FACTA UNIVERSITATIS (NIŠ)
Series: Electronics and Energetics vol. 11, No.3(1998), 263-270

MODERNE FIREWALLS FÜR LANS

Thomas Droste and Wolfgang Weber

Kurzfassung. In Abhängigkeit der geforderten Sicherheit in lokalen Netzen muß eine Firewall weitere Aufgaben übernehmen, um das gefordertes Sicherheitskonzept zu erfüllen. Einfache Paketfilterfunktionen der früheren *dual homed* Firewalls werden durch verschiedene Proxy–Systeme, Virenerkennung und der Kopplung verschiedener Intranetze zu einem VPN (virtual private networking) ergänzt. Moderne *third generation* Firewalls stellen ein Sicherheitsmanagement im Rechnerverbund dar mit Authetifizierung und kryptographischen Mechanismen über z.B. die Implementation der Internet Protokoll Version 6 (IPv6). Neben den Konzepten für moderne Firewalls beschreibt dieser Artikel eine weitere Schutzmöglichkeit des Intranet durch eine Erweiterung der Firewall durch einen zentralen Server innerhalb des Intranet.

1. Einführung

Eine moderne Firewall, die das interne Netz gegen Angriffe schützt, wird mittlerweile durch mehrere Funktionen erweitert. Eine größtmögliche Flexibilität in Bezug auf Datenfluß, Sicherheit und Konfigurierbarkeit muß durch die geforderte Sicherheitspolitik bei der Einrichtung und Umsetzung eingehalten werden.

Die Filterung und Bewertung von Paketen läßt sich auf mehreren Ebenen im TCP/IP–Schichtenmodell betrachten. Durch die Festlegung und Regeleinbindung von IP–Adressen kann der Datenverkehr von oder zu bestimmten Rechern erlaubt bzw. verboten werden. Eine Selektierung wird direkt durch die Zugehörigkeit zum internen Netz festgelegt. Alle übrigen Pakete werden verworfen. Eine Ebene höher, auf TCP–Ebene, kann eine Filterung von Internet–Diensten erfolgen. Dies geschieht über Freigabe von

Manuscript eingegangen am June 1, 1998.

Dipl.–Ing. Thomas Droste, Wissenschaftlicher Mitarbeiter, Lehrstuhl für Datenverarbeitung, Ruhr-Universität Bochum, 44780 Bochum, BRD, E-mail: droste@etdv.ruhr-uni-bochum.de. Prof. Dr.–Ing. Wolfgang Weber, Lehrstuhlinhaber des obigen Institutes, E-mail: weber@etdv.ruhr-uni-bochum.de.

Portnummern. Als Nebenbedingung werden weitere Felder im Header überprüft. Um einen selektiven Verbindungsaufbau z.B. via Telnet zu kontrollieren, genügt es, das Acknowledge–Flag zu betrachten, um die Richtung des Aufbaus festzustellen und bei Bedarf zu verbieten.

Durch sukzessive Anwendung von weiteren Regeln erfolgt die Auswahl über erlaubte und verbotene Zugriffe durch die Firewall.

Die Bewertung eines Angriffversuches für z.B. Spoofing–Attacken stellt eine weitere Funktion dar. Dabei hört ein potentieller Angreifer den Datenverkehr ab und sendet IP–Pakete mit gefälschten Paketinhalten. Dadurch kommt es zu einem "IP–Storm" und zu Fehlerpaketen mit falschen Sequenznummern, die von der Firewall erkannt werden müssen.

Um den Aufbau des Intranets für Außenstehende zu verschleiern und keinen direkten Zugriff aus dem Intranet ins Internet zu gestatten, werden Proxy–Systeme eingesetzt. Diese werden zumeist direkt in der Firewall als Dienst gestartet und fungieren durch Austausch der IP–Adresse als Vermittler. *Transparente Proxy Systeme* greifen aktiv und im Hintergrund in den Datenverkehr ein, d.h. die Umlenkung auf einen Proxy–Dienst wird für den Anwender nicht ersichtlich.

