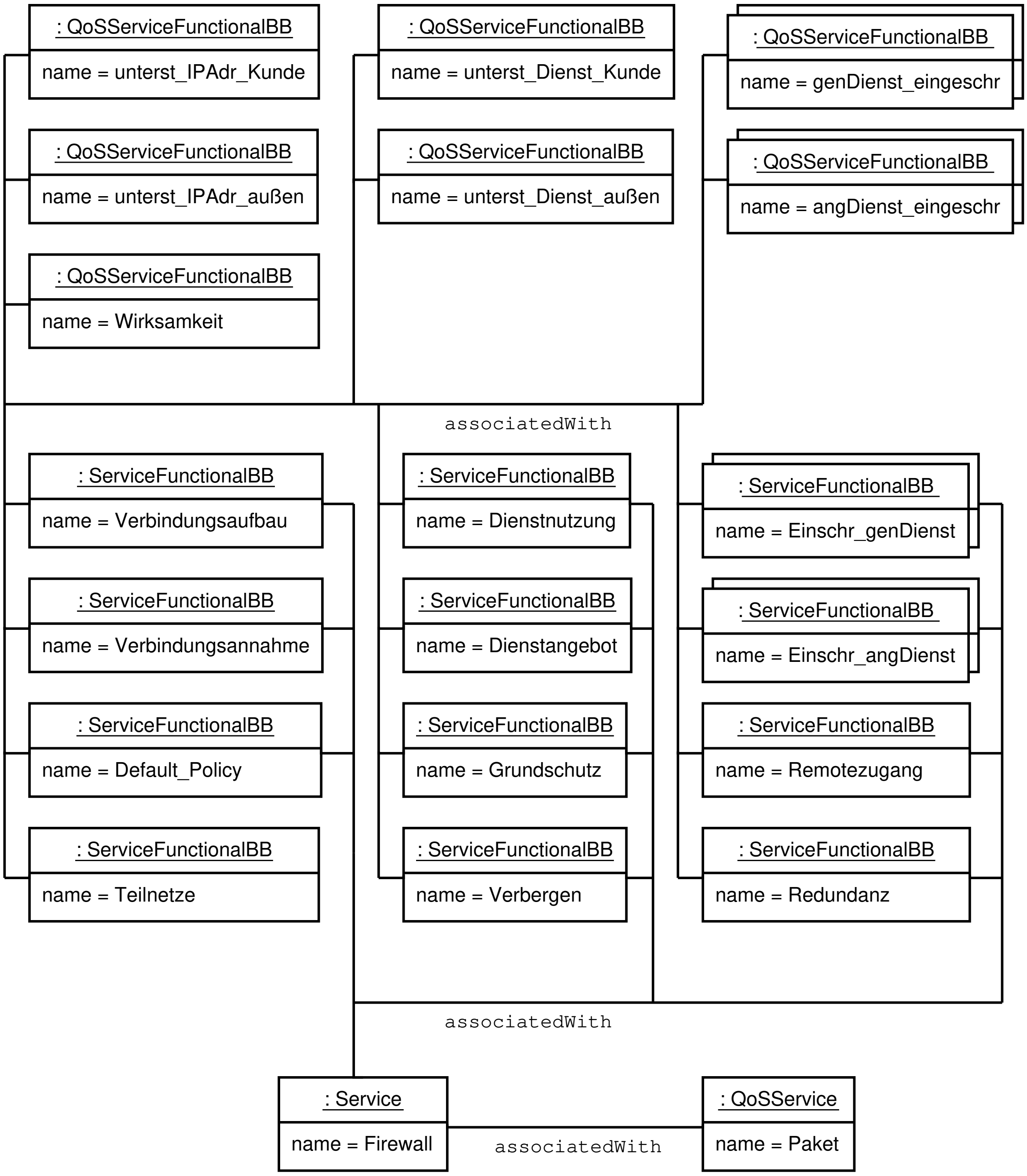

Abbildung 4.1: Instanzen des Klassenmodells

4.2 Instanzen der Klasse ServiceFunctionalBB

4.2.1 Default Policy

Name: Default_Policy

Bei der Konzeption einer Firewall gibt es zwei grundsätzliche Herangehensweisen. Die erste erlaubt in der Default-Einstellung jede Kommunikation über die Firewall hinweg. Darauf aufbauend werden Regeln definiert, mit deren Hilfe einzelne unerwünschte oder gefährliche Dienste gefiltert werden. Die zweite Herangehensweise unterbindet in der Default-Einstellung jede Kommunikation. Die über die Firewall verbundenen Subnetze sind somit voneinander getrennt. Erwünschte Dienste sind gezielt zuzulassen.

Es ist unstrittig, dass die erste Herangehensweise vom Standpunkt der Sicherheit aus problematischer ist. Eine vergessene Filterregel in der Konfiguration führt zu einer Sicherheitslücke in der Firewall. Bei der zweiten Herangehensweise würde in diesem Fall nur ein bestimmter Dienst nicht oder nur eingeschränkt genutzt werden können. Die daraufhin sicher sofort einlaufenden Beschwerden von Seiten der Nutzer, würden den Administrator der Firewall auf den Fehler aufmerksam machen. Ob im ersten Fall entsprechende Hinweise den Firewall-Verantwortlichen erreichen, ist hingegen fraglich.

Aus diesem Grund wird die Default-Policy so gewählt, dass jede Kommunikation von der Firewall blockiert wird. Erwünschte Dienste müssen extra zugelassen werden. Dabei ist allerdings darauf zu achten, dass die dazu notwendigen Firewall-Regeln Durchgänge in der Firewall nur sehr gezielt und eingeschränkt schaffen, da durch zu große Öffnungen die Default-Policy sinnlos wird.

4.2.2 Verbindungsaufbau von Client nach außen

Name: Verbindungsaufbau

Hier handelt es sich um den Fall, dass ein Client im Kundennetz einen Dienst außerhalb nutzen möchte. Zu diesem Zweck wird vom Client eine Session eröffnet. Bei einer Anwendung, die auf TCP basiert, geschieht dies durch einen expliziten Verbindungsaufbau. Unter Umständen können mehrere TCP-Verbindungen zu einer Session gehören, wie dies z. B. bei FTP in Form von Steuerungs- und Datenverbindung der Fall ist. Bei UDP oder ICMP wird die Session durch das initiale Datagram gestartet.

In allen Fällen geht die Eröffnung der Session von einem Rechner im Netz des Kunden aus. Von außen können keine Sessions eingerichtet werden. Nur Datenpakete, die zu einer bereits existierenden Session gehören, können die Firewall von außen nach innen passieren.

4.2.3 Verbindungsannahme von außen auf Server

Name: Verbindungsannahme

In diesem Fall werden im Kundennetz Dienste angeboten, auf die von außerhalb zugegriffen werden kann. Zu diesem Zweck betreibt der Kunde in seinem Netz entsprechende Server. Will ein Client von außerhalb auf einen angebotenen Dienst zugreifen, muss er eine Session aufbauen. Bei einer Anwendung, die auf TCP basiert, geschieht dies durch einen expliziten Verbindungsaufbau. Unter Umständen können mehrere TCP-Verbindungen zu einer Session gehören, wie dies z. B. bei FTP in

Form von Steuerungs- und Datenverbindung der Fall ist. Bei UDP oder ICMP wird die Session durch das initiale Datagram gestartet.

In allen Fällen geht die Eröffnung der Session von einem Rechner außerhalb des Kundennetzes aus. Von einem Server im Kundennetz können keine Sessions eingerichtet werden. Nur Datenpakete, die zu einer bereits existierenden Session, gehören können die Firewall von innen nach außen passieren.

4.2.4 Nutzung ausgewählter Dienste

Name: Dienstnutzung

Hier handelt es sich um den Fall, dass ein Client im Kundennetz einen Dienst außerhalb nutzen möchte. Die Dienstnutzung ist jedoch eingeschränkt. Es ist nur der Zugriff auf bestimmte Dienste auf bestimmten Servern erlaubt. Es ist nicht allen Rechnern im Kundennetz die Nutzung von Diensten im gleichen Maße gestattet.

Auf diese Weise können Datenpakete die Firewall von innen nach außen nur dann passieren, wenn sie an einen erlaubten Dienst auf einem bestimmten Server gerichtet sind und von einem berechtigten Client im Kundennetz stammen. In der umgekehrten Richtung können Pakete die Firewall nur dann passieren, wenn sie von einem erlaubten Dienst auf einem bestimmten Server stammen und an einen berechtigten Client gerichtet sind.

4.2.5 Angebot ausgewählter Dienste

Name: Dienstangebot

In diesem Fall werden vom Kunden Dienste angeboten, auf die von außerhalb zugegriffen werden kann. Das Anbieten von Diensten ist jedoch eingeschränkt. Es können nur erlaubte Dienste auf vorgesehenen Servern von außen erreicht werden. Es ist nicht allen Rechnern außerhalb des Kundennetzes der Zugriff auf diese Dienste gestattet.

Auf diese Weise können Datenpakete die Firewall von außen nach innen nur dann passieren, wenn sie an einen erlaubten Dienst auf einem bestimmten Server im Kundennetz gerichtet sind und von einem berechtigten Client stammen. In der umgekehrten Richtung können Pakete die Firewall nur dann passieren, wenn sie von einem erlaubten Dienst auf einem bestimmten Server stammen und an einen berechtigten Client gerichtet sind.

Wird dieser Service FunctionalBB nicht unterstützt, hat der Kunde die Möglichkeit, seine Dienste auf Server anderer Institute auszulagern.

4.2.6 Einschränkung genutzter Dienste

Name: Einschr_genDienst

Zu der im FBB Dienstnutzung (siehe Abschnitt 4.2.4) vorgenommenen Begrenzung bei der Dienstnutzung, erfolgt zusätzlich eine Einschränkung der Funktionalität eines einzelnen Dienstes. Die Art der Einschränkung ist abhängig vom Dienst. Deshalb sind mehrere Instanzen dieser Art notwendig. Im Falle des WWW ist z. B. das Filtern nach URLs oder von aktiven Inhalten denkbar.

4.2.7 Einschränkung angebotener Dienste

Name: Einschr_angDienste

Zu der im FBB Dienstangebot (siehe Abschnitt 4.2.5) vorgenommen Begrenzung beim Angebot von Diensten, erfolgt zusätzlich eine Einschränkung der Funktionalität eines einzelnen Dienstes. In vielen Fällen kann auch durch entsprechende Konfiguration des Servers die Funktionalität eines Dienstes angepasst werden. Auf Grund immer wieder vorkommender Fehlkonfigurationen und zum Durchsetzen bestimmter Policies ist es jedoch sinnvoll, auch auf der Firewall eine solche Möglichkeit vorzusehen. Die Art der Einschränkung ist abhängig vom Dienst. Deshalb sind mehrere Instanzen dieser Art notwendig. Im Falle von SMTP wird z. B. der direkte Zugriff aus dem Internet auf einen Mail-Server im Kundennetz unterbunden, um den Missbrauch des Servers als Spam-Relay zu vermeiden.

4.2.8 Teilnetze für Rechner mit gleichen Sicherheitsanforderungen

Name: Teilnetze

Kundenrechner mit ähnlichen Sicherheitsanforderungen sollen in extra Subnetzen zusammengefasst werden. Die auf diese Weise entstandenen Sicherheitszonen werden durch die Firewall getrennt. Anzahl und Umfang der Teilnetze richtet sich nach den Sicherheitsanforderungen.

4.2.9 Verbergen von Teilnetzen

Name: Verbergen

Nach außen tritt als Kommunikationspartner an Stelle eines Rechners im Teilnetz die Firewall auf. Dadurch bleibt die Struktur des Teilnetzes verborgen, die einzelnen Rechner werden nicht sichtbar. Ein direkter Zugriff von außen auf einen Rechner im abgeschirmten Teilnetz wird unterbunden.

4.2.10 Remotezugang

Name: Remotezugang

Ein Remotezugang ist für Rechner oder Subnetze außerhalb des Kundennetzes gedacht. Über den Remotezugang ist eine Verbindung mit dem Kundennetz möglich, die weitergehende Kommunikationsmöglichkeiten bietet als der ansonsten vorgesehene Zugang von außen. Im Idealfall hat der Nutzer des Remotezugangs die gleichen Kommunikationsmöglichkeiten wie ein Nutzer innerhalb des Kundennetzes.

4.2.11 Redundante Sicherheit

Name: Redundanz

Redundanz wird durch unterschiedliche Sicherheitsmechanismen oder durch unterschiedliche Implementierungen eines Sicherheitsmechanismus erreicht. Zu diesem Zweck werden unterschiedliche Firewall-Produkte eingesetzt. Beim Versagen des einen Produkts bleibt der Schutz des anderen.

Name	Typ	Beschreibung
IP-Adresse im Kundennetz	IP-Adresse / Subnetmask	Wird bei ausgehenden Paketen als Quelladresse, bei eingehenden Paketen als Zieladresse verwendet. Es wird davon ausgegangen, dass jeder Host im Kundennetz eine eindeutige IP-Adresse besitzt.
IP-Adresse außerhalb	IP-Adresse / Subnetmask	Wird bei eingehenden Paketen als Quelladresse, bei ausgehenden Paketen als Zieladresse verwendet. Es wird davon ausgegangen, dass jeder erreichbare Host außerhalb des Kundennetz eine eindeutige IP-Adresse besitzt.
Protokoll	Integer (0 – 255)	Protokollnummer im Header von IP, spezifiziert Protokoll der Vermittlungs- oder Transportschicht (bei IPv4: Protocol; bei IPv6: next Header). Die Nummern sind bei der International Assigned Numbers Authority (IANA) registriert.
Port im Kundennetz	Integer (0 – 65.535)	Wird bei ausgehenden Paketen als Quellport, bei eingehenden Paketen als Zielport verwendet. Die Nummern sind bei der IANA registriert.
Port außerhalb	Integer (0 – 65.535)	Wird bei eingehenden Paketen als Quellport, bei ausgehenden Paketen als Zielport verwendet. Die Nummern sind bei der IANA registriert.
Dienstsepzifische Einschränkung	String	Abhängig vom einzelnen Dienst. Im Beispiel der URL-Filterung wäre der Parameter die entsprechende URL.
Anzahl Subnetze	Integer	Anzahl Teilnetze im Kundennetz, die durch die Firewall getrennt sind.

Tabelle 4.1: Objekte der Klasse FunctionalParameter

4.2.12 Abwehr dienstunabhängiger Angriffstechniken

Name: Grundschutz

Viele Angriffe nutzen nicht die Schwachstellen eines Servers oder Anwedungsprotokolls, sondern die Unzulänglichkeiten der Protokolle der Vermittlungs- und Transportschicht und deren Implementierung. Im wesentlichen sind dies die Protokolle IP, ICMP, TCP und UDP. Die Angriffe werden zu unterschiedlichen Zwecken genutzt: Scannen von Netzen nach offenen Ports, Sammeln von Informationen über die vorhandenen Betriebssysteme und Anwendungen, Denial of Service, Fälschen von IP-Adressen etc.

4.3 Instanzen der Klasse FunctionalParameter

In Tabelle 4.1 sind die Instanzen der Klasse FunctionalParameter beschrieben. Tabelle 4.2 zeigt welche FunctionalParameter von den einzelnen FBB verwendet werden. Die Objekte der Klasse FunctionalParameter dienen der Konfiguration eines FBB. Notwendige Parameter sind IP-Adressen, Ports,

	Default_Policy	Verbindungsaufbau	Verbindungsannahme	Dienstnutzung	Dienstangebot	Einschr_genDienst	Einschr_angDienst	Teilnetze	Verbergen	Remotezugang	Redundanz	Grundschutz
IP-Adresse im Kundennetz	-	x	x	-	-	-	-	x	x	x	-	x
IP-Adresse außerhalb	-	x	x	-	-	-	-	-	-	-	-	x
Protokoll	-	x	x	x	x	x	x	-	-	x	-	x
Port im Kundennetz	-	-	-	x	x	x	x	-	-	x	-	x
Port außerhalb	-	-	-	x	x	x	x	-	-	-	-	x
Dienstsepzifische Einschränkung	-	-	-	-	-	x	x	-	-	-	-	-
Anzahl Subnetze	-	-	-	-	-	-	-	x	-	-	-	-

Tabelle 4.2: Zusammenhang zwischen den Objekten der Klasse ServiceFunctionalBB und FunctionalParameter

Protokolle etc. Die aufgeführten Parameter erheben nicht den Anspruch auf Vollständigkeit. Je nach FBB und eingesetztem Produkt sind weitere Parameter notwendig.

Bei den Parametern "IP-Adresse im Kundennetz" und "IP-Adresse außerhalb" sind zwei Extremsituationen denkbar. In der einen erfolgt die Konfiguration eines FBB für jeden einzelnen Host im Kundennetz. In der anderen wird eine einzige Konfiguration eingerichtet, die für alle Hosts des Kundennetz gilt. Mehr noch als die IP-Adressen selbst spielt demnach die Granularität eine Rolle. Durch die Verwendung von Netzadressen und Subnetmasks kann sie variiert werden.

4.4 Instanzen der Klasse QoSServiceFunctionalBB und ihrer Unterklassen

4.4.1 Unterstützte IP-Adresse im Kundennetz

Name: unterst_IPAdr_Kunde

Description: Neben den IP-Adressen selber ist dieser Parameter vor allem durch die Granularität beeinflusst. Eine Konfiguration mit feiner Granularität kann die Kommunikationsinteressen und Sicherheitsanforderungen eines jeden einzelnen Hosts berücksichtigen, verursacht jedoch auch einen größeren Aufwand. Außerdem erhöht sich mit dem Umfang der Konfigurationsdaten auch die Unübersichtlichkeit und Fehleranfälligkeit.

Value Type: List of IP-Address/Subnetmask

Value Range: Beliebige Liste von IP-Adressen/Subnetzmasken aus dem Bereich, der dem Kunden zur Verfügung steht.

Parameter Type: basic

Calculation Metric: Kann direkt aus den Konfigurationsdaten gewonnen werden.

Provider-centric QoS: Bei einer zu feinen Granularität ist der Aufwand bei der Einrichtung einer Firewall sehr groß und während des Betriebs ist mit häufigen Änderungen zu rechnen. Auf Grund der beschränkten Kapazitäten des LRZ muss dieser Parameter deshalb eingeschränkt werden. In Abschnitt 3.5 wurden zwei Zonen mit ähnlichen Sicherheitsanforderungen vorgeschlagen, die als getrennte Teilnetze realisiert werden sollen. Von Seiten des Betreibers wird deshalb der Wertebereich des QoS-Parameters auf zwei mögliche Listen eingeschränkt:

- Gesamtes Kundennetz,
- internes Netz, Servernetz.

Bei beiden Werten kann davon ausgegangen werden, dass die Übersichtlichkeit der Konfiguration gewahrt bleibt und somit nur eine geringe Fehleranfälligkeit besteht. Werden im Kundennetz Server betrieben, so sollte auf jeden Fall die zweite Variante gewählt werden, da die Server sich von den übrigen Rechnern hinsichtlich der Sicherheitsanforderungen deutlich unterscheiden.

