SADRŽAJ

POGLAVLJE I

1. UVOD

• • • •

Mora da implementira politiku sigurnosti. Ako određeno svojstvo nije dozvoljeno, Firewall mora da onemogući rad u tom smislu. Firewall treba da beleži sumnjive događaje. Firewall treba da upozori administratora na pokušaje proboja i kompromitovanja politike sigurnosti. U nekim slučajevima Firewall može da obezbedi statistiku korišćenja. -1-

Firewall može biti softverski ili hardverski. Softverski firewall omogućuje zaštitu jednog računara , osim u slučaju kada je isti računar predodređen za zaštitu čitave mreže. Hardverski firewall omogućuje zaštitu čitave mreže ili određenog broja računara. Za ispravan rad firewall-a, potrebno je precizno odrediti niz pravila koja definiraju kakav mrežni promet je dopušten u pojedinom mrežnom segmentu. Takvom politikom se određuje nivo zaštite koji se želi postići implementacijom firewall usluge.

-2-

POGLAVLJE II

2. PODJELA POTENCIJALNIH 'NAPADAČA' 2.1. ZAŠTITA LOKALNE MREŽE OD ŠTETNOG DJELOVANJA 'NAPADAČA' Firewalli koji nemaju čvrste i stroge politike prema dolaznim paketima podložni su različitim vrstama napada. Ukoliko firewall ne podržava kreiranje virtualnih privatnih mreža, a organizacija želi omogućiti pristup sa određenih IP adresa lokalnoj mreži, moguće je konfigurirati firewall

da propušta pakete sa točno određenim izvorišnim IP adresama. Ali takav način postavljanja sadrži brojne nedostatke. Na primjer napadač se može domoći paketa te saznati logičku adresu sa kojom je dozvoljeno spajanje na lokalnu mrežu. Nakon toga napadač može kreirati pakete kojim kao izvorišnu stavlja logičku adresu računara kojem je dozvoljeno spajanje i tako pomoću posebno prilagođenih paketa nanijeti štetu lokalnoj mreži. Firewall je potrebno konfigurisati tako da onemogućava različite postojeće napade. Većina današnjih proizvođača firewalla ponosno ističe na koje napade su njihovi firewalli otporni, ali nove vrste napada se svakodnevno razvijaju i sve su kompliciraniji i kompleksniji. Ipak svaki firewall bi trebao biti otporan na poznate napade kao što su sljedeći navedeni. • Address Spoofing napad omogućava da paket bude proslijeđen sa vanjskog okruženja na neko od internih računara ukoliko napadač kao izvorišnu adresu uzme neku od adresa unutar lokalne mreže. U tom slučaju firewall je možda konfigurisan da omogućava prolazak paketa i time ciljni računar može primiti posebno prilagođeni paket. Da bi se ovakva vrsta napada onemogućila potrebno je onemogućiti prosljeđivanje paketa koji kao izvorišnu adresu imaju neku od lokalnih adresa, a kao ulazno okruženje ono okruženje koje je spojeno na Internet. Smurf napad spada u grupu napada koje imaju za cilj onemogućavanje rada pojedinih