Universität Ulm - SAI

Seminararbeit

zum Thema

Firewalls

bearbeitet von: Frank Weidlich

betreut von: Prof. Dr. Franz Schweiggert

und Dr. Matthias Grabert

Ulm, Juli 2003

Inhaltsverzeichnis

1. Einleitung

Jede Organisation, ob sich nun um eine Behörde, eine Schule oder ein privates Unternehmen handelt, verfügt über eine enorme Menge an Informationen, die wenn sie in falsche Hände geraten, schwerwiegende Folgen für die Betroffenenen nach sich ziehen können. Ich denke hier vor allem an Informationen wie Krankheitsdaten, unternehmensinterne Daten (z.B. Höchstgebot bei UMTS-Lizenz-Versteigerung, u.a.), aber auch schon die Offenlegung von Gehaltsinformationen kann für viele Einzelne sehr unangenehm sein.
Gleichzeitig ist nicht nur die Weitergabe von Informationen für die Organisation ein enormes Problem, sondern die Zerstörung oder Modifikationen von Daten ist als mindestens genauso problematisch anzusehen. Ganz zu schweigen von den Auswirkungen, wenn ein Angreifer die Kontrolle über das ganze System bekommt.
Es besteht also hoffentlich kein Zweifel, dass der IT-Sicherheit eine elementare Wichtigkeit eingeräumt werden muss. Ich möchte nun in meinem Seminar auf das Konzept/Produkt/Einrichtung "Firewall" näher eingehen, um den Leser einen grundlegenden Einblick darüber zu geben.

1.1 Was ist eine Firewall?

Eine Firewall ist eine Einrichtung, die auf Netzwerkebene als Zugriffssteuerungs-mechanismus für ein oder mehrere bestimmte Netzwerke eingesetzt wird. In den meisten Fällen dienen Firewalls dazu, Unbefugten den Zugriff auf ein internes Netzwerk zu verweigern. Firewalls werden aber auch dazu verwendet, um innerhalb von LANs sichere Subnetze (z.B. für eine Entwicklungsabteilung) zu schaffen. Meistens sind Firewalls eigenständige Computer, Router oder sonstige Hardwaregeräte mit z.T. spezieller Software. Firewalls sind als Kontrollpunkte für das Netzwerk gedacht. Wenn Verbindungsanfragen gestellt werden, dann werden diese von der Firewall bearbeitet. Basierend auf einem vordefinierten Satz von Regeln (auch Richtlinien genannt) wird festgelegt, ob der Datenaustausch zulässig ist oder nicht.
(Vgl. anonymous, S.244f)

2. Firewall-Typen

2.1 Packet Filtering Firewall

Packet Filtering Firewalls (bzw. Paket Filter) sind oft Router, die über Funktionen zur Paketfilterung verfügen. Der Router bekommt Pakete von einem Netzwerk und leitet sie an ein anderes Netzwerk weiter. Zuvor vergleicht er die Pakete mit den vom Admininstrator definierten Regeln. Abhängig vom TCP- und IP-Header der Pakete und von den Regeln kann die Firewall das Paket ablehnen, es weiterleiten oder eine Nachricht zum Ursprung zurücksenden. Ein Ereignis, das gegen Filterregeln verstößt, wird protokolliert.

Kontrollmöglichkeiten der Firewall:

- Auf der Netzzugangsebene (im Intranet) werden Quell-, Zieladressen und der verwendete Protokolltyp kontrolliert.
- Auf der Netzwerkebene werden beim IP-Protokoll die Quell- und Zieladresse, sowie das Optionsfeld und Flags überprüft, außerdem die ICMP-Kommandos und die physikalische MAC-Adresse.
- Auf der Transportebene werden bei TCP und UDP die Portnummern kontrolliert, bei TCP zusätzlich die Richtung des Verbindungsaufbaus.

(Vgl. Pohlmann, S. 119ff)

Grundsätzlich können die Filterregeln generell entweder als Gebotsregeln oder als Verbotsregeln ausgelegt werden:

- Bei den Gebotsregeln ist alles, was nicht explizit erlaubt ist, verboten.
- Bei den Verbotsregeln ist alles, was nicht explizit verboten ist, erlaubt.

