Name: Lukas Müller Thema: Proxy-Firewall Abgabe: 07.01.2020

Proxy-Firewall

Was ist eine Firewall und wie funktioniert sie? (kurze vorab Info)

Eine Firewall schützt einen Computer oder ein Netzwerk vor unerwünschten Zugriffen über Datenleitungen von außen, sodass sie nicht verändert, kopiert oder gelöscht werden können.
Alle Daten zwischen dem User und dem Internet müssen durch die Firewall, dabei hat die Firewall bestimmte Regeln, nach denen sie entscheidet ob der Zugriff genehmigt wird oder nicht.

Was ist konkret eine Proxy Firewall, wie funktioniert sie und wie sicher ist sie?

Eine Proxy Firewall filtert und überwacht die Kommunikation auf der Anwendungsebene, sie schützt dabei vor ungewolltem oder gefährlichen Datenverkehr. Die Proxy Firewall ist ein Security System, welches die Kommunikation auf der Anwendungsebene überwachen und filtern kann. Dabei unterscheidet sie sich von den rein paketorientiert arbeitenden Firewalls, den sie wertet nicht nur Adress- und Protokolldaten von IP-Paketen aus, sondern analysiert und wertet den Datenverkehr direkt in der Anwendungsschicht. Für eine Bestimmung, welcher Datenverkehr erlaubt ist und welcher nicht, werden zustandsbezogene Prüfungen (Stateful Inspection) und Deep Packet Inspection benutzt.
Das heißt, dass sie Datenpakete analysiert werden und der Verbindungstatus in die Entscheidung mit einbezogen wird (Stateful Inspection) und zusätzlich wird das Datenteil und der Headerteil des Datenpaketes auf bestimmte Merkmale wie Protokollverletzungen, Computerviren, Spam und weitere unerwünschte Inhalte untersucht. Sie nutzt das Proxy-Grundprinzip, indem sie wie ein Stellvertreter zwischen den zu schützenden Ressourcen und anderen Netzwerken wie dem Internet auftritt, dabei fängt sie sämtliche Anfragen in und aus dem Internet ab, analysiert sie und leitet sie dann entweder stellvertretend weiter oder blockiert sie. Alle Verbindungen von dem zu schützenden Netz oder in das geschützte Netz koordiniert die Proxy Firewall selbst. Dadurch tritt sie für die Ziel- und Quell Systeme als eigenständiger Kommunikationspartner auf. Durch diese Stellvertreter Funktion kann die Proxy Firewall den Datenverkehr bis auf Schicht 7 des OSI-Schichtmodells$_1$ (Anwendungsschicht) werten und analysieren. Gegenüber dem Zielsystem gibt die Proxy Firewall vor ein Programm zu sein, welches die Dienste eines Servers in Anspruch nimmt (=Client), gegenüber dem Client gibt sie jedoch vor einen Server zu sein. Als Voraussetzung um den Datenverkehr filtern zu können, muss die Proxy Firewall die zu überwachenden Protokolle kennen, daher besitzt sie für jedes Protokoll wie HTTP, SMTP, FTP und DNS einen eigenen Filter. In diesem lassen sich unerwünschte Protokolloptionen oder Datenkommunikationen blockieren. Die proxybasierte Firewall ist eine sehr sichere Form der Firewall, da sie dafür sorgt, dass der direkte Netzverkehr zwischen internen und externen Systemen unterbindet. Die Firewall ist dabei immer dazwischengeschaltet und zugleich Ziel und Quelle jeglicher Kommunikation. Zum Beispiel kann ein internes Gerät nicht direkt ein Datenpaket von einem externen System erhalten.

Eine Proxy Firewall funktioniert nachdem Proxy-Grundprinzip. Was ist das Proxy-Grundprinzip konkret?

Das Proxy-Grundprinzip basiert auf der Stellvertreterfunktion für Netzwerkservices. (Zitat, Quelle 1) Dabei arbeitet ein Proxy als Stellvertreter für einen Client, welcher die Dienste eines Servers in Anspruch nehmen will. Der Client und der Server werden dadurch voneinander abgeschirmt und verhindert direkte Verbindungen zwischen den beiden Kommunikationspartner. Möchte ein Client Verbindung zu einem Server aufbauen, kommuniziert er zuerst mit dem Proxy. Dieser stellt dann stellvertretend für den Client die Verbindung zum Server her, danach leitet der Proxy die Daten vom Client zum Server

Und übermittelt die vom Server empfangenen Daten an den Client.

Name: Lukas Müller Thema: Proxy-Firewall Abgabe: 07.01.2020

Vorteile einer Proxy Firewall!

Die Proxy Firewall bietet eine sehr hohe Sicherheit, da sie auch auf der Anwendungsebene arbeitet und agiert. Im Vergleich zu paketorientiert arbeitenden Firewalls kann sie den Datenverkehr wesentlich detaillierter und tiefer analysieren. Dabei verbirgt sie die Anordnung der Geräte und Leitungen, die ein Rechnernetz bilden (Topologie), des geschützten Netzwerks vollständig vor der Außenwelt. Aus der Perspektive des Servers aus dem Internet agiert nur die IP-Adresse des Proxys. Da die Geräte hinter dem Proxy keinerlei Pakete direkt von potenziell gefährlichen Systemen empfangen können, werden ungewollte Zugriffe enorm erschwert. Angriffe lassen sich besser auswerten und schneller identifizieren da umfangreiche Logging-optionen zur Verfügung stehen.

