

Firewalls

Dienstag, 24. November 2020 09:23

Bedrohungen: Einchöpfen in das Netzwerk
Viren, Trojäne, DDOS

Desktopfirewall: lokale Firewall auf einem Rechner, Windows Firewall

Portfilter: Ports öffnen bzw schließen => fail 2 ban
accept, reject, drop

→ **Portknodung:** - verschiedene Ports werden in einer bestimmten Reihenfolge angefragt
- stimmt die Reihenfolge, werden definierte Ports geöffnet

Pathfilter: kann zusätzlich zum Portfilter weitere Headerinformationen auswerten:
- Adressen
- Typ (Protokoll)

Stateful Packet Inspection: besonderer Portfilter => openSense

→ weist sich Verbindungsverständnis (State Table) auf
→ kontrolliert eine einmal genehmigte Verbindung ständig (für eine gewisse Zeit)

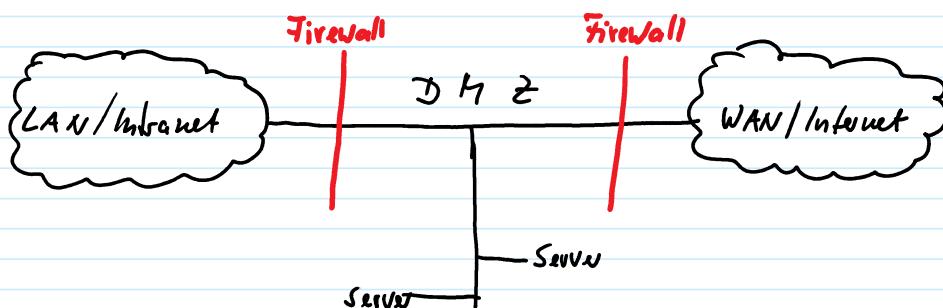
Application Layer Gateway: kann bis zu OSI-Schicht 7 filtern

=> Sophos UTM
benötigt jedoch Datenrate und Anzahl Clients je nach Leistung

Deep Packet Inspection: ähnlich ALG → Providerverseite

- kann filieren Verbrechen
- Mobilfunkanbieter filtern VoIP
- Einschränkung der Datenraten

Demilitarized Zone (DMZ):



↳ Firewalls von unterschiedlichen Herstellern!