

Firewall-Systeme

Einführung

Ein Firewall-System weist eine unverkennbare Analogie zu einem elektronischen Pförtner und einer elektronischen Brandschutzmauer auf. Sie sichert und kontrolliert den Übergang von einem zu schützenden Netz zu einem unsicheren öffentlichen Netz. Dabei muss ein Firewall-Element grundsätzlich zwei Aspekte erfüllen, um der besagten Analogie gerecht zu werden:

- **Brandschutzmauern**
Als erstes ist ein Firewall-Element dafür zuständig einen Bereich in einem Netzwerk abzusichern, um eine Schadensbegrenzung in einem Notfall einzuräumen. Die eskalierende Seite wird so abgeschottet, dass Schäden nicht auf andere Teile des Netzes überschwappen können. Entsprechend wird das Gebäude einer Organisation in bestimmte Abschnitte unterteilt, damit beim Ausbruch von Feuer in einem Segment nicht andere Teile der Location ohne weiteres griffig für Schäden werden können. Auf Kommunikationsnetze bezogen bedeutet dies, dass das Firewall-Element das zu schützende Netz gegen Gefahren aus dem unsicheren Netz abkapselt. Es wird nur ein einziger, sicherer und bewachter Durchgang zwischen den beiden Teilnetzen gewährleistet: Der sogenannte "Common Point of Trust".
- **Pförtner**
Ein Firewall-System hat zudem die Aufgabe als Analogie zum Pförtner den Transfer zu kontrollieren. Möchte ein Besucher das Gebäude der Organisation betreten, so wird er identifiziert und authentisiert. Mitarbeiter werden als Mitarbeiter vermerkt, und Gäste werden als Gäste notiert. Außerdem wird kontrolliert, welche Gegenstände in das Gebäude eingeführt und ausgeführt werden. All diese Ereignisse werden sorgfältig beim Pförtner protokolliert, zum Beispiel, wann welcher Besucher gekommen und gegangen ist. Ebenso, wen er besucht hat und welche Gegenstände er beim jeweiligen Übertritt des Kontrollpunktes bei sich trug. Eventuell auftretende Unregelmäßigkeiten oder verdächtige Aktionen können anhand der Protokollierung im Nachhinein analysiert werden. Das elektronische Äquivalent zum Pförtner ist ein Firewall-Element, das überprüft, wer aus dem unsicheren Netz auf das zu schützende Netz zugreifen darf. Es kontrolliert, über welche Protokolle und Dienste zugegriffen wird und mit welchen Hosts kommuniziert werden darf. In diesem Sinne ist ein Firewall-System also gleichzeitig eine Brandschutzmauer und ein elektronischer Pförtner. Eine Firewall-Lösung und -Implementierung fällt jeweils sehr individuell aus und muss den jeweiligen Ansprüchen angepasst werden. Außerdem darf nicht außer Acht gelassen werden, dass ein solcher Knotenpunkt technische, personelle, organisatorische und infrastrukturelle Sicherheitsmechanismen erfordert.

Voraussetzung für das effiziente Ausnutzen (im positiven Sinne!) der Möglichkeiten eines Firewall-Systems ist ein durchdachtes Sicherheitskonzept. Ähnlich wie beim Pförtner gilt, dass nicht die Firewall etwas sicher macht, sondern mit ihr kann man etwas sicher machen, wenn sie richtig betrieben wird. Das bedeutet, dass ein Unternehmen sich vor dem Angehen an die Implementierung einer proprietären Zwischenlösung an sich an die Ausarbeitung eines Sicherheitskonzeptes machen sollte. In diesem analytischen Zusammentragen muss definiert werden, was vor wem und wer von was geschützt werden soll. Es macht wenig Sinn, sich Hals über Kopf für eine vermeintliche ultimative Lösung zu entscheiden, wenn man sich eigentlich gar nicht über das Problem im Klaren ist. Die Reduzierung des Zugriffs erhöht die Sicherheit und erleichtert die Kontrolle und Administration des Firewall-Systems. Das Fehlen von Überschaubarkeit kann bei einem solchen Projekt zur Achilles-Ferse werden.

Zielsetzung

Ein Firewall-System wird quasi als Schranke zwischen das zu schützende und das unsichere Netz geschaltet, so dass der ganze Datenverkehr zwischen den beiden Netzen nur über das Firewall-Element möglich ist. Es stellt also im wahrsten Sinne des Wortes den "Common Point of Trust" für den Übergang zwischen unterschiedlichen Netzen dar. Auf der Firewall werden Mechanismen implementiert, die die ganzen Transaktionen sicher und beherrschbar machen sollen. Dazu analysiert das Firewall-System die Kommunikationsdaten, kontrolliert die Kommunikationsbeziehungen und Kommunikationspartner, reglementiert die Kommunikation nach einer Sicherheitspolitik, protokolliert Ereignisse und alarmiert gegebenenfalls bei

ans Internet in vielerlei Hinsicht sicherer zu machen. Doch auch das aufteilen in Segmente oder Subnetze macht Sinn; besonders bei großen Netzwerken. Die Vorteile des "Common Point of Trust" lässt sich auf die geringen Kosten, Umsetzung der Sicherheitspolitik, Möglichkeiten, erhöhte Sicherheit und Überprüfbarkeit aufsummieren.

