

Firewallsysteme

Konzeption - Implementation - Audit

Cebit 2000

Thomas Veit

1. Einleitung

2. Grundlegende Filterverfahren

2.1 Paketfilter

2.2 Application Level Gateways

2.3 Lokale Paketfilter und Application Level Gateway auf einer Maschine

2.4 Stateful Inspection Filter

3. Konzeption und Implementation

3.1 IT-Sicherheitskonzept

3.2 Anordnung von Informationsservern

3.3 Intrusion Detection und Response Systems

3.4 Filterung Aktiver Inhalte (praxisnahe Lösungsansätze)

3.5 Zentrale Administration

3.6 Performance u. Verfügbarkeit (High-Availability Lösungen)

3.7 Auswahl der Komponenten des Firewallsystems

3.8 Lösungsbeispiele

4. Audit

4.1 Betriebsüberwachung

4.2 Interne Revision

4.3 Unabhängige Sicherheitsüberprüfung

5. Fazit

6. Literatur

1. Einleitung

Integraler Bestandteil der Konzeption einer Internet-Anbindung muss die Beachtung von Sicherheitsaspekten sein. Eine stetig zunehmende Anzahl sicherheitsrelevanter Vorfälle im Internet stellt ein nicht zu unterschätzendes Schadens- und Bedrohungspotential nicht nur für Integrität, Authentizität, Vertraulichkeit und Verfügbarkeit der Daten, sondern auch für das Ansehen einer Organisation dar. Firewallsysteme stellen hier aus heutiger Sicht unter Beachtung organisatorischer Randbedingungen - Einbindung in das IT-Sicherheitskonzept, Sensibilisierung der Mitarbeiter, Schulung der Administratoren - eine zuverlässige Schutzmaßnahme dar, deren Wirksamkeit jedoch entscheidend von einer richtigen Konzeption, modularer und abgestimmter Implementation sowie einem regelmäßigen Audit der Komponenten und des Gesamtsystems bestimmt wird.

Unter dem Begriff Firewallsystem wird eine Architektur aus Sicherheitskomponenten verstanden, die zum Schutz und zur sicheren Kommunikation zwischen Netzwerken benötigt wird. In Auswahl können folgende Elemente enthalten sein : statischer oder dynamischer Paketfilter, mindestens ein Application Level Gateway, Intrusion Detection und Response Systems, Content-Filter, Einwahl- und Authentisierungsserver, Managementstation. Im weiteren Sinne zählen sicherheitsrelevante Router, Lastverteiler oder Dienste-Server zum Begriff Firewallsystem.

Beginnend mit einer kurzen Erläuterung grundlegender Verfahren und Begriffe - Paketfilter, Application Level Gateway, Stateful Inspection Filter - einschließlich Diskussion der Vor- und Nachteile, wird anschließend detailliert die Konzeption eines Firewallsystems vorgestellt. Ausgehend von einer unerläßlichen Einbettung in ein allgemeines IT-Sicherheitskonzept schließt sich eine Betrachtung von Teilproblematiken an, wobei der Fokus auf praxisnahen Lösungsvorschlägen liegt:

- sichere Anordnung von Informationsservern,
- Einbindung von Intrusion Detection und Response Systems,
- Filterung von Aktiven Inhalten (Java, JavaScript, ActiveX, ...),
- zentrale Administration,
- High-Availability-Firewallsysteme,
- Kriterien für Auswahl der Komponenten des Firewallsystems,
- beispielhafte Darstellung von Lösungsansätzen.

Bedingt durch die Komplexität der eingesetzten Hard- und Software und ein damit hohes Fehlerpotential sind Maßnahmen zur permanenten Kontrolle des Firewallsystems unerläßlich. Im abschließenden Teil werden daher Möglichkeiten zur betrieblichen Überwachung der Komponenten sowie ein systematischer Ansatz zur Durchführung eines unabhängigen IT-Sicherheitsaudits vorgestellt.

2. Grundlegende Filterverfahren

Die Implementation von Firewallsystemen wird bestimmt von einer Kombination der folgenden drei grundlegenden Verfahren: Paketfilterung, Stateful Inspection Filterung und Application Level Gateway Filterung, wobei die Qualität der Sicherheitseigenschaften mit der Reihenfolge der Aufzählung zunimmt.

Stateful Inspection Filter oder sog. dynamische Filter stellen eine Mischform aus Paketfiltern und Application Level Gateways dar. Die zueinander synonymen Begriffe Circuit-Level-Gateway, Plug-Gateway, Generischer Proxy, tcp-relay, udp-relay bezeichnen Application Level Gateways mit minimaler Funktionalität.

2.1 Paketfilter

Paketfilter sind die einfachste Variante einer IP-Filterkomponente. Folgende, sich am Beginn eines Paketes befindlichen Bestandteile werden geprüft: IP-Header, ICMP-Header, TCP-Header, UDP-Header. In Abhängigkeit von konfigurierten Filterregeln werden die Pakete dann durchgelassen (allow), verworfen (deny) oder mit einer Fehlermeldung (reject) zurückgewiesen. Paketfilter zeichnen sich aus Anwendersicht durch eine sehr gute Transparenz aus. Anwendungen auf den Arbeitsplatz-PCs müssen

nicht wartungsaufwendig konfiguriert werden. Die sicherheitstechnisch nachteilige Konsequenz liegt jedoch im Fehlen einer verlässlichen Trennung der Datenströme. Die Funktionalität von Paketfiltern ist oft bereits in Routern integriert. Sie muss dann vom Administrator aktiviert und konfiguriert werden. Im Vergleich zu dedizierten Paketfiltern ist durch die zusätzliche Funktionalität auf den Routern jedoch ein größeres Risiko von Fehlfunktionen, z.B. aufgrund von Konfigurationsfehlern, gegeben. Resultierend aus der nur eingeschränkten Prüfung der Pakete zeichnen sich Paketfilter durch eine relativ gute Performance aus. Als erste nachteilhafte Eigenschaft von Paketfiltern muss die fehlende Prüfung von Protokollsequenzen, d.h. des sich unmittelbar an TCP- oder UDP-Header anschließenden Datenstromes genannt werden. Die sich daraus ergebenden Konsequenzen sind z.B.:

- nur sehr eingeschränkte Möglichkeiten zur Protokollierung,
- Missbrauch von Protokollen nicht erkennbar (z.B. versteckte Kommunikationskanäle, Ausnutzung von spezifischen Schwachstellen z.B. mittels Buffer Overflows),
- keine Content-Filterung (z.B. Cookies, FTP-PUT).

Durch Paketfilter ist keine verlässliche Trennung der Netzwerksegmente erreichbar. So akzeptieren die meisten Paketfilter von der unsicheren Seite TCP-Pakete mit gesetztem ACK-Bit, um die Antwortpakete der von innen nach außen initiierten Verbindungen wieder nach innen zu lassen. Es ist jedoch nicht schwierig, auf der externen Seite künstliche Pakete mit ACK-Bit zu erzeugen und nach innen zu senden. Als Folge davon lassen sich einige Betriebssysteme, die hinter dem Paketfilter im als sicher eingestuftem Bereich angesiedelt sind, z.B. einem Portscan unterziehen.

Weiterhin problematisch ist die Filterung von UDP-Paketen (z.B. DNS, RealAudio): der Initiator einer Kommunikationsbeziehung kann von einem Paketfilter nicht festgestellt werden. Als Konsequenz hieraus müssten UDP-Pakete in beide Richtungen durchgelassen werden. Die unmittelbare Folge davon wäre, dass von externer Seite initiierte UDP-Pakete über den Paketfilter in das interne LAN gesandt werden können. Problembehaftet ist die Filterung fragmentierter Pakete. Dieser im Internet standardisierte und oft angewandte Mechanismus spaltet ein größeres IP-Paket in mehrere kleine Pakete auf. Da dann nur das erste Paket einen TCP-, UDP- oder ICMP-Header besitzt, muss eine Entscheidung getroffen werden, wie die nachfolgenden Pakete behandelt werden sollen. Eine Lösungsmöglichkeit kann in der automatischen Defragmentierung der Fragmente auf dem Paketfilter bestehen. Dabei muss jedoch ein hohes Vertrauen in die Korrektheit der eigentlichen Defragmentierungsroutine bestehen. Eventuelle Programmierfehler könnten hier Angriffen Vorschub leisten, die sich u.U. massiv auf die Verfügbarkeit des Paketfilters auswirken. Nicht vorhandene Möglichkeiten zum Einblick in den Quellcode oder eine unabhängige Überprüfung führt in der überwiegenden Mehrzahl der Anwendungsfälle dazu, dass die Fragmente einfach durchgelassen werden. Es muss dann darauf vertraut werden, dass die verschiedenen Zielsysteme die Pakete wieder korrekt zusammensetzen.

Ein sehr oft erfolgreicher Angriff unter Ausnutzung der o.a. Schwierigkeiten bei der Behandlung fragmentierter Pakete besteht im Senden eines sehr kleinen ersten

Fragments. Hierbei wird der TCP- oder UDP-Header auf das erste und zweite Paket verteilt. Da ein Paketfilter immer nur das aktuelle Paket beurteilt und sich keine Zustände merkt, ist eine Entscheidungsfindung hier besonders schwer. Wünschenswert ist die Angabe einer Minimalgröße für das erste Fragment bei der Konfiguration des Paketfilters.

Mit zunehmender Anzahl von Filterregeln wird es schwieriger, den Überblick über den Regelsatz als Ganzes zu behalten. Der Faktor Mensch, insbesondere die Fähigkeit des Administrators, bei komplexen Regelsätzen die Bedeutung einzelner Anweisungen zu verstehen, spielt hier eine entscheidende Rolle.

Mit einer steigenden Anzahl erlaubter Protokolle wird der Paketfilter immer durchlässiger. Unter Umständen zeigen sich hier ungewollte Seiteneffekte wie z.B. das implizite Erlauben einer Kommunikationsverbindung, die eigentlich verboten sein sollte. Eine nutzerbezogene Filterung ist aufgrund fehlender Möglichkeiten zur Authentisierung nur eingeschränkt erreichbar. Alleine anhand der IP-Adresse der Absender-Maschine muss dann entschieden werden, ob eine Kommunikation stattfinden darf oder verboten ist. Diese Vorgehensweise ist jedoch z.B. bei Nutzung dynamischer IP-Adressen (DHCP) nicht praktikabel.

Ein maßgeblicher Faktor für die korrekte Arbeitsweise eines Paketfilters ist die Abarbeitungsreihenfolge der Regeln. Werden hier vom System undokumentierte Änderungen vorgenommen, können die Effekte bis zum impliziten Erlauben unerwünschter Kommunikationsbeziehungen reichen.

In jedem Fall sollte klar dokumentiert sein, ob es eine automatische Deny All - Regel gibt oder eine solche vom Administrator explizite am Ende des Regelsatzes eingefügt werden muss.

2.2 Application Level Gateways (ALG)

Im Gegensatz zu Paketfiltern wird mit Application Level Gateways eine verlässliche Trennung zwischen unterschiedlich vertrauenswürdigen Netzwerksegmenten erreicht. Das Application Level Gateway fungiert dabei als Stellvertreter zwischen Client und Server: es gibt keinen direkten Aufbau einer Kommunikationsbeziehung, vielmehr kontaktiert der Client zuerst das Application Level Gateway, welches dann das eigentliche Zielsystem - den Server - kontaktiert. Manipulierte Pakete werden zuverlässig abgefangen und entsprechend protokolliert.

Für jede TCP-Verbindung wird dabei ein separates Programm (ein sog. Proxy oder Stellvertreter) gestartet. Hierdurch wird eine logische Trennung der einzelnen Kommunikationsbeziehungen untereinander erreicht. Zusätzlich zu einigen von Paketfiltern vorgenommenen Prüfungen der Daten auf Ebene der Paketheader filtern Application Level Gateways auf Anwendungsebene. Die Vorteile hiervon sind u.a. erweiterte Möglichkeiten zur Benutzer-Authentisierung, zur Kontrolle der Protokollsequenzen und zur benutzerbezogenen Protokollierung.

