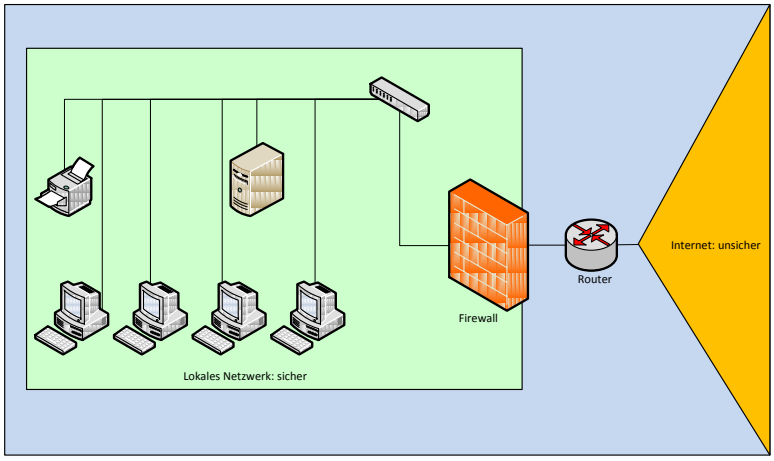
Firewalls

Brandschutzmauern (Firewalls) wurden und werden zwischen eng beieinander stehenden Gebäudeteilen eingezogen, um das Übergreifen von Feuer zu verhindern. Übertragen auf den in der Informationstechnik gebräuchlichen Begriff der Firewall, stimmt das Bild nicht ganz. Erstens handelt es sich bei den Bedrohungen, welche von Computersystemen abzuwehren sind, selten um außerordentliche und in ihrem Zeitablauf engbegrenzte Elementarereignisse. Statt dessen gilt es, vielfältige, meist in kurzen Intervallen immer wiederkehrende Angriffsversuche zu erkennen und abzuwehren. Zweitens wandeln sich Ziel und Vorgehensweise der Attacken beständig. Und drittens besteht die Hauptfunktion einer IT-Firewall eben gerade nicht darin, zwei Bereiche (hier: Netzwerke) vollständig voneinander abzuschotten. Statt dessen müssen sie zulässigen von unzulässigem Nachrichtenverkehr unterscheiden und nur letzteren blockieren, ersteren aber möglichst verzögerungsfrei hindurch leiten. So gesehen ist also "Firewall" eine Metapher für Kontrollstelle und Filtereinrichtung des netzwerkübergreifenden Datenverkehrs.

Der am häufigsten anzutreffende Einsatzort[1] einer Firewall ist die Verbindungsstelle zwischen einem lokalen Computernetzwerk (LAN[2]) und dem Internet. Die Firewall bildet faktisch den Grenzposten. Gerätetechnisch betrachtet handelt es sich hierbei um einen Computer mit sicherheitsspezifischen Funktionen und Ausstattungen, der mindestens zwei physische Netzwerkanschlüsse besitzt: einen zum LAN und einen zum Internet. Gleichzeitig stellt die Firewall die einzige Verbindung zwischen diesen beiden Netzen dar. Der gesamte Datenverkehr zwischen dem lokalen Netzwerk und dem Internet muss somit durch die Firewall geleitet werden. Existieren neben der Firewall noch weitere Kommunikationsverbindungen zwischen dem lokalen Netzwerk und dem Internet, beispielsweise über Drahtlosverbindungen (UMTS etc.) einzelner Notebooks, kann das Netzwerk nicht als abgesichert angesehen werden.



Aus diesem Szenario lassen sich bestimmte charakteristische Anforderungen an Funktion und Arbeitsweise einer Firewall ableiten:

- Weitgehend verzögerungsfreie Durchleitung zulässigen Datenverkehrs.
- Erkennung und Blockieren unzulässigen Datenverkehrs.

[1] Hier geht es ausschließlich um sogenannte Netzwerkfirewalls. Programme, die auf Arbeitsplatzrechnern installiert oder bereits ins Betriebssystem integriert sind, um verschiedenste lokale Schutzfunktionen wahrzunehmen, werden hier nicht betrachtet.

