

iFSS/5: Ein integriertes Firewall-/Server-System

Norbert Luttenberger
Fachhochschule Gelsenkirchen

Autor

Norbert Luttenberger studierte Elektrotechnik an der TU Braunschweig. Von 1977–84 arbeitete er im Bereich Automatisierungstechnik der Siemens AG in Erlangen. 1984 wechselte er an den Lehrstuhl für Rechnerarchitektur und Verkehrstheorie (Prof. Dr. U. Herzog) der Universität Erlangen-Nürnberg, wo er 1989 zum Dr.-Ing. promoviert wurde. Danach war er am Europäischen Zentrum für Netzwerkforschung der IBM in Heidelberg in den Bereichen Multimedia-Kommunikation und Mobile Datenkommunikation tätig. Seit 1995 ist er Professor für Datenübertragung und Netzwerke im Fachbereich Informatik der Fachhochschule Gelsenkirchen.

Zusammenfassung

Für den Schutz der in einem Intranet betriebenen Server vor Angriffen aus dem Internet und für die Aufrechterhaltung der Verfügbarkeit der entsprechenden Rechensysteme werden heute von vielen Intranet-Betreibern Firewall-Systeme eingesetzt. Firewall-Systeme lassen sich als Schutzsysteme betrachten, die den einzigen Verbindungspunkt eines Intranets zum Internet darstellen, und die jedweden ein- und ausgehenden Verkehr überwachen. Die Praxis hat gezeigt, daß sowohl die Formulierung von Überwachungsregeln für Firewall-Systeme als vor allem auch die Integration von Firewall-Funktionen und Intranet-Services komplizierte Probleme sind, die von den Netzwerkadministratoren oftmals eine sehr detaillierte Kenntnis der Funktionsweise aller eingesetzten Komponenten erfordern. In diesem Aufsatz wird ein integriertes Firewall-/Server-System vorgestellt, in dem durch die hardware- und softwaremäßige Integration von Firewall- und Server-Funktionen in einer *black box* der Aufbau eines Intranet erheblich vereinfacht werden kann. Das iFSS/5 bietet neben der Schutzfunktion sowohl externe Services für Benutzer aus dem Internet (z.B. einen WWW-Dienst), als auch strikt interne Dienste. Die Administration des gesamten Komplexes erfolgt über eine einheitliche, diensteorientierte graphische Benutzeroberfläche.

1 Einführung

Für viele Unternehmen, öffentliche und private Organisationen verbindet sich heute die Entscheidung, im Internet mit einem eigenen Informationsangebot aufzutreten, mit der weitgehendsten Entscheidung, ein eigenes Intranet aufzubauen (oder die vorhandene Netzwerkinfrastruktur in diese Richtung umzubauen) und dieses Intranet mit dem Internet zu verbinden. Wegen der vielen bekannt gewordenen Angriffe aus dem Internet auf die Informationsbestände in Intranets ist es unumstritten, daß der Anschluß eines Intranets an das Internet nur dann vollzogen werden darf, wenn die im Intranet gespeicherten Information vor fremden Zugriffen geschützt und die Verfügbarkeit der Rechensysteme im Intranet durch ein Firewall-System gesichert wird.

Im angeführten Szenario sind – genau hingeschaut – drei technische Aufgaben zu lösen: die Einrichtung einer öffentlichen Internet-Präsenz, die Einrichtung einer internen, nicht-öffentlichen Kommunikationsinfrastruktur und die Sicherung des Übergangs Intranet/Internet durch ein Firewall-System. Ist schon jede einzelne dieser Aufgaben nicht ohne Schwierigkeiten zu bewältigen, so zeigt vielfältige praktische Erfahrung, daß vor allem die Kombination und Integration von Firewall-Technik und differenzierter Bereitstellung von Intranet- und Internet-Kommunikationsdiensten einige nicht unerhebliche Probleme bereitet. Dies liegt insbesondere daran, daß alle Dienste eine individuelle Konfiguration verlangen und sie alle auf jeweils unterschiedliche Weise mit dem Firewall-System kooperieren.

Es war deshalb das Ziel der hier dargestellten Arbeit, eine schlüsselfertige Hardware-/Software-Lösung bereitzustellen, bei der die diversen Konfigurationsprobleme entweder abgeschlossen gelöst sind oder über ein integriertes Administrationswerkzeug mit einer graphischen Benutzeroberfläche vom Systemverwalter in einer konsistenten Art und Weise einer Lösung zugeführt werden können.

Heute wird eine Vielzahl von Firewall-Systemen kommerziell angeboten. Diese unterscheiden sich in den Überwachungsmechanismen, in der Leistungsfähigkeit, in der Hardwarebasis und in der Benutzeroberfläche. Dieser Aufsatz zielt nicht darauf, solche Firewall-Systeme mit ihren jeweiligen Stärken und Schwächen zu analysieren; vielmehr soll gezeigt werden, welche Integrationsprobleme sich bei der oben angesprochenen dreifachen Aufgabe stellen und wie diese systematisch gelöst werden können. Dazu wird die an der FH Gelsenkirchen prototypisch entwickelte Lösung mit der Bezeichnung iFSS/5 („integriertes Firewall-/Server-System im FB 5“) vorgestellt [3].

Der Aufsatz ist wie folgt aufgebaut: Zunächst werden einige grundsätzliche Design-Überlegungen zum iFSS/5 dargestellt. Die eigentliche Firewall-Software wird im dritten Abschnitt erläutert. Im vierten Abschnitt geht es um die vom iFSS/5 bereitgestellten internen und/oder externen Dienste und die zugehörigen Server. Ein wesentlicher Aspekt für die Integration von Firewall-Funktionalität und Dienstangebot ist die einheitliche und konsistente Systemadministration; diese wird im fünften Abschnitt dargestellt. Der Aufsatz schließt mit einem Ausblick auf zukünftige Entwicklungen.

Noch zwei Hinweise: (1) Durch ein Firewall-System kann selbstverständlich nicht nur ein Übergang Intranet/Internet gesichert werden, sondern auch ein allgemeiner Übergang zwischen zwei Teilnetzen. Deshalb ist hier meist von einem „externen Netz“ die Rede, wenn es

um das Netz geht, gegen das man sich abgrenzen möchte. In vielen Fällen wird dies jedoch das Internet sein. (2) In den Bildern wird das Intranet der Einfachheit halber als ein Ethernet-LAN mit Bustopologie dargestellt; selbstverständlich kann ein Intranet jedoch jede beliebige Topologie haben.

2 Entwurfsüberlegungen

2.1 Systemkonfiguration

Die Diskussion einer Systemkonfiguration muß notwendigerweise bei einer Betrachtung der Netzwerkdienste anfangen, die in dieser Konfiguration erbracht werden sollen. Netzwerkdienste lassen sich in einer ersten Klassifikation unterscheiden nach Standard-Diensten einerseits und nach speziellen Diensten andererseits, wobei die letzteren auf die besonderen Bedürfnisse der jeweiligen Organisation abgestimmt sind. Aus offensichtlichen Gründen konnte es bei der iFSS/5-Entwicklung nur um Standarddienste gehen, weshalb im Rahmen dieses Aufsatzes auch nur darauf eingegangen wird. Spezielle Dienste sind in aller Regel nur als Intranet-interne Dienste realisiert; die entsprechenden Server befinden sich „hinter“ dem Firewall-System und werden durch dieses vor unberechtigten Zugriffen geschützt. Selbstverständlich können die zugehörigen Server auf dem weiter unten vorzustellenden *inside host*, der integraler Bestandteil des iFSS/5 ist, installiert werden.

Für die ordnungsgemäße Erbringung von Diensten muß geregelt sein, welche Benutzer auf welche Dienste zugreifen dürfen. Dabei ist meist eine nur dienstspezifische Regelung allein nicht ausreichend: Es muß zusätzlich geklärt werden, auf welche Datenbestände mit welchem Dienst zugegriffen werden darf: Die zu vergebenden Zugriffsrechte sind also in der Regel dienst- und datenabhängig. Im Zusammenhang mit einem Firewall-System haben wir es dabei vor allem mit der Durchsetzung dieser Zugriffsrechte gegen unbefugte Benutzer „von außen“ zu tun.

