

# Einführung

## Was wir mit diesem Buch erreichen wollen

Moderne IP-Netzwerke und Einwahlverbindungen sind genauso wie TK-Anlagen und Telefonendgeräte zu einem unverzichtbaren Bestandteil unseres täglichen Lebens geworden. Von Sprach- und Datendiensten erwarten wir, dass sie a priori vorhanden sind – und das mit zeitgemäßer Qualität.

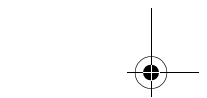
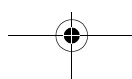
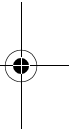
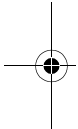
Noch Mitte der 90er Jahre nutzten Privatanwender das Internet mit einem Analogmodem, das eine stattliche Bandbreite von 14.400 Bit/s aufwies. Heute sind bei den Providern ISDN- und DSL-Produkte im Angebot, die die Bandbreiten von damals je nach Produktmerkmal um den Faktor fünf bis 30 übersteigen.

Gleichzeitig hat noch Ende der 90er Jahre eine 2-Mbit/s-Direktleitung ausgereicht, um mehrere tausend PC-Arbeitsplätze eines Konzerns mit Zugang zu E-Mail und zum Internet zu versorgen. Heute besitzen diese Arbeitsplätze im Durchschnitt Zugänge mit 34 Mbit/s oder gar  $2 * 34$  Mbit/s, was einen Zuwachs in etwa gleicher Größenordnung wie bei den Einwahlverbindungen (Faktor 16 bis 32) bedeutet.

Durch diesen Boom hat die Komplexität moderner IP-Netzwerke in den letzten Jahren einen gewaltigen Sprung gemacht. Firewalls als Gateways von und zum Internet – wie auch an internen Knotenpunkten – müssen heute schon bei der Planung als Netzwerkbestandteil ausgelegt werden. Know-how zum Schutz von Netzwerken, das in den letzten Jahren als gut oder gar exzellent galt, ist heute veraltet. Die moderne eSociety fordert neue Konzepte zur Gewährleistung hoher Sicherheit bei maximaler Bandbreite, Performance und Transparenz.

Die auf dem Markt erhältliche Literatur zum Thema Firewalls beschäftigt sich hauptsächlich mit den Grundlagen, der Bedienung von GUIs oder ist ein Abklatsch der Handbücher des Herstellers und verschiedener Newsgroups.

Bei DoS/DDoS-Angriffen durch z. B. Smurf-Attacken auf die Firewall oder eines der dahinter liegenden Systeme, aber auch schon bei einem simplen Broadcast-Sturm in einer DMZ können schlecht konzeptionierte Firewalls bereits außer Betrieb gesetzt werden. Das hat jedoch ganz selten mit Dingen zu tun, die sich über das GUI konfigurieren lassen, und ganz oft mit technischen und konzeptionellen Details, über die zurzeit keine umfassende Literatur erhältlich ist.



## Einführung

Unser Buch will diese Lücke schließen, beim Leser Verständnis für moderne Lösungen wecken und Know-how weitergeben, das den Anforderungen der eSociety gerecht wird.

Der Fokus des Buchs liegt auf der technischen Betrachtung von Firewalls als Netzwerkbestandteil bzw. Router mit Sicherheitsfunktion. Unser Ausgangspunkt ist ein Beispielnetzwerk eines Unternehmens, das im Verlauf des Buches mit verschiedenen Lösungen abgesichert wird. Alle vorgeschlagenen Systeme werden an geeigneter Stelle im Testnetzwerk eingeführt, und das dabei verfolgte Konzept wird mit Netzwerkdigrammen ausführlich erläutert.

Je nach den Merkmalen und der Qualität der vorgeschlagenen Lösungen verändert sich das Testnetzwerk (bzw. Subnetze daraus) chamäleonartig zu einer Struktur, in der sich sowohl mittelständische Unternehmen als auch große Konzerne und Internetportale wiederfinden.

## Zielgruppe



»Denn wer vieles bringt, wird manchen etwas bringen; und Jeder geht zufrieden aus dem Haus ... « (Goethe)

### *Der Aufbau dieses Buches*

Das Zitat klingt gut. Im Original folgt ein seitenlanger Disput zum Gegensatz von perfektem Werk und großer Massentauglichkeit. Er endet witzigerweise damit, dass es die (Bühnen)Technik, nicht der Inhalt des Werkes schon irgendwie schaffen wird, die Massen anzulocken.

