



Institut für Telematik

unter Betreuung der
Fraunhofer Management GmbH

Internet / Intranet

Preprint 98-15

ISSN 1433-8106

Dipl.-Inform. E.-G. Haffner

Dr. T. Engel

Prof. Dr. Ch. Meinel

Flood-Gates statt Firewalls –

Eine „High Security“-Lösung zum sicheren Datenaustausch
zwischen Internet und Intranet

Abstract.....	2
Sicherheit im Internet.....	2
Flood-Gates.....	4
Praxis der Flood-Gates.....	6
Zusammenfassung und Ausblick.....	7
Literaturverzeichnis.....	8

Abstract

Die klassische Rolle der *Firewall* besteht darin, ein unternehmensweites Intranetz vor dem unberechtigten Zugriff aus dem Internet zu schützen. Wenn die Sicherheitsbedürfnisse des Unternehmens jedoch enorm hoch sind und der Informationsfluß zwischen dem internen Netz und der „weiten Welt“ nicht interaktiv (durch sog. „Browser“) erfolgen muß, sondern ein passiver Informationsaustausch (z.B. Transfer sicherheitsrelevanter Dokumente, E-Mails u.a.) genügt, so empfiehlt sich der Einsatz der „*Flood-Gates*“, der mit vergleichsweise geringem Konfigurationsaufwand höchste Sicherheitsvorgaben erfüllt.

Die Funktionsweise dieser Flood-Gates entspricht dabei dem Passieren einer Schleuse: Zu keinem Zeitpunkt besteht eine direkte Verbindung zwischen Intranet und Internet, sondern je nach Zustand der „Schleusentore“ findet der Informationsaustausch nur jeweils mit einer Seite der Kommunikationspartner statt.

Sicherheit im Internet

Das „Internet“ ist ein Oberbegriff für den Zusammenschluß verschiedener Rechnernetzwerke, deren gemeinsames Protokoll TCP/IP¹ den Informationsaustausch an beliebigen Knotenpunkten ermöglicht. Ursprünglich als Wissenschaftsnetz konzipiert, hat sich durch die Einführung multimedialer Übertragungsprotokolle und –sprachen wie HTTP² und HTML³ das Internet inzwischen zu einem gigantischen Kommunikationsmedium entwickelt und längst haben kommerzielle Unternehmen, darunter Dienstleister, Industrie und Handel die Möglichkeiten des neuen Mediums erkannt [ME97], [MEM97].

Allerdings wachsen mit den Chancen des Netzes auch seine Risiken. Nicht allein unberechtigte, räuberische Zugriffe auf das Firmennetz sind abzuwehren, auch unbeabsichtigte Preisgabe sensibler Daten, Kunden-, Personal- oder Unternehmensinformationen müssen geschützt werden und dürfen „von außen“ nicht einzusehen sein.

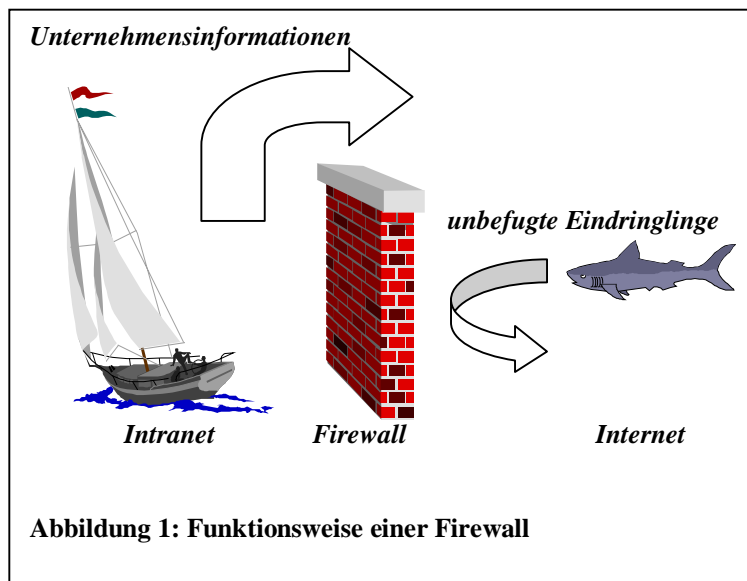
Das Standardverfahren zum Schutze der eigenen Daten gegen unbefugten Zugriff aus dem Internet sieht als Vermittlungsstelle zwischen Intranet und Internet eine sogenannte „**Firewall**“ vor: Aufgabe dieses Systems ist das Filtern von IP-Paketen durch Überprüfung von Quellen- und Zieladressen, TCP-Ports und den angeforderten Diensten. Die

