

# Entwicklung und Umsetzung eines technischen Konzeptes "Firewalltechniken"

Version 1.4/20.06.2000

Lehrgebiet Rechnernetze und Verteilte Systeme  
Universität Hannover

Bernd Böker  
boeker@rvs.uni-hannover.de

## Inhaltsverzeichnis

<b>1</b>	Vorwort.....	5
<b>2</b>	Einleitung .....	6
<b>3</b>	Bestandsaufnahme .....	6
3.1	Netz-Komponenten des lokalen Netzes .....	6
3.2	Analyse der Schwachstellen.....	7
3.2.1	Übergänge in andere Netze .....	7
3.2.1.1	Einwahlverbindungen .....	8
3.2.1.2	Telefonanlagen.....	8
3.2.1.3	Faxserver .....	8
3.2.2	Firewall .....	8
3.2.3	Inhaltliche Schwachstellen.....	10
3.2.3.1	Aktive Web-Inhalte .....	10
3.2.3.2	Viren/Trojanische Pferde .....	10
3.3	Aufbau des izn-net.....	10
<b>4</b>	Technisches Konzept .....	12
4.1	Kommunikationsanforderungen.....	12
4.2	Auswahl der Netzdienste.....	12
4.3	Festlegung der Schutzstufe.....	15
4.4	Sicherheitspolitik .....	15
4.4.1	Anordnung von Server-Komponenten.....	16
4.4.2	Protokollentkopplung.....	17
4.4.2.1	HTTP.....	17
4.4.2.2	FTP .....	18
4.4.2.3	Mail.....	19
4.4.3	Sammeln von Logging-Informationen .....	21
4.4.3.1	Separater Logserver .....	21
4.4.3.2	Snipped Wire.....	21
4.4.3.3	Audit .....	22

4.4.3.4	Netzwerk-Monitore .....	23
4.4.4	Organisatorische Regelungen .....	23
4.5	Anforderungen an ein Firewall-System .....	24
4.5.1	Paketfilter .....	24
4.5.2	Application-Gateway.....	24
4.5.3	Protokollierung .....	24
4.6	Besondere Anforderungen für Netze mit sensitiven Daten .....	25
4.6.1	Graphical Wall .....	25
4.6.2	Trennung von Netzbereichen .....	26
4.6.3	Kryptografische Sicherheitsmaßnahmen.....	27
4.7	Auswahl einer Firewall.....	27
4.8	Festlegung von Firewall-Regeln.....	28
<b>A</b>	<b>Sicherheitshinweise für Windows NT .....</b>	<b>30</b>
A.1	Sichere Passworte.....	30
A.2	Minimierung der Systemdienste.....	30
A.3	Umbenennen der Administratorkennung .....	32
A.4	Aktivierung des Logbuchs.....	33
A.5	NTFS-Dateisystem .....	33
A.6	Sichern der Konsole.....	34
A.7	Installieren von Patches und Service Packs .....	34
A.8	Sichern der Registry und der Benutzerkontendatenbank.....	34
<b>B</b>	<b>Installation der Checkpoint Firewall-1 .....</b>	<b>35</b>
B.1	Installation.....	35
B.2	Netzskizze .....	36
B.3	Regeln des Firewall-Moduls .....	37
B.4	Zeitschemata .....	38
B.5	Services .....	38
B.6	Netzwerkobjekte .....	39
B.6.1	Workstations.....	39
B.6.2	Gruppen .....	40
B.7	Benutzer und Nutzergruppen .....	40

B.8	Address Translation .....	41
B.9	Properties Setup .....	41
B.9.1	Security Policy .....	42
B.9.2	Services .....	43
B.9.3	Log and Alert .....	44
B.9.4	Security Servers .....	45
B.9.5	Authentication .....	46
B.9.6	SYNDefender .....	47
B.9.7	Resolving .....	48
B.9.8	Miscellaneous .....	49
B.9.9	AccessLists .....	50
B.10	Auswertung der Log-Informationen.....	50
B.11	Konfiguration der WWW-Klienten.....	51
B.11.1	WWW-Zugriff mit Netscape .....	51
B.11.2	WWW-Zugriff mit Internet-Explorer 5 .....	51

## 1 Vorwort

Das vorliegende Konzept *Entwicklung und Umsetzung eines technischen Konzeptes "Firewalltechniken"* ist im Auftrag des Landesbeauftragten für den Datenschutz Niedersachsen erstellt worden. Das Ziel dieses Konzeptes ist, eine sichere Anbindung der Dienststellen des Landes Niedersachsen an das izn-net, ein privates Intranet des Landes Niedersachsen, zu ermöglichen. Dabei wird das izn-net aufgrund seiner Größe, der physikalischen Ausdehnung, der großen Anzahl der Nutzer und der Vielzahl an administrativen Stellen wie ein unsicheres Netz betrachtet.

Die Ausführungen in diesem Konzept sind so ausgelegt, dass sie als Orientierung für die Dienststellen des Landes benutzt werden können, auch wenn sie exemplarisch für das LAN des LfD aufgebaut worden sind.

Hannover, den 20. Juni 2000

## 2 Einleitung

Mit der Öffnung des Datennetzes der Landesregierung (izn-net) zum Internet und dem Aufbau von Intranets in den Landesdienststellen werden neue Möglichkeiten der kooperativen Zusammenarbeit geboten, die für die Dienststellen zunehmend an Bedeutung gewinnen. Neben dem Zugriff auf Informationen aus dem Internet wird auch eine verbesserte Kommunikation mit anderen Landeseinrichtungen sowie die Bereitstellung eines eigenen Internet- und Intranetangebots im izn-net ermöglicht.

Die neuen Möglichkeiten durch die Nutzung des Internet sollen dabei den Mitarbeitern an ihren Arbeitsplatzrechnern zur Verfügung stehen. Es entsteht daher die Motivation, das Dienststellen-LAN mit dem izn-net zu verbinden.

Die Verbindung von Dienststellen-LAN und izn-net bietet aber nicht nur Vorteile, sie erhöht auch die Gefährdung der lokalen Infrastruktur und Daten durch Angriffe aus den anderen an das izn-net angeschlossenen Einrichtungen oder dem Internet. Durch das Eindringen nichtautorisierter Personen in das Intranet besteht die Gefahr der Manipulation der lokal gespeicherten Daten. Durch Spionage besteht die Gefahr des Verlustes der Vertraulichkeit von Informationen.

Auch wenn das izn-net zum Internet über eine High-Security-Firewall geschützt ist, so ist dennoch von einem hohen Gefahrenpotential durch die Größe des izn-net und die große Anzahl der angeschlossenen Einrichtungen sowie die große räumliche Ausdehnung, die sich über ganz Niedersachsen erstreckt, auszugehen. Es wird daher eine Anbindung gesucht, die den hohen Sicherheitsanforderungen der Landesdienststellen genügt.

Um einen umfassenden Schutz der Dienststellen-LAN gewährleisten zu können, ist eine Bestandsaufnahme der lokalen Netzkomponenten erforderlich. In diesem Konzept, das vom Landesbeauftragten für den Datenschutz Niedersachsen (LfD) in Auftrag gegeben worden ist, wird diese Bestandsaufnahme exemplarisch am LAN des LfD vorgenommen. Die hier gewonnenen Ergebnisse sind mit kleineren Änderungen auch auf die anderen Dienststellen zu übertragen. Hierauf aufbauend wird eine Analyse möglicher Schwachstellen in den lokalen Netzen und Möglichkeiten zu deren Behebung vorgestellt. Das technische Konzept beinhaltet dann die Beschreibung der Kommunikationsanforderungen sowie Auswahl der Netzdienste, die für die Kommunikation genutzt werden sollen. Auf Basis dieser Informationen wird eine Realisierung zur Anbindung der Dienststellen-LAN an das izn-net unter Nutzung moderner Firewall-Techniken vorgestellt.

## 3 Bestandsaufnahme

### 3.1 Netz-Komponenten des lokalen Netzes

Für eine Bestandsaufnahme der Dienststellen-LAN dient exemplarisch das Netz des Landesbeauftragten für den Datenschutz (LfD). Hierbei handelt es sich um ein auf TCP/IP basiertes LAN, das mit IP-Adressen aus dem für private Zwecke reservierten Adressbereich 10.x.x.x eingerichtet ist.<sup>1</sup> Die

---

<sup>1</sup> Vgl. [RFC1918].

Vergabe der Subnetze des 10er-Netzes ist vom IZN erfolgt und damit innerhalb des izn-net und der hier angeschlossenen Einrichtungen eindeutig.

Im LAN des LfD sind ca. 20 Arbeitsplatzrechner eingerichtet, als Desktop-Betriebssystem wird Windows NT Workstation 4.0 verwendet. Als lokaler Server dient ein Windows NT Server 4.0, der vorrangig die Aufgaben eines Mail- und Kommunikationservers übernimmt.

Der Informationsaustausch innerhalb des LfD bzw. zum IZN erfolgt über einen Microsoft Exchange Server, wobei Microsoft Outlook als Mailklient auf den Workstations eingesetzt wird.

Der Mailaustausch zu anderen Einrichtungen des Landes erfolgt über das X.400-Protokoll. Es besteht daher eine Anbindung des Mail-Servers an das X.400-Gateway des IZN über ein separate Netzwerk-Karte des Mail-Servers (vgl. Abbildung 1). Hiermit soll verhindert werden, dass eine direkte Verbindung zwischen dem izn-net und dem lokalen Netz geschaffen wird. Dieses Interface wird direkt auf den IZN-Router geführt.

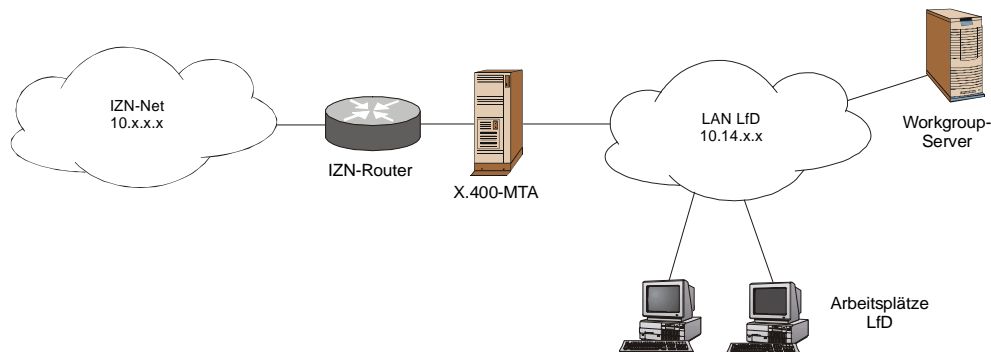


Abbildung 1: Topologie des Dienststellen-LAN des LfD

Das LfD plant den Einsatz einer Firewall zur Anbindung an das izn-net, über die die Kommunikation und der Informationsaustausch mit den anderen Landeseinrichtungen erfolgen soll. Diese Anbindung soll gleichzeitig als kontrollierte Verbindung zum Internet verwendet werden. Es ist daher die Firewall-Software Checkpoint Firewall-1 für Windows NT mit einer Lizenz für 25 interne Knoten beschafft worden.

## 3.2 Analyse der Schwachstellen

Für einen sicheren Betrieb eines Firewall-geschützten Netzes ist es wichtig, die Schwachstellen dieses Netzes zu kennen. Dabei spielt die Firewall als zentrales Element zwar die wichtigste Rolle, es ist aber dennoch immer die Gesamtheit des Netzes mit allen Komponenten zu betrachten. Ein besonderes Augenmerk muss hier auf alle Netzübergänge wie z. B. Faxserver gelegt werden, da hier mögliche illegale Zugriffe auf das Intranet geschaffen werden können. Im folgenden sollen die Schwachpunkte der Bestandsaufnahme näher beleuchtet und bewertet werden.

### 3.2.1 Übergänge in andere Netze

Im Sicherheitskonzept muss festgelegt werden, dass neben der Firewall keine Übergänge in andere Netze existieren dürfen. Dies gilt auch für Wählverbindungen zum Telekommunikationsnetz, so z. B. Einwählverbindungen in das Datennetz, Verbindung von Telefonanlagen mit dem Datennetz und Faxserver. Im folgenden werde die Gefahren der Schwachstellen analysiert.

### 3.2.1.1 Einwahlverbindungen

Durch Einwahlverbindungen z. B. auf Terminalserver ist es möglich, direkt auf das Datennetz zuzugreifen. In der Regel sind diese Einwahlverbindungen durch einen Benutzernamen und Kennwort geschützt, diese werden aber häufig unverschlüsselt übertragen oder sind auf dem einwählenden Rechner dauerhaft hinterlegt, so dass die Authentizität des Benutzers nicht gewährleistet ist. Aus diesem Grunde müssen Einwahlverbindungen prinzipiell als unsicher angesehen werden und zusätzlich durch geeignete Sicherheitsmassnahmen geschützt sowie eine geeignete Authentisierung der Benutzer durchgeführt werden.

### 3.2.1.2 Telefonanlagen

Viele Telefonanlagen bieten die Möglichkeit, über eine LAN-Schnittstelle an das Datennetz gekoppelt zu werden, um dann direkt von einem Rechner im lokalen Netz konfiguriert werden zu können. Auch diese Verbindung stellt ein Sicherheitsrisiko dar, da die Möglichkeit des Eindringens über die Telefonanlage in das Datennetz nicht ausgeschlossen werden kann.

### 3.2.1.3 Faxserver

Auch bei Faxservern besteht die Möglichkeit, durch Ausnutzung von evtl. vorhandenen Schwachstellen in der Software einen unbefugten Zugriff auf den Server über die Telefonleitung zu erlangen. Damit kann von hier aus auf das Datennetz zugegriffen werden, an dem der Faxserver angeschlossen ist. Aus diesem Grunde darf der Faxserver nicht im lokalen Datennetz angeschlossen werden.<sup>2</sup>

## 3.2.2 Firewall

Die Firewall als zentrales Element der Sicherheitspolitik muss ausreichend gegen feindliche Angriffe geschützt werden. Dabei werden Gefährdungen, die aus dem gesicherten Netz heraus kommen, genauso berücksichtigt wie Gefährdungen aus dem externen Netz.<sup>3</sup>

Handelt es sich bei der eingesetzten Firewall um eine Architektur, die auf Windows NT aufsetzt, so sind hier besondere Vorkehrungen zu treffen, da bereits bekannte und behobene Fehler des Betriebssystems durch das Einspielen neuerer Updates immer wieder auftreten. Es konnte in der Vergangenheit außerdem häufiger festgestellt werden, dass für bekannte Schwachstellen zunächst nur Fehlerkorrekturen für die US-Amerikanische Version des Betriebssystems zur Verfügung stehen, internationale Korrekturen sind oft erst nach Wochen verfügbar. In dieser Zeit ist das System über die vorhandenen und öffentlich bekannten Schwachstellen angreifbar.<sup>4</sup>

Auch wenn die Firewall-Komponenten sich zwischen der Vermittlungsschicht und der Sicherungsschicht in den Protokoll-Stack des Rechnersystems einbettet (Vgl. Abbildung 2 am Beispiel der Checkpoint Firewall-1), so können dennoch nicht alle Sicherheitsrisiken ausgeschlossen werden.

---

<sup>2</sup> Faxserver enthalten in der Regel Datenmodems und bieten somit eine mögliche Angriffsstelle über die Modem-Verbindung.

<sup>3</sup> Nach Angaben des CERT erfolgen ca. 80% der Angriffe aus dem lokalen Netz.

<sup>4</sup> Vgl. CERT-Advisories des DFN-CERT.

Aus diesen Gründen wird eine Firewall-Architektur empfohlen, die mit zusätzlichen Paketfiltern zu beiden Netzen geschützt wird.<sup>5</sup>

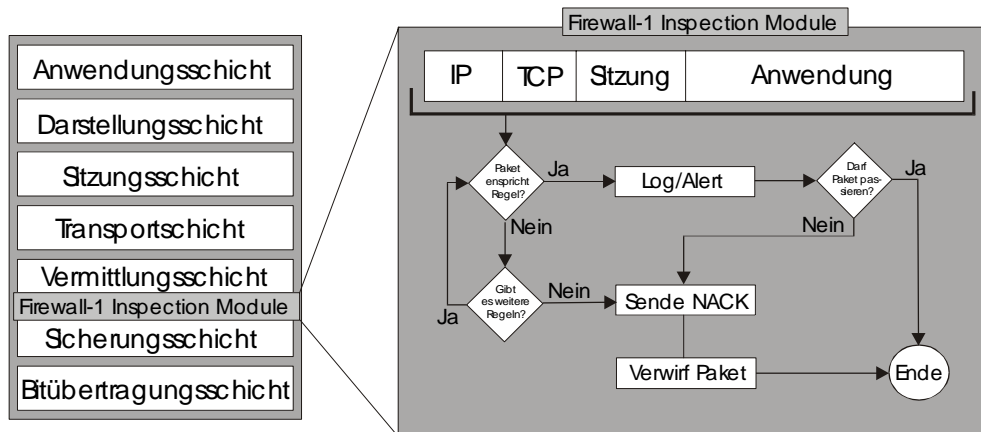


Abbildung 2: Architektur des Firewall-1 Inspection Moduls (Quelle: [Ckp98])

Zusätzlich muss eine Optimierung des Betriebssystems nach sicherheitstechnischen Gesichtspunkten vorgenommen werden. Windows NT wird mit sehr weitgehenden Zugriffsrechten auf das Dateisystem und auf die Registrierung ausgeliefert. Wenn diese Zugriffsrechte nicht nach der Installation entsprechend den lokalen Sicherheitsanforderungen restriktiver eingestellt werden, besitzt jeder Benutzer Zugriff auf alle Dateien und auf die gesamte Registrierung, d.h. der Zugriffsschutz ist de facto ausgeschaltet. Weiterhin ist Windows NT nicht in der Lage, den Zugriff auf Disketten- und CD-ROM-Laufwerke sowie auf Bänder zu kontrollieren, so dass hier eine Möglichkeit zu unzulässigem Datenimport- und export besteht, wenn nicht durch zusätzliche Maßnahmen der Zugriff auf diese Datenträger eingeschränkt oder zumindest auf organisatorischer Ebene kontrolliert wird.

Für die Administrator-Kennung bestehen bei einer Standardinstallation unzureichende Schutzmechanismen. Diese Kennung wird nicht durch eine automatische Sperrung bei wiederholten Login-Versuchen geschützt. Wird die Administrator-Kennung nicht auf einen nicht leicht erratbaren Namen umbenannt, ist sie einem erhöhten Einbruchrisiko ausgesetzt.

