XIII – Karakteristike mrežnih barijera

S A D R Ž A J

8.1 – Osnovni pojmovi

- Zaštitini zid (*firewall*) vrši zaštitu računara na osnovu filtriranja,analize i provere paketa podataka koji prenose informacije od i u LAN mrežu
- Namena je da zaštiti poverljive korisničke podatke od neautorizovanih korisnika **blokiranjem** i **zabranom** saobraćaja prema nekim pravilima
- ***Firewall*** može biti softverski ili hardverski.
- **Softverski *firewall*** obično štiti jedan računar, osim u slučaju kada je taj računar predodređen za zaštitu čitave LAN mreže.
- **Hardverski *firewall*** štiti čitavu LAN mrežu ili određeni broj računara
- Za ispravan rad *firewall*-a, potrebno je precizno odrediti niz pravila koja određuju kakav saobraćaj je dopušten, a kakav zabranjen.
- On omogućava pristup samo onima kojima smo to dopustili, a svi ostali su onemogućeni i njihovi pokušaji pristupa se samo beleže.
- Prilikom podešavanja *firewall*-a potrebno je pažljivo razmotriti koji saobraćaj smatramo poželjnim a koji ne
- Dobro konfigurisan *firewall* automatski dopušta aplikacijama pristup Internetu ili pristup pojedinim serverima preko definisanih protokola i portova i obrnuto.

8.1 – Osnovni pojmovi

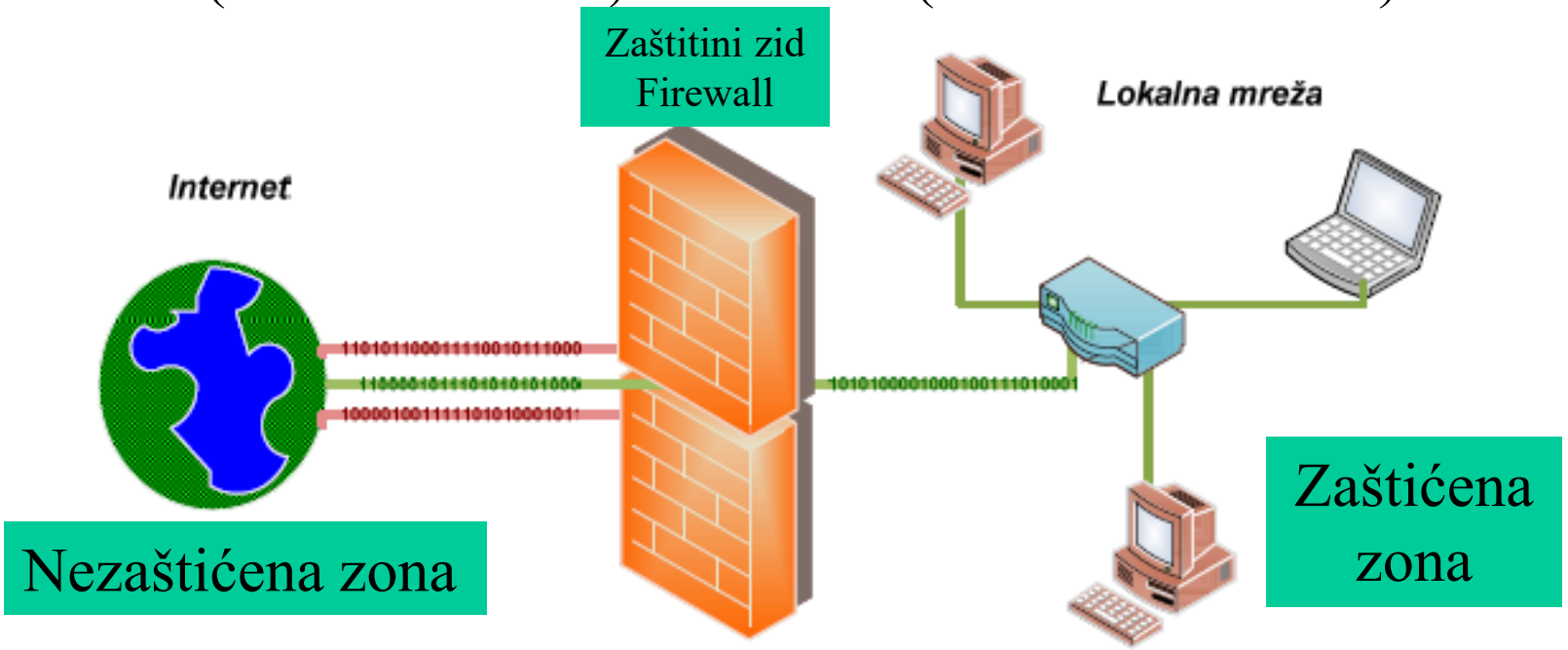
- Gotovo svi antivirusni programi sadrže i softverski *firewall*
- Na Internetu je dostupan veći broj *firewall* programa koje korisnik može instalirati na vlastiti računar i podesiti prema svojim potrebama:
- **Besplatne verzije**:
  - ✓Outpost: **http://www.outpost.com**,
  - ✓Comodo: **https://www.comodo.com/home/internet-security/firewall.php**,
  - ✓ GlassWire: **https://www.glasswire.com/**,
  - ✓Zone alarm: **http://www.zonealarm.com**,
  - ✓Kerio: **http://www.kerio.com**,
  - ✓Sygate: **http://www.sygate.com**.
- **Probne** (*trial*) verzije:
  - ✓Sygate Personal Firewall Pro 5.0 https://uk.pcmag.com/firewalls/30074/sygate-personal-firewall-pro-50
  - ✓Norton Personal Firewall **http://www.symantec.com/sabu/nis/npf/**,
  - ✓Black Ice Defender from NetworkICE **http://www.networkice.com**.

