

14.2.4 Firewall-Systeme

Firma Lütgens möchte ihr lokales Netzwerk, das mit dem Internet verbunden ist, vor Bedrohungen aus dem Internet schützen. So sollen z. B. keine Programme mit schädigender Wirkung aus dem Internet eingeschleust werden dürfen und keine unbefugten Zugriffe über das Internet auf das lokale Netzwerk erfolgen können.

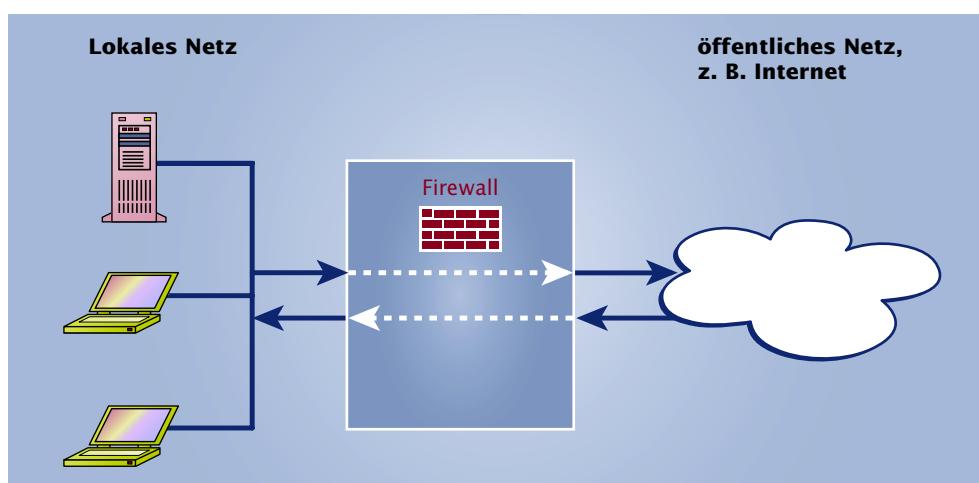
Aus der Anbindung eines Rechners oder lokalen Netzes an ein öffentliches Netz wie dem Internet ergeben sich vielfältige Bedrohungen. Hierzu gehören u. a.:

- Address Spoofing¹:
Unter einer gefälschten Identität wird eine Kommunikationsverbindung aufgebaut. Hierbei erzeugt der Angreifer IP-Pakete mit gefälschter IP-Absenderadresse.
- Denial-of-Service-Angriff²:
Ziel ist es, einen bestimmten Server „lahmzulegen“ und ihn so daran zu hindern, Antworten auf Anfragen zu erzeugen. Dies geschieht meist in der Form, dass die Ressourcen des Servers voll belegt werden und so für weitere Anfragen keine Ressourcen mehr zur Verfügung stehen.
- Abhören fremder Zugangsdaten während des Netzverkehrs.

Eine Schutzmaßnahme gegenüber diesen Bedrohungen ist die Verwendung von Firewall-Systemen³, kurz Firewalls. Der Begriff der Firewall stammt aus dem Bereich des Feuerschutzes von Gebäuden. Dort haben Firewalls als Brandschutzmauern die Aufgabe, die Ausbreitung von Bränden von einem Gebäude auf das nächste zu verhindern.

Abb. 14.2.4-1 zeigt die Platzierung einer Firewall zum Schutz eines lokalen Netzes vor Bedrohungen aus einem öffentlichen Netz. Sie wird so zwischen beide Netze geschaltet, dass die Firewall die einzige Verbindung zwischen den Netzen darstellt und hierdurch ein kontrollierter Netzübergang entsteht.

Eine Firewall ist ein System, das zwei Netzwerke koppelt und hierbei sicherstellt, dass jeglicher Verkehr zwischen den beiden Netzen ausschließlich durch die Firewall geleitet wird. Dabei wird die Weiterleitung von solchen Paketen verhindert, die eine mögliche Bedrohung eines Netzes bedeuten können.



14.2.4-1 Schutz eines lokalen Netzes mittels Firewall

¹ **Address Spoofing** wird häufig auch als IP Spoofing bezeichnet. (spoof: engl. beschwindeln)

² **Denial of Service**: engl. Diensteverweigerung

³ **Firewall**: engl. Brandschutzmauer

Eine Firewall bietet keinen Schutz vor Angreifern, die sich innerhalb des zu schützenden Netzes befinden!¹

Die in Abschnitt 14.2 getroffene Aussage, dass es keine vollständige Sicherheit gibt, gilt insbesondere auch für Firewall-Systeme. Ziel für den Einsatz von Firewalls kann somit nur sein, die Hürden für Angreifer möglichst hoch zu setzen.

