Firewall

aus Wikipedia, der freien Enzyklopädie

Als **Firewall** [ˈfaɪəwɔːl] oder **Zugangsschutzsystem** bezeichnet man bei Rechnernetzwerken ein organisatorisches und technisches Konzept zur Trennung von Netzbereichen, dessen korrekte Umsetzung und dauerhafte Pflege.

Durch den immer größer werdenden Ausbau von Netzen wird der Schutz einzelner Netze immer wichtiger. Firewalls greifen hier ein; sie sitzen an den Schnittstellen zwischen einzelnen Netzen und kontrollieren den Netzwerkverkehr zwischen den Netzen, um ungewünschten Verkehr zu verhindern und nur den gewünschten Verkehr weiterzuleiten.

Der häufige Einsatz einer Firewall besteht darin, den Verkehr zwischen einem lokalen Netzwerk und dem Internet zu kontrollieren und zu steuern. Ein komplexes Szenario stellt die DMZ dar.

Rund um das Thema Firewall existieren viele Begriffe, die teilweise richtig sind, aber manchmal nur die halbe Wahrheit vermitteln. Umgangssprachlich ist mit einer Firewall sehr oft die Software gemeint, welche den Datenverkehr zwischen den getrennten Netzbereichen kontrolliert und regelt. Man muss also zwischen dem (Sicherheits-)Konzept Firewall, und den zwei Hauptbestandteilen der Firewall, nämlich Hardware und Software, unterscheiden. Die Hardware ist für das Empfangen und Senden der einzelnen Netzwerkpakete zuständig und die Software regelt den Verkehr. (Was wird durchgelassen? Was wird nicht durchgelassen?)

Inhaltsverzeichnis [Verbergen]

[Bearbeiten]

Hardware

Die Hardwarekomponente hat im Regelfall zwei Netzwerkschnittstellen, an denen jeweils die zu trennenden Netzwerke angeschlossen sind. Die zwei Schnittstellen werden aus

Sicherheitsgründen (oft aber wegen der Netzwerkstruktur und damit aus der konzeptionellen Notwendigkeit) gewählt, damit gewährleistet ist, dass nur solche Pakete von einem Netz ins andere durchgelassen werden, die von der Software als gültig anerkannt werden.

[Bearbeiten]

Software

Die Softwarekomponente der Firewall arbeitet auf den Schichten 2 bis 7 des OSI-Referenzmodells und demzufolge kann das Implementationsniveau sehr unterschiedlich ausfallen. Deswegen besteht eine Firewall oft aus verschiedenen Softwarekomponenten. Die verschiedenen Teile sollen hier kurz beschrieben werden:

[Bearbeiten]

Paketfilter

Für solch einfache Aufgaben wie das Vergleichen von Quell- und/oder Zieladresse der Pakete, die die Firewall passieren, ist der Paketfilter zuständig. Er hat die Aufgabe, bestimmte Filterungen oder Reglementierungen im Netzwerkverkehr vorzunehmen. Wenn man sich das Internet als eine gigantische Ansammlung von Häusern vorstellt, dann stellen die IPs sozusagen die Hausnummern dar. (Straßennamen sind in der Welt des Internets unbekannt.) Unter einer bestimmten Hausnummer kann man nun direkt mit einem Rechner kommunizieren, egal wo sich dieser Rechner befindet. In den einzelnen Etagen dieser Rechner wohnen nun die verschiedenen Dienste wie HTTP, FTP oder SSH. Die einzelnen Etagen sind mit einer Nummer gekennzeichnet, die man auch Port nennt. Ein Paketfilter kann nun verschiedene Etagen/Ports für die Besucher aus dem Internet sperren, d. h. jede Verbindung aus dem Internet wird an der Haustüre schon abgewiesen. Durch die entsprechende Konfiguration einer Firewall kann so ein Computernetzwerk vor Angriffen und/oder Zugriffen geschützt werden. Ein Paketfilter definiert Regeln, welche festlegen, ob einzelne oder zusammenhängende Pakete das Zugangsschutzsystem passieren dürfen oder abgeblockt werden. Eine solche Regel wäre zum Beispiel: verwerfe alle Pakete, die von der IP-Adresse 1.2.3.4 kommen. Eine solche Regel ist programmtechnisch einfach: es ist nur ein Zahlenwert zu vergleichen.

[Bearbeiten]

Content-Filter / Application-Level-Gateway

Eine Firewall kann aber nicht nur auf der niedrigen Ebene des Paketfilters arbeiten, sondern auch komplexere Aufgaben übernehmen. Ein Content-Filter überprüft zum Beispiel die Inhalte der Pakete und nicht nur die Meta-Daten der Pakete wie Quell- und/oder Zieladresse. Solche Aufgaben können zum Beispiel folgende sein:

- Herausfiltern von ActiveX und/oder JavaScript aus angeforderten HTML-Seiten.
- Filtern/Kennzeichen von Spam-Mails
- Löschen von Viren-Mails

Solche Regeln sind normalerweise sehr einfach zu definieren, ihre Ausführung ist aber sehr komplex: hierfür müssen einzelne Pakete zusammengesetzt werden, damit die HTML-Seite

als Ganzes erkannt, durchsucht und verändert werden kann. Anschließend muss die Seite wieder in einzelne Pakete zerteilt werden und kann weitergeschickt werden.