8.1 – Osnovni pojmovi

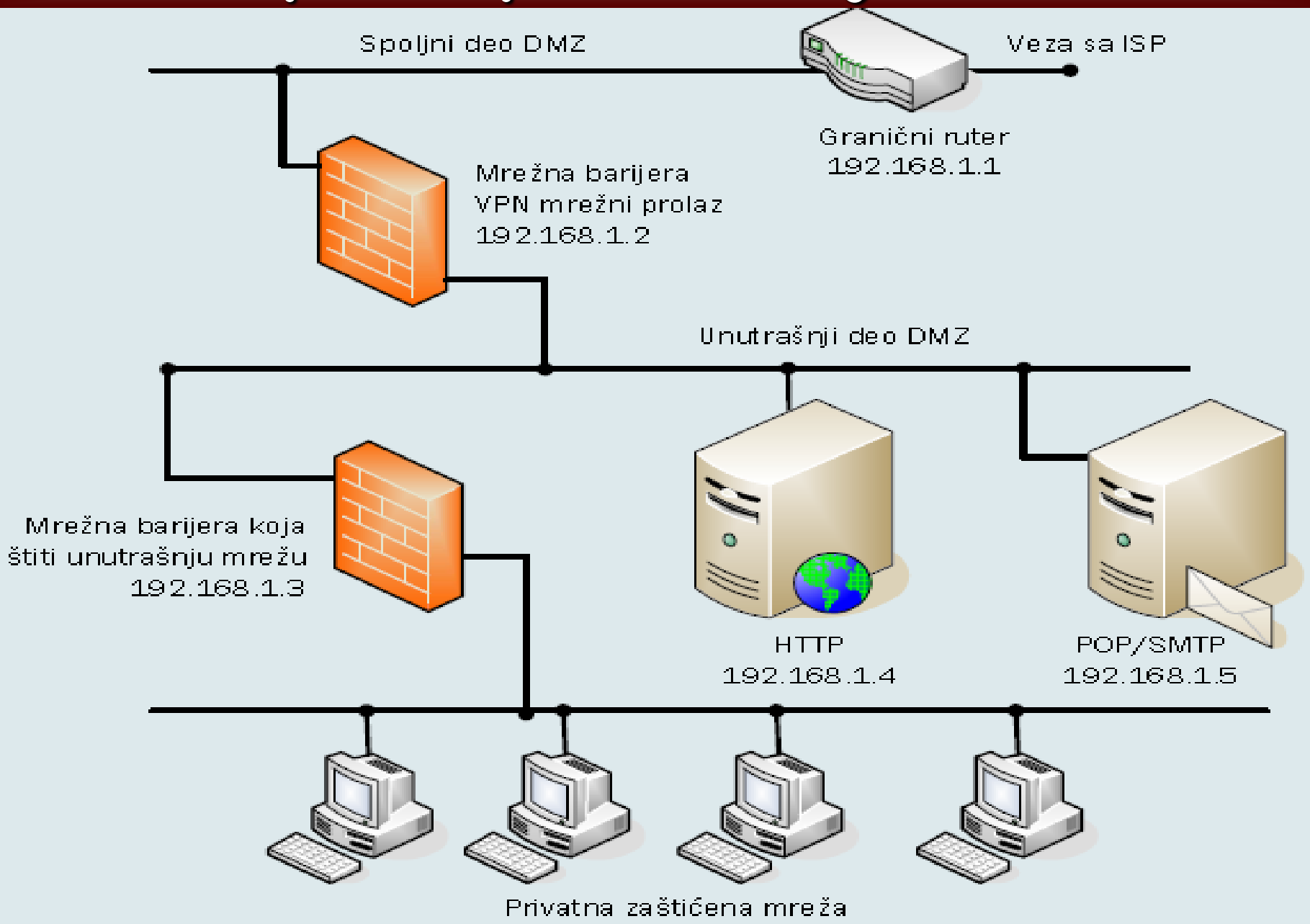
- *Firewall* je sigurnosni element smešten između LAN-a i javne mreže
- Svi korisnici u LAN-u ne moraju da imaju ista prava pristupa Internetu
- Postavljanjem *Firewall* uređaja između dva ili više mrežnih segmenata kontrolišu se i prava pristupa korisnika pojedinim delovima LAN-a
- *Firewall* predstavlja idealno rešenje za kreiranje VPN mreže
- Stvarajući virtualni tunel kroz koji putuju šifrirani podaci omogućuje se sigurna razmena osetljivih podataka imeđu dislociranih korisnika.
- *Firewall* je servis koji se tipično sastoji od ***firewall*** uređaja i ***Policy***-a (pravilnika o zaštiti), koji omogućuje korisniku filtriranje određenih tipova mrežnog saobraćaja kako bi povećao sigurnost na mreži.
- Vrlo jednostavni *firewall*-ovi implementirani su da na niskom nivou pregledaju pakete i na osnovu pravila preduzimaju neke aktivnosti
- Osnovne karakteristike su **izvorna** i **odredišna adresa** te **mrežni portovi**, a najvažnije aktivnosti su propuštanje i odbacivanje paketa.
- Napretkom Internet tehnologija, ovakvi jednostavni *firewall*-ovi postali su nedovoljni i neotporni na novije oblike napada.

8.1 – Osnovni pojmovi

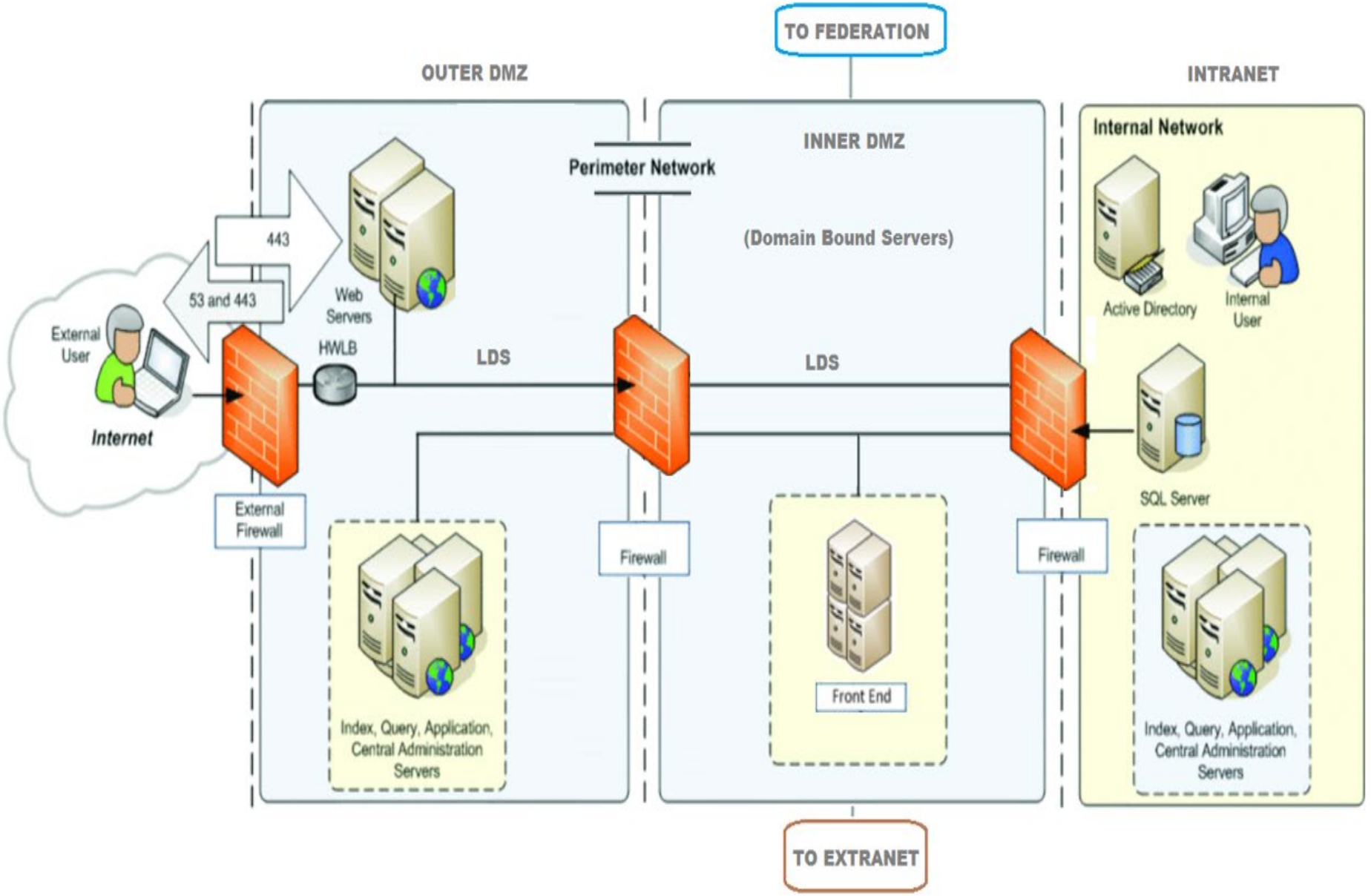
- Uvode se napredniji oblici *firewall* zaštite koji pakete analiziraju na višem aplikativnom nivou i time omogućuju znatno kvalitetniju zaštitu
- To ne znači da se prva grupa *firewalla* ne koriste i danas.
- Oni su toliko značajni da se ugrađuju u jezgra OS zajedno s drugim sigurnosnim i funkcionalnim mehanizmima i neizbežan su alat u borbi protiv stalno rastućih Internet pretnji.
- *Firewall* se može pojednostavljeno prikazati kao mehanizam ubačen između LAN-a (**zaštićena zona**) i Interneta (**nezaštićena zona**)



8.1 – Tipično povezivanje firewall-a



8.1 – Tipično povezivanje firewall-a



8.1 – Ograničenja firewall-a

- ***Firewall*** nije svemoguć i ne može biti jedina mera bezbednosti
- Postoje stvari od kojih **ne može da nas zaštiti**:
  1. korisnik u našoj lokalnoj mreži se može povezati i na neku drugu mrežu (npr. putem WiFi veze) i tako zaobići ***firewall***
  2. ***firewall*** ili ne - ako neko od korinsika u našoj mreži prevarom (***social engineering***) oda poverljive informacije i tako omogući napadaču direktno povezivanje na lokalnu mrežu
  3. **tuneliranjem** se ***firewall*** takođe može zaobići - aplikacija koja svoju komunikaciju maskira u pakete koji izgledaju kao obično surfovanje ili e-mail, a moguće je da bude čak i neka zaražena aplikacija
- Postoji više načina kako se ***firewall*** zaobilazi:
  1. zaposleni u kompaniji može **instalirati backdoor** na računaru,
  2. **nepodešen servis** koji je "odobren" na ***firewallu*** može imati **slabosti**,
  3. napadač može **presresti odobrenu komunikaciju** sa LAN mrežom (***connection hijacking***) i iskoristiti je
- Ipak i pored svojih slabosti, ***firewall*** je nezamenljiv alat u odbrani od hakera, ali nikako ne sme biti jedino sredstvo odbrane od napada