¹ Transport Control Protocol/Internet Protocol

² Hypertext Transport Protocol

³ Hypertext Markup Language

Rechnersysteme im Intranet werden so „unsichtbar“ aus Sicht eines Beobachters von seiten des Internets. (vgl. Abbildung 1)



Eine derartige „Software-Lösung“ genügt jedoch den Sicherheitsexperten einiger Firmen nicht. Sie beunruhigt neben dem hohen Konfigurationsaufwand und einem nicht unerheblichen Kostenfaktor die Kreativität und kriminelle Energie unberechtigter Eindringlinge. Simulation zugriffsberechtigter IP-Nummern, „Schnüffeln“ von TCP/IP-Paketen und die mißbräuchliche Nutzung bestimmter TCP-Dienste machen in regelmäßigen Abständen negative Schlagzeilen und führen zur Verunsicherung der Unternehmensführung. Neuerlich zeigen sich etwa Schwachpunkte von Firewalls im Umgang mit ATM-Netzen [PP98], auch [LA94].

Immer wieder zeigt sich, daß Kommunikationsabläufe, die „eigentlich“ als sicher eingestuft wurden, durch raffinierte Tricks der „Hacker“ zu unberechtigtem Eindringen in das firmeneigene Netz geführt haben.

Natürlich werden enorme Anstrengungen unternommen, den Datentransfer im Internet sicherer zu machen [RA97]. Beispielsweise kann die Einführung des SSL⁴ zum Verschlüsseln der IP-Pakete als ein wichtiger Schritt in diesem Bestreben angesehen werden. Allein das Unbehagen bleibt. Wie kann die Kontrolle über den Datenfluß aus dem Internet auf klare und einfache Weise beim Unternehmen verbleiben?

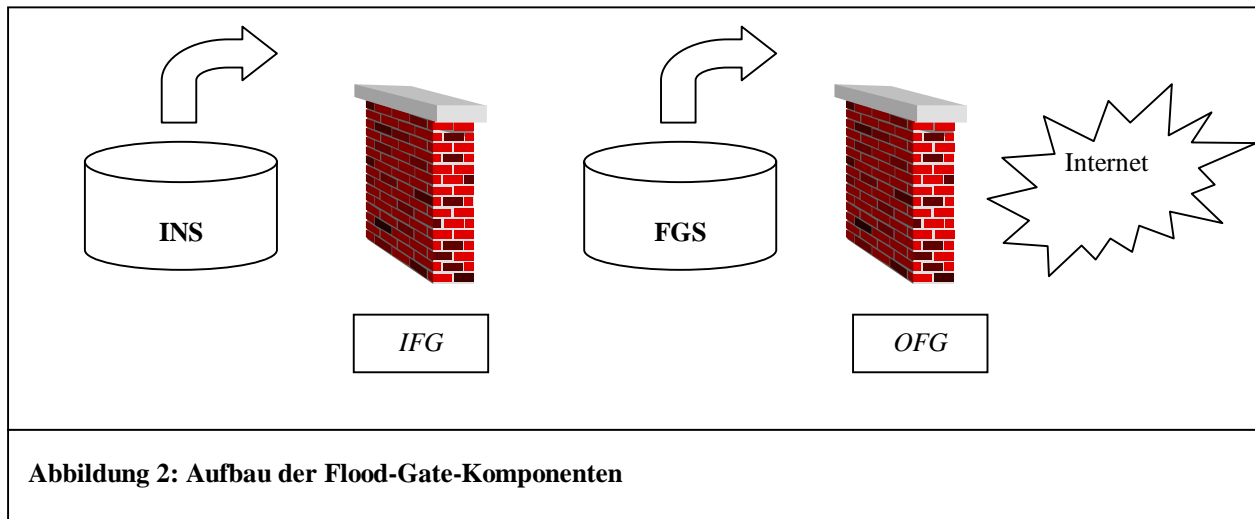
Hinzu kommt eine weitere, prekäre Anforderung bezüglich der Kommunikation aus dem Intranet in die „weite Welt“. Wie können Mitarbeiter davor geschützt werden, freiwillig oder unfreiwillig sensible Daten ins „Netz der Netze“ zu senden? Im allgemeinen wird der Datenaustausch in dieser Richtung weniger stark als Bedrohung thematisiert, doch was nützen Sicherheitsvorkehrungen wie das Entfernen lokaler Diskettenlaufwerke und die ausschließliche Verwendung von Fileserver-Speichermedien, wenn Mitarbeiter unerlaubt und unbeobachtet Daten ins Internet versenden?

