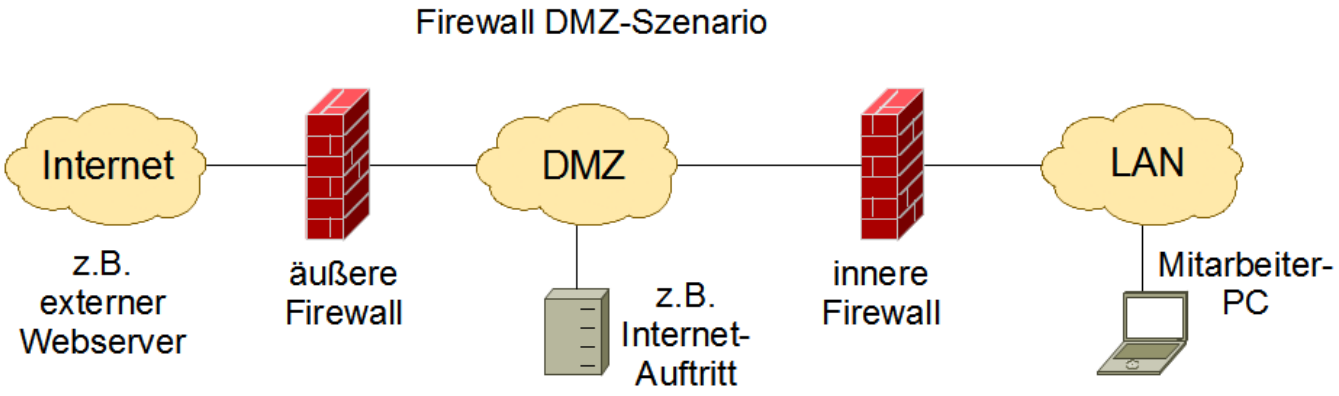
Einführung in Firewalls

Hier geht es zur Laborübung zu Firewall.

Firewall Grundidee

Nahezu alle Unternehmen haben eine Verbindung zum Internet. Sei es für den eigenen Internetauftritt, der lokal bereitgestellt wird, sei es zum Datenaustausch mit Kunden oder Partnern. Mit der großen Anzahl an Unternehmen im Internet ist auch die Anzahl der potenziellen Ziele für Angriffe gestiegen. Damit wird die zwingende Notwendigkeit der Absicherung der eigenen Netze immer wichtiger. Neben Angriffen von außen möchten Unternehmen aber auch unzulässige Zugriffe durch die eigenen Mitarbeiter (von „innen“) unterbinden können. Eine etablierte Technik dies zu tun ist der Einsatz von Firewalls.



Da es sich bei einer Firewall meist um ein einzelnes Netzelement innerhalb eines Netzes handelt[1], gibt es keine standardisierten Protokolle wie Firewalls miteinander kommunizieren. Allen Firewall-System ist das Grundprinzip eines sicheren **inneren Bereichs (LAN)**, eines **unsicheren äußeren Bereichs (Internet)** gemeinsam. Weiterhin kann eine innere **DMZ**[2], in der nur eingeschränkter Schutz gewährt wird, aufgesetzt werden. Die Idee liegt nun primär im Schutz der inneren Bereiche. Sekundäres Ziel kann es sein, Zugriffe von innen nach außen zu filtern bzw. zu unterbinden. Weiterhin geht man davon aus, dass man die konkrete Bedrohung nicht kennt, da sich Angreifer eben nicht an irgendwelche „Spielregeln“ halten. Firewalls können als reine Software oder auf dedizierter Hardware ausgeliefert werden. Letztere gelten als sicherer, da der Hersteller das gesamte System unter seiner Kontrolle hat, im Gegensatz zu einer Software-Lösung, die auf einem „fremden“ Betriebssystem läuft, wodurch sich neue Sicherheitslücken ergeben können. Schließlich handelt es sich bei beiden Varianten um Software, die auf einer Hardware ablaufen. Allen Firewalls ist die Grundstruktur gemein, dass anhand von Kriterien Regeln ausgewählt werden, wie mit dem einzelnen Paket zu verfahren ist[3].

Im Folgenden werden unterschiedliche Varianten von Firewalls aufgezeigt.

- Port-Filterung / Paketfilter
- Stateful Inspection
- Application Firewall / Proxy

Port-Filterung / Paketfilter

Bei der Port-Filterung bzw. Paketfilter werden äußere Kriterien der transportierten Daten herangezogen. Die folgenden Informationen dienen dabei als Kriterien für die Anwendung der Regeln:

- IP-Adressen
- Port (UDP- / TCP-Ports)
- Subnetze

Eine Port-Filterung bietet Basisschutz und sollte als Minimum zum Schutz eines Netzes verwendet werden.

