BS Info München

Firewall-Grundlagen
Next-Generation-Firewalls

Firewall-Grundlagen

von Peter Klau (TecChannel)

Sobald zwischen dem lokalen Netz und dem Internet eine Verbindung besteht, können Angreifer versuchen, Daten zu stehlen oder das Netz lahm zu legen. Verschiedene Firewall-Konzepte sorgen für Sicherheit.

Die Sicherheit steht an erster Stelle, wenn das private Netzwerk eines Unternehmens (LAN) mit dem Internet verbunden ist. Eine zunehmende Anzahl von Mitarbeitern braucht Zugang zu Internet-Diensten wie dem WWW, E-Mail, FTP und Remote-Verbindungen (Telnet, SSH). Unternehmen wollen zudem für ihre Webseiten und FTP-Server den öffentlichen Zugang über das Internet ermöglichen. Dabei muss die Sicherheit der privaten Netze gegenüber unautorisierten Zugriffen von außen gewährleistet sein. Der Administrator muss das lokale Netzwerk gegen das große Chaos "Internet" abschirmen, damit Daten nicht in unbefugte Hände geraten oder gar verändert werden. Für Firmen,
die vom Internetzugang abhängig sind, stellen auch die sogenannten DoS-Attacken eine große Gefahr dar.

Mit Firewalls lassen sich Netzwerke gegen unbefugte Zugriffe von außen absichern. Die verfügbaren Lösungen reichen von der Zusatzsoftware bis hin zu speziellen Geräten, die ausschließlich auf diese Aufgabe ausgelegt sind. In ihrer grundlegenden Funktionsweise unterscheiden sich die Systeme allerdings nur wenig.

Definition einer Firewall

Eine Firewall besteht aus einer Gruppe von Netzwerkkomponenten (Hard- und Software) an der Schnittstelle zweier Netze. Sie gewährleistet die Einhaltung von Sicherheitsrichtlinien zwischen einem privaten und einem öffentlichen (nicht sicheren) Netz, wie zum Beispiel dem Internet. An dieser "Brandschutzmauer" entscheidet sich, auf welche Dienste innerhalb des privaten Netzes zugegriffen werden kann und welche Dienste des nicht sicheren Netzes aus dem privaten Netz heraus nutzbar sind. Damit
eine Firewall effektiv arbeiten kann muss entsprechend der gesamte Datenverkehr zwischen dem privaten Netz und dem Internet über diese Station laufen. Die Firewall untersucht alle Pakete und lässt nur die unverdächtigen passieren.

Dabei muss die Firewall ihrerseits immun gegen Eindringlinge sein. Was würde eine Firewall nutzen, wenn Hacker sie nach Belieben anpassen könnten? Daraus lässt sich eine "Schwäche" von Firewalls ableiten: Diese Systeme bieten leider keinen Schutz, sobald es einem Angreifer gelungen ist, sie zu überwinden. Daher ist auf die eigene Sicherheit der Firewall ebenso viel Augenmerk zu legen wie auf die Sicherheit des privaten Netzes selbst, die durch die Firewall gewährleistet werden soll.

Eine Firewall ist nicht wie ein Router, ein Bastion-Host oder ein anderes Gerät Teil des Netzes. Sie ist lediglich eine logische Komponente, die ein privates Netz vor einem öffentlichen Netz schützt. Ohne eine Firewall wäre jeder Host im privaten Netz den Attacken von außen schutzlos ausgeliefert. Das bedeutet: Die Sicherheit in einem
privaten Netz wäre von der Unverwundbarkeit der einzelnen Rechner abhängig und somit nur so gut wie das schwächste Glied im Netz.

Zentraler Sicherheitsknoten

Der Vorteil einer zentralen Firewall ist, dass sie das Sicherheitsmanagement vereinfacht. Damit gilt die von ihr hergestellte Sicherheit für das gesamte Netz und muss nicht für jeden Rechner einzeln definiert werden. Die Überwachung geschieht ebenfalls zentral über die Firewall. So kann sie gegebenenfalls auch einen Alarm auslösen, da Angriffe von außen nur über diese definierte Schnittstelle zwischen den Netzen erfolgen können. Das Erkennen eines Angriffs ist der erste Schritt zur Abwehr des Angreifers.

Als in den letzten Jahren die Internet-Adressen knapp wurden, trat auch in Unternehmen eine Verknappung von IP-Adressen (http://www.tecchannel.de/internet/209/index.html) ein. Eine Internet-Firewall ist in diesem Zusammenhang die geeignete Stelle zur Installation eines Network Address Translators (NAT), der die Adressenknappheit lindern kann. Und schließlich eignen sich Firewalls auch, um den gesamten Datenverkehr von und zum Internet zu überwachen. Hier kann ein Netzwerk-Administrator auch Schwachstellen und Flaschenhälse erkennen.

Nachteile und Begrenzungen

Eine Firewall kann keine Angriffe abwehren, wenn die Pakete nicht durch sie hindurch geleitet werden. Wenn zum Beispiel eine Einwählverbindung via Modem oder ISDN aus dem geschützten Netzwerk besteht, können interne Benutzer eine direkte PPP-Verbindung zum Internet aufbauen. Benutzer, welche die zusätzliche Authentifizierung am Proxy-Server scheuen, werden schnell diesen Weg nehmen. Durch die Umgehung der Firewall erzeugen sie jedoch ein großes Risiko für eine Backdoor-Attacke.

