PEARSON Education

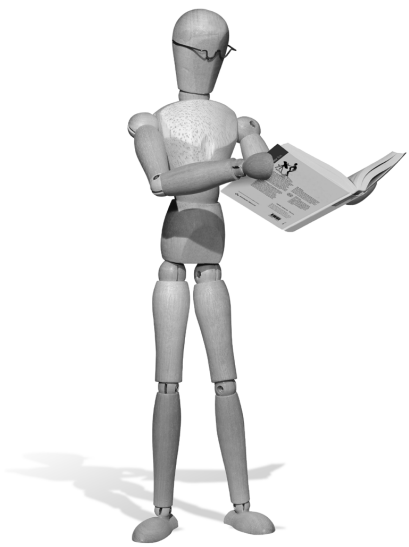
ADDISON-WESLEY

open source library

Ralf Spenneberg

Linux-Firewalls mit iptables & Co.

Sicherheit mit Kernel 2.4 und 2.6 für Linux-Server und -Netzwerke



ADDISON-WESLEY

An imprint of Pearson Education

München • Boston • San Francisco • Harlow, England
Don Mills, Ontario • Sydney • Mexico City
Madrid • Amsterdam

3 Firewall-Architekturen

Eine Firewall ist nicht ein einzelnes Gerät oder eine Gruppe von Geräten, sondern ein Konzept. Für die Implementierung eines Firewall-Konzepts haben sich in den vergangenen Jahren verschiedene Architekturen durchgesetzt. Diese Architekturen möchte ich Ihnen in diesem Kapitel vorstellen. Jede Architektur hat ihre Daseinsberechtigung. Es gibt keine absolut richtige Architektur. Wie bei allen anderen Betrachtungen sollten Sie immer Aufwand und Nutzen abwägen. Speziell bei der Wahl der Architektur müssen Sie den Aufwand in Form der benötigten Hardware analysieren.

Verabschieden Sie sich von dem Gedanken, eine absolut sichere Firewall aufzubauen, wenn Sie nicht das Netzwerkkabel durchschneiden wollen. Eine 100%ig sichere Firewall gibt es nicht. Daher muss Ihre Architektur mögliche Fehler in Ihrer Konfiguration und der Implementierung durch den Hersteller möglichst lange überleben, um Ihnen die Gelegenheit für eine Reaktion auf einen erfolgreichen Angriff auf Ihre Firewall einzuräumen. Ihre Firewall-Architektur sollte keinen Single-Point-of-Failure besitzen. Das ist ein Punkt, bei dessen Ausfall die Sicherheit komplett kompromittiert ist.

3.1 Screening-Router

Die erste Implementierung des Screening-Routers war der `screend` von Jeffrey Mogul. Ein Screening-Router ist im Grunde nichts anderes als ein einfacher Paketfilter, wie er in diesem Buch beschrieben wird. Als Architektur basiert die Firewall lediglich auf diesem Screening-Router und verwendet keine andere zusätzliche Struktur. Abbildung 3.1 zeigt die Architektur.

Der Screening-Router erlaubt üblicherweise nur Verbindungen von innen nach außen. Eine Verbindungsaufnahme von außen nach innen wird von dem Screening-Router unterbunden.

In vielen Umgebungen, bei denen nur der Zugriff von innen nach außen erlaubt werden soll, ist ein Screening-Router ausreichend, um die Sicherheit eines Netzes zu gewährleisten. Dies hängt sicherlich auch stark davon ab, ob auch interne Dienste angeboten werden sollen. Dann ist in vielen Fällen ein Screening-Router nicht ausreichend, und Sie sollten sich Gedanken über die Verwendung einer demilitarisierten Zone machen (siehe Abschnitt 3.2).

