Netzsicherheit durch Firewalls

Warum werden Firewalls benötigt?

Im Internet gibt es zahlreiche potentielle Angreifer, die versuchen in fremde Rechner einzubrechen, um diese anschließend für ihre Zwecke zu missbrauchen. Die Gründe hierzu sind vielfältig. Beispielsweise können diese Personen an Daten interessiert sein, die von sicherheitsrelevanter Natur sind (Industriespionage), oder es wird versucht, den Rechner für weitere Angriffe (z. B. Distributed Denial Of Service) zu missbrauchen. Auch ein Abhören des Fremdnetzes kann stattfinden, um an Daten oder Passwörter zu gelangen, da Passwörter oft noch im Klartext übermittelt werden. Häufig sind auch Implementierungsfehler in Software dafür verantwortlich, dass Rechner gekapert werden. Keine Software ist vor solchen Fehlern gefeit.

Um diese Angriffspunkte nicht zu bieten, müsste man jeden einzelnen Rechner in einem Netz absichern, was einen sehr großen Aufwand darstellt. Ein anderer Weg, diese Gefahren zu mindern, ist eine Firewall, die sämtlichen eingehenden und ausgehenden Datenverkehr überwacht.

Was ist eine Firewall?

1. Theoretisch

Eine Firewall ist ein Konzept, um den Informationsfluss zwischen dem externen Internet und den lokalen Maschinen zu überprüfen und ggf. entsprechend zu reagieren. Dieses Konzept muss sich nahtlos in die gesamte Sicherheitsstrategie eines Unternehmens eingliedern, und regelmäßig kontrolliert und aktualisiert werden.

2. Technisch

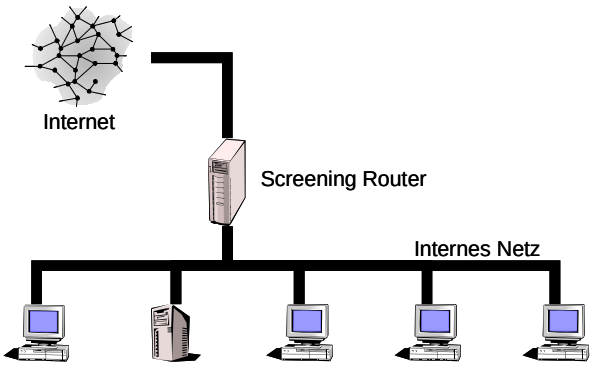
Eine Firewall ist ein informationstechnisches System, das aus mehreren Komponenten besteht. Die wesentlichen Komponenten sind:

- Überwachungsrouter (auch Screening Router, Paketfilter)
- Bastion-Host (auch Application Level Gateway)

Aus diesen Komponenten ergeben sich zwangsläufig verschiedene Anordnungsmöglichkeiten. Die grundlegenden Möglichkeiten werden im Folgenden aufgezeigt.

Wie kann eine Firewall realisiert werden?

Screening Router



Ein Screening Router ist ein Router mit konfigurierten Regeln, sog. Access Control Lists (ACLs). Dieser arbeitet auf IP-Ebene, d. h. er kann die Datenpakete anhand von Quell-IP-Adressen und Quell-Ports, sowie Ziel-IP-Adressen und Ziel-Ports filtern. Diese Regeln arbeiten richtungsbezogen, was bedeutet, dass der Router auch nach Interfaces filtern kann.

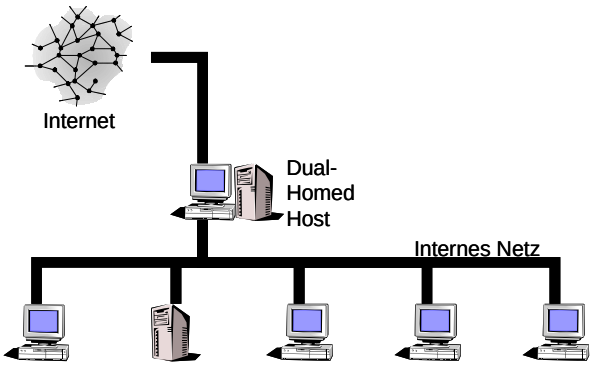
Vorteile:

- Durch einen Screening Router kann man sehr einfach selektiv bestimmte Dienste, Rechner oder ganze Teilnetze freischalten.
- Die Kosten für eine solche Lösung sind sehr gering, da fast alle Router derartige Filterfunktionen schon eingebaut haben.
- Der technische Aufwand, der für diese Lösung betrieben werden muss ist ebenfalls im unteren Bereich anzusiedeln.
- Für den Benutzer stellt sich ein Screening Router meist völlig transparent dar.