Die Wahrung von Zugriffsrechten kann durch verschiedene Maßnahmen erzwungen werden, die – sinnvoll miteinander kombiniert – ein angepaßtes Schutzkonzept ergeben:

- Server können z.B. so konfiguriert werden, daß ein Zugriff auf bestimmte Datenbestände nur nach erfolgreicher User-Id/Paßwort-Abfrage gewährt wird. Nachteil dieser Technik: Wenn es einem Angreifer gelingt, auf dem Host, auf dem der Server läuft, durch Ausnutzen einer „Hintertür“ Superuser-Rechte zu erlangen, kann er die fraglichen Datenbestände ausspähen. Deshalb ist dieser Schutzmechanismus eher für die Differenzierung von Zugriffsrechten *innerhalb* des Intranet als für das Aufbauen eines allgemeinen „Schutzzauns“ zum externen Netz hin geeignet. Es ist also sinnvoll, Dienste und Datenbestände, die nur im Intranet zugreifbar sein sollen, auf einem separaten Host zu hinterlegen, der vom externen Netz aus nicht sichtbar ist und auf den von dort aus also auch nicht zugegriffen werden kann. Dieser Host heißt im iFSS/5 *inside host*.

- Zur Durchsetzung von Zugriffsrechten zum externen Netz hin ist der Einsatz eines Firewall-Systems notwendig, das alle vom externen Netz kommenden Zugriffsversuche überprüft. Um einem externen Angreifer eine möglichst geringe „Angriffsfläche“ zu bieten, wird das Firewall-System auf einer separaten Maschine installiert, die einzig und allein diese Schutzfunktion wahrnimmt, d.h. auf der außer Betriebssystem und Firewall-Software keine weiteren Programme und Datenbestände installiert sind. Diese Maschine ist direkt sowohl mit dem Intranet als auch mit dem externen Netz verbunden (Konfiguration als *dual-homed host*) und bildet den sog. *bastion host* des Intranet.
- Aus den genannten Gründen verbietet es sich, auf der letztgenannten Maschine Server zu installieren, die ein Informationsangebot des Intranet-Betreibers für Benutzer aus dem externen Netz bereithalten. Da auch auf dieses Informationsangebot nur kontrolliert, d.h. nach einer Überprüfung der Zugriffswünsche durch das Firewall-System, zugegriffen werden darf, müssen die gleichen Schutzmechanismen wie beim *inside host* implementiert werden: Auch diese Maschine darf vom externen Netz aus nicht sichtbar sein, und alle Zugriffswünsche müssen durch das Firewall-System überprüft werden können. Diese Maschine wird im iFSS/5 als *outside host* bezeichnet. Der *outside host* wurde bewußt nicht direkt an das externe Netz angeschlossen, sondern indirekt über den *bastion host* und ein *secure subnet*, damit Zugriffe aus dem externen Netz zuvor kontrolliert werden können.

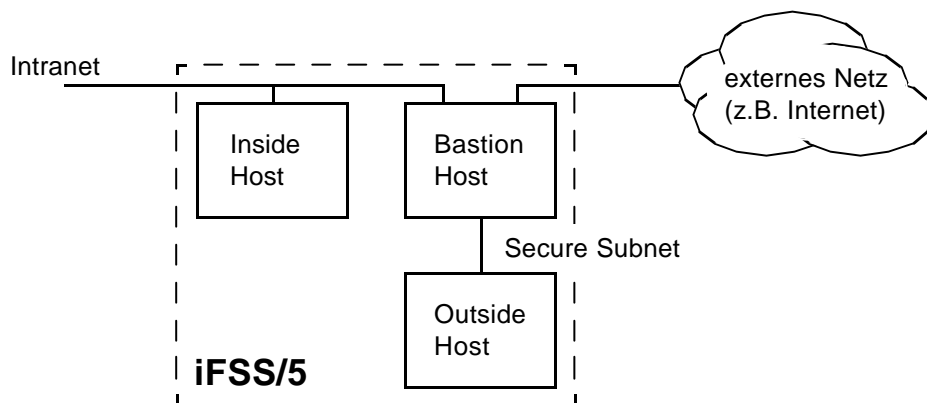


Bild 1: Das iFSS/5 als 3-Rechner-System

Offensichtlich ist es also im Interesse eines wirkungsvollen Zugriffsschutzes erforderlich, die unterschiedlichen Dienste und Datenbestände auf mehrere Server, die auf unterschiedlichen Hosts laufen, aufzuteilen; ein integriertes Firewall-/Server-System ist als Mehrrechner-System zu konzipieren, dessen „Wurzel“ der *bastion host* mit der Firewall-Funktion bildet. Bild 1 zeigt die resultierende Konfiguration.

2.2 Das Schutzkonzept des iFSS/5

In der Literatur (z.B. [1], [2], [5]) findet sich eine ausführliche Diskussion der unterschiedlichen Möglichkeiten, Schutzmechanismen mit Hilfe eines Firewall-Systems aufzubauen. Die hohe Anzahl der Kombinationsmöglichkeiten von Hardware- und Softwarekonfigurationen

macht Entwurf und Bewertung von Firewall-Systemen zu einem komplexen technischen Prozeß, der dem Anwender durch abgestimmte vorkonfektionierte Lösungen abgenommen werden sollte. Beim iFSS/5 lagen dem Entwurf der Schutzfunktion durch ein Firewall-System die folgenden vier Leitlinien zugrunde:

1. Wie dargestellt werden Dienste und Datenbestände, wo dies sinnvoll und möglich ist, auf „interne Server“ und „externe Server“ aufgeteilt. Unter einem internen Server wird hier ein Server verstanden, der auf dem *inside host* läuft; ein externer Server läuft auf dem *outside host*.
2. Das Firewall-System macht die Struktur des Intranet durch *address translation* unsichtbar: Aus dem externen Netz heraus ist nur der *bastion host* „sichtbar“, da als Absende-Adresse aller Pakete aus dem Intranet die Adresse des *bastion host* auftaucht.¹ Dadurch kann ein Angreifer im externen Netz nicht in Erfahrung bringen, welche Maschinen und welche Server sich im internen Netz befinden. Was verborgen ist, kann logischerweise nicht angegriffen werden. Durch Anwendung der *address translation* können im Intranet die privaten IP-Adressen nach RFC-1918 [4] eingesetzt werden. Trotz der Knappheit der IP-Adressen (in der IP-Version 4) kann damit im Intranet ein großer Adreßraum zur Verfügung gestellt werden, der es gestattet, das Intranet detailliert und freizügig zu strukturieren. Zum Anschluß des Intranets an das externe Netz wird nur eine einzige öffentliche (eindeutige) IP-Adresse benötigt, und zwar für die Netzwerkschnittstelle des *bastion host* zum externen Netz (Bild 2).
3. Die enge Integration von Schutzfunktion und Dienstleistung legt es nahe, im iFSS/5 eine dienstorientierte Zugriffskontrolle durch den Einsatz von geeigneten *proxy*-Servern² zu installieren. Im Betriebssystem des *bastion host* ist deshalb die IP-Routing-Funktion ausgeschaltet, so daß Pakete durch den *bastion host* nur dann weitergeleitet werden, wenn sie an einen auf dem *bastion host* installierten *proxy*-Server gerichtet sind und durch die Zugriffskontrollregeln dieses *proxy*-Servers nicht abgewiesen werden. Die Art der eingesetzten *proxy*-Server entscheidet zunächst, welche Dienste überhaupt zugelassen werden: Ist für einen bestimmten Dienst im Firewall-System kein *proxy*-Server vorhanden, so kann auf diesen Dienst generell nicht „grenzüberschreitend“ zugegriffen werden. Ein vorhandener *proxy*-Server verhindert sodann mit Hilfe von Zugriffskontrollregeln, daß von extern auf interne Server zugegriffen werden kann. Weitere Regeln leiten externe Zugriffe auf externe Services über das *secure subnet* auf externe Server um. Mit dem Einsatz von *proxy*-Servern ist offensichtlich der Nachteil

1. Selbstverständlich werden interne Strukturen auch durch den *Name Server* des Systems nicht nach außen „verraten“.
2. Das englische Wort *proxy* bedeutet „Stellvertreter“. Ein *proxy*-Server ist ein Programm, das zum Netz hin das gleiche Verhalten zeigt wie das Server-Programm, für das es stellvertretend eingesetzt wird. Der *proxy*-Server erbringt jedoch nicht den eigentlich gewünschten Dienst, sondern eine andere, ggf. zusätzliche Funktion. In unserem Fall besteht die zusätzliche Funktion vor allem darin, daß der *proxy*-Server, bevor er eine bei ihm eintreffende Dienstanfrage an den „richtigen“ Server weiterleitet, eine Überprüfung der Zugriffsberechtigung durchführt.

verbunden, daß bei Einführung neuer Dienste auch neue *proxy*-Server bereitgestellt werden müssen. Dieser Nachteil wird durch die einfache Konfigurierbarkeit und die höhere Sicherheit des *proxy*-Server-Mechanismus mehr als kompensiert.