Um einen unautorisierten physikalischen Zugriff auf das Firewall-System auszuschließen, muss der Rechner in einem nicht-öffentlichen Bereich aufgestellt werden.

Die im Anhang A genannten Maßnahmen zur Absicherung von Rechnersystemen unter Windows NT müssen daher für ein Firewall-System unbedingt umgesetzt werden. Zusätzlich sollte die Firewall durch Paketfilter geschützt werden, die auf beiden Seiten die Verbindungen zum externen Netz sowie zum Intranet herstellen.<sup>6</sup> Die Paketfilter sichern das Firewall-System zusätzlich vor unbefugten Zugriffen auf das System. Diese Maßnahme wird auch aufgrund der großen Anzahl von Sicherheitswarnungen, die über das CERT weitergegeben werden, als zwingend notwendig angesehen.

<sup>5</sup> Vgl. Kapitel 4.6.

<sup>6</sup> Vgl. auch Abbildung 13.

### 3.2.3 Inhaltliche Schwachstellen

#### 3.2.3.1 Aktive Web-Inhalte

Durch das Übertragen von aktiven Web-Inhalten (z. B. ActiveX, JavaScript oder Java) werden Anweisungen auf dem Rechner des WWW-Benutzers ausgeführt. Durch Sicherheitslöcher in der verwendeten Klientensoftware (meist Microsoft Internet Explorer oder Netscape Navigator) kann die Ausführung des Codes zum Auslesen von Daten auf des Benutzerrechners oder zu Denial-of-Service-Angriffen benutzt werden.

#### 3.2.3.2 Viren/Trojanische Pferde

Viren und Trojanische Pferde werden über Verbindungen zum Internet (z. B. per WWW oder Mail) auf den lokalen Rechner kopiert. Sie können auch über Disketten oder andere Medien eingeschleust werden. Befinden sie sich einmal im lokalen Netz, sind sie oftmals schnell verbreitet. Während Viren in der Regel ausschließlich zerstörende Wirkungen haben, werden Trojanische Pferde meist zum Ausspähen von Daten benutzt.

Ein Computer-Virus ist eine nicht selbständige Programmroutine, die sich selbst reproduziert und dadurch vom Anwender nicht kontrollierbare Manipulationen in Systembereichen, an anderen Programmen oder deren Umgebung vornimmt. Die Eigenschaft der Reproduktion führte in Analogie zum biologischen Vorbild zu der Bezeichnung "Virus". Die Möglichkeiten der Manipulation sind sehr vielfältig. Besonders häufig sind das Überschreiben oder das Anlagern des Virus-Codes an andere Programme und Bereiche des Betriebssystems.

Ein Trojanisches Pferd ist ein Programm mit einer verdeckten, nicht dokumentierten Funktion oder Wirkung. Der Benutzer kann daher auf die Ausführung dieser Funktion keinen Einfluss nehmen, insofern besteht eine gewisse Verwandtschaft mit Computer-Viren. Es ist jedoch keine Selbstreproduktion vorhanden. Als Träger für Trojanische Pferde lassen sich alle möglichen Anwenderprogramme benutzen. Aber auch Scriptsprachen, wie Batch-Dateien, ANSI-Steuersequenzen, Postscript u. ä., die vom jeweiligen Betriebssystem oder Anwenderprogramm interpretiert werden, können für schädliche Funktionen missbraucht werden. Die Schadwirkung eines Trojanischen Pferdes ist um so wirkungsvoller, je mehr Rechte sein Trägerprogramm besitzt.

### 3.3 Aufbau des izn-net

Bei dem vom IZN betriebenen landeseinheitliches Telekommunikationsnetz (izn-net<sup>7</sup>) handelt es sich um ein Wide Area Network (WAN), das die Liegenschaften des Landes und die Citynetze (Metropolitan Area Network, MAN) einschließt. Neben der Landesverwaltung und Körperschaften des öffentlichen Rechts wurden auch die Netze der Polizei und der Oberfinanzdirektion integriert.<sup>8</sup>

Das izn-net verfügt derzeit über rund 1500 Netzzugänge mit Übertragungsraten von 64 kbps bis 34 Mbps, die als Festverbindungen, Einwahlverbindungen oder Richtfunkverbindungen realisiert sind. Die Topologie des Netzes stützt sich auf ein Backbone mit Hauptnetzknotten in den Standorten Oldenburg, Lüneburg, Braunschweig und Hannover, die über Festverbindungen mit 34 Mbps untereinander verbunden sind.

---

<sup>7</sup> Das Netz trug früher den Namen KOMNET.

<sup>8</sup> Vgl. [Kös00].

Das izn-net kann auf einer flächendeckend installierten Infrastruktur den jeweiligen Anforderungen entsprechend als ein Virtual Private Network (VPN) betrieben werden. Geschlossene Benutzergruppen als VPN innerhalb des izn-net sind ebenfalls möglich. Ausfallsicherheit wird im Backbone über Backupschaltungen durch Vermaschung der Netzverbindungen zwischen den Netzwerkknoten erreicht.

Das izn-net ist über eine High-Security-Firewall mit dem Internet verbunden (vgl. Abbildung 3), bei der die interne Struktur des izn-net nach außen verborgen bleibt. Sie besteht aus den Komponenten Paketfilter - Application-Gateway - Paketfilter und bietet den nach Stand der Technik umfassendsten Schutz. Aus dem izn-net können damit die Internet-Dienste WWW, FTP und E-Mail genutzt werden. Der Verbindungsaufbau aus dem Internet in das izn-net wird durch die Firewall mit Ausnahme von E-Mail nicht gestattet.

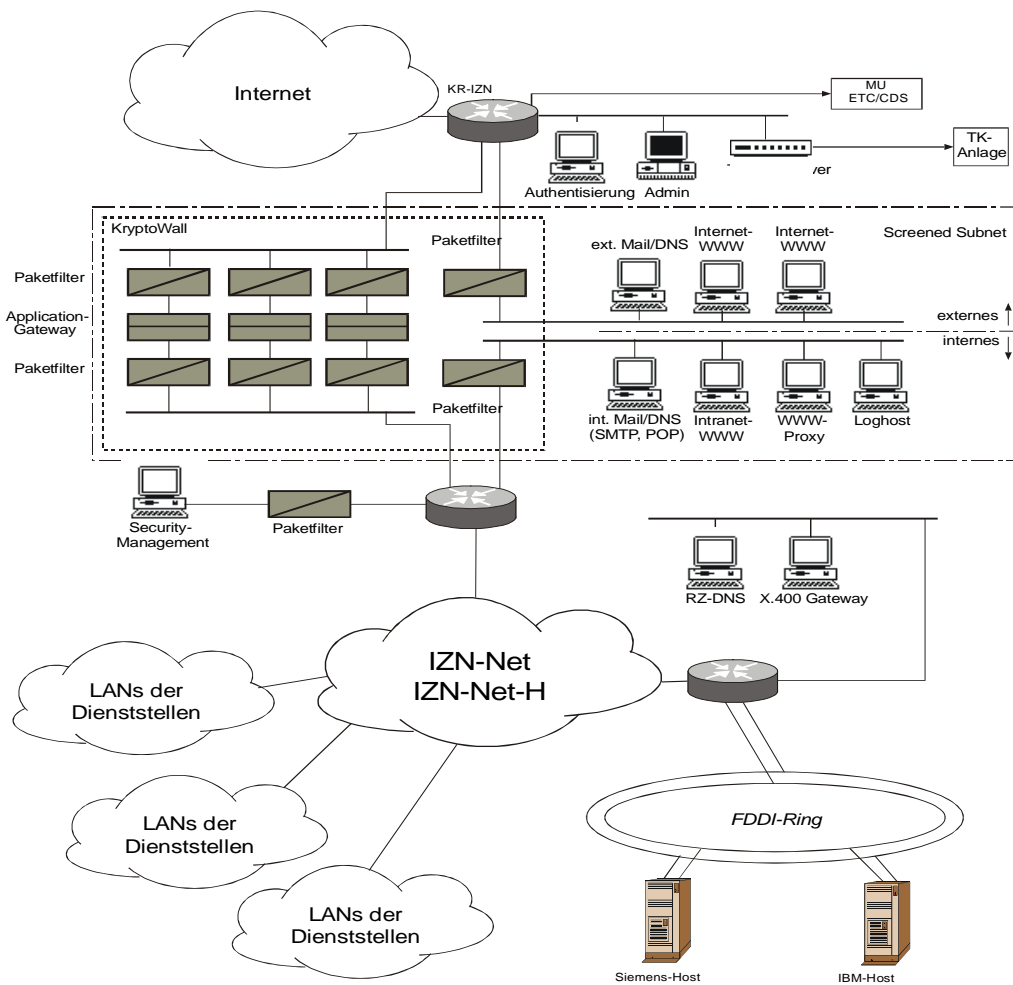


Abbildung 3: Aufbau des izn-net

Server mit Diensten, die öffentlich zugänglich sind, werden in Grenznetzen über Paketfilter vor dem unbefugten Zugriff geschützt. Über die Paketfilter werden nur die zugelassenen Dienste freigeschaltet. Im externen Grenznetz befinden sich die Server mit dem Internetangebot der Dienststellen sowie Mail- und DNS-Server. Das interne Grenznetz enthält die Server mit Dienstangeboten für die am izn-net angeschlossenen Einrichtungen, so z. B. ein WWW-Proxy-Server für die Nutzung des WWW im Internet.

Über das izn-net werden vom IZN zentrale Dienste für die Einrichtungen des Landes angeboten, so z. B. IBM- und Siemens-Hosts, der zentrale X.400-Mailserver oder das Finanzbuchhaltungssystem. Diese sind im Einzelfall noch über Paketfilter gesichert.

## 4 Technisches Konzept

### 4.1 Kommunikationsanforderungen

Alle Kommunikationsbeziehungen zwischen dem Dienststellen-LAN und dem izn-net basieren auf dem Internet Protocol (IP). Andere Transportprotokolle wie z. B. NetBeui, Internet Packet Exchange (IPX) oder Appletalk werden nicht unterstützt. Zur Verbindung der X.400-MTAs wird das *ISO Transport Services on Top of the TCP<sup>9</sup>* genutzt, das die Verbindung von ISO-TSAP über TCP/IP festlegt.

Die zu erwartende Datenrate der Verbindung ist abhängig von den zur Verfügung stehenden Diensten und der Anzahl der Nutzer im LAN. Es ist zu erwarten, dass der am meisten genutzte Dienst WWW sein wird. Bei einer geringen Anzahl von Nutzern kann eine Verbindung mit 10 Mbps ausreichend sein. Einrichtungen mit einer größeren Nutzerzahl ist zu empfehlen, eine Verbindung mit 100 Mbps vorzusehen. In den Fällen, bei denen Einrichtungen über ISDN-Leitungen angebunden sind, sollte der Einsatz von WWW-Proxy-Servern zur Reduktion der Last auf den Verbindungsleitungen vorgesehen sein.

Die Verbindungseinrichtung der Datenkommunikation ist vorrangig nach außen gerichtet, so dass kein Verbindungsaufbau aus dem izn-net in das LAN möglich ist. Die einzige Ausnahme bildet die Verbindung der X.400-Mailserver, die in beiden Richtungen aufgebaut werden kann.

### 4.2 Auswahl der Netzdienste

Die Verbindung zwischen den Dienststellen des Landes und des izn-net soll vorrangig der Kommunikation der Dienststellen untereinander und der Nutzung von Informationsdiensten im Landes-Intranet dienen. Die wichtigsten Netzdienste werden daher das *World Wide Web (WWW)* und der Mail-Dienst sein. Beim Betrieb eines WWW-Servers im izn-net für die Intranet-Präsentation der Dienststelle ist außerdem das *File Transfer Protocol (FTP<sup>10</sup>)* erforderlich, um die Inhalte im WWW-Server einzupflegen.

Dienststellen mit Finanzbuchhaltungssystemen benötigen außerdem einen Zugriff auf den zentralen Finanzbuchhaltungsserver, der vom IZN betrieben wird.

Für die Nutzung des WWW im Internet kann auf die zentralen Dienste des IZN zugegriffen werden, das einen WWW-Proxy-Server betreibt. Andere Internet-Dienste (wie z. B. das Diskussionsforum News oder Zugriff auf Bibliothekssysteme mit PICA) können direkt über die Internet-Firewall des IZN geführt werden.

Alle anderen Dienste werden zunächst nicht zugelassen.

---

<sup>9</sup> Vgl. [RFC983].

<sup>10</sup> Vgl. [RFC959].

### World Wide Web (WWW) als Intranet-Informationsdienst

Viele Dienststellen und das IZN befinden sich z. Z. im Aufbau eines Intranet-Angebotes, das über den Dienst WWW bereitgestellt wird. Als Transportprotokoll dient das *Hypertext Transport Protocol (HTTP)*<sup>11</sup>. Für den Aufbau eines eigenen Informationsservers bleibt zu prüfen, wie dieser in die Netztopologie eingebunden wird.

### Electronic Mail (Email)

Der Mailaustausch innerhalb des Landes Niedersachsen wird über das X.400-Protokoll abgewickelt. Dafür ist eine Verbindung zwischen dem Mailserver der Dienststellen und der zentralen MTA des IZN über das Protokoll ISO-TSAP (Port 102)<sup>12</sup> erforderlich. Mails zu anderen Dienststellen werden vom IZN-MTA weitergeleitet, so dass keine weiteren Verbindungen zu anderen MTAs benötigt werden.

Für das Versenden von Mails an Empfänger im Internet ist eine Konvertierung der Mails zum Transport über das *Simple Mail Transfer Protocol (SMTP)*<sup>13</sup> erforderlich. Diese Konvertierung wird ebenfalls vom IZN-MTA übernommen und automatisch für alle Empfänger ausgeführt, die nicht über X.400 erreicht werden können. Das Empfangen von Mails aus dem Internet wird ebenfalls über den IZN-MTA realisiert, der alle Mails aus dem Internet über SMTP empfängt und nach X.400 konvertiert.

### File Transfer Protocol (FTP)

Ein Zugriff mittels FTP auf Server im izn-net ist insbesondere für Administratoren und Betreuer von WWW-Seiten notwendig, die mit der Wartung der Rechnersysteme oder Web-Inhalten betraut sind. Daher soll berücksichtigt werden, dass für einzelne Personen ein FTP-Zugang möglich ist.

Die Möglichkeit zum Download von Treibern und aktueller Software kann auch mittels FTP über das HTTP-Protokoll ermöglicht werden. Dies setzt voraus, dass ein Proxy-Server im izn-net genutzt werden kann.

Zur Vereinfachung des Zugriffs und Reduzierung der Last über die Firewall wird die Einrichtung eines FTP-Spiegel-Servers im izn-net diskutiert, der Daten von verschiedenen Internet-Servern im Intranet vorhält.

### telnet/Secure Shell

Für die Einrichtung von Dialogsitzungen wird zunächst kein Bedarf gesehen. Erst bei der Betreuung von Servern im äußeren Grenznetz ist ein Zugang über telnet<sup>14</sup> oder Secure Shell (ssh)<sup>15</sup> notwendig

---

<sup>11</sup> Vgl. [RFC2068].

<sup>12</sup> Vgl. [RFC983].

<sup>13</sup> Vgl. [RFC821].

<sup>14</sup> Vgl. [RFC854].

<sup>15</sup> Vgl. [SSH].

und kann dann zugelassen werden. Hier ist eine einfache Authentisierung mittels Benutzername und Kennwort vorgesehen.

### **World Wide Web (WWW) als Internet-Dienst**

Für die Nutzung des WWW im Internet stellt das IZN einen Proxy-Server bereit, der von den Dienststellen angesprochen werden kann. Der Zugang zum Proxy-Server wird auf Antrag der Dienststelle freigeschaltet.

Zur Reduktion der Netzlast und Erhöhung der Sicherheit sollte geprüft werden, ob der Einsatz eines Proxy-Servers im LAN der Dienststelle sinnvoll ist.

### **FTP auf Internet-Server**

Zur Pflege des eigenen WWW-Servers im Internet sowie für administrative Zwecke (z. B. Download von Treibersoftware) ist der Zugriff per FTP auf Server im Internet erforderlich. Die Technikfolgenabschätzung *izn-net*<sup>16</sup> legt fest, dass die FTP-Verbindung nach Möglichkeit über das HTTP-Protokoll geführt werden soll. Eine direkte FTP-Verbindung sollte daher nur in Einzelfällen eingerichtet werden.

### **News**

Der Zugang zum Internetdienst News ist für einige Ressorts von größerer Bedeutung. In einem ersten Schritt ist daher der Zugriff auf dedizierte Newsserver, so z. B. den Newsservern des Regionalen Rechenzentrums für Niedersachsen (RRZN) und der Softwarefirma Microsoft, eingerichtet. Als Zugriffsprotokoll dient das *Network News Transfer Protocol (NNTP)*<sup>17</sup>. Es muss geprüft werden, inwieweit das Betreiben eines eigenen Newsservers sinnvoll werden kann, wobei hier die bestimmenden Faktoren Anzahl der Nutzer und übertragenes Datenvolumen zu beobachten sind. Es ist ebenso von Bedeutung, ob seitens der Nutzer ein Interesse besteht, eigene Foren für die Diskussion landesspezifischer Themen einzurichten.

### **PICA**

Über das Protokoll PICA ist ein Zugriff auf die Datenbestände der Universitätsbibliothek/Technische Informationsbibliothek möglich. Es handelt sich hierbei um eine TCP-Verbindung, die auf einen dedizierten Port eines Servers in der Technischen Informationsbibliothek Hannover (TIB) geführt wird. Dieser Zugang ist für einzelne Personen und Gruppen notwendig und kann bei Bedarf auch aus dem Dienststellen-LAN eingerichtet werden.

### **Finanzbuchhaltung (P53)**

Dienststellen, die am Projekt P53 teilnehmen, benötigen Zugriff auf den Finanzbuchhaltungsserver (Baan-Server) im *izn-net*. In der vorliegenden Version des Buchungssystems wird hierfür eine TCP-Verbindung auf Port 512 (remote exec) benötigt.

---

<sup>16</sup> Vgl. [TFA-IN].

<sup>17</sup> Vgl. [RFC977].

Zur Pflege der Klienten-Software ist eine Netzverbindung zwischen einem Software-Distribution-Server im izn-net und den Baan-Klienten erforderlich. Der Software-Distribution-Server pflegt die Daten auf den Klientensystemen ein und benötigt hierfür eine Verbindung mittels Secure FTP (sftp, Port 115) auf die Klientensysteme. Bei dieser Verbindung ist zu beachten, dass eine Verbindung von einem externen Rechner zu Systemen im lokalen Netz eingerichtet wird.

