SIGURNOST RAČUNARSKIH MREŽA (SRM)

Tema 5:

Kontrola pristupa i mrežne barijere

URLs:

- Zvanična Web strana: www.viser.edu.rs/predmeti.php?id=122
- Dodatni resursi: www.conwex.info/draganp/teaching.html
- Knjige:

  www.conwex.info/draganp/books.html
- Teme za seminarske radove:

  www.conwex.info/draganp/SRM_seminarski_radovi.html

Kontrola pristupa i mrežne barijere

engl. *access control, firewalls*

- Sadržaj poglavlja i predavanja:
  - 5.1 Osnovni pojmovi o računarskim mrežama
  - 5.2 Šta je mrežna barijera?
  - 5.3 iptables
  - 5.4 Skeniranje portova - provera konfiguracije mrežne barijere
  - 5.5 Proksi server Squid
  - 5.6 Kućna rešenja – mrežne barijere za Windows XP / Vista / W7
  - 5.7 Filtriranje paketa pomoću Cisco rutera

Quote

The function of a strong position is to make the forces holding it practically unassailable

— On War, Carl Von Clausewitz

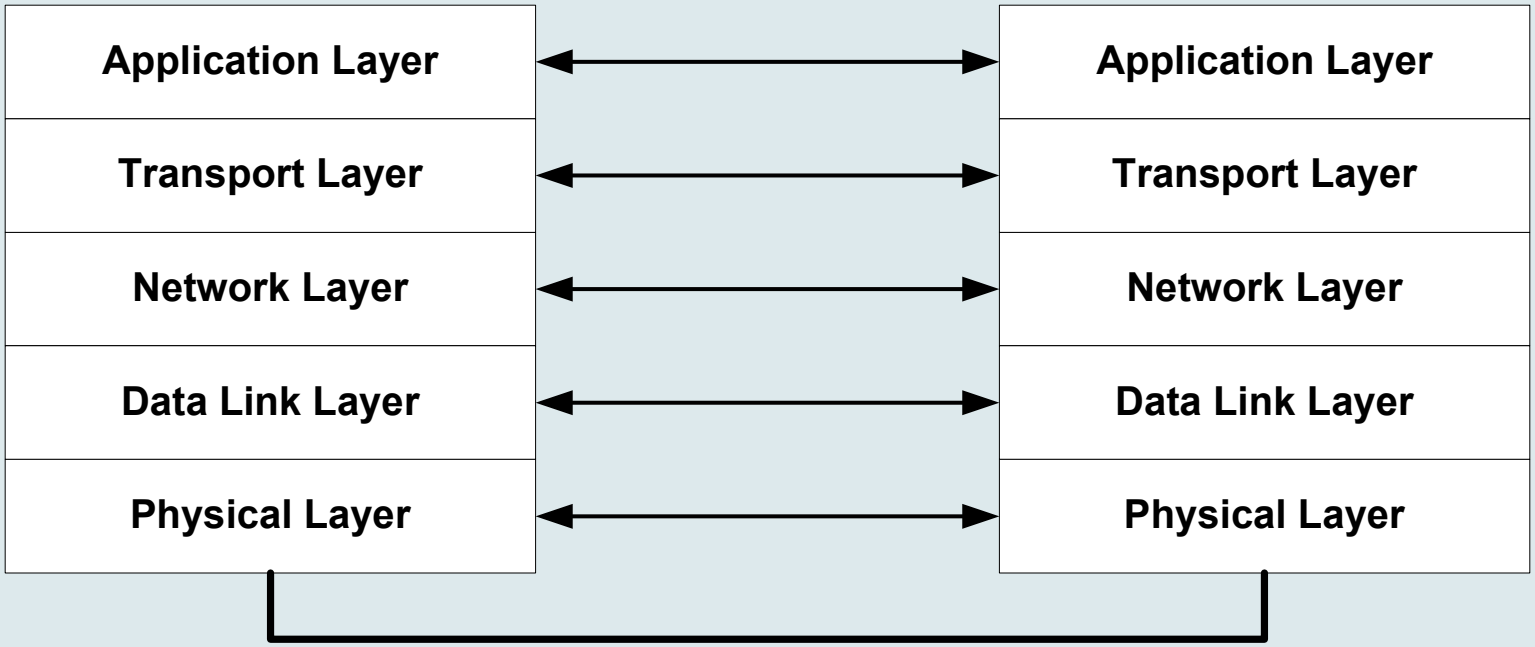
Potrebna predznanja

- Programiranje
- Za primenu:
  - Računarske mreže i protokoli
  - Operativni sistemi
  - Sistemsko programiranje
  - Internet

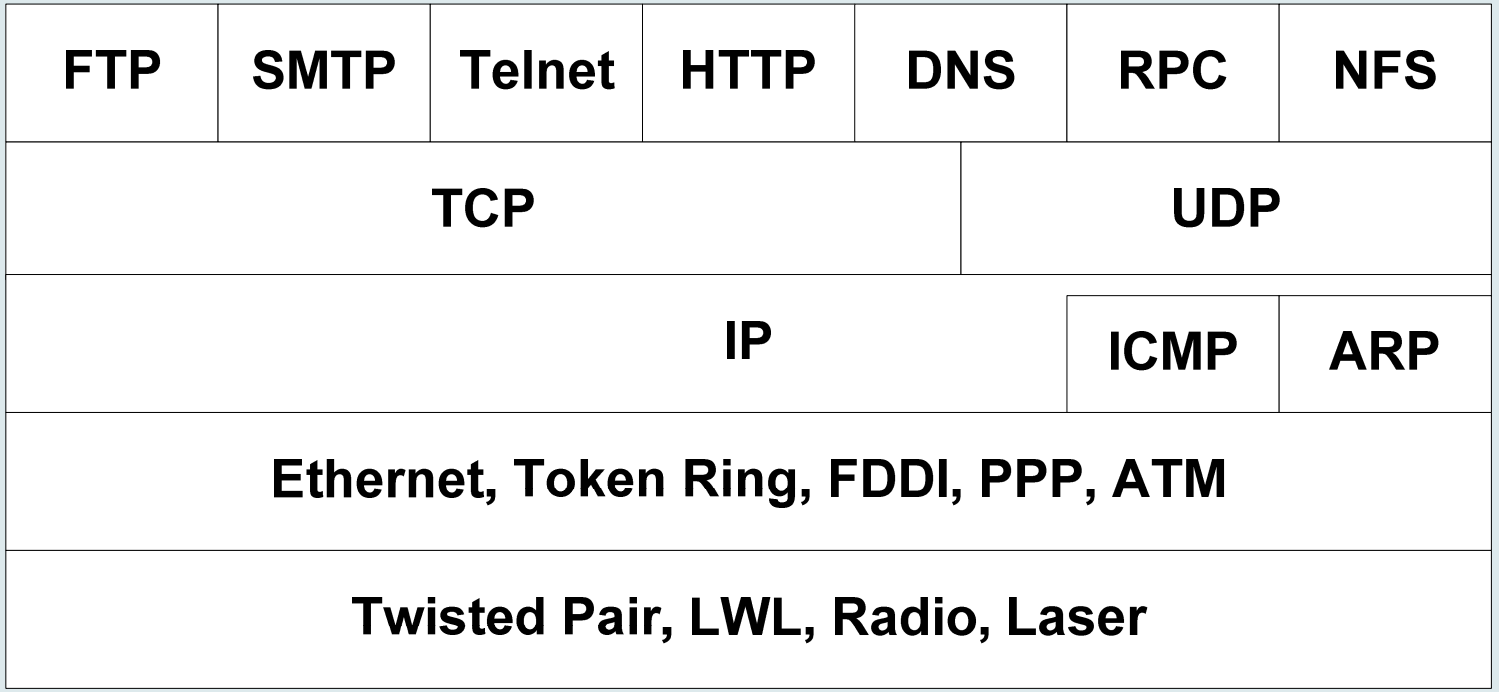
5.1 Osnovni pojmovi o računarskim mrežama