Es existieren zwei Prinzipien von Proxy–Systemen. Das erste, ein *Circuit Level Proxy*, hat nur eine Filterfunktion auf Basis der in der Firewall festgelegten Sicherheitspolitik integriert. Pakete werden nur weitergeleitet, wenn sie voll der Regelgebung entsprechen. Diese *generischen Proxy* sind keinem Anwendungsprotokoll zugeordnet und besitzen dadurch keine Kenntnis über das Protokoll. Ein neues Protokoll kann jedoch schnell implementiert werden. Das zweite Prinzip, die *Application Level Proxy*, haben hingegen volle Kenntnisse über das jeweilige Anwendungsprotokoll, d.h. jeder Befehl kann analysiert und eventuell abgeblockt werden. Diese *dedizierten Proxy–Server* sind jeweils einem Anwendungsprotokoll fest zugeordnet.

2. Erweiterte Funktionalität

Neben der Paketfilterung und dem Einsatz als Proxy–System läßt sich eine Firewall mittlerweile als Sicherungskonzept ansehen. Neben den eigentlichen Sicherheitsaufaben gegen unerlaubten Zugriff ist der Aufbau von VPN eine weitere Funktionalitätserweiterung. Dadurch wird es möglich, eine gesicherte Verbindung zwischen verschiedenen Intranetze über das Internet aufzubauen (Bild 1). Die normale Kommunikation erfolgt durch den Aufbau eines *Tunnels* zwischen den einzelnen Intranetzen, dabei wird eine Protokollschachtelung vorgenommen, die das IPv6 in die bislang übliche IPv4 einbettet oder alternativ den Datenverkehr kontinuierlich anderweitig verschlüsselt. Das Internet fungiert für das VPN als ein Art *Backbone* für den verteil-

ten Rechnerverbund. Zusätzlich besteht die Möglichkeit, verschiedene Verschlüsselungsverfahren anzuwenden. Bei der Übertragung von z.B. Emails über das VPN werden diese automatisch und für den Anwender vollkommen transparent per PGP (Pretty Good Privacy) verschlüsselt. Die Firewalls der beiden Intranetze führen diese Verschlüsselung selbsttätig durch, wobei durch die Email–Adresse verschiedene Geheimhaltungsstufen des Inhaltes angegeben werden und dies eine verschieden starke Verschlüsselung zur Folge hat. Die Firewall verwaltet über einen Keyserver die verschiedenen Schlüssel und stellt weitere kryptographische Verfahren für die Kommunikation bereit. Der Vorteil von VPN über das Internet besteht in der Kostenersparnis, da keine zusätzliche Standleitung zwischen den Intranetzen erforderlich ist und alle Dienste des Internet im Intranet ständig nutzbar sind.

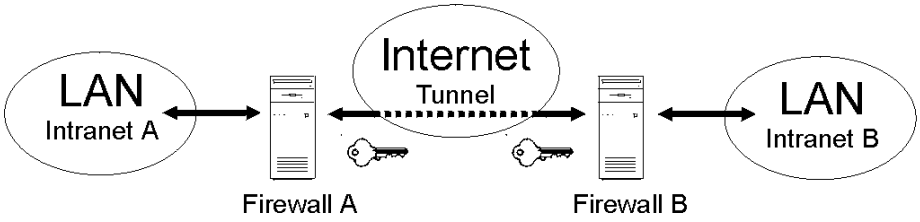

Bild 1. Nutzung des Internet als Backbone für VPN.

Angehörigen des Intranetverbundes, die sich außerhalb des VPN aufhalten, erlangen durch spezielle Client–Software, die ein *dynamisches* VPN (DVPN) erzeugt, Zugang. Durch den Aufbau eines *temporären Tunnels* und der damit verbundenen Ersetzung des IP–Stacks gegen die neue IPv6 erfolgt eine Registrierung im Rechnerverbund. Um eine Authentifizierung vorzunehmen, werden verschiedene Mechanismen eingesetzt, so z.B. die Authentifizierung via Pin–Kodes, ähnlich zum Online–Banking. Der Vorteil liegt wiederum in der gesicherten Verbindung von diesmal jedoch jedem beliebigen Internetzugang aus.