4.4.2 Unterstützte IP-Adresse außerhalb

Name: unterst_IPAdr_außen

Description: Neben den IP-Adressen selber ist dieser Parameter durch die Granularität beeinflusst. Wie beim QoS-Parameter unterst_IPAdr_Kunde (siehe Abschnitt 4.4.1) kann durch eine feinere Granularität eine bessere Anpassung an die Kommunikationsinteressen und Sicherheitsanforderungen erreicht werden. Mit dem Umfang der Konfiguration erhöht sich jedoch auch die Unübersichtlichkeit und Fehleranfälligkeit.

Value type: List of IP-Address/Subnetmask

Value range: Beliebige Liste von IP-Adressen/Subnetzmasken aus dem Bereich, der dem Kunden *nicht* zur Verfügung steht.

Parameter type: basic

Calculation metric: Kann direkt aus den Konfigurationsdaten gewonnen werden.

Provider-centric QoS: Bei einer zu feinen Granularität ist der Aufwand bei der Einrichtung einer Firewall sehr groß und während des Betriebs ist mit häufigen Änderungen zu rechnen. Auf Grund der beschränkten Kapazitäten des LRZ muss dieser Parameter deshalb eingeschränkt werden. Wie in Abschnitt 3.6 gezeigt wurde, ist die Vertrauenswürdigkeit des MWN gegenüber dem übrigen Internet nur unwesentlich größer. Trotzdem ist eine Unterscheidung zwischen diesen beiden Zonen sinnvoll. Darüber hinaus bietet es sich bei einigen Diensten an, ausschließlich Verbindungen zwischen dem Kundennetz und einem dezidierten Host im MWN zuzulassen. Dazu zählen Dienste, die auf Grund fehlerhafter und missbräuchlicher Nutzung schon heute eingeschränkt sind, oder die vom LRZ als zusätzliche Leistungen angeboten werden und außerhalb des MWN keine Rolle spielen (siehe Abschnitt 4.4.4). Auf diese Weise entstehen drei Listen von IP-Adressen, die auch miteinander kombiniert werden können:

- Einzelne Server im MWN,
- MWN (ohne Kundennetz),
- Internet (ohne Kundennetz).

Da die Zahl der einzelnen Server in der ersten Liste klein und für alle Institute einheitlich ist, kann davon ausgegangen werden, dass die Übersichtlichkeit der Konfiguration gewahrt bleibt und somit nur eine geringe Fehleranfälligkeit besteht. Die dienstspezifischen Konfigurationen sollen nur im Block angeboten werden, um den Aufwand für das LRZ bei Einrichtung und Betrieb der Firewall gering zu halten. Anpassungen während des Betriebs sind dann nötig, wenn eine Änderung bei einem dieser Dienste eintritt. Da die vorzunehmenden Änderungen für alle Firewalls gleich sind, ist dieser Vorgang für das LRZ leistbar.

4.4.3 Unterstützter Dienst beim Kunden

Name: unterst_Dienst_Kunde

Description: Die meisten Kunden betreiben in ihrem Netz eigene Server, auf die auch von außen zugegriffen werden darf. Die Firewall soll das Anbieten dieser Dienste unterstützen. Zu diesem Zweck muss die Firewall eine Verbindung von außen zum entsprechenden Dienst gestatten. Alle anderen Verbindungsversuche sollen geblockt werden. Die Dienste sind an Hand der Portnummern identifizierbar. Die meisten Dienste nutzen Nummern aus dem Bereich der Well Known Ports (0 - 1023), weniger gebräuchliche Dienste verwenden Nummern aus dem Bereich der Registered Ports (1024 - 49151). Nummern über 49151 werden in der Regel nur als dynamische oder private Ports genutzt [IANA].

Value type: List of Integer

Value range: Liste mit Werten zwischen 0 und 49151

Parameter type: basic

Calculation metric: Kann direkt aus den Konfigurationsdaten gewonnen werden. Zu Berücksichtigen sind Portnummern, auf denen eine Verbindung von außen nach innen aufgebaut werden kann.

Provider-centric QoS: Auf Grund der geringen Personalkapazitäten auf Seiten des Betreibers muss der Wertebereich eingeschränkt werden, um den Aufwand für Einrichtung und Betrieb der Firewall gering zu halten. Die von den Kunden angebotenen Dienste wurden mit Hilfe der Umfrage ermittelt und in zwei Diensteprofilen zusammengefasst (Profil 3 und 4, siehe Abschnitt 3.3). Profil 3 enthält Dienste, die aus dem Internet erreichbar sein sollen. Profil 4 enthält Dienste, die aus dem MWN erreichbar sein sollen. Profil 4 enthält im Vergleich zum Profil 3 zwei zusätzliche Dienste. Dabei handelt es sich um Radius sowie um Datei- und Druckdienste. Wie beim QoS-Parameter Unterstützte_IP-Adresse_außerhalb bereits ausgeführt wurde, soll mit dem Radiusdienst der Radius-Server des LRZ fest verknüpft werden. Hinsichtlich der Datei- und Druckdienste muss eine geeignete Lösung gefunden werden. Ergänzend muss die Firewall einen Zugriff vom MWN auf den Remoteserver beim Kunden gestatten. Der Betreiber bietet als mögliche Optionen an:

- Liste mit für Remotezugang notwendigen Ports,
- Liste mit Ports für die in Diensteprofil 3 enthaltenen Dienste und Remotezugang,
- Liste mit Ports für die in Diensteprofil 4 enthaltenen Dienste und Remotezugang.

Durch diese Auswahl bleibt der Aufwand beim Betreiber gering, die Konfiguration bleibt übersichtlich und damit wenig fehleranfällig. Generell gilt, dass das Kundennetz um so sicherer ist, je weniger

Dienste von außen erreichbar sind. Will der Kunde Dienste in seinem Netz anbieten, ist er für die Konfiguration und Pflege der Server selber verantwortlich.

4.4.4 Unterstützter Dienst außerhalb

Name: unterst_Dienst_außen

Description: Die Kunden wollen das Angebot des Internet und MWN nutzen. Zu diesem Zweck muss die Firewall eine Verbindung nach außen zu gewünschten Diensten gestatten. Alle anderen Verbindungsversuche zu unerwünschten Diensten sollen geblockt werden. Wie zum QoS-Parameter unterst_Dienst_Kunde (siehe Abschnitt 4.4.3) bereits ausgeführt wurde, werden die Dienste an Hand der verwendeten Portnummern identifiziert.

Value type: List of Integer

Value range: Liste mit Werten zwischen 0 und 49151

Parameter type: basic

Calculation metric: Kann direkt aus den Konfigurationsdaten gewonnen werden. Zu Berücksichtigen sind Portnummern, auf denen eine Verbindung von innen nach außen aufgebaut werden kann.

Provider-centric QoS: Das LRZ ist nicht in der Lage für jeden eine maßgeschneiderte Liste von Portnummern zu verwalten. Aus diesem Grund wurden aus den Ergebnissen der Umfrage zwei Diensteprofile gebildet, die die häufig genutzten oder für das MWN wichtigen Dienste umfassen (Profil 1 und 2, siehe Abschnitt 3.3). Profil 1 umfasst im Internet genutzte Dienste, Profil 2 im MWN genutzte Dienste. Profil 2 enthält neben den Diensten aus Profil 1 noch zusätzlich DNS, DHCP, ASF und TSM. Wie beim QoS-Parameter unterst_IPAdr_außen (siehe Abschnitt 4.4.2) dargestellt, sollen mit diesen Diensten die entsprechenden Server des LRZ fest verknüpft werden. Der Betreiber des Firewall-Dienstes bietet zwei Listen an:

- Liste mit Ports für die in Diensteprofil 1 enthaltenen Dienste,
- Liste mit Ports für die Dienste DNS, DHCP, ASF und TSM.

Da diese Listen für alle Kunden gleich sind, bleibt der Aufwand für das LRZ überschaubar, die Fehleranfälligkeit sollte gering sein.

4.4.5 Einschränkung bei Dienstnutzung

Eine mögliche Einschränkung ist abhängig vom Dienst, von den genutzten FBB und deren Realisierungen. Sie können nur qualitativ erfasst werden, eine Berechnung aus Basis-QoS-Parametern ist nur schwer möglich. Für jeden genutzten Dienst muss ein eigener QoS-Parameter eingeführt werden.

Name: genDienst_eingeschr

Description: Durch den FBB Einschr_genDienst (siehe Abschnitt 4.2.6) erfolgt eine gewollte Reduzierung der Funktionalität eines bestimmten Dienstes. Andere FBBs und deren Realisierungen können ebenfalls zu Einschränkungen führen. Als Beispiel diene aktives FTP: In diesem Modus baut der FTP-Server eine Datenverbindung zum Client auf. Der FBB Verbindungsaufbau (siehe

Abschnitt 4.2.2) erkennt nicht bei allen Realisierungen, dass die ankommende Datenverbindung zu einer bereits existierende FTP-Sitzung gehört. Auch durch den FBB Verbindungsannahme (siehe Abschnitt 4.2.3) wird der Verbindungsaufbau von außen auf den FTP-Client nicht gestattet. Deshalb ist bei verschiedenen Realisierungen statt aktivem nur passives FTP möglich.

Value type: Boolean

Value range: {uneingeschränkt, eingeschränkt}

Parameter type: aggregated

Unter Umständen ist es sinnvoll zusätzlich Informationen über die Art der Einschränkung mit aufzunehmen.

4.4.6 Einschränkung beim Dienstangebot

Eine mögliche Einschränkung ist abhängig vom Dienst, von den genutzten FBB und deren Realisierungen. Sie können nur qualitativ erfasst werden, eine Berechnung aus Basis-QoS-Parametern ist nur schwer möglich. Für jeden genutzten Dienst muss ein eigener QoS-Parameter eingeführt werden.

Name: angDienst_eingeschr

Description: Durch den FBB Einschr_angDienst (siehe Abschnitt 4.2.7) erfolgt eine gewollte Reduzierung der Funktionalität eines bestimmten Dienstes. Andere FBB und deren Realisierungen können ebenfalls zu Einschränkungen führen. Als Beispiel kann hier ebenfalls aktives FTP dienen – diesmal mit vertauschten Rollen.

Value type: Boolean

Value range: {uneingeschränkt, eingeschränkt}

Parameter type: aggregated

Unter Umständen ist es sinnvoll zusätzlich Informationen über die Art der Einschränkung mit aufzunehmen.

4.4.7 Wirksamkeit der Sicherheitsmaßnahme

Name: Wirksamkeit

Description: Die Wirksamkeit einer Sicherheitsmaßnahme hängt von der Realisierung des FBB und dem Einfluss anderer FBB ab. Die Wirksamkeit kann nur auf bereits bekannte Angriffe hin getestet werden. Dies kann mit Hilfe von Security-Scannern geschehen. Zu diesem Thema existiert bereits eine fertige Diplomarbeit [Pank 00]. Es ist empfehlenswert den Firewall-Dienst regelmäßig mit einem solchen Werkzeug zu testen.

Value type: Boolean

Value range: {wirksam, unwirksam}

Parameter type: basic

Calculation metric: Der Wert ergibt sich aus dem Ergebnis des Scans.

Es ist anzumerken, dass der Firewall-Dienst nicht die vom Kunden betriebenen Server umfasst. Eine fehlerhafte Konfiguration oder eine nicht behobene Sicherheitslücke auf einem Server lässt die beste Firewall “alt” aussehen.

FBB-Name \ Paket	1	1 (Alt.)	2	3	4
Default_Policy	x	x	x	x	x
Grundschutz	x	x	x	x	x
Verbindungsaufbau	x	x	x	x	-
Dienstnutzung (opt.)	(x)	(x)	(x)	(x)	-
Verbergen	x	x	x	x	-
Teilnetze	x	-	x	x	x
Remotezugang	x	x	x	x	x
Verbindungsannahme	-	-	x	x	x
Diensteangebot	-	-	x	x	x
Redundante Sicherheit	-	-	-	-	x
Einschr_genDienst	(x)	(x)	(x)	(x)	x
Einschr_angDienst	(x)	(x)	(x)	(x)	x
Anteil der Institute	**16 %**		**9 %**	**38 %**	

Tabelle 4.3: Die in den Firewall-Paketen verwendeten FBB

4.5 Firewall_Paket: QoSService

Name: Paket

Description: Aus den in Abschnitt 4.4 beschriebenen QoS-Parametern für die einzelnen FBBs wird nun ein qualitativer QoS-Parameter für den gesamten Firewall-Dienst aggregiert. Die Werte werden einzelne Paketlösungen repräsentieren, die den unterschiedlichen Kommunikationsinteressen und Sicherheitsanforderungen der Kunden entsprechen, aber gleichzeitig die Kapazitäten des LRZ nicht überfordern. Die Pakete sind so zusammengesetzt, dass sie den in Abschnitt 3.4 gebildeten Kundenprofilen entsprechen.

Value type: String

Value range: {Firewall-Paket 1, Firewall-Paket 2, Firewall-Paket 3, Firewall-Paket 4}

Parameter type: aggregated

Calculation metric: Die Werte ergeben sich aus der gezielten Auswahl einzelner QoS-Parameter des Abschnitts 4.4.

Vorgeschlagen sind vier Werte für den QoS-Parameter, also vier Paketlösungen. Zum Erreichen eines Wertes müssen nicht alle FBBs des Dienstes verwendet werden. Tabelle 4.3 gibt einen Überblich darüber, welche FBBs zum Erfüllen eines bestimmten QoS-Wertes notwendig sind. Das LRZ hat einge Einschränkungen und Regeln aufgestellt, die für das gesamte MWN gelten [Läpp 02]. Beispielsweise können nur wenige SMTP-Server direkt aus dem Internet erreicht werden. Für die meisten muss der Mail-Verkehr über die Mail-Relays des LRZ laufen. Dort findet eine Filterung statt. Aus diesem Grund können die beiden FBB Einschr_genDienst und Einschr_angDienst bei allen Firewall-Paketen auftreten. Ähnliches gilt für den FBB Dienstnutzung. So können beispielsweise die üblichen Filesharing-Protokolle im Internet nicht genutzt werden. Diese Einschränkungen gelten für alle Institute unabhängig davon, ob sie den Firewall-Dienst des LRZ nutzen oder nicht.

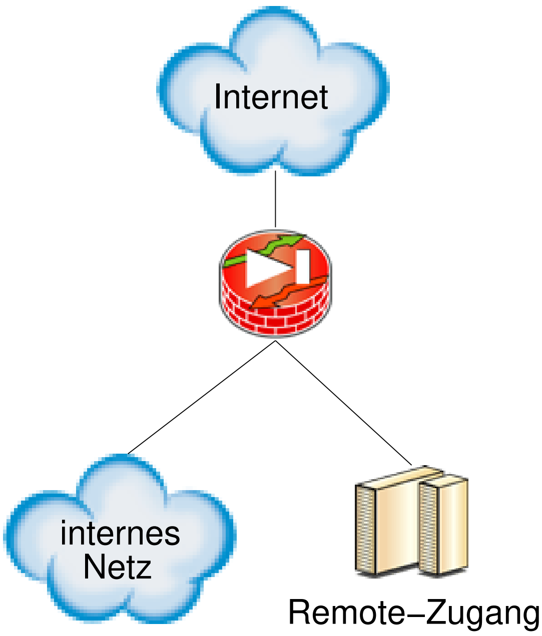

Abbildung 4.2: Firewall-Paket 1

nach von	internes Netz	Servernetz	einzelne Server im MWN	MWN/Internet
internes Netz	-	SSH für Konfiguration	DNS, opt. DHCP, ASF, TSM	alles, opt. Diensteprofil 1
Servernetz	kein Zugriff	-	DNS, opt. DHCP, ASF, TSM	kein Zugriff
MWN	kein Zugriff	Remote-Zugang	-	-
Internet	kein Zugriff	kein Zugriff	-	-

Tabelle 4.4: Kommunikationsprofil für Firewall-Paket 1

nach von	internes Netz	einzelne Server im MWN	MWN/Internet
internes Netz	-	DNS, opt. DHCP, ASF, TSM	alles, opt. Diensteprofil 1
MWN	Remote-Zugang	-	-
Internet	kein Zugriff	-	-

Tabelle 4.5: Kommunikationsprofil für Firewall-Paket 1a

4.5.1 Firewall-Paket 1

Das Institutsnetz besteht aus dem internen Netz und einem Rumpf-Servernetz. Beide Subnetze sind an die selbe Firewall (siehe Abbildung 4.2) angeschlossen. Die Firewall benötigt deshalb mindestens drei Interfaces (dreibeinige Firewall). Das Servernetz beherbergt nur einen von außen zugänglichen Server. Dabei handelt es sich um einen Server, der den Remote-Zugang zum Institutsnetz ermöglicht. Dieser Server ist nur aus dem MWN erreichbar. Für den Server ist eine öffentliche IP-Adresse vorgesehen. Für Angebote nach außen stehen die Server des LRZ oder anderer Einrichtungen zur Verfügung.

Auf das interne Netz kann nicht zugegriffen werden. Die Struktur des internen Netzes ist nach außen verborgen. Für die Nutzung von Diensten im MWN oder Internet können Verbindungen nach außen aufgebaut werden. Optional haben die Kunden die Möglichkeit, die Nutzung auf bestimmte Dienste einzuschränken. Das Kommunikationsprofil ist in Tabelle 4.4 dargestellt. Einen Überblick über die verwendeten FBB gibt Tabelle 4.3. Folgende QoS-Werte wurden gewählt:

unterst_IPAdr_Kunde: internes Netz, Servernetz,

unterst_IPAdr_außen: einzelne Server im MWN, MWN, Internet,

unterst_Dienst_Kunde: Liste mit für Remotezugang notwendigen Ports,

unterst_Dienst_außen, optional: Liste mit Ports für die in Diensteprofil 1 enthaltenen Dienste und/oder Liste mit Ports für die Dienste DNS, DHCP, ASF und TSM.

Dieses Firewall-Paket ist für die Institute gedacht die nach der Umfrage im Profil 1 zusammengefasst wurden. Dabei handelt es sich um 16 Prozent der Institute.

4.5.2 Firewall-Paket 1 (Alternative)

Diese Alternative ist für den Fall vorgesehen, dass das Einrichten eines VLAN zu aufwändig oder nicht möglich ist. Gedacht wurde dabei vor allem an die Gebäude, die zur Zeit noch eine 10Base5-Verkabelung besitzen. Zum Teil werden Server durch den direkten Anschluss an den Gebäude-Switch realisiert. Um diesen Aufwand zu umgehen, wird vorgeschlagen, den Remote-Server in das interne Netz zu verlegen (siehe Abbildung 4.3). Auch in diesem Fall wird das interne Netz nach außen verborgen. Abgesehen vom Remote-Server kann auf keine anderen Rechner von außen zugegriffen werden. Der Remote-Server ist nur aus dem MWN zu erreichen. Es ist jedoch zu bedenken, dass im Falle eines erfolgreichen Hacks des Remote-Servers das ganze interne Netz gefährdet ist. Andere Server müssen ausgelagert werden.