### 4.3 Festlegung der Schutzstufe

Im Allgemeinen ist davon auszugehen, dass in den Landesverwaltungen personenbezogene Daten verarbeitet werden, die den Schutzstufen A bis C zuzuordnen sind.<sup>18</sup> In diesen Fällen sollte die Nutzung der oben beschriebenen Netzdienste möglich sein, wenn die im folgenden beschriebenen technischen und organisatorischen Maßnahmen umgesetzt werden. Die Nutzer sind über das höhere Restrisiko, das von der Verbindung der Netze ausgeht, in Kenntnis zu setzen und zur Einhaltung einer noch zu erstellenden Dienstanweisung zu verpflichten.

### 4.4 Sicherheitspolitik

Bei der Anbindung der Dienststellen-LAN der Landesregierung Niedersachsen an das izn-net wird das Ziel verfolgt, die schutzbedürftigen Daten in den lokalen Netzen vor unbefugtem Zugriff zu sichern. Es soll die Integrität und Verfügbarkeit der lokalen Rechner gewährleistet und somit auch die Vertraulichkeit der lokalen Daten sichergestellt sein.

Um diesen Schutz erreichen zu können, ist der Einsatz einer Firewall zu empfehlen. Damit diese einen effektiven Schutz bieten kann, müssen folgende Bedingungen erfüllt sein.

Die Firewall muss:

- auf einer Sicherheitspolitik aufsetzen,
- im IT-Sicherheitskonzept der Dienststelle eingebettet sein,
- korrekt installiert und
- korrekt administriert werden.<sup>19</sup>

Als Grundlage für das Sicherheitskonzept dient die oben beschriebene Analyse der Kommunikationsbeziehungen, aus denen eine Sicherheitspolitik und die Anforderungen für den Betrieb der Firewall erarbeitet werden. Diese lehnen sich an die Forderungen des Bundesamtes für Sicherheit in der Informationstechnik an. Auch die Anordnung der Netzkomponenten und Verteilung der Dienste auf den Komponenten wird in dieses Konzept integriert. Der abschließende Teil beschäftigt sich mit dem Betrieb der Firewall und der Pflege aller Netzwerkkomponenten.

Zu den Sicherheitszielen, die mit dem Einsatz der Firewall erreicht werden sollen, gehören:

- Schutz des Dienststellen-LAN gegen unbefugten Zugriff von außen,
- Schutz der Firewall gegen Angriffe aus dem izn-net, aber auch gegen Manipulationen aus dem internen Netz,

---

<sup>18</sup> Vgl. [TFA-LAN].

<sup>19</sup> Vgl. [BSI97a].

- Schutz der lokal übertragenen und gespeicherten Daten gegen Angriffe auf deren Vertraulichkeit oder Integrität,
- Schutz der Netzkomponenten gegen Angriffe auf deren Verfügbarkeit,
- Verfügbarkeit der Informationen des izn-net und des Internet im lokalen LAN.

Weiter sind einige grundlegende Voraussetzungen für einen wirkungsvollen Schutz gegen Angriffe aus dem izn-net oder dem Internet zu erfüllen:

- Jede Kommunikation zwischen dem internen Netz und dem izn-net oder dem Internet muss über die Firewall geführt werden.
- Die Firewall wird ausschließlich für den Übergang zwischen den Netzen eingesetzt, auf ihr dürfen keine weiteren Dienste installiert werden.
- Der administrative Zugang zur Firewall darf nur über einen gesicherten Weg möglich sein.
- Die Firewall erlaubt nur genau festgelegte Verbindungen, die nach Adresse, Dienst, Zeit, Richtung und Benutzer spezifiziert sind. Alle anderen Verbindungen sind zu verbieten.
- Für den Betrieb der Firewall muss geeignetes Personal zur Verfügung stehen.
- Den Benutzern der Dienststellen-LAN sollten durch den Einsatz der Firewall keine Nachteile entstehen.

#### 4.4.1 Anordnung von Server-Komponenten

Ein sicherer Betrieb von Servern, die aus unsicheren Netz erreichbar sein sollen, kann nur gewährleistet werden, wenn diese auch von der Firewall geschützt werden. Diese lässt sich durch die Einrichtung einer sogenannten *entmilitarisierten Zone* erreichen, die ohne benutzerspezifischen Regeln zugänglich ist (siehe Abbildung 4). Durch diese Anordnung wird vermieden, dass bei Übernahme des Servers ein Zugang zum Intranet verschafft wird.

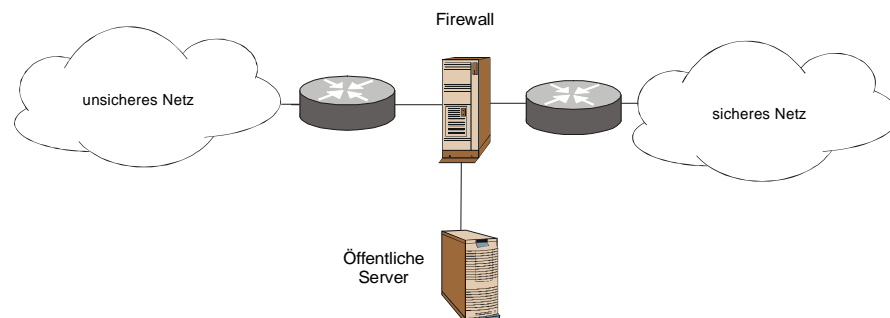


Abbildung 4: Anordnung öffentlicher Server in einer "entmilitarisierten Zone"

Eine solche Anordnung setzt voraus, dass die Firewall über freie Netzwerk-Interfaces verfügt. Stehen keine freien Interfaces zur Verfügung, so lässt sich der Aufbau einer entmilitarisierten Zone auch über Paketfilter erreichen, die beispielsweise über Access-Listen in Routern gebildet werden können.

## 4.4.2 Protokollentkopplung

### 4.4.2.1 HTTP

Im izn-net befindet sich ein WWW-Proxy-Server-Verbund im Aufbau, über den der Zugriff auf die Informationen des WWW im Internet erfolgen soll. Das IZN betreibt zentrale WWW-Proxy-Server, über die die Verbindung zum Internet über die Landes-Firewall hergestellt werden kann. In den Landesdienststellen werden weitere Proxy-Server eingerichtet, die ihre Daten von den zentralen Servern anfordern. Ziel dieses Verbundes ist zum einen die Reduzierung der Netzlast über die Firewall und zum anderen der schnelle Zugriff auf die Daten des Internet.

In Abbildung 5 sind die Verbindungen dargestellt, die bei der Anforderung eines WWW-Dokumentes aufgebaut werden, wenn dieses nicht auf den Proxy-Servern zwischengespeichert ist. Bei Dienststellen, die einen eigenen Proxy-Server betreiben, wird die Verbindung des Klienten zu diesem Server hergestellt. Dieser nimmt dann über die Firewall Verbindung zum zentralen Proxy-Server des IZN auf. Wird in der Dienststelle kein Proxy-Server eingesetzt, so wird die Verbindung von den Klienten selbst zum Proxy des IZN aufgebaut.

Handelt es sich bei der eingesetzten Firewall um ein Application-Gateway, so wird diese Verbindung zum Proxy des IZN nicht direkt weitergeführt, sondern auf der Firewall unterbrochen und eine neue Verbindung zum Proxy hergestellt. Es können damit auch protokollspezifische Filter eingerichtet werden, mit denen bestimmte Ereignisse gesperrt werden können. Diese Unterbrechung der Verbindung und die Filterung des Datenstroms läuft in der Regel transparent für den Benutzer ab.

Vom Proxy-Server des IZN wird dann die Verbindung zur Landes-Firewall aufgebaut, auf der die Verbindung von einem Proxy-Prozess entgegengenommen wird. Dieser nimmt die HTTP-Anfrage entgegen, prüft die angegebene Adresse und führt dann die entsprechende Anfrage zum Internet-Server aus. Die Antwort vom Internet-Server kann dann noch auf deren Inhalte, so z. B. Java, JavaScript oder ActiveX, untersucht und gefiltert werden.

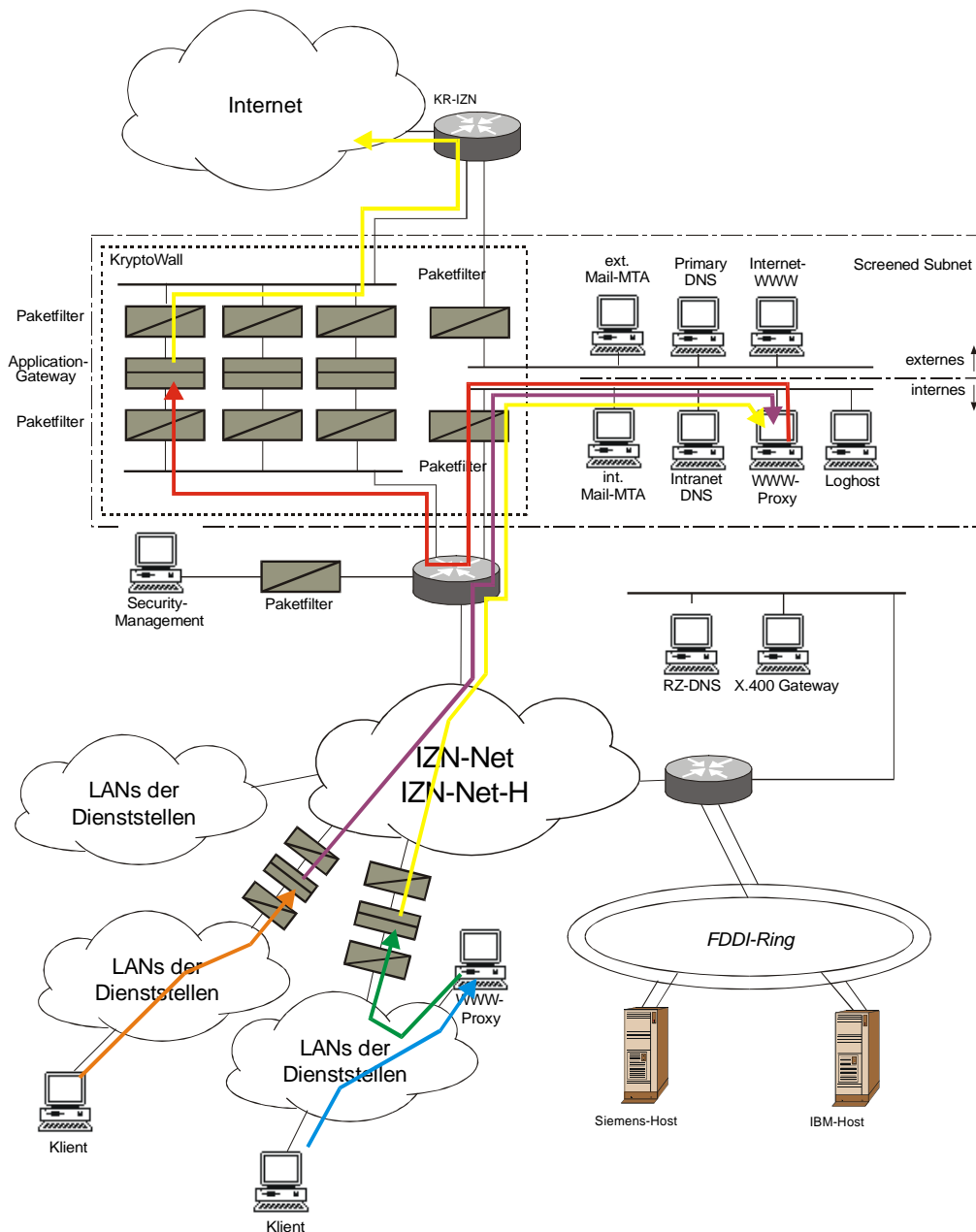


Abbildung 5: Protokollentkopplung durch HTTP-Proxies

#### 4.4.2.2 FTP

Zur Pflege z. B. von WWW-Servern im Internet ist ein direkter FTP-Zugang zu den Servern erforderlich. Diese Verbindung kann in der Regel nicht über WWW-Proxy-Server aufgebaut werden, da dies von den Anwendungen (so z. B. Microsoft Frontpage) nicht unterstützt wird. Daher ist es notwendig, eine FTP-Verbindung vom Klienten über die Firewall der Dienststelle zur Internet-Firewall zuzulassen. Von der Internet-Firewall wird die Verbindung dann zum WWW-Server aufgebaut.

Es ist bei der Konfiguration zu beachten, dass für FTP eine Datenverbindung benötigt wird, die vom Server zum Klienten aufgebaut wird. Es werden daher immer Verbindungen in beiden Richtungen benötigt.

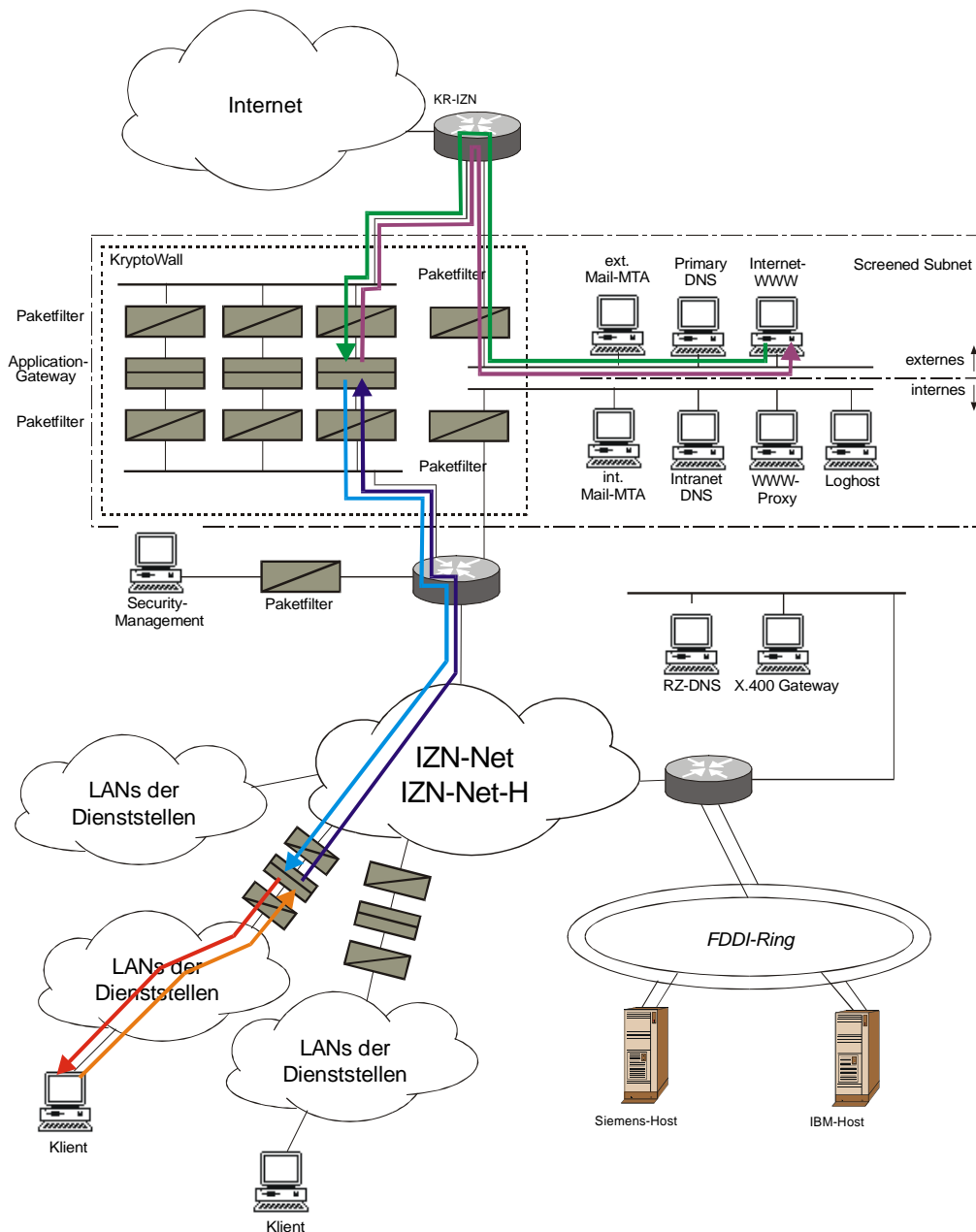


Abbildung 6: Verbindungswege bei FTP

#### 4.4.2.3 Mail

Eingehende Mails durchlaufen mehrere Stationen, bevor sie den Endnutzern zugestellt werden (Siehe Abbildung 7). Aus dem Internet kommend werden sie zunächst dem externen Mail Transport Agent (MTA) zugestellt, auf dem die Absender- und Empfängeradresse überprüft werden. Es werden nur Mails angenommen für Domänen, die im Zuständigkeitsbereich des Mailserver liegen. Die Absenderadresse wird auf ihre Gültigkeit hin überprüft, Mails von Domains, die nicht über DNS auflösbar sind, werden nicht angenommen. Darüber hinaus werden die Adressen der Mailserver mit einer "schwarzen Liste" verglichen, in der alle Mailserver eingetragen sind, die in der Vergangenheit durch Versenden von Spam-Mails aufgefallen sind. Mails von diesen Adressen werden ebenfalls nicht angenommen.