8.2 – Uloga firewall-a

- Da spreči neautorizovani pristup sa jedne na drugu mrežu
- Ako sistem raspolaže *Firewall*-om, to znači da je odluka o tome šta je dozvoljeno, a šta nije - već doneta.
- Odluke su u direktnoj vezi sa politikom sigurnosti informacion.sistema
- Pri planiranju koji će informacioni servisi biti korišćeni, politika sigurnosti direktno određuje opcije konfigurisanja tih servisa.
- Osnova rada *Firewall*-a je kontrola IP paketa između klijenta i servera, čime se ostvaruje kontrola toka za svaki servis po IP adresi i portu
- Za *Firewall* je tipičan i kompromis između sigurnosti i lake upotrebe.
- Stav da "sve što nije dozvoljeno je zabranjeno" zahteva da se svaki novi servis individualno omogućava i konfiguriše.
- *Firewall* je **odgovoran** za više važnih stvari unutar sistema:
  - ✓ Mora da implementira politiku sigurnosti.
  - ✓ Treba da beleži sumnjive događaje.
  - ✓ Da upozori administratora na pokušaje proboja i kompromitovanja politike sigurnosti.
  - ✓ U nekim slučajevima da obezbedi statistiku korišćenja.

8.2 – Firewall usluge

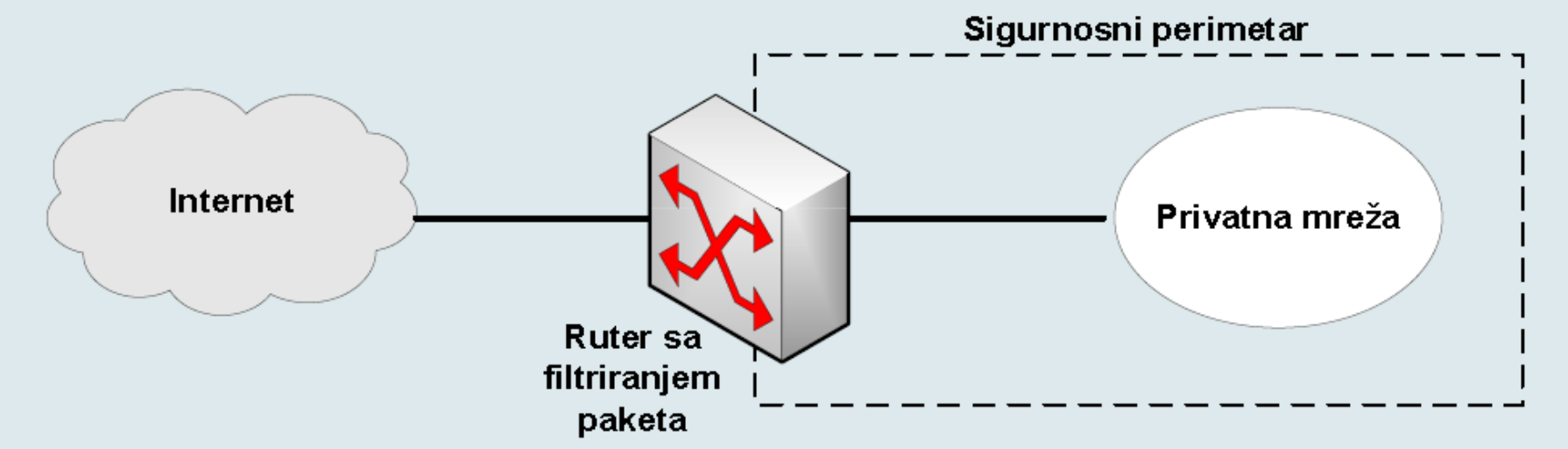
1. ***Filtriranje paketa***: zaglavlje paketa (tip protokola, izvorišna i odredišna adresa, broj porta) se analizira i upoređuje sa pravilima mrežne barijere. U zavisnosti od toga da li paket zadovoljava unapred postvljena pravila, dozvoljava se prolaz paketa ili se on odbacuje.

2. ***Prevođenje mrežnih adresa*** (*network address translation*, NAT): prevodi adrese računara u privatnoj mreži u jednu ili više javnih IP adresa i na taj način sakriva identitet računara u lokalnoj mreži.

3. ***Proksi servisi*** (*proxy*): to je sloj između lokalne i spoljašne mreže koji omogućava većem broju računara da dele jednu vezu ka Internetu i skladišti, odnosno kešira podatke, kako bi se ubrzao pristup tim podacima sa lokalne mreže. Proksi serveri rade na aplikacionom sloju OSI modela, što znači da se svaki klijent mora konfigurisati pojedinačno (navode se adrese proksi servera i port na kome taj server pruža usluge).

8.3 – Filtriranje paketa

- Paketi se analiziraju i upoređuju na osnovu definisanih pravila.
- Filtriranje je moguće na osnovu bilo kog dela zaglavlja paketa a većina filtera donosi odluke na osnovu:
  - ✓ ***tipa protokola***, mrežna barijera odbacuje sve ICMP ili IGMP pakete, a propušta sve TCP ili UDP pakete.
  - ✓ ***IP adrese***, prihvatanje/odbijanje paketa na osnovu IP adrese najjači je oblik zaštite koji se može postići pri prostom filtriranju paketa.
  - ✓ ***TCP/UDP porta***, svim računarima se može dozvoliti da pristupe TCP portu 80(HTTP), dok je pristup TCP portu 22(ssh) dozvoljen samo računarima koji pripadaju određenom opsegu IP adresa.



8.3 – Filtriranje paketa

- Na osnovu definisanih pravila i zaglavlja konkretnog IP paketa, filter paketa može da ***prihvati paket***, ***odbaci paket*** i ***odbaci paket i istovremeno obavesti pošiljaoca*** da njegov paket nije prihvaćen.

1. ***Firewall bez uspostavljanja stanja*** ***(stateless firewall)***, odbacuje paket ukoliko nema dovoljno informacija šta bi sa njim trebalo da uradi. Većina mrežnih barijera ovog tipa ostavlja portove >1024 otvorene, kako bi omogućila slanje odgovora računara koji je poslao zahtev. Ozbiljan sigurnosni propust jer trojanci mogu iskoristiti ove portove.
2. ***Firewall sa uspostavljanjem stanja*** ***(statefull firewall)***: LAN računaru koji odluči da inicira vezu, omogućena je obostrana komunikacija dok je spoljnjem računaru to onemogućeno. *Firewall* dozvoljava da paket prođe u spoljašnju mrežu i pamti informacije iz zaglavlja paketa. Nakon prijema paketa, spoljašnji računar šalje odgovor na specifični port. *Firewall* proverava sve podatke koji su razmenjeni između ta dva računara, pošto zna da je vezu inicirao računar iz LAN-a, dozvoljava računaru iz spoljašnje mreže da odgovori na taj zahtev. Kada učesnici u sesiji zatvore TCP vezu, *firewall* briše zapise iz svoje tabele stanja.

8.4 - Vrste Firewall-ova

- Prema mrežnom sloju na kome obavljaju filtriranje, firewall-ovi se mogu podeliti na sledeće tri kategorije:
  1. **Packet-Filtering Firewall** - funkcioniše na (niskom) **IP nivou** gde proverava svaki pojedinačni paket i to na osnovu nekoliko parametara od kojih su najvažniji: polazna i odredišna IP adresa, kao i izvorni i odredišni port.
  2. **Circuit-Level Gateway** - funkcioniše na nivou **sesije**, odnosno na **TCP sloju**. Ne vrše filtriranje samih paketa, već proveravaju da li je uspostavljena TCP sesija. Sakrivaju lokalnu mrežu od Interneta - na Internetu se vidi samo IP adresa ***gateway*** uređaja (rutera ili računara).
  3. **Application-Level Firewall** - funkcionišu na **najvišem nivou** i koncentrišu se na to koja aplikacija pokušava da komunicira putem mreže. Mogu da rade i kao **proxy** keš serveri, koji pamte rezultate zahteva za istim podacima i time ubrzavaju rad sa Internetom
- Naravno, različiti tipovi **firewall-a** ne isključuju jedni druge.
- U stvari, poželjno je koristiti kombinaciju svih kategorija ***firewall***-ova.

