Firewall 🔥🧱

**Personal FW** („Software“ FW):

* Oft Teil des Betriebssystems
* Durch User selbst verwaltbar
* Vorteil:
  + Schützt auch gegenüber anderen Hosts im selben Netz
* Nachteil:
  + Läuft am eigenen Host
    - Rechenleistung wird genutzt
    - Andere Prozesse können Einfluss nehmen

**Dedicated FW** („Hardware“ FW, Network FW, „Corporate“ FW):

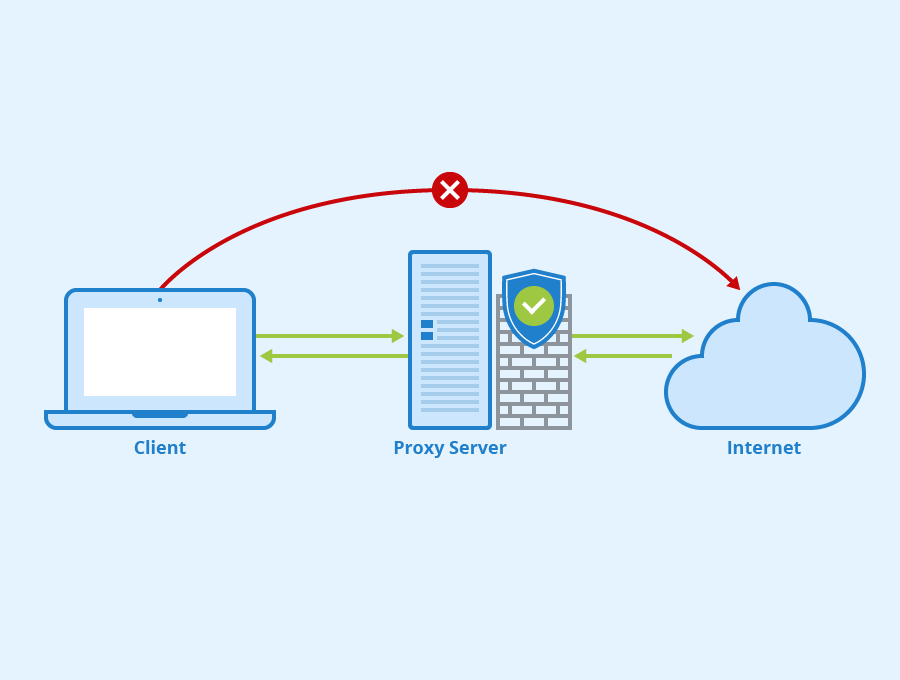
* Eigene Hardware, oft ein Router
* Eigene Administrator
* Vorteil:
  + Zentrale Durchsetzbarkeit von Regeln
  + Eigene Hardware 🡪 Rechenleistung, Sicherheit
* Nachteil:
  + Teuer
  + Man muss alles selbst administrieren

**Allgemein:**

Firewalls filtern nach:

* Adressen des Network (Internet) Layers (IP)
* Adressen & Protokolle des Transport Layers (TCP, UDP, Portnummer)
* „deep Packet Inspection“
* stateful Inspection

**Proxy:**

Ein Proxy ist eine Kommunikationsschnittstelle in einem Netzwerk aus Rechnern in Form eines physischen Computers.

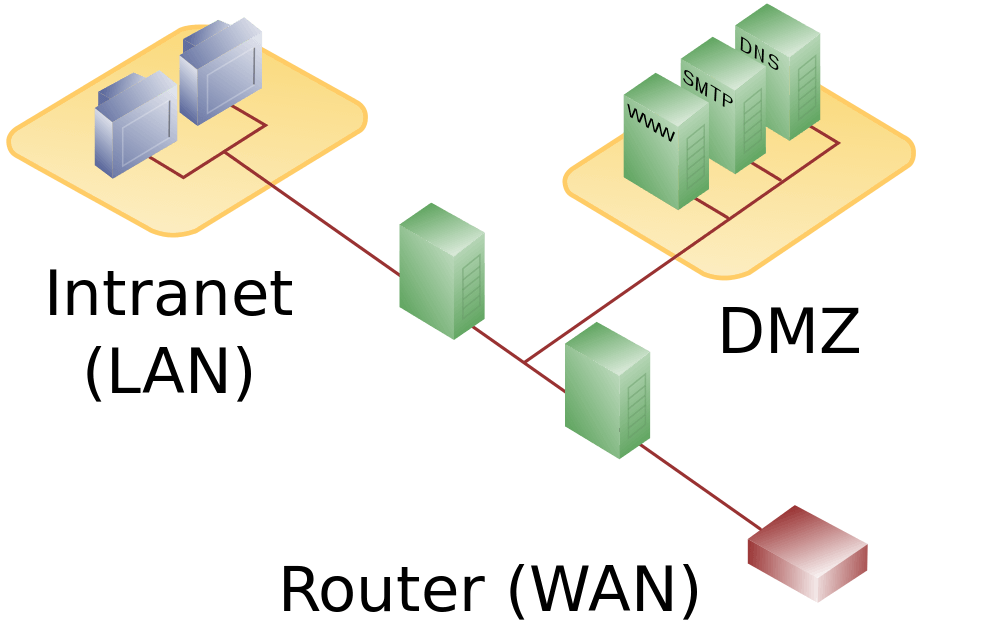
Er arbeitet als Vermittler, der auf der einen Seite Anfragen entgegennimmt, um dann über seine eigene Adresse eine Verbindung zur anderen Seite herzustellen.