Allgemeine Ziele

Die allgemeinen Ziele von Firewall-Systemen sind folgende:

- Zugangskontrolle auf Netzwerkebene
- Zugangskontrolle auf Benutzerebene
- Zugangskontrolle auf Datenebene
- Rechteverwaltung
- Kontrolle auf der Anwendungsebene
- Entkoppelung von Diensten
- Beweissicherung und Protokollauswertung
- Alarmierung
- Verbergen der internen Netzstruktur
- Vertraulichkeit von Nachrichten

Um diese Ziele in greifbare Nähe rücken zu lassen, muss das Firewall-System selber gewisse Anforderungen erfüllen:

- Das Firewall-System muss selbst resistent gegen Angriffe sein.
- Accounting (IP- und benutzerorientiert)
- NAT - Network Adress Translation (auch IP-Masquerading genannt)

Paketfilter

Einführung

Das aktive Firewall-Element Packet Filter analysiert und kontrolliert die ein- und ausgehenden Pakete auf der Netzzugangs-, der Netzwerk- und der Transportebene. Dazu werden die Pakete, nicht nur TCP/IP-Protokolle, aufgenommen und analysiert. Diese Analyse wird aufwendiger, sobald auch der Inhalt der einzelnen Pakete durchforstet werden soll; daher wird normalerweise nur ein rascher und hastiger Blick auf den Header geworfen. Die beiden Netze werden bei einer solchen Implementierung physikalisch entkoppelt. Ein Paket-Filter verhält sich wie eine normale Bridge und werden transparent in eine Leitung eingefügt.

Nach der Analyse des Pakets wird verifiziert, ob sie unter eine bestimmte Regel fallen, und dementsprechende Reaktionen ausgeführt. In den Regeln wird vorzugsweise definiert, dass nur die notwendigste Kommunikation erlaubt ist; alle Verstöße werden abgewiesen (engl. deny) oder verworfen (engl. drop). Dadurch können sicherheitskritische Aktionen, wie zum Beispiel IP-Fragmentierung, von vornherein ausgeschlossen werden.

Name	Hersteller	Homepage
Axent Eagle Raptor		
Biodata BIGfire	Biodata	http://www.biodata.com/ch/products/network/bigfire.cphtml
Biodata BIGfire+	Biodata	http://www.biodata.com/ch/products/network/bigfireplus_office.cphtml
Cisco PIX Firewall	Cisco	
Check Point Firewall-1		

Allgemeine Arbeitsweise

- Es wird überprüft, von welcher Seite das Paket empfangen wird (Informationen aus dem Einbindungsmodul).
- Auf der Netzzugangsebene werden die Quell- und Ziel-Adresse und der verwendete Protokoll-Typ kontrolliert.
- Auf Netzwerkebene wird je nach Protokoll-Typ das Paket anders kontrolliert.
 - IP: die Ziel-, Quell-Adresse, verwendetes Schicht-4-Protokoll, Optionsfeld und Flags
 - ICMP: die ICMP-Kommandos/-Typen
 - IPX: Network und Node
 - OSI-Protokoll: die OSI-Netzwerkadresse
- Auf Transportebene findet bei UDP und TCP eine Überprüfung der Portnummern (Quell- und Ziel-Port) statt, bei TCP zusätzlich eine Überprüfung der Richtung des Verbindungsaufbaus statt.
- Zusätzlich kann überprüft werden, ob der Zugriff in einem erlaubten Zeitrahmen geschieht.

Die entsprechenden Prüfinformationen werden aus dem Regelwerk (Accessliste und Rechtestliste) entnommen und mit den Ergebnissen der jeweiligen Analysen verglichen.

Dynamische Paketfilter

Bei verbindungslosen Kommunikationsverbindungen, wie dies zum Beispiel bei UDP der Fall ist, kann nicht grundsätzlich festgelegt werden, von wem ein Verbindungsaufbau durchgeführt wird. Dynamische Paketfilter besitzen in einem solchen Fall die zusätzlich Eigenschaft, sich die Informationen (IP-Adresse und Port) der nach außen geschickten UDP-Pakete zu merken und nur die entsprechend passenden Antworten der virtuellen Verbindung zurückzulassen. Das bedeutet genauer, dass nur die Antwortpakete durchgelassen werden, die vom selben Host und gleichen Port kommen, an den das ursprüngliche UDP-Paket gesendet worden ist und entsprechend zum gleichen System retourniert wird. Der Name rührt also daher, dass die Filter-Regeln intern dynamisch gehandhabt werden. Dienste wie SNMP können über dynamische Paketfilter also viel sicherer angeboten werden.

Zustandsorientierte Paketfilter

Der Leistungsumfang von Paketfiltern kann dadurch erweitert werden, indem die Interpretation der Pakete auch auf höheren Kommunikationsebenen durchgeführt wird. In Fall einer solchen "stateful inspection" werden die Pakete auch auf der Anwendungsebene interpretiert und die Informationen bewertet und festgehalten.

