Der kleinste gemeinsame Nenner

Ausgewählte Firewalls in der Gegenüberstellung

Kai-Oliver Detken

Die Sicherung von lokalen Netzen vor Außenangriffen erfordert den Einsatz von Firewalls, allerdings stehen hier viele Unternehmen mittlerweile vor der Entscheidung, welche Lösung zum Einsatz kommen soll. Legt man ihre Funktionsweise zugrunde, lassen Firewalls sich hauptsächlich in Paketfilter und Applikationsfilter (Proxies) unterteilen. Paketfilter-Produkte entscheiden über das Weiterleiten oder Ablehnen von Paketen aufgrund der Daten in den Protokoll-Headern. Bei Applikationsfiltern dagegen trennt die Firewall die Kommunikationsbeziehung und agiert als Proxy-Server. Dies ermöglicht eine Analyse der Daten auf Anwendungsebene. Paketfilter sind leistungsfähiger als Applikationsfilter, bieten jedoch weniger Sicherheit.

Kai-Oliver Detken ist Senior IT Consultant der Detken Consultancy & Internet Technologies e.K. sowie Dozent und freier Autor in Grasberg

Eine Firewall ist eine Barriere zwischen zwei Netzen, die überwunden werden muß, um Systeme im jeweils anderen Netz zu erreichen. Dabei muß dafür gesorgt werden, daß jede Kommunikation zwischen beiden Netzen über eine Firewall stattfindet. Auf der Firewall sorgen Zugriffskontrolle und Audit dafür, daß das Prinzip der geringsten Berechtigung durchgesetzt wird und potentielle Angriffe so schnell wie möglich erkannt werden.

Da jede Kommunikation über die Firewall geführt wird, ermöglicht diese das Durchsetzen einer Sicherheitspolitik bzw. Security Policy. Die zu diesem Zweck eingesetzten Maßnahmen wirken in beide Richtungen:

- Outbound: Benutzerzugriff auf das Internet aus dem Intranet;
- Inbound: aus dem Internet auf öffentliche Angebote bzw. Dienste durch anonyme Benutzer;
- Inbound: auf Dienste für einen geschlossenen, definierten Teilnehmerkreis.

Nicht alle Firewalls sind in der Lage, alle Bereiche abzudecken. Zu beachten ist auch, daß mit steigender Komplexität der Firewall für höchstmögliche Sicherheit Einbußen in der Performance einzukalkulieren sind. Begnügt man sich hingegen mit weniger Sicherheitsmechanismen, so ist auch das Intranet von außen anfälliger.

Bei den heutigen Firewalls unterscheidet man im wesentlichen vier Konzepttypen:

- statisches Paketfilter;
- dynamisches Paketfilter (Paketfilter, die Kontext speichern können);
- Applikationsfilter (Application Gateway);
- überwachtes Applikationsfilter.

Sie können technisch unterschiedlich realisiert werden. Das statische oder dynamische Paketfilter wird meist auf einem Router eingerichtet, während Applikationsfilter auf einer Workstation (Bastion-Host) installiert werden. Eine Kombination beider Typen nutzt einen Bastion-Host mit einer durch Paketfilter geschützten demilitarisierten Zone, d.h., dem Applikationsfilter sind Paketfilter vor- und nachgeschaltet.

Vom Paketfilter zum Screened Subnet

Aufgabe des *Paketfilters* ist es, anhand der IP-Adressen und Portnummern Sockets zu sperren oder zu erlauben. In den hierzu notwendigen Filterregeln, die aus der zu definierenden Sicherheitspolitik abgeleitet werden, werden obige Daten verwendet, um z.B. UDP-Dienste generell zu sperren oder gewisse TCP-Dienste (via Portnummer) zu erlauben.