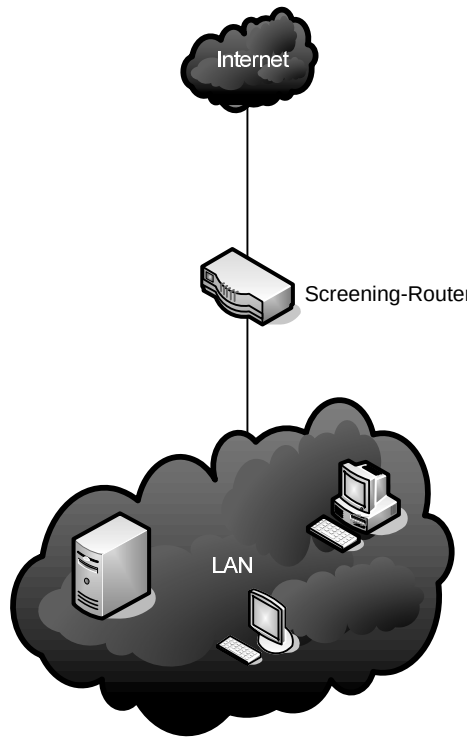


Abbildung 3.1: Ein Screening-Router schützt das interne Netz.

Ein nicht zu unterschätzender Nachteil eines einzelnen Screening-Routers ist bei einem Fehler in der Implementierung oder einem erfolgreichen Angriff das offene Netz. Wenn Ihre Firewall-Architektur nur aus einer Komponente besteht, kann ein Angreifer durch die Überwindung dieser Komponente kompletten Zugriff auf Ihr Netzwerk erhalten. Um dieses zu verhindern, sollten Sie eine mehrstufige Firewall-Architektur wie die Multiple DMZ wählen (siehe Abschnitt 3.3).

3.2 DMZ

Sobald Sie Dienste anbieten möchten, die von anderen Anwendern im Internet oder von einem nicht vertrauenswürdigen Netz genutzt werden sollen, sollten Sie sich für die Implementierung Ihres Firewall-Konzepts mit der DMZ-Architektur beschäftigen. Hierbei handelt es sich um eine demilitarisierte Zone (häufig auch entmilitarisierte Zone genannt). Dies ist ein besonderes ausgelagertes Netz, in dem Sie die Systeme positionieren, auf die ein Zugriff aus dem Internet erforderlich ist. Auch ein Proxy wird üblicherweise in dieser DMZ aufgestellt. Ein zusätzlicher Screening-Router steuert den Paketfluss, so dass aus dem internen Netz nur ein Zugriff auf die Systeme der DMZ möglich ist (siehe Abbildung 3.2).

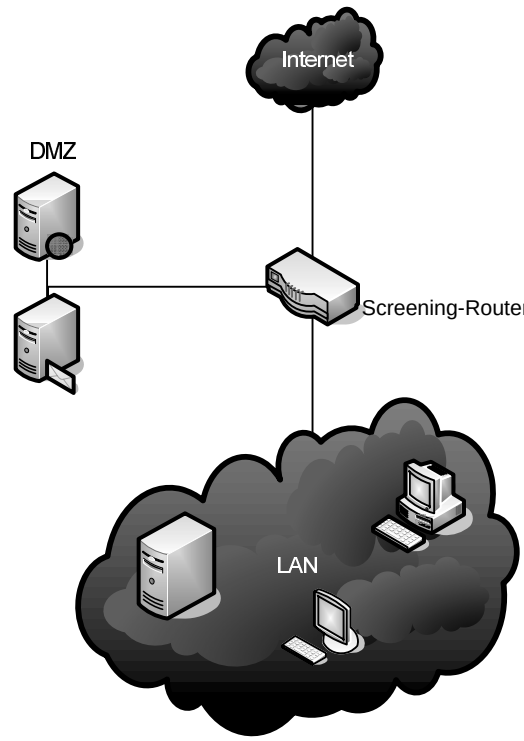


Abbildung 3.2: Die DMZ wird am einfachsten durch ein drittes Bein am Screening-Router realisiert. Der Screening-Router regelt den Paketfluss.

Ein direkter Zugriff auf das Internet wird so unterbunden[1]. Die Proxys greifen dann auf die Dienste im Internet zu und dienen dem internen Netz beim Zugriff auf das Internet als Mittelsmann. Alle Dienste, die Sie dem Internet anbieten möchten, wie zum Beispiel ein Web- und ein -Server, werden ebenfalls von Systemen in der DMZ implementiert. Da Sie diese Dienste anbieten möchten, können Sie diese Systeme nicht so schützen wie die internen Systeme, auf die kein Zugriff erlaubt wird. Bei einem erfolgreichen Angriff und Einbruch in diese weniger geschützten Systeme, sind die internen Systeme aber immer noch durch den Screening-Router geschützt, der hoffentlich nicht jeden Zugriff aus der DMZ in das interne Netz erlaubt.

