Firewall – Schutz vor Angriffen aus dem Internet

Für Firewalls die zum Schutz vor Angriffen aus dem Internet eingesetzt werden, ist auch der Begriff Internet-Firewall gebräuchlich. Geht es lediglich um den Schutz eines einzelnen PCs, dann spricht man von Personal-Firewall.

Jeder mit dem Internet verbundene Rechner ist grundsätzlich von aussen erreichbar und daher angreifbar. Unter dem Oberbegriff Firewall sind verschiedene Techniken bekannt, um sich vor Angriffen aus dem Internet zu schützen. Dieser Beitrag erläutert die technischen Grundlagen[1] sowie typische Firewall-Konfigurationen.

Angriffe aus dem weltumspannenden Netz

So vielfältig die Motive für Angriffe über das Netz sind – sie reichen von Vandalismus bis hin zu den verschiedenen Formen der Spionage – so vielfältig sind auch die Arten der Angriffe über das Netz. Nahezu im Monatsrythmus werden hier neue Sicherheitslücken entdeckt und mit Patches[2] „repariert".

Versucht man, sich einen Überblick über die Gefährdungspotentiale zu verschaffen, muss man zunächst zwischen externen und internen aktiven Angriffen unterscheiden [1]. Die Berücksichtigung von internen Angriffen erscheint in diesem Zusammenhang als Widerspruch, da ja Firewalls vor Angriffen aus einem unsicheren Netz – in den meisten Fällen also dem Internet – schützen sollen. Aber was nützt der beste Schutz der eigenen Daten vor Ausspähung aus dem Internet, wenn interne Benutzer sich unbemerkt und unberechtigt sensibler Daten bemächtigen können und diese dann per Filetransfer versenden. Die Analyse der Gefährdungspotentiale und die Formulierung der tatsächlichen Sicherheitsbedürfnisse ist daher in den meisten Fällen weitaus schwieriger als die Realisierung [2] konkreter Schutzmechanismen vor bekannten Gefahren.

Firewall – was ist das?

Am einfachsten lässt sich der Begriff Firewall mit Brandschutzmauer übersetzen. Aber treffender als diese Übersetzung des Begriffes ist ein Vergleich mit dem Haupttor bzw. dem Burggraben einer mittelalterlichen Burg:

- Das Haupttor erlaubt das Betreten und Verlassen der Burg nur an einer sorgfältig bewachten Stelle.
- Der Burggraben verhindert, dass Angreifer zu nahe an die zu verteidigende Burgmauer herankommen.

Mit Blick auf diesen sehr treffenden Vergleich ist die Darstellung nach Bild ❶ zwar üblich, aber nicht ganz vollständig.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) liefert zur Erklärung des Begriffes Firewall folgende Umschreibung:

„Eine Firewall dient zur Kontrolle der Kommunikation zwischen zwei Netzen. Im Regelfall wird sie zum Schutz eines Netzes gegen Angriffe aus einem Netz mit einem geringeren Schutzbedarf eingesetzt, z. B. bei der Anbindung eines zu schützenden Teilnetzes an ein organisationsumspannendes Netz oder der Anbindung eines Firmennetzes an das Internet." Als „Firewall wird eine Kombination von Hard- und Software bezeichnet, die als alleiniger Übergang zwischen zwei zu trennenden TCP/IP-Netzen dient".

Grundbausteine

Paketfilter

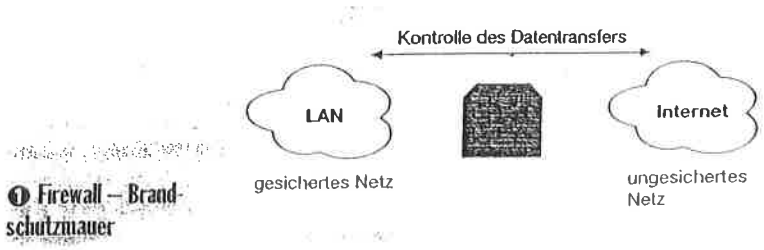
Die einfachste Möglichkeit zur Realisierung einer Firewall ist die Filterung der Datenpakete. Dazu werden die auf der Internet- und der Transportschicht verfügbaren Adressierungsinformationen genutzt, also

- IP-Adresse des Senders/Empfängers,
- Protokolltyp und
- Port-Nummer des Senders/Empfängers.