Aufgaben einer Firewall:

- Schutz vor unbefugten Netzzugriffen.
- Zugangskontrolle:
Steuerung, welche Nutzer in welcher Form auf welche Netzressourcen zugreifen dürfen.
- Protokollierung der Netzwerkaktivitäten:
Aufzeichnung des Netzverkehrs, um hieraus Rückschlüsse auf erfolgte Angriffe ziehen zu können.
- Alarmierung bei sicherheitsrelevanten Ereignissen:
Werden sicherheitsrelevante Aktionen von hierzu nicht befugten Nutzern durchgeführt, so wird durch die Firewall ein Alarm ausgelöst.
- Verbergen der internen Netzstruktur:
Um Angreifern mögliche Angriffspunkte des internen Netzwerks vorzuenthalten, verhindert die Firewall das Einsehen der Struktur dieses Netzwerks von außen.
- Gewährleistung der Vertraulichkeit von Daten:
Sicherstellung, dass der interne Netzverkehr nicht abgehört werden kann.

Firewalls werden in verschiedene Klassen eingeteilt:

- Paketfilter
- Proxy-Firewalls
- Applikationsfilter

Diese Klassen werden häufig kombiniert eingesetzt, so dass sich eine vielfältige Anzahl von Firewall-Architekturen ergibt.

Paketfilter:

Eine Paketfilter-Firewall verhält sich wie ein IP-Router, der alle ankommenden Pakete nach bestimmten Regeln filtert. Erlaubte Pakete werden mittels der konfigurierten Routen an den Empfänger weitergeleitet, unerlaubte Datenpakete dagegen werden gesperrt.

Paketfilter-Firewalls arbeiten auf den ISO/OSI-Schichten drei und vier. Sie überprüfen alle ankommenden Datenpakete auf bestimmte Eigenschaften, die den einzelnen

Feldern der jeweiligen Protokollheader entnommen werden. Hierbei werden nur die Header-Informationen der in den Schichten 3 und 4 verwendeten Protokolle ausgewertet. Höhere Schichten, insbesondere die in den Anwendungsprotokollen abgesetzten Kommandos und die in den Paketen enthaltenen Daten,

bleiben unberücksichtigt. Die folgende Tabelle zeigt häufig zur Filterung herangezogene Felder der Protokollheader (vgl. Abschnitt 9.3.2: Protokolle der Transportschicht):

Paketfilter sind IP-Router mit der zusätzlichen Fähigkeit, Datenpakete entsprechend eines Regelwerks weiterzuleiten oder zu sperren.

¹ Eine gängige Faustregel besagt, dass 80% aller Angriffe aus dem internen Netz stammen!

Protokoll	Feld	Beschreibung
IP	Source Address	IP-Quelladresse
	Destination Address	IP-Zieladresse
	Protocol	Verwendetes Transportprotokoll (z. B. TCP, UDP oder ICMP)
TCP	Flags	Steuerung des Verbindungsaufbaus und -abbaus sowie der Datenübertragung
	Source-Port	Quell-Portnummer
	Destination Port	Ziel-Portnummer
UDP	Source-Port	Quell-Portnummer
	Destination Port	Ziel-Portnummer
ICMP	Typ	Typ der versendeten ICMP-Nachricht
	Code	Nähere Informationen zur ICMP-Nachricht

Tab. 14.2.4-1
Häufig für die Paketfilterung verwendete Protokollfelder

Die eigentliche Filterung der Datenpakete erfolgt anhand von Regeln, die vom Administrator aufgestellt und am Paketfilter konfiguriert werden. Mittels dieser Regeln entscheidet die Firewall darüber, wie mit den einzelnen Paketen umzugehen ist. So kann eine Regel das Passieren oder das Zurückweisen der Pakete durch die Firewall bewirken. Beispiele für solche Regeln sind:

- „Sperre alle Datenpakete mit der IP-Quelladresse 135.67.214.12.“
- „Leite alle Datenpakete des Rechners 192.169.0.5 an den Rechner 135.67.214.12 weiter, verwaffe jedoch alle Pakete, die in umgekehrter Richtung die Firewall erreichen.“
- „Sperre alle Datenpakete, die den Dienst SMTP verwenden.“

Im Allgemeinen werden die aufgestellten Regeln für jedes Paket von oben nach unten abgearbeitet. Sobald eine Regel auf das zu untersuchende Datenpaket passt, wird die in der Regel definierte Aktion ausgeführt. Alle nachfolgenden Regeln werden dann nicht weiter berücksichtigt.

Bei der Paketfilterung wird unterschieden zwischen

- statischen Paketfiltern:

Statische Paketfilter arbeiten zustandslos, d. h. die Filterregeln sind unabhängig von vorangegangenen bereits untersuchten Datenpaketen. Auf jedes Paket wird immer derselbe Satz von Filterregeln angewendet.

- dynamischen Paketfiltern:

Dynamische Paketfilter¹ arbeiten zustandsabhängig: Wenn eine bestimmte Verbindung erlaubt wurde, wechselt der Paketfilter in einen Zustand, in dem automatisch auch die benötigte Rückrichtung für die Dauer der Verbindung freigeschaltet wird. Hierzu muss sich die Firewall jeden Verbindungsauflauf merken, um Folgepakete einer bestimmten Verbindung zuordnen zu können.