Bezüglich der Nutzung von Diensten im MWN oder Internet seitens der Mitglieder des Instituts gibt es keine Unterschiede zwischen den Alternativen. Das Kommunikationsprofil ist in Tabelle 4.5 dar-

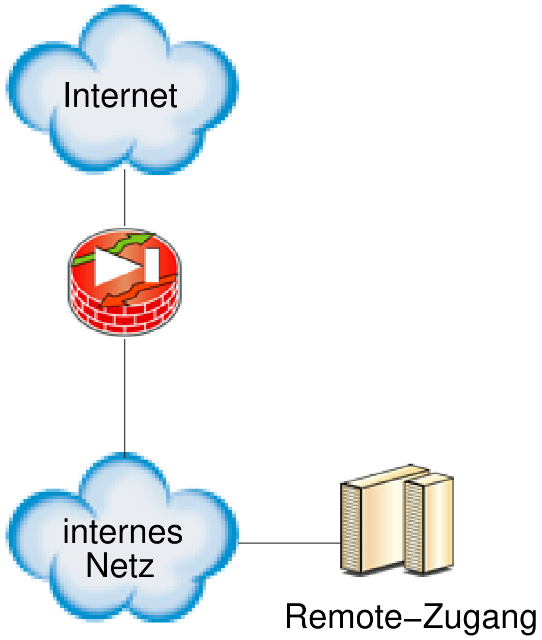

Abbildung 4.3: Firewall-Paket 1 (Alternative)

nach von	internes Netz	Servernetz	einzelne Server im MWN	MWN/Internet
internes Netz	-	SSH für Konfiguration, Diensteprofil 4	DNS, opt. DHCP, ASF, TSM	alles, opt. Diensteprofil 1
Servernetz	kein Zugriff	-	DNS, opt. DHCP, ASF, TSM	kein Zugriff
MWN	kein Zugriff	Remote-Zugang, Diensteprofil 4	-	-
Internet	kein Zugriff	kein Zugriff	-	-

Tabelle 4.6: Kommunikationsprofil für Firewall-Paket 2

gestellt. Einen Überblick über die verwendeten FBB gibt Tabelle 4.3. Folgende QoS-Werte wurden gewählt:

unterst_IPAdr_Kunde: internes Netz,

unterst_IPAdr_außen: einzelne Server im MWN, MWN, Internet,

unterst_Dienst_Kunde: Liste mit für Remotezugang notwendigen Ports,

unterst_Dienst_außen, optional: Liste mit Ports für die in Diensteprofil 1 enthaltenen Dienste und/oder Liste mit Ports für die Dienste DNS, DHCP, ASF und TSM.

4.5.3 Firewall-Paket 2

Im Gegensatz zum Paket 1 (siehe Abschnitt 4.5.1) ist das Servernetz zusätzlich für Rechner vorgesehen, die Dienste für das MWN anbieten. Angeboten werden können Dienste, die im Diensteprofil

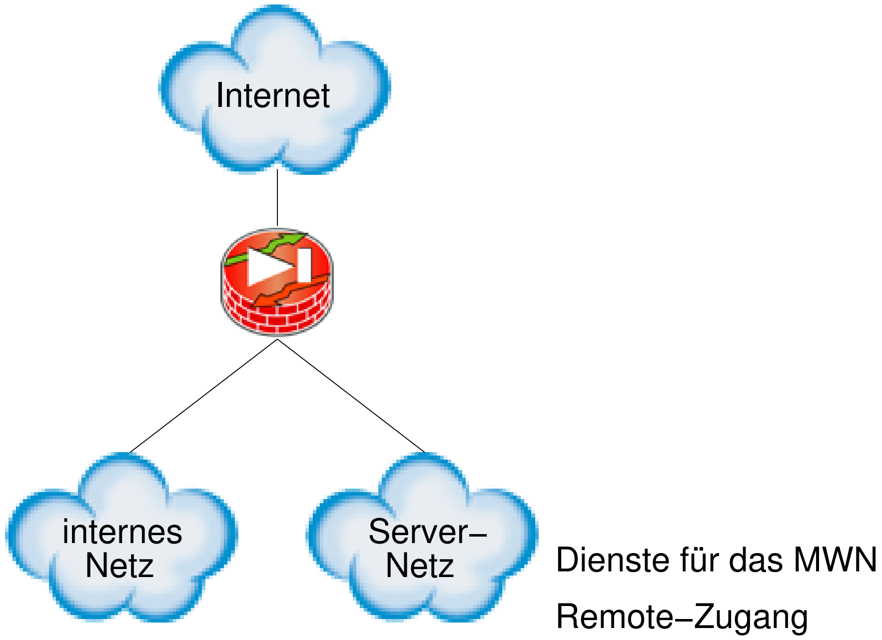

Abbildung 4.4: Firewall-Paket 2

4 (siehe Abschnitt 3.3) vorgesehen sind (siehe Abbildung 4.4). Dienste für das Internet können nicht angeboten werden, müssen deshalb auf externen Servern betrieben werden. Für die Abschottung des internen Netzes und die Nutzung von Diensten gilt das im Abschnitt 4.5.1 gesagte. Das Kommunikationsprofil ist in Tabelle 4.6 dargestellt. Einen Überblick über die verwendeten FBB gibt Tabelle 4.3. Folgende QoS-Werte wurden gewählt:

unterst_IPAdr_Kunde: internes Netz, Servernetz,

unterst_IPAdr_außen: einzelne Server im MWN, MWN, Internet,

unterst_Dienst_Kunde: Liste mit für Remotezugang notwendigen Ports und Liste mit Ports für die in Diensteprofil 4 enthaltenen Dienste,

unterst_Dienst_außen, optional: Liste mit Ports für die in Diensteprofil 1 enthaltenen Dienste und/oder Liste mit Ports für die Dienste DNS, DHCP, ASF und TSM.

Das Firewall-Paket 2 ist für Institute gedacht, die dem Profil 2 (siehe Abschnitt 3.4) angehören. Dies sind neun Prozent der befragten Institute. Zusätzlich muss berücksichtigt werden, dass u. U. nicht alle Institute mit der Einschränkung des Diensteprofils (siehe Abschnitt 3.2.8) leben können. Nach der Umfrage reduziert sich der Anteil dadurch auf sieben Prozent.

4.5.4 Firewall-Paket 3

Dieses Paket erweitert das vorhergehende, indem das Servernetz nocheinmal weiter geöffnet wird. Es kann nun auch Server aufnehmen die Dienste für das Internet anbieten (siehe Abbildung 4.5). Angeboten werden können Dienste die den Diensteprofilen 3 und 4 (siehe Abschnitt 3.3) entsprechen. Die Nutzung von externen Servern ist in diesem Fall nicht mehr notwendig, kann aber dennoch genutzt werden. Für die Abschottung des internen Netzes und die Nutzung von Diensten gilt das im Abschnitt

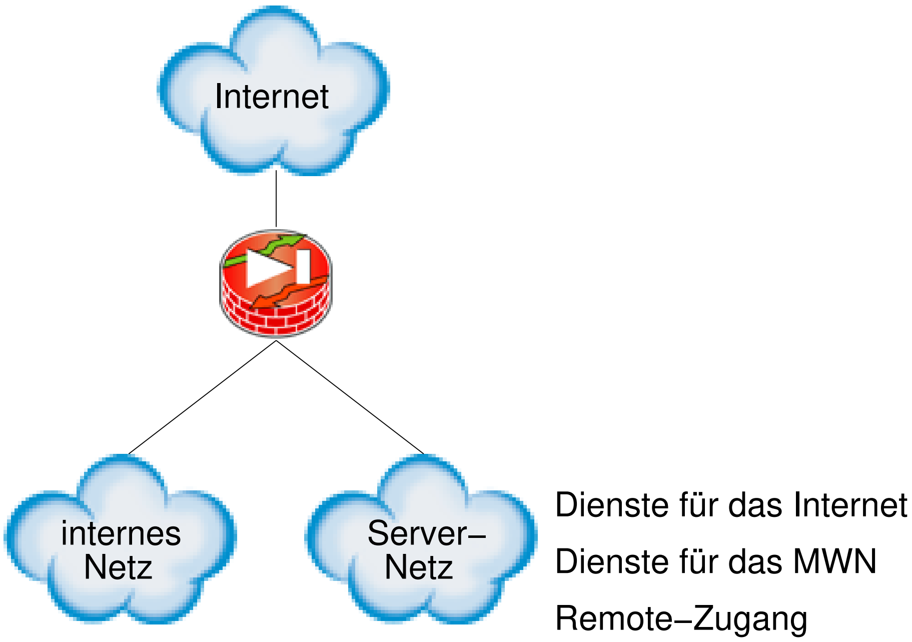

Abbildung 4.5: Firewall-Paket 3

nach / von	internes Netz	Servernetz	einzelne Server im MWN	MWN/Internet
internes Netz	-	SSH für Konfiguration, Diensteprofil 4	DNS, opt. DHCP, ASF, TSM	alles, opt. Diensteprofil 1
Servernetz	kein Zugriff	-	DNS, opt. DHCP, ASF, TSM	kein Zugriff
MWN	kein Zugriff	Remote-Zugang, Diensteprofil 4	-	-
Internet	kein Zugriff	Diensteprofil 3	-	-

Tabelle 4.7: Kommunikationsprofil für Firewall-Paket 3 und 4

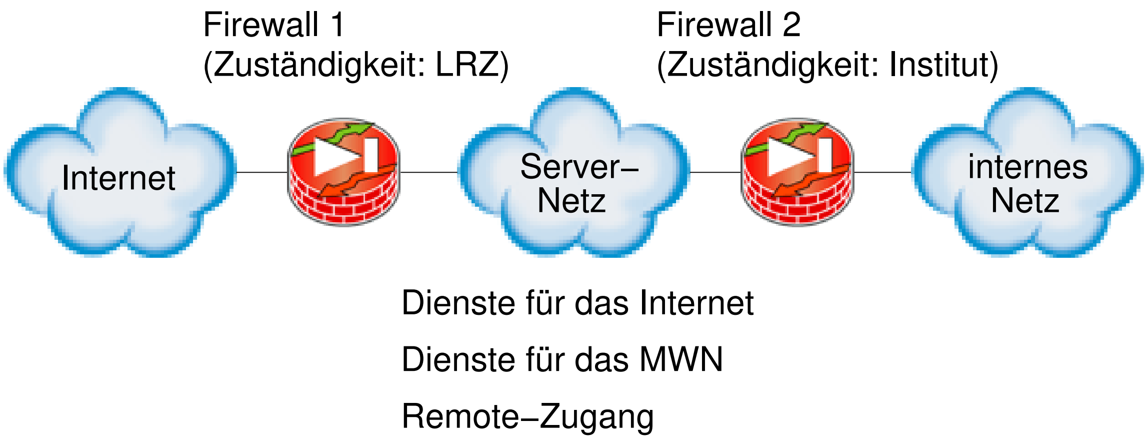

Abbildung 4.6: Firewall-Paket 4

4.5.1 gesagte. Das Kommunikationsprofil ist in Tabelle 4.7 dargestellt. Einen Überblick über die verwendeten FBB gibt Tabelle 4.3. Folgende QoS-Werte wurden gewählt:

unterst_IPAdr_Kunde: internes Netz, Servernetz,

unterst_IPAdr_außen: einzelne Server im MWN, MWN, Internet,

unterst_Dienst_Kunde: Liste mit für Remotezugang notwendigen Ports, Liste mit Ports für die in Diensteprofil 4 enthaltenen Dienste, Liste mit Ports für die in Diensteprofil 3 enthaltenen Dienste,

unterst_Dienst_außen, optional: Liste mit Ports für die in Diensteprofil 1 enthaltenen Dienste und/oder Liste mit Ports für die Dienste DNS, DHCP, ASF und TSM.

Dieses Paket ist für Institute vorgesehen, die dem Profil 3 (siehe Abschnitt 3.4) entsprechen. Dabei handelt es sich um 38 Prozent der Institute. Auch hier gibt es eine Einschränkung durch die Diensteprofile, die nach der Umfrage nicht von allen Instituten akzeptiert wird. Deshalb kann sich der Anteil auf 34 Prozent reduzieren.

4.5.5 Firewall-Paket 4

Der verhältnismäßig große Anteil der Institute des Profils 3 rechtfertigt es, ein weiteres Firewall-Paket zu schnüren. Statt einer einzigen Firewall wird eine zweite Firewall vorgesehen, die zwischen Servernetz und dem internen Netz angebracht wird (siehe Abbildung 4.6). Über die erste Firewall ist nur noch die DMZ direkt angeschlossen. Das LRZ übernimmt allerdings nur die Konfiguration der ersten Firewall, für die zweite können nur Produktvorschläge gemacht werden. Durch die zweite Firewall haben die Institute die Möglichkeit das interne Netz noch besser abzuschotten. Denkbar sind die erzwungene Nutzung von Proxies, URL-Filtering oder Content-Filtering. Falls eine der beiden Firewalls ausfallen sollte, bleibt durch die verbleibende Firewall ein gewisser Schutz erhalten. Für das LRZ reduziert sich der Konfigurations-Aufwand bei der ersten Firewall.

Kapitel 5

Realisierung des Firewall-Dienstes

Im Kapitel 2 wurden einige Produkte und Konzepte betrachtet, die für den Firewall-Dienst von Bedeutung sind. Weil die bisher eigenständigen Firewall-Lösungen der Institute meist auf Linux basieren (siehe Tabelle 3.13), wurden die Möglichkeiten dieses Betriebssystems untersucht. Die vom LRZ betrieben Router (Cisco Catalyst 6509) besitzen umfangreiche Filtermöglichkeiten und wurden deshalb ebenfalls betrachtet. Darüber hinaus wurden eigenständige kommerzielle Firewall-Produkte in den Überblick einbezogen. Schließlich wurden die Firewall-Konzepte der Universitäten Passau und Karlsruhe analysiert. Ziel war es nicht eine Evaluation und Produktauswahl vorzunehmen. Vielmehr sollte ein Überblick gewonnen werden über die aktuellen Techniken und Verfahren, die für den zu entwickelnden Firewall-Dienst relevant sein können.

In diesem Kapitel sollen auf dieser Basis Realisierungsvorschläge für die in Kapitel 4 eingeführten Service Functional Building Blocks gemacht werden. Dies geschieht im Abschnitt 5.1.

Für den Betrieb des Firewall-Dienstes ist außerdem ein Betriebskonzept notwendig. Dafür werden in Abschnitt 5.3 für das Management relevante Aspekte betrachtet. Dabei werden drei Managementdimensionen berücksichtigt:

- Ressourcen
- Lebenszyklusphasen
- Funktionsbereiche

Aufgrund dieser Analyse können dann notwendige Managementprozesse identifiziert und beschrieben werden (siehe Abschnitt 5.4). Dabei ist zu berücksichtigen, dass sich das Management des Firewall-Dienstes in die Ablauf- und Aufbauorganisation des LRZ einfügen muss. Dies bedeutet, dass für das LRZ geeignete Policies und Betriebsregeln erstellt werden müssen. Für die konkrete Umsetzung sind entsprechende Workflows notwendig. Die Erstellung von Policies und Workflows setzt genaue Kenntnisse der Strukturen des LRZ voraus und kann deshalb hier nicht geleistet werden.

5.1 Möglichkeiten zur Realisierung der ServiceFunctionalBB

5.1.1 Default Policy

Der ServiceFunctionalBB Default Policy (siehe Abschnitt 4.2.1) soll grundsätzlich alle Pakete verwerfen. Dadurch kann sichergestellt werden, dass bei einer Fehlkonfiguration keine unerwünschten Pakete die Firewall passieren können. Das Verwerfen eines Paketes kann auf zweierlei Weisen realisiert werden. Zum einen kann dies kommentarlos geschehen (DROP), zum anderen durch eine Nachricht, die den Absender über das Verwerfen des Pakets informiert (REJECT).

In diesem Zusammenhang ist es wichtig zu verstehen, wie ein normaler Host auf eine Anfrage nach einem nicht vorhandenen Dienst reagiert. Bei einem auf TCP basierenden Dienst beginnt der Verbindungsaufbau mit einem Paket, bei dem das SYN-Flag gesetzt ist. Ist der gewünschte Dienst beim Host nicht vorhanden sendet er ein Reset-Paket mit gesetztem ACK- und RST-Flag zurück. Bei einem nicht angebotenen UDP-Dienst wird auf den Request eine ICMP-Nachricht (Typ: destination unreachable, Code: port unreachable) zurückgesendet.

Es ist umstritten, wie eine Firewall reagieren soll, wenn sie ein Paket verwirft.

Folgende Argumente sprechen für ein DROP:

- Jede Antwort – auch eine Fehlermeldung – liefert einem Angreifer unter Umständen Informationen über Betriebssystem und Firewall-Software.
- Antwortpakete können als Teil eines Denial-of-Service-Angriff eingesetzt werden. Einerseits reduzieren sie die eigene Bandbreite. Andererseits kann ein Angreifer die Absendeadresse fälschen, so dass die Fehlernachrichten an den rechtmäßigen Besitzer der IP-Adresse gehen und sein Netz unnötig belasten.
- Manche Portscanner warten auf Reaktionen der gescannten Rechner. Bleiben Reaktionen aus kann dies den Scanvorgang erheblich verzögern.

Folgende Argumente sprechen für ein REJECT:

- Da ein normaler Host immer Fehlermeldungen generiert, ist ein REJECT die unauffälligere Methode. Ein kommentarloses Verwerfen eines Pakets deutet hingegen auf eine Firewall hin. Allerdings muss die Firewall den REJECT richtig ausführen. Der im Linux-Kernel 2.2 vorhandene Paketfilter “ipchains” reagierte auch auf TCP-Anfragen mit einer ICMP-Fehlernachricht, statt mit Reset.
- Verschiedene Client-Programme blockieren während sie auf eine Antwort warten.
- In Zusammenhang mit der dynamischen Vergabe von IP-Adressen ist ein REJECT häufig die einzige Möglichkeit einem Client klar zu machen, dass sich die Adresse eines bestimmten Servers geändert hat.

Wird ein Dienst für das Internet angeboten, so ist auch klar, dass es einen Rechner gibt. Die Verwendung von DROP deutet darauf hin, dass zusätzlich zum Server eine Firewall vorhanden sein muss. Die meisten Scanner zeigen dies auch sofort an. (Der Security-Scanner Nessus beispielsweise markiert gesperrten Ports als “filtered”.) Die Information über das Vorhandensein einer Firewall, lässt andere Informationen wie z. B. das eingesetzte Betriebssystem eher zweitranging erscheinen. Die aktuellen Scanner kommen zudem mit der durch DROP verursachten Verzögerung gut zu Recht. Die weit verbreitete Meinung, ein DROP sei grundsätzlich sicherer als ein REJECT, kann deshalb nicht bestätigt werden.

Die zunehmende Zahl von Netzwerk-Scans und DoS-Angriffen wirft allerdings die Frage auf, ob noch immer – sozusagen aus Höflichkeit – auf jedes Paket reagiert werden sollte. Die damit verbundene Belastung des eigenen Netzes kann einen DROP durchaus als bessere Alternative erscheinen lassen. Zudem sind im MWN die IP-Adressen statisch vergeben, so dass evtl. Probleme mit dynamischen IP-Adressen nicht auftreten können. Aus diesen Gründen soll für das Firewallkonzept DROP statt REJECT standardmäßig verwendet werden.

