

Externe Firewall

Eine **externe Firewall** (auch **Netzwerk-** oder **Hardwarefirewall** genannt) kontrolliert die Verbindung zwischen zwei Netzen und dient dazu, den Netzwerkzugriff zu beschränken, basierend auf Absender- oder Zieladresse 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.

Die Netze könnten beispielsweise ein privates Netz (LAN) und das Internet (WAN) sein; möglich ist aber auch eine Verbindung unterschiedlicher Netzwerksegmente ein und desselben Netzwerks.

In Abgrenzung zur Personal Firewall arbeitet die Software einer externen Firewall nicht auf den zu schützenden Systemen selbst, sondern auf einem separaten Gerät, welches Netzwerke oder Netzsegmente miteinander verbindet und dank der darauf laufenden Firewall-Software gleichzeitig den Zugriff zwischen den Netzen beschränkt. Ein derart spezialisiertes Gerät bietet vorwiegend ein sicherheitsoptimiertes und netzwerkseitig stabiles System, welches dank der physischen Trennung zu den zu schützenden Computersystemen nicht so einfach manipuliert werden kann.

Eine externe Firewall besteht somit aus Soft- und Hardwarekomponenten. Hardwarekomponenten sind Geräte mit Netzwerkschnittstellen, die die Netze miteinander verbinden, wie Bridge, Router oder Proxy; Softwarekomponenten sind deren Betriebssystem sowie die Firewall-Software, die auf diesen Geräten installiert wurde (inklusive deren Paket- oder Proxyfilter).

Inhaltsverzeichnis

Grundlagen

Firewalltypen

Bridging-Firewall

Routing-Firewall

Proxy-Firewall

Hardwarefirewall

Netzwerkzonen (Schnittstellen)

Das externe Netz (meist als WAN-Port betitelt)

Das interne Netz (meist als LAN-Port betitelt)

Das Management-Netz

Die demilitarisierte Zone (DMZ)

Die exposed DMZ (auch kurz DMZ) und der exposed Host

Filterverfahren

Anpassung der Netzwerkadresse im Übergang zwischen dem internen und externen Netz

Kontroverse zum Begriff Firewall beim DSL-Router

Grundlegende sicherheitstechnische Grenzen

Beispiel einer einfachen Firewallumgebung

Weitere Funktionen und Aspekte

Anti-Spoofing (Ingress filtering)

Authentifizierung

Intrusion Detection und Intrusion Prevention Systeme

Hochverfügbarkeit

Hochsicherheitsumgebungen

Virtual Local Area Networks

Routing und Multicast

Administration

Leistungsmessung und Optimierung

Fehlersuche

Problematische Protokolle

Voice over IP und Videokonferenzen

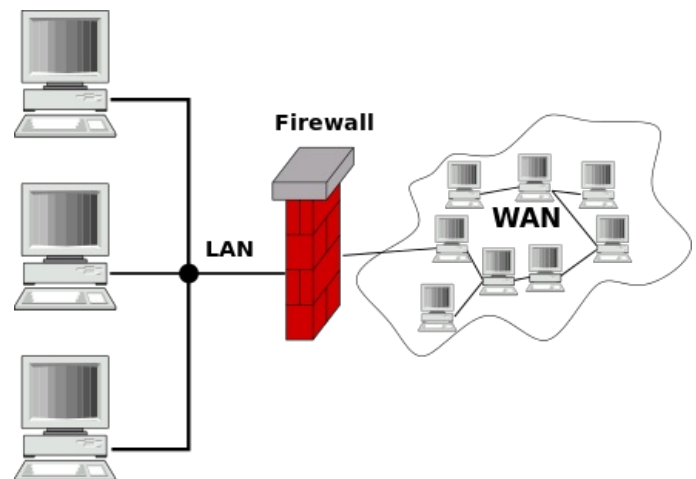
File Transfer Protocol (FTP)

Entstehung der Firewall

Produkte

Firewall-Software

Firewall-Geräte



Die externe Firewall befindet sich zwischen verschiedenen Rechnernetzen und beschränkt den Zugriff zwischen diesen Netzen, in diesem Beispiel zwischen dem Local Area Network (LAN) und dem Wide Area Network (WAN).

Siehe auch

Quellen

Literatur

Weblinks

Grundlagen

Firewalltypen

Neben der Möglichkeit, auf einer geeigneten Maschine eine Firewall-Software (beispielsweise Check-Point-Firewall 1 oder IPFire) zu installieren und das Betriebssystem selber zu härten, gibt es die Möglichkeit, eine Firewall-Appliance zu benutzen: Sie bieten eine aufeinander abgestimmte Kombination aus Hardware, gehärtetem Betriebssystem und Firewall-Software (z. B. Cisco ASA oder Astaro Security Gateway).^[1]

Man unterscheidet zwischen den folgenden Typen:

Bridging-Firewall

Hier sind die Netzwerkschnittstellen wie bei einer Bridge (heute meist durch einen Switch ersetzt) gekoppelt. Eine Bridge ist dafür gedacht, zwei physisch getrennte Netzsegmente miteinander auf OSI-Schicht 2 zu verbinden. Sie zeichnet sich dadurch aus, dass sie nur dann Daten (Frames) in das jeweils andere Segment durchreicht, wenn sich der adressierte Teilnehmer auch in dem betreffenden Segment befindet. Grundlage für diese Filterung bilden die OSI-Schicht-2-Adressen (MAC) der Daten-Rahmen.

Um ihre Arbeit zu verrichten, benötigt eine Bridge für sich selbst also keine höheren (IP-)Adressen (anders als bei einem Router wird sie auf dieser Ebene von keinem Kommunikationspartner direkt adressiert) und ist daher im Netz praktisch unsichtbar und auf dieser Ebene auch nicht angreifbar („Bump in the wire“). Allerdings lässt sich der Bridging-Firewall per entsprechender Konfiguration meist eine höhere (IP-)Adresse zuordnen, damit sie nicht nur lokal, sondern auch vom Netz aus administriert werden kann. Dies erfolgt in der Regel auf einer dediziert für Firewall-Verwaltungszwecke vorgesehenen Management-Schnittstelle.

Damit ihre Filterung nicht auf Low-Level-Adressen beschränkt bleibt, unterscheidet sich die Bridging-Firewall von einer typischen Bridge dahingehend, dass sie intern auch auf höhere Protokollebenen zugreift und damit in der Lage ist, IP-Adressen und Ports zu filtern, mitunter inklusive Stateful Packet Inspection. Darüber hinaus kann sie auch Adressen umleiten (*IP- und Port-Forwarding*), sobald die Bridging-Firewall Teil des Kommunikationswegs ist. Realisiert werden kann eine solche Firewall beispielsweise mit dem Netfilter-Framework.

Routing-Firewall

Hier sind die Netzwerkschnittstellen wie bei einem Router gekoppelt. Das ist die am weitesten verbreitete Art; sie kommt bei praktisch allen SoHo-Geräten (für den privaten Gebrauch und kleinere Unternehmen), aber mitunter auch bei größeren Systemen zum Einsatz. Im Vergleich zur Bridge arbeitet ein Router auf einer höheren Abstraktionsebene, indem er zwischen unterschiedlichen IP-Domänen (Subnetze) vermittelt (sämtliche Wege, die ein Netzwerkpaket in vermaschten Netzen nehmen soll, verwaltet der klassische Router anhand der IP-Adresse). Ein Nachteil ist, dass eine darauf aufgesetzte Firewall daher im Netz sichtbar ist und direkt angegriffen werden kann (entweder erscheint sie als Verbindungsglied zwischen den Subnetzen – Router ohne NAT – oder aber sie wird gar als vermeintlicher Kommunikationspartner angesprochen – Router im NAT-Modus).