8.4 - Vrste Firewall zaštite

- ***Firewall***-ovi koji nemaju čvrste i stroge politike prema dolaznim paketima podložni su različitim vrstama napada.
- Ukoliko ***firewall*** ne podržava kreiranje VPN-a, a želi da se omogući pristup sa određenih IP adresa LAN-u, moguće je konfigurirati ***firewall*** da propušta pakete sa tačno određenim izvorišnim IP adresama.
- Ovaj način sadrži brojne nedostatke jer napadač može doći do paketa i saznati IP adresu sa kojom je dozvoljeno spajanje na LAN.
- Sada on može kreirati pakete u kojima kao izvorišnu stavlja logičku adresu računara kojem je dozvoljen spajanje sa LAN-om i naneti štetu
- ***Firewall*** je potrebno konfigurisati tako da onemogućava različite postojeće napade.
- Većina današnjih proizvođača *firewall*-a ponosno ističe na koje napade su njihovi *firewall*-ovi otporni, ali nove vrste napada se svakodnevno razvijaju i sve su **komplikovaniji i kompleksniji**.
- Ipak svaki *firewall* bi trebao biti otporan na poznate napade kao što su:

8.4 – Vrste Firewall zaštite

1. ***Address Spoofing*** - napad omogućava da paket bude prosleđen sa spoljnog okruženja na neki od internih računara ukoliko napadač kao izvorišnu adresu uzme neku od adresa unutar LAN-a. Onemogućiti prosleđivanje paketa koji kao izvorišnu adresu imaju neku od LAN adresa, a dolaze sa spoljne mreže – Internet-a.
2. ***Smurf*** napad spada u grupu DoS napada. Napadač šalje ICMP echo request paket na *broadcast* adresu cele lokalne mreže. Dovoljno je u konfiguracijskoj datoteci ***firewall***-a onemogućiti ***broadcast*** paket.
3. ***Syn-Flood*** napadač šalje veliki broj početnih konekcijskih TCP paketa koji imaju postavljen SYN bit a ignoriše TCP odgovore sa postavljenim SYN i ACK bitovima. Time su resursi ciljanog računara zaokupljeni odgovaranjem na pakete. Da bi se sprečio ovakav oblik napada potrebno je ograničiti na ***firewall***-u broj dolazećih TCP paketa.
4. ***Port-Scanner*** otkrivanje otvorenih TCP i UDP portova slanjem SYN ili FIN paketa na ciljane portove i čekanjem na RST odgovor.
5. ***Ping-of-Death*** napad može uzrokovati rušenje OS, ukoliko se na računar usmeri veliki broj ICMP ***echo*** zahteva.

8.4 – Zaštita od lokalnih korisnika

- Prilikom konfigurisanja *firewall* najveća se pažnja posvećuje paketima
- Sve više komercijalnih *firewall*-a omogućava bolju kontrolu rada ljudi
- Oni su konfigurisani na način da ne dozvoljavaju lokalnim korisnicima pristup određenim Web sajtovima: porno, stranice koje propagiraju mržnju, stranice za skidanje raznih video i audio zapisa, itd...
- Sa obzirom na činjenicu da takve stranice sve češće nastaju potrebno je osvežavati podatke unutar *firewall-a*.
- Prilikom konfiguracije *firewalla* moguće je primeniti različita pravila ograničenja spajanja lokalnih korisnika na Internet.
- Prvi koncept bio bi da se prema svim korisnicima LAN-a jednako odnosi, tj. da su svi u istom položaju.
- Moguće je LAN računare svrstati u klase i na taj način samo jednom sektoru omogućiti nesmetani pristup Internetu, a ostalim ograničen
- *Firewall* može biti konfigurisan na način da propušta sve pakete osim paketa koji su usmereni prema računarima sa određenim IP adresama
- Moguće je propustati samo pakete koji dolaze samo od nekih računara iz LAN mreže i obrnuto.

8.5 – Povezivanje Firewall-a

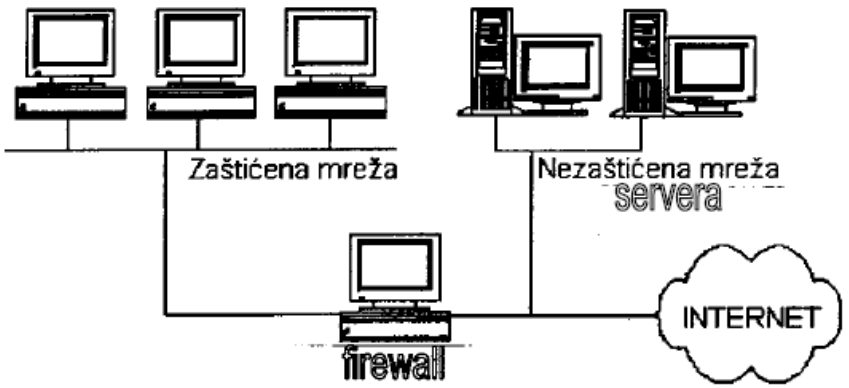
1. MREŽE BEZ SERVERA

- ✓ Kada organizacija koja koristi *firewall* ne pruža nikakve usluge korisnicima Interneta, *firewall* je dovoljno konfigurirati na način da propušta samo pakete koji napuštaju LAN, i pakete koji dolaze kao povratne informacije na osnovu uspostavljenih veza.
- ✓ Ova konfiguracija u odnosu na konfiguracije mreža sa serverima je prvenstveno jednostavnija za konfigurisanje, ali i sigurnija za LAN.
- ✓ Ali danas je takva mreža izrazito nekorisna gledano sa poslovne i informacijske strane, jer se organizacije sve češće ne koncentrišu na jednom mestu, već radnike raspoređuju po udaljenim lokacijama
- ✓ U slučajevima kad je potrebno ostvariti vezu udaljenih lokacija, moguće je uz datu konfiguraciju jedino primeniti fizičko povezivanje udaljenih LAN-ova što je preskupo.
- ✓ Ređe se koristi kod većih organizacija, ali češće kod **malih kućnih mreža**.

8.5 – Povezivanje Firewall-a

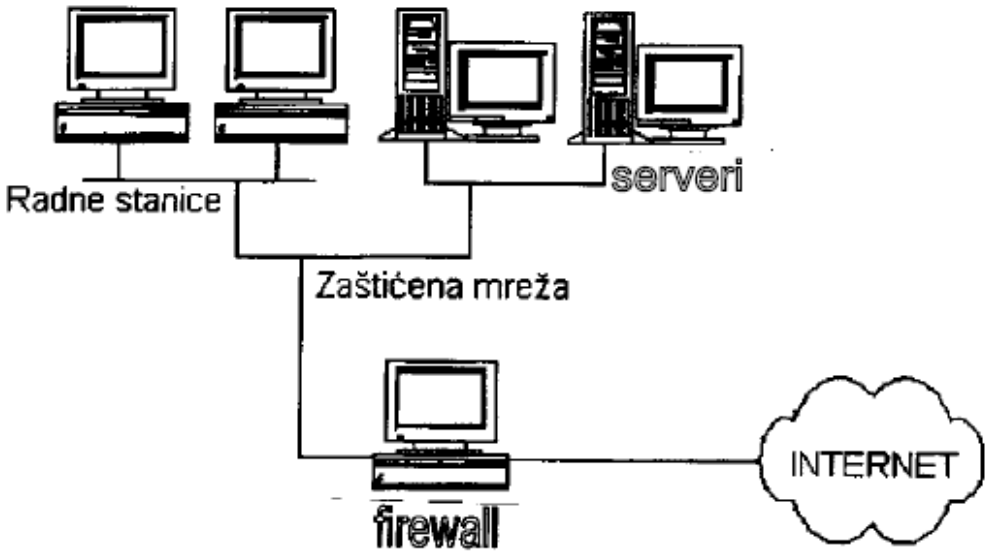
2. MREŽE SA JEDNIM SERVEROM I JEDNIM FIREWALL-OM

