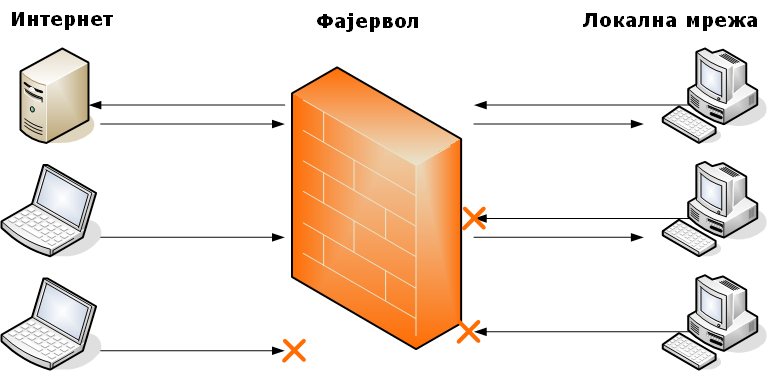
**MREŽNE BARIJERE**

****

**Opšte**

Mrežna barijera ili Firewall je mrežni bezbednosni sistem koji prati i kontroliše dolazni i odlazni mrežni saobraćaj zasnovan na predodređenim bezbednosnim pravilima. Zaštitni zid obično uspostavlja barijeru između poverljive interne mreže i nepoverljive eksterne mreže, kao što je internet.

Zaštitni zidovi se često kategorizuju kao mrežne barijere ili barijere zasnovane na hostu. Mrežne barijere filtriraju saobraćaj između dve ili više mreža i rade na mrežnom hardveru. Barijere zasnovane na hostu rade na host računarima i kontrolišu mrežni saobraćaj unutar i van tih mašina.

**Istorija**

Termin „zaštitni zid“ izvorno potiče od zida koji je namenjen primanju vatre unutar zgrade. Kasnije upotrebe se odnose na slične strukture kao što je lim koji odvaja motor vozila od odeljka za putnike. Termin je kasnih 1980ih primenjen na mrežnu tehnologiju koja je izbila kada je internet ****bio relativno nov gledajući na njegovu globalnu upotrebu i povezanost. Prethodnici zaštitnih zidova mrežne bezbednosti su bili ruteri koji su korišćeni kasnih 1980ih.

Mrežne barijere su nastale zato što je ponestajalo adresnog mesta, a najviše zbog sigurnosnih razloga. U ranim devedesetim godinama prošlog veka, firme su počele da koriste mrežne barijere primarno zbog smanjenja mogućnosti povezivanja koje su do tada postojale.

**Vrste**

Zaštitni zidovi se obično kategorizuju kao zaštitni zidovi zasnovani na mreži i na hostu. Zaštitni zidovi zasnovani na mreži su pozicionirani na izlazu LAN-a, WAN-a i intraneta. Oni su ili softverski uređaji koji rade na posebno napravljenom hardveru ili su hardverski računarski uređaji. Uređaji zaštitnog zida takođe mogu ponuditi druge funkcionalnosti internoj mreži koju štite, kao što je mogućnost rada kao DHCP ili VPN server za tu mrežu.

Zaštitni zidovi zasnovani na hostu su pozicionirani na samom mrežnom čvoru i kontrolišu mrežni saobraćaj unutar i van tih mašina. Zaštitni zid zasnovan na hostu može biti usluga kao deo operativnog sistema.Obe vrste imaju svoje prednosti i mane. Međutim, svaki ima svoju ulogu u slojevitoj bezbednosti. Zaštitni zidovi variraju u vrsti u zavisnosti od toga odakle potiče komunikacija, gde je presretnuta kao i stanje komunikacije koja se prati.

**Zaštita lokalne mreže od štetnog delovanja napadača**

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 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 nanjeti štetu lokalnoj mreži. Firewall je potrebno konfigurisati tako da onemogućava različite postojeće napade.

**Aplikativni sloj**

Zaštitni zidovi aplikativnog sloja rade na aplikativnom nivou TCP/IP steka i mogu da presreću sve pakete koji putuju ka ili od aplikacije. Oni blokiraju druge pakete (obično ih odbacuju bez potvrde pošiljaocu).