Die Integration verschiedener Kommunikationspartner stellt mittlerweile eine weitere Anforderung an eine Firewall. Durch Verschlüsselung und Authentifizierung, die durch die *IP Security* (IPSec) *Working Group* definiert worden ist, lassen sich skalierbare Verbindungen über das WAN mit Einzelbenutzern, Firmen und Rechnerverbunden herstellen. Unterstützen die Kommunikationspartner das IPSec, kann *unabhängig* von der eingesetzten Firewall eine authentifizierte Verbindung hergestellt werden. Mit IPSec läßt sich somit auch ein VPN auf Basis eines Rechnerbundes aufbauen.

Die Firewall als zentraler Knoten zum Internet trennt mittlerweile nicht nur das Intranet vom Internet, sondern z.T. auch die öffentlich zugänglichen Dienste über das *Security Server Net* (SSN) von den jeweiligen anderen beiden (Bild 2). Der Vorteil der Trennung liegt in der erhöhten Sicherheit durch doppelten Schutz. Bei einem Angriff auf den öffentlichen Bereich des Intranet impliziert dies nicht direkt den Sicherheitsverlust für das übrige interne Netz. Eine physikalische und logische Trennung durch die Firewall schützt den jeweilig anderen Bereich. Die Firewall fungiert als doppelte Firewall, da die Sicherheitspolitik nicht nur zwischen Firewall und Intranet bzw. SSN umgesetzt wird, sondern auch zwischen SSN und Intranet.

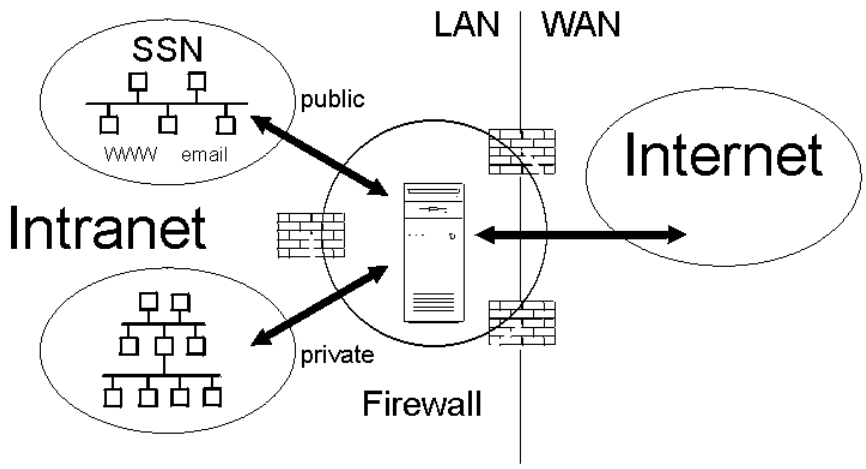

Bild 2. Sicherheitserhöhung durch getrennte und gesicherte Netzsegmente.

Die Definition einer Firewall als Filter ist mittlerweile nicht mehr akzeptabel. Eine *Sicherheitsmanagement* beschreibt die modernen Firewalls besser. Darunter ist nicht nur die Abblockung am Übergang zum internen Netz gemeint, sondern auch weiterreichende Analysemöglichkeiten auf höheren Protokollschichten für die im internen Netz fließende Datenpakete. Durch z.B. die Überprüfung der SMTP–Befehle in einer Email mit Hilfe der Application Level Proxy wird eine kritische Email direkt von der Firewall ausgefiltert. Eine Weiterleitung über das *Content Vectoring Protocol* (CVP) und ein nachfolgender Viruscheck von eingegangenen Emails an einen Virusscan–Server bietet die Möglichkeit den Inhalt einer Email inklusive angefügter Dateien zu überprüfen. Dadurch wird die Sicherheit in Bezug auf Datenin-

tegrität und versteckte Angriffe erhöht. Für andere Dienste (FTP, WWW, etc.) lassen sich diese Analysemöglichkeiten ebenfalls anwenden.