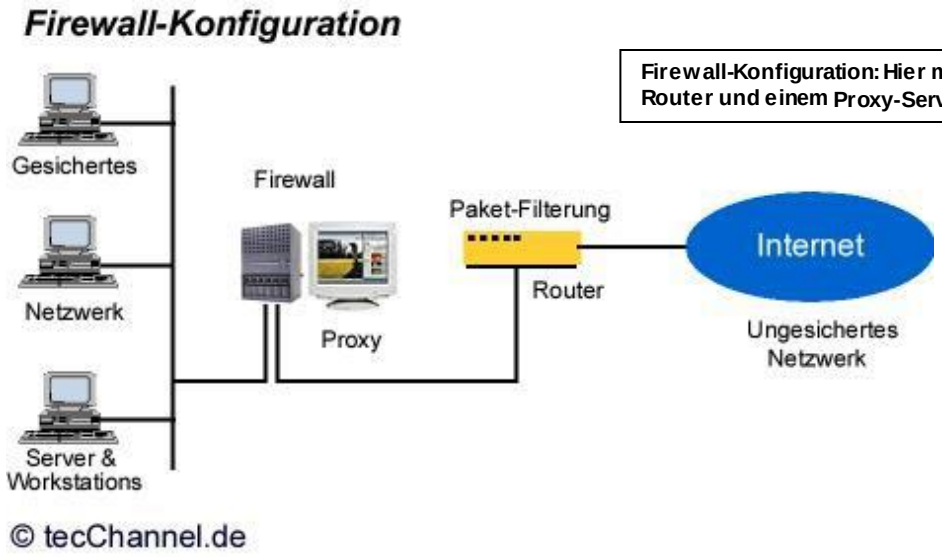
Firewalls nützen nichts bei Angriffen aus den eigenen Reihen. Sie hindern niemanden daran, sensitive Daten auf eine Diskette zu kopieren und sie außer Haus zu schaffen. Erst recht nicht, wenn diese Person weitreichende Rechte hat oder durch Diebstahl an Passwörter gelangt ist. Firewalls schützen auch nicht vor Computerviren oder Trojanern, da sie nicht jedes Datenpaket nach potenziellen Viren durchsuchen können. Auch sogenannte Data-driven Attacks können Firewalls nicht verhindern. Dabei handelt es sich um scheinbar harmlose Daten mit versteckt em Code zur Änderung von Sicherheitseinstellungen.

Zudem muss die Firewall leistungsfähig genug sein, um den Datenstrom analysieren zu können. Je schneller die Internetanbindung, desto mehr Pakete fließen pro Sekunde in und aus dem Netzwerk. Soll die Firewall zudem noch die Datenströme - also nicht nur die einzelnen Pakete, sondern auch den logischen Datenfluss - überwachen, ist ein umso leistungsfähigeres System erforderlich.

Komponenten einer Firewall

Ein Firewall-System kann aus ein bis drei Komponenten bestehen:

- Paketfilterungs-Router
- Proxy-Server (Application Level Gateway)
- Verbindungs-Gateway (Circuit Level Gateway)



Firewall-Konfiguration: Hier mit Paketfilterungs-Router und einem Proxy-Server.

Grundsätzlich konkurrieren zwei Firewall-Konzepte:

Die "passive" Paketfiltertechnologie und die "aktiven" Application Level Gateways. Alle anderen Firewall-Systeme sind Varianten und Weiterentwicklungen dieser beiden Konzepte oder werden damit kombiniert. Dazu gehören etwa das Stateful Packet Filtering, Circuit Level Gateways oder sogenannte Hybrid-Firewalls. Diese Variante stellt eine Kombination aus Paketfilter und Application Level Gateway dar.

Paketfilterungs-Router

Ein Paketfilterungs-Router entscheidet bei jedem Datenpaket anhand festgelegter Filterregeln, ob er es weiterleitet oder nicht. Überprüft werden Header-Informationen wie:

- IP-Ursprungsadresse
- IP-Zieladresse
- das eingebettete Protokoll (TCP, UDP, ICMP, oder IP Tunnel)
- TCP/UDP-Absender-Port
- TCP/UDP-Ziel-Port
- ICMP message type
- Eingangsnetzwerkschnittstelle (Ethernetkarte, Modem, etc.)
- Ausgangsnetzwerkschnittstelle

Falls das Datenpaket die Filter passiert sorgt der Router für die Weiterleitung des Pakets, andernfalls verwirft er es. Wenn keine Regel greift, verfährt der Paketfilterungs-Router nach den Default-Einstellungen.

Anhand der Filterregeln kann ein Router auch eine reine Service-Filterung durchführen. Auch hier muss der Systemadministrator die Filterregeln vorher definieren.
Service-Prozesse benutzen bestimmte Ports (Well Known Ports), wie zum Beispiel FTP den Port 21 oder SMTP den Port 25. Um beispielsweise den SMTP-Service abzublocken, sondert der Router alle Pakete aus, die im Header den Ziel-Port 25 eingetragen haben oder die nicht die Ziel-IP-Adresse eines zugelassenen Hosts besitzen.

Einige typische Filterrestriktionen sind:

- Nach außen gehende Telnet-Verbindungen sind nicht erlaubt.
- Telnet-Verbindungen sind nur zu einem bestimmten internen Host erlaubt.
- Nach außen gehende FTP-Verbindungen sind nicht erlaubt.
- Pakete von bestimmten externen Netzwerken sind nicht erlaubt.

Abwehr von Angriffen

Bestimmte Angriffstypen verlangen eine vom Service unabhängige Filterung. Diese ist jedoch schwierig umzusetzen, da die dazu erforderlichen Header-Informationen Service-unabhängig sind. Die Konfiguration von Paketfilterungs-Routern kann auch gegen diese Art von Angriffen erfolgen, für die Filterregeln sind jedoch zusätzliche Informationen notwendig. Beispiele für diese Angriffe sind:

Source IP Address Spoofing Attacke

Bei einer Spoofing-Attacke fälscht der Angreifer die IP-Absenderadresse eines Datenpakets und verwendet stattdessen die Adresse eines Rechners im internen Netz. Die Firewall kann einen solchen Angriff erkennen, indem sie überprüft, ob ein von außen kommendes Paket eine interne Adresse nutzt. Um den Angriff abzuwehren, sind solche Pakete entsprechend herauszufiltern.