[Bearbeiten]

Proxy

Ein Proxy ist ein Stellvertreter, der Anfragen (im Normalfall sind dies Anforderungen von HTML-Seiten, oder aber auch FTP Verbindungen) entgegennimmt und diese Anfrage weiterleitet. Der Proxy verhält sich gegenüber dem anfragenden Client wie ein Server. Gegenüber dem eigentlichen Ziel, z. B. dem Web-Server, verhält er sich wie ein Client. Dies geschieht nicht auf der Paketebene, sondern es wird in diese Pakete hineingeschaut und eine Anfrage generiert, die der ursprünglichen Anfrage entspricht. Der Vorteil bei dieser Methode ist, dass keine Pakete die Firewall direkt passieren können, was die Sicherheit nochmals erhöht. Oft ist ein Proxy auch mit einem Content-Filter kombiniert.

[Bearbeiten]

SOCKS

Ein Socks-(Secure Sockets)Server wird in einem Netzwerk dazu verwendet, Anwendungen und Protokolle zu bedienen, die von dem Proxy nicht unterstützt oder von der Firewall geblockt werden. Funktionsweise: Die Socks-Software hört als Server auf dem Port 1080. Eine Clientanwendung kann, wenn sie 'socksifiziert' ist, einen Tunnel zu dem Socks-Server aufbauen und die Daten durch diesen Tunnel an den Server schicken. Der Server packt das 'Socks-Paket' aus und schickt die Anfrage 1-zu-1 weiter ins Internet - und die entsprechende Antwort wieder zurück an den Client.

[Bearbeiten]

NAT / Network Address Translation / Circuit Relay Firewall

Das NAT stellt oft auch einen Bestandteil einer **Firewall** dar. Es wird besonders dann benötigt, wenn nur eine oder wenige öffentliche IPs zur Verfügung stehen.

[Bearbeiten]

Router-Funktionalitäten

Damit die Pakete von der einen Seite der Firewall auch auf die andere Seite weitergeleitet werden können, muss die Firewall Router-Funktionaliäten besitzen.

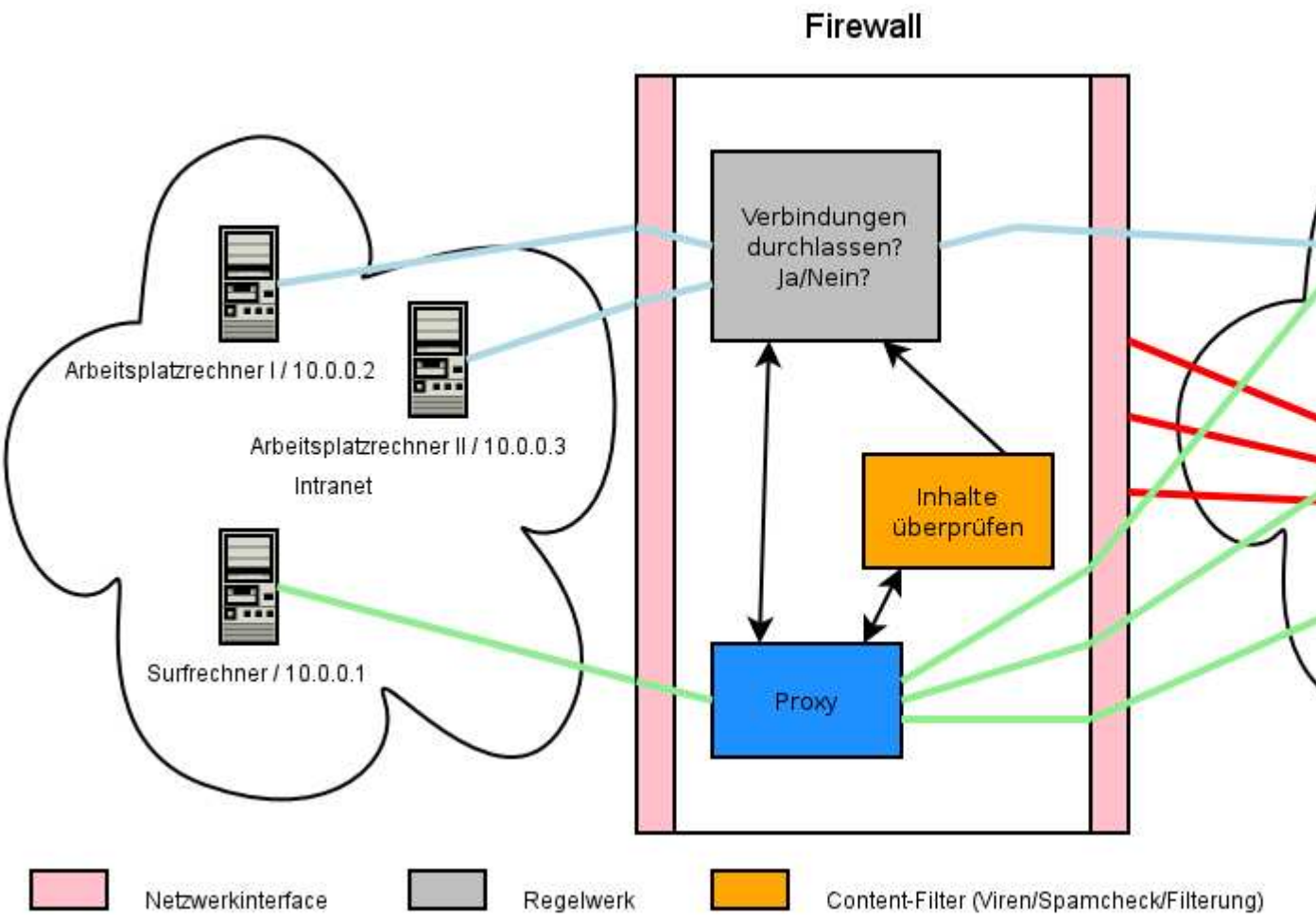
[Bearbeiten]