Diese zustandsorientierten Paketfiltern haben die Vorteile von herkömmlichen Packet Filter, können aber zusätzlich die Anwendungen kontrollieren. Einige Risiken bleiben jedoch, weil keine direkte Entkoppelung der Dienste realisiert ist. Außerdem ist dieses Interpretieren und Festhalten zusätzlicher Kommunikationsdaten dieser verschiedenen Ebenen sehr komplex. Aus diesem Grund findet aus technischen Gründen eine weitaus weniger tiefgründige Analyse statt oder jene sind oft stark fehleranfällig, da eine sehr komplexe und mächtige Software genutzt wird.

Vorteile von Paketfiltern

- Transparent für Benutzer und die Rechensysteme. Ausnahmen sind natürlich explizite Authentifizierungen.
- Einfach erweiterungsfähig für neue Protokolle.
- Flexibel für neue Dienste.
- Für andere Protokollfamilien verwendbar (IPX, OSI, DECNET, SNA, ...).
- Hohe Performance durch optimale Mechanismen (Hardware, Betriebssystem, Treiber, ...).
- Leicht realisierbar, da geringe Komplexität.

Nachteile von Paket-Filtern

- Daten, die oberhalb der Transportebene sind, werden in der Regel nicht analysiert.
- Für die Anwendungen (FTP, HTTP, SMTP, ...) besteht keine Sicherheit.
- Falsch konfigurierte oder kompromittierte Hosts im internen Netz können für normalerweise nicht erlaubte Kommunikationen zwischen den beiden Netzen missbraucht werden.
- Protokolldaten werden nur bis zur Transportebene zur Verfügung gestellt.
- Typische Paketfilter können die Struktur des internen Netzes nicht verbergen (NAT ist kein zwingendes Feature).

Application-Gateways

Einführung

Ein Benutzer, der über ein Application-Gateway kommunizieren möchte, muss sich zuerst beim Firewall-System identifizieren und authentisieren. Es gibt verschiedene Möglichkeiten, wie diese Authentifizierung von statten gehen kann. Danach wird die Kommunikation für den Anwender transparent weitergeführt: Für ihn sieht es so aus, als würde er einen direkten Datenaustausch mit seinem Ziel abhalten. Damit diese Lösung realisiert werden kann, muss auf dem Application-Gateway ein Dienst laufen, der über einen definierten Port ansprechbar ist. Die Pakete an diesen Port werden analysiert und gegebenenfalls weitergeleitet. Eine solche Software ist in der Regel nur für einen Dienst (HTTP, FTP, SMTP, ...) konzipiert worden und wird als Proxy bezeichnet. Für jeden Dienst, der über das Application-Gateway ansprechbar und weiterleitbar sein soll, muss ein eigener Proxy vorhanden sein, aber auch keine weitere Software, die diesen Dienst ermöglichen könnte.

Jeder Proxy auf dem Application-Gateway kann speziell für seinen Dienst, für den er zuständig ist, weitere Sicherheitsdienste anbieten. Auch die Analyse ist auf dieser Kommunikationsebene sehr intensiv möglich, da der Kontext der Anwendungsdaten für den jeweiligen Dienst klar definiert ist. Der Vorteil ist, dass kleine überschaubare Module genutzt werden, und so die Fehleranfälligkeit erfreulich niedrig gehalten werden kann.

Das Security-Management darf aus Sicherheitsgründen nicht auf demselben Rechnersystem laufen oder zumindest nicht zur gleichen Zeit, wie das Application-Gateway. Zudem sollen keine Routing-Funktionen auf dem Host aktiv sein, damit nicht an den Proxies vorbeigeschmuggelt werden kann.

Da das Application-Gateway bei der Kommunikation jeweils zum Rechnersystem des unsicheren Netzes und zu dem zu schützenden Netzes eine Kommunikationsverbindung hat, bietet es eine "Network Address Translation". Dabei hat das Application-Gateway für die jeweiligen Interfaces zwei verschiedene IP-Adressen, die auch jeweils nur für die jeweilige Richtung genutzt werden.

Name	Hersteller	Homepage
Biodata BIG Application	Biodata	http://www.biodata.com/ch/products/network/bigapplication.cphtml
Microsoft ISA Server	Microsoft	
Microsoft Proxy 2.0	Microsoft	http://www.microsoft.com/germany/backoffice/proxy/
Squid	Squid	http://www.squid-cache.org/
Surfcontrol CSM Enterprise	Surfcontrol	http://www.csm.co.at/download/products/ep/index.htm

Application-Level-Proxies

Application-Level-Proxies sind für bestimmte Dienste/Anwendungen implementiert. Aus diesem Grund kennen sie die Kommandos der Anwendungsprotokolle und können diese detailliert analysieren und ebenso haargenau kontrollieren. Application-Level-Proxies arbeiten mit der gängigen, unveränderten Clientsoftware für ihre individuellen Dienste. Oft wurde aber zudem eine veränderte Vorgehensweise im Falle einer gewünschten Authentifikation beim Application-Level-Proxy implementiert.

