Firewall

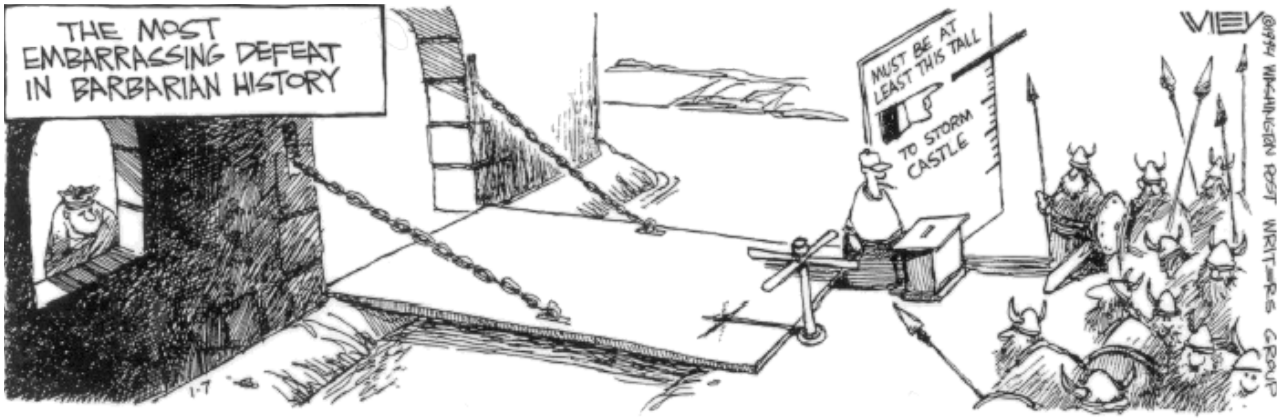
AvHG, Inf, My

Definition

Eine Firewall besteht aus einer Gruppe von Netzwerkkomponenten (Hard- und Software) an der Schnittstelle zweier Netze. Sie gewährleistet die Einhaltung von Sicherheitsrichtlinien zwischen einem zu schützenden und einem unsicheren Netz (z.B. dem Internet).

[aus Wikipedia, der freien Enzyklopädie:]

Durch den immer größer werdenden Ausbau von Netzen wird der Schutz einzelner Netze immer wichtiger. Firewalls greifen hier ein; sie sitzen an den Schnittstellen zwischen einzelnen Netzen und kontrollieren den Netzwerkverkehr zwischen den Netzen, um ungewünschten Verkehr zu verhindern und nur den gewünschten Verkehr weiterzuleiten. Der häufigste Einsatz einer Firewall besteht darin, den Verkehr zwischen einem lokalen Netzwerk und dem Internet zu kontrollieren und zu steuern.



Rund um das Thema Firewall existieren viele Begriffe, die teilweise richtig sind, aber manchmal nur die halbe Wahrheit vermitteln. Umgangssprachlich ist mit einer Firewall sehr oft die Software gemeint, welche den Datenverkehr zwischen den getrennten Netzbereichen kontrolliert und regelt. Man muss also zwischen dem (Sicherheits-)Konzept Firewall, und den zwei Hauptbestandteilen der Firewall, nämlich Hardware und Software, unterscheiden. Die Hardware ist für das Empfangen und Senden der einzelnen Netzwerkpakete zuständig und die Software regelt den Verkehr. (Was wird durchgelassen? Was wird nicht durchgelassen?)

Hardware

Die Hardwarekomponente hat im Regelfall zwei Netzwerkschnittstellen, an denen jeweils die zu trennenden Netzwerke angeschlossen sind. Die zwei Schnittstellen werden aus Sicherheitsgründen (oft aber wegen der Netzwerkstruktur und damit aus der konzeptionellen Notwendigkeit) gewählt, damit gewährleistet ist, dass nur solche Pakete von einem Netz in's andere durchgelassen werden, die von der Software als gültig anerkannt werden.