Das Paketfilter schützt das innere Netz vor unerwünschten Verbindungen sowie IP-Spoofing (Fälschen der Quelladresse). Bei letzterem muß das Paketfilter in seinen Regeln den physikalischen I/O-Port referenzieren, um gefälschte Quelladressen des zu schützenden Netzes auf dem äußeren I/O-Port erkennen und abweisen zu können. Die Konfiguration von Paketfiltern erfolgt in drei Schritten:

- Festlegen einer Sicherheitspolitik (was ist erlaubt, was ist verboten);
- mittels obiger Aussagen werden die

Das Thema in Kürze

Gegenstand des Beitrages sind die vier verschiedenen Konzepttypen, in die Firewalls heutzutage unterschieden werden. Neben der Darstellung ihrer technischen Realisierung und voneinander abweichenden Sicherheitsmechanismen wird ausführlich auf ihre jeweiligen Vor- und Nachteile eingegangen. Darüber hinaus werden vier am Markt erhältliche Firewalls verschiedener Hersteller in ihren Eigenschaften einander gegenübergestellt.

zugelassenen Pakettypen formal spezifiziert;
- abschließend werden diese formalen Spezifikationen in die Syntax des Paketfilters übersetzt.

Die dabei entstehenden Regeln wendet das Paketfilter streng sequentiell an. Sobald eine Regel auf ein Paket zutrifft, bricht die Regelprüfung ab und die betreffende Regel wird auf dieses Paket angewendet. Danach wird die Regelprüfung für das nächste Paket ausgeführt. Pakete, die nicht explizit durch eine Filterregel zugelassen sind, müssen somit durch eine abschließende generelle Sperregel abgewiesen werden.

Vorteile des statischen Paketfilters sind die relativ einfache Handhabung sowie der geringe finanzielle und zeitliche Aufwand bei der Installation. Hinzu kommt, daß in der Regel für die Anbindung an das externe Netz ohnehin ein Router benötigt wird, der heute zumeist die Funktionalität eines statischen Paketfilters bereits integriert hat. Nachteile sind hauptsächlich die Einschränkungen bei den Filterregeln: Es können nur die Dienste ohne Sicherheitsrisiko durchgelassen werden, die feste Portnummern verwenden und verbindungsorientiert arbeiten – also TCP-Pakete. Bei UDP-Paketen ist es auf UDP-Ebene nicht möglich festzustellen, ob es sich um eine Anfrage oder eine Antwort handelt. Daher sind UDP-Pakete durch statische Paketfilter nur sicher handhabbar, wenn es sich um Dienste handelt, bei denen sichergestellt ist, daß sie keinen Schaden anrichten .

Dynamische Paketfilter können zusätzlich zur Filterungsfähigkeit auf IP- und TCP-Ebene Kontext (Stateful Inspection) sowie nach außen gesendete UDP-Pakete speichern. Dadurch besteht die Möglichkeit, nur erwartete Antworten durch den Filtermechanismus passieren zu lassen. Für sie gelten nur diejenigen Pakete als Antwort, die vom selben Rechner und vom selben Port kommen, an den die Anfrage ursprünglich gerichtet wurde und deren Ziel derselbe Rechner und derselbe Port ist, von dem die Anfrage ausging. Ebenso müssen Quelladresse und -port des ankommenden Paketes mit Zieladresse und -port eines zuvor gesendeten Paketes übereinstimmen.

Applikationsfilter laufen üblicherweise auf sog. multi-homed Hosts, d.h. auf Rechnern mit zwei oder mehreren Netzkarten. Von Vorteil ist hierbei die Möglichkeit, zusätzlich zur Paketfilterung protokollabhängige Informationen auf Anwendungsebene (im TCP/IP-Stack) zu speichern. Dies geschieht durch Proxy-Dienste auf dem Applikationsfilter. Da das Applikationsfilter Angriffen direkt ausgesetzt ist, sollten unbedingt die folgenden Prinzipien gelten:
- nur fehlerfreie Software einsetzen;
- nur die notwendige Software installieren und aktivieren;
- keine grafische Oberfläche und keine Benutzer auf dem Applikationsfilter.

