Kapitel 12

VPN-Systeme versus Firewall-Systeme

Der Sicherheitsmechanismus Verschlüsselung bei VPN-Systemen wirkt nur gegen die unerlaubte Einsicht der Informationen während der Kommunikation per Internet. Zusätzlich muss noch – mit Hilfe von Firewall-Systemen – das zweite Hauptrisiko beim Anschluss an das Internet, der unerlaubte Zugriff auf die eigenen Rechnersysteme, verhindert werden.

12.1 Die Idee von Firewall-Systemen

Firewall-Systeme werden als Schranke zwischen ein zu schützendes Netz (zum Beispiel ein internes Unternehmensnetzwerk) und ein unsicheres Netz (zum Beispiel das Internet) geschaltet, so dass der gesamte Datenverkehr zwischen den beiden Netzen nur über das Firewall-System möglich ist. Ein Angreifer darf nicht in der Lage sein, ein Firewall-System zu überwinden.

Ein Firewall-System ist somit das elektronische Äquivalent zu einem Pförtner: Es überprüft, wer aus dem unsicheren Netz auf das zu schützende Netz der Organisation zugreifen darf, und kontrolliert, über welche Protokolle und Dienste zugegriffen und mit welchen Rechnersystemen kommuniziert wird.

Auf dem Firewall-System werden Sicherheitsmechanismen implementiert, die diesen Übergang sicher und beherrschbar machen. Dazu analysiert das Firewall-System die Kommunikationsdaten, kontrolliert die Kommunikationsbeziehungen und Kommunikationspartner, reglementiert die Kommunikation gemäß der Sicherheitspolitik des Unternehmens, protokolliert sicherheitsrelevante Ereignisse und alarmiert bei starken Verstößen den Security Administrator.

Allgemeine Ziele eines Firewall-Systems sind:

- Zugangskontrolle auf der Netzwerkebene
  Es wird überprüft, welche Rechnersysteme (IP-Adressen) über das Firewall-System miteinander kommunizieren dürfen.
- Zugangskontrolle auf der Benutzerebene
  Das Firewall-System überprüft, welche Benutzer über das Firewall-System eine Kommunikationsverbindung aufbauen dürfen. Dazu wird die Echtheit (Authentizität) des Benutzers verifiziert.

- Rechteverwaltung
  Im Rahmen der Rechteverwaltung wird festgelegt, mit welchen Protokollen und Diensten und zu welchen Zeiten eine Kommunikation über das Firewall-System stattfinden darf.
- Kontrolle auf der Anwendungsebene
  Es wird überprüft, ob Kommandos genutzt oder Dateiinhalte übertragen werden, die nicht zu der durch die Anwendung definierten Aufgabenstellung gehören.
- Entkopplung von Diensten
  Dienste werden entkoppelt, damit Implementierungsfehler, Schwachstellen und Konzeptionsfehler der Dienste keine Möglichkeit für Angriffe bieten.
- Beweissicherung und Protokollauswertung
  Verbindungsdaten und sicherheitsrelevante Ereignisse werden protokolliert und können für die Beweissicherung von Handlungen der Benutzer und für die Erkennung von Sicherheitsverletzungen ausgewertet werden.
- Alarmierung
  Besonders sicherheitsrelevante Ereignisse werden an ein Sicherheitsmanagement gesendet, damit bei Sicherheitsverletzungen schnell reagiert werden kann.
- Verbergen der internen Netzstruktur
  Die Kenntnis der Kommunikationswege erleichtert Hackern die Arbeit. Daher ist es wichtig, die Struktur des zu schützenden Netzes gegenüber dem unsicheren Netz geheim zu halten. Das Firewall-System schirmt die Struktur des zu schützenden Netzes nach außen hin ab. Es soll vom unsicheren Netz aus nicht sichtbar sein, ob im zu schützenden Netz 10, 100, 1.000 oder 10.000 Rechnersysteme vorhanden sind.

Ein Firewall-System stellt den »Common Point of Trust« für den Übergang zwischen unterschiedlichen Netzen dar, das heißt der einzige Weg zwischen den Netzen führt kontrolliert über das Firewall-System.

Firewall-Systeme werden eingesetzt, um sich an unsichere Netze wie zum Beispiel das Internet sicher ankoppeln zu können. Sie werden aber auch eingesetzt, um das eigene Netz zu strukturieren und hier Sicherheitsdomänen mit unterschiedlichem Schutzbedarf zu schaffen.

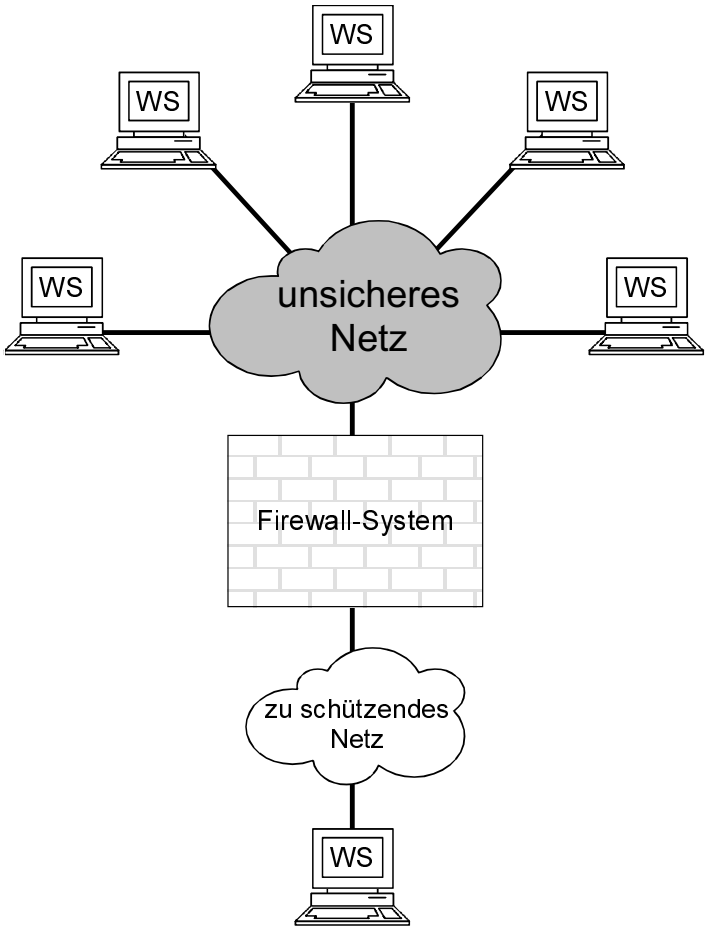

Abb. 12.1: Firewall-System

12.2 Grundsätzliche Unterschiede von VPN- und Firewall-Systemen

In diesem Abschnitt werden die grundsätzlichen Unterschiede von VPN- und Firewall-Systemen dargestellt.

- Geltungsbereich
  - *Firewall-Systeme* schützen eine Organisationseinheit.
  - *VPN-Systeme* schützen die Kommunikation mehrerer Einheiten (Kommunikationspartner) untereinander.

  Typischerweise werden Firewall-Systeme hinter die VPN-Gateways geschaltet.

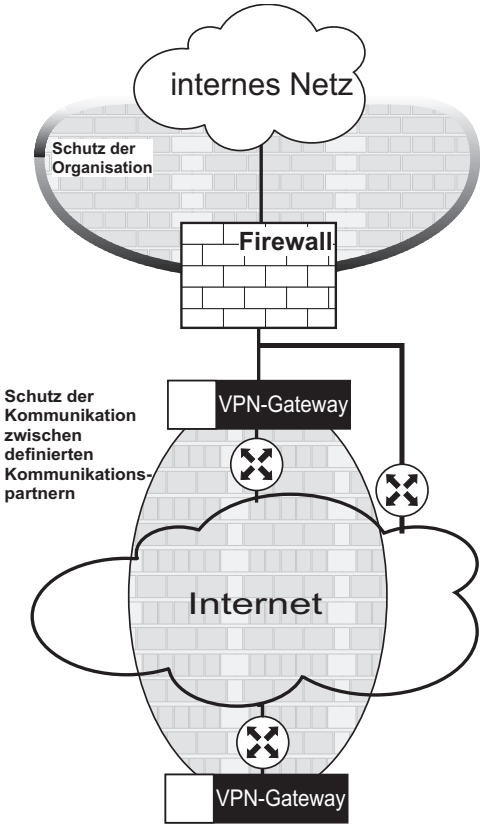

Abb. 12.2: Geltungsbereiche von VPNs und Firewall-Systemen

- Ziele
  - *Firewall-Systeme* schützen vor unerlaubtem Zugriff auf Rechnersysteme und deren Dienste und Daten. Hacker, Cracker, Spione und sonstige Angreifer werden aktiv abgehalten und erlaubte Kommunikationsverbindungen werden auf das für die Aufgabenstellung notwendige Maß reduziert.
  - *VPN-Systeme* schützen vor unerlaubten Zugriff auf die Daten während der Übertragung zwischen definierten Kommunikationspartnern.
- Unabhängigkeit
  - Ein besonderer Aspekt bei *Firewall-Systemen* ist, dass sie lokal verwaltet werden können, das heißt, bezogen auf die Kommunikationsmöglichkeiten und die Protokollierung kann die eigene lokale Sicherheitspolitik unabhängig von anderen realisiert werden.

– Bei *VPN-Systemen* muss die Sicherheitspolitik in Übereinstimmung mit den Kommunikationspartnern realisiert werden, damit eine einheitliche Sicherheit gewährleistet werden kann.

Einige Hersteller bieten in ihren VPN-Lösungen auch Firewall-Funktionalitäten. Diese müssen dann aber auch den Kriterien vom sicheren Aufbau von Firewall-Systemen genügen /Pohl2001a/.

12.3 Kombinationen von VPN- und Firewall-Systemen

Es gibt verschiedene Möglichkeiten, VPN- und Firewall-Systeme miteinander zu kombinieren. In diesem Abschnitt werden die Vor- und Nachteile der unterschiedlichen Kombinationen diskutiert.

Bei der Beschreibung der verschiedenen Anordnungen wird die Sichtweise »von außen«, d.h. aus dem Internet, zugrunde gelegt.

12.3.1 VPN-System vor einem Firewall-System

Bei dieser Kombination steht das Firewall-System hinter den VPN-Gateways. Die Kommunikation, die nicht verschlüsselt werden soll, z.B. der Zugriff auf frei zugängliche Web-Server, wird an den VPN-Gateways vorbeigeführt.

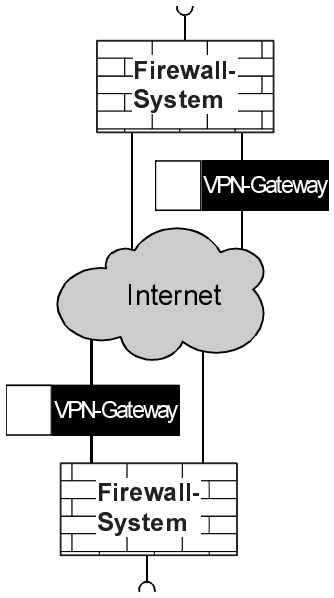

Abb. 12.3: VPN-System vor einem Firewall-System

- **Vorteile:**
  - Der gesamte Datenstrom kann vom Firewall-System analysiert und kontrolliert werden, da er im Klartext vorliegt.
  - Die Verwaltung von Firewall- und VPN-System kann getrennt durchgeführt werden.
- **Nachteile:**
  - Die Daten liegen im Firewall-System im Klartext vor. Dies ist ein Problem, wenn die Verwaltung des Firewall-Systems in der Verantwortung einer Organisation steht, die die Daten nicht lesen soll oder darf. Dieser Fall tritt jedoch in der Praxis selten auf.
  - Da Application Gateways nicht jedes Protokoll (z. B. NetBIOS) unterstützen und dies auch nicht sollen, können evtl. nicht alle Kommunikationsverbindungen durch das Firewall-System geführt werden.

12.3.2 VPN-System vor einem Firewall-System, dahinter ein weiteres VPN-System

Bei dieser Kombination wird ein weiteres VPN-System im Intranet installiert.

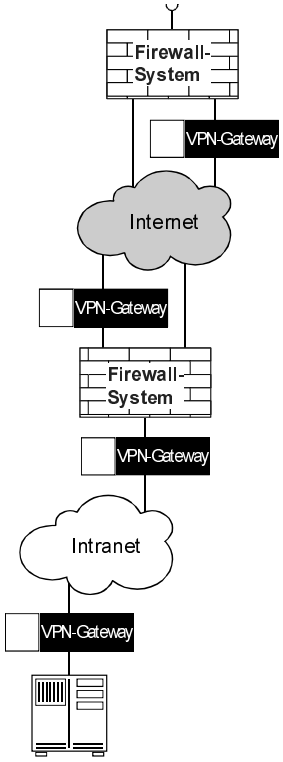

Abb. 12.4: VPN-System vor einem Firewall-System, dahinter ein weiteres VPN-System

- **Vorteile**
  - Es bestehen die gleichen Vorteile wie bei der in Kapitel 12.3.1 *VPN-System vor einem Firewall-System* beschriebenen Anordnung.
  - Die Sicherheitsumgebung ist modular aufgebaut und es können granuläre Regeln verwendet werden.
  - Bei dieser Anordnung kann eine höhere Tiefe der End-to-End-Verschlüsselung erzielt werden.
  - Verschlüsselte Kommunikation kann nur mit Server-Systemen durchgeführt werden, die in den Verbindungsregeln der VPN-Gateways eingetragen sind.

Nähere Informationen hierzu finden Sie in dem Buch »Firewall-Systeme. Sicherheit für Internet und Intranet« von Norbert Pohlmann, MITP-Verlag, 5. Auflage 2002, Kap. 10.2 *Internet Server.*

- **Nachteile**
  - Es bestehen die gleichen Nachteile wie bei der in Kapitel 12.3.1 *VPN-System vor einem Firewall-System* beschriebenen Anordnung.
  - Aufgrund der zusätzlichen Geräte sind die Kosten für Anschaffung und Betrieb hoch.

12.3.3 VPN-System hinter einem Firewall-System

Bei dieser Kombination steht das VPN-Gateway hinter dem Firewall-System. Die Kommunikation, die nicht verschlüsselt werden soll, z. B. der Zugriff auf frei zugängliche Web-Server hinter dem Firewall-System oder in der DMZ, wird an den VPN-Gateways vorbeigeführt.

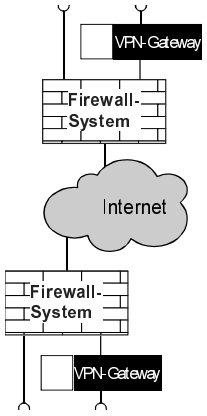

Abb. 12.5: VPN-System hinter einem Firewall-System

- **Vorteile**
  - Hierbei wird eine höhere Tiefe der End-to-End-Verschlüsselung erreicht.
  - Die VPN-Gateways können auch außerhalb des Intranets positioniert werden, z. B. vor dem Ziel-System.
  - Das VPN-System ist optimal vor Angriffen und Manipulationsversuchen aus dem Internet geschützt. Über das Firewall-System können nur die verschlüsselten Dienste (ESP, AH, IKE) auf das VPN-Gateway zugreifen.
- **Nachteile**
  - Das Firewall-System ist nicht in der Lage, den verschlüsselten Datenstrom zu analysieren und zu kontrollieren, da die Daten auf der IP-Ebene (IPSec-Tunnel) verschlüsselt sind. Dies ist dann ein Problem, wenn über die verschlüsselte Kommunikation ein Angriff durchgeführt wird.
  - Da ein Firewall-System typischerweise eine Adressumwandlung (Network Address Translation, NAT) durchführt, können viele VPN-Gateways nicht verwendet werden, da IPSec die NAT-Funktionalität nicht unterstützt. Stattdessen gibt es verschiedene proprietäre NAT-Lösungen (L2TP, NAT traversal u. Ä.).

12.3.4 VPN- und Firewall-System zusammen realisiert

Bei dieser Kombination sind die Firewall- und VPN-Lösung in einem System zusammengefasst.

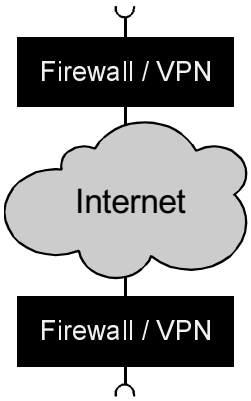

Abb. 12.6: VPN- und Firewall-System zusammen realisiert

- **Vorteile**
  - Typischerweise sind die Kosten geringer.
  - Aufgrund der einheitlichen Verwaltung der Firewall- und VPN-Lösung können transparentere Regeln verwendet werden.

- **Nachteile**
  - Falls eine organisationsübergreifende Verschlüsselung notwendig ist, muss eine VPN-Kommunikation auch mit anderen Lösungen realisiert werden.
  - Da der Geltungsbereich und die Ziele von VPN- und Firewall-Systemen unterschiedlich sind (siehe Kapitel 12.2 *Grundsätzliche Unterschiede von VPN- und Firewall-Systemen*), können Konflikte auftreten.

12.3.5 VPN- und Firewall-System parallel

Bei dieser Kombination arbeiten Firewall- und VPN-System parallel und voneinander unabhängig.