Als Folge der Arbeitsweise der Proxies auf Applikations- und nicht auf Systemkernebene (Kernel) kann weitestgehend sichergestellt werden, dass eine Fehlfunktion eines Proxy keinen Einfluss auf Integrität und Stabilität des Gesamtsystems hat. Eine strikte Trennung

zwischen Kernel und Applikationen ist dafür Bedingung. Voraussetzung für eine korrekte Implementation eines Application Level Gateways ist die Deaktivierung des IP-Routings, d.h. des Weiterleitens von Paketen auf Betriebssystem-Ebene. So wird sichergestellt, dass die Daten die Anwendungsschicht mit den entsprechenden Kontrollen passieren müssen.

2.3 Lokale Paketfilter und Application Level Gateway auf einer Maschine

Bedingt durch Analyse der Datenströme vorwiegend auf Anwendungsebene sind Application Level Gateways allein nicht in der Lage, bestimmte Angriffe auf unteren Protokollebenen zu erkennen und zu protokollieren. Daher muss der Widerstandsfähigkeit des zugrundeliegenden Betriebssystems eine hohe Bedeutung zugemessen werden. Entsprechend sind robuste, fehlertolerante und stabile TCP/IP-Stacks Voraussetzung für Integrität und Verfügbarkeit der Netzwerkfunktionalität des Betriebssystems.

Unzureichende Protokollierung in der Standardkonfiguration sowie potentielle Schwachstellen vieler TCP/IP-Stacks können jedoch den Einsatz von lokalen Paketfiltern auf der Maschine als zweckmäßig erscheinen lassen. Einerseits läßt sich dadurch das Kommunikationsprofil restriktiver konfigurieren (z.B. Verbot von ICMP), andererseits können bestimmte Angriffe auf unteren Protokollebenen erkannt und protokolliert werden. Lokale Paketfilter stellen somit eine sinnvolle zusätzliche Schutzmaßnahme für ein Application Level Gateway dar. Als empfehlenswert sind in diesem Zusammenhang die mehrstufigen Paketfilter (z.B. pre-input-filter und input-filter) moderner Betriebssysteme zu nennen.

Bei der Konzipierung einer Internet-Anbindung kann jedoch die Kombination von Paketfiltern und Application Level Gateway auf einer einzigen Maschine nicht als Ersatz für eine getrennte Anordnung von Paketfilter und Application Level Gateway gesehen werden. Zu groß ist das Risiko, dass Sicherheitsmechanismen, die nur auf einer Maschine konzentriert sind, durch Schwachstellen umgangen werden können.

2.4 Stateful Inspection Filter

Als auf Paketfiltern basierende Technologie sind Stateful Inspection Filter in der Lage, sich die aktuelle Status- und Kontextinformation einer Kommunikationsbeziehung in internen Zustandsautomaten zu merken. Diese grundsätzliche Arbeitsweise läßt sich am 3-stufigen Aufbau einer TCP-Verbindung veranschaulichen:

1. Verbindungsanfrage des Quellrechners : (SYN)
2. Bestätigung der Anfrage vom Zielrechner : (SYN-ACK)
3. Bestätigung vom Quellrechner : (ACK)
4. Weiterer Datentransfer : (ACK)

Während ein konventioneller Paketfilter i.d.R. von außen ACK-Pakete unabhängig vom Status eines eventuellen Verbindungsaufbaus passieren läßt, wird ein Stateful Inspection Filter ACK-Pakete nur nach dem Auftreten eines von innen nach außen gesandten SYN-Paketes nach innen weiterleiten. Die potentielle Gefahr, dass von außen manipulierte ACK-Pakete nach innen gesandt werden, ohne dass von innen ein Verbindungsaufbau nach außen stattfand, wird durch diese Maßnahme stark reduziert.

Ähnliche Filtermöglichkeiten bestehen für UDP-basierte Dienste: z.B. "erlaube DNS-Antwort nur falls eine DNS-Anfrage gestellt wurde". Voraussetzung für eine qualifizierte Umsetzung dieses Beispiels ist jedoch, dass nicht nur Quell- und Zieladresse sowie Quell- und Zielport, sondern auch der DNS-Header im Anfrage-Paket in die Speicherung der Status- und Kontextinformation einbezogen wird. Hintergrund ist hier die verhältnismäßig leichte Fälschbarkeit von UDP-Paketen.

Ein vorteilhafter Aspekt von Stateful Inspection Filtern ist die Fähigkeit, die Daten auf allen Protokollebenen (d.h. von Netzwerk- bis Anwendungsebene) zu prüfen. So kann z.B. ein FTP-GET erlaubt, ein FTP-PUT jedoch verboten werden.

Ein positiver Effekt der im Vergleich zu konventionellen Paketfiltern erhöhten Eigenintelligenz ist die Option, einzelne Pakete während einer Kommunikationsbeziehung zu assemblieren und damit erweiterte Möglichkeiten zur Benutzer-Authentisierung zur Anwendung zu bringen.

Als Folge der nicht verlässlichen Trennung der Netzwerksegmente sind Stateful Inspection Filter nicht immun gegen bestimmte auf unteren Protokollebenen stattfindende Angriffe. So z.B. werden fragmentierte Pakete i.d.R. von außen nach innen ohne weitere Prüfung durchgelassen (vgl. Paketfilter).

Eine Konfigurationsoption einiger Stateful Inspection Filter besteht in der Aktivierung sog. FAST-Modi für einzelne oder alle TCP-Verbindungen, was die Sicherheitseigenschaften jedoch auf die eines konventionellen Paketfilters reduziert. Eine weitere konzeptionelle Eigenschaft der meisten Stateful Inspection Filter besteht darin, dass nicht für jeden Dienst bzw. jede Kommunikationsbeziehung ein separater Proxy-Prozess gestartet wird. Die Filterung findet im gleichen Prozessraum statt. Ein einziger potentieller Schwachpunkt kann somit zum Absturz der gesamten Filterkomponente führen. Zwingend erforderlich sollte deshalb ein spezieller Prozess (evtl. doppelte Auslegung) sein, der Aktivität, Funktionsfähigkeit und insbesondere die Integrität der Filterkomponente überwacht.

Ein aus Anwendungssicht positiver Aspekt ist die sehr gute Transparenz eines Stateful Inspection Filters. Modifikationen auf Clients sind in der Regel nicht nötig. Zu den vorteilhaften betrieblichen Eigenschaften zählen weiterhin die guten Performanzenwerte.

3. Konzeption und Implementation

Ziel einer Konzeption muss es sein, nicht nur den aktuellen, sondern auch den zukünftigen Anforderungen hinsichtlich Sicherheit und Performance gerecht zu werden. Eine modulare Vorgehensweise bei Auswahl und Anordnung der Einzelkomponenten, die Konzentration auf Internet-Standards und damit transparente und nachvollziehbare Lösungen sind dafür von hoher Bedeutung.

Elementare Voraussetzung für die konzeptionelle Phase ist die Existenz eines IT-Sicherheitskonzeptes. In Abhängigkeit von allgemeinen IT-Sicherheitszielen (z.B. Gewährleistung von Vertraulichkeit und Integrität der Daten) und dem Schutzbedarf der Daten lassen sich daraus grundlegende Anforderungen an das Firewallsystem ableiten. Ein zu erarbeitendes Firewallkonzept sollte in enger Beziehung zum allgemeinen IT-Sicherheitskonzeptes stehen.

3.1 IT-Sicherheitskonzept

Sicherheitsziele

Basis des IT-Sicherheitskonzeptes als übergeordneter Rahmen für das zu entwickelnde Firewallkonzept ist die Definition des Anspruches an Integrität, Vertraulichkeit, Authentizität und Verfügbarkeit der Daten. Aus dieser globalen Einschätzung leiten sich die folgenden Maßnahmen ab. Das zu erzielende Schutzniveau und das konkret vorhandene Gefahrenpotential (intern und extern) gehen in eine Risiko- bzw. Gefahrenanalyse ein, in der das Verhältnis eines potentiellen - auch nichtmateriellen - Schadens im Vergleich zum Aufwand für das konkret geplante Firewallsystem abgewägt wird. Die nachfolgenden Sicherheitsaspekte und Kriterien beziehen sich nicht nur auf die Spezifika eines Firewallsystems. Vielmehr ist eine Integration und Abstimmung mit den Vorkehrungen und Maßnahmen des allgemeinen IT-Sicherheitskonzeptes notwendig. Hierzu zählen technische, organisatorische und personelle Aspekte, im Folgenden eine Auswahl:

Technische Aspekte:

- Zentraler Netzübergang zum Internet

Es muss sichergestellt werden, dass das Firewallsystem der zentrale Netzübergang - in der Regel in das Internet - ist. Umgehungswege wie Modems am Arbeitsplatz-PC oder sonstige Internet-Zugänge sind nicht zulässig.

- Netzwerktopologie und Kommunikationsbeziehungen

Technische Basis des IT-Sicherheitskonzeptes ist eine Erfassung und Dokumentierung der aktuellen Netzwerkstrukturen und der bereits vorhandenen Einzelkomponenten. Wesentlich ist eine komplette Darstellung der Kommunikationswege (z.B. Liegenschaftskommunikation, Kommunikationsverbindungen zu anderen Organisationen oder Firmen).

- Vertrauensbeziehungen

Über die Einstufung des Internets als nicht vertrauenswürdigen Netzwerk hinaus wird hier das Sicherheitsniveau der internen und angeschlossenen Netzwerke eingeschätzt. So z.B. kann das LAN einer Liegenschaft oder eines Application Providers ebenfalls als unsicher eingestuft werden. Weiterhin können unter diesem Abschnitt Nutzergruppen gebildet und Zugangsprofile definiert werden.

- Administration

Es ist festzulegen, welche Personen für die Administration des Firewallsystems zuständig sind. Neben Zuweisung der Verantwortlichkeiten - Wer z.B. für die Administration der einzelnen Komponenten zuständig ist - ist zu klären, wieviel Betriebspersonal benötigt wird. Ferner sind die Administrationswege zu konzipieren. Ein wichtiges Kriterium kann die Verfügbarkeit der Administration bei Ausfall von Teilen des Netzwerkes sein. Ein wichtiger Teilaspekt der Administration ist eine Backupstrategie.

- Protokollierung

Zwingend müssen die Arbeitsabläufe für eine kontinuierliche und zeitnahe Protokollerhebung und -auswertung definiert werden. Insbesondere sind Mechanismen vorzusehen, welche die Flut der Logeinträge reduzieren und auf ein von einer Person - die auf jeden Fall die letztendliche Bewertung in der konkreten Umgebung vornehmen muss - überschaubares und interpretierbares Volumen bringt.

Für Protokollierung, Auswertung und Lagerungsfristen der Protokolldaten sollte eine Abstimmung mit der Personalvertretung erfolgen. Ähnliches gilt für Filtermechanismen (z.B. URL-Filterung) und die Integration von Intrusion Detection und Response Systems.

- Authentisierung der User

Die allgemeine Anforderung nach einem Single-Sign-On (nur einmalige Authentisierung der User beim Zugriff auf die zur Verfügung stehenden verschiedenen Ressourcen) kann aus heutiger Sicht nicht zufriedenstellend umgesetzt werden. Hier gilt es, einen Kompromiss zu treffen: Ist eine

zusätzliche Authentisierung beim Internet-Zugriff überhaupt erforderlich ? Unter Umständen reicht eine Pseudo-Authentisierung anhand der IP-Adresse des Arbeitsplatz-PCs. Bei dieser Variante sollte aber eine qualifizierte Authentisierung der User am Arbeitsplatz-PC erfolgen.