Seit dem 19. Jahrhundert hat sich die Situation kaum verändert. Massentauglichkeit, d.h. das Ansprechen einer möglichst großen Zielgruppe, ist wünschenswert, geht aber in der Regel zu Lasten der Qualität und fachlichen Tiefe eines Werkes. Deswegen war bei der Arbeit an diesem Buch der Mut erforderlich, ein reines Fachbuch zu schreiben, der Mut, Qualität abzuliefern, in der Hoffnung, dass diese die eingeschränkte Zielgruppe dann auch vollkommen überzeugt.

Die Zielgruppen sind:

- ▶ Firewall-Administratoren und Mitarbeiter, die mit dem Betrieb von Netzwerken betraut sind. Sie wissen bereits, wie man mit einem Firewall-GUI umgeht. Unser Buch hilft Ihnen, tiefer in die Technik, IP und konzeptionelle Aspekte einzusteigen, um anspruchsvollere Aufgaben als die Beschäftigung mit dem GUI zu übernehmen, wie zum Beispiel ein besserer 2nd- und 3rd-Level-Support für die von Ihnen betreuten Systeme, die Planung neuer Systeme und ein effektiveres Troubleshooting.
- ▶ Berater und Entscheider, die ein Kompendium zum Einsatz moderner Sicherheitstechnik in anspruchsvollen Umgebungen suchen. Sie verfügen nicht unbedingt über Detailwissen zu allen Technologien, müssen aber genug Know-how besitzen, um die Folgen, Kosten und Skalierbarkeit Ihrer Entscheidungen abschätzen zu können.
- ▶ Netzwerkingenieure, deren täglich Brot Routing-Protokolle wie RIP oder BGP4 sind. Gerade auf Ihrem Gebiet wird Sicherheit immer wichtiger. Fast jeder Router macht heute mit Sicherheitsfeatures Werbung, und die Schnittmenge Ihrer Arbeit mit der Arbeit der Kollegen von der Netzwerksicherheit nimmt zu.

Zu guter Letzt handelt dieses Buch von nichts anderem als von faszinierender Technik, von der sich mancher wünscht, dass er sie einmal im Leben zu Gesicht bekommt. Und vielleicht hat es Goethes Theaterdirektor ja richtig erkannt und dies ist wirklich das Merkmal, das die Massen anlockt, unser Buch zu lesen.

## **Der Aufbau dieses Buches**

Das Buch ist in drei Teile und neun Kapitel gegliedert. Das Testnetzwerk ist gewissermaßen der rote Faden, der sich durch (fast) alle Kapitel zieht. Auch der fortgeschrittene Leser sollte sich die Zeit nehmen, zumindest das Kapitel zum Testnetzwerk durchzuarbeiten, bevor er sich andere Kapitel vornimmt. Trotzdem können die Kapitel auch unabhängig voneinander gelesen werden. Querverweise stellen sicher, dass das Verständnis nicht verloren geht.

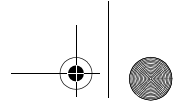
## Einführung

*Teil 1:* Der erste Teil ist als Einstieg in das Buch, das Testnetzwerk und erste technische und logische Interna von Firewalls gedacht. Es ist der einzige Teil des Buches, der sich nicht mit konkreten Implementierungen auseinandersetzt.

- ▶ *Kapitel 1, »Tatort: Das Testnetzwerk«:* Dieses Kapitel erläutert den Aufbau und das IP-Adresskonzept des fiktiven Firmennetzwerks, das in den folgenden Kapiteln dieses Buches durchgängig verwendet wird. Zusätzlich blicken wir mit etwas Terminologie zu Equipment und Datenleitungen kurz über den Tellerrand, betrachten die Anbindung ans Internet und versuchen die genaue Grenze zum Internet zu fassen (Autor: Jörg Fritsch).
- ▶ *Kapitel 2, »Technologien und Techniken«,* ist ein Grundlagenkapitel, das neben den für das Verständnis von Firewalls erforderlichen TCP/IP-Konzepten vor allem die Technologien vorstellt, die modernen Firewalls zugrunde liegen. Anfängen von einfachen statischen Access-Listen auf Routern über dynamische Paketfilter und Application-Level-Firewalls bis hin zu Hybrid-Technologien werden die jeweiligen Prinzipien vermittelt und die Vor- und Nachteile diskutiert (Autor: Steffen Gundel).
- ▶ *Kapitel 3, »IP Forwarding«,* beleuchtet den Weg von IP-Paketen durch ein System und die hardwareseitigen Unterschiede der auf dem Markt erhältlichen Technologien. Dieses Buch orientiert sich hauptsächlich an dem Marktführer Check Point, wenn es auf geeignete Hardware und dedizierte Appliances eingeht. Es gibt aber auch eine Vielzahl anderer ernst zu nehmender Technologien, die sich in der Paketverarbeitung oder bei der Auswertung der Verbindungen unterscheiden (Autor: Jörg Fritsch).