Einfache Paketfilter können unter Nutzung vorhandener Router realisiert werden. Viele kommerzielle Router besitzen bereits die Fähigkeit, Pakete nach vorgegebenen Regeln zu analysieren, so dass sie unmittelbar als Paketfilter eingesetzt werden

¹ Ein anderer Begriff für **dynamische Paketfilterung** lautet „Stateful Inspection“.

TIPP

Da Router auf der Schicht 3 des ISO/OSI-Referenzmodells arbeiten, können sie lediglich den IP-Header untersuchen. Portadressen sind jedoch im Header der Schicht 4 eingebettet und können daher bei Screening Routern nicht ausgewertet und für die Paketfilterung verwendet werden.

können. Aus diesem Grund wird dieser Router-Typ auch als Screening¹ Router bezeichnet.

Für den Aufbau komplexerer Router sind eigene Rechnersysteme zu installieren und zu konfigurieren oder ist auf spezielle bereits vorgefertigte Komponenten zurückzugreifen.



14.2.4-2 Router mit Paketfilter

Vorteile:

- **hohe Arbeitsgeschwindigkeit**
- **kostengünstig**
- **leichte Konfiguration und Wartung**

Nachteile:

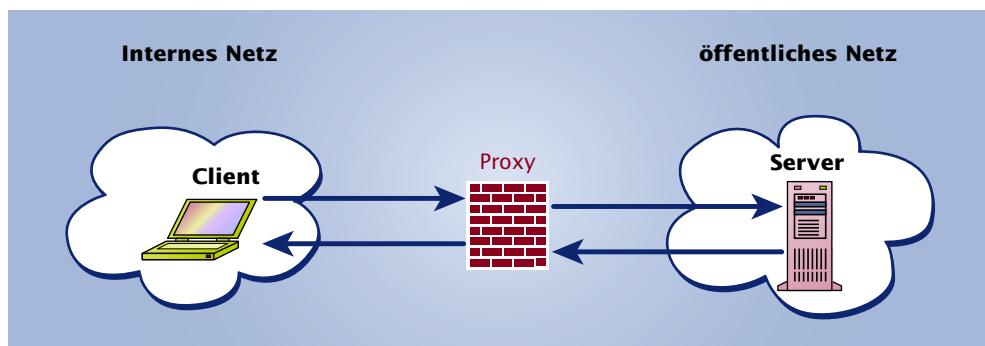
- **kein umfassender Schutz**
- **nur einfache Protokollierungsmöglichkeiten**
- **Eine einzelne Komponente ist für den Schutz des gesamten Netzwerks zuständig.**

Proxy²-Firewalls:

Ein großes Problem bei der Kontrolle von Verbindungen zwischen dem internen und dem externen Netz besteht darin, dass einzelne Rechner des internen Netzes oftmals nicht ausreichend gegen Angriffe von außerhalb geschützt sind. So könnten unbedarfte Nutzer Programme für den Aufbau einer Internetverbindung verwenden, die einen unbefugten Zugriff über das Internet auf diesen Rechner zulassen. Aus diesem Grund werden häufig Proxy-Server eingesetzt.

*Unter einem **Proxy** versteht man eine Software, die bestimmte Dienste stellvertretend für einen Rechner ausführt.*

Der Proxy befindet sich zwischen den beiden Netzwerken und vermittelt zwischen Client und Server (siehe Abb. 14.2.4-3). Soll ein Zugriff auf das jeweilige andere Netz erfolgen, so kann das nicht direkt durch Client und Server vonstatten gehen. Stattdessen wird vom Proxy-Server ein entsprechender Dienst angeboten, den die beiden Rechner verwenden müssen. Auf diese Weise kann man sicherstellen, dass die eigentliche Netzverbindung nur über die sichere Software des Proxy-Servers erfolgt.



