

Zusammenfassung

Eine so genannte Firewall (dt. "Brandmauer") ist eine physische (Hardware) oder logische (Software) Vorrichtung, die als Schutzsystem für Computer dient. Sie kann ebenso als Schnittstelle zwischen einem oder mehreren Unternehmensnetzwerken zur Kontrolle und ggf. Blockierung des Datenverkehrs eingesetzt werden, indem die im Datenfluss enthaltenen Informationen analysiert werden (Abschirmung des Netzwerks).

Eine Firewall ermöglicht daher Angriffe oder verdächtige Verbindungen, über die möglicherweise Viren, Würmer oder Trojaner verbreitet werden, abzublocken und nachzuverfolgen. Ebenfalls dient eine Firewall in vielen Fällen auch dazu, die unkontrollierte Weitergabe von Daten nach aussen zu unterbinden.

Inhalt

- 1 Was ist eine Firewall? →
- 2 Wie funktioniert eine Firewall? →
- 3 Gegen welche Bedrohungen schützt die Firewall? →
- 4 Beispiele →
- 5 Ratschläge →



1 Was ist eine Firewall?

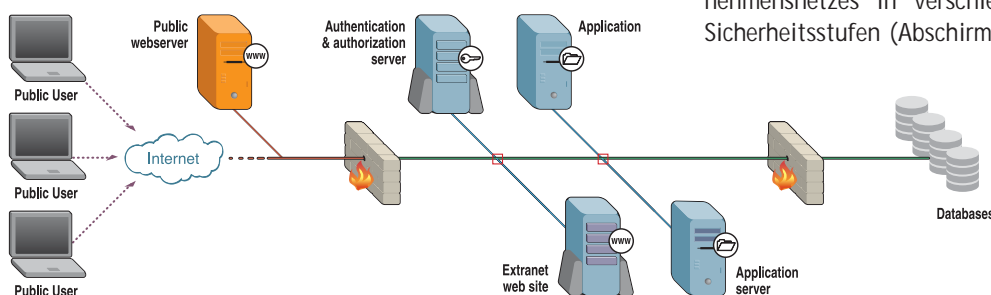
Eine so genannte Firewall ist eine physische (Hardware) oder logische (Software) Vorrichtung, die als Schutzsystem für Heimcomputer dient. Sie kann ebenso als Schnittstelle zwischen einem oder mehreren Unternehmensnetzwerken zur Kontrolle und ggf. Blockierung des Datenverkehrs eingesetzt werden. Hierbei werden die im Datenfluss enthaltenen Informationen analysiert (Abschirmung des Netzwerks).

Sie ermöglicht Angriffe oder verdächtige Verbindungen, über die möglicherweise Viren, Würmer oder Trojaner verbreitet werden, abzublocken und nachzuverfolgen, als auch die unkontrollierte Weitergabe von Daten nach aussen zu unterbinden.

Es gibt im Wesentlichen zwei Kategorien von Firewalls:

- ➔ Persönliche Firewalls schützen ausschliesslich Arbeitsstationen und Computer. Sie werden direkt auf dem Rechner des Anwenders installiert.
- ➔ Firewalls zum Schutz von Unternehmen werden auf speziellen Geräten installiert. Hier wird eine Firewall oft zwischen dem Internet und einem Unternehmensnetzwerk eingerichtet, um letzteres gegen verschiedene Bedrohungen aus dem Internet zu schützen.

Die Firewall wird auch zur Einrichtung so genannter demilitarisierter Zonen (DMZ) für das Hosting öffentlicher Server verwendet. In manchen Fällen dient sie sogar zur Unterteilung des Unternehmensnetzes in verschiedene Teile mit unterschiedlichen Sicherheitsstufen (Abschirmung des Netzwerks).



2

Wie funktioniert eine Firewall?

Funktionsweise

Eine Firewall funktioniert auf Grundlage von Regeln, die von einem Anwender korrekt anhand folgender allgemeiner Grundsätze definiert werden:

⚠ Alles was nicht ausdrücklich erlaubt ist, ist verboten.

Das heisst, dass in den Regeln, die einen Teil der Konfiguration der Firewall darstellen, eine Handlung oder ein Datenfluss ausdrücklich zugelassen sein muss, damit eine Verbindung aufgebaut werden kann.

Die untenstehende Tabelle zeigt ein Beispiel für die Konfiguration der Regeln einer Firewall:

Regle	Handlung	Absender-IP	Empfänger-IP	Protokol	Absender-Port	Empfänger-Port
1	Accept	192.168.10.20	194.154.192.3	tcp	any	25
2	Accept	any	192.168.10.3	tcp	any	80
3	Accept	192.168.10.0/24	any	tcp	any	80
4	Deny	any	any	any	any	any

Filtern des Inhalts

Einige Firewalls ermöglichen neben dem Filtern von Paketen auch das Filtern und die Analyse der in den Paketen enthaltenen Daten. Dies ermöglicht es in manchen Fällen:

- ➔ den Besuch von verbotenen Websites zu verhindern,
- ➔ das Herunterladen von böswilligen Dateien oder Softwareprogrammen aus dem Internet zu verhindern,
- ➔ das Versenden und Empfangen von potenziell gefährlichen E-Mails zu verhindern.

Neben den oben genannten Funktionen prüfen manche Firewalls sogar, ob die Anwendungsinhalte des Datenverkehrs, der über die Firewall geht (verwendetes Anwendungsprotokoll, Befehle, Kodierung usw.) dem voraussichtlichen Anwendungsprotokoll entsprechen.

Filtern der Daten-Pakete

Das Internet und seine Netze funktionieren durch das Senden und Empfangen von Datenblöcken, so genannten "Paketen". Eine Firewall analysiert jedes dieser Pakete auf Grundlage einer gewissen Anzahl von in den Regeln festgelegten Eigenschaften.

Eine Firewall, die nach dem Filter-Prinzip arbeitet, analysiert die Header der zwischen zwei Rechnern ausgetauschten Pakete nach folgenden Gesichtspunkten:

- ➔ IP-Adresse des sendenden Rechners
- ➔ IP-Adresse des empfangenden Rechners
- ➔ Pakettyp: TCP, UDP, ICMP oder IP
- ➔ dem angeforderten Dienst oder Port

Dadurch kann verhindert werden, dass ein Cracker mit Hilfe eines anderen Anwendungsprotokolls über Port 80 (http) auf einen Trojaner zugreift.

3

Gegen welche Bedrohungen schützt die Firewall?

Die Anwendung einer richtig konfigurierten Firewall schützt vor folgenden Bedrohungen:

- ➔ Eindringen ins Netzwerk
- ➔ Trojaner
- ➔ Würmer