Diese Kombination aus Proxys und Paketfilter erhöht die Sicherheit der geschützten Systeme. Selbst wenn Sie keine Proxys einsetzen, erhöht die Auslagerung der angebotenen Dienste aus dem internen Netz die Sicherheit desselben, da nun bei einem Angriff kein direkter Zugriff auf die weiteren Rechner des internen Netzes möglich ist.

[1] Da einige Protokolle nicht von Proxys unterstützt werden, ist für diese Protokolle häufig noch ein direkter Zugriff auf das Internet notwendig, wenn diese Protokolle genutzt werden sollen.

Dennoch basiert die Sicherheit der Architektur auf einem Single-Point-of-Failure, dem Screening-Router. Wenn der Administrator oder der Programmierer bei der Einrichtung oder Entwicklung des Screening-Routers einen Fehler macht, der erfolgreich von einem Angreifer ausgenutzt werden kann, ist der Angreifer in der Lage, auf das interne Netz zuzugreifen, da nur der Screening-Router dieses Netz schützt. Wenn dies nicht akzeptabel ist, können Sie die DMZ durch zwei Paketfilter realisieren: einen externen und einen internen Paketfilter. Der interne Paketfilter regelt den Verkehr zwischen der DMZ und dem internen Netz. Der externe Paketfilter regelt den Verkehr zwischen der DMZ und dem Rest. Dies ähnelt der multiplen DMZ (nächster Abschnitt).

3.3 Multiple DMZ

Den Begriff der multiplen DMZ verwende ich, um eine mehrstufige Firewall zu beschreiben, die über mehrere DMZs verfügt. Abbildung 3.3 zeigt das Prinzip.

Bei der multiplen DMZ existiert kein Single-Point-of-Failure. Die in Abbildung 3.3 dargestellte Architektur wird durch zwei Screening-Router realisiert, die keine direkte Verbindung besitzen. Anstatt die beiden Screening-Router direkt miteinander zu verbinden, verfügen die Application-Level-Gateways über zwei Netzwerkkarten und stehen mit jeweils einem Bein in der inneren und der äußeren DMZ. Kann der Angreifer den äußeren Screening-Router überwinden, so ist das interne Netz immer noch durch die Application-Level-Gateways und den inneren Screening-Router geschützt. Selbst wenn der Angreifer direkt ein Application-Level-Gateway angreifen könnte, wird das interne Netz immer noch von dem inneren Screening-Router geschützt. Die angebotenen Dienste besitzen nur eine Netzwerkkarte und befinden sich in der äußeren DMZ. Falls diese Dienste auf interne Datenbanken zugreifen müssen, ist der Zugriff nur über die Application-Level-Gateways möglich, oder diese Systeme benötigen für diesen Zugriff ein weiteres Bein in der inneren DMZ.

Der schiere Hardware-Aufwand und der damit einhergehende Administrationsaufwand lassen diese Lösung natürlich nur für Netze mit einem hohen Schutzbedürfnis adäquat erscheinen. Natürlich sind auch zahlreiche Variationen der Architektur denkbar.

Der Vorteil dieser Architektur ist das Fehlen des Single-Point-of-Failure. Sie haben hoffentlich beim erfolgreichen Angriff auf die Firewall genügend Zeit, mit entsprechenden Maßnahmen (Unterbrechung der Netzwerkverbindung) zu reagieren.

3.4 Wahl der Architektur

Die Wahl der richtigen Architektur ist nicht einfach. Wie schon erwähnt: eine 100%ig sichere Firewall gibt es nicht. Diese mag in Hochglanzprospekten der Hersteller existieren. In der Realität habe ich sie noch nie gefunden. Falls Sie einen Hersteller finden, der Ihnen diese verspricht, fragen Sie ihn, warum er Ihnen dann auch noch ein IDS und einen Virenscanner verkaufen möchte.