- Podrazumeva se predzanje:
  - Skup protokola TCP/IP
  - IP adresiranje i podmrežavanje
  - Sockets & Ports

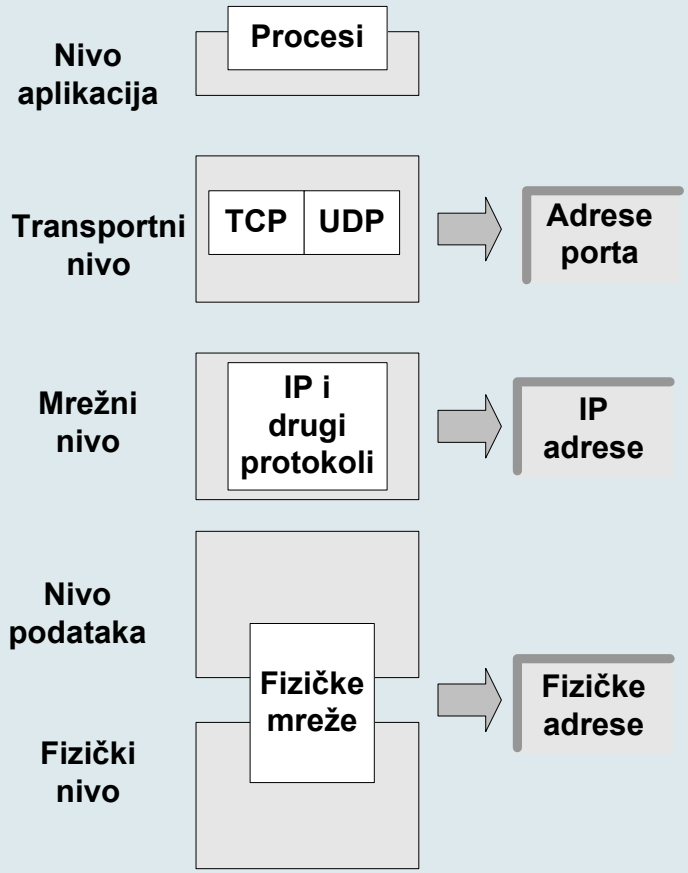
TCP/IP model



Internet protokoli



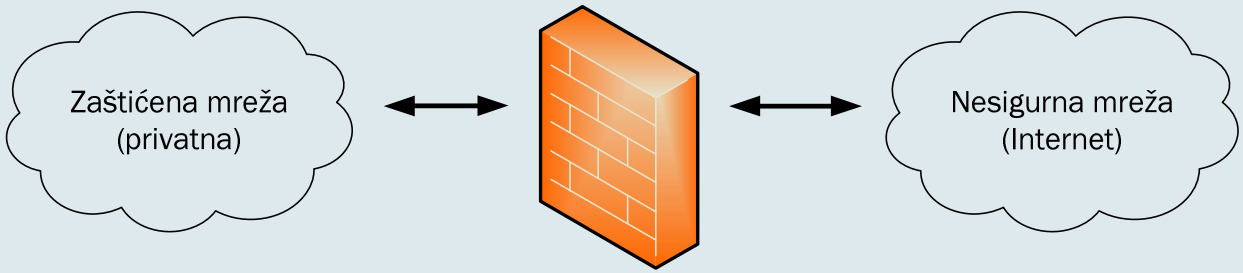
TCP/IP i adresiranje



5.2 Šta je mrežna barijera?

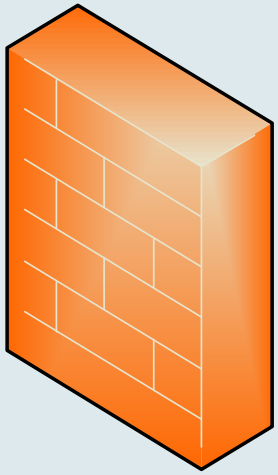
- Mrežne barijere (engl. *firewalls*) koriste se za postavljanje kontrolnih tačaka bezbednosti na granicama privatnih mreža.
- U kontrolnim tačkama mrežna barijera ispituje sve pakete koji prolaze između privatne mreže i Interneta.
- U zavisnosti od toga da li paketi zadovoljavaju pravila definisana listama za kontrolu pristupa, mrežna barijera će dozvoliti ili zabraniti protok tog paketa.
- Mrežna barijera je filter na relaciji lokalna mreža – Internet.

Mrežna barijera (engl. *firewall*)

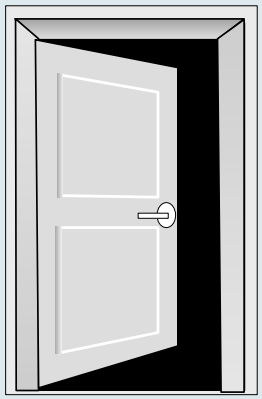


Razmena podataka je neophodna

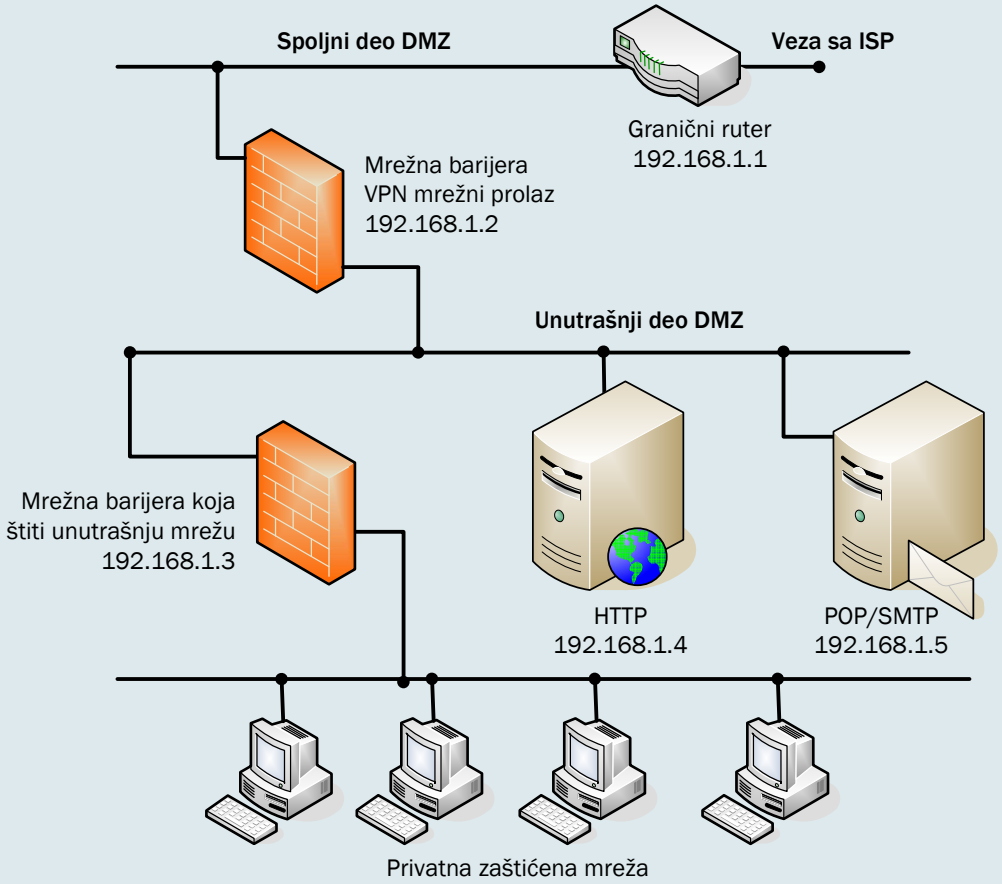
Zameniti



sa



Skica povezivanja privatne mreže na javnu preko mrežne barijere



Funkcije mrežne barijere

- Filtriranje paketa (engl. *packet filtering*)
- Prevođenje mrežnih adresa (*engl. network address translation*, NAT)
- Proksi servisi (engl. *proxy*)

Realizacija mrežne barijere

- Mrežna barijera može biti:
  - Hardverski uređaj (na primer: Cisco PIX)
  - Softver (na primer: iptables ili Kerio Winroute Firewall, ZoneAlarm...)