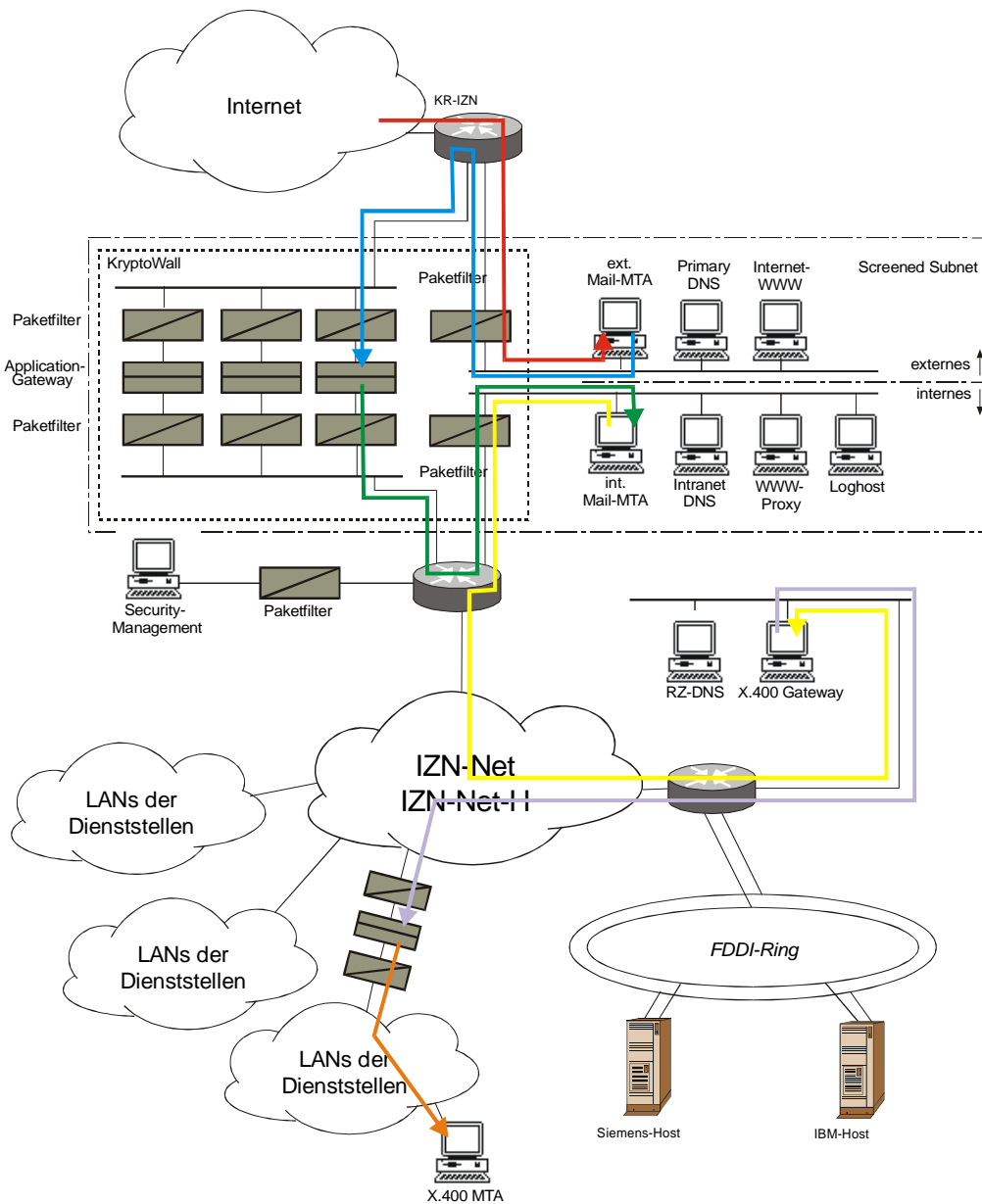


Abbildung 7: Mailtransport vom Internet zu den Dienststellen

Vom externen MTA wird die Mail dann zum Application-Gateway der Internet-Firewall übertragen, wo sie einem Store-and-Forward-Proxy zugeführt und im Dateisystem gespeichert wird. Bei diesem Proxy handelt es sich um ein Minimal-System, das damit die geringstmöglichen Angriffspotentiale bietet. Die Mail wird dann von einem separaten Prozess aus dem Dateisystem gelesen und an den internen MTA weitergeleitet.

Die Aufgabe des internen, zentralen MTA ist die richtige Zuordnung der Mail anhand der Empfängeradresse. Mails an Empfänger in den Dienststellen werden in der Regel dem X.400-Gateway des IZN zugestellt. Dieses nimmt die Konvertierung der bis hierhin über SMTP übertragenen Mail nach X.400 vor.

Die Übertragung zum Mailserver der Dienststelle erfolgt somit über das X.400-Protokoll. Die Verbindung zwischen dem X.400-Gateway und dem MTA der Dienststelle wird dabei über einen gemeinsamen Proxy der Firewall der Dienststelle geführt.

Eine inhaltliche Überprüfung der Mails z. B. auf Viren wird vom IZN nicht vorgenommen. Es empfiehlt sich, einer Überprüfung der Mail entweder auf der Firewall der Dienststelle oder dem MTA der Dienststelle vorzunehmen. Wird eine Mail als infiziert oder möglicherweise infiziert erkannt, muss sie auf ein Quarantäne-System ausgegliedert werden. Der Benutzer wird dann über diesen Vorgang informiert und kann mit Hilfe des Systemadministrator die Mail auf dem Quarantäne-System lesen oder verwerfen.

### 4.4.3 Sammeln von Logging-Informationen

#### 4.4.3.1 Separater Logserver

Zum Erkennen eines möglichen Angriffs und zur nachträglichen Analyse ist es unerlässlich, Logging-Informationen der Server und der Firewall-Komponenten zu sammeln und auszuwerten. Dabei ist eine einfachere Auswertung der Informationen möglich, wenn die Daten an einer zentralen Stelle gesammelt werden. Es ist dazu erforderlich, ein gesichertes Verfahren zur Übertragung der Daten an den Server einzusetzen. Zusätzlich ergibt sich eine erhöhte Sicherheit gegen eine Manipulation der Daten, wenn der zentrale Log-Server gegen unbefugten Zugriff abgesichert wird.

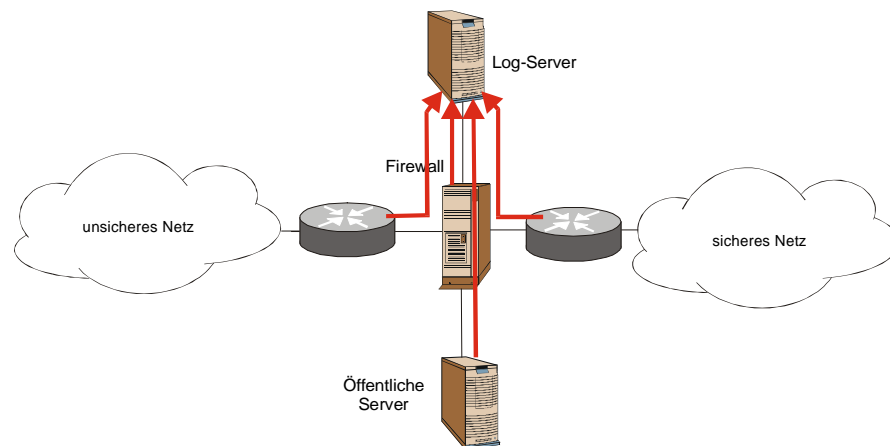


Abbildung 8: Sichere Einbindung eines Log-Servers

Im Regelfall genügt zu diesem Zweck der Einsatz eines zentralen Log-Servers, der möglichst an einem separaten Anschluss der Firewall eingebunden sein sollte. Um ihn bei Inbesitznahme der Firewall gegen Übergriffe zu schützen, sollte er auf die minimalsten Netzwerkdienste reduziert werden. Es ist zu prüfen, ob dieser Rechner mit einem besonderen Betriebssystem ausgestattet werden soll, das auf den anderen Systemen nicht eingesetzt wird, um das Risiko der mehrfachen Ausnutzung eines Betriebssystemfehlers als Angriffspunkt zu minimieren.

#### 4.4.3.2 Snipped Wire

Mit dem Konzept Snipped Wire soll ein zusätzlicher Schutz für den Log-Server geschaffen werden. Die Protokolldaten werden über eine zusätzliche Netzwerkkarte an einen Log-Server geschickt, wobei der Rückkanal dieser Netzverbindung physikalisch unterbrochen wird. Die Daten werden mit einem verbindungslosen Protokoll übertragen, das ohne Rückkanal auskommt. Dadurch ist ein Zugriff auf den Log-Server nicht möglich.

Zusätzlich besteht die Möglichkeit, den Log-Server ohne TCP/IP-Stack zu betreiben und die Log-Informationen über spezielle Anwendungen von der Netzwerkkarte auszulesen und auszuwerten. Damit ist der Log-Server nicht über das Netz angreifbar.

Die Schwächen dieses Verfahrens liegen in der unsicheren Übertragung der Logging-Informationen. Durch den fehlenden Rückkanal gibt es nicht die Möglichkeit, den Empfang der Logging-Informationen zu bestätigen. Die einseitige Netzverbindung schützt auch nicht vor Denial-of-Service-Attacken, die gegen den Log-Server gefahren werden können. Über die Vertrauenswürdigkeit der Inhalte der Logging-Informationen können keine Aussagen gemacht werden, ein in Besitz genommener Server kann bewusst Fehlinformationen an den Log-Server senden, die einen normalen Betrieb des Server vortäuschen.

Weitere Probleme dürften in der Durchführung mit einigen Netzwerkkarten auftreten, die die physikalische Verbindung zu einer Gegenstelle prüfen (Link-Test). In der Regel wird hier bei einer der beiden Verbindungsrichtungen (Receive oder Transmit) ein Verbindungstest durchgeführt. Die Karte ist nur dann betriebsbereit, wenn eine Gegenstelle vorhanden ist. Wird der Rückkanal physikalisch unterbunden, wird dieser Link-Test bei einer der beiden beteiligten Netzwerkkarten fehlschlagen und die Karte wird deaktiviert.

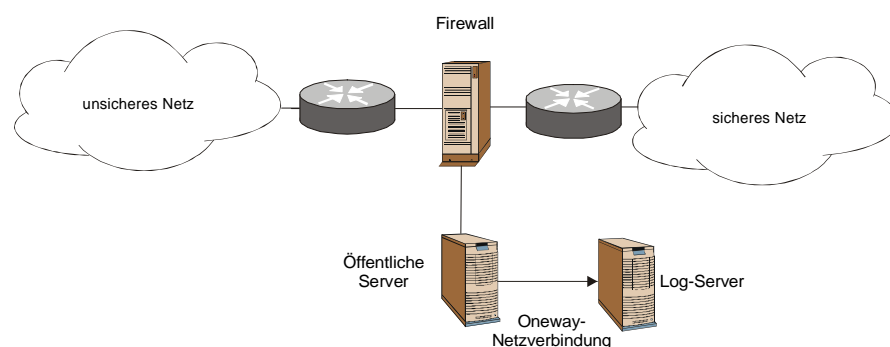


Abbildung 9: Snipped Wire-Konzept zum sicheren Sammeln von Logging-Informationen

#### 4.4.3.3 Audit

Ein geeigneteres Konzept zur Überwachung von Rechnersystemen ist ein Intrusion Detection System auf Basis eines Audits der Systemfunktionen. Hierbei wird auffälliges Verhalten direkt auf dem Server registriert und an einen Intrusion-Detection-Server über ein gesichertes Protokoll mit einer verschlüsselten Verbindung übertragen. Der IDS-Server selbst ist mit einem gehärteten Betriebssystem ausgestattet und damit nicht direkt angreifbar (Abbildung 10).

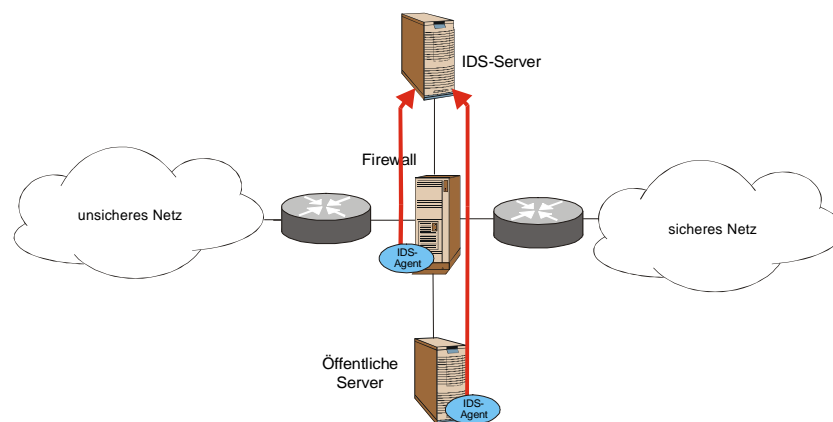


Abbildung 10: IDS-System auf Basis eines System-Audit

#### 4.4.3.4 Netzwerk-Monitore

Eine Überwachung der Server auf Basis der über das Netzwerk übertragenen Daten kann mit Hilfe von Netzwerk-Monitoren erreicht werden. Der Vorteil der Netzwerk-Monitore ist, dass sie völlig transparent in das Netzwerk eingebunden werden können und für den Angreifer nicht sichtbar sind. Netzwerk-Monitore sammeln die Daten der über das Netz übertragenen Daten und schicken sie an einen Server weiter, der die Auswertung der Daten vornimmt und auf bestimmte Angriffsmuster untersucht.

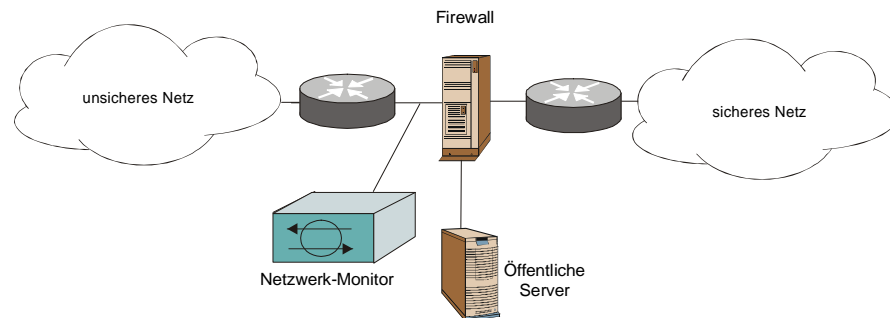


Abbildung 11: Netzwerküberwachung durch Monitore

#### 4.4.4 Organisatorische Regelungen

Neben den technischen Voraussetzungen für eine sichere Anbindung an ein öffentliches Netz sind organisatorische Regelungen für einen sicheren Betrieb von größter Bedeutung. Es ist daher erforderlich, dass ein Gremium gebildet wird, das über die Sicherheitspolitik der Dienststelle entscheidet. Für die Umsetzung der Sicherheitspolitik muss ein Verantwortlicher gefunden werden, der sowohl für die Aufstellung als auch die Implementierung und den Test der Sicherheitsregeln zuständig ist.

Für die Administration der Firewall muss fachkundiges Personal vorhanden sein. Es muss sichergestellt sein, dass die Firewall nur autorisierten Personen zugänglich ist.

Es muss festgelegt werden, welche Informationen protokolliert werden und wer die Protokolle auswertet. Es müssen sowohl alle korrekt aufgebauten als auch die abgewiesenen Verbindungen protokolliert werden. Die Protokollierung muss den datenschutzrechtlichen Bestimmungen entsprechen.

Die Benutzer müssen über ihre Rechte, insbesondere auch über den Umfang der Nutzdatenfilterung umfassend informiert werden. Angriffe auf die Firewall sollten nicht nur erfolgreich verhindert, sondern auch frühzeitig erkannt werden können. Angriffe können über die Auswertung der Protokolldateien erkannt werden. Die Firewall sollte aber auch in der Lage sein, aufgrund von vordefinierten Ereignissen, wie z. B. häufigen fehlerhaften Passworteingaben auf einem Application-Gateway oder Versuchen, verbotene Verbindungen aufzubauen, Warnungen auszugeben oder evtl. sogar Aktionen auszulösen.

Es ist zu klären, welche Aktionen bei einem Angriff gestartet werden, ob z. B. der Angreifer verfolgt werden soll oder ob die Netzverbindungen nach außen getrennt werden sollen. Da hiermit starke Eingriffe in den Netzbetrieb verbunden sein können, müssen Verantwortliche bestimmt sein, die entscheiden können, ob ein Angriff vorliegt und die entsprechenden Maßnahmen einleiten. Die Aufgaben und Kompetenzen der betroffenen Personen und Funktionen müssen eindeutig festgelegt sein.

## 4.5 Anforderungen an ein Firewall-System

Zum Erreichen der in Abschnitt 4.4 definierten Sicherheitsziele muss eine Firewall gewissen Mindestanforderungen genügen. Dazu gehört, dass die Struktur des zu schützenden Netzes (Rechnernummern, -namen und Mailadressen) verdeckt wird, damit sich keine Rückschlüsse auf die interne Netzstruktur und die internen Anwender ziehen lassen. Dies lässt sich z. B. durch den Einsatz eines Application-Gateways erreichen.

Die Firewall muss in der Lage sein, bestimmte Rechner gegen einfache Angriffe zu schützen, ohne dass diese Rechner im zu schützenden Teilnetz stehen müssen. Für diese Rechner brauchen dann keine benutzerspezifischen Filterregeln festgelegt werden. Dies können z. B. Informationsserver sein, die an einem dedizierten Interface angeschlossen sind (siehe auch Abschnitt 4.4.1).

### 4.5.1 Paketfilter

Ein Paketfilter kann Daten bis zur Transportebene des Netzwerk-Schichten-Modells (Ebene 4 des OSI-Modells) filtern. Die Angabe der Filterregeln umfasst die Quell- und Zieladresse, den Quell- und Zielport sowie die Richtung des Verbindungsaufbaus. Es dürfen nur Pakete mit gültigen Regeln weitergeleitet werden, alle anderen Pakete müssen verworfen werden.

Eine Protokollierung von IP-Adresse, Dienst und Zeit muss für jedes Paket möglich sein. Die Protokollinformationen müssen an einen externen Rechner verschickt werden können. Spezielle, einstellbare Ereignisse müssen zu einer unverzüglichen Warnung führen.

### 4.5.2 Application-Gateway

Das Application-Gateway ist für eine Filterung der Daten in der Anwendungsschicht verantwortlich. Damit ist es möglich, protokollspezifische Filterungen vorzunehmen, z. B. kann bei einer FTP-Verbindung RETR erlaubt werden, STOR und DELE jedoch verboten werden. Ebenso können eine Benutzerauthentisierung und Auditing durchgeführt werden.

Die Filterung wird durch spezielle Proxy-Prozesse vorgenommen, die für jeden Dienst Filtermöglichkeiten nach den Eigenschaften des Protokolls bieten. Für jeden Dienst existiert dabei ein eigener Proxy. Für alle wesentlichen Dienste müssen Proxies vorhanden sein, ebenso muss eine leichte Integration neuer Proxies möglich sein.

Auch im Application-Gateway ist eine umfangreiche Protokollierung erforderlich, die die IP-Adressen, Dienst, Zeit und evtl. Benutzer als Informationen enthalten. Sie müssen auch zu einem externen Rechner verschickt werden können, spezielle Ereignisse führen zu einer unverzüglichen Meldung.

