Einrichten von Internet Firewalls

Von Elizabeth D. Zwicky, Simon Cooper & D. Brent Chapman
2. Auflage Februar 2001
ISBN 3-89721-169-6
928 Seiten, DM 99,-

Inhalt

Kapitel 6: Firewall-Architekturen

Dieses Kapitel beschreibt eine Vielzahl von Methoden, Firewall-Komponenten zusammenzusetzen, und befaßt sich mit deren Vor- und Nachteilen. Wir werden Ihnen sagen, welche Architektur sich für welche Anwendung eignet.

Single-Box-Architekturen

Die einfachsten Firewall-Architekturen bestehen aus einem einzigen Gerät, das als Firewall agiert. Im allgemeinen besteht bei *Single-Box-Architekturen* der Sicherheitsvorteil darin, daß es nur eine einzige Stelle gibt, auf die Sie sich konzentrieren und die Sie richtig konfigurieren müssen. Andererseits hängt Ihre Sicherheit völlig von dieser einen Stelle ab. Es ist keine besonders umfassende Verteidigung, aber andererseits wissen Sie genau, wo Ihre schwächste Stelle liegt und wie schwach sie ist. Bei mehreren Schichten läßt sich das nicht so genau feststellen.

In der Praxis liegen die Vorteile von Single-Box-Architekturen nicht in ihrer Sicherheit, sondern in anderen praktischen Überlegungen. Verglichen mit mehrschichtigen Systemen, die in Ihr Netzwerk integriert sind, ist eine Single-Box-Architektur preiswerter, leichter verständlich und dem Management besser zu erklären. Außerdem ist der Einkauf eines solchen Systems problemloser zbu bewerkstelligen. Für kleine Standorte stellt sie daher eine gute Lösung dar. Sie ist auch eine attraktive Alternative für Leute, die nach einer magischen Schutzvorrichtung suchen, die sie einmal einbauen und anschließend vergessen können. Es gibt zwar sehr gute Single-Box-Firewalls, aber keine magischen Firewalls. Single-Box-Lösungen erfordern ebenso schwierige Entscheidungen, sorgfältige Konfiguration und weitere Betreuung wie andere Firewalls.

Überwachungsrouter

Es ist möglich, ein Paketfiltersystem allein als Firewall einzusetzen, wie in Abbildung 6-1 zu sehen ist. Dabei wird nur ein *Überwachungsrouter* eingesetzt, um das gesamte Netzwerk zu schützen. Dies ist ein preiswertes System, da Sie sowieso fast immer einen Router benötigen, um die Verbindung zum Internet herzustellen. Sie konfigurieren einfach die Paketfilterung auf diesem Router. Andererseits ist es nicht besonders flexibel; Sie können Protokolle per Port-Nummer erlauben oder verbieten, es ist aber schwierig, bestimmte Operationen zuzulassen, während Sie andere im gleichen Protokoll verbieten, oder sicherzugehen, daß das, was an einem bestimmten Port ankommt, wirklich das

Protokoll ist, das Sie erlauben wollten. Außerdem reicht die Verteidigung nicht besonders weit. Wenn der Router überwunden wird, haben Sie keinen weiteren Schutz.

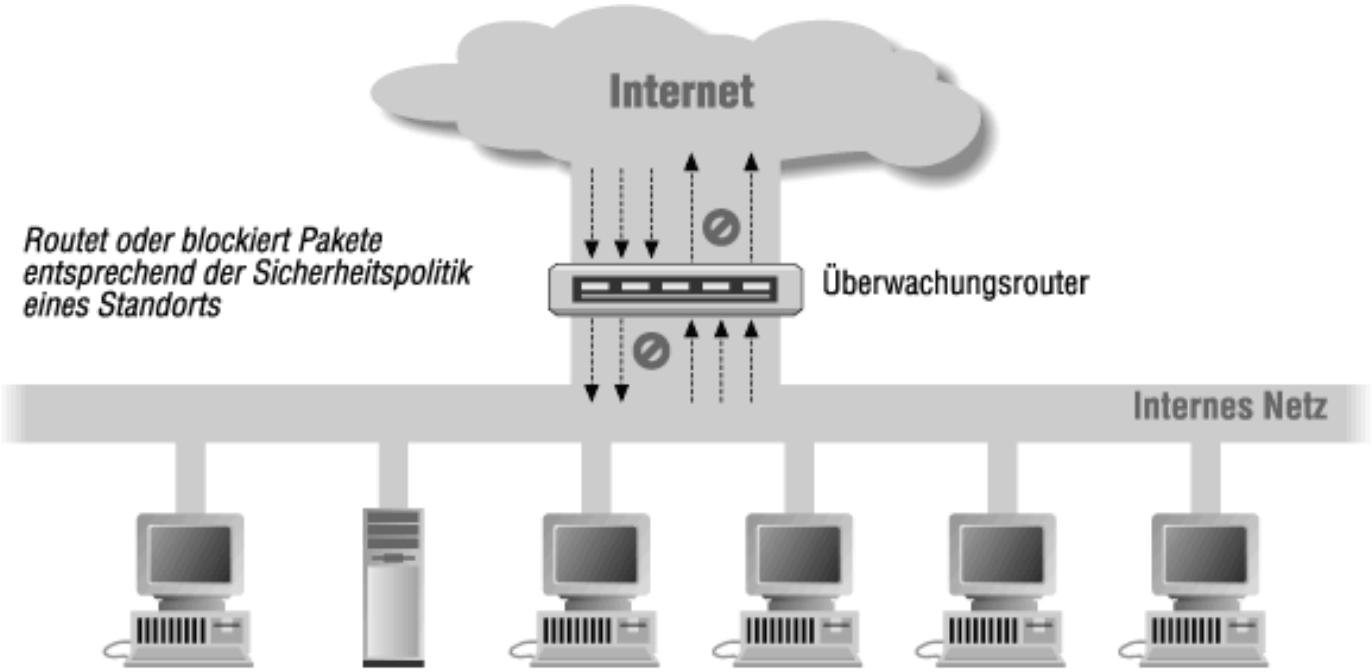

Abbildung 6-1 : Einsatz eines Überwachungsrouters zur Durchführung der Paketfilterung

Geeignete Einsatzmöglichkeiten

Ein Überwachungsrouter ist in solchen Situationen eine geeignete Firewall, in denen:

- das zu schützende Netzwerk bereits über einen sehr hohen Grad an Rechnersicherheit verfügt
- die Anzahl der benutzten Protokolle beschränkt ist, und die Protokolle selbst relativ einfach strukturiert sind
- Sie maximale Leistung und Redundanz fordern

Überwachungsrouter eignen sich am besten für interne Firewalls und für Netzwerke, die dazu gedacht sind, Dienste für das Internet zur Verfügung zu stellen. So ist es zum Beispiel nicht unüblich, daß Internet Service Provider nichts weiter als einen Überwachungsrouter zwischen ihren Hosts und dem Internet einsetzen.

Dual-Homed-Host

Eine *Dual-Homed-Host-Architektur* wird um einen Dual-Homed-Host herum aufgebaut, einen Computer, der mindestens zwei Netzwerkschnittstellen besitzt. Solch ein Host könnte als Router zwischen den Netzwerken auftreten, an die diese Schnittstellen angeschlossen sind; er ist in der Lage, IP-Pakete von einem in das andere Netzwerk weiterzuleiten. Wenn Sie jedoch einen Dual-Homed-Host als Firewall einsetzen, deaktivieren Sie diese Routing-Funktion. Auf diese Weise werden IP-Pakete aus dem einen Netzwerk (z.B. dem Internet) nicht direkt in das andere Netzwerk (z.B. das interne, geschützte Netzwerk) geroutet. Die Systeme innerhalb der Firewall können mit dem Dual-Homed-Host kommunizieren und die Systeme außerhalb der Firewall (im Internet) ebenfalls. Es ist diesen Systemen jedoch nicht möglich, direkt miteinander zu kommunizieren. Der IP-Verkehr zwischen ihnen wird vollständig blockiert.

Manche Varianten der Dual-Homed-Host-Architektur benutzen IP im Internet und ein anderes Netzwerkprotokoll (zum Beispiel NetBEUI) im internen Netzwerk. Dies verstärkt die Trennung zwischen den beiden Netzwerken, wodurch es unwahrscheinlicher wird, daß durch Fehlkonfigurationen Verkehr von einer Schnittstelle auf die andere gelangt. Außerdem verringert sich die Gefahr, daß die Clients verwundbar werden, falls dies doch einmal passiert. Diese Variante hat jedoch keinen besonderen Einfluß auf die Gesamtsicherheit der Firewall.

Die Netzwerkarchitektur für eine Dual-Homed-Host-Firewall ist denkbar einfach: Der Dual-Homed-Host befindet sich zwischen dem Internet und dem internen Netzwerk und ist an beide angeschlossen. Abbildung 6-2 stellt diese Architektur dar.

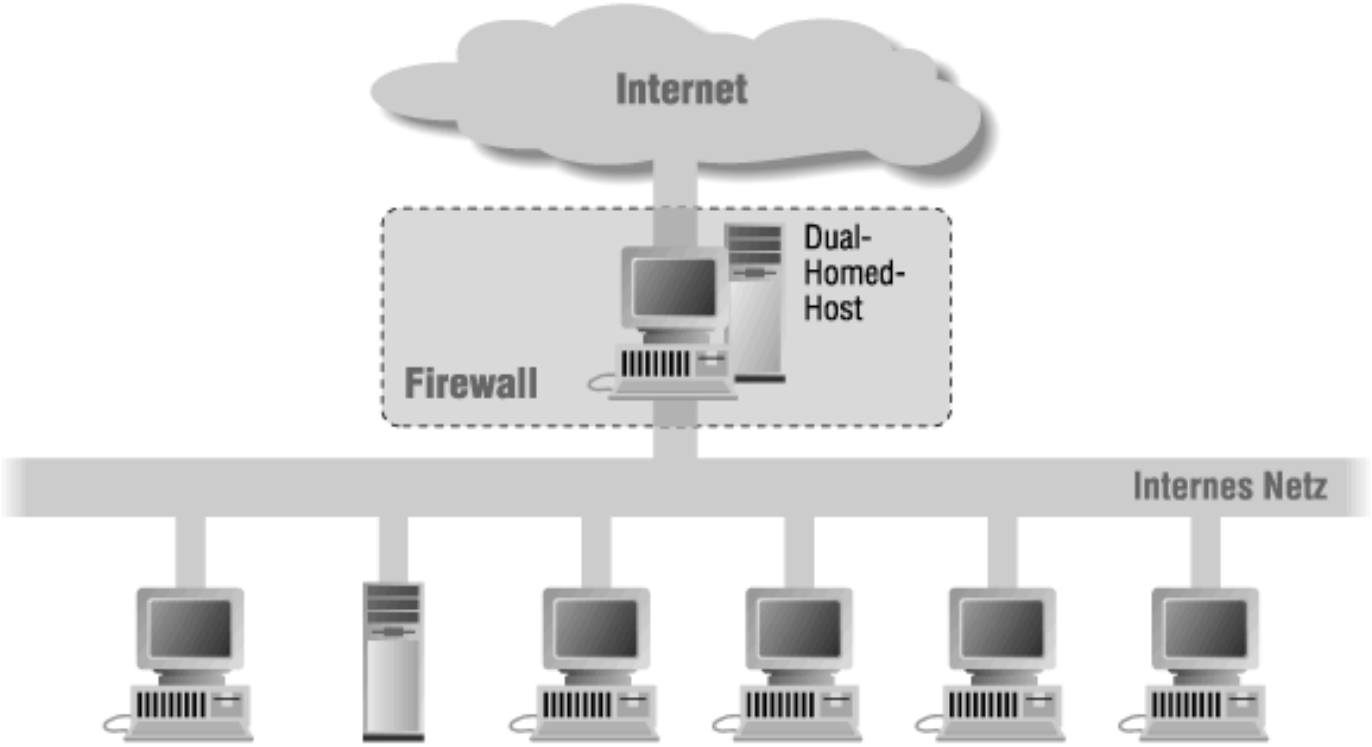

Abbildung 6-2 : Dual-Homed-Host-Architektur

Dual-Homed-Hosts ermöglichen einen sehr hohen Grad an Kontrolle. Wenn Sie überhaupt keine Pakete zwischen dem externen und dem internen Netzwerk zulassen, dann wissen Sie ziemlich genau, daß alle Pakete im internen Netzwerk, die eine externe Quelle aufweisen, auf ein Sicherheitsproblem hinweisen.

Andererseits sind Dual-Homed-Hosts nicht besonders leistungsfähig. Ein Dual-Homed-Host muß bei jeder Verbindung mehr Arbeit erledigen als ein Paketfilter und benötigt entsprechend mehr Ressourcen. Außerdem erlaubt er nicht so viel Verkehr wie ein äquivalentes Paketfiltersystem.

Da ein Dual-Homed-Host einen einzigen Schwachpunkt bildet, ist es wichtig, dafür zu sorgen, daß seine Rechnersicherheit absolut tadellos ist. Ein Angreifer, der es schafft, den Dual-Homed-Host zu überwinden, besitzt vollständigen Zugriff auf Ihren Standort (unabhängig davon, welche Protokolle Sie betreiben). Ein Angreifer, der den Dual-Homed-Host zum Absturz bringt, schneidet Sie vom Internet ab. Dual-Homed-Hosts sind deshalb ungeeignet, wenn es für Ihre Firma unerläßlich ist, ins Internet zu gelangen.

Sie sind besonders anfällig für Probleme mit der IP-Implementierung des Rechners, die die Maschine zum Absturz bringen oder Verkehr durchlassen kann. Diese Probleme gibt es auch bei Paketfilter-Routern, allerdings treten sie nicht so häufig auf und sind normalerweise leichter zu beheben. Architekturen mit mehreren Geräten sind meist weniger empfindlich, da mehrere verschiedene IP-Implementierungen im Spiel sind.

Ein Dual-Homed-Host kann entweder Dienste nur in Form eines Proxy anbieten oder indem sich die Benutzer direkt auf dem Dual-Homed-Host anmelden. Sie werden es sicher vermeiden wollen, daß sich die Benutzer direkt auf dem Rechner einloggen. Wie wir in Kapitel 10, Bastion-Hosts, ausführen, bringen Benutzer-Zugänge selbst schon deutliche Sicherheitsrisiken mit sich. Auf Dual-Homed-Hosts sind sie besonders problematisch, da Benutzer möglicherweise unerwartet Dienste aktivieren, die Sie als unsicher ansehen. Außerdem empfinden es die meisten Benutzer als unbequem, einen Dual-Homed-Host erst benutzen zu können, nachdem sie sich auf ihm angemeldet haben.

Der Betrieb als Proxy ist weit weniger problematisch, steht aber möglicherweise nicht für alle Dienste zur Verfügung, an denen Sie interessiert sind. Kapitel 9, Proxy-Systeme, zeigt Ihnen einige Vorgehensweisen für diese Situation, die sich allerdings nicht für jeden Fall eignen. Wenn Sie einen Dual-Homed-Host als einzige Netzwerkverbindung benutzen, verringern sich einige Probleme mit Proxies ein wenig; wenn der Host vorgibt, ein Router zu sein, kann er Pakete abfangen, die in die Außenwelt gerichtet sind, und sie transparent und ohne fremde Hilfe als Proxy weiterleiten.

Proxies eignen sich besser zur Unterstützung ausgehender (interne Benutzer, die Ressourcen im Internet verwenden) als eingehender Dienste (Benutzer im Internet verwenden Ressourcen im internen Netzwerk). In einer Konfiguration mit einem Dual-Homed-Host müssen Dienste, die Sie für das Internet zur Verfügung stellen wollen, normalerweise auf dem Dual-Homed-Host ausgeführt werden. Das ist nicht immer anzuraten, da es ein gewisses Risiko in sich birgt, Dienste im Internet verfügbar zu machen, und der Dual-Homed-Host eine sicherheitskritische Maschine darstellt, die Sie nicht unnötig durch riskante Dienste gefährden sollten. Es mag akzeptabel sein, einen minimal ausgestatteten Webserver auf einem Dual-Homed-Host zu betreiben (zum Beispiel einen, der zwar HTML-Seiten zur Verfügung stellen kann, aber keine aktiven Inhalte, zusätzlichen Protokolle oder Verarbeitungsmöglichkeiten für Formulare beinhaltet), das Ausführen eines normalen Webservers dagegen wäre dagegen extrem gefährlich.

Bei der Architektur mit überwachtem Teilnetz, die wir in einem späteren Abschnitt beschreiben, besitzen Sie mehr Möglichkeiten für neue, nicht vertrauenswürdige oder eingehende Dienste (zum Beispiel können Sie eine weniger wertvolle Maschine in das überwachte Teilnetz einbinden, auf der Sie nur einen nicht vertrauenswürdigen Dienst zur Verfügung stellen).

Geeignete Einsatzmöglichkeiten

Ein Dual-Homed-Host ist in Situationen eine geeignete Firewall, in denen:

- es nur wenig Verkehr ins Internet gibt
- der Verkehr ins Internet nicht ausschlaggebend für die geschäftliche Tätigkeit ist
- benutzern im Internet keine Dienste zur Verfügung gestellt werden
- das zu schützende Netzwerk keine übermäßig wertvollen Daten enthält

Mehrzweck-Maschinen

Viele Single-Box-Firewalls sind in Wirklichkeit eine Kombination aus Proxy und Paketfilterung. Dadurch ziehen Sie einen Nutzen aus den Vorteilen beider Systeme; Sie können einige Protokolle mit hoher Geschwindigkeit zur Verfügung stellen und behalten dennoch weitgehende Kontrolle. Sie bekommen aber auch die Nachteile beider Systeme zu spüren; Sie werden anfällig gegenüber Problemen, bei denen Protokolle, von denen Sie angenommen haben, daß sie durch die Proxies aufgefangen werden, einfach durch die Paketfilter hindurchgelassen werden. Zusätzlich gehen Sie all die normalen Risiken ein, die daraus resultieren, daß nur ein einziges Element zwischen Ihnen und der großen weiten Welt liegt.

Geeignete Einsatzmöglichkeiten

Eine einzelne Maschine, die sowohl Proxy als auch Paketfilter ist, bietet sich in Situationen an, in denen:

- das zu schützende Netzwerk klein ist
- keine Dienste für das Internet zur Verfügung gestellt werden

Architekturen mit überwachten Hosts

Während eine Dual-Homed-Host-Architektur Dienste auf einem Rechner zur Verfügung stellt, der an mehrere Netzwerke angeschlossen ist (aber mit deaktiviertem Routing), bietet eine *Architektur mit einem überwachten Host*

(engl. screened host architecture) Dienste auf einem Rechner an, der nur an das interne Netzwerk angeschlossen ist und einen separaten Router verwendet. In dieser Architektur wird ein Großteil des Schutzes durch Paketfilterung gewährleistet. (Zum Beispiel ermöglicht Paketfilterung es nicht, die Proxy-Server zu umgehen und direkte Verbindungen aufzubauen.)

