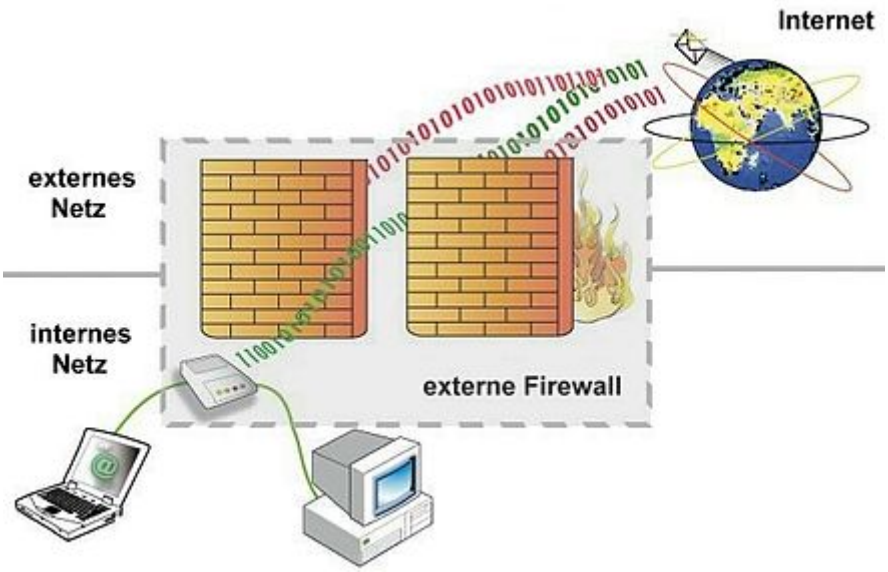
WIKIPEDIA

Firewall

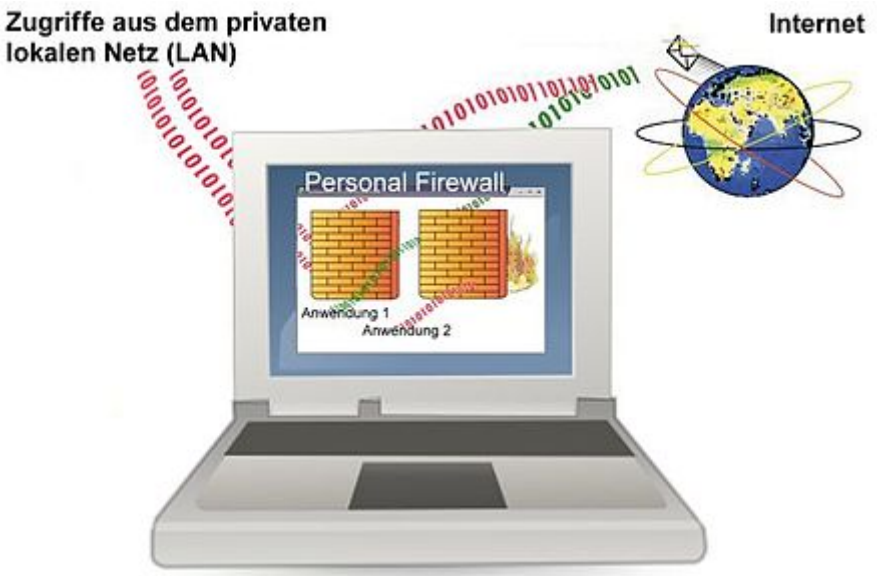
Eine **Firewall** (von englisch *firewall* [ˈfaɪəwɔːl] ‚Brandwand' oder ‚Brandmauer') ist ein Sicherungssystem, das ein Rechnernetz oder einen einzelnen Computer vor unerwünschten Netzwerkzugriffen schützt.[1] Weiter gefasst ist eine Firewall auch ein Teilaspekt eines Sicherheitskonzepts.[2]

Jedes Firewall-Sicherungssystem basiert auf einer Softwarekomponente. Die Firewall-Software dient dazu, den Netzwerkzugriff zu beschränken, basierend auf Absender oder Ziel und genutzten Diensten. Sie überwacht den durch die Firewall laufenden Datenverkehr und entscheidet anhand festgelegter Regeln, ob bestimmte Netzwerkpakete durchgelassen werden oder nicht. Auf diese Weise versucht sie, unerlaubte Netzwerkzugriffe zu unterbinden.

Abhängig davon, wo die Firewall-Software installiert ist, wird unterschieden zwischen einer *Personal Firewall* (auch *Desktop Firewall*) und einer *externen Firewall* (auch *Netzwerk-* oder *Hardware-Firewall* genannt). In Abgrenzung zur Personal Firewall arbeitet die Software einer externen Firewall nicht auf dem zu schützenden System selbst, sondern auf einem separaten Gerät, das Netzwerke



Die externe Firewall befindet sich zwischen verschiedenen Rechnernetzen. In diesem Beispiel beschränkt sie den Netzwerkzugriff des Internets (*externes Netz*; WAN) auf das private (in sich geschlossene) Netz (*internes Netz*; LAN). Sie tut dies, indem sie beispielsweise (Antwort-)Pakete durchlässt, die aus dem internen Netz heraus angefordert wurden, und alle anderen Netzwerkpakete blockiert.



Die Software der Personal Firewall läuft auf dem zu schützenden Computersystem und beschränkt dort den Zugriff auf Netzwerkdienste des Computers. Abhängig vom Produkt kann sie zudem versuchen, innerhalb gewisser Grenzen, s. u., den unerlaubten Zugriff von Anwendungen auf das Netz zu unterbinden.

oder Netzsegmente miteinander verbindet und dank der Firewall-Software gleichzeitig den Zugriff zwischen den Netzen beschränkt. In diesem Fall kann „Firewall“ auch als Bezeichnung für das Gesamtsystem stehen (ein Gerät mit der beschriebenen Funktion).[3] Bauartbedingt gibt es große konzeptionelle Unterschiede zwischen den beiden Arten.

Die Funktion einer Firewall besteht nicht darin, Angriffe zu erkennen. Sie soll ausschließlich Regeln für die Netzwerkkommunikation umsetzen. Für das Aufspüren von Angriffen sind sogenannte IDS-Module zuständig, die durchaus auf einer Firewall aufsetzen und Bestandteil des Produkts sein können. Sie gehören jedoch nicht zum Firewall-Modul.[4]

Inhaltsverzeichnis

Allgemeine Grundlagen

Für das Verständnis der Funktionsweise einer Firewall ist das folgende Grundlagenwissen hilfreich. Die jeweiligen Hauptartikel stellen die Themen im Detail dar.

Funktionsweise eines Fernzugriffs auf ein Computersystem

→ *Hauptartikel: Netzwerkdienst und Netzwerkprotokoll*

Der Zugriff auf einen Netzwerkdienst

Ein Netzwerkdienst ist ein Computerprogramm, das den Zugriff auf Ressourcen wie Dateien und Drucker über ein Netzwerk ermöglicht. Beispielsweise sind Internetseiten als Dateien auf einem Computer (Server) abgelegt. Erst ein auf dem Server laufender Netzwerkdienst (hier eine Webserver-Software) ermöglicht es, aus dem Internet heraus auf die Seiten zuzugreifen und sie so auf einem entfernten Gerät zu laden und anzuzeigen. Damit Netzwerkdienste vom Netzwerk aus erreichbar sind, binden sie sich an je einen Port der Netzwerkschnittstelle. Man spricht davon, dass sie „einen *Port öffnen*“, was im Umkehrschluss bedeutet, dass ein offener Port immer zu einem Computerprogramm gehört, das Netzwerkanfragen entgegennehmen kann.

Eine Sicherheitslücke in einem Netzwerkdienst kann die Basis dafür liefern, um über die zulässigen Zugriffsfunktionen hinaus Aktionen auf dem Computer auszuführen.[5]

Hinweis: Ein *Dienst* (unter Microsoft Windows englisch *Service*; unter Unix englisch *Daemon*) zeichnet sich dadurch aus, dass er bei jedem Systemstart ausgeführt wird, unabhängig davon, ob sich ein Anwender an dem Computer anmeldet.[6] Es gibt Programme mit einer dem Netzwerkdienst entsprechenden

Funktionalität, die also einen Port öffnen, jedoch erst nach der Benutzeranmeldung gestartet werden. Obgleich diese Programme genau genommen keine Dienste sind, werden sie der Einfachheit halber im Folgenden ebenfalls als Netzwerkdienst betitelt.

Der Rückweg vom entfernten Netzwerkdienst zum Client

Der Rückweg vom entfernten Netzwerkdienst hin zum anfragenden PC (genauer dem Client), der auf den Dienst zugreift, lässt sich mitunter für einen übergreifenden Fernzugriff nutzen. Um bei dem obigen Beispiel zu bleiben, startet der Anwender einen Browser, der auf seinem PC Webseiten aus dem Internet darstellen soll. Enthält der Browser eine entsprechende Sicherheitslücke, so kann der kontaktierte Internetserver nun auf diesen PC zugreifen und dort Aktionen ausführen, die über die normale Anzeige von Internetseiten hinausgehen. Im schlimmsten Fall genügt der bloße Aufruf einer entsprechend präparierten Internetseite, um sogar heimlich eine Schadsoftware auf dem PC zu installieren.[7] Eine Schadsoftware kann wiederum als Netzwerkdienst auf dem PC arbeiten und so einen ständigen Fernzugriff auf den PC ermöglichen.[8]

Statt einen Netzwerkdienst auf den PC zu installieren, kann die Schadsoftware auch von sich aus eine Verbindung zum Internet herstellen und sich mit einem Netzwerkdienst verbinden, der im Internet betrieben wird. Beispielsweise läuft ein Botnet meist auf diese Weise. In einem solchen Fall wird der Rückweg für einen ständigen Fernzugriff auf den PC benutzt.

Die Netzwerkimplementierung des Betriebssystems

Für die Kommunikation im Netz benötigen die beteiligten Rechner – beziehungsweise die auf ihnen installierten Dienste ("Kommunikationspartner") – Kenntnis über die grundlegenden Protokolle, die für die Adressierung und den Transport von Daten verwendet werden. Mitunter kann eine fehlerhaft implementierte Netzwerkanbindung des Betriebssystems (inklusive fehlerhafter Treiber-Software) für einen Netzwerkzugriff genutzt werden, der in dieser Form vom Hersteller nicht vorgesehen war. Ein Beispiel für die Ausnutzung eines ehemals weitverbreiteten Fehlers in der Implementierung des IP-Protokolls stellt Ping of Death dar, der das Zielsystem gezielt zum Absturz brachte. Ähnliche Lücken ermöglichen es mitunter auch, Programmcode auf dem Zielsystem einzuschleusen und auszuführen.[9]

Schutzfunktion und Grenzen einer Firewall

Eine Firewall dient dazu, ungewollte Zugriffe auf Netzwerkdienste zu unterbinden.[10] Sie orientiert sich dabei an den Adressen der Kommunikationspartner (also „wer darf worauf zugreifen“). In der Regel kann eine Firewall nicht die Ausnutzung einer Sicherheitslücke in dem Netzwerkdienst verhindern, wenn der Kommunikationspartner darauf zugreifen darf.

Bei der Ausnutzung des Rückwegs kann eine Firewall nicht vor dem Zugriff auf Sicherheitslücken des Browsers schützen, wenn der Kommunikationspartner auf die gefährdeten Bereiche des Programms zugreifen kann. Daher sollten Programme, die für den Netzwerkzugriff bestimmt sind, auf dem aktuellen Stand gehalten werden, um bekannte Sicherheitslücken dort zu schließen. Einige Firewalls bieten Filter an, die den Fernzugriff auf den genutzten Netzwerkdienst weiter einschränken, indem beispielsweise die Filterung von gefährdeten ActiveX-Objekten aus Webseiten vorgenommen wird.[11] Der Browser kann dann auf solche in einer Webseite eingebetteten Objekte nicht mehr zugreifen (er zeigt sie nicht an), was gleichzeitig bedeutet, dass er über diese Objekte nicht angegriffen werden kann. Alternativ dazu lässt sich dieses Verhalten auch über die Konfiguration des verwendeten Browsers erreichen.