Dodatne funkcije mrežnih barijera

- Šifrovana provera identiteta
- Virtualno privatno umrežavanje (VPN – Virtual Private Network)

- Dodatne usluge:
  - Traženje zlonamernog koda u paketima
  - Filtriranje na osnovu sadržaja (engl. *content filtering*)

Filtriranje paketa

- Mrežne barijere analiziraju pakete i upoređuju ih s prethodno definisanim skupom pravila.

- Filtriranje je moguće na osnovu bilo kog dela zaglavlja paketa:
  - tipa protokola
  - IP adrese
  - TCP/UDP porta

Filtriranje paketa

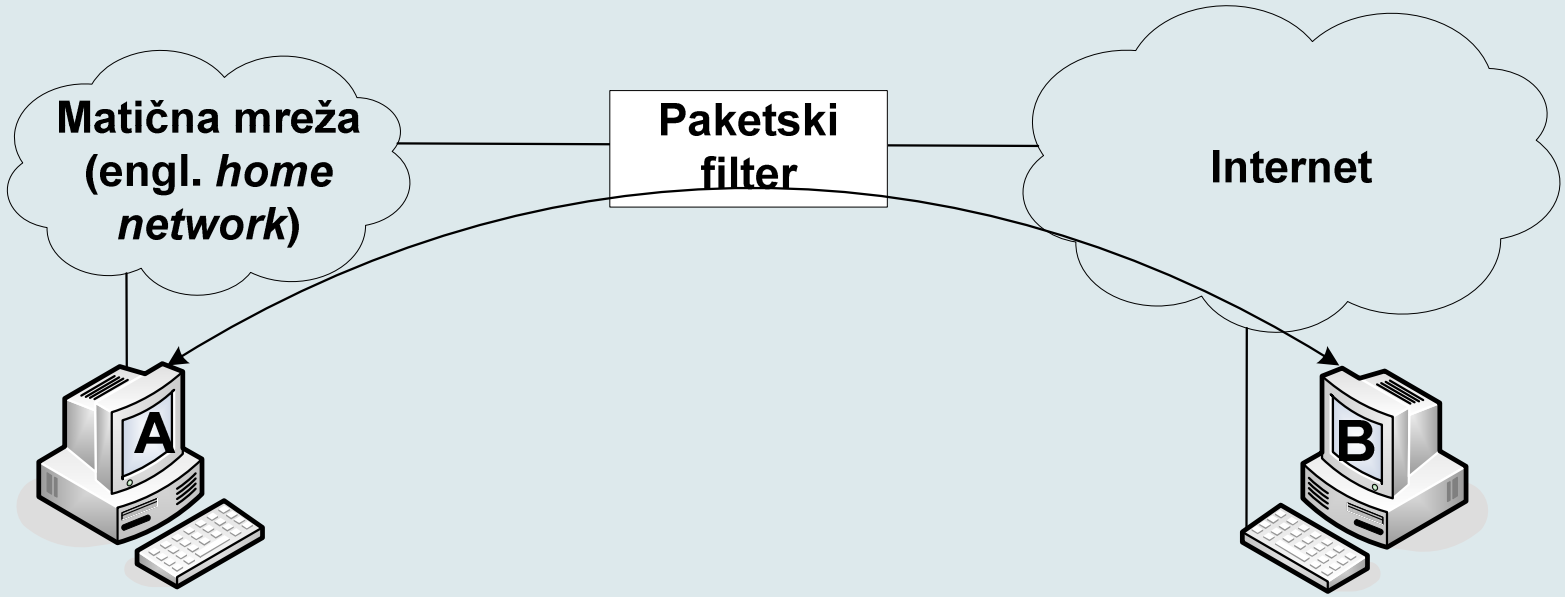
- Na osnovu definisanih pravila i zaglavlja konkretnog IP paketa, filter paketa može da odluči da:
  - prihvati paket
  - odbaci paket
  - odbaci paket i obavesti pošiljaoca da njegov paket nije prihvaćen.

Vrste filtera paketa

- Postoje dve vrste filtara paketa:
  - mrežne barijere bez uspostavljanja stanja (engl. *stateless firewall*)
  - mrežne barijere sa uspostavljanjem stanja (engl. *statefull firewall*).

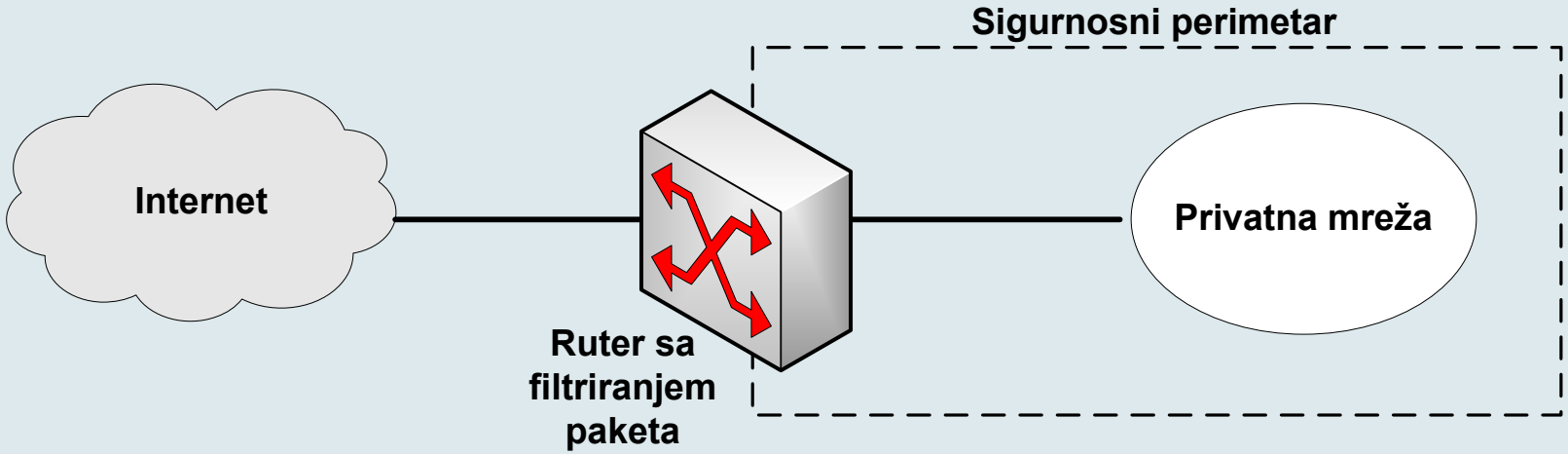
Firewall kao filter paketa

Pravila su implementirana na IP nivou
Ruteri se koriste kao paketski filteri



IP-Saobraćaj (paketi) dozvoljeni samo između A i B

Mrežna barijera – filter paketa



Uzorak skupa pravila za filtriranje paketa

	Izvorišna adresa	Izvorišni port	Odredišna adresa	Odredišni port	Akcija	Opis
1	Bilo koja	Bilo koji	192.168.1.0	>1023	Dozvoli	Rule to allow return TCP connections to internal subnet
2	192.168.1.1	Bilo koji	Bilo koja	Bilo koji	Odbij	Spreči samu mrežnu barijeru da se direktno povezuja na bilo šta
3	Bilo koja	Bilo koji	192.168.1.1	Bilo koji	Odbij	Spreči spoljne korisnike da direktno pristupaju mrežnoj barijeri
4	192.168.1.0	Bilo koji	Bilo koja	Bilo koji	Dozvoli	Interni korisnici mogu pristupati spoljašnjim serverima
5	Bilo koja	Bilo koji	192.168.1.2	SMTP	Dozvoli	Dozvoli spoljnim korisnicima da šalju mail unutra
6	Bilo koja	Bilo koji	192.168.1.3	HTTP	Dozvoli	Dozvoli spoljnim korisnicima da pristupe Web serverima
7	Bilo koja	Bilo koji	Bilo koja	Bilo koji	Odbij	„Uhvati sve" pravilo - sve što nije prethodno eksplicitno dovoljeno, zabranjeno je.