Nachteile:

- Die Filterregeln können bei größeren Netzen sehr schnell unübersichtlich werden, was der Sicherheit wiederum abträglich ist.
- Eine Überprüfung der Regeln ist meist sehr aufwendig.
- Es stellt sich dem potentiellen Angreifer nur eine Sicherheitsbarriere (Screening Router) in den Weg, danach ist das ganze lokale Netz ungeschützt.
- Es kann keine Kontrolle der Nutzdaten erfolgen.

Dual-Homed Host



Ein Dual-Homed Host ist eine Maschine, die Paketfilter und Gateway in sich vereint. Hierbei darf allerdings kein Routing zwischen externem und internem Netz stattfinden, da dies den Dual-Homed Host wieder auf die Stufe eines Screening Router zurückfallen ließe. Diese Maschine arbeitet nur auf der Anwendungsebene, worauf die erhöhte Sicherheit in diesem System basiert. Dadurch wird auch der Einsatz spezieller Programme von Nöten, sog. Proxy-Servern.

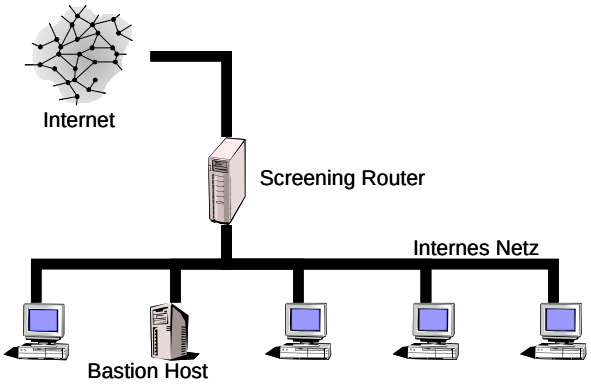
Vorteile:

- Es kann hierbei eine vollständige Kontrolle der Verbindungen erfolgen, da auf Anwendungsebene gearbeitet wird.
- Der Konfigurationsaufwand hält sich in Grenzen, da nur ein Rechner die Firewall bildet.
- Die Kontrolle der Verbindungen kann hierbei inhaltsbezogen durchgeführt werden.
- Die Identität der dahinterliegenden Rechner kann durch Network Address Translation (NAT) verborgen werden.

Nachteile:

- Es entsteht ein Mehraufwand, da für jeden Internetdienst, evtl. ein eigener Proxy-Server installiert werden muss.
- Die Firewall verhält sich dem Benutzer gegenüber nicht mehr transparent. Die Clientprogramme müssen dafür ausgelegt sein.
- Nur der Dual-Homed Host trennt das lokale Netz vom Internet, so ist beispielsweise ein Abhören der internen Kommunikation möglich, falls der Host durch einen Angreifer eingenommen wurde.
- Die größte Gefahr für die Sicherheit ist die Reaktivierung des IP-Forwarding durch einen Einbruch in den Dual-Homed Host.
- Es müssen evtl. Leistungseinbußen durch den potentiellen Engpass Dual-Homed Host in Kauf genommen werden.

Screened Host



Die Firewall besteht hierbei aus einem Screening Router und einem Bastion-Host, wobei der Bastion-Host selbst im lokalen Netz liegt. Der Screening Router leitet den Datenverkehr auf den Bastion-Host um. Es findet hierbei keine direkte Kommunikation zwischen den lokalen Clients und dem Internet statt, alles muss über den Bastion-Host laufen. Dies regelt der Screening Router, der nur Datenpakete vom Bastion-Host passieren lässt.

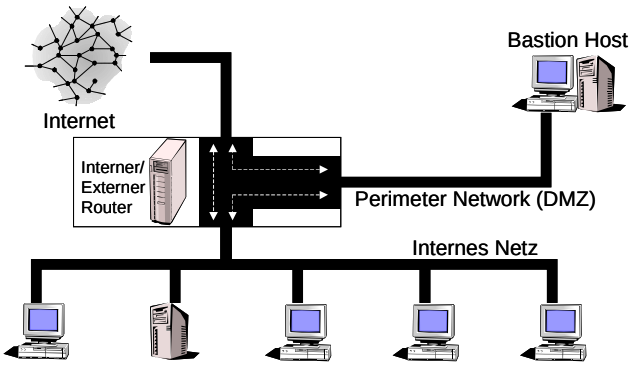
Vorteile:

- Bastion-Host und Screening Router sind verschiedene Maschinen.
- Es entsteht hier ein geringer zusätzlicher Routingaufwand, um die Daten zusätzlich durch den Bastion-Host zu schicken.
- Der Bastion-Host selbst wird gegenüber dem Internet vom Screening Router geschützt.
- Die Gefahr, die durch unentdecktes Reaktivieren des IP-Forwarding ausging, ist vermieden.
- Es können auch mehrere Bastion-Hosts eingesetzt werden, falls die Last zu groß werden sollte. Der Router verteilt die Pakete dann dienstabhängig.
- Ein Router ist wesentlich leichter zu verteidigen, da er nur eine überschaubare Funktionalität besitzt.