Source Routing Attacke

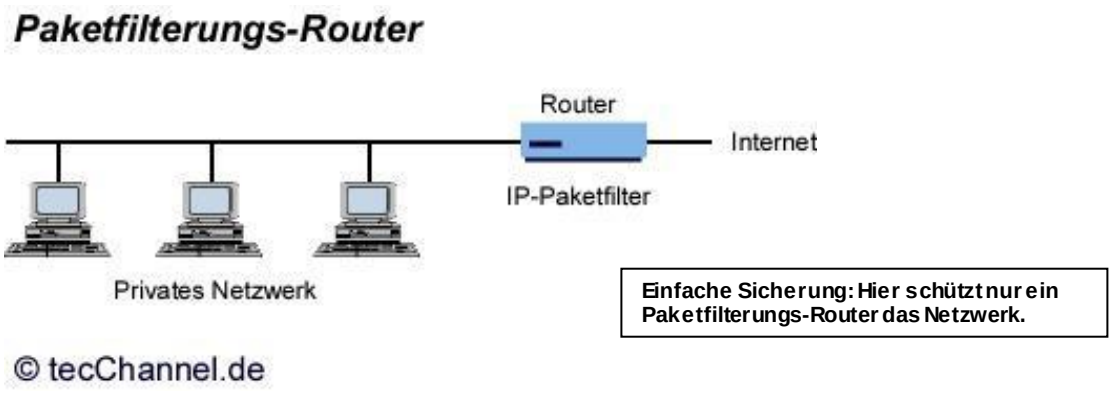
Bei einer Source Routing Attacke gibt der Angreifer die konkrete Route vor, die ein Datenpaket nehmen soll, um Sicherheitsmaßnahmen zu umgehen. Das Verfahren zum Source Routing ist zwar im TCP/IP-Standard vorgesehen, kommt jedoch kaum noch zum Einsatz. Deshalb kann die Firewall die Pakete mit diesem Flag bedenkenlos verwerfen.

Tiny Fragment Attacke

Bei dieser Angriffsform erzeugt der Hacker extrem kleine Datenpakete, von denen nur das erste den TCP-Header enthält. Das soll den Router veranlassen, nur das erste Fragment zu prüfen und die restlichen ungeprüft durchzulassen. Dies erlaubt dem Hacker, die gewünschten Befehle ins Netz zu schmuggeln. Als Abwehr kann die Firewall alle Pakete verwerfen, bei denen das Feld Fragment-Offset (http://www.tecchannel.de/internet/209/4.html) auf eins gesetzt ist

Vorteile von Paketfilterungs-Routern

Viele Firewall-Systeme setzen nur einen Paketfilterungs-Router ein. Außer der Zeit, die für die Planung der Konfiguration des Routers erforderlich ist, entstehen keine weiteren Kosten, denn die Filtersoftware ist Bestandteil der Router-Software. Um den Datenverkehr zwischen privatem und öffentlichem Netz nicht zu stark einzuschränken, sind von Haus aus nur sehr moderate und wenige Filter definiert. Die Paketfilterung ist im Allgemeinen durchlässig für Benutzer und Applikationen. Sie erfordert zudem kein spezielles Training und keine zusätzliche, auf den einzelnen Rechnern installierte Software.



Einfache Sicherung: Hier schützt nur ein Paketfilterungs-Router das Netzwerk.

Nachteile

Doch die Paketfilterung hat auch Nachteile. So ist neben detaillierten Protokollkenntnissen für eine komplexe Filterung auch eine lange Regelliste notwendig. Derartige Listen sind sehr aufwändig und daher schwer zu verwalten. Es ist zudem schwierig, die Filter auf Wirksamkeit zu testen. Auch sinkt der Router-Durchsatz, wenn zu viele Filter definiert sind.

Daneben können Hacker die Firewall durch Tunneln der Pakete überwinden, wobei ein Paket vorübergehend in einem anderen gekapselt wird. Und schließlich: Data-driven-Attacken kann der Router nicht erkennen.

Proxy-Server

Ein Proxy-Server (engl. Proxy: Stellvertreter, Bevollmächtigter), auch Application Level Gateway genannt, erlaubt dem Netzwerk-Administrator die Installation von strengeren Sicherheitsregeln als dies bei einem Paketfilterungs-Router möglich ist. Der Server dient als sicheres Gateway zwischen einem privaten und einem öffentlichen (ungesicherten) Netz. Als Gateway bezeichnet man entweder die Software, die eine Verbindung zwischen zwei Netzwerken herstellt, oder den Computer, auf dem diese Software ausgeführt wird.

Ein Proxy-Server dient nebenbei zur Zwischenspeicherung von Web-Inhalten und kann als erweiterbare Firewall verwendet werden. Das ermöglicht gleichzeitig Datensicherheit und einen schnelleren Zugriff auf Internetinhalte. Der Proxy hat dabei zwei Gesichter: Für den lokalen Client operiert er beim Abruf eines Web-Dokuments wie ein Webserver. Gegenüber dem entfernten Internet-Server tritt er wie ein Webclient auf. Proxy-Server sprechen aber nicht nur HTTP, sondern beherrschen auch Dienste wie FTP, POP3 oder IRC - allerdings abhängig vom jeweiligen Produkt. Da sie als einziger Knotenpunkt zwischen lokalem und globalem Netz geschaltet sind, schützen sie zudem die lokalen Clients. Denn nur der Proxy-Server ist Angriffen von außen ausgesetzt. Die Clients liegen "unsichtbar" hinter ihm.

Vorteile eines Proxy-Servers

Das Betriebssystem auf Client-Seite spielt prinzipiell keine Rolle. Nur spezielle Funktionen wie beispielsweise eine automatische Konfiguration der Clients oder das Trennen einer Internet-Verbindung vom Client funktionieren lediglich von Windows-Clients aus.

Daneben lässt sich für jeden Dienst wie FTP oder HTTP ein separater Proxy einrichten. Unerwünschte Dienste filtert der Proxy heraus. Zudem findet kein direkter Paketfluss zwischen internen und externen Rechnern statt.

Bastion-Host

Unter einem Bastion-Host versteht man einen besonders gesicherten Rechner, der wie eine Festung wirken soll. Er schützt die Rechner im privaten Netz vor Angriffen von außen. Wie bei einer Festung gibt es nur einen Ein- und Ausgang, der ständig bewacht ist und bei Bedarf sofort geschlossen werden kann. Die Überwachung des Aus- und Eingangs übernimmt meist ein Router als Paketfilter. Bastion-Hosts sind von ihrer Art her damit die gefährdetsten Rechner in einer Firewall. Auch wenn sie in der Regel mit allen Mitteln geschützt sind, sind sie häufigstes Ziel eines Angriffs, da ein Bastion-Host als einziges System Kontakt zur Außenwelt unterhält.