Je nach Firewall-Typ kann eine Firewall im günstigsten Fall auf den Netzwerkzugriff einer heimlich installierten Schadsoftware aufmerksam machen und mitunter sogar deren Netzwerkzugriff unterbinden. Ein solcher Erfolg ist allerdings stark von dem Geschick der jeweiligen Schadsoftware abhängig (siehe dazu die Grenzen der Personal Firewall und der externen Firewall).[12][13][14]

Die Ausnutzung von Fehlern in der Netzwerkimplementierung des Betriebssystems kann eine Firewall im günstigsten Fall abwehren.

Die aufgezeigten Grenzen einer Firewall im Vergleich zum Nutzen lassen sich mit dem Sicherheitsgurt eines Automobils vergleichen, für den es ebenfalls Szenarien gibt, in denen er den Fahrer nicht zu schützen vermag. Es ist sinnvoll, den Gurt anzulegen und gleichzeitig mit dem Wissen um seine Grenzen vorsichtig zu fahren. Eine Ausnahme könnte ein Gurt bilden, der den Autofahrer gleichzeitig gefährdet (hier mit Bezug zur Personal Firewall), was unter Umständen dazu führen kann, dass alternative Lösungen eine höhere Sicherheit bieten.

Die Firewall als Teilaspekt eines Sicherheitskonzepts

Erst wenn bekannt ist, gegenüber welchen Szenarien ein bestimmtes Maß an Sicherheit erreicht werden soll, kann man sich Gedanken über die Art und Weise machen, wie dies umgesetzt wird. Dabei hilft die Erstellung eines Sicherheitskonzepts. In größeren Organisationen kommt dafür üblicherweise eine eigene Sicherheitsrichtlinie zum Einsatz.[15]

Die Firewall ist ein Teilaspekt des Sicherheitskonzepts.[2] So wie „Brandschutz“ ein Bündel von Maßnahmen ist (und nicht allein der Rauchmelder im Treppenhaus), kann dieser Teilaspekt je nach Sicherheitskonzept ein Bündel mehrerer Maßnahmen sein. Die Firewall kann aus mehreren Komponenten bestehen, von denen einige beispielsweise eine DMZ versorgen. Ebenso kann die Wartung ein fester Bestandteil des Teilaspekts sein, genauso wie die Auswertung der Protokollierung von Firewallkomponenten.

Filtertechniken

→ Zu einer detaillierten Beschreibung siehe Firewall-Techniken

Paketfilter

→ Hauptartikel: Paketfilter

Die einfache Filterung von Datenpaketen anhand der Netzwerkadressen ist die Grundfunktion aller Firewalls (in einem TCP/IP-Netz ist damit genauer die Filterung des Ports und der IP-Adresse des Quell- und Zielsystems gemeint).

Stateful Packet Inspection

→ Hauptartikel: Stateful Packet Inspection

Diese zustandsgesteuerte Filterung ist eine erweiterte Form der Paketfilterung. Damit gelingt es, den Zugriff auf eine etablierte Verbindung genauer zu beschränken und so das interne Netz besser vor ungewollten Zugriffen von außen zu schützen.

Proxyfilter

→ Hauptartikel: Proxy (Rechnernetz)

Ein Proxyfilter stellt stellvertretend für den anfragenden Client die Verbindung mit dem Zielsystem her und leitet die Antwort des Zielsystems an den tatsächlichen Client weiter. Da er die Kommunikation selbst führt, kann er sie nicht nur einsehen, sondern auch beliebig beeinflussen. Auf ein bestimmtes Kommunikationsprotokoll spezialisiert, wie z. B. HTTP oder FTP, kann er so die Daten zusammenhängend analysieren, Anfragen filtern und bei Bedarf beliebige Anpassungen vornehmen, aber auch entscheiden, ob und in welcher Form die Antwort des Ziels an den tatsächlichen Client weitergereicht wird. Mitunter dient er dazu, bestimmte Antworten zwischenzuspeichern, damit sie bei wiederkehrenden Anfragen schneller abrufbar sind, ohne sie erneut anfordern zu müssen. Auf einem einzigen Gerät kommen oft mehrere solcher Filter parallel zum Einsatz, um unterschiedliche Protokolle bedienen zu können.

Contentfilter

→ *Hauptartikel: Contentfilter*

Dieser Inhaltsfilter ist eine Form des Proxyfilters, der die Nutzdaten einer Verbindung auswertet und zum Beispiel dafür gedacht ist, ActiveX und/oder JavaScript aus angeforderten Webseiten herauszufiltern oder allgemein bekannte Schadsoftware beim Herunterladen zu blockieren. Auch das Sperren von unerwünschten Webseiten anhand von Schlüsselwörtern und Ähnliches fallen darunter.

Deep Packet Inspection

→ *Hauptartikel: Deep Packet Inspection*

Mittels Deep Packet Inspection können weitergehende, insbesondere protokollspezifische Informationen analysiert werden. Dadurch wird es möglich, Regeln zu verwenden basierend auf URLs, Dateinamen, Dateiinhalten (Virenscan oder Data Loss Prevention) und ähnlichem. Dies ähnelt den Möglichkeiten eines Proxies oder eines Content Filters, deckt in der Regel aber zahlreiche Protokolle ab.

Um auch verschlüsselte Verbindungsdaten und Inhalte analysieren zu können, wird *SSL Deep Packet Inspection* eingesetzt, das eine bestehende SSL-Verschlüsselung terminiert, die Inhalte untersucht und anschließend für den Client wieder neu verschlüsselt. Dazu ist es in der Regel notwendig, auf dem Client ein CA-Root-Zertifikat zu installieren, das es der Firewall erlaubt, im laufenden Betrieb passende Zertifikate selbst zu generieren. Technisch entspricht dies einem Man-in-the-Middle-Angriff.

Sichtbarkeit für Anwender

→ *Hauptartikel: Network Address Translation*

Um Netzwerkpakete filtern zu können, muss sich die Firewall zwischen den Kommunikationspartnern befinden. Dabei kann sie den Kommunikationspartnern gegenüber auf unterschiedliche Weise in Erscheinung treten, wobei die ersten vier Erscheinungsformen nur auf einer externen Firewall vorkommen können:

Sichtbar

Die Firewall stellt sich als Vermittlungsstelle für beide Seiten sichtbar zwischen das Quell- und Zielsystem. Hier bittet der Client die Proxy-Firewall, stellvertretend für ihn die Kommunikation mit dem Zielsystem zu übernehmen. So wird beispielsweise der Webbrowser so konfiguriert, dass er sämtliche Internetanfragen nicht direkt zur jeweiligen Zieladresse schickt, sondern als Anforderung zum Proxy sendet. Der Proxy nimmt nun die Verbindung zum Zielsystem auf. Erst nach erfolgter Analyse gibt der Proxy die Antwort des Zielsystems an den anfragenden Client weiter.

Einer Seite gegenüber transparent

Eine der beiden Seiten adressiert hier direkt das Ziel und nicht die Firewall. Durch eine entsprechend konfigurierte Infrastruktur des Netzes wird die betreffende Anfrage dort automatisch über die (NAT- oder Proxy-)Firewall geleitet, ohne dass der Absender dies bemerkt oder gar beeinflussen kann. Die Verbindung zur anderen Seite wird nun über die Adresse der Firewall hergestellt. Mögliche Angriffe von dort sind auch hier an die Firewall gerichtet und treffen nicht direkt den Client. Denn für diese Seite stellt die Firewall den zu adressierenden Kommunikationspartner dar, der stellvertretend für den tatsächlichen Kommunikationspartner angesprochen wird. Diese Form ist die am häufigsten verbreitete Art bei Firewall-Geräten für den Heimbereich.

Beiden Seiten gegenüber transparent

Hierbei legt sich die Firewall transparent (nahezu unsichtbar) zwischen beide Netzwerke und ermöglicht so eine durchgehende Verbindung der Kommunikationspartner, sodass sich die Systeme vor und hinter der Firewall direkt sehen können. Der Datenstrom fließt einfach durch die Firewall hindurch. Auf der Ebene der IP-Adressierung sieht die Gegenstelle die Firewall also nicht als Kommunikationspartner, sondern erkennt diese lediglich als Verbindungsglied zwischen den Subnetzen (Router ohne NAT). Dennoch kann die auf dem Netzwerkgerät (Router) laufende Firewall-Software den Datenstrom unterbrechen (bestimmte Pakete herausfiltern).

Unsichtbar

Genau wie bei dem beidseitig transparenten Modus fließt hier der Datenstrom einfach durch die Firewall hindurch. Das Gerät, auf dem die Firewall-Software läuft, arbeitet nun aber wie eine Bridge, wodurch sie für die Kommunikationspartner weder auf IP-Ebene noch aus Sicht der Low-Level-Adressierung sichtbar ist.

Lokal

Eine lokal auf dem Computer installierte Firewall-Software (Personal-Firewall) überwacht den durch sie hindurch fließenden Datenstrom vor Ort (auf dem Computer, deren Netzwerkpakete sie filtern soll; in diesem Absatz *Quellsystem* genannt). Aus Sicht des Zielsystems liegt die Firewall also hinter dem Netzwerkadapter des Quellsystems. Dadurch verändert sich weder die Netzwerkadresse des Quellsystems noch der Kommunikationsweg zum Zielsystem. Somit ist auch die Personal Firewall aus Sicht der Adressierung praktisch unsichtbar. Das bezieht sich jedoch lediglich auf den Kommunikationsweg und bedeutet nicht, dass sie sich nicht aufspüren lässt (aufgrund des Verhaltens des Quellsystems) oder über die Adresse des Quellsystems nicht direkt angreifbar wäre (im Gegensatz zur externen Bridge-Firewall, die keine Netzwerkadresse besitzt).

Regelwerk

→ *Hauptartikel: Firewall-Regelwerk*

Die Regeln einer Firewall legen fest, was mit einem Netzwerkpaket passieren soll, das in das Muster eines Filters passt. Die Aktionen können je nach Produkt unterschiedlich betitelt sein. Entweder ist die Anfrage nicht erlaubt und das Paket wird lokal verworfen (meist DROP genannt) oder sie wird aktiv abgelehnt (REJECT), indem sie beispielsweise mit einem ICMP-Paket beantwortet wird. Eine erlaubte Anfrage nennt man ACCEPT, ALLOW, PASS oder FORWARD, wobei FORWARD je nach Produkt und Konfiguration auch auf eine Umleitung der Anfrage hindeuten kann.

Überprüfbarkeit des Quelltextes

→ Hauptartikel: Proprietäre Software, Open Source und Freie Software

Bei Softwareprodukten ist eine freie Einsicht in deren Quellcode ein Aspekt der Computersicherheit. Dabei gilt es unter anderem die Gefahr zu minimieren, dass ein Produkt Funktionalitäten enthalten kann, von denen der Anwender nichts wissen soll. So gibt es beispielsweise einige Closed-Source-Produkte aus dem Bereich der Personal Firewalls, die selbst heimlich Daten zum Hersteller schicken, also genau das tun, was einige Anwender mit dem Produkt eigentlich zu verhindern suchen.[16] Quelloffene Software lässt sich von der Öffentlichkeit dahingehend überprüfen und darüber hinaus mit rechtlich unbedenklichen Mitteln auf Schwachstellen untersuchen, die auf diese Weise schneller geschlossen werden können. Dabei sind quelloffene Lizenzmodelle nicht mit kostenloser Software gleichzusetzen; *Open Source* genauso wie *Freie Software* umfassen auch kommerzielle Produkte (*Freie Software* ist nicht dasselbe wie *Freeware*).

Firewall-Arten im Vergleich

Je nach ihrem Einsatzort unterscheidet man zwei Arten von Firewalls. *Personal Firewalls* sind Programme, die auf dem Computer laufen, den sie schützen sollen. *Externe Firewalls* sind dem zu schützenden Computer bzw. Computernetzwerk physisch vorgeschaltet.