Organisatorische Aspekte:

Nicht alle Gefährdungspotentiale und Anwendungsfälle können sinnvoll von einem Firewallsystem behandelt werden. Für folgende Aspekte (Auswahl in nicht bewerteter Reihenfolge) sind daher weitergehende organisatorische Vereinbarungen zu treffen und im Sinne einer transparenten IT-Sicherheitsphilosophie den Usern im Rahmen von Schulungen bekanntzugeben und darüberhinaus in einem Benutzerhandbuch zu dokumentieren:

- **EMail und Trojanische Pferde**

Unverlangt per Email zugesandte Attachments und nicht standardmäßig installierte Programme (z.B. aus dem Internet) dürfen nicht auf dem Arbeitsplatz-PC ausgeführt werden. So kann wirksam verhindert werden, dass Viren oder Trojanische Pferde Schaden anrichten. Da nicht davon ausgegangen werden kann, dass diese Forderung vollständig umgesetzt wird, kann es erforderlich sein, weitere Maßnahmen zu treffen. Um den ungewollten Export vertraulicher Daten per EMail (z.B. durch ein Trojanisches Pferd) zu verhindern, kann vorgesehen werden, dass nur signierte EMail in das Internet versandt werden dürfen. Eine Sicherheitskomponente (z.B. EMail-Gateway im Bereich des Firewallsystems) kontrolliert, ob jede EMail signiert und die Signatur gültig ist. Diese Vorgehensweise impliziert die Notwendigkeit, die User darüber zu informieren, dass jede EMail zweifelsfrei einer Person zugeordnet werden kann.

- **Verschlüsselung**

Es muss geklärt werden, ob die Übertragung verschlüsselter Informationen zulässig ist (z.B. SSL, verschlüsselte EMail). Die prinzipiell eingeschränkten Filter- und Protokollierungsmöglichkeiten müssten dann akzeptiert werden.

- **URL-Filterung**

Der Anspruch an die Zuverlässigkeit einer URL-Filterung kann in der Realität häufig nicht erreicht werden. Zu leicht ist eine Umgehung unter Nutzung speziell formulierter URLs möglich. URL-Filterung sollte daher nicht das alleinige Entscheidungskriterium für eine Zugangsbeschränkung sein.

- Mitarbeiter-Motivation

Selbst Application Level Gateways prüfen i.d.R. nicht die Nutzdaten. Ein guter Kenntnisstand und eine gute Motivation der Mitarbeiter ist nicht zuletzt deshalb die beste Voraussetzung für den Verbleib vertraulicher Informationen innerhalb der Organisation.

- Passwortwahl

Regeln zum qualifizierten Gebrauch von Passwörtern sind aufzustellen, bekanntzugeben und einzuhalten. Ein kontinuierlicher Prüfprozess, der maschinell abläuft, kann eine Hilfe zur Beurteilung der Umsetzung sein.

- IT-Sicherheitsaudit

Neben Konzeption der Strukturen für eine betriebliche Überwachung (z.B. zentrale Administration) ist festzulegen, wer für die interne IT-Sicherheitsrevision verantwortlich ist. Darüberhinaus sollte eine unabhängige Sicherheitsüberprüfung einmal nach Inbetriebnahme und anschließend in geeigneten Abständen vorgesehen werden. Das Ergebnis einer Revision ist der Leitungsebene vorzulegen.

- Notfallkonzept und Eskalationsmaßnahmen

Selbst mit einer hohen Qualität der Sicherheitsmaßnahmen können außerplanmäßige Situationen (z.B. Angriff aus dem Internet, Ausfall einer Komponente) nicht ausgeschlossen werden. Basis für ein der Situation angemessenes Handeln ist die Erkennung des Problems, die Einschätzung der potentiellen Tragweite, die zeitnahe Einleitung und das Wirksamwerden der korrekten Gegenmaßnahmen. Für diesen komplexen organisatorischen Vorgang insbesondere bei größeren Internet-Anbindungen muss ein detailliertes, logisch aufgebautes und nachvollziehbares Konzept vorliegen. Dabei ist es unerlässlich, dass die vor Ort tätigen

Administratoren mit diesem Konzept vertraut sind, um ein zeitaufwendiges Studium im Notfall zu vermeiden.
Bestandteil dieses Konzeptes sollten u.a. die Alarmierungswege sein (z.B. weitere Personen innerhalb der Organisation und externe Organisationen (z.B. Computer Emergency Response Teams - CERTs) sein.

Personelle Aspekte:

- Verantwortung für IT-Sicherheit und Datenschutz

Sinnvoll und zweckmäßig ist die Ernennung einer Person mit diesem Aufgabengebiet, welche für die Umsetzung der Maßnahmen verantwortlich ist und der Leitungsebene Bericht erstattet.

- Know-How des Betriebspersonals

Ein entsprechend hoher Wissensstand des Betriebspersonals ist eine zwingende Voraussetzung für den Betrieb eines Firewallsystems.

3.2 Anordnung von Informationsservern

Zu den Informationsservern, die durch Sicherheitskomponenten des Firewallsystems geschützt werden sollten, zählen z.B. öffentliche WWW- und FTP-Server, EMail-Gateways, aber auch WWW-Server, deren Angebot nur vom firmeninternen Intranet aus abrufbar sein darf.

Der Betrieb komplexer Dienstprogramme wie WWW-Server, FTP-Server und EMail-Gateway (Mail Transfer Agent - MTA) auf einem Application Level Gateway kann als Folge zahlreicher Schwachstellen, die sich aus Konzeption, Programmierung, Implementation und Konfiguration ergeben können, nicht empfohlen werden. Zweckmäßig ist daher der Betrieb eigener Rechner, die entweder in einer der Demilitarisierten Zonen (DMZ), oder aber an einem speziellen Segment des Application Level Gateways aufgestellt werden. Vorteilhaft ist dabei nicht nur der Schutz dieser Rechner durch einen Paketfilter oder das Application Level Gateway - welches spezielle Proxies für jeden Dienst bereithält - vor evtl. Angriffen, sondern auch die Eingrenzung des von den Informationsservern ausgehenden Datenverkehrs.

Gegen WWW-Server, FTP-Server sowie gegen EMail-Gateways existieren zahlreiche Angriffsmethoden, die auf Applikationsebene stattfinden. Ein Paketfilter oder ein Application Level Gateway bieten hier nur eine eingeschränkte Schutzfunktion. Daher müssen für Informationsserver die allgemeinen Anforderungen zum sicheren Betrieb eines Servers (z.B. keine unnötigen Dienste, aktuelle Software und Patches etc.) mit Priorität umgesetzt werden.

Eine ähnliche Problematik stellt sich für Konzeption und Implementation des DNS-Dienstes, welcher in jüngster Vergangenheit eine besondere Auffälligkeit in den einschlägigen Sicherheits-Mailing-Listen zeigte. Um gegen dieses Schadenspotential verlässliche Vorkehrungen zu treffen, ist auch hier eine vom Application Level Gateway separierte Anordnung vorzuziehen, um der Ausnutzung eventueller Schwachstellen mit der Folge eines Verlustes der Integrität der Sicherheitssoftware und des darunterliegenden Betriebssystems des Application Level Gateways vorzubeugen. Vorteilhaft ist die Separierung in einen externen DNS-Server, der z.B. für die EMail-Verteilung (MX-Record) verantwortlich ist und einen internen DNS-Server. Das Application Level Gateway ist dann nur für die Weiterleitung der DNS-Pakete zwischen den beiden DNS-Servern zuständig. Der hauptsächlich positive Effekt dieser Aufspaltung besteht im Verbergen interner Strukturen zum Internet hin.

Als Folge der Komplexität der Informationssysteme und der Tatsache, dass eine 100 % korrekte Implementierung nicht vorausgesetzt werden kann, kann trotz aller Sicherheitsvorkehrungen die Ausnutzung einer Schwachstelle nicht ausgeschlossen werden. Elementar für Integrität des Rechners, des Betriebssystems und anderer lokaler Dienste ist in einem solchen Fall, dass das Sicherheitsproblem auf den einzelnen anfälligen Dienst auf der Maschine (z.B. der WWW-Server) begrenzt bleibt. Erreicht werden kann diese Anforderung durch eine Abgrenzung der Laufzeitumgebung des Prozesses. Eine Verlagerung des Wurzelverzeichnisses (sog. chroot) kann hier eine erste sinnvolle Maßnahme sein, reicht bei erhöhten Sicherheitsanforderungen allerdings nicht aus. Es kann nicht ausgeschlossen werden, dass aus einer chroot-Umgebung nicht ausgebrochen werden kann. Daher ist die Anwendung sog. Cages oder Partitions, innerhalb derer die Dienste ablaufen, vorzuziehen. Bei Realisierung einer solchen Umgebung kann dann auch erwogen werden, DNS auf dem Application Level Gateway zu implementieren.

3.3 Intrusion Detection und Response Systems

Erste Aufgabe eines Intrusion Detection Systems (IDS) ist die zeitnahe und zuverlässige Erkennung von Angriffen. Neben der vorwiegenden Positionierung eines IDS im externen Bereich zur Erkennung von Angriffen aus dem Internet kann die Feststellung von Fehlverhalten im Intranet (z.B. undefinierte oder nicht zugelassene Protokolle) eine weitere Aufgabe eines IDS sein.

Ein IDS kann ein Firewallsystem nicht ersetzen. Es ist vielmehr eine sinnvolle Ergänzung zu bereits vorhandenen Erkennungsmechanismen (z.B. Protokollierung). Zudem ist aus heutiger Sicht die Verlässlichkeit und insbesondere die Interpretation der Ereignisse auf einem IDS noch ausbaufähig.

Der hauptsächlichste Arbeitsaufwand bei Implementation und Konfiguration besteht in der Definition von Ereignissen und Schwellwerten, die einen Angriff kennzeichnen. In Abhängigkeit von der konkreten Einsatzumgebung kann eine solche angepasste Konfiguration letztendlich erheblich von einer initialen Standardkonfiguration abweichen.

Bei Überwachung mehrerer kritischer Bereiche ist der Einsatz von sog. IDS-Agenten

empfehlenswert, die die gesammelten Daten einer Vorauswertung unterziehen und die Resultate danach einer IDS-Management-Station zusenden.

An ein IDS/IRS sind folgende Anforderungen zu stellen:

- Das Netzwerkinterface muss vom Netzwerk her unsichtbar sein. Damit kann möglichen Angriffen auf das IDS selbst effektiv vorgebeugt werden.
- Bei Konzipierung einer verteilten IDS-Struktur muss darauf geachtet werden, mögliche administrative Umgehungswege am Firewallsystem vorbei entsprechend abzusichern.
- Die Kommunikation zwischen IDS und Admin-Workstation muss zuverlässig abgesichert werden. Empfehlenswert ist ein separates Segment.
- Die Kommunikation zwischen IDS-Agenten und IDS-Management-Station sollte, falls sie über das Produktionsnetzwerk läuft, kryptographisch abgesichert werden. Die bessere Alternative ist aber in jedem Fall die Konzeption eines Administrationssegmentes (s.a. Zentrale Administration).
- In Abhängigkeit von der Dimensionierung des zu überwachenden Netzwerkes ist bei Konzipierung der IDS-Maschine auf ausreichende Performance zu achten. Neben der Datensammlung müssen noch genügend Ressourcen für eine Vorauswertung zur Verfügung stehen.
- Das den IDS-Agenten zugrundeliegende Betriebssystem sollte als Minimalsystem konfigurierbar sein (z.B. keine unnötigen aktiven Dienste, keine unnötigen installierten Programme - GUI, Compiler). Ferner können durch einen regelmäßigen Integritätscheck Veränderungen an lokalen Dateien erkannt werden.
- Hohe Anforderungen sind an die Stabilität der IDS-Software zu stellen: die Interpretation bössartiger konstruierter Pakete darf keinen Absturz verursachen.
- Als vorteilhaft erweist es sich, mindestens die Protokollheader sowie die ersten Nutz-Bytes eines jeden Paketes zu speichern. Nur so kann später detailliert ein Angriff nachvollzogen werden. Welche Details vom IDS gespeichert werden, sollte vom Administrator konfigurierbar sein.
- Die IDS-Management-Station muss in der Lage sein, Alarm-Meldungen auf verschiedenen Wegen auszusenden (z.B. EMail mit Signatur, SNMP-Trap, Syslog-Message).
- Das IDS sollte die TCP/IP-Stacks verschiedener Betriebssysteme "kennen", um die Wirksamkeit von Angriffen einschätzen zu können.

