MREŽNE BARIJERE

Firewall

FIREWALL

Firewall je sigurnosni element smešten između neke lokalne mreže i javne mreže (Interneta).

Osnovna namena je da spreči neautorizovani pristup sa jedne mreže na drugu (zaštita unutrašnje mreže od interneta).

Dizajniran je kako bi zaštitio poverljive, korporativne i korisničke podatke od neautorizovanih korisnika

Firewall pravila:

DOZVOLJAVANJE SAOBRAĆAJA

BLOKIRANJE SAOBRAĆAJA

TRAŽENJE POTVRDE KORISNIKA DA SE PROPUSTI ILI NE PROPUSTI ODREĐENI SAOBRAĆAJ

Karakteristike Firewall-a

- Saobraćaj prolazi kroz firewall
- Dozvoliće prolazak ovlašćenom saobraćaju
- Imun je na prodore i pruža 4 kontrole:
    1) Kontrola servisa
    2) Kontrola smera
    3) Kontrola korisnika
    4) Kontrola ponašanja

Mogućnosti Firewall-a

- Definiše jedinstveno usko grlo – koje zadržava neovlašćene korisnike van zaštićene mreže, zabranjuje servisima da ulaze u mrežu ili da je napuštaju, štiti od lažiranja IP adresa...
- Obezbeđuje lokaciju za nadgledanje događaja vezanih za bezbednost – mogu se implementirati praćenja i upozorenja
- Pogodan je za nekoliko Internet funkcija koje nisu vezane za bezbednost – (prevođenje mrežnih adresa, funkcije upravljanja mrežama...)
- Može da služi kao platforma za Ipsec – putem tunelovanja firewall može da se koristi za implementiranje VPN-a

Ograničenja Firewall-a

- Ne može da štiti od napada koje zaobilaze FW
- Ne može da pruži punu zaštitu od unutrašnje pretnje
- Nepravilno obezbeđenom WLAN-u može da se pristupi izvan organizacije
- Prenosivi uređaji mogu da se zaraze spolja i onda uključe u mrežu

Slabosti Firewall-a koji filtrira pakete

- Ne mogu da spreče napade koji iskorišćavaju slabosti i funkcije
- Funkcionalnost filtriranja je ograničena
- Ne podržava napredne šeme za autentifikaciju
- Osetljive su na napade koje iskorišćavaju probleme iz TCP/IP specifikacije
- Osetljive su na provale bezbednosti