Dabei ist die erste Regel der zweiten Regel vorzuziehen , da diese wesentlich strenger in der Auslegung ist.

Stärken von Paket Filtern:

Paketfilterung ist eine kostengünstige Technologie mit recht guter Performance. Ein Paketfilter ist heute auf fast allen Router-Produkten standardmäßig implementiert. Oft ist kein zusätzlicher Administrations- und Konfigurationsaufwand notwendig. Paket Filter sind leicht erweiterbar, wenn neue Dienste oder Protokolle transportiert werden müssen (hinzufügen neuer Regeln reicht im Normalfall).

Schwächen von Paket Filtern:

Paketfilterregeln sind für den Durchschnittsbenutzer oft recht verwirrend. Bei großen Netzen können Filterregeln sehr umfangreich und schwer nachvollziehbar werden. Protokollmeldungen enthalten oft keine Informationen über den Inhalt der übertragenen und verworfenen Pakete. Einige Protokolle sind für Paket Filter ungeeignet, da variable Portnummern verwendet werden. Des Weiteren besitzen Portnummern und IP-Adressen eine unzureichende Integrität der, da diese leicht gefälscht werden können (IP-Spoofing). Ein weiterer Nachteil ist die fehlende Benutzerauthentifizierung und die fehlende Kontrolle der Inhalte der Datagramme.

2.2 Proxys bzw. Application Gateways

Ein Application Gateway trennt das sichere und das unsichere Netzwerk physisch, indem es zwei Netzwerkanschlüsse hat (einen Anschluss für das sichere und einen für das unsichere Netzwerk). Die logische Trennung zwischen dem sicheren und dem unsicheren Netzwerk wird dadurch realisiert, dass Benutzer im sicheren Netzwerk Kommunikationsanfragen und Daten an den Application Gateway richten, der Application Gateway die Kommunikationsanfragen und Daten analysiert und, wenn es die Sicherheitspolitik der Unternehmung erlaubt, diese an die eigentlichen Empfänger im unsicheren Netzwerk - stellvertretend für die Benutzer im sicheren Netzwerk - weiterleitet. Andersherum nimmt der Application Gateway auch Kommunikationsanfragen und Daten aus dem unsicheren Netzwerk entgegen, analysiert sie und leitet diese, unter Beachtung der Sicherheitspolitik der Unternehmung, an die eigentlichen Empfänger im sicheren Netzwerk, stellvertretend für die Kommunikationspartner im unsicheren Netzwerk, weiter. (Vgl. Pohlmann S. 146 f.; Hegering S. 197 ff.)

Für jeden Dienst ist ein spezifisches Proxyprogramm auf dem Proxy-Server erforderlich (z.B. FTP). Im Gegensatz zu Paket Filtern ist eine Nutzdatenanalyse möglich, das heißt, Daten können analysiert und z.B. nach bestimmten Schlüsselwörtern durchsucht werden (z.B. E-Mail, HTML-Seiten). Einige HTTP-Proxys bieten sogar die Möglichkeit, alle Zeilen innerhalb einer Seite, die zu Java-Applets gehören, zu löschen. Des weiteren können bestimmte Dienstmerkmale eingeschränkt werden. Meist ist eine Cache Funktionalität für Webseiten verfügbar. Im Gegensatz zu Paket-Filtern wird mit Application Gateways eine verlässliche Trennung zwischen unterschiedlich vertrauenswürdigen Netzwerk-

segmenten erreicht. Manipulierte Pakete werden zuverlässig abgefangen und entsprechend protokolliert.

Stärken von Proxys / Application Gateways:

- Bieten ein hohes Maß an Sicherheit
- Sehr umfangreiche Protokollierung möglich
- Authentisierung des Benutzers
- Granularität auf Dienstebene
- Dienste können benutzerabhängig erlaubt werden
- Verbindung zwischen dem zu schützenden Netz und dem Internet wird durch den Application Gateway völlig entkoppelt

Schwächen von Proxys / Application Gateways:

- Höherer Rechenaufwand nötig
- Wenig skalierbar
- Bei neuentwicklten Protokollen kann es (vorläufig zumindest) noch keinen entsprechenden Proxy geben