Beispiel

Ein einfaches Konzept soll diese trockene Materie verdeutlichen: Eine Firma möchte ihre Arbeitsplatzrechner ins Internet bringen. Man entscheidet sich für eine Firewall, und aufgrund der Viren-/Würmergefahr möchte man nur die Verbindungen zu einem Mail-Server aufbauen. Damit auch eine Recherche im Internet möglich ist, soll ein PC über einen Proxy Zugriff zu

Webseiten erhalten. Weiterhin steht der Firma nur eine öffentliche IP zur Verfügung, so dass NAT genutzt werden muss. Der Surf-Rechner wird zusätzlich dadurch geschützt, dass ActiveX aus den angeforderten HTML-Seiten aus Sicherheitsgründen rausgefiltert werden.

Sonstige Zugriffe von außen auf das Firmennetz sollen einfach geblockt werden.



[Bearbeiten]

DSL-Modems/DSL-Router

DSL-Router übernehmen normalerweise die Routing-Funktionalität und können Zugriffe aus dem Internet auf das LAN blockieren (Portfilter-Funktionalität). Mit Hilfe von NAT ist es möglich mehrere Rechner an einem DSL-Modem zu betreiben. Einen Content-Filter enthalten solche Produkte zumeist nicht.

[Bearbeiten]

Personal Firewalls

Personal Firewalls oder auch Desktop Firewalls sind Programme, die lokal auf dem zu schützenden Rechner installiert sind. Sie beinhalten einen Paketfilter und einen Content-Filter. Darüber hinaus sind oft noch Virenscanner für den normalen Betrieb vorhanden.

Die Wirkung von Personal Firewalls ist allerdings umstritten: Ist der Rechner ordentlich konfiguriert und laufen nur vertrauenswürdige Programme, so wird das System selbst nur sinnvolle Pakete annehmen und verschicken. Läuft dagegen zweifelhafte Software auf dem Rechner, die unautorisiert auf das Netz zugreifen will, so wird diese auch so weit gehen, den normalen Weg des Versands zu verlassen und die Personal Firewall zu umgehen oder auszuschalten. So sind schon Viren in freier Wildbahn entdeckt worden, die die Regeln der gängigen Firewalls modifizieren, damit Sie ihre eigentliche Aufgabe durchführen können.

[Bearbeiten]

Siehe auch

- Computersicherheit
- DMZ
- Paketfilter
- Router
- Intrusion Detection System
- Proxy
- Application_Gateway
- Smoothwall

[Bearbeiten]

Literatur

- Zwicky, Cooper, Chapman, *Einrichten von Internet Firewalls*, O'Reilly 2001, ISBN 3897211696
- W. R. Cheswick, S. M. Bellovin, A. D. Rubin, *Firewalls and Internet Security - Repelling the Wily Hacker*, 2nd Edition, Addison-Wesley 2003, ISBN 0-201-63466-X
- Wolfgang Barth *Das Firewall Buch, Grundlagen, Aufbau und Betrieb sicherer Netzwerke mit Linux* (iptables), SuSE Press, ISBN 3-934678-40-8
- [1] (*http://www.amazon.de/exec/obidos/redirect?tag=movieplanet24-21&creative=2966&camp=446&link_code=st1&path=tg/sim-explorer/explore-items/-/389864152X*) Stefan Strobel *Firewalls und IT-Sicherheit, Dieses Buch gibt einen umfassenden Überblick über praktische IT-Sicherheit in Unternehmen.*, Dpunkt Verlag, ISBN 389864152X

[Bearbeiten]

Weblinks

- de.comp.security.firewall FAQ (*http://www.iks-jena.de/mitarb/lutz/usenet/Firewall.html*)
- Firewall Ruleset Anleitung (*http://www.protecus.de/Firewall_Security/ruleset.html*)
- Netfilter - Paketfilter innerhalb des Linux Kernel (*http://www.netfilter.org*)
- Die Eindiskettenfirewall (*http://www.fli4l.de*) ist neben der CD-Variante Gibraltar (*http://www.gibraltar.at/*) ein Projekt, das im Sinne einer nachhaltigen Nutzung die Verwendung von alten PCs als Firewall gestattet.
- IPCop (*http://www.ipcop.org/*) ist eine einfach zu bedienende Linux-Distribution, die zum Ziel hat, eine durch und durch sichere Firewall zu sein.

