

Firewalls

Dienstag, 24. November 2020

09:23

Bedrohungen: Eindringen in das Netzwerk
Viren, Trojaner, DDOS

Desktopfirewall: lokale Firewall auf einem Rechner, Windows Firewall

Portfilter: Ports öffnen bzw. schließen
accept, reject, drop

=> fail 2 ban

-> Portknodrig : - verschiedene Ports werden in einer
bestimmten Reihenfolge angefragt
- stimmt eine Reihenfolge, werden definierte
Ports geöffnet

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

Stateful Paket Inspection: Erweiterte Paketfilter => openseense

→ behält sich Verbindungszustände (State Table)
→ kontrolliert eine einmal genehmigte Verbindung nicht ständig (für eine gewisse Zeit)

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

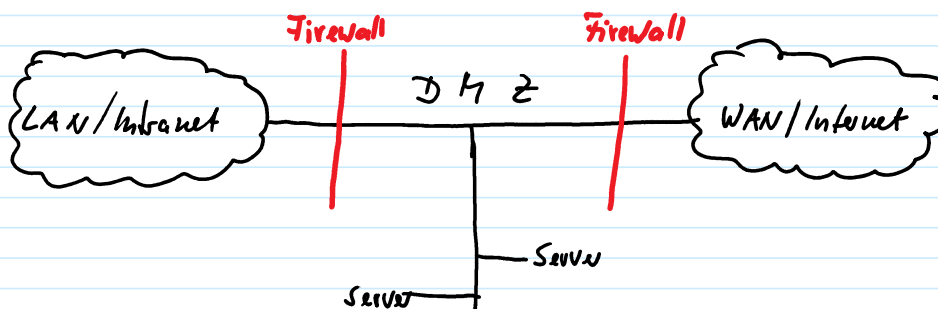
=> Sophos UTM

benötigt je nach Datenrate und Anzahl
Clients viel Rechenleistung

Deep Paket Inspection: ähnlich ALG -> Providerseite

- Länder filtern Webseiten
- Telefonfunkanbieter filtern VoIP
- Einschränkung der Datenraten

Demilitarisierte Zone (DMZ):



↳ Firewalls von unterschiedlichen Herstellern!