Firewall

> Bei einer Firewall handelt es sich um ein System, das in der Lage ist, Datenverkehr zu analysieren. Sie schützt IT-Systeme vor Angriffen oder unbefugten Zugriffen. Die Firewall kann als dedizierte Hardware oder als Softwarekomponente ausgeführt sein.

Jede Firewall besteht aus einer Softwarekomponente, die Netzwerkpakete lesen und auswerten kann. Innerhalb dieser Software lassen sich die Regeln, welche Datenpakete durchgelassen werden und welche zu blockieren sind, definieren.
Häufig sind Firewalls an Netzwerkgrenzen zwischen einem internen und einem externen Netzwerk platziert. An dieser zentralen Stelle kontrollieren Sie den ein- und ausgehenden Datenverkehr.

Wichtigsten Funktionskomponenten

Um die Schutzfunktion zu erfüllen, besitzen klassische Firewalls verschiedene Funktionskomponenten. Die Anzahl und der Featureumfang der einzelnen Komponenten kann sich je nach Leistungsfähigkeit von Firewall- zu Firewalllösung unterscheiden. Wesentliche in Firewalls implementierte Funktionen sind häufig diese:

Paketfilter	Kann IP-Pakete anhand von Merkmalen wie IP-Absenderadressen, IP-Zieladressen und Ports filtern.
Network Address Translation	Setzt dynamisch eine öffentliche IP-Adresse auf mehrere private IP-Adressen um. Jede ausgehende Verbindung wird mit IP-Adresse und Portnummer festgehalten. Anhand der Portnummer kann NAT eingehende Datenpakete einer lokalen Station zuordnen.
URL-Filter	Hiermit wird eingeschränkt, auf welche Webinhalte Benutzer zugreifen können. Dazu wird das Laden bestimmter URLs blockiert.
Content-Filter	Bezeichnet die Nutzung eines Programms zum Screenen und/oder Unterbinden von Zugriff auf als unzulässig betrachtete Webinhalten oder E-Mails.
Proxyserver	Ist ein Vermittler in einem Netzwerk, der Anfragen entgegennimmt und sie stellvertretend weiterleitet. Mithilfe des Proxyservers lässt sich die Kommunikation zwischen einem lokalen Client und einem Webserver absichern, verschleiern oder beschleunigen.
Virtual Private Networks (VPN)	Eine VPN-Verbindung bietet die Möglichkeit, von außen auf ein bestehendes Netzwerk zuzugreifen.

Stateful Packet Inspection	Ist eine dynamische Paketfiltertechnik für Firewalls, die im Gegensatz zu statischen Filtertechniken den Zustand einer Datenverbindung in die Überprüfung der Pakete einbezieht und entscheidet, ob ein Datenpaket zugelassen oder blockiert wird.
Stateless Packet Filtering	Stateless Firewalls sind für den Schutz von Netzwerken auf der Grundlage statischer Informationen wie Quelle und Ziel konzipiert. Während Stateful Firewalls Pakete auf der Grundlage des gesamten Kontexts einer bestimmten Netzwerkverbindung filtern, filtern Stateless Firewalls Pakete auf der Grundlage der einzelnen Pakete selbst.
Deep Packet Inspection	In einem Netzwerk übertragene Datenpakete lassen sich bis auf Anwendungsebene des ISO/OSI-Schichtenmodells inspizieren und filtern. Im Gegensatz zur Stateful Packet Inspection (SPI) werden nicht nur die Daten-Header, sondern auch die Nutzlast eines Datenpakets analysiert.
Routing	Routing sorgt dafür, dass Datenpakete über Netzgrenzen hinweg einen Weg zu anderen Hosts finden. Es kann die Daten über jede Art von physikalischer Verbindung oder Übertragungssystem vermitteln.

Revision #6
Created 2022-08-02 14:43:13 UTC by Joshua Lieder
Updated 2022-08-05 08:10:22 UTC by Joshua Lieder