[2] LAN: Local Area Network. Ein IT-Netzwerk an einem bestimmten Standort, in einem Gebäude oder einer Gebäudeetage, das einem Unternehmen, einer Organisation oder auch einer Privatperson gehört.

- Protokollierung erkannter Angriffe oder blockierter Nachrichten.
- Anpassbarer Regelsatz als Grundlage für die Entscheidungsfindung zwischen Blockieren und Durchlassen.
- Zuverlässiges, vor Kompromittierung sicheres System der Firewall selbst, einschließlich vor Missbrauch geschützter Konfigurationsschnittstellen.
- Keine weiteren Kommunikationsverbindungen über Netzwerkgrenzen hinweg, außer der Firewall.

Nach ihrer Grundkonfiguration lassen sich drei Typen von Netzwerkfirewalls unterscheiden: Kombinierte Firewall-Router, Appliances und individuell konzipierte Firewallsysteme.

Kombinierte Firewall-Router kommen häufig im Privatkundensegment zum Einsatz. Hier sind die technische Funktion der Verbindung zwischen dem lokalen Netzwerk und dem Internet (die Routerfunktion) und die Funktion der Firewall in einem Gerät vereint. Es handelt sich dabei um kompakte, preiswerte und in großen Stückzahlen vertriebene Geräte. Häufig erhalten Kunden als Bestandteil des Vertrages über die Bereitstellung eines Internetzugangs vom jeweiligen Provider ein bereits vorkonfiguriertes Gerät. Im Idealfall wird damit bei der ersten Internetverbindung die Firewall aktiviert. Auf einem anderen Blatt hingegen steht, ob die Voreinstellungen (wenn vorhanden) hinreichend vor gezielten Angriffsversuchen schützen, ob die Konfiguration an zukünftige Szenarien anpassbar ist und ob die Anwender zur Anpassung überhaupt in der Lage sind. Weil diese Gerätetypen jeweils in großen Stückzahlen und oft über lange Zeiträume im Dauereinsatz sind, bieten sie natürlich ein beliebtes Ziel für Attacken. Häufig werden im Laufe der Zeit Sicherheitslücken bekannt, die nicht von allen Nutzern rechtzeitig behoben, von Angreifern aber schnell ausgenutzt werden können. Eklatante Beispiele sind fehlerhafte Updatefunktionen und kompromittierte Fernzugänge: Die Geräte stellen in regelmäßigen Abständen eine Verbindung zum Hersteller her, um Softwareaktualisierungen herunterzuladen. Wenn dabei die Verbindungsinformationen manipuliert sind, können sich die Geräte sozusagen selbstständig mit Schadsoftware infizieren, die in einem nächsten Schritt Eindringlingen Tür und Tor öffnet. Oder es existiert eine Funktion auf der Router-Firewall, womit eine Fernkonfiguration aus dem Internet heraus möglich ist. Ist diese Funktion nun werksseitig auf den Geräten aktiviert und gleichzeitig ein Standardkennwort vorhanden, welches bestimmt von einigen Nutzern nicht vor der Inbetriebnahme geändert wurde, ist die "Öffnung" der Firewall nur noch ein Kinderspiel.

Router-Firewall "Fritzbox®", copyright: AVM GmbH

Als **Appliance** wird die Verbindung einer bestimmten, auf einen konkreten Einsatzzweck hin entwickelten Hardware mit einer darauf abgestimmten "gehärteten" Softwarelösung, die auf dieser Hardware zur Anwendung kommt, bezeichnet. Diese Geräte sind meist für den Einsatz im professionellen Umfeld ausgelegt und

Firewall-Appliance (copyright: Gateprotect GmbH)

bieten neben der Firewall-Funktion oft noch weitere Anwendungsmöglichkeiten wie Virtual Private Networking (VPN), Demilitarisierte Zonen (DMZ) und Intrusion Prevention/Detection System (IPS/IDS). Über konsolen- oder webbasierte Schnittstellen können alle erforderlichen Konfigurationen vorgenommen werden.