Eine weitere Möglichkeit, den Datenfluß direkt zu beeinflussen, liegt in der Erweiterung der Proxy. Dabei ist speziell der Datenfluß für den Informationsaustausch der HTTP–Proxy zu betrachten. Optionen für die Deaktivierung von z.B. Java Script, Java und Axtive–X, die durch ihre plattformunabhängige Implementierung Sicherheitslücken darstellen können, und der Viruscheck von herunterladbaren Dateien stellen eine direkte Erweiterung der Proxy dar. Zudem werden bei Bedarf verschiedene Operationen in Logfiles festgehalten, um spätere Analysen durchzuführen zu können.

Die Administration und Wartung dieser *third generation* Firewall erfolgt per Fernadministration über das interne Netz. Die Grundkonfiguration wird lokal am Firewall–Host eingerichtet, weitere Einstellungen erfolgen über gesicherte Verbindungen. An dieser Stelle ist besonders auf Sicherheitsmechanismen hinzuweisen. Neben der Authentifizierung des Administrators, ist es sinnvoll diese Aufgabe aus dem Intranet durchzuführen, um Sicherheitsrisiken durch z.B. *Sniffer*–Attacken zu vermeiden. Die Administration erfolgt mit Hilfe von GUI (Graphical User Interface), dadurch wird eine bessere Visualisierung gewährleistet und eine Fehlkonfigutation weitgehend ausgeschlossen. Die Regelumsetzung wird von der dahinter liegenden Applikation übernommen. Die benutzerdefinierte Administration erfolgt z.B. über einen Browser mittels dem gesicherten HTTPS via Java oder durch eine eigenständige lokale Applikation von einem beliebigen Rechner aus. Die Basisfilterfunktionen, die erweiterten Funktionen für die Application–Server, das VPN und die Zugriffssteuerung nach Host, Dienst, Verbindungsrichtung und Zeitfenster lassen sich direkt einstellen. Ein weiterer Vorteil liegt besonders bei VPN vor, hierbei kann ein Administrator aus dem anderen Intranet die Administration der Firewall übernehmen.

Im Fall einer Sicherheitsverletzung muß die Firewall eine Alarmmeldung ausgeben. Dies kann über verschiedene Wege geschehen und unterschiedliche Aktionen zur Folge haben. Von einer einfachen Zugriffsverletzung durch z.B. Benutzung eines nicht freigegebenen oder existierenden Dienstes bis zu schwerwiegenden Sicherheitsverstößen. Die Warnhinweise und Alarmmeldungen können auf einem Monitor angezeigt und per Email oder über ein SMS–Gateway an den Administrator versendet werden. Durch letzteres kann der Administrator direkt und überall erreicht werden und bei Bedarf direkt eingreifen.

3. Authentifizierung und Kryptographie

Durch Authentifizierung und Kryptographie auf Paketebene kann eine eindeutige, sichere Identifizierung stattfinden, wobei die Daten zusätzlich verschlüsselt werden. Durch die Erzeugung von *Session–Keys* wird eine Analyse und das Abhören des Netzverkehres nahezu unmöglich. Ein potentieller Angreifer kann den Session–Key nicht in Echtzeit bzw. endlicher Zeit errechnen und in die damit verbundene Sitzung eingreifen. Durch die Nutzung des neuen IPv6 bzw. des IPSec als standardisiertes Protokoll werden im *Authentication Header* (AH) die abgesendeten Daten authenitfiziert und mit Hilfe des *Encapsulated Security Payload* (EPS) die Nutzdaten des Datagramms selbst verschlüsselt. Als Algorithmus zur Verschlüsselung kommen der Data Encryption Standard (DES), der tripple DES (3DES), Define–Hellmann und RSA zum Einsatz. Die Authentifizierung erfolgt im Sinne der Unveränderlichkeit der Nutzdaten. Durch Hash–Funktionen (MD5, SHA–1) wird ein digitaler Fingerabdruck des Datagrammes erstellt und dieser mittels der obigen Algorithmen verschlüsselt. Der Empfänger entschlüsselt und prüft das Datagramm und erhält die Originaldaten zurück.

