

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

Teil I

Firewall-Grundlagen





1 Firewall-Geschichte

Ich persönlich empfinde es immer als hilfreich, die geschichtliche Entwicklung der eingesetzten Produkte und Technologien zu kennen, um diese besser bewerten und einschätzen zu können. Dieses Kapitel versucht, skizzenhaft die Entwicklung der Firewalls aufzuzeigen.

1.1 Der Anfang des Internets

Das Internet begann als eine Reihe von Notizen von J.C.R. Licklider am MIT, in denen er 1962 ein »Galactic Network« beschreibt. Ein Jahr früher veröffentlichte Leonard Kleinrock (ebenfalls am MIT) eine erste Arbeit über paketvermittelnde Netzwerke. Aus diesen Ideen entstand 1965 das erste Wide-Area-Network (WAN), in dem Lawrence G. Roberts gemeinsam mit Thomas Merrill den TX-2 Computer des Lincoln Labs in Massachusetts mit dem Q-32-Computer des SDC in Kalifornien verband. 1966 ging Roberts dann zur Defense Advanced Research Projects Agency (DARPA), um dort ein Konzept für ein Computer-Netzwerk zu entwickeln. Angeblich versprach Charlie Hertzfeld (Direktor der DARPA) dem IPTO-Direktor Bob Taylor eine Million Dollar für die erfolgreiche Implementierung eines verteilten Kommunikationsnetzwerks. Die Entwicklung des ARPANET begann. Im Dezember 1970 wurde das erste Netzwerkprotokoll für das ARPANET offiziell verabschiedet: das Network Control Protocol (NCP). Die Entwicklung der Anwendungen konnte beginnen. 1972 wurde als erste Applikation E-Mail vorgestellt.

Das NCP-Protokoll erlaubte zwar die Kommunikation in dem Netz. Je größer das ARPANET wurde, desto deutlicher wurden jedoch seine Schwächen. So wurde die Entwicklung der Internetprotokollfamilie TCP/IP begonnen. TCP/IP wurde 1980 vom Department of Defense bereits als Standard anerkannt und 1982 in einem RFC beschrieben. Am 1.1.1983 wurde das ARPANET auf TCP/IP umgestellt. In den folgenden Jahren wuchs das ARPANET. Weitere Netzwerke wurden aufgebaut: BITNET, USENET, MFENET, HEPNET, SPAN, CSNET. Im kommerziellen Bereich entstanden XNS (Xerox), IBM SNA und das DECNET. Speziell für den akademischen Bereich wurde das NSFNET gestartet. Dieses wuchs in nur 8 Jahren von einem Backbone mit 6 Knoten (56 kBit/s) zu 21 Knoten mit bis zu 45 Mbit/s. Das Internet wuchs in dieser Zeit zu einer Zahl von 50.000 Netzen weltweit.

Dennoch handelte es sich beim Internet lange Zeit um eine heile Welt. Jeder kannte und vertraute jedem anderen Teilnehmer, und unter dem Aspekt Sicherheit betrachtete man lediglich die Gefahr eines Paketverlustes und entwickelte Methoden und

Protokolle, um den Verlust von Paketen zu verhindern und die Verfügbarkeit der Dienste und der Kommunikation zu garantieren.

1.2 Der Morris-Wurm

Im November 1988 löste der Morris-Wurm von Robert Tappan Morris eine Epidemie im Internet aus. Dieser Wurm drang über Sicherheitslücken in den Unix-Betriebssystemen ein und nutzte Sendmail, Finger und die R-Dienste für seine Verbreitung aus. Die verwendeten Sicherheitslücken werden in der Bugtraq-Datenbank unter den Nummern 1 und 2 geführt (<http://www.securityfocus.com/bid/1>). Während seiner Verbreitung infizierte dieser Wurm mit 6000 Rechnern etwa 10% des damaligen Internets. Robert Morris wurde am 26. Juli 1989 als Freisetzer des Wurms identifiziert und am 22. Januar 1990 zu 400 Stunden gemeinnütziger Arbeit und 10.400 Dollar Geldstrafe verurteilt. Interessanterweise war sein Vater, Robert Morris Senior, zu diesem Zeitpunkt Chef-Wissenschaftler der National Security Agency (NSA).

Als direkte Reaktion auf den Wurm wurde noch im November 1988 das Computer Emergency Report Team Coordination Center (CERT/CC) von der Defense Advanced Research Projects Agency (DARPA) gegründet.

Des Weiteren begannen die Unternehmen, über einen Schutz ihrer Netzwerke vor dem Internet nachzudenken. Bis zu diesem Zeitpunkt gab es keine Firewalls, kein NAT und auch keinen anderweitigen Schutz.