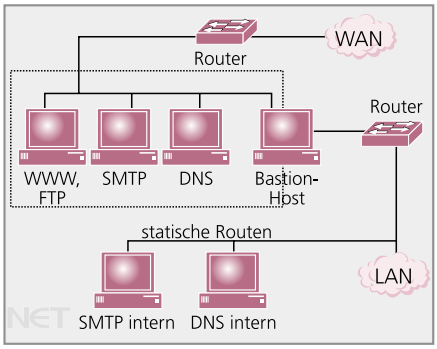
Technisch gesehen verbindet sich bei dieser Lösung der Client nicht direkt mit dem Server, sondern mit dem Proxy auf dem Bastion-Host. Dieser wiederum kontaktiert den eigentlichen Server. Weil der Proxy protokollspezifisch ist und sich inmitten der Verbindung befindet, können die benötigten Kontextdaten gespeichert werden. Ein Vorteil ist die protokollspezifische Filterung auf Applikationsebene. Dabei untersucht der Proxy die Nutzdaten und entscheidet, ob Befehle, Dateiangaben oder Programme der Sicherheitspolitik entsprechen.

Ein weiterer Vorteil ist die Möglichkeit, zusätzliche Funktionalität wie erweiterte Protokollierung oder Sicherheitsmaßnahmen einfügen zu können. Letztere erlauben es überhaupt erst, Telnet- oder FTP-Verbindungen von außen zuzulassen, ohne gravierende Sicherheitseinbußen hinnehmen zu müssen.

Wird für das Applikationsfilter ein multi-homed Host verwendet, ist darauf zu achten, daß das oftmals bereits eingestellte IP-Forwarding unterbunden wird, da sonst die Filterung unterwandert werden kann. Die Pakete würden direkt (innerhalb des Betriebssystemkerns) weitergeleitet werden.

Vorteile des Applikationsfilters sind die (weitgehende) Abkopplung der internen Rechner vom äußeren Netz, umfassendere Protokollierungsmöglichkeiten sowie der Einsatz verstärkter Sicherheitsmaßnahmen. Ein weiterer Vorteil ist die Konzentation sicherheitstechnisch relevanter Programme auf einem Rechne.

Von Nachteil ist, daß ein Applikationsfilter sowohl von außen als auch von innen direkt angreifbar ist. Sollte also ein Dienst irgendeine nutzbare Schwäche haben, so ist die Gefahr für das Applikationsfilter sehr groß. Weiterhin läßt sich die Struktur des inneren Netzes nicht vor dem äußeren Netz verbergen, ohne daß auf dem Applikationsfilter nur die unbedingt notwendige Software abläuft. Für jeden Dienst muß ein dedizierter Proxy zur Verfügung gestellt werden. Dies kann dazu führen, daß einige Dienste dem internen Benutzer nicht zur Verfügung stehen, sofern kein generischer Proxy vorhanden ist. Auch ist der Datendurchsatz bei gleicher Rechenleistung gegenüber Paketfiltern geringer, da jedes Paket bis zur Applikationsebene hochgereicht wird.



Überwachter Bastion-Host

Überwachte Applikationsfilter sind Applikationsfilter, die ihrerseits durch Paketfilter gegenüber dem externen und internen Netz abgeschirmt sind (Screened Subnet). Durch das Vor- und Nachschalten von Paketfiltern wird gewährleistet, daß jeglicher Datenverkehr über das Applikationsfilter geleitet wird. Außerdem schützen die Paketfilter das Applikationsfilter vor Angriffen aus dem Internet (und von innen) und verhindern, daß die Folgen einer Kompromittierung des Applikationsfilters in vollem Umfang bis in das zu schützende Netz vordringen. Ferner können durch vor- und nachgeschaltete Paketfilter bereits viele Pakete abgewiesen werden, so daß die Performance des Applikationsfilters nicht zu sehr beansprucht wird (*Bild*).

Außerdem können Dienste wie DNS

und SMTP getrennt nach internem und externem Netz implementiert werden, wodurch die Struktur des internen Netzes verborgen werden kann und sich zudem Angriffsmöglichkeiten verringern.
Neben reinen Softwarelösungen werden Firewall-Systeme auch als sog. Appliances bezeichnet. Die softwaregestützten Produkte laufen auf Plattformen wie Sun Solaris, Linux oder Windows NT/2000 und integrieren häufig zusätzliche Dienste wie Mail- oder Web-Server. Eine Firewall-Appliance dagegen ist eine kombinierte Hard- und Softwarelösung, die die Einhaltung der vom Administrator festgelegten Regeln für die Zugangskontrolle überwacht. Je nach Produktstrategie kann auch eine Appliance zusätzliche Dienste realisieren, z.B. Network Address Translation (NAT), Tunneling für Virtual Private Networks (VPN), WebProxy, Mail-Server, Aufspüren von Angriffsversuchen oder Aufzeichnungs- und Alarmfunktionen.