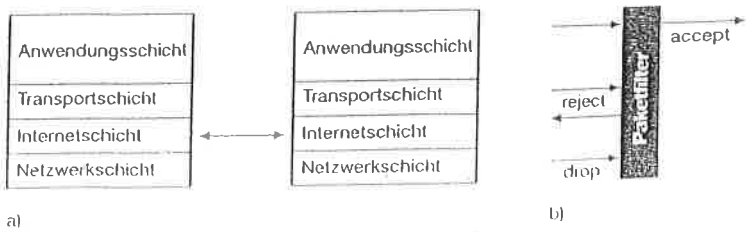
Über die IP-Adresse erfolgt die Adressierung des Endsystems (also des jeweiligen Rechners) und über die Port-Nummer und den Protokolltyp die Adressierung des Dienstes. Im TCP/IP-Protokollstapel lassen sich Paketfilter der Internetschicht (Bild ❷a) zuordnen. Prinzipiell gibt es dabei drei Möglichkeiten (Bild ❷b) zur Behandlung eines Datenpaketes:

- normal weiterleiten (accept)
- verwerfen, aber eine Fehlermeldung an den Absender schicken (reject) und
- kommentarlos verwerfen (drop).

Da man zur Formulierung der Regeln für die Filterung vorzugsweise die Port-Nummern heranzieht, werden Paketfilter auch als Portfilter bezeichnet. Deshalb spricht man vom Freischalten von Ports. Der Mechanismus der Paketfilterung erscheint zunächst sehr einfach. Jedoch muss man dabei bedenken, dass die Filterregeln gesondert für die abgehenden und ankommenden Pakete formuliert werden müssen.



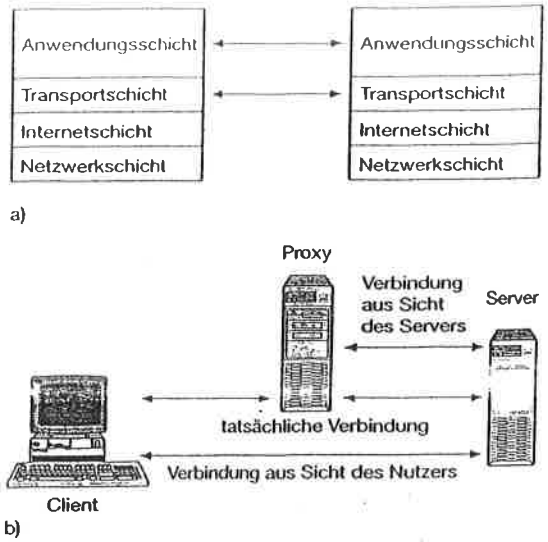
❶ Firewall – Brandschutzmauer



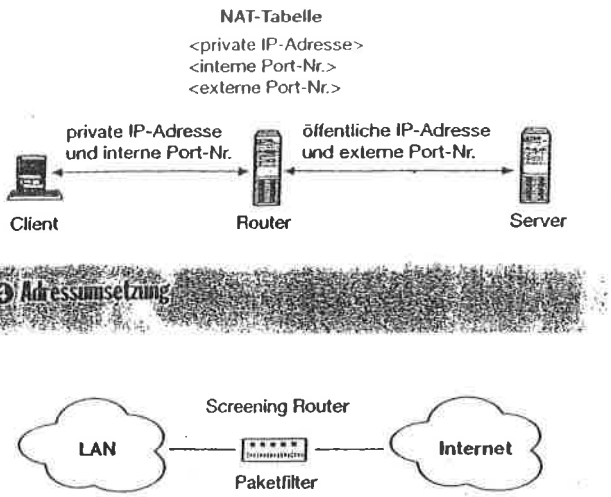
❷ a) Paketfilter arbeiten auf der Internetschicht b) Prinzipielle Funktion eines Paketfilters

[1] Dieser Beitrag setzt die Kenntnis der in LuK 2-02 bis 6/02 zum TCP/IP-Protokollstapel erläuterten Zusammenhänge voraus.