Unterschiede zwischen Personal Firewalls und externen Firewalls

→ Hauptartabschnitt: Personal Firewall (auch Desktop Firewall) und Externe Firewall (auch Netzwerk- oder Hardware-Firewall)

Beide Firewallarten können als eine Ergänzung zueinander betrachtet werden. Man kann nicht pauschal sagen, dass eine der beiden durch die jeweils andere Art ersetzbar wäre, da es große konzeptionelle Unterschiede gibt:

- Eine externe Firewall vermittelt *üblicherweise* zwischen zwei Netzen, indem sie beispielsweise den Internetzugriff kontrolliert. Im Unterschied dazu filtert die Personal Firewall zusätzlich auch die Verbindungen des Computers von und zu den Kommunikationspartnern des eigenen lokalen Netzes (LAN).[17]

  Bei höheren Sicherheitsanforderungen kann eine externe Firewall Verbindungen auch innerhalb des lokalen Netzes filtern, indem sie dem zu schützenden Computer physisch direkt vorgeschaltet wird. Die externe Firewall kann auch ein speziell gesichertes Netz(-Segment) innerhalb des lokalen Netzes überwachen, womit sie wenigstens einen Teil der Kommunikation im LAN filtert. In einem Heimnetz ist das jedoch kaum anzutreffen.

- Auf mobilen Computern setzt die Personal Firewall exklusiv eine elementare Funktion um: Sie unterscheidet, an welchem Netzwerk der Computer aktuell betrieben wird, und schaltet dann auf das dazugehörende Regelwerk um. So kann beispielsweise die Dateifreigabe des mobilen Computers innerhalb des privaten Netzes erreichbar sein, wohingegen innerhalb eines öffentlichen Netzes (beispielsweise im Internetcafé) der Zugriff darauf unterbunden wird.
- Eine externe Firewall, die stellvertretend für den Computer die Verbindung zum Internet aufbaut, verhindert automatisch (bauartbedingt), dass jemand aus dem Internet auf Netzwerkdienste der geschützten Computer zugreifen kann. Damit bietet sie auch einen wirkungsvollen Schutz gegen den Netzwerkzugriff auf eine Schadsoftware, wenn diese einen Netzwerkdienst installiert, der darauf wartet, dass jemand aus dem Internet heraus

eine Verbindung zu ihm aufbaut. Im Unterschied zur Personal Firewall ist dazu keine Pflege eines Regelwerks notwendig.
- Andersherum sind einfache externe Firewalls nicht oder nur sehr bedingt dazu in der Lage, eine Schadsoftware davon abzuhalten, von sich aus eine Verbindung zum Internet herzustellen, denn sie wurden – im Unterschied zu den meisten Personal Firewalls – für eine solche Aufgabe nicht konzipiert. Wird die von der Schadsoftware ausgehende Netzwerkkommunikation nicht unterbunden, ist über diesen Weg sogar ein uneingeschränkter Fernzugriff auf den Computer trotz Einsatz einer externen Firewall möglich.

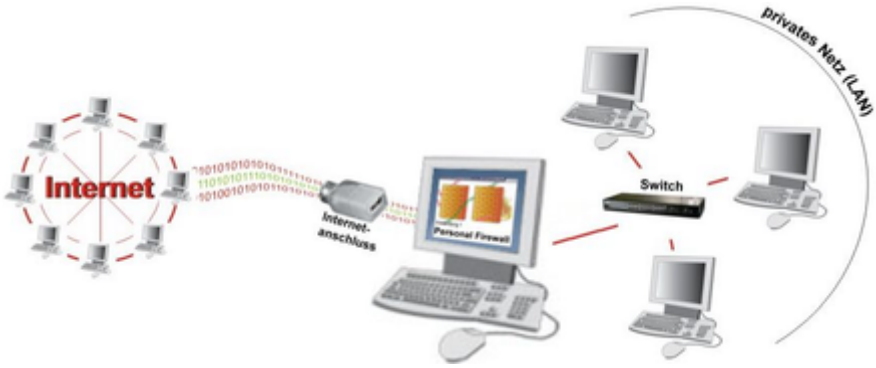
  Eine Ausnahme bilden die externe Proxy-Firewall und die so genannte *Next-Generation Firewall*[18][19], die eine Möglichkeit unterstützen können, um die Netzwerkkommunikation nur für bestimmte Anwendungen zuzulassen.

Eine Personal Firewall ist nicht pauschal besser oder schlechter als eine externe Firewall, sondern vor allem anders. In all den Punkten, in denen sich die Funktionalitäten jedoch gleichen, ist die externe Firewall zuverlässiger. Denn ein derart spezialisiertes Gerät bietet vorwiegend ein sicherheitsoptimiertes und netzwerkseitig stabiles System, das dank der physischen Trennung zu dem zu schützenden Computersystem nicht so einfach manipuliert oder sogar deaktiviert werden kann.

Personal Firewall (auch Desktop Firewall)

→ Hauptartikel: Personal Firewall

Als *Personal Firewall* oder *Desktop Firewall* wird eine lokal auf dem Computer installierte Firewall-Software bezeichnet. Zu ihrer Aufgabe gehört es, ungewollte Zugriffe von außen auf Netzwerkdienste des Computers zu unterbinden. Abhängig vom Produkt kann sie zudem versuchen, Anwendungen davon abzuhalten, ohne das Einverständnis des Anwenders mit der Außenwelt zu kommunizieren.



Eine Personal Firewall beschränkt den Zugriff des PCs auf das Internet und das lokale Netz.

Vorteile

Computerwürmer, die einen Sicherheitsfehler in einem Netzwerkdienst ausnutzen, um sich zu verbreiten, können den Computer nur dann infizieren, wenn der entsprechende Netzwerkdienst für den Wurm erreichbar ist. Hier kann eine Personal Firewall den Fernzugriff auf den Netzwerkdienst einschränken und somit eine Infektion erschweren oder sogar verhindern. Gleiches gilt für einen Netzwerkzugriff eines möglichen Eindringlings.[17]

Benötigt wird eine solche Filterung, wenn ein Netzwerkdienst auf dem Computer gestartet wird, der für den Betrieb erforderlich ist und der *Zugriff darauf beschränkt* werden soll.[20] Ein Fernzugriff auf nicht benötigte Netzwerkdienste lässt sich dagegen ohne Firewall verhindern, indem diese Dienste deaktiviert werden.[20]

Darüber hinaus können die Regeln der Personal Firewall im günstigsten Fall unterbinden, dass ein durch eine Schadsoftware heimlich reaktivierter oder installierter Dienst ungehindert vom Netzwerk aus ansprechbar ist. Der Einsatz der Personal Firewall hat sich gelohnt, wenn die (mögliche) Meldung der Firewall-Software dazu genutzt wird, um reaktivierte Dienste nebst Schadsoftware gleich wieder zu entfernen.

Grenzen

Personal Firewalls können vor einigen Computerwürmern schützen, die sich über das Netzwerk verbreiten,[17] bieten darüber hinaus jedoch keinen Schutz vor der Installation einer andersartigen Schadsoftware.

Abhängig vom Produkt und Betriebsmodus kann eine Personal Firewall neu hinzukommende Netzwerkdienste (und Anwendungen mit entsprechender Funktionalität) erkennen[17] und den Anwender fragen, ob ein Fernzugriff darauf erlaubt sein soll. Damit dieser Teil der Schutzfunktion zuverlässig funktioniert, muss zum einen die Firewall-Software durchgängig stabil laufen. Das stellt selbst bei einem nicht-kompromittierten System eine Herausforderung dar.[21] Zum anderen muss der Anwender wissen, was er tut.

Einige Produkte versuchen darüber hinaus Anwendungsprogramme davon abzuhalten, ohne das Einverständnis des Anwenders mit der Außenwelt zu kommunizieren, in der Absicht dabei auch den Netzwerkzugriff einer entsprechenden Schadsoftware zu beschränken. Ein solcher Erfolg der Firewall-Software ist allerdings stark von dem Geschick der jeweiligen Schadsoftware abhängig (in Fachartikeln aus Microsofts *TechNet Magazine*[12] und der c’t[13] wird davor gewarnt, dass die Personal Firewall unerwünschte Netzwerkzugriffe nur unterbinden kann, wenn sich die Schadsoftware keine große Mühe gibt, ihre Aktivitäten zu verbergen).[22] Vergleichen lässt sich diese Art der Schutzwirkung mit einem Gartenzaun, der zwar ein durchaus vorhandenes, aber kein unüberwindbares Hindernis darstellt. Vor allem auf einem kompromittierten System kann die Firewall-Software im Unterschied zum Gartenzaun jedoch plötzlich und unerwartet ausfallen.[23][24]

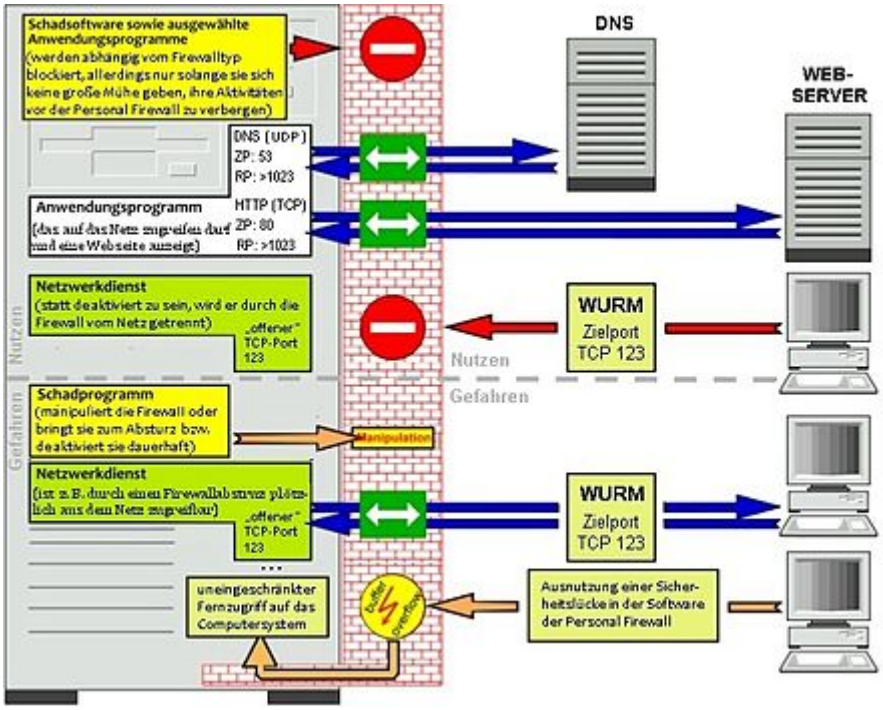
Wird eine Schadsoftware auf dem zu schützenden PC entdeckt, lässt sich der Netzwerkzugriff daher effizient durch deren Entfernung unterbinden,[25] statt durch eine Firewall, weil das auch dann noch Wirkung zeigt, wenn die Firewall-Software ausfällt. Innerhalb ihrer Grenzen kann hier die Personal Firewall mitunter dabei helfen zu erkennen, wann eine solche Kommunikation stattfindet.

Nachteile

Programme, die auf derselben Hardware wie die Personal Firewall-Software laufen, haben wesentlich mehr Möglichkeiten diese zu manipulieren und zu umgehen, als bei einer externen Firewall. Ein Absturz oder gar eine dauerhafte Deaktivierung der Firewall-Software durch einen Softwarefehler[21] oder ein Schadprogramm[23] führen dazu, dass ein uneingeschränkter Zugriff auf die zuvor gefilterten Netzwerkdienste möglich wird, mitunter ohne dass der Anwender dies bemerkt. Abhängig vom Produkt und Wissensstand des Anwenders kann auch eine Fehlbedienung diesen Zustand herbeiführen.

Es ist zudem ein Problem des Konzepts, dass sich die Firewall-Software zwischen die normale Netzwerkimplementierung des Betriebssystems und die Außenwelt stellt, wodurch zwar zum Teil nicht mehr die ursprüngliche Netzwerkimplementierung,[26] dafür aber die wesentlich komplexere Firewall-Software direkt angreifbar wird.[27][28] Die Erfahrung zeigt, dass eine Software mehr Fehler und Angriffspunkte enthält, je komplexer sie ist.[29] So können Personal Firewalls selbst Sicherheitslücken enthalten, die beispielsweise einem Computerwurm erst Ansätze für einen Fernzugriff bieten.[30]

Da die Komponenten einer Personal Firewall (zumindest teilweise) mit erweiterten Rechten laufen und in der Regel Kernel-Komponenten installiert werden, wirken sich Programmier- und Designfehler hier besonders stark auf die Sicherheit, Performance und Stabilität des Computersystems aus. Je nach Produkt können über diese Komponenten auch beispielsweise heimlich Daten zum Hersteller übermittelt und weitere Funktionen geschaffen werden, die der Anwender nicht ausdrücklich wünscht und die es ohne die installierte Firewall-Software nicht gäbe.[16]



Nutzen und Gefahren einer Personal Firewall

Sicherheitstechnisch bedenklich wird der Einsatz einer Personal Firewall, wenn sie beispielsweise für den reibungslosen Betrieb während eines Computerspiels abgeschaltet wird. Auf einem solchen System ergibt der Einsatz einer Personal Firewall keinen Sinn, da die Firewall-Software die verbleibenden Risiken lediglich kaschiert und so selbst zum Sicherheitsrisiko wird (sie gibt dem Anwender in der übrigen Zeit ein Sicherheitsgefühl, das auf diesem System jeglicher Grundlage entbehrt).