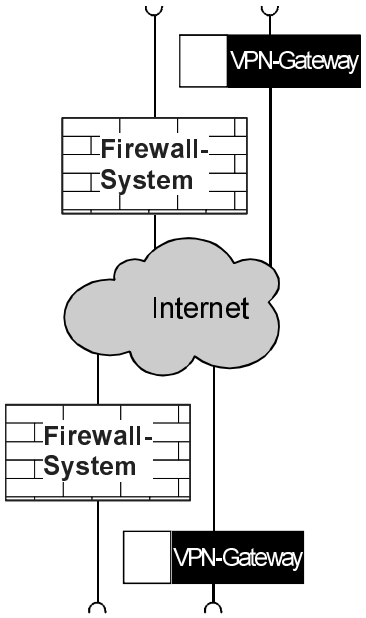

Abb. 12.7: VPN- und Firewall-System parallel

- **Vorteile**
  - VPN- und Firewall-System sind völlig unabhängig voneinander.
- **Nachteile**
  - Die verschlüsselte Kommunikation wird in dieser Kombination nicht analysiert und kontrolliert, da in diesen Kommunikationsweg kein Firewall-System eingebunden ist.
  - Die Sicherheit gegen Angriffe aus dem Internet hängt von der Sicherheit des VPN-Gateways ab.

12.4 Grundelemente von Firewall-Systemen

In diesem Abschnitt wird beschrieben, aus welchen Grundelementen ein Firewall-System aufgebaut werden kann. Es soll aufgezeigt werden, wie technische Sicherheitsmechanismen für Firewall-Elemente realisiert werden können, welche konkreten Möglichkeiten bestehen, um Sicherheit zu gewährleisten, wie sie wirken und wo ihre Grenzen liegen.

Ein Firewall-System kann aus den folgenden Grundelementen bestehen:

- Packet Filter
- Stateful Inspection
- Application Gateway
- Proxies
- Adaptive Proxies

Um die konzeptionellen Unterschiede zu verdeutlichen und so das Verständnis zu erleichtern, werden die einzelnen Firewall-Elemente im Folgendenmit Hilfe von Analogien erläutert.

Eine plastische, leicht fassbare Analogie zu einen Firewall-System ist ein Pförtner. Alle Zugänge zu einem Gebäude sollen vom Pförtner überwacht werden. Hier gilt: Je weniger Zugänge es gibt, desto besser kann der Pförtner den Zugang kontrollieren (Common Point of Trust).

12.4.1 Packet Filter

Das aktive Firewall-Element »Packet Filter« analysiert und kontrolliert die ein- und ausgehenden Pakete auf der Netzzugangs-, der Netzwerk- und der Transportebene. Dazu werden die Pakete (zum Beispiel Ethernet oder Token Ring), die durch das physikalische Kabel übertragen werden, aufgenommen und analysiert. Durch den Packet Filter werden die Netze physikalisch entkoppelt. Ein Packet Filter verhält sich im Normalfall wie eine einfache Bridge. Packet Filter sind nicht nur auf TCP/IP-Protokolle beschränkt.

Ein Packet Filter interpretiert den Inhalt der Pakete und verifiziert, ob die Daten in den entsprechenden Headers der Kommunikationsebenen den definierten Regeln entsprechen. Die Regeln werden so definiert, dass nur die notwendige Kommunikation erlaubt ist und bekannte sicherheitskritische Einstellungen, zum Beispiel die IP-Fragmentierung, vermieden werden. Die Packet Filter werden transparent (als Black Box) in die Leitung eingefügt.

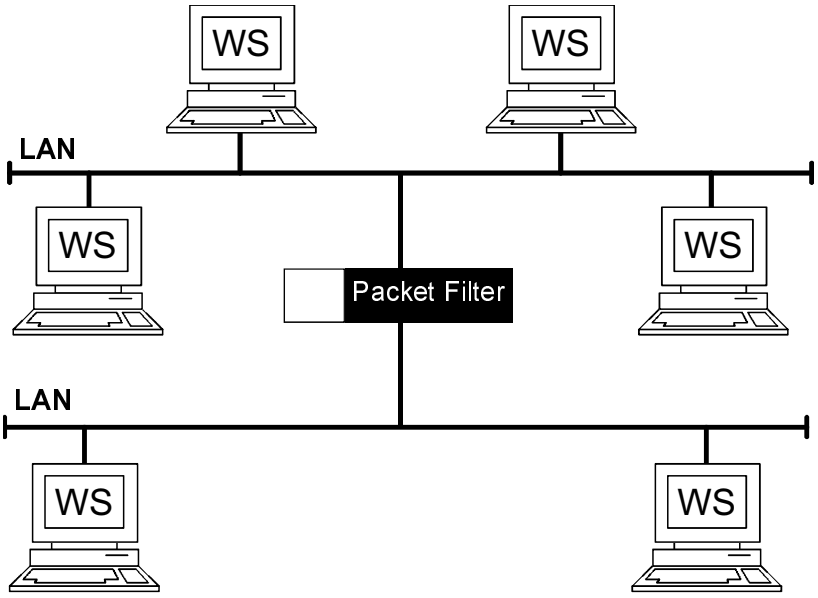

Abb. 12.8: Firewall-Element: Packet Filter

Analogie zum Pförtner:

Wenn der LKW eines Lieferanten am Werktor mit einer Lieferung vorfährt, schaut der »Packet-Filter-Pförtner« auf das Logo an der Seite des LKW, um zu überprüfen, ob es ihm bekannt ist, und lässt den LKW gegebenenfalls unmittelbar durch das Tor, ohne den Lieferschein zu kontrollieren.

Allgemeine Arbeitsweise von Packet Filtern

In der folgenden Abbildung ist die allgemeine Arbeitsweise von Packet Filtern dargestellt. Hier ist zu erkennen, welche Informationen aus den Paketen zur Analyse verwendet werden.

Hier können auf den verschiedenen Kommunikationsebenen unterschiedliche Überprüfungen durchgeführt werden:

- Es wird überprüft, von welcher Seite das Paket empfangen wird (Information aus dem Einbindungsmodul).
- Auf der Netzzugangsebene werden die Quell- und Ziel-Adresse und der verwendete Protokolltyp kontrolliert.

- Auf Netzwerkebene wird je nach Protokoll überprüft:
  - IP-Protokoll: zum Beispiel die Ziel- und die Quell-Adresse und das verwendete Schicht-4-Protokoll, aber auch Optionsfeld und Flags
  - ICMP: die ICMP-Kommandos
  - IPX-Protokoll: zum Beispiel Network/Node
  - OSI-Protokoll: die OSI-Netzwerkadresse
- Auf Transportebene findet
  - bei UDP/TCP zum Beispiel eine Überprüfung der Portnummern (Quell- und Ziel-Port) statt. (Hierüber werden die Dienste wie FTP, Telnet, HTTP definiert.)
  - bei TCP beispielsweise zusätzlich eine Überprüfung der Richtung des Verbindungsaufbaus statt.
- Zusätzlich kann überprüft werden, ob der Zugriff über den Packet Filter in einem definierten Zeitraum durchgeführt wird (zum Beispiel montags bis freitags von 7 Uhr bis 19 Uhr, samstags von 7 bis 13 Uhr, sonntags nicht).

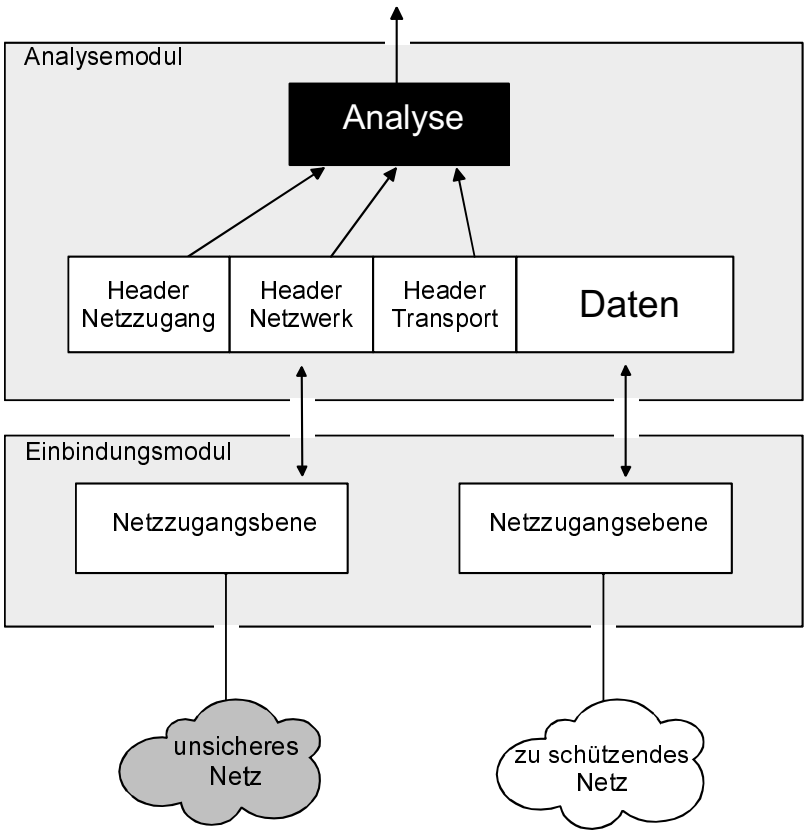

Abb. 12.9: Allgemeine Arbeitsweise eines Packet Filter

Die entsprechenden Prüfinformationen werden dem Regelwerk (Accessliste, Rechteliste) entnommen und mit den Analyse-Ergebnissen verglichen.

Bei Verstoß gegen die Regeln wird dies als sicherheitsrelevantes Ereignis entsprechend protokolliert. Falls diese Option eingerichtet ist, wird eine Spontane Meldung mit den Protokolldaten des sicherheitsrelevanten Ereignisses an das Sicherheitsmanagement gesendet, um eine schnelle adäquate Reaktion zu ermöglichen.

Im Folgenden wird dargestellt, welche Überprüfungen auf den verschiedenen Kommunikationsebenen durchgeführt werden können. Dabei ist zu berücksichtigen, dass die Überprüfung auf der Netzzugangsebene in der Regel bei Intranets im lokalen Bereich zur Anwendung kommt und die Überprüfungen der Netzwerk- und Transportebene bei der Kontrolle der Kommunikation über Internet und Intranets Anwendung finden.

Überprüfungen auf der Netzzugangsebene

Auf der Netzzugangsebene sind unterschiedliche Standards zu unterstützen. Im folgenden werden die Möglichkeiten beim Ethernet aufgezeigt /IEEE1/.

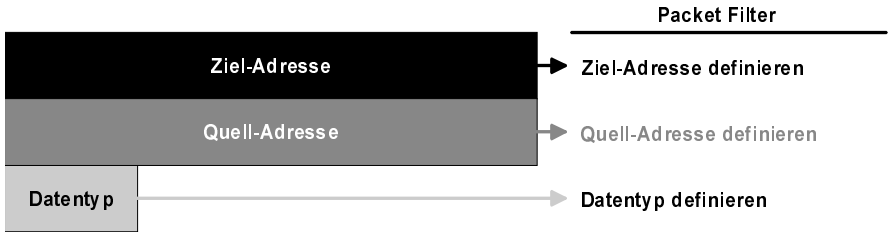

Abb. 12.10: Aufbau des Ethernet MAC-Frame (DIX2)

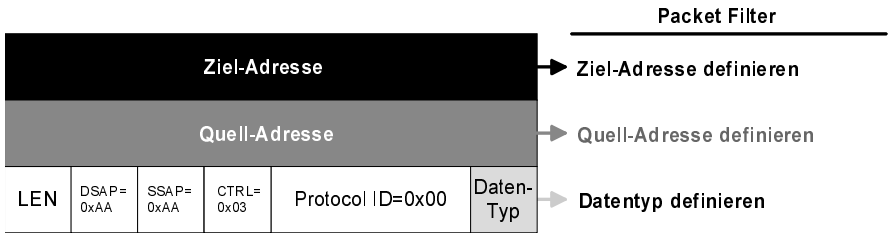

Abb. 12.11: Aufbau des Ethernet MAC Frame (802.3 + 802.2 SNAP)

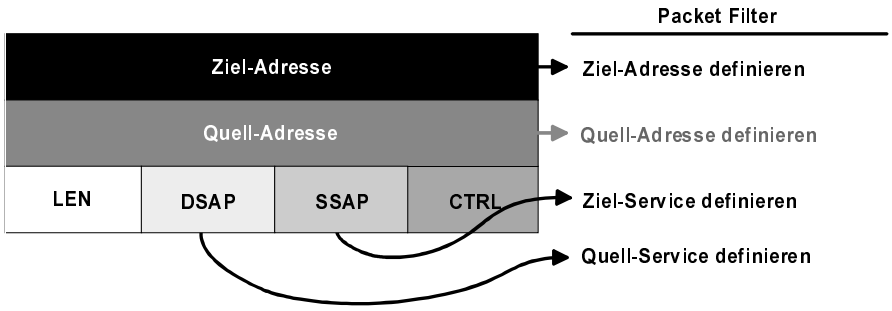

Abb. 12.12: Aufbau des Ethernet MAC Frame (802.3 + 802.2)

Bei Ethernet-Paketen kann der Packet Filter die Ziel- und Quell-Adresse analysieren und im entsprechenden Regelwerk nachsehen, ob die Rechnersysteme, Server und Router, zu denen die Adressen (MAC-Adressen) gehören, eine Kommunikation über den Packet Filter durchführen dürfen oder nicht. Bei Firewall-Systemen kann hier der unmittelbare Kommunikationspartner auf unterster Kommunikationsebene (zum Beispiel Application Gateway, Mail- oder DNS-Server) definiert werden.

Im »Datentyp«-Feld oder DSAP/SSAP-Feld kann festgestellt werden, über welches Kommunikationsprotokoll die Kommunikation auf der nächsthöheren Schicht stattfindet, zum Beispiel IPX, IP, DECNET-Protokolle usw. Die Definitionen für das »Datentyp«-Feld sind in /RFC1700/ festgelegt.

Außerdem wird zum Beispiel bei einer IP-Kommunikation unterbunden, dass mehrere IP-Pakete in einem MAC-Frame enthalten sind. Dabei wird eine Verbindung zwischen der Analyse der Netzzugangs- und Netzwerkebene realisiert. Hier sind in der Vergangenheit Angriffe durchgeführt worden.

Überprüfungen auf der Netzwerkebene

Auf der Netzwerkebene werden im Fall eines IP-Protokolls die Ziel- und Quell-Adresse und das Transport-Protokoll überprüft. Im Fall eines IPX-Protokolls werden Network und Node überprüft.

In Abbildung 12.13 ist dargestellt, welche Möglichkeiten bei IP-Frames (/RFC791/) bestehen, eine Analyse durchzuführen, um die Kommunikation über den Packet Filter zu kontrollieren.

Bei einem IP-Frame werden Ziel- und Quell-Adresse überprüft und festgestellt, ob hier eine Kommunikationsverbindung über den Packet Filter erlaubt ist. Außerdem kann dem »Protokoll«-Feld entnommen werden, welches Transport-Kommunikationsprotokoll verwendet wird. Auch hier kann gegenüber der Rechteliste überprüft werden, ob das entsprechende Transport-Kommunikationsprotokoll (wie TCP oder UDP) verwendet werden darf oder nicht.

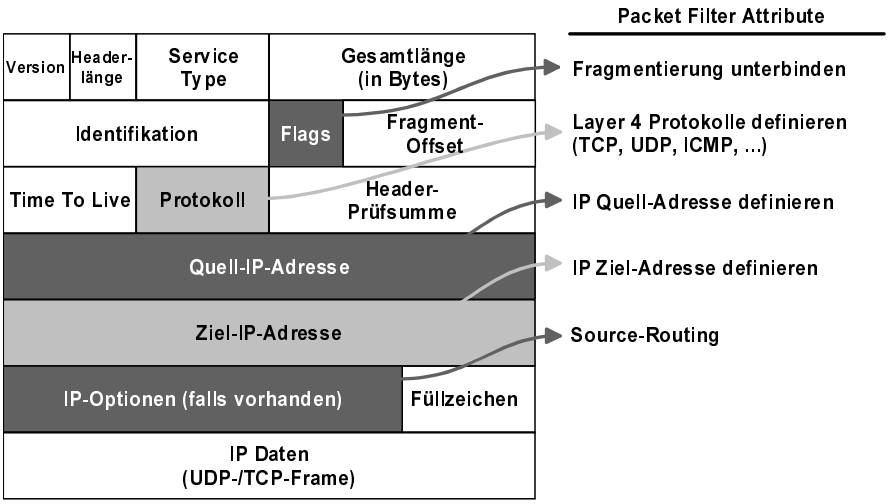

Abb. 12.13: Aufbau des IP-Frame

Dem »Flags«-Feld kann entnommen werden, ob eine Fragmentierung der IP-Pakete durchgeführt wird. Da über Fragmentierungen Angriffe durchgeführt werden können, kann die Fragmentierung über die Festlegung der Rechte unterbunden werden.