	Checkpoint FW-1	Symantec Enterprise Firewall	SunScreen Secure Net	Cisco PIX Firewall
Fernadministration	zentrale Fernadministration	ja	ja	ja
administrative Rollen	Administrator und Revisor	keine	4 verschiedene Zugriffsmodelle: Read, Status, Write, All	keine
Revisionsfähigkeit	vorhanden, ohne Rücksicht auf Betriebssystem	vorhanden; ohne Trennung zwischen Administrator und Revisor	vorhanden; unterstützt durch unterschiedliche Rollen	vorhanden; ohne Trennung zwischen Administrator und Revisor
Fernrevision	nein	keine Trennung zwischen Nah- und Fernadministration	ja	ja
Paketfilter	möglich; ohne Einbeziehung von TCP- und IP-Optionen	Paketfilter vorhanden; kann nicht unabhängig von den Proxy-Diensten verwendet werden	möglich; ohne Einbeziehung von TCP- und IP-Optionen sowie unzureichende Einbeziehung fragmentierter Pakete	möglich; ohne Verifizieren von fragmentierten Paketen
Application Proxy	möglich; ohne transparenten Betrieb von http-Proxies; NNTP; generischer Proxy	vorhanden; Skriptsprachen und ausführbarer Code können nur unzureichend gefiltert werden	unzureichend möglich; ohne Sperrung aktiver Inhalte; kein generischer Proxy	unzureichend möglich; ohne Sperrung aktiver Inhalte; Cut-Through-Proxy
Protokollierung	Auswertung der Logdateien	Auswertung der Logdateien ohne zentrale Administration	Auswertung der Logdateien ohne GUI-Oberfläche	zentrale Auswertung der Logdateien
Archivierung	k.A.	ja	ja	ja
Alarmierung	ja	ja	nicht ausreichend; Standardangriffe werden nicht erkannt	ja
Authentifizierung	interne/externe Benutzer werden erkannt (auch über LDAP möglich)	interne/externe Benutzer werden erkannt	Authentifizierung wird den internen Nutzern nur durch Proxies angeboten	interne/externe Benutzer werden erkannt (TACACS+ und RADIUS)
Integritätsschutz	nicht ausreichend	über Zusatzprodukte möglich	nicht ausreichend	nicht ausreichend
IDS-Systeme	können eingebunden werden	können eingebunden werden	nicht ausreichend	können eingebunden werden
VPN	können eingebunden werden oder eigene Erweiterung	können eingebunden werden	teilweise möglich; es fehlen IPv6- oder Directory-Dienste	können eingebunden werden oder eigene Erweiterung
Virenscanner	können eingebunden werden	können eingebunden werden	nicht ausreichend	kein Virenscanner
Clustering	ja	ja	ja	nein
Hochverfügbarkeit	ja ist gegeben	ja ist gegeben	ja	ja

Produktvergleich von Firewall-Systemen

Firewall-Systeme im Vergleich

Aus Platzgründen konnte leider nur eine kleine Auswahl von Firewall-Systemen verglichen werden (*Tabelle*).
Die zentrale Komponente der *Firewall-1* der israelischen Firma *Check Point* wurde Schritt für Schritt um Zusatzfunktionalitäten erweitert und läßt sich auch in komplexe Umgebungen mit hohen Anforderungen gut integrieren. Dennoch ist sie in erster Linie ein dynamischer Paketfilter für Windows NT/2000, Linux, AIX, HP-UX und Solaris. Proxies werden nur für wenige Protokolle angeboten.
Vor- und Nachteile:

- gute Einbindung in ein umfassendes Netzsicherheitsmanagement, Konfigurieren und Überwachen von Routern und Switche verschiedener Hersteller mit Administrationskonsole;
- zur Unterstützung gemeinsamer Schnittstellen und Prinzipien können eine Reihe von Produkten anderer Herstellern verwendet werden;
- Zertifizierung bereits 1999 nach ITSEC E3 sowie von ICSA;
- Vernachlässigung der Proxy-Dienste;
- unvollständige Standarddokumentation;
- Defizite bei partiellen Ausfällen und im fehlenden Integritätstest.