14.2.4-3 Proxy-Firewall

¹ **to screen:** engl. abschirmen

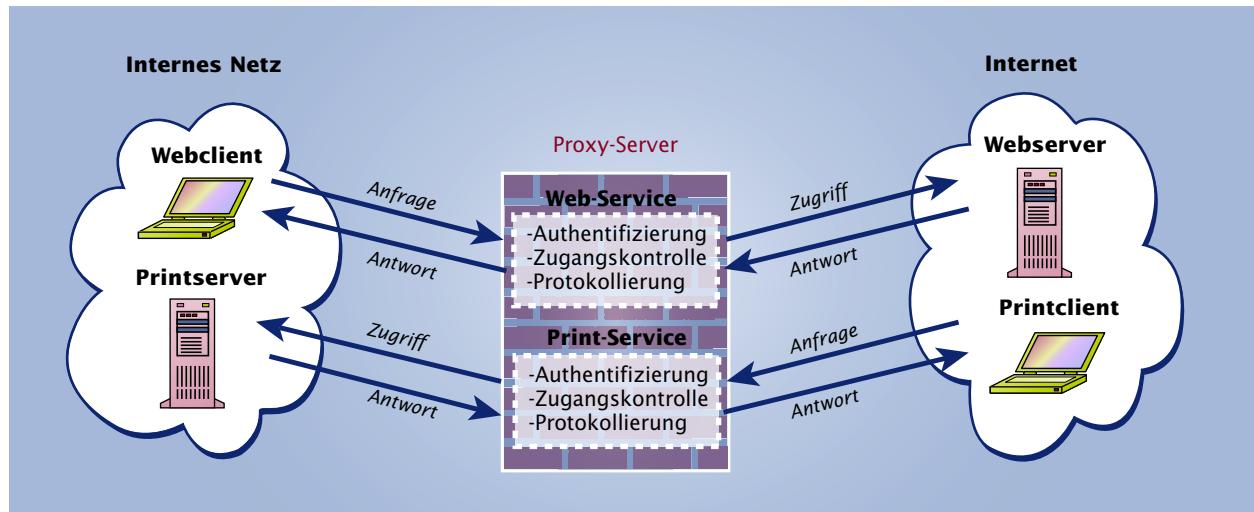
² **Proxy:** engl. Stellvertreter

Eine Proxy-Firewall verhält sich gegenüber dem Client wie der im anderen Netz anzusprechende Server. Umgekehrt verhält sich die Proxy-Firewall gegenüber dem

Server wie der im anderen Netz anzusprechende Client. Die Firewall übernimmt damit eine Art Stellvertreterfunktion und vermittelt zwischen Client und Server. Hierbei kann sie die Zulässigkeit des beantragten Verbindungsaufbaus überprüfen. Dazu gehören insbesondere die Authentifizierung des aufrufenden Clients und die Protokollierung der durchgeführten Aktivitäten. Proxy-Firewalls arbeiten auf der Transportschicht des ISO/OSI-Referenzmodells. Sie werden daher häufig auch als Verbindungs-Gateways bezeichnet.

Neben der Funktion als Firewall dient ein Proxy-Server häufig auch der Zwischen-speicherung von Webseiten. Hierbei speichert der Proxy oft angeforderte Webseiten und kann diese dann ausgeben ohne vorher den eigentlichen Webserver kontaktiert zu haben. Anfragen können so schneller beantwortet und die Netzlast reduziert werden.

Abb. 14.2.4-4 zeigt ein Beispiel einer Proxy-Firewall, die die Dienste „Web“ und „Print“ unterstützt. Beim Abrufen von Internetseiten sendet der Client zunächst eine entsprechende Anfrage aus dem internen Netz an den Web-Service des Proxy. Nachdem dort die erforderlichen Zugriffskontrollen durchgeführt wurden, baut der Proxy die Verbindung zum gewünschten Webserver des Internets auf. Die von diesem Webserver gelieferten Webseiten passieren anschließend ebenfalls den Proxy und werden entsprechend überwacht. Eine ähnliche Vorgehensweise ergibt sich, wenn vom Internet aus der Printserver des internen Netzes verwendet werden soll. Hier sendet der Client zunächst seinen Druckauftrag an den Print-Service der Proxy-Firewall. Nach der Zugangskontrolle erfolgt dann die Weiterleitung des Auftrags an den eigentlichen Printserver des internen Netzes.



14.2.4-4 Proxy-Firewall mit Web- und Printdienst

Bevor die Daten aus dem internen Netz mittels Proxy weitergeleitet werden, ersetzt der Proxy die IP-Absendeadressen jeweils durch seine eigene. Die Rechner des externen Netzes kontaktieren dann direkt den Proxy und haben keine Kenntnis davon, dass sie eigentlich mit einem Rechner des internen Netzes in Verbindung stehen. Durch diese Verschleierung der Struktur des internen Netzes entsteht ebenfalls eine erhöhte Sicherheit.

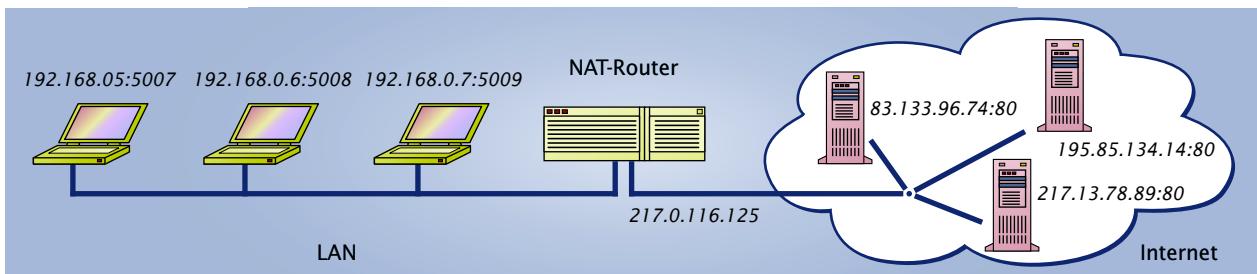
Das Ersetzen der IP-Adresse eines Datenpakets durch eine andere IP-Adresse bezeichnet man als „Network Address Translation“ (NAT).