Auf Systemen, bei denen eine Personal Firewall bereits ein fester Bestandteil des Betriebssystems ist, kann es durchaus fragwürdig sein, eine weitere Firewall-Software zu installieren. Der Parallelbetrieb kann zu Problemen führen[21] und ist nicht zwingend mit Vorteilen verbunden.

Alternative Lösungen zur Unterbindung eines Fernzugriffs

Die Deaktivierung aller nicht benötigten Netzwerkdienste bietet den besten Schutz gegen ungewollte Fernzugriffe. Denn selbst wenn die Firewall-Software ausfällt, kann niemand auf Netzwerkdienste zugreifen, die nicht gestartet wurden. Zudem verlangsamt der Start eines jeden Dienstes die Startgeschwindigkeit des Betriebssystems und sie benötigen danach weiterhin Computerressourcen für ihre Arbeit. Je nach Betriebssystem gibt es mitunter einfach zu bedienende Hilfsmittel, die es auch unerfahrenen Benutzern ermöglichen, nicht benötigte Netzwerkdienste auf eine unkomplizierte Art zu deaktivieren.[31]

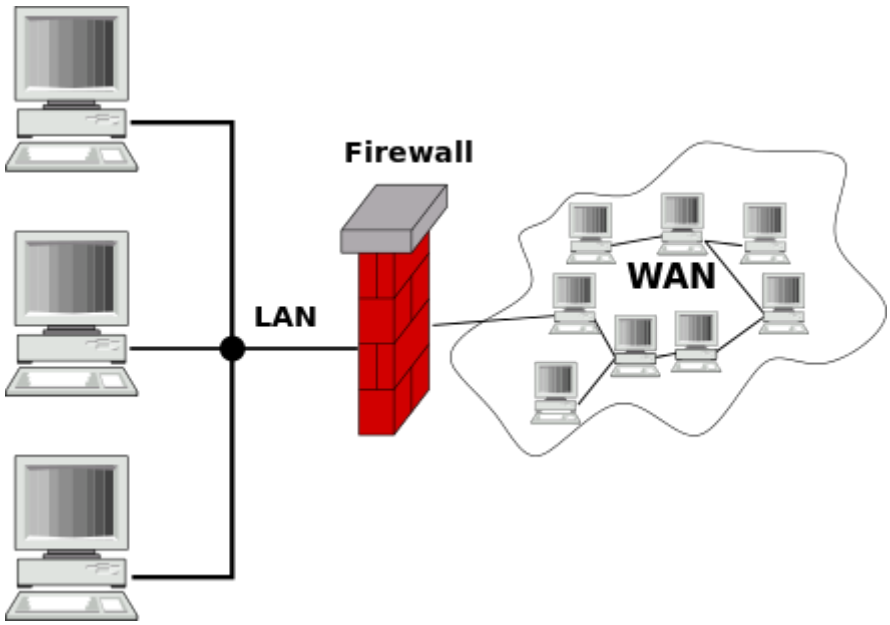
Um einen Zugriff auf verbleibende Netzwerkdienste aus dem Internet heraus zu verhindern, sollten sie nicht an den Netzwerkadapter gebunden sein, der an dem Internet angeschlossen ist. Diese Aufgabe ist für einen unerfahrenen Benutzer nicht ganz trivial, weshalb sich der Einsatz eines vermittelnden Gerätes, wie beispielsweise ein DSL-Router, anbietet. Dieses Gerät sorgt automatisch dafür, dass ein Netzwerkdienst nur aus dem internen (privaten) Netz, nicht jedoch aus dem Internet heraus direkt zugreifbar ist (siehe auch „Vorteile bei der Verwendung einer externen Firewall“).

Externe Firewall (auch Netzwerk- oder Hardware-Firewall)

→ *Hauptartikel: Externe Firewall*

Eine externe Firewall (auch Netzwerk- oder Hardware-Firewall genannt) beschränkt die Verbindung zwischen zwei Netzen. Das könnten beispielsweise ein Heimnetzwerk und das Internet sein.

Die externe Firewall ist dafür prädestiniert, unerlaubte Zugriffe von außen (in der Abbildung das WAN) auf das interne System zu unterbinden. Im Unterschied zur Personal Firewall besteht das interne System hier nicht zwangsläufig aus nur einem einzigen Computer, sondern kann sich auf einen Verbund mehrerer Computer beziehen, die das interne Netz bilden (in der Abbildung das LAN).



Die Firewall liegt zwischen dem LAN (dem lokalen Netzwerk) und dem WAN (dem Internet). Sie soll den Zugriff zwischen diesen Netzen beschränken.

Hardware-Firewall

Es gibt in der Praxis keine Firewalls, die ausschließlich auf Hardware basieren. Eine Firewall kann zwar auf einem eigenen Betriebssystem laufen und auf unterschiedliche Netzwerkebenen zugreifen, jedoch wird sie dadurch nicht Bestandteil der Hardware. Eine Firewall enthält immer als wesentlichen Bestandteil eine Software.

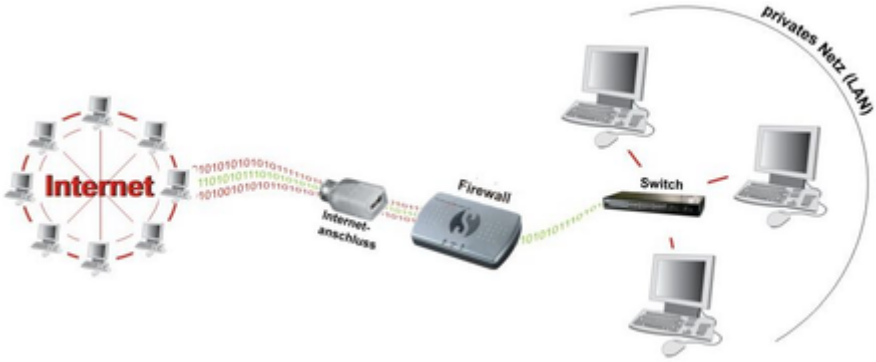
Der Begriff *Hardware-Firewall* wird vielmehr als Synonym für *externe Firewalls* verwendet. Er soll zum Ausdruck bringen, dass es sich hierbei um eine separate Hardware handelt, auf der die Firewall-Software läuft. Dabei gibt es allerdings Hardware, die für die Verwendung der Firewall-Software optimiert wurde, zum Beispiel indem ein entsprechender Hardware-Entwurf dabei hilft, Teile der Ent- und Verschlüsselung bestimmter Protokolle zu beschleunigen.

Vorteile

Ein direkter Anschluss eines Computers an das Internet (genauer an ein entsprechendes Modem) hat zur Folge, dass alle Computer aus dem Internet auf die an diesem Netzwerkanschluss gebundenen Dienste des Computers zugreifen können, was einen Fernzugriff auf den Computer ermöglicht.

Um Fernzugriffe aus dem Internet zu unterbinden, wäre es eine Lösung, zwischen dem internen (privaten) Netz und dem externen Netz (Internet) zu unterscheiden und benötigte Dienste nur an die Netzwerkschnittstelle des internen Netzes zu binden. Eine im sichtbaren oder einseitig transparenten Modus laufende externe Firewall kann diese Aufgabe übernehmen: Statt des PCs wird die externe Firewall an das Internet angeschlossen, wobei die PCs aus dem internen Netz wiederum mit diesem Gerät vernetzt werden. Die PCs übermitteln ihre Anfragen an das Internet nun an die Firewall, die stellvertretend für die PCs auf das Internet zugreift. Das Zielsystem sieht daher als Absender nur die Firewall, die wiederum die

Antwortpakete des Zielsystems an den entsprechenden PC im internen Netz weiterleitet. Je nach Firewall-Typ ist es ihr dadurch möglich, die Netzwerkpakete in beiden Richtungen zu analysieren und zu filtern, noch bevor sie die tatsächlichen Kommunikationspartner erreichen.



Anschluss einer externen Firewall, die den Zugriff zwischen dem Internet und dem privaten (in sich geschlossenen) Netz beschränkt

Beispielkonfiguration der Abbildung: Der Internetanschluss könnte ein DSL-Anschluss inklusive DSL-Modem sein. Die Firewall könnte dann auf einem DSL-Router installiert sein, der von den PCs im privaten (in sich geschlossenen) Netz als default Gateway angesprochen wird. Das Gerät verwaltet dadurch die Netzwerkanfragen der internen PCs und kann zwischen Anfragen an das interne (private) und externe Netz (Internet) unterscheiden und sie entsprechend weiterleiten. Der Switch verbindet die PCs des internen Netzes miteinander und ist meist in einer solchen Firewall integriert, wird hier aber bewusst als eigenständiges Gerät dargestellt, um zu verdeutlichen, dass eine derartige Firewall nur den Zugriff zwischen dem internen und externen Netz filtert, jedoch keinen Einfluss auf die Kommunikation im internen Netz hat.

Da das Zielsystem aus dem Internet nicht den internen PC, sondern nur die Firewall sieht, sind mögliche Angriffe aus dem Internet an die dafür prädestinierte Firewall gerichtet und treffen nicht direkt den internen PC. Jemand aus dem Internet, der auf der Netzwerkadresse der Firewall nach einem Netzwerkdienst (wie beispielsweise die Datei- und Druckerfreigabe) sucht, wird nicht fündig, da der Dienst auf dem PC und nicht auf der Firewall läuft. Auf diesem Level ist die Firewall also nicht angreifbar und die Netzwerkdienste der internen PCs aus dem Internet heraus nicht erreichbar.

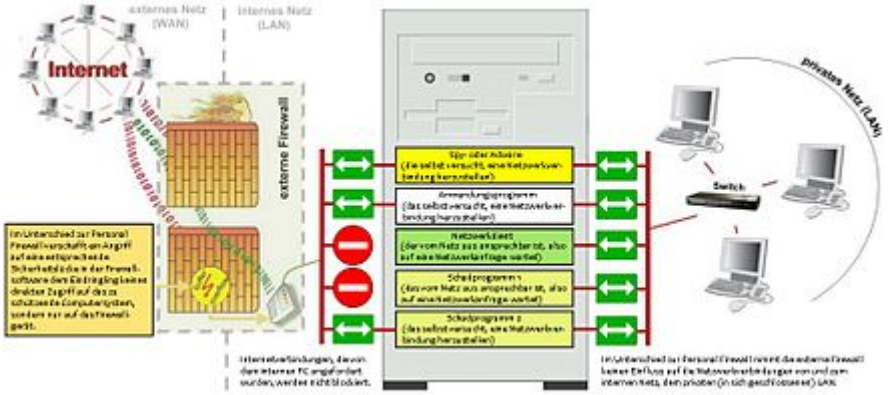
Auch eine Schadsoftware, die womöglich auf dem PC heimlich einen Netzwerkdienst installiert, kann an diesem Zustand nichts ändern. Der Netzwerkdienst ist nur aus dem privaten Netz heraus ansprechbar, nicht jedoch aus dem Internet heraus (die Schadsoftware kann schließlich keinen Dienst auf der Firewall installieren, sondern nur auf dem PC).

Hinweis: Für die beschriebene Funktionalität ist es erforderlich, dass das Firewall-Gerät entsprechend konfiguriert wurde (das zu schützende Computersystem darf nicht als „Standardserver“ oder *Exposed Host* betrieben werden, bzw. sollte es in keiner „DMZ“ stehen, was je nach der Benutzeroberfläche des Firewall-Gerätes meist auch ohne fundierte Fachkenntnisse leicht überprüft und im Bedarfsfall angepasst werden kann).