Mit Hilfe des »IP-Optionen«-Felds kann festgelegt werden, welche Optionen (Source-Routing etc.) über den Packet Filter verwendet werden dürfen. Hier kann und sollte das Source-Routing unterbunden werden, da über diese Funktion Angriffe durchgeführt werden können.

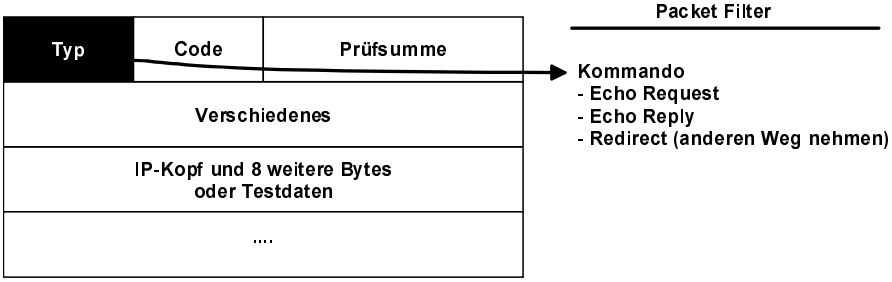

Abb. 12.14: Aufbau des ICMP-Frame

Bei ICMP /RFC792/ kann das »Type«-Feld analysiert werden, in dem die Kommandos definiert sind. Hier können Kommandos wie `EchoRequest`, `EchoReply`, `Redirect`, `Destination Unreachable` etc. erlaubt oder verboten werden. Zum Bei-

spiel werden `EchoRequest` und `EchoReply`, die für den »Ping«-Befehl verwendet werden, erlaubt, aber der Befehl `Redirect`, der für Angriffe benutzt werden kann, verboten. Die Kommandos sind durch RFCs definiert.

Überprüfungen auf der Transportebene

Auf der Transportebene findet im Fall von UDP/TCP (und damit auch indirekt für die TCP/IP-Anwendungen HTTP, FTP, Telnet usw.) eine Überprüfung der Portnummern statt. Im Fall von TCP wird zusätzlich die Richtung des Verbindungsaufbaus überprüft.

- Transportprotokoll – UDP:
  UDP ist ein verbindungsloses Kommunikationsprotokoll, das heißt, die UDP-Pakete werden unabhängig voneinander übertragen. Bei UDP gibt es keine Garantie oder Kontrolle über die korrekte Auslieferung der Pakete. Zwischen dem Aufbau einer neuen UDP-Verbindung oder den Paketen innerhalb einer bestehenden UDP-Verbindung wird nicht unterschieden.

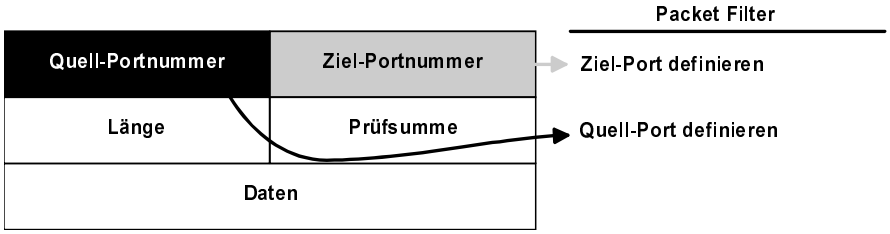

Abb. 12.15: Aufbau des UDP-Frame

Beim UDP-Frame /RFC768/ können durch den Packet Filter Quell- und Ziel-Port analysiert werden. Anhand einer Rechteliste kann bestimmt werden, welche Dienste über UDP gefahren werden können, zum Beispiel SNMP, TFTP usw.

In der Regel sollen UDP-Pakete möglichst nicht zugelassen werden, weil sonst mehr Angriffe realisiert werden können.

- Transportprotokoll – TCP:
  In Abbildung 12.16 ist zu sehen, welche Informationen bei einem TCP-Frame analysiert und kontrolliert werden können.

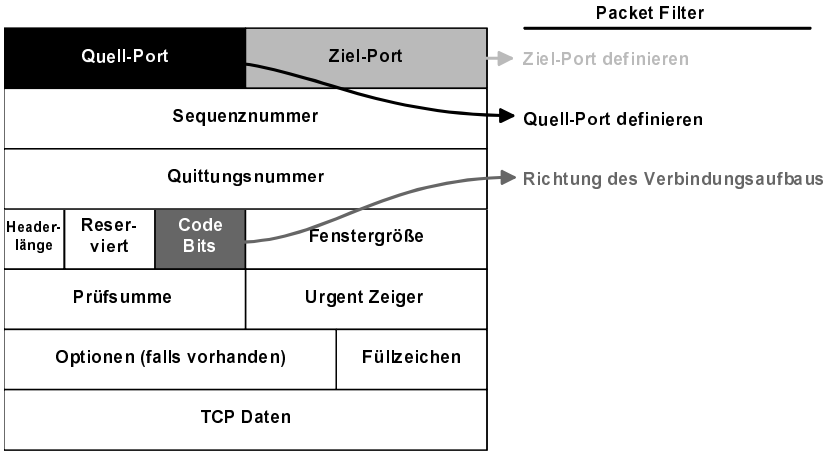

Abb. 12.16: Aufbau des TCP-Frame

Beim TCP-Frame /RFC793/ können durch den Packet Filter wiederum Quell- und Ziel-Port analysiert werden. In einer Rechteliste wird festgelegt, welche Dienste zu welcher Zeit über den Packet Filter erlaubt sind. Außerdem kann dem »Code Bits«-Feld durch die Interpretation des ACK-Bits (acknowledge) entnommen werden, in welche Richtung der Verbindungsaufbau durchgeführt wird. So besteht die Möglichkeit, aus Sicherheitsgründen für den Verbindungsaufbau nur eine bestimmte Richtung zu erlauben (siehe unten das Beispiel für den Einsatz von Packet Filtern).

Überprüfung des Verbindungsaufbaus

TCP ist ein verbindungsorientiertes Kommunikationsprotokoll. Beim Verbindungsaufbau arbeitet TCP immer ohne das ACK-Bit im »Code Bits«-Feld, das heißt ACK=0. Alle weiteren Pakete einer TCP-Verbindung haben dann das ACK-Bit gesetzt, das heißt ACK=1 /ChZw96/. Dadurch sind TCP-basierte Anwendungen besser durch einen Packet Filter zu kontrollieren (siehe Abb. 12.17).

Filterung bei FTP-Verbindungen

Die FTP-Anwendungen /RFC959/ arbeiten mit zwei logischen TCP-Verbindungen: eine für den Austausch der Kommandos, die andere für den Austausch der Daten. Für den Aufbau dieser logischen TCP-Verbindungen gibt es zwei Methoden, die aktive und die passive Methode aus der Sicht des FTP-Clients /ChZw96/.

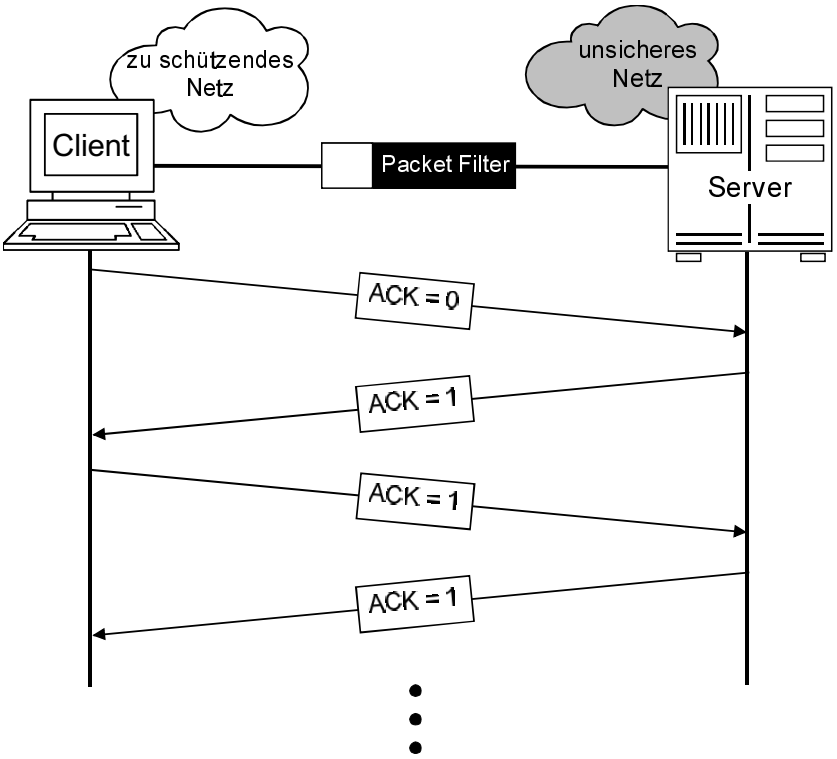

Abb. 12.17: Überprüfung des Verbindungsaufbaus

FTP-Verbindungsaufbau

Bei einem FTP-Verbindungsaufbau nutzt der Client zwei Portnummern oberhalb 1024 (zum Beispiel 4320 und 4321). Über den ersten Port (zum Beispiel 4320) baut er die TCP-Verbindung für die Kommandos auf. Der Server empfängt die Kommandos über den definierten Port 21.

Im folgenden werden die beiden Methoden beschrieben, wie der Datenkanal bei der FTP-Anwendung von den Rechnersystemen aufgebaut werden kann.

- Aktive Methode
  Mit dem Kommando »PORT 4321« teilt der Client dem Server mit, über welche Portnummer er die Daten abwickeln möchte. Der Server sendet die Daten von seinem definierten Port 20 auf die Portnummmer 4321 des Clients.

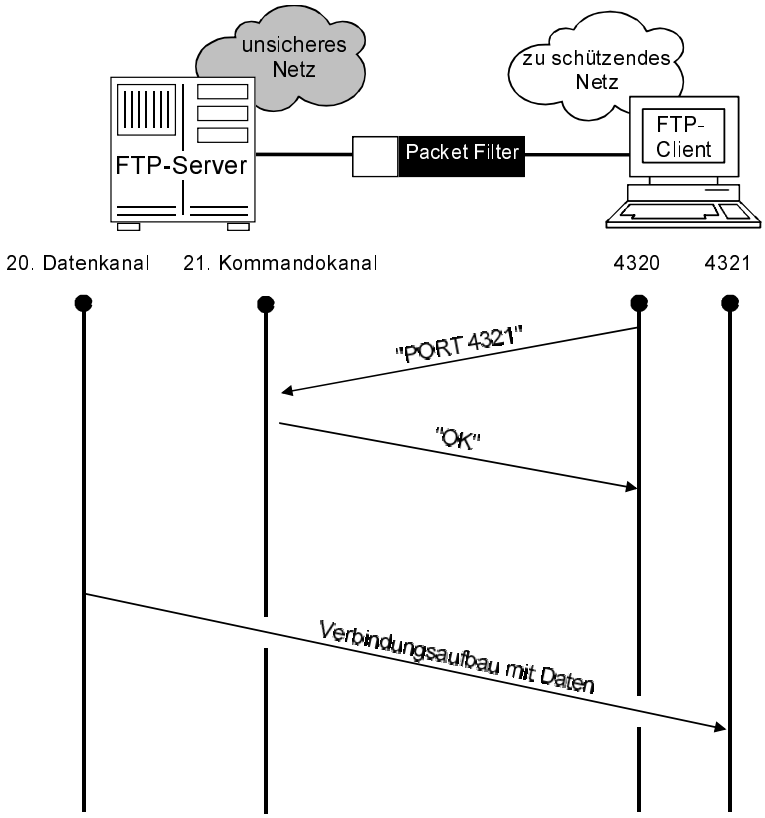

Abb. 12.18: Aktive Methode

Ein Packet Filter, der diese Verbindungen kontrollieren soll, muss für die TCP-Verbindung einen Verbindungsaufbau aus dem unsicheren Netz in das zu schützende Netz ermöglichen. Da dies sicherheitskritisch ist, sollte diese Methode, wenn möglich, nicht verwendet werden. Aus diesem Grund ist es empfehlenswert, die Methode des passiven FTP-Verbindungsaufbaus zu verwenden, bei der der Client den Verbindungsaufbau durchführt.

- Passive Methode
  Bei der passiven Methode baut der Client die TCP-Verbindung auf. Hierdurch kann mit Hilfe eines Packet Filter eine größere Sicherheit erreicht werden. In Abbildung 12.19 ist die passive Methode dargestellt.

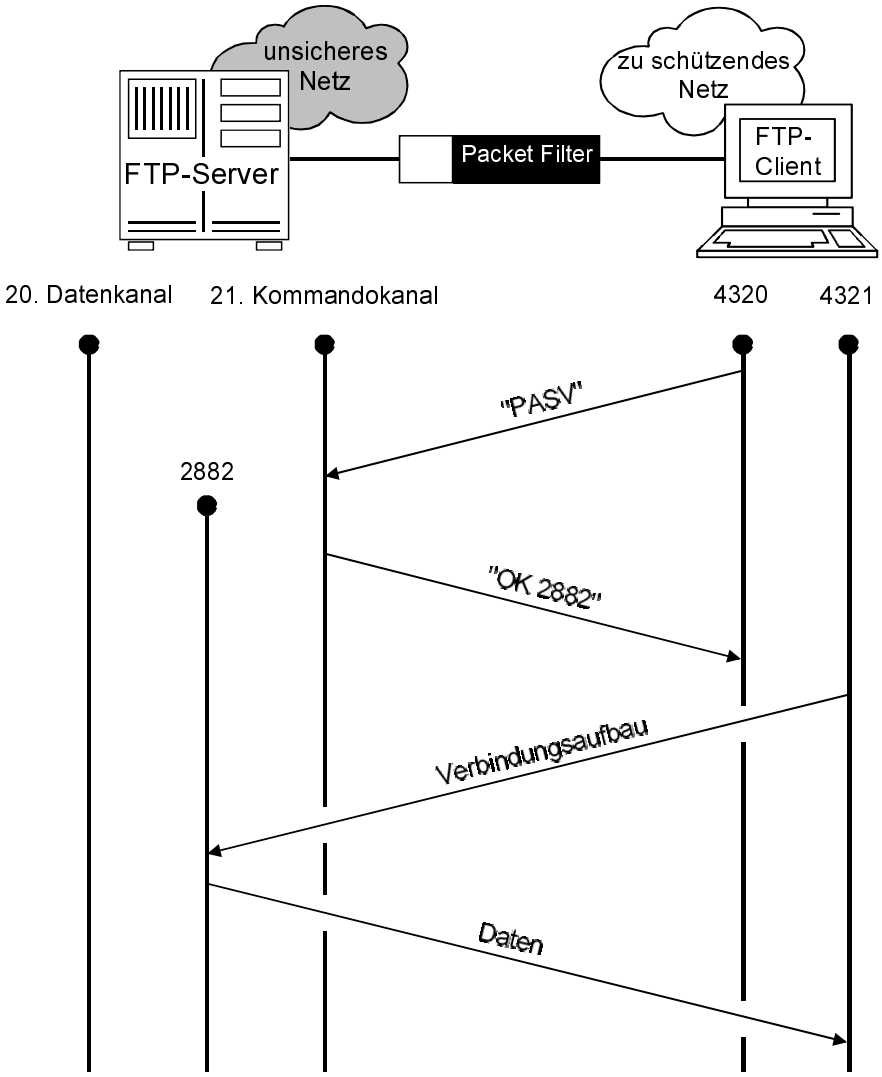

Abb. 12.19: Passive Methode

Aus Sicherheitsgründen ist die passive Methode zu bevorzugen. Dabei ist zu bedenken, dass diese nicht von allen Client- und Server-Realisierungen angeboten wird.

Weitere mögliche Festlegungen:

Zusätzlich sollte in den Packet Filtern pro Filterregel festgelegt werden, zu welchen Zeiten eine Regel (zum Beispiel die Nutzung eines Dienstes) möglich ist, beispielsweise montags bis freitags von 8.00-17.00 Uhr oder samstags von 8.00-12.00 Uhr und sonntags gar nicht.

Strategien für den Aufbau und die Bewertung der Filterregeln

Es gibt unterschiedliche Ansätze, nach denen die Strategie für den Aufbau und die Bewertung von Filterregeln bestimmt werden kann. Im Folgenden sollen zwei Strategien vorgestellt werden.

- Festlegung positiver Filterregeln:
  - Bei dieser Strategie muss genau festgelegt werden, was erlaubt sein soll.
  - Alles, was nicht explizit erlaubt wird, ist automatisch verboten.
  - Das Firewall-Element erlaubt nur das, was explizit in der Access-Liste als »erlaubt« gekennzeichnet ist.
- Festlegung negativer Filterregeln:
  - Zunächst ist alles grundsätzlich erlaubt.
  - Durch spezielle Einträge kann festgelegt werden, was verboten sein soll.
  - Der Packet Filter verhindert nur das, was explizit in der Access-Liste als »nicht erlaubt« gekennzeichnet ist.
- Bewertung:
  Positive Filter sind zu bevorzugen, weil hier nicht durch Unbedachtsamkeit ein Eintrag (Verbot) vergessen werden und dadurch ein Sicherheitsproblem entstehen kann. Negative Filter sind mit Vorsicht zu behandeln, weil durch ungeschickte Festlegungen oder das Vergessen von Einträgen sicherheitskritische Einstellungen auftreten können.