Der NAT-Modus ist eine mögliche Eigenschaft des Routers. Er beeinflusst das Verhalten der Firewall, wenn sie auf einem solchen Gerät aufgesetzt wird: Im NAT-Modus, aus dem privaten Bereich vor allem durch DSL-Router bekannt, bildet diese Firewall ihre eigene externe Adresse auf den jeweiligen internen Client ab, der eine Verbindung zum externen Netz (Internet) hergestellt hat. Bildlich gesehen funktioniert sie dann wie ein automatisiertes Postfach, welches alle ausgehenden Pakete, die die Firewall passieren, mit der eigenen Absenderadresse versieht. Dadurch stellt sie sicher, dass das Zielsystem die Antwortpakete auch wieder an das „Postfach“ schicken wird. Dank einer speziellen NAT-Verwaltung (PAT) erkennt sie, zu welchem internen Gerät ein aus dem Internet eingehendes Antwortpaket gehört. Dorthin leitet sie das Paket weiter, ohne dass der Versender aus dem Internet die wirkliche (interne) Adresse seines Kommunikationspartners kennt. Dieses Verhalten ist auf einer Bridging-Firewall nicht möglich. In diesem Modus verdeckt die Routing-Firewall – genau wie eine *Proxy-Firewall* – die Struktur des internen Netzes, ist im Unterschied dazu aber nicht in der Lage, die Kommunikation zu beeinflussen.

Proxy-Firewall

Hier arbeitet die Firewall als Proxy zwischen dem Quell- und Zielsystem.

Als *transparenter Proxy* verhält sich die Proxy-Firewall ähnlich wie unter der *Routing-Firewall* im NAT-Modus beschrieben. Durch eine entsprechend konfigurierte Infrastruktur des Netzes wird die Anfrage des Clients automatisch über die Proxy-Firewall geleitet, ohne dass der Absender dies bemerkt oder gar beeinflussen kann. Im Unterschied zu NAT leitet eine Proxy-Firewall die Kommunikation nicht einfach weiter. Vielmehr baut sie eine eigene Verbindung zum Zielsystem auf. Sie führt die Kommunikation also selbst, stellvertretend für den anfragenden Client. Daher kann eine

Proxy-Firewall den Inhalt der Netzwerkpakete 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.

Daneben gibt es den *konventionellen Proxy*, der ebenfalls die Kommunikation selbst führt, dabei aber *beiden* Seiten als direkter Kommunikationspartner gegenübertritt. Er wird von ihnen also bewusst angesprochen (adressiert). Hier bittet der Client den Proxy, stellvertretend für ihn die Kommunikation mit dem Zielsystem zu übernehmen. So wird z. B. der Webbrowser derart konfiguriert, dass er sämtliche Internetanfragen nicht direkt zur Zieladresse schickt, sondern als Anforderung formuliert zur Proxy-Firewall sendet.

Bezugnehmend auf das OSI-Schichtenmodell wird eine Proxy-Firewall auch *Application Level Firewall* genannt. Jeder ihrer Proxy-Filter baut stellvertretend für die Clients die Verbindung zum Zielsystem auf. Für jedes höhere Kommunikationsprotokoll (wie HTTP, FTP, DNS, SMTP, POP3, MS-RPC usw.) gibt es einen eigenen Filter, *dedicated proxy* genannt. Auf einem einzigen Gerät können mehrere ‚dedicated proxies‘ gleichzeitig laufen, um unterschiedliche Protokolle bedienen zu können. Sie können unter anderem unerwünschte Protokolloptionen verbieten, etwa in einer SMTP-Transaktion kein BDAT, VRFY o. Ä. zulassen.^[2]

Hardwarefirewall

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.

Netzwerkzonen (Schnittstellen)

Die Hardwarekomponente einer externen Firewall besitzt mehrere Netzwerkschnittstellen (üblicherweise zwischen 2 und 20), an denen jeweils die zu trennenden Netzbereiche angeschlossen sind. Je nach Produkt können diese in folgende Netzwerk- und Vertrauenszonen unterteilt sein:

Das externe Netz (meist als WAN-Port betitelt)

Meist das Internet, aber auch ein weiteres Kundennetz. Diese gelten als unsicher (kein Vertrauen).

Das interne Netz (meist als LAN-Port betitelt)

Aus Sicht der Firewall handelt es sich hierbei um das *eigene* Netz, welches es zu schützen und der Firewall gegenüber als vertrauenswürdig gilt (hohes Vertrauen).

Das Management-Netz

Dieser Netzwerkanschluss ist optional. Von hier aus erfolgen alle Zugriffe zur Konfiguration des Firewallsystems, zum Einspielen der Regeln und andere Verwaltungsfunktionen (absolutes Vertrauen). Mit Hilfe dieses Netzes wird erreicht, dass sich die Firewall nicht einfach aus dem internen Netz heraus anpassen lässt.

Die demilitarisierte Zone (DMZ)

→ Hauptartikel: Demilitarized Zone

An diesem (ebenfalls optionalen) Netzwerkanschluss werden die vom externen Netz aus erreichbaren Server beherbergt (wenig Vertrauen). Diese Server können von sich aus keine eigenen oder nur beschränkte Verbindungen zum internen Netz aufbauen, wohingegen die internen Clients in der Regel auf diese Server genauso zugreifen können, wie auf Server aus dem Internet. Das hat den Vorteil, dass – sollte ein solcher Server aus dem externen Netz heraus eingenommen werden – von dort aus kein direkter Zugriff des Eindringlings auf das interne Netz möglich wird.

Größere Firmen besitzen oft mehrere Firewalls und DMZs mit jeweils unterschiedlichen Rechten, z. B. um die leichter angreifbaren Web- und Mailserver von den Servern mit den Daten für die Außendienstmitarbeiter zu trennen.

Die exposed DMZ (auch kurz DMZ) und der exposed Host

Die Bezeichnung ‚exposed DMZ‘ („freiliegende demilitarisierte *Zone*“) lässt die Vermutung zu, dass es sich hierbei um ein separates Netz handeln könnte, obgleich man deren virtuellen Netzwerkanschluss nur einem *einzigsten* internen Computer zuordnen kann. Diese „Zone“ wird je nach Hersteller manchmal sogar kurz „DMZ“ (ohne „exposed“) genannt, hat aber weder etwas mit einer echten DMZ, noch mit einer separaten Netzwerkzone gemein. Vielmehr gebrauchen einige Hersteller die Bezeichnung „DMZ“ für eine andere Funktionalität, die in Fachkreisen als *exposed Host* bezeichnet wird. Obgleich viele Geräte aus Kostengründen nicht die technischen Voraussetzungen für eine echte DMZ bieten, wird ihr Produkt also mit einem falschen Fachbegriff beworben.

An diesem *exposed Host* werden alle Pakete aus dem externen Netz durchgereicht, die nicht einem anderen Empfänger zugeordnet werden können. Er ist dadurch über die externe Adresse der Firewall auf allen seinen Ports aus dem Internet heraus erreichbar, wodurch die Teilnehmer aus dem Internet praktisch uneingeschränkt auf alle seine Netzwerkdienste zugreifen können. Sobald aber dieser (exposed-) Computer von einem Eindringling eingenommen wird, hat man den Firewallschutz auch für alle anderen internen Teilnehmer verloren, da von dort aus ein ungehinderter Zugriff auf das interne Netz möglich ist. Man setzt damit ein Element mit geringer Vertrauensstufe (exposed Host), das eigentlich in eine echte DMZ gehört, inmitten einer Zone mit einer hohen Vertrauensstufe (das interne Netz).

Filterverfahren

→ Hauptartikel: Firewall

Paketfilter

Die einfache Filterung von Datenpaketen anhand von Port, Quell-IP- und Ziel-IP-Adresse ist die Grundfunktion aller Netzwerk-Firewalls.