Abbildung 6-3 zeigt eine einfache Version einer Architektur mit überwachtem Host. Der Bastion-Host befindet sich im internen Netzwerk. Die Paketfilterung auf dem Überwachungsrouter ist so eingerichtet, daß der Bastion-Host das einzige System im internen Netzwerk ist, zu dem Hosts aus dem Internet Verbindungen aufbauen können (zum Beispiel, um eingehende E-Mails abzuliefern). Selbst in diesem Fall sind nur bestimmte Arten von Verbindungen erlaubt. Jedes externe System, das versucht, auf interne Systeme zuzugreifen, muß eine Verbindung zu diesem Host herstellen. Der Bastion-Host muß daher einen gewissen Grad an Sicherheit gewährleisten.

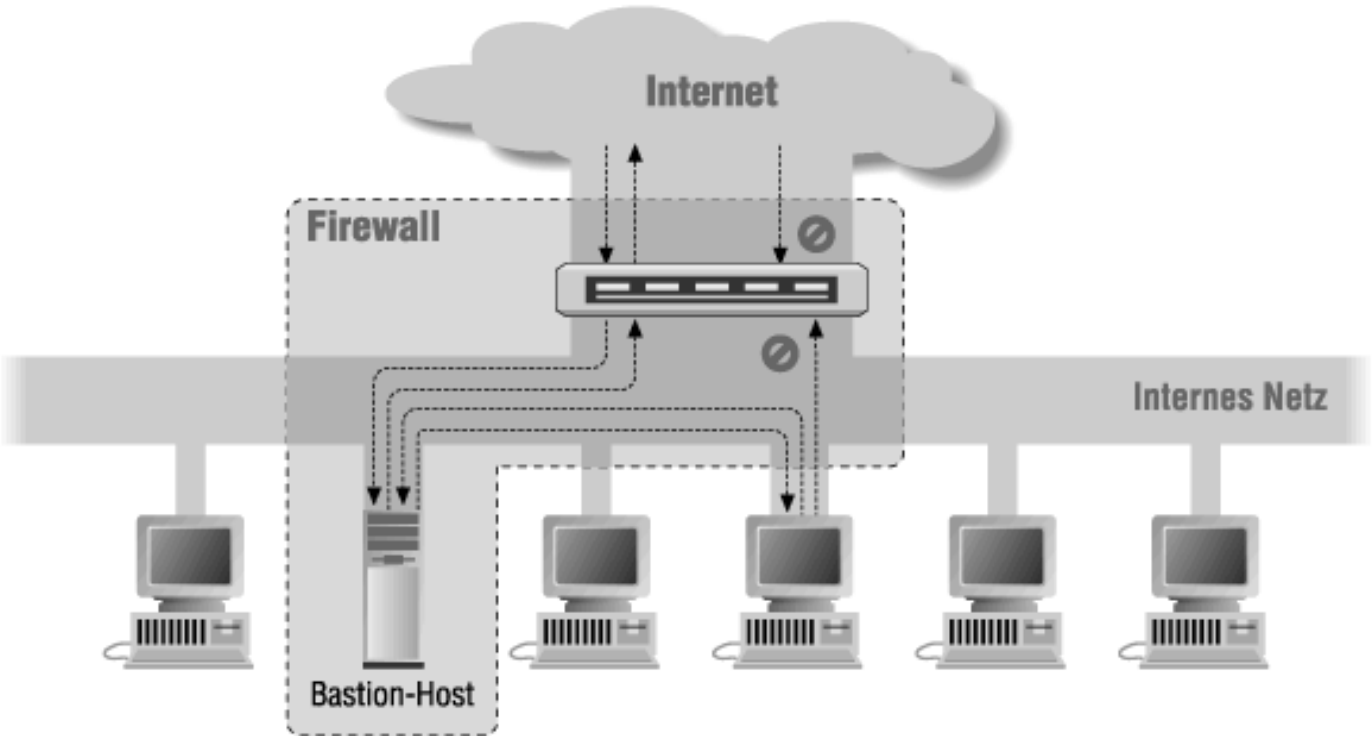

Abbildung 6-3 : Eine Architektur mit überwachtem Host

Die Paketfilterung erlaubt es dem Bastion-Host außerdem, zulässige Verbindungen (was »zulässig« ist, wird durch die Sicherheitspolitik Ihres Standorts bestimmt) in die Außenwelt zu öffnen. Der Abschnitt »Bastion-Host« in der Besprechung der »Architekturen mit überwachtem Teilnetz« weiter hinten in diesem Kapitel enthält mehr Informationen über die Funktionsweise von Bastion-Hosts. Kapitel 10, Bastion-Hosts, beschreibt genau, wie Sie einen Bastion-Host aufbauen können.

Über die Konfiguration der Paketfilterung im Überwachungsrouter kann folgendes erreicht werden:

- Es wird anderen internen Hosts erlaubt, Verbindungen zu Rechnern im Internet zu öffnen, um auf bestimmte Dienste zuzugreifen (wie diese Dienste über Paketfilterung zugelassen werden, erfahren Sie in Kapitel 8, Paketfilterung).
- Es werden alle Verbindungen von internen Hosts verboten (wodurch die Hosts gezwungen werden, die Proxy-Dienste über den Bastion-Host in Anspruch zu nehmen, wie in Kapitel 9, Proxy-Systeme, beschrieben).

Sie können diese Ansätze für verschiedene Dienste mischen; einige könnten direkt über Paketfilter erlaubt sein, während andere nur indirekt über einen Proxy möglich sind. Das hängt allein von der Sicherheitspolitik ab, die Sie an Ihrem Standort etablieren wollen.

Da diese Architektur es Paketen erlaubt, vom Internet aus in die internen Netzwerke zu gelangen, scheint sie riskanter

zu sein als eine Dual-Homed-Host-Architektur, die so gestaltet ist, daß externe Pakete nicht in das interne Netzwerk gelangen können. In der Praxis neigt jedoch die Dual-Homed-Host-Architektur dazu, fehlerhaft zu arbeiten und Pakete aus dem externen in ein internes Netzwerk durchzulassen. (Da diese Sorte Fehler vollkommen unerwartet auftritt, gibt es kaum Schutz vor Angriffen dieser Art.) Es ist außerdem einfacher, einen Router zu verteidigen als einen Host. Für die meisten Anwendungsfälle bietet die Architektur mit überwachtem Host sowohl einen besseren Schutz als auch eine bessere Benutzbarkeit als die Architektur mit Dual-Homed-Host.

Verglichen mit anderen Architekturen wie etwa der Architektur mit überwachtem Teilnetz, bringt die Architektur mit überwachtem Host einige Nachteile mit sich. Der Hauptnachteil besteht darin, daß kein Schutz mehr zwischen dem Bastion-Host und den restlichen internen Hosts vorhanden ist, wenn es ein Angreifer schafft, in den Bastion-Host einzubrechen. Der Router bildet ebenfalls eine Schwachstelle. Wenn er überwunden wird, steht einem Angreifer das gesamte Netzwerk offen. Aus diesem Grund hat die Architektur mit überwachtem Teilnetz, der wir uns als nächstes zuwenden, an Popularität gewonnen.

Da der Bastion-Host den entscheidenden Schwachpunkt darstellt, ist er nicht für den Betrieb stark risikobehafteter Dienste, wie Webserver, geeignet. Sie müssen den gleichen Grad an Sicherheit zur Verfügung stellen, den Sie auch für einen Dual-Homed-Host aufbringen würden, der die einzige Firewall für Ihren Standort wäre.

Geeignete Einsatzmöglichkeiten

Eine Architektur mit überwachtem Host ist geeignet, wenn:

- nur wenige Verbindungen aus dem Internet ankommen (daher ist diese Architektur vor allem dann nicht geeignet, wenn der überwachte Host ein öffentlicher Webserver ist)
- das zu überwachende Netzwerk einen relativ hohen Grad an Rechnersicherheit bietet

Architekturen mit überwachtem Teilnetz

Die *Architektur mit überwachtem Teilnetz* (engl. screened subnet architecture) erweitert die Architektur mit überwachtem Host um eine weitere Schutzschicht, indem sie ein Grenznetzwerk hinzufügt, durch welches das interne Netzwerk weiter vom Internet isoliert wird.

Wozu? Entsprechend ihrer Natur sind die Bastion-Hosts die verwundbarsten Maschinen in Ihrem Netzwerk. Egal, wie sehr Sie sich anstrengen, bei diesen Maschinen ist die Wahrscheinlichkeit, daß sie angegriffen werden, am größten, da es die Maschinen sind, die angegriffen werden *können*. Wenn Ihr Netzwerk, wie dies in einer Architektur mit überwachtem Host der Fall ist, für einen Angriff von Ihrem Bastion-Host aus weit offensteht, dann ist Ihr Bastion-Host ein ausgesprochen lohnendes Ziel. Zwischen diesem Rechner und Ihren internen Maschinen gibt es keine weiteren Verteidigungsanlagen (neben den Maßnahmen zur Rechnersicherheit, die normalerweise relativ gering ausfallen). Ein Einbrecher, der erfolgreich in den Bastion-Host einer Architektur mit überwachtem Host einbricht, hat quasi den Hauptgewinn gezogen. Durch die Isolierung des Bastion-Hosts in einem Grenznetzwerk können Sie die Auswirkungen eines Einbruchs in den Bastion-Host abschwächen. Er bildet nicht mehr den sofortigen Hauptgewinn; der Eindringling kann zwar immer noch bis zu einem gewissen Grad auf Ihre Technik zugreifen, er besitzt aber keinen völligen Zugang mehr.

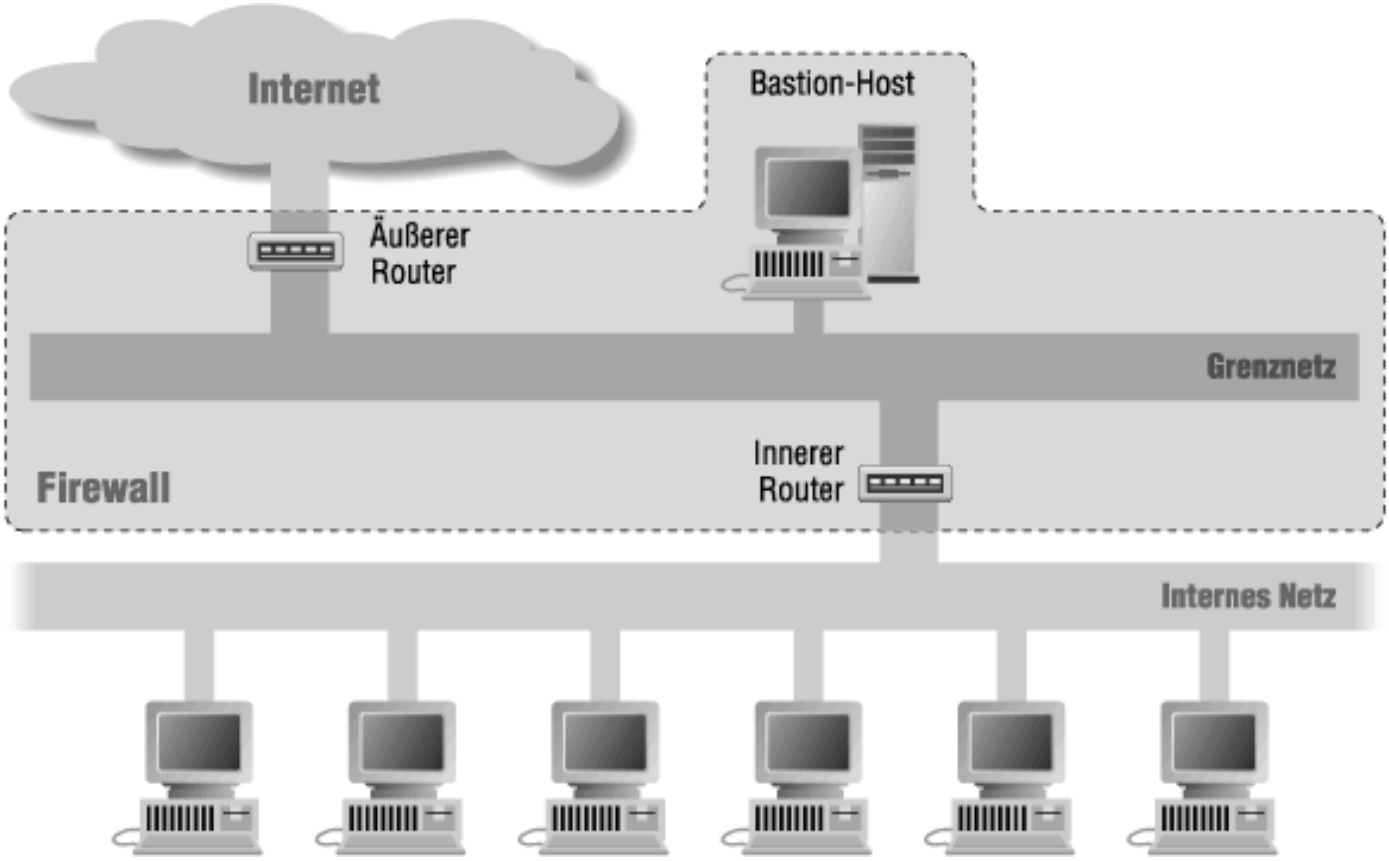

Abbildung 6-4 : Architektur mit überwachtem Teilnetz (mit zwei Routern)

Bei der einfachsten Variante der Architektur mit überwachtem Teilnetz gibt es zwei Überwachungsrouter, die jeweils an das Grenznetz angeschlossen sind. Einer befindet sich zwischen dem Grenznetz und dem internen Netzwerk, der andere sitzt zwischen dem Grenznetz und dem externen Netz (üblicherweise ist dies das Internet). Um bei dieser Architektur in das interne Netzwerk eindringen zu können, muß der Angreifer erst *beide* Router überwinden. Selbst wenn es ein Angreifer irgendwie in den Bastion-Host schafft, muß er dann noch den inneren Router knacken. Es gibt jetzt nicht mehr die eine verwundbare Stelle, die das interne Netzwerk gefährdet.

Abbildung 6-4 zeigt eine mögliche Firewall-Konfiguration, die eine Architektur mit überwachtem Teilnetz einsetzt. Die nächsten Abschnitte beschreiben die Bestandteile dieser Art von Architektur.

Das Grenznetzwerk

Das Grenznetz ist eine weitere Schutzschicht, ein zusätzliches Netzwerk zwischen dem externen Netz und Ihrem geschützten internen Netz. Wenn ein Angreifer erfolgreich in den äußeren Bereich Ihrer Firewall eindringt, stellt das Grenznetz ein weiteres Hindernis zwischen dem Angreifer und Ihren internen Systemen dar.

Das folgende Beispiel verdeutlicht, weshalb ein Grenznetzwerk hilfreich sein kann. In vielen Netzwerken ist es möglich, daß eine Maschine den Verkehr aller anderen Maschinen im gleichen Netzwerk sehen kann. Dies gilt für die meisten Ethernet-basierten Netze (und die Ethernet-Technik ist heutzutage im Bereich der lokalen Netzwerke mit Abstand am weitesten verbreitet); dies gilt aber auch für verschiedene andere beliebte Techniken wie Token-Ring und FDDI. Schnüffler könnten durchaus Paßwörter aufschnappen, indem sie in laufenden Telnet-, FTP- und *rlogin*-Sitzungen danach suchen. Doch selbst wenn keine Paßwörter bekanntwerden, könnten sie den Inhalt geheimer Dateien, interessanter E-Mails oder ähnlicher Dinge mitbekommen, auf die zugegriffen wird. Der Schnüffler könnte praktisch jeder Person im Netzwerk »über die Schulter blicken«. Es gibt eine Menge Werkzeuge, die Angreifer für diese Art von Schnüffelei sowie für das Verwischen ihrer Spuren einsetzen können.

Bei einem Grenznetzwerk stellt sich die Lage etwas anders dar: Wenn jemand in einen Bastion-Host in einem Grenznetz einbricht, kann er nur den Verkehr in diesem Netz abhören. Der ganze Verkehr im Grenznetz muß entweder

zum oder vom Bastion-Host oder zum oder vom Internet verlaufen. Da kein rein interner Verkehr (das ist Verkehr zwischen zwei internen Hosts, der wahrscheinlich geheim oder zumindest nicht für die Außenwelt bestimmt ist) das Grenznetz passiert, ist dieser interne Verkehr vor neugierigen Augen geschützt, falls in den Bastion-Host eingebrochen wird.

Augenscheinlich wird der Verkehr zum oder vom Bastion-Host oder mit der äußeren Welt immer noch sichtbar sein. Beim Aufbau einer Firewall gilt es sicherzustellen, daß dieser Verkehr selbst nicht so vertraulich ist, daß sofort Ihr ganzer Standort gefährdet ist, wenn er gelesen wird.

Bastion-Host

Bei der Architektur mit überwachtem Teilnetz verbinden Sie einen Bastion-Host (oder mehrere Hosts) mit dem Grenznetz. Dieser Host bildet die Hauptkontaktstelle für eingehende Verbindungen aus der Außenwelt, zum Beispiel:

- für eingehende E-Mail- (SMTP) Sitzungen zum Ausliefern elektronischer Post an diesen Standort
- für eingehende FTP-Verbindungen an den anonymen FTP-Server des Standorts
- für eingehende Anfragen Ihres Standortes an das Domain Name System (DNS)

und so weiter.

Für die Behandlung nach außen gerichteter Dienste (von internen Clients an Server im Internet) gibt es folgende Möglichkeiten:

- Einrichtung von Paketfiltern sowohl auf den inneren als auch auf den äußeren Routern, um es den internen Clients zu erlauben, direkt auf externe Server zuzugreifen.
- Einrichtung von Proxy-Servern auf dem Bastion-Host (falls Ihre Firewall Proxy-Software einsetzt), um es den internen Clients zu erlauben, indirekt auf externe Server zuzugreifen. Sie sollten auch Paketfilter einrichten, um es den internen Clients zu ermöglichen, mit den Proxy-Servern auf dem Bastion-Host zu kommunizieren und umgekehrt, direkte Kommunikation zwischen den internen Clients und der Außenwelt jedoch zu verbieten.

In jedem Fall erlaubt es die Paketfilterung dem Bastion-Host, Verbindungen zu Rechnern im Internet aufzubauen und von ihnen kommende Verbindungen zu akzeptieren; um welche Hosts und Dienste es sich handelt, hängt von der Sicherheitspolitik des Standorts ab.

Ein Großteil der Arbeit des Bastion-Host besteht darin, als Proxy-Server für verschiedene Dienste zu fungieren. Dazu wird entweder besondere Proxy-Server-Software für bestimmte Protokolle ausgeführt (wie etwa HTTP oder FTP), oder es werden Standard-Server für Protokolle eingesetzt, die selbst Proxy-Dienste beinhalten (wie SMTP).

Kapitel 10, Bastion-Hosts, beschreibt, wie Sie einen Bastion-Host sichern, und die Kapitel in Teil III, Internet-Dienste, zeigen, wie Sie einzelne Dienste für den Betrieb mit einer Firewall konfigurieren.