Die Rechner im privaten Netz sind aus dem Internet nicht direkt erreichbar und dadurch unsichtbar. Andersherum ist auch das Internet nur über den Bastion-Host zugänglich. Deshalb ergibt sich für diesen Rechner die logische Grundhaltung: je einfacher der Bastion-Host aufgebaut ist, desto leichter ist er zu schützen. Denn jeder auf dem
Bastion-Host angebotene Dienst kann Software- oder Konfigurationsfehler enthalten. Bei minimalen Zugriffsrechten sollte der Bastion-Host gerade so viele Dienste anbieten, wie er für die Rolle als Firewall unbedingt braucht.

Bastion-Hosts werden in unterschiedlichen Architekturen installiert, wie zum Beispiel als Dual-Homed-Host, in Kombination mit einem Überwachungs-Router.

Vorteile eines Bastion-Hosts

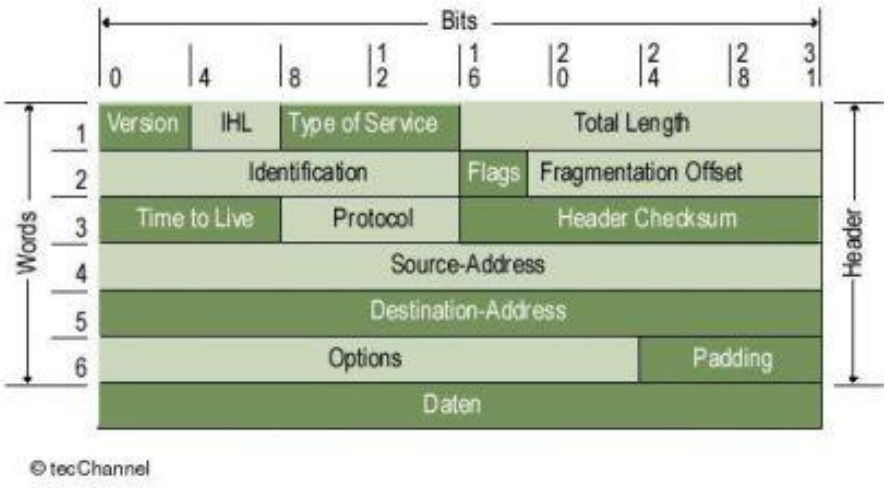
Ein Bastion-Host lässt sich so einrichten, dass Dienste nur über eine Authentifizierung abrufbar sind. Zudem kann der Administrator spezielle Bestandteile dieser Dienste komplett abschalten, etwa den PUT-Befehl für FTP-Server. Die voneinander unabhängigen Proxy-Dienste laufen unter einer unprivilegierten Benutzerkennung in separaten, gesicherten Verzeichnissen, so dass ein Angriff über diese Dienste nur schwer möglich ist. Alle anderen Dienste wie SMTP oder HTTP sind auf diesem Rechner komplett abgeschaltet und stellen somit keine Sicherheitslücke dar. Im Bedarfsfall kann der Administrator auch den kompletten Datenverkehr überwachen, um Angreifer zu erkennen.

Nachteile von Bastion-Hosts

Bei bestimmten Diensten, wie etwa Telnet oder FTP müssen sich die Benutzer zweimal einloggen: Einmal auf dem Proxy des Bastion-Hosts und danach auf dem eigentlichen Server. Zudem muss die Client-Software speziell an den Proxy angepasst werden.

Verbindungs-Gateways

Verbindungs-Gateways (Circuit Level Gateways) sind Proxy-Server mit Zusatzfunktionen. Sie beschränken sich, ähnlich wie Application Level Gateways, nicht nur auf die Kontrolle der IP- und Transportschicht-Header. Stattdessen bauen Sie die Datagramme der Transportschicht aus den IP-Paketen, die unter Umständen fragmentiert sind, zusammen. Wie bei Application Level Gateways gibt es auch hier keine direkten Verbindungen zwischen der Innen- und Außenwelt. Vielmehr findet automatisch eine Adressübersetzung statt. So lässt sich eine Benutzerauthentifizierung erzwingen. Auf der anderen Seite verstehen die Circuit Level Gateways das Anwendungsprotokoll nicht und können deshalb keine Inhaltskontrolle durchführen. Beide Gateway-Varianten verfügen zwar über gemeinsame Merkmale; aber die Fähigkeit, das Anwendungsprotokoll zu verstehen, besitzt nur das Application Level Gateway.



IP-Pakete: Ein Verbindungs-Gateway muss aus den Daten im IP-Header ersehen, welche Pakete zu einem Datenstrom gehören.

Verbindungs-Gateways vertrauen den internen Benutzern. In der Praxis werden Proxy-Server daher für die Verbindungen nach innen benutzt, während man Verbindungs-Gateways für den Datenverkehr von innen nach außen einsetzt.

Hybrid-Firewalls

Hybrid-Firewalls bestehen aus Paketfilter und Application Level Gateway, wobei das Gateway die Filterregeln des Paketfilters dynamisch ändern kann. Als "Stateful Inspection" bezeichnet man einen Paketfilter "mit Gedächtnis". Dieser speichert allerdings nur die Informationen aus den Paket-Headern.

Der Vorteil einer Hybrid-Firewall gegenüber einem alleinigen Application Level Gateway liegt in der höheren Performance. Allerdings bedingt dies auch einen gewissen Sicherheitsverlust. Der Grund liegt darin, dass bei den meisten Protokollen der Proxy keinerlei Kontrolle mehr über die Verbindung besitzt, nachdem er den Paketfilter geöffnet hat. Deshalb muss ein Angreifer den Proxy nur eine Zeit lang in Sicherheit wiegen, um anschließend durch den (für ihn geöffneten) Paketfilter freies Spiel zu haben.

Grundlage des Paketfilters mit Stateful Inspection ist die sogenannte "Stateful Inspection Engine". Diese analysiert die Datenpakete während der Übertragung auf Netzwerkebene. Im gleichen Arbeitsgang erstellt die Engine dynamische Zustandstabellen, welche die Betrachtung mehrerer Pakete erlauben. Die Korrelationen zwischen zusammengehörenden ein- und ausgehenden Paketen ermöglichen ausgefeilte Analysen.