Das IDS/IRS sollte in der Lage sein, die Authentizität von Angriffen zu bewerten. Diese prinzipielle Forderung kann aber in der Praxis bei bestimmten Angriffen nicht umgesetzt werden. Beispielsweise lässt sich die IP-Adresse des Absenders von Paketen relativ leicht fälschen (IP-Spoofing). Eine erste Reaktion des IRS kann dann darin bestehen, das Firewallsystem zu instruieren, von dieser Adresse keine Pakete mehr entgegenzunehmen bzw. zu blockieren. Eine zeitnahe Auswertung und Reaktion durch das Betriebspersonal ist dann jedoch Bedingung, um zu entscheiden, ob Verfügbarkeitsanforderungen Vorrang vor dem Blockieren einer Kommunikationsbeziehung haben. Eine erweiterte automatische Reaktion mit dem Ziel, Informationen über den Angreifer zu sammeln oder gar einen Gegenangriff zu starten, kann jedoch aus heutiger Sicht nicht empfohlen

werden. Rechtliche Probleme und die durchaus nicht unrealistische Möglichkeit, eine unbeteiligten Dritten zu treffen, lassen den Schluss zu, die Einsatzmöglichkeiten eines IRS auf das lokale Blockieren von Paketen und Verbindungen zu beschränken. Voraussetzung dafür ist eine klar definierte, transparente Schnittstelle zwischen IRS und Firewallsystem. Es muss zu jedem Zeitpunkt nachvollziehbar sein, wer das Firewallsystem administriert: die Administratoren und/oder das IRS.

3.4 Filterung Aktiver Inhalte (praxisnahe Lösungsansätze)

Die unkontrollierte und unbewusste Ausführung von Programmen auf einem Arbeitsplatz-PC kann aus sicherheitstechnischer Sicht nicht toleriert werden. Zu groß ist das Risiko, das z.B. über ein Netzwerklaufwerk zugängliche, vertrauliche Daten durch konzeptionelle Mängel oder durch Schwachstellen in der Implementierung des Browsers an die Öffentlichkeit gelangen. Zwingend erforderlich ist deshalb eine kontrollierte und zuverlässige Filterung an zentraler Stelle.

Aus praktischer Sicht muss jedoch festgestellt werden, dass viele Webseiten bei Deaktivierung der Ausführung von Aktiven Inhalten (engl. Active Content), insb. JavaScript, leider nicht mehr vernünftig darstellbar sind bzw. es versäumt wird, alternative Angebote, die ohne Active Content auskommen und aus der Sicht des Autors vielfach ohne Verlust der eigentlichen Funktionalität arbeiten könnten, bereitzustellen. Deshalb kann es erforderlich sein, den Zugriff auf Server mit Active Content zu ermöglichen. Ausgehend vom Verbot aller Active Content Typen kann folgende Risikoeinschätzung auf Basis des jeweiligen Sicherheitsmodells und der Schwachstellen in den Implementationen als Orientierung für ein abgestuftes Vorgehen dienen, wobei sich das Sicherheitsrisiko mit der Reihenfolge der Aufzählung erhöht:

- signierte Java-Applets von einzelnen, vertrauenswürdigen Servern können akzeptiert werden, wenn die Signatur nachprüfbar gültig ist.
- signierter JavaScript-Code von einzelnen, vertrauenswürdigen Servern kann akzeptiert werden, wenn die Signatur nachprüfbar gültig ist.
- signierte Java-Applets von allen Servern können akzeptiert werden, wenn die Signatur nachprüfbar gültig ist.
- signierter JavaScript-Code von allen Servern kann akzeptiert werden, wenn die Signatur nachprüfbar gültig ist.
- unsignierte Java-Applets von einzelnen, vertrauenswürdigen Servern können akzeptiert werden
- unsignierter JavaScript-Code von einzelnen, vertrauenswürdigen Servern kann akzeptiert werden
- unsignierte Java-Applets von allen Servern können akzeptiert werden
- unsignierter JavaScript-Code von allen Servern kann akzeptiert werden.

Hierbei muss man sich aber bewusst sein, dass JavaScript aus Java heraus aufgerufen werden kann (und umgekehrt), mithin die Filterung nur eines der beiden Bestandteile lückenhaft ist.

Weiterhin lässt sich selbst aus der Echtheit einer Signatur kein Rückschluss auf die Funktionalität oder die Korrektheit der Implementierung der Komponente ableiten. Daher ist die Vertrauenswürdigkeit der Signatur-Stelle ein wichtiger Aspekt.

Aufgrund des Fehlens eines Sicherheitsmodells erscheint das Risiko bei der Ausführung von ActiveX nicht tragbar. Daher sollte die zentrale Filterkomponente in der Lage sein, diesen Objekttyp herauszufiltern. Problematisch bei diesem Ansatz ist jedoch, dass ActiveX aus Java heraus aufgerufen werden kann.

Folgende konzeptionelle Möglichkeiten, die alle hinter einem zentralen Firewallsystem angeordnet sein sollten, stehen zur Wahl:

1. Nutzung des vorhandenen Arbeitsplatz-PCs, wenn eine zuverlässige Trennung des Prozessraumes des Browsers von sonstigen Daten erfolgen kann (s.u. Anforderungen)
2. speziell separierter LAN-Bereich mit erweiterten Rechten bzgl. Ausführung von Active Content
3. Ausführung des Browser-Prozesses und damit von Active Content auf einem separaten, speziell abgesicherten Rechner, dessen Display-Ausgabe dann auf die Arbeitsplatz-PCs umgeleitet wird. Voraussetzung ist eine ausreichend hohe Performance dieses Rechners, um das gleichzeitige Ausführen mehrerer Browser-Prozesse zu ermöglichen. Für die Display-Umlenkung sollte ein Protokoll mit einer hinreichenden Eigenintelligenz zum Einsatz kommen, welches Bildschirmhalte als abstrakte Beschreibung und nicht als Graphik überträgt. Entsprechend performant sollte das Netzwerk ausgelegt werden.

An Variante 1, die ohne zusätzliche Hardwareinvestitionen auskommen kann, sind folgende Anforderungen zu stellen:

- Definition eines speziellen Account mit minimalen Rechten auf dem Arbeitsplatz-PC. Unter diesem Account kann ein lokaler WebBrowser gestartet und auf das Internet zugegriffen werden.
- Laufende Prozesse unter diesem Account (z.B. der WebBrowser) dürfen nur in ein Heimatverzeichnis sowie in ein temporäres Verzeichnis Daten schreiben. Damit wird effektiv verhindert, dass Betriebssystem-Dateien von Trojanischen Pferden ersetzt werden. Falls die Möglichkeit besteht, das Wurzelverzeichnis des Dateisystems auf das Homeverzeichnis zu setzen, kann dieses Ziel sehr effizient umgesetzt werden.
- Es muss eine weitestgehende Einschränkung der Lese-, Schreib- und Ausführungsrechte auf die Programme und Bibliotheken möglich sein, die essentiell für Start und Lauffähigkeit des WebBrowsers notwendig sind.
- Es muss eine klare, nachvollziehbar und transparent gestaltete Trennung dieses speziellen Nutzerprozesses vom Betriebssystem einrichtbar sein, mithin dürfen

Schreib- und Lesezugriffe z.B. auf Speicherbereiche des Betriebssystems nicht möglich sein.

- Netzwerklaufrerke z.B. von Abteilungsservern dürfen nicht unter diesem speziellen Account gemountet werden.
- Um einen unberechtigten Zugriff auf Dokumente oder Anwendungsdateien auszuschließen, dürfen diese nicht lokal auf dem Arbeitsplatz-PC abgelegt sein.
- Die Einrichtung und Aktivierung lokale Paketfilter auf dem Arbeitsplatz-PC ist vorzusehen, um einen unkontrollierten Verbindungsaufbau vom Arbeitsplatz-PC aus zu verbieten bzw. entsprechende Versuche zu protokollieren und eine Auswertung zu ermöglichen. Für das Versenden von EMail kann bei Einhaltung der Randbedingungen erwogen werden, einen Verbindungsaufbau zum EMail-Gateway zu erlauben.

Dieses Sicherheitsprofil wird bei jedem Login-Vorgang aktiviert und bleibt für die Dauer des Logins bestehen.

3.5 Zentrale Administration

Aus betrieblicher Sicht sollte es das Ziel sein, alle sicherheitsrelevanten Komponenten des Firewallsystems ausgehend von einer Oberfläche bzw. Workstation zu administrieren. Hierin eingeschlossen sein sollte das Versenden von Protokolldaten und Alarmmeldungen, um eine komponentenübergreifende Auswertung und Einschätzung von Ereignissen zu ermöglichen. Vielfach ergeben Einzelereignisse erst einen Sinn, wenn sie im Kontext bewertet werden.

In der Praxis nachteilig ist jedoch, dass die Einzelkomponenten proprietäre Administrationsmechanismen und -protokolle aufweisen, die nur unzulänglich unter einer Administrationsoberfläche integrierbar sind. Ein erster sinnvoller Ansatz ist hier z.B. die Möglichkeit, Router oder Paketfilter von der Firewall-Admin-GUI aus zu konfigurieren. Dabei sollte jedoch darauf geachtet werden, dass in Abhängigkeit vom Standort der Admin-Workstation, von den konkreten Gefährdungspotentialen und damit in Verbindung stehendem Schutzniveau Passwörter und sonstige administrative Daten nicht im Klartext über das allgemeine LAN transportiert werden.

Empfehlenswert ist entweder die Positionierung der Admin-Workstation in einer ähnlich einer DMZ abgesicherten Zone im Bereich des Firewallsystems oder alternativ die Absicherung des Übertragungsweges zwischen Admin-Workstation und Firewallsystem durch qualifizierte kryptographische Verfahren. Alternativ empfehlenswert kann die Einrichtung eines speziell separierten Administrationssegmentes sein, welches vom Produktionsnetz durch genau definierte logische Übergänge getrennt ist. Folgenden Anforderungen (Auswahl) kann damit Rechnung getragen werden:

- hoher Anspruch an Verfügbarkeit der Administrationswege,
- hoher Anspruch an die Vertraulichkeit der administrativen Kommunikation,
- Einsatz administrativer Protokolle, die keine immanenten Sicherheitseigenschaften bieten (z.B. Telnet, TFTP, SNMPv2) und deshalb im Klartext übertragen werden müssen.

Die Nutzung von VLANs oder Switches zur Separierung von Netzwerksegmenten kann unter Sicherheitsaspekten nicht als hinreichend betrachtet werden. Konzeptionelle Schwächen und Probleme bei der Implementierung erfordern hier zusätzliche Maßnahmen (z.B. Einrichtung eines Admin-VPNs)

3.6 Performance u. Verfügbarkeit (High-Availability Lösungen)

Die permanent steigenden Anforderungen an Performance und Verfügbarkeit insbesondere im Bereich von Firewallsystemen als zentrales Nadelöhr für die Internetkommunikation erzwingen Überlegungen und Lösungen hinsichtlich Konzeption von Möglichkeiten für eine dynamische Lastverteilung und redundante Zugangswege. Wesentlich dabei ist die Beibehaltung des einmal definierten und festgestellten Sicherheitsniveaus. Performanceprobleme können keinen Rückschritt z.B. von einem Application Level Gateway auf einen Stateful Inspection Filter begründen. Bei modularer und wohlüberlegter Konzeption von Firewallsystem und Intranet ist es nach Stand der Technik durchaus möglich, auf Basis von mehreren Application Level Gateways eine hochperformante und -verfügbare Lösung zu installieren.

Eine erste Lösungsmöglichkeit besteht in der Einführung einer protokollspezifischen Lastverteilung. So z.B. kann ein Application Level Gateway für HTTP und FTP, ein zweites für EMail und News verantwortlich sein. Erweiterungsfähig ist dieser Ansatz durch eine statische Parallelisierung : Abteilung X benutzt Application Level Gateway 1 und 2, Abteilung Y benutzt Application Level Gateway 3 und 4.