*Teil 2* behandelt das Testnetzwerk als Hausnetzwerk eines mittelständischen Unternehmens und führt zwei vorerst nicht redundante Firewalls verschiedener Hersteller an verschiedenen Stellen ein. Kapitel zu VPN-Verbindungen und zum Firewall-Management inklusive Meta-Management (zum Beispiel Provider-1) runden diesen Teil ab.

- ▶ *Kapitel 4, »Firewalls und Firewall-Management«:* In diesem Kapitel wird zunächst die FireWall-1 von Check Point zur Absicherung des Internetzugangs ins Spiel gebracht. Es werden detailliert die einzelnen Installations- und Konfigurationsschritte, angefangen von der Systemhärtung bis hin zur Definition des Regelwerks, erläutert. Im Anschluss daran wird eine Intranet-Firewall auf Basis der Cisco Pix in das Unternehmensnetzwerk integriert (Autor: Steffen Gundel).
- ▶ *Kapitel 5, »Management-Architekturen«,* beschäftigt sich mit Management-Architekturen von Firewalls. Zunächst wird das Prinzip von 2-Tier- und 3-Tier-Architekturen vorgestellt. Anschließend wird der Begriff Meta-Management definiert und Provider-1 als ein entsprechendes Produkt vorgestellt. Das Kapitel wird durch einen Abschnitt zu virtuellen Systemen abgerundet (Autor: Steffen Gundel).



### Der Aufbau dieses Buches

- ▶ *Kapitel 6, »Virtual Private Networks und sichere Verbindungen«*: In diesem Kapitel werden die Grundlagen für den Einsatz verschiedener VPN-Technologien (zum Beispiel ATM und MPLS) sowie für IPSec-Verbindungen gelegt. Die verschiedenen VPN-Technologien zeichnen sich meist entweder durch sehr hohe Flexibilität oder durch sehr hohe Sicherheit aus. Es gibt demnach vPns und Vpns (Autor: Jörg Fritsch).
- ▶ Anknüpfend an Kapitel 6 wird in *Kapitel 7, »Remote-Access-VPNs«*, auf der Basis von Check Point-Produkten ein Remote-Access-VPN für das Netzwerk unseres fiktiven Unternehmens geschaffen. Dabei wird anschaulich erläutert, wie der sichere Zugriff über das Internet auf die schützenswerten Ressourcen des Unternehmens erfolgen kann. (Autor: Steffen Gundel).

*Teil 3*: Bei zunehmender Verlagerung der Kommunikation mit Geschäftspartnern und Kunden auf das Internet werden Verbindungsabbrisse und Ausfallzeiten immer teurer. Hochverfügbarkeit entwickelt sich zunehmend von einem Privileg großer Unternehmen zur Lösung der Wahl für einen breiten Anwenderkreis.

Der dritte Teil behandelt hochverfügbare Umgebungen und beleuchtet zusätzlich Aspekte wie BGP und Multilink-Anbindungen, die in das Thema Hochverfügbarkeit hineinspielen.

- ▶ *Kapitel 8, »Redundanz und Loadbalancing«*: Die Firewalls des Firmennetzwerks werden nun durch hochverfügbare Systeme abgelöst. Von reinen Hot-Standby-Lösungen bis hin zu lastverteilten Systemen werden die auf Netzwerkebene angewendeten technologischen Prinzipien wichtiger Hersteller (Nokia, Stonesoft, Rainfinity, Nortel und Radware) erläutert und angewendet (Autor: Jörg Fritsch).
- ▶ *Kapitel 9, »Multilink-Anbindungen, Multihoming«*: Die gleichzeitige Anbindung moderner Firmennetzwerke an Mietleitungen verschiedener Carrier durch Alternativen zu BGP ist in letzter Zeit auch für den Mittelstand erreichbar geworden. Im letzten Kapitel dieses Buches binden wir die externe Firewall unseres Firmennetzwerks mit BGP an die Backbones verschiedener Provider an und vergleichen sie dann mit zwei alternativen Produkten, deren Technologie auf DNS und NAT aufsetzt (Autor: Jörg Fritsch).