Protivmere Firewall-a za napade

- Lažiranje IP adrese
- Napadi rutiranjem iz izvora
- Napadi sitnim fragmentima

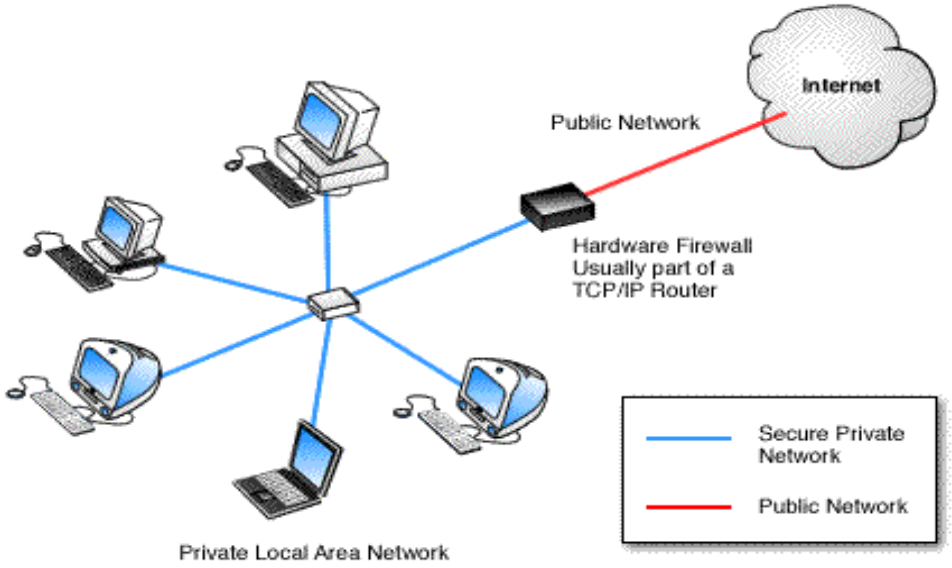
Firewall na računaru

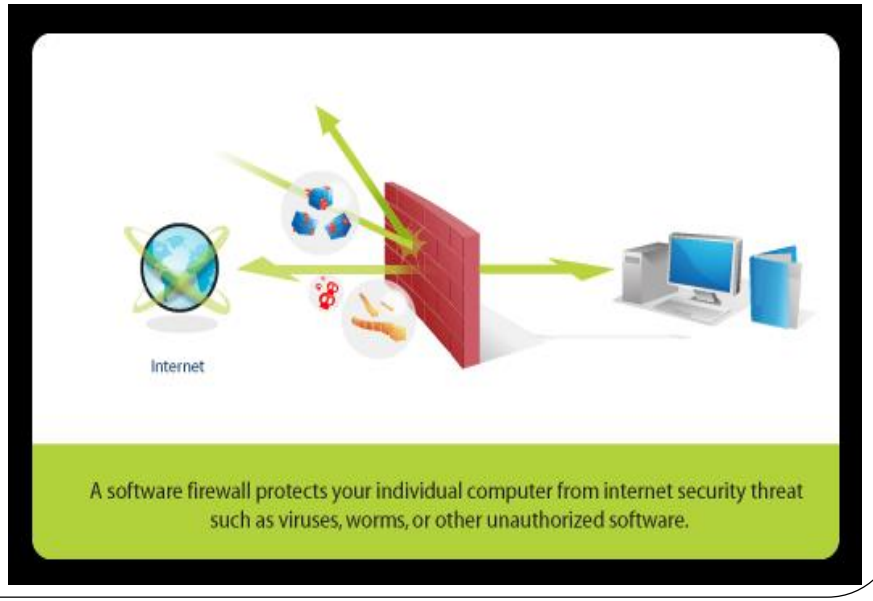
- Pravila filtriranja mogu da se kroje prema okruženju računara
- OBEZBEĐUJE SE ZAŠTITA NEZAVISNO OD TOPOLOGIJE
- Ako se koristi u kombinaciji sa samostalnim FW, FW na računaru pruža dodatni sloj zaštite

HARDVERSKI FIREWALL

Može se naći kao poseban uredjaj, ali češće se nalazi u širokopojasnim ruterima.

Većina ima najmanje 4 priključka. Koristi filtriranje paketa tako što ispituje zaglavlje da bi odredio izvor i odredište. Štiti unutrašnju mrežu. Primeri: Cisco pix, natscreen, watchfuard...





SOFTVERSKI FIREWALL

Za individualne korisnike bolje rešenje je softverski firewall.

Instalira se kao svaki drugi softver, može se ručno konfigurisati, dozvoljava kontrolu nad svojim funkcijama i mogućnostima zaštite.

Štiti od neautorizovanog daljinskog pristupa, malverskih programa, nebezbednih aplikacija koje se realizuju, kontroliše instaliranje fajlova i deljenje štampača, vrši web filtriranje.

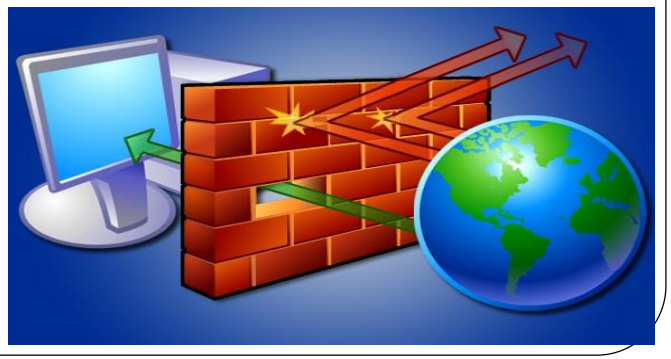
Služi samo za zaštitu računara na koji je instaliran, a ne za mrežu.

Tipovi firewall-a

Firewall-ovi su kategorisani na mrežne i racunarske Firewall-ove.

Računarski Firewall-ovi (host-based) su smešteni na samom mestu gde uredjaj ili računar pristupa mreži (network node).

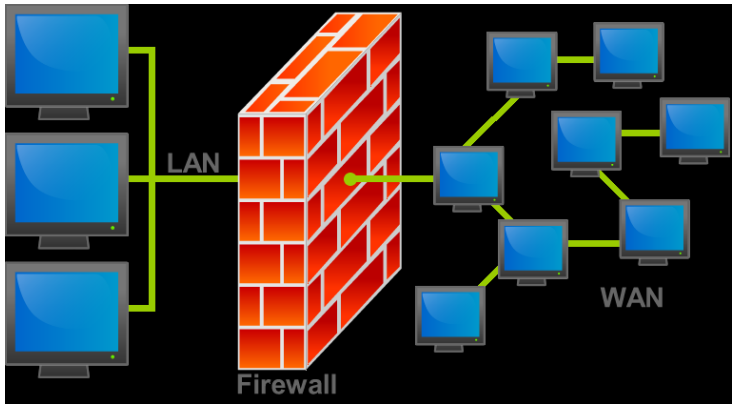
To je deo softvera koji radi samo na jednom uredjaju, kontroliše saobraćaj i može ograničiti dolazni ili odlazni saobraćaj samo za taj uredjaj.