Software

Die Softwarekomponente der Firewall arbeitet auf den Schichten 2 bis 7 des OSI-Referenzmodells und demzufolge kann das Implementationsniveau sehr unterschiedlich ausfallen. Deswegen besteht eine Firewall oft aus verschiedenen Softwarekomponenten. Die verschiedenen Teile sollen hier kurz beschrieben werden:

Paketfilter

Für solch einfache Aufgaben wie das Vergleichen von Quell- und/oder Zieladresse der Pakete, die die Firewall passieren, ist der Paketfilter zuständig. Er hat die Aufgabe, bestimmte Filterungen oder Reglementierungen im Netzwerkverkehr vorzunehmen. Wenn man sich das Internet als eine gigantische Ansammlung von Häusern vorstellt, dann stellen die IPs sozusagen die Hausnummern dar. (Straßennamen sind in der Welt des Internets unbekannt.) Unter einer bestimmten Hausnummer kann man nun direkt mit einem Rechner kommunizieren, egal wo sich dieser Rechner befindet. In den einzelnen Etagen dieser Rechner wohnen nun die verschiedenen Dienste wie http und FTP. Die einzelnen Etagen sind mit einer Nummer gekennzeichnet, die man auch Port nennt. Ein Paketfilter kann nun verschiedene Etagen/Ports für die Besucher aus dem Internet sperren, d. h. jede Verbindung aus dem Internet wird an der Haustüre schon abgewiesen. Durch die entsprechende Konfiguration einer Firewall kann so ein Computernetzwerk vor Angriffen und/oder Zugriffen geschützt werden. Ein Paketfilter definiert Regeln, welche festlegen, ob einzelne oder zusammenhängende Pakete das Zugangsschutzsystem passieren dürfen oder abgeblockt werden. Eine solche Regel wäre zum Beispiel: verwerfe alle Pakete, die von der IP-Adresse 1.2.3.4 kommen. Eine solche Regel ist programmtechnisch einfach: es ist nur ein Zahlenwert zu vergleichen.

Content-Filter / Application-Level-Gateway

Eine Firewall kann aber nicht nur auf der niedrigen Ebene des Paketfilters arbeiten, sondern auch komplexere Aufgaben übernehmen. Ein Content-Filter überprüft zum Beispiel die Inhalte der Pakete und nicht nur die Meta-Daten der Pakete wie Quell- und/oder Zieladresse. Solche Aufgaben können zum Beispiel folgende sein:

- Herausfiltern von ActiveX und/oder JavaScript aus angeforderten HTML-Seiten.
- Filtern/Kennzeichen von Spam-Mails
- Löschen von Viren-Mails

Solche Regeln sind normalerweise sehr einfach zu definieren, ihre Ausführung ist aber sehr komplex: hierfür müssen einzelne Pakete zusammengesetzt werden, damit die HTML-Seite als Ganzes erkannt, durchsucht und verändert werden kann. Anschließend muss die Seite wieder in einzelne Pakete zerteilt werden und kann weitergeschickt werden.

Proxy

Ein Proxy ist ein Stellvertreter, der Anfragen (im Normalfall sind dies Anforderungen von HTML-Seiten) entgegennimmt und diese Anfrage weiterleitet. Der Proxy verhält sich gegenüber dem anfragenden Client wie ein Server. Gegenüber dem eigentlichen Ziel, z. B. dem Web-Server, verhält er sich wie ein Client. Dies geschieht nicht auf der Paketebene, sondern es wird in diese Pakete hineingeschaut und eine Anfrage generiert, die der ursprünglichen Anfrage entspricht. Der Vorteil bei dieser Methode ist, dass keine Pakete die Firewall direkt passieren können, was die Sicherheit nochmals erhöht. Oft ist ein Proxy auch mit einem Content-Filter kombiniert.

NAT / Network Address Translation

NAT **(**Network Address Translation**)** ist in Computernetzwerken ein Verfahren, bei dem private IP-Adressen auf öffentliche IP-Adressen abgebildet werden. Werden auch die Port-Nummern umgeschrieben spricht man dabei von **Maskieren** oder PAT (Port Address Translation).