4. Nachrichten, die zwischen externem Netz und Intranet ausgetauscht werden müssen (z.B. e-Mail, News, Name Resolution Requests/Responses), werden mit Hilfe sicherer *relays* durch das Firewall-System hindurch geleitet.

Das realisierte System stellt eine typische Installation dar und dürfte eine große Zahl von Anwendungsfällen abdecken.

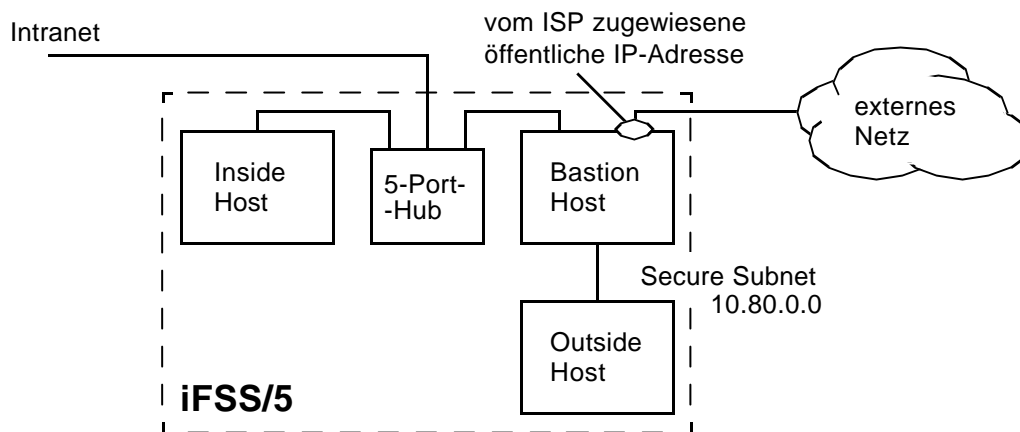


Bild 2: IP-Adressen und iFSS/5-Hardwaresystem

2.3 Hardwaresystem des iFSS/5

Die Hardware des iFSS/5 umfaßt drei Industrie-PCs und einen 5-Port-Hub in einem gemeinsamen Gehäuse. Die resultierende Konfiguration zeigt Bild 2.

Die drei Host-Rechner sind Pentium-Prozessoren) ausgestattet, der Hauptspeicherausbau beträgt 128 Mbyte (64 Mbyte beim *inside host*), es stehen Festplatten mit jeweils 2,1 Gbyte Kapazität zur Verfügung. Erweiterungen können über lokale ISA- und/oder PCI-Busse angeschlossen werden. Auf allen drei Rechnern läuft das Betriebssystem Linux.

Alle Netzwerkverbindungen basieren derzeit auf der Ethernet-Technik. Der *bastion host* verfügt über drei Netzwerkkarten. Über eine Karte ist der *bastion host* an den internen 5-Port-Hub angeschlossen. Dieser Hub bildet quasi die „Intranet-Wurzel“; an ihn ist auch der *inside host* angeschlossen. Die drei verbleibenden Hub-Ports stehen für den Anschluß von Komponenten des Intranets zur Verfügung. Über die zweite Netzwerkkarte ist der *bastion host* mit dem *outside host* verbunden; hier erfolgt die Verbindung nicht über einen Hub, sondern über ein „*cross-over*“-Kabel. (Dies ist eine aufwandsarme Lösung, die bei Interesse an einer redundanten und besser skalierbaren Lösung sicherlich dem Einsatz eines weiteren Hub zu weichen hat.) Über die dritte Netzwerkkarte schließlich kann der *bastion host* an das externe Netz angeschlossen werden. Es wurde aus mehreren Gründen entschieden, das iFSS/5 nicht mit einer Netzwerkkarte für ein Weitverkehrsnetz (z.B. ISDN) auszustatten. Zum einen wären dadurch ggf. Kompatibilitätsprobleme zwischen der vom ISP¹ eingesetzten Technik und dem

iFSS/5 entstanden, zum anderen ist davon auszugehen, daß in kurzer Zeit xDSL-Anschlüsse zur Verfügung stehen werden, die neue Perspektiven für den Anschluß von Intranets an das Internet eröffnen werden, und schließlich stellen die ISPs in der Regel das erforderliche Equipment für den WAN-Übergang, so daß das lokale Netz des Kunden direkt angeschlossen werden kann. Im letztgenannten Fall kann das durch den ISP gestellte Equipment oftmals eine zusätzliche Paketfilterung durchführen.

Alle genannten Komponenten sind in ein 19"-Chassis mit 4 Höheneinheiten eingebaut. Zusätzlich befinden sich ein Netzteil, zwei Lüfter und eine Anzeigeeinheit in diesem Chassis. Es verfügt über eine in vier Segmente aufgeteilt Backplane mit insgesamt 20 Slots (ein Segment ist also noch frei), wobei jedes Segment einen separaten PCI-Bus für Standard-Erweiterungskarten umfaßt.

3 Firewall-Software

Die iFSS/5-Schutzfunktionen werden durch diverse *proxy*-Server erbracht, die auf dem *bastion host* installiert sind.

Für die Dienste Telnet, FTP und HTTP(S) werden die *proxy*-Server aus dem frei verfügbaren *Firewall Toolkit* der Fa. *Trusted Information Systems* (TIS-FWTK) verwendet [6]. (Neben diesem Toolkit gibt es noch weitere freie Implementierungen von Firewall-Systemen; das TIS-FWTK wurde ausgewählt, da es vielfach verwendet und gut dokumentiert ist.) Die Arbeitsweise dieser *proxy*-Server wird durch eine Menge von Regeln beschrieben, die in der sog. *Net Permission Table* gemeinsam für alle *proxy*-Server abgespeichert sind. Das formulierbare Regelwerk ist sehr rudimentär, aber dies ist wohl als Ausdruck der Tatsache zu werten, daß das TIS-FWTK, das im Quellcode zur Verfügung gestellt wird, dazu einladen will, eigene Erweiterungen bzw. Detaillierungen der Schutzfunktionen vorzunehmen.

Eine besondere Schwierigkeit bei der Formulierung der Regeln für den FTP- und den HTTP-*proxy* bestand darin, daß Regeln für drei Zugriffswege formuliert werden mußten:

- aus dem Intranet auf Server im externen Netz (im iFSS/5 unbeschränkt, s. Ausblick!),
- aus dem Intranet auf die Server auf dem *outside host* (für die Ablage und Ansicht von öffentlich zugänglichem Informationsmaterial) und
- aus dem externen Netz auf die Server auf dem *outside host* (nur für die Ansicht des öffentlich zugänglichen Informationsmaterials).

Eine detaillierte Diskussion der damit verbundenen Probleme erfolgt in Zusammenhang mit den entsprechenden Diensten in folgenden Abschnitt 4.1, in dem auch auf die Funktion eines zusätzlich verwendeten sog. *plug*-Gateways eingegangen wird, über das eine „Durchschaltung“ zu einem fest definierten Server hergestellt wird.

1. Die Abkürzung ISP bedeutet *Internet Service Provider*.

Ebenfalls mit Komponenten des TIS-FWTK wird der e-Mail-Dienst vor unberechtigten Zugriffen geschützt, nämlich mit den *smap/smapi*-Komponenten, die man zusammengenommen als *proxy*-Server für e-Mail betrachten kann. Eine detaillierte Diskussion erfolgt in Abschnitt 4.2.

Die Sicherung des *Domain Name Service* erfolgt durch eine Aufteilung der Gesamtfunktion in eine externe Namensauflösung, die nur die symbolischen Namen auflöst, die dem *bastion host* zugeordnet sind, und in eine interne Namensauflösung, die alle im Intranet vorhandenen Namen auflöst. Eine detaillierte Diskussion erfolgt in Abschnitt 4.3.