Računarski firewall

Računarski Firewall-ovi za servere i za neke računare koriste sličan set pravila kao mrežni Firewall-ovi, ali uglavnom propuštaju ili odbacuju aktivnost na osnovu liste aplikacija.

Saobraćaj koji se odnosi na aplikacije koje nisu na listi aplikacija, automatski se odbacuje ili propušta, ili se to radi na osnovu povratnog odgovora korisnika na pitanje o izboru dozvole propuštanja te aktivnosti.



Računarski firewall

Mnogi računarski Firewall-ovi uključuju antivirusnu i zaštitu od upada, kao i onemogućavanje iskačućih prozora, ograničavanje mobilnih kodova, blokiranje “kolačića“, i identifikaciju potencijalnih problema unutar web stranica i elektronske pošte.

Mobilni kod je softver koji se salje preko mreže sa udaljenog sistema da bi se pokrenuo na lokalnom sistemu bez instalacije ili kontrole od strane korisnika lokalnog sistema.

Računarski Firewall-ovi su konkretno važni za sisteme koji su povezani na mrežu (internet), a koji nisu zaštićeni mrežnim Firewall-ovima ili drugim mrežnim zaštitnim elementima.

Mrežni firewall

Mrežni (network-based) Firewall-ovi su pozicionirani na mreži izmedju interneta i intraneta.

Rade na osnovu poredjenja mrežnog saobraćaja sa setom pravila, od kojih svako precizira mrežni ili aplikacioni protokol i izvor i odredište podataka.

Prema načinu rada razlikujemo nekoliko vrsta mrežnih firewall-a:

- FILTER PAKETA
- FIREWALL STATEFUL INSPECTION
- CIRCUIT LEVEL GATEWAY
- GEJTVEJ APLIKACIONOG NIVOA
- BEDEMSKI UREDJAJ (Bastion host)

FILTRIRANJE PAKETA

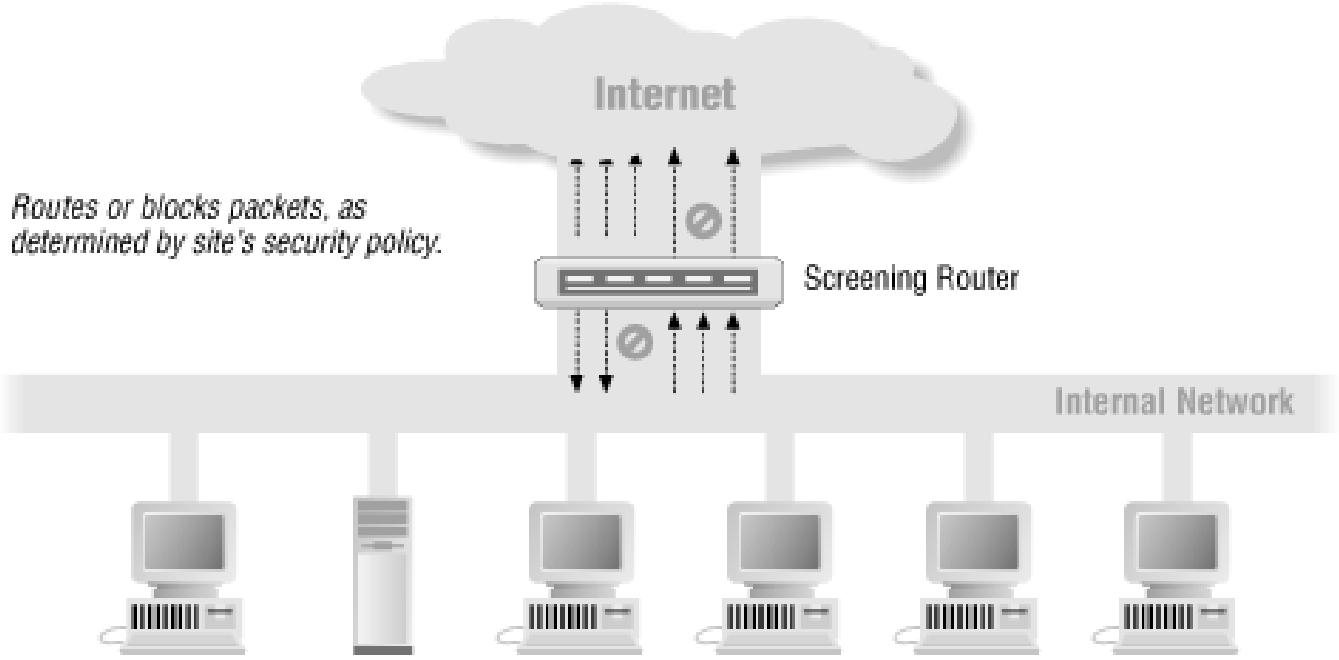
Primenjuje se skup pravila na svaki dolazeći IP paket koji se prosledjuje ili odbacuje.