### 4.5.3 Protokollierung

Alle Aktionen der Firewall müssen in Protokollen festgehalten werden. Damit ist es möglich, bei Unregelmäßigkeiten einzelne Vorgänge zu rekonstruieren und mögliche Angriffe zu erkennen. Die Protokollinformationen sollten auf einem Rechner zentral gesammelt werden und nur für die Mitarbeiter einsehbar sein, die für den Betrieb der Firewall verantwortlich sind.

Das Einsehen der Protokolle sollte in regelmäßigen Abständen erfolgen und zu den täglichen Arbeiten des Operating gehören. Zusätzlich müssen die unverzüglich verschickten Meldungen unmittelbar vom Operating ausgewertet werden und ggf. Maßnahmen ergriffen werden, die mögliche An-

griffe abwehren. Die Meldungen und die zu ergreifenden Maßnahmen sind in einem Maßnahmenkatalog zusammenzufassen.

## 4.6 Besondere Anforderungen für Netze mit sensitiven Daten

Dienststellen, in denen sensitiven Daten verarbeitet werden und einen erhöhten Schutzbedarf haben, benötigen zusätzliche Maßnahmen zur Gewährleistung der Vertraulichkeit dieser Daten. Im folgenden werden Verfahren vorgestellt, die zum Ziel haben, diese Vertraulichkeit herzustellen. Jedes dieser Verfahren bietet unterschiedliche Vor- und Nachteile und birgt Risiken, die bei einem möglichen Einsatz abzuwägen sind.

### 4.6.1 Graphical Wall

Unter einer Graphical Wall<sup>20</sup> wird ein dedizierter Rechner verstanden, der in einer demilitarisierten Zone installiert wird. Dieser Rechner dient den Benutzern des Intranet als Verbindung zum externen Netz, im Falle der Landesverwaltung dem izn-net oder dem Internet. Die Verbindung aus dem Internet zu diesem Rechner wird ausschließlich über die Umlenkung der grafischen Benutzeroberfläche hergestellt, woraus sich der Name dieses Konzeptes ableitet.

Das Produkt, mit dem die Umleitung der grafischen Benutzeroberfläche ermöglicht wird, ist das frei verfügbare *Virtual Network Computing (VNC)*<sup>21</sup>, eine Entwicklung von AT&T. Auf der Graphical Wall wird ein Serverprozess unter der Benutzerkennung des jeweiligen Benutzers gestartet, die grafische Darstellung der Oberfläche übernimmt ein Windows-Klient auf dem Arbeitsplatzrechner des Benutzers.

---

<sup>20</sup> Vgl. [Ste99].

<sup>21</sup> Vgl. [VNC].

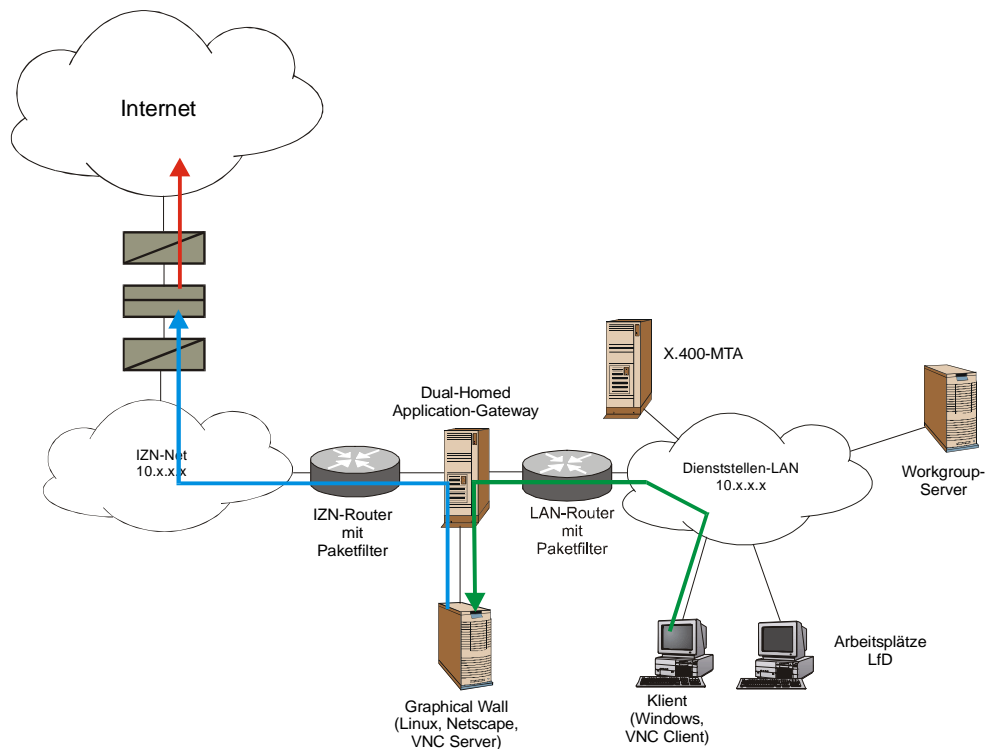


Abbildung 12: Graphical Wall

Der Vorteil dieses Konzeptes ist, dass alle Anwendungen, die Verbindung zum Internet haben, auf der Graphical Wall ablaufen. Damit kann die Gefahr des Einschleusen von Viren oder Trojanischen Pferden in das Intranet vermieden werden. Die Graphical Wall wird unter einem UNIX-Betriebssystem betrieben und ist damit nicht anfällig für Viren. Durch eine zentrale Administration kann die Manipulation des Betriebssystems gegenüber Windows-Systemen deutlich erschwert werden, lediglich die Ausnutzung von Systemfehlern kann zum Angriff auf das System ausgenutzt werden. Der Arbeitsplatzrechner des Benutzers ist nur über das VNC-Protokoll angreifbar. Da es sich um ein Protokoll zur grafischen Darstellung der Benutzeroberfläche handelt, sind hier Denial-of-Service-Attacks denkbar.

Die Nachteile in diesem Konzept sind zum Einen die ungewöhnliche Benutzung des Systems. Ein Nutzer muss zunächst eine Dialogsitzung (telnet oder ssh) zur Graphical Wall aufbauen und einen Serverprozess starten. Dann wird mit einem Windows-Klienten die Verbindung zu diesem Server aufgebaut und die Anwendungen können gestartet werden. Zum Anderen können Anwendungsdaten von Windows-Anwendungen, die z. B. per Mail oder WWW auf die Graphical Wall geladen werden, hier nicht bearbeitet oder eingesehen werden. Sie müssen über eine gesonderte Verbindung (z. B. über Wechseldatenträger, eine separate Verbindung über die Firewall oder per Mail über das X.400-Gateway) in das Intranet transportiert werden. Hier besteht allerdings wieder die Gefahr des Einschleusens von Viren oder Trojanischen Pferden.

Die Graphical Wall bietet einen sehr hohen Schutz des Intranet und ist vor allem für Dienststellen geeignet, die sonst keine Anbindung an die Dienste des izn-net oder des Internet ermöglichen würden.

#### 4.6.2 Trennung von Netzbereichen

Ein weiteres Verfahren zur Sicherung sensibler Daten ist die Trennung von Netzbereichen, in denen sensitive Daten verarbeitet werden, vom übrigen Intranet. Dieses Konzept eignet sich besonders für

größere Dienststellen, in denen z. B. die Personalverwaltung oder die Finanzbuchhaltung in separate, besonders abgesicherte Netze abgesichert wird.

Der Vorteil dieses Verfahrens liegt darin, dass diese Abteilungen nicht nur einen zusätzlichen Schutz vor Zugriffen aus dem Intranet bekommen, sie sind auch vor möglichen Angriffen aus dem Intranet abgesichert. Dies kann bei größeren Dienststellen von entscheidender Bedeutung sein.

Bei diesem Konzept besteht der wesentliche Nachteil darin, dass zentrale Ressourcen (Fileserver, Drucker) nicht mehr von diesen Abteilungen genutzt werden können. Die Protokolle, die eine Nutzung dieser Dienste ermöglichen, basieren in der Regel auf den Windows-Netbios-Protokollen und bieten einen unbegrenzten Zugriff auf die Systeme, die eine zentrale Sicherung des Teilnetzes unterlaufen.

### 4.6.3 Kryptografische Sicherheitsmaßnahmen

Insbesondere bei kleineren Dienststellen bietet sich die Trennung des Intranet in Netze mit verschiedenen Sicherheitsabstufungen nicht an. Hier besteht die Möglichkeit, die sensitiven Daten mit Hilfe kryptografischer Verfahren vor dem unbefugten Zugriff zu sichern. Dies kann zum Einen über frei verfügbare Software-Produkte realisiert werden, bei denen eine manuelle Verschlüsselung der Daten erfolgt. Diese Produkte erfordern aber eine gewisse Übung im Umgang, um Fehler bei der Verschlüsselung zu vermeiden.

Bei Einsatz kommerzieller Produkte wird eine deutlich bessere Benutzerführung geboten. Dateien werden hier automatisch beim Speichern auf Medien verschlüsselt und beim Laden wieder entschlüsselt. Bei Verlust des Schlüssels besteht die Möglichkeit, die Daten mit Hilfe von Master-Keys oder verteilter Schlüssel, die von mehreren Personen eingegeben werden müssen, zu entschlüsseln. Bei hohen Sicherheitsansprüchen kann die Verschlüsselungssoftware mit einem Chipkartenleser gekoppelt werden.

## 4.7 Auswahl einer Firewall

Für die Auswahl einer Firewall ist die Schutzbedürftigkeit des lokalen Netzes ein entscheidender Faktor. Unabhängig hiervon ist der Einsatz eines Dual-Homed Application-Gateways (siehe Abbildung 13) als Mindestanforderung zu sehen. Zur Absicherung des Gateways wird der Einsatz von zusätzlichen Paketfiltern, die zu beiden Seiten des Gateways angeordnet sind, sehr empfohlen. Die Paketfilter haben hierbei die Aufgabe, das Application-Gateway vor direkten Angriffen aus dem Internet oder dem Intranet zu schützen. Durch die Filterfunktion werden nur die Pakete zum Application-Gateway durchgelassen, deren Dienste in der Sicherheitspolitik festgelegt sind. Bei Verzicht auf die Paketfilter besteht eine Gefährdung des Application-Gateways durch Angriffe aus dem fremden wie auch aus dem lokalen Netz, die u. U. zu einer Übernahme des Gateways führen können. Zusätzlich werden durch die Paketfilter weitere Logging-Informationen zu den Netzverbindungen gesammelt, die bei der Aufklärung von sicherheitsrelevanten Vorkommnissen hilfreich sein können.

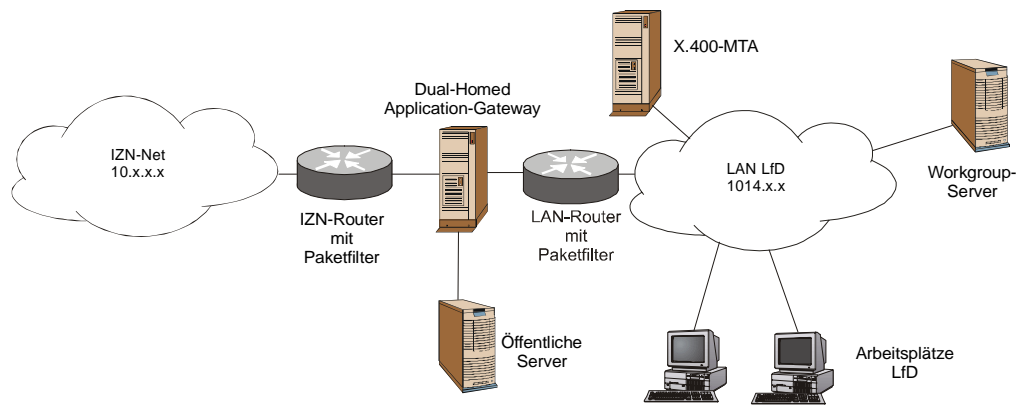


Abbildung 13: Firewall als Dual-Homed Application-Gateway mit Paktefiltern

Öffentliche Server, so z. B. WWW-Server und Fax-Gateways, werden in einer entmilitarisierten Zone an die Firewall angeschlossen<sup>22</sup>. Dadurch wird ein direkter Zugriff auf Ressourcen des Intranets von außen verhindert und ein sicherer Betrieb des Intranets gewährleistet, selbst wenn der öffentliche Server von Dritten übernommen werden sollte.

Bedingt durch die besonderen Kommunikationsanforderungen zwischen dem X.400-MTA und den Mail-Klienten empfiehlt es sich nicht, auch diesen in die entmilitarisierte Zone anzuschließen. Im Unterschied zu anderen öffentlichen Servern werden vom MTA nur Verbindungen zu einem weiteren Server, dem zentralen X.400-MTA des izn, hergestellt, zu dem eine besondere Vertrauensbeziehung besteht.

Für Netze mit besonderen Sicherheitsanforderungen sollten dann zusätzliche Maßnahmen nach Abschnitt 4.6, so z. B. Intrusion Detection oder der Einsatz der Graphical Wall, durchgeführt werden.

## 4.8 Festlegung von Firewall-Regeln

Über die Firewall-Regeln werden die Kommunikationsbeziehungen über die Firewall definiert. Für das Aufstellen der Regeln sind fundierte Kenntnisse über die verwendeten Protokolle und Möglichkeiten des eingesetzten Firewall-Produktes erforderlich. Die Firewall-Regeln sind in einer für die Dienststelle spezifischen Sicherheitspolitik festzuhalten, die die spezifischen Bedürfnisse der Einrichtung berücksichtigen müssen. Tabelle 1 enthält ein Beispiel für eine Minmalkonfiguration, die in der Regel um die Dienste erweitert wird, die für den Betrieb der jeweiligen Dienststelle notwendig ist.

<sup>22</sup> Vgl. Abschnitt 4.4.1.

Quelle	Ziel	Dienst	Aktion	Zeit	Beschreibung
WWW-Klienten	WWW-Proxy-IZN	HTTP	erlaubt	Arbeitszeit	Internet
X.400-GW-IZN	X.400-MTA	ISO-TSAP	erlaubt	immer	Mail
X.400-MTA	X.400-GW-IZN	ISO-TSAP	erlaubt	immer	Mail
Alles	Alles	Alle	verboten	immer	Letzte Regel

Tabelle 1: Firewall-Regeln für eine Minimal-Konfiguration

Für das Aufstellen der Regeln ist es wichtig, die Quell- und Zieladressen aufzulisten und zu benennen. Auch für Dienste ist eine Aufstellung erforderlich, die neben den verwendeten Ports auch protokollspezifische Merkmale definieren, so z. B. welche FTP-Kommandos oder ob aktive Inhalte im HTTP-Protokoll erlaubt sind. Die Möglichkeiten der protokollspezifischen Konfigurationen sind sehr stark vom eingesetzten Firewall-Produkt abhängig.

Quelle	Ziel	Dienst	Aktion	Zeit	Beschreibung
WWW-Klienten	WWW-Proxy-IZN	HTTP	erlaubt	Arbeitszeit	Internet
X.400-GW-IZN	X.400-MTA	ISO-TSAP	erlaubt	immer	Mail
X.400-MTA	X.400-GW-IZN	ISO-TSAP	erlaubt	immer	Mail
WWW-Klienten	izn-net	HTTP	erlaubt	immer	WWW-Intranet
P53-Klienten	P53-Server	exec	erlaubt	immer	FiBu
Asdis-Server	P53-Klienten	sftp	erlaubt	Arbeitszeit	P53-SW-Inst
Alles	Alles	Alle	verboten	immer	Letzte Regel

Tabelle 2: Beispiel für Firewall-Regeln

## A Sicherheitshinweise für Windows NT

Sowohl für die Arbeitsplätze, Server und die Firewall werden Rechner unter dem Betriebssystem Windows NT eingesetzt werden. Es ist daher von besonderem Interesse, Windows NT als Plattform so weit wie möglich gegen Angriffe abzusichern. Besondere Anforderungen an die Sicherheit werden an Firewall-Rechner gestellt, da sie als Common-Point-of-Trust die Verbindung zwischen gesichertem und ungesichertem Netz herstellen. An dieser Stelle werden daher einige Punkte aufgeführt, mit denen ein Rechner unter Windows NT sicherer gemacht werden kann.<sup>23</sup> Dabei werden besonders die Punkte genannt, die für einen Firewall-Rechner mit ausschließlich administrativen Zugriff von Bedeutung sind.

### A.1 Sichere Passworte

Passworte müssen gewissen Mindestanforderungen genügen, damit sie nicht durch Raten ermittelt werden können. Dazu gehört, dass sie eine Mindestlänge von 6 Zeichen haben. Unter Windows NT werden maximal 8 Zeichen unterschieden.

Passworte müssen aus Kombinationen von Buchstaben und Ziffern bestehen. Windows NT unterscheidet zwischen Groß- und Kleinbuchstaben. Die Benutzer müssen dazu veranlasst werden, ihre Passworte regelmäßig zu ändern. Daher darf die Option "Kennwort läuft nie ab" in der Benutzerverwaltung nicht deaktiviert werden. Die Verwendung von Trivial-Passwörtern muss nach Möglichkeit unterbunden werden. Durch die Installation einer zusätzlichen DLL kann eine Filterung von Trivialpasswörtern bei der Eingabe aktiviert werden.<sup>24</sup>

Nicht mehr benutzte Kennungen sollten gelöscht werden, um die Übersicht über die Kennungen zu erleichtern.

### A.2 Minimierung der Systemdienste

Mit dem Start von Windows NT werden Systemdienste gestartet, die oftmals nicht benötigt werden, aber als Angriffspunkt dienen können. Es empfiehlt sich daher, über den Dienste-Manager der Systemsteuerung alle nicht benötigten Dienste abzuschalten. Die benötigten Dienste variieren abhängig von der Hardware im Rechner und der installierten Software. Die folgenden Dienste werden in der Regel benötigt:

- Ereignisprotokolldienst: zeichnet Systemereignisse auf, wird für das Logging sicherheitsrelevanter Ereignisse benötigt
- Lizenzprotokolldienst: verwaltet die Lizenzen in einem NT-Server
- Plug & Play: konfiguriert ISA-Plug-And-Play-Karten in einem Rechner
- Protected Storage: ermöglicht das sichere Ablegen von Inhalten im Speicher

---

<sup>23</sup> Vgl. [Ris98], [Dos98] und [MS00].

<sup>24</sup> Vgl. [Dos98].