Abbildung - Proxy funktion

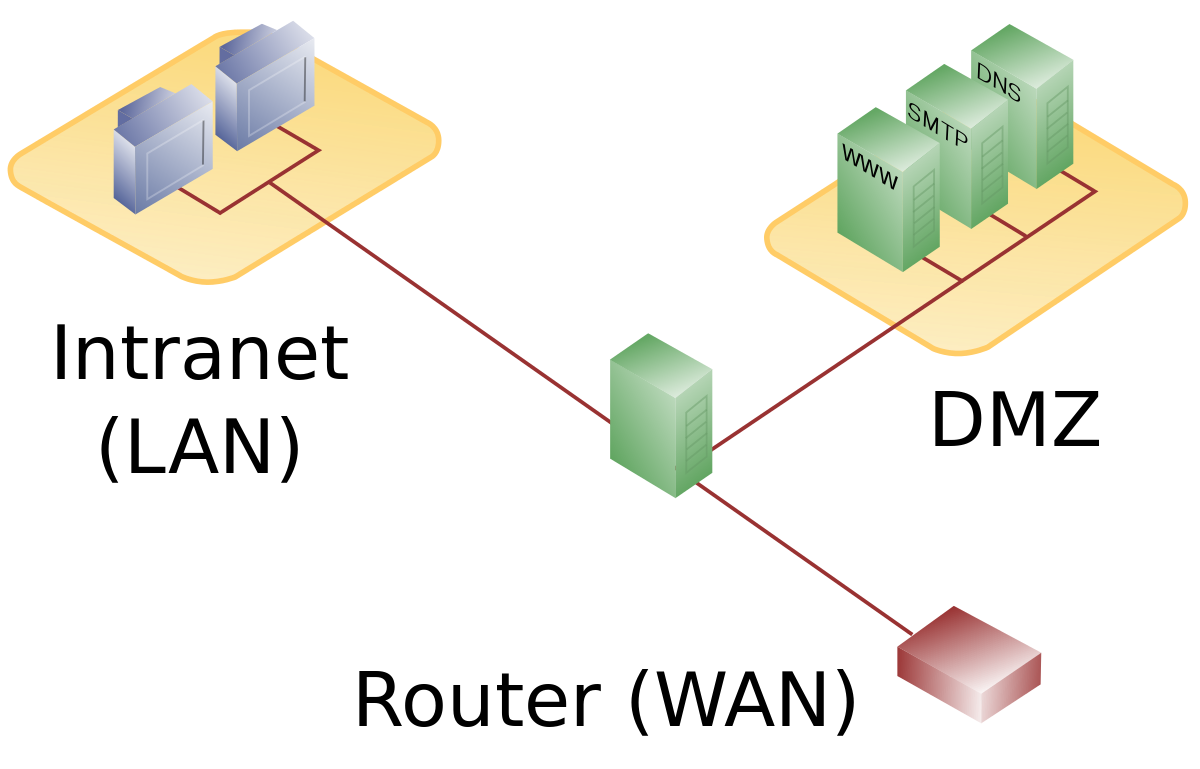
**DMZ:**

Demilitarisierte Zone

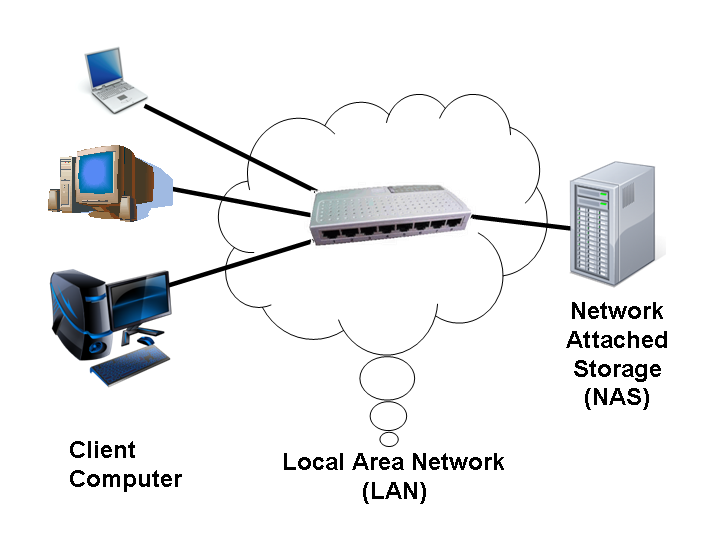
Alte Variante:



Neue Variante:



**SOHO (Small Office Home Office):**



IDS

= Intrusion Detection System

Angriffserkennungssystem ist ein System zur Erkennung von Angriffen, die gegen ein Computersystem oder Rechnernetz gerichtet sind.

Das IDS kann eine Firewall ergänzen oder auch direkt auf dem zu überwachenden Computersystem laufen und so die Sicherheit von Netzwerken und Computersystemen erhöhen. Erkannte Angriffe werden meistens in Log-Dateien gesammelt und Benutzern oder Administratoren mitgeteilt

IPS

= Intrusion Pretencen System