- ✓ Ukoliko u LAN-u imamo servere onda je potrebno konfigurisati mrežu i *firewall* na kompleksniji način od prethodnog.
- ✓ Lokalna mreža može biti konfigurisana na način da se koristi samo jedan *firewall* a da se serveri nađu unutar ili izvan lokalne mreže.
- ✓ Ako je LAN konfigurisan na način da su serveri locirani izvan LAN-a, konfiguracija LAN-a i *firewall*-a može u potpunosti biti jednaka kao u slučaju mreže bez servera ali su onda računari locirani izvan LAN-a, koji rade kao serveri, izloženi različitim napadima.
- ✓ Zlonamerni napadači su sada u mogućnosti da izvedu **DoS** napad
- ✓ Za organizaciju je čak puno gore od spomenutog napada ukoliko napadači modifikuju podatke koji su na serveru
- ✓ Napadači mogu podvaljivati lažne vesti serverima, ili čak programe u kojima se nalaze virusi.



8.5 - Povezivanje Firewall-a

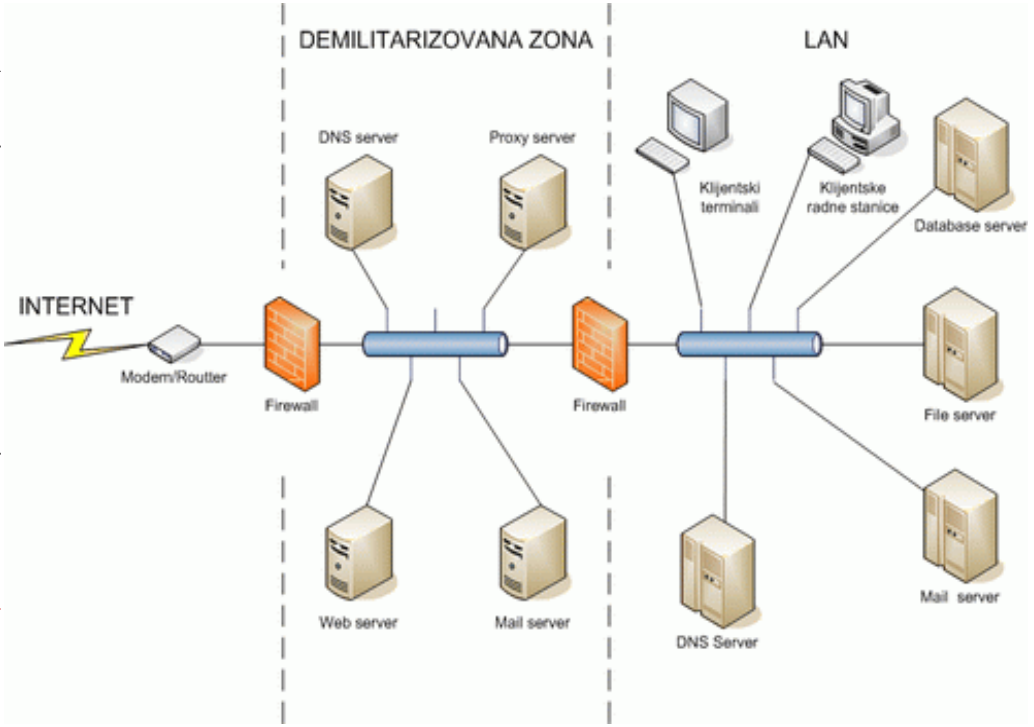
- ✓ U slučaju kada je LAN konfigurisan na način da su serveri locirani unutar LAN-a, konfiguracija lokalne mreže i firewall-a je složenija.
- ✓ Osim dolaznih paketa koji su deo uspostavljene veze potrebno je omogućiti i prolazak početnih paketa samo prema serverima.
- ✓ Konfiguracija LAN-a sa serverima lociranim unutar lokalne mreže ostavlja brojne sigurnosne rupe koje vešti napadači mogu iskoristiti.
- ✓ Napadači mogu iskoristiti konfiguraciju *firewalla* koja propušta i početne pakete kako bi preko servera dospeli do ostalih računara u mreži ili barem saznali određene informacije o njima.



8.5 – Povezivanje Firewall-a

3. MREŽE SA SERVERIMA I DVA FIREWALL-A

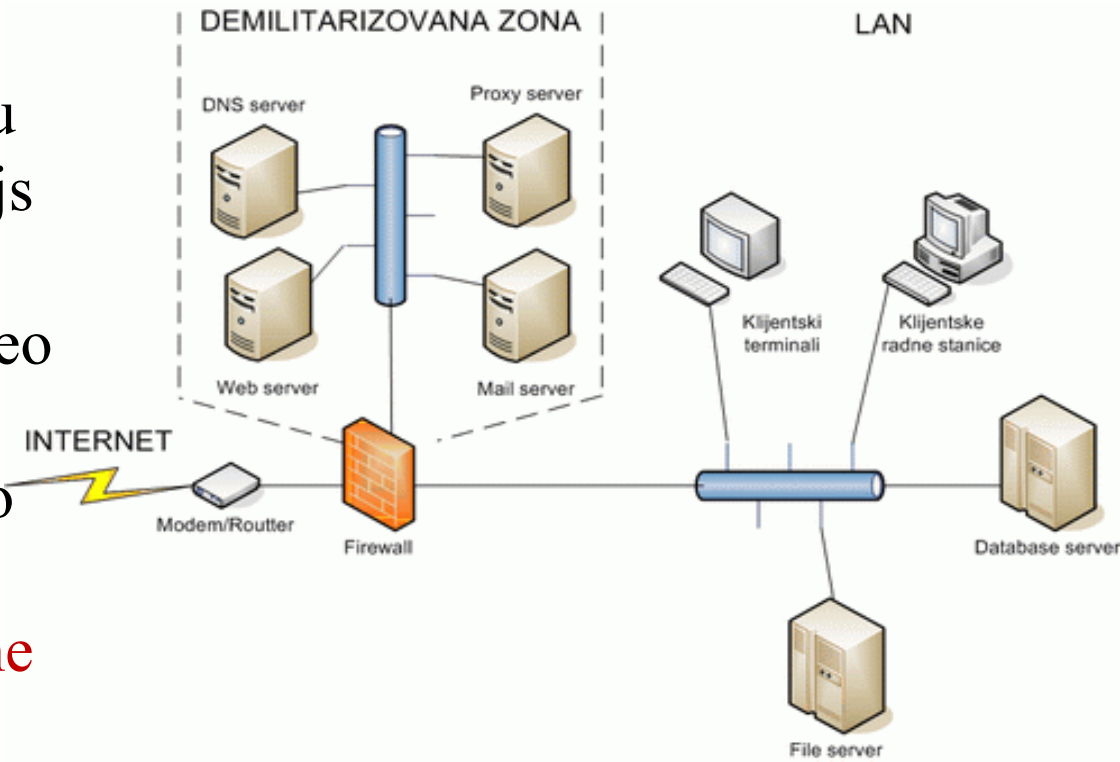
- ✓ Ukoliko organizacija treba LAN sa serverima, onda su prethodna dva opisana rešenja neadekvatna jer omogućavaju različite napade.
- ✓ Korišćenjem dva firewall-a, sprečavaju se različiti oblici napada
- ✓ Prvi *firewall* se spaja na Internet i mrežu servera-spoljna lokalna mreža
- ✓ Između mreže servera i lokalne mreže smešta se drugi *firewall*.
- ✓ Politike propuštanja paketa koju *firewall*-ovi primenjuju su različite.
- ✓ *Firewall* koji štiti unutrašnju lokalnu mrežu propušta prema unutrašnjoj lokalnoj mreži samo one pakete koji su deo neke uspostavljene veze.
- ✓ *Firewall* koji je spojen na Internet mora uz te pakete propuštati i pakete koji su namenjeni serverima.