- Remote Procedure Call (RPC)-Dienst: wird von Protected Storage benötigt

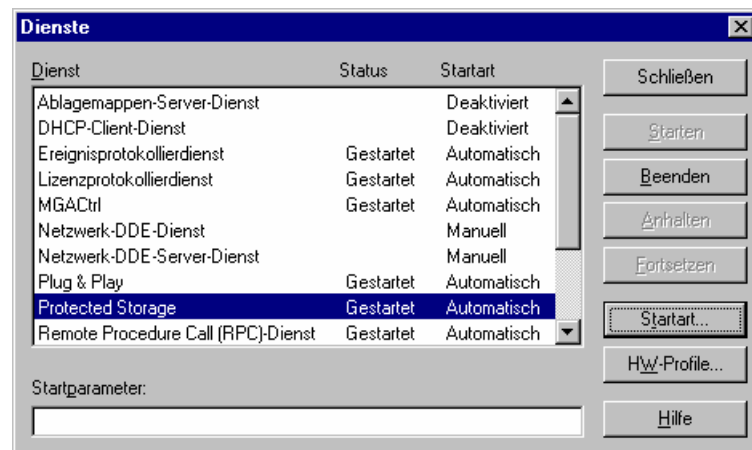


Abbildung 14: Deaktivieren von Systemdiensten im Dienstemanager

Über die Netzwerkkonfiguration werden Netzwerkprotokolle installiert (Abbildung 15). Für den Betrieb einer Firewall wird ausschließlich das Protokoll TCP/IP benötigt. Alle anderen Netzwerkprotokolle sollen unbedingt gelöscht werden.

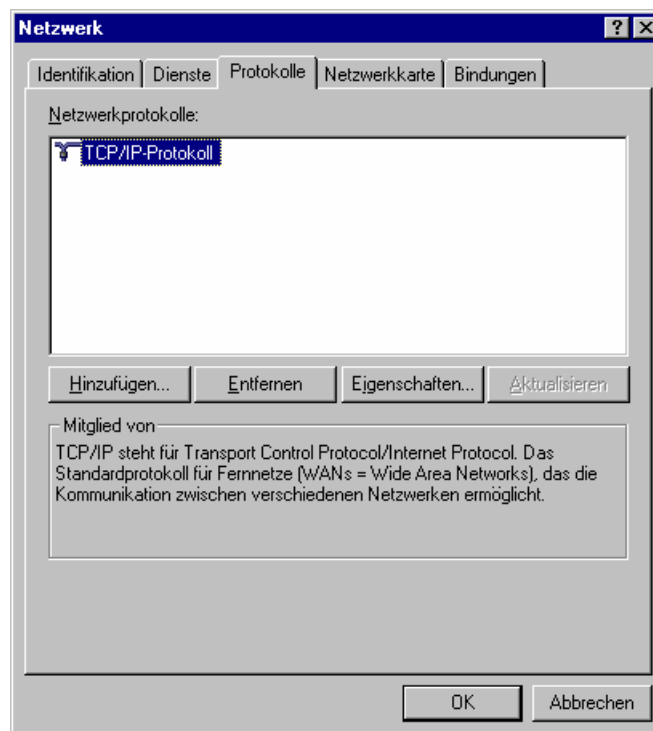


Abbildung 15: Eigenschaften von Netzwerk

Auch bei Minimierung der Systemdienste bleibt der Zugriff auf einen Rechner über das Netzwerk erhalten. Soll der Netzwerk-Zugriff abgeschaltet werden, müssen die Richtlinien in der Benutzerverwaltung angepasst werden (Abbildung 16).

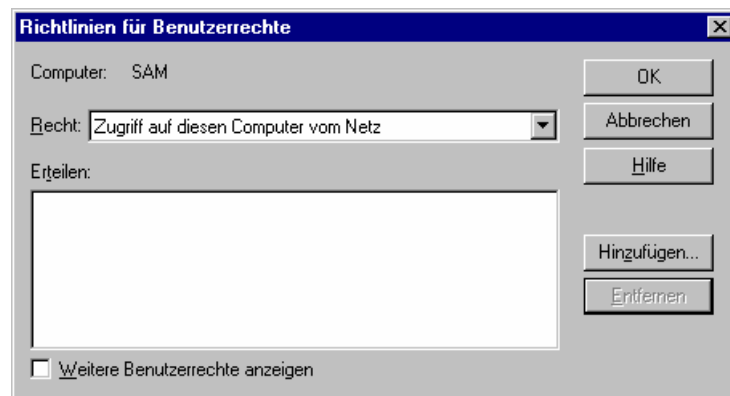


Abbildung 16: Konfiguration der Benutzerrichtlinien

Neben der Autostart-Funktion über die Programm-Gruppe Autostart gibt es die Möglichkeit, Programme durch einen Eintrag in der Registry beim Systemstart auszuführen. Die Einträge finden sich unter dem Registry-Schlüssel `\HKEY_Local_Machine\Software\Microsoft\Windows\CurrentVersion\Run`. An dieser Stelle tragen sich auch häufig Viren oder Trojanische Pferde ein.

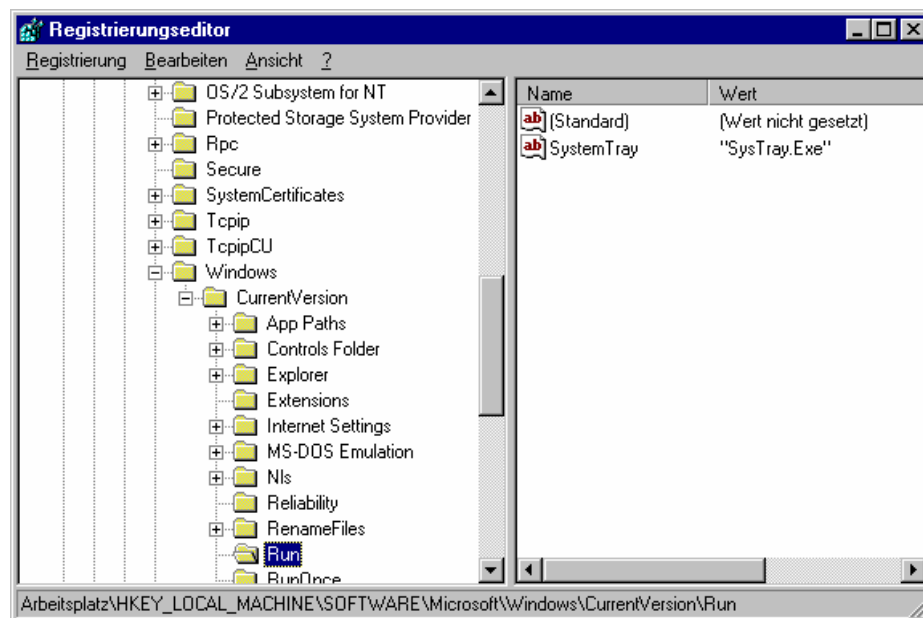


Abbildung 17: Abschalten des automatischen Starts von Programmen in der Systemsteuerung

### A.3 Umbenennen der Administratorkennung

Zur Erhöhung des Zugriffsschutzes auf die Administratorkennung sollte die Standardkennung unter dem Namen Administrator deaktiviert werden. Es ist dann eine neue Kennung mit Administrator-Rechten einzurichten, die nicht allgemein bekannt ist. Um zu vermeiden, dass die Kennung beim nächsten Login auf dem Bildschirm erscheint, muss der Schlüssel `\HKEY_Local_Machine\Software\Microsoft\Windows NT\CurrentVersion\WinLogon\DontDisplayLastUsername` auf den Wert 1 gesetzt werden.

## A.4 Aktivierung des Logbuchs

In der Standardkonfiguration werde unter Windows nur wenige Ereignisse in der Ereignisanzeige gespeichert. Um bei möglichen Angriffen auf ein System die ausgeführten Aktionen nachvollziehen zu können ist es notwendig, wichtige Ereignisse zu überwachen. Diese können über die Überwachungsrichtlinien der Benutzerverwaltung eingestellt werden. In Abbildung 18 ist eine mögliche sinnvolle Einstellung zur Überwachung abgebildet

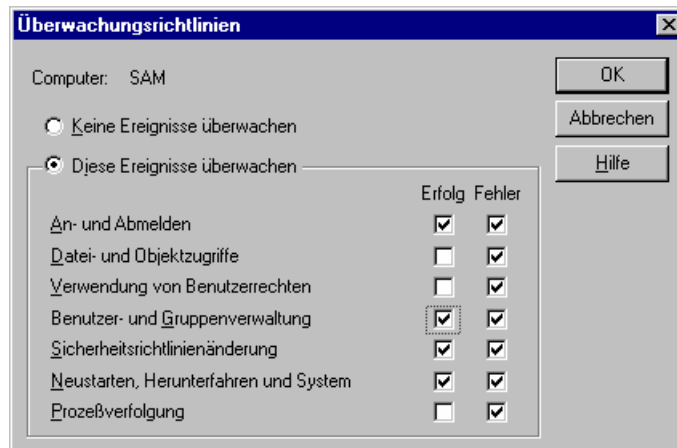


Abbildung 18: Konfiguration von Überwachungsrichtlinien

Die maximale Größe des Ereignisprotokoll ist in der Standardkonfiguration auf 512 KB beschränkt. Dies reicht für eine umfangreichere Überwachung nicht aus. Daher muss in den Einstellungen zur Ereignisanzeige die maximale Größe des Ereignisprotokolls erhöht werden. Mit der Protokollfortsetzung wird festgelegt, wie lange Ereignisse aufgehoben werden. In der Regel sollten diese 14 Tage aufgehoben werden, wenigstens aber 7 Tage.

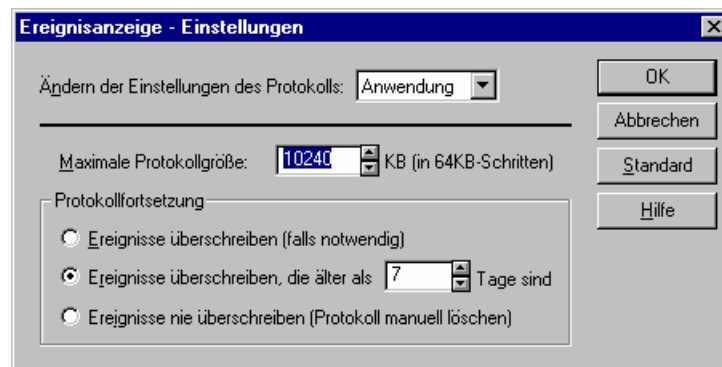


Abbildung 19: Einstellungen zur Ereignisanzeige

## A.5 NTFS-Dateisystem

Um Sicherheitsmaßnahmen im Dateisystem umsetzen zu können, muss das Dateisystem NTFS eingesetzt werden. Damit lässt sich der Zugriff auf Dateien und Verzeichnisse auf Benutzer- und Gruppenebene beschränken.

## A.6 Sichern der Konsole

Der Zugriff auf die Konsole eines NT-Servers - insbesondere für einen Firewall-Rechner - sollte nur den Systemverantwortlichen möglich sein. Sie muss in einem Raum aufgestellt werden, der nur den Verantwortlichen zugänglich ist.

## A.7 Installieren von Patches und Service Packs

Die Sicherheit eines einmal eingerichteten Systems kann nur dann aufrecht gehalten werden, wenn auf aktuelle Sicherheitswarnungen geachtet wird und laufend aktuelle Patches und Service Packs eingespielt werden. Sicherheitshinweise werden von *Computer Emergency Response Teams (CERT)* versandt, so z. B. vom CERT des DFN<sup>25</sup>.

## A.8 Sichern der Registry und der Benutzerkontendatenbank

Um Veränderungen an der Benutzerkontendatenbank zu verhindern besteht die Möglichkeit, diese zu verschlüsseln. Änderungen an der Datenbank können nur vorgenommen werden, wenn der Schlüssel bekannt ist. Es besteht die Möglichkeit, diesen Schlüssel auf einer Diskette zu sichern. Wird diese an einem sicheren Ort aufbewahrt, der nur autorisierten Personen zugänglich ist, können Änderungen an der Datenbank nur von den autorisierten Personen vorgenommen werden. Die Verschlüsselung wird aktiviert durch Aufrufen des Programms `C:\winnt\system32\syskey.exe`.

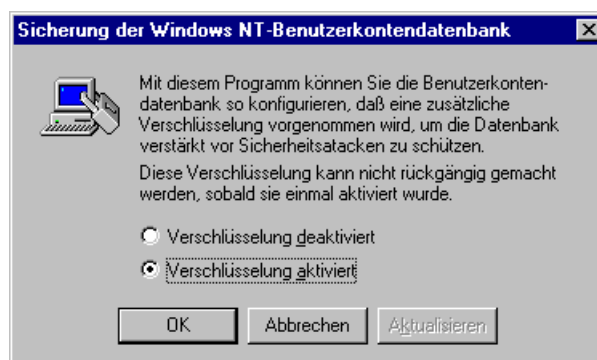


Abbildung 20: Sicherung der Benutzerkontendatenbank

---

<sup>25</sup> Siehe <http://www.cert.dfn.de>.

## B Installation der Checkpoint Firewall-1

### B.1 Installation

Das Netz des LFD ist über eine Checkpoint Firewall-1 Version 3.0b mit dem izn.net verbunden. Als Betriebsplattform wird ein PC unter Windows NT 4.0 Server eingesetzt, der nach den Vorgaben in Anhang A angepasst worden ist. Zusätzlich ist IP-Forwarding in den Eigenschaften zur Netzwerkumgebung **eingeschaltet** worden, da dieses für den Betrieb als Firewall notwendig ist.

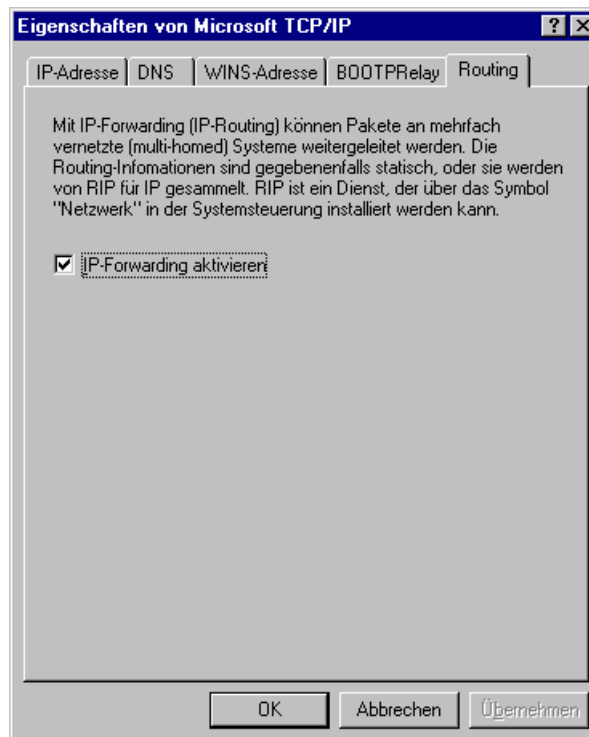


Abbildung 21: Aktivieren des IP-Forwarding

Die Installation der Firewall-Software erfolgte ohne Änderungen der Vorgaben durch die Installationsroutine.

## B.2 Netzskizze

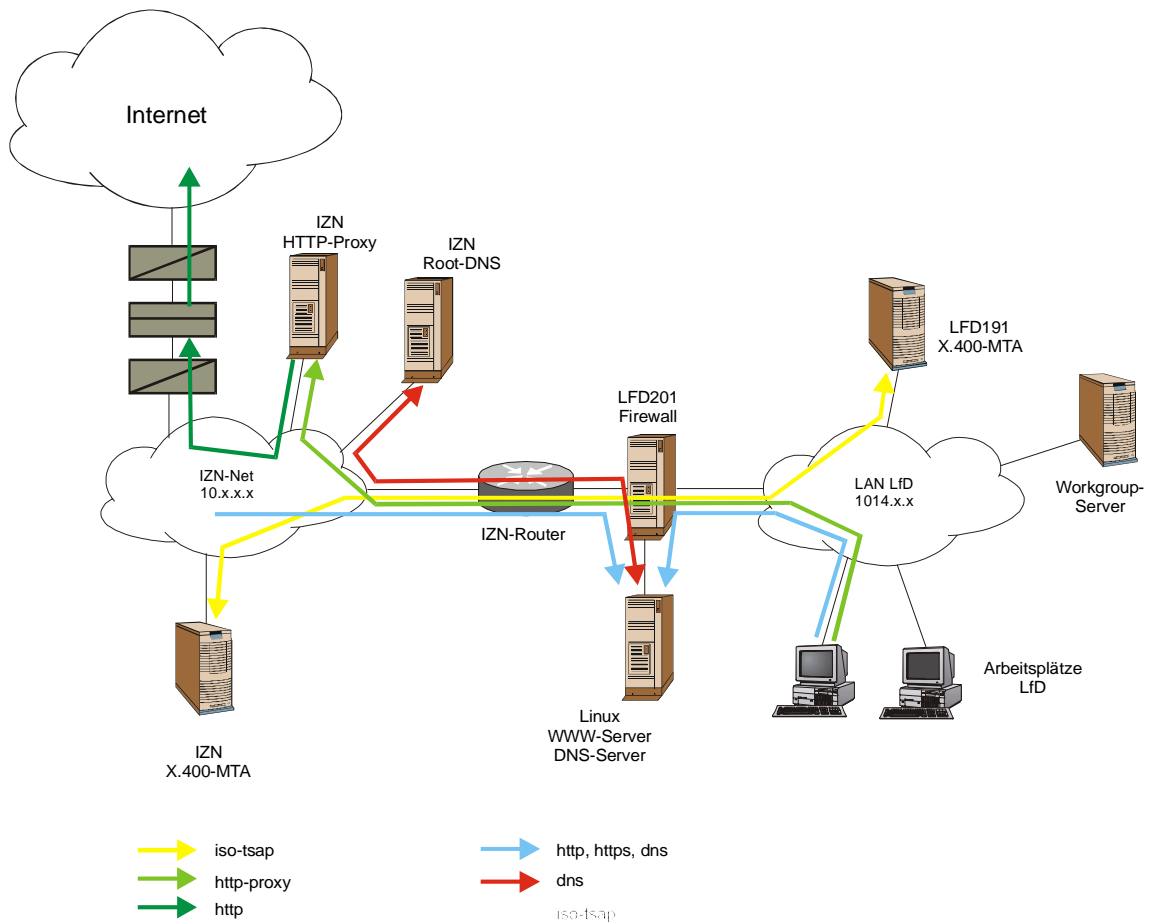


Abbildung 22: Anbindung des Lfd-LAN über Firewall

Mit der Installation der Firewall sind folgende Änderungen am LAN des Lfd vorgenommen worden:

1. Der X.400-MTA ist nur noch über das interne Netzwerk-Interface erreichbar, sein externes Interface ist deaktiviert worden.
2. Die Firewall hat die ehemalige externe IP-Adresse des X.400-MTAs übernommen.
3. Der X.400-MTA wird jetzt vom zentralen MTA des izn über seine interne Adresse angesprochen.
4. Auf dem izn-Router ist eine Route für das Netz 10.14.0.0/24 auf die Adresse 10.14.225.1 (externe Adresse der Firewall) eingerichtet worden.
5. Ein neu installierter Linux-Server ist in einer demilitarisierten Zone angeschlossen worden. Er übernimmt die Aufgaben:
  - WWW-Server zur Darstellung des Lfd im izn-net
  - DNS-Server für die Domain lfd.niedersachsen.de
  - Prüfsoftware zum Selbsttest von Internetanschlüssen (im izn-net).

