



Firewall-Typen

Vom Paketfilter zum Application Level Gateway

GeNUA mbH - Kirchheim

Dieses Whitepaper beschreibt die verschiedenen Firewall-Typen und vergleicht ihre jeweiligen Vor- und Nachteile. Dabei liegt das Hauptgewicht der Betrachtung auf den Anwenderinteressen, technische Gesichtspunkte werden nur insoweit diskutiert, als sie Auswirkungen auf die Anwendung haben.

1 Einführung

Firewalls gewinnen seit etwa 15 Jahren zunehmend an Bedeutung, um Bereiche von IT-Netzen vor Gefährdungen aus anderen, verbundenen Netzen zu schützen. Insbesondere seit der Erschließung der Internet-Dienste durch Firmen und Privatpersonen rücken diese Schutzinstrumente mehr und mehr in den Blickpunkt des Interesses.

Dabei existieren verschiedene Typen von Firewall-Systemen, die sich vom grundsätzlichen Ansatz und damit auch in der Implementierung sehr voneinander unterscheiden. Obwohl diese unterschiedlichen Typen schon lange existieren, sind die Unterschiede zwischen den dabei zur Anwendung kommenden Techniken wenig bekannt. Dieses Dokument soll die fehlenden Informationen bereitstellen.

Dabei werden besonders die Eigenschaften detailliert beschrieben, die für den Anwender sichtbar und von Interesse sind. Aus Benutzersicht sind die folgenden vier Gesichtspunkte ausschlaggebend:

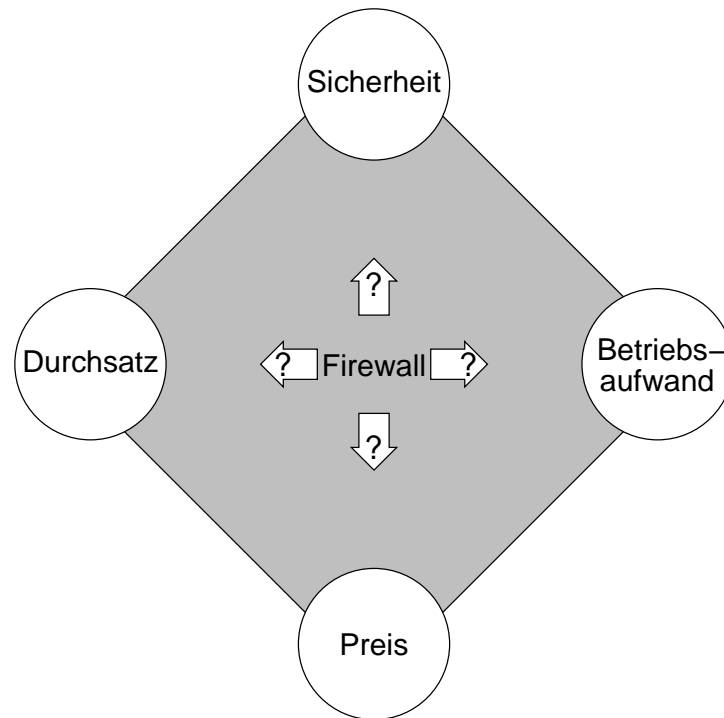
Sicherheit: Der Hauptzweck einer Firewall liegt in der Erhöhung der Sicherheit. Aufgrund ihrer spezifischen Arbeitswege erreichen die verschiedenen Firewall-Typen dieses Ziel in unterschiedlichem Maße.

Durchsatz: Eine Firewall darf nicht zum Flaschenhals der Netzkopplung werden, sondern muss ausreichend Reserven besitzen, um auch die Spitzen der Netzlast zufriedenstellend bedienen zu können.

Betriebsaufwand: Arbeitszeit im IT-Verwalteralltag ist knapp, und eine Firewall darf nicht zu pflegeintensiv werden. Auch sollte der Betrieb ausreichend übersichtlich sein, so dass keine Fehlkonfigurationen durch Missverständnisse entstehen, die dann die Sicherheit der zu schützenden Netze gefährden könnten.

Preis: Auch für wichtige Sicherheitsbelange stehen nicht unbegrenzt Mittel zur Verfügung. Der akzeptable Preis einer Sicherheitslösung richtet sich nach dem Schaden, der dadurch abgewendet werden kann.

Die folgende Abbildung stellt den Entscheidungsraum dar, der durch diese vier Pole des Benutzerinteresses aufgespannt wird.