Tabela stanja konekcija mrežne barijere

Izvorišna adresa	Izvorišni port	Odredišna adresa	Odredišni port	Stanje veze
192.168.1.100	1030	210.9.88.29	80	Veza uspostavljena
192.168.1.102	1031	216.32.42.123	80	Veza uspostavljena
192.168.1.101	1033	173.66.32.122	25	Veza uspostavljena
192.168.1.106	1035	177.231.32.12	79	Veza uspostavljena
223.43.21.231	1990	192.168.1.6	80	Veza uspostavljena
219.22.123.32	2112	192.168.1.6	80	Veza uspostavljena
210.99.212.18	3321	192.168.1.6	80	Veza uspostavljena
24.102.32.23	1025	192.168.1.6	80	Veza uspostavljena
223.212.21.2	1046	192.168.1.6	80	Veza uspostavljena

Firewalls – Packet Filters

A

Akcija	Naš *host*	Port	Njihov host	Port	Komentar
Blokiraj	*	*	SPIGOT	*	Ne verujemo ovim ljudima
Dozvoli	OUR-GW	25	*	*	Povezivanje na naš SMTP port

B

Akcija	Naš *host*	Port	Njihov host	Port	Komentar
Blokiraj	*	*	*	*	*default*

C

Akcija	Naš *host*	Port	Njihov host	Port	Komentar
Dozvoli	*	*	*	25	Povezivanje na njihov SMTP port

Firewalls – Packet Filters (nastavak)

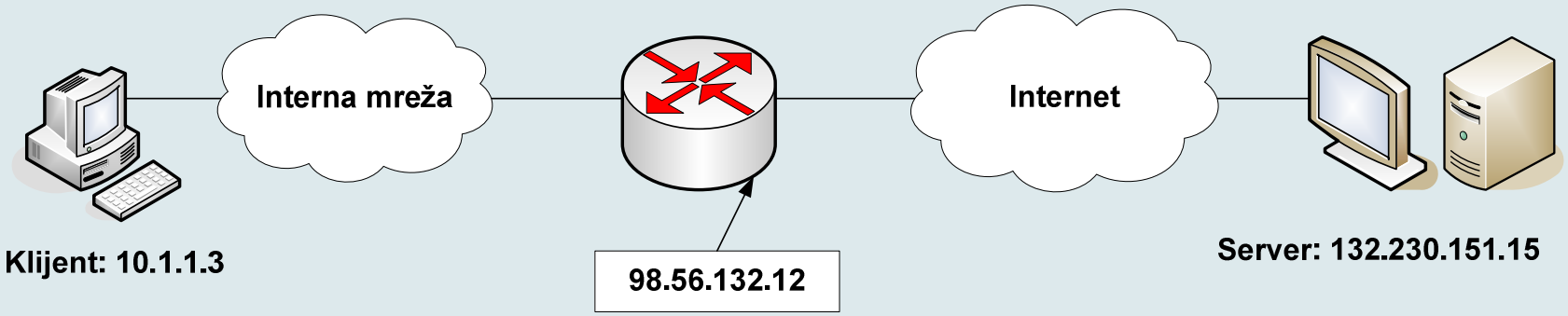
	Akcija	Izvor	Port	Odredište	Port	Flag	Komentar
D	Dozvoli	{Naši *host*-ovi}	*	*	25		Naši paketi ka njihovom SMTP portu
	Dozvoli	*	25	*	*	ACK	Njihovi odgovori potvrde

	Akcija	Izvor	Port	Odredište	Port	Flag	Komentar
E	Dozvoli	{Naši *host*-ovi}	*	*	*		Naši odlazni pozivi
	Dozvoli	*	*	*	*	ACK	Njihovi odgovori potvrde na naše pozive
	Dozvoli	*	*	*	>1024		Saobraćaj ka onima koji nisu serveri

Prevođenje mrežnih adresa

- **NAT – *Network Address Translation***
- NAT skriva informacije o računarima u privatnoj mreži od napadača sa Interneta.
- Prilikom prolaska paketa kroz mrežnu barijeru, NAT skriva IP adrese računara iz privatne mreže prevodeći ih u adresu mrežne barijere.

Firewall – NAT (Network Address Translator)



Pravila su implementirana na IP nivou
Ruteri se koriste kao paketski filteri

Firewall – NAT (Network Address Translator)

- Translacija privatne adrese u javnu adresu
- Adresa odgovora se translira u privatnu adresu
- Statička translacija adresa omogućava konekcije sa Interneta

Prevođenje mrežnih adresa

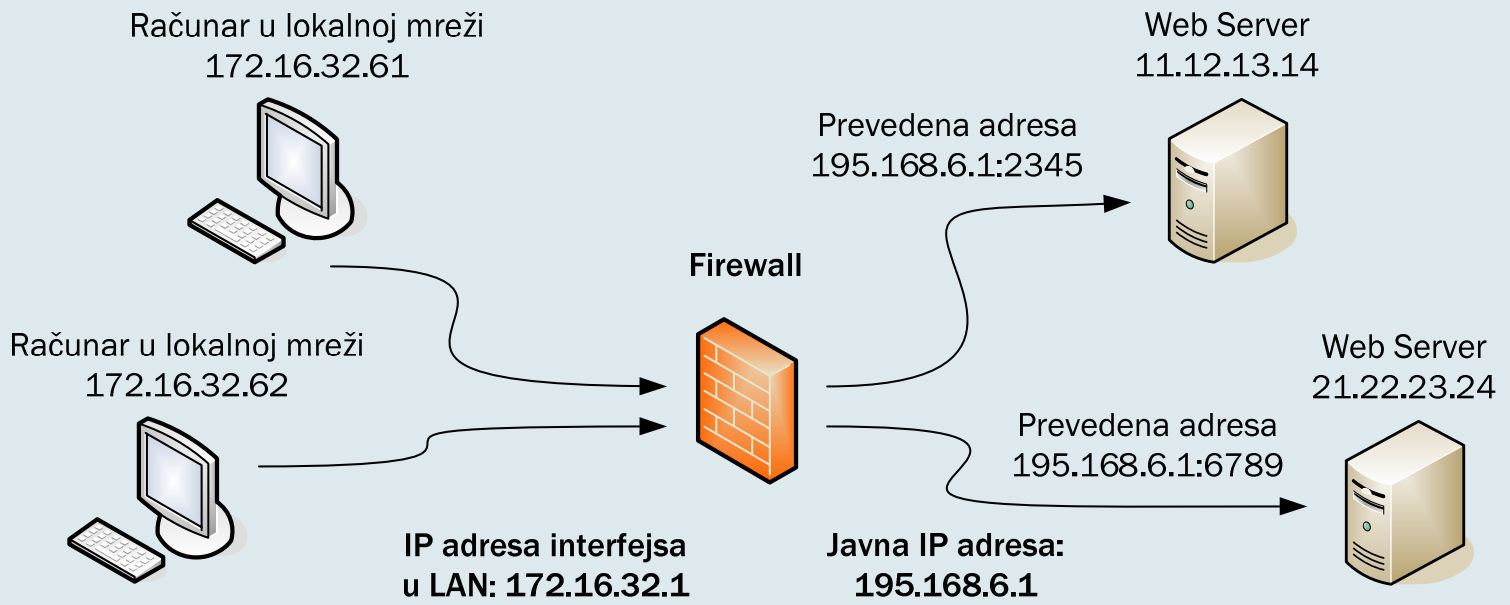


Tabela statičke translacije mrežnih adresa

Interna tj. unutrašnja (RFC 1918) adresa	Eksterna tj. spoljna (globalna) adresa
192.168.1.100	207.119.32.81
192.168.1.101	207.119.32.82
192.168.1.102	207.119.32.83
192.168.1.103	207.119.32.84
192.168.1.104	207.119.32.85
192.168.1.105	207.119.32.86
192.168.1.106	207.119.32.87
192.168.1.107	207.119.32.88
192.168.1.108	207.119.32.89
192.168.1.109	207.119.32.90

Vrsta prevođenja IP adresa

- **Statičko** – blok javnih IP adresa se na osnovu fiksne tablice prevođenja prevodi u blok privatnih IP adresa, tako da jednoj javnoj IP adresi odgovara jedna privatna IP adresa. Na taj način se skriva identitet računara u lokalnoj mreži;

- **Dinamičko** – blok javnih IP adresa dinamički se prevodi u blok privatnih IP adresa. Na taj način se skriva identitet računara u lokalnoj mreži;

- **Dinamičko sa preopterećenjem** (engl. *port address translation*, PAT) – jedna ili više javnih IP adresa se na osnovu broja porta prevodi u veći broj privatnih IP adresa. Na taj način se skriva identitet računara u lokalnoj mreži. Ovaj način prevođenja adresa se najčešće koristi.