5.1.2 Verbindungsaufbau von Client nach außen

Nach den Vorgaben des FBB (Abschnitt 4.2.2) wird im Folgenden angenommen, dass Verbindungen nur von innen nach außen (vom Client zum Server) aufgebaut werden dürfen, in der anderen Richtung blockiert die Firewall solche Versuche. Die Realisierung des FBB ist mit statischen oder dynamischen Paketfiltern möglich.

Statische IP-Paket-Filter

Einige Produkte haben bislang nur einen statischen IP-Paket-Filter implementiert. Beispielsweise nutzen noch viele kommerzielle und freie Linux-Firewall-Lösungen den Kernel 2.2, der noch kein Stateful Filtering unterstützt. In diesem Fall hat man die Möglichkeit bei auf TCP basierenden Anwendungen die Flags im TCP-Header in die Filterregeln mit einzubeziehen. Ein Verbindungsaufbau bei TCP wird mit einem Paket mit gesetztem SYN-Flag (und nicht gesetztem ACK-Flag) signalisiert. Man kann sichergestellen, dass ein Verbindungsaufbau nur von innen aus stattfindet, wenn alle SYN-Pakete von außen blockiert werden. Bei nicht verbindungsorientierten Protokollen (UDP, ICMP) ist dies nicht möglich. Die Situation von auf UDP basierenden Diensten lässt sich etwas entschärfen, wenn man den Zugriff auf bestimmte Server beschränkt. Einen zuverlässigen Schutz bietet dies jedoch nicht, da sich die Source Address im IP-Header leicht fälschen lässt und so die Firewall überwunden werden kann.

Bei vielen Diensten wählt der Client für eine Verbindung aus dem Bereich der unprivilegierten Ports (1024 bis 65535) einen Wert als Source Port aus. Die Antworten des Server benutzen diesen Port entsprechend als Destination Port. Bei statischen Paketfiltern muss deshalb für die meisten Dienste der Bereich der unprivilegierten Ports geöffnet werden und zwar als Quellport für Pakete vom internen Netz nach außen und als Zielport für Pakete von außen nach innen. Das Öffnen dieses großen Bereichs ist insbesondere dann problematisch, wenn im Subnetz des Client Serverdienste aktiv sind, die an einem solchen unprivilegierten Port auf Anfragen warten. Man muss deshalb bei rein statischen Paketfiltern große Löcher in der Firewall öffnen.

- Unprivilegierte Ports: Wird bei einem Dienst ein beliebiger unprivilegierter Port vom Client als Quellport verwendet, so muss vom Prinzip der ganze Bereich der unprivilegierten Ports für Antwortpakete des Servers freigegeben werden.
- Beliebige Zieladressen: Ist bei einem Dienst (z. B. WWW) der Zugriff auf beliebige Server im Internet möglich, so müssen Antwortpakete von beliebigen IP-Adressen die Firewall passieren können.

Dynamische IP-Paket-Filter

Bei vielen Paketfiltern gibt es die Möglichkeit der dynamischen Filterung (siehe Abschnitt 2.1.2). Bei Linux (ab Kernel 2.4) ist sie unter dem Namen Stateful Filtering (siehe Abschnitt 2.2.3) bekannt, bei Cisco Routern unter Reflexive Access Control Lists (siehe Abschnitt 2.3.4).

Im Gegensatz zu statischen sind bei dynamischen Filtern keine der beschriebenen großen Löcher in der Firewall notwendig. Statt dessen wird für die Antwortpakete erst zu dem Zeitpunkt eine entsprechende Lücke in der Firewall geschaffen, zu dem eine neue Verbindung initiiert wird. Durch diese Lücke können nur Pakete mit zur jeweiligen Verbindung passenden Adressen und Ports. Sobald die Verbindung beendet ist, wird die Lücke wieder geschlossen.

Auch das dynamische Filtering hat einen Nachteile, der jedoch nicht im Bereich der Sicherheit liegt, sondern die Nutzung von Diensten einschränkt. Manche Dienste, die mehrere Verbindungen nutzen, benötigen Hilfsroutinen, damit sie mit dynamischer Filterung funktionieren. Dies wurde an Hand von aktivem FTP erläutert (siehe Abschnitt 2.1.2), andere Beispiele sind IRC, ICQ, RealAudio und H.323 (z. B. Netmeeting). Die dynamischen Paketfilter bringen nicht für alle diese Dienste entsprechende Hilfsroutinen mit.

Berücksichtigung der Kundenanforderungen

Das Fehlen entsprechender Hilfsroutinen bei einem dynamischen IP-Paket-Filter bedeutet, dass manche Dienste nicht oder nur eingeschränkt genutzt werden können. Dazu hat die Umfrage bei den Instituten ergeben, dass nur etwas mehr als die Hälfte eine Beschränkung der Dienste akzeptieren möchten. Günstiger ist die Situation bei kleinen Instituten (bis zu 32 Rechner); hier sind es etwa zwei Drittel (siehe Tabelle 3.17). Betrachtet man die von den Instituten häufig genutzten Dienste (siehe Abschnitt 3.3, Profile 1 und 2), so ist abgesehen von FTP kein Dienst dabei, der zusätzliche Hilfsroutinen benötigt. Für FTP bringen alle bekannten dynamischen Paketfilter eine entsprechende Unterstützung mit.

5.1.3 Verbindungsaufbau von außen auf Server

Nach den Vorgaben des FBB (Abschnitt 4.2.3) wird im Folgenden angenommen, dass Verbindungen von außen auf Server im Kundennetz aufgebaut werden dürfen. Diese Server befinden sich in einem eigenen Subnetz (Servernetz). Der Versuch eines Verbindungsaufbaus aus dem Servernetz heraus wird von der Firewall blockiert. Die Realisierung des FBB ist mit statischen oder dynamischen Paketfiltern möglich.

Statische IP-Paket-Filter

Steht nur ein statischer Paketfilter zur Verfügung muss man sich mit dessen Möglichkeiten begnügen. In diesem Fall müssen ähnlich wie bei der Nutzung von Diensten die unprivilegierten Ports (1024 bis 65535) freigegeben werden. Zum einen als Quellports für Pakete von außen nach innen, zum anderen als Zielports für Antwortpakete aus dem Servernetz zurück. Im Zusammenhang mit der in Abschnitt 5.1.4 dargestellten Beschränkung bei der Nutzung von Diensten im Internet, ist dies ein Problem, insbesondere dann, wenn man den Nutzern im eigenen Netz nicht vertrauen kann.

Durch das Öffnen der unprivilegierten Ports können zusätzlich Server im Internet erreicht werden, die auf einem solchen Port auf Anfragen warten. Allerdings lässt die Firewall nur Pakete nach außen, die als Quellport den Port einer der Serverdienste nutzen. Dazu ist in den meisten Fällen ein Fälschen der Paketheader notwendig. Bei auf TCP basierenden Diensten hat man die Möglichkeit einen von einem Client im lokalen Netz ausgehenden Verbindungsaufbau zu blockieren, indem man an der Firewall Pakete mit gesetztem SYN-Flag (und nicht gesetztem ACK-Flag) herausfiltert.

Eine zusätzliche Möglichkeit wäre es, die Pakete eines Dienstes nur dann die Firewall passieren zu lassen, wenn sie vom bzw. zum entsprechenden Server kommen. Dazu müssten die Filteregeln dahingehend verfeinert werden, dass statt der Netzadresse des LAN die konkreten Hostadressen der einzelnen Server verwendet werden. Allerdings können auch die IP-Adressen in den Headern der Pakete gefälscht werden.

Berücksichtigung der Betreiberanforderungen

Da Anzahl und Art der Server in jedem Institut unterschiedlich sind, kann die Konfiguration konkreter Hostadressen nicht mehr Bestandteil eines standardisierten Firewalldienstes sein. Bei Veränderungen in der Serverstruktur der Institute müssten die Konfigurationen der Firewalls auch ständig angepasst werden. Der damit verbundene Aufwand kann zur Zeit vom LRZ nicht geleistet werden.

Dynamische IP-Paket-Filter

Der Einsatz von dynamischen Paketfiltern ist auch im Zusammenhang mit dem Angebot von Serverdiensten denkbar. In diesem Fall werden Anfragen aus dem Internet bzw. dem MWN an Server im Institutsnetz gerichtet. Die Server im Institutsnetz können selbst nur dann Pakete verschicken, wenn zuvor eine entsprechende Verbindung von außen initiiert wurde.

Eine besondere Bedeutung haben auch hier die Hilfsroutinen der dynamischen Paketfilter. Als Beispiel sei angenommen, dass im Institut ein FTP-Server betrieben wird, der auch im aktiven Modus arbeiten soll. Die im aktiven Modus vom Server aus aufgebauten Verbindungen müssen von der Firewall durchgelassen werden, sofern sie in Beziehung zu einer etablierten Steuerungsverbindung stehen. Das Problem der dynamischen Paketfilterung liegt auch hier in der Notwendigkeit von Hilfsroutinen bei einigen Diensten.

Berücksichtigung der Kundenanforderungen

Steht für einen bestimmten Dienst keine solche Hilfsroutine zur Verfügung, bedeutet dies für die Kunden eine Einschränkung beim Dienstangebut. Die in Abschnitt 3.3 aufgeführten Dienste, die von den Instituten angeboten werden (Profile 3 und 4), kommen jedoch mit der dynamischen Paketfilterung zurecht. Alleine FTP benötigt Hilfsroutinen, die aber bei den bekannten dynamischen Filtern zur Verfügung stehen. Bei Diensten, die für das Internet angeboten werden, benutzen 82 Prozent der Institute ausschließlich die zum Profil 3 gehörenden Dienste (siehe Tabelle 3.23, 4. Spalte). Bei Diensten für das MWN sind es 75 Prozent (siehe Tabelle 3.23, 5. Spalte). Folglich ist nur bei wenigen Instituten mit angebotenen Diensten zu rechnen, die auf Grund fehlender Hilfsroutinen nicht funktionieren.

5.1.4 Nutzung ausgewählter Dienste

Zur Realisierung dieses FBB eignen sich statische Paketfilter. Aufbauend auf der Default-Policy wird durch einen Satz statischer Filterregeln der Zugriff auf bestimmte Dienste im Internet und im MWN ermöglicht. In Abschnitt 3.3 wurden Diensteprofile aufgestellt. Diese umfassen Dienste, die von mehr als zehn Prozent der Institute im Internet und im MWN genutzt werden oder eine wichtige Funktion im MWN erbringen (Profile 1 und 2). Die Auswertung der Umfrage hat ergeben, dass rund 80 Prozent der befragten Institute nur diese Dienste nutzen (siehe Tabelle 3.23, Spalten 2 und 3, Zeile 2), bei den Instituten mit wenigen Rechnern (bis zu 32) sind es sogar alle (selbe Tabelle, Zeile 3). Es kann deshalb davon ausgegangen werden, dass dieses Diensteprofil für die meisten Institute geeignet ist. Dem steht das Ergebnis aus Tabelle 3.17 (Zeile 2) gegenüber. Danach sind nur etwas mehr als die Hälfte der Institute damit einverstanden, wenn der Zugriff auf das Internet zukünftig auf bestimmte Dienste beschränkt würde. Etwas günstiger sind die Zahlen für kleine Institute (bis zu 32 Rechner). Von diesen sind etwa zwei Drittel mit einer Beschränkung einverstanden (selbe Tabelle, Zeile 3).

5.1.5 Angebot ausgewählter Dienste

Zur Realisierung des Service FunctionalBB Dienstangebot (siehe Abschnitt 4.2.7) wird ein statischer Paketfilter vorgeschlagen. Daneben wird auf die Möglichkeit eingegangen, das Dienstangebot eines Kunden auf fremde Server auszulagern. Dies stellt zwar keine Realisierung des FBB dar, ist jedoch eine mögliche Alternative. Beim Firewall-Paket 1 (siehe Abschnitt 4.5.1) muss das Dienstangebot sogar auf externe Server ausgelagert werden.

Statische IP-Paket-Filter

Ausgehend von der Default-Policy wird durch einen Satz statischer Filterregeln der Zugriff aus dem Internet und aus dem MWN auf Dienste im lokalen Netz ermöglicht. Dabei ist der Zugriff von außen auf das VLAN für das Servernetz beschränkt. Der Zugriff auf das VLAN für das interne Netz soll grundsätzlich nicht möglich sein. In Abschnitt 3.3 wurden Diensteprofile aufgestellt. Diese umfassen Dienste, die von mehr als zehn Prozent der Institute für das Internet und MWN angeboten werden oder eine wichtige Funktion im MWN erbringen (Profile 3 und 4). Der statische IP-Paket-Filter wird so konfiguriert, dass nur diese Dienste von einem Kunden angeboten werden können.

Auslagerung des Dienstangebots

Es treten bei allen Servern beinahe regelmäßig Sicherheitslücken auf. Dazu passende Würmer, Exploits oder andere Maleware sind im Internet dann schnell verfügbar. Regelmäßiges Einspielen von Updates und Sicherheits-Patches ist deshalb unerlässlich. Aus diesem Grund ist der Betrieb eines Servers mit einem nicht zu unterschätzenden Aufwand verbunden. Nicht alle Institute sind dazu in der Lage. Es ist jedoch möglich das eigene Dienstangebot auf Server einer anderen Institution auszulagern. So bietet das LRZ für verschiedene Dienste Serverkapazitäten an. Sind die Möglichkeiten des LRZ nicht ausreichend, ist es auch denkbar, dass sich Institute zusammenschließen und gemeinsam geeignete Server betreiben. Unter Umständen können kleine Institute dabei von den Kapazitäten großer Institute profitieren. Ein zusätzlicher Vorteil dieser Vorgehensweise ist, dass nicht jedes Institut für sich alleine die Server pflegen muss, sprich Updates und Sicherheits-Patches einspielen und die Konfiguration “wasserdicht” machen. Das LRZ bietet folgende Serverkapazitäten an:

- Hosten von WWW-Seiten, auch als virtuelle Server;
- Nutzung der Mail-Server mit der Möglichkeit benutzerdefinierte Mailadressen (auch für Domain-Teil) einzurichten;
- Bereitstellung eines anonymen FTP-Servers;
- DNS-Server
- DHCP-Server

Bei den für das Internet häufig angebotenen Diensten ergibt sich folgendes Bild:

WWW: Das LRZ bietet hierfür grundsätzlich die Möglichkeit zur Auslagerung. Allerdings werden nur geringe Servererweiterungen unterstützt.

E-Mail: Der E-Mail-Service des LRZ bietet weitreichende Konfigurationsmöglichkeiten. Der Zugriff auf das Postfach ist per POP und IMAP möglich. Auch das Einrichten von Maillisten ist möglich. Laut Umfrage betreiben 70 Prozent der befragten Institute trotzdem einen eigenen SMTP-Server. Seit 1998 ist der Zugriff aus dem Internet auf SMTP-Server im MWN beschränkt, da auf Grund fehlerhafter Konfiguration viele Mail-Server als Spam-Relays verwendet werden konnten. Nur noch einige wenige, zuverlässige Server können aus dem Internet direkt erreicht werden. Ansonsten müssen alle eingehenden Mails über die Mailrelays des LRZ laufen.

FTP: Das LRZ bietet die Möglichkeit der Einrichtung eines anonymen FTP-Servers. Für Uploads können spezielle Verzeichnisse eingerichtet werden. Für den Zugriff per FTP auf Daten des internen Netzes hat dies keine Auswirkungen.

DNS: Für die Verwaltung der Domains (uni-muenchen.de, tu-muenchen.de etc.) ist das LRZ verantwortlich. Subdomains können von Hochschulen, Fakultäten, Instituten oder Lehrstühlen selbst verwaltet werden. Da bei der Konfiguration von DNS-Servern häufig Fehler gemacht werden, haben nicht alle eine Port-53-Berechtigung nach außen. Anfragen müssen deshalb in der Regel an MWN-interne DNS-Server gerichtet werden.

Telnet/SSH: Telnet und SSH wird genutzt um von außen auf Rechner im Institutsnetz zuzugreifen.

Berücksichtigung der Kundenanforderungen

Statische IP-Paket-Filter: Es werden die Dienste der Profile 3 und 4 unterstütz. Die Auswertung der Umfrage hat ergeben, dass 82 Prozent bzw. 75 Prozent der befragten Institute nur diese Dienste anbieten (siehe 3.23, Spalten 4 und 5, Zeile 2). Somit kann davon ausgegangen werden, dass diese Diensteprofile für die meisten Institute geeignet sind. Berücksichtigt man zusätzlich die Anzahl der am Institutsnetz angeschlossenen Rechner, so stellt man fest, dass Institute mit wenigen Rechnern sich fast ausschließlich auf diese Dienste beschränken (selbe Tabelle, Zeile 3). In größeren Institute finden sich andere Dienste hingegen häufiger.

Auslagerung des Dienstangebots: Nach der Umfrage wissen über 90 Prozent der befragten Institute um die Möglichkeit, die das LRZ für die Auslagerung bestimmter Dienste bietet (siehe Tabelle 3.21). Im Schnitt sind nur etwas mehr als die Hälfte der Institute bereit, diese Möglichkeit zu nutzen. Allerdings ergeben sich große Unterschiede bezüglich der Größe der Institute. Bei den kleinen Instituten ist die Bereitschaft deutlich größer – sie liegt hier bei 83 Prozent (siehe Tabelle 3.22).

5.1.6 Einschränkung genutzter und angebotener Dienste

Durch die ServiceFunctionalBB “Einschränkung genutzter Dienste” und “Einschränkung angebotener Dienste” (Abschnitte 4.2.6 und 4.2.7) soll die Funktionalität eines bestimmten Internet-Dienstes eingeschränkt werden. Zu diesem Zweck sind entsprechende Proxies notwendig.

Im Kapitel 2 wurden verschiedene Realisierungsmöglichkeiten vorgestellt. In den Abschnitten 2.2.6 und 2.2.7 wurden auf der Basis von Linux Lösungen für SMTP und HTTP vorgestellt. Die Proxy-Ansätze der Cisco-Router finden sich in Abschnitt 2.3.5. Am umfangreichsten und einfach zu nutzen sind die Proxies der vorgestellten Firewall-Produkte Astaro , PIX und Firewall-1 (siehe Abschnitt 2.4). Sie bieten für viele Anwendungen Möglichkeiten zur Filterung des Anwendungsprotokolls und der transportierten Daten.

Eine Möglichkeit bietet sich außerdem durch vom LRZ oder anderen Instituten betriebene Proxies. Das LRZ betreibt Proxies für HTTP, HTTPS, FTP, MMS und RTSP, sowie einen Socks-Proxy. Von anderen Instituten werden hauptsächlich WWW-Proxies betrieben, die in der Regel ohne Beschränkung genutzt werden dürfen.

Seit 1998 ist außerdem der Zugriff aus dem Internet auf SMTP-Server im MWN beschränkt, da auf Grund fehlerhafter Konfiguration viele Mail-Server als Spam-Relays verwendet werden konnten. Nur noch einige wenige, zuverlässige Server können aus dem Internet direkt erreicht werden. Ansonsten müssen alle eingehenden Mails über die Mailrelays des LRZ laufen. Dabei werden die Mail-Adressen überprüft. Seit 2001 werden E-Mails mit ausführbaren Attachments von den Mailrelays des LRZ zurückgewiesen.