Grenzen

Im privaten Bereich finden meist Paketfilter-Firewalls Anwendung, die auf einem DSL-Router arbeiten. Sie können einzelne Programme nur sehr bedingt davon abhalten, ohne das Einverständnis des Anwenders mit der Außenwelt zu kommunizieren, denn sie wurden für eine solche Aufgabe nicht konzipiert: Damit ein solches Gerät ohne permanenten manuellen Konfigurationsaufwand funktioniert, muss es in der Lage sein, dynamische Regeln zu erstellen. Abgesehen von Anfragen auf explizit gesperrten Adressen und gesperrten Zielports erlaubt er deshalb automatisch alle Kommunikationsverbindungen, die von dem internen Netz (also von den privaten PCs) angefordert wurden.

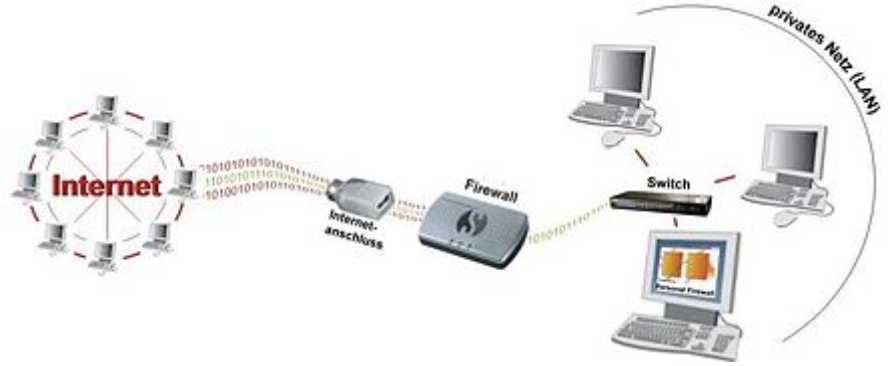
Wenn also eine Schadsoftware lediglich einen Netzwerkdienst installiert, der auf eine externe Verbindung wartet, so funktioniert der Schutzmechanismus recht gut. Baut sie jedoch selbst eine Verbindung zum Internet auf, so wird das Gerät die Verbindung zulassen, da sie vom internen Netz heraus angefordert wurde. Ein solches Gerät kann also lediglich externe Verbindungsanfragen effektiv unterbinden.



Im Unterschied zur Personal Firewall nimmt die externe Firewall keinen Einfluss auf die Verbindungen innerhalb des privaten Netzes. Sie lässt Anfragen vom internen Netz hin zum externen Netz (Internet) zu. Anfragen vom externen Netz hin zu Teilnehmern des internen Netzes werden blockiert, solange sie nicht zu einer Antwort auf einer internen Netzwerkanfrage gehören.

Hier bietet eine Personal Firewall mitunter mehr Möglichkeiten, ist dafür aber nicht notwendigerweise sicherer und beinhaltet die oben genannten Risiken. Eine Personal Firewall ist zwar kein ebenbürtiger Ersatz für solche Geräte, sie kann aber unter bestimmten Bedingungen als eine entsprechende Ergänzung dienen.

Dementsprechend erreichen einige DSL-Router, die im Widerspruch dazu augenscheinlich eine Netzwerkzugriffskontrolle für Anwendungen des PCs zu realisieren scheinen, dies mit einem simplen Trick: Laut Handbuch soll der Anwender zunächst die zu dem Gerät gehörende Administrationssoftware auf dem PC installieren. Zusammen mit der Administrationssoftware gelangt so auch eine hauseigene Personal Firewall auf den heimischen PC. Auch wenn sich die lokal installierte Software mit dem Logo und dem Namen der externen Firewall meldet, hat sie nichts mit ihr zu tun. Eine solche Lösung unterscheidet sich sicherheitstechnisch gewöhnlich nicht von anderen Personal Firewalls, die zusätzlich zu einem DSL-Router installiert werden.

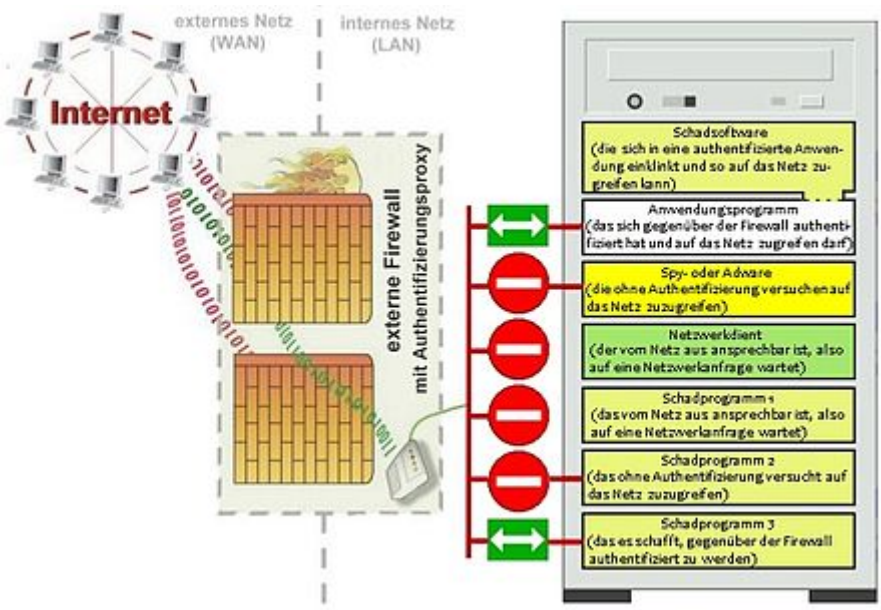


Eine Personal Firewall in Kombination mit einer externen Firewall, um auch ausgehende Netzwerkanfragen zu beschränken

Eine andere Herangehensweise, um die Kommunikation einer Schadsoftware mit dem Internet zu unterbinden, basiert mitunter auf der Idee, dass die Firewall alle Zugriffe des lokalen Netzes auf das Internet sperren soll, die beispielsweise nicht für den Aufruf von Webseiten benötigt werden. Das wird dadurch erreicht, dass eine Filterregel sämtliche Anfragen auf das Internet blockiert. Eine weitere Regel erlaubt nun explizit DNS-Anfragen an den DNS-Server seiner Wahl und Zugriffe auf den Port 80 (HTTP) beliebiger Internetserver, damit der dort laufende Netzwerkdienst für den Zugriff auf Webseiten erreicht werden kann. Die Annahme ist, dass eine auf dem zu schützenden PC installierte Schadsoftware, die selbstständig eine Verbindung zu einem Netzwerkdienst aus dem Internet herstellt, nun blockiert wird, da die Netzwerkanfrage auf deren Port nicht mehr durchgelassen wird.

Diese „Schutzwirkung“ ist jedoch stark begrenzt, denn es ist nicht mit Sicherheit auszuschließen, dass die zu blockierende Schadsoftware nicht auch den freigegebenen Port für ihre Kommunikation verwendet. Je populärer der Port ist, desto wahrscheinlicher wird ein solches Szenario. Da auf fast jeder externen Firewall der Port 80 für die Kommunikation mit dem Internet freigeschaltet ist, nutzen zahlreiche Schadprogramme nun ebenfalls den Port 80 für ihre eigene Kommunikation mit dem Internet, da sie davon ausgehen können, dass der Port nicht blockiert wird. Firmen verwenden solche Filter eher mit dem Ziel, den Zugriff ihrer Mitarbeiter auf das Internet einzuschränken (beispielsweise um zu erreichen, dass HTML-Seiten aufgerufen werden dürfen, eine Teilnahme am Chat jedoch unterbunden wird). Im privaten Heimnetzwerk ergibt solch ein Regelwerk meist keinen Sinn.

Jenseits der Portsperre gibt es auf einigen Geräten erweiterte Methoden, um interne Verbindungsanfragen mithilfe der externen Firewall zu kontrollieren. Sie setzen in der Regel Proxys ein und unterstützen so die Möglichkeit, dass sich jede Anwendung vor der Netzwerkkommunikation bei der externen Firewall authentifizieren muss, bevor die Kommunikation erlaubt wird. Ein Nachteil dieser Methode ist, dass die Anwendung das Authentifizierungsprotokoll (z. B. SOCKS) kennen muss. In einem solchen Umfeld lassen sich also nur Anwendungen nutzen, die entsprechend erweitert wurden, wenngleich die Unterstützung dieser Protokolle bereits breite Verwendung findet, sodass man diesbezüglich fast von einer Standardausstattung der Applikationen sprechen kann. Damit wird es für eine Schadsoftware schwerer, aber nicht unmöglich, unbemerkt mit dem externen Netz zu kommunizieren (siehe Abbildung rechts).



Externe Firewall: Ein Authentifizierungsproxy kann Internetanfragen auf Anwendungen beschränken, die sich der Firewall gegenüber authentifiziert haben. Der Netzwerkzugriff von anderen Anwendungen auf das Internet wird blockiert.

Ergänzend lassen sich auf professionellen Firewalls mitunter spezielle Filter installieren, die nach einigen bekannten Malwaresignaturen in den Netzwerkpaketen eines Dienstes suchen und die Pakete bei Identifikation sperren.

Die genannten erweiterten Methoden erhöhen zwar die schadensbegrenzende Wirkung der externen Firewall auch bei der Kommunikation von innen nach außen. Da sie jedoch bei Geräten für den privaten Gebrauch kaum anzutreffen sind, stellen sie zumindest in diesem Bereich eine Ausnahme dar.

Externe Firewalls sind lediglich dafür ausgelegt, den Netzwerkzugriff zwischen dem internen und externen Netz zu beschränken. Sie bieten also keinen Schutz vor ungewollten Zugriffen aus dem internen Netz, die nach einer Studie des Computer Security Institutes im Jahr 2002 mindestens doppelt so häufig vorkamen wie externe Hacking-Versuche.[32] Vor Computerwürmern, die sich über das Netzwerk verbreiten, bietet sie ebenso wenig Schutz, wenn diese über CDs, USB-Sticks oder Disketten in das interne Netz gebracht werden. Die Computerwürmer Sasser, W32.Blaster und Conficker haben durch Ausbrüche in großen Firmen wie der deutschen Postbank und Delta Air Lines gezeigt, dass diese Infektionswege trotz externer Firewall real funktionieren.[33]

Außerdem ist spätestens seit 2013 bekannt, dass zumindest die US-amerikanische NSA geheime Zugriffsmöglichkeiten entwickelt hat, so genannte Backdoors, welche die Zugangssperren nahezu aller Geräte der bedeutenden Hersteller, darunter auch Router, aushebeln.[34]

Nachteile

Betreibt der eigene Computer an der Internetschnittstelle keine Netzwerkdienste und wird auch sonst entsprechend fachmännisch betrieben, so ist der Einsatz einer externen Firewall fragwürdig, denn die Firewall muss für ihre Arbeit die Netzwerkpakete ggf. separat analysieren. Sie kann die Netzwerkkommunikation also abhängig von ihrer eigenen Hardware-Geschwindigkeit, der Auslastung und dem jeweiligen Algorithmus mehr oder weniger stark verzögern. Allerdings verursachen moderne Geräte innerhalb normaler Parameter üblicherweise Verzögerungen unterhalb der Wahrnehmungsschwelle.

Zusätzlich dazu kann der Einsatz einer Firewall dazu beitragen, dass der Anwender sich in Sicherheit wiegt und unvorsichtig wird, indem er beispielsweise nun leichtfertig Software aus unsicheren Quellen installiert, da ihn die Firewall vermeintlich vor einen Fernzugriff auf eine mögliche Schadsoftware schützt. Dadurch verliert er nicht nur die Sicherheit, sondern gefährdet sein System mehr als zuvor; das trifft auch auf die Verwendung einer Personal Firewall zu.

Siehe auch: Überprüfbarkeit des Quelltextes

Weitere Einsatzgebiete in Unternehmensnetzen

In Unternehmensnetzen rechtfertigt nicht nur der Übergang vom LAN zum Internet den Einsatz einer Firewall. Auch zwischen zwei oder mehreren organisationsinternen Netzen kann eine Firewall verwendet werden, um dem unterschiedlichen Schutzbedarf der Netzwerkzonen Rechnung zu tragen, beispielsweise bei einer Trennung zwischen dem Büronetz vom Netz der Personalabteilung, in dem personenbezogene Daten gespeichert sind.[35]

Firewall-Techniken

Eine Firewall kann mit verschiedenen Methoden erwünschten von unerwünschtem Netzwerkverkehr unterscheiden, von denen aber nicht jedes Produkt alle unterstützt.