SMTP-Proxy

Ein SMTP-Proxy arbeitet nach dem Store-and-Forward-Prinzip, welches in gewissem Masse eine Analogie zum Sammelbriefkasten aufweist. Dabei wird als erstes die komplette Mail vom SMTP-Proxy abgespeichert. Ein Weitersenden wird erst eingeleitet, wenn die erste Phase des Annehmens erfolgreich verlief. Für die Mail-Kommunikation ist also keine end-to-end Beziehung zwischen eigentlichem Sender und seinem nächst direktem Empfänger notwendig.

Der SMTP-Proxy arbeitet nicht benutzerorientiert und erfordert daher keine Authentifikation. Eine ankommende E-Mail wird standardmäßig auf dem TCP-Port25 (SMTP) entgegengenommen und nach der Überprüfung des Absenders auf dem Application-Gateway in einem speziellen Verzeichnis abgelegt. Der SMTP-Daemon prüft periodisch, ob neue Nachrichten eingegangen sind. Der Mail Transfer Agent (MTA) stellt dem Adressaten die elektronische Post direkt oder über einen oder mehrere MTAs zu. Der SMTP-Proxy verhindert damit, dass der MTA direkt mit dem unsicheren Netz kommunizieren kann.

Der wohl beliebteste MTA ist unbestritten Sendmail. Er wird aufgrund seiner hohen Skalierbarkeit vielerorts eingesetzt. Sendmail ist jedoch auch für seine Vielzahl von Sicherheitslücken und Implementierungsfehlern bekannt. Ein SMTP-Proxy verarbeitet daher nur die folgenden Befehle nach RFC 821 (SMTP - Simple Mail Transfer Protocol), die nicht sicherheitskritisch sind:

- HELO
- MAIL
- RCPT
- DATA
- QUIT
- RSET
- NOOP.

Einige weitere Befehle werden mit Standardantworten quittiert:

- HELP
- VRFY
- EXPN.

Bei Nutzen eindeutig sicherheitsrelevanten Befehlen wie

- DEBUG

wird eventuell direkt der Security-Manager mit einer Nachricht informiert. Da die Befehle zuerst den SMTP-Proxy durchlaufen müssen, kann der DEBUG-Befehl einfach ignoriert werden, um den potentiellen Angriff durch eine Suche nach Implementierungsfehlern zu unterbinden. Durch die Verwendung des Store-and-Forward-Prinzips wird eine Entkoppelung des komplexen und fehlerbehafteten MTAs, in diesem und vielen anderen Szenarien erreicht. Sendmail wird nicht direkt mit Befehlen angesprochen, sondern nur die

Software.

Im Logbuch des Application-Gateways können durch das SMTP-Proxy die folgenden Protokolldaten für eine spätere Auswertung festgehalten werden:

- IP-Adresse und Rechnername des Quell-Rechnersystems
- Uhrzeit und Datum des Verbindungsaufbaus
- Absender der Nachricht (wie im Mail-Header angegeben)
- Empfänger der Nachricht (wie im Mail-Header angegeben)
- Anzahl der übertragenen Bytes
- Uhrzeit und Datum des Verbindungsabbaus

Im Logbuch des Application-Gateways werden durch den Message Transfer Agent die folgenden Protokolldaten für eine spätere Auswertung festgehalten:

- IP-Adresse und Rechnername des Ziel-Rechnersystems
- Uhrzeit und Datum des Verbindungsaufbaus
- Absender der Nachricht (wie im Mail-Header angegeben)
- Empfänger der Nachricht (wie im Mail-Header angegeben)
- Anzahl der übertragenen Bytes
- Uhrzeit und Datum des Verbindungsabbaus

Benutzerorientierte Application-Level-Proxies

Die folgenden Proxies für Telnet, FTP und HTTP sind benutzerorientierte Proxies, da sie selbst eine Authentifikation mit dem entsprechenden Benutzer durchführen. Im Falle einer erfolgreichen Identifikation und Authentifikation des Anwenders beim Proxy gilt diese nur für jenen speziellen Proxy. Für das Nutzen eines anderen Dienstes/Proxies, muss sich der User erneut authentifizieren. Benutzerorientierte Proxies haben den Vorteil, dass die Zuordnung zwischen Benutzer und IP-Adresse und dem gewünschten Dienst eindeutig und lückenlos ist.

Telnet-Proxy

Der Telnet-Proxy ist für die kontrollierte Kommunikation über Telnet verantwortlich und stellt entsprechende Sicherheitsfunktionen für diesen Dienst zur Verfügung.

Der Verbindungsaufbau erfolgt vom Quell-Rechnersystem auf TCP-Port23 (Telnet) des Application-Gateways. An diesem well-known Port für Telnet übernimmt der Telnet-Proxy automatisch die Verbindung. Der Telnet-Proxy kann erkennen, ob an diesem Port ein anderer Dienst aktiviert wurde, so dass der Verbindungsaufbau bei Zuwiderhandlung nicht zustande kommt. Der Benutzer auf dem Client identifiziert und authentisiert sich unter der Angabe des Verbindungsziels beim Telnet-Proxy. Wurde diese zweite Phase erfolgreich abgewickelt, wird ein individuelles Benutzerprofil aktiviert, welches sich aus folgenden Punkten zusammensetzt:

- IP-Adresse des Quell-Rechnersystems, das die Verbindung aufbauen möchte.
- Benutzername, mit dem die Identifikation und Authentifikation erfolgte.
- IP-Adressedes Ziel-Rechnersystems
- In der dritten Phase baut der Telnet-Proxy eine zweite Verbindung vom Application-Gateway auf TCP-Port 23 des Ziel-Systems auf. Jetzt kann der Benutzer von seinem Client aus über den Telnet-Proxy mit dem Telnet-Dienst des Ziel-Systems interagieren. Und trotzdem bleibt die Netzstruktur des zu schützenden Netzes verborgen.