Ein weiterer Grund für die Anwendung von NAT (RFC 1631) ist der Einsatz privater IP-Adressen in einem lokalen Netzwerk. Damit eine Kommunikation mit den Rechnern des Internet möglich ist, müssen die privaten Adressen in öffentliche IP-Adressen umgesetzt werden. Die Adressumsetzung erfolgt hierbei z. B. durch Firewalls oder Router am Übergang zwischen LAN und Internet.

Werden nicht nur IP-Adressen, sondern auch Portnummern ersetzt, so bezeichnet man dieses als Masquerading (RFC 3022), Port Address Translation (PAT) oder Network Address Port Translation (NAPT).

Beispiel:

Das lokale Netz 192.168.0.0/24 einer Firma soll mit dem Internet verbunden werden. Der Internet-Service-Provider stellt der Firma hierzu die öffentliche IP-Adresse 217.0.116.125 zur Verfügung (siehe Abb. 14.2.4-5).



14.2.4-5

Anbindung eines LAN an das Internet mittels NAT

Bei Aufruf der Internet-Webserver durch die LAN-Clients werden die Quell-IP-Adressen der Clients mittels NAT durch die einzige verfügbare öffentliche IP-Adresse 217.0.116.125 ersetzt. Die zugehörigen Quell-Portnummern der Clients erhalten neue Werte beginnend mit der Nummer 61000 (siehe Tab. 14.2.4-2).

LAN → Internet		
Quell-IP:Quell-Port	Ziel-IP:Ziel-Port	NAT: Quell-IP-neu:Quell-Port-neu
192.168.0.5:5007	217.13.78.89:80	217.0.116.125:61000
192.168.0.6:5008	83.133.96.74:80	217.0.116.125:61001
192.168.0.7:5009	195.85.134.14:80	217.0.116.125:61002

Tab. 14.2.4-2
NAT bei Aufrufen aus dem LAN in das Internet

Die Datenpakete der Internet-Webserver werden zunächst an den NAT-Router gesendet. Dieser kann anhand der Portnummer der Ziel-IP-Adresse den eigentlichen Empfänger ermitteln und tauscht die Adresse und die Portnummer dann mit den zugehörigen in einer NAT-Tabelle gespeicherten LAN-Werten aus (siehe Tab. 14.2.4-3).

Tab. 14.2.4-3
NAT bei Aufrufen aus dem Internet in das LAN

Internet → LAN		
Quell-IP:Quell-Port	Ziel-IP:Ziel-Port	NAT: Ziel-IP-neu:Ziel-Port-neu
217.13.78.89:80	217.0.116.125:61000	192.168.0.5:5007
83.133.96.74:80	217.0.116.125:61001	192.168.0.6:5008
195.85.134.14:80	217.0.116.125:61002	192.168.0.7:5009

¹ **to masquerade:**
engl. sich maskieren,
verkleiden

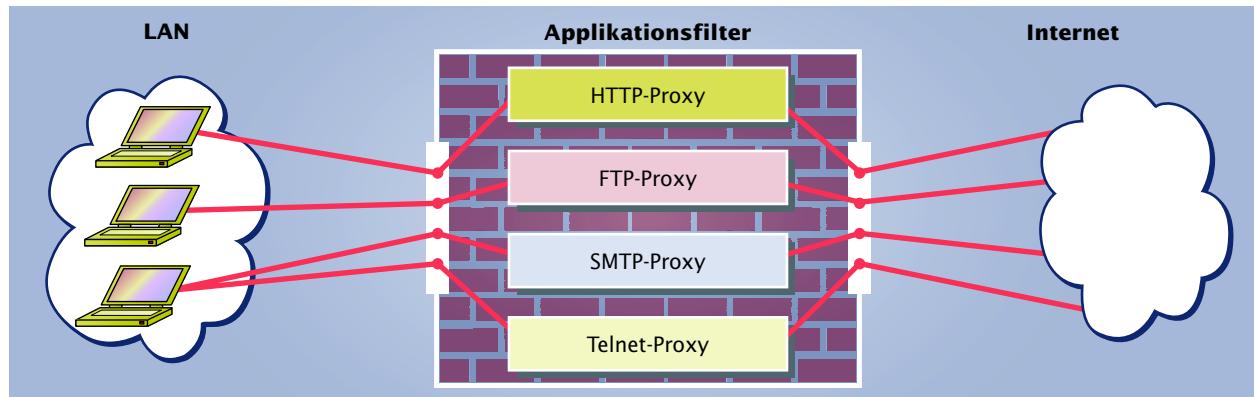
Vor- und Nachteile einer Proxy-Firewall:

Vorteile:	Nachteile:	TIPP
<ul style="list-style-type: none"> ■ Direkte TCP-Verbindungen zwischen Client und Server werden verhindert. ■ Für viele Dienste einsetzbar wie z. B. für Mail-, Web- und Print-Dienste. ■ Verbergen der Netzstruktur durch IP-Adressumsetzung. 	<ul style="list-style-type: none"> ■ Aufgrund der Ansiedlung auf der Transportebene und nicht auf der Anwendungsebene des ISO/OSI-Referenzmodells, können nur allgemeine Vermittlungsdienste zur Verfügung gestellt werden. Besonderheiten einzelner Anwendungsprotokolle bleiben unberücksichtigt. So sind HTML-Verbindungen nur als Ganzes kontrollierbar. Eine unterschiedliche Behandlung der übermittelten Datenpakete in Abhängigkeit der konkreten Inhalte ist jedoch nicht möglich. ■ Der Einsatz einer Proxy-Firewall erfordert in der Regel eine entsprechende Konfiguration der Software auf der Clientseite, da Aufrufe, die sich an einen bestimmten Server richten, auf den Proxy-Server umzuleiten sind. 	<p>Um die Sicherheit des Rechners, auf dem sich die Firewall befindet, vor Angriffen zu erhöhen, sollte dort nur die Software installiert sein, die unbedingt für das Funktionieren der Firewall benötigt wird! Die gleichzeitige Verwendung von Firewall-Rechnern als spezielle Server, z. B. Webserver, sollte vermieden werden. Ebenso sollten keine Benutzer-Accounts über diesen Rechner verwaltet werden.</p>

Applikationsfilter:

Applikationsfilter arbeiten auf der Anwendungsschicht des ISO/OSI-Referenzmodells. Sie stellen im Prinzip eine Proxy-Firewall dar. Im Gegensatz zu den reinen auf der Transportschicht arbeitenden Proxies besitzen sie jedoch die Fähigkeit, die Inhalte der einzelnen Datenpakete entpacken und bzgl. des Inhalts untersuchen zu können. Ein Applikationsfilter für den FTP-Dienst kann so z. B. erkennen, welche FTP-Befehle (siehe Abschnitt 9.3.1: Protokolle des Anwendungssystems) übertragen werden, und behandelt diese dann gemäß der festgelegten Sicherheitsstrategie unterschiedlich. Werden beispielsweise Schreibzugriffe auf einen FTP-Server untersagt, so muss der Applikationsfilter das FTP-Kommando „PUT“ herausfiltern.

Abb. 14.2.4-6 zeigt einen Applikationsfilter, der die Dienste HTTP, FTP, SMTP und Telnet unterstützt. Er schottet das zu schützende LAN gegen das unsichere Internet ab. Alle Nachrichten vom oder in das LAN müssen den Filter über dessen Schnittstellen passieren. Die einzelnen anwendungsspezifischen Proxies kontrollieren dann die zugehörigen Zugriffe.



14.2.4-6 Applikationsfilter

Vorteile:

- Durchführung von Kontrollen in Abhängigkeit der versendeten Nachrichten.
- Hohe Sicherheit

Nachteile:

- Langsamer als Paketfilter und einfache, auf der Transportschicht arbeitende Proxy-Firewalls.

Firewall-Architekturen:

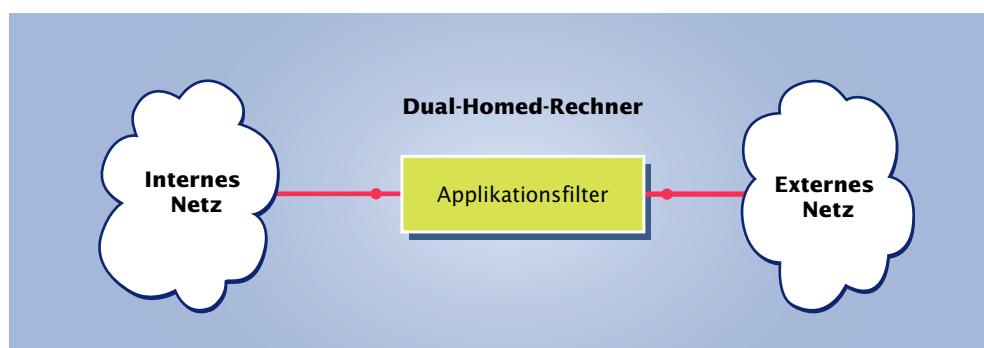
Zur Erhöhung der Sicherheit des internen Netzes werden üblicherweise Kombinationen von Paket- und Applikationsfiltern verwendet. Hieraus ergibt sich eine Vielzahl von Möglichkeiten in der Anordnung von Firewalls. Typische Beispiele derartiger Firewall-Architekturen sind

- Dual-Homed-Firewall
- Screened-Host-Firewall
- Screened-Subnet-Firewall

Dual-Homed-Firewall¹:

Die Dual-Homed-Firewall basiert auf einem Rechner mit zwei Netzwerkschnittstellen (Dual-Homed-Rechner), auf dem sich ein Applikationsfilter befindet (siehe Abb. 14.2.4-7).