Paketfilter-Firewall

→ Hauptartikel: Paketfilter

Zur Aufgabe einer Paketfilter-Firewall gehört es, Netzwerkpakete anhand ihrer Netzwerkadresse zu sperren oder durchzulassen. Dafür wertet sie die Header-Informationen der Netzwerkpakete aus.

Die einfache (zustandslose) Paketfilterung arbeitet auf einem Firewall-Router mit statischen Regeln und betrachtet jedes Netzwerkpaket einzeln. Sie stellt also keine Beziehungen zu den vorherigen Netzwerkpaketen her. Demgegenüber gibt es eine erweiterte Form der (zustandsgesteuerten) Paketfilterung, die solche Beziehungen erfasst, indem sie auf die Technik der Stateful Inspection zurückgreift. So wird der Zugriff auf das Quellsystem, das eine Kommunikation angefordert hat, weiter eingeschränkt. Eine entsprechende Firewall wird ebenfalls als reine Paketfilter-Firewall klassifiziert, zumindest solange darauf keine (möglichen) Proxyfilter installiert werden.

Netzwerkadressierung als Grundlage für die Paketfilterung

→ Hauptartikel: MAC-Adresse, IP-Adresse und Port (Protokoll)

Jede Netzwerkkarte hat eine eindeutige abrufbare Seriennummer, welche man *MAC-Adresse* nennt. Sie setzt sich zusammen aus einer Herstelleridentifikationsnummer und einer angrenzenden laufenden Nummer.

Da diese Nummern eindeutig sind, lassen sie sich für eine simple aber dafür allgemeingültige Art der Adressierung in einem Netz nutzen. Simpel deshalb, weil sich damit zwar beispielsweise ein Computer in einem unverzweigten Netz adressieren lässt, aber in der MAC-Adresse nicht angegeben werden kann, für welches Programm des Computers das Netzwerkpaket bestimmt ist. Unverzweigt deshalb, weil die MAC-Adresse aufgrund ihres Aufbaus nicht dafür geeignet ist, in weitere Teilbereiche zerlegt zu werden. Eine Zuordnung des Adressaten zu einem bestimmten Subnetz ist also mit der MAC-Adresse nicht möglich. Anders formuliert lassen sich MAC-Adressen wie Hausnummern nutzen, aber darüber hinaus weder einer Straße noch einem Bewohner des Hauses zuordnen.

Die Lösung bieten höhere Kommunikationsprotokolle, die über die MAC-Adresse gelegt werden. Ein Netzwerkpaket wird also bildlich gesehen mehrfach verpackt, wobei die MAC-Adresse das äußere Paket darstellt und die weiteren Pakete Schicht für Schicht in diesem Paket stecken. Innerhalb eines TCP-/IP-Netzes bildet die *IP-Adresse* das nächsthöhere Protokoll, also die nächste Verpackung. Es handelt sich dabei um mehrere Ziffernblöcke, vergleichbar mit einer Hausadresse, die eine Straßennummer und eine Hausnummer enthält (welcher Teil der IP-Adresse sinnbildlich die Straßennummer, genauer die *Netzwerk-ID*, repräsentiert und welcher Teil die Hausnummer darstellt, genauer die *Rechner-ID*, wird durch die Subnetzmaske definiert). In einem solchen Netz bildet das nächsthöhere Protokoll, also die Verpackung nach der IP-Adresse, den *Port* ab. Der Port ist vergleichbar mit einer Raumnummer oder einem Namensschild. Er bestimmt, für wen genau „im Haus“ das Paket bestimmt ist (genauer: welches Programm das Paket erhalten soll).

All diese „Verpackungen“ kann eine Firewall auswerten und die Netzwerkpakete entsprechend filtern, indem sie anhand eines „Wer darf worauf zugreifen“-Regelwerks entscheidet, welche Anfragen zulässig sind und welche nicht. In der Regel erfolgt dies jedoch erst ab OSI-Schicht 3, also der IP-Adresse, da sich die MAC-Adress-Information der Netzwerkpakete ändert, wenn sie beispielsweise auf ihrem Weg durchs Netz einen Router passieren.

Die Adressenfilterung bildet die Grundform sämtlicher weiterer Firewall-Arten. Filter, die der reinen Filterung von Netzwerkadressen dienen, also *Paketfilter*, kommen somit auch auf allen anderen Firewalls vor.

Firewall-Router

Ein *Firewall-Router* wird als *Paketfilter-Firewall* klassifiziert und ist eine Software, die auf einem Router installiert ist und die dort die Netzwerkverbindung beschränkt. Dieser Firewall-Typ kann im einseitig transparenten (Router im NAT-Modus) oder beidseitig transparenten Modus in Erscheinung treten (Router ohne NAT).

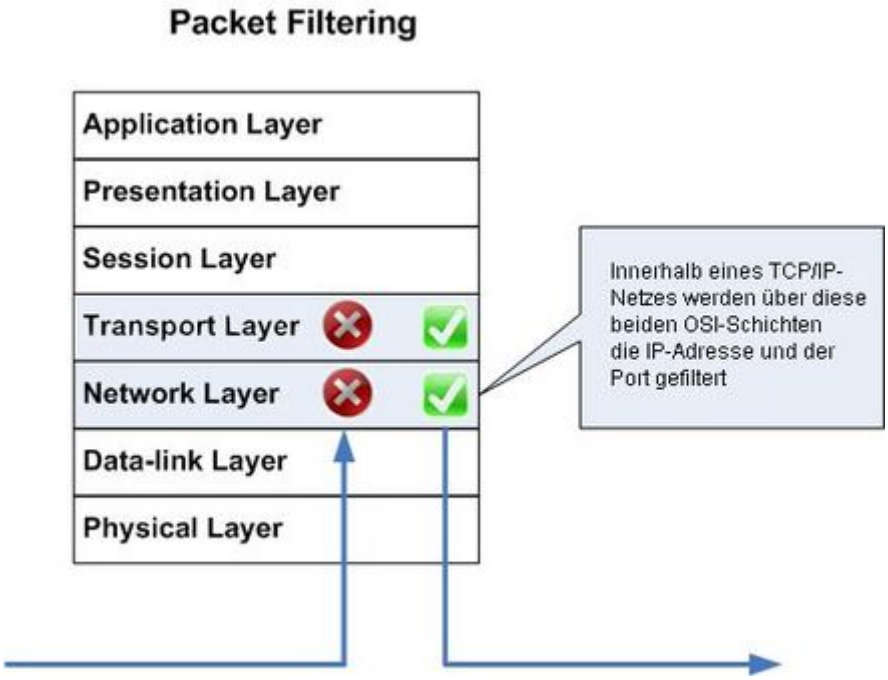
Er wird hauptsächlich mit Firewall-Geräten assoziiert, die statische (zustandslose) Paketfilter verwenden, obgleich genau genommen auch eine Stateful Inspection Firewall auf einem Router aufsetzen kann. Andere Firewall-Arten unterscheiden sich von einem Firewall-Router also dadurch, dass sie zumindest eine genauere Form der Paketfilterung anbieten (Stateful Inspection) oder auf einem vom Router abweichenden Konzept basieren und dabei neben dem Paketfilter meist eine erweiterte Form der Filterung anbieten (wie Proxy Firewall und Personal Firewall).

Der Firewall-Router ist bei gleicher Hardware verglichen mit anderen Firewall-Arten sehr schnell.

OSI-Schichten

→ *Hauptartikel: OSI-Modell*

Das OSI-Schichtenmodell beschreibt die Designgrundlage von Kommunikationsprotokollen in Rechnernetzen. Ein Paketfilter greift nach diesem Schichtenmodell auf die OSI-Schicht 3 (IP-Adresse) und 4 (Port) aus den Header-Informationen eines Netzwerkpaketes zu.



OSI-Schichten: Paketfilter einer Firewall

Beispiel für ein Regelwerk

→ *Hauptartikel: Firewall-Regelwerk*

Bei den folgenden beispielhaften Filterregeln ist zu beachten, dass nicht inhaltlich nach den genannten Protokollen, sondern den zu dem entsprechenden Netzwerkdienst gehörenden TCP- bzw. UDP-Ports gefiltert wird:

- Aus dem Internet sind zum Mailserver in der DMZ Mail-Dienste (SMTP – TCP-Port 25, POP3 – TCP-Port 110 und IMAP – TCP-Port 143) erlaubt.
- Der Mailserver darf aus der DMZ in das Internet Mails per SMTP verschicken und DNS-Anfragen stellen.
- Aus dem lokalen Netz sind Administrationsdienste (SSH, Remote Desktop, Backup – TCP-Port 22) zum Mailserver erlaubt.
- Alle anderen Pakete in oder aus der DMZ werden in eine Logdatei geschrieben und danach verworfen.

Die Filterentscheidungen werden für jedes Paket einzeln und unabhängig getroffen. Diese Art der Filterung ist heutzutage in zahlreichen Routern und Layer-3-Switches implementiert.

Stateful Inspection

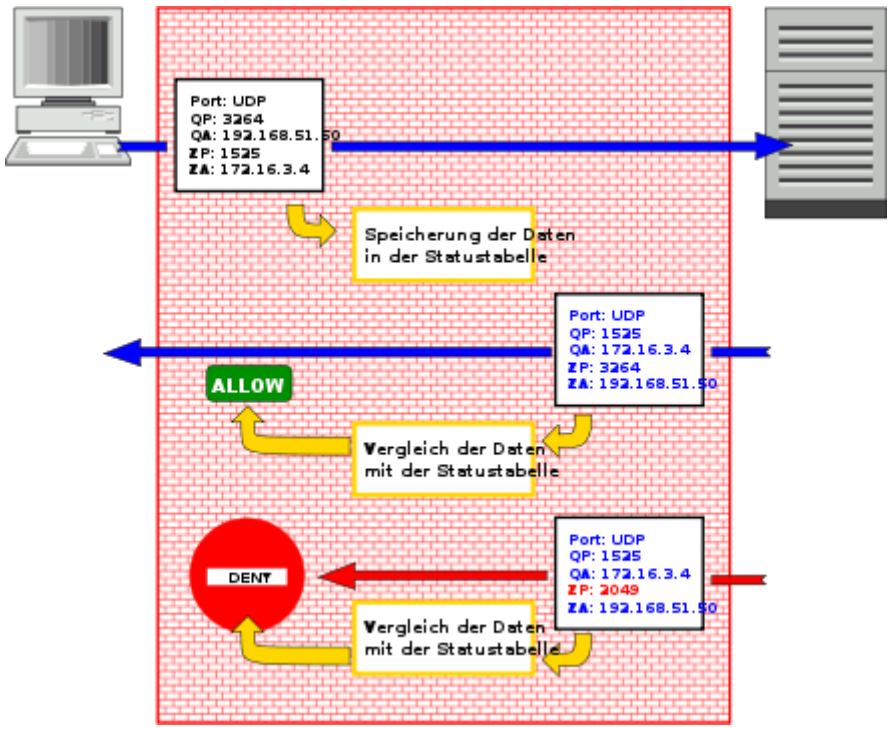
→ *Hauptartikel: Stateful Packet Inspection*

Im Unterschied zu dem statischen (zustandslosen) Paketfilter wird hier die Firewall-Regel bei jeder Verbindungsanfrage dynamisch konkretisiert, um den Zugriff auf eine etablierte Verbindung genauer zu beschränken. Dabei stellt die Firewall den Rückkanal (Ziel- zu Quellsystem) in direkter Beziehung zur zuvor etablierten Verbindung (Quell- zu Zielsystem) und schränkt den Zugriff entsprechend ein, sodass ausschließlich die beteiligten Kommunikationspartner auf die Verbindung zugreifen können. Das ist die Grundfunktion, die alle Stateful Inspection Firewalls beherrschen.