Hochsicherheits-Firewalls

Hochsicherheits-Firewalls können aus einem Firewall-Subnetz mit zwei Paketfilterungs-Routern und einem Proxy (Bastion Host) bestehen. Ein solches Firewall-System sichert auf der Netzwerk- und Applikationsebene durch die Definition einer "entmilitarisierten Zone" (Englisch: demilitarized zone, kurz DMZ). Dabei befinden sich Bastion-Host, Informationsserver, Modem-Pools und andere Server im DMZ-Netz. D as DMZ-Netz agiert so als kleines isoliertes Netzwerk zwischen dem privaten Netz und dem Internet.

Dabei ist das DMZ so konfiguriert, dass Zugriffe aus dem privaten Netz und dem Internet nur auf Server im DMZ erfolgen können. Direkter Verkehr durch das DMZ-Netz hindurch ist nicht möglich - egal in welcher Richtung.

Bei den hereinkommenden Datenpaketen schützt der äußere Router gegen Standard-Angriffe wie IP-Address-Spoofing oder Routing-Attacken und überwacht gleichzeitig den Zugriff auf das DMZ-Netz. Dadurch können externe Rechner nur auf den Bastion-Host und eventuell den Information-Server zugreifen

Durch den internen Router wird eine zweite Verteidigungslinie aufgebaut. Dieses Gerät überwacht den Zugriff vom DMZ zum privaten Netz indem es nur Pakete akzeptiert, die vom Bastion Host kommen. Damit kommen nur Benutzer in das interne Netz, die sich vorher am Bastion-Host authentifiziert haben.

Fazit

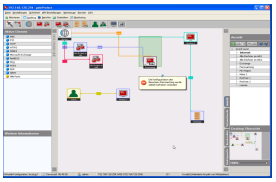
Wer sein Firmennetzwerk an das Internet anschließt geht ein nicht unerhebliches Risiko ein. Da aber kaum noch eine Firma ohne Internet-Anschluss auskommt, gehört eine Firewall zum Pflichtprogramm. Die Paranoia lässt sich beliebig weit treiben, man muss nur genügend Zeit und Geld investieren.

Jede Firewall - egal welcher Art - ist allerdings nur so gut wie ihre Konfiguration und die Absicherung des Hosts, auf dem die Firewall läuft. Wer einfach das Softwarepaket aufspielt oder einen fertigen Firewall-Rechner in sein Netz hängt und sich damit sicher wähnt, handelt fahrlässig. Deshalb ist es oftmals besser, sich an ein auf Netzwerkabsicherung spezialisiertes Unternehmen zu wenden.

Ratgeber Sicherheit

Das können Next Generation Firewalls

von Johann Baumeister (TecChannel)



Aufbau und Arbeitsweise von Firewalls sind seit mehr als einer Dekade nahezu unverändert. Jetzt krempeln Next Generation Firewalls die herkömmlichen Konzepte um. Wir erläutern, wie die neuen Firewalls als zentraler Sicherheitsbaustein in einem Unternehmen arbeiten.

Firewalls überwachen den Datenverkehr und dienen damit dem Schutze des Netzwerkes vor An- griffen von außen wie von innen. Doch das Konzept einer Firewall als Brücke zwischen Intranet und Internet reicht als Schutzvorkehrung mittlerweile meist nicht mehr aus. Die Hersteller reagieren darauf: Sie erweitern die Möglichkeiten ihrer Firewalls schrittweise und bauen sie zu u mfangreichen Sicherheits-Suites aus.

In diesem Beitrag wollen wir daher aufzeigen, wie weit die Hersteller ihre Firewalls bereits entwickelt haben. Dabei gehen wir auf den Stand der Technik der Firewalls ein und zeigen auf, was es mit dem Terminus **Next Generation Firewall** auf sich hat.

Firewalls als Torwächter

Durch Firewalls wird bestimmt, wer mit wem über welchen Kanal oder welches Protokoll kommunizieren darf oder nicht. Die ersten Firewalls waren im Prinzip reine Paketfilter, die auf Ebene 4 des ISO/OSI-Protokolls arbeiteten. Einen Angreifer allerdings, der sich hinter einer Applikation geschickt tarnt, kann so ein Filter nicht abhalten. Daher ging man schon bald dazu über, auch die oberen Schichten der Kommunikation zu untersuchen. Layer 7 Firewalls waren geboren.

Sie werden auch als Application Layer Firewall bezeichnet. Die Application Layer ist die Ebene 7 des ISO/OSI-Protokolls. Die meisten Firewalls arbeiten mittlerweile sowohl auf Layer 4 (Trans- portschicht) als auch auf Layer 7 (Anwendungsschicht). Diese Sicherheitssysteme sind somit in der Lage, auch die Inhalte des Datenverkehrs zu filtern. Notwendig wird dies, da immer mehr schädlicher Code über den Datenanteil der Standardprotokolle geschleust wird. Angriffe dieser Art sind durch reine Paketfilter somit nicht zu verhindern.

Trotz dieser Ausweiterung der Firewall-Funktionen vermögen die Firewalls den neuen Angriffs-techniken nur wenig entgegenzusetzen, Befindet sich der Angreifer erst einmal in Netz, so nützt die Firewall wenig. Eingeschleust wird der Schadcode oftmals durch mobile Geräte. Diese infizieren sich "draußen" und bringen beim Aktivieren im Unternehmensnetz den Gefahrencode nach "drinnen". So werden Viren, Trojaner und Backdoors quasi an der Firewall vorbeigetragen. Den Bedrohungen von "innen" aber haben die traditionellen Firewalls nur wenig entgegenzusetzen.

Bestimmung der Firewall-Position

Eine entscheidende Rolle beim Einsatz einer Firewall-Lösung ist die Position in der Netzwerktopologie. Geht man in chronologischer Reihenfolge an die Konfiguration der Firewalls heran, so wird der erste Schritt immer die Bestimmung des Netzwerkdesigns sein. Bei kleineren Unternehmen mag dieses allein aus dem internen Netzwerk mit allen Server und Clients sowie de m Internet bestehen.