Das anzustrebende Ziel besteht jedoch in einer intelligenten dynamischen Lastverteilung. Eine oder mehrere Lastverteilungskomponenten mit einer virtuellen IP-Adresse zwischen Intranet und Firewallsystem bestimmen z.B. in Abhängigkeit von der aktuellen Auslastung, welches Application Level Gateway von einem Arbeitsplatz-PC aus angesprochen wird. Um diesen Vorgang für die Arbeitsplatz-PCs transparent zu gestalten, wird dort diese virtuelle IP-Adresse als Default-Gateway bzw. Proxy eingetragen.

Eine wichtige Grundlage für eine hochverfügbare Internet-Anbindung kann die Anbindung an zwei Internet-Provider sein. Die zweite, u.U. mit geringerer Kapazität ausgestattete Leitung kann dabei als Wählleitung konzipiert sein, die nur bei Ausfall der Standleitung einspringt. Dabei sollte darauf geachtet werden, zwei voneinander unabhängige Provider zu wählen, die insbesondere mehrere Anbindungen an Internet-Backbones betreiben. Vor Abschluss eines längerfristigen Vertrages sollte mittels eines Test-PCs Performance und Verfügbarkeit des potentiellen Internet-Providers gemessen werden: Im Zeitraum eines Monats kann so durch Messungen von Round-Trip-Zeiten (ping) sowie Messungen zur Wegewahl (traceroute) festgestellt werden, ob Performance-Angaben des Providers und Realität übereinstimmen und damit eine Grundlage für eine hochverfügbare Internet-Anbindung darstellen.

3.7 Auswahl der Komponenten des Firewallsystems

Die Auswahl der Komponenten und einer konkreten Architektur des Firewallsystems kann in Abhängigkeit z.B. folgender Kriterien getroffen werden:

- Gewichtung des zu erzielenden Sicherheitsniveaus und der prinzipiellen Vor- und Nachteile der verschiedenen Filterverfahren (Stateful Inspection oder Application Level Gateway)
- Auswahl eines 2- oder besser 3-stufigen Firewallsystems insbesondere unter Beachtung von für die Zukunft wichtiger modularer Aufrüstbarkeit und Skalierung der Komponenten
- aktuelle oder zukünftig absehbare Anordnung von Informationsservern oder Zugangsservern (RAS) im Bereich des Firewallsystems
- Vorhandensein echter Proxies für zu filternde Protokolle (als Resultat einer Analyse des Kommunikationsprofils); In diesem Rahmen sollte insbesondere auch entschieden werden, dass nicht alle Protokolle sinnvoll über ein Firewallsystem geleitet werden können (z.B. diverse UDP-basierte Dienste, Multicast). Ein weiteres Kriterium ist das Vorliegen generischer Proxies für sonstige Protokolle.
- Anforderungen an Performance und Verfügbarkeit, Abschätzung des Verkehrsaufkommens, Redundanz des Firewallsystems und der Internet-Anbindung,
- übersichtliche Darstellung der aktuellen Konfiguration (Filterregeln etc.) unter einer Administrationsoberfläche
- Stabilitäts- und Sicherheitsanforderungen an zugrundeliegende Betriebssysteme (einschließlich Vertrauenswürdigkeit)
- Beachtung von Exportrestriktionen bei geplanter Nutzung von Verschlüsselungskomponenten
- Vorliegen einer unabhängigen Zertifizierung (ITSEC, Common Criteria)
- Möglichkeiten für eine sichere auf Standards basierende Fernadministration
- Qualität der Applikations-Filter:
- Durchführung von Active Content- bzw. Viren- oder Makro-Filterung, Qualität der Erkennung aller Varianten
- Welche Protokollsequenzen werden kontrolliert ?
- Können interne, nichtöffentliche Informationen zuverlässig verborgen bzw. aus dem Datenstrom entfernt werden (IP-Adressen, DNS-Namen z.B. von EMail-Gateway oder EMail-Clients, Version von Betriebssystemen und Typ der Browser, Existenz interner Proxies, Name und Versionsnummer von Filterkomponenten) ?
- Können weitere unerwünschte Bestandteile z.B. des HTTP-Datenstromes entfernt bzw. ersetzt werden: Cookies, Referer und User-Agent ? Die Filterung der Sequenz "X-forwarded-for" sollte möglich sein, falls die Verbindung intern über einen weiteren Proxy geführt wird. Darüberhinaus sollte die Möglichkeit bestehen, einzelne URLs herauszufiltern (z.B. Werbe- oder Banner-URLs, die intensiven Gebrauch von Cookies machen).

Resultat der konzeptionellen Phase und insbesondere der Beantwortung dieser Kriterien ist die Erarbeitung eines detaillierten Anforderungskataloges für die sich anschließende Ausschreibung und Beschaffung.

3.8 Lösungsbeispiele

Paketfilter auf Basis freier Betriebssysteme

Zu den Einsatzgebieten eines Paketfilters zählen:

- externer oder interner Paketfilter als Ergänzung eines Application Level Gateway
- vor einem Internet-Informationsserver (z.B. WebServer)
- lokale Paketfilter auf einem Application Level Gateway oder Dienste-Server
- Separierung interner Netzbereiche: (z.B. LAN der Personalabteilung vom allgemeinen LAN)

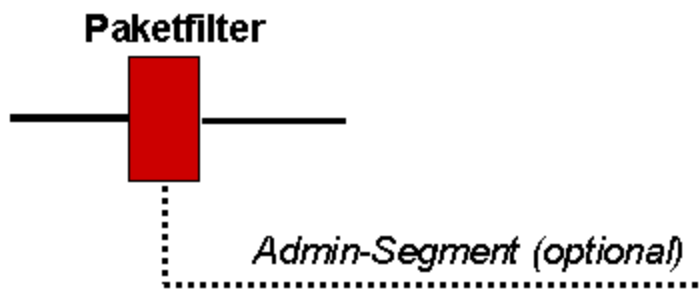
Neben kommerziell erhältlichen Paketfiltern, die in aller Regel als Blackbox mit proprietären Administrationsmechanismen ausgestattet sind, können die in modernen Betriebssystemen bereits integrierten Paketfilter eine praxistaugliche Alternative darstellen, die mit geringem finanziellen und administrativen Aufwand realisier- und betreibbar ist.

Ein hohes Vertrauen in die Implementierung als Folge der Verfügbarkeit des Quellcodes, eine sehr aktuelle und robuste TCP/IP-Implementierung, folglich eine sehr gute Stabilität und gute Widerstandsfähigkeit gegen bestimmte Angriffe sowie eine vergleichsweise hervorragende Transparenz der Komponenten des Betriebssystems begründen eine Eignung frei erhältlicher UNIX-Derivate für den Zweck der Realisierung eines Paketfilters.

Die allgemeine Anforderung zur Konfiguration eines Minimalsystems (keine unnötigen Dienste und Programme etc.) lässt sich exemplarisch anhand eines Linux-Paketfilters demonstrieren, dessen Betriebssystem einschließlich eines Dienstes zur Remote-Administration sowie der notwendigen Paketfilter-Regeln komplett von einer 1,44 MB Floppy geladen wird. An dieser Stelle sei ausdrücklich betont, dass die Reduzierung des Software-Umfangs auf wenige Megabyte aufgrund der überschaubaren Komplexität ein Sicherheitsvorteil ist.

Ein moderner Standard-PC kann als performante Hardwarebasis dienen, wobei eine Festplatte entfallen kann. Einzelne Hardware-Komponenten können bei Bedarf nachgerüstet werden.

In Abhängigkeit von den Anforderungen an Verfügbarkeit, Integrität und Vertraulichkeit der Administrationswege und -protokolle kann der Paketfilter mit einem dritten Netzwerkinterface für ein Admin-Segment (Remote-Administration des Paketfilters sowie Versand von Protokoll Daten und Alarmmeldungen zur Admin-Workstation) ausgestattet werden (Abb. 3.8.a). Alternativ kann eine serielle Schnittstelle genutzt werden.



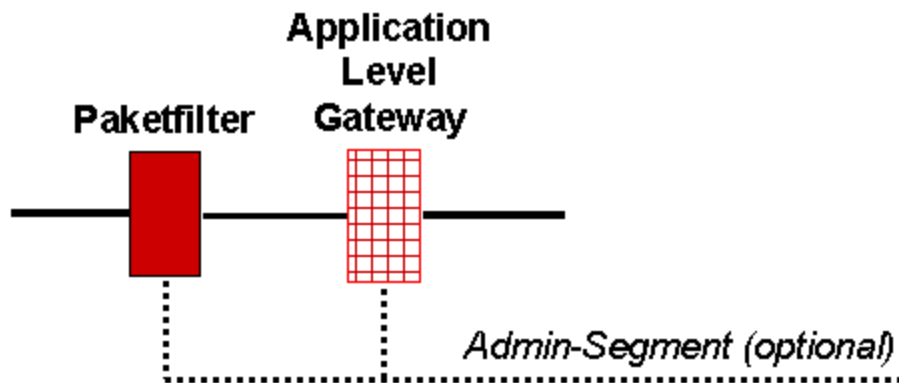
(Abb. 3.8.a) Paketfilter mit separatem Admin-Interface

Bei Konfiguration des entsprechenden Dienstes für die Remote-Administration (z.B. Secure Shell) sollte darauf geachtet werden, die Bindung des Dienstes auf die IP-Adresse des Admin-Interfaces zu beschränken, sodass an externem und internem Interface des Paketfilters kein Netzwerkdienst als potentielles Angriffsziel geöffnet werden muss. Bei alternativer Realisation der Remote-Administration über das normale Netz (kein Admin-Segment) sollte der entsprechende Dienst nur an das interne Interface gebunden werden und durch lokale Filterregeln sichergestellt werden, dass nur die zugelassene Admin-Workstation eine Verbindung herstellen kann. Die einzelnen Schritte für das Herstellen einer solchen Linux-Bootdiskette liegen in Form einer sog. HOWTO-Datei den meisten Linux-Distributionen bei. Für die Konfiguration der Paketfilterregeln ist es in jedem Fall erforderlich, anhand des IT-Sicherheitskonzeptes und des umzusetzenden Kommunikationsprofils eine detaillierte Analyse durchzuführen, aus der dann die konkreten Filterregeln ableitbar sind.

Für die Internet-Anbindung eines LAN reicht eine einzelne Sicherheitskomponente jedoch auf keinen Fall aus. Das damit verbundene Schadens- und Gefährdungspotential kann im Allgemeinen nicht toleriert werden. Prinzipielle Schwächen, die Gefahr von Fehlkonfigurationen, konzeptionellen Schwachstellen und Programmierfehler bedingen eine mindestens 2-stufige Anordnung. Zu empfehlen ist deshalb eine Kombination aus mindestens zwei Sicherheitskomponenten, deren Wirkungsweise auf verschiedenen Filterverfahren beruhen sollte.

2-stufiges Firewallsystem

Bei geringem bis mittlerem Schutzbedarf (vgl. [2]) ist ein 2-stufiges Firewallsystem - bestehend aus Paketfilter und Application Level Gateway - die minimale Anforderung an eine Internet-Anbindung. Zwingend ist eine Realisierung der Komponenten auf getrennten Maschinen, wobei eine Anordnung nacheinander vorgesehen werden sollte (Abb. 3.8.b), sodass eine Umgehung einer Komponente unmöglich ist.