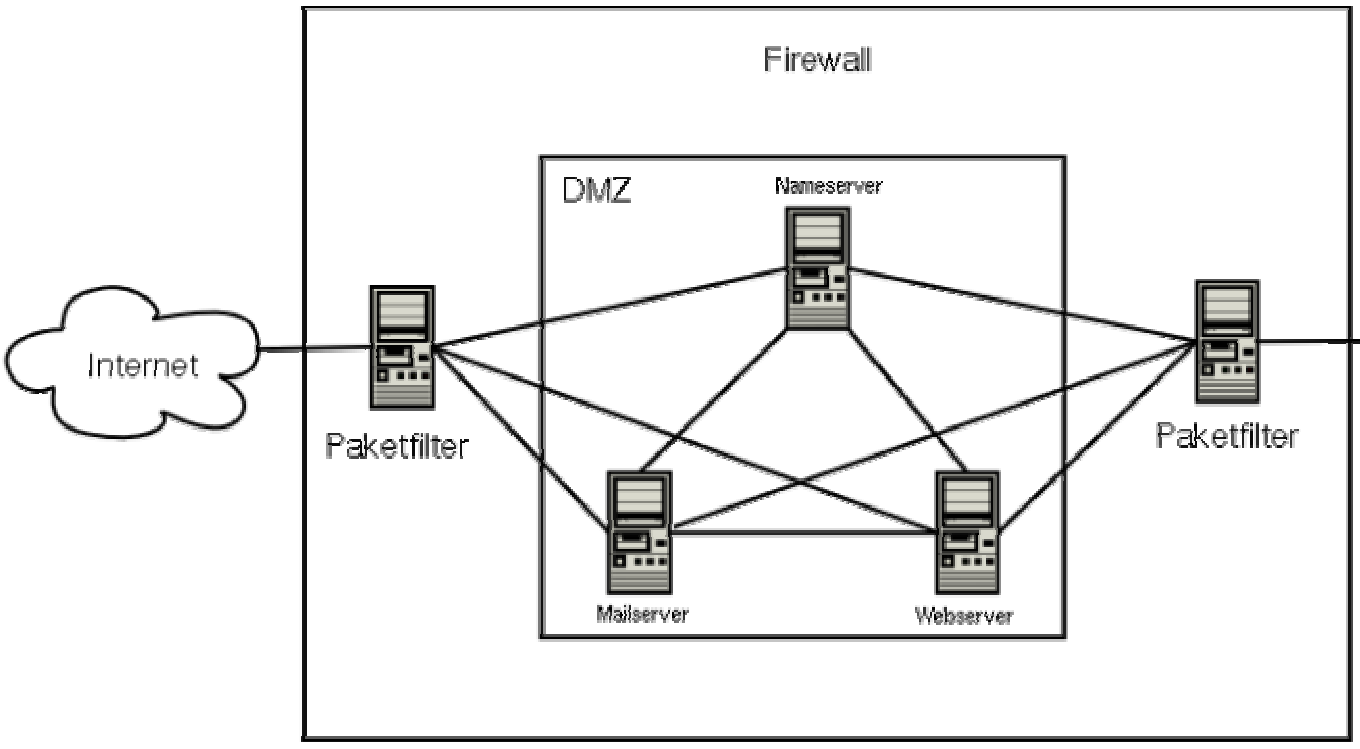
- m0n0wall (*http://www.m0n0.ch/wall*) eine BSD basierende Firewall, die teilweise mit ihren Funktionen an Profi-Firewalls herankommt und trotzdem sehr einfach zu konfigurieren ist.
- PFSense (*http://www.pfsense.org*) ein Fork der "m0n0wall" Firewall.
- Firewall Hilfe und Diskussion (*http://board.protecus.de*)

Demilitarized Zone

aus Wikipedia, der freien Enzyklopädie

(Weitergeleitet von DMZ)

Demilitarized Zone (**DMZ**, deutsch: *entmilitarisierte Zone*) bezeichnet einen geschützten Rechnerverbund, der sich zwischen zwei Computernetzwerken befindet. Der Rechnerverbund wird jeweils durch einen Paketfilter gegen das dahinter stehende Netz abgeschirmt.