Stateful Inspection

Diese zustandsgesteuerte Filterung ist eine erweiterte Form der Paketfilterung, die weitere Verbindungsdaten auswertet und damit erreicht, dass ausschließlich die beteiligten Kommunikationspartner auf die Verbindung zugreifen können. Mit ihr kann die Firewall nach einem Verbindungsaufbau auch erkennen, ob und wann der interne Client mit dem externen Zielsystem kommuniziert, wobei die Firewall nur dann Antworten darauf zulässt. Sendet das Zielsystem also Daten, die von dem internen Client nicht angefordert wurden, so blockiert die Firewall den Transfer selbst nach erfolgter Verbindung zwischen Client und Zielsystem. Darüber hinaus blockiert sie Netzwerkpakete, die nicht in den Kommunikationsfluss passen, die also offenkundig manipuliert wurden oder einfach nur fehlerhaft sind.

Proxyfilter

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 vom Ziel anfordern zu müssen. Auf einem einzigen Gerät kommen oft mehrere Proxys parallel zum Einsatz, um unterschiedliche Protokolle bedienen zu können.

Contentfilter

Dieser Inhaltsfilter ist eine Form des Proxyfilters, der die Nutzdaten einer Verbindung auswertet und zum Beispiel dafür gedacht ist, ActiveX 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 fällt darunter.

Anpassung der Netzwerkadresse im Übergang zwischen dem internen und externen Netz

→ Hauptartikel: Proxy (Rechnernetz) und Network Address Translation

Abhängig vom Typ kann die Firewall eine Änderung der Netzwerkadresse vornehmen (innerhalb des IP-Netzes ist das konkret die IP-Adresse), sobald die Pakete durch das Netz hindurch auf ihrem Weg zum Ziel das Firewallgerät passieren. Dafür gibt es zwei unterschiedliche Verfahren: *Proxy* und *NAT*.

Eine einfache Analogie soll das Proxy-Prinzip verdeutlichen: Freunde kommen zu Besuch. Sie wollen etwas essen und der Gastgeber verfasst zunächst eine Liste der Bestellungen. Dann ruft er den Pizzaservice an, gibt die Bestellung durch, nimmt die Pakete an der Tür entgegen und reicht sie danach an seine Freunde weiter.

Der Gastgeber hat sich dabei analog einer Proxyfirewall verhalten: Er hat stellvertretend für seine Freunde den Kontakt mit dem Pizzaservice aufgenommen. Und er hat die Pakete stellvertretend an der Tür entgegengenommen, um die Pizzen später anhand der Liste an seine Freunde zu verteilen. Er ist in der Lage, die Ware zuvor auf eine korrekte Lieferung hin zu überprüfen und kann, wenn er will, die Pizzen zusätzlich garnieren (die Pakete verändern), ehe er sie weiterreicht.

Der Pizzabote mag sich zwar denken, dass er all die Pizzen nicht alleine verspeisen wird, jedoch hat er nie die Leute gesehen, für die die Pizzen tatsächlich bestimmt waren. Für ihn war einzig und alleine der Gastgeber der Adressat und Ansprechpartner (ein Stellvertreter).

Dank der Anpassung der Adresse lassen sich nicht nur die wahre IP-Adresse des tatsächlichen Kommunikationspartners verbergen, sondern auch einzelne Teilnehmer eines Netzes oder gar ganze Netzwerke selbst dann miteinander verbinden, wenn sie adressierungstechnisch inkompatibel zueinander sind und eine direkte Verbindung daher nicht möglich wäre.

Auch das NAT-Verfahren nimmt eine solche Anpassung vor. Auf das vorherige Beispiel bezogen, lässt sich das NAT-Gerät aber besser mit einem ausgeklügelten Schienensystem hinter dem Türschlitz vergleichen, welches die vom Pizzaboten hindurch geschobenen Pizzen direkt zum wirklichen Empfänger gleiten lässt. Obgleich NAT ebenfalls die Identität der wirklichen Empfänger verbirgt, ist dort eine Manipulation und Analyse der Paketinhalte nicht möglich.

Genau genommen ist es die Port-Verwaltung, die es dem Firewallgerät ermöglicht, ein komplettes privates (in sich geschlossenes) Netz über eine einzigste offizielle Internet-IP-Adresse mit dem Internet zu verbinden. Vergleichbar mit der oben genutzten „Liste der Bestellungen“ erhält jede Verbindung zum Internet im Firewallgerät einen eigenen Rückgabeport. Die Verbindungen können darüber unterschiedlichen internen Clients – den PCs aus dem privaten Netz –

zugeordnet werden. So werden mehrere Computer des privaten Netzes, die mit ihren privaten IP-Adressen (wie z. B. 192.168.0.0/16) nicht direkt mit dem Internet kommunizieren können, durch eine einzige offizielle (also für das externe Netz gültige) IP-Adresse abgebildet. Da das Zielsystem nicht den tatsächlichen Client, sondern nur das Firewallgerät sieht, sind mögliche Angriffe von dort an die dafür prädestinierte Firewall gerichtet und treffen nicht direkt den Client.

Bei einem NAT-Gerät wird dieses Verhalten *Adressumsetzung* genannt, da es die Adresse *ein und derselben* Netzwerkverbindung anpasst. Dagegen realisiert die Proxyfirewall streng genommen keine Adressumsetzung einer Netzwerkverbindung, sondern ist selbst ein in den Verkehr eingreifender Kommunikationspartner. Ein Proxy steht also als End- und Ausgangspunkt separater Verbindungen zum jeweils anderen Netz. Von außen betrachtet ist das Verhalten beider Geräte aber (stark oberflächlich gesehen) ähnlich: Es ändert sich die Absenderadresse, sobald die an das Internet gerichtete Anfrage das Firewallgerät passiert.

Dagegen lässt die Bridgingfirewall und ein Firewallrouter (im Modus ohne NAT) eine direkte Kommunikation mit dem Client zu, ohne die Adresse am Netzwerkübergang zu verändern.

Kontroverse zum Begriff Firewall beim DSL-Router

→ Hauptartikel: DSL-Router

DSL-Router wurden dafür entwickelt, einen DSL-Internetanschluss den Computern eines privaten Netzwerks zugänglich zu machen. Im privaten Netz arbeiten sie als Router (oft sogar in Form eines Layer-3-Switches, der den Router beinhaltet). Dadurch ist es möglich, den DSL-Router auf den internen Geräten als „default Gateway“ zu konfigurieren, wodurch er zwischen den Subnetzen des internen (privaten) Netzes genauso vermitteln kann, wie zwischen dem privaten Netz und dem Internet.

Die Adressumsetzung wird in diesen Geräten dank eines speziellen NAT-Verfahrens realisiert, der dynamischen *Network Address Port Translation* (**NAPT**, auch **PAT**; siehe Port Address Translation). In der Anfangszeit wurden DSL-Router zum Teil bereits dann als DSL-Firewall bezeichnet, wenn sie als Sicherheitstechnik lediglich auf die reine Adressumsetzung durch NAPT setzten.

Die Sicherheitsfunktion der Adressumsetzung basiert darauf, dass diese Geräte ihre Ports *dynamisch* nur an die Kommunikationspartner weiterleiten, die eine Kommunikation aus dem internen Netz heraus angefordert haben. Die Ports des Gerätes sind also gesperrt, solange sie zu keiner internen Verbindung gehören. Die Nutzung der Ports, die zu einer solchen Verbindung gehören, wird bei der Implementierung von NAPT jedoch nicht auf die ursprünglichen Kommunikationspartner beschränkt. Erst durch eine Firewall mit *Stateful Packet Inspection* können selbst die dynamisch geöffneten Ports nur von dem jeweiligen Kommunikationspartner angesprochen werden.