Verwendung

NAT wird aus verschiedenen Gründen verwendet. Hauptsächlich ist NAT notwendig, weil öffentliche IP-Adressen immer knapper werden und man deshalb private IP-Adressen einsetzen muss. Zum Anderen kann es der Datensicherheit dienen, weil die interne Struktur des Netzwerks nach außen hin verborgen bleibt (Security through Obscurity – "Sicherheit durch Unklarheit").

Funktionsweise

Ein NAT-Gerät verbindet mit zwei Netzwerkkarten das lokale Netz mit dem Internet. Man unterscheidet zwischen *Source NAT*, bei dem die Quell-IP-Adresse ersetzt wird, und *Destination NAT*, bei dem die Ziel-IP-Adresse ersetzt wird. Bei **Basic NAT** wird jede interne IP durch eine externe IP ersetzt. Man spricht deshalb von einer 1:1-Übersetzung.

Beispiel: Öffentliche verfügbare Adressen: `205.0.0.0/24`

Source NAT:

Quell-IP	**Ziel-IP**	**Router ----------> NAT**	**Quell-IP**	**Ziel-IP**
192.168.0.2	170.0.0.1		*205.0.0.2*	170.0.0.1
192.168.0.3	170.0.0.1		*205.0.0.3*	170.0.0.1

Bei ausgehenden Paketen wird die (private) Quell-IP-Adresse durch eine noch nicht benutzte (öffentliche) IP ersetzt. Zusätzlich merkt sich der Router mittels einer Tabelle die Quell- und Ziel-IP-Adresse:

192.168.0.2 <-> 170.0.0.1

192.168.0.3 <-> 170.0.0.1

Destination NAT:

Quell-IP	**Ziel-IP**	**Router ----------> NAT**	**Quell-IP**	**Ziel-IP**
170.0.0.1	*205.0.0.2*		170.0.0.1	*192.168.0.2*
170.0.0.1	*205.0.0.3*		170.0.0.1	*192.168.0.3*

Bei eingehenden Paketen kann anhand der Quell-IP-Adresse und des Tabelleneintrags festgestellt werden, welcher Computer die Pakete angefordert hatte (hier: `192.168.0.2` und `192.168.0.3`). Der Router kann dadurch die (öffentliche) Ziel-IP durch die ursprüngliche Quell-IP `192.168.0.2` bzw. `192.168.0.3` austauschen.

Für den Host im internen Netz (z.B. `192.168.0.2`) sind diese Vorgänge transparent, d.h. er bekommt von der Adressumsetzung nichts mit.

Masquerading ist eine Implementation von **NAPT** (Network Address Port Translation), bei dem auch die Ports umgeschrieben werden.