Der Sinn des ganzen Aufwandes ist es, möglichst auf sicherer Basis Dienste des Rechnerverbundes sowohl dem einem als auch dem anderem Netz zur Verfügung zu stellen. Ein typisches Anwendungsbeispiel ist eine Firma, die einen eigenen Mailserver betreibt.

Dieser Mailserver ist ein Teil der DMZ und muss von außen erreichbar sein, da ansonsten E-Mails nicht zugestellt werden könnten. Anderseits müssen die Clients, die am LAN

angeschlossen sind, ihre E-Mails abholen. Deswegen brauchen auch sie Zugriff auf den Server. Der Server selbst kann jedoch von sich aus keine Verbindung ins LAN aufbauen.

Vorteil einer solchen Lösung ist, dass im Falle einer Kompromittierung eines Servers in der DMZ das interne Netzwerk trotzdem noch geschützt bleibt. Wären die Server nicht in einer DMZ, sondern direkt im internen Netzwerk, so wäre auch das gesamte Netzwerk durch eine Kompromittierung betroffen. Gerade weil öffentlich angebotene Dienste oft ein nicht unerhebliches Angriffsziel darstellen, kann man durch eine DMZ das Gesamtrisiko erheblich minimieren.

Paketfilter

aus Wikipedia, der freien Enzyklopädie

Ein **Paketfilter** ist eine Software, die den ein- und ausgehenden Datenverkehr in einem Computernetz filtert. Dies dient in der Regel dem Schutz des Netzes vor Angreifern. Ein Paketfilter kann Teil einer Firewall sein.

[Bearbeiten]

Verwendung

Paketfilter werden verwendet, um das Konzept einer Firewall umzusetzen. Die Paketfilterung kann durch folgende Funktionen ergänzt sein:

- NAT
- Masquerading
- Port Forwarding

Auf Routern kommen sie zum Einsatz um sog. **Ingress Filter** zu implementieren. Mit solchen Filtern wird verhindert, dass Datenpakete aus oder in ein Netz gesendet werden, die ungültige Absender- oder Ziel-Adressen beinhalten. Ist an einem Router das Netz 10.1.1.0/24 angeschlossen und es kommt ein Datenpaket mit der Absender-Adresse 172.16.1.42 aus diesem Netz, sollte der Router das Paket blocken. Es liegt entweder ein Konfigurationsfehler vor, oder ein Angreifer versucht seine Absender-Adresse zu fälschen. Auch Multicast und Broadcast Absender-Adressen lassen sich so filtern.

[Bearbeiten]

Funktionsweise

Die Daten werden in einem Netzwerk von dem sendenden Host in Datenpakete verpackt und versendet. Jedes Paket, welches den Paketfilter passieren will, wird untersucht. Anhand der in jedem Paket vorhanden Daten, wie Absender- und Empfänger-Adresse, entscheidet der Paketfilter aufgrund von Filterregeln was mit diesem Paket geschieht. Ein unzulässiges Paket, welches den Filter nicht passieren darf, kann entweder ignoriert (im Fachjargon **DENY** oder

DROP genannt), an den Absender zurückgeschickt werden, mit der Bemerkung, dass der Zugriff unzulässig war (**REJECT**) oder weitergeleitet werden (**FORWARD**).

Bekannte Paketfilter sind:

- iptables (Linux 2.4 + 2.6) bzw. ipchains (Linux 2.2) bzw. ipfwadm (Linux 2.0)
- pf Paketfilter von OpenBSD
- ipfw Paketfilter von FreeBSD
- IPFilter portabler Paketfilter für Solaris, FreeBSD u.a.

[Bearbeiten]

Weblinks

- FreeBSD ipfw (*http://www.ipfw.edu/*) englisch
- Linux netfilter/iptables Paket Filter (*http://www.netfilter.org/*) englisch
- netfilter HOWTO (*http://www.netfilter.org/documentation/HOWTO/de/packet-filtering-HOWTO.html*)
- PF: The OpenBSD Packet Filter (*http://openbsd.nuug.no/faq/pf/*) englisch
- Ist REJECT oder DENY sinnvoller? (*http://www.iks-jena.de/mitarb/lutz/usenet/Firewall.html#Deny*)

Intrusion Detection System

aus Wikipedia, der freien Enzyklopädie

Ein **Intrusion Detection System (IDS)** ist ein Programm, das der Erkennung von Angriffen auf ein Computersystem oder Computernetz dient. Richtig eingesetzt, ergänzen sich eine Firewall und ein IDS und erhöhen so die Sicherheit von Netzwerken. Man unterscheidet netzwerkbasierte (NIDS) und hostbasierte Intrusion Detection Systeme (HIDS).

