Zaštita računarskih mreža - firewall
Vrsta: Seminarski | Broj strana: 17 | Nivo: BLC

Sadržaj

1. Šta je firewall?

Firewall je odgovoran za više važnih stvari unutar informacionog sistema:
Mora da implementira politiku sigurnosti. Ako određeno svojstvo nije dozvoljeno, Firewall mora da onemogući rad u tom smislu.
Firewall treba da bilježi sumnjive događaje.
Firewall treba da upozori administratora na pokušaje proboja i kompromitovanja politike sigurnosti.
U nekim slučajevima Firewall može da obezbjedi statistiku korišćenja.
Firewall može biti softverski ili hardverski :
Softverski firewall omogućava 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 definišu kakav mrežni promet je dopušten u pojedinom mrežnom segmentu. Takvom politikom se određuje nivo zaštite koji se želi postići implementacijom firewall usluge.

2. Podjela potencionalnih 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 tačno određenim izvorišnim IP adresama. Ali takav način postavljanja sadrži brojne nedostatke. Na primer 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 nanjeti štetu lokalnoj mreži. Firewall je potrebno konfigurisati tako da onemogućava različite postojeće napade.