Prilikom pregledanja neodgovarajućeg sadržaja svih paketa, zaštitni zidovi mogu odgraničiti ili sprečiti potpuno širenje mrežnih računarskih crva ili trojanaca. Dodatni kriterijum pregledanja može dodati latenciju prosleđivanju paketa na njihovo odredište.

****Aplikativni zaštitni zidovi funkcionišu tako što odlučuju da li proces treba da prihvati bilo koju datu vezu. Aplikativni zaštitni zidovi izvršavaju svoju funkciju kačeći se na socket call radi filtriranja veze između aplikativnog sloja i nižih slojeva OSI modela. Aplikativni zaštitni zidovi koji se kače na socket call se takođe nazivaju i soket filteri. Aplikativni zaštitni zidovi rade poput paket filtera ali aplikativni filteri primenjuju pravila filtriranja (dozvoli/odbij) po procesu filtriranja veze umesto prema portu. Obično se koriste upiti radi definisanja pravila za procese koji još uvek nisu primili vezu. Retko se nalaze aplikativni zaštitni zidovi koji se ne kombinuju sa paket filterom.

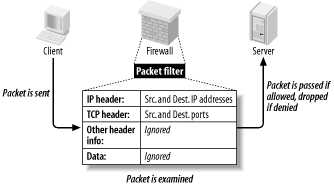
**Paket filteri**

Zaštitni zidovi mrežnog sloja, takođe poznati i kao paket filteri, funkcionišu na relativno niskom nivou TCP/IP protokol steka, ne dozvoljavajući paketima da prođu kroz zaštitni zid osim ako ne odgovaraju ustanovljenoj listi pravila. Administrator zaštitnog zida može da definiše pravila ili se mogu koristiti podrazumevana pravila. Zaštitni zidovi mrežnog sloja obično spadaju u dve podkategorije, sloj stanja i sloj bez stanja.

Zaštitni zidovi stanja održavaju sadržaj o aktivnim sesijama i tu „informaciju stanja“ koriste za ubrzavanje procesiranja paketa.

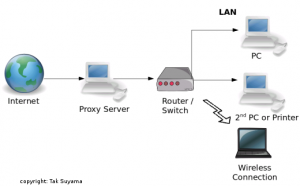
Zaštitni zidovi bez stanja zahtevaju manje memorije i mogu biti brži za jednostavnije filtere koji zahtevaju manje vremena za filtriranje nego za pretragu sesije. Oni takođe mogu biti neophodni za filtriranje mrežnih protokola bez stanja koji nemaju koncept sesije. Međutim, oni ne mogu donositi složenije odluke zasnovane na dostignutom nivou komunikacije između hostova.

Noviji zaštitni zidovi mogu da filtriraju saobraćaj preko mnogo atributa paketa kao što su izvorna IP adresa, izvorni port, odredišna IP adresa ili port, usluga kao što je HTTP ili FTP, protokoli, TTL vrednosti i mnogi drugi atributi.



**Proksi server**

Filtriranje i NAT rešavaju neke probleme vezivanja lokalnih mreža na Internet, ali uzevši u obzir da samo analiziraju i eventualno menjaju zaglavlje paketa, a ne i njegov sadržaj – ne obezbeđuju potpunu kontrolu podataka koji prolaze kroz mrežnu barijeru. Proksi (engl. proxy) aplikativnog sloja sprečava ovaj problem tako što omogućava da se potpuno zabrani protok podataka protokola mrežnog sloja i da se dozvoli saobraćaj samo protokolima viših slojeva, kao što su HTTP, FTP i SMTP. Proksi aplikativnog sloja je klijent-server arhitektura specifična za konkretan protokol koji se koristi.



**Tumačenje mrežne adrese**

Zaštitni zidovi često imaju funkcionalnost tumačenja mrežne adrese (NAT – Network Address Translation), a hostovi koji su zaštićeni iza zaštitnog zida često imaju adrese u „privatnom opsegu adresa“, kao što je definisano u RFC 1918. NAT funkcija je izvorno razvijena da bi adresirala ograničeni broj IPv4 rutabilnih adresa koje se mogu koristiti ili dodeliti kompanijama ili individualnim ljudima kao i da bi smanjila količinu i samim tim i cenu pribavljanja dovoljno javnih adresa za svaki računar unutar organizacije.