Spezielle Filter zahlreicher Stateful-Inspection-Firewalls können darüber hinaus die Nutzdaten einer Kommunikation einsehen. Das ist beispielsweise für Netzwerkprotokolle sinnvoll, die über die Nutzdaten eine zweite Verbindung zwischen den Kommunikationspartnern aushandeln (siehe aktives FTP). Die

Einsicht in die Nutzdaten erlaubt es dem Filter, die Adressfilterung der Pakete weiter zu präzisieren, er ist im Unterschied zu einem Proxyfilter jedoch nicht in der Lage, die Verbindung selbst zu beeinflussen (er kann die Daten nicht verändern).

Je nach Produkt kann die Stateful-Inspection-Firewall auch nach einem Verbindungsaufbau erkennen, ob und wann der zu schützende PC (genauer der Client) mit dem Zielsystem kommuniziert, wobei die Firewall nur dann Antworten darauf zulässt. Sendet das Zielsystem also Daten, die von dem Client nicht angefordert wurden, so blockiert die Firewall den Transfer selbst nach erfolgter Verbindung zwischen Client und Zielsystem.



Stateful Inspection: Die Eigenschaften ausgehender Datenpakete werden in einer Statustabelle gespeichert. Mit dieser werden eingehende Datenpakete verglichen.

OSI-Schichten

→ *Hauptartikel: OSI-Modell*

Ein Paketfilter, der auf die Technik der Stateful Inspection basiert, greift auf die OSI-Schicht 3 (IP-Adresse), 4 (Port) und ggf. 7 (Nutzdaten) eines Netzwerkpaketes zu.

Mögliche Funktionen

Abhängig von der Konfiguration des Gerätes, auf dem die Firewall-Software installiert wurde und dem Firewall-Produkt, kann eine Stateful-Inspection-Firewall unter anderem die folgenden Funktionen bieten:

- Schutz vor SYN-Flooding, z. B. durch SYN-Cookies
- Verwerfen von fehlerhaften Paketen (z. B. widersprüchliche TCP-Flags wie SYN-Bits, ACK-Bits und Sequenznummern)
- Schutz vor Ping of Death, Smurf-Angriffen, Teardrop-Attacken oder Land-Attacken

Proxy Firewall (auch Application Layer Firewall)

→ *Hauptartikel: Proxy (Rechnernetz)*

Die Filter einer *Proxy Firewall* (auch *Application Layer Firewall* genannt) beachten zusätzlich zu den reinen Verkehrsdaten wie Quelle, Ziel und Dienst typischerweise noch die Nutzdaten, also den Inhalt der Netzwerkpakete. Im Unterschied zur Stateful-Inspection-Technik, die abhängig vom Produkt mitunter auch auf die Nutzdaten zugreift, reicht der typische Proxyfilter die Netzwerkanfrage des Quellsystems nicht einfach an das Zielsystem weiter. Vielmehr baut er selbst eine eigene Verbindung zum Zielsystem auf. Da

er stellvertretend für den anfragenden Client mit dem Zielsystem kommuniziert, kann er die Pakete zusammenhängend analysieren und Einfluss auf die Verbindung nehmen. So ist er in der Lage, Anfragen auch in Bezug auf den Kommunikationsfluss der Nutzdaten zu filtern und kann entscheiden, welche Antworten des Zielsystems er an den anfragenden Client weiterreicht. Dabei kann er den Paketinhalt beliebig verändern.

Technisch gesehen arbeitet ein solcher Filter als ein in den Verkehr eingreifender Kommunikationspartner, der die Verbindungen auf beiden Seiten terminiert (es handelt sich um zwei eigenständige Verbindungen), statt die Netzwerkpakete durchzureichen. Der Filter selbst ist ein Dienstprogramm für Computernetze, das im Datenverkehr vermittelt, und wird daher auch *Proxy-Server* genannt: Als aktiver Vermittler verhält er sich dem anfragenden Client gegenüber wie ein Server, der anderen Seite, dem Zielsystem, gegenüber wie ein Client. Da er das Kommunikationsprotokoll kennen muss, gibt es für jedes höhere Kommunikationsprotokoll (HTTP, FTP, DNS, SMTP, POP3, MS-RPC usw.) einen eigenen Filter (man spricht daher auch von *dedicated Proxys*). Sie können u. a. unerwünschte Protokolloptionen verbieten, indem sie etwa in einer SMTP-Transaktion kein BDAT, VRFY o. Ä. zulassen.[36] Es kann sogar für ein und dasselbe Protokoll mehrere *dedicated Proxys* geben, beispielsweise um unterschiedliche Webdienste unter HTTP zu filtern; beispielsweise je einen pro genutzte Webanwendung in einem Unternehmen.[37]

Eine Ausnahme bildet der *Generische Proxy*, auch *Circuit Level Proxy* genannt. Er findet als *protokollunabhängiger* Filter auf der Proxy Firewall Anwendung und realisiert dort ein port- und adressbasiertes Filtermodul, das zudem eine (mögliche) Authentifizierung für den Verbindungsaufbau unterstützt. Dabei ist der Filter nicht in der Lage die Kommunikation einzusehen, sie selbst zu führen und zu beeinflussen, da er das Kommunikationsprotokoll nicht kennt.

Siehe auch: Web Application Firewall

OSI-Schichten

→ Hauptartikel: OSI-Modell

Ein *dedicated Proxy* als Filter, der auf ein bestimmtes Protokoll spezialisiert ist, arbeitet als vermittelndes Dienstprogramm und greift daher (wie jedes Dienst- oder Anwendungsprogramm) auf die OSI-Schicht 7 *(Application Layer)* zu. Der *Circuit Level Proxy* als generischer (protokollunabhängiger) Filter nutzt dagegen die OSI-Schicht 3 (IP-Adresse), 4 (Port) und ggf. 5 (bei Authentifizierung für den Verbindungsaufbau).

Hinweis: Entgegen einem populären Missverständnis besteht die grundlegende Aufgabe einer *Application Layer Firewall* nicht darin, bestimmten Applikationen (Programmen) den Zugriff zum Netz zu gewähren oder zu verbieten. Der Name *Application* wurde lediglich aus dem *Application Layer* der OSI-Schicht 7 abgeleitet, der dafür steht, dass ein entsprechender Filter in die Nutzdaten der Netzwerkpakete hineinsehen kann. Die Aufgabe, den Netzwerkzugriff auf Anwendungen zu beschränken, die sich der Firewall gegenüber authentifiziert haben, fällt (wenn überhaupt) meist dem generischen Proxyfilter zu, also ausgerechnet dem Filter, der den *Application Layer* nicht einmal nutzt.

Grenzen: Durchtunnelung

→ Hauptartikel: Tunnel (Rechnernetz)

Grundsätzlich kann jeder Dienst auf jeder Portnummer funktionieren. Wenn im Regelwerk der TCP-Port 80 für HTTP freigeschaltet ist, kann darüber trotzdem ein anderes Protokoll laufen. Es müssen nur beide Kommunikationspartner (der Client im internen Netz wie auch der Dienst auf dem Server aus dem externen Netz) entsprechend konfiguriert worden sein. Einen Versuch, dies mithilfe der Firewall zu unterbinden, kann mit Application Layer Firewalls erfolgen. Sie können den Aufbau der Nutzdaten untersuchen und alle

Pakete blockieren, welche nicht dem Protokoll des freigegebenen Dienstes entsprechen. Allerdings soll jedes Protokoll Daten übertragen, weshalb die Daten in diesem Fall lediglich entsprechend konvertiert werden müssen. Bettet die Software die zu übertragenden Daten also in HTTP ein, ohne dabei den Standard des Protokolls zu verletzen, ist auch diese Firewall dagegen machtlos (die Gegenstelle, der Dienst auf dem Server also, muss diese Art der Konvertierung allerdings verstehen). Ein Tunnel nimmt eine solche Konvertierung vor. Manipulierte Daten können z. B. in Bilddaten verpackte Datenströme sein.

Tunnel bieten daher eine Methode, um die Kontrolle einer Firewall zu umgehen. Tunnel werden auch verwendet, um unsichere Netzwerkprotokolle mithilfe eines gesicherten und verschlüsselten Netzwerkprotokolls abhör- und manipulationssicher zu transportieren. Dies kann beispielsweise durch einen SSH- oder VPN-Tunnel innerhalb einer legitim freigeschalteten Verbindung geschehen.

Sowohl OpenVPN als auch viele SSH-Clients (z. B. PuTTY) sind zudem in der Lage, einen Tunnel über einen HTTP-Proxy aufzubauen, der eigentlich nur Webseiten weiterleiten sollte. Daneben gibt es spezielle Tunnel-Software für Protokolle wie DNS[38] oder ICMP.

Insbesondere Skype ist ein Beispiel dafür, wie gut sich die meisten Firewalls von innen nach außen umgehen lassen.[39] Solange die Benutzer aus dem internen Netz die Möglichkeit haben, auf Webseiten zuzugreifen, hat der Firewall-Administrator durch die Verschlüsselung technisch kaum eine Chance, eine Durchtunnelung zu verhindern. Dank Whitelists, die den Zugriff auf bestimmte Server beschränken, können Firewalls das Durchtunneln immerhin stark erschweren. Organisationen erweitern die technischen Maßnahmen mitunter durch organisatorische Sicherheitsmaßnahmen, z. B. ein Verbot der bewussten Tunnelnutzung in der Sicherheitsrichtlinie, die der Mitarbeiter unterzeichnen muss.

Ein transparentes Durchdringen einer Firewall wird auch als Firewall Piercing bezeichnet.[40]

Ergänzende Techniken

Intrusion-Detection- und Intrusion-Prevention-Systeme

→ Hauptartikel: Intrusion Detection System und Intrusion Prevention System

„Intrusion Detection Systeme“ (IDS) und „Intrusion Prevention Systeme“ (IPS) erkennen einen Einbruchsversuch anhand von Kommunikationsmustern. Der Unterschied ist, dass ein IDS den Angriff nur erkennt (Detection (engl.) = Erkennung) und ein IPS (Prevention (engl.) = Verhinderung) den Angriff zu blockieren versucht. Diese Systeme gehören zwar nicht zum Firewall-Modul, können dieses aber ergänzen und werden daher vermehrt in eine Firewall-Lösung als zusätzliche Funktion aufgenommen. Einige Firewall-Systeme bieten Erweiterungsmöglichkeiten, um ein IDS nachzurüsten, unter anderem über Slots für Erweiterungsmodule. Diese Module sind mitunter eigenständige Recheneinheiten mit CPU und Arbeitsspeicher, da diese Funktion je nach Aufgabenfeld eine rechenintensive Leistung erfordern kann. Eine ausreichende CPU-Leistung ist für eine geringe Verarbeitungszeit (Latenz) ausschlaggebend. Die durch IPS-Systeme verursachte Latenzzeit kann je nach Hersteller unter 100 Mikrosekunden liegen.[41]

Das Themenfeld, Angriffe zu erkennen und darauf automatisiert zu reagieren, ist sehr komplex. Ein unbedachtes Konzept, eine schlechte Implementierung oder eine ungünstige Konfiguration kann unter Umständen erst die Möglichkeit für einen Denial-of-Service-Angriff schaffen. So legen manche Systeme eine temporäre Firewall-Regel an, die alle weiteren Verbindungsversuche von der vermeintlichen angreifenden IP-Adresse blockieren. Schickt aber nun ein Angreifer Pakete mit einer gefälschten Absender-Adresse an das System (siehe IP-Spoofing), so kann er damit erreichen, dass der Zugriff auf die gefälschte Adresse nicht mehr möglich ist. Wurden hierfür keine Ausnahmen definiert, so kann er nacheinander sämtliche Adressen von dem angegriffenen System abschotten, die dieses für seine Arbeit benötigt (DNS-Server usw.).