### B.3 Regeln des Firewall-Moduls

Bei der Installation der Firewall sind die Regeln nach Abbildung 23 konfiguriert worden. Die Regeln sind nach Priorität geordnet, je weiter oben eine Regel steht, desto höher ist die Priorität. Bei Aufbau einer Verbindung über die Firewall wird das Regelwerk von oben nach unten durchschritten, bis eine Regel gefunden wird, die in Quelladresse, Zieladresse und Service dem Verbindungspaket entspricht. Die letzte Regel im Regelwerk bewirkt, dass alle Pakete, für die keine passende Regel gefunden wurde, verworfen und ein Alarm ausgelöst wird.

No.	Source	Destination	Service	Action	Track	Install On	Time	Comment
1	IZN-MTA LFD191	LFD191 IZN-MTA	iso-tsap	accept	Short	Gateways	Any	X.400
2	LFD-Netz	Linux	dns http https	accept	Short	Gateways	Any	DNS, HTTP
3	LFD-Workstations	IZN-Net	http https	accept	Short	Gateways	Any	HTTP ins IZN-Net
4	LFD161	IZN-HTTP-Proxy	http-proxy telnet	accept	Short	Gateways	Any	HTTP ins Internet
5	IZN-Net	Linux	http https dns	accept	Short	Gateways	Any	HTTP und DNS von izn-net auf Linux-Server
6	Linux	LFD-Netz	Any	drop	Short	Gateways	Any	Kein Zugriff auf LFD-Netz vom Linux-Rechner
7	Linux	IZN-Net	Any	accept	Short	Gateways	Any	Security Scanner
8	Any	Any	ident	reject	Short	Gateways	Any	Vermeidung von Alerts
9	LFD-Netz	Any	NBT	drop		Gateways	Any	Unterdrücken von Logs und Alerts für NetBios-Proc
10	Any	Any	Any	drop	Alert	Gateways	Any	Letzte Regel

Abbildung 23: Regeln des Firewall-Moduls

Erläuterungen zu den Regeln:

1. In der Regel 1 wird die Verbindung zwischen den X.400-MTAs im izn und LFD definiert. Als Service ist der neu eingerichtete Dienst iso-tsap verwendet worden, der ISO-TSAP-Zugriffe über TCP zulässt (siehe unten).
2. Zugriff aus dem lokalen Netz auf den Server in der DMZ über HTTP, Secure-HTTP und DNS.
3. Zugriff von den Arbeitsplätzen im lokalen Netz auf die WWW-Server im izn-net (Server der Landesdienststellen).
4. Regel für einen einzelnen Arbeitsplatz zum Zugriff auf das WWW-Angebot im Internet.
5. Freischalten des Zugriffs aus dem izn-net auf die Dienste des Servers in der DMZ (HTTP, Secure-HTTP und DNS).
6. Regel zum Schutz des internen Netzes.
7. Für die Prüfsoftware wird voller Zugriff auf das izn-net benötigt.

8. Unterbindung von Ident-Verbindungen, ohne dass ein Alarm ausgelöst wird.
9. Unterdrücken von Logs und Alerts für NetBios-Verbindungen aus dem lokalen Netz.
10. Default-Regel: Verwerfen der Pakete mit Alarmauslösung.

## B.4 Zeitschemata

Im Regelwerk der Firewall werden folgende Zeitschemata benutzt:

**Kernzeit:** Mo-Fr 9.00 Uhr bis 15:00 Uhr

**Arbeitszeit:** Mo-Fr 6:30 Uhr bis 20:00 Uhr

## B.5 Services

Neben den vordefinierten Services sind folgende Dienste eingerichtet worden:

**iso-tsap:** Verbindung zur Übertragung von ISO-TSAP-Protokollen über TCP/IP nach RFC 983, die für die Verbindung der X.400-MTAs benötigt wird.

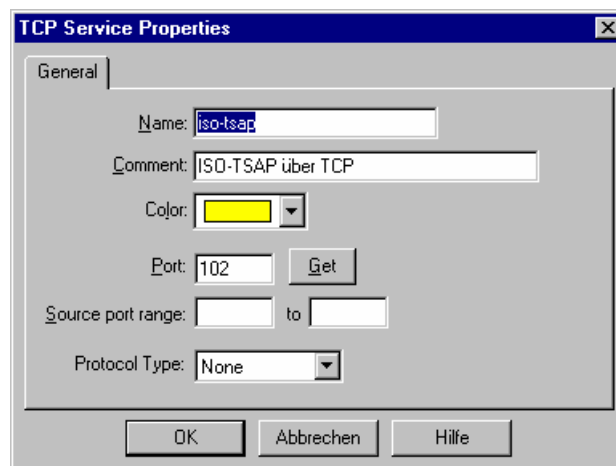


Abbildung 24: Service iso-tsap

**http-proxy:** Verbindung zwischen WWW-Klienten und dem HTTP-Proxy des izn.

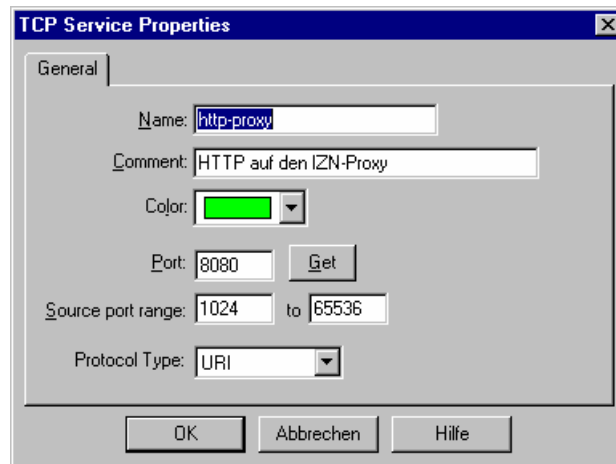


Abbildung 25: Service http-proxy

## B.6 Netzwerkobjekte

Die im Regelwerk definierten Quell- und Zieladressen werden über Netzwerkobjekte abgebildet. Netzwerkobjekte sind Workstations, Netze und Gruppen. Als Workstations werden einzelne Rechner bezeichnet (auch Server), auch die Firewall selbst ist als Workstation zu definieren (Siehe Abbildung 26). Netze können über ihre Netz-Adresse und einer Subnetzmaske definiert werden. Workstations und Netze können in Gruppen zusammengefasst werden, um die Übersichtlichkeit im Regelwerk der Firewall zu erhöhen.

### B.6.1 Workstations

**IZN-MTA:** Zentraler X.400-MTA im izn

**LFD191:** LFD-Server 191 (X.400-MTA)

**LFD201:** LFD-Server 201 (Firewall)

**Linux:** Linux-Server des LFD (WWW-Server, DNS-Server, Prüfsoftware)

**LFD-DHCP:** DHCP-Adressen im LFD

**LFD-Netz:** Interne IP-Adressen des LFD

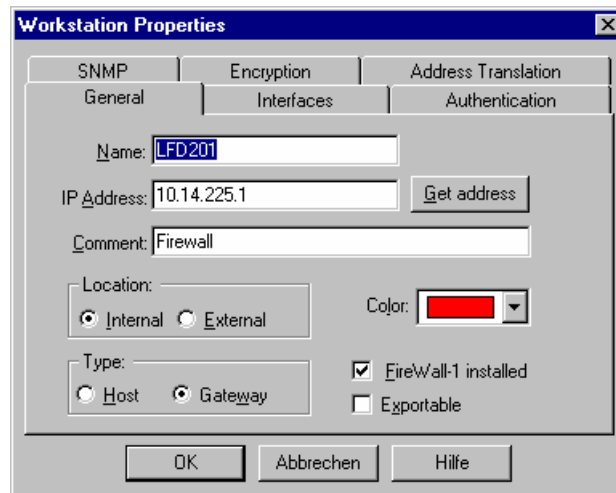


Abbildung 26: Eigenschaften des Netzwerkobjektes der Firewall-1

## B.6.2 Gruppen

**LFD-Workstations:** Arbeitsplätze im LFD, enthält:

LFD-DHCP

evtl. weitere einzelne Rechner

## B.7 Benutzer und Nutzergruppen

Für die Aufstellung benutzerbezogener Regeln können Authentisierungsmechanismen auf der Firewall durchgeführt werden. Die Authentisierung kann wahlweise über fest vergebene Passworte, Benutzerkennungen des Windows-Systems, Einmal-Passworte oder SecurID-Cards erfolgen. Als Beispiel ist in der Startkonfiguration ein Benutzer mit einem fest vergebenem Passwort eingerichtet worden. Hierfür ist es notwendig, die Verwendung von Firewall-1 Passworten auf der Firewall zu aktivieren (Abbildung 27).

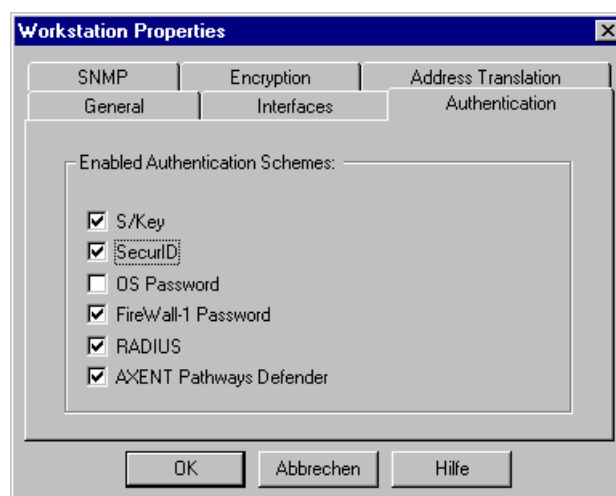


Abbildung 27: Authentication Schemes der Firewall

**Bumm:** Beispiel-Benutzer für Benutzerauthentisierung

**Internet-HTTP:** Benutzer aus dem LFD mit Berechtigung zum Zugriff auf das Internet per HTTP.

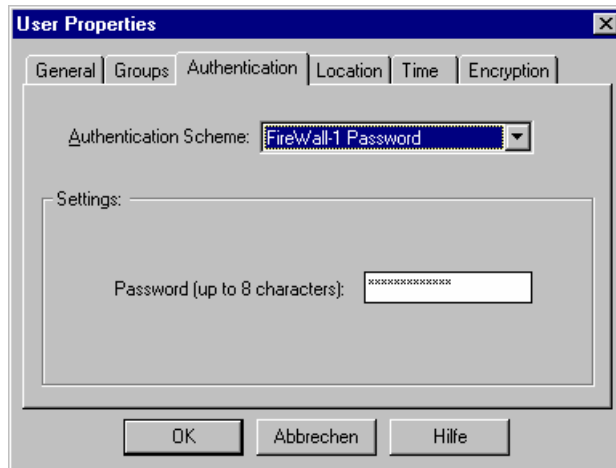


Abbildung 28: Eingabe eines Kennwortes bei Benutzerauthentisierung mit Firewall-1-Paßwörtern

### B.8 Address Translation

Die Adressen der Rechner im Netz des LfD sollen hinter der Adresse der Firewall verborgen werden, um keine Rückschlüsse auf das lokale Netz des LfD führen zu können. Daher ist für die Gruppe LFD-DHCP eine Adress-Translation mit der Methode Hide definiert worden.

No.	Original Packet			Translated Packet			Install On	Comment
	Source	Destination	Service	Source	Destination	Service		
1	LFD-DHCP	LFD-DHCP	Any	Original	Original	Original	Gateways	Automatic rule (see the network obje
2	LFD-DHCP	Any	Any	LFD-DHCP (Hiding Address)	Original	Original	Gateways	Automatic rule (see the network obje

Abbildung 29: Tabelle der Adressumsetzungen

### B.9 Properties Setup

Im folgenden werden die Konfigurationsdialoge im Properties Setup abgebildet und ggf. erläutert.

### B.9.1 Security Policy

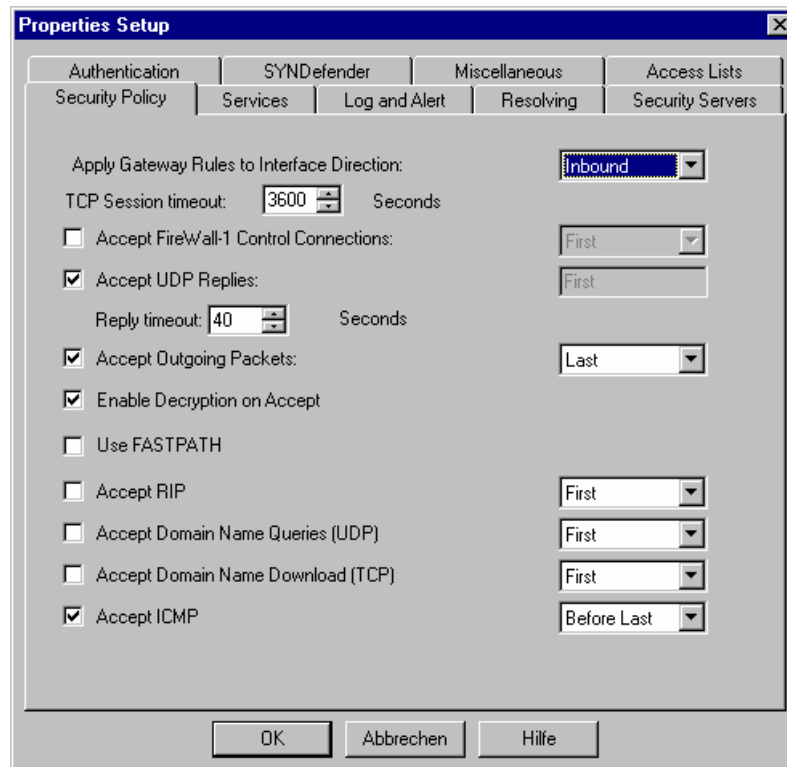


Abbildung 30: Properties Dialog: Security Policy

Anmerkungen:

1. *Accept Firewall-1 Control Connections* wird nicht benötigt, da es sich um ein Single gateway handelt.
2. *Accept UDP Replies* aktiviert das automatische Freischalten für Antworten auf UDP-Requests (wird z. B. für DNS benötigt).
3. *Accept Outgoing Packtes* wird zum Betrieb der Firewall benötigt.
4. Dynamische Routingprotokolle (so auch *RIP*) sind zu deaktivieren.
5. *Domain Name Queries* werden über Filterregeln gesteuert und sind daher hier abgeschaltet.
6. *Accept ICMP* ermöglicht den Transport von ICMP-Meldungen, so z. B. Network unreachable.

## B.9.2 Services

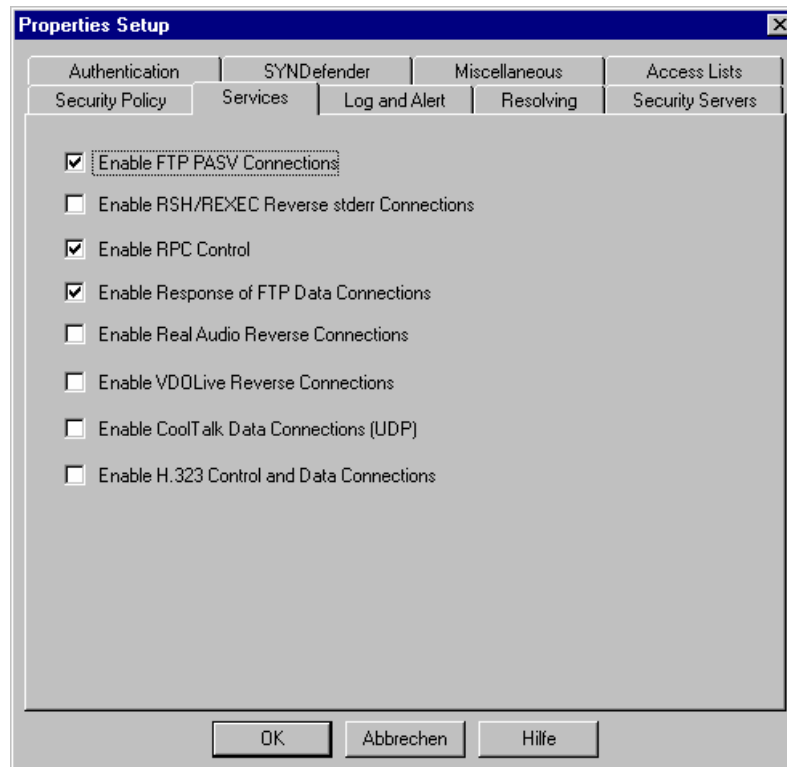


Abbildung 31: Properties Dialog: Services

Anmerkungen:

1. FTP PASV wird für FTP-Verbindungen zum Internet benötigt. Damit ist auch FTP über HTTP möglich.

### B.9.3 Log and Alert

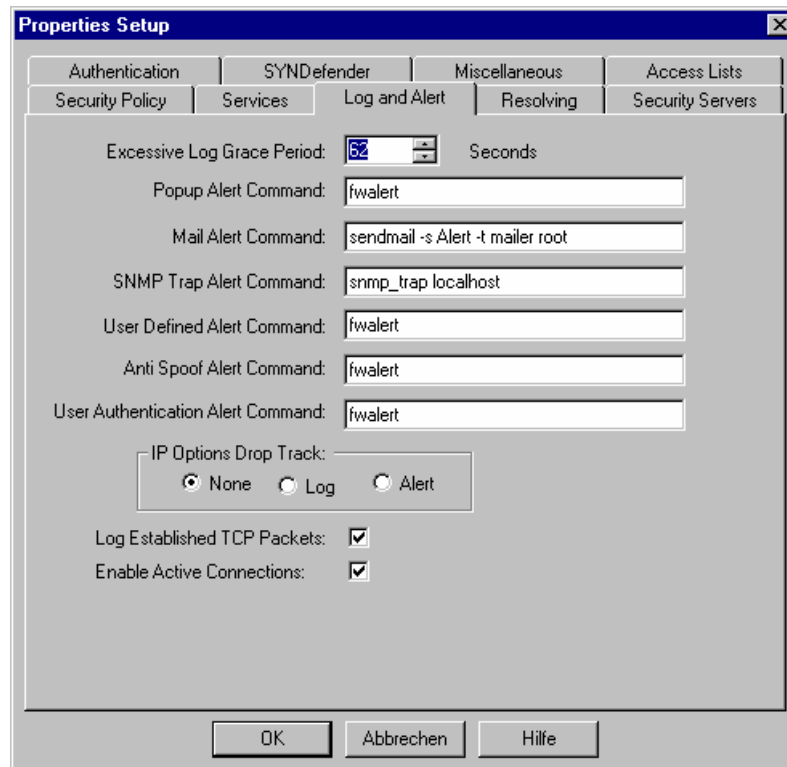


Abbildung 32: Properties Dialog: Log and Alert

Anmerkung:

Die Angaben entsprechen den voreingestellten Werten.