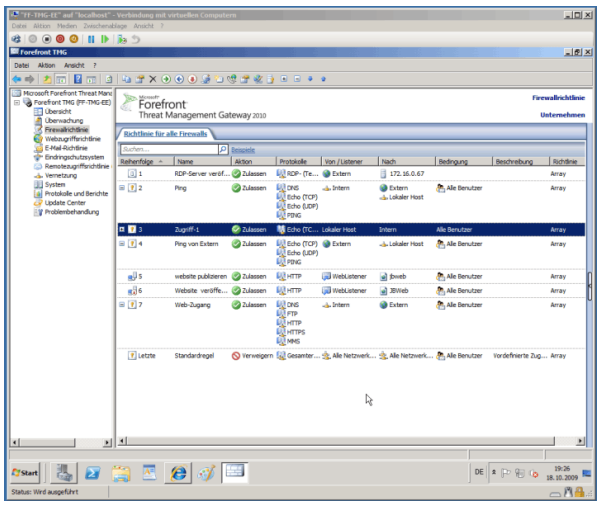
Mit der Unternehmensgröße wächst jedoch auch die Komplexität der IT-Infrastruktur. Die Segmentierung[5] (Demilitarisierte Zone) und verschiedenen weiteren Zonen wird dabei unumgänglich. Um die verschiedenartigen Anforderungen abzudecken, platziert man die Firewall daher an unterschiedlichen Stellen im Netzwerk. Unterschieden wird dabei nach Egde Firewall, Front Firewall, Back Firewall und dem Schutz einzelner Netzwerkadapter.

Netzwerkregeln bestimmen den sicheren Kommunikationsfluss

Ist das grundlegende Layout des Netzwerkes festgelegt, so müssen die Netzwerkregeln für den Datenverkehr bestimmt werden. Hierzu bieten die Produkte zur Konfigurationsunterstützung oftmals Assistenten an.

Die Netzwerkregeln sind allerdings nur als Basisdefinition zu verstehen. Sie bestimmen Transfer- Quelle und -Senke zum Beispiel von intern nach extern oder die Adressumsetzung mittels NAT. Die Regeln können beliebig definiert und auch geschachtelt werden. Kommen mehrere Regeln zur Anwendung, so muss auf die Reihenfolge ihrer Abarbeitung geachtet werden.

In der Terminologie der Firewall-Regeln handelt es sich bei einer Regel immer um eine Kommunikation von einer Quelle zu einem Ziel. Als Kommunikationstechnik kommt ein bestimmtes Protokoll zum Einsatz. Neben diesen grundlegenden Aspekten weisen die Firewall-Regeln natürlich noch weitere Parameter, wie die Zeit oder Angaben zur Protokollierung auf. Im Kern beruhen sie aber auf dem Quelle-Ziel-Prinzip.



Microsoft Forefront TMG: Regelwerk und Filter bilden das Grundgerüst der Firewalls. Dieses gilt auch für die nachkommende Generation der Sicherheitssysteme.

Grundlegend geht es also immer darum, welcher Benutzer oder Dienst über welches Protokoll mit wem kommunizieren darf. Durch Richtlinien wird die Überwachung weiter spezifiziert. Dazu gehört die Auswahl der zulässigen Protokolle, der Kommunikations-Ports oder der Eingrenzung des Transfers auf bestimmte Systemdienste und Ähnliches. Zu den überwachten Netzwerkprotokollen zählen meist alle gängigen Protokolle wie etwa HTTP, SMTP, SSL, RPC oder FTP . Durch die Gruppierung der Protokolle, etwa in Infrastruktur, Authentifizierung, E-Mail-Kommunikation , Instant Messaging, Filetransfer oder Streaming, wollen die Hersteller die Definition der Regeln zusätzlich vereinfachen.

Erweiterte Funktionen zur Angriffserkennung

Eingeschlossen in traditionelle Firewall-Konzepte sind ferner Funktionen zur Erkennung und Vermeidung gängiger Angriffsszenarien wie DNS- oder POP-Angriffen, Ping-of-Death, Portscan oder IP-Half-Scan. Durch DNS-Anwendungsfilter wird in der Regel der DNS-Datenverkehr zum internen Netzwerk überwacht und analysiert. Ferner können natürlich beliebig weitere eigene Filter definiert werden.

Bei Angriffen werden Alarme oder weitergehende Aktionen angestoßen. Ergänzt werden die Sicherheitsmaßnahmen um Vorkehrungen zur Vermeidung der gängigen und bekannten Angriffe. So kann etwa die Begrenzung der gleichzeitigen Verbindungen pro Sekunde oder Client verhindern, dass diese zu Kommunikations-Hosts missbraucht werden. Ist die maximal zulässige Anzahl von Verbindungen erreicht, werden alle neuen Client-Anforderungen von der Firewall abgelehnt.

Angriffe, die sich beispielsweise durch Buffer Overflows, Command Injection oder SQL-Injection ergeben, werden meist durch den HTTP-Proxy/Filter abgewehrt. Durch beliebige weitere HTTP-Filter wird der gesamte ein- und ausgehende HTTP-Verkehr überwacht. Ein anderes beliebtes Angriffsverfahren sind Buffer-Overruns - um sie abzuwehren, setzen die Hersteller meist auf die Begrenzung der Länge der URL-Requests.

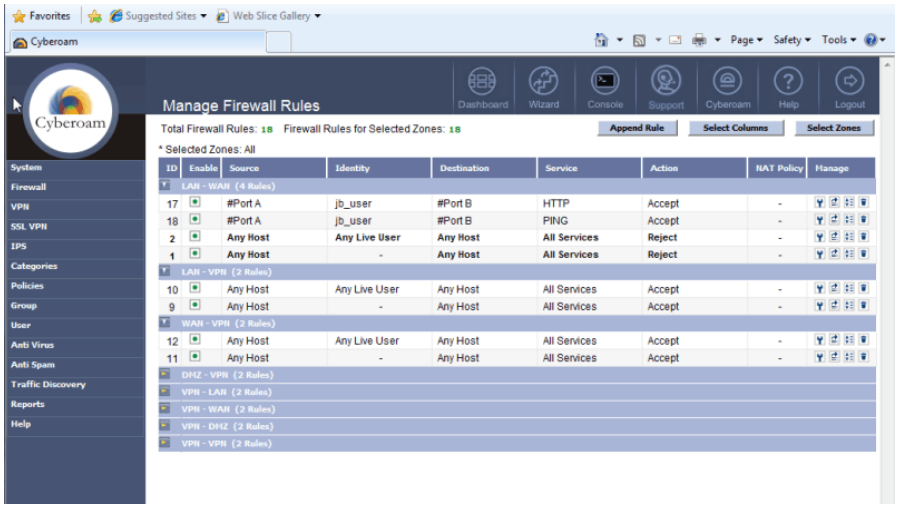
Protokollierung der Aktivitäten schafft Sicherheit

Sicherheitssysteme wir Firewalls oder Intrusion Detection Systems (IDS) müssen ihre Arbeit rund um die Uhr und meist ohne permanente menschliche Kontrolle ausführen. Um dennoch Angriffe oder Unregelmäßigkeiten zu überwachen, erfolgt eine Protokollierung der Aktivitäten. Durch die nachgeschaltete oder begleitende Analyse des Netzverkehrs können so mögliche Angriffen oder Schwachstellen erkannt und hoffentlich verhindert werden.