Bei einer über einen Telnet-Proxy geschauften Telnet-Kommunikation ist es zum Beispiel möglich zu erkennen, ob ein Benutzer unerlaubt vom Quell-Rechnersystems auf ein anderes Rechnersystem als das

Authentifikationen zu unterlaufen. Der Control-Monitor überprüft den Datenstrom auf Bytereihenfolgen, die verdächtigen Aktivitäten zugeordnet werden können. Es ist natürlich auch Möglich nach anderen Informationen zu suschen, wie zum Beispiel Steuerzeichen, die nicht verwendet werden sollen (z.B. [CTRL]+[C]).

Im Logbuch des Application-Gateways werden durch den Message Transfer Agent die folgenden Protokolldaten für eine spätere Auswertung festgehalten:

- IP-Adresse und Rechnername des Ziel-Rechnersystems
- Uhrzeit und Datum des Verbindungsaufbaus
- Absender der Nachricht (wie im Mail-Header angegeben)
- Empfänger der Nachricht (wie im Mail-Header angegeben)
- Anzahl der übertragenen Bytes
- Uhrzeit und Datum des Verbindungsabbaus

FTP-Proxy

Der FTP-Proxy ist für die kontrollierte Kommunikation über das File Transfer Protocol verantwortlich und stellt entsprechende Sicherheitsfunktionen für diesen Dienst zur Verfügung.

Der Verbindungsaufbau für den Kommandokanal erfolgt vom Quell-Rechnersystems auf TCP-Port21 (FTP) des Application-Gateways. Der Benutzer auf dem Client-System identifiziert und authentisiert sich, unter der Angabe des Verbindungsziels, nun gegenüber dem FTP-Dienst. Nach erfolgreicher Authentifikation wird ein den folgenden Bedingungen entsprechendes individuelles Benutzerprofil aktiviert:

- IP-Adresse des Quell-Rechnersystems, das die Verbindung aufbauen möchte
- Benutzername, mit dem die Authentifikation erfolgte
- IP-Adresse des Ziel-Rechnersystems
- Nun baut der FTP-Proxy einen zweiten Kommandokanal vom Application-Gateway auf TCP-Port21 (FTP) des eigentlichen Ziel-Rechnersystems auf.

Der sogenannte Kommando-Filter analysiert und verifiziert alle vom Benutzer eingegebenen FTP-Kommandos hinsichtlich ihres Eintrags in der zuvor definierten Rechtedatei, die für jeden Anwender individuell ausfallen kann. Für den FTP-Proxy kann zum Beispiel bestimmt werden, welche Befehle verwendet werden dürfen und welche unerwünscht sind. Gibt der Benutzer ein Kommando ein, welches nicht geblockt, verworfen oder geloggt wird, so findet ohne Umschweife ein Verbindungsaufbau statt. Dieser kann von irgendeiner der beiden Seiten initiiert werden, jenachdem, ob eine passive oder aktive FTP-Verbindung gewünscht wurde.

Außerdem kann der FTP-Proxy durch einen Datei-Filter eine Namensrestrukturierung vornehmen, die übertragen werden dürfen.

In der Logdatei des Application-Proxies für FTP können die folgenden Protokolleinträge standardmäßig vorgenommen werden:

- IP-Adresse und Rechnername des Quell-Rechnersystems
- IP-Adresse und Rechnername des Ziel-Rechnersystems
- Uhrzeit und Datum des Verbindungsaufbaus
- Name des Benutzers
- Anzahl der übertragenen Bytes
- Name der übertragenen Dateien
- Uhrzeit und Datum des Verbindungsabbaus

HTTP-Proxy

und stellt entsprechende Sicherheitsfunktionen für diesen Dienst zur Verfügung.

Der Verbindungsaufbau erfolgt vom Quell-Rechnersystem auf TCP-Port80 (HTTP) des Application-Gateways. An diesem well-known Port für HTTP übernimmt der HTTP-Proxy automatisch die Verbindung. Der Benutzer auf dem Client identifiziert und authentisiert sich unter der Angabe des Verbindungsziels beim HTTP-Dienst. Wurde diese zweite Phase erfolgreich abgewickelt, wird ein individuelles Benutzerprofil aktiviert, welches sich aus folgenden Punkten zusammensetzt:

- IP-Adresse des Quell-Rechnersystems, das die Verbindung aufbauen möchte
- Benutzername, mit dem die Authentifikation erfolgte
- IP-Adresse des Ziel-Rechnersystems.
- Nun baut der HTTP-Proxy vom Application-Gateway eine zweite Verbindung zum TCP-Port80 (HTTP) des eigentlichen Ziel-Rechnersystems auf. Jetzt kann der Benutzer mit seinem Browser den Dienst des Ziel-Hosts unter transparenter Einwirkung des Application-Gateways nutzen.