2.3 Andere Firewall Systeme:

2.3.1 Stateful Packet Filter Firewall (SPF)

Diese Firewalls basieren grundsätzlich auf dem Konzept der Paketfilterung, erweitern dieses aber noch um einige Aspekte. Auf diesem Modell beruhende Firewalls überwachen die Sitzungen und Verbindungen mit Hilfe interner Zustandstabellen und können dementsprechend sofort reagieren. Aus diesem Grund sind SPF-basierte Produkte flexibler als reine Paketfilterlösungen. Außerdem schützen die meisten SPF-basierten Firewalls auch vor bestimmten DoS-Angriffen[1] und stellen für SMTP-basierte Maildienste und andere sicherheitsrelevante Funktionen erweiterte Sicherheitsvorkehrungen bereit. (Vgl. anonymous, S. 251)

[1]Denial of Service -Angriffe: Nichtverfügbarkeit von Diensten

Mit SPF-basierten Firewalls kann man beispielsweise standardmäßig alle Ports über 1024 schließen. Diese Ports werden dann nur bei Bedarf geöffnet. (siehe auch Kap 4. Linux-Firewall)

2.3.2 Stateful Inspection Firewall

Stateful Inspection Firewalls kombinieren die Vorteile der Paketfilter- sowie der Proxy-Firewalls. Das Client/Server-Modell wird hier im Gegensatz zur Application Gateway-Firewall nicht durchbrochen, d.h. es schaltet sich kein Proxy zwischen den Client und den Server. Zuerst agiert diese Firewall vergleichbar mit einem Paket Filter. Dann werden zustandsbezogene Informationen aus den Anwendungsschichten extrahiert und in dynamischen Tabellen aufbewahrt, um damit nachfolgende Verbingungsaufbauversuche bewerten zu können. Hierbei werden nicht nur die Ports und Adressen untersucht, sondern auch der Datenstrom. Stateful Inspection Firewalls liegen in ihrer Performanz zwischen den Paketfilter- und Proxylösungen. Sie sind eine Erweiterung der SPF-Firewalls (diese können den Datenstrom nicht untersuchen).

3. Firewalls im praktischen Einsatz

(Vgl. Pohlmann, S.189ff)

Allgemeine Grundsätze bei der Verwirklichung/ Implementation einer Firewall:

- Position der eingesetzten Geräte sollte möglichst weit außen sein
- Bei stark zu schützenden Netzen sollten Geräte redundant eingesetzt werden
    - Unterschiedliche Hersteller
    - Unterschiedliche Filterformate

Anzahl und Art der Firewallkomponenten sollte dem Sicherheitskonzept angepasst sein.

3.1 Ausschließlicher Einsatz von PaketFiltern

Dieses Konzept ermöglicht folgende Sicherheitsziele:

- Zugangskontrolle auf Netzzugangs- und Netzwerkebene (nur erlaubte logische Verbindungen können aufgebaut werden)

- Rechteverwaltung (Zugriff nur über erlaubte und definierte Protokolle und Ports)
- Protokollauswertung
- Alarmierung

Reine Packet Filter Lösungen bieten relativ wenig Schutz, um zu schützende Netze mit unsicheren Netzen zu koppeln (z.B. Gefahr durch Spoofing).

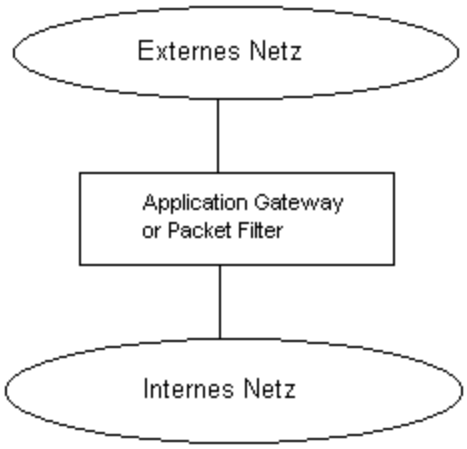


Abb. zu Abschnitt 3.1 und 3.2

3.2 Ausschließlicher Einsatz von Proxys

Hierdurch werden folgende Sicherheitsziele ermöglicht:

- Zugangskontrolle auf Netzwerkebene (s.o.)
- Rechteverwaltung (s.o. und nur solche Dienste sind möglich, für die ein Proxy eingerichtet wurde)
- Zugangskontrolle auf Benutzerebene (Benutzer können identifiziert und authentisiert werden)
- Kontrolle auf der Anwendungsebene (spezielle Anwendungsfilter für Kommandos, Anwendungsdaten und Dateien)
- Entkoppelung der Dienste (risikobehaftete Programme werden nur indirekt über Proxys dem unsicheren Netz zur Verfügung gestellt (z.B. Sendmail))
- Protokollauswertung und Beweissicherung (zusätzliche Beweissicherung von Handlungen einzelner Benutzer)
- Alarmierung
- Verbergen der internen Netzstruktur

Mit diesem Konzept können zwei Netze mit vergleichbarem Schutzniveau verbunden werden (z.B. Kooperation zweier gleichwertiger Organisationen).

3.3 Kombination von Paket Filter und Application Gateway

Um die Sicherheit zu erhöhen verbindet man hier einfach die beiden unterschiedlichen Firewalls. Der Weg aus dem unsicheren Netz in das zu schützende Netz läuft hier zuerst durch den Paket Filter und anschließend durch das Application Gateway. Es gibt keine Möglichkeit, das Application Gateway zu umgehen. Da beide Elemente mit unterschiedlichen Einbindungs- und Analysekonzepten arbeiten, werden sämtliche Sicherheitsziele erreicht und eine äußerst hohe Gesamtsicherheit realisiert. Sie verbinden die Vorteile der paketbasierten wie der proxybasierten Firewalls. Allerdings sind die Kosten höher und die Wartung und Einrichtung ist aufwendiger.

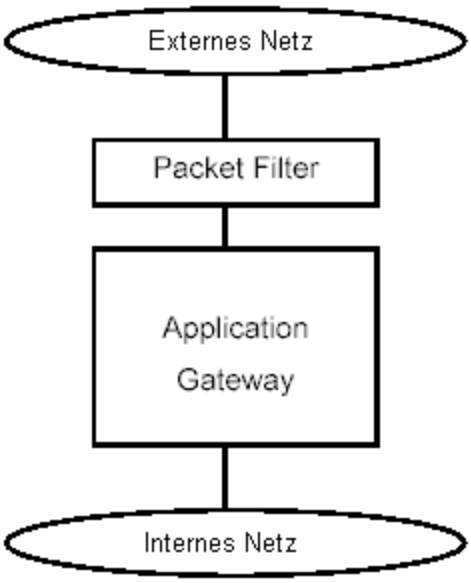


Abb. zu Abschnitt 3.3

3.4 De-Militarized Zone (DMZ)

Hier bedindet sich der Application Gateway im sog. Screened Subnet und wird aus den beiden angeschlossenen Netzen jeweils durch Paket Filter geschützt. Aus der Sicht der Paket Filter kommuniziert immer nur der Application Gateway mit dem jeweils

gekoppelten Netz, wodurch ihre Filterregeln einfach und überschaubar konfiguriert werden können. Durch die Anordnung muss ein Angreifer jetzt drei Barrieren überwinden, um in das zu schützende Netz zu gelangen. Es ist üblich, für die verschiedenen Elemente unterschiedliche Betriebssysteme einzusetzen, um evtl. Betriebssystemfehler oder Lücken auszugleichen. In diesem System können sämtliche Protokollebenen kontrolliert und analysiert werden. Es ist dafür geeignet, zu schützende Netze an sehr unsichere Netze, wie das Internet, zu koppeln. Im Screened Subnet ist es möglich, Internet Server z.B. zwischen den oberen Paket Filter und den Application Gateway oder direkt an den Gateway anzuschließen. Die Netze bleiben über den Application Gateway dabei immer vollständig entkoppelt.