Die Protokollierung der Firewall-Aktivitäten liefert weitere Informationen zum Datenverkehr und zu dessen Verursachern. Dazu gehören meist die IP- und Port-Adressen, die Namen von Rechnern oder Netzen, die Zugriffsregeln, die Anzahl der übertragenen Bytes und Ähnliches.

Generationswechsel mit Next Generation Firewalls

Um die künftigen Anforderungen besser abzudecken, erweitern die Hersteller den Funktionsumfang ihrer Firewalls schrittweise. Dazu zählt beispielsweise eine genauere Untersuchung der Applikationsdienste. Hierbei wird die Scan-Funktion in den Firewalls weiter verfeinert. Die Werkzeuge erhalten dabei einen tieferen Einblick in das Kommunikationsverhalten der Applikationen.



Erhöhte Sicherheit: Cyberoam integriert die Identität der Benutzer in die Firewall-Regeln.

Fehlverhalten beziehungsweise Angriffe, die sich als erlaubte Applikationskommunikation tarnen, werden dabei leichter erkannt. Ferner erfolgt oftmals die Verknüpfung der Benutzer mit den Rechten. Hierbei werden die gebotenen Sicherheitsfunktionen direkt mit dem Benutzer oder einer Benutzergruppe verknüpft. So filtern beispielsweise neuere Firewalls den Datenstrom nach unterschiedlichen Kriterien wie etwa den involvierten Netzwerksegmenten.

Application Firewalls wiederum beziehen die Applikationen mit ein. Der Benutzer und seine Eigenschaften bleiben bis dato aber meist außen vor und wurden nicht in die Untersuchung einbezogen. Durch den Bezug zum Benutzer wird in Zukunft die Brücke von der Firewall-Regel zu einem Benutzer oder einer Gruppe geschlagen. Beim Verbindungsaufbau erfolgt dann eine Abfrage des Benutzers durch die Firewall. Hierzu greift man meist auf das Active Directory, ein LDAP-Verzeichnisdienst oder etwa einen RADIUS-Server zurück.

Die Weiterentwicklung der klassischen Firewall

Der Funktionsumfang herkömmlicher Firewalls hat sich von den klassischen Paketfiltern immer weiter in Richtung universelle Schutzsysteme für das Unternehmensnetz verschoben. Diese bestehen meist aus den traditionellen Paketfiltern und deren Erweiterung zum Erkennen von Unregelmäßigkeit durch Stateful Inspection, den Application Gateways (Proxy) und schließlich IDS/IPS (Intrusion Detection System / Intrusion Prevention System) oder Anomalien Detection Systeme.

Oftmals packen die Hersteller auch die Funktionen Anti-Spam, Anti-Virus, Anti-Spyware und mehrere Content-Filter zu ihren Produkten. Mitunter finden sich gar Möglichkeiten zur Verwaltung der Netzwerkanschlüsse oder der Bandbreiten in den Sicherheitslösungen. Hierbei gilt aber: Sofern sie mit Mustererkennung (Patterns) arbeiten, müssen vorher die Angriffsmuster installiert sein. Diese Nachteile vermeiden heuristische Ansätze oder die Protokollanalyse, deren Trefferrate dafür jedoch ungenauer vorhersagbar ist.

Generell ist anzumerken, dass die traditionellen Sicherheitsvorkehrungen wie die Paketfilter sicher nicht obsolet sind, aber um weitere Aufgaben wie Content Filtering, URL-Blocking, Anti-Spam oder Anti-Virus ergänzt werden. Durch diese Filterfunktionen der Firewalls lassen sich dann auch Data-Leakage-Prevention-Funktionen (DLP) abbilden. Systeme dieser Art arbeiten meist mit externen und zentral gepflegten White oder Black Lists. Daher kooperieren diese Systemanbieter für die Belange des Spam- oder Virenschutzes mit spezialisierten Unternehmen.

Anschlüsse überwachen

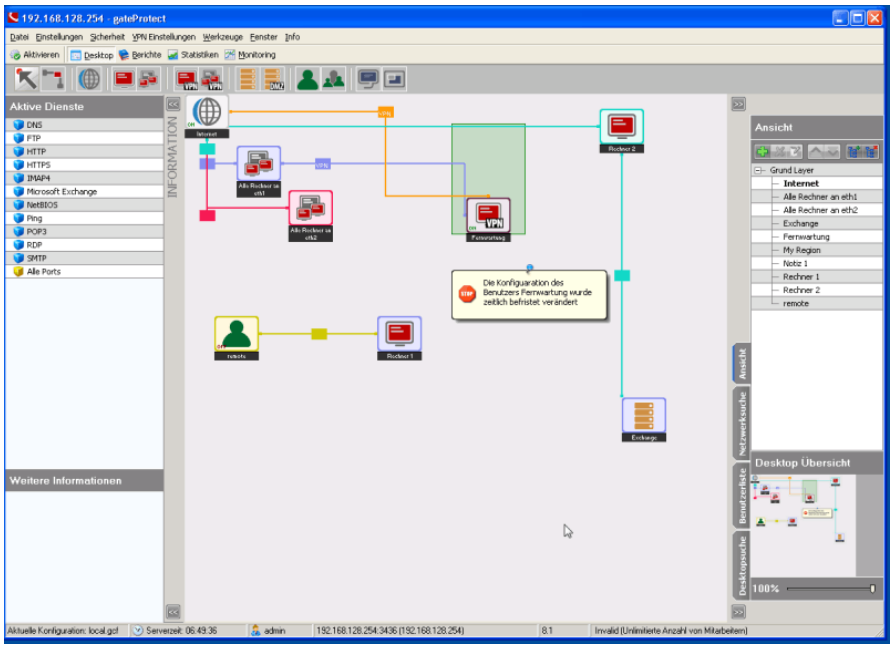
Ein weiterer Block ist die Überwachung der Netzwerkaktivitäten. Hierzu werden die Netzwerkanschlüsse laufend überwacht. Diese Monitoring-Funktionen informieren über die bestehenden Verbindungen, die Kommunikation, die verwendeten Protokolle und weitere Details zur Kommunikation. Dazu zählen beispielweise die einzelnen IP-Adressen der Quelle oder des Ziels, die global gefassten Interfaces oder die verwendeten Kommunikationsprotokolle sowie die involvierten Netzwerk-Ports.