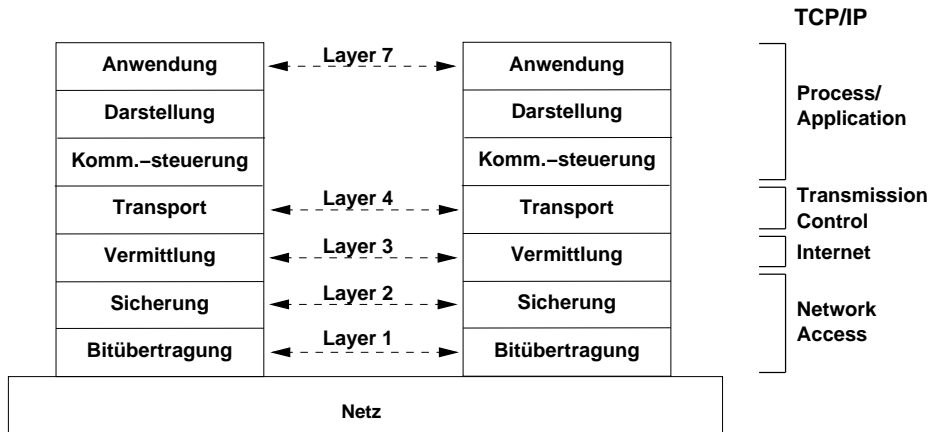


Die Platzierung der Firewall zwischen den vier Polen des Benutzerinteresses

2 Firewall-Typen

In diesem Abschnitt werden die verschiedenen Firewall-Typen mit ihren wesentlichen Eigenschaften dargestellt. Dieser Text kann und soll dabei kein Lehrbuch über Firewall-Technik ersetzen. Zur vertieften Auseinandersetzung mit diesem Stoff wird auf die Standardwerke von Cheswick, Bellovin und Rubin [1], Zwicky, Cooper und Chapman [2] sowie Garfinkel, Spafford und Schwartz [3] verwiesen.

Die folgende Beschreibung der Firewall-Typen wird erleichtert durch eine Erklärung des OSI-Protokoll-Stacks. OSI steht für *Open Systems Interconnect* und liefert ein standardisiertes Schichtenmodell für die Kommunikation zwischen IT-Systemen und damit für IT-Netze. Im OSI-Modell werden sieben aufeinander aufbauende Protokollschichten definiert, die den Ablauf der Kommunikation von sehr elementaren Vereinbarungen (Bitübertragung, Layer 1) bis zu sehr abstrakten Konzepten (Anwendungsebene, Layer 7) regeln. Diese Schichten sind in der nächsten Abbildung dargestellt. Für die folgende Diskussion sind dabei vor allem die Vermittlungs-, Transport- und Anwendungsschicht (Layer 3, 4 und 7) von Bedeutung.



Der OSI-Stack und seine Relation zum TCP/IP-Protokoll

Der OSI-Stack ist vor allem ein theoretisches Modell und wird im Internet praktisch nicht eingesetzt. Dagegen ist TCP/IP eine in der Praxis sehr erfolgreiche Protokolldefinition, die die Grundlage der Internetstruktur bildet. Diese Abbildung zeigt daher auch die Relation der TCP/IP-Schichten zu den OSI-Layern.

2.1 Paketfilter

Paketfilter-Firewalls sind historisch eine Erweiterung von Netzwerk-Routern. Jeder Router hat meist zwei oder mehrere Schnittstellen zu angeschlossenen Netzwerken und führt Tabellen darüber, welche Netze an welcher Schnittstelle angeschlossen oder darüber erreichbar sind (Routing-Tabellen). Es ist recht einfach, Router in ähnlicher Weise um Regelsätze zu erweitern, die festlegen, ob die so festgelegten Routen von unterschiedlichen IP-Paketen benutzt werden dürfen oder nicht.

Router treffen ihre Routing-Entscheidungen ausschließlich auf der Verbindungsschicht (Layer 3) des OSI-Protokolls (entsprechend der Internet-Schicht des TCP/IP-Protokolls). Dazu muss lediglich der IP-Header der Pakete analysiert werden, so dass Router auch mit bescheidener Hardware-Ausstattung ausreichend hohe Durchsatzraten erzielen.

In vergleichbarer Weise werden die Filtermechanismen eines klassischen Paketfilters einfach gehalten, um erhebliche zusätzliche Belastungen zu vermeiden und die Durchsatzraten hoch zu halten. Daher stützen sich diese Paketfilter auch nur auf Informationen, die in den IP- und Transportschicht-Headern enthalten sind und betrachten nicht die Dateninhalte der IP-Pakete auf höheren Protokollebenen. Ein gut ausgerüsteter Paketfilter im TCP/IP-Umfeld trifft seine Entscheidungen daher auf der Basis der folgenden Kenngrößen:

- den IP-Adressen von Absender und Empfänger
- dem verwendeten IP-Protokoll
- den TCP- und UDP-Ports, soweit das IP-Paket eines dieser Protokolle transportiert
- IP- und TCP-Flags, ICMP-Types
- die Netzschnittstellen, über die das IP-Paket den Paketfilter erreicht und gegebenenfalls wieder verlässt