Dynamischer Packet Filter

Im folgenden Abschnitt wird die Arbeitsweise von dynamischen Packet Filtern beschrieben /Bo0l96/. Bei verbindungslosen Kommunikationsverbindungen, wie zum Beispiel UDP, kann nicht festgestellt werden, von wem ein Verbindungsaufbau durchgeführt wird. Dynamische Packet Filter besitzen im Fall der Verwendung des UDP-Protokolls ferner die Eigenschaft, sich für nach »außen« geschickte UDP-Pakete die Quell- und Ziel- IP-Adressen und Ports zu merken, und nur die entsprechenden passenden »Antworten« der virtuellen Verbindung zu erlauben. Das bedeutet, dass nur Antwortpakete durchgelassen werden, die vom gleichen Rechnersystem und dem gleichen Port kommen, an die das ursprüngliche UDP-Paket gesendet worden ist, und die entsprechend zum gleichen Rechnersystem und gleichen Port zurückgesendet werden. Packet Filter, die diese Eigenschaft besitzen, werden als »dynamisch« bezeichnet, weil die Filterregeln intern dynamisch ange-

passt werden. Die angepassten Regeln für die Antwort gelten nur temporär und werden nach einer zu definierenden Zeit, falls keine Antwort kommt, automatisch durch den dynamischen Packet Filter selbst gelöscht.

Der Abbildung 12.20 ist zu entnehmen, welche Informationen (Quelladresse und -port, Zieladresse und -port sowie die Zeit, wann das Paket übertragen wurde) im dynamischen Packet Filter festgehalten werden, damit eine genaue Zuordnung stattfinden kann. Diese Eigenschaft kann auch für TCP-Verbindungen verwendet werden /ChZw96/.

Dienste wie SNMP können über Packet Filter, die diese Eigenschaft besitzen, sicherer angeboten werden.

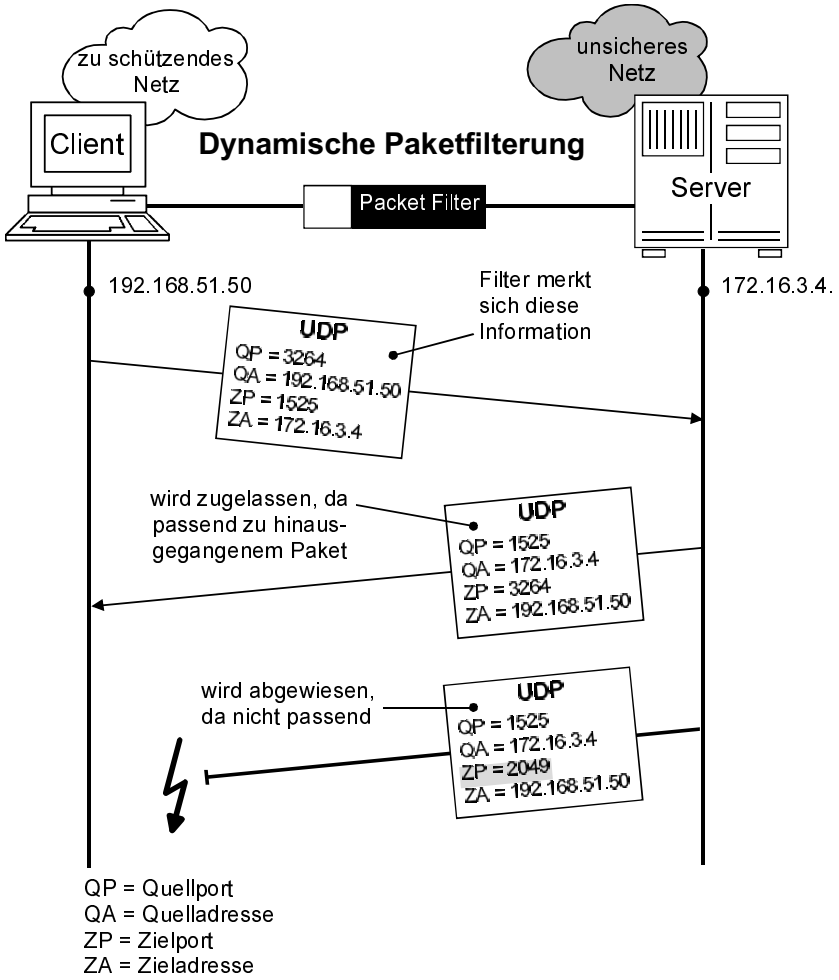

Abb. 12.20: Dynamischer Packet Filter

Anwendungsgebiete von Packet Filtern

Ein Firewall-System, das nur auf Packet Filtern aufbaut, wird sicherlich nicht für die Kopplung eines zu schützenden Netzes an das Internet eingesetzt werden können, da der Schutzbedarf der meisten zu schützenden Netze für die Kontrollmöglichkeiten eines Packet Filter zu hoch ist.

Packet Filter werden zum Aufbau von High-level Security Firewall-Systemen und für die kontrollierte Kommunikation im Intranet verwendet. Für diese Anwendungen ist besonders die Verwendung von Packet Filtern, die gleichzeitig verschlüsseln, eine wirkungsvolle Sicherheitskomponente, mit der Internet- und Intranet-Anwendungen sicher und beherrschbar realisiert werden können.

Möglichkeiten, Vorteile und besondere Aspekte von Packet Filtern

- transparent, das heißt unsichtbar für den Benutzer und die Rechnersysteme und ohne ihre aktive Einwirkung tätig (Ausnahme: wenn eine Authentikation notwendig ist)
- einfach erweiterungsfähig für neue Protokolle
- flexibel für neue Dienste
- für andere Protokollfamilien verwendbar (IPX, OSI, DECNET, SNA, ...)
- hohe Performance durch optimale Mechanismen (Betriebssystem, Treiber usw.)
- leicht realisierbar, da geringere Komplexität

Nachteile und Grenzen von Packet Filtern

- Daten, die oberhalb der Transportebene liegen, werden in der Regel nicht analysiert.
- Für die Anwendungen (FTP, HTTP, ...) besteht keine Sicherheit; so können bei der Freischaltung von SMTP (Port 25) Angriffe über Sendmail auf die Rechnersysteme des zu schützenden Netzes durchgeführt werden.
- Falsch konfigurierte Programme auf Rechnersystemen im zu schützenden Netz können bei erlaubten Kommunikationsverbindungen von außen genutzt werden, da ein direkter Zugriff auf das Rechnersystem besteht.
- Typische Packet Filter können die Struktur des zu schützenden Netzes nicht verbergen.
- Protokolldaten werden nur bis zur Transportebene zur Verfügung gestellt.

12.4.2 Zustandsorientierte Packet Filter (stateful inspection)

Der Leistungsumfang von Packet Filtern kann erweitert werden, indem die Interpretation der Pakete auch auf höheren Kommunikationsebenen durchgeführt wird. In diesem Fall werden die Pakete zum Beispiel auch auf der Anwendungsebene interpretiert und Statusinformationen für jede aktuelle Verbindung auf den unterschiedlichen Kommunikationsebenen bewertet und festgehalten.

Analogie zum Pförtner:

Wenn eine Lieferung ankommt, dann schaut der Pförtner nicht nur auf die Adressen, sondern auch auf den Lieferschein, um zu überprüfen, ob in dem Paket etwas Verbotenes steckt. Das ist eine gute Überprüfung, jedoch nicht so sicher wie das tatsächliche Öffnen des Pakets und die Überprüfung des Inhalts. Wenn das Paket akzeptabel aussieht, dann öffnet der Pförtner das Tor und gestattet dem Fahrer des LKW die Zufahrt auf das Werksgelände.

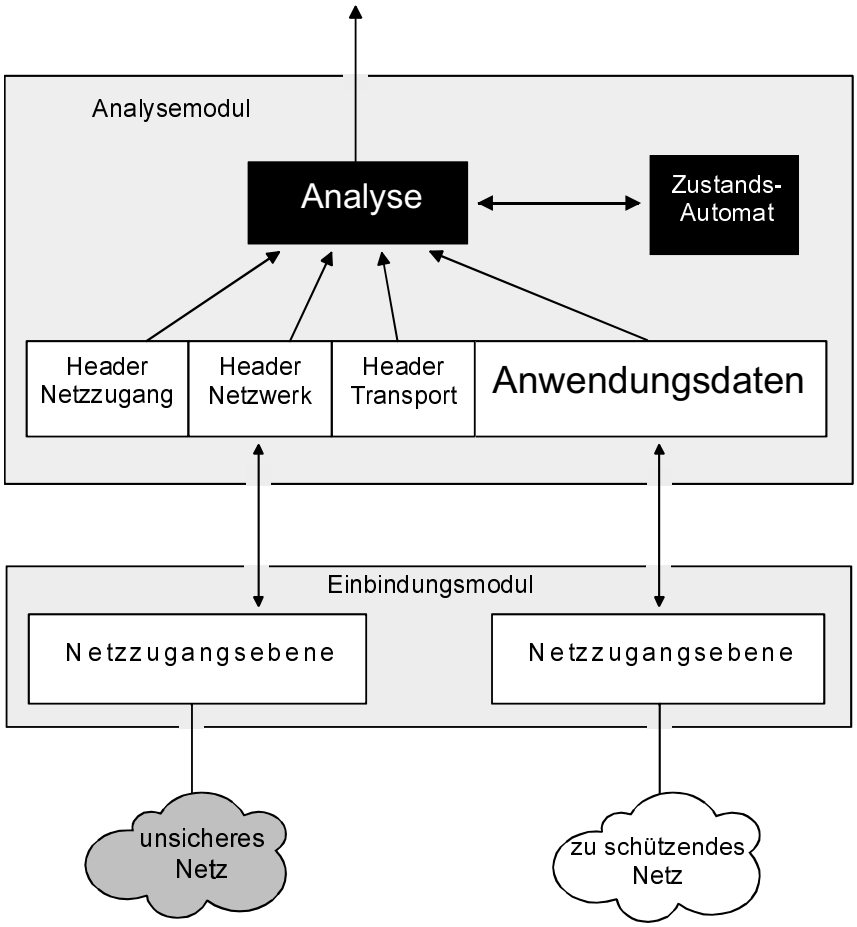

Abb. 12.21: Zustandsorientierte Packet Filter

Die Statusinformationen können in Form von »Zuständen« mit den entsprechenden Informationen festgehalten werden. Zustände sind zum Beispiel Verbindungsaufbau, Transferzustand oder Verbindungsabbau für die jeweilige Kommunikationsebene. In jedem Zustand kann dann eine spezielle Interpretation der

Kommunikationsdaten erfolgen. In der Literatur werden solche erweiterten zustandsorientierten Packet Filter »stateful inspection«, »smart filtering« oder »adaptive screening« genannt. Mit dieser erweiterten Funktionalität werden sie oft als benutzerorientierte Packet Filter angeboten.

Diese zustandsorientierten Packet Filter haben die Vorteile von Packet Filtern, können aber zusätzlich die Anwendungen kontrollieren. Einige Risiken bleiben, weil keine direkte Entkopplung der Dienste realisiert ist (siehe die Beschreibung der Proxies auf Application Gateways und ihrer Vorteile).

Das gleichzeitige Festhalten und Interpretieren der Kommunikationsdaten auf den verschiedenen Kommunikationsebenen ist sehr komplex. Aus diesem Grund haben zustandsorientierte Packet Filter in der Regel eine geringere Tiefe der Analyse oder sind besonders fehleranfällig, da sie eine sehr mächtige Software haben. Prinzipiell ist es auch nicht möglich, die komplexe Software von zustandsorientierten Packet Filtern soweit auszutesten, dass nachweislich in keinem Betriebszustand Fehler auftreten können. Aus diesem Grund muss auch in Zukunft immer wieder damit gerechnet werden, dass die komplexen Programme potentielle Sicherheitsrisiken aufweisen, die für Angriffe verwendet werden können / Kupp99/.

Möglichkeiten, Vorteile und besondere Aspekte von zustandsorientierten Packet Filtern

- Zustandsorientierte Packet Filter arbeiten transparent, das heißt unsichtbar für den Benutzer und die Rechnersysteme und ohne ihre aktive Einwirkung (Ausnahme: wenn eine Authentikation notwendig ist).
- Sie sind einfach erweiterungsfähig für neue Protokolle und flexibel für neue Dienste.
- Eventuell sind sie auch für andere Protokollfamilien verwendbar (IPX, OSI, DECNET, SNA...).

Nachteile und Grenzen von zustandsorientierten Packet Filtern

- Zustandsorientierte Packet Filter stellen eine komplexe Lösung dar.
- Falsch konfigurierte und fehlerbehaftete Programme auf Rechnersystemen im zu schützenden Netz können bei erlaubten Kommunikationsverbindungen von außen genutzt werden, da ein direkter Zugriff auf das Rechnersystem besteht.
- Typische zustandsorientierte Packet Filter können die Struktur des zu schützenden Netzes nicht verbergen.

Ein besseres und sicheres Konzept der Analyse der Anwendungsdaten ist das Konzept von Application Gateways mit Proxies, das im folgenden Abschnitt beschrieben wird.

12.4.3 Application Gateway / Proxy-Technik

Im Folgenden wird die Arbeitsweise des aktiven Firewall-Elements »Application Gateway« beschrieben. Es zeichnet sich dadurch aus, dass es die Netze sowohl logisch als auch physikalisch entkoppeln kann.

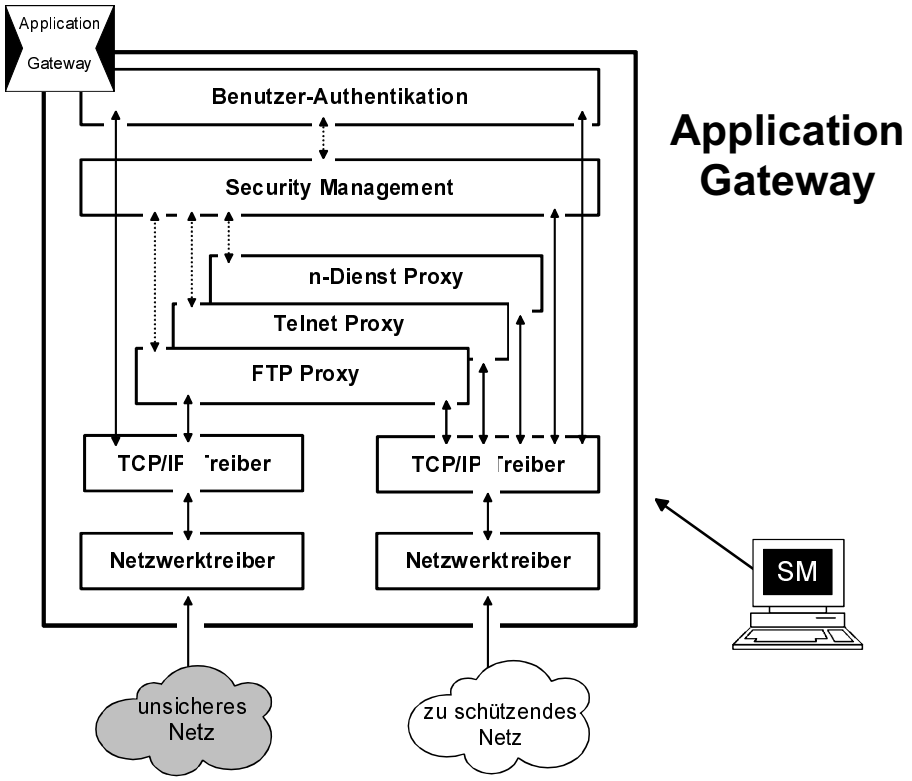

Abb. 12.22: Application Gateway

Da in einigen Firewall-Konzepten das Application Gateway das einzige vom unsicheren Netz (zum Beispiel Internet) aus erreichbare Rechnersystem ist, muss das Application Gateway besonders geschützt werden. Aus diesem Grund wird das Rechnersystem, auf dem das Application Gateway realisiert ist, auch als Bastion bezeichnet.

Das Application Gateway – als Dual-homed Gateway realisiert – arbeitet mit zwei Netzwerk-Anschlüssen. »Dual-homed« bedeutet, daß das Application Gateway die vollständige Kontrolle über die Pakete hat, die zwischen dem unsicheren und dem

zu schützenden Netzwerk übertragen werden sollen. Das Dual-homed Application Gateway besitzt zwei Netzwerkkarten, eine im zu schützenden Netz, eine weitere im unsicheren Netzwerk /SiHa95/.

Das Application Gateway kann auch »Single-homed« mit nur einem Netzwerkanschluss betrieben werden. Dann besteht jedoch die Möglichkeit, daß ein Angreifer das Application Gateway übergeht.

