Firewall
Vrsta: Seminarski | Broj strana: 11 | Nivo: Visoka tehnološka škola

Šta je Firewall ?
Osnovna namena Firewall-a
Stav da "sve što nije dozvoljeno je zabranjeno" zahteva da se svaki novi servis individualno omogućava.
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 upozori administratora na pokušaje proboja I kompromitovanja politike sigurnosti. Firewall treba da beleži sumnjive događaje. •
U nekim slučajevima Firewall može da obezbedi 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. Podela potencijalnih 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 konfigurisati Firewall da propušta pakete sa tačno određenim izvorišnim IP adresama. Ali takav način postavljanja sadrži brojne nedostatke. Na primer napadač se može domoći paketa i 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 Firewall-a ponosno ističe na koje napade su njihovi Firewall-i 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 :
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. •
2.2.Zaštita od štetnog delovanja lokalnih korisnika
Prilikom konfigurisanja Firewall-a najveća se pažnja posvećuje obradi dolaznih paketa. Danas sve više komercijalnih Firewall-a omogućava bolju kontrolu rada korisnika. Oni su konfigurisani na način da ne dozvoljavaju lokalnim korisnicima pristup određenim materijalima.

---------- OSTATAK TEKSTA NIJE PRIKAZAN. CEO RAD MOŽETE PREUZETI NA SAJTU. ----------

www.maturskiradovi.net

MOŽETE NAS KONTAKTIRATI NA E-MAIL: maturskiradovi.net@gmail.com