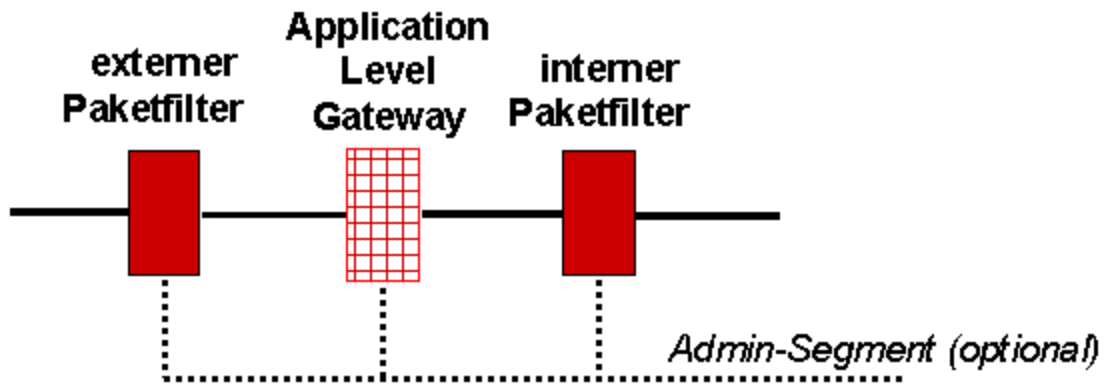
(Abb. 3.8.b) Paketfilter und Application Level Gateway

Bei der Konzipierung muss eine Entscheidung getroffen werden, ob der Paketfilter auf der internen oder externen Seite des Application Level Gateways angeordnet werden soll. Neben dem konkreten Gefährdungspotential muss insbesondere abgeschätzt werden, wie hoch die Wahrscheinlichkeit eines erfolgreichen Angriffes auf das Application Level Gateway ist. Falls diese Gefährdung weitestgehend ausgeschlossen werden kann (z.B. keine Netzwerkdienste auf der externen Seite - keine eingehenden Dienste, sehr stabiler TCP/IP-Stack), mithin hohes Vertrauen darin besteht, dass Angriffe vom Application Level Gateway selbst auf das interne LAN ausgeschlossen sind, kann auf einen internen Paketfilter verzichtet werden. In der Regel bestehen hier aber Zweifel. Daher sollte zusätzlich zum externen ein interner Paketfilter - somit ein 3-stufiges Firewallsystem - zum Einsatz kommen. Als Motivation kann hier angeführt werden, dass ein interner Paketfilter in der Regel sehr einfach zu konfigurieren ist: "erlaube nur nach außen gehende Verbindungen".

Die Alternative, die im Verzicht auf einen externen Paketfilter besteht, hat einen Verlust des Schutzes für das Application Level Gateway zur Folge, der nur in seltenen Fällen toleriert werden kann (z.B. kein hoher Anspruch an Verfügbarkeit).

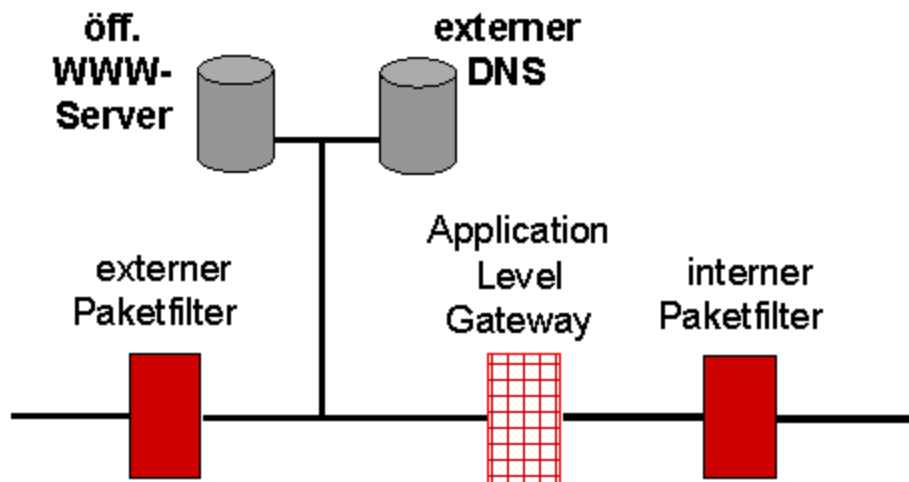
3-stufiges Firewallsystem

Die für eine Internet-Anbindung mittleren, hohen und sehr hohen Schutzbedarfs empfohlene Variante eines Firewallsystems besteht in der Basiskonfiguration aus den Komponenten externer Paketfilter, Application Level Gateway und interner Paketfilter (Abb. 3.8.c).



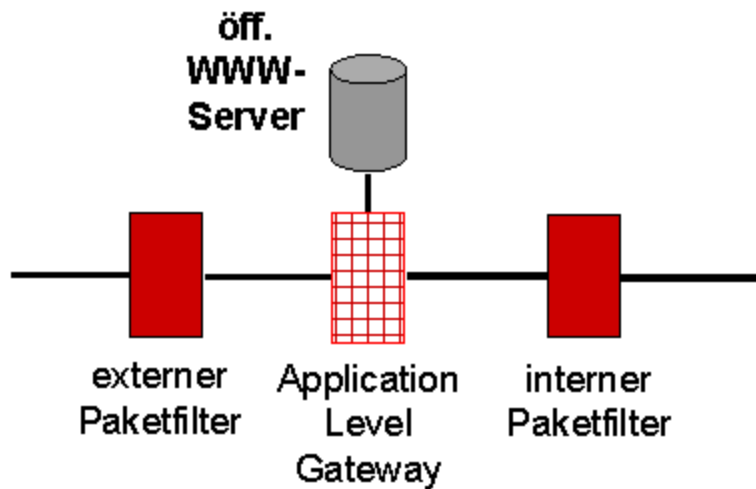
(Abb. 3.8.c) 3-stufiges Firewallsystem - Basiskonfiguration

Neben vorteilhaften Sicherheitseigenschaften bietet diese Anordnung die Voraussetzungen für eine modulare und sichere Integration weiterer Komponenten und Dienste. So können öffentliche Informationsserver (z.B. WWW-Server, DNS-Server) in der externen Demilitarisierten Zone (DMZ) angeordnet werden (Abb. 3.8.d).



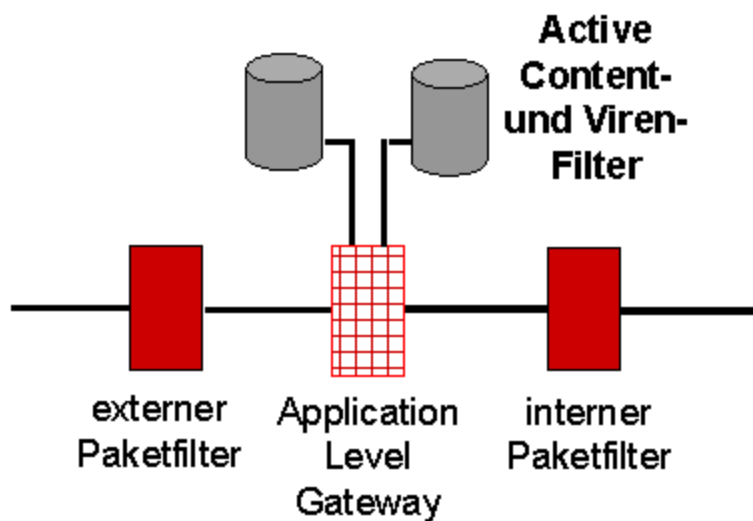
(Abb. 3.8.d) öffentlicher Informationsserver in externer DMZ

Alternativ kann ein zusätzliches Segment am Application Level Gateway für diesen Zweck genutzt werden (Abb. 3.8.e). Der grundsätzliche Vorteil des zusätzlichen Schutzes durch das Application Level Gateway wird mit erhöhten Performance-Anforderungen und einem komplexeren Regelsatz erkauft. Darüberhinaus ist die Unterstützung von mehr als zwei Netzwerkinterfaces eine Voraussetzung für die Produktauswahl.



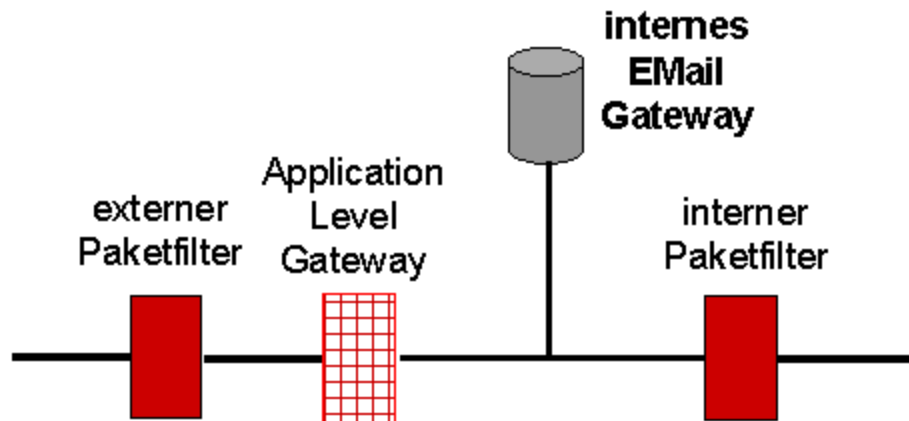
(Abb. 3.8.e) öff. Informationsserver am ALG

Zum Zwecke einer zentralen Active Content- bzw. Virenfilterung kann ein weiteres separates Segment am Application Level Gateway genutzt werden (Abb. 3.8.f). Die Auslagerung dieser rechenzeitintensiven Funktion kann das Application Level Gateways entlasten, hat jedoch im ungünstigsten Fall kaum einen Einfluss auf die Nettodurchsatzrate. Mit Hintergrund der Reduzierung von Komplexität bezüglich Konfiguration und Administrierbarkeit der Software kann eine solche Trennung der Funktionalitäten jedoch sinnvoll sein. Ein wichtiger Aspekt für den Datenaustausch zwischen Firewallsoftware auf dem Application Level Gateway und der Filtersoftware sollte die Interoperabilität des zugrundeliegenden Kommunikationsprotokolls sein (z.B. Content Vector Protocol - CVP).



(Abb. 3.8.f) zusätzl. Active Content Filter am ALG

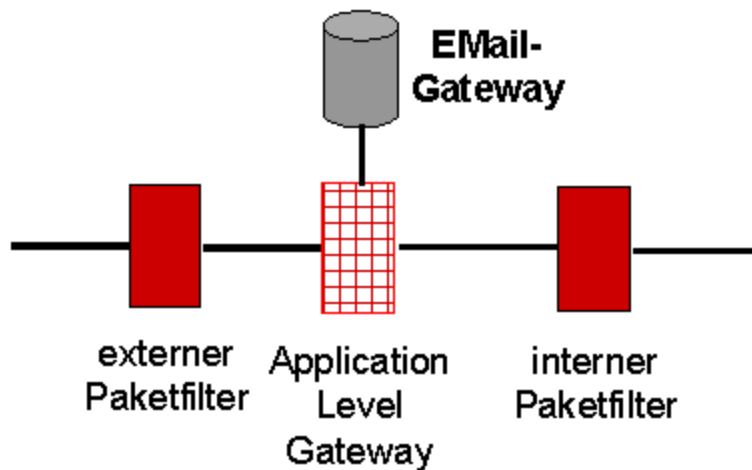
Für EMail-Empfang und Versand geeignet ist die Positionierung eines EMail-Gateways in der internen DMZ (Abb. 3.8.g).



(Abb. 3.8.g) EMail-Gateway in interner DMZ

Von außen eingehende Email wird von einem SMTP-Proxy mit Sicherheitsfunktionalität auf dem Application Level Gateway entgegengenommen und kurzfristig an das interne EMail-Gateway weitergeleitet. Für die umgekehrte Richtung, den EMail-Versand von einem Arbeitsplatz-PC aus nach außen wird von innen über den internen Paketfilter eine Verbindung zum EMail-Gateway hergestellt, welches dann über das Application Level Gateway den Versand nach außen fortsetzt. Eine wichtige Anforderung an den Proxy des Application Level Gateways ist ein Schutz gegen eine Nutzung als Relay (meist in Verbindung mit Versand und Weiterleitung von SPAM-EMail).

Alternativ kann das EMail-Gateway an einem zusätzlichen Segment des Application Level Gateways positioniert werden (Abb. 3.8.h).