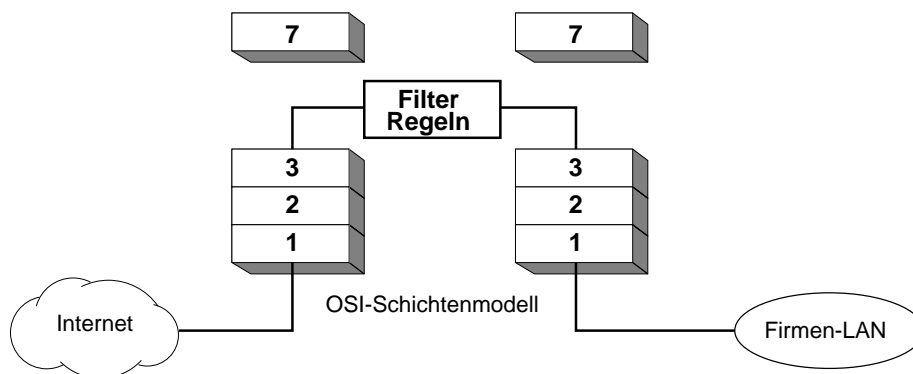


Nicht alle Paketfilter-Implementierungen benutzen alle diese Kenngrößen.

Der Firewall-Administrator legt einen Satz von Filterregeln fest, der im Betrieb statisch bleibt. Jede Regel legt für eine Kombination der oben aufgeführten Kenngrößen fest, ob ein IP-Paket weitergeleitet wird oder nicht. Bei der Bearbeitung eines bestimmten IP-Paketes wird mit den vorhandenen Filterregeln verglichen, ob eine Regel auf die Paket-Kenngrößen passt. Wenn ja, wird die in der Regel festgelegte Aktion (Weiterleiten oder Blockieren) ausgeführt. Wenn keine Filterregel zum Paket passt, kommt eine Voreinstellung zum Zuge (die im Interesse der Sicherheit zum Blockieren des Pakets führen sollte).

Ein klassischer Paketfilter bearbeitet jedes IP-Paket individuell, die Entscheidung über Weiterleitung oder Blockieren ist unabhängig davon, welche IP-Pakete vorher bearbeitet wurden. Viele Paketfilter werden auf der Basis von Routern realisiert, dafür wird gelegentlich die Bezeichnung „Chokes“ benutzt. Die Anordnung der Filterfunktion einer solchen Firewall innerhalb des OSI-Protokoll-Stacks wird in unten stehender Abbildung dargestellt.

Eine Alternative zu den Chokes sind so genannte „Bridging Firewalls“ oder „Screens“, bei denen die Filterregeln den Datenverkehr über eine Netzwerk-Bridge, also auf OSI-Layer 2, regeln. Sicherheitstechnisch entsprechen sie weitgehend den Paketfiltern auf Routing-Ebene, ein kleiner Vorteil kann darin gesehen werden, dass sie ohne eigene IP-Adresse konfiguriert werden und daher auf IP-Ebene nicht sichtbar sind. Netztechnisch sind sie von Vorteil, wenn die angeschlossenen Netzsegmente nicht jeweils eigenständige Subnetze bilden sollen oder können (z.B. wenn ein einzelner Server geschützt werden soll).



Der Einsatz von Filterregeln im OSI-Protokoll-Stack

2.2 Stateful Packet Filter

Die Filtereigenschaften eines Paketfilters lassen sich deutlich verbessern, wenn die IP-Pakete in ihrem Kontext überprüft werden. So ist es zum Beispiel wünschenswert, ein von einem externen Rechner kommendes UDP-Datagramm nur dann nach innen weiterzuleiten, wenn kurz zuvor von innen ein anderes UDP-Datagramm an denselben Rechner geschickt wurde. (Der Hintergrund dieser Kommunikation könnte eine DNS-Anfrage eines Clients im Innernetz an einen externen DNS-Server sein.) Um das zu ermöglichen, muss der Paketfilter zu allen aktuellen Verbindungen einen Status verwalten. Paketfilter, die das leisten, werden dementsprechend als *stateful* bezeichnet. Sie ahmen im Fall von TCP-Verbindungen die Statusüberwachung eines vollständigen TCP/IP-Protokoll-Stacks nach und simulieren virtuelle Verbindungen im Falle von UDP.



Eine andere wichtige Eigenschaft eines Stateful Packet Filters (kurz SPFL) ist die Fähigkeit, Filterregeln dynamisch zu erzeugen und zu löschen. Im oben genannten Fall muss beispielsweise nach dem Passieren des ersten UDP-Datagramms von innen nach außen für einen begrenzten Zeitraum eine Regel aktiviert werden, die das Antwort-Datagramm akzeptiert und an den Client weiterleitet. Nach Ablauf des Zeitfensters für die Antwort muss diese Regel dann wieder gelöscht werden. Dem Firewall-Administrator wird damit die Konfiguration erleichtert, da einige Regeldefinitionen nicht mehr explizit eingepflegt werden müssen. Auf der anderen Seite entzieht sich das Verhalten der Firewall teilweise der Kontrolle des Administrators. Der Ansatzpunkt des Regelwerks ist wie bei einfachen Paketfiltern der OSI-Layer 3 wie in der nächsten Abbildung gezeigt.