Die reine Adressumsetzung durch NAPT lässt sich lediglich als beschränkte Sicherheitstechnik ansehen, die den kontaktierten Internetservern in der Regel mehr Zugriffsmöglichkeiten auf den internen Computern bietet, als dies bei einer konventionellen Firewall üblich ist. Das Schutzniveau einer konventionellen Firewall wird durch bloßes NAPT also nicht erreicht.^[3]

Heute kommen jedoch meist Geräte zum Einsatz, die neben NAPT wenigstens auch *Paketfilter* installiert haben, was die Sicherheitsfunktion dieser Geräte erhöht. Als Beispiel bildet Netfilter das Herzstück zahlreicher moderner DSL-Router. Hierbei handelt es sich um eine Software, die innerhalb eines Linux-Kernels läuft und für die Port- und Adressumsetzung sorgt. Sie kann Pakete auswerten und filtern (einschließlich Stateful Packet Inspection) und Ports weiterleiten (Port-Forwarding). Deren Konfiguration wird meist über Iptables und einer vom Hersteller bereitgestellten Benutzeroberfläche realisiert.

Grundlegende sicherheitstechnische Grenzen

Da DSL-Router dafür gedacht sind, die Netze miteinander zu verbinden und nicht zu trennen, versuchen die Hersteller von Geräten für den privaten Haushalt Verbindungsprobleme möglichst automatisiert zu umgehen, auch wenn dies bedeutet, die Sicherheitsfunktion aufzuweichen oder gar zu brechen. Denn eine Verbindungsblockade führt mitunter zu Problemen mit einigen Anwendungen, die beispielsweise eigene Dienste anbieten. Der externe Zugriff darauf sollte normalerweise durch den DSL-Router blockiert werden, sobald sich der Port des Dienstes von dem Rückgabeport der angeforderten Verbindung unterscheidet. Das hätte aber zur Folge, dass dieser Teil der Anwendung nicht ohne spezielle Konfigurationseinstellungen des DSL-Routers funktioniert, weshalb die Hersteller die NAT-Implementierung entsprechend anpassen.

Funktioniert die Internetverbindung des eigenen privaten Computers auf Anhieb ohne Einschränkung, kommt das Gerät bei den Kunden besonders gut an. Sicherheit spielt hier – wenn überhaupt – nur eine nebensächliche Rolle. Bei professionellen Geräten ist die Anforderung meist genau andersherum. DSL-Router, die für den privaten Bereich bestimmt sind, machen daher sicherheitstechnisch oft eine schlechte Figur. Daher ist es umstritten, diese Geräte als Firewall zu betiteln.^[4] Demgegenüber schreibt beispielsweise Elisabeth D. Zwicky in ihrem Buch „Einrichten von Internet Firewalls“: „Die Welt ist voll von Leuten, die darauf bedacht sind, Ihnen weiszumachen, daß etwas keine Firewall ist. [...] Wenn es dazu gedacht ist, die bösen Jungs von Ihrem Netzwerk fernzuhalten, dann ist es eine Firewall. Wenn es erfolgreich die bösen Jungs fernhält, ist es eine gute, wenn nicht, ist es eine schlechte Firewall. Das ist alles, was es dazu zu sagen gibt.“^[5]

Als Beispiel dafür, dass DSL-Router Sicherheitsfunktionen aufweichen, kann es abhängig vom erworbenen Produkt vorkommen, dass der heimische DSL-Router den ersten von ihm per DHCP verwalteten Computer per Standardeinstellung als exposed Host behandelt, was in der Benutzeroberfläche des DSL-Routes auch gerne als „Standardserver“ betitelt wird. Der Schutz vor ungebetenen Internetzugriffen wird somit für diesen Computer praktisch ausgeschaltet, da hierdurch alle Netzwerkdienste des privaten Computers aus dem Internet heraus sichtbar und

zugreifbar sind. Wenigstens in den Haushalten, die lediglich einen einzigen Computer an den DSL-Router anschließen, umgeht der Hersteller damit zahlreiche mögliche funktionelle Probleme. Dass dies sicherheitstechnisch bedenklich ist, spielt bei diesen Geräten keine Rolle. Schließlich tun sie dies unter dem Aspekt, dass sonst einige Anwendungen nicht ohne manuellen Konfigurationsaufwand fehlerfrei laufen würden.

Um auch mit weniger drastischen Mitteln eine reibungslose Arbeit ohne manuellen Konfigurationsaufwand zu gewähren, kann der DSL-Router je nach Implementierung des Verbindungskonzepts möglichst offen auf Kommunikationsanforderungen des kontaktierten Internetserver reagieren. Baut ein interner Computer also eine Netzwerkverbindung zu einem Internetserver auf, so ist es mitunter möglich, dass dieser Internetserver nun willkürlich eigene Verbindungen zu dem internen Computer aufbauen kann. Dazu wird eine Netzwerkanfrage an einem beliebigen externen Port des DSL-Routers an den internen Computer durchgereicht, sobald die Absenderadresse zu dem Internetserver passt, zu dem der interne Computer zuvor eine Verbindung aufgebaut hat. Eine eingeschränkt offene Reaktion ist möglich, indem der DSL-Router erst dann auf diese Weise reagiert, wenn zuvor die Netzwerkanfrage des Clients auf ein für die Verbindung sonst problematisches Protokoll hinweist (beispielsweise bei aktivem FTP). Haben mehrere interne Computer eine Verbindung zu diesem Server aufgebaut, so versucht der DSL-Router dann mittels einer Heuristik den passenden Empfänger zu erraten.^[6] Abhängig vom Produkt reagieren DSL-Router unterschiedlich restriktiv auf solche Anfragen, weshalb es für den kontaktierten Internetserver auch etwas aufwendiger sein kann, auf einen beliebigen Port des Kommunikationspartners zuzugreifen.^[7]

Gegen eine automatisierte Freischaltung einer Kommunikation gibt es an und für sich nichts auszusetzen, sobald der DSL-Router die Protokolle der Dienste sicher beherrscht und einen kontrollierten Zugriff darauf erlaubt. Genau darin besteht aber das Problem. Ihnen fehlt in der Regel die intime Kenntnis der verwendeten Protokolle.^[6] Dies gilt insbesondere bei verschlüsselten Verbindungen und verbindungslosen Protokollen, beispielsweise auch bei aktivem FTP und SIP. Da bereits die preiswerte Hardware dieser Geräte eine parallele Analyse der Protokolle ausschließt, wenigstens aber auf ein Minimum beschränkt, versuchen einige Geräte einfach *alle* externen Anforderungen nach Möglichkeit zuzulassen, in der Hoffnung, dass damit die entsprechende Anwendung fehlerfrei funktioniert. Verfügt der DSL-Router über keine Paketfilterfunktion, lassen sich dabei nicht einmal bestimmte Ports ausschließen.

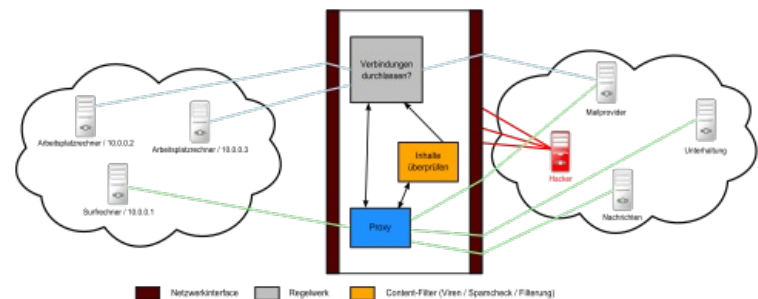
Wie wenig die Sicherheit bei DSL-Firewall- Routern eine Rolle spielt, zeigt bei einigen Geräten die Bezeichnung „DMZ“ für eine Funktionalität, die nichts mit einer echten DMZ gemein hat. Das erhöhte Sicherheitsrisiko des Kunden wird billigend in Kauf genommen.

