Firewalls

Bedrohungen: Viren, Trojaner, DDOS,
Eindringen in das Netzwerk

Desktopfirewall: lokale Firewall auf einem Rechner
z.B. Windows - Firewall

Portfilter: Ports öffnen oder schließen (accept, drop, reject) => fail2ban

→ Portknocking: - Verschiedene Ports werden in einer bestimmten Reihenfolge angefragt
↳ stimmt die Reihenfolge, werden definierte Ports geöffnet

Paketfilter: kann zusätzlich zum Portfilter weitere Headerinformationen auswerten
- Adressen
- Typ (Protokoll, ...)

=> opnsense

Stateful Paket Inspection: besonderer Paketfilter
legt sich Verbindungszustände (State Table)
↳ kontrolliert eine einmal genehmigte Verbindung nicht ständig (für gewisse Zeit)

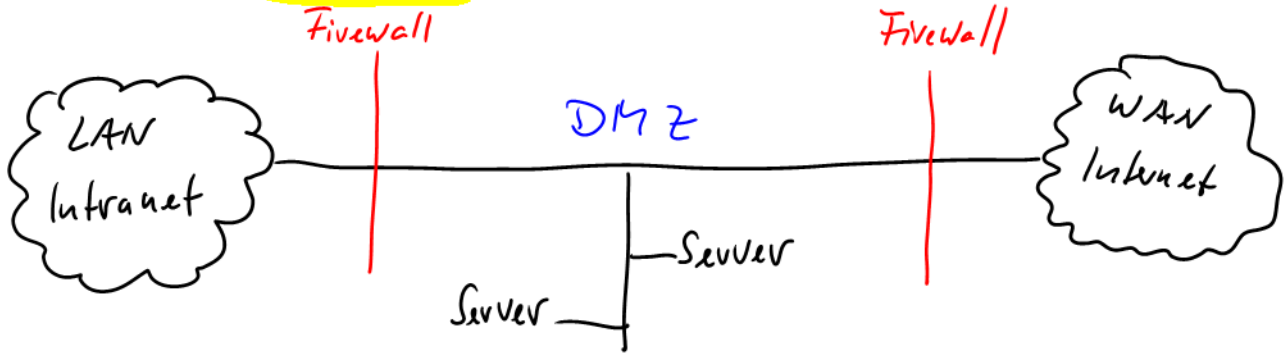
Application Layer Gateway: ⇒ Sophos UTM

- kann bis OSI-7 filtern
- Proxy ⇒ benötigt je nach Datenrate und Anzahl Verbindungen viel Rechenleistung

Deep Paket Inspection: ähnlich ALGs → Provider

- kann filtern Webseiten (Zensur)
- Mobilfunkanbieter filtern VoIP
- Einschränkung von Datenraten

Demilitarisierte Zone:



↳ Firewalls von unterschiedlichen Herstellern