Der innere Router

Der *innere Router* (in der Firewall-Literatur manchmal auch als *Choke-Router* bezeichnet) schützt das interne Netzwerk sowohl vor dem Internet als auch vor dem Grenznetzwerk.

Dieser innere Router erledigt für Ihre Firewall den größten Teil der Paketfilterung. Er erlaubt es ausgewählten Diensten, vom internen Netz ins Internet zu gelangen. Dabei handelt es sich um die Dienste, die Ihr Standort sicher unterstützen und unter Zuhilfenahme von Paketfiltern anstelle von Proxies sicher anbieten kann. (Sie müssen für Ihren Standort selbst definieren, was »sicher« ist. Dazu müssen Sie Ihre eigenen Ansprüche, Fähigkeiten und Beschränkungen berücksichtigen; es gibt keine allgemeingültige Antwort.) Zu den Diensten, die Sie erlauben, können

ausgehende HTTP-, Telnet-, FTP- sowie weitere Dienste gehören, je nachdem, welche Bedürfnisse und Umstände Sie leiten. (Ausführliche Informationen darüber, wie Sie die Paketfilterung einsetzen können, um diese Dienste zu kontrollieren, finden Sie in Kapitel 8, Paketfilterung.)

Die Dienste, die der innere Router zwischen Ihrem Bastion-Host (im Grenznetz) und Ihrem internen Netzwerk zuläßt, sind nicht unbedingt die gleichen Dienste, die er zwischen dem Internet und Ihrem internen Netz erlaubt. Die Ursache für die Beschränkung der Dienste zwischen dem Bastion-Host und dem internen Netz besteht in der Reduzierung der Anzahl der Maschinen (und der Anzahl der Dienste auf diesen Maschinen), die von dem Bastion-Host angegriffen werden können, falls er eingenommen wird.

Sie sollten sich zwischen dem Bastion-Host und dem internen Netzwerk auf die Dienste beschränken, die wirklich benötigt werden, wie etwa SMTP (damit der Bastion-Host ankommende E-Mails weiterleiten kann), DNS (damit der Bastion-Host je nach Art Ihrer Konfiguration Anfragen von internen Maschinen beantworten oder welche an sie weiterleiten kann) und so weiter. Sie sollten die Dienste außerdem so weit wie möglich einschränken, indem Sie sie nur von oder zu bestimmten internen Hosts zulassen; zum Beispiel könnte sich SMTP auf Verbindungen zwischen dem Bastion-Host und Ihrem (bzw. Ihren) internen Mailserver (bzw. -servern) beschränken. Richten Sie Ihre Aufmerksamkeit besonders auf die Sicherheit dieser verbleibenden internen Hosts und Dienste, die durch den Bastion-Host kontaktiert werden können, da es genau solche Hosts und Dienste sind, nach denen Angreifer suchen, wenn sie es schaffen, in Ihren Bastion-Host einzubrechen.

Der äußere Router

Theoretisch schützt der *äußere Router* (in der Firewall-Literatur manchmal auch *Access- oder Zugangs-Router* genannt) sowohl das Grenznetz als auch das interne Netz vor dem Internet. In der Praxis neigen jedoch äußere Router dazu, fast alles, was aus dem Grenznetz nach außen gerichtet ist, hindurchzulassen. Außerdem führen sie im allgemeinen kaum eine Paketfilterung durch. Die Paketfilterregeln zum Schutz der internen Maschinen müßten im Prinzip auf dem inneren und dem äußeren Router gleich sein; wenn in den Regeln ein Fehler auftreten würde, der einem Angreifer den Zugriff ermöglichte, wäre der Fehler wahrscheinlich auf beiden Routern vorhanden.

Häufig wird der äußere Router von einer externen Einrichtung (zum Beispiel Ihrem Internet Provider) bereitgestellt, und Ihr Zugriff darauf ist beschränkt. Eine externe Einrichtung, die den Router betreut, wird möglicherweise einige allgemeine Paketfilterregeln einstellen, aber keine komplizierte oder sich häufig ändernde Regelmenge verwenden wollen. Sie vertrauen ihnen vielleicht auch nicht so stark, wie Sie Ihren eigenen Routern vertrauen. Werden sie daran denken, alle Filter wieder zu installieren, wenn der Router kaputtgeht und sie einen neuen installieren müssen? Würde man sich die Mühe machen, Ihnen mitzuteilen, daß sich der Router geändert hat, damit Sie wieder alles überprüfen können?

Die einzigen wirklich eigenen Paketfilterregeln auf einem äußeren Router sind die Regeln, die die Maschinen im Grenznetzwerk schützen (also den Bastion-Host und den internen Router). Im allgemeinen ist jedoch kein besonderer Schutz notwendig, da die Hosts im Grenznetz vor allem durch die Rechnersicherheit geschützt werden (obwohl Redundanz nie schadet).

Die restlichen Regeln, die Sie auf dem äußeren Router einstellen, sind Kopien der Regeln auf dem inneren Router. Sie sollen verhindern, daß unsicherer Verkehr von den internen Hosts zum Internet verläuft. Zur Unterstützung von Proxy-Diensten, bei denen der innere Router es den internen Hosts erlaubt, Protokolle unter der Bedingung zu verschicken, daß sie mit dem Bastion-Host kommunizieren, könnte der äußere Router diese Protokolle hindurchlassen, solange sie *vom* Bastion-Host kommen. Diese Regeln liefern zusätzliche Sicherheit, allerdings blockieren sie theoretisch nur Pakete, die eigentlich gar nicht existieren können, da sie bereits vom inneren Router blockiert wurden. Wenn sie existieren, hat entweder der innere Router versagt oder jemand einen nicht vorgesehenen Host an das Grenznetz angeschlossen.

Was muß also der äußere Router wirklich tun? Eine der Sicherheitsaufgaben, die der äußere Router gut ausführen kann - eine Aufgabe, die normalerweise von niemandem sonst erledigt werden kann - ist das Blockieren aller aus dem Internet eingehenden Pakete, die gefälschte Quelladressen haben. Solche Pakete geben vor, aus dem internen

Netzwerk zu stammen, kommen aber in Wirklichkeit aus dem Internet.

Der innere Router könnte diese Aufgabe übernehmen. Allerdings ist er nicht in der Lage festzustellen, ob Pakete, die vorgeben, aus dem Grenznetz zu kommen, gefälscht sind. Im Grenznetz befindet sich zwar nichts, dem man vollständig vertrauen kann, allerdings ist es immer noch vertrauenswürdiger als der Rest der Außenwelt; wenn ein Angreifer in der Lage ist, Pakete aus dem Grenznetz zu fälschen, ist er fast genauso weit, als hätte er den Bastion-Host in seiner Gewalt. Der äußere Router befindet sich an einer deutlicheren Grenze. Der innere Router kann die Systeme im Grenznetz auch nicht vor gefälschten Paketen schützen. (Wir befassen uns in Kapitel 4, Pakete und Protokolle, näher mit gefälschten Paketen.)

Eine weitere Aufgabe, die der äußere Router ausführen kann, besteht darin, IP-Pakete am Verlassen des Netzwerks zu hindern, die keine passenden Quelladressen besitzen. Der gesamte Verkehr, der Ihr Netzwerk verläßt, muß von einer Ihrer Quelladressen stammen. Ist dies nicht der Fall, haben Sie entweder ein ernsthaftes Konfigurationsproblem, oder jemand fälscht Quelladressen.

Die Filterung falscher ausgehender Quelladressen erhöht zwar nicht den Schutz und die Sicherheit Ihres Netzwerks; sie verhindert jedoch, daß ein Eindringling Ihre Systeme benutzt, um bestimmte Arten von Angriffen auf andere Standorte zu starten. Wenn der äußere Router Sie alarmiert, sobald gefälschte Quelladressen bemerkt werden, sollten Sie dies gleichzeitig als Hinweis auffassen, nach ernsten Netzwerkproblemen zu suchen. Es reicht vermutlich schon, einen Ruf als gutes Mitglied der Netzgemeinde zu genießen, um den Namen Ihres Standorts aus negativen Schlagzeilen herauszuhalten.

Geeignete Einsatzmöglichkeiten

Eine Architektur mit überwachtem Teilnetz eignet sich für fast alle Anwendungen.

Architekturen mit mehreren überwachten Teilnetzen

Manche Netzwerke benötigen mehr als ein überwachtes Teilnetz. Dieser Fall tritt ein, wenn mehrere Dinge in einem überwachten Teilnetz geschehen sollen, die unterschiedliche Sicherheitsanforderungen stellen.

Geteiltes überwachtes Teilnetz

In einem *geteilten überwachten Teilnetz* (engl. split-screened subnet) gibt es ebenfalls einen inneren und einen äußeren Router, zwischen den beiden Routern befinden sich jedoch mehrere Netzwerke. Im allgemeinen werden die überwachten Netzwerke miteinander über einen oder mehrere Dual-Homed-Hosts und nicht über einen weiteren Router verbunden.

An einigen Standorten wird diese Architektur hauptsächlich dazu verwendet, eine tiefergehende Verteidigung zu realisieren, bei der ein Proxy-Host durch die Router geschützt wird. Die Router bieten Schutz vor Fälschungen sowie vor Fehlern, bei denen der Dual-Homed-Host beginnt, den Verkehr zu routen. Der Dual-Homed-Host ermöglicht eine feinere Kontrolle über die Verbindungen als die Paketfilterung. Er ist praktisch eine Firewall mit Netz und doppeltem Boden, die ausgezeichneten mehrschichtigen Schutz bietet. Sie erfordert allerdings eine sorgfältige Konfiguration des Dual-Homed-Host, um sicherzugehen, daß Sie wirklich alle Möglichkeiten ausnutzen. (Es hat keinen Zweck, einfache Proxies zu verwenden, die die Anfragen einfach nur weiterleiten.) Abbildung 6-5 zeigt diese Konfiguration.

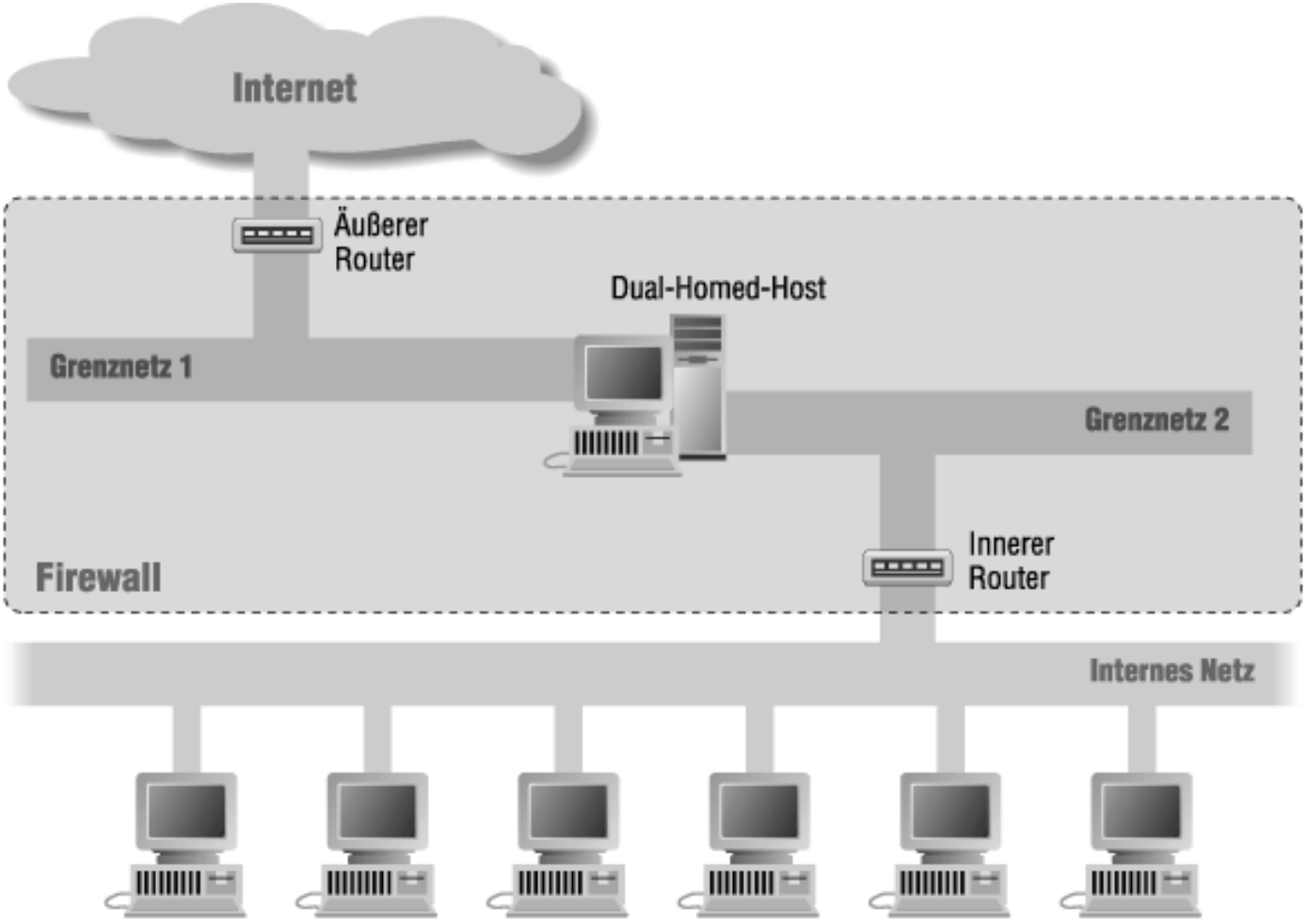

Abbildung 6-5 : Geteiltes überwachtes Teilnetz mit Dual-Homed-Host

Andere setzen diese Architektur ein, um den administrativen Zugang zu Maschinen zu gewährleisten, auf denen außerdem Dienste für das Internet ausgeführt werden. Auf diese Weise können die Administratoren Protokolle verwenden, die zu gefährlich sind, um sie auf einer empfindlichen Maschine im Internet zu erlauben (zum Beispiel die NT-eigenen Protokolle für die entfernte Benutzung des Benutzer-Managers und des Systemmonitors), ohne völlig vom Schutz durch den äußeren Router abzuhängen. Diese Architektur kann auch aus Performance-Gründen für Maschinen nützlich sein, die intensiv das Netzwerk benutzen; so belegt der administrative Verkehr keine Bandbreite, die für die Beantwortung von Benutzeranfragen eingesetzt werden könnte. Abbildung 6-6 zeigt diese Art von Architektur.

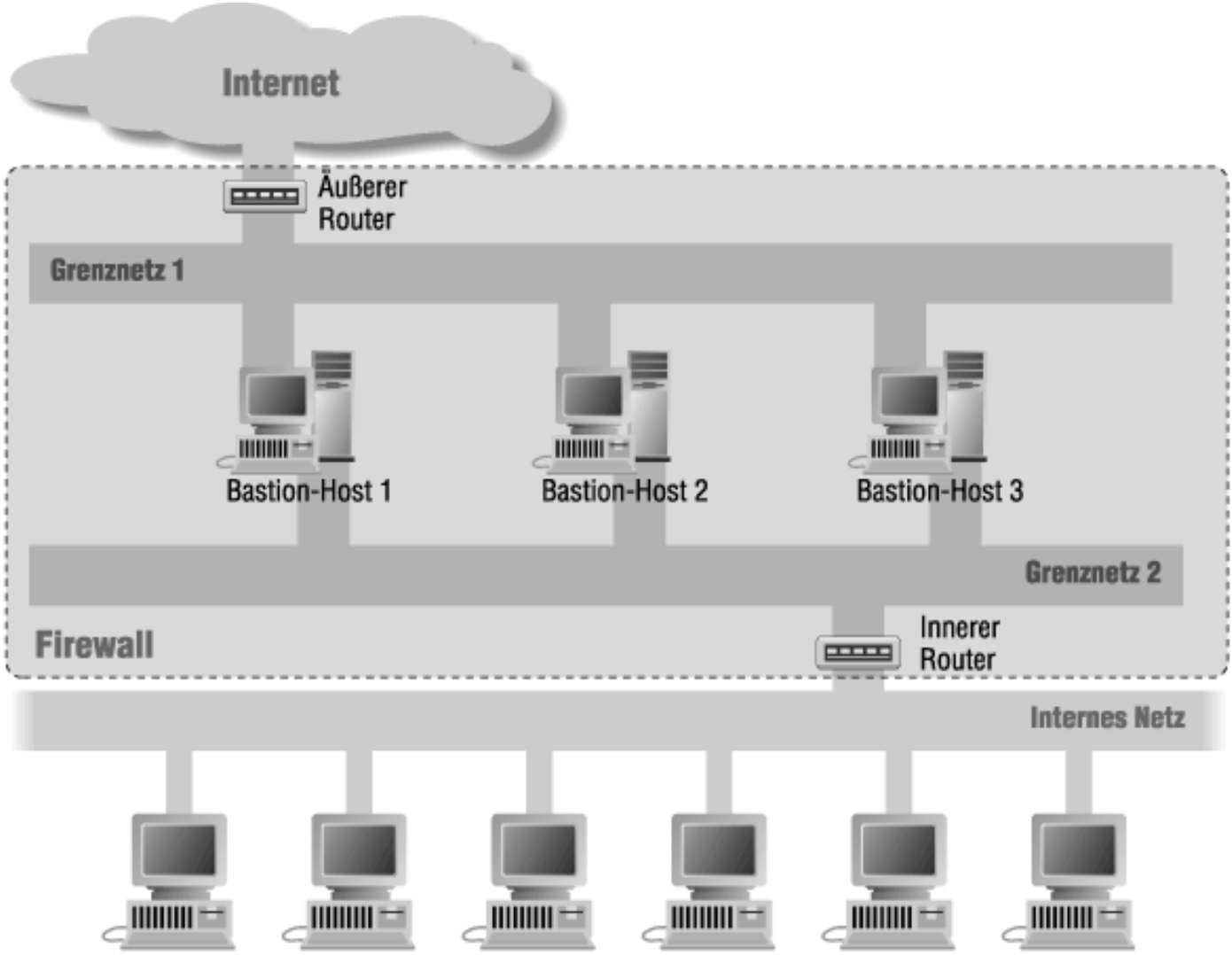

Abbildung 6-6 : Geteiltes überwachtes Teilnetz ohne Durchgangsverkehr

Maschinen, die in der Lage sind, schnelle Netzwerkschnittstellen mit maximaler Geschwindigkeit zu bedienen, können sogar einen Vorteil aus dem Vorhandensein dreier Netzwerkschnittstellen ziehen; die erste dient zur Kommunikation mit externen Benutzern, die zweite zur Kommunikation mit den internen Administratoren und die dritte, die keine Verbindungen zu anderen Netzwerken besitzt, für Backups und/oder zur Kommunikation zwischen den Bastion-Hosts. In Abbildung 6-8 wird eine solche Architektur dargestellt.

Geeignete Einsatzmöglichkeiten

Geteilte überwachte Teilnetze eignen sich für Netzwerke, die eine hohe Sicherheit erfordern, vor allem, wenn sie Dienste für das Internet zur Verfügung stellen.