Stateful Packet Filter bieten damit die zusätzliche Sicherheitseigenschaft, viele Ports für von außen kommende IP-Pakete nicht permanent offen lassen zu müssen, sondern nur bei Bedarf zu öffnen. Dauerhaft offene externe Ports sind nur noch für solche Verbindungen notwendig, die von außen initiiert werden.

2.3 Stateful Inspection Firewalls

Das Stichwort „Inspection“ in der Bezeichnung dieses Firewall-Typs deutet an, in welcher Richtung die Überprüfungsmöglichkeiten hier erweitert werden. Stateful Inspection Firewalls (abgekürzt SIFW) ermöglichen den Zugang auch zu den Paketinhalten, die zu höheren Protokollebenen gehören. Damit ebnet SIFW den Weg zu einer Inhaltskontrolle des Datenverkehrs und auch anderen höheren Kontrollfunktionen wie z.B. Benutzer-Authentisierungen.

Die Voraussetzung dafür wird durch das andere Stichwort des Names, nämlich „Stateful“, gegeben. Erst durch die Statusverfolgung ist es möglich, die einzelnen IP-Pakete den verschiedenen simultan bestehenden Verbindungen zuzuordnen und damit eine Inhaltskontrolle sinnvoll zu ermöglichen. Dem Dateninhalt eines individuellen IP-Pakets ist z.B. kaum anzusehen, ob es zu einer E-Mail gehört – und noch weniger, ob diese E-Mail einen Virus, Trojaner oder Wurm enthält. Diese Überprüfung ist nur möglich, wenn der komplette Datenstrom aus allen IP-Paketen dieser Verbindung zusammengesetzt wird.

In der Regel führen SIFW diese Überprüfung jedoch nicht selbst durch, sondern reichen den Datenstrom mittels des *Content Vectoring Protocols (CVP)* an separate *Security Server* weiter, die dann die übergebenen Daten prüfen. Die Firewall selbst steuert nur die Grundlage in Form der statusgesteuerten Datenextraktion und des CVP bei. Diese Grundlage ist zwar allgemeingültig und machtvoll, aber Security Server stehen nur für sehr wenige Protokolle zur Verfügung. Für diese Protokolle arbeiten SIFW ähnlich wie die im folgenden Kapitel beschriebenen Application Level Gateways, für alle anderen Protokolle jedoch wie ein Stateful Packet Filter. Stateful Inspection Firewalls sind daher als Hybrid-Systeme anzusehen.



2.4 Application Level Gateways

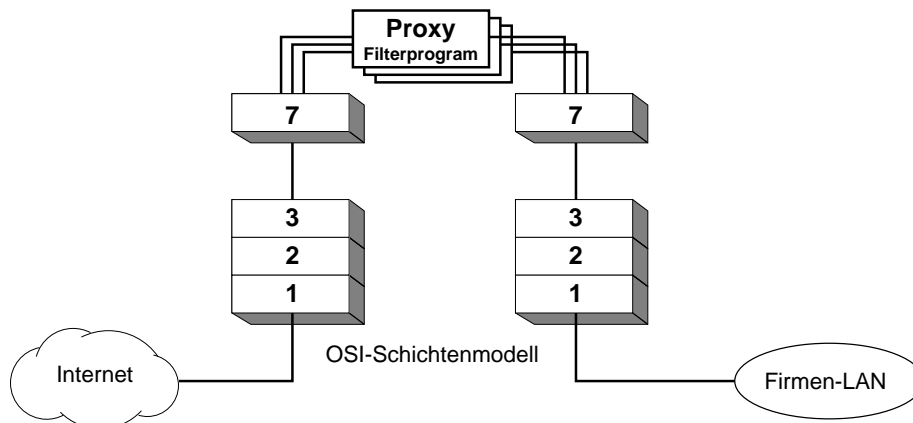
Dieser Firewall-Typ konzentriert seine Überwachungsfunktionen auf die Anwendungsebene. Für jedes behandelte Anwendungsprotokoll gibt es ein spezielles Prüfprogramm, „Proxy“ (auch „Relay“ oder „Gate“) genannt, das den Datenstrom dieser Anwendung vollständig analysiert. Daher wird dieser Firewall-Typ auch als „Proxy-Firewall“ bezeichnet.

