[](https://www.google.at/url?sa=i&url=http%3A%2F%2Fisc-online.at%2Fsicher-im-netz%2F&psig=AOvVaw01kHnCG1mZzE1c_VlrJCjF&ust=1581172518101000&source=images&cd=vfe&ved=0CAIQjRxqFwoTCMDO-OPUv-cCFQAAAAAdAAAAABAJ)LAP-Vorbereitung

# **Firewall (FW)**

Unter einer Firewall (FW) versteht man eine **Schutzeinrichtung**, welche Datenverkehr zwischen Computernetzwerken filtert und einschränkt. Die Aufgabe von Firewalls ist es, durch verschiedene Mechanismen die **Sicherheit in Computernetzen zu erhöhen** (nur gewollte Kommunikation zwischen Netzwerken, Verhinderung unberechtigter Zugriffe auf das eigene Netzwerk, die Beschränkung von extern nutzbaren Diensten).

Firewalls können aus mehreren Hard- und Software-Komponenten bestehen, die je nach Benutzeranforderung an die Dienste und die Sicherheit individuell konfiguriert werden.

Beispiele für eine Software-Firewall wären PF (PacketFilter BSD), Windows Firewall, … .

Beispiele für eine Hardware-Firewall wären Fortinet FortiGate, pfSense, … .

## die zwei Grundsätze bei sicherheitskonzepten

Grundsätzlich wird bei Sicherheitsmaßnahmen oft zwischen **Whitelisting** und **Blacklisting** unterschieden.

Whitelisting bedeutet, alle erlaubten Aktionen werden aufgelistet. Alles was nicht erlaubt ist, ist automatisch verboten.

Blacklisting ist das Gegenteil. Alle verbotenen Aktionen werden aufgelistet, alles was nicht verboten ist, ist erlaubt. Whitelisting ist der grundsätzlich sicherere, weil restriktivere Ansatz. Whitelisting kann auch gegen noch unbekannte Gefahren schützen, wozu Blacklisting nicht in der Lage ist, Beispiel Virenschutz- alle bekannten Viren in einer DB- DB Abgleich- unbekannte Schädlinge haben leichtes Spiel.

## Mögliche Ebenen eines Sicherheitskonzeptes

Packet Filter (OSI 3-4)

Ein Paketfilter überprüft Eigenschaften eines TCP/IP Paketes wie etwa Quelladresse, Zieladresse und Zielport. Anhand dieser Kriterien wird unterschieden ob ein Paket erwünscht ist oder ausgefiltert wird.

Application Level Firewall (OSI 5-7)

Zusätzlich zum Paketfilter einsetzbar. Der Netzwerkverkehr kann für bestimmte Programme/Dienste erlaubt oder verboten werden auch, wenn diese über denselben Port/ dasselbe Protokoll kommunizieren.

## praktisches Beispiel- DMZ- DEMILITARISIERTE ZONE

Möchte man innerhalb des eigenen Netzwerkes Serverdienste auch für Clients aus dem Internet bereitstellen, muss man seine Firewall so konfigurieren, dass Verbindungen von außen auf den entsprechenden Server zugelassen werden. Dadurch wird die Sicherheit des Netzwerks geschwächt. Es wird eine Lücke geöffnet, durch die potentiell auch Angreifer in das Netzwerk gelangen können. Damit ein Angreifer der sich des Servers ermächtigt hat, nicht Zugriff auf das gesamte Netzwerk erhält, wird für diesen Zweck eine sogenannte Demilitarisierte Zone (DMZ) errichtet

In diesem Fall dürfen interne Systeme, sowohl das Internet, als auch den Server in der DMZ kontaktieren. Der Server in der DMZ darf jedoch keine internen Systeme kontaktieren. Systeme aus dem Internet dürfen den DMZ-Server kontaktieren, jedoch nicht die internen Systeme.

