

Firewalls

Termenul de firewall este probabil in top10 cele mai folosite in mediul IT si chiar si in randul utilizatorilor, acestea sunt echipamente de securitate de retea care sunt gandite sa monitorizeze atat traficul care intra (inbound) cat si cel care iese (outbound). Scopul principal al unui firewall este de a forma o bariera intre WAN sau zona rosie si LAN cea verde.

Modul in care functioneaza un firewall este relativ simplu prin compararea pachetelor cu un set de reguli si blocand tot ce nu se aplica, aceste echipamente sunt situate la punctul de conectare a retelei cu o alta retea sau internet, un exemplu de regula ar fi " Adresa sursa 192.168.88.10 se poate conecta la 1.2.3.4 pe portul 80".

Tipuri de Firewall:

- **Next-generation firewalls (NGFW):** sunt acele sisteme care imbina atat tehnologia traditionala cu functii dedicate cum ar fi inspectia traficului criptat, preventia intrusiuni NIDS (Network Intrusion Detection System). O functie primara gasita pe aceste tipuri de firewall este DPI (Deep Packet Inspection) facandu-se prin reasamblarea sirului de pachete analiza sa si compararea cu anumite reguli de protocol de aplicatie.
- **Proxy firewalls:** acest tip functioneaza ca un filtru la nivel de aplicatie. Spre deosebire de celelate firewall-uri, actioneaza ca un intermediar intre doua sisteme. In cele mai multe cazuri acestea lucreaza la nivelul 7 cu protocoale cum ar fi HTTP sau FTP folosindu-se atat de DPI cat si de stateful inspection.
- **Network address translation firewalls (NAT):** acesta permite mai multor dispozitive dintr-o retea independenta sa comunice si sa se conecteze pe internet folosind un singur IP public. In acest mod, adresele IP individuale sunt ascunse si un hacker nu poate, sau poate mult mai greu, sa afle detalii despre fiecare dispozitiv din retea.
- **Stateful multilayer inspection (SMI) firewalls:** acest sistem de firewall are capacitatea de a filtra la nivel de retea, transport si aplicatie. La faza de filtrare face comparatia cu pachetele de incredere inainte de a lua o decizie. Similar cu NGFW, acesta examineaza pachetul in intregime inainte de a lua o decizie de a-l bloca sau trece.