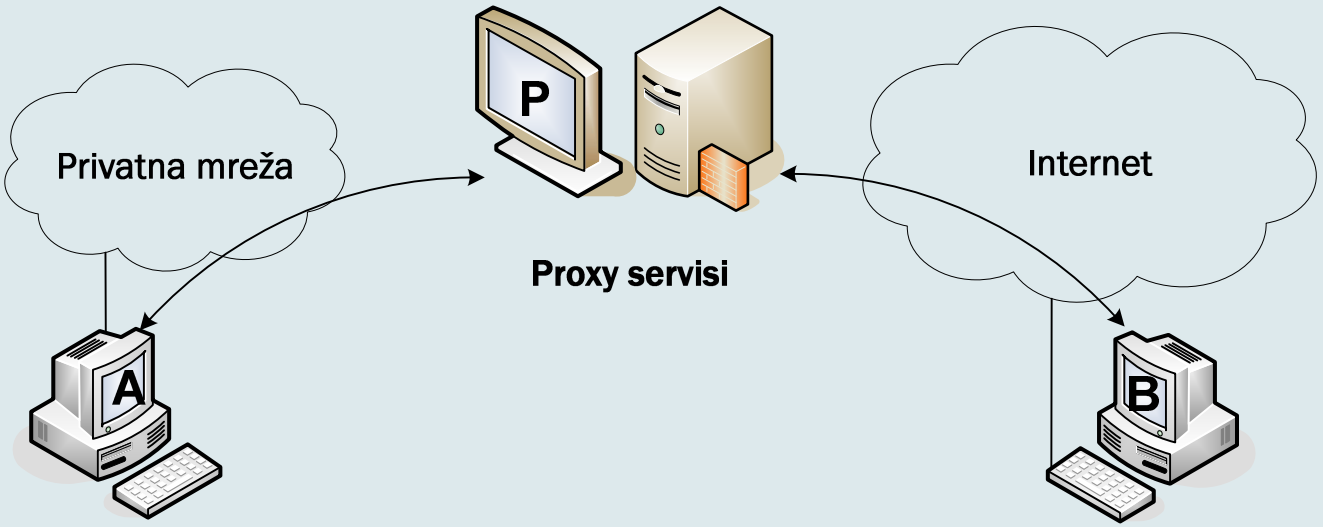
Proksi servisi

- 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.

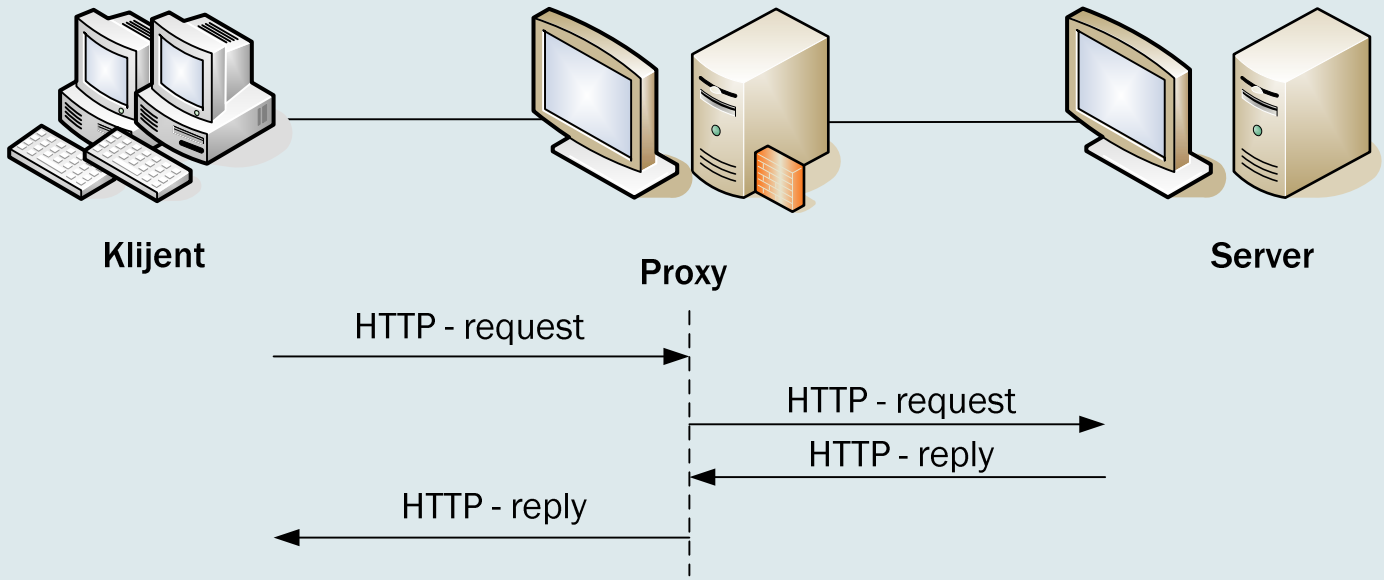
- Proksi (engl. *proxy*) aplikativnog sloja sprečava ovaj problem tako što omogućava da se potpuno zabrani protok podataka protokola mrežnog sloja i da se dozvoli saobraćaj samo protokolima viših slojeva, kao što su HTTP, FTP i SMTP.

- Proksi aplikativnog sloja je klijent-server arhitektura specifična za konkretan protokol koji se koristi.