Unabhängige überwachte Teilnetze

In manchen Fällen werden Sie mehrere *unabhängige überwachte Teilnetze* (engl. independent screened subnets) mit getrennten äußeren Routern benötigen. Abbildung 6-7 zeigt diese Konfiguration.

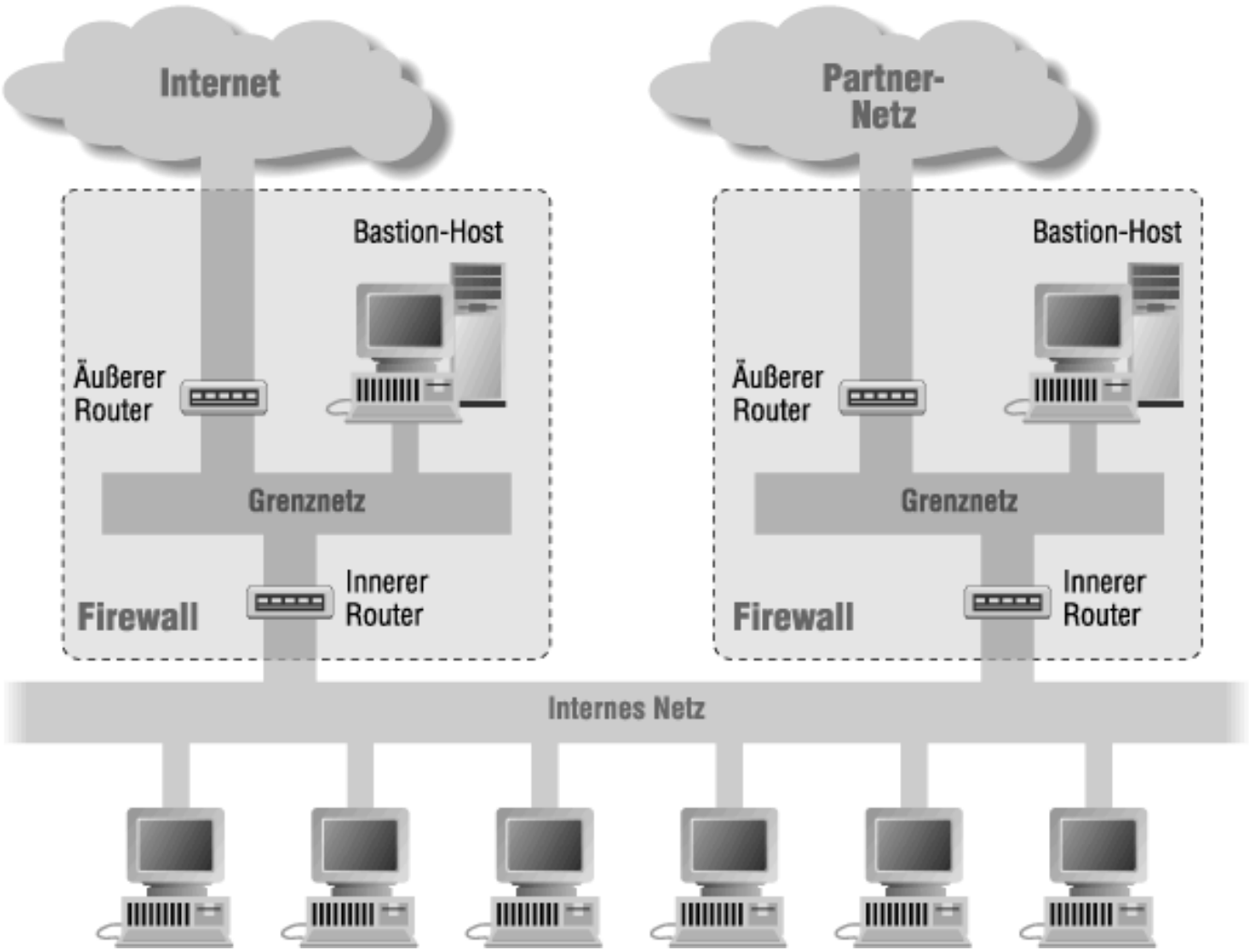

Abbildung 6-7 : Architektur mit mehreren Grenznetzen (mehrere Firewalls)

Sie könnten mehrere Grenznetze einsetzen, um eine gewisse Redundanz zu erzielen. Es ist nicht sehr sinnvoll, für zwei Internet-Verbindungen zu bezahlen und sie dann beide durch den oder die gleichen Router zu betreiben. Wenn Sie zwei äußere Router, zwei Grenznetze und zwei innere Router verwenden, können Sie sicher sein, daß keine einzelne entscheidende Schwachstelle zwischen Ihnen und dem Internet existiert.Fußnoten 1

Auch aus Gründen der Geheimhaltung könnten Sie mehrere Grenznetze verwenden. Auf diese Weise sind Sie in der Lage, Daten, die »ein bißchen« vertraulich sind, über das eine Netzwerk zu schicken und über das andere Netzwerk eine Internet-Verbindung zu betreiben. In diesem Fall könnten Sie sogar beide Grenznetze an den gleichen inneren Router anschließen.

Möglicherweise wollen Sie ja mehrere Grenznetze einsetzen, um die nach innen gerichteten Dienste (Dienste, die Sie im Internet zur Verfügung stellen, wie öffentliche Webserver) von den nach außen gerichteten Diensten (Dienste, die es Ihren Benutzern erlauben, ins Internet zu gelangen, wie etwa ein Web-Proxy) zu trennen. Es ist bedeutend einfacher, für diese Funktionen einen starken Schutz zu gewährleisten, wenn Sie sie trennen und ein getrenntes Grenznetz für die eingehenden Dienste verwenden.

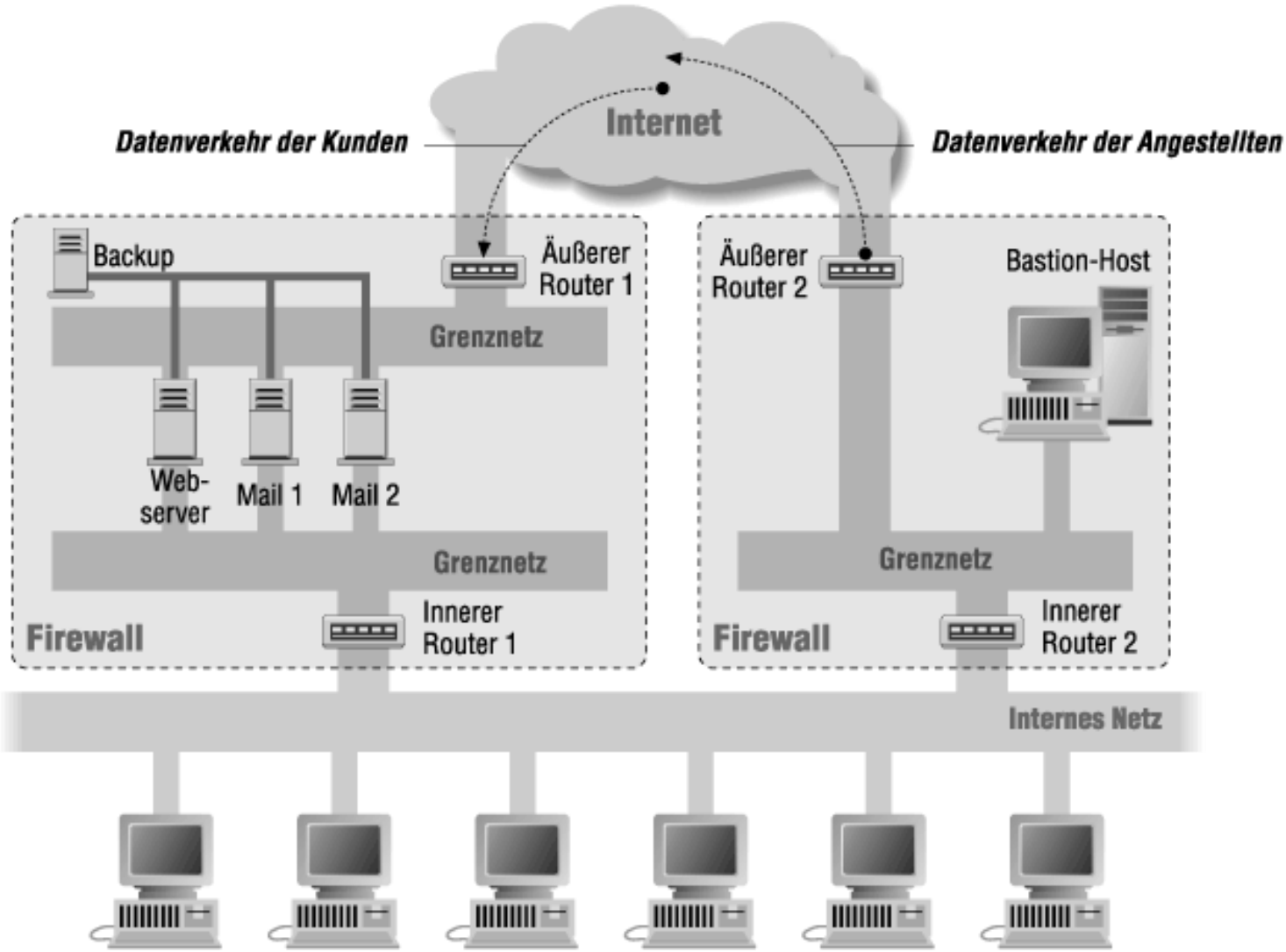

Abbildung 6-8 : Eine komplexe Firewall-Struktur

Der Betrieb mehrerer Grenznetze ist weniger riskant als der Betrieb mehrerer Router, die sich das gleiche interne Netzwerk teilen. Allerdings bleibt die Wartung eine schwierige Aufgabe. Sie werden wahrscheinlich mehrere innere Router haben, die mehrere mögliche Angriffspunkte repräsentieren. Diese Router müssen sehr sorgfältig überwacht werden, damit sie die passenden Sicherheitsrichtlinien verfolgen; werden beide an das Internet angeschlossen, müssen sie die gleiche Sicherheitspolitik geltend machen. Abbildung 6-8 zeigt die Art von Firewall, die ein Internet Service Provider benutzen könnte, mit vielen Grenznetzen und mehreren Verbindungen ins Internet.

Geeignete Einsatzmöglichkeiten

Unabhängige überwachte Teilnetze eignen sich für Netzwerke, die einen besonders hohen Grad an Redundanz benötigen oder die hohe Sicherheitsanforderungen stellen und verschiedene unabhängige Internet-Zugänge brauchen.

Variationen von Firewall-Architekturen

In den Abbildungen 6-2 bis 6-8 haben wir die gebräuchlichsten Firewall-Architekturen dargestellt. Es gibt jedoch eine Vielzahl von Variationen dieser Architekturen. Sie haben viele Möglichkeiten, die Komponenten der Firewall entsprechend Ihrer Hardware, Ihres Budgets und Ihrer Sicherheitspolitik zu konfigurieren und zu kombinieren. Dieser Abschnitt beschreibt einige verbreitete Varianten und deren Vor- und Nachteile.

Es ist O.K., mehrere Bastion-Hosts zu verwenden

Auch wenn wir in diesem Buch immer nur über einen einzelnen Bastion-Host reden, kann es doch manchmal sinnvoll sein, mehrere Bastion-Hosts in Ihrer Firewall-Konfiguration einzusetzen, wenn Sie zum Beispiel die Leistung steigern, Redundanz schaffen oder Daten bzw. Server trennen wollen. Abbildung 6-9 zeigt eine solche Architektur.

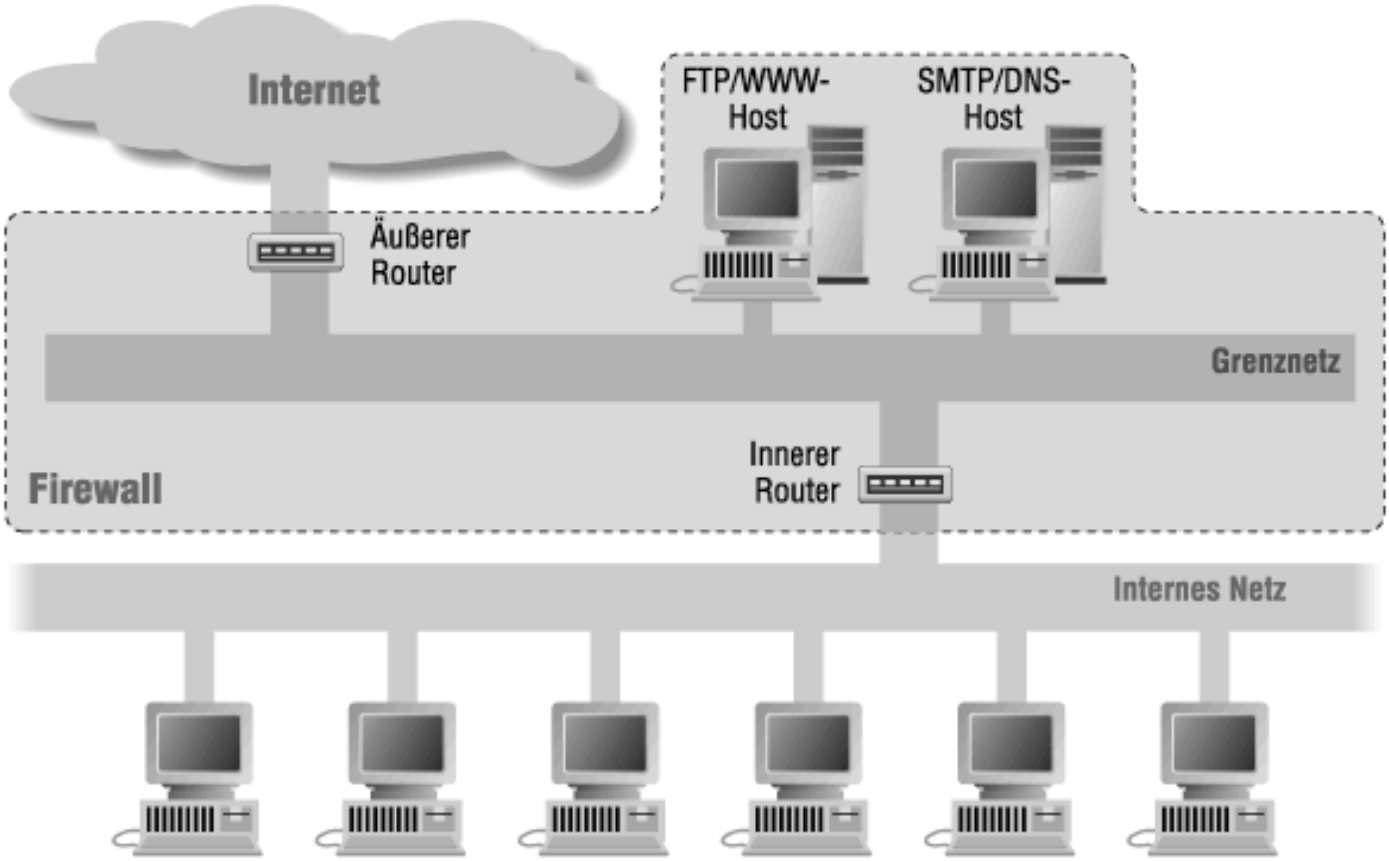

Abbildung 6-9 : Architektur mit zwei Bastion-Hosts

Einer der Bastion-Hosts könnte die Dienste verwalten, die für Ihre eigenen Benutzer wichtig sind (wie SMTP-Server, Proxy-Server usw.), während der andere die Dienste verwaltet, die Sie im Internet bereitstellen, die aber Ihre Benutzer nicht kümmern (zum Beispiel Ihr öffentlicher Webserver). Auf diese Weise verschlechtert sich durch die Aktivitäten der externen Anwender nicht die Leistung für Ihre eigenen Benutzer.

Leistungsanforderungen können auch dann der Grund für den Einsatz mehrerer Bastion-Hosts sein, wenn Sie keine Dienste im Internet zur Verfügung stellen. Manche Dienste, wie etwa Usenet-News, benötigen viele Ressourcen, lassen sich aber auch leicht von anderen trennen. Sie können aus Leistungsgründen auch mehrere Bastion-Hosts mit den gleichen Diensten ausstatten, allerdings bereitet der Lastausgleich möglicherweise Probleme. Die meisten Dienste müssen für bestimmte Server konfiguriert werden. Die Einrichtung mehrerer Hosts für einzelne Dienste funktioniert daher am besten, wenn Sie die Benutzung bereits vorher abschätzen können.

Wie steht es mit der Redundanz? Wenn Ihre Firewall-Konfiguration mehrere Bastion-Hosts enthält, könnten Sie sie redundant einrichten. Fällt also einer aus, können die Dienste von einem anderen übernommen und angeboten werden. Allerdings unterstützen nur einige Dienste diesen Ansatz. Sie könnten zum Beispiel mehrere Bastion-Hosts als DNS-Server für Ihre Domain (über DNS NS- [Name Server] Einträge, welche die Name-Server einer Domain kennzeichnen) oder als SMTP-Server (über DNS MX- [Mail Exchange] Einträge, die angeben, welche Server die E-Mail für einen bestimmten Host oder eine bestimmte Domain annehmen) oder beides konfigurieren und bereitstellen. Steht einer der Bastion-Hosts nicht zur Verfügung oder ist überlastet, verlagern sich die DNS- und SMTP-Aktivitäten auf den anderen.

Mehrere Bastion-Hosts lassen sich auch einsetzen, um die von Diensten verwendeten Daten voneinander zu trennen. Neben den bereits erwähnten Leistungsaspekten sprechen Sicherheitsgründe für eine Trennung. Vielleicht entscheiden Sie sich, einen HTTP-Server für die Benutzung durch Ihre Kunden über das Internet zur Verfügung zu stellen und

einen anderen für die allgemeine Öffentlichkeit. Durch den Einsatz zweier Server haben Sie die Möglichkeit, den Kunden bestimmte Daten mit höherer Geschwindigkeit anzubieten, indem Sie eine weniger belastete bzw. leistungsfähigere Maschine verwenden.

Oder Sie betreiben Ihren HTTP-Server und Ihren anonymen FTP-Server auf getrennten Maschinen, wodurch sich die Wahrscheinlichkeit verringert, daß ein Server benutzt wird, um in den anderen einzudringen. (Um zu erfahren, wie dies vor sich gehen könnte, schauen Sie sich die Beschreibung der Schwachstellen von HTTP-Servern in Kapitel 15, Das World Wide Web, an.)

Es ist O.K., den inneren und den äußeren Router zusammenzulegen

Sie können den inneren und den äußeren Router zu einem einzigen Router zusammenfassen. Sie benötigen dazu allerdings einen Router, der entsprechend leistungsfähig und flexibel ist. Im allgemeinen muß der Router es Ihnen erlauben, an jeder Schnittstelle Filter sowohl für eingehende als auch für ausgehende Daten festzulegen. In Kapitel 8, Paketfilterung, diskutieren wir, was das bedeutet. Wir beschreiben die möglichen Probleme bei der Paketfilterung, die bei Routern auftreten, die über mehr als zwei Schnittstellen verfügen und diese Fähigkeit nicht haben.