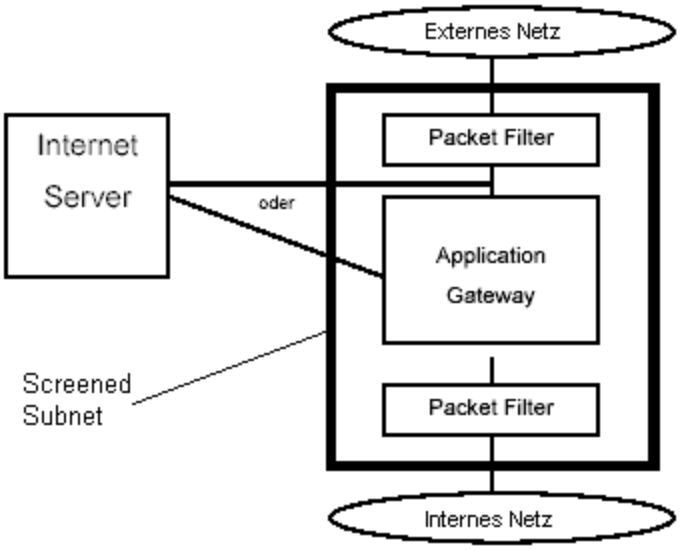


Abb. zu Abschnitt 3.4

Vorteile der Screened Subnet Architektur:

- Gute Skalierbarkeit
- Es müssen zwei Paket Filter überwunden werden (womöglich sogar unterschiedlicher Bauart)

Nachteile der Screened Subnet Architektur:

- Höhere Kosten
- Hoher Administrationsaufwand

4. Linux-Firewall

4.1 Allgemeines

Linux hat, im Gegensatz zu den meisten anderen Betriebssystemen, die Funktionalität der Firewall bereits im Betriebssystemkern (Kernel) fest eingebaut. Das macht die Firewall sowohl stabiler, als auch wesentlich schneller, als wenn sie in dem so genannten Userspace realisiert werden müsste.
Mit der Kernel 2.4 wurde auch die Firewall grundlegend überarbeitet, da die Vorgängerversion nicht mehr auf dem aktuellen Stand der Paketfilter-Technik war. Es wurde ein neues Firewall-Modul namens „Netfilter“ für den Kernel entwickelt. Die Entwickler bezeichneten ihr Werk als „Framework für die Manipulation von Datenpaketen“. Firewall-Entwickler bekommen mit ihm die Basisfunktionen zur Erweiterung von Netfilter an die Hand, ohne sich mit Kernelprogrammierung befassen zu müssen. Zwei grosse Vorteile von Netfilter sind:

- Das Framework selbst ist vollkommen protokoll-unabhängig und damit beliebig erweiterbar.
- An wesentlich weniger Stellen als bisher wird in den Kernel-Code eingegriffen, um die Firewall-Funktionalität unterzubringen, als dies vorher der Fall war. Damit ist der zurzeit vorliegende Code auch wesentlich besser wartbar als seine Vorgänger.

4.2 Grundsätzlicher Aufbau

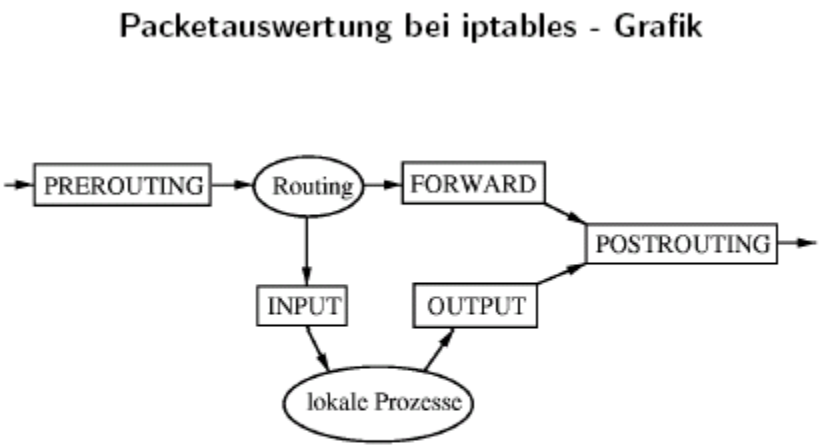
Die Firewall arbeitet mit einer Liste von Annahme- oder Ablehnungskriterien. Daraus entstehen so genannte Regeln, die genau bestimmen, ob ein Paket passieren darf oder nicht.

Nach folgenden Kriterien werden die Regeln aufgebaut:

- Netzwerkschnittstelle
- IP Adressen
- TCP/UDP Portnummern bzw. ICMP Nachrichtentypen
- SYN- und ACK-Flag

Netfilter ist also eine Serie von Regelketten (Chains) auf bestimmten Positionen in einem Protokoll-Stack wie das bereits beim Kernel 2.2.x der Fall war.