Diese Firewall-Architektur bietet eine hohe Sicherheit, da es nicht möglich ist, mit dem Datenpaket eines Dienstes die Dual-Homed-Firewall zu durchqueren, falls der Dual-Homed-Rechner keinen Proxy für diesen Dienst enthält.



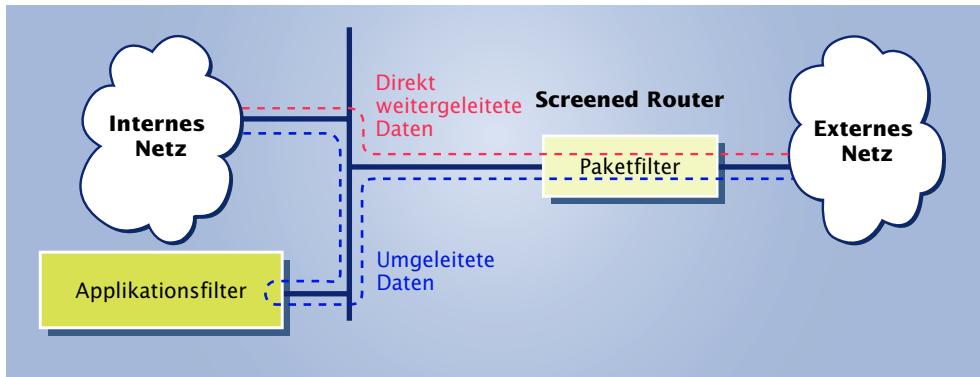
14.2.4-7 Dual-Homed-Firewall

Screened-Host-Firewall:

Die Screened-Host-Firewall enthält als Bastion-Host einen Applikationsfilter, der durch einen Paketfilter zusätzlich geschützt wird. Gegenüber der Dual-Homed-Firewall besitzt der Applikationsfilter nur einen Netzwerkanschluss und ist hierüber mit dem internen Netz verbunden. Der Paketfilter wird daher in Form eines Screening-Routers realisiert, so dass dieser den Datenverkehr aus dem externen in das interne Netz an den Applikationsfilter zur weiteren Bearbeitung weiterleitet. Der Router ist somit eine sicherheitskritische Komponente, deren Routingtabelle besonders vor unautorisierten Zugriffen zu schützen ist.

¹ **Dual Homed:** engl.
Zweifach beheimatet

Im Gegensatz zur Dual-Homed-Firewall ist es bei der Screened-Host-Firewall möglich, dass der Paketfilter spezielle Datenpakete direkt an den Empfänger weiterleitet, also den Applikationsfilter umgeht. Das kann für vertrauenswürdige Dienste sinnvoll sein, für die keine Proxies innerhalb des Applikationsfilters existieren. Es birgt jedoch auch erhöhte Sicherheitsrisiken, so dass Screened-Host-Firewalls nur dann eingesetzt werden sollten, wenn diese Flexibilität unbedingt notwendig ist.



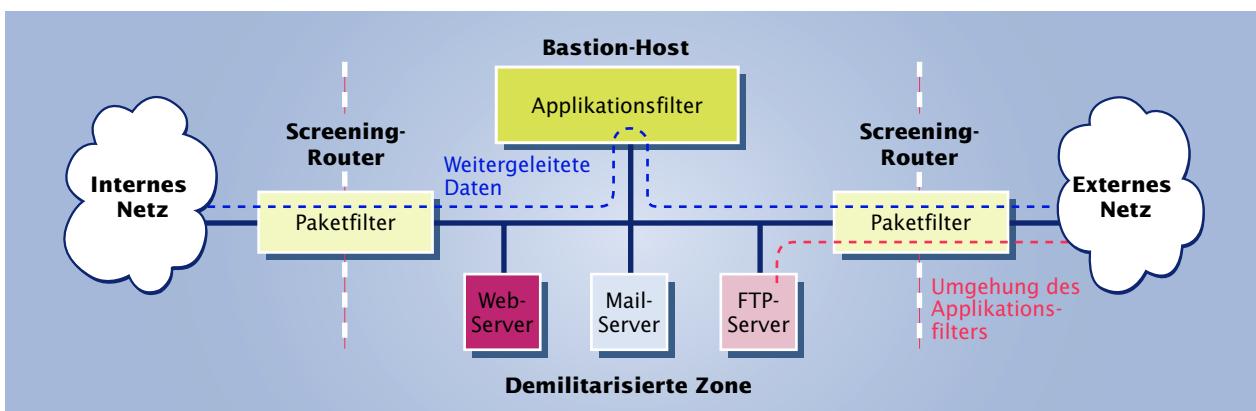
14.2.4-8
Screened-Host-Firewall

Screened-Subnet-Firewall:

Um einen höheren Sicherheitsgrad zu erzielen, wird bei der Screened-Subnet-Firewall ein zusätzliches Netzsegment als Isolierung zwischen dem internen und dem externen Netz eingefügt. Dieses Subnetz bezeichnet man auch als „demilitarisierte Zone“ (DMZ). Zur Realisierung der DMZ ist dem Applikationsfilter je ein Screening Router vor- und nachgeschaltet.