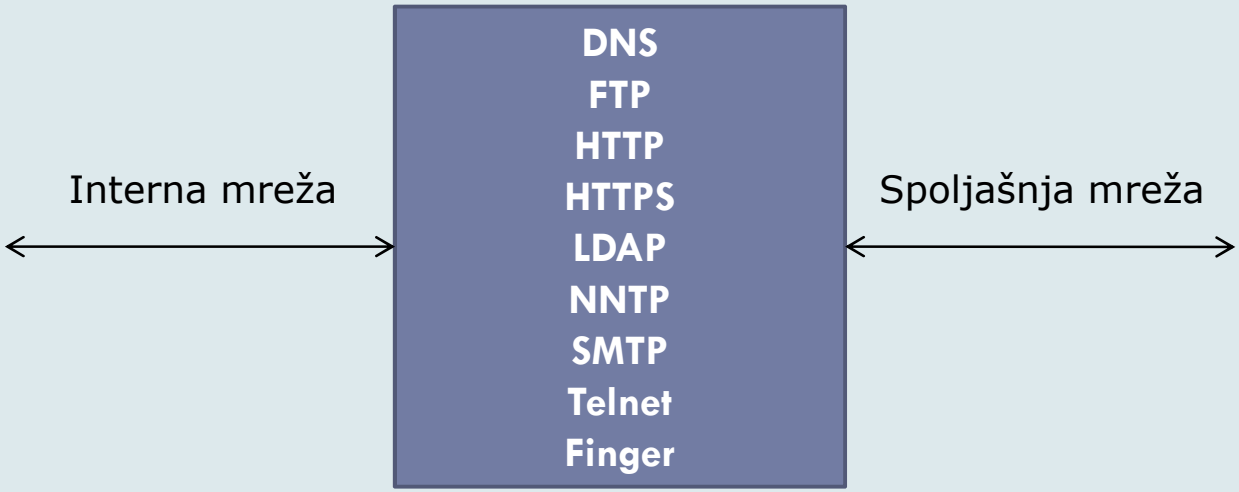
Proksi server



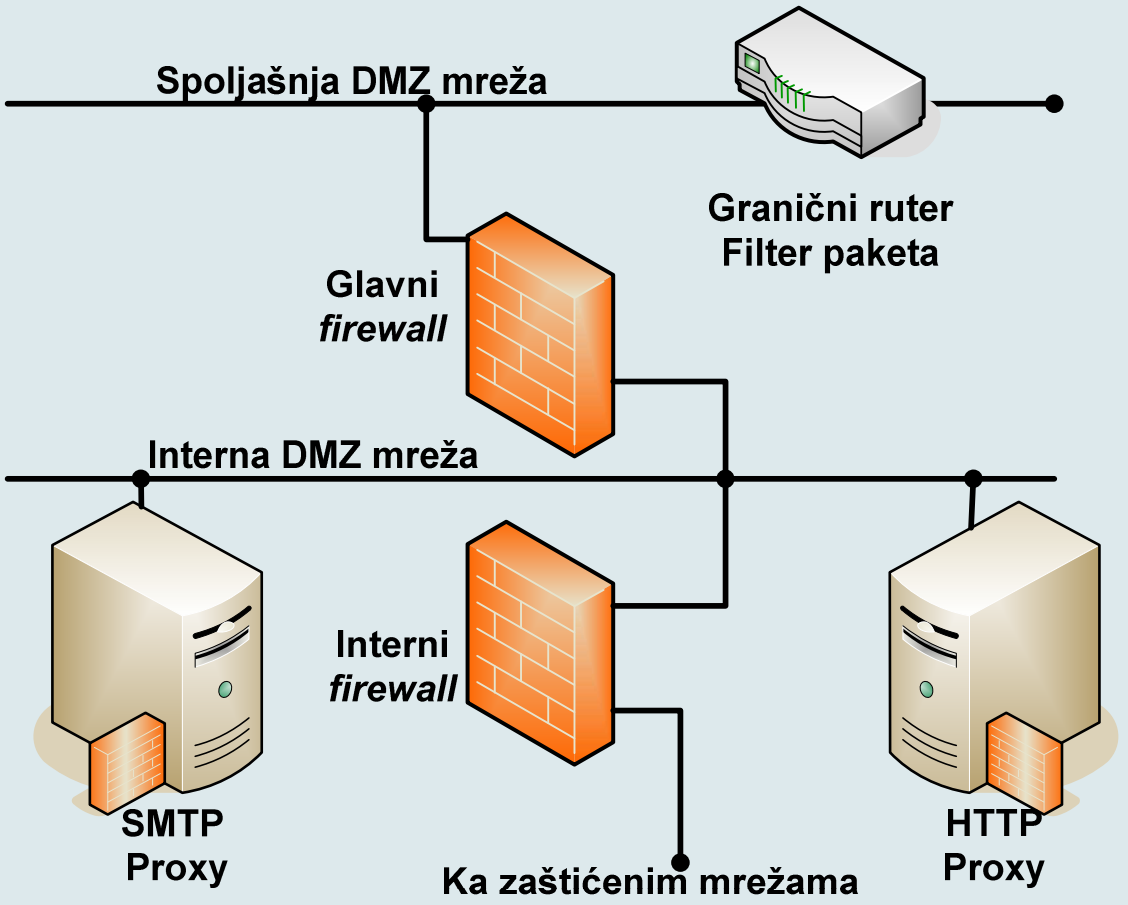
HTTP proksi



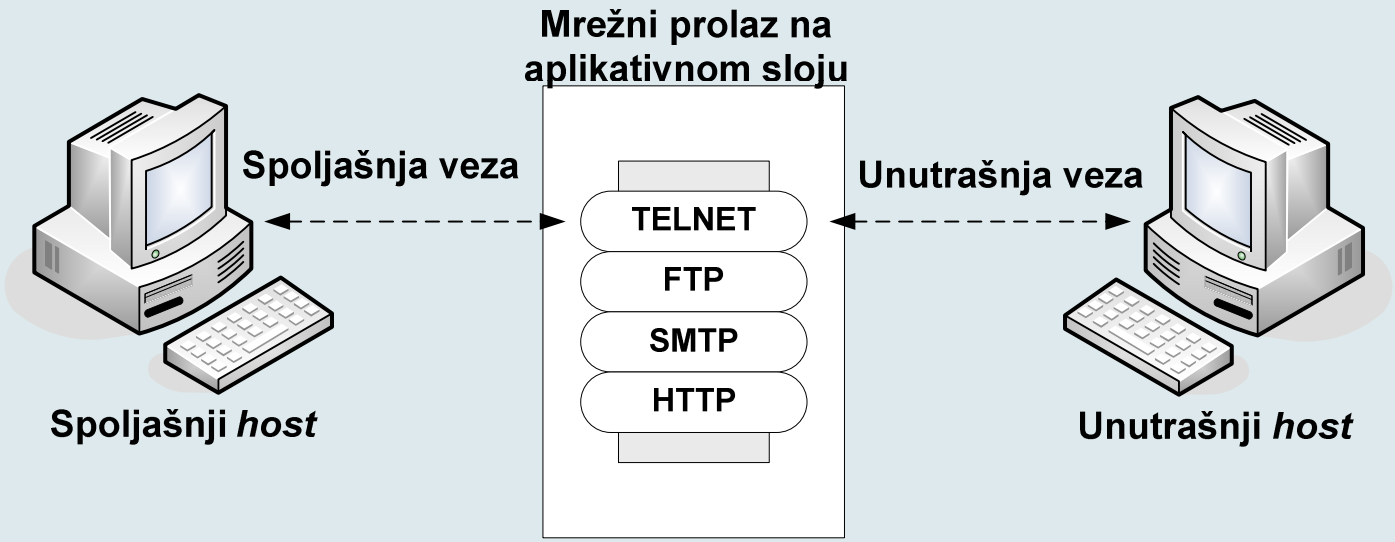
Tipični proksi agenti



Konfiguracija aplikativnog proksija

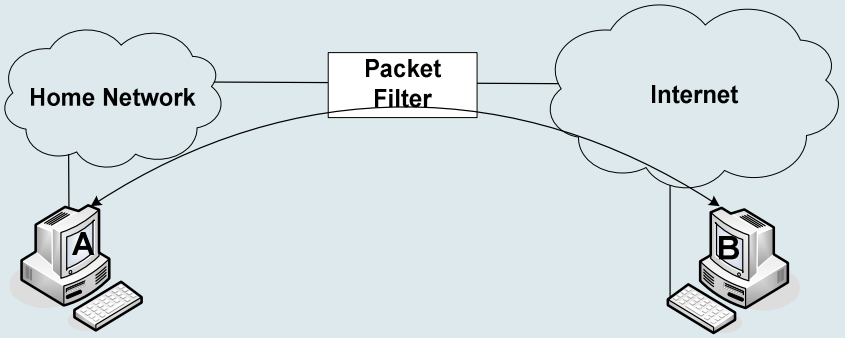


Firewalls - Application Level Gateway (or Proxy)