Kernelmodule können sich registrieren, um an irgendeiner dieser Regelketten zu lauschen. Wenn diese Netfilter Regelkette dann vom Networking-Code aufgerufen wird, hat an diesem Punkt jedes registrierte Modul die Möglichkeit, das Paket zu verändern. Der wesentlichste Unterschied zum Kernel 2.2.x bezüglich des Aufbaus der Firewall ist der, dass die Regelketten innerhalb des Protokoll-Stacks eine andere Position eingenommen haben und somit der Weg der Pakete durch die Firewall grundlegend verändert wurde. Durch die Veränderung des Weges, ändert sich somit auch der ganze Ablauf, welcher bei Netfilter wesentlich logischer aufgebaut ist als der Ablauf im Kernel 2.2.x.



Paketauswertung und -modifikation bei iptables

(entnommen aus Schreiber S. 6)

Doch nicht nur der Ablauf hat sich verändert, sondern auch an der Struktur der Firewall wurden diverse Veränderungen vorgenommen.

4.2.1 Tabellen

In der Netfilterarchitektur gibt es drei Tabellen. Diese Tabellen haben den Zweck, die verschiedenen Arten der Paketbehandlung auf Module verteilen zu können und nur die Module zu laden und damit auch nur die Tabellen mitzuführen, die im Augenblick, beziehungsweise für die gestellte Anforderung, benötigt werden.

Die drei Tabellen sind:

- Filter: Die Standard-Tabelle, die immer dann verwendet wird, wenn keine Tabelle explizit angegeben wird. Die Hauptaufgabe besteht aus dem Herausfiltern unerwünschter Datenpakete.
- Nat: Diese Tabelle ist für alle Arten von Adress-Umsetzungen oder Port-Forwarding verantwortlich.
- Mangle: In dieser Tabelle werden spezielle Änderungen an Paketen vorgenommen (z.B. Veränderung von Parametern wie time to live).

(Vgl. Thüring, S.11)

4.2.2 Chains

Jede Tabelle besteht aus mehreren, in seiner Funktion vordefinierten Regelketten. In den einzelnen Chains werden die einzelnen Regeln definiert, welche für die Pakete gelten sollen. Im Gegensatz zur alten Architektur, gibt es grundsätzlich fünf und nicht mehr drei, von der Architektur gegebene, Chains. Die fünf vorgegebenen Chains sind:

- INPUT: Hier landen alle Pakete, die an einen lokalen Prozess gerichtet sind.
- OUTPUT: Hier laufen alle Pakete durch, die von einem lokalen Prozess stammen.
- PREROUTING: Unmittelbar, bevor eine Routing-Entscheidung getroffen wird, müssen die Pakete hier durch.
- FORWARD: Behandelt alle zu routenden Pakete
- POSTROUTING: Alle Pakete, die geroutet werden, laufen nach dem Routing hier durch.

(Vgl. Thüring, S.11f)

Neben den fünf vordefinierten Chains, können auch beim Netfilter eigens definierte Chains erzeugt werden, in denen spezielle Regeln eingetragen werden können.

4.2.3 Tabellen-Chain Struktur

Da eine grosse Anzahl an Kombinationen zwischen Chains und Tabellen gebildet werden können, war es bei der Entwicklung wichtig eine Struktur zu bilden, welche nur die erlaubten beziehungsweise möglichen und sinnvollen Kombinationen beinhaltet

Hier ist eine Liste mit den verschiedenen Kombinationen:

- Filter/INPUT: Hier landen alle Pakete, die an einen lokalen Prozess gerichtet sind. Damit lassen sich Zugriffe auf lokale Prozesse perfekt regulieren, z.B.:
  -Zugriff auf einen lokal laufenden Server nur aus bestimmten Netzen
  -nur Pakete durchlassen, die zu einer bestehenden Verbindung gehören
- Filter/OUTPUT: Hier gehen alle Pakete durch, die von einem lokalen Prozess erzeugt wurden. Damit lassen sich lokale Prozesse nach aussen schützen, z.B.:
  -keine ausgehenden "verdächtigen" Verbindungen am Server -
  -keine "losen" Pakete nach draussen -- nur gültige Verbindungen
- Filter/FORWARD: Durch diese Chain gehen alle Pakete durch, die durch diese Maschine geroutet werden. Hiermit lassen sich also alle Rechner in jeweils dem Zielnetz des Routing schützen, z.B.:
  -kein UDP nach aussen, ausser DNS
  -keine öffnenden Verbindungen nach innen
  -Pakete, die zu keiner Verbindung gehören, werden gefiltert
- Nat/PREROUTING: Wenn Adress-Übersetzungen durchgeführt werden, müssen alle Pakete vor dem Routing hier durch. Hier lassen sich für zu routende Pakete verändern:
  -die Ziel-IP-Adresse
  -der Ziel-Port
- Nat/OUTPUT: Vom lokalen Rechner stammende Pakete gehen hier durch; gleiche Veränderungen wie Nat/PREROUTING.
- Nat/POSTROUTING: Hier gehen nochmals alle Pakete durch (auch lokal erzeugte Pakete) die geroutet worden sind. Hier werden Angaben über die Herkunft eines Paketes verändert, wie:
  -Quell-IP-Adresse
  -Masquerading (Sonderform von Quell-IP-Änderung)
- Mangle/PREROUTING & Mangle/OUTPUT:
  ähnlich den "nat" chains, nur mit dem Unterschied, dass hier spezielle Paket-Parameter geändert werden können, wie:
  - die TTL (Time to live)

(Vgl. Thüring, S.12f)

4.2.4 Statefull Firewalling

Der grösste Fortschritt ist sicher das "connection tracking". Netfilter überwacht Verbindungen und ordnet ihnen einen der vier Verbindungszustände NEW, ESTABLISHED, RELATED und INVALID zu. Die Erkennung von nicht zu einer Verbindung gehörenden Paketen und ihre Validierung durch den Kernel erhöhen die Sicherheit beträchtlich. Es muss also nicht mehr wie bei der Vorgängerversion alle Ports > 1024 aufgemacht werden, wenn nicht genau definiert ist, wo zum Beispiel die Antwortpakete von einem bestimmten Service hinein kommen. In der INPUT-Chain Regel wird einfach nur noch definiert, dass nur Pakete von aussen hereingelassen werden dürfen, die auch zu einer von innen aufgebauten Verbindung gehören.

5. Grenzen von Firewalls

Dieser Abschnitt soll erläutern, vor welchen Gefahren auch Firewalls nicht schützen können:

- Bei Angreifern aus dem internen Netz kann die Firewall nichts ausrichten. Wenn die Daten nicht über die Firewall geroutet werden, ist diese natürlich machtlos. Ein mögliches Szenario für diesen Fall wäre z.B. das ein Angreifer schon Zuggang zu einem Rechner im internen Netz hat. Jetzt kann er neue Angriffe auf andere Rechner im internen Netz starten, die alle nicht die Firewall passieren müssen, und deshalb erst mal unerkannt und unverhindert bleiben.
- Eine weitere Bedrohung sind Viren. Diese werden meist in ausführbaren Dateien oder eMails von Rechner zu Rechner übertragen und sind somit für die Firewall nicht automatisch zu erkennen. Aber auch hier gilt wieder einschränkend zu sagen, dass manche Virenangriffe (besonders von Würmern via http) zu verhindern sind, wenn der angreifende Virus oder Wurm eine eindeutige Signatur hat, also von der Firewall erkannt werden kann. Hierzu gehören Merkmale wie z.B. die URL, die aufgerufen wird.
- Eine weitere Angriffstaktik, gegen die Firewalls nichts ausrichten können, ist das so genannte Social Engineering . Dabei werden Angestellte vom Angreifer auf geschickte Weise ausgehorcht, in dem der Angreifer zum Beispiel anruft und vorgibt aus der Firma zu sein (bei großen Firmen sehr einfach) und nach Einstellungen, Passwörtern, Geburtstagen oder ähnlichen Daten fragt, die bei einem Einbruch hilfreich sein könnten. Da der Angreifer sich nachher eventuell bei der Firewall mit den

gewonnenen Daten authentifizieren kann, wird er nicht als Eindringling erkannt. (Vgl. Hardt/Tümmel S.18f)

6. Andere Sicherheitssysteme

Nachfolgend möchte ich kurz andere Sicherheitssysteme nennen. Diese sind z.T. in einer Firewall bereits implementiert.