Filtriranjem paketa se može postići sledeće:

- Proslediti paket ka odredištu
- Odbaciti paket
- Odbiti prosledjivanje paketa uz vraćanje informacije o grešci pošiljaocu
- Skladištiti informacije o paketu
- Alarmirati korisnika o određenom paketu
- Modifikovati paket
- Poslati paket na drugačije odredište od prvobitnog

PREDNOSTI FILTRIRANJA PAKETA

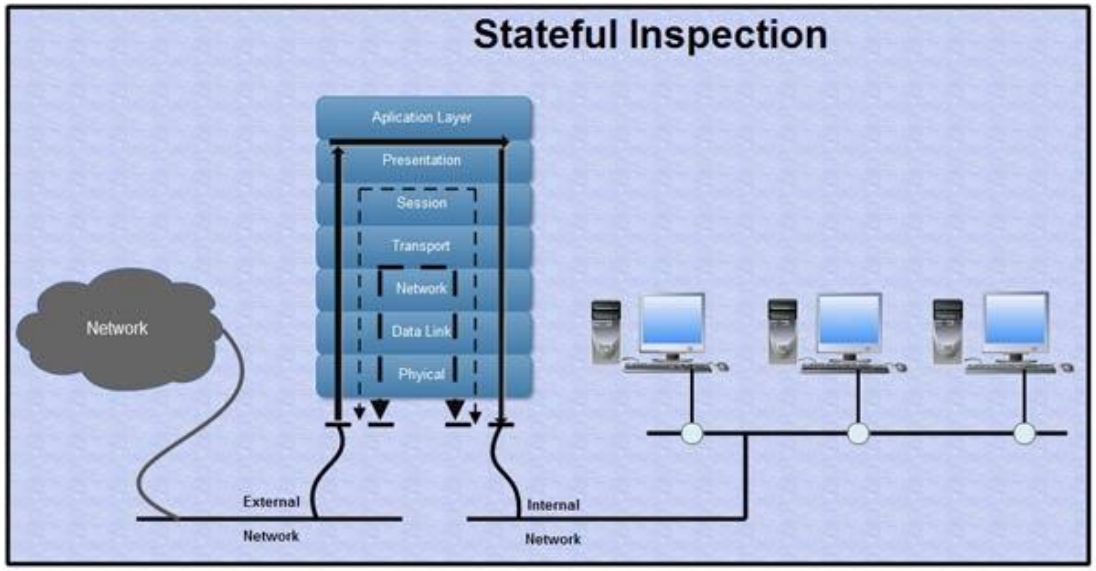
- jedan ruter pomaže zaštiti cele mreže
- „jednostavno“ filtriranje paketa je veoma efikasno
- dostupnost



NEDOSTACI FILTRIRANJA PAKETA

- nesavršenost tehnika filtriranja- ne ispituju podatke gornjih slojeva (ako je dozvoljena aplikacija, dozvoljene su i sve funkcije u toj aplikaciji)
- filtriranje paketa smanjuje performanse rutera
- pojedina pravila ne mogu lako biti primenjena normalnim filtriranjem paketa
- Funkcionalnost evidentiranja je ograničena
- Ne podržavaju svi uređaji napredne tehnike za autentifikaciju korisnika
- Uglavnom su osetljivi na lažiranje adrese u mrežnom sloju

FIREWALL STATEFUL INSPECTION



Kombinuje aspekte:

filtriranja paketa,

circuit level gejtveja i

aplikacionog gejtveja.

Može biti podešen da odbaci pakete koji sadrže specifične komande kao i aplikacioni gejtvej, ali za razliku od aplikacionih gejtveja ne uspostavlja dve posebne konekcije već dopušta direktnu konekciju između klijenta i nepoznate strane.