Die *Symantec Enterprise Firewall* vereinigt die ehemalige Raptor Firewall von Axent und die Merkmale Personal Firewall von Symantec und Virenfilter von Norton. IDS-Produkte werden als Ergänzung angeboten. Sie ist als Proxy-Firewall konzipiert und für Windows NT/2000 und Solaris verfügbar. Generic Service Passer (GSP) können Paketfilterfunktionen nachbilden.
Vor- und Nachteile:

- intuitive Administration mit dem GUI;
- sehr schnelle Proxy bzgl. der Performance;
- Zertifizierung von der ICSA;
- keine Revisionsfähigkeit;
- wenig Hilfestellung hinsichtlich der Filterung von ausführbarem Code durch die Proxy-Dienste;
- keine Möglichkeit, interne Informationen wie HTTP oder E-Mail-Header zu filtern;

- kein Erfassen abgewiesener Pakete bei der Protokollierung.

Die *SunScreen Secure Net* von *Sun Microsystems* ist in erster Linie ein Paketfilter, das auf Solaris einsetzbar ist. Proxies werden nur für wenige Protokolle angeboten. Der Hersteller setzt das Prinzip der Stateful Inspection ein.
Vor- und Nachteile:

- intuitive Installation und Administration, beispielsweise. können verschiedene Regelwerke mit eigenen Versionsnummern versehen, gespeichert und reaktiviert werden);
- Möglichkeit des Definierens verschiedener administrativer Rollen und somit von Revisionsfunktionen;
- Vorgabe unterschiedlicher Regelwerke (Restrictive, Secure, Permissive) erleichtert Standardinstallation;
- Prüfen des Regelwerks auf Überlappungen und Fehlkonfigurationen während des Speicherns, kein Aktivieren der Policy bei auftretenden Fehlern;
- zertifiziert nach CC EAL2, ICSA und ITSEC (versionsabhängig);
- relevante Sicherheitskriterien an Paketfilter und Proxy werden nicht erfüllt;
- zukünftige Produktversionen versprechen bei der funktionalen Erweiterung der Proxies und der VPN-Unterstützung Verbesserungen.

Die *PIX Firewall* von *Cisco Systems* bildet neben zusätzlichen Varianten für das IOS oder für IDS die Basis der Sicherheitsprodukte von Cisco. Dabei können Beschleunigerkarten für die Verschlüsselung eingesetzt werden. Die Einbindung ins Netz erfolgt über ein Terminalprogramm oder einen Webbrowser. Die weiteren Einstellungen kann der Administrator dann von beliebiger Stelle aus mit einem Standardbrowser durchführen.
Vor- und Nachteile:

- sehr viele parallele Sessions möglich;
- bekannte IOS-Kommandozeile;
- sehr gute Performance bei Verwendung von Beschleunigerkarten selbst bei verschlüsseltem VPN;
- ohne Beschleunigerkarte nur mäßige Performance bei Verschlüsselung;
- Fehlen europäischer Zertifikate bei den verschiedenen Versionen;
- schwieriges Bedienen von IOS für Nichtkenner.

Fazit

Bei der Auswahl einer speziellen Firewall ist es nicht ausschlaggebend, jedes einzelne ihrer Merkmale einander gegenüberzustellen. Vielmehr sollten sich die Unternehmen zuerst eine eigene Security Policy erarbeiten. Erst die definierten Richtlinien und die Art der Bedrohung können bei der Auswahl und Implementierung einer Firewall helfen. Ebenso müssen vor dem Einsatz einer Firewall die Schwachstellen in einem Sicherheitskonzept untersucht und bewertet werden. Denn erst das Zusammenspiel aller beteiligter Komponenten kann die notwendige Sicherheit erzeugen. Dabei ist die Firewall der kleinste gemeinsame Nenner. *(bk)*