Weitere mögliche Funktionen

Folgende Funktionen können auf einem Firewall-Gerät noch Anwendung finden:

- Endpunkt für VPN-Verbindungen
- Berücksichtigung von Quality of Service bei der Verarbeitungspriorität
- Etherchannel (je nach Hersteller auch *Link-* oder *Port-Aggregation*, *Bonding* oder *Trunking* genannt), um mehrere physikalische Interfaces zu einem schnellen logischen Interface zusammenzufassen, beispielsweise zwei 100 MBit-Interfaces zu 200 MBit

Siehe auch

- Air Gap
- Web Application Firewall

Literatur

- Jacek Artymiak: *Building Firewalls with OpenBSD and PF*. 2nd edition. devGuide.net, Lublin 2003, ISBN 83-916651-1-9.
- Wolfgang Barth: *Das Firewall-Buch. Grundlagen, Aufbau und Betrieb sicherer Netzwerke mit Linux*. 3. aktualisierte und erweiterte Auflage. Millin-Verlag, Poing 2004, ISBN 3-89990-128-2.
- Bundesamt für Sicherheit in der Informationstechnik: *Konzeption von Sicherheitsgateways. Der richtige Aufbau und die passenden Module für ein sicheres Netz*. Bundesanzeiger, Köln 2005, ISBN 3-89817-525-1.
- W. R. Cheswick, S. M. Bellovin, A. D. Rubin: *Firewalls and internet security. Repelling the Wily Hacker*. Addison-Wesley, Boston MA u. a. 2007, ISBN 978-0-201-63466-2 *(Addison-Wesley Professional Computing Series)*.
- Andreas Lessig: *Linux Firewalls. Ein praktischer Einstieg*. 2. Auflage, O'Reilly, Beijing u. a. 2006, ISBN 3-89721-446-6 (Download (http://www.oreilly.de/german/freebooks/linuxfire2ger/index.html) der LaTeX-Quellen)
- RFC 2979 Behavior of and Requirements for Internet Firewalls.
- Stefan Strobel: *Firewalls und IT-Sicherheit. Grundlagen und Praxis sicherer Netze: IP-Filter, Content Security, PKI, Intrusion Detection, Applikationssicherheit*. 3. aktualisierte und erweiterte Auflage, dpunkt-Verlag, Heidelberg, 2003, ISBN 3-89864-152-X *(iX-Edition)*

Weblinks

Wiktionary: Firewall – Bedeutungserklärungen, Wortherkunft, Synonyme, Übersetzungen
Commons: Firewall (https://commons.wikimedia.org/wiki/Category:Firewall?uselang=de) – Sammlung von Bildern, Videos und Audiodateien

- Checkliste des Landesbeauftragten für den Datenschutz Niedersachsen aus dem Jahr 1999 (http://www.lfd.niedersachsen.de/download/31977/Orientierungshilfe_Grundschutz_durch_Firewall_LfD_Niedersachsen_.pdf) (PDF; 146 kB)
- BSI Firewall Studie aus dem Jahr 2001 (https://web.archive.org/web/20120125183957/https://www.bsi.bund.de/ContentBSI/Publikationen/Studien/firewall/firewall.html) (Memento vom 25. Januar 2012 im *Internet Archive*)
- Artikel im HaBo-Wiki (http://wiki.hackerboard.de/index.php/Firewall)

Einzelnachweise

1. duden.de (http://www.duden.de/rechtschreibung/Firewall), Definition „Firewall“, Stand 26. Mai 2012
2. Michael Wächter, „Falsifikation und Fortschritt im Datenschutz“, ISBN 3-428-09780-7, 1998, S. 92
3. „HIPAA Training and Certification: Job-Role-Based Compliance“, ISBN 978-1-4239-5899-4, Axo Press, Supremus Group 2008, S. 18
4. Erwin Erasim, Dimitris Karagiannis (Hrsg.), „Sicherheit in Informationssystemen – SIS 2002“, ISBN 3-7281-2864-3, Hochschulverlag AG, 2002, S. 88
5. Kritische Sicherheitslücke im Windows Server Dienst (https://www.heise.de/security/meldung/Microsoft-patcht-kritische-Luecke-im-RPC-Dienst-213171.html), heise Security, 23. Oktober 2008
6. Holger Schwichtenberg, Frank Eller: „Programmierung mit der .NET-Klassenbibliothek“, ISBN 3-8273-2128-X, Addison-Wesley-Verlag, 2004, S. 434
7. Newsletter Bürger CERT (https://web.archive.org/web/20150110063619/https://www.buerger-cert.de/archive?type=widnewsletter&nr=NL-T10-0002) (Memento vom 10. Januar 2015 im *Internet Archive*), „Manipulierte Webseiten“, 21. Januar 2010
8. Harald Schumann: Angriff aus dem Netz (http://www.tagesspiegel.de/medien/digitale-welt/angriff-aus-dem-netz/1969710.html), *tagesspiegel.de*, 31. Oktober 2010
9. Sicherheitslücken in Ciscos IOS (https://www.heise.de/security/meldung/Sicherheitsluecken-in-Ciscos-IOS-138366.html), über die Möglichkeit mit einem präparierten Ping-Paket Programmcode einzuschleusen, Heise Security, 25. Januar 2007
10. Andrew Lockhart: „Netzwerksicherheit Hacks“, ISBN 978-3-89721-496-5, O’Reilly Verlag, 2. Auflage 2007, S. 130
11. Richard A. Deal: „Cisco Pix Firewalls“, ISBN 0-07-222523-8, 2002, S. 207
12. *Deconstructing Common Security Myths* (http://www.microsoft.com/technet/technetmag/issues/2006/05/SecurityMyths/default.aspx), von Microsoft *TechNet Magazine*, *Jesper Johansson* und *Steve Riley*, Heft Mai/Juni 2006
13. *ZoneAlarm im Kreuzfeuer (https://www.heise.de/newsticker/meldung/ZoneAlarm-im-Kreuzfeuer-168262.html)*, *Der Spion der aus dem Inneren kam*, c’t Heft 17 (https://web.archive.org/web/20071016052925/http://www.heise.de/ct/06/17/006/) (Memento vom 16. Oktober 2007 im *Internet Archive*), S. 108–110, *Jürgen Schmidt*, 7. August 2006
14. *Schutz vor Viren unter Windows Antworten auf die häufigsten Fragen (https://web.archive.org/web/20071016194852/http://heise.de/ct/06/18/196/) (Memento vom 16. Oktober 2007 im* Internet Archive*)*, c’t Heft 18, *Daniel Bachfeld*, S. 196
15. BSI Grundschutzkataloge: Entwicklung eines Konzepts für Sicherheitsgateways (https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02070.html)
16. Firewall telefoniert nach Hause (http://hefte.com-magazin.de/uploads/tx_commagdb/2006-04_Aktuell.pdf) Zeitschrift *com!*, Ausgabe 4/2006, S. 12
17. G. Borges, J. Schwenk, C. Stuckenberg: „Identitätsdiebstahl und Identitätsmissbrauch im Internet“, ISBN 978-3-642-15832-2, Springer Verlag 2011, S. 61
18. *Unternehmensperimeter (https://www.paloaltonetworks.de/solutions/location/enterprise-perimeter1.html)*. Palo Alto Networks. Abgerufen am 7. Juli 2016.
19. Next Generation Intrusion Prevention System (NGIPS) (https://archive.today/20160706200550/https://de-fortinet.onelink-translations.com/solutions/next-gen-ips.html) (Memento vom 6. Juli 2016 im Webarchiv *archive.today*)
20. W. R. Cheswick, S. M. Bellovin, A. D. Rubin: „Firewalls und Sicherheit im Internet“, ISBN 3-8273-2117-4, Addison-Wesley-Verlag, S. 159 ff.

21. Problem mit BitDefender und den Windows Firewall-Einstellungen unter Windows 10 (https://forum.bitdefender.com/index.php?showtopic=58993), bitdefender.com, 31. Juli 2015
22. Personal Firewalls, Teil2 (https://web.archive.org/web/20100212154510/http://blog.copton.net/articles/pfw-versagen/index.html) (Memento vom 12. Februar 2010 im *Internet Archive*) von copton.net, *Alexander Bernauer*
23. Support von Microsoft (https://support.microsoft.com/de-de/kb/2530126) zum Thema „Windows-Firewall startet nicht wegen Fehler 0x8007042c“, bezogen auf Windows 7, abgerufen am 5. Juli 2016
24. Bagle-Würmer deaktivieren Windows Firewall (https://winfuture.de/news,17316.html), winfuture.de, Meldung vom 31. Oktober 2004
25. Hinweis: Eine bereits ausgeführte (also auf dem System installierte) Schadsoftware lässt sich zuverlässig durch die Einspielung des letzten „sauberen“ Abbildes der Festplatte (Image) aus dem Computersystem entfernen (siehe auch G4L, Clonezilla, Partimage), wohingegen beispielsweise eine Antivirensoftware nur bedingt dazu in der Lage ist, den Schädling und seine Manipulationen am Computersystem vollständig zu entfernen. Siehe: Cleaning a Compromised System (http://technet.microsoft.com/de-de/library/cc512587%28en-us%29.aspx), Microsoft TechNet, Jesper M. Johansson, 7. Mai 2004
26. Personal Firewalls (https://www.arschkrebs.de/slides/firewall.pdf) (PDF), Autor: Ralf Hildebrandt, Vortragsfolien „Nutzen und Gefahren“, S. 6 Schutz vor „Ping of Death“
27. Personal Firewalls, Teil1 (https://web.archive.org/web/20110415061101/http://blog.copton.net/articles/pfw-ds/index.html) (Memento vom 15. April 2011 im *Internet Archive*) von copton.net, *Alexander Bernauer*
28. Kritische Sicherheitslücken in Symantecs Desktop Firewalls (https://www.heise.de/newsticker/meldung/Kritische-Sicherheitsluecken-in-Symantecs-Desktop-Firewalls-98469.html), Heise.de, 13. Mai 2004
29. Software mit Fehlern und deren Folgen (https://web.archive.org/web/20150109184420/http://www.lohmar.de/uploads/media/Info3_fehlerhafte_Software.pdf) (Memento vom 9. Januar 2015 im *Internet Archive*) (PDF), *Melanie Ulrich*; US-Magazin *Wired*; 14. Januar 2007
30. Wurm Witty dringt über Lücke in Sicherheitsprodukte von ISS ein (https://www.heise.de/newsticker/meldung/Wurm-Witty-dringt-ueber-Luecke-in-Sicherheitsprodukte-von-ISS-ein-95783.html), von heise.de, *Daniel Bachfeld*, 22. März 2004
31. Netzwerkdienste auf einem Windows XP/2000 System deaktivieren: win32sec von dingens.org (http://www.dingens.org/) (grafisch), svc2kxp.cmd von ntsvcfg.de (http://www.chip.de/downloads/svc2kxp_13636185.html) (batch)
32. „Sicherheit in Informationssystemen – SIS 2002“, Erwin Erasim, Dimitris Karagiannis (Hrsg.), ISBN 3-7281-2864-3, Hochschulverlag AG, 2002, S. 88
33. Datenschutzbeauftragter von Microsoft sagt im Sasser-Prozess aus (https://www.heise.de/newsticker/meldung/Datenschutzbeauftragter-von-Microsoft-sagt-im-Sasser-Prozess-aus-113914.html), Heise.de, 6. Juli 2005
34. Jacob Appelbaum, Judith Horchert and Christian Stöcker: *Shopping for Spy Gear Catalog Advertises NSA Toolbox* (http://www.spiegel.de/international/world/catalog-reveals-nsa-has-back-doors-for-numerous-devices-a-940994.html), in: Der Spiegel, englischsprachige Online-Ausgabe vom 29. Dezember 2013, Abruf 31. Oktober 2017
35. BSI Grundschutzkataloge: Sicherheitsgateway (Firewall) (https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/baust/b03/b03301.html)
36. BSI Grundschutzkatalog: Geeignete Auswahl eines Application-Level-Gateways (https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02075.html)
37. Claudia Eckert: „IT-Sicherheit – Konzepte, Verfahren, Protokolle“, ISBN 978-3-486-58999-3, 2009, Oldenbourg Wissenschaftsverlag, 6. Auflage, S. 730

38. Eine Firewall mit Hilfe eines DNS-Tunnels umgehen (http://wiki.hackerboard.de/index.php/DNS-Tunnel#Eine_Firewall_mit_Hilfe_eines_DNS-Tunnels_umgehen)
39. Jürgen Schmidt: *Der Lochtrick, Wie Skype & Co. Firewalls umgehen (https://www.heise.de/security/artikel/Wie-Skype-Co-Firewalls-umgehen-270856.html)* In: c't 17/06, S. 142
40. Methoden zur Umgehung einer Firewall (http://tldp.org/HOWTO/Firewall-Piercing/index.html)
41. https://www.trendmicro.de/cloud-content/us/pdfs/business/datasheets/ds_tps_440t.pdf

---