Auf den Telnet- und den News-Dienst wird hier aus Platzgründen nicht eingegangen.

4 Diensteangebot und Server

Für den Aufbau eines Intranets stellt das iFSS/5 eine geschützte Infrastruktur zur Verfügung. Konkret werden in der Standardkonfiguration Server für die folgenden Dienste bereitgestellt:

1. Austausch von e-Mail im Intranet und zwischen Intranet und externem Netz,
2. ein interner und ein externer WWW-Dienst,
3. ein interner und ein externer FTP-Dienst,
4. ein *Telnet*-Dienst aus dem Intranet in das externe Netz,
5. ein interner News-Dienst mit einem *News Feed* aus dem Internet,
6. ein interner und ein externer Dienst für die Namensauflösung.

Die Hardware-Konfiguration mit *inside host* und *outside host* legt den Gedanken nahe, daß sich die Dienste, die über das iFSS/5 bereitgestellt werden, einfach in interne und externe Dienste gliedern lassen. Dies trifft jedoch nur bei einigen Diensten wie WWW und FTP zu, wo jeweils zwei Server eingerichtet werden, die voneinander unabhängig sind. Andere Dienste, insbesondere *e-Mail*, *News* und *DNS*, implizieren einen „grenzüberschreitenden“ Transport von Nachrichten bzw. Request-/Reply-Paketen und werden deshalb von mehreren kooperierenden Komponenten erbracht, die je nach Dienst in unterschiedlicher Art und Weise den iFSS/5-Hosts zugeordnet werden. Dienste mit separater interner und externer Infrastruktur werden im folgenden Kapitel dargestellt. Als Stellvertreter für grenzüberschreitende Dienste werden im Kapitel 4.2 der e-Mail-Dienst und im Kapitel 4.3 der *Domain Name Service* erläutert.

4.1 Separate Intranet-/Internet-Services

Server für die nur intern angebotenen WWW- und FTP-Dienste sind auf dem *inside host* installiert. Die internen Clients können die entsprechenden internen Server ohne den Umweg über einen *proxy*-Server erreichen.

Aus dem externen Netz erreichbare FTP- und WWW-Server sind auf dem *outside host* realisiert. Durch die Anordnung dieses Hosts im *secure subnet* des iFSS/5 können die entsprechenden Server vor Angriffen geschützt werden, da diese Server nicht direkt mit der Außenwelt kommunizieren.

Diese Konfiguration bringt allerdings ein Problem mit sich, wenn man den Zugriff von Clients betrachtet, die aus dem externen Netz auf das öffentliche Informationsangebot auf dem *outside host* zugreifen wollen. Diese Clients „wissen nicht“ (und können es auch nicht wissen), daß sie auf einen *proxy*-Server zugreifen, sie betrachten die Adresse des *bastion host* als die eigentliche Server-Adresse. Wie können externe Clients dennoch den *outside host* erreichen?

Um das gestellte Problem zu lösen, muß auf dem *bastion host* für jeden Server auf dem *outside host* eine sog. *plug*-Funktion installiert sein. Ein *plug*-Funktion schaltet eingehende Requests automatisch an eine definierte Adresse durch, ohne daß der Benutzer dies zuvor berücksichtigen muß oder erkennen kann. Diese *plug*-Funktion wird entweder über ein eigenes sog. *plug*-Gateway erbracht (wie beim WWW-Dienst), oder sie wird von einem *proxy*-Server erbracht (wie beim FTP-*proxy*). Die Umlenkung und die damit verbundene Definition der Adresse, zu der hin umgelenkt wird, erfolgt z.B. beim *plug*-Gateway durch folgende Regel:

```
plug-gw: permit-hosts * -plug-to <outside host addr>
```

Diese Regel ist wie folgt zu interpretieren: Hosts mit beliebiger Adresse wird der Zugriff gestattet, aber alle Zugriffe werden an die Adresse <outside host addr> weitergeleitet.

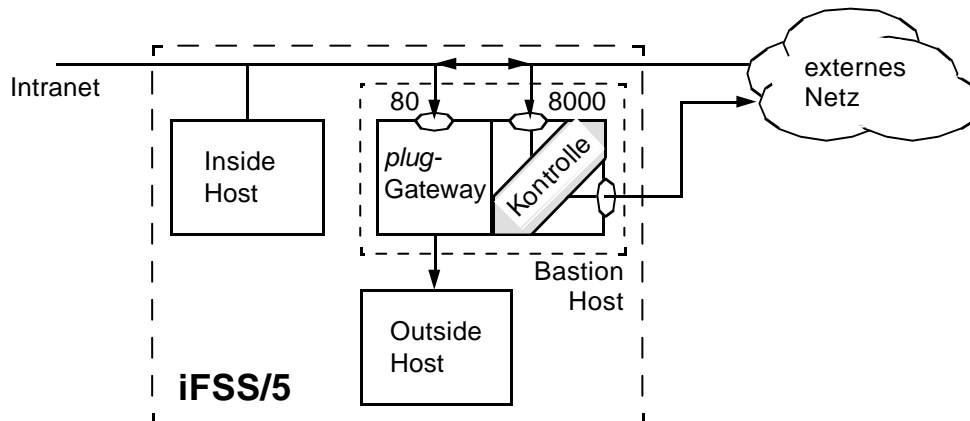


Bild 3: Zugriff auf Dienste über ein *plug*-Gateway

Die Einrichtung von *plug*-Funktionen löst also das Problem für externe Clients; sie hat aber auch eine wichtige Konsequenz für die internen Benutzer: Interne Clients müssen ja auf beide Arten von Servern zugreifen können: auf Server auf dem *outside host* und auf Server im ex-

ternen Netz. Server auf dem *outside host* erreichen interne Benutzer ebenfalls über die *plug*-Funktion¹, Server im externen Netz erreichen sie über einen *proxy*-Server ohne *plug*-Funktion. Diese beiden Wege müssen offensichtlich „auseinandergefahren“ werden.

Wie dieses „Auseinandergefahren“ bewerkstelligt wird, hängt davon ab, ob ein separates *plug*-Gateway benutzt wird, oder ob die *plug*-Funktion in den *proxy*-Server integriert ist. Beim Einsatz eines separaten *plug*-Gateways werden dem *plug*-Gateway und dem *proxy*-Server unterschiedliche TCP-Ports zugeordnet (Bild 3; die angegebenen Port-Nummern beziehen sich auf den WWW-Dienst). In der Regel wird man so verfahren, daß man dem *plug*-Gateway den *well-known*-Port des jeweiligen Dienstes zuordnet und dem *proxy*-Server einen davon verschiedenen. Ist – anders als im Bild 3 dargestellt – die *plug*-Funktion im *proxy*-Server enthalten, so erfolgt das Auseinandergefahren der Zugriffswege innerhalb des *proxy*-Servers, wo es durch Regeln gesteuert wird.

Die Verwendung von internen und externen Servern hat selbstverständlich einen Einfluß auf die Konfiguration der Clients im Intranet. Diese müssen so konfiguriert sein, daß sie grundsätzlich einen *proxy*-Server benutzen, der ja für alle Zugriffe auf Server im externen Netz notwendig ist. Der *Netscape Navigator* z.B. verfügt über eine entsprechende Konfigurationsoption, in dem Adresse und Port für den jeweiligen *proxy*-Server genannt werden müssen. Um auf Server auf dem *inside host* zugreifen zu können, müssen interne Zugriffe in der Client-Konfiguration jedoch von der Benutzung eines *proxy*-Servers ausgenommen werden. Im *Netscape Navigator* gibt es deshalb im gleichen Menü eine Zusatzoption: „*Do not use proxy servers for domains beginning with ...*“, in der der im Intranet verwendete Namensraum anzugeben ist.

Es folgen einige Hinweise zu spezifischen Details des WWW-Dienstes und des FTP-Dienstes.