Analogie zum Pförtner:

Der »Application-Gateway-Pförtner« schaut nicht nur die Adressen der eingehenden Lieferungen an, er öffnet auch jedes Paket, prüft den kompletten Inhalt und checkt die Arbeitspapiere des Absenders gegen eine klar festgelegte Reihe von Beurteilungskriterien. Nach der erfolgten detaillierten Sicherheitsüberprüfung unterzeichnet der Pförtner den Lieferschein und schickt den LKW wieder auf seinen Weg. Statt dessen bestellt er einen vertrauenswürdigen Fahrer der eigenen Firma, der nun die Pakete zum eigentlichen Empfänger bringt. Die Sicherheitskontrolle ist an dieser Stelle wesentlich zuverlässiger und der Fahrer der Fremdfirma erhält keinen weiteren Einblick in das Firmengelände. Die Überprüfungen nehmen zwar mehr Zeit in Anspruch, dafür können jedoch sicherheitsgefährdende Aktivitäten ausgeschlossen werden.

Allgemeine Arbeitsweise des Application Gateway

Ein Benutzer, der über das Application Gateway kommunizieren möchte, muss sich zuerst identifizieren und authentisieren. Application Gateways bieten in der Regel unterschiedliche Authentikationsverfahren an.

Aus diesem Grund baut der Benutzer zuerst eine Verbindung mit dem Application Gateway auf. Sein direkter Kommunikationspartner ist nicht das Ziel-Rechnersystem, sondern das Application Gateway. Nach der Identifikation und Authentikation arbeitet das Application Gateway aber transparent, so dass der Benutzer den Eindruck hat, direkt auf dem Ziel-Rechnersystem zu arbeiten.

Ansatz

Über die Netzzugangs- und TCP/IP-Treiber empfängt das Application Gateway die Pakete an den entsprechenden Ports. Soll nur ein Dienst über einen entsprechenden Port möglich sein, muss auf dem Application Gateway eine Software zur Verfügung gestellt werden, die das entsprechende Paket von der einen Netzwerkseite zur anderen Netzwerkseite des Application Gateway überträgt und umgekehrt. Eine solche Software, die die Paketübertragung nur für einen speziellen Dienst (FTP, HTTP, Telnet, usw.) im Application Gateway durchführt, wird als Proxy bezeichnet (siehe Abb. 12.22).

Der Name »Proxy« (=Stellvertreter) wird verwendet, weil es aus Sicht des zugreifenden Benutzers so aussieht, als würde er mit dem eigentlichen Serverprozess des Dienstes auf dem Ziel-Rechnersystem kommunizieren.

Jeder Proxy auf dem Application Gateway kann speziell für den Dienst, für den er zuständig ist, weitere Sicherheitsdienste anbieten. Bedingt durch den jeweiligen speziellen Proxy und das Wissen um den Kontext eines speziellen Dienstes ergeben sich umfangreichere Sicherungs- und Protokollierungsmöglichkeiten im Application Gateway (siehe dazu die Beschreibungen der speziellen Proxies).

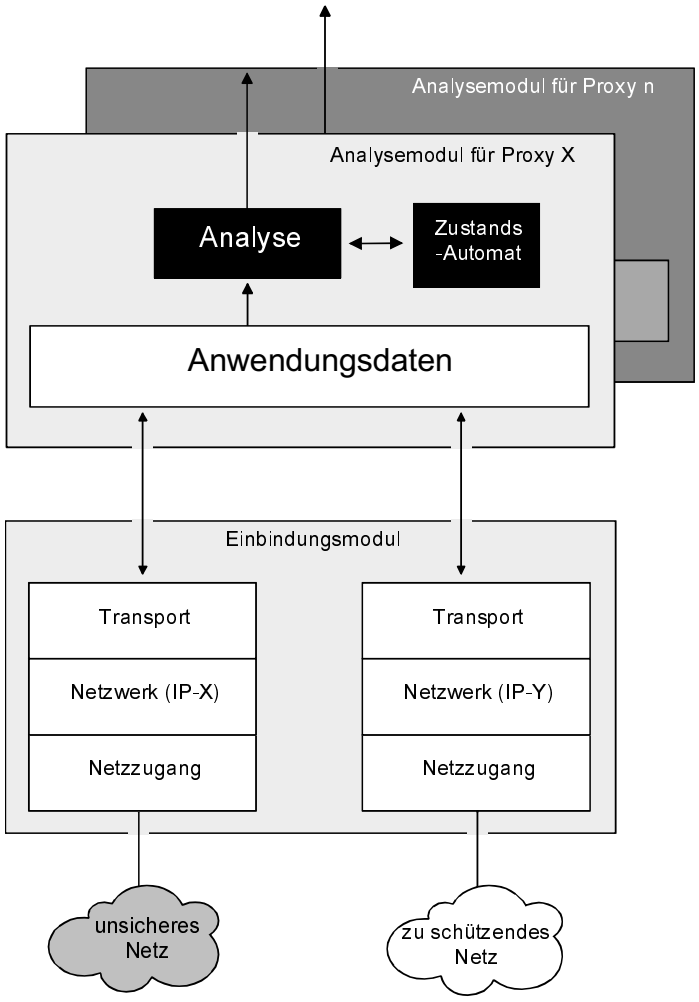

Abb. 12.23: Analysemodule für Proxies auf dem Application Gateway

Die Analyse ist auf dieser Kommunikationsebene besonders intensiv möglich, da der Kontext der Anwendungsdaten für den jeweiligen Dienst klar definiert ist. Die Proxies konzentrieren sich auf das Wesentliche. Der Vorteil ist, dass kleine, überschaubare Module verwendet werden, wodurch die Fehleranfälligkeit durch Implementierungsfehler reduziert wird (siehe Abb. 12.23).

Eventuell wird im Proxy auch eine Umverschlüsselung oder Umcodierung durchgeführt.

Sicherheitskonzept eines Application Gateway:

Für jeden Dienst, der über das Application Gateway möglich sein soll, muss ein spezieller Proxy zur Verfügung gestellt werden.

Sollen bestimmte Dienste generell nicht möglich sein, dann darf für diese Dienste kein Proxy auf dem Application Gateway vorhanden sein, aber auch keine weitere Software, die den Dienst ermöglichen könnte!

Aus diesem Grund ist so wenig Software wie möglich auf dem Application Gateway zu installieren, damit nicht zufällig – oder absichtlich durch einen Angreifer von außen provoziert – eine andere Software die Aufgabe eines Proxy (Paketübertragung im Application Gateway) für einen Dienst übernimmt, der nicht erlaubt sein soll.

Das Sicherheitsmanagement, das dem Benutzer die Arbeit so leicht wie möglich gestalten soll und deshalb mit einer mächtigen Software (X-Terminal, Datenbank etc.) ausgestattet ist, darf aus Sicherheitsgründen nicht auf dem selben Rechnersystem oder zumindest nicht zur gleichen Zeit wie das Application Gateway laufen.

Application Gateways sollen aus Sicherheitsgründen keine Routing-Funktionalität haben, damit nicht an den Proxies vorbeigeroutet werden kann /Stol98/.

Da das Application Gateway bei der Kommunikation jeweils zum Rechnersystem des unsicheren Netzes und zu dem des zu schützenden Netzes eine Kommunikationsverbindung hat, bietet es eine »Network Address Translation«. Dazu hat das Application Gateway eine IP-Adresse im unsicheren Netz (zum Beispiel eine offizielle Internet-IP-Adresse 194.173.3.1) und eine IP-Adresse im zu schützenden Netz (zum Beispiel eine für diesen Zweck reservierte IP-Adresse 192.168.1.60). Bei der Kommunikation mit den Rechnersystemen des unsicheren Netzes verwendet das Application Gateway die IP-Adressen des unsicheren Netzes, bei der Kommunikation mit den Rechnersystemen des zu schützenden Netzes die IP-Adressen des zu schützenden Netzes.

In den Logbüchern des Application Gateway können eine Vielzahl von Informationen festgehalten werden. Schon in der Sicherheitspolitik einer Organisation sollte festgelegt werden, welche Informationen protokolliert werden sollen und welche nicht, da die Datenmenge sonst sehr groß werden kann und einen hohen administrativen Aufwand verursacht.

12.4.4 Proxies

Bei der Realisierung von Proxies wird zwischen Application Level Proxies und Circuit Level Proxies unterschieden.

Außerdem gibt es weitere spezielle Proxies, die für bestimmte Applikationen wiederum zusätzliche, auf diese Dienste zugeschnittene Sicherheitsdienste zur Verfügung stellen. Es können auch für nicht-standardisierte Dienste Proxies realisiert werden.

Application Level Proxies

Application Level Proxies sind für bestimmte Dienste/Anwendungen implementiert. Das heißt, dass sie die Kommandos der Anwendungsprotokolle kennen und diese analysieren und kontrollieren können. Application-Level Proxies arbeiten mit der gängigen, unveränderten Client-Software für FTP oder Telnet oder auch mit Browsern zusammen. Bei Application Level Proxies ist aber für die benutzerorientierten Dienste oft eine veränderte Vorgehensweise notwendig, zum Beispiel ist zuerst eine Identifikation und Authentikation mit dem Application Level Proxy notwendig und anschließend wird dem Benutzer eine transparente Kommunikation zur Verfügung gestellt (siehe hierzu auch die Kommunikation über Application Level Proxies).

Im Folgenden werden einige Application Level Proxies am Beispiel bestimmter Realisierungsarten näher beschrieben, um das Grundprinzip der Proxy-Technik darzustellen. Einige Proxies funktionieren nach dem Store-and-Forward-Prinzip (SMTP), andere interaktiv und benutzerorientiert (Telnet, FTP, HTTP, ...).

SMTP Proxy

Abbildung 12.24 zeigt, wie ein SMTP Proxy, der nach dem Store-and-Forward-Prinzip arbeitet, aufgebaut werden kann. Store-and-Forward-Prinzip bedeutet, dass der MTP Proxy die Mail vollständig annimmt, zwischenspeichert und dann weitersendet. Hierfür ist keine End-to-End-Beziehung zwischen dem eigentlichen Sender und Empfänger notwendig.

Analogie zum Sammelbriefkasten (Mail Proxy):

Ein Mail Proxy kann mit einem Sammelbriefkasten einer Organisation verglichen werden. Möchte jemand einer Organisation einen Brief senden, so wirft er diesen direkt oder indirekt in den Sammelbriefkasten der Organisation. Die Briefe wer-

den dort von der internen Poststelle entgegengenommen und mit einem Boten der eigenen Organisation verteilt. Die externen Briefboten brauchen die Organisation also nicht zu betreten und stellen somit auch kein Risiko dar. Der Schlitz nach außen definiert die potenzielle Angriffsfläche.

Bei SMTP Proxies gibt es Lösungen, die ohne oder mit einem auf dem gleichen System vorhandenen MTA (Message Transfer Agent) arbeiten. In diesem Beispiel wird ein SMTP Proxy mit vorhandenem MTA beschrieben.

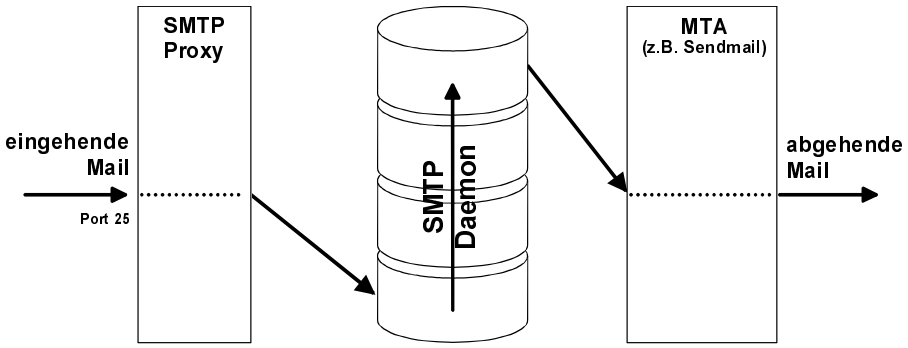

Abb. 12.24: SMTP Proxy

Beschreibung:

Der SMTP Proxy arbeitet nicht benutzerorientiert. Aus diesem Grund ist hier auch keine Benutzerauthentikation erforderlich.

Eine eingehende Mail wird von einem SMTP Proxy auf Port 25 entgegengenommen und nach Überprüfung des Absenders (IP-Adresse und Rechnername des Mail-Servers) auf dem Application Gateway in einem speziellen Verzeichnis abgelegt. Der SMTP Daemon prüft periodisch, ob Mails eingegangen sind. Das Mail Transfer Agent (MTA) stellt dem Adressaten die Mail direkt oder über einen oder mehrere MTAs zu. Der SMTP Proxy verhindert damit, dass der MTA direkt vom unsicheren Netz angesprochen werden kann.

Ein solches MTA ist zum Beispiel »Sendmail«, das häufig eingesetzt wird und das bekanntlich eine Vielzahl von Sicherheitslücken und Implementierungsfehlern aufweist.

Ein SMTP Proxy verarbeitet nur die folgenden Befehle, die nicht sicherheitskritisch sind: `helo, mail, rcpt, data, quit, rset, noop.`

Einige weitere Befehle werden mit Standardantworten bedient, damit eine Kommunikation ermöglicht werden kann: `help, vref, expn.`

Bei sicherheitsrelevanten Befehlen wie debug wird eventuell direkt eine Spontane Meldung an das Sicherheitsmanagement gesendet.

Falls der Befehl debug in einem SMTP-Proxy erkannt wird, kann dadurch kein Fehler auftreten, weil der SMTP-Proxy darauf nicht reagiert. Wenn aber ein Fremder versucht, diesen Befehl auszuführen, kann die Tatsache dahingehend interpretiert werden, dass sich dahinter ein Angriffsversuch verbirgt. Diese Information über einen Angriffsversuch kann wichtig sein.

Durch die Verwendung des Store-and-Forward-Prinzips wird zum Beispiel eine Entkopplung des komplexen und fehlerbehafteten Programms Sendmail (MTA) erreicht. So werden bekannte Angriffe über Sendmail verhindert, denn mit Hilfe der Befehle kann Sendmail nicht direkt angesprochen werden, sondern nur die Stellvertreter-Software der SMTP Proxies. Der SMTP Proxy ist überschaubar und damit gut testbar Software.

Logbuch:

Durch den SMTP Proxy können im Logbuch des Application Gateway die folgenden Protokolldaten festgehalten werden:

- IP-Adresse und Rechnername des Quell-Rechnersystems
- Uhrzeit und Datum des Verbindungsaufbaus
- Absender der Mail (wie im Kopf der Mail angegeben)
- Adressat der Mail (wie im Kopf der Mail angegeben)
- Anzahl der übertragenen Bytes
- Uhrzeit und Datum des Verbindungsabbaus

Durch den Message Transfer Agent (MTA) werden im Logbuch des Application Gateway die folgenden Protokolldaten festgehalten:

- IP-Adresse und Rechnername des Ziel-Rechnersystems
- Uhrzeit und Datum des Verbindungsaufbaus
- Absender der Mail (wie im Kopf der Mail angegeben)
- Adressat der Mail (wie im Kopf der Mail angegeben)
- Anzahl der übertragenen Bytes
- Uhrzeit und Datum des Verbindungsabbaus

Wenn ein Problem auftritt, können die umfangreichen Protokolldaten der Ereignisse im SMTP Proxy verwendet werden, um es zu lösen.

Benutzerorientierte Application Level Proxies

Die folgenden Proxies für Telnet, FTP und HTTP sind benutzerorientierte Proxies, die – ähnlich wie ein Pförtner – selbst eine Authentikation mit dem entsprechenden Benutzer durchführen. Im Falle einer erfolgreichen Identifikation und Authentikation eines Benutzers mit dem Proxy gilt diese Authentikation auch nur für diesen speziellen Proxy. Falls der Benutzer einen anderen Dienst, das heißt

einen anderen Proxy, nutzen möchte, muss eine erneute Identifikation und Authentikation stattfinden. Benutzerorientierte Proxies haben den Vorteil, dass die Zuordnung zwischen Benutzer und IP-Adresse und dem gewünschten Dienst eindeutig und lückenlos ist.