Neben dem Applikationsfilter können innerhalb der DMZ noch Server enthalten sein wie z. B. ein Web-, Mail- oder FTP-Server. Durch die Einbettung dieser Server in die isolierte Zone wird erreicht, dass Angreifer, die es geschafft haben, einen dieser Server unter ihre Kontrolle zu bringen, trotzdem keinen direkten Zugriff auf das interne Netz haben. Sie müssen zunächst den Paketfilter überwinden.

Genau wie bei der Screened-Host-Firewall kann der Applikationsfilter gezielt umgangen werden, so dass die Datenpakete direkt den Servern in der DMZ zugestellt werden können. Aufgrund der DMZ ist es jedoch nicht möglich, die Datenpakete direkt zwischen dem internen und dem externen Netz auszutauschen.



14.2.4-9 Screened-Subnet-Firewall

¹ Die Bezeichnung basiert auf dem sich zwischen Nord- und Südkorea befindenden „Niemandsland“.

Grenzen von Firewalls:

Ein gut konfiguriertes Firewall-System trägt erheblich zur Steigerung der Sicherheit von Rechnernetzen bei. Eine Universallösung für alle Sicherheitsprobleme existiert damit jedoch nicht. Insbesondere sind folgende Hinweise für den Betrieb von Firewall-Systemen zu beachten:

- Das korrekte und widerspruchsfreie Konfigurieren von Firewall-Systemen ist komplex und schwierig! Zur Erstellung einer Sicherheitsstrategie für das zu schützende System sind präzise Kenntnisse über mögliche Bedrohungspotenziale, die Netzinfrastruktur sowie die von den Nutzern durchzuführenden Aktivitäten erforderlich.
- Eine Firewall erfordert eine ständige und sorgfältige Administration, damit mögliche Angriffe frühzeitig erkannt und entsprechende Schutzmaßnahmen eingeleitet werden können.
- Firewalls bieten nur einen begrenzten Schutz gegen die Einschleusung von Programmen mit schädigender Wirkung. Durch eine in die Firewall implementierte Stichwortsuche lässt sich nur der Code aufdecken, der bekannte Virenkennungen enthält. Mittels einfacher Codierungstechniken lassen sich solche Informationen jedoch bereits leicht verschleiern, so dass Programme mit schädigender Wirkung dann ungehindert die Firewall passieren können.
- Die Verwendung der Tunneltechnik (siehe Abschn. 14.2.5: Virtual Private Networks) kann dazu missbraucht werden, die Filterregeln einer Firewall zu umgehen.

1. Gibt es in Ihrer Schule bzw. Ihrem Betrieb eine Firewall? Welcher Klasse und welcher Architektur ist die Firewall ggf. zuzuordnen?
2. Realisieren Sie mit einem Rechner einen Paketfilter. Dieser soll nur den Webdienst zulassen.

14.2.5 Virtual Private Networks¹

Firma Lütgens möchte ihr lokales Netzwerk, das mit dem Internet verbunden ist, vor Bedrohungen aus dem Internet schützen. So sollen z. B. keine Programme mit schädigender Wirkung aus dem Internet eingeschleust werden dürfen und keine unbefugten Zugriffe über das Internet auf das lokale Netzwerk erfolgen können.

Für den Zugriff auf entfernte Rechner bieten sich zwei Möglichkeiten an:

- Direkteinwahl über das Telefonnetz per DFÜ
- Zugang über das Internet

Die Direkteinwahl über das Telefonnetz ist sehr sicher, jedoch teuer. Der Zugang über das Internet ist dagegen preisgünstig, birgt aber ein erhebliches Sicherheitsrisiko. Um das Internet dennoch für eine geschützte Datenübertragung nutzen zu können, sind daher besondere Sicherheitsvorkehrungen notwendig. Hier bietet sich der Einsatz eines **Virtual Private Network (VPN)** an.

Zur Realisierung der geschützten Verbindung stellt das VPN eine logische Verbindung über das öffentliche Netz zur Verfügung. Da die Daten ähnlich wie bei einem Tunnel zum Zielrechner fließen, wird dieses Verfahren auch als „Tunneling“ be-

¹ Virtual Private Network:
engl. Virtuelles privates Netz