- Intrusion Detection Systeme:
  Sie dienen der Erkennung von Angriffen. Dies geschieht z.B. durch Untersuchung von rohen Datenpaketen auf bekannte Angriffsmuster oder durch Untersuchung von Systemprotokollen.
- Scanner:
  Dies sind Erkennungstools für Sicherheitslücken. Der Scanner sucht dabei nach Schwachpunkten (aus einer Datenbank bekannt). Beispielsweise gibt ein Portscanner eine Liste mit allen offenen Ports zurück
- Protokollierung:
  Sie dient der Aufdeckung von Anomalien im Netzwerk und später zum Beweisen von betimmten Sachverhalten vor Gericht. Es ist darauf zu achten, dass der Cracker die Protokolldateien nicht modifizieren kann. Die Protokollierung ist mehr oder weniger in einer Firewall intergriert.

7.Trends

7.1 Firewalls basierend auf künstlicher Intelligenz

Die Grundlagenforschung im Bereich Computersicherheit beschäftigt sich seit einiger Zeit auch mit der Einbeziehung von Expertenssystemen in die Architektur von Firewall-Systemen. Dem Szenario von sich ständig ändernden Angriffsmethoden und neu hinzukommenden Sicherheitslücken wird versucht, mit Angriffserkennungsmethoden, die selbstlernende Strukturen wie neuronale Netzwerke oder Entscheidungsbäume

benutzen, zu begegnen. Erste Prototypen von intelligenten Firewalls wurden im Labormaßstab bereits getestet. (Vgl. Kyas, S.327)

7.2 Post-Firewall Ära

In welchem Ausmaß Firewall-Syseme auch in Zukunft als zentrale, für ein gesamtes Netzwerk zuständige Einheit realisiert werden müssen, läßt sich heute noch nicht abschätzen. Mit der zunehmenden Leistungsfähigkeit der Prozessoren rückt jedenfalls das Szenario von Comtputer-Systemen, die genügend Reserven an Rechenleistung besitzen, um sich selbst mit Hilfe von leistungsfähigen Authentifikations- und Verschlüsselungsmechanismen zu schützen, näher. Jedes einzelne System wird dann Daten ausschließlich über gesicherte Kommunikationskanäle mit identifizierten Kommunikationspartnern austauschen und so über ein privates Firewall-System verfügen, welches an Leistungsfähigkeit die heutigen System bei weitem übertrifft. (Vgl. Kyas, S.327f)

8. Fazit

Eine Firewall ist von unbedingter Notwendigkeit für die Erhöhung der Sicherheit. Eine gut administrierte Firewall ist in der Lage, die "normalen" (externen) Anwender von Spionage, Zerstörung von Dateien, u.a. wirkungsvoll abzuhalten. Aber dennoch ist ein Netzwerk auch mit der besten und teuersten Firewall (zumindest bis heute) noch nicht hundertprozentig sicher. Um die Sicherheit zu erhöhen sperrt man normalerweise Dienste und deinstalliert nicht benötigte Software, um die Anzahl der Sicherheitslücken zu verringern. Dabei muss man abwägen, in wieweit man diese Dienste beschränkt, um nicht den Nutzen und die Chancen, die die (weltweite) Vernetzung bringt, gänzlich wieder zunichte zu machen.

Literaturverzeichnis

anonymous: Der neue Hacker's Guide, München 2001,
Markt + Technik-Verlag

Kyas Othmar: Sicherheit im Internet, 2. Auflage, Bonn 1998
MITP-Verlag

Pohlmann, Norbert: Firewall System, Bonn 2001, MITP-Verlag

Hardt Oliver und Tümmel Michael.: Seminararbeit "Firewalls",
Universität Hamburg

Thüring, Roman: Seminararbeit "Die SuSE Linux 7.3 Firewall"
Fachhochschule Aargau, 2002

Hegering H.G.: Praktikumunterlagen IT-Sicherheit, Universität
München, 2002

Abbildungsverzeichnis

Schreiber, Alexander: Seminararbeit "Linux 2.4 Netfilter/iptables"
TU Chemnitz, 2000