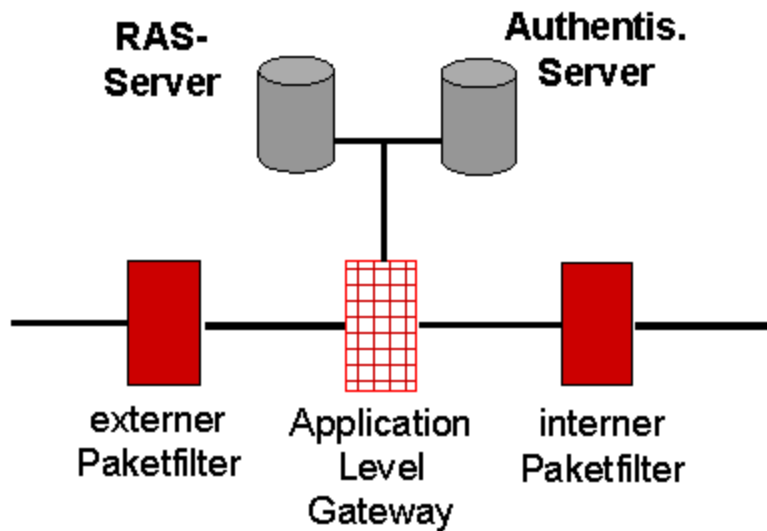
(Abb. 3.8.h) EMail-Gateway an ALG

Dem Vorteil des zusätzlichen Schutzes bei Zugriff aus dem internen LAN auf das EMail-Gateway steht der Nachteil gegenüber, dass die Email zweimal das Application Level Gateway passieren muss.

Bei Abwägung der zwei dargestellten Varianten für Positionierung des EMail-Gateways kann im Rahmen des IT-Sicherheitskonzeptes die interne Absicherung durch einen Paketfilter durchaus hinreichend sein.

Für die stets problembehaftete Integration von Remote Access Services unter Beibehaltung des Sicherheitsniveaus lassen sich mehrere Lösungsvarianten finden. In jedem Fall sollte nach erfolgreicher Einwahl - unter Nutzung qualifizierter kryptographischer Verfahren - eine Begrenzung des möglichen Kommunikationsprofils zwischen Einwahl-Server und dem internen LAN erfolgen. Erforderlich ist daher mindestens ein Paketfilter an dieser Schnittstelle. Eine u.U. wünschenswerte weitere Authentisierung für Zugriff auf interne Ressourcen ist unter Nutzung eines Paketfilters allerdings nicht möglich.

Realisiert werden kann diese Anforderung durch ein weiteres Netzwerksegment am Application Level Gateway (Abb. 3.8.i), wobei der zusätzliche Vorteil dieser Struktur in der unmittelbaren Einschränkung der Kommunikationswege bei einem u.U. erfolgreichen Angriff auf den Einwahl-Server liegt.



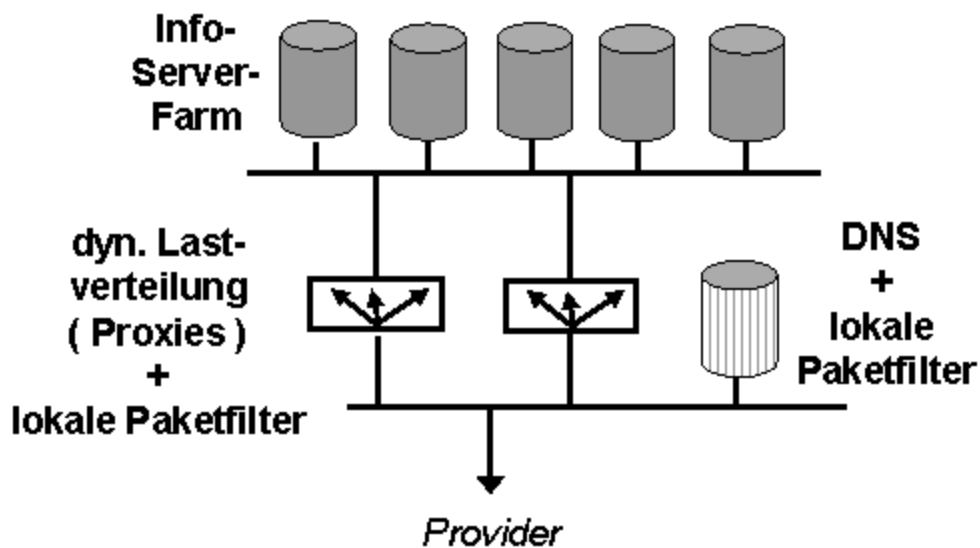
(Abb. 3.8.i) RAS und Authentisierungs-Server am ALG

Hochverfügbarkeit mehrerer Internet-Informationsserver

Die Herausforderung für die Konzipierung liegt hier neben der Sicherstellung einer ausreichenden Performance in der Beachtung und Integration von Sicherheitsaspekten. Dargestellt werden soll exemplarisch die Absicherung einer Hochverfügbarkeitslösung mittels lokaler Paketfilter und Proxies auf vorgeschalteten Sicherheitskomponenten, die zusätzlich für die dynamische Lastverteilung zu den dahinterliegenden Informationsservern verantwortlich sind (Abb. 3.8.k).

Geeignet erscheint dieser Aufbau insbesondere für Server, die bei einer starken Frequentierung pro Anfrage eine hohe lokale Rechenlast erzeugen und deshalb im Sinne einer modularen und ausbaufähigen Anordnung zwingend parallel ausgelegt werden müssen.

Für die Umsetzung der Sicherheitsfunktionalität sind sowohl lokale Paketfilter als auch Proxies verantwortlich. Die lokalen Paketfilter unterbinden dabei unerlaubte Protokolle und Verbindungsaufbauten. Der TCP/IP-Stack der Sicherheitskomponenten sollte immun gegen eine Vielzahl von "Denial of Service" - Angriffen sein. Ferner wird durch die Entkopplung der Kommunikationsverbindung und Nutzung der Proxies eine zusätzliche Schutzfunktion erzielt.

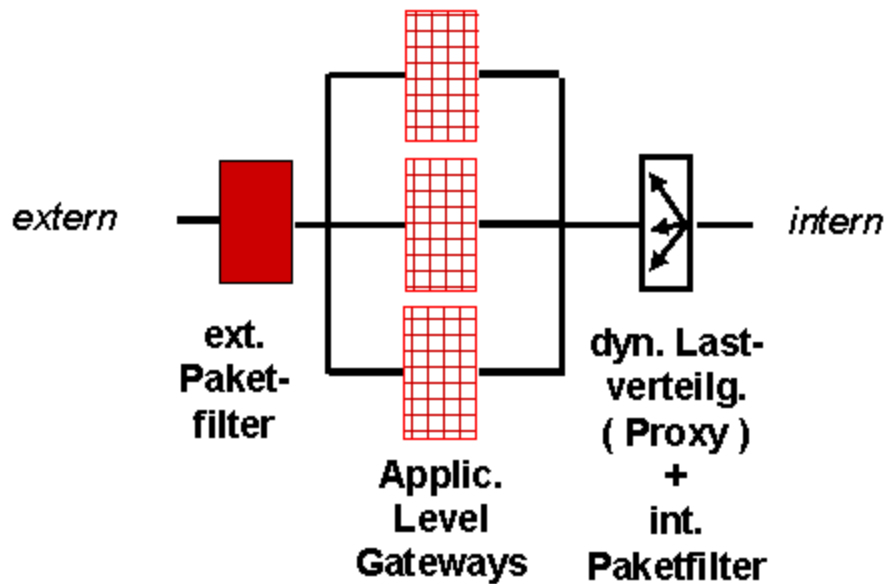


(Abb. 3.8.k) Hochverfüg. und dyn. Lastverteiltg. Infoserver

Erwähnenswert ist die Tatsache, dass ein solcher Proxy die aus Sicherheitsaspekten sehr vorteilhafte Integration von Positiv-Filtern bietet, die in der Lage sind, Angriffe auf Applikationsebene (z.B. böse formulierte URLs) zuverlässig zu unterbinden. Die praktische Einschränkung besteht jedoch darin, dass hier nur Speziallösungen existieren. Um durch die Sicherheitskomponenten keinen neuen Single-Point-of-Failure zu schaffen, sollten diese ebenfalls parallel ausgelegt werden und z.B. über ein DNS Robin Round angesprochen werden. Ferner sollte beachtet werden, die Komponenten in Richtung des Providers ebenfalls redundant auszulegen. Schließlich sei angemerkt, dass eine Reihe von kommerziellen Systemen zur dynamischen Lastverteilung existiert, diese jedoch in der Regel ohne Proxies arbeiten, daher u.U. nur die Möglichkeit bieten, Paketfilter einzurichten. Als Konsequenz wird dann auf diesen Systemen auf die wünschenswerte Entkopplung der Kommunikationsverbindung sowie auf zusätzlich mögliche Applikationsfilter verzichtet.

Sicherheit und dynam. Lastverteilung bei einer Internet-Anbindung

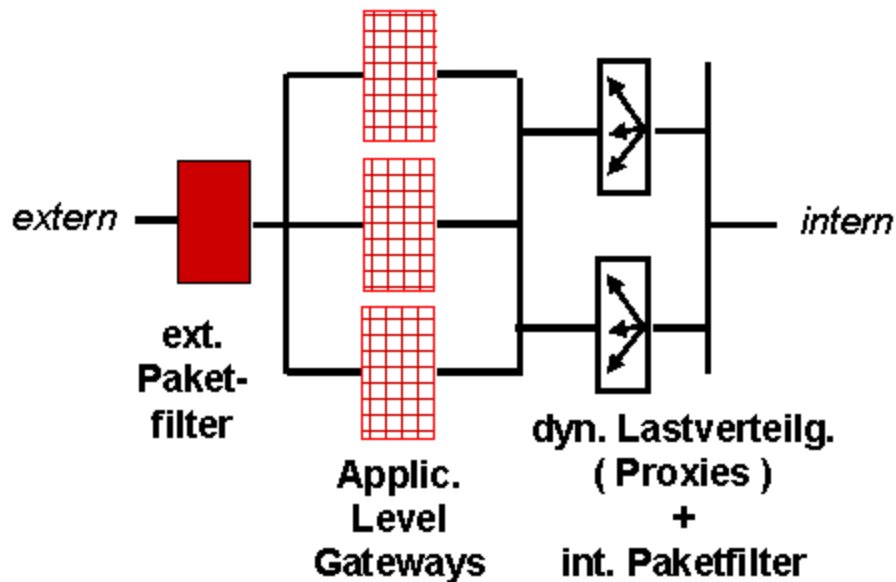
Bereits bei mittelständigen Unternehmens- und Organisationsgrößen können die Anforderungen an einen zuverlässig und annähernd permanent zur Verfügung stehenden Internet-Zugang sehr hoch sein. Im Rahmen der Konzeption des Firewallsystems muss dabei die redundante Auslegung des internen LAN (z.B. Backbone in Ringform) fortgesetzt werden. Die hier vorgestellte Lösung basiert auf einem internen Proxy, der die Kommunikationsanforderungen dynamisch auf eine parallele Anordnung von Application Level Gateways weiterleitet (Abb. 3.8.1).



(Abb. 3.8.1) Dynamische Lastverteilung durch 1 Proxy

Zusätzlich aktivierte lokale Paketfilter auf der Proxy-Maschine bilden die Funktionalität eines internen Paketfilters nach. Wesentlich in dieser Anordnung ist die Deaktivierung des IP-Routings, womit sichergestellt werden kann, dass sämtliche Kommunikationsanforderungen über diesen Proxy geleitet werden. Auf der Proxy-Maschine können sog. generische Proxies (tcprelay, plug-gw etc.) zum Einsatz kommen. Die eigentliche Sicherheitsfunktionalität auf Anwendungsebene wird von den Application Level Gateways übernommen.

Für erhöhte Verfügbarkeits- bzw. Performance-Anforderungen kann diese Basisvariante durch einen zweiten parallel geschalteten Proxy modular erweitert werden (Abb. 3.8.m).