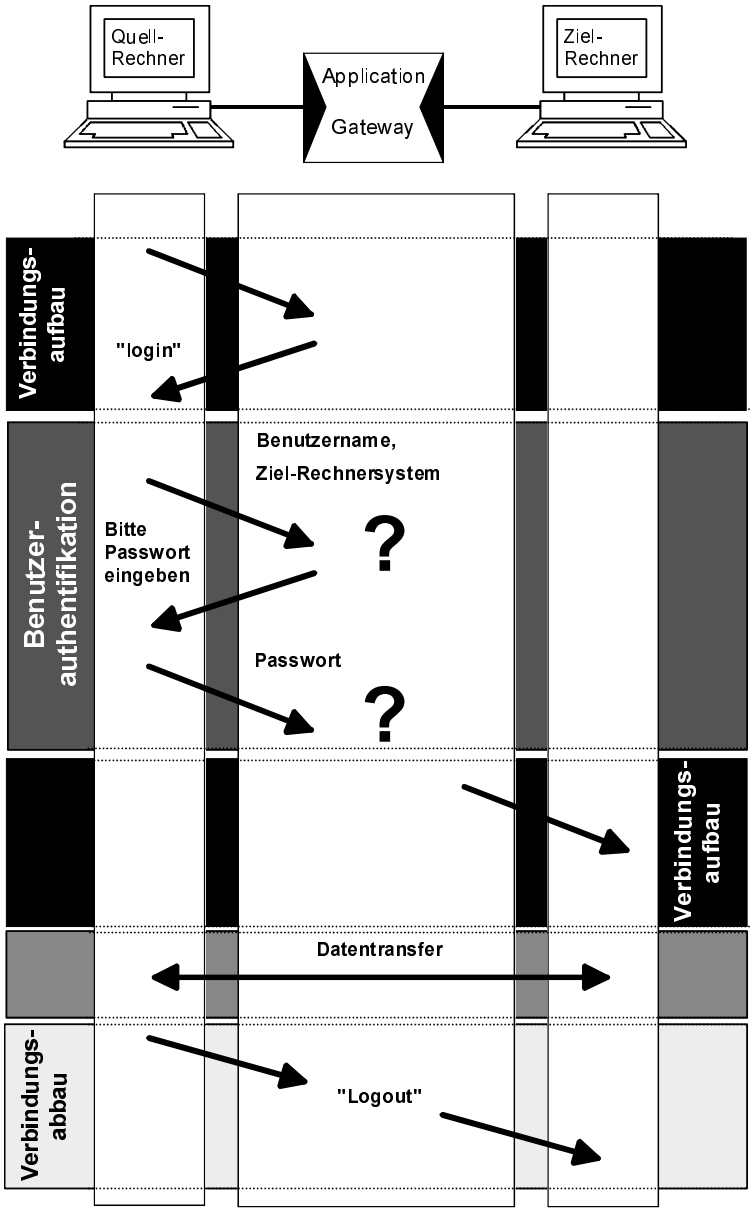

Abb. 12.25: Kommunikation über einen Application Level Proxy

Im Folgenden wird der Verbindungsaufbau über das Applikation Gateway mit Hilfe eines einfachen Passwortverfahrens für benutzerorientierte Dienste exemplarisch dargestellt.

- **1. Phase: Verbindungsaufbau zum Application Gateway**
  Der Benutzer versucht, über das Application Gateway eine Verbindung von seinem Quell-Rechnersystem zu einem gewünschten Ziel-Rechnersystem aufzubauen. Das Application Gateway nimmt den Verbindungsaufbau an und fordert den Zugreifenden auf, eine Identifikation und Authentikation durchzuführen.

- **2. Phase: Benutzerauthentikation**
  Der Zugreifende gibt seine Benutzer-Identifikation und sein Ziel-Rechnersystem an. Auf dem Application Gateway wird überprüft, ob der Benutzer von seinem Quell-Rechnersystem auf das angestrebte Ziel-Rechnersystem zugreifen darf und welche Restriktionen für den Zugriff bestehen. Anschließend wird der Benutzer in diesem Beispiel aufgefordert, sein Passwort einzugeben. Auf dem Application Gateway wird dann überprüft, ob der Benutzer das richtige Passwort eingegeben hat (wie beim Pförtner).

  Die Authentikation bei Firewall-Systemen kann in der Regel unterschiedlich realisiert werden, zum Beispiel durch Passwortverfahren, Einmal-Passwortverfahren oder Challenge-Response-Verfahren. Die Authentikationsverfahren, die mit Hilfe von kryptographischen Algorithmen arbeiten, nutzen für den Benutzer Security Tokens, Chipkarten usw. Welches Authentikationsverfahren verwendet wird, hängt in der Regel vom Schutzbedarf und der Richtung der Kommunikation über das Firewall-System ab. Von einem zu schützenden Netz in ein unsicheres Netz kann die Kommunikation über das Firewall-System mit einem einfachen oder sogar ohne ein Authentikationsverfahren realisiert werden. Bei der Kommunikation von einem unsicheren Netz in ein zu schützendes Netz sollte immer ein kryptographisches Verfahren (zum Beispiel mit Security Token oder Chipkarte) verwendet werden.

- **3. Phase: Verbindungsaufbau zum Ziel-Rechnersystem**
  Wenn sich der zugreifende Benutzer erfolgreich identifizieren und authentisieren konnte, wird durch den Proxy auf dem Application Gateway eine zweite Verbindung vom Application Gateway zum gewünschten und erlaubten Ziel-Rechnersystem aufgebaut.

- **4. Phase: Datentransfer**
  Dann findet der Datentransfer statt. Abhängig vom jeweiligen Proxy wird der Datentransfer über den Proxy auf dem Application Gateway überwacht, kontrolliert und protokolliert. Diese Phase ist für den Benutzer transparent.

- **5. Phase: Verbindungsabbau**
  In der letzten Phase wird die Verbindung über das Application Gateway abgebaut.

Telnet Proxy

Der Telnet Proxy ist für die kontrollierte Kommunikation über Telnet verantwortlich und stellt entsprechende spezielle Sicherheitsfunktionen für diesen Dienst zur Verfügung.

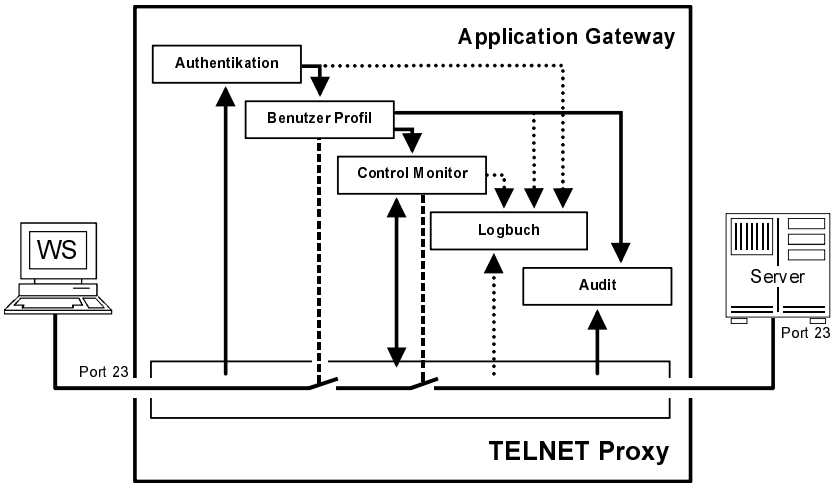

Abb. 12.26: Telnet Proxy

Der Verbindungsaufbau erfolgt vom Quell-Rechnersystem (Client) auf Port 23 (Port für den Telnet-Dienst) des Application Gateway. An Port 23 übernimmt der Telnet Proxy die Verbindung. Der Benutzer auf dem Quell-Rechnersystem identifiziert und authentisiert sich unter Angabe des Verbindungsziels gegenüber dem Telnet Proxy. Nach erfolgreicher Identifikation und Authentikation wird ein den folgenden Bedingungen entsprechendes Benutzerprofil aktiviert:

- IP-Adresse des Quell-Rechnersystems, das die Verbindung aufbauen möchte
- Benutzername, mit dem die Identifikation und Authentikation erfolgte
- IP-Adresse des Ziel-Rechnersystems

Nun baut der Telnet Proxy eine zweite Verbindung vom Application Gateway auf Port 23 des Ziel-Rechnersystems auf. Jetzt kann der Benutzer vom Quell-Rechnersystem über den Telnet Proxy den Telnet-Dienst des Ziel-Rechnersystems nutzen (siehe Abb. 12.26).

Control Monitor:

Bei der Telnet-Session ist es zum Beispiel möglich, mit Hilfe eines »Control Monitors« zu überprüfen, ob der Benutzer unerlaubterweise vom Quell-Rechnersystem auf ein anderes Rechnersystem als das erlaubte Ziel-Rechnersystem zugreift.

Dabei überprüft der Monitor den Datenstrom auf Bytefolgen, die unter Umständen für ein Hopping genutzt werden können. Es ist auch möglich, nach anderen Informationen zu suchen, zum Beispiel nach Steuerzeichen, die nicht verwendet werden sollen (`Ctrl-C etc.`)

Logbuch:

In das Logbuch des Application Gateway können durch den Telnet Proxy die folgenden Protokolleinträge vorgenommen werden:

- IP-Adresse und Rechnername des Quell-Rechnersystems
- IP-Adresse und Rechnername des Ziel-Rechnersystems
- Uhrzeit und Datum des Verbindungsaufbaus
- Name des Benutzers
- Anzahl der übertragenen Bytes
- Uhrzeit und Datum des Verbindungsabbaus

Bei der Telnet-Verbindung ist es oft sinnvoll, einen Mitschnitt der kompletten Kommunikation aufzuzeichnen (Audit). Neben der Möglichkeit, diesen Mitschnitt später auszuwerten, hat diese Sicherheitsfunktion einen nicht zu unterschätzenden Warneffekt.

Anwendungsbeispiel für Audit:

Der Sicherheitsmechanismus »Audit« kann zum Beispiel vertraglich mit einer Firma vereinbart werden, die Remote-Service durchführt.. Dadurch ist dem Mitarbeiter der Servicefirma bewusst, dass alles, was er tut, protokolliert wird. Allein das Wissen um diese Überwachung wird den Serviceleistenden motivieren, nur das zu tun, was er für seine Aufgabenstellung wirklich benötigt. Im Fall eines Schadens kann dann das Protokoll aufklären, ob über den Remote-Zugriff unerlaubte oder nicht notwendige Aktionen durchgeführt worden sind. Der Mitarbeiter der Service-Firma kann für seine Handlungen im Nachhinein dezidiert verantwortlich gemacht werden.

FTP Proxy

Der FTP Proxy ist für die kontrollierte Kommunikation über FTP verantwortlich und stellt entsprechende spezielle Sicherheitsfunktionen für diesen Dienst zur Verfügung.

Der Verbindungsaufbau für den Kommandokanal erfolgt vom Quell-Rechnersystem (Client) auf Port 21 (FTP-Kommando-Port) des Application Gateway. Der Benutzer auf dem Quell-Rechnersystem identifiziert und authentisiert sich nun unter Angabe des Verbindungsziels gegenüber dem FTP-Dienst. Nach erfolgreicher Identifikation und Authentikation wird ein den folgenden Bedingungen entsprechendes Benutzerprofil aktiviert:

- IP-Adresse des Quell-Rechnersystems, das die Verbindung aufbauen möchte

- Benutzername, mit dem die Authentikation erfolgte
- IP-Adresse des Ziel-Rechnersystems

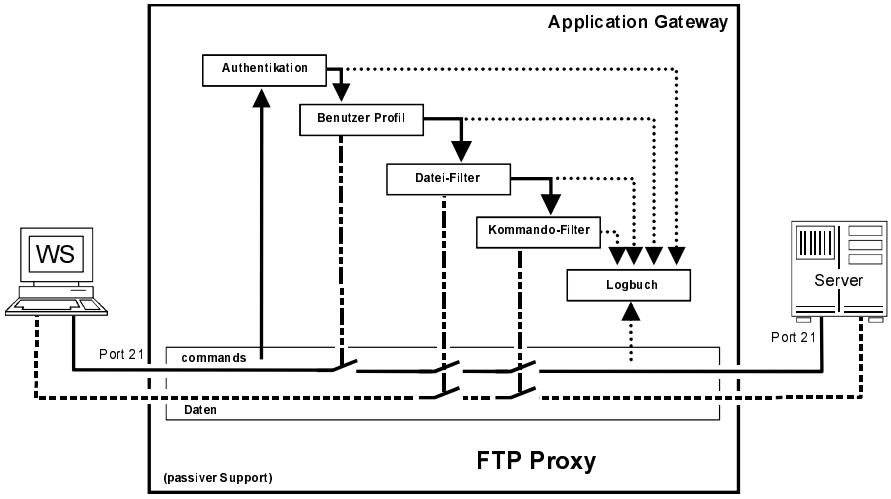

Abb. 12.27: FTP Proxy

Nun baut der FTP Proxy einen zweiten Kommandokanal vom Application Gateway auf Port 21 des Ziel-Rechnersystems auf (siehe Abb. 12.27).

Kommando-Filter:

Der Kommando-Filter analysiert und überprüft alle vom Benutzer eingegebenen FTP-Kommandos hinsichtlich ihres Eintrags in der Rechtedatei (Benutzerprofil). Für den FTP Proxy kann zum Beispiel definiert werden, welche Befehle (`cd, put, get, del` usw.) verwendet werden dürfen und welche nicht.

Gibt der Benutzer ein Kommando ein, zu dem er berechtigt und bei dem ein Datentransfer erforderlich ist, erfolgt der Verbindungsaufbau des Datenkanals abhängig davon, ob auf dem Quell-Rechnersystem (Client-Seite) eine aktive oder eine passive FTP-Verbindung gewünscht wurde.

Wird ein Kommando von einem nicht dazu berechtigten Benutzer verwendet, wird dies dem Benutzer angezeigt, der unberechtigte Versuch wird in das Logbuch des Application Gateway eingetragen und, falls definiert, als Spontane Meldung an das Security Management gesendet.

Datei-Filter:

Außerdem kann bei FTP Proxies durch einen Datei-Filter in der Regel eine Namensrestriktion für die Dateien vorgenommen werden, die übertragen werden dürfen. Beispiele für solche Regeln sind:

- Es dürfen nur Dateien mit dem Namen »Input.neu« und »Output.neu« transferiert werden.
- Es dürfen keine Dateien mit der Endung ».exe« übertragen werden.

Logbuch:

In das Logbuch des Application Gateway können durch den FTP Proxy die folgenden Protokolleinträge standardmäßig vorgenommen werden:

- IP-Adresse und Rechnername des Quell-Rechnersystems
- IP-Adresse und Rechnername des Ziel-Rechnersystems
- Uhrzeit und Datum des Verbindungsaufbaus
- Name des Benutzers
- Anzahl der übertragenen Bytes
- Name der übertragenen Dateien
- verwendete Befehle
- Uhrzeit und Datum des Verbindungsabbaus

Anwendungsbeispiel für den FTP Proxy:

Mit Hilfe des FTP Proxy kann genau definiert werden, welche Befehle verwendet werden dürfen. Falls zum Beispiel ein Softwarehaus auf einen bestimmten Server ein Update senden möchte, wird einem Mitarbeiter des Softwarehauses erlaubt, die Befehle `cd` und `put` zu verwenden. Diese Befehle reichen aus, um die Arbeit durchführen zu können.

Die Reduzierung der erlaubten Befehle verhindert, dass bei dieser Aktion versehentlich oder absichtlich Schaden angerichtet wird. Falls zum Beispiel versucht wird, den Befehl `del` (Löschen) auszuführen, wird dies im FTP Proxy des Application Gateway erkannt und dem Benutzer angezeigt. Das Ereignis wird in das Logbuch eingetragen und, falls im Regelwerk definiert, eine Spontane Meldung mit den entsprechenden Protokolldaten an das Security Management gesendet.

HTTP Proxy

Der HTTP Proxy ist für die kontrollierte Kommunikation über HTTP verantwortlich und stellt spezielle Sicherheitsfunktionen für diesen Dienst zur Verfügung.

Der Verbindungsaufbau erfolgt vom Quell-Rechnersystem (Client) auf Port 80 (Port für den HTTP-Dienst) des Application Gateway. Der Benutzer auf dem Quell-Rechnersystem (Client-Seite) identifiziert und authentisiert sich nun unter Angabe des Verbindungsziels gegenüber dem HTTP-Dienst. Nach erfolgreicher Identifikation und Authentikation wird ein den folgenden Bedingungen entsprechendes Benutzerprofil aktiviert:

- IP-Adresse des Quell-Rechnersystems, das die Verbindung aufbauen möchte
- Benutzername, mit dem die Authentikation erfolgte
- IP-Adresse des Ziel-Rechnersystems

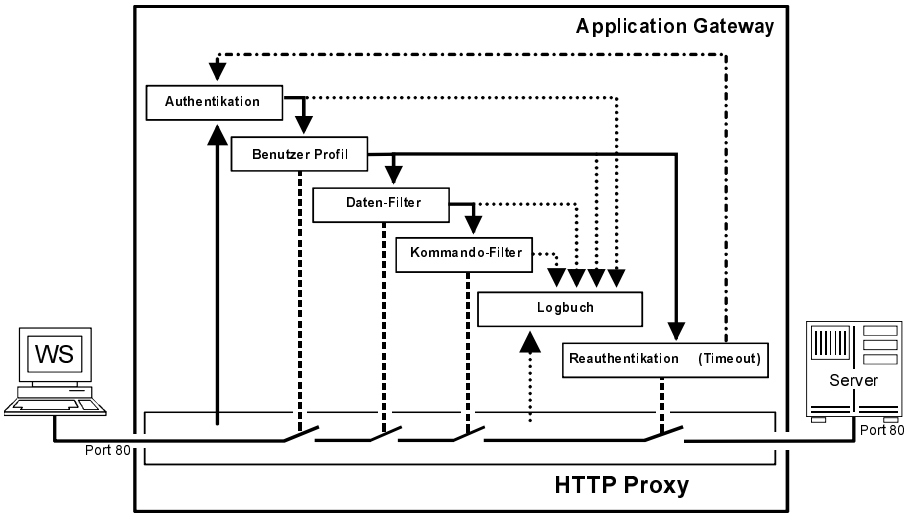

Abb. 12.28: HTTP Proxy

Nun baut der HTTP Proxy eine zweite Verbindung vom Application Gateway auf Port 80 des Ziel-Rechnersystems auf. Jetzt kann der Benutzer vom Quell-Rechnersystem über das Application Gateway (HTTP Proxy) den HTTP-Dienst des Ziel-Rechnersystems nutzen (siehe Abb. 12.28).