FIREWALL STATEFUL INSPECTION

Firewall stateful inspection je popularno rešenje za bezbedne Internet i Intranet konekcije jer je transparentan korisnicima, analizira podatke sa najvišeg sloja OSI modela i ne zahteva modifikovanje klijenta ili pokretanje posebnog proksija za svaki servis koji radi preko firewall-a.

Jedan od najpopularnijih komercijalnih firewall-a je FireWall-1 koji je proizvela kompanija Point Software Technologies, i taj firewall je stateful inspection.

Ovakav firewall nudi bolju zaštitu od gejtveja circuit level

CIRCUIT LEVEL GEJTVEJ (PROXY)

Može raditi kao samostalni sistem, ali uglavnom nije tako.

Radi na transportnom nivou OSI modela, ili izmedju transportnog i aplikacionog nivoa TCP/IP steka.

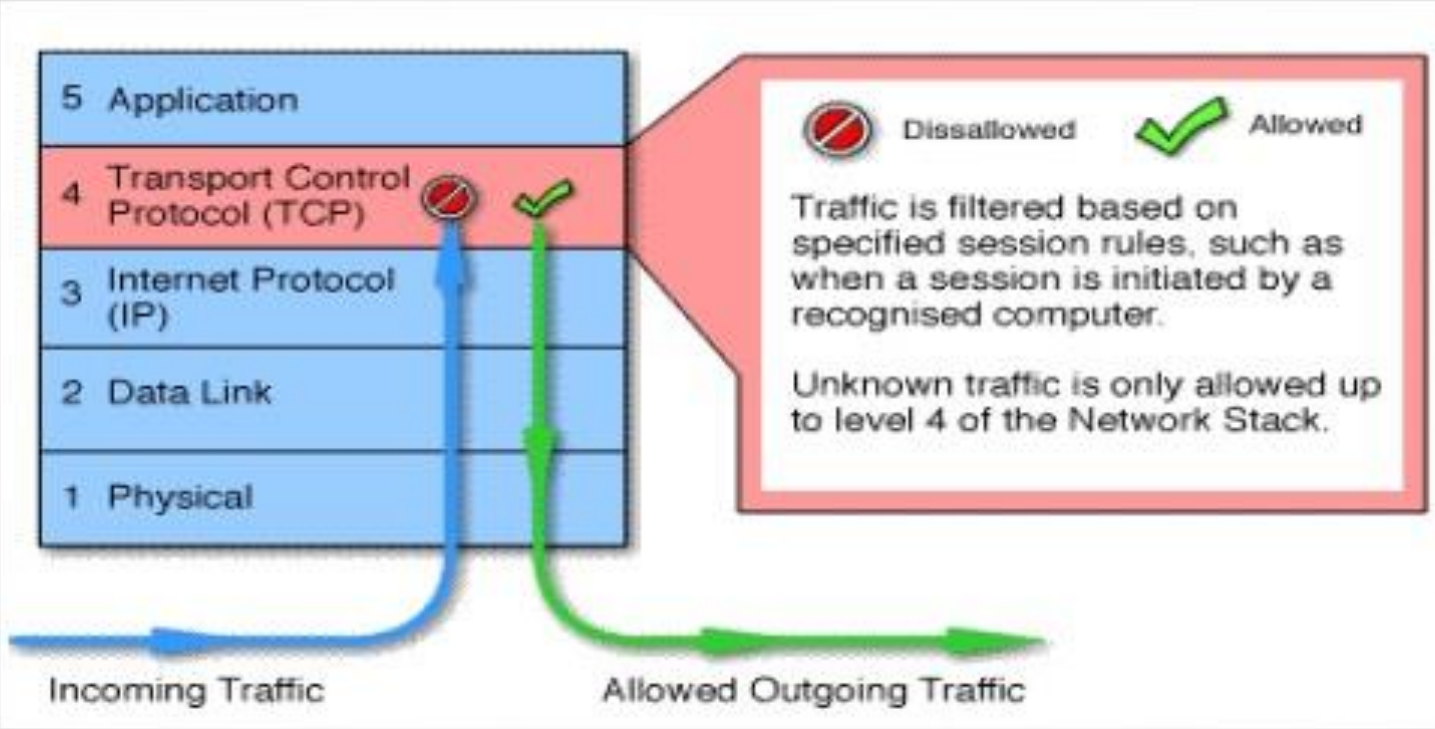
Posmatra TCP rukovodjenje izmedju paketa, izmedju lokalnog i udaljenog uredjaja, da bi odredio legitimnost uspostavljene sesije, odnosno da li je udaljeni sistem bezbedan.