Inhaltsverzeichnis [Verbergen]

[Bearbeiten]

Architekturen

Man unterscheidet zwei Arten von IDS

- Host-Basierte IDS
- Netzwerk-Basierte IDS

[Bearbeiten]

Host-Basierte IDS

Sie stellen die älteste Art von Intrusion Detection Systemen dar. Sie wurden ursprünglich vom Militär entwickelt und sollten die Sicherheit von Großrechnern garantieren. Ein HIDS muss auf jedem zu überwachenden System installiert werden. Der Begriff "Host" darf allerdings nicht missverstanden werden. In diesem Kontext ist als Host jedes System gemeint, auf welchem ein IDS installiert ist. Ein HIDS muss das Betriebssystem unterstützen. Es erhält seine Daten aus Log-Dateien, Kernel-Daten und anderen Systemdaten wie etwa der Registry. Es schlägt Alarm, wenn es in den gescannten Daten einen Angriff erkennt.

Vorteile:

- sehr spezifische Aussagen über den Angriff
- kann ein System umfassend überwachen

Nachteile:

- kann durch einen DoS-Angriff ausgehebelt werden
- wenn das System außer Gefecht gesetzt wurde, ist auch das IDS lahm gelegt
- HIDS muss auf jeden Rechner installiert werden => Lizenz-Kosten

[Bearbeiten]

Netzwerk-Basierte IDS

NIDS versuchen, alle Pakete im Netzwerk mitzulesen, zu analysieren und verdächtige Aktivitäten zu melden. Diese Systeme versuchen außerdem, aus dem Netzwerkverkehr Angriffsmuster zu erkennen. Da in der heutigen Zeit überwiegend das TCP/IP-Protokoll eingesetzt wird, muss auch ein Angriff über dieses Protokoll erfolgen. Mit nur einem Sensor kann ein ganzes Netzsegment überwacht werden. Jedoch kann die Datenmenge eines modernen 100 MBit-LANs die Bandbreite des Sensors übersteigen. Dann müssen Pakete verworfen werden, was keine lückenlose Überwachung mehr garantiert.

Vorteile:

- ein Sensor kann ein ganzes Netz überwachen
- durch Ausschalten eines Zielsystems ist die Funktion des Sensors nicht gefährdet

Nachteile:

- keine lückenlose Überwachung bei Bandbreitenproblemen
- keine lückenlose Überwachung in geswitchten Netzwerken (nur durch Mirror-Port auf einem Switch)

[Bearbeiten]

Funktionsweise

Grundsätzlich gibt es zwei Verfahren zur Einbruchserkennung: den Vergleich mit bekannten Angriffssignaturen und die sogenannte statistische Analyse. Die meisten IDS arbeiten mit Filtern und Signaturen, die spezifische Angriffsmuster beschreiben. Der Nachteil dieses Vorgehens ist, dass nur bereits bekannte Angriffe erkannt werden können und durch das Modifizieren bekannter Angriffe ist das System leicht umgehbar.

Andere IDS verwenden heuristische Methoden um auch bisher unbekannte Angriffe zu erkennen. Ziel ist, nicht nur bereits bekannte Angriffe, sondern auch ähnliche Angriffe oder ein Abweichen von einem Normalzustand zu erkennen.

In der Praxis haben signaturbasierte Systeme mit Abstand die größte Verbreitung. Ein Grund dafür ist, dass ihr Verhalten leichter voraussehbar ist. Ein Hauptproblem beim praktischen Einsatz von IDS ist, dass sie entweder viele falsche Warnungen (sog. *false positives*) generieren oder einige Angriffe nicht entdecken (sog. *false negatives*).

Anstatt nur einen Alarm auszulösen, wie ein NIDS, ist ein **Network Intrusion Prevention System** (**NIPS**, oder kurz **IPS**) in der Lage, Datenpakete zu verwerfen, die Verbindung zu unterbrechen oder die übertragenen Daten zu ändern.

IPS neuerer Bauart arbeiten oft mit einer Kombination aus *Stateful inspection*, *Pattern Matching* und Anomalieerkennung. Damit lassen sich Abweichungen von der im RFC-Standard (Request for Comment) festgelegten Protokollspezifikation erkennen und verhindern.

[Bearbeiten]

IDS Software

Auf dem Markt gibt es eine ganze Reihe von kommerziellen Network Intrusion Detection Systemen. Aber auch freie Software wird angeboten: Snort ist ein kostenloses IDS für Unix/Linux- und Windows-Systeme.

- Umfangreiche Übersicht über HIDS, NIDS, ... (*http://www.forinsect.de/ids/ids-tools.php*)
- Snort [1] (*http://www.snort.org/*) - Freies, signaturbasiertes NIDS
- Winsnort (*http://www.winsnort.com/*) - Windows-Version von Snort
- Snort Inline (*http://snort-inline.sourceforge.net/*) - Freies NIPS
- Tripwire (*http://www.tripwire.org/*) - HIDS, verwendet Prüfsummen um Änderungen am System zu überwachen
- AIDE (*http://www.cs.tut.fi/~rammer/aide.html*) Freies HIDS, ähnlich Tripwire
- Prelude (*http://www.prelude-ids.org/*) - Freies, signaturbasiertes HIDS
- GFI LANguard System Integrity Monitor (*http://www.gfisoftware.de/de/lansim/*) - Freies HIDS
- AFICK (Another File Integrity CHecker) (*http://afick.sourceforge.net/*) - Freies HIDS