⁴ Secure Socket Layer

Das Konzept der *Firewalls* wurde im Laufe der letzten Jahre stark verbessert und verfeinert, doch mit dem Anspruch der interaktiven Kommunikation zwischen Intranet und Internet lassen sich Restrisiken nicht vermeiden.

Flood-Gates

Hier setzt das Prinzip der *Flood-Gates* an: Die Flood-Gates setzen (mindestens) 2 voneinander unabhängige Rechnersysteme voraus, einen „Intranet-Server“ (*INS*) und einen „Flood-Gate-Server“ (*FGS*). Zwischen *INS* und *FGS* befindet sich das „innere Schleusentor“ (inner flood-gate, *IFG*) und zwischen *FGS* und dem Internet das „äußere Schleusentor“ (outer flood-gate, *OFG*). (vgl. Abbildung 2)



Physikalisch muß gewährleistet sein, daß zu keinem Zeitpunkt beide Schleusentore, *IFG* und *OFG*, geöffnet sind. Somit kann keine *durchgängige* Verbindung zwischen Intranet und Internet bestehen.

Alle Daten aus dem Intranet werden zum *INS* gesendet und hier eingehend analysiert (Phase 1). Erst bei geöffnetem *IFG* gelangen die „bereinigten Informationen“ in die „entmilitarisierte Zone“, den *FGS* (Phase 2). Anschließend wird das innere Schleusentor geschlossen und die auszutauschenden Daten befinden sich auf dem *FGS* (Phase 3). Hier finden allerdings, aus Gründen, die weiter unten erläutert werden, keine weiteren Analyseprozesse statt. Die Verweildauer der Informationen richtet sich nach den Anforderungen des Unternehmens und der Dringlichkeit der Inhalte. Sobald das *OFG* geöffnet ist, werden die Daten ins Internet gesendet (Phase 4). Zugleich können berechtigte oder gegebenenfalls auch unberechtigte Zugriffe von außen an den *FGS* erfolgen. In diesem Moment ist die Sicherheit des *FGS* nicht höher als die einer herkömmlichen Firewall, dennoch bleibt das Intranet des Unternehmens unangetastet, da *keine physikalische Verbindung* hierzu *aufgebaut werden kann*, solange der Kontakt zum Internet aufrecht erhalten bleibt!

Das OFG wird nach Austausch der Daten mit dem Internet-POP⁵ wieder geschlossen und die Daten verbleiben auf dem FGS (Phase 5). An dieser Stelle wird klar, warum der FGS die transferierten Informationen nicht analysieren darf: durch den direkten Kontakt mit dem Internet könnte der Analysemechanismus selbst durch unberechtigte Eindringlinge manipuliert worden sein.

Wenn im letzten Schritt das IFG erneut geöffnet wird und die Daten vom FGS zum INS gelangen (Phase 6), können zwar „infizierte“ Dateien im IFS abgelegt werden; dennoch besteht hier ein qualitativer Unterschied zur Funktionsweise von Firewalls. Anstatt „online“ alle Analyseprozesse durchzuführen, kann der INS ohne Bedrohung durch interaktive Manipulationen die „passiven“ Daten, die der FGS aus dem Internet erhalten hat, je nach gewünschter, skalierbarer Analysetiefe untersuchen und gegebenenfalls vernichten (Phase 7). Der Schwerpunkt dieser Untersuchungen richtet sich auf das Eindringen sogenannter „Trojanischer Pferde“, Daten, die selbst wiederum Prozesse ausführen und beispielsweise als Makroviren Schaden anrichten können⁶.