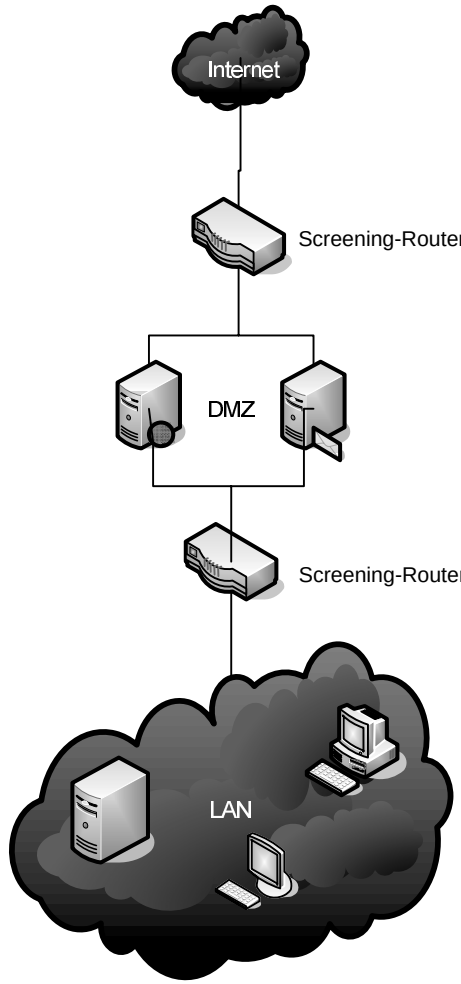


Abbildung 3.3: Bei einer multiplen DMZ gibt es keinen Single-Point-of-Failure.

Die Wahl der Architektur ist entscheidend für die Standhaftigkeit der Firewall. Vergleichen Sie Ihr Netzwerk mit einer Stadt aus dem Mittelalter. Im Mittelalter war jede Stadt in Bezug auf ihren Schutz auf sich allein gestellt. Es gab keine Polizeigewalt, die den Austausch von Waren und das Reisen zwischen den Städten überwachte. Vielmehr regierten außerhalb der Städte meistens Raubritter und Diebe. Es herrschte Anarchie, wie es heute in vielen Bereichen des Internets der Fall ist. Sobald Sie Ihr Netz mit dem Internet verbinden, sind Sie daher bezüglich der Sicherheit Ihres Netzes auch auf sich allein gestellt. Sie müssen sich, wie die Städte im Mittelalter, gegen jeden nur möglichen Angriff verteidigen. Im Mittelalter bauten die Stadtbewohner daher Burgmauern und zogen Gräben. Meist wurde nicht nur eine Mauer oder ein Graben gezogen, damit die Verteidiger ausreichend Zeit für

die Vorbereitung der Verteidigung erhielten. Musste der Angreifer nur eine Mauer überwinden, benötigte er nur genügend lange Leitern, um den Angriff erfolgreich durchzuführen. Gute Verteidigungsanlagen verfügten über mehrere Mauern und Gräben und deren Kombination, so dass die Mauer zwar mit einer Leiter überwunden werden konnte, aber der Angreifer für den Graben Boote benötigte und die Leitern nicht einsetzen konnte. Die Verteidiger hatten in der Zeit die Gelegenheit, ihr Öl zum Sieden zu bringen, um es über die Angreifer zu gießen.

Nutzen auch Sie daher in Ihrer Firewall-Architektur unterschiedliche Technologien zur Verteidigung, und bauen Sie mehrere Schutzwälle auf. Auch heute zeigt sich wie im Mittelalter, dass Angreifer häufig auch nur die schlecht geschützten Ziele angreifen. Diese werden auch als »low hanging fruits« (niedrig hängende Früchte) bezeichnet.

Gegen derartige Angriffe sind Sie mit einer mehrstufigen Firewall durch die Abschreckung gut geschützt. Falls ein Angreifer Sie tatsächlich gezielt angreift, bietet ein mehrstufiges System Ihnen hoffentlich die notwendige Zeit zur Vorbereitung der Verteidigung, bevor der Angreifer in Ihr Netz gelangt.