Zu generellen sicherheitstechnischen Mängeln von NAT-basierten Geräten siehe RFC 2663 („IP Network Address Translator (NAT) Terminology and Considerations“, Abschnitt 9 und in diesem Kontext Abschnitt 7; englisch).

Beispiel einer einfachen Firewallumgebung

Ein einfacher Firewall-Aufbau soll die Materie verdeutlichen: Eine Firma möchte ihre Arbeitsplatzrechner mit dem Internet verbinden. Um zu verhindern, dass beispielsweise Schadsoftware aus dem Internet heruntergeladen wird, kann eine Firewall sicherstellen, dass die Arbeitsplatz-PCs nur auf erlaubte Webseiten zugreifen dürfen (White-List).

Um das Beispiel einfach zu halten, dürfen die Arbeitsplatz-PCs 10.0.0.2 und 10.0.0.3 nur Verbindungen zu dem Mail-Server der Firma aufbauen. Damit eine Recherche im Internet möglich ist, kann es auch einen dedizierten Surf-Computer geben, der über einen Proxy-Zugriff zu Webseiten erhält. Der Surf-Rechner wird zusätzlich dadurch geschützt, dass ActiveX aus den angeforderten HTML-Seiten aus Sicherheitsgründen herausgefiltert wird (für ein sicheres Surfen müssten noch andere Objekte herausgefiltert werden, ebenso gibt es Sandboxen – auch Kiosk-Modes – für den PC, aber das Beispiel soll ja einfach bleiben).



Beispiel einer Firewall zwischen lokalem Netz und Internet

Sonstige Zugriffe von außen auf das Firmennetz werden blockiert. Wichtig ist, dass in dieser Konstellation die Arbeitsplatzrechner selbst keinerlei direkte Verbindung zum Internet aufbauen können, die nicht erlaubt ist. Damit können über andere Wege eingeschleuste Schadprogramme keine Informationen über das Internet übertragen und sich nur weiterverbreiten oder weitere Schädlinge aus dem Internet nachladen, wenn sie über den Proxy oder den Mailserver einen Weg finden.

Das Firewall-Regelwerk eines Systems mit Stateful Inspection würde in diesem Beispiel folgendermaßen aussehen:

1. Die Quellen 10.0.0.2 und 10.0.0.3 (Arbeitsplatzrechner) dürfen zum Ziel „Mailprovider“ per IMAP (Mails abholen) und SMTP (Mails senden) zugreifen
2. Quelle 10.0.0.1 (Surfrechner) darf über den Proxy auf beliebige Ziele mit den Diensten HTTP (Webseiten herunterladen) und HTTPS zugreifen (ActiveX wird dabei gefiltert)
3. Alle anderen Kommunikationsversuche werden verworfen

Weitere Beispiele finden sich im Artikel Demilitarized Zone

Weitere Funktionen und Aspekte

Anti-Spoofing (Ingress filtering)

Eine wichtige Funktion von Firewalls ist das Verhindern von IP-Spoofing. Da die Filterung sich wesentlich an den IP-Adressen orientiert, muss so gut wie möglich sichergestellt werden, dass diese nicht gefälscht sind. Firewalls mit Anti-Spoofing-Funktionalität bieten daher die Möglichkeit, bestimmten Netzwerk-Schnittstellen bestimmte IP-Adressen und Netze zuordnen zu können. Der Internet-Schnittstelle werden dann automatisch alle IP-Adressen außer den anderweitig genutzten zugeordnet. IP-Pakete, die an einer falschen Schnittstelle ankommen, werden protokolliert und verworfen. Firewalls mit Internetanbindung können auf der Internet-Schnittstelle alle Pakete von und an Private IP-Adressen (RFC 1918) verwerfen, da diese im Internet sowieso nicht geroutet werden. Dadurch ist ein IP-Spoofing mit diesen Adressen aus dem Internet ausgeschlossen. Obwohl die Zuordnung von IP-Netzen zu bestimmten Netzwerk-Schnittstellen eigentlich eindeutig sein sollte, treten in der Praxis manchmal Probleme auf mit Dual homed host und Routing-Loops (Pakete die auf Hin- und Rückweg unterschiedliche Routen nehmen).

Authentifizierung

Da der Filterung anhand von IP-Adressen wegen potenziellem IP-Spoofing nicht vollständig vertraut werden kann, bieten manche Firewalls die Möglichkeit sich authentifizieren zu lassen und erst dann bestimmte Regeln zeitbeschränkt freigeschaltet zu bekommen. Für eine starke Authentifizierung bieten zum Beispiel die Check Point Firewall-1 und die Juniper Networks Firewalls die Kompatibilität zu den SecurID-Token der Firma RSA Security.

Intrusion Detection und Intrusion Prevention Systeme

→ Hauptartikel: Intrusion Detection System und Intrusion Prevention System

„Intrusion Detection Systeme“ (IDS) und „Intrusion Prevention Systeme“ (IPS) werden mitunter auf einem Firewallgerät installiert, gehören jedoch nicht zum Firewallmodul. Während das Firewallmodul keine Angriffe erkennt, sondern lediglich dafür gedacht ist, bestimmte Kommunikationsbeziehungen – basierend auf Absender- oder Zieladresse und genutzten Diensten – zu erlauben, ergänzen diese zusätzlichen Module das System um die Eigenschaft, nun auch einen Einbruchversuch anhand von Kommunikationsmustern zu erkennen. Im Unterschied zum IPS kann ein IDS den Einbruch nur erkennen (Detection (engl.) = Erkennung), während ein IPS (Prevention (engl.) = Verhinderung) den unerwünschten Zugriff auch zu blockieren versucht.

Ein solches System kann mitunter auch 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, so kann er damit erreichen, dass der Zugriff auf die gefälschte Adresse nicht mehr möglich ist. So kann er nacheinander sämtliche Adressen von dem angegriffenen System abschotten, die dieses für seine Arbeit benötigt (DNS-Server usw.).

Hochverfügbarkeit

Durch die Bedeutung des Internets sind Firewalls in vielen Firmen mittlerweile zu kritischen Netzwerkkomponenten geworden und stellen teilweise sogar einen Single Point of Failure für wichtige Geschäftsprozesse dar. Daher wird durch Hochverfügbarkeits-Techniken wie Failover- oder Cluster-Betrieb versucht, das Risiko eines Ausfalls zu reduzieren.^[8]

Ein weiterer Vorteil dieser Techniken ist, dass einzelne Firewalls zu Wartungszwecken oder für Softwareaktualisierungen abgeschaltet werden können, ohne die Verbindung zu unterbrechen.

Zur Umsetzung werden oft die gleichen Lösungen wie bei hochverfügbaren Routern eingesetzt (beispielsweise HSRP, VRRP oder CARP) oder spezielle Produkte wie Rainwall von EMC2.

Für den Failover-Fall gibt es zwei Möglichkeiten, wie die übernehmende Stateful Inspection-Firewall mit den bestehenden Verbindungen umgeht. Eine Methode ist, dass alle Firewalls permanent ihre dynamische Verbindungstabellen untereinander synchronisieren, damit ist jede Firewall in der Lage alle Verbindungen korrekt zuzuordnen. Das andere Verfahren arbeitet ohne Abgleich, aber alle bestehenden Verbindungen werden nach dem Wechsel von der übernehmenden Firewall nochmals gegen das Regelwerk geprüft. Diese Lösung ist einfacher, bereitet aber Probleme bei komplexen Protokollen wie aktivem FTP. Da die hierbei ausgehandelten Ports für die Daten-Verbindungen zufällig sind, kann die übernehmende Firewall diese Pakete keiner Regel zuordnen und wird sie verwerfen.

Eine Synchronisation der Verbindungstabellen bieten unter anderem die Firewalls von Check Point, OpenBSD (über pf_sync) und Linux (über ct_sync).

Hochsicherheitsumgebungen

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.^[9]

Die Firewall ist ein Teilaspekt des Sicherheitskonzepts.^[10] 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.