CIRCUIT LEVEL GEJTVEJ

To radi tako što gejtvej prihvati zahtev klijenta, procenjuje da li zahtev zadovoljava uslove, zatim glumeći klijenta, gejtvej otvara vezu sa neproverenim uredjajem i onda prati TCP uspostavu veze.

Gejtvej odredjuje da je sesija legitimna samo ako su SYN, ACK oznake i broj sekvence u uspostavi veze logični i tada uspostavlja konekciju.

Circuit Level



CIRCUIT LEVEL GEJTVEJ

Ne dopušta TCP vezu sa kraja na kraj već podešava dve konekcije:

- izmedju sebe i TCP korisnika na uredjaju unutar mreže
- izmedju sebe i TCP korisnika na uredjaju van mreže

Gejtvej održava tabelu uspostavljenih konekcija.

Funkcioniše i kao proksi server – vrši sakrivanje internih adresa pod jednom “bezbednom” adresom gejtveja.

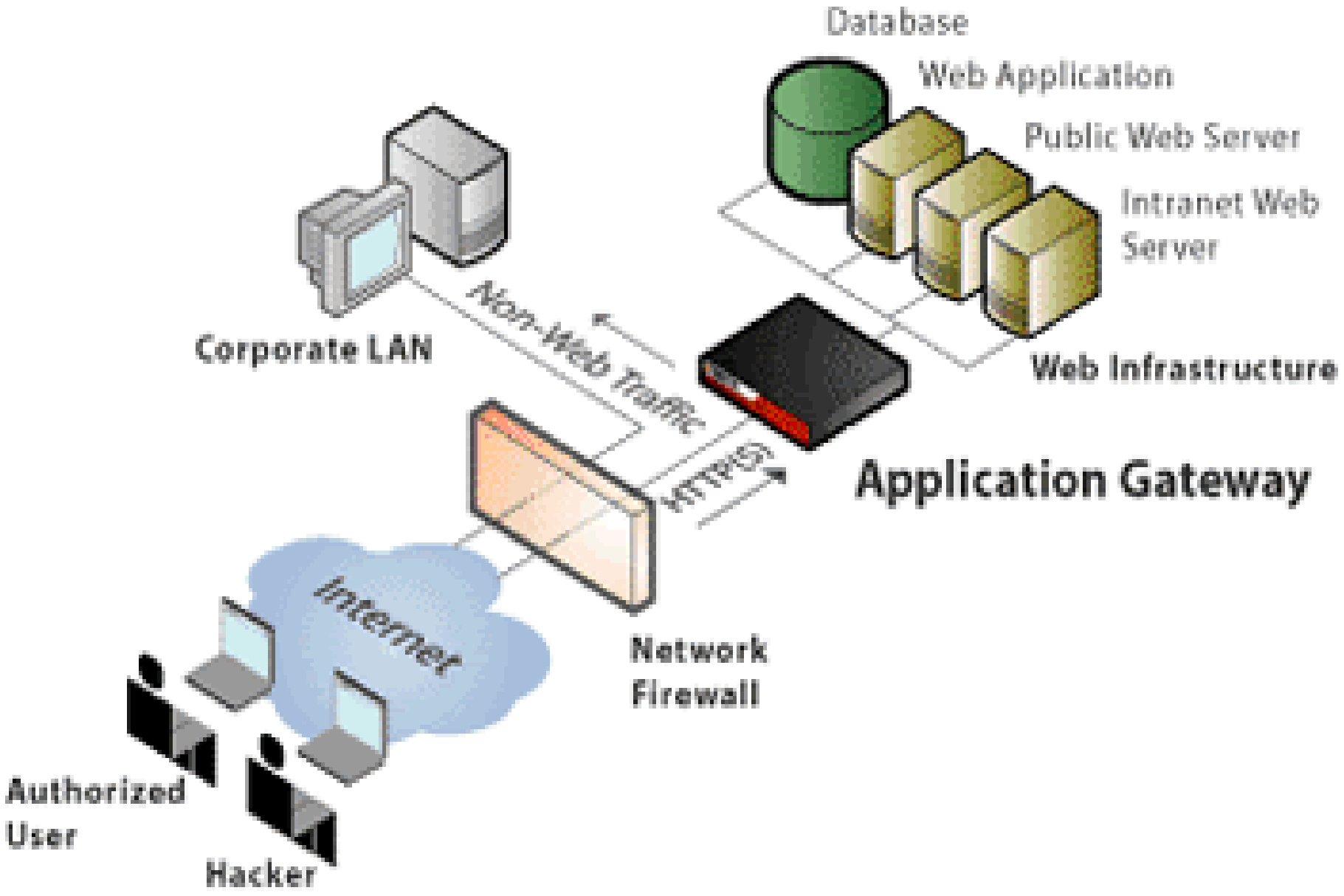
Ne ispituje svaki paket i podatke sa aplikacionog nivoa.