8.5 – Povezivanje Firewall-a

4. MREŽE SA DEMILITARIZOVANOM ZONOM

- ✓ U prethodnom primeru konfiguracije mreže potrebno je koristiti čak dva ***firewall***-a što poskupljuje i usporava brzinu prenosa podataka
- ✓ Korišćenje konfiguracije sa **demilitariziranom zonom**, koja pruža jednaku funcionalnost, ali bržu i jeftiniju od prethodno opisane.
- ✓ ***Firewall***-u pomoću kojeg se filtrira mrežni saobraćaj dodeljene su dve mreže: interna LAN i mreža servera, tzv. **demilitarizirana zona**.
- ✓ Na ***firewall***-u je potrebno postaviti takvu konfiguraciju koja će propuštati na interfejs prema unutrašnjoj lokalnoj mreži samo pakete koji su deo uspostavljene veze.
- ✓ Prema serverima je potrebno omogućiti slanje početnih paketa i sa unutrašnje lokalne mreže, i sa Interneta.



8.5 - Povezivanje Firewall-a

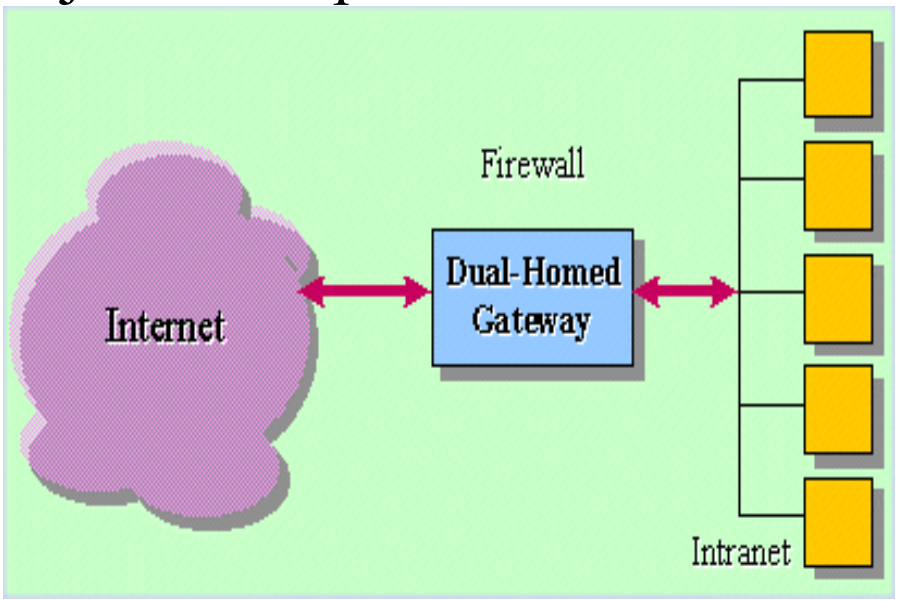
5. **FIREWALL-i ZASNOVANI NA HOSTU**

- ✓ U ovom slučaju se koristi računar umesto rutera.
- ✓ To nudi mnogo više mogućnosti praćenja aktivnosti
- ✓ Dok ***firewall*** zasnovan na ruteru nadgleda pakete na IP nivou, hostovi prenose kontrolu na nivou aplikacije.
- ✓ Da bi se osigurali od potencijalnih problema koji bi se mogli pojaviti zbog propusta u implementaciji sigurnosti u uobičajenoj programskoj podršci za mrežne usluge, ovi ***firewall***-i obično koriste posebne verzije programa koji pružaju podršku potrebnim servisima.
- ✓ To su najčešće ogoljene verzije originalnih programa koje su zbog svoje kratkoće puno jednostavnije za održavanje, pa je i manja mogućnost za slučajne propuste (*bug*-ove) koji narušavaju sigurnost.
- ✓ Nedostatak takvih *firewall-ova* je potreba za posebnom prog.podrškom za svaki od servisa koji treba podržati za mrežu "iza" *firewall*-a
- ✓ Kao dodatna mera zaštite najčešće se koristi kombinacija zaštite na nivou aplikacije i filtrirajućeg rutinga koga takođe obavlja sam host ili spoljni ruter.

8.5 – Načini povezivanja Firewall-a

1. ***DUAL-HOMED GATEWAY*** ("među-sistemski")

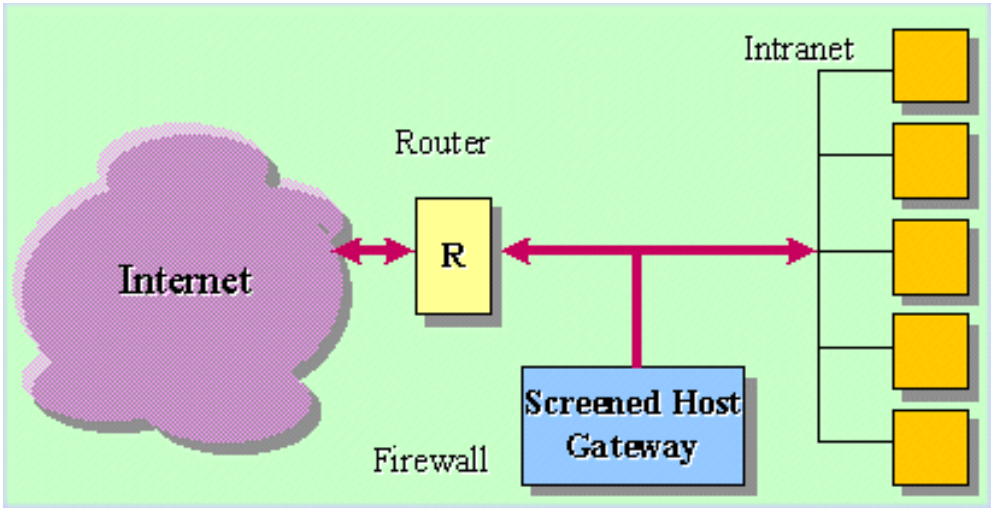
- ✓ Sastoji se od računara sa najmanje dva mrežna adaptera.
- ✓ Ovakav sistem se normalno konfiguriše tako da se paketi ne rutiraju direktno sa jedne mreže (Internet) na drugu mrežu (Intranet).
- ✓ Računari na Internet-u mogu da komuniciraju sa *Firewall*-om, kao i računari sa unutrašnje mreže, ali je direktan saobraćaj blokiran.
- ✓ Glavna mana ***Dual-Homed Gateway***-a je činjenica da blokira direktni IP saobraćaj u oba pravca što dovodi do nemogućnosti rada svih programa koji zahtevaju direktnu putanju TCP/IP paketa.
- ✓ Da bi se rešio ovaj problem, ovi *firewall*-ovi izvršavaju programe pod nazivom **Proxy**, kako bi prosledili pakete između dve mreže.
- ✓ Umesto da direktno razgovaraju, klijent i server "pričaju" sa Proxy-jem koji je transparentan za sve korisnike



8.5 – Načini povezivanja Firewall-a

2. ***SCREENED HOST GATEWAY*** ("zaklonjeni")