Verschiedene Installationen haben verschiedene Sicherheitsanforderungen. Beispielsweise bei Banken, Börse, Militär usw. gibt es ein hohes Sicherheitsbedürfnis. Stellt beispielsweise die Durchtunnelung ein Risiko dar, welches minimiert werden soll, kann dies eventuell durch die Regelung des Verkehrs explizit durch Whitelists umgesetzt werden. In einer Hochsicherheitsumgebung bietet es sich an, jeglichen Verkehr, der nicht unbedingt benötigt wird, zu unterbinden.

Eine absolute Sicherheit kann es jedoch nicht geben; auch eine gut konfigurierte Firewall stellt keinen Sicherheitsmechanismus dar, der nicht über kurz oder lang überwunden werden kann. Bestenfalls lässt sich die Barriere zu einer großen Herausforderung für einen Eindringling gestalten, die so groß ist, dass sich der Angriff nicht lohnt.

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. Quelloffene Software lässt sich von der Öffentlichkeit dahingehend überprüfen und darüber hinaus mit rechtlich unbedenklichen Mitteln auf Schwachstellen untersuchen (Audit), die auf diese Weise schneller geschlossen werden können. Zudem kann der Nutzer eine eigene Übersetzung des Quellcodes durchführen und so sicherstellen, dass tatsächlich auch nur dieser Quellcode auf seinem Gerät Anwendung findet.

Um die Ausnutzung von Sicherheitslücken innerhalb der Firewall zu minimieren, können im Extremfall auch mehrstufige Lösungen helfen. So kann das Netzwerkpaket beispielsweise mehrere hintereinander geschaltete Firewallsysteme unterschiedlicher Hersteller passieren, damit systembedingte Fehler oder eventuell von Hersteller eingebaute Hintertüren je nach Abstimmung der Systeme einen Großteil ihrer Wirksamkeit verlieren.

Virtual Local Area Networks

Moderne Firewalls unterstützen Virtual Local Area Networks (VLANs), d. h. über eine physische Netzwerkschnittstelle lassen sich mehrere logische Netze erreichen. Dadurch lassen sich mehr Netze an die Firewall anschließen, als das physikalische Limit an Netzwerk-Interfaces erlaubt.

Die Benutzung von VLANs ist unter Umständen billiger, als weitere Netzwerkschnittstellen für die Firewall zu kaufen. Ein weiterer Vorteil ist, dass zur Verbindung neuer Netze allein eine Software-Konfiguration von Firewall und den weiteren Netzwerkkomponenten ausreicht; es müssen keine neuen Kabel gezogen werden.

Nachteilig ist, dass alle VLANs die Kapazität der LAN-Verbindung teilen. Sicherheitstechnisch bedenklich ist, dass die Trennung der verschiedenen Netze nicht der Hoheit der Firewall unterliegt; das System ist somit leichter kompromittierbar. In einem solchen Fall ist die Firewall auf die Zusammenarbeit mit den eingesetzten Netzwerkkomponenten angewiesen. Diese Komponenten sind nicht zwangsläufig gehärtete Systeme und bieten mitunter zusätzliche Angriffsflächen (WWW, SNMP, Telnet usw.), sind für Sicherheitslösungen also nicht oder nur bedingt geeignet.

Sicherheitsprobleme können aus verschiedenen Gründen auftauchen: durch eine fehlerhaft arbeitende Netzwerkkomponente, durch eine falsche Konfiguration der Komponente (z. B. SNMP), eine fehlerhafte Implementierung oder Konfiguration der VLAN-Trennung oder auch durch einen Einbruch in die Administration des Netzwerkgerätes. Möglicherweise wird auch ein Konfigurations-Reset einer Komponente nicht sofort auffallen, denn beispielsweise viele Switches transportieren VLAN-Pakete (solche mit VLAN-TAGs) auch ohne eine entsprechende VLAN-Konfiguration. Weiter können beispielsweise durch Einschleifen eines Hubs LAN-Segmente des VLANs gleichzeitig und unbemerkt abgehört werden.

Auf der WAN-Seite können VLANs wertvolle Dienste leisten. Im Bereich der DMZ sind die Nachteile je nach Umgebung mitunter noch akzeptabel; in einer sicherheitsrelevanten Umgebung werden die Nachteile jedoch überwiegen.

Routing und Multicast

Die meisten Firewalls sind als Router aufgebaut. Das ist gerade im SoHo-Bereich praktisch, denn zum Anschluss mehrerer Rechner wird dort üblicherweise ein Router mit kombinierter NAT- und PPPoE-Funktionalität benötigt. Bei Firmennetzwerken wird oft auch die Routingfunktionalität gewünscht, denn hier ersetzt die Routing-Firewall das früher übliche „default Gateway“.

Genauso wie das Routing hängt die IP-Multicasting-Fähigkeit einer Firewall vom Betriebssystem des Gerätes ab, auf dem die Firewallsoftware läuft. Die Regeln werden mit den Multicast-Adressen (224.0.0.0-239.255.255.255) eingetragen. Weitere Aspekte sind in RFC 2588 beschrieben.

Administration

Leistungsmessung und Optimierung

Da die Geschwindigkeit von vielen dynamischen Faktoren abhängt, ist es nicht trivial die Leistung einer Firewall zu bewerten. Dazu gehören die Größe des Regelwerks und Reihenfolge der Regeln, Art des Netzwerk-Verkehrs und Konfiguration der Firewall (z. B. Stateful, Logging). Ein einheitliches Benchmarking von Firewalls ist in RFC 2647 beschrieben.

Zur Optimierung sind folgende Maßnahmen möglich:

- Mehr Hauptspeicher und/oder eine schnellere CPU.
- Ausschalten von Logging für einzelne Regeln.

- Unbenutzte Regeln und Routing-Einträge entfernen.
- Häufig benutzte Regeln im Regelwerk nach oben stellen. Dabei ist zu beachten, dass sich dadurch die Bedeutung des Regelwerks ändern könnte.
- Bei hochverfügbaren Systemen die Synchronisation der Verbindungstabelle für einzelne Regeln ausschalten. Insbesondere bei kurzlebigen HTTP-Verbindungen ist dies gut möglich.
- Produktspezifische Leistungsmerkmale nutzen, wie z. B. Nokia IPSO Flows oder Check Point SecureXL.
- Überprüfung, dass alle Netzwerk-Interfaces mit Full-Duplex arbeiten.
- Anpassung von Netzwerk-Parametern des Betriebssystems^[11]

Fehlersuche

Die Fehlersuche in einem großen Netzwerk kann sehr komplex werden.

Häufige Fehler sind z. B., dass eine Firewall-Regel IP-Adressen enthält, die durch eine NAT-Verbindung oder ein VPN geändert wurden. Je nach eingesetzter Firewall-Software und Betriebssystem unterscheiden sich die Möglichkeiten zur Fehlersuche.

Anhand der Logdateien können falsche Firewall-Regeln oder IP-Spoofing erkannt werden. Mit Werkzeugen wie beispielsweise tcpdump oder snoop unter Solaris lässt sich der aktuelle Netzwerkverkehr an ein- und ausgehender Netzwerkschnittstelle beobachten und vergleichen. Des Weiteren bieten manche Systeme einen Einblick in die interne Verarbeitung der Firewall-Software (z. B. bei Check Point FW1 mit „fw monitor“).

Bei einem Firewallsystem im Cluster-Betrieb sind Logdateien nützlich, um festzustellen, welche Maschine die fehlerhafte Verbindung überhaupt bearbeitet. Die Logdateien sind für eine detaillierte Fehlersuche ungeeignet, wenn sie nicht für jedes einzelne Paket einen Eintrag schreiben, sondern nur pro Verbindung.