Wird für einen Dienst ein Proxy betrieben, so kann ein direkter Zugriff aus dem internen Netz auf das Internet für diesen Dienst durch die Firewall verhindert werden. Dadurch lässt sich die Nutzung des Proxy erzwingen.

5.1.7 Teilnetze für Rechner mit gleichen Sicherheitsanforderungen

In Abschnitt 3.5 wurde bereits vorgeschlagen bei den Kunden zwei Teilnetze einzurichten. Ein Servernetz, das Dienste für den Zugriff aus dem MWN und dem Internet zugänglich macht, sowie ein internes Netz, auf das von außen nicht zugegriffen werden kann. Die Realisierung ist mit Hilfe von VLANs möglich.

In dieser Form ist das Servernetz gleichbedeutend mit einer DMZ. Eine DMZ wird heute bereits von einem Drittel der Institute betrieben. Allerdings existiert hier ein deutlicher Unterschied zwischen kleinen und großen Instituten. Von den kleinen Instituten (bis zu 32 Rechner) hat kein einziges eine eigene DMZ (siehe Tabelle 3.10). Um so erfreulicher ist die große Bereitschaft der befragten Institute eine DMZ einrichten zu wollen. Drei Viertel der befragten Institute könnten sich dies vorstellen (siehe Tabelle 3.20).

5.1.8 Verbergen von Teilnetzen

Durch den FBB “Verbergen von Teilnetzen” (siehe Abschnitt 4.2.9) sollen erreicht werden, dass die Rechner im geschützten Netz nach außen nicht sichtbar werden. Je weniger Informationen über das eigene lokale Netz nach außen preisgegeben werden, desto besser. Eine Realisierung ist mit Hilfe von Proxies möglich, auf die in Abschnitt 5.1.6 eingegangen wurde. Proxies stehen allerdings nicht für alle Anwendungen zur Verfügung. Außerdem muss sichergestellt werden, dass der gesamte Verkehr über die Proxies läuft.

Eine alternative Realisierungsmöglichkeit, die unabhängig von der jeweiligen Anwendung eingesetzt werden kann, ist NAT. Zum Verbergen des internen Netzes mit Hilfe von NAT ist Masquerading oder SNAT geeignet. Bei manchen Diensten, die mehrere Verbindungen nutzen, ist eine Unterstützung des zugehörige Anwendungsprotokolls nötig. Beim Verbergen des Servernetzes muss sicher gestellt werden, dass die Server von außen angesprochen werden können. Eine Möglichkeit ist Port Forwarding. NAT wurde ausführlich in Abschnitt 2.1.2 besprochen.

Private IP-Adressen können die Realisierung dieses FBB ergänzen.

Berücksichtigung der Kundenanforderungen

Im Zusammenhang mit NAT ist zu berücksichtigen, dass nicht für jedes Anwendungsprotokoll entsprechende Hilfsroutinen vorhanden sind, so dass manche Dienste nicht oder nur begrenzt mit Masquerading und SNAT zusammenarbeiten. Da damit eine Einschränkung bei der Nutzung von Diensten im Internet verbunden ist, muss darauf hingewiesen werden, dass nur etwas mehr als die Hälfte der Institute dies akzeptieren (siehe Tabelle 3.17). Die in den Diensteprofilen 1 und 2 (siehe Abschnitt 3.3) zusammengefassten Dienste haben mit Masquerading bzw. SNAT keine Schwierigkeiten. Allein FTP benötigt im aktiven Modus ein Hilfsmodul, das aber bei den meisten Firewall-Lösungen voranden ist.

Zusätzlich ist die Frage interessant, wieviele Institute bereit sind, eine Veränderung der Adressierung in ihrem Netz vorzunehmen, da dies bei der Verwendung privater IP-Adressen notwendig ist. Hier konnte eine Bereitschaft bei 80 Prozent der befragten Institute festgestellt werden (siehe Tabelle 3.20). Dieses positive Bild wird verstärkt durch das Ergebnis, dass bereits 41 Prozent der befragten Institute private IP-Adressen einsetzen. Wie aus Tabelle 3.9 ersichtlich ist, setzen vor allem die große Institute auf private IP-Adressen. Bei den kleinen Instituten ist die Zahl geringer (nur 25 Prozent). Dies ist damit zu erklären, dass in den kleinen Instituten zur Zeit noch wesentlich seltener Firewalls zum Einsatz kommen (siehe Tabelle 3.12) und somit keine Möglichkeit für Masquerading gegeben ist.

Berücksichtigung der Betreiberanforderungen

Bei der Verwendung von Port Forwarding muss für jeden einzelnen Dienst, der vom Institut angeboten werden soll, eine entsprechende Übersetzungsregel auf der Firewall konfiguriert werden. Da davon auszugehen ist, dass die Serverstrukturen in den Instituten unterschiedlich sind, müsste für jedes Institut eine spezielle Konfiguration vorgenommen werden. Dies ist mit dem Ziel standardisierte Firewallpakete zu bilden nicht vereinbar. Erschwerend kommt hinzu, dass jede Veränderung in der Serverlandschaft auch eine Veränderung der Firewallkonfiguration nach sich ziehen würde, was zur Zeit vom LRZ nicht geleistet werden kann.

5.1.9 Remotezugang

Von beinahe 90 Prozent der Institute wird laut Umfrage ein Remotezugang zum Institutsnetz gewünscht. Es wird vorgeschlagen, für diesen Zweck einen SSH-Server im Servernetz einzurichten. Da auch häufig Sicherheitsprobleme im Zusammenhang mit SSH auftreten, wird ein SSH-Zugang im internen Netz nicht befürwortet. Bei den OpenSSH-Versionen 3.4p1 und 3.2.2p1 ist es Hackern sogar gelungen einen Trojaner über das CVS-System der OpenSSH-Entwickler einzuschleusen. Inzwischen sind für Linux (Fish, z. B. als Modul für Konqueror) und Windows (WinSCP) auch kostengünstige Tools mit GUI erhätlich, die einen einfachen Dateizugriff per SSH ermöglichen.

Im Rahmen eines allgemeinen VPN-Konzepts könnte der SSH-Zugang durch einen VPN-Zugang abgelöst werden. Dies sollte mit dem vom LRZ betriebenen VPN-Dienst verknüpft werden. Der VPN-Dienst des LRZ basiert zur Zeit noch auf PPTP und verwendet keine Verschlüsselung. Ein zukünftiges allgemeines VPN-Konzept sollte auf jeden Fall auch Verschlüsselung unterstützen. Ein Endpunkt des VPN-Tunnels sollte die Instituts-Firewall sein. Liegt der Endpunkt dahinter, kann die Firewall die gekapselten Daten nicht analysieren. Liegt er davor, so ist der Verkehr zwischen dem Endpunkt und der Firewall unverschlüsselt.

5.1.10 Redundante Sicherheit

Durch den Einsatz einer zweiten Firewall kann die Sicherheit deutlich erhöht werden. Es bietet sich folgende Realisierungsmöglichkeit. Die erste Firewall trennt Internet und Servernetz, die zweite Servernetz und internes Netz. Das zwischen den Firewalls gelegene Servernetz entspricht einer DMZ. Der Sicherheitszugewinn ist dann am größten, wenn für die beiden Firewalls unterschiedliche Produkte eingesetzt werden. Fehler im Produkt oder in der Konfiguration der einen Firewall können durch die zweite Firewall abgefangen werden. So bleibt das interne Netz auch dann noch vom Internet getrennt, wenn eine der Firewalls bereits ausgefallen ist. Werden die Vorgänge im Servernetz – z. B. mit Hilfe eines Network Intrusion Detection Systems (NetIDS) – aufmerksam beobachtet, können Einbrüche früh erkannt werden. Die DMZ ist dann zwar schon korrumpiert, das interne Netz bleibt bei schnellem Handeln jedoch verschont. Die Bereitschaft der Institute zukünftig mit einer DMZ zu arbeiten wurde in Abschnitt 5.1.7 bereits dargestellt.

5.1.11 Abwehr dienstunabhängiger Angriffstechniken

Das LRZ nutzt dazu bereits die Paketfiltermöglichkeiten des Routers, der den Zugang zum Internet herstellt. Damit werden primitive Angriffe abgewehrt ohne die Konnektivität einzuschränken. Dieses Vorgehen entspricht dem anderer großer Universitäten, wie beispielsweise der Universität Karlsruhe [Lort 00]. Blockiert werden Pakete mit gefälschten IP-Adressen (IP-Spoofing) und Pings auf Broadcast-Adressen [Läpp 02]. Ein solcher Grundschutz ist auch im Rahmen dieses Firewall-Konzepts zu befürworten. Ein solcher Grundschutz sollte auch die Basis der Instituts-Firewalls darstellen, um auch primitive Angriffe innerhalb des MWN abwehren zu können.

5.2 Realisierungsvorschlag für die Firewall-Pakete 1, 2 und 3

Für die Firewall-Pakete 1, 2 und 3 soll nun ein Vorschlag für die Realisierung gemacht werden. Dazu werden die Möglichkeiten der im MWN eingesetzten Router (Cisco Catalyst 6509) herangezogen. Die von diesen Routern gebotenen Sicherheitsfunktionen wurden in Abschnitt 2.3 dargestellt. Die Nutzung der Router hat den Vorteil, dass der Firewall-Dienst auf deren Basis schnell umgesetzt werden kann. Probleme, wie beispielsweise Ausfallsicherheit, sind für die Router bereits gelöst. Trotzdem darf dieser Realisierungsvorschlag keine Evaluation ersetzen.

Das Firewall-Pakets 4 soll hier nicht betrachtet werden. Für diese Lösung ist eine zweite Firewall notwendig. Dazu muss auf jeden Fall zunächst eine Evaluierung durchgeführt werden.

Nach Tabelle 4.3 müssen zur Realisierung der Firewall-Pakete 1, 2 und 3 folgende Service FunctionalBB realisert werden:

Paket 1: Default_Policy, Grundschutz, Verbindungsaufbau, Verbergen, Teilnetze und Remotezugang.

Paket_2_und_3: FBBs aus Paket 1, sowie Verbindungsannahme und Dienstangebot.

Option: Dienstnutzung.

5.2.1 Teilnetze

Die Aufteilung des Kundennetzes in zwei VLANs für das interne Netze und das Servernetz stellt die Grundlage aller drei Pakete dar. Es bestehen folgende grundlegende Kommunikationsbeziehungen, die von anderen FBBs noch ergänzt werden:

*	→	internes Netz	kein Zugriff
alles bis auf internes Netz	→	Servernetz	kein Zugriff (Zugriff durch andere FBBs)
internes Netz	→	Servernetz	SSH (zur Server-Konfiguration)
internes Netz	→	einzelne Server im MWN	DNS
internes Netz	→	MWN/Internet	alles (Einschränkung durch anderen FBB)
Servernetz	→	einzelne Server im MWN	DNS
Servernetz	→	MWN/Internet	kein Zugriff

Die sich aus den Kommunikationsbeziehungen ergebenden Regeln, können mit Hilfe eines statischen Paket-Filter realisiert werden. Auf den Cisco Routern werden statische Filterregeln mit Hilfe von IOS ACLs eingerichtet.

5.2.2 Dienstnutzung

Der optionale FBB Dienstnutzung soll die Nutzung des Internet und MWN auf bestimmte Dienste beschränken. Nach den Kommunikationsprofilen der drei Firewall-Pakete ergeben sich Beschränkungen auf folgende Dienste:

internes Netz	→	einzelne Server im MWN	DNS, DHCP, AFS und TSM
internes Netz	→	MWN/Internet	Dienste aus dem Diensteprofil 1 (siehe 3.3), im einzelnen sind dies E-Mail (POP3, SMTP, IMAP), FTP, Time (NTP), Proxy-Dienste, Telnet, SSH, Usenet und WWW (HTTP, HTTPS)
Servernetz	→	einzelne Server im MWN	DNS, DHCP, AFS und TSM

Für die Realisierung dieses FBB wurde ein statischer Paket-Filter vorgeschlagen (siehe Abschnitt 5.1.4). Auf den Cisco Routern werden statische Filterregeln mit Hilfe von IOS ACLs eingerichtet.

5.2.3 Remotezugang

Der Remotezugang kann mit Hilfe eines SSH-Servers im Servernetz realisiert werden. Der Zugriff auf den SSH-Server ist nur aus dem MWN gestattet. Für den Zugriff aus dem Internet muss zuvor eine Verbindung zum MWN hergestellt werden – entweder per Wählzugang oder über VPN. Das Kommunikationsprofil muss dazu ergänzt werden.

MWN	→	Servernetz	SSH

Für die Realisierung muss neben der Einrichtung des SSH-Servers im Servernetz eine ergänzende Filterregel auf Basis der IOS ACLs konfiguriert werden.

5.2.4 Verbergen

Wie in Abschnitt 5.1.8 ausgeführt wurde, kann wegen des hohen Aufwands das Servernetz nicht verborgen werden. Für das interne Netz bietet sich der Einsatz von SNAT in Kombination mit privaten IP-Adressen an. Die Cisco-Router unterstützen dies.

5.2.5 Verbindungsaufbau

Dieser FBB soll einen Verbindungsaufbau nur aus dem internen Netz heraus zulassen. Es wird der Einsatz einer dynamischen Paketfiltertechnik empfohlen. Bei den Cisco-Routern hat diese Technik den Namen Reflexive ACL. Seit kurzem bietet das LRZ den Instituten die Einrichtung eines solchen Filters bereits an. Die Reflexive ACLs sind wie folgt zu konfigurieren:

*	→	internes Netz	kein Verbindungsaufbau
internes Netz	→	*	Verbindungsaufbau

Wie bereits in Abschnitt 2.1.2 dargestellt wurde, kann es bei manchen Anwendungen, die auf mehreren Verbindungen der Transportschicht beruhen, zu Problemen im Zusammenspiel mit einem dynamischen Paketfilter kommen. Diese Anwendungen benötigen eine besondere Unterstützung. Die Reflexive ACL der Cisco Router bietet keine solche Unterstützung an. Von den häufig genutzten Diensten des Diensteprofils 1 – E-Mail (POP3, SMTP, IMAP), FTP, Time (NTP), Proxy-Dienste, Telnet, SSH, Usenet und WWW (HTTP, HTTPS) – benötigt FTP eine solche Unterstützung. Ohne dies ist nur passives FTP möglich.

Einen Ausweg bieten die Context-Based Access Control. Mit deren Hilfe kann auch aktives FTP realisiert werden.

5.2.6 Default Policy, Grundschutz

Die beiden FBB Default Policy und Grundschutz lassen sich mit Hilfe von IOS ACL realisieren.

5.2.7 Dienstangebot

Mit Hilfe dieses FBB kann der Zugriff auf bestimmte Dienste im Servernetz ermöglicht werden. Dieser FBB ist für die Pakete 2 und 3 vorgesehen. Es ergeben sich für das Paket 2 folgende Ergänzungen beim Kommunikationsprofil:

internes Netz, MWN	→	Servernetz	Dienste aus dem Diensteprofil 4 (siehe 3.3), im einzelnen sind dies E-Mail (POP3, SMTP, IMAP), FTP, Telnet, SSH, WWW (HTTP, HTTPS), DNS, VPN (IPsec, PPTP), Radius, Datei- und Druckdienste

Für das Firewall-Paket 3 sind folgende Ergänzungen notwendig:

internes Netz, MWN	→	Servernetz	Dienste aus dem Diensteprofil 4 (siehe 3.3), im einzelnen sind dies E-Mail (POP3, SMTP, IMAP), FTP, Telnet, SSH, WWW (HTTP, HTTPS), DNS, VPN (IPsec, PPTP), Radius, Datei- und Druckdienste
Internet	→	Servernetz	Dienste aus dem Diensteprofil 3 (siehe 3.3), im einzelnen sind dies E-Mail (POP3, SMTP, IMAP), FTP, Telnet, SSH, WWW (HTTP, HTTPS), DNS und VPN (IPsec, PPTP).

Auch der auf diese Dienste kann durch eine IOS ACL ermöglicht werden.

5.2.8 Verbindungsannahme

Dieser FBB soll sicherstellen, dass aus dem Servernetz heraus kein Verbindungsaufbau möglich ist. Ausnahmen von dieser Regel sind DNS, sowie optional DHCP, ASF und TSM. Diese Dienste können allerdings nur Verbindungen zu bestimmten Servern im MWN aufbauen. Der FBB ist für die Pakete 2 und 3 vorgesehen. Dazu können Reflexive ACLs eingesetzt werden, die für folgende Kommunikationsbeziehungen zu konfigureieren sind.

*	→	Servernetz	Verbindungsaufbau
Servernetz	→	*	kein Verbindungsaufbau (bis auf DNS, opt. DHCP, ASF und TSM)

Wie bereits in Abschnitt 2.1.2 dargestellt wurde, kann es bei manchen Anwendungen, die auf mehreren Verbindungen der Transportschicht beruhen, zu Problemen im Zusammenspiel mit einem dynamischen Paketfilter kommen. Diese Anwendungen benötigen eine besondere Unterstützung. Die Reflexive ACL der Cisco Router bietet keine solche Unterstützung an. Von den Diensten der Diensteprofile 3 und 4 – E-Mail (POP3, SMTP, IMAP), FTP, Telnet, SSH, WWW (HTTP, HTTPS), DNS, VPN (IPsec, PPTP), Radius, Datei- und Druckdienste – benötigt FTP (je nach eingesetzten Datei- und Druckdienst auch dieser) eine solche Unterstützung. Ohne dies ist nur passives FTP möglich.

Einen Ausweg bieten die Context-Based Access Control. Mit deren Hilfe kann auch aktives FTP realisiert werden.

5.3 Aspekte des Managements

5.3.1 Ressourcen

Der Firewall-Dienst ist für das MWN konzipiert. Aus diesem Grund sind zunächst die vorhandenen Ressourcen des MWN zu betrachten. In Abschnitt 1.1 wurde die Infrastruktur des MWN beschrieben, und besonders auf die Router und Switches eingegangen. Zusätzliche Ressourcen ergeben sich, wenn dezidierte Firewall-Produkte beschafft und in das MWN integriert werden.

Router zum G-WiN

In der Beschreibung des Firewall-Dienstes wurde vorgeschlagen, den G-WiN-Router mit in das Firewall-Konzept einzubeziehen. Er soll primitive Angriffe abwehren und dazu beitragen, für das gesamte MWN geltende Regeln durchzusetzen. Zu diesem Zweck sind bereits einige Paketfilterregeln auf dem Router eingerichtet. Weitere notwendige Regeln müssen identifiziert und installiert werden.

Switches

An den an das MWN angebundenen Standorten sind die einzelnen Gebäude über Switches angeschlossen. Innerhalb der Gebäude sind bei einer strukturierten Verkabelung ebenfalls Switches im Einsatz. Die Switches ermöglichen das Einrichten von VLANs. In der Dienstbeschreibung wurde vorgesehen, dass jedes Institutsnetz aus einem internen Netz und einem Servernetz besteht. Dazu müssen mit Hilfe der Switches jeweils zwei VLANs eingerichtet werden. Wird eine dezidierte Firewall eingesetzt, muss darauf geachtet werden, dass dem LRZ der Zugriff auf Netzkomponenten hinter der Firewall möglich bleibt. Ein Lösungsvorschlag ist neben den VLANs für die Institute ein eigenes VLAN für das Management- und Transportnetz einzurichten, das sich immer vor der Firewall befindet. Für die Konfiguration eines VLANs sind die entsprechenden Switch-Ports festzustellen.