Für den WWW-Dienst ist sowohl auf dem *outside host* als auch auf dem *inside host* jeweils ein *Apache Web Server* eingerichtet, auf denen öffentliche bzw. nur intern zugängliche Informationen vorgehalten werden. Der Zugriff auf den WWW-Server auf dem *outside host* erfolgt durch ein separates *plug*-Gateway. Es ist so eingerichtet, daß es Anfragen auf dem Standard-HTTP-Port 80 entgegennimmt und diese immer an den externen WWW-Server umlenkt. Dies gilt auch, wenn die Anfrage aus dem Intranet stammt. Auf beliebige WWW-Server im externen Netz greifen Intranet-Clients über das sog. *http-gw* zu, das Bestandteil des TIS-FWTK ist und als *proxy*-Server für den HTTP-Netzverkehr fungiert. Im iFSS/5 ist dieser *proxy*-Server

1. D.h., daß interne ebenso wie externe Benutzer für die fraglichen Server auf dem *outside host* die Adresse des *bastion host* angeben müssen.

so konfiguriert, daß er HTTP-Requests aus dem Intranet über den Port 8000 annimmt und alle anderen HTTP-Requests abweist (Bild 3). Die folgende Tabelle faßt die notwendigen Einstellungen für die Clients im Intranet zusammen.

Intranet-Zugriff auf WWW-Server		Server auf dem <i>inside host</i>	Server auf dem <i>outside host</i>	Server im externen Netz
Konfiguration des Intranet-Client	<i>proxy</i>	nein	nein	ja
	Port	http-/https-Ports	<i>plug</i> -Port (80)	<i>proxy</i> -Port (8000)
anzugebende Server-Adresse		<i>inside</i>	<i>bastion</i>	Server-Adr.

Tabelle 1: Konfiguration der HTTP-Clients im Intranet

Ähnlich wie für den WWW-Dienst sind auch für den FTP-Dienst separate FTP-Server sowohl auf dem *outside* als auch auf dem *inside host* eingerichtet. Als Server-Programm wird das `proftpd`-Paket verwendet, dessen Konfigurationsdateien genauso strukturiert sind wie die Konfigurationsdateien des *Apache Web Servers*.

Die Datenbereiche beider Server sind unterteilt in einen Bereich für *anonymous ftp* und einen Bereich, auf den nur nach Authentifizierung zugegriffen werden kann. Aus beiden Datenbereichen kann nur gelesen werden. Zusätzlich ist auf jedem Server ein dritter Datenbereich eingerichtet, der sog. *incoming*-Datenbereich, in den nur geschrieben werden kann. Durch diese Restriktion wird verhindert, daß der FTP-Server als Zwischenstation für illegale Transaktionen wie z.B. die Verteilung von Raubkopien mißbraucht werden kann.

Der FTP-Dienst wird durch einen *proxy*-Server, der auf dem *bastion host* läuft, vor unerwünschten Zugriffen geschützt. Es handelt sich um das FTP-Gateway *ftp-gw* aus dem TIS-FWTK, das durch einen Zusatz um die benötigte *plug*-Funktion erweitert wurde.

4.2 Der e-Mail-Dienst

Der in einem Intranet einzurichtende e-Mail-Dienst soll es ermöglichen, daß Intranet-Benutzer sowohl untereinander elektronische Nachrichten austauschen können, als auch mit beliebigen Benutzern im externen Netz. Ein Firewall-System muß also e-Mail in beiden Richtungen passieren lassen.

Mail-Systeme sind in der Vergangenheit häufig das Ziel von Angriffen gewesen. Diese Angriffe wurden dadurch erleichtert, daß die für den Transfer von e-Mail zuständigen *Message Transfer Agents* (MTAs) – z.B. das Programm *sendmail* – sehr komplex sind und damit auch Fehler aufweisen, die Angreifer in geschickter Art und Weise für das unautorisierte Eindringen in Netze zu nutzen wußten. Deshalb darf in einem Firewall-System keinesfalls ein komplexer MTA die Schnittstelle zum externen Netz bilden.

Weiterhin sollen auf dem *bastion host*, der die Schnittstelle zum externen Netz bildet, auf keinen Fall die Mailboxen der Benutzer eingerichtet sein, in denen die für die Intranet-Benutzer von extern eingetroffene Mail zwischengespeichert wird. Diese müssen für Angreifer unsichtbar bleiben.

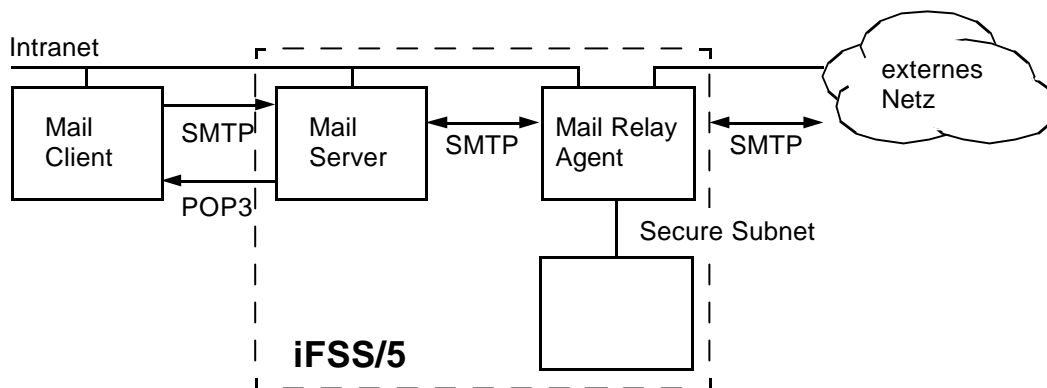


Bild 4: Dienstfunktionen für den e-Mail-Dienst

Um diesen Anforderungen zu genügen, wurde im iFSS/5 die für den e-Mail-Dienst erforderlichen Funktionalität in einen *Mail Relay Agent* und einen *Mail Server* aufgeteilt (Bild 4). Der *Mail Relay Agent* läuft auf dem *bastion host*, der *Mail Server* läuft auf dem *inside host*.

Im Vergleich zu einem MTA ist ein *Mail Relay Agent* ein wenig komplexes Programm: Ein *Mail Relay Agent* untersucht eingehende e-Mail lediglich danach, ob sie ins Intranet oder ins externe Netz gerichtet ist; im ersten Fall stellt er sie an den *Mail Server* im Intranet zu, im zweiten Fall stellt er sie an den adressierten *Mail Host* im externen Netz zu. Alle anderen Funktionen, die mit MTAs gewöhnlich verbunden sind (Umschreiben von Adressen, Verwaltung von Mailboxen, Zugriff auf Paßwort-Dateien usw.) entfallen hier. Aus dieser Reduzierung der Funktionalität resultiert ein Programm mit geringer Komplexität, dessen Widerstandsfähigkeit gegen Angriffe leichter getestet werden kann. Als Software für den *Mail Relay Agent* stellt das TIS FWTK die beiden zusammengehörigen Tools *smap* und *smapd* zur Verfügung. Durch die Aufteilung auf zwei Komponenten wurden – im Interesse einer weiteren Verringerung der Programmkomplexität – die sende- und die empfangsbezogenen SMTP-Funktionen voneinander separiert.

Der *Mail Server* im internen Netz empfängt eingehende e-Mail und speichert sie in Mailboxen zwischen, von denen die Benutzer sie über das POP3-Protokoll abholen können. Weiterhin ist er für die korrekte Weiterleitung von e-Mail ins externe Netz zuständig. Zur Einrichtung des Mail-Servers wurde wegen der bekannten Sicherheitsmängel und der schwierigen Konfigurierung nicht auf das weitverbreitete *sendmail*-Paket zurückgegriffen, sondern auf das frei erhältliche Paket *qmail*. Zusammen mit einigen Zusätzen bietet diese Software den gleichen Funktionsumfang wie *sendmail*, verfügt aber über wesentlich bessere und einfachere Konfigurationsmöglichkeiten. Die Sicherheit des *qmail*-Systems beruht unter anderem auf der Aufteilung der verschiedenen Funktionen eines Mail-Servers auf einzelne Programme, die für ihre Teilaufgabe spezialisiert sind. Diese Einzelprogramme laufen unter jeweils eigener Benutzererkennung, wodurch die Gefahr verringert wird, daß bei einem Einbruch über den e-Mail-Dienst ein Angreifer Superuser-Rechte erlangen kann.