Die dritte Gruppe der Firewallsysteme umfasst die anforderungsbezogen und **individuell konfigurierten Systeme**. Die Basis bildet meist eine PC-typische Hardware, wobei diejenigen Ausstattungs- und Leistungsmerkmale im Vordergrund stehen, welche für die geplante Netzwerkfunktion besondere Relevanz haben. Das betrifft insbesondere Anzahl und Leistungsfähigkeit der Netzwerkadapter. Rechenleistung und Massenspeicherkapazität sind ebenso wie Grafikfähigkeiten in der Regel von untergeordneter Bedeutung. Demgegenüber wird auf ausfallsichere, zum Teil redundante Komponenten (Netzteile, lüfterlose Bauart, …) besonderes Augenmerk gelegt. Als Betriebssystem kommt normalerweise ein angepasstes, das heißt auf die tatsächlich benötigten Funktionen reduziertes und mit den erforderlichen Sicherheitsmerkmalen versehenes Linux- oder UNIX-Derivat zum Einsatz. Diese Betriebssysteme bringen die für die eigentliche Firewall-Funktion erforderlichen Filterwerkzeuge bereits mit. Eine umfassende softwaretechnische Anpassung an die Anforderungen des technisch-organisatorischen Umfelds ist in jedem Fall erforderlich.

Logo der Linux-Firewall IPCop

Um eine individuell konzipierte Firewalllösung sach- und fachgerecht aufbauen zu können, sind umfangreiche Netzwerk-, Betriebssystem- und teilweise auch Programmierkenntnisse erforderlich. Sind diese Voraussetzungen gegeben und wird mit der erforderlichen Sorgfalt vorgegangen, können flexible, anforderungsgerechte und sichere Systeme konstruiert werden. Da häufig bereits vorhandene Hardware genutzt wird und die erforderliche Software frei von kommerziellen Lizenzen ist, fallen hier keine Kosten an. Allerdings muss berücksichtigt werden, dass der Arbeitsaufwand, um eine solche Lösung zu konzipieren, zu installieren, zu konfigurieren, zu testen und zu dokumentieren, beträchtlich sein kann.

Häufig wird gerade in kleinen Organisationen mit einer demensprechend überschaubaren IT-Infrastruktur das Firewallsystem als Plattform für weitere netzwerkbezogene Dienste genutzt. Insbesondere sind das Router, VPN-Gateways, Proxy-Server und DNS-Server. Obwohl durch solche kombinierten Kommunikationsserver natürlich Ressourcen für Bereitstellung, Installation und Betrieb weiterer Server eingespart werden, wird die Funktion der Firewall und damit die Netzwerksicherheit geschwächt. Einerseits ist jede zusätzliche Anwendung auf einem System grundsätzlich eine Quelle potenzieller Instabilität. Andererseits können alle zusätzlichen, für die Firewall nicht zwingend erforderlichen Komponenten unter Umständen kompromittiert werden und damit Sicherheitslücken bilden.

Die klassische Funktion einer Firewall besteht darin, den zwischen verschiedenen Netzwerken oder Netzwerkbereichen ausgetauschten Datenverkehr zu überwachen. Das bedeutet: Die überwachten Nachrichten stammen nicht von der Firewall und sind auch nicht an sie gerichtet. Sie werden nur hindurch geleitet. Die Firewall "entscheidet" lediglich, ob die Weiterleitung zulässig ist oder nicht. Die Firewall kann also im allgemeinen nicht feststellen, von welcher Anwendung die Nachricht stammt und an welche Anwendung sie gerichtet ist. Dazu müsste sie über Informationen darüber verfügen,

wie der sendende und der empfangende Computer, also Quell- und Zielsystem des Kommunikationsprozesses, konfiguriert sind. Die Firewall besitzt diese Informationen normalerweise nicht. Sie ist somit nicht in der Lage, anhand bestimmter, miteinander kommunizierender Programme darüber zu befinden, ob die Kommunikation zulässig ist oder nicht. In diesem Aspekt unterscheiden sich übrigens die Netzwerkfirewalls von den häufig als Desktop-Firewall bezeichneten Schutzprogrammen, die sich auf den Endgeräten befinden: diese "kennen" die lokal installierten Programme und können also Nachrichtenaustausch auch anwendungsbezogen blockieren oder zulassen.