Ein Proxy überprüft auf jeden Fall die Einhaltung des Anwendungsprotokolls, für das er geschrieben wurde. Hinzu kommen protokoll- und konfigurations-abhängig weitere Möglichkeiten:

Filterung von Protokoll-Elementen: Nicht alles, was im Anwendungsprotokoll definiert ist, mag im konkreten Einsatzfall erlaubt sein. Ein denkbares Beispiel ist z.B. die Filterung des *PUT*-Kommandos im FTP-Protokoll, wenn der angesprochene FTP-Server keine Uploads erhalten darf.

Suche nach Schadsoftware: Auf Anwendungsebene liegen die Daten in einem Format vor, das die Überprüfung auf Viren, Trojaner, Würmer und andere Schadsoftware mittels eines üblichen Virenschanners möglich macht.

Benutzer-Authentisierung: Sofern das Anwendungsprotokoll selbst eine Benutzer-Authentisierung vorsieht, kann diese bereits vom Proxy verlangt werden, bevor der eigentlich adressierte Server angesprochen wird. Ein nicht autorisierter Benutzer kann den Server dann gar nicht mehr erreichen.



Der Einsatz von Proxy-Programmen im OSI-Protokoll-Stack

Da Proxies auf der Anwendungsebene arbeiten, sind sie wie in dieser Abbildung dargestellt in den OSI-Stack eingebettet. Aus der Abbildung werden mehrere Eigenschaften eines Application Level Gateways deutlich:

- Auf jeder Netzseite wird der komplette Netzwerkprotokoll-Stack durchlaufen. Eingehende IP-Pakete auf der einen Netzseite werden im Stack zu einem Datenstrom auf Anwendungsebene zusammengesetzt und verlieren dabei ihre Existenz. Nach der Inhaltsüberprüfung erzeugt der ausgabeseitige Stack vollkommen neue IP-Pakete. Angriffe auf den Protokoll-Stack attackieren deshalb stets die Firewall und werden in keinem Fall auf die jeweils andere Netzseite weitergeleitet.



- Von der Firewall ausgesendete IP-Pakete wurden im dortigen Protokoll-Stack erzeugt und enthalten grundsätzlich als Absender die Adresse der sendenden Netzwerkschnittstelle. Damit verschleiert ein Application Level Gateway vollständig die Adressen der gegenüberliegenden Netzseite, das Resultat entspricht dem *Network Address Translation*-Mechanismus (NAT) der Paketfilter-Firewalls.
- Durch den Einschluss des kompletten Netzwerkprotokoll-Stacks in die Datenbearbeitung und die Anwendungslogik wird der vollständige Status der Verbindung überwacht. Ein Application Level Gateway ist daher wenigstens so „stateful“ wie jeder Stateful Packet Filter.
- Durch das Setzen von *Access Control Lists* (ACLs) für die Protokoll-Stacks können die gleichen Kontrollen auf Netzwerk-Kenngrößen (IP-Adressen, Portnummern) durchgeführt werden wie durch die Filterregeln der Paketfilter-Firewalls.

Proxy-Programme arbeiten, wie bereits dargestellt, auf der Anwendungsebene und treten deshalb auch auf dieser Ebene sichtbar in den Verbindungsweg zwischen den angeschlossenen Netzen. Daraus erklärt sich der englische Name „Proxy“, der auf deutsch „Stellvertreter“ bedeutet. Gegenüber einem Client in dem einen Netz tritt der Proxy als Server-Dienst auf, dem eigentlich gemeinten Server in dem anderen Netz gegenüber verhält er sich aber als Client-Anwendung, in jedem Fall also als Stellvertreter des eigentlichen Verbindungspartners.

Die Stellvertreter-Eigenschaft hat grundsätzlich zur Folge, dass entweder die Client-Anwendung oder der Endbenutzer von der Existenz des Proxies wissen und ihr Verhalten darauf einstellen. Zum Beispiel muss ein FTP-Benutzer beim Einsatz eines klassischen FTP-Proxies wissen, dass er mit seinem FTP-Client zunächst das Application Level Gateway adressieren muss. Auch WWW-Browser müssen so konfiguriert werden, dass sie bei jedem Verbindungswunsch den entsprechenden Proxy auf der Firewall ansprechen und nicht den in der URL spezifizierten Webserver. In moderneren Implementierungen von Application Level Gateways lässt sich diese Einschränkung aber durch den Einsatz von „transparenten“ Proxies umgehen. Die Bezeichnung leitet sich aus der Möglichkeit ab, solche Proxies aus Client- und auch aus Server-Sicht unsichtbar zu machen, indem die IP-Adressen des Absenders und/oder des Adressaten weitergeleitet werden.