Da das HTTP-Protokoll nicht session-orientiert arbeitet, ist der HTTP-Proxy dementsprechend auch nicht in der Lage, das Ende einer Sitzung zu erkennen. Bei jeder Anforderung einer WWW-Seite wird eine Verbindung über das Firewall-System aufgebaut, die Dokumente übertragen und die Kommunikationsverbindung wieder abgebaut. Beim ersten Mal wird vor der Übertragung die Authentifikation durchgeführt. Aus diesem Grund wird ein Timer gesetzt, der den Beginn der Session festhält. Nach Ablauf dieses Timers wird der HTTP-Proxy automatisch abgeschaltet. Bei jeder weiteren Kommunikation über den HTTP-Proxy wird der Timer nach erfolgreicher Authentifikation erneut gesetzt.

Der Kommando-Filter analysiert und überprüft die verwendete Methoden (FTP, HTTP, NNTP, SMTP, ...) und die dafür verwendeten Befehle (z.B. put, get, post). Jeder Versuch, eine nicht zulässige Anforderung abzusetzen, wird ihm angezeigt und es erfolgt der entsprechende Eintrag in die Protokolldateien. Es können auch spontane Benachrichtigungen vom Security-Management durchgeführt werden, falls grobe Regelverstöße registriert worden sind.

Mit der Hilfe eines Daten-Filters im HTTP-Proxy können definierte URLs zugelassen oder geblockt werden. So können zum Beispiel nur bestimmte Top-Level-Domains (z.B. ch und de) ansprechbar sein. Durch den Daten-Filter können jedoch auch bekannte, nicht gewünschte Dateien oder HTTP-Seiten durch den Proxy ausgefiltert werden.

Aktive Inhalte innerhalb von HTML-Dokumenten können eine Gefährdung für einen Host darstellen, der das Dokument interpretieren soll. Hier kommt Content-Security ins Spiel, der vor solchen schädlichen Webapplicationen schützen soll. Ein Applet-Filter kann Java, JavaScripts und ActiveX kontrollieren oder ausschliessen. Durch den sogenannten Malware-Filter können korrupter Programmcode (z.B. Viren, trojanische Pferde, Würmer, ...) aufgespürt und ihnen durch externe Lösungen (z.B. Antiviren-Software) entgegengewirkt werden.

In der Logdatei des Application-Proxies für HTTP können die folgenden Protokolleinträge standardmäßig vorgenommen werden:

- IP-Adresse und Rechnername des Quell-Rechnersystems
- IP-Adresse und Rechnername des Ziel-Rechnersystems
- Uhrzeit und Datum des Verbindungsaufbaus
- Name des Benutzers
- Anzahl der übertragenen Bytes
- Name der übertragenen Dateien oder übertragenen HTML-Seite
- Uhrzeit und Datum des Verbindungsabbaus

Authentication-Proxy (Global Authentication)

sogenannten Authentication-Proxy durchführen lässt. Diese Art der Authentifizierung wird auch "Global Authentication" genannt. Dieser spezielle Proxy führt die Rechteverwaltung für die unterschiedlichen Dienste durch.

Der Vorteil liegt darin, dass keine erneute Authentifizierung des Benutzers durchgeführt werden muss, wenn er den Dienst wechseln möchte.

Der Nachteil dieser Methode tritt besonders bei Multiuser-Systemen ins Rampenlicht, denn es kann keine eindeutige Verbindung zwischen Dienst und Benutzer erkannt werden. Ausserdem kann während der Zeit der Freischaltung der Verbindung auf dem Application-Gateway und dem Connect des Clients der Dienst von Angreifern benutzt werden.

Transparent Proxies

Transparente Proxies haben die Eigenschaft sich komplett transparent dem Benutzer gegenüber zu verhalten. Der Vorteil dieser Lösung besteht darin, dass die Client-Software nicht verändert oder modifiziert werden muss, um den Proxy-Service zu nutzen. Viele ISPs (Internet Service Provider) nutzen transparente Proxies, das beste Beispiel ist AOL (American Online), um eine höhere Performance bei der Netzanbindung gewährleisten zu können.

Circuit-Level-Proxies

Da bei Application-Gateways aus Sicherheitsgründen kein Routing auf der Netzwerkebene möglich sein darf, können für Dienste, für die keine Proxy-Suite zur Verfügung steht, sogenannte Circuit-Level-Proxies implementiert werden, wenn eine Kommunikation über das Application-Gateway realisiert werden soll. Circuit-Level-Proxies sind eine Art generische Proxies, die für eine Mehrzahl von Diensten mit verschiedenen Protokollen verwendet werden können. Diese Proxy-Art, die auch als generische Proxies, Port-Relays oder Plug-Gateways bezeichnet werden, können in der Regel für TCP- und UDP-Anwendungen Verwendung finden.