Eine Netzwerkfirewall ist vom Grundsatz her nur in der Lage, anhand von Adressierungs- und Statusinformationen zu entscheiden. An dieser Stelle ist ein Basisverständnis dafür erforderlich, wie der Nachrichtenaustausch zwischen modernen Informationssystemen prinzipiell funktioniert. Fundamental dafür sind folgende zwei Sachverhalte: 1.: Nachrichten, die von einem Sender zu einem Empfänger übertragen werden sollen, wie beispielsweise eine eMail, werden nicht als Ganzes verschickt, sondern in kleinere Abschnitte zerlegt. Diese Abschnitte werden Pakete genannt. 2.: Jedes Paket besteht aus zwei Teilen: Dem jeweilige Teil der eigentlichen Nachricht und, vorangestellt, vollständige Adress- und Zustellinformationen. Der Nachrichteninhalt, also die "Nutzdaten" heißt Payload, die Adress- und Zustellinformationen bilden den Header. Auf Grund der vollständigen Adressierung jedes einzelnen Pakets, kann es unabhängig vom Weg der anderen Nachrichtenfragmente sein Ziel erreichen. Der Empfänger sorgt am Ende der Kommunikationsstrecke dafür, dass alle Teile der Nachricht wieder in der richtigen Reihenfolge zusammengesetzt werden und übergibt sie anschließend dem zuständigen Programm.

Eine Netzwerkfirewall wertet nur die Headerinformationen aus. Sie ist also grundsätzlich nicht dazu fähig, den eigentlichen Nachrichteninhalt zu bewerten. Das gilt natürlich insbesondere, wenn es sich um zusätzlich gesicherte, das heißt verschlüsselte oder auch komprimierte Nachrichtentypen handelt. Es bietet sich die folgende Analogie an: Wir stellen uns einen Straßen-Grenzübergang vor. Am Kontrollposten fährt ein Fahrzeug mit Diplomaten-Kennzeichen vor. Die Grenzbeamten sind in diesem Fall nur befugt, das Fahrzeugkennzeichen und die Pässe der Insassen zu überprüfen. Sie dürfen jedoch nicht in den Kofferraum des Wagens schauen und das Gepäck kontrollieren. Einen solchen "Diplomatenstatus" genießen auch die Nachrichtenpakete beim Passieren der Netzwerkfirewall.

Ich will kurz erwähnen, dass auch Firewallsysteme existieren, die sehr wohl den Inhalt der Nachrichten und nicht nur den Header unter die Lupe nehmen. Diese werden als Application-Level-Firewall oder Anwendungsfirewall bezeichnet und sind in der Lage, potenziell schädigende Inhalte ("Viren", "Würmer" und "Trojaner") zu erkennen und zu blockieren. Netzwerkfirewalls haben diese Funktion normalerweise nicht.

Ohne eine Firewall würde der gesamte, ordnungsgemäß adressierte Nachrichtenverkehr die Netzwerkgrenzen passieren. Das ist im allgemeinen nicht gewünscht. Für die Basiskonfiguration einer Firewall, auch als Default Policy bezeichnet, kommen zwei Strategien in Frage: Strategie 1: Den Nachrichtenverkehr generell durchlassen und nur bestimmte, als problematisch eingeschätzte Pakete herausfiltern. Strategie 2: Alles blockieren und nur bestimmte, ausdrücklich als zulässig deklarierte Kommunikationsflüsse erlauben. Der vordergründig einfachere Weg besteht sicherlich in der Anwendung von Strategie 1. Relative Sicherheit lässt sich hingegen nur durch die Strategie 2 erreichen.