Proxy-Programme sind anwendungsspezifisch. Daher muss ein Application Level Gateway grundsätzlich für jedes Protokoll, das über die Firewall geleitet werden soll, einen passenden Proxy zur Verfügung stellen. Für Standardanwendungen ist das eine legitime und auch erfüllbare Forderung (wobei im Zweifelsfall das Prädikat „Standard“ passend zu definieren ist). Auf der anderen Seite gibt es eine grundsätzlich unbegrenzte Zahl von Spezialanwendungen, deren Protokolldefinition häufig nicht einmal publiziert und damit verfügbar ist. Für solche Anwendungen kann es keinen Proxy im eigentlichen Sinne geben.

Damit solche Nicht-Standardanwendungen ebenfalls über ein Application Level Gateway geführt werden können, existieren so genannte „generische Proxies“. Diese sind eben nicht mehr anwendungsspezifisch, können und sollen also keine Protokollüberprüfung mehr vornehmen. Dementsprechend arbeiten sie auch nicht auf der Anwendungsebene, sondern als „Circuit Level Gateways“ auf Transportschichtebene oder sogar als generisches „IP-Relay“ auf der Internetschicht.



Trotz der notwendigen Einschränkung gegenüber Proxies im eigentlichen Sinne bieten generische Proxies immer noch einen hohen Schutzgrad, da sie zum einen wie Stateful Packet Filter den Status der Verbindung kontrollieren und darüber hinaus keine Pakete aus einem Netz in andere Netze weiterleiten.

3 Bewertung

In diesem Abschnitt werden die Vor- und Nachteile der verschiedenen Firewall-Typen, wie sie sich aus der vorangegangenen Funktionsbeschreibung ergeben, tabellarisch zusammengestellt. Vorteile werden dabei durch ein vorangestelltes Plus-Zeichen, Nachteile entsprechend durch ein Minus-Zeichen gekennzeichnet.

Paketfilter

- ⊕ Geringer Funktionsaufwand, hoher Durchsatz
- ⊕ Geringe oder gar keine Kosten
- ⊕ Fast jeder Service wird unterstützt (Ausnahme: *active FTP* u.ä. Protokolle mit dynamisch vereinbarten Ports)
- ⊕ Sehr transparent für die Endbenutzer
- ⊖ Direkter Austausch von IP-Paketen zwischen den angeschlossenen Netzen, daher Angriffe auf Protokoll-Stacks der beteiligten Rechner möglich
- ⊖ Viele ständig offene Ports auf der externen Seite
- ⊖ In komplexen Anwendungsfällen ist die Konfiguration schwer zu übersehen und zu warten
- ⊖ Keine Benutzer-Authentisierung möglich, daher einzige Quellidentifikation durch IP-Adresse, Angriffsmöglichkeit durch IP-Spoofing
- ⊖ Keine Inhaltskontrolle möglich
- ⊖ Protokollierung nur bis zum OSI-Layer 4 möglich (keine Dateinamen, URLs etc)
- ⊖ Adressverschleierung nur durch NAT möglich
- ⊖ Die Offenheit für fast jedes Anwendungsprotokoll führt leicht zu *quick-and-dirty*-Freischaltungen ohne Risikoanalyse und Policy-Prüfung

Stateful Packet Filter

- ⊕ Durch Statusüberwachung und dynamische Port-Verwaltung weniger ständig offene Ports auf der externen Seite als bei einfachen Paketfiltern

Alle anderen Vor- und Nachteile entsprechen denen des einfachen Paketfilters.

Stateful Inspection Firewall:

- ⊕ Möglichkeit der Einbindung von Prüfmöglichkeiten auf höheren OSI-Layern
- ⊖ Prüfmöglichkeiten nur für wenige Protokolle realisiert



Alle anderen Vor- und Nachteile entsprechen denen des oben beschriebenen Stateful Packet Filters.

Application Level Gateway:

- ⊕ Kein IP-Paketaustausch zwischen den angeschlossenen Netzen
- ⊕ Protokollüberprüfung
- ⊕ Filtermöglichkeit von Protokollelementen
- ⊕ Unterstützt Benutzer-Identifizierung und -Authentisierung
- ⊕ Untersuchung auf Schadsoftware möglich (z.B. Viren, aktive Inhalte)
- ⊕ Einbindungsmöglichkeit zusätzlicher Dienste (z.B. Virens Scanner, Webcache)
- ⊕ Detaillierte Protokollierungsmöglichkeiten (z.B. Dateinamen, URLs, Identifizierungs- und Authentisierungs-Informationen)
- ⊕ Adressverschleierung erfolgt auf IP-Ebene automatisch
- ⊕ Vollständige Statusverfolgung, virtuelle UDP-Verbindungen
- ⊖ Geringerer Durchsatz bei gegebener Hardware
- ⊖ Höherer Entwicklungsaufwand
- ⊖ Erhöhter Betriebsaufwand durch protokollspezifische Konfiguration und Protokollierung
- ⊖ Für jede Anwendung wird ein spezifischer Proxy benötigt, sofern nicht generische Proxies zum Einsatz kommen

