FIREWALL

Pojam firewall izvorno se odnosio na zid namenjen da ograniči vatru ili potencijalni požar unutar zgrade, kasnije se odnosio na slične strukture, kao što je lim koji radvaja motor u autu ili na avionu od putničke kabine. Firewall tehnologija nastala je kasnih 1980-ih godina, kada je internet još uvijek bio prilično nova tehnologija u smislu globalnog korištenja i povezivanja. Prethodnici forewalla za mrežnu sigurnost su bili ruteri koji su se koristili kasnih 1980-ih godina

Danas, pod pojmom "Firewall" podrazumevamo softver koji se instalira na lični računar ili na računar koji služi kao server u malim mrežama ako se koristi deljena internet konekcija. Njegov zadatak je kontrola komunikacije računara koji direktno izlazi na mrežu, a to znači da vodi računa o:

1. Koji programi izlaze sa računara
2. Kuda oni idu, odnosno sa kojim serverima i preko kojih protokola i portova stupaju u kontakt
3. Konroliše sta ulazi na računar

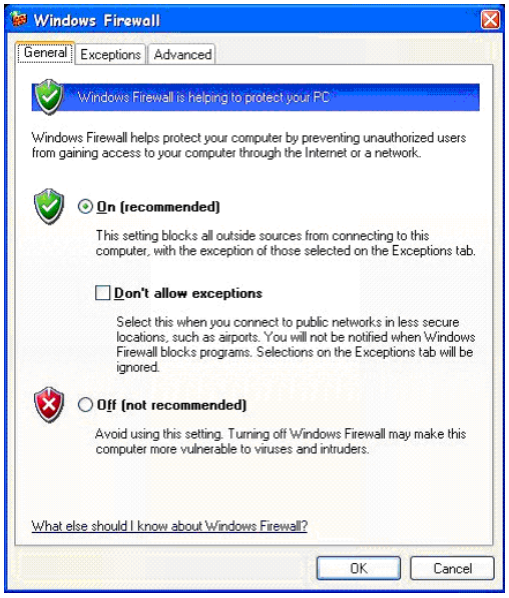
Firewall takođe može sprečiti hakere ili zlonamerne softvere (poput "worms" i sličnih) da pristupe vašem kompjuteru preko mreže ili interneta. Firewall takođe može i sprečiti lokalni kompjuter da šalje zlonamerne softvere drugim kopjuterima.

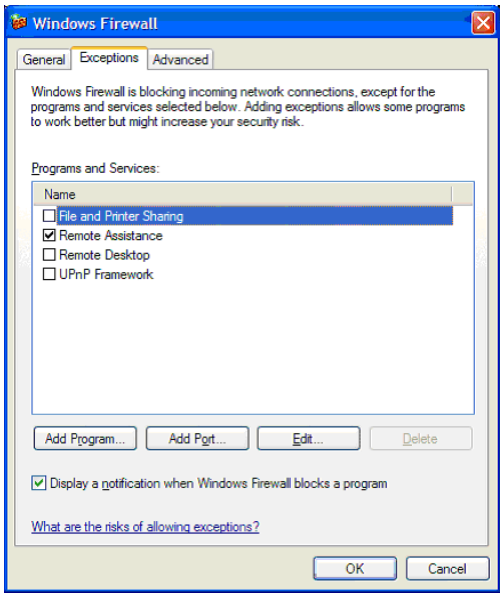
Većina firewall-ova pita za dozvolu koji program će da pusti da izađe, pod kojim uslovima, koji protokol program koristi i na kojim portovima se obavlja komunikacija. Naravno, isto se odnosi i na suprotan smer, na ulaznu komunikaciju. Postoji i firewall softver koji ništa ne pita i koji je u težnji za dostizanjem savršenstva po nekim kriterijumima; on je toliko automatizovan da stiže praktično unapred podešen i potrebna je samo instalacija.

Dobar program ove vrste će ispravno registrovati svaku konekciju pre nego što bude uspostavljena, blokirati je ili preciznije, ostaviti na čekanju, i tek ako korisnik dozvoli njeno ostvarivanje ona će biti uspostavljena. Ovo u stvari znači da ako se preuzima neki *patch* za program, moguće je da se onemoguće sve ostale konekcije osim one preko koje se razmena, odnosno primanje podataka obavlja. Nekada i ovo nije dovoljno i treba reći da savršena zaštita ne postoji.

Dobra osibina nekih firewall-a je da imaju mogućnost da se trenutno blokira sav saobraćaj između računara i interneta i/ili da se dozvoli samo nekim programima da nastave normalno da rade.

Kako podesiti firewall?





Prva stvar koju je potrebno uraditi po završetku instalacije je provera koja pravila u njemu postoje. Ako je program napravljen tako da su već da data pravila za neke aplikacije, i ako korisnik nije pristalica ovakvih metoda, onda može da ih samo onemogući.

Sledeći korak je da se obezbedi NetBIOS. Neki firewall-i imaju već pravila podešena za njega. Ne bi bilo loše da se i ona onemoguće, ako ne zadovoljavaju kriterijume da zabranjuju bilo kakvu komunikaciju na portovima 137, 138, 139, i preko TCP i preko UDP protokola. Ako računar nije u lokalnoj mreži, potrebno je preduzimanje ranije opisanih koraka za potpuno deaktiviranje NetBIOS-a.

Izlazak na internet:

Ako se onemoguće, ili pak izbrišu sva pravila koja se odnose na portove i protokole, tokom uspostavljanja raznih konekcija od strane različitih aplikacija firewall će uvek da pita šta da radi. To je trenutak da se postavi novo pravilo, koje može biti trajno, ili će važiti samo za vreme dok traje data konekcija. Ono bez čega se sigurno ne može na internet je DNS (Domain Name System) i browser (pretraživač interneta). DNS radi na portu 53 i mora da bude omogućen, da bi moglo da se obavi upoznavanje dva računara. Dozvoljen je protokol UDP, kao i dvosmerna komunikacija samo na portu 53 (domen), s tim što treba dodati i TCP protokol. Poslije toga može se pokrenuti browser. Potrebno je da se dozvoli komunikacija TCP protokolom samo na portovima 80(http) i 8080(http-proxy) ako se koristi proxy server, a većina provajdera ga ima.

Dakle, firewall se može zamisliti kao granični prelaz; oni koji imaju pasoš (dozvolu za ulazak ili izlazak) proći će tu granicu, a svima ostalima biće zabranjen prolaz.