[Bearbeiten]

Siehe auch

Firewall, TCP, UDP, Internet Protocol, Netzwerksicherheit

[Bearbeiten]

Literatur

- Stephen Northcutt/Judy Novak: *IDS: Intrusion Detection System*, Bonn 2001

[Bearbeiten]

Weblinks

- SecurityFocus IDS (*http://www.securityfocus.com/ids/*) englisch
- IDS FAQ (*http://www.robertgraham.com/pubs/network-intrusion-detection.html*) englisch

Proxy

aus Wikipedia, der freien Enzyklopädie

Dieser Artikel behandelt Computersysteme/-programme mit Zwischenspeicherfunktion. Für den proxy als Softwareschnittstelle in verteilten Applikationen siehe Stub.

Ein **Proxy** oder **Proxyserver** (vom engl. *proxy representative* = Stellvertreter von lat. *"proximus"* = "Der Nä(c)hste") ist ein Computerprogramm, das im Datenverkehr zwischen Computern oder Computer-Programmen in so genannten Computernetzen zwischen angefragtem Server und anfragendem Client vermittelt. Dem Server gegenüber verhält sich das Programm wie ein Client, dem Client gegenüber wie ein Server. Strukturell/logisch liegt der Proxyserver zwischen anfragendem Client und dem angefragten Server, zu dem er vermittelt. Der strukturell Nächste ist hier aber nicht notwendigerweise auch der räumlich Nächste. Beispielsweise vermittelt ein Proxyserver einer Firma allen Datenverkehr der Computer der Mitarbeiter mit dem Internet. Der Proxyserver JAP hingegen vermittelt den anonymen Internetdatenverkehr eines Surfers möglicherweise über eine seiner Komponenten in New York zu einem Internetcafé seiner Stadt.

Inhaltsverzeichnis [Verbergen]

[Bearbeiten]

Funktion

Im einfachsten Fall leitet der Proxy die Daten einfach weiter. Oft hat ein Proxy jedoch zusätzlich einige der folgenden Funktionen:

- *Zwischenspeicher (Cache)*: Der Proxy speichert gestellte Anfragen bzw. vielmehr deren Ergebnis. Wird die gleiche Anfrage erneut gestellt, kann diese aus dem Speicher beantwortet werden, ohne zuerst den Webserver zu fragen. Die Proxys stellen sicher, dass die Anfrage nicht veraltet ist. Durch das Zwischenspeichern können Anfragen schneller beantwortet werden, und es wird gleichzeitig die Netzlast verringert.
- *Filter*: Mittels Proxy können beispielsweise bestimmte Kategorien von Webseiten für den Benutzer gesperrt werden. Es kann auch der Inhalt auf schädliche Programme durchsucht werden. Somit ist ein Proxy meist Teil von Firewalls.
- *Zugriffssteuerung*: Ist der Server nicht frei im Internet erreichbar, so kann ein vorgeschalteter Proxy den Zugriff ermöglichen. Ein Angreifer kann dann den Server nicht mehr direkt angreifen, sondern nur den Proxy. Es kann auch der Zugriff von Clients auf Webserver nur über einen Proxy ermöglicht werden.
- *Vorverarbeitung von Daten*: Proxys können auch gewisse Applikationsfunktionen übernehmen, beispielsweise Daten in ein standardisiertes Format bringen.
- *Anonymisierungsdienst*: Der Proxy leitet die Daten des Clients zum Server weiter, wodurch der Server die IP-Adresse des Clients nicht auslesen kann. Siehe auch: Anonymität im Internet

[Bearbeiten]

Protokolle

Proxys sind generell für jedes verbindungsorientierte Protokoll möglich. Häufig werden sie für die folgenden Protokolle verwendet:

- **HTTP**: Die meisten Provider bieten Ihren Kunden die Verwendung eines Proxys an. Dadurch wird die Netzlast verringert und der Zugriff beschleunigt. In Firmen hingegen wird über solche Proxys oft das Surfverhalten der Mitarbeiter eingeschränkt bzw. kontrolliert.
- **ICP**: Inter Cache Protokoll. Wird in Netzen aus Proxyservern zum Informationsaustausch verwendet.
- **SMTP**: Manche Firewalls bieten einen SMTP-Proxy an, der den Mailverkehr zwischen Internet und Mailserver überwacht und bestimmte gefährliche bzw. unerwünschte Befehle ausfiltert. Durch das Design des SMTP-Protokolls ist jeder SMTP-Server auch als SMTP-Proxy verwendbar.
- **Applikationsproxy**: Ein Proxy, der auf ein bestimmtes Server-Programm zugeschnitten ist, und nur dessen Protokoll erkennt. Diese Form eines Proxys wird oft dazu verwendet, den eigentlichen Server in ein geschütztes Netz zu stellen und nur durch den Proxy erreichbar zu machen. Auf diese Art ist der Server weitgehend vor Angriffen geschützt. Die Proxy-Software ist weit weniger komplex und daher auch sicherer gegen Angriffe.