Mit einem Port-Relay wird eine Kommunikation über die Portnummer des Port-Relays adressiert und kann daher nur auf eine definierte IP-Adresse erfolgen. Aus diesem Grund sind Port-Relays immer n:1. Viele Hosts (IP-Adressen) von der einen Seite können auf einen Rechner (eine IP-Adresse) auf der anderen Seite zugreifen - Der umgekehrte Weg ist nicht möglich.

In der Logdatei des Port-Proxies können die folgenden Protokolleinträge standardmäßig vorgenommen werden:

- IP-Adresse und Rechnername des Quell-Rechnersystems
- IP-Adresse und Rechnername des Ziel-Rechnersystems
- Uhrzeit und Datum des Verbindungsaufbaus
- Anzahl der übertragenen Bytes
- Uhrzeit und Datum des Verbindungsabbaus

SOCKS

SOCKS stellt eine standardisierte Umgebung zur transparenten und sicheren Nutzung eines Firewall-Systems zur Verfügung. Um dies zu erreichen, schaltet es sich zwischen die Anwendungs- und Transportebene:



In dieser Zwischenschicht sitzend fängt SOCKS die TCP- und UDP-Verbindungsanfragen der Applikationen ab und setzt diese auf das SOCKS-Protokoll um. Die Kommunikation findet alsdann in der Form eines sogenannten Tunnels zwischen dem SOCKS-Client und dem SOCKS-Server statt. Die Integration dieser Möglichkeit und der SOCKS-Protokoll-Standard in der Version 5 ist in RFC 1927 definiert.

SOCKS vereint die Möglichkeiten eines Circuit-Level-Proxies mit denen eines Application-Level-Proxies. Der eindeutige Nachteil des Nutzens von SOCKS ist, dass in jedem Fall Änderungen auf der Client-Seite durchgeführt werden müssen, da es bisher nur sehr wenige Applikationen gibt, die SOCKS direkt unterstützen.

Die veraltete Version 4 des SOCKS-Protokolls enthielt keinerlei Sicherheitsmassnahmen zur Authentikation und Wahrung der Vertraulichkeit und Integrität. Es wurden nur die Kommandos "Bind" und "Connect" unterstützt.

Die aktuelle Version 5 von SOCKS enthält folgende Merkmale:

- Standardisierte Schnittstellen zur Integration von starken Authentifikationsmechanismen.
- Erweitertes Adress-Schema zur Unterstützung von IPv4, IPv6 und Domain-Namen.
- Unterstützung für TCP und UDP.
- Verfügbare Implementationen integrieren sich transparent in das Betriebssystem.

Allerdings weist auch SOCKS gewisse Nachteile auf:

- Der Aufbau simultaner und paralleler Verbindungen von einem Server zu einem Client ist nicht ausreichend unterstützt.
- Die UDP-Implementation bietet keine Unterstützung von Multicasts.
- Großer Protokoll-Overhead pro Verbindung.
- Es existieren keine standardisierten Erweiterungen.
- Die Skalierbarkeit von SOCKS 5 ist nicht ausreichend.

Für die nächste Protokoll-Generation von SOCKS sind folgende Erweiterungen geplant:

- Major und Minor Version Nummerierung für bessere Rückwärts-Kompatibilität.
- Standard Mechanismus zur Aushandlung von Protokoll-Erweiterungen.
- Nutzung eines Kontrollkanals zur Reduzierung des Payloads.
- TCP: Bind-Kommandoerweiterungen zur Unterstützung von mehreren Verbindungen auf den offenen Port, sowie die Möglichkeit der Vorgabe eines bestimmten Ports durch den Client.
- UDP: Unterstützung für Multicast
- UDP: Wahlmöglichkeit zwischen Senden und Empfangen von Datagrammen
- UDP: Möglichkeit der Tunnelung von Datagrammen durch einen zuverlässigen Kanal

Adaptive Proxies

Viele Firmen für IT-Security versuchen in dem Namen "Adaptive Proxies" die Vorteile von Paket-Filtern und Application-Gateways zu kombinieren. Die Idee hinter diesem Ansatz ist, dass das Firewall-System in einer der Verbindungsaufbauphase wie ein Application-Proxy arbeitet und später in der Datentransferphase wie ein Paket-Filter agiert. Die Vorteile dieser Methode liegen auf der Hand: In der ersten Phase wird eine hohe Sicherheit erreicht, danach erst werden die schnellen Tests durchgeführt.

Desktop-Firewalls

Einführung

Die Gefahr, beim Durchforsten des Internets auf Viren oder korrupten Programmcode zu stoßen, egal ob nun in Form eines ActiveX-Elements oder eines Java-Applets, wächst mit der Bedeutung des Internets. Für eine professionelle Lösung muss relativ tief in die Tasche gegriffen werden, um das eigene Netzwerk vor solchen Gefahren hermetisch abzuriegeln. Daher werden auf Software-Ebene sogenannte Desktop-Firewalls realisiert, welche vorzugsweise Windows-Systeme von Normalanwendern vor Gefahren aus dem Internet bewahren sollen.