Neben den Möglichkeiten der Firewall sind Werkzeuge wie ping, nmap oder traceroute hilfreich, um festzustellen, ob der Fehler außerhalb des Systems liegt, z. B. im Routing oder dass der Ziel-Port gar nicht geöffnet ist.

Problematische Protokolle

Voice over IP und Videokonferenzen

Voice over IP (VoIP) und Videokonferenzen sind für Stateful Firewalls nicht trivial, da meist mehrere verschiedene Protokolle (z. B. für Anrufsignalisierung, Tonübertragung, Bildübertragung, Application-Sharing) und Teilnehmer (Anrufer, Angerufener, Telefonanlagen, Konferenzschaltung) involviert sind. Manche kommerzielle Firewalls verstehen die VoIP-Protokolle (SIP oder Skinny) und sind daher in der Lage, Ports dynamisch zu öffnen.

Siehe auch Session Initiation Protocol (SIP)

File Transfer Protocol (FTP)

FTP ist zwar ein ziemlich altes, aber für Firewalls schwieriges Protokoll. Insbesondere der aktive FTP-Modus, bei dem zusätzlich zur Steuerverbindung auf Port 21 eine weitere Datenverbindung quasi rückwärts vom Server zum Client aufgebaut wird, bereitet manchen Firewalls Probleme.

Die rückwärts aufgebaute Verbindung lässt sich vom Betreiber des FTP-Servers theoretisch auch für Angriffe missbrauchen.^[12] Daher verbieten manche Firewallsysteme den Aufbau der Datenverbindung auf Portnummern, die für andere Dienste bekannt sind. Dies hat den Vorteil, dass die Anfälligkeit gegenüber einem Missbrauch der Datenverbindung für Angriffe reduziert wird.

Typische Symptome einer Firewall, die Probleme mit FTP hat, ist eine funktionierende Navigation durch die Verzeichnisse, aber Verbindungsabbrüche ohne Fehlermeldung bei der Datenübertragung. Die oben genannten Probleme treten nicht auf bei passivem FTP (Konfigurierbar im FTP-Client oder durch Eingabe von „PASV“ in Kommandozeilen-Clients) oder bei Verwendung des verschlüsselten auf dem SSH-Protokoll basierenden SCP.

Entstehung der Firewall

Die ersten Packet Filter wurden im Jahr 1985 von Cisco in ihre Router eingebaut.^[13] Die erste Studie über das Filtern von Netzwerkverkehr wurde im Jahr 1988 von Jeff Mogul veröffentlicht.^[14]

In der Anfangszeit des Internets waren Administratoren meist nicht sensibilisiert gegenüber möglichen Angriffen innerhalb des Netzes. Das änderte sich erst im Jahr 1988, als von Robert Morris der erste Computerwurm programmiert und freigesetzt wurde. Er legte ca. 6000 Rechner lahm – das entsprach zu dieser Zeit ungefähr 10 % des weltweiten Netzes.^[15] Danach wurde der Einsatz von Firewalls populär.

Produkte

Firewall-Software

- „Astaro Security Linux“ ist eine kommerzielle Linux-Distribution für Firewall-Systeme.
- Check Point Firewall 1 ist eine kommerzielle Firewall-Applikation, die auf Unix- Windows- und Nokia-Appliances läuft
- Endian Firewall ist eine Open-Source-Linux-Distribution für Gateway/Router/Firewall-Systeme, die umfassenden Gateway-Schutz bietet (Antivirus, Antispam, DMZ, Intrusion Detection etc.) und als Headless Server sehr einfach über ein Webfrontend zu konfigurieren ist.
- Der Eindisketten-Router fli4l ist neben der CD-Variante Gibraltar ein Projekt, das im Sinne einer nachhaltigen Nutzung die Verwendung von alten PCs als Firewall gestattet.
- IPFire ist eine freie Linux-Distribution die in erster Linie als Router und Firewall fungiert, diese sich durch einen Paketmanager leicht um vielen Zusatzfunktionen erweitern lässt.
- IPCop ist eine einfach zu bedienende Linux-Distribution, ein ausgewogener Kompromiss zwischen sicherer Firewall und reichem Funktionsumfang (Antivirus, Antispam, DMZ, Proxy).
- ipfw ist ein Paketfilter des FreeBSD-Betriebssystems, als wipfw auch für Windows-Systeme verfügbar.
- Netfilter / IPTables – Paketfilter innerhalb des Linux-Kernels.
- M0n0wall ist eine BSD-basierte Firewall, auf Sicherheit optimiert, eine Lösung, die mit ihren Funktionen an Profi-Firewalls herankommt und trotzdem sehr einfach zu konfigurieren ist.
- OPNsense eine freie Firewall auf Basis von FreeBSD und der Address Space Layout Randomization (ASLR) von HardenedBSD, erlaubt die Benutzung der freien Kryptobibliothek LibreSSL, alternativ zum Standard OpenSSL (wählbar in der GUI).^{[16][17]}
- pfSense ist eine einfach zu bedienende BSD-basierte Firewall, Ableger von M0n0wall, ein Kompromiss zwischen sicherer Firewall und reichem Funktionsumfang (Antivirus, Antispam, DMZ, Proxy).
- phion netfence – europäisches Enterprise Firewall Produkt, welches als Software- und Hardware Appliance verfügbar ist.
- Microsoft Internet Security and Acceleration Server ist eine kommerzielle Firewall von Microsoft, basiert auf Windows Server 2000/2003. Vorteilhaft ist die Integration in die Active Directory-Verzeichnisstruktur.
- pf ist eine Open-Source-Firewall, die ursprünglich für OpenBSD entwickelt und später auf andere BSD-Betriebssysteme portiert wurde.
- „Securepoint Linux“ ist eine kommerzielle UTM-Linux-Distribution.
- Shorewall
- SME Server ist eine auf Open-Source-Software basierende Firewall, die auch Serverfunktionen zum Einsatz im SoHo-Bereich enthält.

Firewall-Geräte

Firewall-Geräte bieten eine aufeinander abgestimmte Kombination aus Hardware, gehärtetem Betriebssystem und Firewall-Software:

- Check Point VPN-1 Edge und UTM-1
- Cisco ASA (Vorgänger: PIX) und Firewall Service Module (FWSM) für Catalyst Switches
- Juniper Networks Netscreen und SSG
- Innominate Security Technologies (ein Phoenix Contact Unternehmen) mGuard industrial appliances
- Palo Alto Networks Next-Generation Firewall
- phion
- Watchguard Firebox X Core und Peak Appliances

Siehe auch

- Air Gap

Quellen


1. BSI Grundschriftkataloge: Geeignete Auswahl eines Paketfilters (<https://web.archive.org/web/20120211183622/https://www.bsi.bund.de/ContentBSI/grundschrift/kataloge/m/m02/m02074.html>) (Memento des Originals (<https://giftbot.toolforge.org/deref.fcgi?url=https%3A%2F%2Fwww.bsi.bund.de%2FContentBSI%2Fgrundschrift%2Fkataloge%2Fm%2Fm02%2Fm02074.html>) vom 11. Februar 2012 im *Internet Archive*) ⓘ **Info:** Der Archivlink wurde automatisch eingesetzt und noch nicht geprüft. Bitte prüfe Original- und Archivlink gemäß Anleitung und entferne dann diesen Hinweis.
2. BSI Grundschriftkatalog: Geeignete Auswahl eines Application-Level-Gateways (https://www.bsi.bund.de/cln_165/ContentBSI/grundschrift/kataloge/m/m02/m02075.html) (Seite nicht mehr abrufbar, Suche in Webarchiven (http://timetravel.mementoweb.org/list/2010/https://www.bsi.bund.de/cln_165/ContentBSI/grundschrift/kataloge/m/m02/m02075.html)) ⓘ **Info:** Der Link wurde automatisch als defekt markiert. Bitte prüfe den Link gemäß Anleitung und entferne dann diesen Hinweis.
3. RFC 2663: IP Network Address Translator (NAT) Terminology and Considerations, Section 9.0
4. Worauf Sie beim Router-Kauf achten sollten (https://web.archive.org/web/20101230082856/https://www.sicher-im-netz.de/privatnutzer/1297_1304.aspx) (Memento des Originals (https://giftbot.toolforge.org/deref.fcgi?url=https%3A%2F%2Fwww.sicher-im-netz.de%2Fprivatnutzer%2F1297_1304.aspx) vom 30. Dezember 2010 im *Internet Archive*) ⓘ **Info:** Der Archivlink wurde automatisch eingesetzt und noch nicht geprüft. Bitte prüfe Original- und Archivlink gemäß Anleitung und entferne dann diesen Hinweis., sicher-im-netz.de, sicher im Netz e. V., Berlin
5. Elisabeth D. Zwicky, ISBN 3-89721-169-6, 2001, S. 34
6. Firewall FAQ (<http://www.iks-jena.de/mitarb/lutz/usenet/Firewall.html#NAT>) von *Lutz Donnerhacke*