Ein Dschungel an Regeln für mehr Sicherheit

Der Kern der Next Generation Firewalls sind dessen Regeln. In größeren Szenarien können diese Regelsätze sehr umfangreich werden. Die Zahl der dabei involvierten "Objekte" erreicht leicht die 1000er-Grenze. Ein Objekt solch einer Firewall-Regel ist beispielsweise ein Benutzer, eine Organisationseinheit, ein Rechner mit seiner IP-Adresse, eine Applikation, ein Server, ein Dienst, ein Prozess, eine Netzwerkfreigabe oder ein Netzwerksegment. Da sich diese Objekte, wie etwa die Unternehmensstrukturen mit ihren Mitarbeitern, ständig ändern, müssen auch die Regeln laufend angepasst werden.

Hinzu kommt, dass die Verwaltung einer dezentralen Firewall-Infrastruktur oft auch nur verteilt erfolgen kann. Die Kommunikation zwischen zwei Objekten muss mitunter jedoch mehrere Firewalls nacheinander passieren. Hierbei fällt es schwer, einen genauen Überblick darüber zu haben, was nun letztendlich erlaubt oder verboten ist. Um dabei noch die Übersicht zu wahren, werden häufig grafische Hilfsmittel eingesetzt.

Hilfreich sind auch Werkzeuge, die eine Emulation der Auswirkungen der Firewall-Regeln ermöglichen. So kann der Administrator noch vor der Durchführung von Änderungen sehen, was die geplante Änderung bewirkt. Sind diese Auswirkungen nicht wie gewünscht, so wird die Regel eben kurzerhand verworfen oder wieder geändert.



Gateprotect: Die Firewall unterstützt die Konfiguration seiner Sicherheitssysteme durch grafische Editoren.

Durch Überwachungs-Tools sollen das Erstellen und Ändern von Regeln effizient werden und vor allem auch nachvollziehbar. Dies beginnt bei der Anforderung einer Änderung an einer Firewall- Regel, schließt die Risikoanalyse ein und kümmert sich schließlich auch um die letztendliche Implementierung der Regel. Parallel dazu werden diese Änderungen in einem Security Audit festgehalten.

Diese Werkzeuge unterlegen die Erstellung von Firewall-Regeln einem formalisierten Prozess. Jede an einer Firewall erstellte oder geänderte Regel muss dabei in einem mehrstufigen Prozess mehrere Personen oder Gruppen durchlaufen. Die Grundlage dazu stellt meist ein Rollenmodell dar. An diese Rollen werden dann die Aufgaben gebunden. Die Rollen sind frei zu definieren, ebenso der Workflow. So kann beispielsweise eine Person eine Anforderung (einen Request) für eine Regel definieren. Ein Beispiel hierfür ist die Anforderung, dass ein Benutzer über einen Internetzugang auf seine Mails im Unternehmen zugreifen kann. Diese Person, die diese Anforderung definiert, muss aber nicht unbedingt mit den Details der involvierten Firewalls vertraut sein.

Umsetzung einer Security-Anforderung in eine Regel

Bei der Definition einer Sicherheitsanforderung ist es nicht notwendig, dass etwa der Administrator weiß, welche Firewalls und Serversysteme davon im Detail betroffen sind. Er formuliert nur die allgemeine Anforderung. In einem nachgeschalteten Schritt wird diese Anforderung an eine weitere Person oder Gruppe übergeben. Diese kümmert sich dann um die eigentliche Umsetzung. Sind die Regeln erstellt, so wird oder kann diese zur Prüfung an eine weitere Administrationsstelle geschleust werden. Diese Instanz wiederum prüft die Auswirkungen der neuen Regel auf den gesamten Regelsatz hin. Dieser "Prüfer" kann sich dazu auch weitere Informationen einholen. Reichen diese Angaben nicht aus, so kann er die Regel zurückweisen. Wenn alles passt und keine Komplikationen zu erwarten sind, wird er die Regel zur Implementierung freigeben. Damit ist diese Sicherheitsanforderung im ganzen Unternehmen - auch global - gültig.

Fragen zu Firewalls

Finden Sie die Antworten zu folgenden Fragen und formulieren Sie die Antworten schriftlich!

1. Welchen Schutz bietet eine richtig konfigurierte Firewall?
2. Die beste Firewall bietet keinen Schutz gegen .....
   Nennen Sie zwei Beispiele!
3. Firewalls gibt es als Hard- und Softwarelösung.
   Nennen Sie jeweils die Vor- und Nachteile!
4. Man unterscheidet verschiedene Firewall-Konzepte.
   Skizzieren Sie zwei verschiedene Varianten!
5. Was ist ein Bastion Host?
6. Was versteht man unter einer demilitarisierten Zone (DMZ)?
7. Welchen Namen gibt es noch für eine DMZ?
8. Was versteht man unter einer Paketfilter-Firewall?
9. Welche Parameter sind in Paketfilter-Regeln enthalten?
10. Worin liegt der Vorteil von SPI-Firewalls?
11. Nennen Sie die wesentlichen Eigenschaften einer Application Level Gateway!
12. Was versteht man unter einem Proxy-Server?
13. Erklären Sie den Begriff „Hybrid-Firewall“!
14. Welchen Vorteil bietet eine Firewall mit NAT-Funktion?
15. Wo werden in der Regel Personal Firewalls installiert?
16. Worin liegt die Schwäche von Personal Firewalls?
17. Worin unterscheiden sich Next-Generation-Firewalls von klassischen Firewalls?