Wenn Sie den inneren und den äußeren Router zusammenlegen, wie in Abbildung 6-10 dargestellt wird, haben Sie weiterhin ein Grenznetz (an der einen Schnittstelle des Routers) und eine Verbindung in das interne Netzwerk (an der anderen Schnittstelle des Routers). Ein Teil des Verkehrs würde direkt zwischen dem internen Netz und dem Internet verlaufen (der Verkehr, der durch die Paketfilterregeln des Routers erlaubt wird), ein anderer Teil des Verkehrs bewegt sich zwischen dem Grenznetz und dem Internet oder dem Grenznetz und dem internen Netz (der Verkehr, der durch die Proxies verwaltet wird).

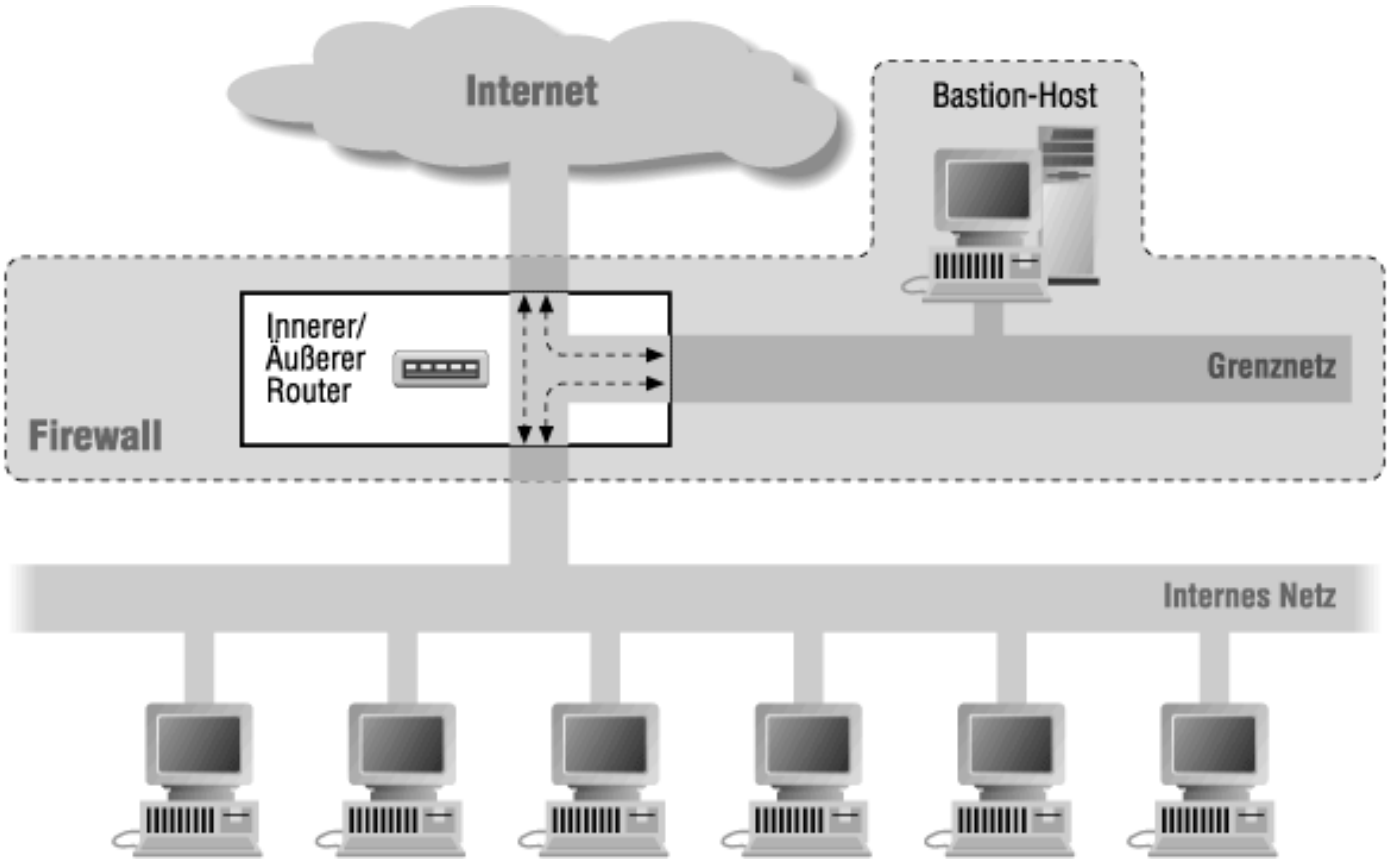

Abbildung 6-10 : Architektur mit zusammengelegtem inneren und äußeren Router

Diese Architektur erzeugt - ebenso wie die Architektur mit überwachtem Host - eine einzelne entscheidende Schwachstelle. Da sich jetzt nur noch ein Router zwischen der Innen- und der Außenseite befindet, wird durch die

potentielle Gefährdung dieses Routers der gesamte Standort verwundbar. Router sind zwar im allgemeinen leichter zu schützen als Hosts, doch auch sie sind nicht undurchdringlich.

Es ist O.K., den Bastion-Host und den äußeren Router zusammenzulegen

Es könnten Situationen auftreten, in denen Sie eine einzige Dual-Homed-Maschine sowohl als Bastion-Host als auch als externen Router benutzen. Hier ist ein Beispiel: Nehmen Sie einmal an, Sie haben nur eine Wählverbindung über SLIP oder PPP ins Internet. In diesem Fall würden Sie vermutlich PPP auf Ihrem Bastion-Host betreiben und ihn gleichzeitig als Bastion-Host und als äußeren Router arbeiten lassen. Dies ist funktional äquivalent zur Konfiguration mit drei Maschinen (Bastion-Host, innerer Router, äußerer Router), die im Abschnitt über die Architektur mit überwachtem Teilnetz bereits beschrieben wurde.

Mit einem Dual-Homed-Host zum Routen des Verkehrs werden Sie nicht die gleiche Leistung oder Flexibilität erzielen wie mit einem eigentlichen Router, allerdings sind bei einer einzelnen Verbindung mit geringer Bandbreite weder hohe Leistung noch hohe Flexibilität nötig. Je nach verwendetem Betriebssystem und eingesetzter Software steht Ihnen Paketfilterung zur Verfügung oder auch nicht. Verschiedene verfügbare Schnittstellen-Treiber besitzen ganz gute Fähigkeiten zur Paketfilterung. Da jedoch der äußere Router nicht viel Paketfilterung durchführen muß, stellt es kein besonders großes Problem dar, wenn Sie Schnittstellen-Software verwenden, deren Paketfilterung nicht so gut funktioniert.

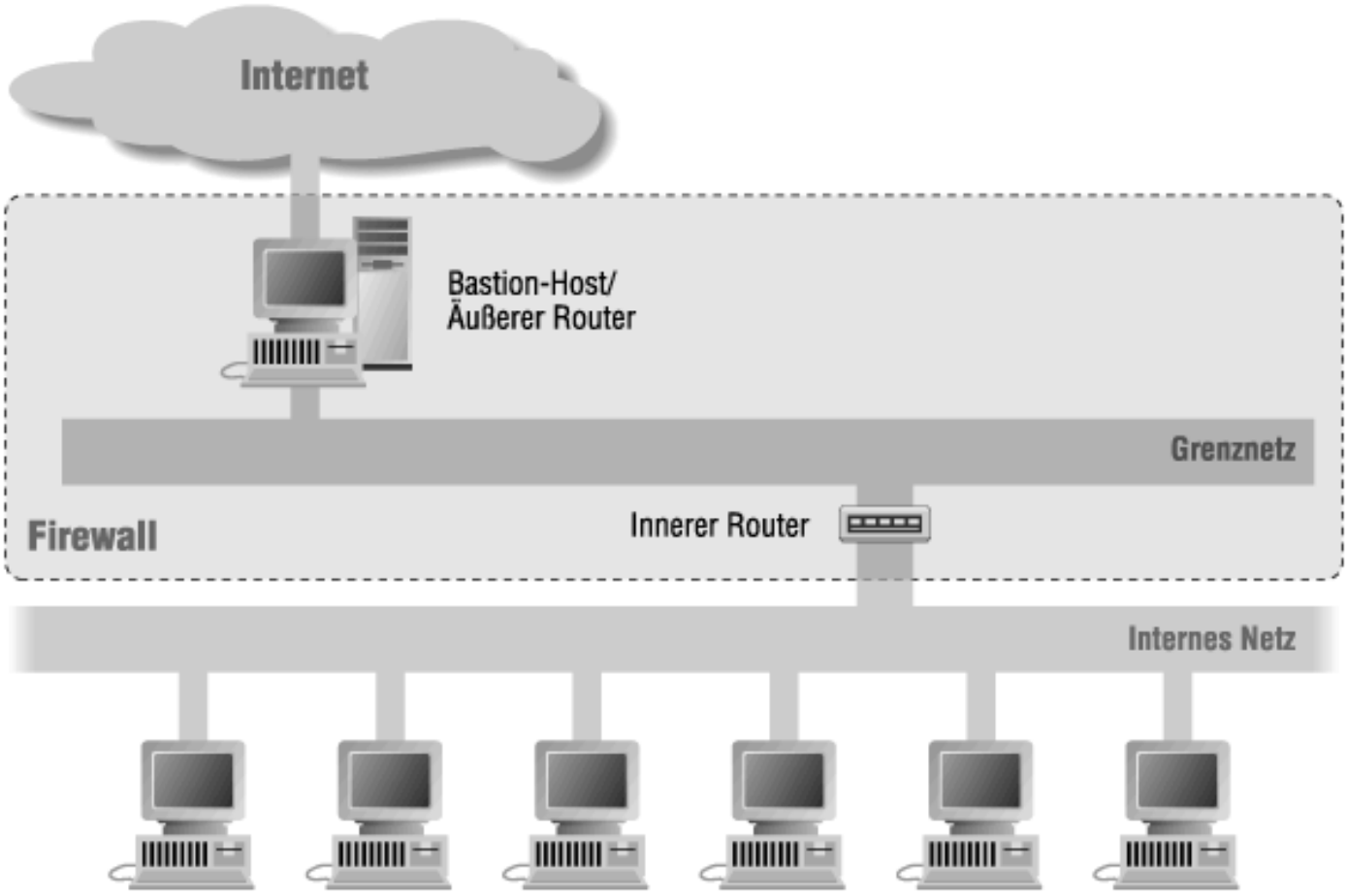

Abbildung 6-11 : Architektur mit zusammengelegtem Bastion-Host und äußerem Router

Im Gegensatz zum Zusammenlegen des inneren und äußeren Routers erhöht sich die Verwundbarkeit beim Zusammenlegen des Bastion-Hosts mit dem äußeren Router nicht merklich. (Die Konfiguration ist in Abbildung 6-11 zu sehen). Die exponierte Stellung des Bastion-Host wird weiter ausgebaut. In dieser Architektur steht der Bastion-Host dem Internet in höherem Maße offen und wird nur durch die Paketfilterung (falls vorhanden) seiner eigenen Schnittstellen-Treiber geschützt. Sie müssen sich daher verstärkt seinem Schutz zuwenden.

Es ist gefährlich, den Bastion-Host und den inneren Router zusammenzulegen

Oftmals ist es durchaus akzeptabel, den Bastion-Host und den äußeren Router zusammenzulegen, wie wir im vorangegangenen Abschnitt besprochen haben. Es wäre allerdings keine gute Idee, den Bastion-Host und den inneren Router zusammenzulegen, wie in Abbildung 6-12 dargestellt. Damit würden Sie Ihre Gesamtsicherheit gefährden.

Der Bastion-Host und der äußere Router führen jeweils unterschiedliche Schutzmaßnahmen durch; sie ergänzen einander, unterstützen sich jedoch nicht direkt. Der innere Router funktioniert teilweise als Absicherung für beide.

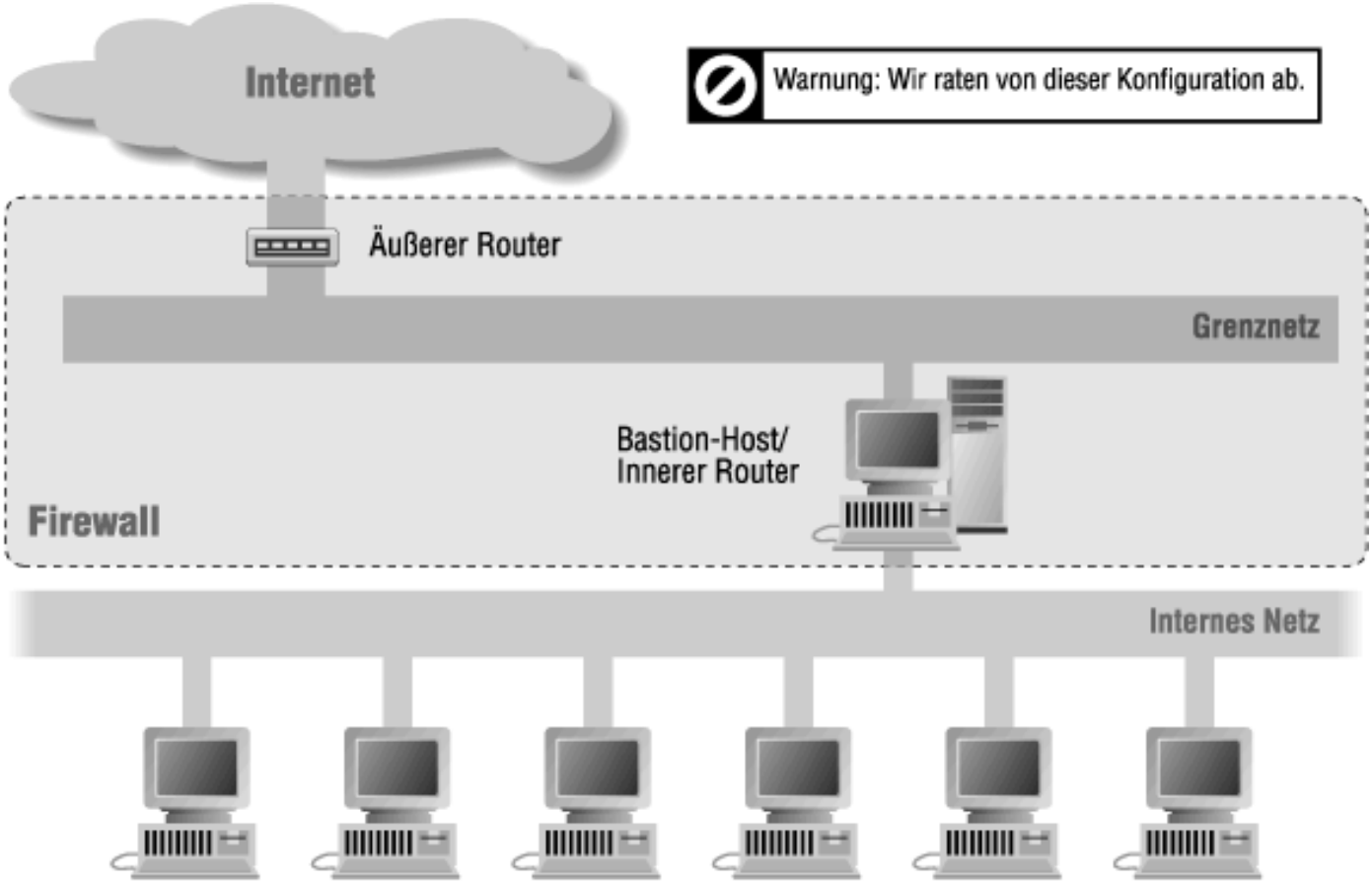

Abbildung 6-12 : Architektur mit zusammengelegtem Bastion-Host und innerem Router

Wenn Sie den Bastion-Host und den inneren Router zusammenlegen, verändern Sie die Konfiguration der Firewall auf fundamentale Weise. Im ersten Fall (Bastion-Host und innerer Router sind getrennt) haben Sie eine Architektur mit überwachtem Teilnetz. Bei dieser Konfiguration überträgt das Grenznetz für den Bastion-Host keinen rein internen Verkehr. Dieser Verkehr ist deshalb selbst dann vor dem Ausspähen geschützt, wenn in den Bastion-Host erfolgreich eingebrochen wurde; um in das interne Netzwerk zu gelangen, muß der Angreifer noch den inneren Router überwinden. Im zweiten Fall (Bastion-Host und innerer Router werden zusammengelegt) haben Sie eine Firewall-Architektur mit überwachtem Host. Wird bei dieser Art von Konfiguration in den Bastion-Host eingebrochen, besteht überhaupt kein Schutz mehr zwischen dem Bastion-Host und dem internen Netzwerk.

Eine der Hauptaufgaben des Grenznetzwerks besteht darin, den Bastion-Host am Ausspähen des internen Verkehrs zu hindern. Wenn Sie den Bastion-Host auf den inneren Router verschieben, kann er den gesamten internen Verkehr sehen.

Es ist gefährlich, mehrere innere Router zu benutzen

Der Einsatz mehrerer innerer Router zum Anschluß Ihres Grenznetzes an mehrere Teile Ihres internen Netzwerks kann eine Menge Probleme mit sich bringen und ist im allgemeinen keine gute Idee.

Das Grundproblem ist, daß die Routing-Software in einem internen System beschließen könnte, daß der schnellste Weg zu einem anderen internen System über das Grenznetz führt. Wenn Sie Glück haben, funktioniert dieser Ansatz einfach nicht, weil die Daten durch die Paketfilterung eines der Router blockiert werden. Falls Sie kein Glück haben, funktioniert es, und vertraulicher, rein interner Verkehr fließt über Ihr Grenznetz, wo er von jemandem ausgespäht werden kann, der es geschafft hat, in den Bastion-Host einzubrechen.

Außerdem ist es schwierig, die korrekte Konfiguration mehrerer innerer Router aufrechtzuerhalten. Der innere Router besitzt die wichtigsten und kompliziertesten Paketfilterregeln. Wenn Sie zwei von dieser Sorte haben, verdoppelt sich die Wahrscheinlichkeit, daß die Regeln fehlerhaft sind.

Nichtsdestotrotz werden Sie vielleicht so vorgehen wollen. Abbildung 6-13 zeigt die grundlegende Architektur mit mehreren inneren Routern. In einem großen internen Netzwerk kann das Vorhandensein nur eines einzigen inneren Routers Probleme sowohl mit der Leistung als auch mit der Zuverlässigkeit nach sich ziehen. Wenn Sie versuchen, Redundanz zu erreichen, verursacht dieser einzelne Angriffspunkt eigentlich nur Ärger. In diesem Fall ist es die sicherste Sache (mit der größten Redundanz), alle inneren Router an getrennte Grenznetze und äußere Router anzuschließen; diese Konfiguration wurde in diesem Kapitel bereits vorgestellt. Das ist zwar komplizierter und teurer, erhöht jedoch die Leistung und die Redundanz. Außerdem wird es recht unwahrscheinlich, daß der Verkehr versucht, zwischen den inneren Routern zu verlaufen (wenn das Internet die kürzeste Route zwischen zwei Teilen Ihres internen Netzwerks ist, haben Sie viel schlimmere Probleme als die meisten Standorte), und fast unmöglich, daß er damit Erfolg hat (vier Sätze von Paketfiltern bemühen sich darum, ihn fernzuhalten).