Re-Authentikation:

Das HTTP-Protokoll arbeitet nicht Session-orientiert, das heißt, der HTTP Proxy ist nicht in der Lage, von sich aus das Ende einer Session zu erkennen. Jedes Mal, wenn eine WWW-Seite angefordert wird, wird eine Verbindung über das Firewall-System aufgebaut, die WWW-Seite übertragen und wieder abgebaut. Beim ersten Mal wird vor der Übertragung die Authentikation durchgeführt. Dabei wird ein Timer gesetzt, der den Beginn der Session festhält. Nach Ablauf des Timers beendet der HTTP Proxy die zugehörige HTTP-Session automatisch. Sobald eine Benutzeraktivität in dieser Session stattfindet, wird der Timer erneut gestartet. Läuft der Timer ab, muss – falls eingestellt – bei einer erneuten Kommunikation wieder eine Identifikation und Authentikation stattfinden.

Kommando-Filter:

Der Kommando-Filter analysiert und überprüft die verwendeten Methoden (FTP, HTTP, NNTP, SMTP) und die verwendeten Befehle (zum Beispiel `put`, `get`, `post`).

Bei jedem Versuch, eine nicht gültige Methode oder einen nicht erlaubten Befehl zu verwenden, wird dem Benutzer eine entsprechende Meldung angezeigt und es erfolgt ein Eintrag in das Logbuch des Application Gateway. Falls im Regelwerk

definiert, wird in diesem Fall auch eine Spontane Meldung mit den Protokolldaten an das Sicherheitsmanagement gesendet.

Daten-Filter:

Mit Hilfe eines Daten-Filters im HTTP Proxy ist es auch möglich, nur definierte URLs zuzulassen (URL-Blocker). Zum Beispiel kann festgelegt werden, dass die Benutzer nur HTTP-Server mit der Länderkennung ».de« nutzen dürfen. Durch den Daten-Filter kann der Proxy aber auch bekannte unerwünschte Dateien oder HTTP-Seiten ausfiltern. Dies kann zum Beispiel bei bekannten Dateien, die Viren enthalten, oder bei HTTP-Seiten, auf denen pornographische Bilder zu sehen sind, genutzt werden.

Content Security:

Unter den Begriff Content Security werden hier die Sicherheitsmechanismen verstanden, die gegen die Gefährdungen durch aktive Inhalte innerhalb von HTML-Seiten wirken /Fuhr98//Koke97/.

- Applet-Filter
  Mit Hilfe eines Applet-Filters kann die Nutzung von Java, Java Scripts und ActiveX verhindert werden. Dies ermöglicht, die Sicherheitspolitik einer Organisation in bezug auf die Nutzung von dynamischen Programmteilen durchzusetzen. Ein mögliches Beispiel ist, Java im zu schützenden Netz für die Intranet-Anwendungen zuzulassen, aber bei der Kommunikation mit Rechnersystemen im unsicheren Netz über das Firewall-System zu verhindern.
- Malware-Filter
  Mit Hilfe eines Malware-Filters können Viren, Würmer und Trojanische Pferde aufgespürt und mögliche Schäden verhindert werden.

Logbuch:

Durch den HTTP Proxy können zum Beispiel die folgenden Protokolleinträge in das Logbuch des Application Gateway vorgenommen werden:

- IP-Adresse und Rechnername des Quell-Rechnersystems
- IP-Adresse und Rechnername des Ziel-Rechnersystems
- Uhrzeit und Datum des Verbindungsaufbaus
- Name des Benutzers
- Anzahl der übertragenen Bytes
- Name der übertragenen Datei oder der übertragenen HTML-Seite (Name der Seite und IP-Adresse des Servers/Ziel-Rechnersystems)
- Uhrzeit und Datum des Verbindungsabbaus

Authentication Proxy (Global Authentication)

Ein etwas anderes Konzept für ein Application Gateway dient dazu, dass der Benutzer eine Identifikation und Authentikation mit einem sogenannten Authentication Proxy durchführt.

Diese Art der Identifikation und Authentikation wird bei Firewall-Systemen auch »globale Authentikation« genannt. Der Authentication Proxy führt die Rechteverwaltung für die unterschiedlichen Dienste durch, zum Beispiel für FTP, Telnet, HTTP. In diesem Fall muss keine erneute Authentikation durchgeführt werden, wenn der Benutzer einen Dienst wechseln möchte. Ein Nachteil dieser Methode, der sich besonders bei Multiuser-Systemen zeigt, ist die nicht eindeutige Verbindung zwischen Dienst und Benutzer. Außerdem kann der Dienst während der Zeit zwischen der Freischaltung der Verbindung auf dem Application Gateway und dem Connect des Clients von Angreifern benutzt werden /uti99/.

Der Authentication Proxy regelt die Identifikation und Authentikation eines Clients auf einem Server über das Application Gateway. Anschließend können die erlaubten Dienste über das Firewall-System kontrolliert genutzt werden.

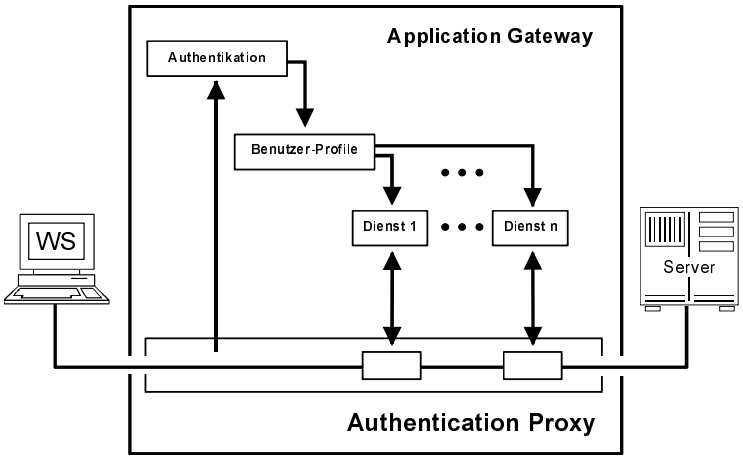

Abb. 12.29: Authentication Proxy

Transparent Proxy

Unter »Transparent Proxies« werden Proxies verstanden, die in der Lage sind, sich aus der Sicht der Clients transparent zu verhalten. Diese Proxies sorgen zum Beispiel dafür, dass aus dem zu schützenden Netz direkt Rechnersysteme im unsicheren Netz (zum Beispiel dem Internet) adressiert werden können. Der Vorteil dieser Proxies, die sich transparent von innen nach außen verhalten, liegt darin, dass die Client-Software bei der Integration eines Firewall-Systems nicht verändert werden

braucht. Bestimmte Anwendungen, wie zum Beispiel Home-Banking-Lösungen, die über Java-Applets feste IP-Adressen mitsenden, können dann auch über Firewall-Systeme realisiert werden.

Circuit Level Proxies

Da bei Application Gateways ein Routing auf der Netzwerkebene aus Sicherheitsgründen nicht möglich sein darf, könnten für Dienste, für die kein Application Level Proxy zur Verfügung steht, sogenannte Circuit Level Proxies zur Verfügung gestellt werden, wenn eine Kommunikation über das Application Gateway realisiert werden soll. Circuit Level Proxies sind eine Art generische Proxies, die für eine Mehrzahl von Diensten mit verschiedenen Protokollen verwendet werden können /BoW097/.

Diese Circuit Level Proxies, die auch als generische Proxies, Port-Relays oder Plug-Gateways bezeichnet werden, können in der Regel für TCP und UDP-Anwendungen verwendet werden.

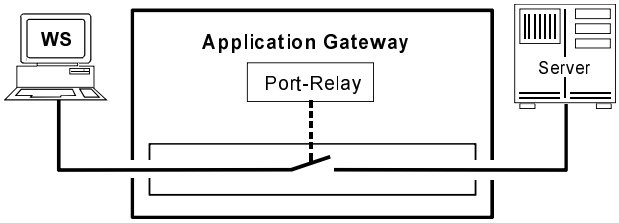

Abb. 12.30: Port-Relay

Mit einem Port-Relay kann eine Kommunikation über das Application Gateway kontrolliert über einen definierten Port auf eine definierte IP-Adresse erfolgen. Da die Kommunikation über die Port-Nummer des Port-Relay adressiert wird, kann die Kommunikation über das Application Gateway nur auf eine IP-Adresse auf der »anderen Seite« erfolgen. Aus diesem Grund sind Port-Relays immer n:1. Das heißt, dass viele Rechnersysteme (IP-Adressen) von der einen Seite auf ein Rechnersystem (eine IP-Adresse) auf der anderen Seite zugreifen können, während der umgekehrte Weg nicht möglich ist.

Im folgenden werden zwei Anwendungsbeispiele dargestellt, die aufzeigen, welche Möglichkeiten mit den Circuit Level Proxies – Port Relays – realisiert werden können.

Beispiel eines n:1 Port-Relay:

In diesem Beispiel wird ein Mail-Server vor dem Application Gateway im unsicheren Netz positioniert. Mit Hilfe eines POP3-Servers können Mails in das zu schüt-

zende Netz übertragen werden. Auf dem Application Gateway wird dann ein Port-Relay definiert, über den mehrere Clients (IP-Adressen) über eine bestimmte Portnummer (hier 110) auf die IP-Adresse des Mail-Servers zugreifen dürfen.

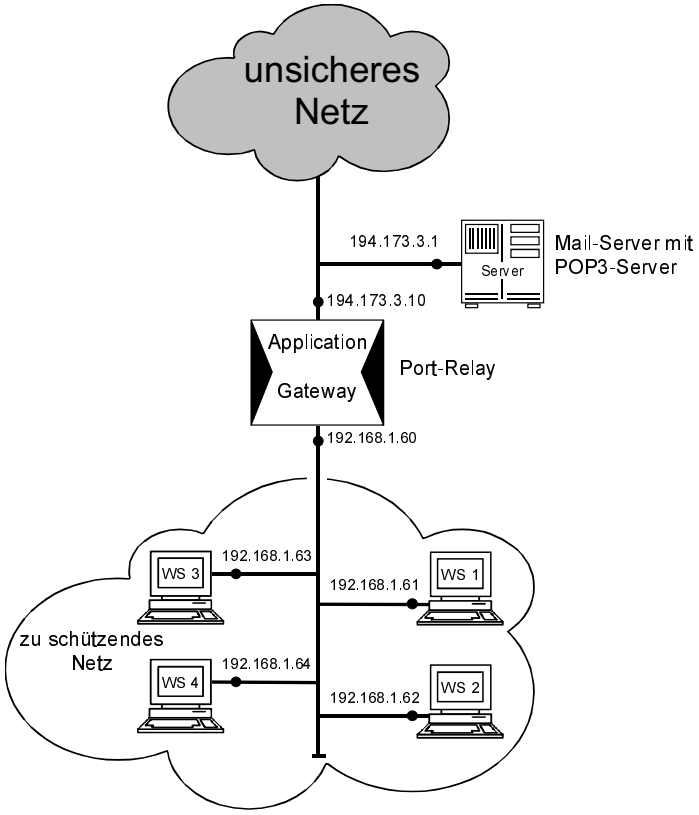

Abb. 12.31: Beispiel eines n:1 Port-Relay

Somit können die Clients (Quell-Rechnersysteme) über den definierten Port auf den Mail-Server (Ziel-Rechnersystem) zugreifen, um ihre Mail abzurufen. Das Port-Relay überprüft, ob von den zugelassenen IP-Adressen über den erlaubten Port auf die IP-Adresse des Mail-Servers zugegriffen wird. Der umgekehrte Weg ist nicht möglich.

Die n:1 Port-Relays sind sehr starr und können nicht für jede mögliche Anwendung verwendet werden. Es gibt aber die Möglichkeit, aus vielen n:1 Port-Relays einen n:m Port-Relay zu gestalten.

Quell-IP-Adressen (n) zu schützendes Netz	Ziel-IP-Adresse des Application Gateway zu schützendes Netz	Portnummer	Quell-IP-Adresse des Application Gateway unsicheres Netz	Ziel-IP-Adresse (1) unsicheres Netz
192.168.1.1 192.168.1.2 192.168.1.3 192.168.1.4	192.168.1.60	110	194.173.3.10	194.173.3.1

Tabelle 12.1: Beispiel für einen n:1 Port-Relay

Beispiel eines n:m Port-Relay

In diesem Beispiel wird beschrieben, wie die Möglichkeit geschaffen werden kann, aus dem unsicheren Netz über verschiedene IP-Adressen des unsicheren Netzes (zum Beispiel Internet) auf unterschiedliche Rechnersysteme im zu schützenden Netz (zum Beispiel Intranet) zuzugreifen. Das Application Gateway kann dann über mehrere IP-Adressen aus dem unsicheren Netz angesprochen werden. Dabei sollen die IP-Adressen der Rechnersysteme des zu schützenden Netzes verborgen bleiben.

Dazu wird m-mal ein n:1 Port-Relay für die unterschiedlichen IP-Adressen definiert, die aus dem unsicheren Netz auf das zu schützende Netz zugreifen können, und es wird festgelegt, auf welche Rechnersysteme im zu schützenden Netz sie zugreifen dürfen.

Aus der Sicht der Rechnersysteme im unsicheren Netz werden die IP-Adressen der Server im zu schützenden Netz wie IP-Adressen des unsicheren Netzes betrachtet.

Dabei wird auch genau definiert, über welchen Port dies ermöglicht wird (siehe Tabelle 12.2: Port 2000). Durch den n:m Port-Relay wird erreicht, dass die IP-Adressen des zu schützenden Netzes verborgen bleiben, weil sich nur die externen IP-Adressen darstellen, und dass die Kommunikation über den Port nur mit definierten Rechnersystemen in eine Richtung ermöglicht wird.

Logbuch der Port Proxies:

Durch den Port Proxy können folgende Einträge in das Logbuch des Application Gateway vorgenommen werden:

- IP-Adresse und Rechnername des Quell-Rechnersystems
- IP-Adresse und Rechnername des Ziel-Rechnersystems
- Uhrzeit und Datum des Verbindungsaufbaus
- Anzahl der Bytes, die übertragen wurden
- Uhrzeit und Datum des Verbindungsabbaus

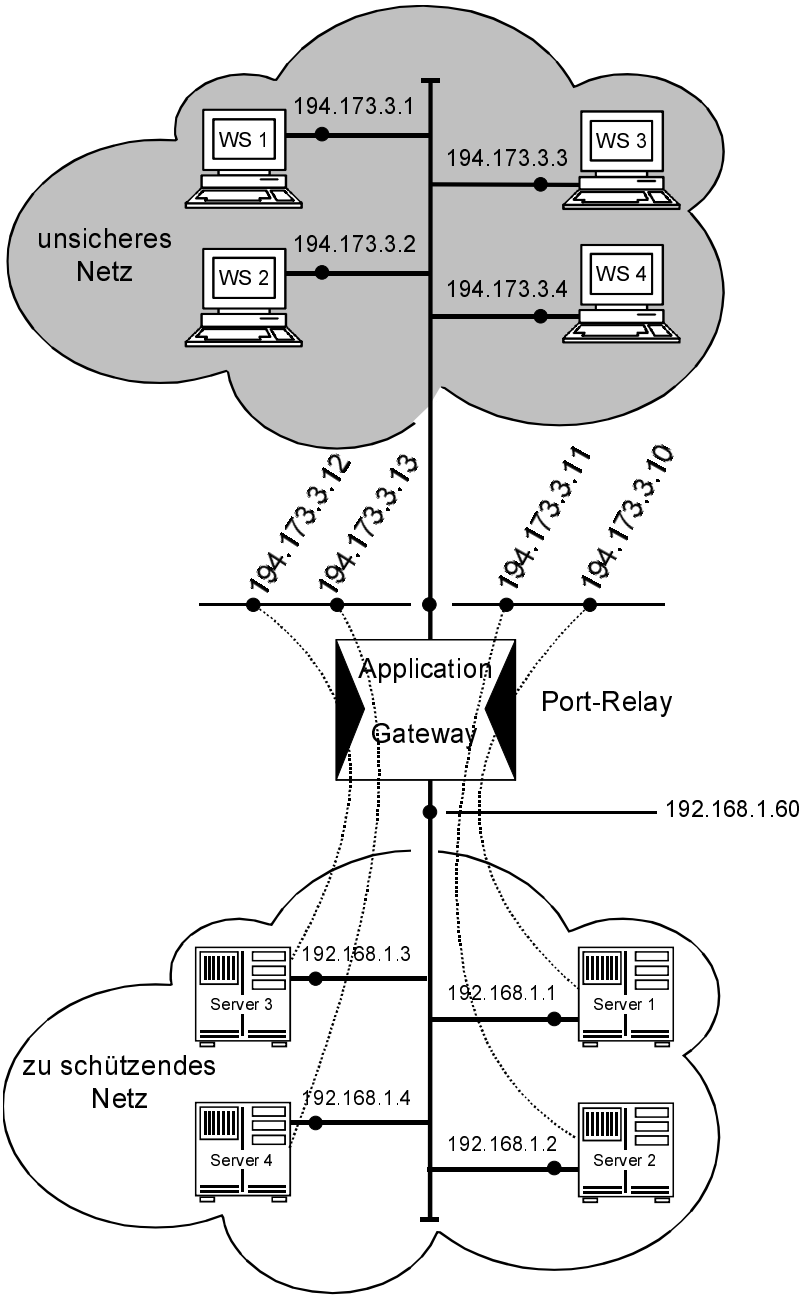

Abb. 12.32: Beispiel eines n:m Port-Relay

Quell-IP-Adressen unsicheres Netz	Ziel-IP-Adresse des Application Gateway unsicheres Netz	Portnummer	Quell-IP-Adresse des Application Gateway zu schützendes Netz	Ziel-IP-Adresse zu schützendes Netz
194.173.3.1 194.173.3.2 194.173.3.3 194.173.3.4	194.173.3.10	2000	192.168.1.60	192.168.1.1
194.173.3.1 194.173.3.2 194.173.3.3 194.173.3.4	194.173.3.11	2000	192.168.1.60	192.168.1.2
194.173.3.1 194.173.3.2 194.173.3.3 194.173.3.4	194.173.3.12	2000	192.168.1.60	192.168.1.3
194.173.3.1 194.173.3.2 194.173.3.3 194.173.3.4	194.173.3.13	2000	192.168.1.60	192.168.1.4

Tabelle 12.2: Beispiel für einen n:m Port-Relay

Beispiel eines speziellen Circuit Level Proxies:

Im folgenden soll exemplarisch ein spezielles Circuit Level Proxy dargestellt werden, wie es von manchen Application Gateways angeboten wird.