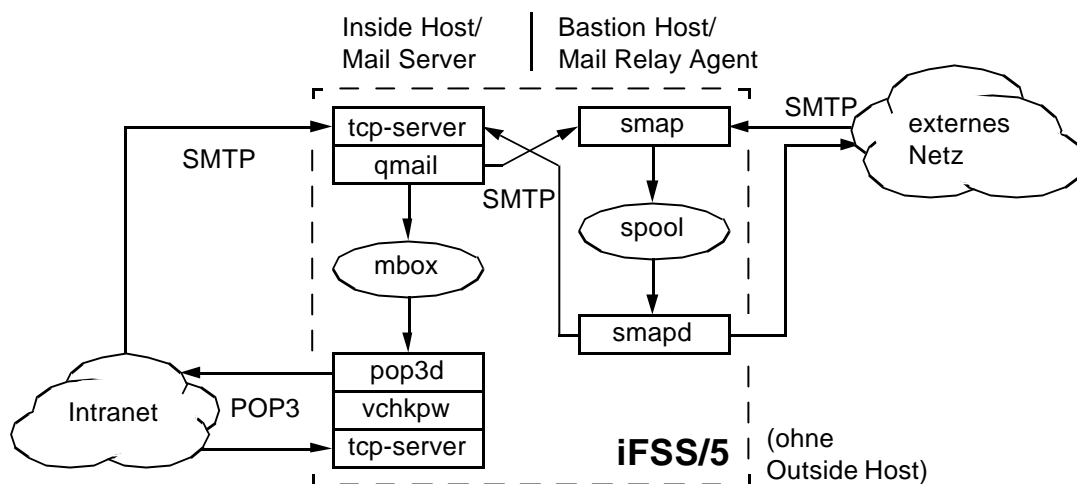


Bild 5: Komponenten für den e-Mail-Dienst

Bild 5 zeigt das Zusammenspiel der einzelnen Komponenten des e-Mail-Dienstes. Die Komponente *smap* (im *Mail Relay Agent*) ist dafür zuständig, e-Mails aus dem Intranet und dem externen Netz entgegenzunehmen und in einem Spool-Verzeichnis auf dem Bastion-Host zwischenspeichern. In periodischen Abständen prüft der *smap*-Dämon (*smapd*), ob Nachrichten im Spool-Verzeichnis liegen und sendet diese entsprechend der Empfängeradresse weiter. Nachrichten, die für Benutzer im Intranet bestimmt sind, werden an den Mail-Server zur Weiterbearbeitung verschickt, während alle anderen an die Zieladresse im externen Netz geleitet werden.

Alle beim Mail-Server eingehenden SMTP- und POP3-Anforderungen werden zur Erhöhung der Sicherheit nicht direkt vom Mail-Server entgegengenommen, sondern zuvor durch einen sog. *TCP wrapper* gefiltert¹. Im *iFSS/5* wird der *tcp-server* aus dem Softwarepaket *ucspi-tcp* verwendet, das frei verfügbar ist. So soll unter anderem verhindert werden, daß der Mail-Server von außerhalb mißbraucht wird, um etwa Nachrichten unter einem falschen Namen zu versenden.

Zur Einrichtung und Verwaltung der Accounts der Intranet-Benutzer kommt das Softwarepaket *vchkpw* zum Einsatz. Die Abkürzung *vchkpw* steht für „virtual check password“ und deutet an, daß das Tool zur Verwaltung virtueller Postfächer genutzt wird.

1. Unter einem *TCP wrapper* versteht man ein lokales „Vorschalt“-Programm, das vor einen Server geschaltet wird, eintreffende Datenpakete auf der TCP/IP-Stufe filtert und akzeptable Pakete an den zugeordneten Server weiterleitet. Im Gegensatz zu einem *proxy*-Server interpretiert ein *TCP wrapper* das jeweilige Anwendungsprotokoll nicht.

4.3 Domain Name Service

Der *Domain Name Service* (DNS) war in vielen Fällen der Ausgangspunkt von Angriffen: Angreifer nutzten die durch das DNS bereitgestellten Informationen, um eine Netzkonfiguration auszuspähen und sich dadurch eine geeignete „Einbruchstelle“ zu suchen. Eine andere Art von Angriffen richtet sich auf den Datenbestand von *Name Servern*: Durch Kompromittierung dieses Datenbestands (d.h. die Manipulation von *DNS Records*, mit denen Namen in Adressen aufgelöst werden) können Nachrichten umgelenkt und damit ein System nahezu vollständig von der Kommunikation mit dem externen Netz abgeschnitten werden. Deshalb ist auf die Sicherung dieses Dienstes besonderer Wert zu legen.

Im iFSS/5 wird der DNS durch die beiden folgenden Maßnahmen gesichert:

- Einrichtung eines internen und eines externen *Name Servers*
Durch die Einführung von zwei *Name Servern* können die zur Namensauflösung benötigten Datenbestände separiert werden: Der interne *Name Server* löst alle Anfragen auf, die aus dem Intranet kommen und die sich auf Hosts im Intranet beziehen. Der externe *Name Server* löst nur Namensanfragen für den *bastion host* auf. Der *bastion host* erscheint dabei ggf. unter verschiedenen Alias-Namen: z.B. *mail.<domain>*, *www.<domain>*, *ftp.<domain>* usw.
- Auch wenn der interne *Name Server* einen Namen aus dem externen Netz auflösen muß, so kommuniziert er dazu nicht direkt mit anderen *Name Servern* im externen Netz, sondern wendet sich dazu an einen *Name Server*, der auf dem *bastion host* installiert ist, und der als einziger *Name Server* im externen Netz für die betreffende Domain in Erscheinung tritt.¹

Bei der Realisierung stellte sich eine wichtige Frage: Auf welchen der Hosts des iFSS/5 sollen die beiden gewünschten *Name Server* angesiedelt werden? Nach der oben beschriebenen Zweiteilung in einen internen und einen externen *Name Server* scheint es naheliegend zu sein, in Analogie zum WWW- und zum FTP-Dienst den internen *Name Server* auf dem *inside host* und den externen *Name Server* auf dem *outside host* zu installieren, und dabei den externen *Name Server* über eine *plug*-Funktion zugänglich zu machen.

Leider erwies sich dieses Vorgehen auf der Basis verfügbarer Software als nicht durchführbar. Zur Begründung müssen drei Fälle unterschieden werden:

1. Ein interner Client stellt eine Anfrage, die sich auf die eigene Domain bezieht.
2. Ein externer Client stellt eine Anfrage, die sich auf einen nach extern sichtbaren Namen des *bastion host* bezieht.
3. Ein interner Client stellt eine Anfrage, die sich auf einen Host im externen Netz bezieht.

Die Fälle 1 und 2 sind offensichtlich unproblematisch: Der interne *Name Server* kann auf dem *inside host* installiert werden, und der externe *Name Server* kann auf dem *outside host* installiert werden. Für den externen *Name Server* wird auf dem *bastion host* ein *plug*-Gateway in-

1. Selbstverständlich muß es für diesen *Name Server* noch einen *Secondary Name Server* geben. Dieser Umstand wird hier jedoch nicht diskutiert.

stalliert, das externe Anfragen an den *outside host* weiterleitet. Schwieriger ist der Fall 3. Da der interne *Name Server* eine solche Anfrage nicht auflösen kann, muß er sie an einen anderen *Name Server* auf dem *bastion host* weiterleiten. Bei der vorgestellten Konfiguration steht dort aber unter dem DNS-Port das *plug-Gateway* bereit und leitet eintreffende Anfragen an den *outside host* weiter. Der dort befindliche *Name Server* kann die entsprechende Anfrage jedoch nicht beantworten ...

Auch der Trick, den wir beim WWW-Dienst zur Umgehung dieses Problems angewendet hatten, nämlich die Verwendung von zwei unterschiedlichen Ports (hier analog: der Standard-Port für das *plug-Gateway*, ein anderer Port für das Durchreichen von Anfragen aus dem Intranet ins externe Netz), scheidet hier aus, da die *Resolver Libs* auf den Rechnern im Intranet ähnlich dazu wie die HTTP-Clients konfigurierbar sein müßten. Solche *Resolver Libs* sind jedoch leider nicht verfügbar.

Quintessenz: Soll der externe *Name Server* auf dem *outside host* untergebracht werden, so wird ein „echter“ *DNS-proxy* mit integrierter *plug-Funktion* benötigt, der unterscheiden kann, ob eine externe Anfrage vom externen *Name Server* des iFSS/5 aufgelöst werden soll, oder ob eine interne Anfrage an einen *Name Server* im externen Netz durchgereicht werden soll. Leider erwies sich die Suche nach einem solchen *DNS-proxy* als erfolglos.