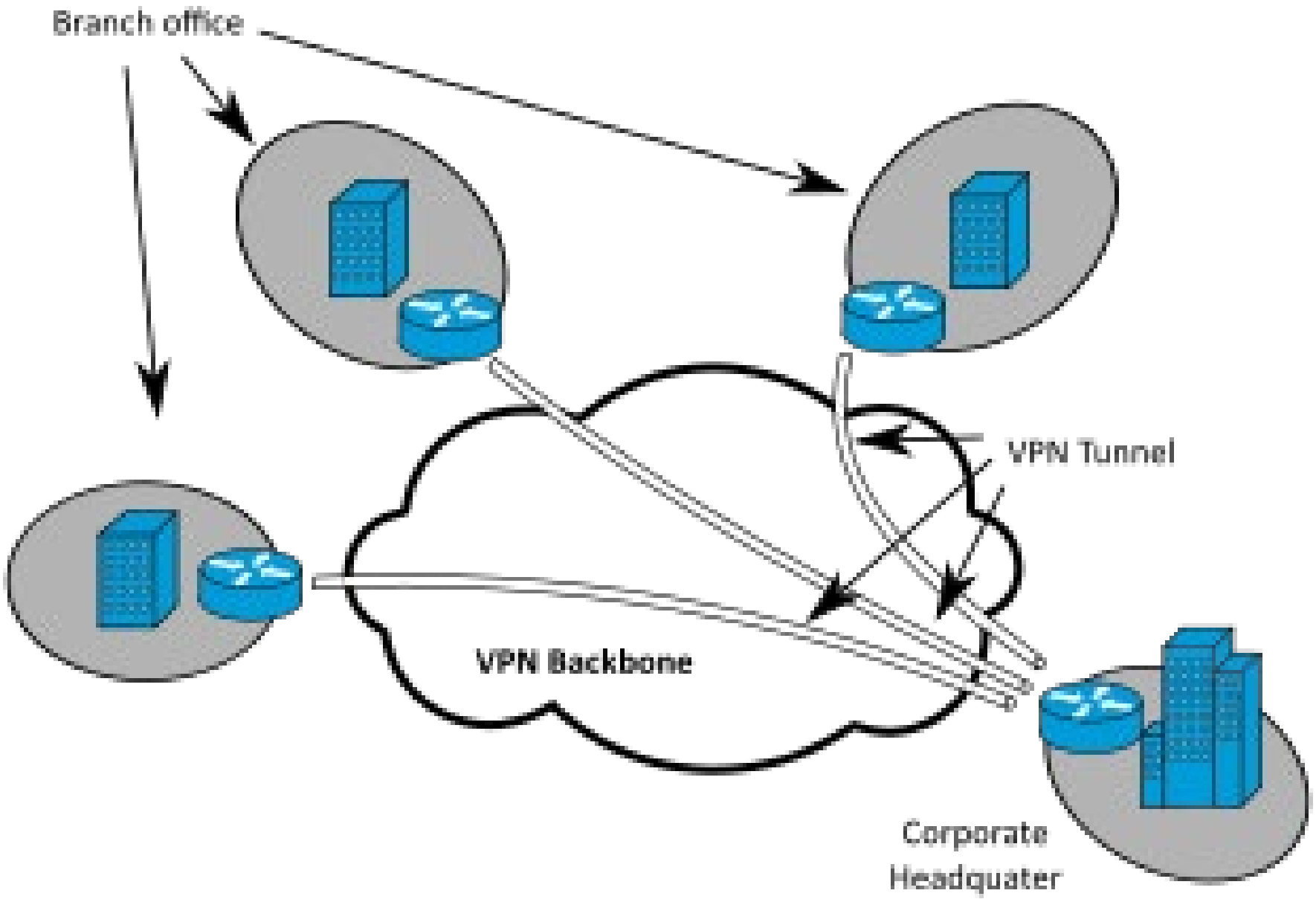
- ✓ Sastoji se od bar jednog rutera i ***bastion hosta*** sa jednostrukim mrežnim interfejsom.
- ✓ Ruter se tipično konfiguriše da blokira sav saobraćaj do unutrašnje mreže tako da je ***bastion host*** jedini računar kome se spolja pristupa.
- ✓ Ovaj *firewall* ne forsira sav saobraćaj kroz ***bastion host***; pomoću konfiguracije rutera moguće je da se otvore "rupe" u *Firewall*-u, tako da postoji prolaz i do drugih računara u okviru unutrašnje LAN mreže.
- ✓ Ruter se konfiguriše tako da dozvoli saobraćaj samo za određene portove na ***bastion hostu***.
- ✓ Ruter se može konfigurisati tako da dozvoljava saobraćaj samo sa određenih spoljnih računara.
- ✓ Često se ruter konfiguriše tako da se dozvoljava prolaz svih konekcija koje su potekle sa unutrašnje mreže.



8.6 - VPN-Virtuelne privatne mreže

- Virtualne privatne mreže (enkripcijski tuneli) omogućavaju sigurno spajanje dve fizički odvojene mreže preko Interneta
- Zadatak *firewall*-a je da omogući sigurno stvaranje virtuelne veze sa nekog udaljenog računara prema zaštićenoj LAN mreži.
- Nakon što je jednom uspešno uspostavljena, VPN je zaštićena od neovlašćenih iskorišćenja sve dok su enkripcijske tehnike sigurne.
- Koncept VPN-a omogućava udaljenim korisnicima na nezaštićenoj strani da direktno adresiraju računare unutar LAN-a, što drugim korisnicima nije moguće zbog NAT-a i filtriranja paketa.
- Brzina kojom takvi udaljeni računari komuniciraju sa lokalnim računarima mnogo je sporija od one koju računari u LAN-u koriste.
- Razlog tome je njihova fizička udaljenost i oslonjenost na brzinu Interneta, ali i procesi enkripcije podataka, filtriranja paketa na *firewall*-u, i dekripcije originalnih podataka.
- Kako bi udaljeni korisnici uspešno prošli fazu spajanja na LAN potrebno je da se uspešno obavi autentifikacija istih koja mora biti šifrovana da bi se sprečila krađa podataka od strane napadača

8.6 - VPN - Virtual Private Network



8.6 – Izolacijske mreže

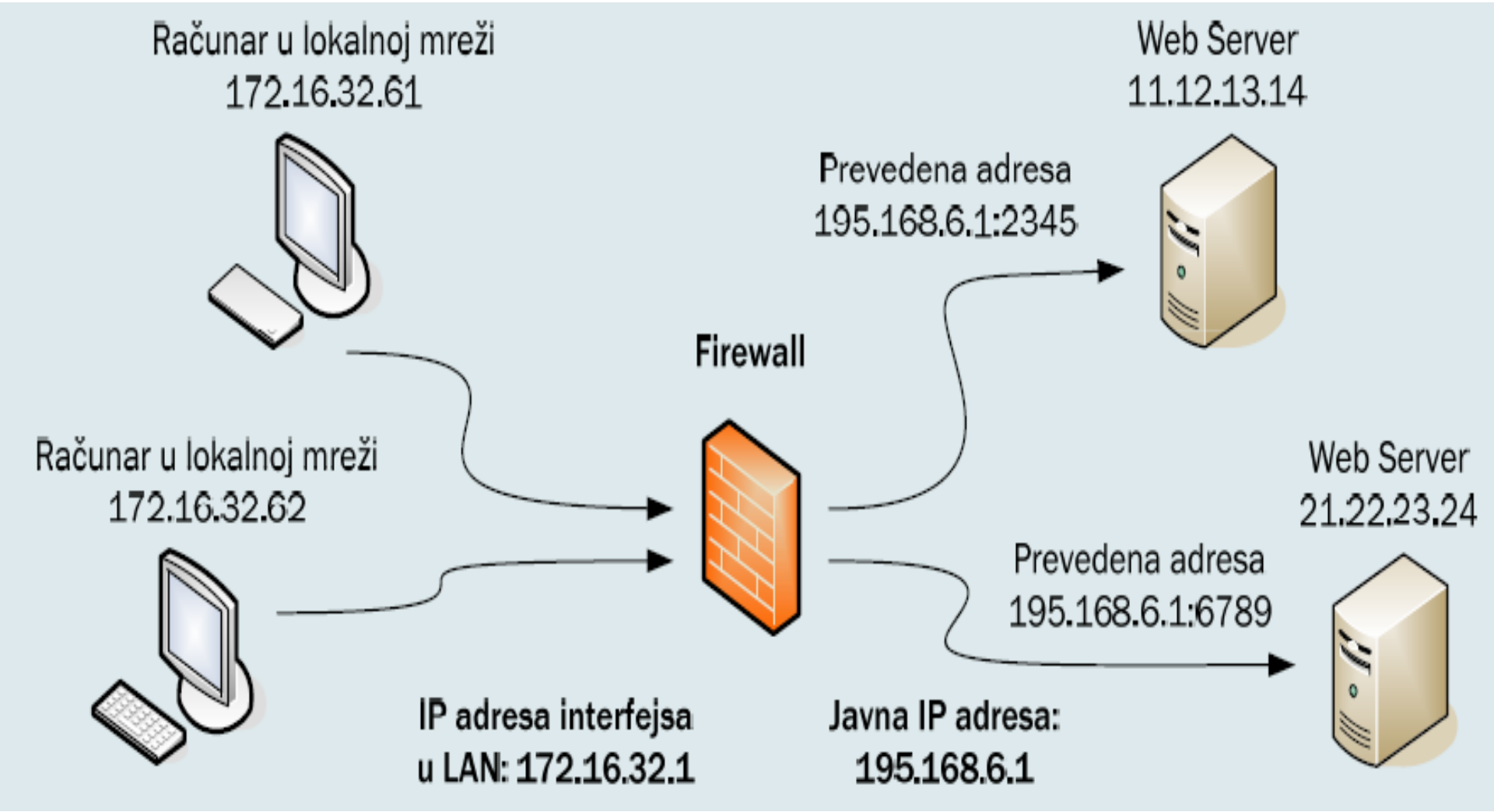
- Izolacijske mreže su vrlo slične *firewall*-ima zasnovanim na hostu, osim što se između LAN-a i Interneta ne postavlja host nego mreža.
- Ta se mreža može sastojati i od samo jednog čvora konfigurisanog tako da i jedna i druga mreža može pristupiti izolacijskoj mreži, ali istovremeno tako da izolacijska mreža ne propušta direktan saobraćaj između privatne mreže i Interneta.
- Glavna prednost izolacijske mreže je u tome što omogućava jednostavnije postavljanje i dodeljivanje novih Internet adresa, naročito kod velikih privatnih mreža koje bi se inače morale znatno rekonstruisati.
- To u osnovi znači da računari "iza" izolacijske mreže ne moraju imati adrese koje su poznate računarima na Internetu.
- Na taj način se može priključiti cela mreža računara "iza" ***firewall***-a na Internet korišćenjem samo jedne Internet adrese.