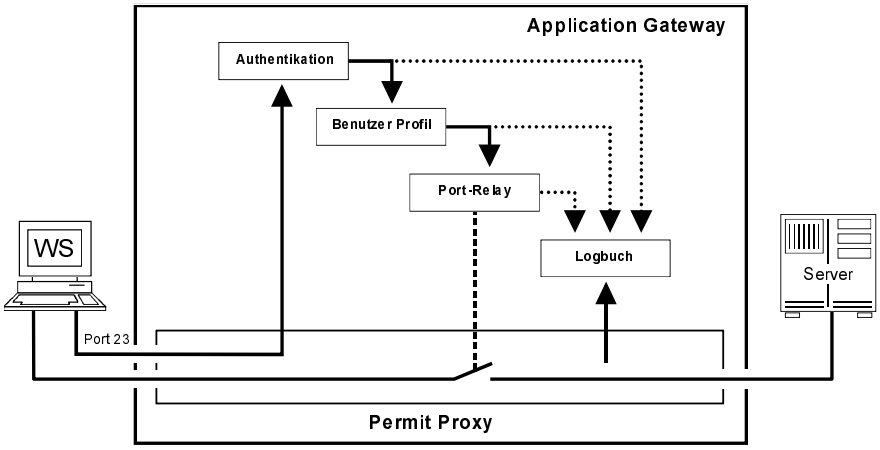

Abb. 12.33: Permit Proxy

Ein Permit Proxy regelt den Zugriff eines Client auf einen Server über das Application Gateway für TCP-basierte Dienste, die keinerlei Identifizierungs- und Authentisierungsmöglichkeiten bieten. Ein gutes Beispiel dafür sind NetBios-Protokolle, die per IP getunnelt werden. Für solche Protokolle können keine speziellen Proxies eingesetzt werden, weil bei den Programmen auf der Client-Seite kein Login-Mechanismus vorgesehen ist. Um dennoch den Zugriff auf bestimmte Rechnersysteme und Benutzer einzugrenzen, kann ein sogenannter Permit Proxy eingesetzt werden.

Dazu muss der Benutzer auf einem externen Rechnersystem zuerst eine Telnet-Verbindung (beziehungsweise eine HTTP-Verbindung) zum Application Gateway aufbauen, bevor er seine eigentliche Applikation starten kann. Nach einer erfolgreichen Identifikation und Authentikation kann der Benutzer den eigentlichen Dienst über einen »Port-Proxy« in Anspruch nehmen /uti98/.

Mit Hilfe des Permit Proxy kann dann festgelegt werden, über welchen Port, mit welchen Rechnersystemen (IP-Adressen) aus dem unsicheren Netz und mit welchem Rechnersystem (IP-Adresse) im zu schützenden Netz eine Kommunikation stattfinden darf. In diesem Beispiel wäre es auch möglich, über die Telnet-Verbindung weitere Verabredungen mit dem Application Gateway durchzuführen, zum Beispiel die Festlegung der IP-Adresse, mit der die Kommunikation stattfinden soll (wie ein flexibler n:m Port-Relay).

Die Telnet-Sitzung wird automatisch durch das Beenden der Applikation geschlossen. Falls das Telnet-Progamm vor der Anwendung beendet wird, unterbricht der Permit Proxy die Verbindung zur Applikation.

Logbuch:

Durch den Permit Proxy können folgende Einträge in das Logbuch des Application Gateway vorgenommen werden:

- IP-Adresse und Rechnername des Quell-Rechnersystems
- IP-Adresse und Rechnername des Ziel-Rechnersystems
- Uhrzeit und Datum des Verbindungsaufbaus
- Name des Benutzers
- Uhrzeit und Datum des Verbindungsabbaus

Der Permit Proxy ist im Prinzip ein Circuit Level Proxy mit Authentikation.

12.4.5 Adaptive Proxy

Einige Sicherheitshersteller versuchen, in einem sogenannten »Adaptive Proxy« die Vorteile von Packet Filter und Application Gateway zu kombinieren /NAI98/. Die Idee bei diesem Ansatz ist, dass der »Adaptive Proxy« in der Phase des Verbindungsaufbaus wie ein Application Proxy arbeitet und sich in der Phase des Datentransfers wie ein Packet Filter verhält. Der Vorteil dieser Methode liegt auf der Hand: In der ersten Phase wird eine sehr hohe Sicherheit erreicht, erst danach wer-

den die schnellen Tests der Packet Filter durchgeführt. Unter der Annahme, dass alle Angriffe die erste Phase, also den Aufbau einer Kommunikationsverbindung, betreffen, würde man mit diesem Ansatz eine hohe Sicherheit erreichen.

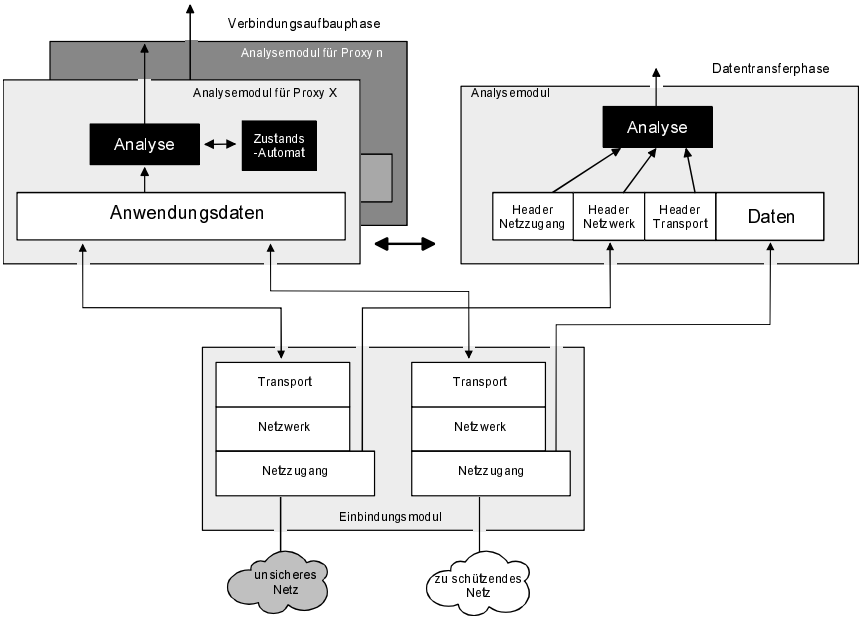

Abb. 12.34: Adaptive Proxy

Analogie zum Pförtner:

Der »Adaptive-Proxy-Pförtner« arbeitet in der ersten Phase (Verbindungsaufbau) wie der »Application-Proxy-Pförtner«: Er schaut sich nicht nur die Adresse der eingehenden Pakete an, er öffnet auch das Paket und überprüft den gesamten Inhalt. Wenn der »Adapive-Proxy-Pförtner« den Lieferanten seit langem kennt, dann sendet er den LKW des Lieferanten durch das Tor, damit dieser die Lieferung direkt zustellt. Kennt er den Lieferanten jedoch nicht, dann schickt er den LKW-Fahrer nach dem Ausladen der Lieferung weg und bestellt den firmeneigenen Fahrer, der im eigenen LKW das Paket zum Empfänger bringt.

Möglichkeiten und Grenzen eines Adative Proxy

Da ein elektronischer Pförtner aber nicht auf persönliche, menschliche Bindung aufbauen kann, scheint der Adaptive Proxy eher in der Theorie interessant zu sein als in der Praxis, da er kaum die Qualität eines Application Proxy erreichen kann. Soll das Äquivalent der persönlichen, menschlichen Bindung mit Hilfe von vertrauenswürdigen Netzen und/oder der Nutzung von Verschlüsselungssystemen

realisiert werden, muss eine genaue Analyse der Bedrohungen und der Einsatzumgebung durchgeführt werden.

12.4.6 Anwendungsgebiete von Application Gateways

Immer dann, wenn es notwendig ist, Schutzmaßnahmen für die Anwendungen zur Verfügung zu stellen, ist ein Application Gateway ein ideales aktives Firewall-Element. Die Möglichkeit der Protokollierung auf der Anwendungsebene kann ebenfalls ein besonderer Grund sein, ein Application Gateway in einem Firewall-Konzept zu berücksichtigen.

Für die Ankopplung an das Internet ist auf jeden Fall ein Application Gateway in der Firewall-Konstellation zu berücksichtigen, wenn die Rechnersysteme im zu schützenden Netz einen hohen Schutzbedarf haben (siehe auch Kapitel 3.2).

Außerdem können Organisationseinheiten, die sich innerhalb eines Intranet abschotten wollen, hiermit einen besonderen Schutz erzielen.

Möglichkeiten, Vorteile und besondere Aspekte von Application Gateways

- Das Design-Konzept ist sicher, da kleine, gut überprüfbare Module (Proxies) verwendet werden.
- Eine Konzentration auf das Wesentliche findet statt.
- Durch die ausnahmslose Übertragung aller Pakete durch den Proxy wird eine höhere Sicherheit erreicht.
- Der Kommunikationspartner der Rechnersysteme, die über das Application Gateway kommunizieren, ist der Proxy; dadurch kann eine echte Entkopplung der Dienste erreicht werden.
- Verbindungsdaten und Applikationsdaten können protokolliert und dadurch die Handlungen der Benutzer, die über das Application Gateway kommunizieren, nachvollzogen werden.
- Die interne Netzstruktur bleibt nach außen hin verborgen.
- Sicherheitsfunktionen für die Anwendungen werden zur Verfügung gestellt (Kommando-, Datei- und Daten-Filter usw.)
- Eine Network Address Translation findet statt.

Nachteile und Grenzen von Application Gateways

- Die Flexibilität ist gering, da für jeden neuen Dienst ein neuer Proxy zur Verfügung gestellt werden muss.
- Die Kosten für ein Application Gateway sind in der Regel höher.
- Die Kommunikation über das Application Gateway ist nicht transparent und erfordert daher eine veränderte Vorgehensweise.
- Einige Application Gateways können kein IP-Spoofing erkennen (dies ist kein generelles Problem).

12.4.7 Firewall-Elemente und das Verhältnis von Geschwindigkeit zu Sicherheit

Diese Abbildung stellt eine Art der Klassifizierung von Firewall-Elementen dar. Es wird das Verhältnis der unterschiedlichen Firewall-Elemente bezüglich Speed und Security qualitativ dargestellt.

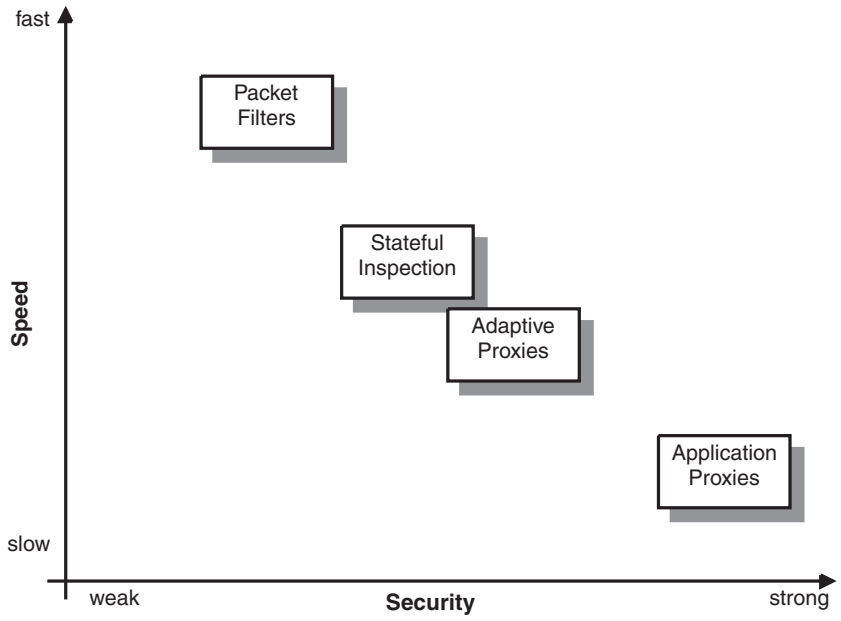

Abb. 12.35: Speed/Security

Durch den parallelen Einsatz mehrerer Application Gateways mit Application Proxies ist insgesamt eine höhere Leistungsfähigkeit (Durchsatz) zu erreichen und der dargestellte Nachteil in der Praxis zu kompensieren.

12.4.8 Unterschiedliche Firewall-Konzepte

Packet Filter, Application Gateway oder ein High-level Firewall-Konzept haben unterschiedliche Wirksamkeiten, wie sie die Kommunikation nach außen kontrollieren und wie sie einen Übergriff aus einem fremden auf das eigene Netz verhindern können.

Welches Firewall-Konzept nun bei der Etablierung eines VPN über öffentliche Kommunikationsinfrastrukturen verwendet werden sollte, hängt auch von der Kommunikationsinfrastruktur selbst ab.

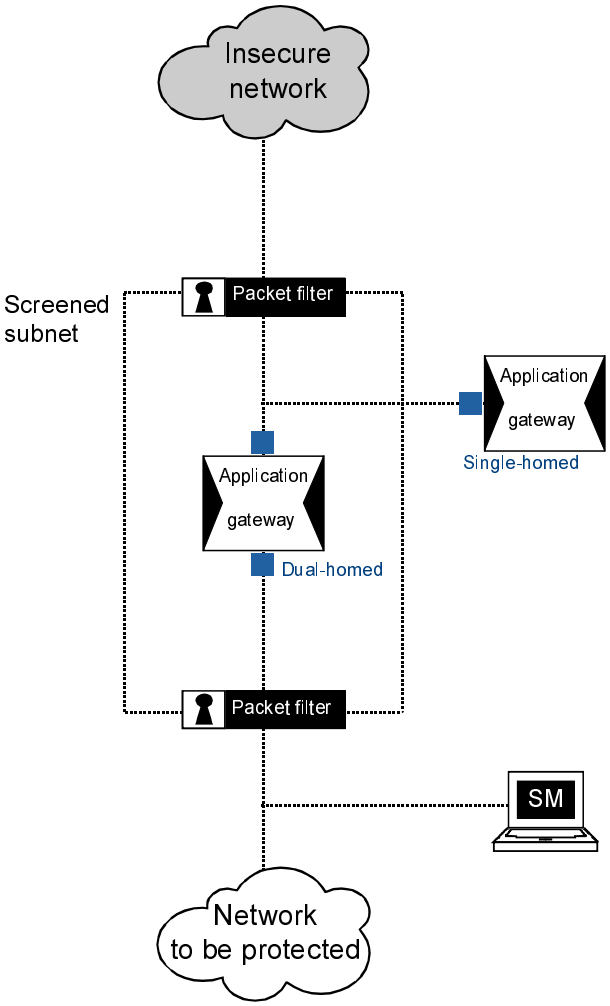

Abb. 12.36: Firewall-Konzepte

Wenn die Kommunikationsinfrastruktur an sich schon ein Höchstmaß an Sicherheit und Vertrauenswürdigkeit bietet, das heißt, wenn alle angeschlossenen Teilnehmer ungefähr die gleichen Sicherheitsbedürfnisse haben, kann auch mit einer einfachen Firewall-Lösung (zum Beispiel einem Packet-Filter) eine ausreichende Sicherheit erreicht werden /Pohl2001a/,/Pohl2000a/.

Wird aber beispielsweise ein VPN über das Internet realisiert, wo beliebig viele Teilnehmer mit äußerst heterogenen Zielen die gleiche Kommunikationsinfrastruktur benutzen, sollte ein Teilnehmer mit einem hohen Schutzbedarf bei der Ankopplung auf jeden Fall einen hohen Widerstand gegen Angriffe (mit einem High-level Security Firewall-System) realisieren.