

Vorwort

In den vergangenen zwanzig Jahren hat die Entwicklung des Internets einen weiten Weg hinter sich gebracht. Anfangs spielte das Design die wichtigste Rolle. Heute ist das Design noch immer die Basis, aber darauf stapeln sich proprietäre Lösungen, eigenartige Protokolle und unzählige Netzwerkkomponenten, die aktiv jedes Paket modifizieren, das sie passieren will. Dieses Buch bietet eine Übersicht über Netzwerksicherheit, Management und Hochverfügbarkeit in diesem neuen und immer noch in Entwicklung begriffenen Umfeld – und das immer mit dem Fokus auf dem Netzwerk selbst. Das Internet mag nicht mehr die anfängliche Schönheit besitzen, aber kein System, das auf so vielfältige Weise Verwendung findet, kann sich dauerhaft den Erweiterungswünschen seiner Anwender entziehen. Der Leser dieses Buchs mag sich jedoch damit trösten, dass das Netzwerken grundsätzlich noch immer vorhersehbaren Regeln folgt. Das Studium der Netzwerktechnik belohnt noch immer diejenigen, die bereit sind, die Ärmel hochzukrempeln und sich die einzelnen Pakete anzusehen.

Eine der zahlreichen Netzwerkkomponenten ist natürlich noch immer die Firewall. Aus der Not geboren, ist die Firewall diejenige Einrichtung, die jedes Paket unter die Lupe nimmt. Sie ist lästig und nützlich zugleich, indem sie den mühsam zustande gebrachten Datenverkehr zwischen Client und Server manchmal einfach unterbindet. Der erste Abschnitt dieses Buchs erklärt Firewalls vom einfachen Paketfilter bis zum professionellen, genau konfigurierbaren Produkt.

Vereinfacht gesagt, stellen Firewalls widerliche Dinge mit den Datenpaketen an. Sie sind nicht damit zufrieden, Pakete einfach zu überwachen und einige aus dem Verkehr herauszufiltern. Sie verändern Pakete auch, wenn sie vorbeikommen. Sie verstellen IP-Adressen und Portnummern, sie schnüffeln in der Anwendungsschicht herum, sie stopfen Datenverkehr in Tunnel und sie speichern genaue Informationen über jede Sitzung. Ein Paket, das die Firewall durchlässt, muss keine große Ähnlichkeit mehr mit dem Paket haben, das dort hineingelangt ist.

Im Extremfall produzieren Netzwerkkomponenten Pakete, die nicht mehr zu erkennen sind. Eine ganze Reihe neuer Entwicklungen widmet sich der Aufgabe, Netzwerkpakete so sehr zu verändern, dass sie theoretisch für Uneingeweihte nicht mehr lesbar sind. Damit kommen wir zum heute so beliebten VPN. Man kann keine Abhandlung über Firewalls schreiben, ohne das VPN anzuschneiden. Die Firewall ist häufig das sensibelste Element, platziert an den Enden der Datentunnel. Überraschend ist auch die Beobachtung, wie sehr VPNs das Netzwerk-Management verkompliziert haben.

Und ironischerweise lassen sich gerade mit VPNs manche Hindernisse in Form der Firewall wieder einreißen.

Wenn etwas den einzigartigen Ansatz dieses Buches hervorhebt, dann ist es die Besprechung von Netzwerksicherheits-Management in großem Maßstab. Das Einrichten und die Fehlersuche bei Gateway-zu-Gateway-VPNs kann sehr kompliziert werden, wenn an den beiden Enden verschiedene Administratoren arbeiten. Räumlich getrennte VPN-Anwender müssen von der Firewall überwacht werden, um zu verhindern, dass die Endpunkte der Verbindung eine Hintertür in das vertraute private Netzwerk öffnen. Die Firewall-Regeln müssen flexibel und wiederwendbar sein, um zu erreichen, dass für die Netzwerksicherheit ausgewählte Komponenten auch eingesetzt werden können. Das System erfolgreich zu managen ist das Ziel neuer Produkte, die auf dem Meta-Management basieren: weg von den Einzelheiten, hin zum Formulieren von Regeln für die einzelnen Objekte, aus denen das Netz besteht. Die Firewall, die ehemals für die Sicherheit von Endpunkten eingesetzt wurde, wird jetzt zum Universalwerkzeug. Es überrascht nicht, dass Unternehmen im Bereich Netzwerksicherheit sich zu Management-Unternehmen für Endpunkte entwickeln. Wir sind nicht weit davon entfernt, dass der PC zu einer gemanagten Netzwerkkomponente wird, die einer zentralen Sicherheitsverwaltung unterliegt.

Wenn mir ein Abschnitt dieses Buches besonders wichtig ist, dann ist es der über die Hochverfügbarkeit. Die Firewall ist per Definition ein Engpass und durch Ausfälle gefährdet. Hierin liegt die Bequemlichkeit und auch die Gefahr der Firewall: Sie bietet einen einzigen Punkt für die Sicherheitsadministration. Netzwerksicherheit allein bewegt sich auf dem schmalen Grat zwischen Blockieren des Unerwünschten und Zulassen des Erwünschten. Im Laufe der Zeit wurde die Netzwerkverfügbarkeit genauso wichtig wie die Netzwerksicherheit und hochverfügbare Netzwerksicherheit wurde das Ziel. Hochverfügbare Systeme sind auch heute noch keineswegs Standard. Dieses Buch erläutert die besten Verfahren in Sachen Firewall-Loadbalancing und -Hochverfügbarkeit. ISP-Hochverfügbarkeit hilft dabei, das Thema zu entwickeln. Ein Thema kann jedoch nicht Gegenstand von Untersuchungen werden, wenn es keinen Namen hat und nicht allgemein definiert wird. Ich hoffe, dass dieses Buch andere dazu anregt, sich den angesprochenen Themen unter neuen Perspektiven anzunehmen.

Die Zukunft wird viele neue aktive Netzwerkkomponenten mit sich bringen, und die Firewall ist nur der Anfang davon. Der flexible Netzwerkarchitekt tut gut daran, sich an die bescheidenen Anfänge zu erinnern und sein Denken auf das Netz selbst zu richten. Wie ich eingangs erwähnt habe, ist das Studium der Netzwerktechnik eine lohnende Sache für die, die bereit sind, die Ärmel hochzukrempeln und sich die einzelnen Pakete anzusehen.

Paul LeMahieu

paul@rainfinity.com