[Bearbeiten]

Sonderformen

- **Transparenter Proxy**: Die Verwendung eines Proxyservers muss meist dem Client explizit mitgeteilt werden. Ein transparenter Proxy muss hingegen nicht explizit angegeben werden. Ein Paketfilter auf einem Gateway zwischen Client und Server kann die Datenpakete abfangen und sie an den Proxy weiterleiten. Dieses Verfahren ist für den Client transparent, d. h. er bemerkt nicht, dass er einen Proxy verwendet.
- **Automatischer Proxy**: Eine URL, die auf einen Webserver zeigt, auf dem ein Javascript-Programm liegt, das den Proxy des Clients konfiguriert. Das Javascript kann auch bedingte Verzweigungen enthalten, z.B. primärer und sekundärer Proxy.
- **Reverse Proxy**: Tritt statt des eigentlichen Servers in Erscheinung. Es können auch mehrere Web Server im internen Netz über eine einzige öffentliche IP Adresse erreicht werden. Die Filterung erfolgt über den Header des TCP-Pakets, bzw. über die URL. Dadurch können etwa Zugriffskontrollen oder Caches realisiert werden.

[Bearbeiten]

Proxy Software

Bekannte Proxyserver-Software:

- http://www.microsoft.com/isaserver - Microsoft Internet Security and Acceleration Server
- WebWasher (*http://www.webwasher.com/client/home/index.html?lang=de_DE*) - Lokaler HTTP-Proxy, Freeware
- Deutschsprachiges Proxomitron-Forum (*http://www.buerschgens.de/Prox/*) Proxomitron - Lokaler HTTP-Proxy
- http://www.privoxy.org/ Privoxy - ehemals http://www.junkbusters.com/ Junkbuster - Lokaler HTTP-Proxy (Win32, Unix/Linux, AmigaOS, Mac OS)
- http://www.squid-cache.org/ Squid (Linux/Unix)
- http://www.research.att.com/sw/tools/iproxy iProxy (AT&T)
- http://bfilter.sourceforge.net/index.php BFilter - Lokaler HTTP-Proxy, Freeware
- http://www.janaserver.de Jana-Server - Freeware für private Anwendungen
- http://zipper.paco.net/~igor/oops.eng/ Oops! - Schneller Open Source-Proxy
- Wwwoffle

[Bearbeiten]

Listen von Proxies

- Proxy-World (*http://www.proxy-world.de*)
- Atomintersoft (*http://www.atomintersoft.com/products/alive-proxy/proxy-list/*)
- Samair.ru (*http://www.samair.ru/proxy/*)
- www.Proxylisten.de (*http://www.proxylisten.de*)

Bekannte Proxy-Client-Software:

- Java Anonymity & Privacy (*http://anon.inf.tu-dresden.de/*) (JAP) - Anonymisierungsprogramm

Application Gateway

aus Wikipedia, der freien Enzyklopädie

Ein **Application Gateway**, oder auch Application Level Gateway ist eine Firewall, die auf der Anwendungsschicht arbeitet. Dabei werden die Datenpakete nicht nur einzeln betrachtet (z.B. nach Quell- oder Zieladresse überprüfen), sondern auf Inhalt bzw. Bedeutung überprüft. Zum Beispiel ist ein Spamfilter oder ein Proxy *Application Level Gateways*.

Smoothwall

aus Wikipedia, der freien Enzyklopädie

Smoothwall ist ein Open Source-Projekt, das es zum Ziel hat, eine leicht konfigurierbare Firewall auf Basis von Linux mit wenig Hardwareressourcen (min 468SX, 32MB RAM, 512 MB HDD, CD-ROM-Laufwerk für die Installation) zu realisieren. Das System ist geeignet, um kleinere Firmen und Privatanwender mit einer Firewall zu schützen. Die neueste Version von 2003, Smoothwall Express 2.0, basiert auf Linux-Kernel 2.4.27 und installiert sich vollautomatisch auf einer Festplatte. Die Administration erfolgt bei der Installation lokal am Rechner. Ein logisch aufgebauter Assistent macht dies auch ohne Linuxkentnisse möglich. Ist das System dann einmal gestartet, kann man über ein Webinterface mit jedem beliebigen Browser zugreifen. Es gibt auch die Möglichkeit, diverse Internetanbindungen zu konfigurieren (DSL, ISDN, Modem). Integriert ist auch ein SSH-Zugang zur Administration von außen. Außerdem beinhaltet diese Firewall auch eine IDS (Intrusion Detection System) (snort).

Die Vorversion Smoothwall GPL 1.0 beruht auf Linux-Kernel 2.2, wird aber weiterhin gepflegt. Sie ist auch in deutscher Version verfügbar. Allerdings liegt ihr der veraltete Paketfilter IPchains zugrunde.

[Bearbeiten]

Weblinks

- http://www.smoothwall.org - Projektwebseite
- http://www.little-idiot.de/firewall/zusammen.html - Deutsche Beschreibung des Linux-Paketfilters