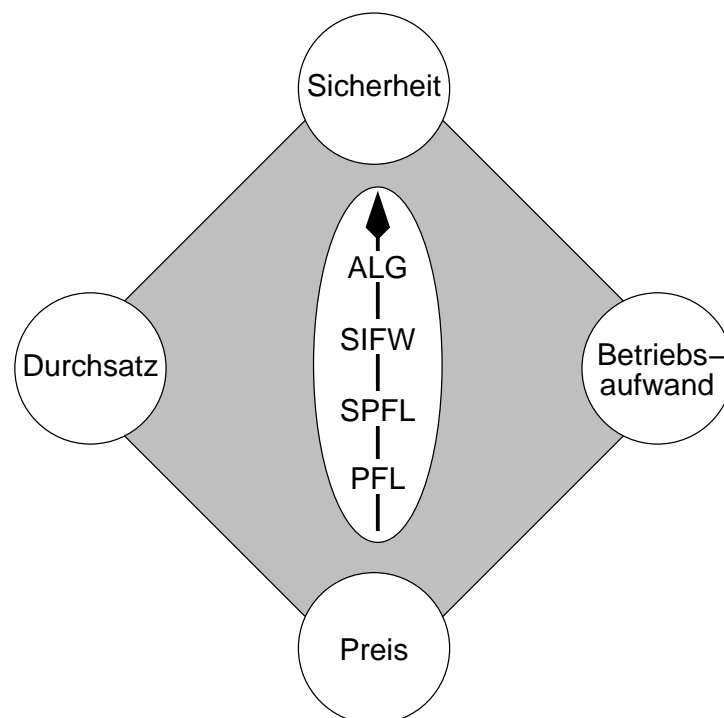


4 Schlussfolgerung

Aus der Gegenüberstellung von Vor- und Nachteilen der betrachteten Firewall-Typen ergibt sich ein Bild, das sich etwa wie in der Abbildung darstellen lässt: In der Reihenfolge Paketfilter – Stateful Packet Filter – Stateful Inspection Firewall – Application Level Gateway steigt die erreichbare Sicherheitsstufe an, wegen des steigenden Implementierungs-Aufwands tendenziell auch der Preis. (Im Einzelfall sorgen hier einzelne Lizenzierungsmodelle allerdings für Überraschungen.)

Da jede Überprüfung Rechenzeit kostet, sinkt bei steigendem Sicherheitsniveau naturgemäß der Durchsatz der Firewall bei gegebener Hardware. Allerdings erlaubt auch durchschnittliche PC-Hardware heute Durchsatzraten bei Application Level Gateways, die die Bandbreite der meisten WAN-Anbindungen übertrifft, so dass der geforderte Durchsatz nur noch in Ausnahmefällen die in Frage kommende Firewall-Technik beschränkt.

Die Frage des Betriebsaufwands lässt sich nicht einfach beantworten. Firewalls auf Paketfilter-Technik und deren Weiterentwicklungen zeichnen sich zunächst durch einheitliche Regel- und Protokollformate aus, so dass die Einarbeitung leicht fällt. Auf der anderen Seite hängen die Proxy-Konfigurationen eines Application Level Gateways genauso wie die erzeugten Log-Informationen von dem jeweiligen Protokoll ab und sind deshalb nicht einheitlich. Diese Erschwernis wird aber teilweise oder ganz wettgemacht durch die Tatsache, dass die Proxies das von ihnen kontrollierte Protokoll kennen und damit dem Administrator viel Arbeit abnehmen, die bei Paketfiltern manuell geleistet werden muss. Als Beispiel sei hier auf das FTP-Protokoll verwiesen, bei dem sowohl statische als auch unbegrenzt viele dynamische Ports für beide Transportrichtungen freigeschaltet werden müssen.



Trend der Firewall-Typen im Raum der Benutzerinteressen



5 Glossar

In diesem Glossar sind vornehmlich Begriffe aus dem Bereich der IT-Sicherheit aufgeführt. Auf allgemeinere Begriffe der Informationstechnik wird hier nicht eingegangen.

ALG: Abkürzung für → *Application Level Gateway*

Application Level Gateway: Ein im Haupttext genauer beschriebener Firewall-Typ, bei dem sich die Datenüberprüfung bis auf die Anwendungsschicht erstreckt. Die Überprüfung findet durch → *Proxy*-Programme statt, daher wird der Begriff *Proxy-Firewall* als Synonym zum A. gebraucht.

Authentifizieren: Das Belegen der Identität einer Person gegenüber einer Gegenstelle (einer anderen Person, einem Zugangskontrollsystem, einem Rechner u.a.), z.B. durch Passwort-Nennung oder Schlüssel

Authentisieren: Das Anerkennen der Identität einer Person durch eine Gegenstelle als Reaktion auf das → *Authentifizieren*.