Die Sicherheit einer Firewall hängt auch von der Protokollsicherheit der IPv6 ab. Durch die Sicherungsmechanismen auf Protokollebene wird ein Mißbrauch verringert. Der sichere Austausch von Schlüsseln und Identifikationen muß als Grundvoraussetzung durchgeführt werden. Im internen Netz kann dies über einen Keyserver geschehen, um die Daten als authentisch anzusehen. Jede Verschlüsselung und Authentifizierung beansprucht Zeit und erhöht das Kommunikationsaufkommen durch zusätzlich notwendige Daten. Wird eine generelle Verschlüsselung und Verifizierung durch die Firewall vorgenommen, besteht die Möglichkeit, diese über integrierte Hardware umzuleiten und zu automatisieren. Hierzu existieren bereits schnelle IC, die z.B. den DES Algorithmus oder IDEA als Hardwarerealisierung durchführen und einen hohen Datendurchsatz erreichen.

Die Forderung nach einen hohen Datendurchsatz und Ausfallsicherheit impliziert das duplizieren einer Firewall. Eine primäre und eine sekundäre Firewall arbeiten simultan. Je nach Auslastung oder Zuordnung zwischen Internet und VPN können sich die Firewalls die Aufgaben teilen. Der Nachteil liegt hierbei in zwei möglichen Angriffspunkten, da zwei Rechner direkt mit dem Internet verbunden sind.

Bei der Aufsplittung eines Intranet in zwei oder mehr unabhängige Teile ist es hingegen sinnvoll, jeweils eine eigene Firewall zu verwenden und eine Kaskadierung von mehreren Firewalls bei weiterer Unterteilung einzurichten.

4. Konzept eines Kommunikationspools

Übergreifend auf die gesamte Netzwerktopologie ist es hilfreich, ein Konzept zu entwickeln, welches neben den Sicherungskonzepten auch den internen Datenverkehr und die Administration erleichtert. Werden mittlerweile viele verschiedene Anwendungen auf verschiedenen Systemen benötigt, ist es sinnvoll, eine zentrale Basisstruktur zu benutzen. Ein zentraler Server im geschützten Intranet stellt in einem Rechnerverbund zentrale Dienste für z.B. die Sicherheit, Virenüberprüfung, Installation und Administration bereit. Neben der Sicherheit in Form einer Firewall als Tor zum Internet findet die Kontrolle des Netzes auch innerhalb statt. Dies gilt nicht nur für die Installation von Softwarepatches verschiedener Betriebssysteme oder Anwendungen die zentral installiert werden, sondern vielmehr ist eine verteilte Firewall als Sicherheitsmanagement denkbar. Gleichzeitig laufen auf mehreren Rechnern verschiedene Dienste, die durch eine zentralen Server gesteuert werden. Dieser muß im internen Netz liegen und darf keine direkte Verbindung zum eigentlichen Firewall-Host besitzen, damit er gegen Angriffe von außen abgesichert ist (Bild 3). Die gestarteten Dienste auf den Arbeitsstationen im Intranet bedienen sich der Informationen aus dem internen, zentralen Server. Übertragene Daten im Intranet werden automatisch auf Viren überprüft, sobald diese zwischen Rechnern übertragen werden. Unerlaubte Verbindungen in das Internet durch z.B. verbotene Modems können durch eine ständige Überprüfung des internen Netzwerkverkehrs erkannt werden. Der Vorteil der zentralen Datenhaltung von Diensten und Konfigurationsdateien liegt in der Homogenität des Netzwerkes. Ein Netzwerk kann nur so sicher sein, wie sein schwächstes Element. Dabei kann eine interne Störung oder unerlaubte Verbindung aus dem Internet das Gesamtnetz gefährden, ebenso eine veraltete Protokollumsetzung oder ein Betriebssystembug. Durch das zentrale Management und die Verteilung der Dienste besteht die Forderung nach Zuverlässigkeit und Sicherheit der Einzelanwendungen. Ein gemeinsamer Nenner für die Kommunikation dieser Anwendungen in Form eines Standardmechanismus muß eingesetzt werden. Die Ausfallsicherheit des internen Servers ist als unproblematisch zu bewerten, da die Firewall die eigentliche Hauptaufgabe des Sicherheitskonzeptes übernimmt. Denkbar bei diesem Konzept ist die Verteilung von Anwendungen auf verschiedenen Rechnern, wobei der zentrale Server als Recover–Server zur Verfügung steht, der den Datenverkehr und die übertragenen Daten mitprotokolliert und temporär zwischenspeichert.