[2] Patch = Flickzeug. Software zum Reparieren von Fehlern oder zur Aktualisierung von Programmen.



❸ a) Proxies arbeiten oberhalb der Internetschicht
b) Prinzipielle Funktion von Proxies



❹ Adressumsetzung

❺ Screening Router

Beispiel eines statischen Paketfilters. Der Zugriff auf Web-Server soll möglich sein. Dazu muss geprüft werden, ob das abgehende Paket z. B. die Port-Nummer 80 als Zielport und beispielsweise eine Port-Nummer größer 1024 als Quellport hat. Jedes eingehende Paket muss nun von Port 80 kommen und einen Port größer 1024 ansprechen.

Erfolgt die Formulierung der Filteregeln in dieser Form, spricht man von einem **statischen Paketfilter.** Die Regeln werden getrennt für die ein- und ausgehenden Pakete formuliert und unabhängig vom aktuellen Zustand des Systems auf jedes Paket angewandt. Mit Blick auf das o. g. Beispiel wird schnell deutlich, dass der Wirksamkeit der statischen Paketfilter doch recht enge Grenzen gesetzt sind. Daher wurden Paketfilter entwickelt, bei denen sich die Filterregeln dem jeweiligen Systemzustand anpassen. Diese werden als **dynamische Paketfilter** bezeichnet. Bezogen auf das obige Beispiel werden die abgehenden Pakete in gleicher Weise geprüft. Aber die konkrete Quellport-Nummer wird nun zur Aktualisierung der Filterregeln für eingehende Pakete genutzt. Diese Form der Paketfilterung wird auch „Stateful Inspection" bezeichnet. Die Formulierung der Filterregeln für dynamische Paketfilter ist eine recht anspruchsvolle Aufgabe.

Proxies

Einen völlig anderen technischen Ansatz verkörpern die Proxies. Der Begriff Proxy kann dabei mit „Stellvertreter" übersetzt werden. Softwareseitig können Proxies sowohl auf der Transportschicht als auch auf der Anwendungsschicht (Bild ❸a) arbeiten.

- Proxies, die auf der Anwendungsschicht arbeiten, werden als „Application Level Gateway" bezeichnet. Für jeden Dienst der Anwendungsschicht muss in diesem Fall ein gesonderter Proxy (z. B. HTTP-Proxy, SMTP-Proxy) installiert sein.
- Ein auf der Transportschicht arbeitender Proxy (z. B. SOCKS-Proxy) wird als „Circuit Level Gateway" bezeichnet und kann mehrere Dienste der Anwendungsschicht bedienen.

Um sich die Funktion von Proxies zu veranschaulichen, ist dieser Unterschied jedoch nicht massgeblich.

Die Stellung und Funktion des Proxies veranschaulicht Bild ❸b. Eigentlich liegt den Diensten im Internet immer das Client-Server-Prinzip zugrunde. Ein System (der Server) stellt Dienste bereit und ein anderes System (der Client) nimmt diese Dienste in Anspruch. Der Proxy steht nun als drittes Element zwischen Client und Server. Gegenüber dem Client nimmt der Proxy die Rolle des Servers ein, daher wird manchmal auch von Proxy-Server gesprochen. Gegenüber dem „eigentlichen" Server verhält sich der Proxy wie ein Client. Neben der Tatsache, dass Proxies eine wesentlich detailliertere Kontrolle des Datenverkehrs erlauben, wird durch deren Einsatz eine Abschirmung des dahinter liegenden Netzes erreicht, da nach aussen nur die IP-Adresse des Proxy bekannt ist. Darüber hinaus können an dem als Proxy fungierenden Rechner wiederum Maßnahmen ergriffen werden, um ihn gegen unerlaubte Zugriffe zu schützen. Typische Maßnahmen in diesem Zusammenhang sind:

- Entfernung von Betriebssystembestandteilen, die der Proxy zum regulären Betrieb nicht benötigt,
- Booten des System von CD-ROM (oder einem anderen Nur-Lese-Speicher) statt von einer Festplatte.