Stateful Inspection

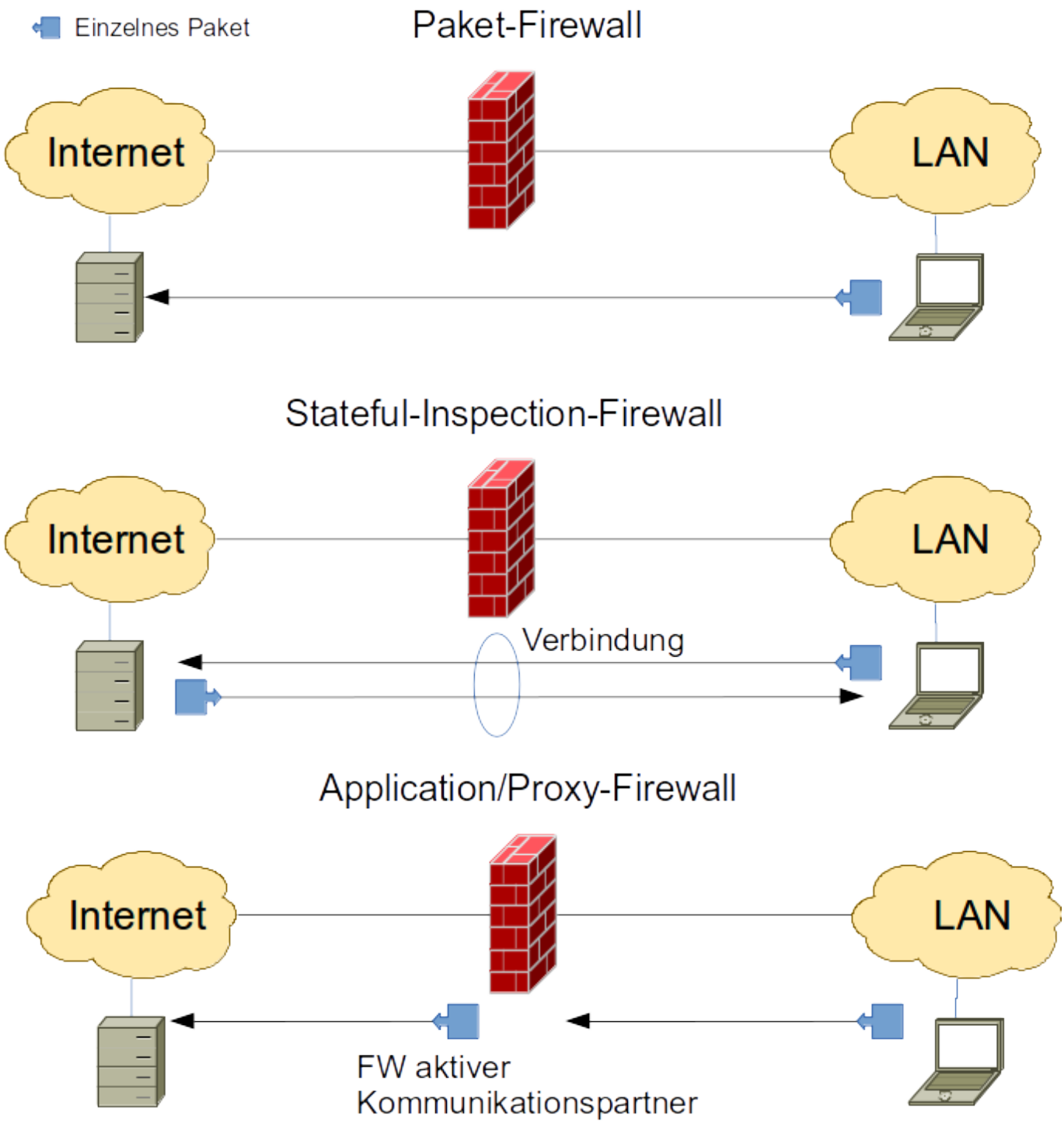
Eine **Stateful Inspection Firewall** bezieht neben den auch hier integrierten Port-/Paketfiltern zusätzlich noch den Status der Verbindung in die Bewertung der einzelnen Pakete mit ein. So kann zum Beispiel ein Sync-Flooding in einer Stateful Inspection, nicht aber in einer reinen Port-Filterung erkannt werden. Aus Sicht eines Portfilters, ist jeder Sync in sich u.U. korrekt und passiert so das Regelwerk. Ein Stateful Inspection Filter könnte aber erkennen, dass der Angreifer zu schnell und zu viele Sync sendet ohne den TCP-Verbindungsaufbau mit einem abschließenden Sync zu bestätigten. Dies kann demnach als Kriterium für eine Firewall-Regel dienen.

Application / Proxy Firewall

Eine Application Firewall (auch Proxy Firewall genannt) stellt eine weitere Variante dar, die als aktiver Kommunikationsendpunkt interpretiert werden kann. Dabei findet der Verbindungsaufbau stellvertretend für den Client durch die Firewall statt. D.h. anders als bei den ersten beiden Varianten greift die Firewall aktiv in die Pakete ein und filtert diese nicht nur. Abschließend soll im folgenden Schaubild der Unterschied nochmals verdeutlicht werden.

Übersicht Firewall-Typen

Die folgende Abbildung zeigt die drei vorgestellten Firewall-Typen. Durchgehende Pfeile symbolisieren dabei direkte Kommunikation.



1)

Redundanzen werden hierbei nicht betrachtet, da es sich aus Netzsicht ebenfalls um EINE Funktionseinheit handelt.

2)

DMZ: **D**e**M**ilitarisierte **Z**one

3)

vgl. Routing, Netzmaske und IP-Adresse als Kriterium zur Wegewahl in der Routing Table