Standort-Router

Die Unterteilung der Institutsnetze in zwei VLANs und die evtl. notwendige Schaffung eines VLAN für das Management- und Transportnetz muss bei der Konfiguration der Routingfunktionalität berücksichtigt werden. Die im MWN als Router eingesetzten Cisco 6509 bieten zudem Möglichkeiten zur Paketfilterung. Erfolgt die Implementierung des Firewalldienstes auf dieser Basis, müssen für die Router-Interfaces entsprechende Filterregeln eingerichtet werden. Außerdem müssen während des Betriebs anfallende, sicherheitsrelevante Informationen an einen Syslog-Server weitergegeben werden.

Dezidierte Firewall

Abhängig von den Ergebnissen einer Evaluation und Produktauswahl können zur Realisierung des Firewall-Dienstes auch eigenständige Firewall-Produkte zum Einsatz kommen. Dabei ist die Beschaffung der notwendigen Hard- und Software zu berücksichtigen. Weitere Aspekte sind der Ort der Aufstellung, sowie die Art und Weise der Installation und Konfiguration. Die Firewall sollte in das Management-Netz des LRZ einbezogen werden. Wie bei den Standort-Routern müssen auch bei dezidierten Firewalls die anfallenden, sicherheitsrelevanten Informationen an einen Syslog-Server weitergegeben werden.

Eine dezidierte Firewall kann auch von einem Institut selbst betrieben werden. Diese sollte dem LRZ bekannt sein und es muss sichergestellt werden, dass hinter der Firewall liegende MWN-Komponenten für das LRZ noch erreichbar sind.

Syslog-Server

Auf den Firewall-Systemen fallen sicherheitsrelevante Informationen in Form von Logs an. Für die Speicherung und Auswertung dieser Daten müssen ein oder mehrere besonders gesicherte Server eingerichtet werden. Es ist zu prüfen, ob die Syslog-Server an das Management-Netz angeschlossen werden können.

5.3.2 Lebenszyklusphasen

Planung

Der Firewall-Dienst wurde in Kapitel 4 beschrieben. Anschließend wurde in Form eines State of the art ein Überblick über verschiedene Sicherheitsmechanismen gegeben. Schließlich wurden Realisierungsvorschläge für die einzelnen Functional Building Blocks des Dienstes gemacht. Für die konkrete Realisierung sollte eine Evaluierung verschiedener Firewall-Produkte vorgenommen werden. In die Evaluation können die in Kapitel 2 dargestellten Lösungen einbezogen werden. Auf der Basis der Evaluation können dann geeignete Produkte ausgewählt werden. Für die konkrete Realisierung der Functional Building Blocks sind für das gewählte Produkt geeignete Regelsätze zu erstellen.

Aushandlung

Zwischen einem Institut als Kunden und dem LRZ als Anbieter muss die Dienstgüte ausgehandelt werden. Das LRZ bietet den Firewall-Dienst in Form von vier Klassen an, aus denen der Kunde auswählen kann. Ist der Kunde noch über das alte Yellow-Cable angeschlossen, bleibt nur die Auswahl einer Klasse. Optional bietet das LRZ ein Zusatzpaket an, das eine Einschränkung bei der Nutzung von Internetdiensten ermöglicht.

Der Kunde muss dem LRZ neben der gewählten Dienstklasse mitteilen, wie die VLANs aufgeteilt werden sollen und wie die IP-Subnetze gebildet werden sollen.

Will ein Institut eine eigene Firewall betreiben, so muss unter Umständen auf den Switches ein Management- und Transport-VLAN eingerichtet werden. Dies muss ebenfalls zwischen dem Kunden und dem LRZ vereinbart und dokumentiert werden.

Das Aushandeln des Firewall-Dienstes sollte keinen eigenen Management-Prozess nötig haben, sondern in bereits bestehende Vereinbarungsabläufe für andere vom LRZ angebotene Dienste integriert werden können.

Installation

Für die Installation eines Firewall-Pakets bei einem Institut müssen zunächst die notwendigen VLANs (internes Netz, Servernetz, Management- und Transportnetz) eingerichtet werden. Die übrige Installation hängt sehr von der Realisierung des Firewall-Pakets ab.

Wird das Firewall-Paket als eigenständiges System angeboten, muss die Beschaffung, Aufstellung und Installation des Systems mit in die Überlegungen einbezogen werden. Für die Aufstellung ist ein geeigneter Ort auszuwählen, der ausreichend gesichert ist. Beim Anschluss der Firewall ist darauf zu achten, dass dahinterliegende Komponenten für Management-Zwecke noch erreichbar sind. Es folgt die Konfiguration des Systems unter Einbeziehung kundenspezifischer Daten, wie IP-Adressen, Domainnamen etc.

Wird das Firewall-Paket auf einem Router realisiert, reicht es aus, das System für den Firewall-Dienst anzupassen. In beiden Fällen ist auf der Firewall Systemlog geeignet zu konfigurieren und der Syslog-Server auf den Empfang und die Speicherung der Daten vorzubereiten.

Die vorgenommene Konfiguration muss dokumentiert werden. Im Falle einer institutseigenen Firewall-Lösung ist ebenfalls eine Eintragung in der Netzdokumentation sinnvoll. Abschließend muss das System getestet und vom Kunden abgenommen werden. Beim Test ist sowohl die Nutzbarkeit anderer zugesicherter Dienste, sowie die Schutzwirkung zu überprüfen. Letzteres kann mit Hilfe eines Security-Scanners erfolgen.

Betrieb

Während des Betriebs müssen eventuell anfallende Fehler und Leistungsprobleme behoben werden. Die Systemlogs müssen gesichert und bei Bedarf ausgewertet werden. Zur Sicherstellung der Wirksamkeit der Firewall-Lösung müssen regelmäßig Sicherheitstests mit Hilfe eines Security-Scanners durchgeführt werden.

Änderungen

Änderungen am Firewall-Dienst müssen vorgenommen werden, wenn der Kunde die Dienstklasse wechseln möchte. Durch die Bildung von vier standardisierten Firewall-Paketen sollten Änderungen selten sein, und die Personalkapazitäten nicht übermäßig beanspruchen. Weitere Änderungen können im Zusammenhang mit den VLANs anfallen, wenn sich die Belegung der Switch-Ports verändert.

Die Firewall-Pakete müssen regelmäßig gepflegt werden, eventuelle Updates oder Sicherheits-Patches müssen zuverlässig eingespielt werden. Unter Umständen muss auch die Konfiguration nach Bekanntwerden eines Sicherheitsproblems angepasst werden.

Außerbetriebnahme

Zur Außerbetriebnahme eines Firewall-Pakets müssen die Regelsätze auf dem Router oder der Firewall gelöscht werden. Bei einer dezidierten Firewall muss das System abgebaut werden und in einer Inventarliste als wieder verfügbar gekennzeichnet werden. Die Netzdokumentation muss an die neue Situation angepasst werden. Schließlich sind die für den Firewall-Dienst eingerichteten VLANs aufzulösen.

5.3.3 Funktionsbereiche

Konfiguration

- Es müssen die involvierten Ressourcen identifiziert, evtl. angeschafft, aufgestellt und angepasst werden.
- Die Konfiguration sollte von einer zentralen Management-Station möglich sein.
- Die neue Firewall muss dokumentiert und die Konfiguration gesichert werden.
- Die notwendigen VLANs müssen konfiguriert und dokumentiert werden.

Fehler

Das Handhaben von Fehlern im Firewall-Dienst soll in das allgemeine Fault-Management des LRZ integriert werden. Darin spielt das Trouble-Ticket-System eine wichtige Rolle. Die Integration ist sinnvoll, da sich ein Fehler im Firewall-Dienst auch auf andere Dienste des LRZ auswirken kann. Mögliche Fehler lassen sich in zwei Bereiche einteilen:

Probleme bei der Nutzung anderer Dienste: Der Firewall-Dienst kann die Nutzung einzelner Dienste beschränken oder unmöglich machen. Zum Teil ist dies gewollt. Beispielsweise wird die Nutzung von Filesharing-Diensten grundsätzlich verhindert. In manchen Fällen können Dienste auch zu Gunsten einer größeren Schutzwirkung der Firewall von Beschränkungen betroffen sein. Beispielsweise haben dynamische Paketfilter Probleme mit Diensten, die für den Datenaustausch mehrere TCP- und UDP-Ports verwenden. Es besteht aber auch die Möglichkeit, dass auf Grund einer fehlerhaften Konfiguration die Nutzung eines Dienstes nicht mehr möglich ist.
In allen Fällen ist die Firewall nicht unbedingt sofort als Verursacher des Fehlers zu identifizieren. Aus diesem Grund muss der Firewall-Dienst in das übliche Fehler-Management des LRZ als mögliche Fehlerquelle aufgenommen werden.

Sicherheitsvorfall: Als Fehler gilt eine "Abweichung von gesetzten Betriebszielen, Systemfunktionen oder Diensten" [HAN 99a]. Ein Ziel des Firewall-Dienstes ist es, ein Kundennetz vor Angriffen von außen zu schützen. Tritt ein Sicherheitsvorfall auf, hat der Dienst offensichtlich dieses Ziel nicht erfüllt. Ein Sicherheitsvorfall ist deshalb ebenfalls als Fehler des Dienstes zu werten. Allerdings kann nicht jeder Sicherheitsvorfall auf eine fehlerhafte Firewall zurückgeführt werden. Genauso kommen falsch konfigurierte oder schlecht gepflegte Server des Kunden als Ursache in Frage. Tritt ein Sicherheitsvorfall auf, muss dieser geeignet behandelt werden. Letztlich kann eine Anpassung des Firewall-Dienstes notwendig werden.

Leistung

Ein Firewall-System kann die Leistung des MWN beeinflussen. Beispielsweise kann ein zu umfangreicher Regelsatz auf einem Router zu Performance-Einbußen führen.

Die Leistungsfähigkeit des Firewall-Dienstes hinsichtlich seiner Schutzwirkung kann durch den regelmäßigen Einsatz eines Security-Scanners überprüft werden. Unter Umständen muss bei festgestellten Problemen der Firewall-Dienst angepasst werden.

Accounting

Da für den Firewall-Dienst derzeit keine Kosten berechnet werden sollen, ist eine besondere Berücksichtigung dieses Funktionsbereichs nicht notwendig. Es reicht aus zu dokumentieren, welche Kunden welches Firewall-Paket in Anspruch nehmen.

Sicherheit

Der Management-Zugriff auf die Systeme des Firewall-Dienstes darf wie bei anderen Netzkomponenten nur den berechtigten Mitarbeitern des LRZ möglich sein. Dies geschieht von dezidierten Servern aus.

5.4 Managementprozesse

5.4.1 Evaluation und Produktauswahl

Ein Teil der in der Beschreibung des Firewall-Dienstes aufgeführten Functional Building Blocks lässt sich mit Hilfe der Paketfiltermöglichkeiten der vorhandenen Router realisieren. Damit können zumindest die Firewall-Pakete 1 - 3 implementiert werden (siehe Abschnitt 5.2). Allerdings wurde keine Evaluation vorgenommen. Es ist zu empfehlen, dass dies vor einer endgültigen Realisierung des Dienstes geschieht. Dabei spielen nicht nur Sicherheitsaspekte eine Rolle. In eine Evaluation sollten auch Einschränkungen bei der Nutzung von Diensten berücksichtigt werden. Beispielsweise benötigen viele Internet-Dienste bei einer dynamischen Paketfilterung Hilfsroutinen, die die Protokolle der Anwendungsschicht analysieren. Häufig ist die Zahl der unterstützten Anwendungs-Protokolle klein.

In Kapitel 2 wurden in Form eines State of the art für einen Firewall-Dienst geeignete Sicherheitsmechanismen vorgestellt. Es wurde auf die Möglichkeiten des vom LRZ eingesetzten Routers Cisco Catalyst 6509 eingegangen. Außerdem wurden verschiedene Möglichkeiten des Betriebssystems Linux vorgestellt. Auf der Basis von Linux existieren zahlreiche freie und kostengünstige Lösungen. Wie die Umfrage bei den Kunden MWN ergeben hat, wird Linux oft als institutseigene Firewall-Lösung eingesetzt. Schließlich wurden noch die Produkte PIX und Firewall-1 aufgeführt.

Auf dieser Basis sollte es möglich sein geeignete Produkte für eine Evaluation auszuwählen. Die Kriterien für die Evaluation ergeben sich aus der Beschreibung des Firewall-Dienstes. Insbesondere die einzelnen Functional Building Blocks und die Vorschläge zu deren Realisierung müssen bei der Aufstellung des Kriterienkatalogs berücksichtigt werden. An Hand der Kriterien können die Produkte getestet werden und eine Produktauswahl erfolgen.

5.4.2 Regelsätze erstellen und anpassen

Die Form der Regelsätze ist abhängig von der Produktauswahl. Die Regelsätze sind nach den Vorgaben der Dienstbeschreibung aufzustellen. Als Parameter sind die IP-Adressen der Kunden zu berücksichtigen. Die Regelsätze sind nicht als statische Konfiguration zu betrachten, sondern müssen laufend angepasst werden. Eine Anpassung kann nötig werden nach

- Bekanntwerden eines sicherheitsrelevanten Hard- oder Softwareproblems,
- Bekanntwerden einer neuen Angriffstechnik,
- Auftreten eines Problems bei der Nutzung bestimmter Dienste,
- Auftreten eines Sicherheistvorfalls,
- Erkennen einer Sicherheitslücke nach einem Test des Firewall-Dienstes.

5.4.3 Installation und Inbetriebnahme

Auch die Installation ist abhängig von der getroffenen Produktauswahl. Im einzelnen sind folgende Schritte notwendig:

1. Beschaffung der notwendigen Hard- und Software (Lizenzen) – entfällt bei Realisierung auf Router.

2. Einrichten der notwendigen VLANs (internes Netz, Servernetz, Management-/Transportnetz) auf den Switches nach den Wünschen des Kunden.
3. Anpassen des Routings hinsichtlich der eingerichteten VLANs und nach Angaben des Kunden.
4. Aufstellung der Firewall-Komponente an einem geeigneten Ort – entfällt bei Realisierung auf Router.
5. Aufnahme der Firewallkomponente in das Managementnetz – entfällt bei Realisierung auf Router.
6. Konfiguration des Firewall-Systems entsprechend der vom Kunden gewählten Dienstklasse.
7. Testen der Erreichbarkeit von Komponenten, die sich hinter der Firewall befinden.
8. Konfiguration des Syslog-Servers für den Empfang des Log von der neuen Firewall.
9. Test des Systems.
10. Abnahme durch den Kunden.
11. Dokumentation des Systems.
12. Inbetriebnahme.

Dokumentation In die Dokumentation sind verschiedene Daten aufzunehmen. Dabei sind zwei Fälle zu unterscheiden.

1. LRZ-Firewall:
   - Daten des Kunden,
   - ausgewähltes Paket,
   - Ort der Installation,
   - aktuelle Konfiguration.
2. Institutseigene Firewall:
   - Daten des Kunden,
   - Ort der Installation.

5.4.4 Test der Konfiguration

Um die Wirksamkeit der Firewall zu testen, wird die Nutzung eines Security-Scanner vorgeschlagen. In einer früheren Diplomarbeit wurde bereits ein Konzept für den Einsatz eines Security-Scanners erarbeitet [Pank 00]. Jede Firewall sollte

- nach der Installation
- und in regelmäßigen Abständen

einer solchen Sicherheitsüberprüfung unterzogen werden. Werden durch den Test Sicherheitslücken entdeckt, deren Ursache bei der Firewall liegen, muss die Konfiguration der Firewall angepasst werden.

Das in der erwähnten Diplomarbeit vorgestellte Konzept sieht ein Web-Interface vor, über das Mitarbeiter des LRZ und die Netzverantwortlichen der Institute den Security-Scanner nutzen können. Dabei kann der Zeitpunkt eines Scans und ein Wiederholintervall eingestellt werden. Die Ergebnisse eines Scans können ebenfalls über das Web-Interface zugänglich gemacht werden.

5.4.5 Sicherheitsvorfall

Ein Sicherheitsvorfall wird als Fehler im Firewall-Dienst und somit als Teil des Fault-Management betrachtet. Ein Sicherheitsvorfall kann auf unterschiedliche Arten festgestellt werden:

- Fehlermeldung eines Kunden,
- Auswertung der Systemlogs,
- auffälliger Netzverkehr.

Ein auffälliger Netzverkehr kann durch einen aufmerksamen Mitarbeiter des LRZ festgestellt werden. Es empfiehlt sich jedoch zusätzlich ein IDS einzusetzen. Zu diesem Thema liegt eine frühere Diplomarbeit [Brüc 00] vor. Bei der Behandlung eines Sicherheitsvorfalls empfiehlt sich folgendes Vorgehen:

1. Erste Reaktionen: Keine Panik! Das sofortige Trennen des betroffenen Rechners vom Netz oder gar das Abschalten ist nicht unbedingt die beste Methode, da dadurch viele Spuren und Beweise (offene Netzverbindungen, aktive Prozesse) verloren gehen können. Die richtige Reaktion ist abhängig von den auf dem Rechner gespeicherten Daten.
2. Beweissicherung: Folgende Daten können wichtige Spuren sein: Datum und Uhrzeit, Konfiguration (IP-Adressen) und Status (Promiscious Mode) der Netzwerk-Interfaces, Prozessinformationen (Namen, Parameter, Ausfühurngsdauer, Benutzer), offene Netzwerk-Sockets (Prozess-ID), offene Files (Prozess-ID), Archivieren verdächtiger Programme, Routing-Tabellen, eingeloggte Benutzer, geladene Treiber und Betriebssystem-Module, Zeitpunkt des letzten Zugriffs auf Dateien, Sichern von Logfiles, Sichern der Benutzerrechte, Sichern der Konfiguration von Serverprogrammen. Diese Daten sollten dann in einem Archiv gesichert, mit einer Prüfsumme versehen (MD5) und auf einem unveränderbaren Medium gespeichert werden (CD-R). Auf diese Weise lässt sich später die Authentizität der Beweise bestätigen. Der Vorgang der Beweissicherung sollte zusätzlich dokumentiert werden. Es empfiehlt sich festzuhalten, welche Spuren gesichert wurden, welche Tools dazu verwendet wurden und zu welchen Zeitpunkt dies geschehen ist.
3. Wiederherstellen der betroffenen Systeme.
4. Dokumentation des Vorfalls.
5. Einleiten MWN-interner oder juristischer Konsequenzen.

Die fachgerechte Behandlung von Sicherheitsvorfällen setzt entsprechende Kenntnisse bei den zuständigen Personen voraus und ist zeitintensiv. Es scheint sinnvoll ein für das MWN zuständiges Computer Emergency Response Team (CERT) einzurichten. Es gibt Überlegungen auf Grund der knappen Personalkapazitäten, studentische Hilfskräfte in das CERT aufzunehmen. Weitere Mitglieder des CERT könnten sich aus dem Arbeitskreis Firewall gewinnen lassen. Es sollte zudem geprüft werden, inwieweit eine Zusammenarbeit mit dem DFN-CERT möglich ist.