Damit kann der Missbrauch von Diensten und das Einschleppen von schädlichen Programmen [3] (z. B. Trojaner) weitestgehend verhindert werden.

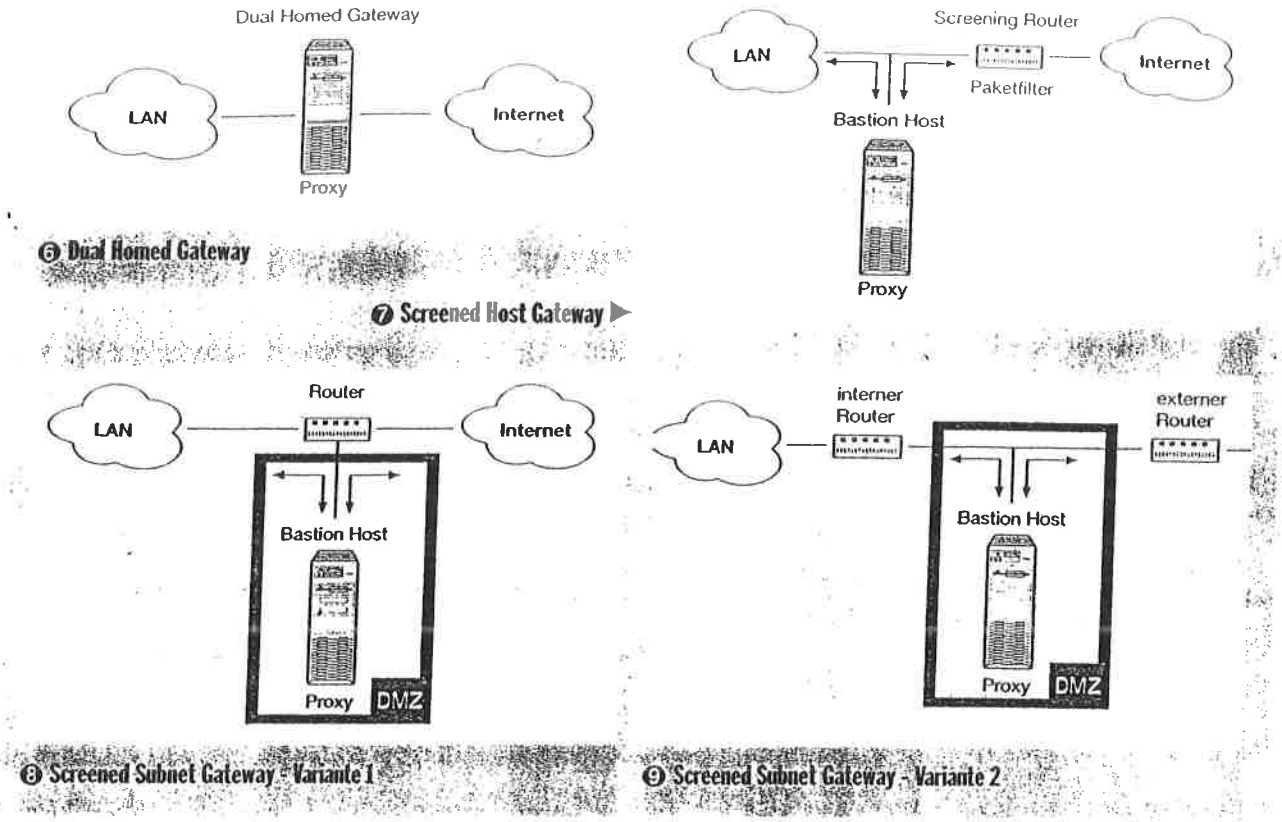
Eine solcherart „gehärtete" Station wird im Zusammenhang mit Firewalls auch als Bastion Host bezeichnet.