## B.9.4 Security Servers

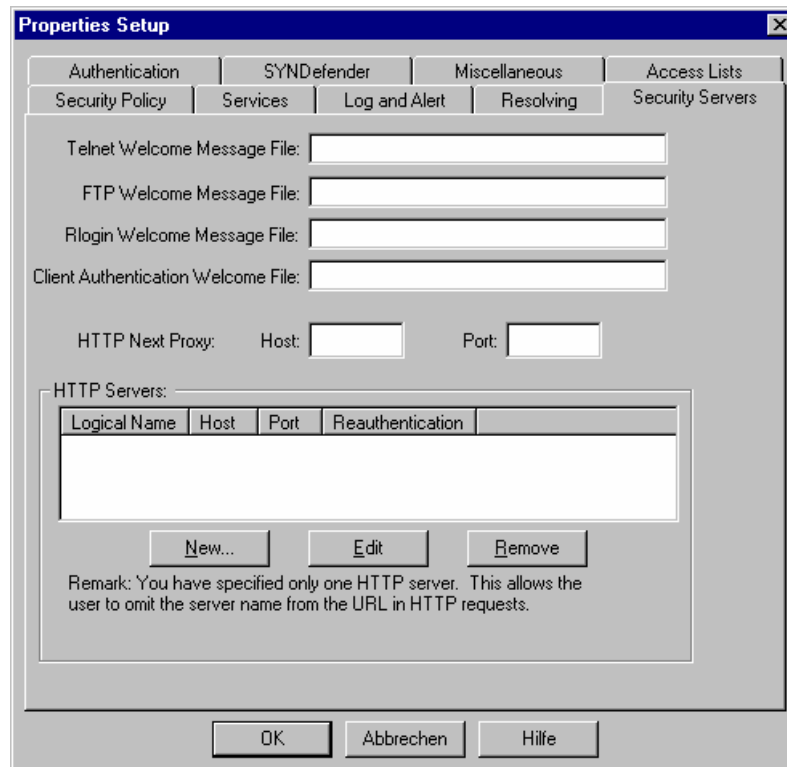


Abbildung 33: Properties Dialog: Security Servers

Anmerkung:

Security Server werden z. Z. nicht verwendet.

## B.9.5 Authentication

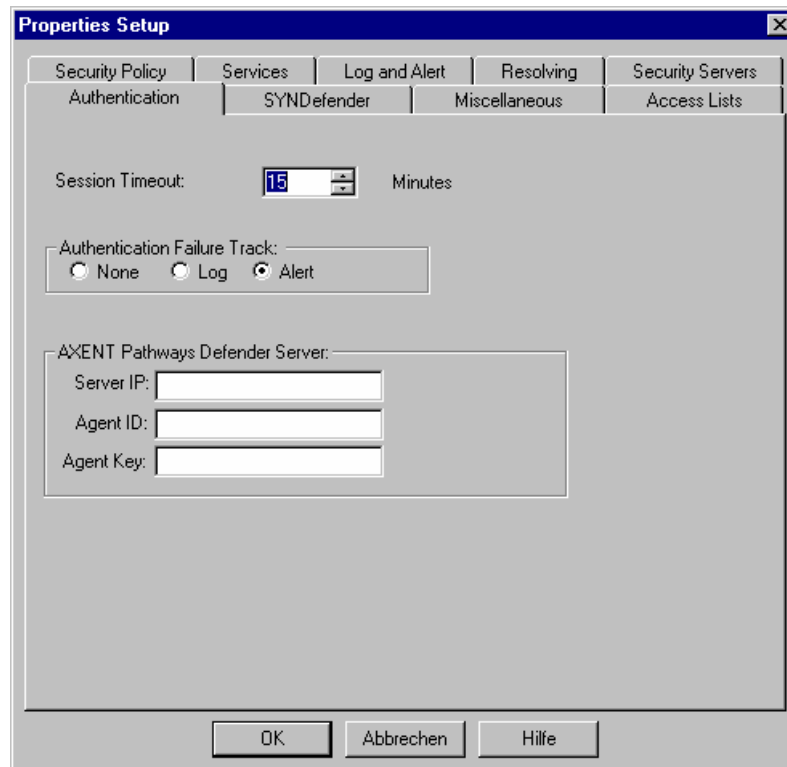


Abbildung 34: Properties Dialog: Authentication

Anmerkung:

Die Angaben entsprechen den voreingestellten Werten.

## B.9.6 SYNDefender

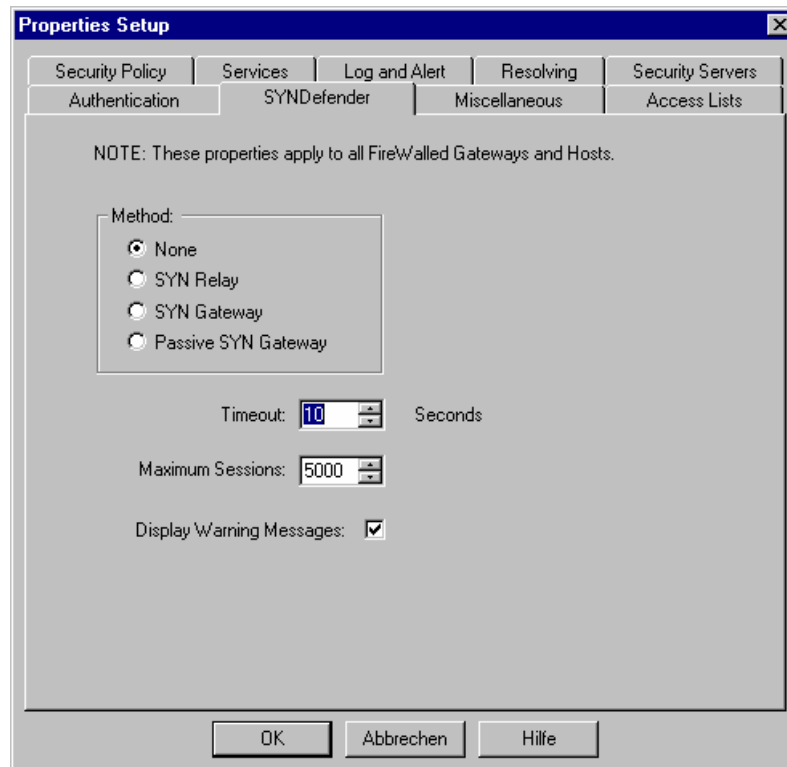


Abbildung 35: Properties Dialog: SYNDefender

Anmerkung:

Die Angaben entsprechen den voreingestellten Werten.

## B.9.7 Resolving

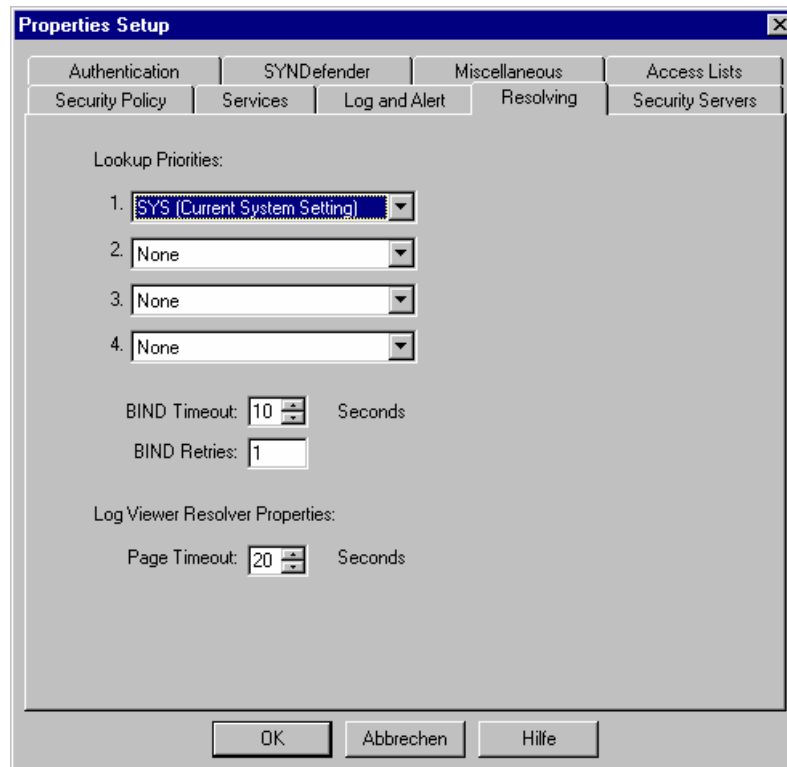


Abbildung 36: Properties Dialog: Resolving

Anmerkung:

Die Verwendung weiterer DNS-Server ist möglich.

### B.9.8 Miscellaneous

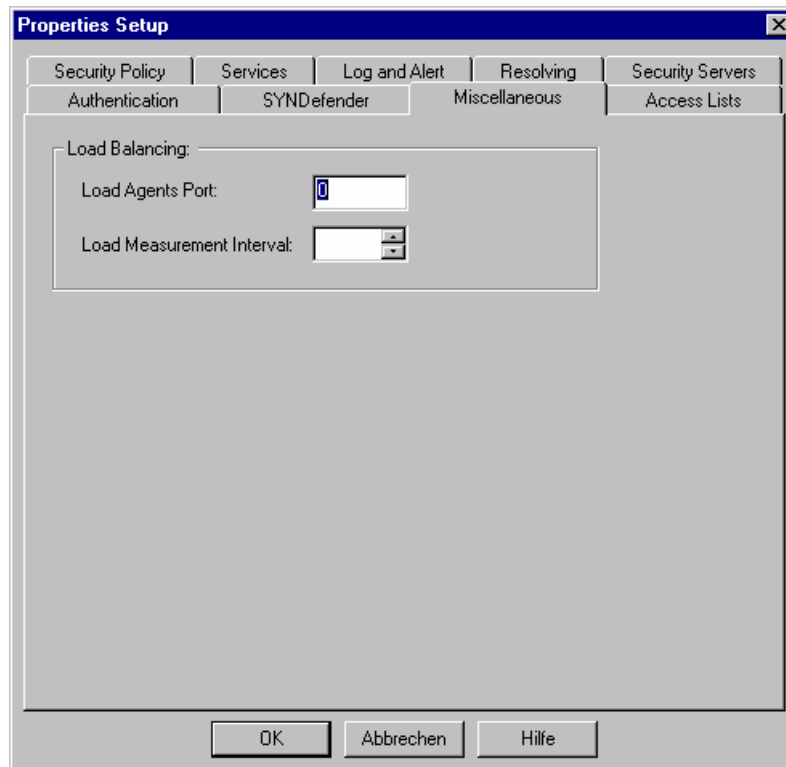


Abbildung 37: Properties Dialog: Miscellaneous

Anmerkung:

Die Angaben entsprechen den voreingestellten Werten.

### B.9.9 AccessLists

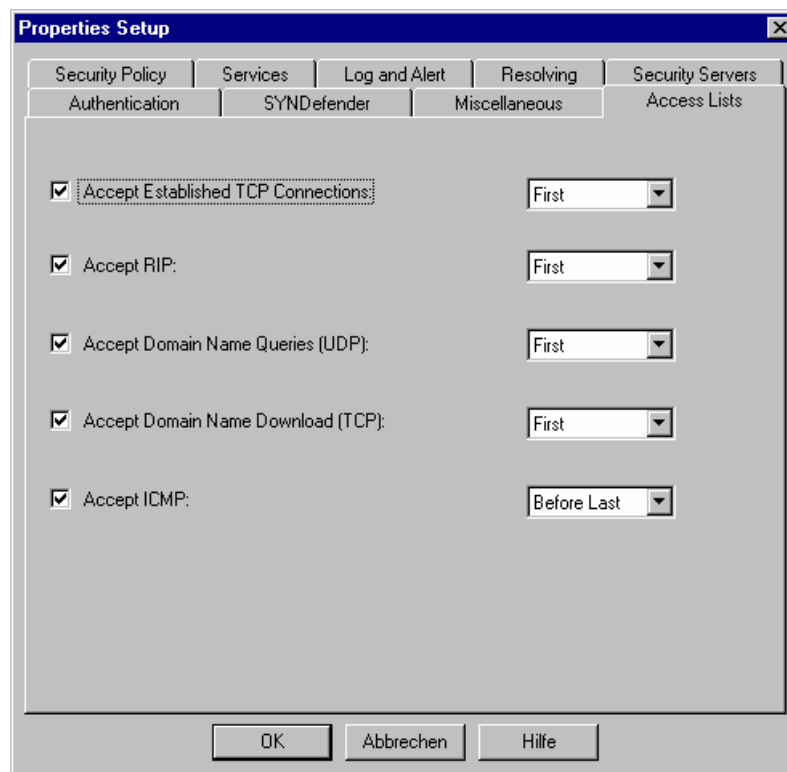


Abbildung 38: Properties Dialog: Access Lists

Anmerkung:

Wird nicht benutzt.

### B.10 Auswertung der Log-Informationen

Die Log-Informationen werden in eigenen Log-Dateien gesammelt. Zu den Protokoll-Informationen gehören:

- Datum und Uhrzeit
- Quell-IP-Adresse und Port
- Ziel-IP-Adresse und Port
- IP-Protokollkennung (TCP/UDP/ICMP)
- Policy (Accept/Deny)

Eine automatische Auswertung der Log-Dateien ist z. Z. nicht eingerichtet. Denkbar wäre eine Bearbeitung, bei der die Informationen tageweise ausgewertet und benutzerspezifische Informationen herausgefiltert werden. Die Informationen können wochenweise in einzelnen Dateien gespeichert und über einen festgelegten Zeitraum aufgehoben werden. Der Zugriff auf die Protokoll-Daten ist dem Systemadministrator der Firewall möglich. Bei Auslösung von Firewall-Alarmen (z. B. bei unerlaubten Zugriffen auf die Firewall aus dem izn-net) können die Protokollinformationen diese Zugriffs sofort über benutzerdefinierte Aktionen ausgewertet oder per Mail an den Systemadministrator geschickt werden.

## B.11 Konfiguration der WWW-Klienten

### B.11.1 WWW-Zugriff mit Netscape

Edit -> Preferences -> Advanced -> Proxies -> Manual Proxy Configuration:



Abbildung 39: Proxy-Konfiguration des Netscape-Communicators

### B.11.2 WWW-Zugriff mit Internet-Explorer 5

Extras -> Internetoptionen -> LAN-Einstellungen -> Proxy-Server verwenden -> Erweitert:



Abbildung 40: Internetoptionen des Internet-Explorer

## Literatur

- [BSI97a] Bundesamt für Sicherheit in der Informationstechnik, Grundschutzhandbuch. 1997.
- [BSI97b] Bundesamt für Sicherheit in der Informationstechnik, Informationen zu Computer-Viren. Band 2 der Schriftenreihe zur IT-Sicherheit, 1997.  
<http://www.bsi.de/antivir1/virbro/inhalt/inhalt.htm>
- [Bö99] B. Böker. Anbindung der Landesregierung Niedersachsen an das Internet. 1999.
- [Ckp98] Checkpoint. Getting started with Firewall-1. User Guide. 1998.
- [Dos98] W. Doser. Sicherheit unter NT 4.0. Kommunikation/Gruppe, Protokolle und Sicherheit. September 1998.  
<http://www.kom.id.ethz.ch/security/nt40/index.htm>
- [Gra99] R. Graham. Network Intrusion Detection.  
<http://www.robertgraham.com/network-intrusion-detection.html>
- [Kös00] W.-H. Köster: Spezieller Vertrag ermöglicht schnelle Netzanbindung. In: izn Mail Januar 2000.
- [LfD98] Der Landesbeauftragte für den Datenschutz Niedersachsen Grundschutz durch Firewall, Orientierungshilfe und Checkliste. 1998.
- [MS00] Microsoft Corporation. Windows NT C2 Configuration Checklist. April 2000.  
<http://www.microsoft.com/technet/security/c2config.asp>
- [Ris98] O. Rist. Lock The Doors on Windows NT in 10 Steps. November 1998.  
<http://www.zdnet.com/windows/stories/main/0,4728,2163194,00.html>
- [SSH] SSH Communications Security. SSH Secure Shell.  
<http://www.ssh.org/>
- [Ste99] G. Stepken. Firewall-Handbuch.  
<http://www-little-idiot.de/firewall/>
- [TFA-LAN] Technikfolgenabschätzung Anschluss lokaler Netze an das Landes-Intranet mit Zugang zum Internet. 1999.
- [TFA-IN] Technikfolgenabschätzung izn-net (Internet/Intranet). 1999.
- [VNC] Virtual Networking Computing (VNC)  
<http://www.uk.research.att.com/vnc/>

## RFCs

- [RFC821] J. Postel. Simple Mail Transfer Protocol. RFC 821. 1982.
- [RFC854] J. Postel, J. Reynolds. Telnet Protocol Specification. RFC 854. 1983.
- [RFC959] J. Postel, J. Reynolds. File Transfer Protocol (FTP). RFC 959, STD 9. 1985.

- [RFC977] B. Kantor, P. Lapsley. Network News Transfer Protocol. RFC 977. 1986.
- [RFC983] D. E. Cass, M. T. Rose. ISO Transport Protocol on Top of the TCP. RFC 983. 1986.
- [RFC1918] Y. Rekter. et al. Address Allocation for Private Intranets. RFC 1918. 1996.
- [RFC2068] R. Fielding, J. Gettys, J. Mogul, H. Frystyk, and T. Berners-Lee. RFC 2068: Hypertext Transfer Protocol HTTP/1.1, Jan. 1997.