Kapitel 6

Zusammenfassung und Ausblick

6.1 Zusammenfassung

Ziel dieser Diplomarbeit war die Konzeption eines Firewall-Dienstes für das MWN. In der Einleitung wurde gezeigt, dass die rund 700 Kunden des MWN sehr heterogen sind. Daraus ergaben sich unterschiedliche Sicherheits- und Kommunikationsbedürfnisse und somit unterschiedliche Erwartungen an den Firewall-Dienst. Demgegenüber hat das LRZ als Betreiber des MWN nur begrenzte Kapazitäten für den Firewall-Dienst zur Verfügung. Auf Grund dieses Gegensatzes war schon sehr früh klar, dass ein Kompromiss gefunden werden muss zwischen den vielfältigen Bedürfnissen der Institute und den begrenzten Kapazitäten des LRZ.

Als erster Schritt hin zur Entwicklung des Firewall-Dienstes wurden mehrere existierende Firewall-Lösungen betrachtet, um einen Überblick über aktuelle Sicherheitsmechanismen zu gewinnen. Das Betriebssystem Linux wird als Firewall vielfach von Kunden des MWN eingesetzt. Laut Umfrage basieren mehr als drei Viertel der Instituts-Firewalls auf Linux und wurde deshalb näher beleuchtet. Die im MWN eingesetzten Router (Cisco Catalyst 6509) besitzen Firewall-Funktionen. Auch diese wurden in die Betrachtung mit einbezogen, genauso wie drei eigenständige, kommerzielle Firewall-Produkte von Astaro, Cisco und Checkpoint. Es hat sich gezeigt, dass alle diese Produkte Möglichkeiten zur statischen und dynamischen Paketfilterung besitzen. Dabei ist die große Verbreitung der dynamischen Filterung eher neu – Linux beispielsweise kennt diese Technik erst seit Version 2.4. Ebenfalls gut unterstützt wird NAT. Die größten Unterschiede bestehen bei Proxies und ALGs.

Von großem Interesse war die Betrachtung von Firewall-Konzepten anderer Universitäten. Es standen die Konzepte der Universitäten Passau und Karlsruhe zur Verfügung. Diese beiden Universitäten unterscheiden sich hinsichtlich ihrer Größe. In Passau gibt es etwa 10 Institute, in Karlsruhe sind es rund 150. Entsprechend unterschiedlich sind die Firewall-Konzepte. Während man in Passau auf eine zentrale Firewall-Lösung setzt, hat man in Karlsruhe ein gestaffeltes Konzept. Eine sog. Hauptpforte schützt das gesamte Hochschulnetz vor einfachen Angriffen. Die sog. Institutspforten bieten dann einen umfassenden Schutz für die einzelnen Institute. Auf Grund der Größe des MWN hat sich das Firewall-Konzept dieser Diplomarbeit eher am Modell von Karlsruhe orientiert.

Die angesprochene Heterogenität der am MWN angeschlossenen Institute hat es notwendig gemacht, genauere Informationen über die Struktur und Bedürfnisse der Kunden in Erfahrung zu bringen. Dazu wurde eine Umfrage durchgeführt. Die Auswertung der Umfrage sollte das Aufstellen von Kundenprofilen ermöglichen, an denen der Firewall-Dienst ausgerichtet werden kann. Die Umfrage umfasste

Fragen nach Größe und Beschaffenheit der Institutsnetze, nach genutzten und angebotenen Diensten, nach bereits selbst getroffenen Sicherheitsmaßnahmen, sowie nach der Akzeptanz verschiedener Einschränkungen, die sich aus dem Firewall-Dienst ergeben können. Die Durchführung der Umfrage hat mehr Zeit beansprucht als ursprünglich angenommen wurde. Dies lässt sich auf technische Schwierigkeiten und auf den zögerlichen Rücklauf der Fragebögen zurückführen. Von den etwa 650 angeschriebenen Instituten haben knapp zehn Prozent geantwortet. Da darunter auch einige große Institute waren, konnte durch die Umfrage mehr als ein Viertel der am MWN angeschlossenen Rechner abgedeckt werden.

An Hand der Auswertung der Umfrage war es möglich, vier Kundenprofile für den Firewall-Dienst zu erstellen. Ein Profil umfasst allerdings Institute, die keine Einschränkung bei der Nutzung des MWN und des Internet wünschen und somit nicht Zielgruppe des Firewall-Dienstes sind. Die übrigen drei Profile umfassen Kunden, die in unterschiedlichem Ausmaß Einschränkungen akzeptieren, die mit dem Firewall-Dienst verbunden sind. Neben den Kundenprofilen wurden noch Diensteprofile gebildet, die von den Instituten genutzte und angebotene Dienste umfassen. Die Umfrage hat außerdem ergeben, dass die kleinen Institute einen größeren Bedarf an einem Firewall-Dienst haben.

Aus den bis zu diesem Zeitpunkt entwickelten Anforderungen wurde nun der Firewall-Dienst konzipiert. Basierend auf dem "Framework for IT Service Management" [DR 02] wurde der Dienst beschrieben. Dazu wurden zwölf Service Functional Building Blocks gebildet und sieben QoS-Parameter identifiziert. Die QoS-Parameter wurden zunächst aus dienstzentrierter und dann aus providerzentrierter Sicht betrachtet. Dadurch konnten die beschränkten Kapazitäten des LRZ beim Design des Dienstes berücksichtigt werden. Auf der Basis der Dienstgütemerkmale wurden dann vier Dienstklassen aggregiert, die den Bedürfnissen der Kunden – das bedeutet den Kundenprofilen – gerecht werden. Die Dienstklassen wurden als Firewall-Pakete 1 bis 4 bezeichnet. Für das Paket 1 wurde zusätzlich eine Alternativlösung für nicht geswichte Netze erarbeitet. Als Option können die Pakete 1 bis 3 durch ein Zusatzmodul ergänzt werden.

Aus dem im State of the Art gewonnenen Überblick über die Sicherheitsmechanismen wurden Realisierungsvorschläge für den Firewall-Dienst erarbeitet. Zunächst wurden Vorschläge für die einzelnen FBBs gemacht. Für die Firewall-Pakete 1 bis 3 wurde dann eine Realisierungsmöglichkeit auf der Basis der Cisco-Router aufgezeigt. Für den Betrieb des Firewall-Dienstes ist ein Betriebskonzept notwendig. Dazu wurden für das Management relevante Aspekte betrachtet und die drei Management-Dimensionen Ressourcen, Lebenszyklusphasen und Funktionsbereiche berücksichtigt. Auf Grund dieser Analyse konnten abschließend Management-Prozesse identifiziert und beschrieben werden.

In Abschnitt 3.7 wurden die Anforderungen an den Firewall-Dienst zusammengefasst. Zum Abschluss der Diplomarbeit sollen diese noch einmal betrachtet werden, und es soll dargestellt werden, in wie weit man ihnen gerecht werden konnte.

6.1.1 Anforderungen des Dienstes

Kontrolle des Datenverkehrs: Zwischen MWN und G-WiN sollen nach wie vor einfache Filtervorgänge stattfinden. Damit können primitive Angriffe abgewehrt und eine missbräuchliche Nutzung des MWN (z. B. Filesharing, Spam-Relay) verhindert werden. Die Pakete des entwickelten Firewall-Dienstes beziehen sich auf den Übergang vom MWN-Backbone zum Institutsnetz. Auf diese Weise kann der Verkehr vom und zum Institutsnetz kontrolliert werden und auf die unterschiedlichen Interessen der Institute eingegangen werden.

Zugriffe aus dem Internet und dem MWN: Für Rechner, die Dienste anbieten, ist ein eigenes Subnetz in Form eines VLAN vorgesehen. Die Firewall lässt nur Dienste zu, die in den Diensteprofilen 3 und 4 enthalten sind.

Nutzung von Diensten: Um die missbräuchliche Nutzung des MWN einzuschränken, wurde empfohlen, dass weiterhin bestimmte Dienste (z. B. Filesharing-Dienste) am Roter zum G-WiN blockiert werden. Außerdem können die Firewall-Pakete optional eine Einschränkung der Dienstnutzung enthalten. Dazu sind die Diensteprofile 1 und 2 vorgesehen.

Erschweren von Scans: Das interne Netz wird durch den Einsatz von NAT und privaten IP-Adressen nach außen verborgen. Zusätzlich muss die Firewall so konfiguriert sein, dass sie möglichst wenig Informationen über sich selbst preisgibt. Aus diesem Grund wurde u. a. für die Default Policy ein kommentarloses Verwerfen unerwünschter Pakete vorgeschlagen.

Erschweren von Hacks: Server die Dienste nach außen anbieten und so grundsätzlich erreichbar sind, können gehackt werden. Die Pflege dieser Server liegt weiterhin in der Hand der Institute. Durch das Firewall-Konzept wird jedoch sichergestellt, dass Server in einem eigenen Subnetz (Servernetz) zusammengefasst sind. Die Rechner im internen Netz können von außen nicht erreicht werden.

Filterung der Anwendungsdaten: Die Filterung der Anwendungsdaten wird von den Instituten unterschiedlich beurteilt. Eine Filterung von aktiven Inhalten wünschen beispielsweise nur 23 Prozent der befragten Institute. Für die Filterung auf Anwendungsebene ist das Firewall-Paket 4 vorgesehen. Mit einer zweiten Firewall, die im Verantwortungsbereich des Kunden liegt, kann ein Institut individuelle Filterregeln für Anwendungsdaten einrichten. Für bestimmte Dienste ist auch ein Betrieb eines zentralen Proxies durch das LRZ denkbar. Im Zusammenhang mit SMTP wird dies bereits gemacht.

Schutz vor sonstigen Angriffen: Unter diese Rubrik fallen Angriffe wie Spoofing und DoS. Spoofing und viele DoS-Angriffe lassen sich durch eine geeignete Konfiguration der Firewall abfangen.

6.1.2 Anforderungen des Betreibers

Kosten des G-WiN-Zugangs: Bestimmte unerwünschte, aber großvolumige Dienste sollen generell im MWN unterbunden werden. Dazu bietet es sich an, den G-WiN-Router mit entsprechenden Filterregeln zu konfigurieren, wie dies beispielsweise im Zusammenhang mit den Filesharing-Diensten bereits gemacht wird.

Berücksichtigung der vorhandenen Infrastruktur: Für die noch vorhandene 10Base5-Verkabelung wurde eine Alternative für das Firewall-Paket 1 vorgeschlagen.

Nutzung vorhandener Kapazitäten: Um den begrenzten Kapazitäten des LRZ gerecht zu werden, wurden vier standardisierte Firewall-Pakete entwickelt. Es wurde ein Realisierungsvorschlag für die Pakete 1 bis 3 gemacht, der auf den vorhandenen Cisco-Routern aufsetzt. Außerdem wurde darauf hingewiesen, dass andere Dienste des LRZ (z. B. Mail-Relay) mit in den FW-Dienst einbezogen werden können.

Betrieb des Dienstes: Für den Betrieb des Dienstes wurden verschiedene Aspekte des Management analysiert und Management-Prozesse identifiziert und beschrieben.

6.1.3 Anforderungen des Kunden

Diensteprofile: Zu den genutzten und angebotenen Diensten wurden Diensteprofile erstellt. Diese Profile sind jeweils für mindestens 80 Prozent der an der Umfrage teilgenommenen Institute geeignet. Bei kleinen Instituten sind es oft 100 Prozent.

Nutzung von Diensten: Grundsätzlich macht der Firewall-Dienst keine Einschränkungen bei der Nutzung von Diensten. Ausnahmen sind Dienste wie Filesharing. Optional kann zu den Paketen 1 bis 3 jedoch eine Einschränkung auf die Dienste der Profile 1 und 2 erfolgen.

Content Filtering: Für das Content Filtering ist das Firewall-Paket 4 vorgesehen.

Kundenprofile: Die Kundenprofile wurden bei der Entwicklung des Firewall-Dienstes berücksichtigt. Firewall-Paket 1 entspricht dem Kundenprofil 1, Firewall-Paket 2 dem Kundenprofil 2 und die Firewall-Pakete 3 und 4 entsprechen dem Kundenprofil 3.

6.2 Ausblick

Evaluation von Firewall-Produkten: Es wurde betont, dass der enthaltene State of the Art keine Evaluation von Firewall-Produkten ersetzen kann. Trotzdem wurde für die Firewall-Pakete 1 bis 3 ein Realisierungsvorschlag auf der Basis der Cisco-Router gemacht. Eine Evaluierung, insbesondere in Hinblick auf das Firewall-Paket 4, ist aber nach wie vor notwendig. Als Ausgangspunkt für die Evaluation kann diese Diplomarbeit dienen. Aus dem vorgestellten Firewall-Dienst lassen sich die notwendigen Bewertungskriterien gewinnen. Als Vorauswahl für die zu untersuchenden Produkte können die im State of the Art betrachteten Lösungen dienen.

Betriebskonzept: Für das Betriebskonzept wurden für das Management relevante Aspekte analysiert und Management-Prozesse identifiziert und beschrieben. Es bleibt übrig, dies an die Aufbau- und Ablauforganisation des LRZ anzupassen und geeignete Policies und Workflows zu erstellen.

Remote-Zugang: Für den Remote-Zugang, der vom Großteil der befragten Institute gefordert wird, wäre ein durchgängiges VPN-Konzept wünschenswert. Dies könnte auf der Basis des bisherigen VPN-Zugangs zum MWN entwickelt werden. Die bisherige Lösung vermittelt jedoch nur einen allgemeinen Zugang zum MWN. Eine Erweiterung sollte den Zugang zu den einzelnen Instituten für berechtigte Nutzer ermöglichen.

Dateizugriff: Viele Institute wünschen einen Zugriff vom MWN aus auf Dateiserver im eigenen Institutsnetz. Für dieses Problem gibt es zur Zeit keine Lösung. Ungeeignet im Zusammenhang mit einer Firewall sind Verfahren die auf RPC basieren. Denkbar wäre eine Erweiterung des AFS-Dienstes. Die Universität Karlsruhe setzt auf Windowsoperationen.

Offene Ports: Mehr als die Hälfte der befragten Institute gab an, dass es in ihrem Netzbereich frei zugängliche Netzdosen gibt. In einem allgemeinen Sicherheitskonzept muss dieses Problem gelöst werden. Mit dem schon vorhandenen Radius-Dienstes wäre eine Lösung auf Basis von IEEE 802.1x möglich.

Modem: Bei der Umfrage haben 16 Prozent der Institute angegeben, dass sie Modems betreiben. Eine zentrale Forderung des Firewall-Dienstes ist, dass die Firewall den einzigen Zugang zum Institutsnetz darstellt. Gerade in Hinblick auf die Dialer-Problematik sollten Modems im Zusammenhang mit dem Firewall-Konzept nicht zulässig sein. Es ist allerdings fraglich, wie dies durchgesetzt und kontrolliert werden kann.

Anhang A

Fragebogen

Auf den folgenden Seiten ist der Fragebogen abgebildet, wie er den Netzverantwortlichen vorgelegt wurde.

Fragebogen zum zukünftigen Firewall-Dienst des LRZ

Stand: 2002-05-27

Eine Sicherheitsstudie aus dem Jahr 2000 geht davon aus, dass rund 40 Prozent der in Deutschland, Österreich und der Schweiz ansässigen Behörden und Unternehmen in der Vergangenheit mindestens einmal Ziel von Hackern waren oder unzulässige Manipulationen ihrer Internetdienste bemerkten. Das amerikanische FBI befragte 273 Behörden und Unternehmen nach den entstandenen Schäden in Folge von Angriffen auf ihre Computersysteme. Die finanziellen Verluste wurden dabei auf insgesamt 265 Mio. US-Dollar innerhalb von 12 Monaten geschätzt. Auch der periodische Sicherheitsbericht des Bundesinnenministeriums spricht von einer steigenden Tendenz der polizeilich registrierten Kriminalität im Zusammenhang mit dem Internet (http://www.bmi.bund.de/frame/dokumente/Artikel/ix_49371.htm).

Auch im Münchner Wissenschaftsnetz (MWN) werden immer wieder Angriffe auf die Computersysteme verzeichnet. So kam es beispielsweise in jüngster Zeit zu einem mehrere Tage andauernden Denial-of-Service-Angriff. Eine Schwachstelle eines SSH-Dämon wurde genutzt um einen Server zu cracken. Das MWN stellt mit seiner sehr guten Anbindung (622 MBit/s) an das Internet für Hacker ein interessantes Ziel dar, Server für diverse Tauschbörsen lassen sich hier "ideal" platzieren.

Dabei ist auf Seiten der Angreifer kein allzu großes Know-How notwendig. Mit entsprechenden Netz-Scannern kann nach Schwachstellen gesucht werden, zum Teil automatisieren diese Tools auch den Einbruch. Für alle Betriebssysteme (auch Linux) kursieren im Internet Rootkits und Backdoors, die sich so einfach wie eine normale Anwendung installieren lassen.

Ein Schutz der am MWN angeschlossenen Institute durch eine Firewall ist unter diesen Umständen dringend geboten. Das Leibniz-Rechenzentrum (LRZ) möchte deshalb seinen Kunden zukünftig einen Firewall-Dienst anbieten. Da das LRZ personell nicht in der Lage ist, für jedes Institut eine maßgeschneiderte Firewall einzurichten, wird es einige wenige Lösungen anbieten, aus denen die Institute auswählen können. Um diese Lösungen von vornherein möglichst gut auf die Bedürfnisse der Institute auszurichten, dient der folgende Fragebogen. Er ist Teil einer Diplomarbeit, in deren Rahmen ein Firewall-Konzept erstellt werden soll. Damit die Diplomarbeit und der dabei entstehende Firewall-Dienst erfolgreich wird, wäre eine breite Beteiligung an dieser Umfrage sehr hilfreich. (Einige der im Fragebogen vorkommenden Abkürzungen werden am Ende der Seite erläutert.)

Fragebogen

Institut:	
	LMU TUM FH Sonstige
Bearbeiter:	
Mail-Adresse (für evtl Rückfragen):	

Beschreibung des Institutsnetzes

Die Fragen in diesem Block sollen dazu beitragen, einen eventuellen Zusammenhang zwischen Größe des Instituts und Anforderungen an den Firewall-Dienst aufzuzeigen. Auch die eingesetzten Betriebssysteme sind hierbei von Interesse, außerdem stellen sie unterschiedliche Herausforderungen an eine Firewall. Besonderes problematisch für ein IT-Sicherheitskonzept sind ungeschützte Modems oder ISDN-Adapter, sowie offene Ports im Netz.

Welche IP-Adressbereiche haben Sie vom LRZ erhalten?	
Benutzen Sie darüber hinaus private IP-Adressen?	ja nein
In wieviele IP-Subnetze haben Sie Ihr Institutsnetz unterteilt?	
Wieviele Rechner (Desktop, Server etc.) sind an Ihrem Institutsnetz angeschlossen?	
Wieviele mobile Rechner (Notebooks etc.) werden fallweise in Ihrem Institutsnetz angeschlossen?	

Welche Betriebssysteme sind im Einsatz?