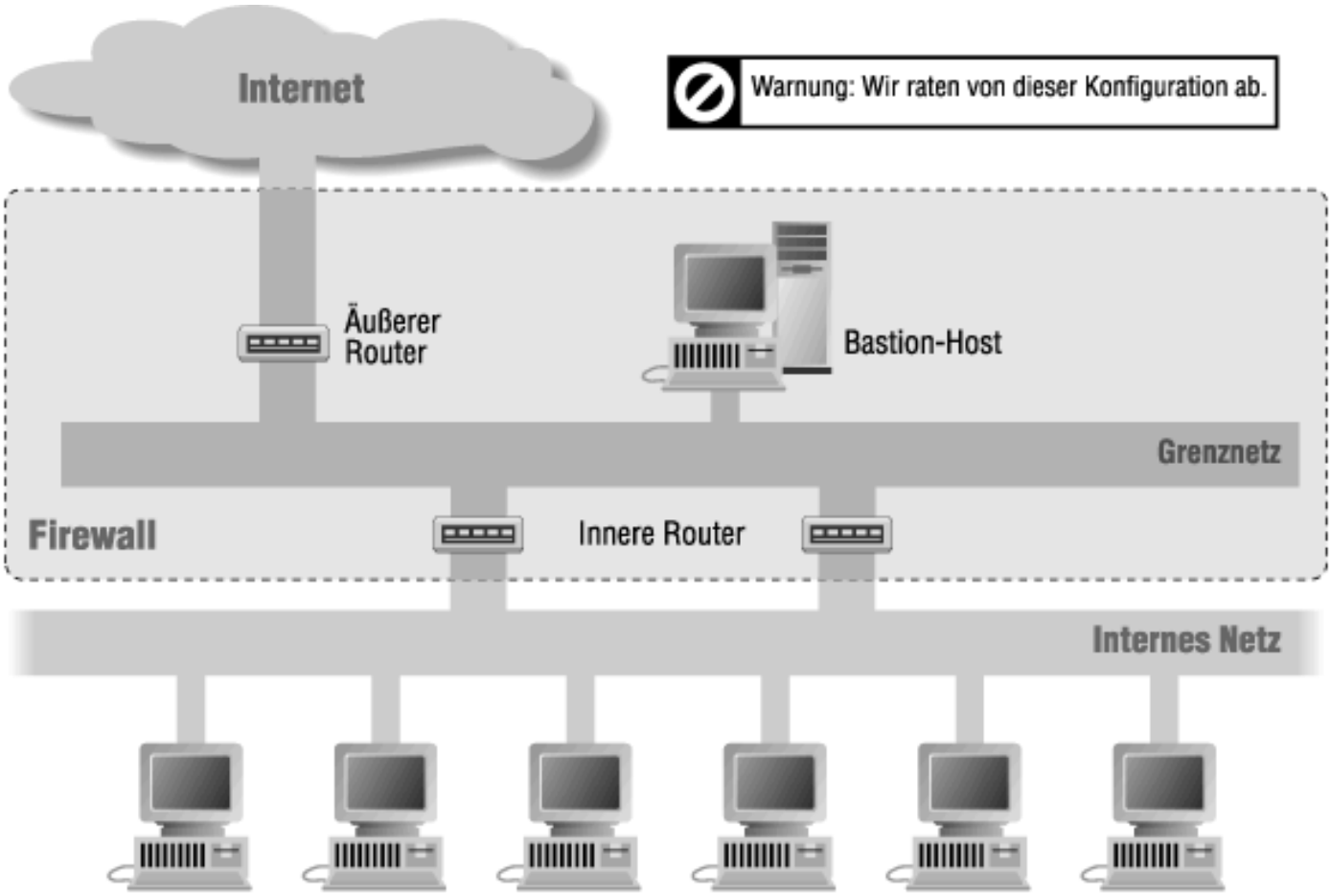

Abbildung 6-13 : Architektur mit mehreren inneren Routern

Wenn Sie sich allein durch Leistungsprobleme dazu veranlaßt sehen, mehrere innere Router einzusetzen, ist es schwer, die Kosten für getrennte Grenznetze und äußere Router zu rechtfertigen. In den meisten Fällen bildet jedoch nicht der

innere Router den Leistungsengpaß. Falls doch, liegt das an einem der folgenden Gründe:

- Es fließt viel Verkehr zum Grenznetz, der dann nicht weiter zum externen Netzwerk führt.
- Ihr äußerer Router ist viel schneller als Ihr innerer Router.

Im ersten Fall haben Sie möglicherweise etwas fehlkonfiguriert; das Grenznetz nimmt in manchen Konfigurationen gelegentlich Verkehr auf, der nicht für die Außenwelt bestimmt ist (zum Beispiel DNS-Anfragen über externe Hosts, wenn die Informationen bereits in einem Cache-Speicher vorliegt), dieser Verkehr sollte aber keine größeren Ausmaße annehmen. Im zweiten Fall müssen Sie ernsthaft darüber nachdenken, den inneren Router gegen ein anderes Modell auszutauschen, das eher dem äußeren Router entspricht, anstatt einen zweiten inneren Router hinzuzufügen.

Ein anderer Grund für den Einsatz mehrerer innerer Router könnte das Vorhandensein mehrerer interner Netzwerke sein, die aus technischen, organisatorischen oder politischen Gründen keinen gemeinsamen inneren Router benutzen können. Die einfachste Möglichkeit, diese Netzwerke anzuschließen, besteht darin, ihnen getrennte Schnittstellen an einem Router zuzuweisen, wie in Abbildung 6-14 gezeigt wird. Das verkompliziert die Konfiguration des Routers zwar beträchtlich (wie beträchtlich, hängt stark von dem fraglichen Router ab, wie Sie in Kapitel 8, Paketfilterung, erfahren), zieht aber nicht die Risiken einer Architektur mit mehreren inneren Routern nach sich. Wenn es für einen einzigen Router zu viele Netzwerke gibt oder die gemeinsame Nutzung eines Routers aus anderen Gründen nicht akzeptabel ist, sollten Sie ein internes Backbone in Betracht ziehen, das mit einem einzigen Router an das Grenznetz angeschlossen wird, wie Abbildung 6-15 zeigt.

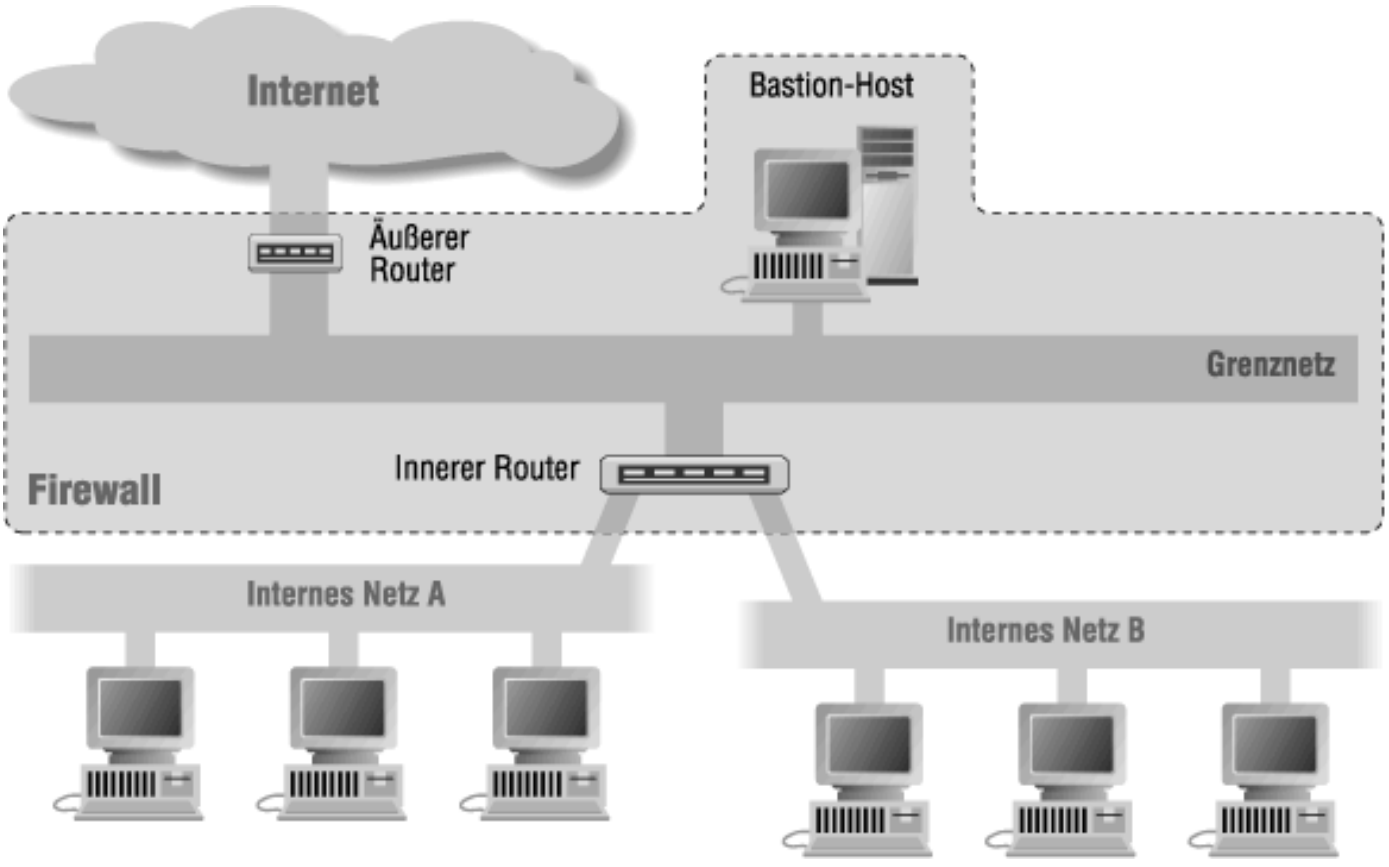

Abbildung 6-14 : Mehrere interne Netzwerke (getrennte Schnittstellen an einem Router)

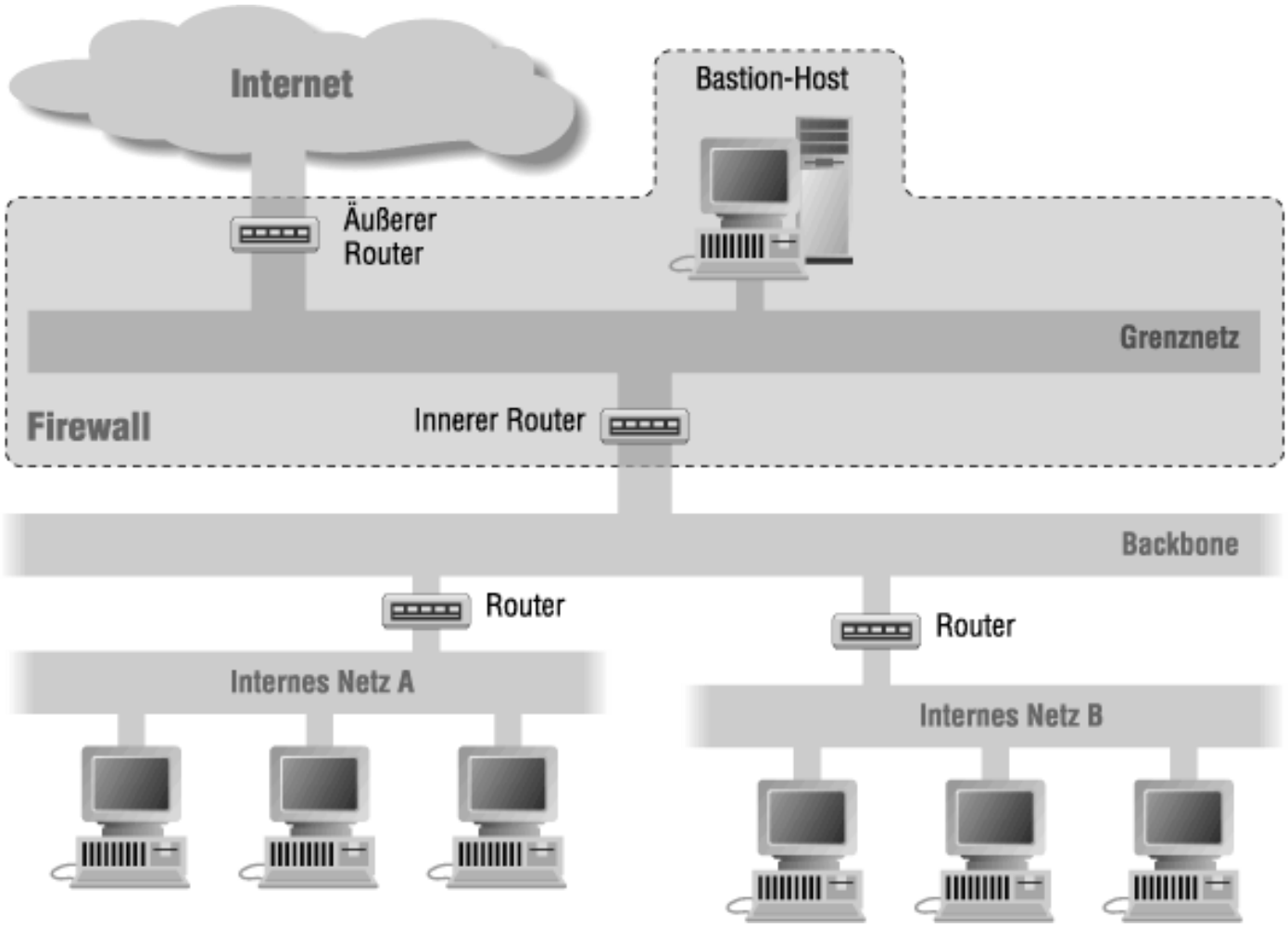

Abbildung 6-15 : Mehrere interne Netzwerke (Backbone-Architektur)

Sie werden vielleicht feststellen, daß sich verschiedene Sicherheitsmaßnahmen in den unterschiedlichen internen Netzen am effektivsten durchsetzen lassen, wenn diese über getrennte Router an das Grenznetz angeschlossen sind (wenn z.B. ein Netzwerk Verbindungen erlaubt, die ein anderes als unsicher betrachtet). In diesem Fall sollte das Grenznetz die *einzige* Verbindungsstelle zwischen den internen Netzwerken darstellen; zwischen ihnen darf kein vertraulicher Verkehr ausgetauscht werden; jedes interne Netzwerk sollte die anderen als nicht vertrauenswürdige externe Netzwerke behandeln. Das ist wahrscheinlich für einige Benutzer in diesen Netzwerken extrem unbequem, aber alles andere würde entweder die Sicherheit des gesamten Standorts gefährden oder die Trennung aufheben, die Sie mit der Einrichtung der zwei Router ursprünglich bezweckt hatten.

Wenn Sie sich dazu entschließen, die Risiken beim Einsatz mehrerer innerer Router in Kauf zu nehmen, können Sie sie minimieren, indem Sie alle inneren Router von der gleichen Gruppe verwalten lassen (damit keine sich widersprechenden Sicherheitsrichtlinien auftreten). Sie sollten außerdem sorgfältig nach internem Verkehr Ausschau halten, der das Grenznetz passiert, und bei seinem Auftreten sofort die Ursachen beseitigen.

Es ist O.K., mehrere äußere Router zu benutzen

In manchen Fällen ist es sinnvoll, mehrere äußere Router an das gleiche Grenznetz anzuschließen, wie wir in Abbildung 6-16 demonstrieren. Beispiele:

- Sie haben mehrere Internet-Verbindungen (zum Beispiel über mehrere verschiedene Service Provider - aus Gründen der Redundanz).
- Sie verfügen über eine Verbindung ins Internet sowie weitere Verbindungen zu anderen Standorten.

In diesen Situationen könnten Sie statt dessen einen äußeren Router mit mehreren Netzwerkschnittstellen einsetzen.

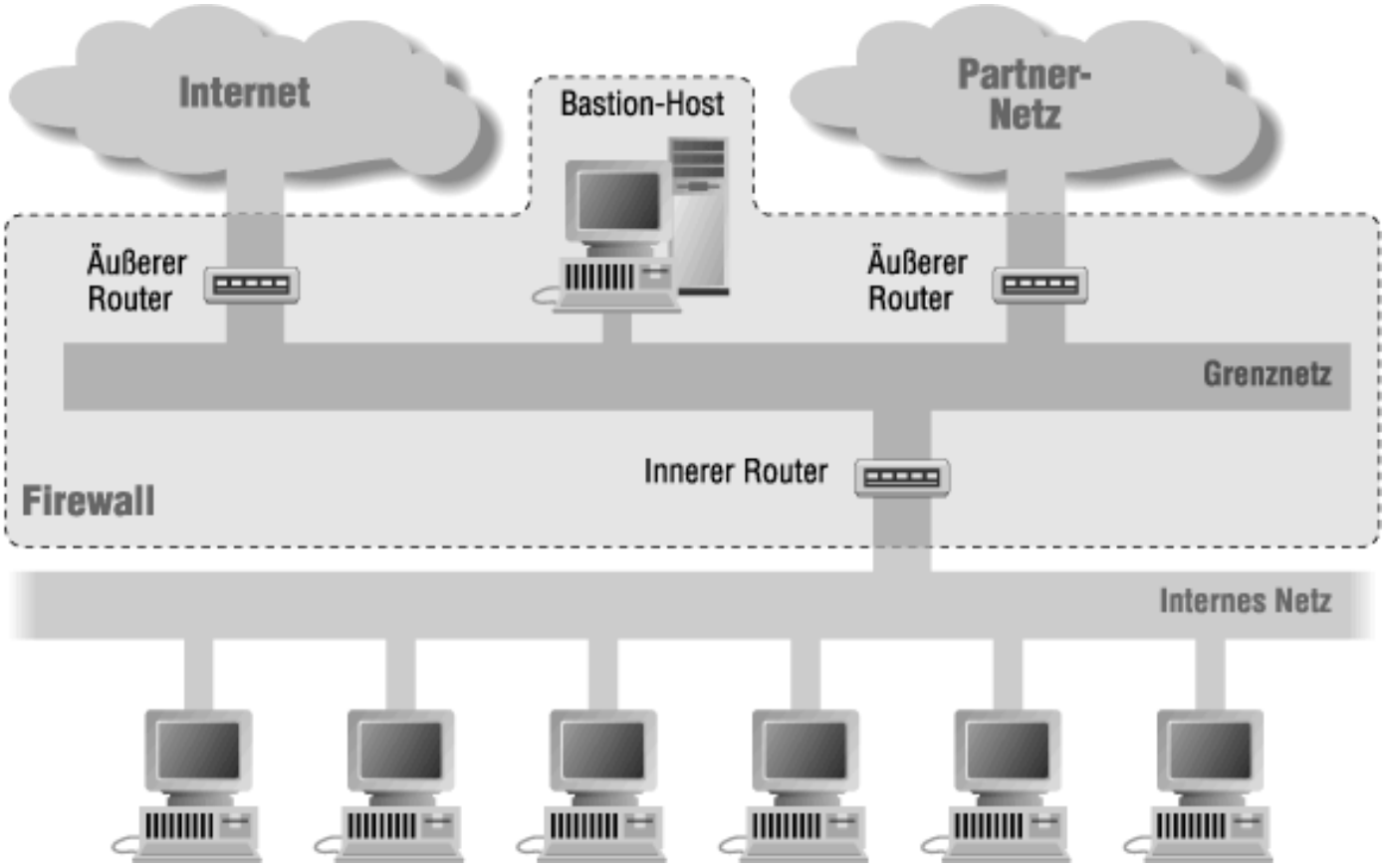

Abbildung 6-16 : Architektur mit mehreren äußeren Routern

Mehrere äußere Router, die in dasselbe externe Netzwerk führen (z.B. zwei verschiedene Internet-Provider), stellen kein signifikantes Sicherheitsproblem dar. Sie können sogar unterschiedliche Filterregeln aufweisen, ohne daß sich dadurch Probleme ergeben. Die Gefahr eines Einbruchs verdoppelt sich zwar, das Eindringen in einen äußeren Router stellt aber keine besondere Bedrohung dar.