Interessant scheint auch die Perspektive zur semantischen Analyse von Texten. Dürfen bestimmte Inhalte das unternehmensweite LAN/WAN verlassen? Oftmals können derartige Entscheidungen nur durch menschliche Experten gefällt werden. Auch diese Option steht durch den Flood-Gate-Mechanismus zur Verfügung, weil die Analysezeiträume flexibel zu gestalten sind.

Tabelle 1 verdeutlicht den Zusammenhang zwischen den geschilderten Phasen und dem jeweiligen Zustand der beiden Schleusentore.

Phase	Beschreibung	IFG	OFG	Status
1	Analyse ausgehender Daten durch INS	geschlossen	geschlossen	α
2	Datentransfer vom INS zum FGS	offen	geschlossen	β
3	Warten des FGS auf Öffnung OFG	geschlossen	geschlossen	α
4	Datentransfer vom FGS ins Internet und in der Gegenrichtung	geschlossen	offen	γ
5	Warten des FGS auf Öffnung IFG	geschlossen	geschlossen	α
6	Datentransfer vom FGS zum INS	offen	geschlossen	β
7	Analyse eingehender Daten durch INS	geschlossen	geschlossen	α

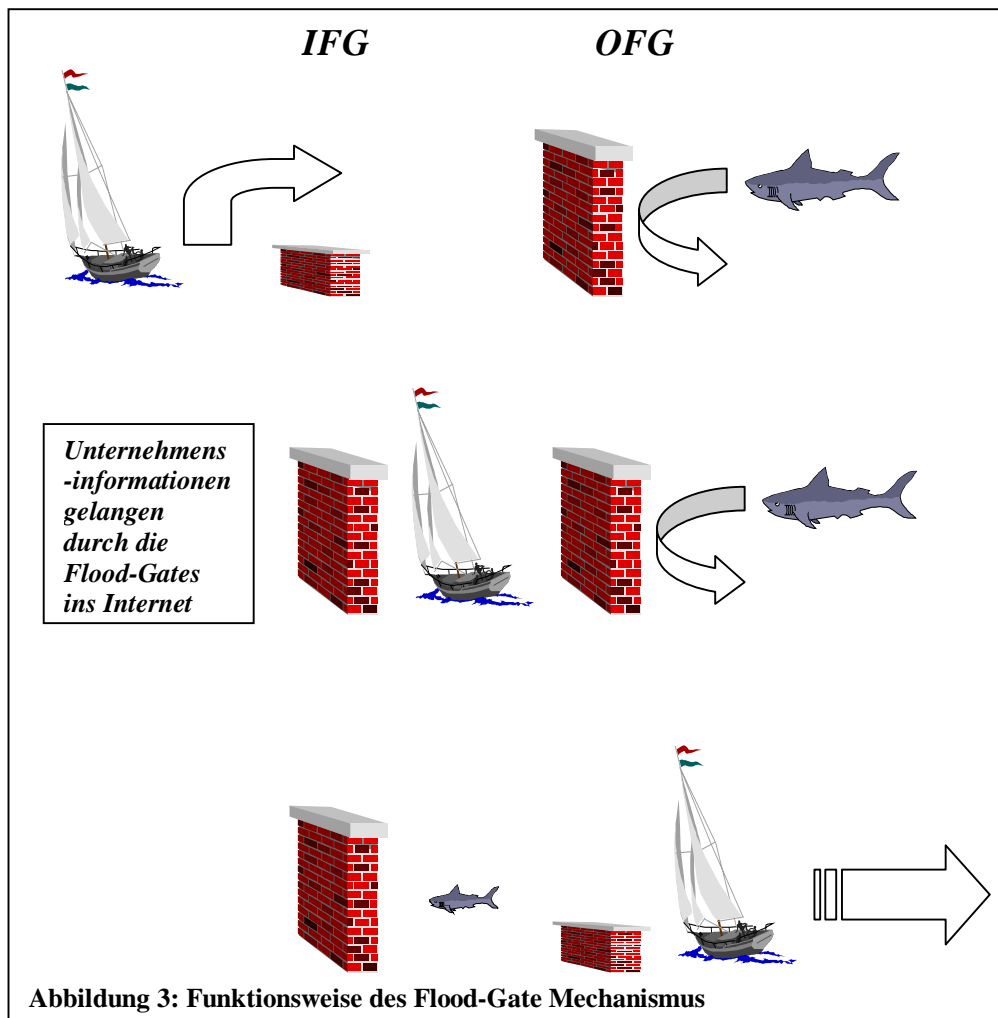
Tabelle 1: Phasen des Austauschmechanismus und Zustände der Flood-Gates