Autorisieren: Das Erteilen einer Berechtigung, in der Regel als Folge des → *Authentisierens*

Bridging Firewall: Variante eines → *Paketfilters*, die auf einer Netzwerk-Bridge (OSI-Layer 2) anstelle eines Routers (OSI-Layer 3) aufsetzt. Diese Variante kann deshalb auch dort eingesetzt werden, wo die Trennung in IP-Subnetze auf beiden Seiten der Firewall nicht erwünscht oder möglich ist. Außerdem ist eine B.F. auf IP-Ebene nicht sichtbar.

Choke: Synonym für eine → *Paketfilter-Firewall*

Circuit Level Gateway: Ein Prüfprogramm ähnlich eines → *Proxies*, mit dem Unterschied, dass ein C. auf Transportschichtebene arbeitet und nicht anwendungsspezifisch ist. Damit entfällt die Möglichkeit der Protokollüberprüfung, aber die Funktionen der Statusüberwachung und der IP-Paketseparation sind voll vorhanden.

Gate oder **Gateway:** Synonym für einen → *Proxy*

Identifizierung: Die Zuordnung einer Anfrage zu einer Person. Achtung: Die I. beinhaltet keine Überprüfung der Korrektheit, das wird erst durch die → *Authentifizierung* geleistet.

IP-Spoofing: Das Vortäuschen einer falschen Absender-IP-Adresse im IP-Paket, um als vertrauenswürdiger Kommunikationspartner zu erscheinen

NAT: Abkürzung für → *Network Address Translation*

Network Address Translation: Die Bezeichnung für das gezielte Umschreiben von IP-Adressen und Port-Nummern in IP-Paketen durch → *Paketfilter-Firewalls*, um die Adressen in internen Netzen zu verschleiern. Diese Verschleierung kann zur Geheimhaltung oder auch durch die Verwendung privater IP-Adressbereiche notwendig sein.



OSI-Modell: Abkürzung für *Open Systems Interconnection*, einem standardisierten Schichtenmodell für den Datenaustausch zwischen IT-Systemen und damit theoretische Referenz für IT-Netze

Paketfilter: Ein im Haupttext genauer beschriebener Firewall-Typ, der für jedes IP-Paket anhand einfacher Regeln entscheidet, ob dieses Paket weitergeleitet oder blockiert wird.

PFL: Abkürzung für → *Paketfilter*.

Proxy: Engl. für „Stellvertreter“. Ein Programm, das im Verbindungsweg zwischen einem Client und einem Server die ausgetauschten Daten bis auf Anwendungsebene hinauf überprüft. Dabei tritt der Proxy dem Client gegenüber als Server-Dienst, dem echten Server hingegen als Client auf (daher die Bezeichnung als Stellvertreter). Proxies sind die wesentlichen Prüfinstanzen eines → *Application Level Gateways*.

Proxy-Firewall: Synonym für → *Application Level Gateway*

Screen: Synonym für → *Bridging Firewall*

SIFW: Abkürzung für → *Stateful Inspection Firewall*

SPFL: Abkürzung für → *Stateful Packet Filter*

Stateful Inspection: Eine Erweiterung des → *Stateful Packet Filters* um eine Untersuchung der Paketinhalte. Stateful Inspection Firewalls werden im Haupttext genauer beschrieben.

Stateful Packet Filter: Ein → *Paketfilter*, der über zusätzliche Statustabellen den Zustand von TCP- und (virtuellen) UDP-Verbindungen kontrolliert und gegebenenfalls dynamisch Ports freischaltet und schließt. Dieser Firewall-Typ wird im Haupttext genauer erläutert.

Transparenz: Eine Eigenschaft modernerer → *Proxy-Programme*, die den Einsatz von → *Application Level Gateways* auch für solche Protokolle und Client-Anwendungen erlaubt, die klassisch nicht proxy-fähig sind. Dazu werden (getrennt einstellbar) Ziel- und/oder Quelladressen der Verbindungen weitergeleitet.

Literatur

- [1] Bill Cheswick, Steve Bellovin, Aviel D. Rubin, *Firewalls und Internet Security: Repelling the Wily Hacker*, Addison-Wesley, 2. Auflage, 2003
- [2] Elizabeth Zwicky, Simon Cooper, D. Brent Chapman, *Building Internet Firewalls*, O'Reilly, 2. Auflage, 2000
- [3] Simson Garfinkel, Gene Spaffort, Alan Schwartz, *Practical Internet & Unix Security*, O'Reilly, 3. Auflage, 2003



So erreichen Sie uns:

GeNUA mbH • Domagkstrasse 7 • 85551 Kirchheim

tel +49 (89) 99 19 50-0 • fax +49 (89) 99 19 50-999 • info@genua.de • www.genua.de