8.7 – NAT servis

- Prolaskom paketa kroz *firewall*, NAT sakriva IP adrese računara iz privatne mreže tako što sve njih prevodi u adresu mrežne barijere.
- Kada primi podatke sa Interneta on ih šalje odgovarajućim računarima u LAN-u, koristeći se pri tom tabelom prevođenja adresa.
- Osim zaštitne funkcije, NAT omogućava uštedu javnih IP adresa, zato što jedna javna IP adresa, uz korišćenje različitih brojeva porta, može prevesti u veći broj privatnih IP adresa.
- Prevođenje IP adresa može biti:

1. **Statičko** - gde se blok **javnih IP adresa**, na osnovu fiksne tablice prevođenja, prevodi u blok **privatnih IP adresa**, tako da jednoj javnoj adresi odgovara jedna privatna IP adresa. Na taj način se skriva identitet računara u lokalnoj mreži.
2. **Dinamičko** prevođenje obuhvata dinamičko prevođenje bloka javnih u blok privatnih IP adresa, gde se sakriva identitet računara u LAN
3. **Dinamičko sa preopterećenjem** (*port address translation*, PAT) - jedna ili više javnih IP adresa se na osnovu broja porta prevodi u veći broj privatnih IP adresa, gde se sakriva identitet računara u LAN-u.

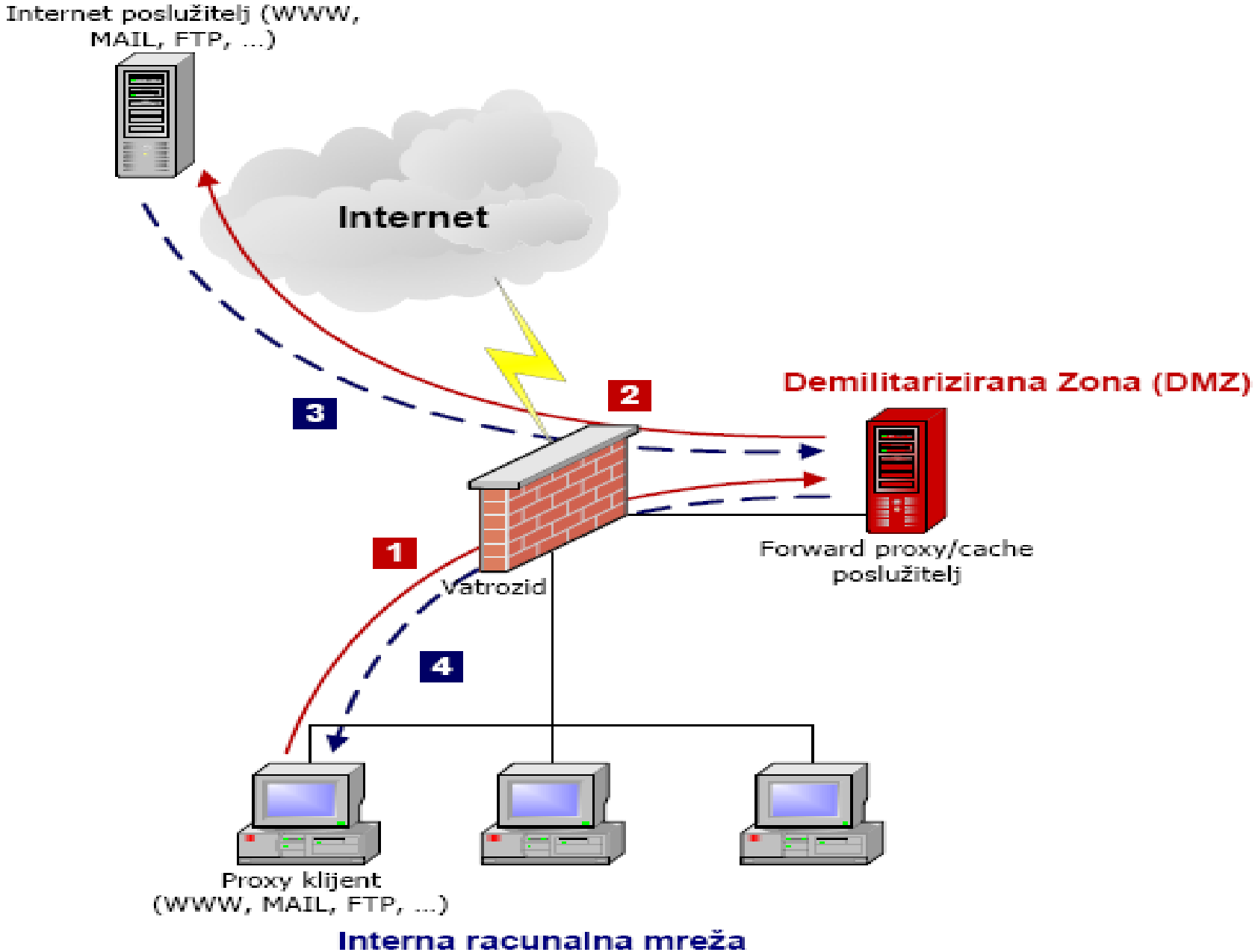
8.7 – NAT servis



8.8 – Proxy serveri

- *Proxy serveri* ili u prevodu "ovlašćeni serveri", u suštini predstavljaju jednu vrstu filtera u mrežnoj komunikaciji.
- Kada korisnik Interneta preko svog provajdera (ISP-a) ili lokalne mreže (u slučaju Intraneta) uputi zahtev za nekim sadržajem (*web* strana, slike i dr.), proxy server će proveriti da li dati zahtev nije protivan podešenim filterima, tj. da li korisnik ima dozvolu za pristup
- On će prvo "pogledati" u sopstvenu "cache" (privremenu) memoriju, da li se tu možda ne nalazi tražena stranica.
- Ukoliko nema traženih sadržaja u kešu, kontaktiraće sa odgovarajućim serverom i zatražiti *web* stranicu sa Interneta korišćenjem IP adrese
- Za korisnike, proxy server je nevidljiva komponenta mreže.
- Proxy serveri poboljšavaju performanse obezbeđivanjem često traženih sadržaja sa Interneta, i filtrira i odbacuje zahteve koje vlasnik ne smatra podobnim, i to u oba smera - ka i od LAN-a.
- Proxy server ima dve glavne funkcije
  1. služi kao posrednik koji pomaže korisnicima na privatnoj mreži
  2. proxy server može sačuvati često tražene podatke u kešu

8.8 - Povezivanje proxy-a



Hvala na pažnji !!!

Pitanja

? ? ?