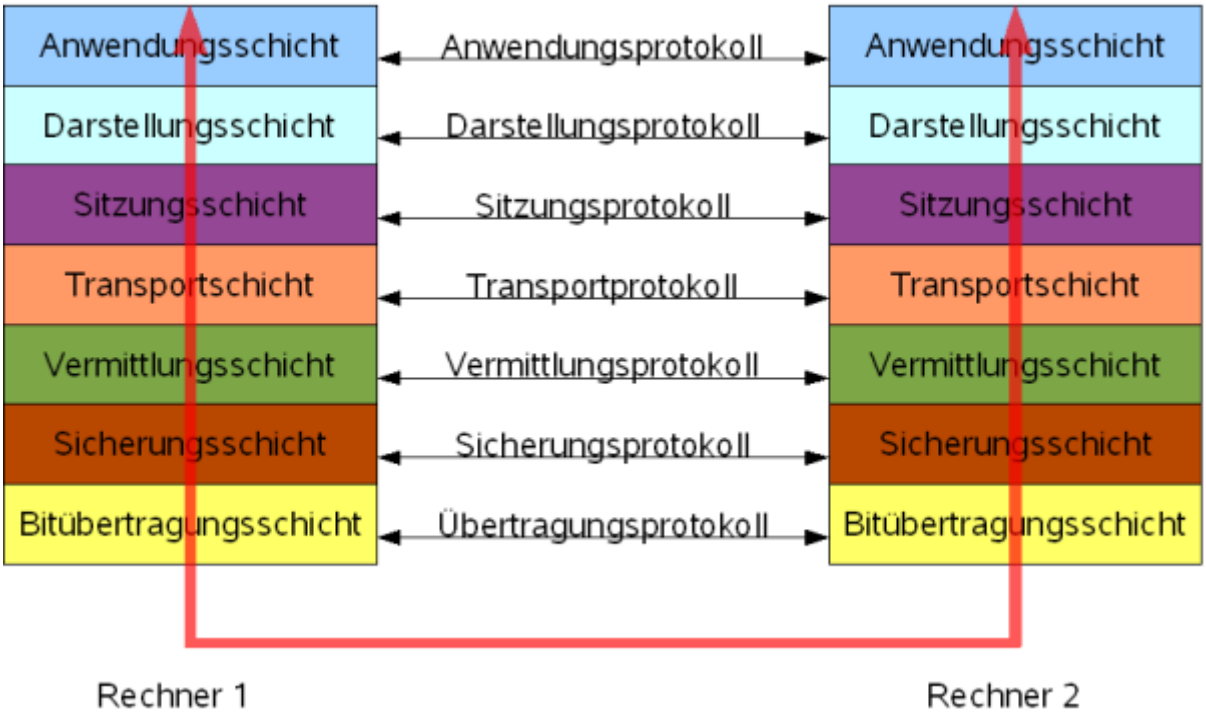
Nachteile einer Proxy Firewall!

Die Proxy Firewall hat zwar einige kompatible Protokolle, aber längst nicht alle. Bei Protokollen, die nicht allgemeinen Standards unterliegen kann es problematisch und aufwendig werden. Der Aufbau einer verschlüsselten Verbindung (Virtual Private Network (VPN)) ist meist nicht möglich. Durch die umfangreichen Analysen und durch die Funktion der Proxy Firewall als Stellvertreter aufzutreten, gibt es Einbußen in der Performance und der Datenkommunikation. Daher kommen für große Netzwerke Highend-Server für die Proxys zum Einsatz. Ein weiterer und großer Nachteil ist die oft komplexe und schwierige Konfiguration der Firewall, da zum Teil tiefergehende Kenntnisse der einzelnen Protokolle und Anwendungen nötig sind.

Was ist die Zielgruppe der Proxy Firewall?

Meist mittel bis große Unternehmen, die für die interne Sicherheit einen Proxy-Server haben, der alle Verbindungen bündelt, analysiert und wertet. Aber auch privat Personen, die im Internet anonym bleiben wollen und daher die schnellere und kostengünstiger Alternative zu einer VPN Verbindung nutzen. Da kostenlose VPN´s meist langsamer sind und der Nutzer für eine schnellere Verbindung Geld ausgeben muss, ist eine Proxy Verbindung eine meist praktische Alternative. Der große Unterschied ist, dass die Proxy Verbindungen im Gegensatz zu einem VPN nicht verschlüsselt sind. Außerdem haben kostenlose Proxys hohe Sicherheitsrisiken, daher ist es besser sensible Daten über VPN oder einen eigenen Proxy Server laufen zu lassen.

[1]OSI-Schichtmodells


Anwendungsschicht
Darstellungsschicht
Sitzungsschicht
Transportschicht
Vermittlungsschicht
Sicherungsschicht
Bitübertragungsschicht
Anwendungsprotokoll
Darstellungsprotokoll
Sitzungsprotokoll
Transportprotokoll
Vermittlungsprotokoll
Sicherungsprotokoll
Übertragungsprotokoll
Anwendungsschicht
Darstellungsschicht
Sitzungsschicht
Transportschicht
Vermittlungsschicht
Sicherungsschicht
Bitübertragungsschicht
Rechner 1
Rechner 2