(Abb. 3.8.m) Dynamische Lastverteilung durch 2 Proxies

Die Lastverteilung aus dem internen LAN auf die beiden Proxies kann mittels DNS Round Robin vorgenommen werden, wofür den zwei IP-Adressen von Proxy-1 und Proxy-2 nur ein symbolischer Name zugeordnet wird. Für die Internet-Nutzung ist es dann erforderlich, auf den Arbeitsplatz-PCs den symbolischen Namen des Proxy einzutragen. Eine DNS-Abfrage beim DNS-Server sorgt dann für die Zuordnung einer der beiden IP-Adressen. Eine wichtige Voraussetzung für die Anwendbarkeit von DNS Round Robin ist die Begrenzung der lokalen Cache-Zeiten nach einer einmaligen DNS-Abfrage. Ziel sollte es sein, bei jeder neuen Session eine erneute Abfrage beim DNS-Server zu initiieren.

Um eine Abhängigkeit von einem DNS-Server auszuschließen, sollte eine Aufteilung in Primary und Secondary DNS vorgesehen werden.

Für eine zeitnahe Reaktion bei Ausfall eines Proxy ist die Integration der beiden Proxies in eine betriebliche Überwachung der Komponenten vorzusehen. Bei Ausfall oder Wartungsarbeiten an einem der beiden Proxies ist es dann notwendig, die DNS-Konfiguration so anzupassen, dass der symbolische Name nur noch in die IP-Adresse des einen funktionierenden Proxy aufgelöst wird.

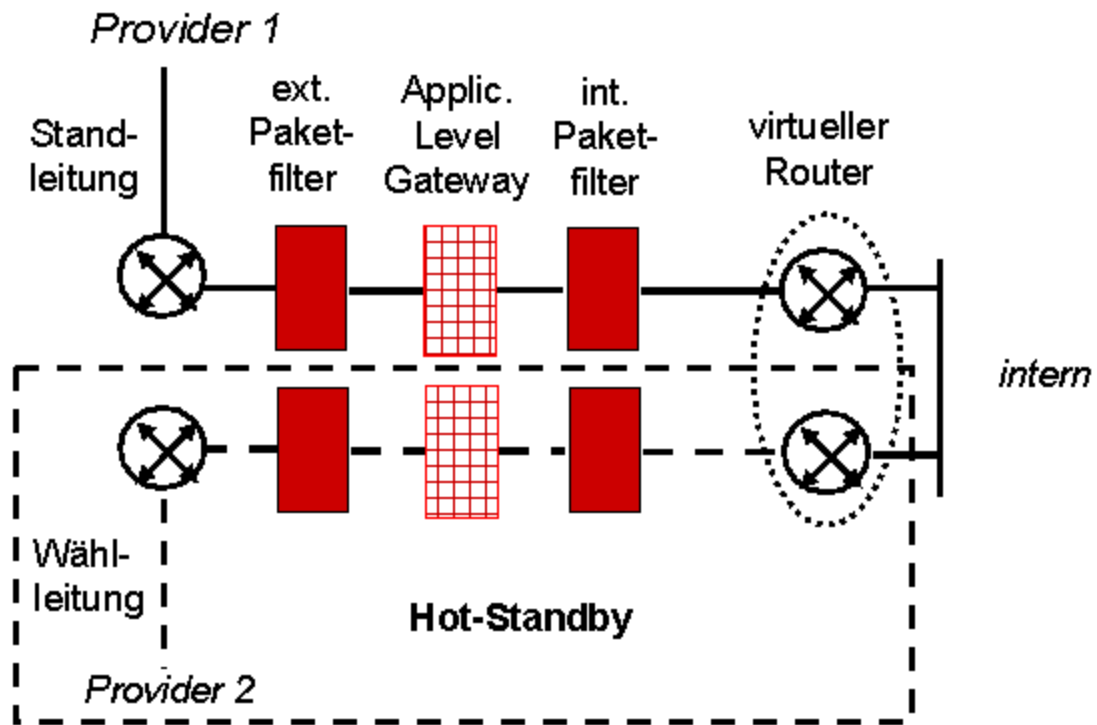
Bei Konzipierung einer Hot-Standby Lösung (nur ein Proxy einschl. nachgeschaltetem Application Level Gateway im Wirkbetrieb) sind äquivalente DNS-Anpassungen erforderlich. Im Fehlerfall kann dann zeitnah auf die Backup-Strecke umgeschaltet werden.

Nicht unerwähnt soll bleiben, dass der externe Paketfilter einen Single-Point-of-Failure darstellt. Um hier das Risiko zu minimieren, sollte eine Cold-Standby-Lösung oder eine ebenfalls parallele Auslegung in Erwägung gezogen werden.

Nicht jede Anwendung besitzt die Fähigkeit, über Proxies hinweg Kommunikationsbeziehungen aufzubauen (sog. proxy-awareness). Für diese Programme können sog. transparente Proxies zum Einsatz kommen. Ein Vorteil dieses Lösungsweges besteht darin, dass die Anwendungen nicht angepasst oder speziell konfiguriert werden müssen, was insbesondere bei einer großen Anzahl von Clients ein positiver Nebeneffekt ist, der den Wartungsaufwand reduzieren kann. Redundanz und Lastverteilung müssen jedoch dann über Routing-Mechanismen gelöst werden.

Hochverfügbarkeit einer Internet-Anbindung (Virtueller Router)

Um die Abhängigkeit von einem einzigen Internet-Provider zu reduzieren und gleichzeitig eine redundante Firewall-Lösung zu betreiben, kann eine Struktur aus einem internen virtuellen Router, einer doppelten Anordnung von internem Paketfilter, Application Level Gateway, externem Paketfilter und Zugangsroutern zum Provider konzipiert werden (Abb. 3.8.n).



(Abb. 3.8.n) Hochverfügbarkeit einer Internet-Anbindung

Aus Sicht des internen LAN existiert als Übergang in das Internet ein Default-Gateway, welches die IP-Adresse des Virtuellen Routers darstellt. Über ein spezielles Protokoll wird zwischen den beiden Routern festgelegt, wer für die Weiterleitung des

Datenverkehrs verantwortlich ist. Im Fehlerfall eines Routers übernimmt dann der andere die Arbeit (Hot-Standby).

Eine parallele Auslegung der Application Level Gateways in Verbindung mit einer vorgeschalteten Komponente für die dynamische Lastverteilung kann bei steigenden Performance-Anforderungen geboten sein, erhöht jedoch die Komplexität und den Betriebsaufwand beträchtlich.

4. Audit

Der Begriff Audit im weiteren Sinne bezeichnet hier ein Framework aus kontinuierlicher betrieblicher Überwachung, interner IT-Revision und einer unabhängigen, vorzugsweise externen Revision bzw. IT-Sicherheitsüberprüfung.

Hohe Verfügbarkeits- und Sicherheitsanforderungen an die IT-Strukturen lassen sich nur durch eine permanente betriebliche Überwachung sicherstellen. Unerlässlicher Bestandteil der Konzipierung eines Firewallsystems ist daher die Überwachung der Komponenten und des Gesamtsystems.

4.1 Betriebsüberwachung

Erste Voraussetzung für eine effiziente Betriebsüberwachung sind neben zentralen Administrationswegen standardkonforme und sichere Management-Protokolle. Eine Integration der Überwachung des Firewallsystems in u.U. bereits bestehende zentrale Überwachungs- und Managementstationen ist anzustreben. Eine sinnvolle Arbeitsteilung in größeren Netzwerktopologien kann in einer Vorauswertung der Ereignisse im Bereich des Firewallsystems durch die zugehörige Admin-Workstation bestehen. Das Ergebnis dieser Vorauswertung kann danach zur zentralen Überwachungs- und Managementstation gesandt werden.

4.2 Interne Revision

Für die Durchführung der internen Revision kann insbesondere in größeren Strukturen ein speziell geschultes Team zur Verfügung stehen. In Ermangelung entsprechender personeller Ressourcen kann innerhalb des Firewall-Betriebspersonals einer Person diese Aufgabe zugewiesen werden. In geeigneten Abständen werden dann systematische Kontrollen hinsichtlich Organisation des Betriebs und der aktuellen Konfiguration vorgenommen. Das Ergebnis sollte in schriftlicher Form dem Management vorgelegt werden.

4.3 Unabhängige Sicherheitsüberprüfung

Betriebliche Überwachung der Komponenten und interne Revision sind Grundlagen für eine korrekte und wirksame Umsetzung der Sicherheitsmaßnahmen, können eine unabhängige Überprüfung des IT-Sicherheitskonzeptes auf Vollständigkeit, Widerspruchsfreiheit und Angemessenheit der Maßnahmen jedoch nicht ersetzen. Neben der theoretischen Prüfung des IT-Sicherheitskonzeptes zählt die Verifikation der korrekten Umsetzung in Form des Firewallsystems vor Ort, mithin die Aufdeckung von Schwachstellen und die Formulierung von konkreten Empfehlungen zur Verbesserung des IT-Sicherheitsniveaus zu den Zielen der Überprüfung. Ein weiterer Aspekt kann die Durchführung eines Angriffes sein, um die praktische Anwendbarkeit des Notfallkonzeptes zu testen. In Absprache aller Beteiligten kann exemplarisch folgender Ablauf gewählt werden:

- erstes Vorgespräch, in dem der Auftraggeber seine Erwartungen darlegt und der Auftragnehmer seine Vorgehensweise erläutert
- schriftliche, vertragsrelevante Fixierung folgender Aspekte: Prüfumfang, Prüfungsschwerpunkte, Prüfzeitraum, personeller und finanzieller Aufwand, konkrete Arbeitsabläufe (Black- und oder Whitebox-Test), Risikoaufklärung (Denial of Service-Angriffe), Umfang und Format des Prüfprotokolls, Haftungsmodalitäten, vertrauliche Behandlung sämtlicher Ergebnisse
- Durchführung eines Blackbox-Tests über das Internet (ein sog. Penetrationstest kann hier Bestandteil sein)
- erste Darstellung der Ergebnisse
- Fortsetzung in einem Whitebox-Test unter Begutachtung des IT-Sicherheitskonzeptes mit Schwerpunkt Firewallsystem
- Prüfung der Realität vor Ort auf Konformität zum IT-Sicherheitskonzept als nächster Schritt des Whitebox-Tests
- abschließende Diskussion der Resultate
- schriftliche Stellungnahme mit Interpretation der Ergebnisse und - falls erforderlich - mit konkreten Verbesserungsvorschlägen

Ein alleiniger Blackbox-Test oder gar nur ein Penetrationstest von außen ist für eine qualifizierte Beurteilung der Internet-Anbindung unzureichend. Die komplexen Netzwerkstrukturen mit vielfältigen Schwachpunkten sowie das erhebliche Potential von Innentätern erfordern eine Vorgehensweise im Sinne eines Whitebox-Tests.

5. Fazit

Die heutigen Kommunikationsstrukturen lassen sich in einem hohen Maße zuverlässig absichern. Sicherheit, Performance und Hochverfügbarkeit müssen dabei keine sich

widersprechenden Anforderungen sein. Anhand von Beispiellösungen wurde demonstriert, wie Sicherheitsanforderungen bei einer Internet-Anbindung umgesetzt und kontrolliert werden können. Dabei ist der zum Teil beträchtliche Aufwand dem Nutzen gegenüberzustellen, zu bewerten und unter Betrachtung des Gefährdungs- und Schadenspotentials eine Entscheidung zu treffen.

6. Literatur

- [1] S. Garfinkel, G. Spafford : Practical Unix & Internet Security, O'Reilly 1996
- [2] IT-Grundschutzhandbuch, BSI 1999
- [3] W. Cheswick, S. Bellovin : Firewalls und Sicherheit im Internet, Addison-Wesley '96
- [4] B. Chapman, E. Zwicky : Einrichten von Internet Firewalls, O'Reilly 1998
- [5] W. Stevens : TCP/IP Illustrated Vol.I/II, Addison-Wesley 1994
- [6] Sicherheit im Internet, [Informationsangebot des BSI](#)
- [7] [Firewall-Studie im Auftrag des BSI 1997](#)
- [8] [IDS Studie im Auftrag des BSI 1998](#)
- [9] T. Veit : Sicherheitsüberprüfung einer Internet-Anbindung, 6. Deutscher IT-Sicherheitskongress des BSI 1999