Dagegen wird es komplizierter, wenn die Verbindungen zu unterschiedlichen Stellen führen (zum Beispiel eine in das Internet und eine zu einem Standort, mit dem Sie zusammenarbeiten und für dessen Verbindung Sie eine größere Bandbreite benötigen). Stellen Sie sich folgende Fragen, um zu ermitteln, ob eine solche Architektur in diesen Situationen sinnvoll ist: Welchen Verkehr könnte man sehen, wenn man in einen Bastion-Host im Grenznetz einbricht? Könnte zum Beispiel ein Angreifer nach einem erfolgreichen Einbruch den geheimen Datenverkehr zwischen Ihrem Standort und einer angeschlossenen Filiale ausspähen? Falls dies der Fall ist, sollten Sie in Erwägung ziehen, mehrere Grenznetze einzurichten, anstatt mehrere äußere Router in einem einzigen Grenznetz zu installieren. (Dieser Fall wird im nächsten Abschnitt erläutert.)

Beim Einrichten von Verbindungen zu externen Netzwerken, mit denen Sie besondere Beziehungen pflegen, treten andere bedeutende Probleme auf. Wir werden uns im Abschnitt »Interne Firewalls« näher damit befassen.

Es ist gefährlich, überwachte Teilnetze und überwachte Hosts zusammen zu verwenden

Wenn Sie ein überwachtes Teilnetz haben, sollten Sie keine direkten Verbindungen aus dem Internet an Ihre internen Netzwerke zulassen. Das scheint zwar offensichtlich zu sein (was nützt einem ein überwachtes Teilnetz, wenn man es dann nicht benutzt?), Sie wären aber überrascht, wenn Sie wüßten, wie viele Leute dabei Ausnahmen machen. Solche Ausnahmen sind extrem gefährlich. Wenn Sie einmal ein überwachtes Teilnetz eingerichtet haben, werden Sie sich auf den Schutz und die Sicherheit in diesem Netz konzentrieren. Es ist fast unmöglich, sowohl ein überwachtes Teilnetz als auch einen überwachten Host in einem internen Netzwerk zu schützen.

Es gibt zwei Situationen, in denen auf die Ausnahmen zurückgegriffen wird. Erstens, Leute, die Internet-Benutzern Dienste anbieten, stellen fest, daß der innere Router entweder die Administration der Dienste oder die Kommunikation zwischen Komponenten behindert (zum Beispiel einen Webserver, der mit einem internen Datenbank-Server kommunizieren muß). Zweitens, Leute mit Werkzeugen für den Zugriff auf neue Protokolle (Proxy-Server für das neueste Multimedia-3D-Universal-Überlebenswerkzeug zum Beispiel) wollen sich nicht den Streß machen, sie in den sorgfältig geschützten Bereich anderer Leute zu integrieren, und sind vollkommen davon überzeugt, daß sie so sicher sind, daß man ruhig den Verkehr zu ihnen durchlassen kann.

Kapitel 23, Datenbanken und Spiele, befaßt sich genauer mit der Positionierung von Webservern und der mit ihnen verbundenen Komponenten. An dieser Stelle sei nur kurz zusammengefaßt, daß es extrem riskant ist, den Webserver selbst im internen Netzwerk anzuordnen, selbst wenn Sie sich sicher sind, daß nur Verkehr aus dem Web bei ihm ankommt. Wenn Sie Probleme damit haben, administrative Protokolle zu erlauben, dann wenden Sie sich Kapitel 11, Unix- und Linux-Bastion-Hosts, und Kapitel 12, Windows NT- und Windows 2000-Bastion-Hosts, zu. Dort werden Methoden zur sicheren Administration von Bastion-Hosts vorgestellt.

Was die theoretisch sicheren, brandneuen Protokolle betrifft - es gibt eine Menge zu bedenken, bevor Sie die Kontrolle über einen experimentellen Bastion-Host übergeben. Sorgen Sie dafür, daß:

- kein anderer Bastion-Host dem experimentellen Bastion-Host vertraut
- der experimentelle Bastion-Host wichtigen Netzwerkverkehr nicht ausspähen kann
- die Maschine in einer sicheren Konfiguration startet
- Sie in der Lage sind, Einbrüche auf dem experimentellen Bastion-Host zu erkennen

Übergeben Sie ihn dann, und lassen Sie die Leute damit spielen. Es ist besser, wenn sie unter kontrollierten Bedingungen damit herumexperimentieren können, wo Sie sie im Auge behalten können, anstatt die Firewall komplett zu umgehen. Wenn Sie die dazu notwendigen Mittel besitzen, können Sie ein separates überwachtes Teilnetz einrichten, das ganz allein für die Experimente zur Verfügung steht.

Terminal-Server und Modem-Pools

Es gibt noch eine weitere Frage, die nur entfernt mit Firewalls zu tun hat, mit deren Beantwortung sich jedoch die Leute, die die Firewall einrichten, nur zu oft befassen müssen. Sie lautet: An welcher Stelle im Netzwerk eines Standorts sollen die Terminal-Server und Modem-Pools plaziert werden? Sie müssen der Sicherheit Ihres Einwahlzugangs auf jeden Fall genausoviel Aufmerksamkeit widmen wie der Sicherheit Ihrer Internet-Verbindung. Allerdings ist die Einwahlsicherheit (Authentifizierungssysteme, Callback-Systeme usw.) ein ganz eigenes Thema, unabhängig von Firewalls. Wir werden uns daher an dieser Stelle auf Kommentare beschränken, die in irgendeiner Weise etwas mit Firewalls zu tun haben.

Die große Firewall-Frage im Zusammenhang mit Terminal-Servern und Modem-Pools ist, wohin sie gehören: Plaziert man sie innerhalb des Sicherheitsbereichs oder außerhalb? (Dies ist vergleichbar der bereits behandelten Frage, an welcher Stelle in einem virtuellen privaten Netzwerk die Verschlüsselungsendpunkte plaziert werden sollen.) Wir empfehlen Ihnen, sie im Inneren zu plazieren und sorgfältig zu schützen. Sie tun sich nicht nur selbst einen Gefallen, sondern erweisen sich auch noch als guter Nachbar. Offene Terminal-Server in das Internet zu bringen ist nicht nur für Ihren, sondern auch für andere Standorte eine Gefahr.

Wenn die Modem-Ports vor allem für den Zugriff auf interne Systeme und Daten verwendet werden (das heißt, wenn Angestellte von zu Hause aus oder unterwegs arbeiten), ist es sinnvoll, sie innerhalb des Sicherheitsbereichs zu plazieren. Installieren Sie sie außerhalb, müssen Sie Löcher in Ihrem Schutzwall vorsehen, um den Zugriff auf die internen Systeme und Daten zu ermöglichen - Löcher, die ein Angreifer ausnutzen könnte. Außerdem könnte ein Angreifer, der Ihre Grenze überwunden hat (der zum Beispiel in Ihren Bastion-Host eingebrochen ist), potentiell die Arbeit Ihrer Benutzer überwachen, ihnen sozusagen beim Zugriff auf private, geheime Daten über die Schultern schauen. Wenn Sie die Modems nach innen legen, müssen Sie sie sorgfältig schützen, damit sie kein einfacheres Angriffsziel werden als Ihre Firewall. Es ist ziemlich peinlich, wenn Sie eine erstklassige Firewall bauen, die man

umgehen kann, indem man sich einfach über ein ungeschütztes Modem in Ihr internes Netzwerk einwählt.

Wenn die Modem-Ports andererseits vor allem dazu benutzt werden, auf externe Systeme zuzugreifen (das heißt durch Angestellte oder Gäste, die Ihren Standort hauptsächlich als Zugangspunkt in das Internet benutzen), ist es sinnvoll, sie auf die Außenseite zu legen. Sie sollten niemandem Zugriff auf Ihre internen Systeme gewähren, der dies nicht benötigt. Dieser externe Modem-Pool muß mit dem gleichen Mißtrauen bedacht werden wie Ihr Bastion-Host und die anderen Komponenten Ihrer Firewall.

Falls Sie feststellen, daß Sie beide Zugangsarten brauchen, dann sollten Sie die Einrichtung zweier Modem-Pools in Betracht ziehen: einen innerhalb, der sorgfältig geschützt wird, zum Zugriff auf die internen Systeme, und einen weiteren außerhalb als Zugang zum Internet.

Wenn Ihre Terminal-Server und Modem-Pools für Einwahl-Netzwerkverbindungen von zu Hause oder von anderen Standorten aus benutzt werden sollen, müssen Sie versuchen, die richtigen Annahmen über die künftige Nutzung zu treffen und die Technik entsprechend einzurichten. Zum Beispiel gehen Leute, die PPP-Zugänge auf Terminal-Servern einrichten, im allgemeinen davon aus, daß der PPP-Zugang von einer einzelnen externen Maschine benutzt wird. Allerdings gehören immer mehr Maschinen zu lokalen Netzwerken, und das selbst in privaten Haushalten (Papis PC ist im Arbeitszimmer, Mamis PC steht im Wohnzimmer). Diese PPP-Verbindung könnte nicht nur von der Maschine aus benutzt werden, für die Sie sie eingerichtet haben, sondern auch von jeder anderen Maschine, die an diese eine angeschlossen ist, usw. Die Maschine, die den PPP-Zugang benutzt, könnte an ein lokales Netzwerk mit einer beliebigen Anzahl Rechner angeschlossen sein, von denen wiederum beliebige mit anderen Standorten oder Internet Service Providern verbunden sind (zum Beispiel über weitere PPP-Verbindungen). Wenn Sie es nicht verhindern, könnte der Verkehr vom Internet zum zweiten PC zum »rechtmäßigen« PC und schließlich in Ihr eigenes Netz gelangen und Ihre Firewall dabei vollständig umgehen.

Sie beugen diesem Problem vor, indem Sie für die PPP-Verbindung Paketfilter aktivieren, mit denen Sie das, was diese Verbindung tun *kann*, auf das beschränken, was Sie von ihr *erwarten* (d.h., Sie beschränken die Pakete in der Verbindung auf solche Pakete zur oder von der Maschine, die Sie am anderen Ende der Verbindung vermuten).

Manche Standorte mit vielen Einwahlverbindungen bauen für diese Aktivitäten sogar eine eigene Firewall. Hinweise finden Sie im Abschnitt über die Netzwerke mit mehreren Grenznetzen.

Wir werden uns in Kapitel 14, Vermittelnde Protokolle, näher mit Protokollen für den Fernzugriff befassen. In Kapitel 21, Authentifizierungs- und Auditing-Dienste, besprechen wir die Authentifizierungsprotokolle, die im allgemeinen verwendet werden, um Modem-Pools und Terminal-Server zu schützen.

Interne Firewalls

In diesem Buch wird zunächst einmal davon ausgegangen, daß Sie eine Firewall aufbauen, um Ihr internes Netzwerk vor dem Internet zu schützen. In manchen Situationen jedoch wollen Sie vielleicht auch Teile Ihres internen Netzwerks vor anderen Teilen schützen. Dafür gibt es eine Reihe von Gründen:

- Sie verfügen über Test- oder Labornetzwerke, in denen seltsame Dinge vor sich gehen.
- Sie verfügen über Netzwerke, die weniger sicher sind als der Rest Ihres Standorts - zum Beispiel Demonstrations- oder Lehrnetzwerke, in denen häufig Außenstehende arbeiten.
- Sie verfügen über Netzwerke, die sicherer sind als der restliche Standort - zum Beispiel geheime Entwicklungsnetzwerke oder Netzwerke, in denen Finanz- oder Personaldaten kursieren.

Auch in anderen Situationen erweisen sich Firewalls als nützlich. Manchmal ist es angebracht, *interne Firewalls* aufzubauen; das heißt Firewalls, die sich zwischen zwei Teilen der gleichen Organisation befinden oder zwischen zwei Organisationen, die sich ein Netzwerk teilen, anstatt zwischen einer einzelnen Organisation und dem Internet.

Es ist oft sinnvoll, einen Teil Ihrer Organisation von den anderen zu trennen. Nicht jeder benötigt die gleichen Dienste

oder Informationen, und in manchen Bereichen Ihrer Organisation spielt Sicherheit möglicherweise eine größere Rolle als in anderen (im Rechnungswesen zum Beispiel).

Viele der Werkzeuge und Techniken zum Aufbau von Internet-Firewalls eignen sich auch zur Erstellung dieser internen Firewalls. Es gibt jedoch einige Besonderheiten, die Sie beim Aufbau einer internen Firewall beachten müssen. Abbildung 6-17 zeigt diese Architektur.

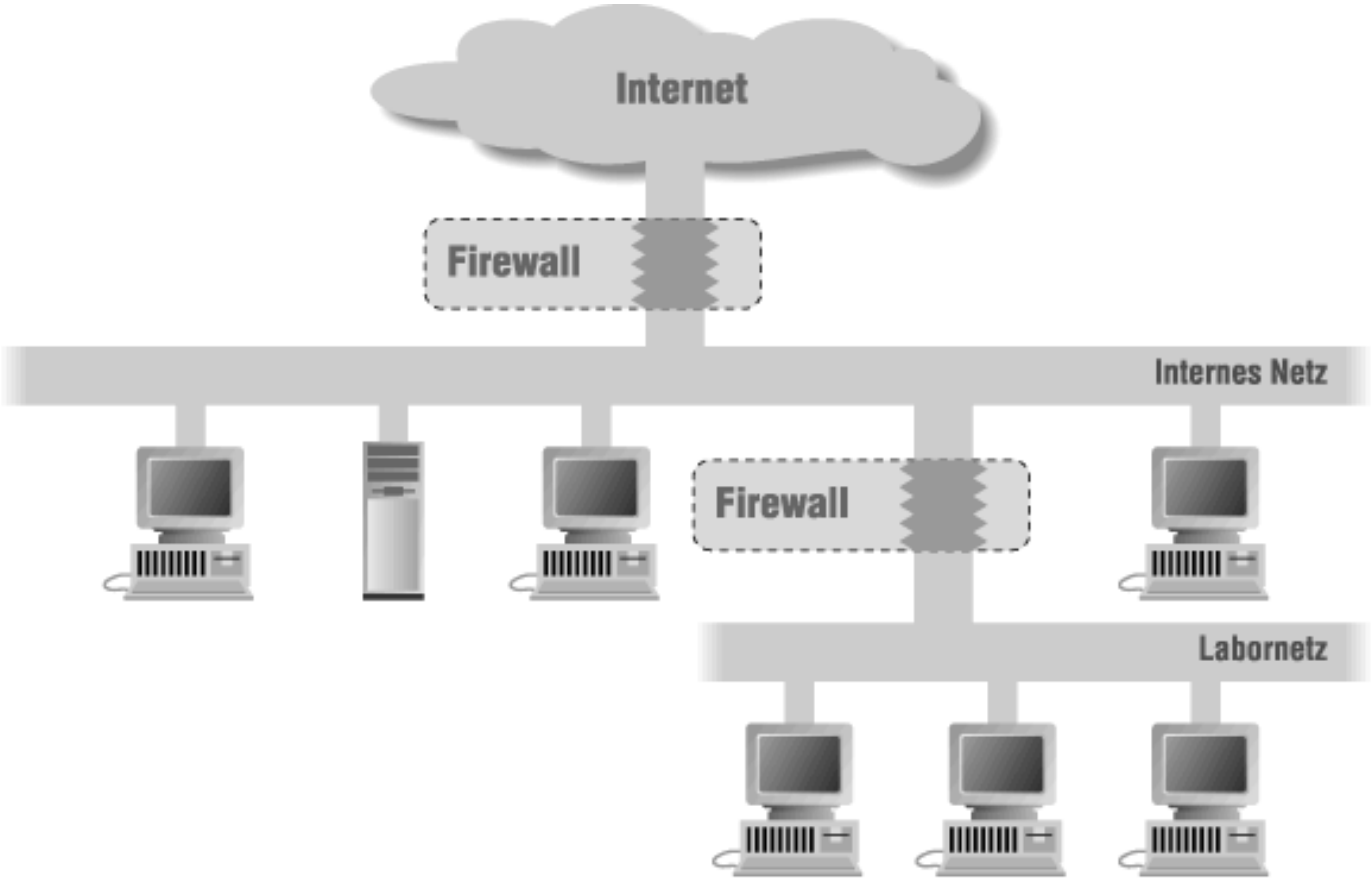

Abbildung 6-17 : Firewall-Architektur mit einer internen Firewall

Labornetzwerke

Labor- und Testnetzwerke gehören oft zu den ersten Netzwerken, die mit Hilfe einer Firewall abgetrennt werden sollen (üblicherweise als Ergebnis der schrecklichen Erfahrungen, wenn irgendetwas aus der Laborumgebung entflieht und verrückt spielt). Wenn nicht auf Routern gearbeitet wird, kann diese Art von Firewall recht einfach sein. Es wird weder ein Grenznetz noch ein Bastion-Host benötigt, noch muß man sich Gedanken über Schnüffler machen (alle Benutzer sind sowieso intern). Sie müssen auch nicht viele Dienste anbieten (es handelt sich schließlich nicht um die normalen Arbeitsplatzrechner der dort arbeitenden Benutzer). In den meisten Fällen werden Sie einen Paketfilter-Router einsetzen, der Verbindungen zum Testnetz uneingeschränkt zuläßt, aber nur bekanntermaßen sichere Verbindungen aus dem Testnetz heraus erlaubt. (Was unter »sicher« zu verstehen ist, hängt nicht von den üblichen Sicherheitsüberlegungen, sondern von der speziellen Verwendung des Testnetzes ab.)