Nachteile:

- Der Bastion-Host ist immer noch absolut entscheidend für die Sicherheit des lokalen Netzes.
- Das Anbieten von Diensten an das Internet stellt eine potentielle Gefahr dar, da der Server sich im lokalen Netz befinden würde.
- Auch vom lokalen Netz aus sind Angriffe auf die Firewall denkbar, da durch IP-Spoofing versucht werden könnte, den Bastion-Host zu umgehen.

Screened Network (1)



Bei dieser Konzeption ist der zentrale Punkt ein Screening Router mit 3 Schnittstellen. Er routet damit zwischen dem externen Internet, dem lokalen Netz und einem Grenznetz (Perimeter Network) , der Demilitarized Zone (DMZ). In dieser DMZ befindet sich der Bastion-Host. Der Router leitet Pakete vom internen Netz an den Bastion-Host in der DMZ und von der DMZ an das externe Internet.

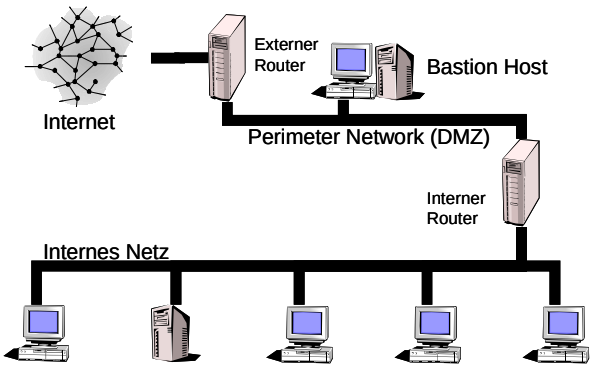
Vorteile:

- Es wird nur ein Router benötigt.
- Die internen Rechner haben keine Möglichkeit die Firewall zu umgehen, da die Gefahr durch IP-Spoofing gebannt ist.
- Das Anbieten von Diensten an das Internet findet auf Maschinen in der DMZ statt, d.h. keine Gefahr für das lokale Netz.

Nachteile:

- Filterregeln für Router mit mehr als zwei Schnittstellen werden deutlich aufwändiger und komplexer.
- Es wird zusätzliche Hardware für den Aufbau der DMZ benötigt, da diese ein eigenes Netz darstellt.
- Da die Datenpakete den Router zweimal durchlaufen müssen, erhöht sich die Verzögerung (Latenz).
- Durch Einbrechen in den Router ist der Zugang zum lokalen Netz möglich.

Screened Network (2)



Hierbei kommen zwei Router (intern/extern) zum Einsatz, wobei der Bastion-Host sich in einem eigenen Netzstrang befindet, und von beiden Routern geschützt wird. Der externe Router leitet alle eingehenden Datenpakete an den Bastion-Host weiter. Der innere Router lenkt ebenfalls alle Datenpakete aus dem lokalen Netz auf den Bastion-Host um.

Vorteile:

- Durch die beiden Router wird eine sehr hohe Sicherheit erreicht.
- Es gibt hier Logging-Möglichkeiten für nahezu jeden Angriff.
- Die Rechner des lokalen Netzes können nur mit dem Bastion-Host kommunizieren (kein IP-Spoofing)
- Die potentiellen Angriffsmöglichkeiten werden auf den Bastion-Host eingeschränkt.
- Es kann kein Abhören des lokalen Datenverkehrs stattfinden, da dies der interne Router verhindert.
- Es werden eine Reihe von Abwehrmaßnahmen möglich.

Nachteile:

- Es wird ein hoher materieller Aufwand benötigt, da zwei Router und eine DMZ benötigt werden.
- Auch der wartungstechnische Aufwand steigt.

Zusammenfassung

Firewalls stellen im allgemeinen einen sehr guten Schutz vor Angriffen von Außen dar. Sie können aber vor vielen anderen Gefahren, die IT-Anlagen drohen, nicht oder nur in sehr eingeschränktem Umfang schützen. Unter anderem wären hier innere Angriffe, Unachtsamkeit, Irrtümer, Nachlässigkeit, Technische Defekte und Computerviren zu erwähnen.
Es gibt über die gezeigten Konzepte hinaus auch noch weitere, hier nicht berücksichtigte. Diese können z. B. durch das Zusammenlegen von verschiedenen Komponenten einer Firewall entstehen.

Literatur

- Luckhardt, Norbert: „Schwer entflammbar“, c’t 4/1997
- Kienle, M.: „Standhafte Mauern“, iX 7/1994
- Chapman, Brent; Zwicky, Elisabeth: „Building Internet Security“, O’Reilly 1995
- Dr. Bernhard Röhrig: „Linux im Netz”, Computer- und Literaturverlag 1997