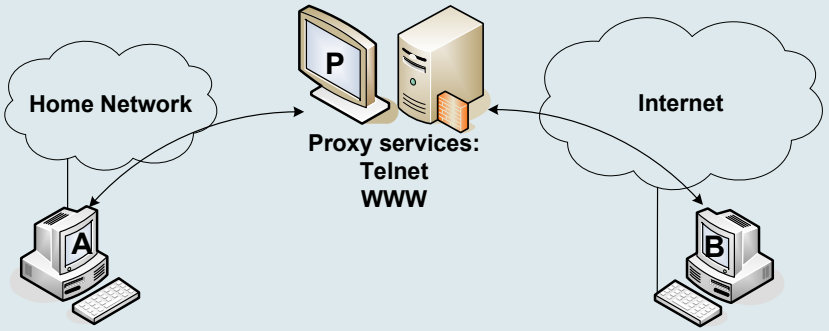


(b) Mrežni prolaz na aplikativnom sloju

Filter paketa ili proxy

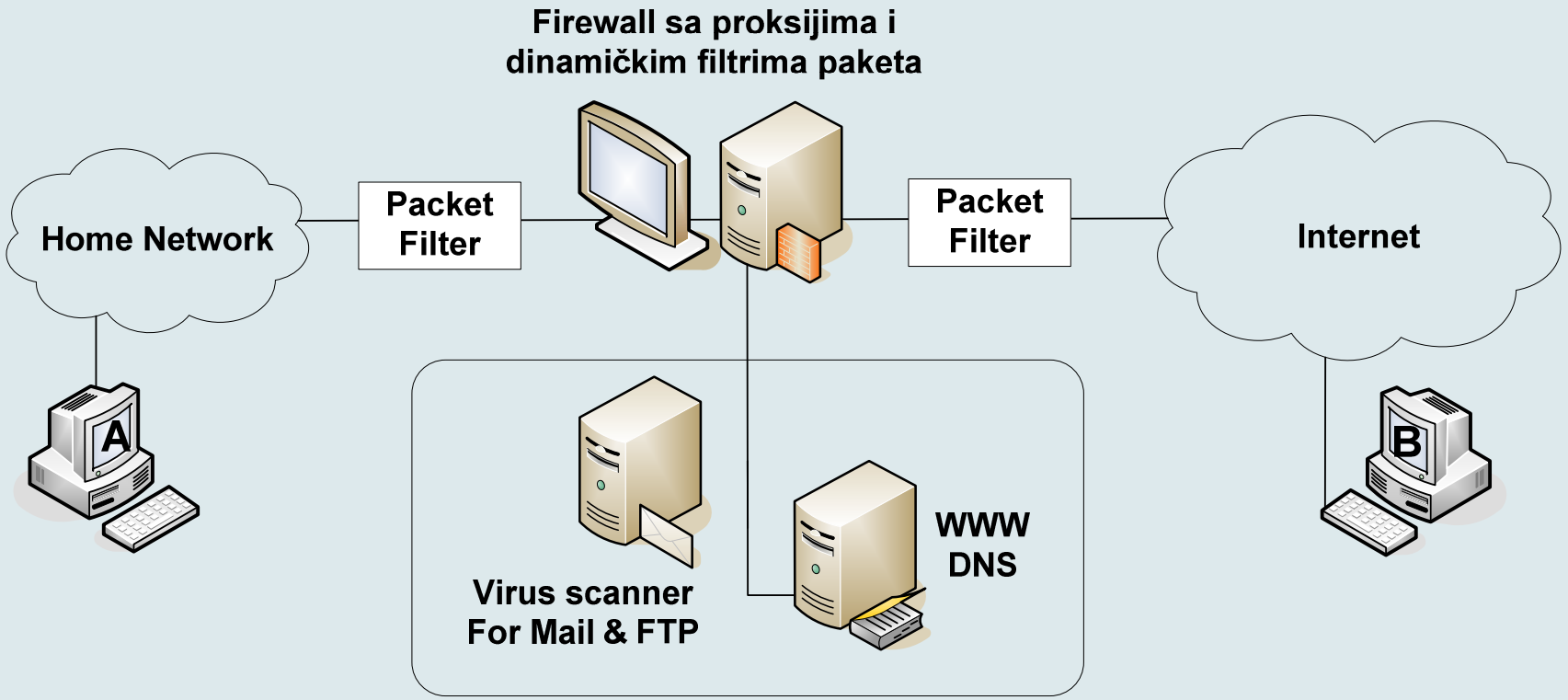


- Implementacija na IP nivou
- Većinom na ruterima
- Dozvoljava saobraćaj između IP adresa
- Vrši evaluaciju TCP zaglavlja, ako je moguće
- Filtriranje portova (SMTP, TELNET)
- Filtriranje protokola (RIP, ICMP)
- Filtriranje IP opcija (Source Routing) i odbrana od IP-spoofing-a

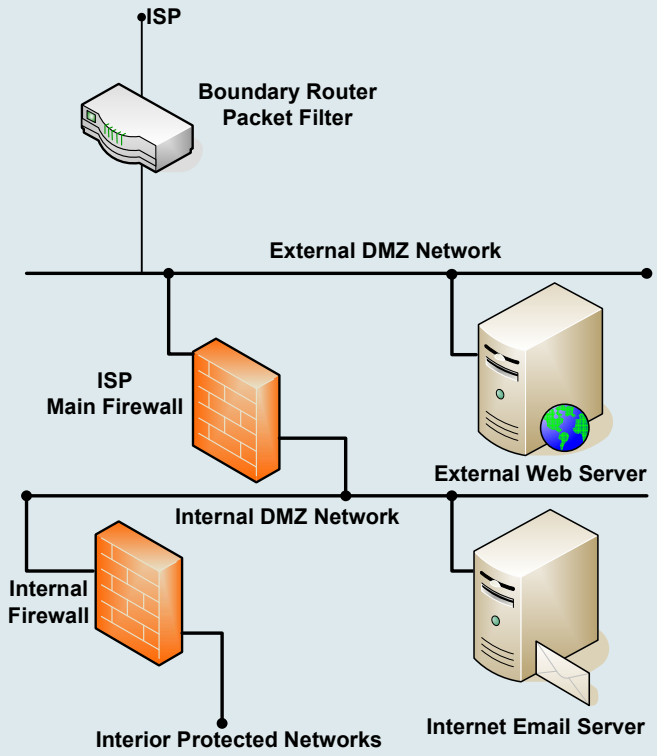


- Implementacija na aplikativnom sloju
- Provera identiteta korisnika, ako je moguće
- Nema direktne razmene podataka (prekoračenje bafera i *flooding attacks* u matičnu mrežu nisu mogući)
- Evaluacija aplikativnih protokola omogućava filtriranje servisa (SMTP command VRFY, EXPN)

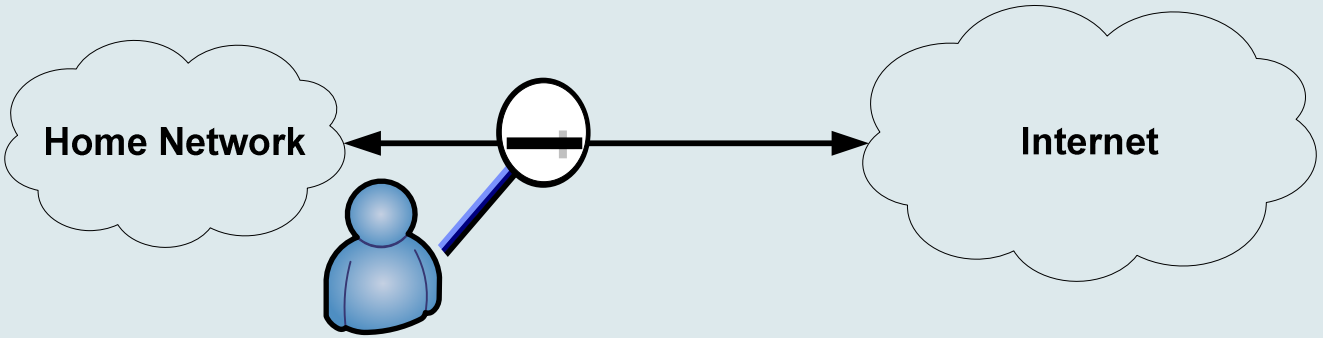
Primer firewall-a



Primer DMZ (dve mrežne barijere međusobno povezane)