In einigen wenigen Fällen (wenn Sie zum Beispiel die Bandbreite im Netzwerk testen) müssen Sie das Netzwerk vor dem außerhalb verlaufenden Verkehr schützen, der die Tests verfälschen würde. Dazu verbieten Sie eingehende Verbindungen und lassen nur ausgehende Verbindungen zu.

Wenn Sie Router testen, ist es vermutlich das beste, das Netzwerk komplett abzutrennen; ist das nicht möglich, verhindern Sie wenigstens, daß der Firewall-Router die Routing-Informationen aus dem Testnetzwerk mithört. Zum Testen Ihrer Router gibt es verschiedene Möglichkeiten, die von Ihrem Netzwerkaufbau, den Testbedingungen und den vorhandenen Routern abhängen. Sie könnten einen der folgenden Wege wählen:

- Verwenden Sie ein anderes als das zu testende Routing-Protokoll, und deaktivieren Sie das zu testende Protokoll vollständig.
- Lassen Sie den Router keine Routing-Daten von der zu testenden Schnittstelle empfangen und Pakete aus dem Routing-Protokoll filtern.
- Legen Sie fest, von welchen Hosts der Router aktualisierte Daten akzeptieren soll.

Wenn Sie über mehrere Testnetzwerke verfügen, sollten Sie vielleicht ein Grenznetz einrichten und jedem einen eigenen Router im Grenznetz zuweisen. Lassen Sie den Hauptteil der Paketfilterung im Router zwischen dem Grenznetz und dem Hauptnetz erledigen. Bringt eines der Testnetzwerke jetzt seinen Router zum Absturz, bleiben die Verbindungen der anderen Netze erhalten.

Gehören zu Ihren Tests externe Verbindungen, muß das Testnetzwerk selbst wie ein externes Netzwerk behandelt werden. Beachten Sie dazu den Abschnitt »Firewalls für Gemeinschaftsunternehmen« weiter hinten in diesem Kapitel.

Unsichere Netze

Testnetze sind zwar gefährlicher, aber nicht unbedingt unsicherer als andere Netzwerke. Viele Organisationen haben aber auch Netze, die an sich weniger sicher sind als andere. Zum Beispiel könnte eine Universität die Netzwerke, die in den Studentenwohnheimen verlegt worden sind, als besonders unsicher ansehen; in einem Unternehmen dürften Demonstrationsnetzwerke, Labornetze und Schulungsnetze als unsicher gelten. Dennoch sind diese unsicheren Netzwerke enger an den Rest der Einrichtung angebunden als rein externe Netzwerke.

Wohnheim- oder Labornetze, zu denen verstärkt externe Personen Zugang haben, die ihre eigenen Werkzeuge mitbringen können, sind wirklich so unsicher wie vollkommen externe Netzwerke und sollten auch so behandelt werden. Richten Sie sie entweder als zweite externe Verbindung ein (eine neue Verbindung an Ihrem äußeren Router oder ein neuer äußerer Router), oder installieren Sie ein getrenntes Grenznetz für sie. Der einzige Vorteil, den diese Netzwerke gegenüber echten externen Netzwerken besitzen, ist der, daß Sie die Software festlegen können, die in ihnen ausgeführt werden darf, und damit effektiv Verschlüsselung benutzen können.

Externe Personen könnten auch über drahtlose Netzwerke Zugang zu Ihrem internen Netzwerk erlangen. Solche Netzwerkeinrichtungen stellen eine bessere Zugänglichkeit und geringere Sicherheit zur Verfügung als traditionelle fest verkabelte Netzwerke. Vor allem haben Sie häufig eine Reichweite, die über Ihr Gebäude hinausgeht, und verlangen kaum oder keine Authentifizierung. Dadurch kann sich praktisch jeder, der über ein kompatibles Gerät verfügt, mit Ihrem Netzwerk verbinden, wobei er auf dem Parkplatz vor Ihrem Haus oder in einem Nachbargebäude sitzt. Selbst wenn die Reichweite der drahtlosen Anlage nicht über Ihre Einrichtungen hinausgeht, erschwert sie das Aufspüren eines Besuchers, der versucht, sich Zugang zu Ihrem Netz zu verschaffen. Manche drahtlosen Netzwerkeinrichtungen unterstützen eine stärkere Authentifizierung und Verschlüsselungsmöglichkeiten, die das Lauschen und den nichtautorisierten Zugang verhindern. In den meisten Fällen sollten Sie jedoch ein drahtloses Netzwerk wie ein nicht vertrauenswürdiges Netzwerk behandeln und eine Firewall zwischen diese Anlage und den Rest Ihres Netzes plazieren.

Demonstrations- und Schulungsnetze, zu denen externe Personen nur relativ kurzen, überwachten Zugang haben und in denen sie keine eigenen Tools einsetzen können, sind zuverlässiger (zumindest solange Sie garantieren können, daß der Zugang kurz und unter Aufsicht erfolgt und keine eigenen Tools im Spiel sind!). Sie müssen auch hier einen Paketfilter-Router oder einen Dual-Homed-Host einsetzen, um zu verhindern, daß vertrauliche Daten in diese Netzwerke gelangen. Außerdem sollten Sie diese Netze nur an Server anschließen, die Sie für sicher halten. Allerdings könnten Sie von bestimmten Servern NFS-Dienste anbieten. Bei einem Netzwerk, das nicht vertrauenswürdig wäre, würden Sie das unterlassen. Sie müssen vor allem dafür sorgen, daß Ihre vertrauenswürdigen Benutzer keine unsicheren Dinge tun, während sie in diesen Netzwerken arbeiten (zum Beispiel, sich auf ihren Arbeitsplatzrechnern anmelden und dann vergessen, sich wieder abzumelden, oder vertrauliche E-Mails lesen). Setzen Sie dies mit einer Mischung aus Schulung und Druck durch (stellen Sie sicher, daß die unsichersten Anwendungen fehlschlagen).

An dieser Stelle kann sich ein Dual-Homed-Host selbst ohne Proxies als äußerst nützlich erweisen; die Anzahl der

Benutzer des Hosts ist wahrscheinlich relativ klein. Durch den Zwang, sich auf dem Host anzumelden, können Sie sicher sein, daß die Benutzer die Warnmeldungen sehen. Der Host wird auch keine verlockenden, aber hochgradig unsicheren Dienste anbieten können. Zum Beispiel könnten Sie NFS nur vom Dual-Homed-Host aus anbieten, und die Leute können die Dateisysteme ihrer Arbeitsplatzrechner nicht aufsetzen (mounten).

Besonders sichere Netzwerke

In den meisten Organisationen gibt es einerseits Orte, die besonders unsicher sind, und andererseits Stellen, an denen man besonderen Wert auf Sicherheit legt, wie etwa:

- besonders wichtige Forschungsprojekte
- neue, in der Entwicklung befindliche Produkte
- Rechner aus der Buchhaltung, der Personal- und der Finanzabteilung
- das Kanzlerbüro einer Universität
- Regierungsarbeit, die zwar nicht geheim, aber in gewisser Weise vertraulich ist
- Zusammenarbeit mit anderen Organisationen

In vielen Ländern existieren gesetzliche Anforderungen für den Schutz von persönlichen Daten, die wahrscheinlich überall dort zutreffen, wo Angestellten-, Studenten-, Kunden- oder Patientendaten aufbewahrt werden. Auch bestimmte Regierungstätigkeiten, die nicht sowieso geheim sind, unterliegen einem besonderen Schutz.

Netzwerke für geheime Tätigkeiten müssen - auf jeder Geheimhaltungsstufe - nicht nur sicherer sein, sondern sollten allen relevanten gesetzlichen Vorschriften entsprechen. Das heißt im allgemeinen, daß sie von den nicht geheimen Netzwerken getrennt werden müssen. Auf jeden Fall geht dieses Thema über das Themenspektrum dieses Buchs hinaus. Falls Sie ein solches supergeheimes Netzwerk einrichten müssen, dann fragen Sie Ihren Sicherheitsbeauftragten; traditionelle Firewalls entsprechen diesen Anforderungen nicht.Fußnoten 2

Die zusätzlich erforderliche Sicherheit können Sie erreichen, indem Sie den Verkehr verschlüsseln, der über Ihre normalen internen Netzwerke verläuft, oder getrennte Netze für den sicheren Verkehr einrichten. Getrennte Netzwerke lassen sich technisch leichter umsetzen, solange in ihnen getrennte Maschinen vorliegen. Das heißt, wenn bei Ihnen ein sicheres Forschungsprojekt läuft, das auf seinen eigenen Computern realisiert wird, auf denen sich die Leute anmelden, um an diesem Projekt zu arbeiten, läßt sich leicht eine einfache Firewall installieren (vermutlich eine Lösung mit einem Paketfilter-Router). Diese Firewall behandelt Ihr normales Netzwerk als unsichere Außenwelt. Da die Labormaschinen wahrscheinlich nicht viele Dienste benötigen, ist ein Bastion-Host unnötig, und ein Grenznetz wird nur für die allersichersten Aufgaben gebraucht.

Wenn Sie es mit Leuten zu tun haben, deren tägliche Arbeit zu sichern ist, die für diesen Zweck aber keine getrennten Maschinen besitzen, erschwert sich die Umsetzung eines getrennten Netzwerks. Plazieren Sie deren Maschinen in ein stärker abgesichertes Netzwerk, können sie nicht mehr so leicht mit den anderen Leuten an diesem Standort zusammenarbeiten und brauchen zahlreiche Dienste. In diesem Fall benötigen Sie einen kompletten Bastion-Host und wahrscheinlich auch ein Grenznetz, in dem Sie diesen postieren. Es ist zwar verlockend, die Maschinen sowohl an das sichere als auch an das unsichere Netzwerk anzuschließen, damit sie über das eine Netz die vertraulichen Daten übertragen und über das andere Netz mit dem Rest des Standorts kommunizieren können, vom Standpunkt der Konfiguration aus ist es jedoch ein Alptraum. Jeder Rechner, der gleichzeitig an beide Netze angeschlossen wird, bildet im Prinzip eine Dual-Homed-Firewall, mit allen damit zusammenhängenden Wartungsproblemen. Es ist sicherer, eine Maschine immer nur an ein Netz anzuschließen. Die Konfiguration stellt jedoch für Sie weiterhin eine undankbare Aufgabe dar, während die ständige Umstellung für die Benutzer denkbar unbequem ist.

An einer Universität, an der es deutliche Unterscheidungen zwischen den verschiedenen Einrichtungen gibt, ist es vermutlich möglich, das Kanzlerbüro und die Finanzabteilung in sicheren Netzwerken zu betreiben, die vom Rest der Uni durch eine Firewall getrennt sind. In Unternehmen oder Behörden, in denen die meisten Leute in der gleichen Umgebung arbeiten, sollten Sie statt dessen besser auf Verschlüsselungstechniken zurückgreifen.

Firewalls für Gemeinschaftsunternehmen

Manchmal schließen sich Organisationen nur für einen bestimmten Zweck, wie etwa ein Gemeinschaftsprojekt, zusammen; sie müssen daher in der Lage sein, für die Dauer des Projekts auf die gleichen Maschinen, Daten und andere Ressourcen zuzugreifen. Schauen Sie sich zum Beispiel die Zusammenarbeit von IBM und Apple am PowerPC-Projekt an; nur weil sie ein Gemeinschaftsprojekt auf die Beine gestellt haben, werden IBM und Apple noch nicht ihre gesamte Organisation zusammenlegen oder sich gegenseitig alle Geschäftsvorgänge offenlegen.

Die beiden Parteien haben zwar beschlossen, einander im Rahmen dieses Projekts zu vertrauen, stehen aber immer noch im Wettbewerb miteinander. Sie wollen daher die meisten ihrer Systeme und Informationen vor dem anderen schützen; außerdem ist nicht klar, wie gut die Sicherheit der anderen Seite ist. Sie möchten nicht riskieren, daß ein Eindringling in das System des anderen durch dieses Gemeinschaftsunternehmen einen Weg in das eigene Netzwerk findet. Solche Sicherheitsprobleme treten selbst dann auf, wenn die Partner nicht in Konkurrenz miteinander stehen.

Vielleicht möchten Sie auch eine Verbindung zu einem externen Geschäftspartner herstellen. Eine ganze Reihe von Dienstleistungen ist auf Datenübermittlung angewiesen, von Versandfirmen (Sie teilen mit, was zu vertreiben ist, und man informiert Sie über die durchgeführten Aufträge) über Architekturbüros (Sie liefern die Spezifikationen und erhalten die Entwürfe) bis zu Chip-Herstellern (Sie senden das Chip-Design und beziehen Informationen über das Stadium des Fertigungsprozesses). Diese externen Geschäftspartner stellen keine Konkurrenz dar, arbeiten jedoch häufig auch für diese. Sie sind sich der Vertraulichkeit der Informationen bewußt und versuchen, sie nach bestem Wissen zu schützen. Wenn es jedoch Routing-Probleme gibt, können Daten durch die Netze der Geschäftspartner wandern, die Sie gar nicht dorthin gesendet haben. Die Geschäftspartner sind sich dessen vielleicht gar nicht bewußt, Ihre Daten allerdings sind stark gefährdet.

Das scheint vielleicht weit hergeholt, tritt aber öfter auf, als man denkt. In einem Unternehmen stellte man verblüfft fest, daß durch das eigene Netzwerk Routen für das interne Netzwerk des Konkurrenten verliefen. Noch erstaunter war man dann, als man Verkehr entdeckte, der über diese Routen verlief. Es stellt sich heraus, daß der kürzeste Weg zwischen ihnen und dem Netzwerk der Konkurrenz durch das Netz eines gemeinsamen Geschäftspartners verlief. Der Verkehr war nicht vertraulich, da es sich um Verkehr handelte, der sowieso über das Internet geführt worden wäre. Andererseits wurde die Verbindung zum externen Geschäftspartner nicht wie eine Internet-Verbindung behandelt (der Geschäftspartner selbst war nicht mit dem Internet verbunden, und niemand hätte die Möglichkeit dieser Querverbindungen angenommen). Beide Unternehmen entdeckten plötzlich unerwartete und ungeschützte Schwachstellen.

Eine interne Firewall begrenzt den Schaden in einer solchen Situation. Sie stellt einen Mechanismus zum gemeinsamen Nutzen einiger Ressourcen bereit, während die anderen Ressourcen geschützt werden. Bevor Sie damit beginnen, eine interne Firewall zu bauen, müssen Sie sich darüber klarwerden, was Sie teilen, was Sie schützen und was Sie erreichen wollen. Stellen Sie sich folgende Fragen:

- Was genau wollen Sie durch das Verbinden Ihres Netzwerks mit dem Netzwerk einer anderen Einrichtung erreichen? Die Antwort auf diese Frage legt fest, welche Dienste Sie bereitstellen müssen (und implizit, welche Dienste blockiert werden müssen).
- Versuchen Sie, eine vollständige Arbeitsumgebung für ein Gemeinschaftsprojekt auf die Beine zu stellen, in der Mitglieder beider Organisationen zusammenarbeiten und weiterhin Zugriff auf ihre »Heimat«-Systeme haben können (die vor der anderen Organisation geschützt werden müssen)? In diesem Fall brauchen Sie möglicherweise zwei Firewalls: jeweils eine zwischen dem Gemeinschaftsprojekt und den beiden Heimatorganisationen.

Die Art der zu verwendenden Firewall-Technik wird durch Ihre Ziele und Ihre Sicherheitsanforderungen bestimmt.

Ein gemeinsam genutztes Grenznetz für distanzierte Beziehungen

Gemeinsam genutzte Grenznetze bilden eine gute Möglichkeit für den Aufbau von Gemeinschaftsnetzwerken. Jede

Partei kann auf dem Grenznetz zwischen den beiden Organisationen ihren eigenen Router unter ihrer eigenen Kontrolle installieren. In manchen Konfigurationen sind diese beiden Router die einzigen Maschinen im Grenznetz, es gibt keinen Bastion-Host. Wenn das der Fall ist, dann wird das »Netz« einfach durch eine schnelle serielle Leitung (z. B. eine 56 Kbps- oder T1/E1-Leitung) zwischen den Routern anstatt durch ein Ethernet oder eine andere Art lokales Netzwerk gebildet.

Bei einem externen Geschäftspartner ist diese Vorgehensweise sehr zu empfehlen. Die meisten sind keine Netzwerkexperten und versuchen zu sparen, indem sie mehrere Clients an das gleiche Grenznetz anschließen. Wenn das Grenznetz ein Ethernet-Netz oder etwas ähnliches ist, kann jeder Client, der dessen Router im Grenznetz erreicht, den gesamten Verkehr für alle Clients im Grenznetz sehen - wobei es sich bei manchen Providern mit ziemlicher Sicherheit um vertrauliche Informationen der Konkurrenz handelt. Durch den Einsatz einer Punkt-zu-Punkt-Verbindung als »Grenznetz« zwischen dem externen Geschäftspartner und jedem Client anstelle eines gemeinsam genutzten Grenznetzes mit mehreren Clients wird dieses Verhalten unterbunden - auch dann, wenn es zufällig auftritt.

Eine interne Firewall mit oder ohne Bastion-Hosts

Sie brauchen vielleicht wirklich keinen Bastion-Host im Grenznetz zwischen zwei Organisationen. Die Entscheidung darüber hängt von den Diensten ab, die für Ihre Firewall notwendig sind, sowie vom Vertrauen der Organisationen zueinander. Bastion-Hosts im Grenznetz werden für die Beziehungen zu einem externen Geschäftspartner selten benötigt; normalerweise senden Sie die Daten über ein bestimmtes Protokoll und können dies auf einem überwachten Host angemessen schützen.

Wenn die Organisationen ausreichend Vertrauen zueinander (und auch in die jeweilige Sicherheit) aufbringen, scheint es vernünftig zu sein, die Paketfilter so zu konfigurieren, daß die Clients auf der anderen Seite direkte Verbindungen zu den internen Servern (wie etwa SMTP- und DNS-Servern) herstellen können.

Haben die Organisationen andererseits kein Vertrauen zueinander, wollen Sie vermutlich ihren eigenen Bastion-Host unter eigener Kontrolle und Verwaltung im Grenznetz plazieren. Der Verkehr bewegt sich von den internen Systemen der einen Partei zu ihrem Bastion-Host, von dort zum Bastion-Host der anderen Partei und schließlich zu deren internen Systemen.
Fußnoten 1

```
Vorausgesetzt natürlich, daß Ihre beiden Internet-Provider auch wirklich
über zwei unterschiedliche
Kabel in zwei verschiedenen Kabelschächten angebunden sind.
Unterschätzen Sie niemals die
zerstörerische Wirkung einer Spitzhacke oder eines Bohrhammers.
```

Fußnoten 2

```
Wenn es bei Ihnen keinen Sicherheitsbeauftragten gibt, dann werden Sie
auch kein geheimes Netzwerk
aufbauen können.
```

---

zurück zu Einrichten von Internet Firewalls