Ein zentrales Management soll den Aufwand minimieren und die Sicherheit maximieren, dabei darf der Einzelrechner in seiner Leistung nicht eingeschränkt werden, ebenso nicht die Geschwindigkeit des Netzwerkverkehrs.

Letztendlich hängt die Sicherheit stark von der Sicherheitspolitik ab. Die Forderung nach der globalen Unterstützung der IPv6 ist gerade durch eine Firewall ideal zu lösen, da die Protokollumsetzung bis zur generellen Benutzung im gesamten Internet zumindest das eigene Intranet schützt.

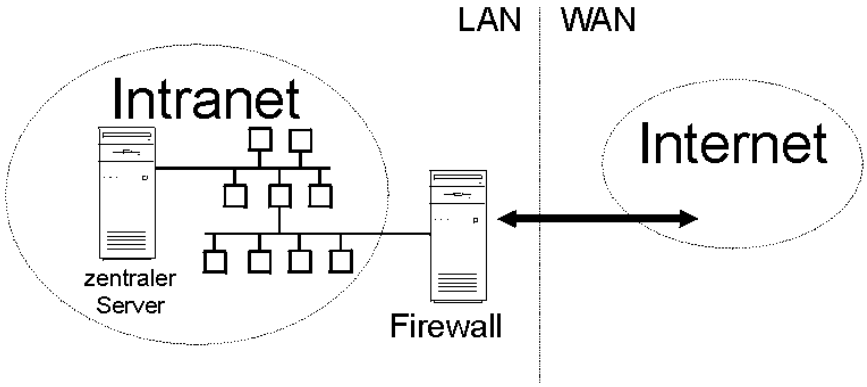

Bild 3. Zentraler Server im lokalen Netz.

LITERATUR

1. Borderware Firewall Server: *http://www.securecomputing.com.*
2. D.B. Chapman, E.D. Zwicky: *Building Internet Firewalls.* O'Reilly & Associates Inc., Sebastopol 1995.
3. W.R. Cheswick, S.M. Bellovin: *Firewalls und Sicherheit im Internet.* Addison–Wesley Publ. Comp., Bonn 1996.
4. V. Gupta, S. Glass: *Firewall Traversal for Mobile IP: Goals and Requirements.* http://www.ietf.org/internet–drafts/draft–ietf–mobileip–ft–req–00.txt Internet Engineering Task Force (IETF), Internet–Draft 1997.
5. M. Hennecke, T. Droste: *Sicherheit im Internet – Umsetzung von Firewall–Konzepten.* Seminar Datenverarbeitung WS 97/98, Lehrstuhl für Datenverarbeitung, Ruhr–Universitäet Bochum, 1998.
6. A. Paweletz, T. Droste: *Sicherheit im Internet – Mechanismen zum sicheren Datenverkehr.* Seminar Datenverarbeitung WS 97/98, Lehrstuhl für Datenverarbeitung, Ruhr–Universitäet Bochum, 1998.
7. Security Policy: *http://csrc.nist.gov/isptg/html/ISPTG.html.*
8. TIS Gauntlet Firewall: *http://www.tis.com.*