Adressumsetzung

Die Adressumsetzung (NAT – Network Adress Translation) ist ursprünglich kein Firewall-Konzept, im Gegensatz zu den zuvor besprochenen Paketfiltern bzw. Proxies. Da aber bei der Adressumsetzung die internen Adressen der Rechner eines Netzes nach aussen nicht sichtbar sind, stellt diese Verfahrensweise eine sinnvolle Ergänzung der anderen Möglichkeiten dar. Zwangsläufig wird die Adressumsetzung vor allem in kleinen Firmen verwendet. Dort wird innerhalb des lokalen Netzes mit privaten IP-Adressen (Bild ❹) gearbeitet. Lediglich der Router, über den die Einwahl ins Internet erfolgt, bekommt eine öffentliche Adresse zugewiesen. Die Verbindungen zwischen Client und Router bzw. zwischen Router und Server werden über eine Tabelle definiert. Diese enthält

- die private IP-Adresse des Clienten,
- dessen Portnummer sowie
- die dieser Verbindung zugeordnete Portnummer des Routers.

Von der Adressumsetzung wird vor allem im Zusammenhang mit dem Einsatz von Paketfiltern Gebrauch gemacht.



❻ Dual Homed Gateway ❼ Screened Host Gateway ▶

❽ Screened Subnet Gateway - Variante 1 ❾ Screened Subnet Gateway - Variante 2

Typische Konfigurationen

Auf der Grundlage von Paketfiltern und Proxies haben sich einige typische Firewall-Konfigurationen in der Praxis durchgesetzt. An dieser Stelle sei noch einmal ausdrücklich darauf hingewiesen, dass eine Firewall immer eine Kombination von Hard- und Software ist und diese verschiedenen Kombinationsmöglichkeiten auch begrifflich unterschieden werden.

Screening Router

Der Screening Router ist ein Router, der gleichzeitig auch Paketfilter (Bild ❺) ist. Er realisiert die einfachste Variante einer Firewall. Dieser Router ist an der Grenze zwischen dem zu schützenden Netz und dem Netz, aus dem ein Angriff vermutet wird, angeordnet. Das damit erreichbare Schutzniveau ist gering, da die Firewall lediglich aus dem auf dem Router installierten Paketfilter besteht.

Dual Homed Gateway

Werden das zu schützende Netz und das Netz, aus dem ein Angriff erwartet wird, über einen Proxy miteinander verbunden, wird diese Konfiguration als Dual Homed Gateway (Bild ❻) bezeichnet. Der Begriff leitet sich aus der Tatsache her, dass der Proxy sowohl Bestandteil des LAN als auch des Internets (Dual Homed) ist und den Übergang (Gateway) zwischen beiden ermöglicht. Obwohl dieser Konfiguration ein höheres Schutzniveau zugebilligt wird als dem Screening Router, besteht ein deutlicher Schwachpunkt. Als Nachteil dieser Konfiguration erweist sich, dass der Proxy sowohl direkt aus dem äusseren als auch aus dem inneren Netz angegriffen werden kann.

Screened Host Gateway

Eine Kombination von Paketfilter und Proxy stellt das Screened Host Gateway (Bild ❼) dar. Der Proxy ist in diesem Fall Bestandteil des zu schützenden Netzes. Über den Router erfolgt einerseits eine Paketfilterung und andererseits sorgt der Router dafür, dass alle ankommenden Datenpakete dem Proxy zugestellt werden. Die Stationen des zu schützenden Netzes kommunizieren nur über den Proxy mit der Aussenwelt. Gegenüber Angriffen aus äusseren Netzen ist der Bastion Host hier zwar zusätzlich geschützt, aber nicht gegen Angriffe von innen.

Screened Subnet Gateway

Wird nun der Proxy noch aus dem zu schützenden Netz herausgelöst und in einem separaten Netz (Bild ❽) angeordnet, dann wird diese Konfiguration als Screened Subnet Gateway bezeichnet. Der Router wirkt wiederum als Paketfilter und sorgt gleichzeitig dafür, dass der gesamte Datenverkehr zwischen dem internen Netz und dem Internet über den Bastion Host geleitet wird.