Bei der Konzeption, Konfiguration und Dokumentation einer individuellen Firewalllösung ist wie folgt vorzugehen:

- Festlegung der Default Policy (Dringende Empfehlung: Alles Blockieren!)
- Analyse der über die Netzwerkgrenze hinaus tatsächlich benötigten Kommunikationsströme.
- Aufstellung eines detaillierten Regelsatzes für die als zulässig deklarierte Kommunikation.
- Festlegung der zu protokollierenden Ereignisse (Angriffsversuche, ungewöhnliche Intensitäten etc.).
- Programmierung bzw. Konfiguration der Firewall.
- Funktionstest und ggf. Anpassung der Konfiguration.
- Dokumentation!
- Inbetriebnahme.

Moderne Firewalls arbeiten nach dem Prinzip der **Statefull Inspection**. Das bedeutet, der Nachrichtenverkehr wird nicht mehr nur anhand der in jedem Paket enthaltenen Headerinformationen bewertet. Zusätzlich werden auch Statusinformationen in Bezug auf den gesamten Kommunikationsprozess einbezogen. So werden beispielsweise Pakete, die als Antwort auf einen zulässigen Nachrichtenstrom erkannt werden, automatisch ebenfalls als zulässig eingestuft. Oder, ein anderes Beispiel für Statefull Inspection, es kann eingestellt werden, wie viele Pakete von einem bestimmten Typ innerhalb einer bestimmten Zeit zulässig sind. Beim Überschreiten dieser Grenze wird automatisch blockiert.

Ich fasse zusammen: Jedes Computernetzwerk, ob privat oder zu einer Organisation gehörig, benötigt angemessene Schutzfunktionen. Dabei geht es übrigens nicht nur um die Sicherheit der eigenen Daten und Infrastrukturen. Offene Netzwerke können von Kriminellen leicht dazu ausgenutzt werden, ihrerseits Schadfunktionen zu verbreiten und für Angriffe auf Dritte missbraucht werden. Die Wahl des eingesetzten Firewallsystems (Router-Firewall, Appliance oder individuell konzipiert) ist anforderungsabhängig und in Bezug auf den erreichbaren Schutzgrad sekundär. Wichtig ist, dass die Firewall den Erfordernissen entsprechend konfiguriert ist und keine vermeidbaren Sicherheitslücken bestehen. Dazu sollte die Firewall auf einer angepassten, ausfallsicher konzipierten Hardware installiert sein. Das Betriebssystem der Firewall sollte ebenfalls unter Sicherheitsaspekten ausgewählt und modifiziert werden. Insbesondere sollte die Funktionalität des Systems auf den unbedingt erforderlichen Umfang reduziert werden. Zusätzliche, möglicherweise im Hintergrund des Betriebssystems laufende Dienste stellen, insbesondere wenn sie auf das Netzwerk zugreifen, immer potenzielle Sicherheitslecks dar. Die Firewall sollte sich an der einzigen Kommunikationsverbindung zwischen dem lokalen (sicheren) Netzwerk und dem (unsicheren) öffentlichen Netzwerk befinden. Existieren weitere Netzwerkverbindungen "nach draußen", sind diese selbstverständlich ebenfalls abzusichern. Andernfalls ist die Firewall wirkungslos. Insbesondere für den Firewalleinsatz zur Absicherung von Unternehmensnetzwerken gelten zusätzliche Anforderungen: Die Firewall sollte in ihrer Grundkonfiguration sämtlichen Datenverkehr blockieren. Zulässige Kommunikationsbeziehungen sind entsprechend der jeweiligen Anforderungen explizit zu definieren. Firewalls, die nach dem Prinzip der Statefull Inspection arbeiten, erleichtern die Konfiguration und erlauben darüber hinaus den Einsatz erweiterter Kontrollmechanismen. Eine professionelle Firewall sollte nicht nur in Bezug auf die Filterfunktion korrekt konfiguriert sein. Wichtig sind weiterhin die Protokollfunktionen und die aktuelle Dokumentation.