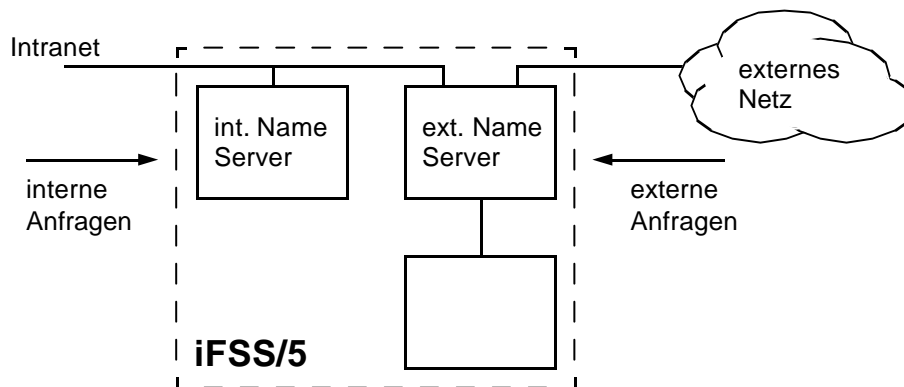


Bild 6: DNS-Konfiguration

Um das Problem zu lösen, wurde der externe *Name Server* auf dem *bastion host* eingerichtet (Bild 6). Dieser bearbeitet Anfragen aus dem externen Netz und aus dem Intranet; Anfragen aus dem Intranet gelangen nur dann zu ihm, wenn sie vom internen *Name Server* nicht aufgelöst werden können.

Der Datenpool des internen *Name Servers* verfügt über sämtliche Informationen zur Domain, inklusive der Namensauflösungen für den *bastion host*. Damit ist dieser *Name Server* so eingerichtet, daß er alle Anfrage aus dem Intranet auflösen kann, die die eigene Domain betreffen. Anfragen aus dem Intranet nach internen Namen, für die keine Auflösungen vorhanden sind, reicht der interne *Name Server* nicht an den externen *Name Server* weiter, sondern beantwortet die Anfrage mit einer Fehlermeldung. Der interne *Name Server* leitet lediglich solche Anfragen weiter, die nicht die eigene Domain betreffen. Diese Anfragen werden ausschließlich an den externen *Name Server* weitergeleitet, um so nur einen einzigen, kontrol-

lieberbaren Weg für diesen Dienst durch das iFSS/5 zu öffnen. Der externe *Name Server* ist damit als einziger *Name Server* in der Lage, für das gesamte Intranet Kontakt mit übergeordneten *Name Servern* im externen Netz aufzunehmen.

Bei der Umsetzung des DNS wurde auf die frei erhältliche Referenzimplementierung des *Internet Software Consortiums (ISC)* zurückgegriffen, nämlich das Softwarepaket *bind*.

5 Administration des iFSS/5

5.1 Übersicht

Das gesamte iFSS/5 umfaßt, wie gezeigt wurde, eine große Anzahl von Softwarekomponenten, die über eigene Konfigurationsdateien konfiguriert werden müssen. Diese Konfigurationsdateien sind nicht nach einem einheitlichen Muster aufgebaut und enthalten teilweise überschneidende Informationen. Um dem Administrator bei der Systemkonfiguration das Leben einfacher zu machen und um die Konfigurationsdaten konsistent zu halten, wurde deshalb für das iFSS/5 ein Werkzeug für die einheitliche Systemadministration (Bild 7) entwickelt.

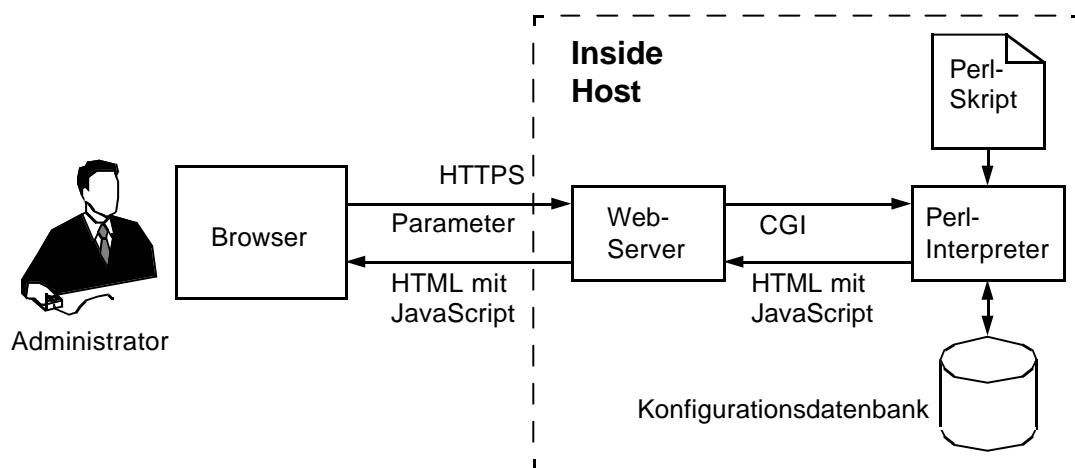


Bild 7: Schematischer Aufbau des Administrationstools

Dieses Administrationstool ist auf dem *inside host* installiert. Es verfügt über ein HTML-basiertes Frontend und kann über jede Station im Intranet benutzt werden. Zur Sicherung der Kommunikation im Intranet wird das HTTPS-Protokoll verwendet, über das sich der Web-Server¹ gegenüber dem Browser authentifiziert und mit dessen Hilfe die übertragenen Datenströme verschlüsselt werden. Der Administrator muß sich gegenüber dem Web-Server durch Eingabe von User-Id und Paßwort authentifizieren.

1. Es handelt sich hier um den schon erwähnten *Apache Web Server*.

Der Web-Server kommuniziert mit dem eigentlichen Administrationstool über die CGI-Schnittstelle. Das Administrationstool ist in der Programmiersprache *Perl* geschrieben. Es erzeugt HTML-Ausgaben, in denen ggf. JavaScript-Programme enthalten sind. Der Einsatz von JavaScript war notwendig, da mehrere Browser-Fenster verwaltet werden müssen.

Die Administration des iFSS/5 verläuft in drei Schritten, die ggf. mehrfach durchlaufen werden: Navigation, Konfiguration und Systemabgleich. Sie werden im folgenden erläutert.

5.2 *Navigation*

Um das iFSS/5 gezielt konfigurieren zu können, muß dem Benutzer in der graphischen Schnittstelle des Administrationstools ein Modell des Systems präsentiert werden, so daß er zu den „Stellen“ hinnavigieren kann, die jeweils bearbeitet werden sollen. Für die Entwicklung eines solchen Modells bestanden zwei Optionen.

Zum einen wäre es möglich gewesen, das iFSS/5 als ein System aus drei Rechnern darzustellen und die damit die Navigation an dieser inneren Struktur auszurichten. Diese Option wurde schnell verworfen, da die Komplexität des inneren Aufbaus des iFSS/5 vor dem Administrator verborgen werden soll, da diese für das Verständnis der Funktionsweise des iFSS/5 irrelevant ist und das iFSS/5 vielmehr als eine geschlossene *black box* erscheinen soll.

Die zweite – und auch realisierte – Option besteht darin, die Sicht auf das System diensteweise aufzuschlüsseln. Der Administrator konfiguriert also nicht ein Hardwaresystem, sondern er konfiguriert die einzelnen Dienste, die vom iFSS/5 erbracht werden. Die Konfiguration ist also losgelöst vom Hardwaresystem des iFSS/5; das iFSS/5 erscheint dem Administrator vielmehr als ein geschlossener Block, der über zwei Netzwerkschnittstellen verfügt, einer Intranet-Schnittstelle und einer Schnittstelle zum externen Netz. Entsprechend teilen sich mehrere Dienste in zwei Komponenten auf.

Das Administrationstool sieht dienstespezifische Sichten auf die folgenden Dienste vor: WWW (intern und extern), FTP (intern und extern), Telnet, e-Mail, News und DNS.