Demilitarisierte Zone – DMZ. Das Subnetz des Bastion Hosts kann auch als Zwischennetz (Bild ❾) zwischen dem zu schützenden Netz und dem Netz, aus dem die Angriffe erwartet werden, ausgeführt sein. In diesem Fall ist ein weiterer Router nötig. Für die separaten Netze, in denen die Bastion Hosts in den Bildern ❽ und ❾ angeordnet sind, ist der Begriff demilitarisierte Zone (DMZ) gebräuchlich.

Überwachung der Schutzwirkung

Nicht einmal nach der Installation einer Firewall kann ein Einbruch in das Datennetz mit Sicherheit ausgeschlossen werden. Deshalb werden zusätzlich Programme eingesetzt, die dazu dienen, Angriffsversuche zu erkennen. Die Wirksamkeit dieser Einbruchserkennungssysteme (Intrusion Detection System – IDS) beruht auf der Annahme, dass Angriffsversuche durch Anomalien beim Datenverkehr und an bestimmten Angriffsmustern (ähnlich wie bei Viren) erkennbar sind.

IDS-Software überwacht den Datenverkehr und signalisiert Anomalien und be-

Fortsetzung auf Seite 22

Fortsetzung von Seite 19

reits bekannte Angriffsmuster. Die Auswertung der so gesammelten Informationen ermöglicht es, ggf. Angriffsversuche noch rechtzeitig zu erkennen. In den zum Schutz von Einzel-PCs verfügbaren Personal-Firewall sind einfache Formen dieser Überwachung integriert. Beispielsweise wird angezeigt, ob der Rechner aus dem Internet heraus nach offenen Ports abgesucht wird.

Security-Checker. Eine andere Programmkategorie, sogenannte Security-Checker, ist speziell dazu geschaffen worden, Firewalls auf ihre Wirksamkeit hin zu testen. Sie sollen gezielt Schwachstellen offenbaren. Aber bei diesen Programmen liegt Gut und Böse nahe beieinander. Auch wenn die Programme im Internet frei verfügbar sind, kann deren ungeschickte Handhabung strafrechtliche Konsequenzen haben.

Fazit

Die Einrichtung von Firewalls ist eine technische Maßnahme, die die Gefahr zwar minimiert, aber keinen 100%-igen Schutz gewährleisten kann. Je aufwändiger die technischen Schutzeinrichtungen sind, umso komplizierter wird deren Handhabung. In vielen Fällen sind deshalb einfache organisatorische Maßnahmen wie Netztrennung und Nutzungsbeschränkung langfristig wirkungsvoller. Zur Vertiefung des Wissens über die Zusammenhänge zwischen Computeranwendungen, Firewall usw. sind besonders die Schriften [2], [4], [5] und [6] anzuraten.

Literatur:

[1] *Möbus, H.*: Datensicherheit und -schutz; Teil 1: Begriffe und Grundzusammenhänge. Berlin: Elektropraktiker 56(2002)10 Lernen und Können S. 16 bis 19.

[2] *Barth, W.*: Das Firewall Buch; Grundlagen, Aufbau und Betrieb sicherer Netze mit Linux. Nürnberg: SuSE PRESS 2001.

[3] *Möbus, H.*: Datensicherheit und -schutz; Teil 2: Viren und Angriffe aus dem Netz. Berlin: Elektropraktiker 56(2002)11 Lernen und Können S. 17 bis 19.

[4] *Fischer, St., Walter, U.*: Linux-Netzwerke; Aufbau, Administration Sicherung. Nürnberg: SuSE PRESS 2000.

[5] *Röhrig, B.*: Linux im Netz, Das Handbuch zu LAN und WAN. Vaterstetten: C&L Verlag 1997.

[6] *Casselberry, R.*: Das perfekte Intranet. Haar: Verlag Markt&Technik 1997.

H. Möbus

Suchen Sie Informationen für Hardware-Firewall`s im Internet zu folgenden Themen:

- Paketfilter
- Content-Filter
- Proxy
- Application-Level-Firewall
- Stateful inspection