Leider ist es so, dass viele auf dem Markt erhältliche Systeme nicht die Anforderungen erfüllen können, die eigentlich an das Objekt in Extremsituationen gestellt werden. Auch die Performance auf dem System nimmt rapide ab, obwohl dies heutzutage bei der eingesetzten Hardware, auch im privaten Bereich, nicht mehr so als negativ ausschlaggebend eingestuft werden muss. Die größte Angriffsfläche bietet jedoch in den wenigsten Fällen die Private-Firewall selbst, sondern das Betriebssystem, auf dem sie aufsetzt.

Trotzdem gilt es für Vielsurfer und im Firmennetz als Muss, stets mit on-the-fly Anti-Viren-Software und Desktop-Firewall in die Weiten des Internets vorzudringen, da dadurch wenigstens sämtliche TCP/IP-Pakete kontrolliert werden können, die den Rechner erreichen. Auch fungieren einige Desktop-Firewalls automatisch als Viren-Scanner, denn sie überprüfen automatisch das Verhalten von ActiveX- und Java-Elementen, die lokale Daten löschen oder auf dem eigenen Rechner unbemerkt im Hintergrund Daten per FTP an einen entfernten Cracker schickt. Die Software-Firewall schafft um ihren Zweck zu erfüllen, einen Schutzbereich, der so eine Art Quarantäne bildet. Dieser Schutzbereich wird Sandbox genannt, wobei ein Programm, welches innerhalb dieser virtuellen Umgebung ausgeführt wird, nur sehr begrenzten Zugriff auf Ressourcen des Systems gewährt bekommt. Zwar ist der Ansatz dieses Sandbox-Systems sehr gut, doch sind die verschiedenen Umsetzungen noch nicht genug ausgereift, um einen umfassenden Schutz in dieser Hinsicht zu geben.

Name	Hersteller	Homepage
Anti-Hack	CarbonSoft	http://www.carbosoft.com/anti-hack.htm
AtGuard	WRQ	http://www.wrq.com/
Back Protection 2001	JMMG Communications	http://www.jmmgc.com/backprotection/index.html
Black ICE Defender	Network ICE Corporation	http://www.netice.com/products/blackice_defender.html
ConSeal PC Firewall	Signal 9	http://www.consealfirewall.com/
Digital Robotics Firewall	Digital Robotics	http://www.digitalrobotics.com/IFW2000.htm
eSafe Desktop	Aladdin / eSafe	http://www.eSafe.com/

GNAT Box Light	Global Technologies Associates, Inc.	http://www.gnatbox.com/Pages/gblight.html
HackerWacker	HackerWacker	http://www.hackerwacker.com/hackerwacker/
HackTracer	Sharp Technology /Neoworx	http://www.neoworx.com/products/hacktracer/default.asp
Jammer	Agnitum	http://www.agnitum.com/products/jammer/
LockDown 2000	LockDown2000	http://lockdown2000.com/
Look 'n' Stop	Soft4Ever	http://www.soft4ever.com/LooknStop/En/decouvrir.htm
McAfee Internet Guard Dog	McAfee	http://www.mcafee.com/myapps/firewall/ov_firewall.asp?
McAfee Personal Firewall	McAfee	http://www.mcafee.com/myapps/firewall/ov_firewall.asp?
Neoworx NeoWatch	Neoworx	http://www.neoworx.com/download/
NetWatcher 2000	Moonlight Software	http://www.moonlight-software.com/netwatcher.htm
Norman Personal Firewall	Norman	http://www.norman.no/products_npf.shtml
Norton Internet Security	Symantec	http://www.symantec.com/region/de/product/nis/
NukeNabber	Dynamicsol	http://www.dynamicsol.com/puppet/nukenabber.html
PC Viper	Edge Technologies	http://www.pcviper.com/
PGP Network Security	Network Associates	http://www.nai.com/international/uk/asp_set/about_nai/at_a_glance/intro.asp
Port Detective	Tzolkín	http://www.portdetective.com/
Privatefirewall	PrivacyWare	http://www.privacyware.com/
Secure4U	Sandbox Security	http://www.sandboxsecurity.com/main.htm
SessionWall-3	AbirNet / Computer Associates	http://www.cai.com/solutions/enterprise/etrust/intrusion_detection/
Sphinx	Biodata	http://www.sphinxwall.com/
Sygate Personal Firewall	Sygate	http://www.sygate.com/
Tiny Personal Firewall	Tiny Software	http://www.tinysoftware.com/pwall.php
Tiny WinRoute Lite	Tiny Software	http://www.tinysoftware.com/winlite.php

Tiny WinRoute Professional	Tiny Software	http://www.tinysoftware.com/winpro.php
ZoneAlarm	ZoneLabs	http://www.zonelabs.com/

Vorteile von Desktop-Firewalls

- Niedrige Kosten.
- Meist für Normal-Anwender zugeschnitten und daher leicht verständlich.

Nachteile von Desktop-Firewalls

- Nicht besonders zuverlässig, da schon alleine das Betriebssystem zu viel Angriffsfläche bietet.
- Viele Anwender können aufgrund fehlender TCP/IP Kenntnisse keine korrekten Filter-Regeln setzen und die Protokollierung auswerten.
- Performance-Einbussen auf der Workstation.