Der Tabelle 1 ist zu entnehmen, daß sich aufgrund eines identischen Schleusenzustands (Stati α , β oder γ) sowohl die Phasen 1, 3, 5 und 7 als auch die Phasen 2 und 3 gleichzeitig durchführen lassen. Die Phase 4 beinhaltet als Teilphasen die Datenausgabe ins Internet sowie deren Aufnahme.

Die folgende Abbildungen 3 verdeutlicht noch einmal die Funktionsweise der Flood-Gates. Zur besseren Übersicht werden allerdings nur die Phasen 2 bis 4 dargestellt.

⁵ Point of Presence. Nicht zu verwechseln mit dem Post-Office-Protocol zum Empfangen von Mails!

⁶ Jüngst ist es zwei Schülern gelungen, mittels eines solchen „Trojanisches Pferds“ unberechtigt in das Netz „T-Online“ einzudringen



Es zeigt sich, daß der physikalischen Trennung der beiden Flood-Gates IFG und OFG eine zentrale Rolle zukommt. Würde hier eine Software-Lösung anvisiert, könnte die Sicherheit des Gesamtsystems kaum höher als die herkömmlicher Firewalls eingestuft werden.

Praxis der Flood-Gates

Das oben beschriebene Verfahren wurde durch das *Institut für Telematik* konkret angewendet auf ein Mailaustausch-Verfahren einer großen Bank.

Ziel dieses Projektes war der sichere Datenaustausch zwischen der Bank und dem Internet. Die auszutauschenden Informationen beschränkten sich hierbei auf elektronische Post. Es mußte gewährleistet werden, daß sowohl die Nachrichtenübermittlung der Mitarbeiter ins Internet als auch die Analyse der eingehenden Daten aus dem Internet auf höchstem Sicherheitsniveau stattfinden sollte. Selbstverständlich haben diese E-Mails nicht den Status einer „privaten“ Post, die nur vom Empfänger dekodiert werden sollte (vgl. [LU98], [WE97]).

Wir entschieden uns für ISDN-PPP-Connections als Flood-Gates, um einen schnellen Verbindungsaufbau zu gewährleisten und einen ansehnlichen Datendurchsatz zu erzielen. Die beiden Server FGS und INS wurden durch Linux-PC's bereitgestellt.

Unser Flood-Gate-Konzept bestach durch das einfache Grundprinzip und seine offensichtlichen Sicherheitscharakteristika. Das Problem der physikalischen Trennung der Schleusen konnte von uns elegant gelöst werden, indem wir beide Server, INS und FGS, an **denselben** ISDN-NTBA hängten. Dieses Endgerät gestattet maximal 2 Amtsverbindungen zu jedem Zeitpunkt. Wenn INS zu FGS eine Verbindung aufbaute, wurden beide Kanäle hierfür beansprucht: einer für die Auswahl, einer für die Einwahl. Eine gleichzeitige Verbindung von FGS ins Internet war so per se ausgeschlossen. Wenn dagegen bereits eine Verbindung zwischen dem POP-Server im Internet und FGS bestand, konnte INS nur den einen verbleibenden Kanal für die Wahl nach außen einsetzen, während die Verbindung zum FGS nicht mehr möglich war.

Eigene Mailanalyse-Programme führten eine Vorsortierung der Information in „kritische“ und „unkritische“ aus. Erstere wurden zur weiteren Behandlung an einen menschlichen Experten weitergeleitet, während letztere sofort zugestellt werden konnten.