5.3 *Konfiguration und Systemabgleich*

Eingaben und Änderungen von den Dienst-Parametern erfolgen über eine HTML-basierte graphische Schnittstelle, in der die Metapher der Kartei verwendet wird. Die Einstellungsmöglichkeiten eines Dienstes verteilen sich auf mehrere, optisch hintereinander angeordnete Karteikarten. Jede ist mit einem Thema überschrieben. Der Kartenwechsel erfolgt über die Anwahl des Themas, welches auf der Lasche oberhalb der Karteikarte dargestellt ist.

Die vom Administrator eingegebenen Daten werden nach Betätigung der „Übernehmen“-Schaltfläche, wie sie in HTML-basierten Benutzerschnittstellen üblich ist, noch nicht sofort wirksam. Die Betätigung dieser Schaltfläche löst zunächst eine Plausibilitätsprüfung der eingegebenen Daten durch das Administrationstool aus. So werden z.B. in einem Eingabefeld für eine IP-Adresse keine Buchstaben angenommen. Solche Fehler werden dem Administrator in der Karteikarte mit einer roten Warn-oder Fehlermeldung angezeigt. Zusätzlich wird in einer

Dialogbox ein Hinweis auf den Eingabefehler gegeben. Weiterhin werden alle Parameter, die vom aktuellen Stand auf dem iFSS/5 abweichen, besonders hervorgehoben. Plausibilisierte Daten werden in der Konfigurationsdatenbank des Administrationstools zwischengespeichert.

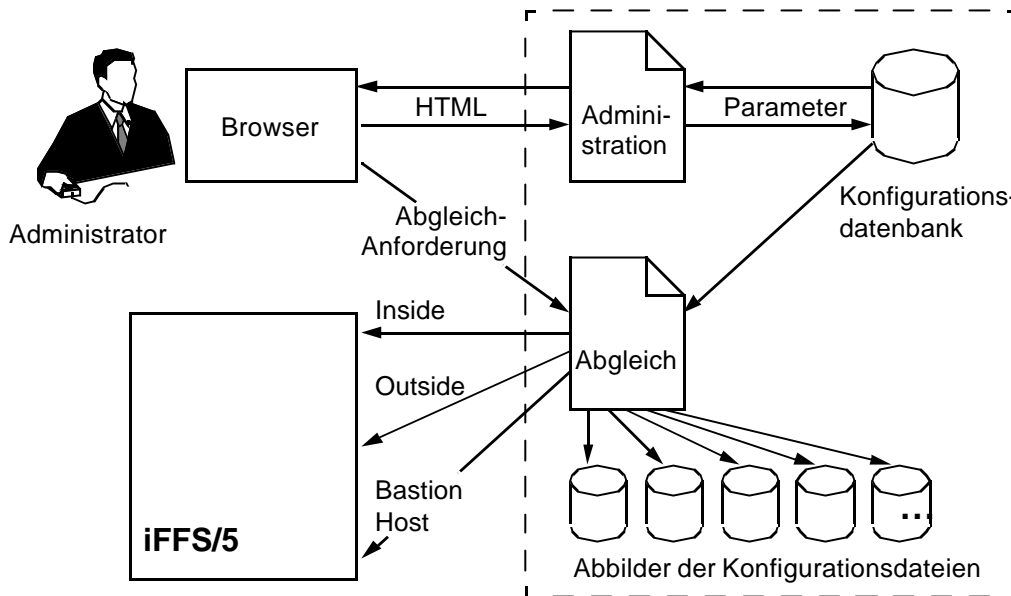


Bild 8: Arbeitsweise des Administrationstools

Nach Eingabe und Plausibilisierung aller Eingaben kann der Administrator einen sog. Systemabgleich – für alle Dienste oder selektiv für einzelne Dienste – einleiten (Bild 8). Mit dem Systemabgleich werden die neu eingegebenen Daten aus der Konfigurationsdatenbank des Administrationstools extrahiert und in Abbilder der Konfigurationsdateien übernommen, die im Administrationstool vorhanden sind. Schließlich werden die neu erzeugten Abbilder mit Hilfe des Softwarepaketes *Secure SHell* (SSH) zu den drei Rechnern des iFSS/5 transferiert, und dort werden damit die vorhandenen Konfigurationsdateien überschrieben. Auf diese Weise braucht der Administrator alle Konfigurationsdaten nur einmal eingeben, und die Konfigurationsdateien bleiben konsistent. Nach dem Dateitransfer werden bei Bedarf die entsprechenden Dienste neu gestartet.

Bei all diesen Arbeiten wird der Administrator durch ein umfangreiches Hilfesystem unterstützt.

6 Ausblick

Das iFSS/5 befindet sich im erfolgreichen praktischen Einsatz im Fachbereich Informatik der FH Gelsenkirchen. Es arbeitet stabil und bildet die Basis für eine Reihe bereits begonnener oder erst geplanter Weiterentwicklungen. Diese beziehen sich auf die folgenden Problemstellungen:

- Das vorhandene Logging-System muß ausgebaut und seine Bedienung vereinfacht werden.
- Durch Hinzufügung von Redundanzen muß das System sicher gegen Ausfälle gemacht werden.
- Eine Komponente für die *Intrusion Detection* muß dem System hinzugefügt werden
- Wünschenswert ist die Entwicklung eines DNS *proxy*-Servers mit den oben beschriebenen Eigenschaften.
- Durch eine Weiterentwicklung der *proxy*-Server des TIS-FWTK soll es möglich gemacht werden, noch detailliertere Zugriffskontrollregeln anzugeben. Durch solche Regeln können z.B. auch Zugriffe von intern nach extern auf Anwendungsebene ausgefiltert werden, wenn es z.B. das Ziel ist, unerwünschte Zugriffe auf bestimmte WWW-Seiten im Internet unterbinden zu können usw.
- Die angeführten Relays können mit zusätzlicher Filterfunktion versehen werden, z.B. mit Virenscannern für eingehende e-Mails.

In einer anderen Richtung der Weiterentwicklung, die den Problembereich der Firewall-Systeme verläßt, soll dem iFSS/5 die Funktionalität eines *Security Gateway* (SG) im Sinne von IPsec (RFC-2401) hinzugefügt werden. Die Kombination aus Firewall und Security Gateway erlaubt es, auf sichere Art und Weise mehrere Intranet-Teilnetze über das öffentliche Internet zu einem geschützten Virtuellen Privaten Netz zusammenzubinden. Es wird davon ausgegangen, daß diese Technik in Zukunft eine große Bedeutung für die Kommunikationsinfrastruktur von Unternehmen und Organisationen haben wird.

Danksagung

Den Studenten Benedikt Heitmann, Marc Jung und Andreas Schouten sei für die engagierte Durchführung ihrer Diplomarbeit gedankt, deren Ergebnisse die Grundlage für das iFSS/5 bilden. Diese Arbeit wurde als Gruppenarbeit angefertigt, und der Erfolg gibt dieser Form der Abschlußarbeit mehr als Recht. Ein herzliches Dankeschön auch an Hn. Dr. Michael Rietz von der Articon AG in München, der wichtige Hinweise für die Entwicklung der Systemkonfiguration gegeben hat. Keinesfalls vergessen werden soll hier Hr. Dirk Bugzel, der durch tatkräftige Unterstützung der Studenten, durch ständige Diskussionsbereitschaft und durch die Öffnung von Perspektiven für weitere Arbeiten ebenfalls erheblich zum Gelingen beigetragen hat.

Literatur

- [1] Chapman, D.B., Zwicky, E.D.:
Building Internet Firewalls.
Sebastopol (O'Reilly & Associates) 1995, ISBN 1-56592-124-0.
- [2] Cheswick, W.R., Bellovin, St.M.:
Firewalls und Sicherheit im Internet.
Bonn u.a. (Addison-Wesley), ISBN 3-89319-875-X.
- [3] Heitmann, B., Jung, M., Schouten, A.:
Konzeption und Aufbau eines integrierten Firewall-/Server-Systems.
Diplomarbeit im Fachbereich Informatik der Fachhochschule Gelsenkirchen, 1998.
- [4] Rekhter, Y., Moskowitz, B., Karrenberg, D., de Groot, G. J., Lear, E.:
Address Allocation for Private Internets .
RFC-1918, Feb. 1996.
- [5] Strobel, St.:
Firewalls für das Netz der Netze.
Heidelberg (dpunkt) 1997, ISBN 3-920993-31-4.
- [6] Trusted Information Systems:
TIS Internet Firewall Toolkit.
<http://www.tislabs.com>