Windows 95/98/Me	Windows NT/2000/XP
Linux	Solaris

andere:

Werden in Ihrem Institutsnetz Modems oder ISDN-Adapter betrieben (nur in Absprache mit dem LRZ), die einen Zugang zu Rechnern oder zum Institutsnetz ermöglichen?	ja nein
Sind in Ihrem Verantwortungsbereich frei zugängliche Netzwerksteckdosen vorhanden?	ja nein

Nutzung von Diensten

Für die einzelnen Dienste des Internets gibt es unterschiedliche Verfahren zur Filterung. Der Firewall-Dienst des LRZ wird nicht für alle Dienste ein gleich hohes Schutzniveau anbieten können, sondern wird sich auf die häufig genutzten Dienste konzentrieren müssen.

Innerhalb des MWN: Das LRZ oder andere Institute im MWN bieten verschiedene Internet-Dienste an. Welche davon werden in Ihrem Institut genutzt?

E-Mail	News (Usenet)	Telnet	SSH	FTP	WWW	DNS	DHCP	Time (NTP)	Proxy

andere:

Außerhalb des MWN: Welche Dienste des Internet werden in Ihrem Institut genutzt?

E-Mail	News (Usenet)	Telnet	SSH	FTP	WWW	DHCP	Time (NTP)	Proxy

andere:

Eigene Dienste

Dienste die von außen erreichbar sein müssen, stellen unterschiedliche Anforderungen an die Firewall. Außerdem sollten die zugehörigen Server nach Möglichkeit in einem eigenen Subnetz untergebracht sein.

Welche Dienste Ihres Institutsnetzes sollen aus dem MWN erreichbar sein?

E-Mail News (Usenet) Telnet SSH FTP WWW DNS Datei-Zugriff Drucken

andere:

Welche Dienste Ihres Institutsnetzes sollen aus dem Internet erreichbar sein?

E-Mail News (Usenet) Telnet SSH FTP WWW DNS

andere:

Befinden sich die Server-Rechner, die Dienste für das MWN oder das Internet anbieten, in einem eigenen Subnetz?	ja nein

Welche Dienste Ihres Institutsnetzes sollen von außen nicht erreichbar sein?

Telnet SSH FTP WWW DNS SMB/CIFS NFS NIS

andere:

Eigene Maßnahmen zum Schutz des Institutsnetzes

Um den zukünftigen Firewall-Service des LRZ möglichst gut auf die Bedürfnisse der Institute abzustimmen, ist es hilfreich zu wissen, welche Sicherheitsmaßnahmen in den Instituten bereits ergriffen wurden.

Ist Ihr Institutsnetz bereits durch eine Firewall geschützt?	ja nein

Wenn ja, welche Firewall-Produkte werden verwendet?

Wieviele Rechner sind mit Antiviren-Software ausgestattet?	
Wieviele Rechner sind mit einer Desktop-Firewall ausgestattet?	

Fragen zum Firewall-Dienst des LRZ

Das LRZ wird nicht für jedes Institut eine maßgeschneiderte Lösung anbieten können. Stattdessen wird es einige standardisierte Lösungen geben. Trotzdem sollen die Pakete möglichst an den Bedürfnissen der Institute ausgerichtet werden. Die Fragen in diesem Block sollen feststellen, ob bestimmte Einschränkungen oder Umstrukturierungen in den Instituten möglich sind.

Angenommen, der Zugriff auf das Internet würde auf bestimmte Dienste beschränkt, wäre Ihr Institut mit dieser Maßnahme einverstanden?	ja nein
Angenommen, der Firewall-Dienst würde mit Hilfe von Content-Filtering Java-Applets und andere aktive Inhalte des WWW blockieren, wäre Ihr Institut mit dieser Maßnahme einverstanden?	ja nein
Angenommen, der Zugriff auf bestimmte Sites (URL-Filtering) im Internet würde unterbunden, wäre Ihr Institut mit dieser Maßnahme einverstanden?	ja nein
Angenommen, der Firewall-Dienst würde eine Änderung der IP-Adressierung in Ihrem Institutsnetz nötig machen, wäre es in Ihrem Institut möglich, diese Änderungen vorzunehmen?	ja nein
Angenommen, der Zugriff aus dem Internet auf das Institutsnetz würde vollständig unterbunden. Dies würde bedeuten, dass kein Rechner Ihres Institutsnetzes aus dem Internet erreichbar wären. Ein Remote-Zugang (z.B. für den Datei-Zugriff) wäre noch möglich. Wäre Ihr Institut mit dieser Maßnahme einverstanden?	ja nein
Angenommen, der Zugriff aus dem MWN auf das Institutsnetz würde vollständig unterbunden. Dies würde bedeuten, dass kein Rechner Ihres Institutsnetzes von anderen Instituten aus erreichbar wären. Ein Remote-Zugang (z.B. für den Datei-Zugriff) wäre noch möglich. Wäre Ihr Institut mit dieser Maßnahme einverstanden?	ja nein
Wird ein Remote-Zugang in Ihr Institutsnetz benötigt, so dass z.B. von zu Hause auf Daten im Institut zugegriffen werden kann?	ja nein
Angenommen, der Zugriff aus dem Internet auf das Institutsnetz wäre auf ein Subnetz (Demilitarisierte Zone) beschränkt. In diesem könnten alle Server zusammengefasst werden, die aus dem Internet erreichbar sein sollen (z.B. WWW-Server mit öffentlichen Informationen). Wäre Ihr Institut mit dieser Maßnahme einverstanden?	ja nein
Angenommen, der Zugriff aus dem MWN auf das Institutsnetz wäre auf ein Subnetz (Demilitarisierte Zone) beschränkt. In diesem könnten alle Server zusammengefasst werden, die aus dem MWN erreichbar sein sollen (z.B. Datei-Server für den Remote-Zugriff). Wäre Ihr Institut mit dieser Maßnahme einverstanden?	ja nein
Das LRZ bietet für verschiedene Dienste (z.B. WWW, E-Mail, News (Usenet), DNS, DHCP, Backup- bzw. Archiv-Service) Serverkapazitäten an, die von den Instituten für öffentliche Dienstangebote genutzt werden können. Dadurch müssen im Institutsnetz keine aus dem Internet zugänglichen Server betrieben werden. Weiss Ihr Institut von dieser Möglichkeit?	ja nein
Wäre Ihr Institut im Rahmen einer Firewall-Lösung bereit, die in der letzten Frage genannten Serverkapazitäten des LRZ statt eigener Server verstärkt zu nutzen?	ja nein

Fragen, Ergänzungen, Anregungen

Das Textfeld bietet Ihnen die Möglichkeit für Anmerkungen: Welche Fragen waren nicht verständlich? Welche Fragen konnten Sie nur mit Vorbehalten beantworten? Haben Sie ergänzende Informationen oder Anregungen?

Vielen Dank für Ihre Mitarbeit!

Abkürzungen

CIFS	Common Internet File System: Verfahren für den Zugriff auf Dateien und Drucker über ein Rechnernetz. Wird von den Windows-Betriebssystemen verwendet.
DHCP	Dynamic Host Configuration Protocol: Ein DHCP-Server vergibt dynamisch IP-Adressen an Rechner im Netz. Auch Informationen über Server und Routing können an die Clients weitergegeben werden.
DNS	Domain Name Service: Ein Datenbankdienst, der Rechnernamen in IP-Adressen übersetzt und umgekehrt.
NFS	Network File System: Verfahren zur gemeinsamen Nutzung von Dateisystemen auf vernetzten Rechnern. Wird überwiegend in UNIX-Umgebungen verwendet.
NIS	Network Information Service: Zur zentralen Verwaltung von Benutzeraccounts und Informationen über Rechner in einem Netz. Wird überwiegend in UNIX-Umgebungen verwendet.
NTP	Network Time Protocol: Protokoll zur Synchronisation der Rechneruhren in einem Netz.
Proxy	Programm, das stellvertretend für ein anderes Programm (auf dem Client-Rechner) eine Verbindung ins Internet aufbaut und unterhält. Damit kommt es zu keiner direkten Verbindung zwischen dem Client und dem Server. Proxy-Programme gibt es für verschiedene Anwendungen des Internet. Am weitesten verbreitet sind Proxys für WWW und FTP.
SSH	Secure Shell: Ermöglicht authentifizierte und verschlüsselte Netzwerkverbindungen. Ist als sicherer Ersatz für Telnet und die R-Programme entwickelt worden.
SMB	Server Message Block: siehe CIFS
URL	Uniform Resource Locator: Schema zur Identifikation von Dateien, Dokumenten und anderen Ressourcen im Internet.

Abkürzungsverzeichnis

ACE Access Control Entry

ACL Access Control List

ADSM ADSTAR Distributed Storage Management

AFS Andrew File System

ALG Application Level Gateways

API Application Program Interface

ARP Address Resolution Protocols

ASA Adaptive Security Algorithm

ASCII American Standard Code for Information Interchange

ATM Asynchronous Transfer Mode

CBAC Context-Based Access Control

CGI Common Gateway Interface

CIFS Common Internet File System

CLG Circuit Level Gateways

DCE Distributed Computing Environment

DFN Deutschen Forschungsnetz Vereins

DFS Distributed File System

DHCP Dynamic Host Configuration Protocol

DMZ Demilitarisierte Zone

DNAT Destination Network Address Translation

DNS Domain Name Service

DoS Denial of Service

FH Fachhochschule

FTP File Transfer Protoco

G-WiN Gigabit-Wissenschaftsnetz

GUI Graphical User Interface

HTML Hypertext Markup Language

HTTP Hypertext Transfer Protocol

HTTPS Hypertext Transfer Protocol Secure

ICMP Internet Control Message Protocol

IDS Intrusion Detection System

IEEE Institute of Electrical and Electronics Engineers

IMAP Internet Message Access Protocol

IMAPS Internet Message Access Protocol Secure

IOS Internetwork Operating System

IP Internet Protocol

IPsec Internet Protocol Secure

IPX Internetwork Packet Exchange

IRC Internet Relay Chat

ISDN Integrated Services Digital Network

LAN Local Area Network

LDAP Lightweight Directory Access Protocol

LMU Ludwig-Maximilians-Universität München

LPR Line Printer

LRZ Leibniz-Rechenzentrum der Bayerischen Akademie der Wissenschaften

MAC Media Access Control

MBONE Multicast Backbone

MMS Microsoft Media Server

MTA Mail Transfer Agent

MWN Münchner Wissenschaftsnetz

NAT Network Address Translation

NFS Network File System

NIS Network Information Service

NNTP Network News Transfer Protocol

NTP Network Time Protocol

OPSEC Open Plattform for Security

PAM Pluggable Authentication Modul

PC Personal Computer

POP Post Office Protocol

PPTP Point-to-Point Tunneling Protocol

RDP Reliable Data Protocol

RPC Remote Procedure Call

RTSP Real Time Streaming Protocol

RZ Rechenzentrum

SIP Session Initiation Protocol

SMB Server Message Block

SMTP Simple Mail Transfer Protocol

SNAT Source Network Address Translation

SNMP Simple Network Management Protocol

SOHO Small Office/Home Office

SPOP Secure Post Office Protocol

SQL Structured Query Language

SSH Secure Shell

TACACS Terminal Access Controller Access Control System

TCP Transport Control Protocol

TFTP Trivial File Transfer Protocol

TK Telekommunikation

TOS Type of Service

TSM Tivoli Storage Manager

TUM Technischen Universität München

UDP User Datagram Protocol

URL Uniform Resource Locator

VACL VLAN ACL, Virtual Local Area Network Access Control List

VLAN Virtual Local Area Network

VPN Virtual Private Network

WDM Wavelength Division Multiplexing

WELF WebTrends Enhanced Log Format

WLAN Wireless Local Area Network

WWW World Wide Web

Literaturverzeichnis

[ApLä 02] APOSTOLESCU, V. und A. LÄPPLE: *Das Münchner Wissenschaftsnetz (MWN)*. WWW, Februar 2002, http://www.lrz-muenchen.de/services/netz/mwn-netzkonzept/mwn-netzkonzept.pdf.

[Astaro] *Astaro Security Linux 3.2*. WWW, http://www.astaro.de/html/de/asl.htm.

[BADW] *Benutzungsrichtlinien für Informationsverarbeitungssysteme des Leibniz-Rechenzentrums der Bayerischen Akademie der Wissenschaften*. WWW, Juni 1999, http://www.lrz-muenchen.de/wir/regelwerk/benutzungsrichtlinien/.

[BaHå 02] BALTZERSEN, P. und L. E. HÅLAND: *squidGuard - An ultrafast and free filter, redirector and access controller for Squid*. WWW, März 2002, http://www.squidguard.org/.

[BMI 01] *Erster Periodischer Sicherheitsbericht*. WWW, Juli 2001, http://www.bmi.bund.de/frame/dokumente/Artikel/ix_49371.htm.

[Brüc 00] BRÜCKNER, H.: *Konzeption und Produktauswahl eines Intrusion Detection Systems für das LRZ*. Diplomarbeit, Technische Universität München, Institut für Informatik, November 2000.

[BrLi 00] BRICART, CH. und R. LINK: *AMaViS - A Mail Virus Scanner*. WWW, Oktober 2000, http://www.amavis.org/amavis.html.

[Buyt 01] BUYTENHEK, L.: *bridge - Linux ethernet bridging*. WWW, November 2001, http://bridge.sourceforge.net/.

[Chad 02] CHADD, A.: *Squid Web Proxy Cache*. WWW, September 2002, http://www.squid-cache.org/.

[Cis 02a] CISCO SYSTEMS, INC: *Catalyst 6000 Family - Multilayer Switches*, Oktober 2002, http://www.cisco.com/univercd/cc/td/doc/pcat/ca6000.htm.

[Cis 02b] CISCO SYSTEMS, INC: *Cisco PIX Firewall and VPN Configuration Guide, Version 6.2*, Oktober 2002, http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_sw/v_62/config/index.htm.

[Cis 02c] CISCO SYSTEMS, INC: *Configuring Access Control*, September 2002, http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/sw_7_3/confg_gd/acc_list.htm.

[Cis 02d] CISCO SYSTEMS, INC: *Configuring Context-Based Access Control*, Mai 2002, http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fsecur_c/ftrafwl/scfcbac.htm.

[Cis 02e] CISCO SYSTEMS, INC: *Configuring IP Session Filtering (Reflexive Access Lists)*, April 2002, http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/secur_c/scprt3/scdreflx.htm.

[Cis 02f] CISCO SYSTEMS, INC: *Configuring Lock-and-Key Security (Dynamic Access Lists)*, Mai 2002, http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fsecur_c/ftrafwl/scflock.htm.

[dante] *Dante - A Free Socks Implementation*. WWW, Juni 2002, http://www.inet.no/dante/.

[DR 02] DREO RODOŠEK, G.: *A Framework for IT Service Management*. Habilitationsschrift, Ludwig-Maximilians-Universität München, 2002.

[Fros 01] FROST, S.: *netfilter/iptables - Home*. WWW, November 2001, http://www.netfilter.org/.

[FW-1] *Firewall-1*. WWW, http://www.checkpoint.com/products/protect/firewall-1.html.

[HAN 99a] HEGERING, H.-G., S. ABECK und B. NEUMAIR: *Integriertes Management vernetzter Systeme — Konzepte, Architekturen und deren betrieblicher Einsatz*. dpunkt-Verlag, ISBN 3-932588-16-9, 1999, http://www.dpunkt.de/produkte/management.html.

[Hege 01] HEGERING, H.-G.: *Brief: Missbräuchliche Nutzung der Netze*. WWW, Oktober 2001, http://www.lrz-muenchen.de/services/security/sec-brief/.

[Hunt 95] HUNT, C.: *TCP/IP — Netzwerk Administration*. O'Reilly Verlag, ISBN 3-930673-02-9, 1995.

[IANA] *IANA - Protocol/Number Assignments Directory*. WWW, April 2002, http://www.iana.org/numbers.html.

[Lort 00] LORTZ, B.: *Maßnahmen zur Abwehr von Angriffen auf Rechensysteme über Netzverbindungen*. Technischer Bericht, Universität Karlsruhe, Rechenzentrum, März 2000, http://www.rz.uni-karlsruhe.de/Uni/RZ/Netze/Sicherheit/FW_SichKon.pdf.

[Läpp 01] LÄPPLE, A.: *Richtlinien zum Betrieb des Münchner Wissenschaftsnetzes (MWN)*. WWW, Oktober 2001, http://www.lrz-muenchen.de/wir/regelwerk/netzbenutzungsrichtlinien/.

[Läpp 02] LÄPPLE, A.: *Einschränkungen und Regeln im Netzbetrieb*. WWW, September 2002, http://www.lrz-muenchen.de/services/netz/einschraenkung/.

[milter] *Milter: Helping You Mangle Your Mail At Will*. WWW, September 2002, http://www.milter.org/.

[openwall] *Linux kernel patch from the Openwall Project*. WWW, September 2002, http://www.openwall.com/linux/.

[Pank 00] PANKE, P.: *Konzeption und Produktauswahl eines externen Security-Scanners für das LRZ*. Diplomarbeit, Technische Universität München, Institut für Informatik, November 2000.

[Proe 98] PROEBSTER, W. E.: *Rechnernetze — Technik Protokolle Systeme Anwendungen*. Oldenburg Verlag, ISBN 3-486-24540-6, 1998.

[Rank 00] RANK, C.: *Netzwerksicherheit an der Universität Passau - Entwurf*. Technischer Bericht, Universität Passau, Rechenzentrum, Oktober 2000.

[RZ-KA] *Grundeinstellung für die Firewallsysteme der Universitätsinstitute*. WWW, `http://www.rz.uni-karlsruhe.de/Uni/RZ/Netze/Sicherheit/FW_GrundEin.html`.

[Schu] DE SCHUYMER, B.: *Ebtables homepage*. WWW, `http://users.pandora.be/bart.de.schuymer/ebtables/`.

[Selo] SELOS, W.: *Eine einfache Firewall-Lösung*. WWW, `http://www.zid.tuwien.ac.at/security/firewall.php`.

[sendmail] *Sendmail Homepage*. WWW, Oktober 2002, `http://www.sendmail.org/`.

[Tane 98] TANENBAUM, A. S.: *Computernetzwerke*. Prentice Hall, ISBN 3-8272-9568-8, 1998.

[Weis] WEIS, D.: *Proxy ARP with Linux*. WWW, `http://www.sjdjweis.com/linux/proxyarp/`.

[Wimm 01] WIMMER, C.: *Kochrezept für die Wartung von Netzkomponenten hinter einem Paketfilter (Firewall)*. WWW, Oktober 2001, `http://www.lrz-muenchen.de/services/security/kochrezept-fw/`.

[XBB 02] XIE, H., PH. BIONDI und S. BREMER: *LIDS Project - Secure Linux System*. WWW, April 2002, `http://www.lids.org/`.

[Youn 01] YOUNG, K.: *FWTK FAQ*. WWW, November 2001, `http://www.iem.RWTH-Aachen.DE/mirrors/www.fwtk.org/fwtk/faq/`.

[Zieg 00] ZIEGLER, R.: *Linux Firewalls — Konzeption und Implementierung für kleine Netzwerke und PCs*. Markt+Technik Verlag, ISBN 3-8272-5849-9, 2000.