1.3 Die erste Firewall

Recht früh wurden bereits Router als Sicherheitssysteme für die Abschottung eines Netzes von den anderen Netzen eingesetzt. Zu Beginn nutzte man diese Router, um zu verhindern, dass Netzwerk-Fehlkonfigurationen Broadcast-Stürme auslösten, die sämtliche Netze in Mitleidenschaft zogen¹.

Die ersten richtigen Firewalls wurden relativ gleichzeitig bei DEC und AT&T entwickelt. Bei DEC betrieb zunächst Brian Reid und dann Paul Vixie ein System mit dem Namen `gatekeeper.dec.com`. Für den Zugriff auf das Internet mussten die Anwender sich auf diesem System anmelden (telnet und ftp) und konnten dann von diesem System auf Systeme im Internet zugreifen.

Gleichzeitig arbeitete Marcus J. Ranum für Frederick Avolio in einer anderen Abteilung bei DEC. Sie verfügten über eine Internetverbindung mit 9600 Baud und benötigten eine ähnliche Sicherheitsstruktur. Marcus Ranum wollte jedoch den Anwendern keine Konten auf dem System für eine Anmeldung zur Verfügung stellen

¹ Ein Broadcast-Paket wird von jedem Rechner entgegengenommen. Viele der ersten Protokolle verwendeten Broadcast-Pakete für die Kommunikation. Ein Router leitet Broadcast-Pakete nicht weiter. So sind die Rechner hinter dem Router nicht von einem Broadcast-Paket betroffen. Ansonsten kann in einem großen Netzwerk der Broadcast-Verkehr einen großen Teil der Netzwerkkapazität belegen.

und schrieb daher den ersten FTP-Proxy für seinen Gatekeeper. Kurze Zeit später (1991) wurde diese Firewall bereits als erste kommerzielle Firewall DEC-SEAL (Securing External Access Link) an einen großen Chemie-Konzern verkauft und dort im Juni 1991 auf mehreren Systemen eingerichtet. Ein Firewall-System bestand aus einem Gatekeeper, der als einziges System auf das Internet zugreifen durfte, und einem Gate, das den Zugriff des internen Netzes auf den Gatekeeper als Paketfilter überwachte. Der Gatekeeper verfügte über eine gewisse Anzahl von Proxys, die den Zugriff per telnet, ftp, E-Mail, News, Whois und X erlaubten. Die DEC SEAL wurde schließlich zur AltaVista Firewall weiterentwickelt.

Frederick Avolio und Marcus Ranum wechselten zu Trusted Information Systems (TIS) und programmierten dort das TIS Firewall-Toolkit (TIS FWTK, <http://www.fwtk.org/>). Nach dem Kauf von TIS durch NAI 1998 wurde diese Firewall als Gauntlet kommerziell vermarktet.

Gleichzeitig wurde bei AT&T von William R. Cheswick und Steven M. Bellovin in den Bell Laboratories eine Firewall entwickelt, die nicht über einzelne Proxys für jedes Protokoll verfügte, sondern als Circuit-Relay-Proxy ausgelegt war. Dies war der Vorgänger des SOCKS-Protokolls und des SOCKS-Proxy. Kommerziell wurde diese Firewall als Raptor Eagle kurze Zeit später verkauft.

Die ersten Firewalls waren also immer Systeme, die für die Funktion auf Proxys zurückgriffen. Auch heute gibt es noch viele Firewall-Systeme, die für die Realisierung Proxys einsetzen. Bei einigen Protokollen ist dies auch sinnvoll, um eine Filterung von Viren oder unerwünschten Inhalten durchzuführen.

Im Jahr 1994 betrat Check Point den Markt der Firewalls und bot von Anfang an einen Paketfilter mit einer grafischen, leicht zu administrierenden Oberfläche an. Gleichzeitig war dieser Paketfilter in der Lage, den Zustand der TCP-Verbindungen zu überwachen und Verbindungen nur in bestimmten Richtungen zu erlauben.

1.4 Firewalls heute

Heute bestehen Firewall-Systeme meist aus einer Kombination aus Paketfilter und Proxy. Während einige Protokolle auf Grund ihrer Natur nicht mit einem Proxy gefiltert werden können (z.B. IPsec), ist es bei anderen Protokollen zum Schutz der eigenen Infrastruktur zwingend erforderlich, Proxys einzusetzen. Ein Paketfilter kann keinen Virus oder andere bösartige Inhalte in E-Mails oder in Webseiten erkennen und entfernen.

Dennoch gibt es auch häufig Szenarien, bei denen dieses gar nicht gewünscht wird oder eine Proxy-Firewall nicht den Datendurchsatz bewältigen könnte. Hier werden dann reine Paketfilter eingesetzt.