Sowohl bei ausgehenden als auch bei eingehenden Sendungen wurde der Mitarbeiter, der Empfänger bzw. Sender der kritischen Information gewesen ist, automatisch informiert.

Zusammenfassung und Ausblick

Das Flood-Gate-Konzept bietet eine sehr hohe Sicherheit beim Informationsaustausch zwischen firmeneigenen Intranets und dem Internet. Die Einfachheit des Konzepts und die freie Skalierbarkeit der Analysetiefe sind die großen Stärken dieser Lösung. Das Verfahren ist dazu geeignet, das Vertrauen der Sicherheitsexperten großer Unternehmen bezüglich der Kontrolle des Informationsflusses zu genießen.

Obgleich das Mehr an Sicherheit den Unternehmensanforderungen nahe kommt, erscheint der nicht-interaktive Informationsaustausch im Flood-Gate-Konzept als wenig attraktiv. Nicht zuletzt den modernen Browsern, die sowohl HTTP als auch HTML umsetzen, ist es zu verdanken, daß das weltumspannende Netz der Netze seinen Siegeszug in so kurzer Zeit vollziehen konnte.

Allerdings bietet sich für Firmen die Möglichkeit, den eigenen Mitarbeitern an Terminals einen Zugang zu gewähren, der nicht durch den Flood-Gate-Mechanismus kontrolliert wird. Selbstverständlich dürfen dann auch die zugehörigen Rechner nicht mit dem Intranet verbunden sein. Für das interaktive Surfen würde diese Lösung genügen, doch was geschieht, wenn Dateien zum Download angefordert werden? Die vorzusehenden Arbeitsstationen lassen einen derartigen Transfer nicht zu. Hier bietet sich ein Ausweg, den alle modernen Browser bereitstellen: eine HTML-Seite könnte beispielsweise per Email versendet werden und so die beiden Flood-Gates passieren. Erst nach eingehender Analyse dürfte die Information anschließend im Intranet des Unternehmens verwendet werden.

Das Konzept ließe sich ferner dahingehend erweitern, daß weitere Flood-Gates, dem Intranet-Server nachgeschaltet, die unterschiedlichen Sicherheitsanforderungen verschiedener Abteilungen und Mitarbeiter adäquater abbildeten.

Literaturverzeichnis

- [BO97] Greg Bossert et al.: Request for Comments: 2084, Considerations for Web Transaction Security, January 1997
- [CB95] William R. Cheswick, Steven M. Bellovin: Firewalls and Internet Security, Addison-Wesley, 5th printing April, 1995
- [CO84] F. Cohen: Computer Viruses: Theory and Experiments”, proceedings of the 7th National Computer Security Conference, Gaithersburg 1984, 240-263
- [DO91] Douglas E. Comer: Internetworking with TCP/IP: Principles, Protocols and Architecture, Vol. 1, Prentice-Hall, second edition, 1991
- [ED97] M. Edwards, Security gets easier, cheaper, Communication News, November 1997, S. 82-83
- [ME97] Ch. Meinel, Wie funktioniert das Internet?, ITWM-Preprint 97-01, 1997
- [MEM97] S. Müller, T. Engel, Ch. Meinel, Das Internet – Neues Medium für kommerzielle Aktivitäten, Studie erstellt am ITWM-Trier, 1997
- [LA84] C. E. Landwehr: The Best Available Technologies for Computer Security, Advances in Computer Security, vol. 2, Artech House, 1984, 108-122
- [LA94] M. Laubach, Request for Comments: 1577, Classical IP and ARP over ATM, 1994
- [LU98] N. Luckhardt, Kryptokampagne, c't 6/98, S. 32-33, 16.03.98
- [PE94] Heribert Peuckert: Datenschutz und Datensicherheit aus technischer Sicht, Sichere Daten, sichere Kommunikation, Springer-Verlag, 1994, 13-26
- [PP98] I. Pakhomenko, E. Pless, Sicherheitsprobleme in IP-über-ATM-Netzen, iX 3/98, S. 118-121, März 98
- [RA97] M. J. Ranum, Network security: safety is next, Data Communication, 21.10.97, S. 128-132
- [WE97] T. E. Weber, Should only the paranoid get E-mail protection?, Wall Street Journal, 25.09.97