GEJTVEJ APLIKACIONOG NIVOA – APPLICATION PROXY

Presreće pakete, pokreće proksi koji kopira i prosledjuje podatke preko gejtveja i funkcioniše kao proksi server, ne dozvoljavajući direktnu konekciju izmedju klijenta i nepoznate strane.

Proksi kod apliakcionog gejtveja radi različito na dva načina od onog koji koristi gejtvej kružnog nivoa:

- aplikaciono je specifičan
- mogu filtrirati pakete na nivou aplikacije OSI modela


Database
Web Application
Public Web Server
Intranet Web Server
Web Infrastructure
Corporate LAN
Non-Web Traffic
HTTP(S)
Application Gateway
Internet
Network Firewall
Authorized User
Hacker

GEJTVEJ APLIKACIONOG NIVOA

Aplikaciono specifični proksiji prihvataju samo one pakete generisane servisom za koji su napravljeni da kopiraju, prosledjuju i filtriraju.

Ako se mreža oslanja samo na aplikacioni gejtvej, paketi ne mogu proći ako za njihov servis ne postoji proksi kod.

Aplikaciono specifični proksiji proveravaju svaki paket koji prolaze kroz gejtvej, proveravaju sadržaj kroz aplikacioni sloj.

Aplikacioni gejtvej može ograničiti da određene akcije budu realizovane.

Neki prodavci i klijenti tvrde da zaštita aplikacionog gejtveja ima jednu manu – nedostatak transparentnosti.

FIREWALL KAO BEDEMSKI UREDJAJ

To je uređaj posebne namene na mreži koji je dizajnirana i konfigurisan da se suprostavi napadima.

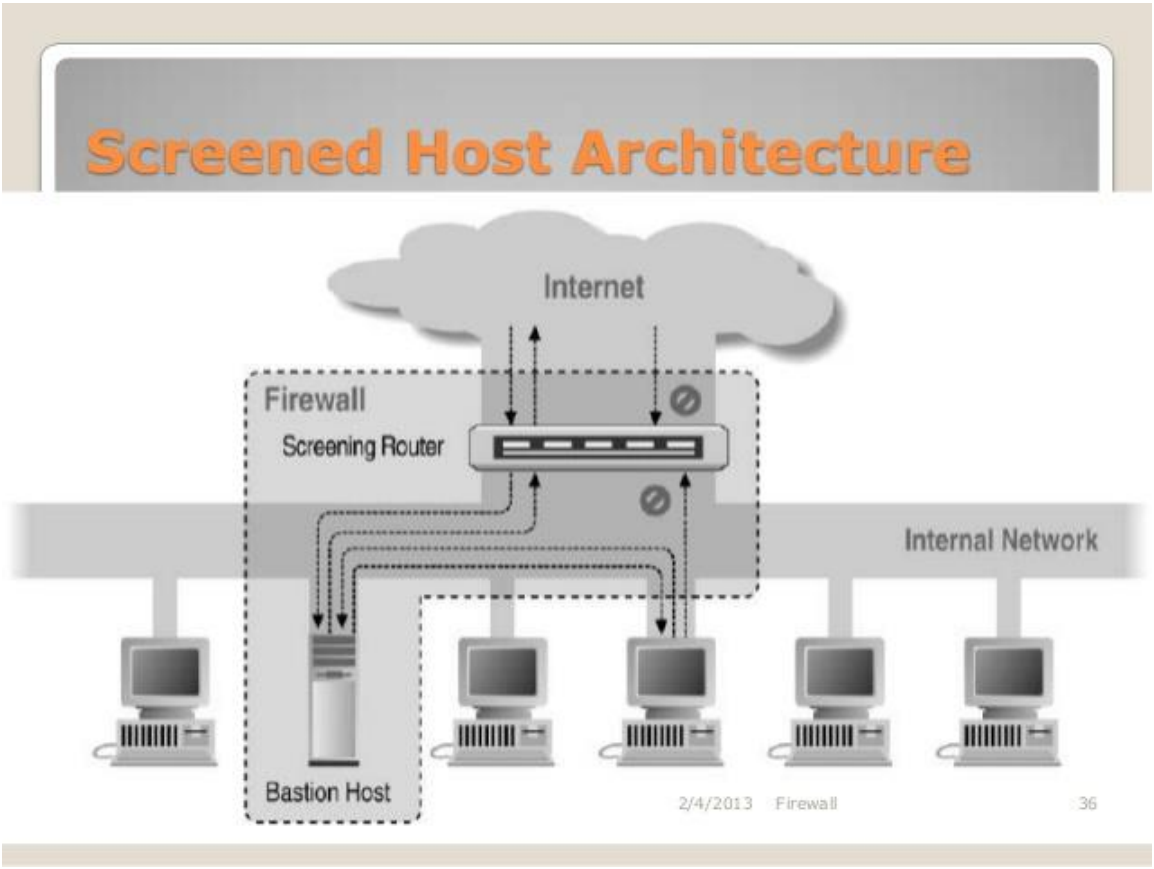
Ovakav sistem je određen da bude kritična jaka tačka u mrežnoj zaštiti. Služi kao platforma za gejtveje apliakcionog i circuit level.