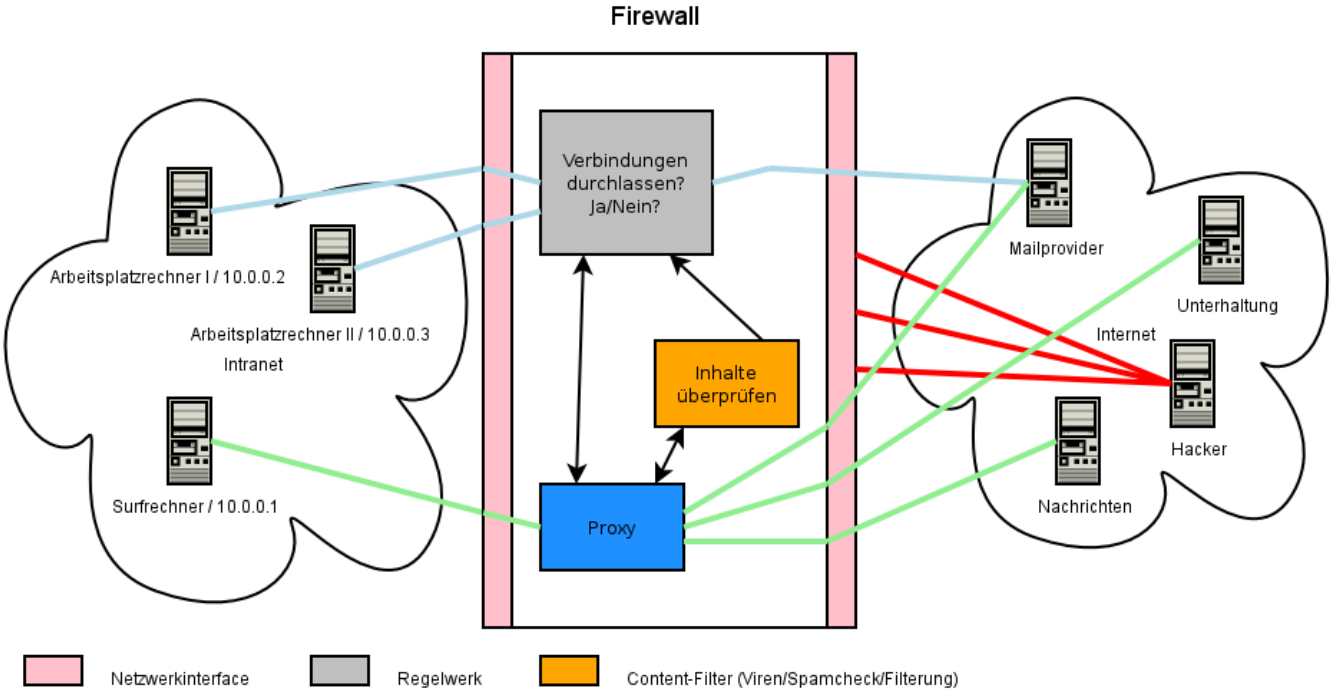
Router-Funktionalitäten

Damit die Pakete von der einen Seite der Firewall auch auf die andere Seite weitergeleitet werden können, muss die Firewall Router-Funktionaliäten besitzen.

Beispiel

Ein einfaches Konzept soll diese trockene Materie verdeutlichen: Eine Firma möchte gerne ihre Arbeitsplatzrechner ins Internet bringen. Man entscheidet sich für eine Firewall, und aufgrund der Viren/Würmer Gefahr möchte man gerne nur die Verbindungen zu einem Mail-Server aufbauen. Damit auch eine Recherche im Internet möglich ist, soll ein PC über einen Proxy Zugriff zu Webseiten erhalten. Weiterhin steht der Firma nur eine öffentliche IP zur Verfügung, so dass NAT genutzt werden muß. Der Surf-Rechner wird zusätzlich dadurch geschützt, dass ActiveX aus den angeforderten HTML-Seiten aus Sicherheitsgründen rausgefiltert werden.

Sonstige Zugriffe von außen auf das Firmennetz sollen einfach geblockt werden.



Personal Firewalls

Personal Firewalls oder auch Desktop Firewalls sind Programme, die lokal auf dem zu schützenden Rechner installiert sind. Sie beinhalten einen Paketfilter und einen Content-Filter. Darüber hinaus sind oft noch Viren-Scanner für den normalen Betrieb vorhanden.

Die Wirkung von Personal Firewalls ist allerdings umstritten: Ist der Rechner ordentlich konfiguriert und laufen nur vertrauenswürdige Programme, so wird das System selbst nur sinnvolle Pakete annehmen und verschicken. Läuft dagegen zweifelhafte Software auf dem Rechner, die unautorisiert auf das Netz zugreifen will, so wird diese auch soweit gehen, den normalen Weg des Versands zu verlassen und die Personal Firewall zu umgehen oder auszuschalten. So sind schon Viren in freier Wildbahn entdeckt worden, die die Regeln der gängigen Firewalls modifizieren, damit Sie ihre eigentliche Aufgabe durchführen können.