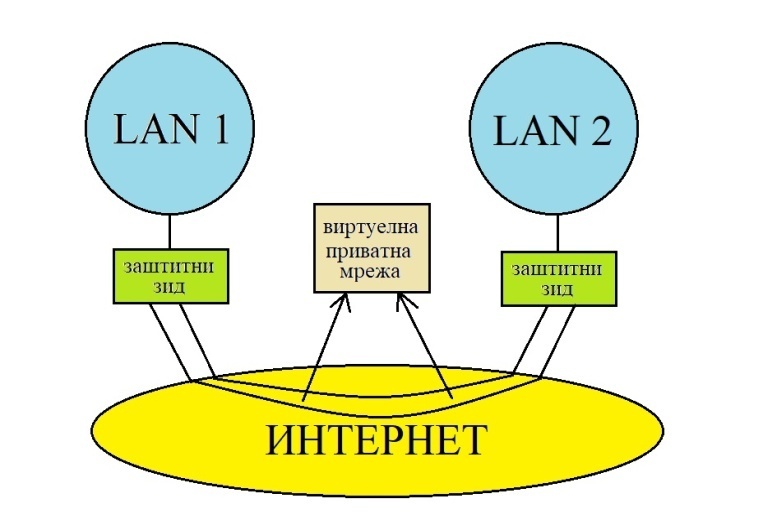
**Među-sistemski prolaz**

Među-sistemski prolaz (engl. Dual-Homed Gateway) jeste zaštitni zid koji se sastoji od računara sa najmanje dva mrežna adaptera. Ovakav sistem se normalno konfiguriše tako da se paketi ne rutiraju direktno sa jedne mreže (internet) na drugu mrežu (intranet). Računari na internetu mogu da komuniciraju sa zaštitnim zidom, kao i računari sa unutrašnje mreže, ali je direktan saobraćaj ****blokiran. Glavna mana među-sistemskog prolaza je činjenica da blokira direktni IP saobraćaj u oba pravca.

**Virtualne privatne mreže**

Virtuelne privatne mreže (engl. Virtual Private Network) su takozvani enkripcijski tuneli koji omogućavaju sigurno spajanje dve fizički odvojene mreže preko interneta bez izlaganja podataka neautorizovanim korisnicima. Zadatak zaštitnog zida je da omogući sigurno stvaranje virtuelne veze nekog udaljenog računara sa zaštićenom mrežom.

Nakon što je jednom uspešno uspostavljena, virtuelna privatna mreža je zaštićena od neovlašćenog korišćenja sve dok su enkripcijske tehnike sigurne. Koncept virtuelne privatne mreže omogućava udaljenim korisnicima na nezaštićenoj strani da direktno adresiraju računare unutar lokalne mreže, što drugim korisnicima nije moguće zbog preslikavanja mrežne adrese i filtriranja paketa. Brzina kojom takvi udaljeni računari komuniciraju sa lokalnim računarima mnogo je sporija od one koju računari u lokalnoj mreži koriste.



**Skeniranje portova**

Najčešće korišćene tehnike napada na umrežene računare jesu skeniranje portova (engl. port scanning) i analiza mrežnog saobraćaja.Ove tehnike upotrebljavaju i administratori kako bi otkrili potencijalne sigurnosne propuste ili neželjeni saobraćaj na mreži.Skeniranje portova je tehnika slanja ispravnih ili neispravnih (loše formatiranih) ICMP, UDP i TCP paketa računaru čiju sigurnost ispitujemo.

Na osnovu odgovora računara na te pakete mogu se odrediti otvoreni portovi, dostupni mrežni servisi i vrsta operativnog sistema. Pomoću ove tehnike možete proveriti da li ste mrežnu barijeru ispravno konfigurisali, tj. da li su na njoj zatvoreni svi portovi osim onih koji moraju biti otvoreni.

****Jedan od najpoznatijih programa za skeniranje portova jeste nmap. Nmap obezbeđuje različite metode skeniranja; pri tome možete navesti opseg portova koje želite da skenirate, pojedinačne IP adrese, opseg adresa i vreme skeniranja.

**Napadi na firewall**

Načini da se napadne i zaobiđe firewall su:

* Kriptoanaliza,
* Napad preko određenih virusa,
* Pogađanje lozinke,
* Ponavljanje poslatih poruka,
* Napadi kroz sadržaj i pasivni napadi,
* Napadi kroz spoljne sisteme,itd…