Obezbeđen da izdrži onemogućavanje nezahtevanih sesrvisa i da ih učini jednostavnim.

Bezbedan u primenjivanju separacije između mrežnih konekcija.

FIREWALL KAO BEDEMSKI UREDJAJ

Pokreće gejtveje circuit level i aplikacionog nivoa ili nudi spoljne pristupačne servise.



VRSTE NAPADA

- Address Spoofing napad
- Smurf napad
- Syn-Flood napad
- Port-Scanner napad
- Ping-of-Death napad

Address Spoofing

- Uljez šalje paket prosleđen sa spoljašnjeg okruženja koji u polju IP adrese izvora ima adresa nekog računara unutar lokalne mreže.
- Ovo je čest napad na firewall-ove koji filtriraju pakete
- Protivmera je odbacivanje paketa koji stižu na spoljni interfejs, a imaju unutrašnju izvornu adresu

Smurf

- Spada u grupu napada koje imaju za cilj onemogućavanje rada pojedinih servera i računara, tzv. DoS napad.

Syn-Flood

- Zasniva se na napadačevom slanju velikog broja početnih konekcijskih TCP paketa koji imaju postavljenu SYN zastavicu, i ignorisanjem TCP odgovora sa postavljenim SYN i ACK zastavicama.

Port-Scanner

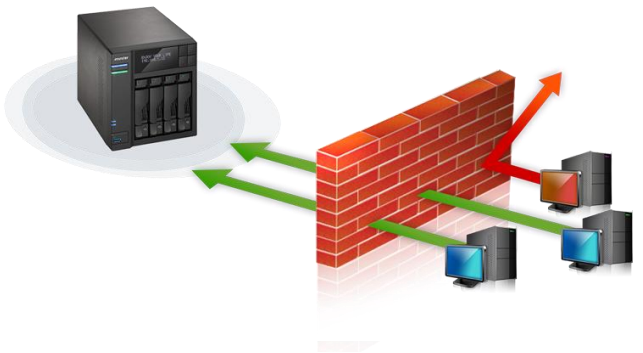
- Zasniva se na otkrivanju otvorenih TCP i UDP portova slanjem SYN ili FIN paketa na ciljane portove i čekanjem na RST odgovor.

Ping-of-Death

- Može uzrokovati rušenje operativnog sistema, ukoliko se na računar usmeri veliki broj ICMP echo zahteva.

OSNOVNE FIREWALL KONFIGURACIJE

- Dual-Homed Gateway ("*među-sistemski*")
- Screened Host Gateway ("*zaklonjeni*")
- Firewall-i zasnovani na host-u
- Izolacijske mreže



Međusistemski

- Firewall 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).

Zaklonjeni firewall

- Sastoji se od bar jednog rutera i bastion hosta sa jednostrukim mrežnim interfejsom. Ruter se tipično konfiguriše da blokira sav saobraćaj do unutrašnje mreže tako da je bastion host jedini računar kome se može spolja pristupiti.

Firewall-i zasnovani na host-u

- U ovom slučaju se koristi računar umesto rutera. To nudi mnogo više mogućnosti praćenja aktivnosti koje se odvijaju preko firewalla.

Izolacijske mreže

- Vrlo su slične firewall-ima zasnovanim na hostu, osim što se između privatne mreže i Interneta ne postavlja host nego mreža.