7. PAT-Angriff auf Computer hinter einem Firewallrouter (http://wiki.hackerboard.de/index.php/PAT-Angriff_auf_Computer_hinter_einer_externen_Firewall)
8. BSI Grundsatzkataloge: Sicherheit Gateways und Hochverfügbarkeit (<https://web.archive.org/web/20120211192926/https://www.bsi.bund.de/ContentBSI/grundsatz/kataloge/m/m02/m02302.html>) (Memento des Originals (<https://giftbot.toolforge.org/deref.fcgi?url=https%3A%2F%2Fwww.bsi.bund.de%2FContentBSI%2Fgrundsatz%2Fkataloge%2Fm%2Fm02%2Fm02302.html>) vom 11. Februar 2012 im *Internet Archive*) ⓘ **Info:** Der Archivlink wurde automatisch eingesetzt und noch nicht geprüft. Bitte prüfe Original- und Archivlink gemäß Anleitung und entferne dann diesen Hinweis.
9. BSI Grundsatzkataloge: Entwicklung eines Konzepts für Sicherheit Gateways (https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt_content/m/m02/m02070.html)
10. Michael Wächter, „Fälschung und Fortschritt im Datenschutz“, ISBN 3-428-09780-7, 1998, S. 92
1. Tuning Check Point Performance (https://web.archive.org/web/20081201190236/http://www.checkpoint.com/techsupport/documentation/FW-1_VPN-1_performance.html) (Memento des Originals (https://giftbot.toolforge.org/deref.fcgi?url=http%3A%2F%2Fwww.checkpoint.com%2Ftechsupport%2Fdocumentation%2FFW-1_VPN-1_performance.html) vom 1. Dezember 2008 im *Internet Archive*) ⓘ **Info:** Der Archivlink wurde automatisch eingesetzt und noch nicht geprüft. Bitte prüfe Original- und Archivlink gemäß Anleitung und entferne dann diesen Hinweis.
2. FTP-NAT-Test (<https://web.archive.org/web/20060429225220/http://bedatec.dyndns.org/ftpnat/>) (Memento des Originals (<https://giftbot.toolforge.org/deref.fcgi?url=http%3A%2F%2Fbedatec.dyndns.org%2Fftpnat%2F>) vom 29. April 2006 im *Internet Archive*) ⓘ **Info:** Der Archivlink wurde automatisch eingesetzt und noch nicht geprüft. Bitte prüfe Original- und Archivlink gemäß Anleitung und entferne dann diesen Hinweis.
3. Evolution of the Firewall Industry (<https://web.archive.org/web/20070311041019/http://www.cisco.com/univercd/cc/td/doc/product/iaabu/centri4/user/scf4ch3.htm>) (Memento des Originals (<https://giftbot.toolforge.org/deref.fcgi?url=http%3A%2F%2Fwww.cisco.com%2Funivercd%2Fcc%2Ftd%2Fdoc%2Fproduct%2Fiaabu%2Fcentri4%2Fuser%2Fscf4ch3.htm>) vom 11. März 2007 im *Internet Archive*) ⓘ **Info:** Der Archivlink wurde automatisch eingesetzt und noch nicht geprüft. Bitte prüfe Original- und Archivlink gemäß Anleitung und entferne dann diesen Hinweis. Cisco, 2002
4. The Packet Filter: An Efficient Mechanism for User-level Network Code (<http://citeseer.ist.psu.edu/mogul87packet.html>) Jeffrey C. Mogul, November, 1987
5. RFC 1135 The Helminthiasis of the Internet
6. OPNsense GUI, Select LibreSSL [1] (<https://docs.opnsense.org/manual/install.html#openssl-libressl>)
7. Moritz Förster: *Open-Source-Firewall: Neuer Major Release von OPNsense für mehr Sicherheit*. (<https://www.heise.de/newsticker/meldung/Open-Source-Firewall-Neuer-Major-Release-von-OPNsense-fuer-mehr-Sicherheit-3280812.html>) In: *Heise Open Source (online)*. KW30, Nr. 2016, 28. Juli 2016. Abgerufen am 4. August 2016.

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, Pöng 2004, ISBN 3-89990-128-2.
- Bundesamt für Sicherheit in der Informationstechnik: *Konzeption von Sicherheit Gateways. Der richtige Aufbau und die passenden Module für ein sicheres Netz*. Bundesanzeiger, Köln 2005, ISBN 3-89817-525-1.
- William R. Cheswick, Steven M. Bellovin, Aviel D. Rubin: *Firewalls and internet security. Repelling the Wily Hacker*. 2nd edition, 3rd printing. 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 Strobelt: *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

- Ein Vergleich zwischen Personal- und Hardwarefirewall sowie detaillierte Erklärungen zum Thema Firewall finden sich im Habo-WiKi (<http://wiki.hackerboard.de/index.php/Firewall>)
- Eine Checkliste des Landesbeauftragten für den Datenschutz Niedersachsen (http://www.lfdi.saarland.de/images/stories/pdf/Information/Checkliste_Firewall.pdf) (PDF; 149 kB) kann als allgemeine Orientierungsgrundlage für ein Sicherheitskonzept dienen
- [compute.ch](https://www.compute.ch/download.php?list.8) (<https://www.compute.ch/download.php?list.8>) listet freie deutschsprachige Publikationen zum Thema Firewalling auf
- Eine BSI Firewall Studie (<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*) aus dem Jahr 2001 zeigt den direkten Vergleich von sechs Hardwarefirewalls
- websec.security-check.ch (<http://websec.security-check.ch/>) eine Website für den Funktionstest von Firewalls
- Ein Fachartikel auf Security-Insider.de (<http://www.security-insider.de/firewall-strategie-v-36834-13274/>) gibt Entscheidungshilfen für den Einsatz von Firewalls
- Firewall-Lexikon (<http://www.firewallshop24.de/info/Firewall-Lexikon.html>) – Ein kleines Lexikon wo Begriffe wie z. B. Bridging, Application Level, NAT, Load Balancing und vieles mehr verständlich erklärt werden

Diese Seite wurde zuletzt am 11. Januar 2020 um 19:30 Uhr bearbeitet.

Der Text ist unter der Lizenz „Creative Commons Attribution/Share Alike“ verfügbar; Informationen zu den Urhebern und zum Lizenzstatus eingebundener Mediendateien (etwa Bilder oder Videos) können im Regelfall durch Anklicken dieser abgerufen werden. Möglicherweise unterliegen die Inhalte jeweils zusätzlichen Bedingungen. Durch die Nutzung dieser Website erklären Sie sich mit den Nutzungsbedingungen und der Datenschutzrichtlinie einverstanden.

Wikipedia® ist eine eingetragene Marke der Wikimedia Foundation Inc.