Zaštita Računarskih Sistema - Firewall (Vatreni Zid)
Vrsta: Seminarski | Broj strana: 28 | Nivo: Viša Železnička Škola

SADRŽAJ



## 1. Šta je Firewall ?

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

## 2. Podela potencionalnih napadača

### 2.1.Zaštita lokalne mreže od štetnog delovanja “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 postavlja Smurf napad spada u grupu napada koje imaju za cilj onemogućavanje rada pojedinih servera i računara, tj. DoS napad (eng. Denial of Service). Napadač šilje ICMP echo request paket na broadcast adresu cele lokalne mreže. Time su adresirani svi računari unutar lokalne mreže. Kao odredište navodi se ciljni računar koji se želi onesposobiti velikim brojem odgovora. Za odbranu od ovakve vrste napada dovoljno je u konfiguracijskoj datoteci firewalla onemogućiti broadcast paket.• Address Spoofing napad omogućava da paket bude prosleđen sa nepoznatog 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. •nja 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 naneti 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 komplikovani i kompleksniji. Ipak svaki firewall bi trebao biti otporan na poznate napade kao što su :