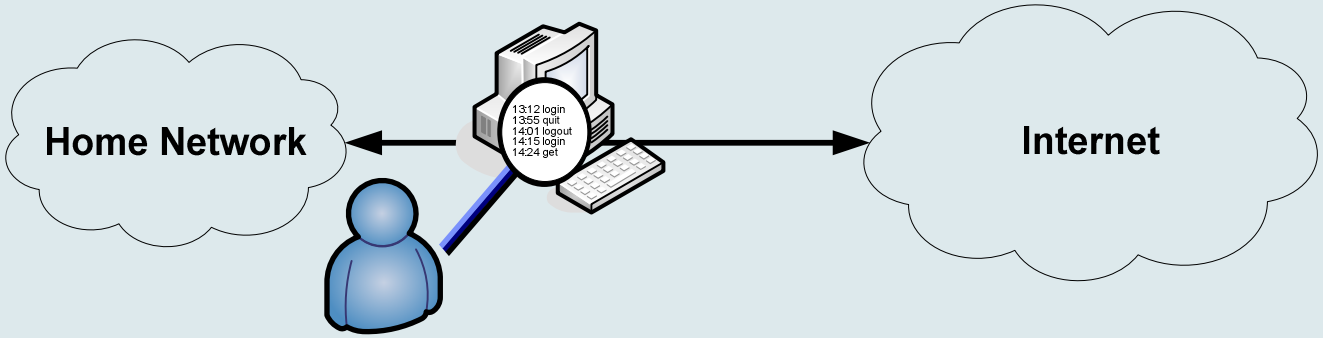
Firewall-ovi i privatnost



Sav Internet saobraćaj prolazi *firewall*:

- **Log datoteke mogu da budu korišćeni da se nadziru korisnici**
- **Svako ko ima pristup *firewall*-u može da čita celokupan Internet saobraćaj**
- **Visoka cena administracije**
- **Interni korisnici mogu narušiti sigurnosne procedure i politike**

Firewall i detekcija napada

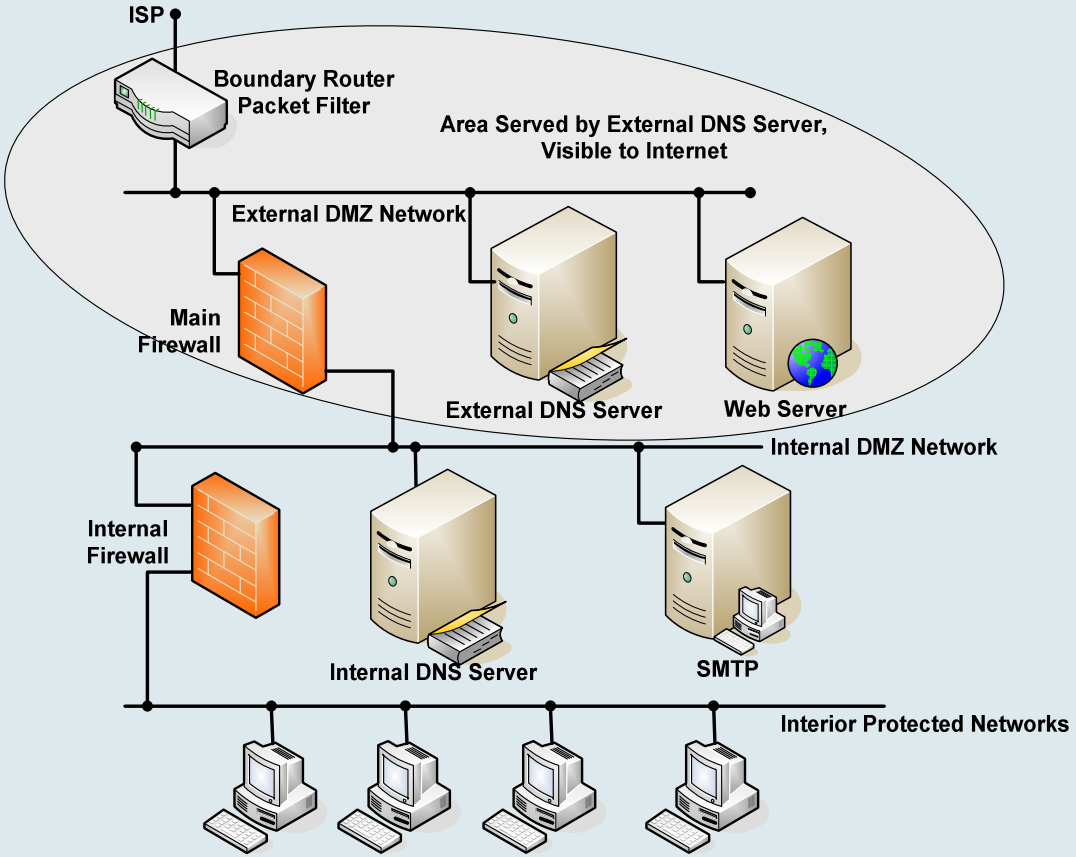


Nadziranje *firewall* log datoteka:

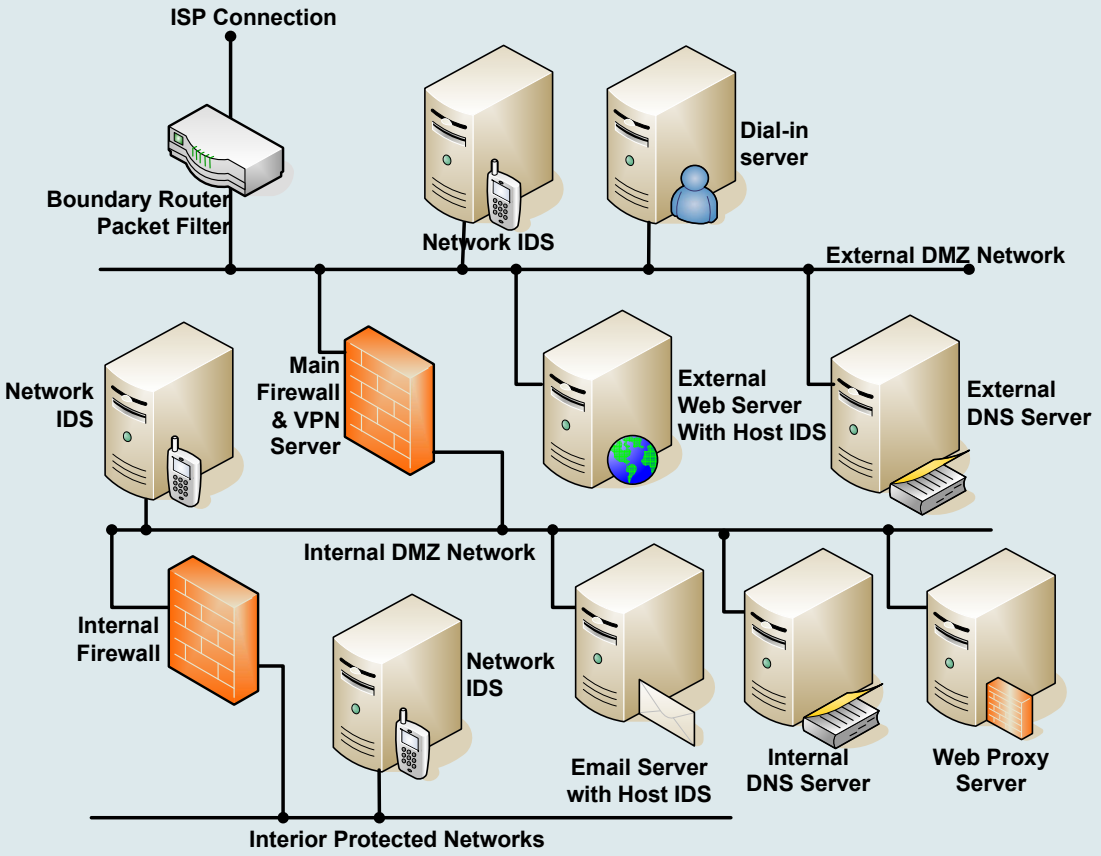
- **Upravljanje vezama izmedju matične mreže i Interneta**
- **Osiguranje intergriteta *firewall*-a**
- **Otkrivanje skeniranja portova, *Syn flooding*-a itd.**

Nedostatak: Napadi iznutra (insajderski napadi) ne mogu biti lako otkriveni

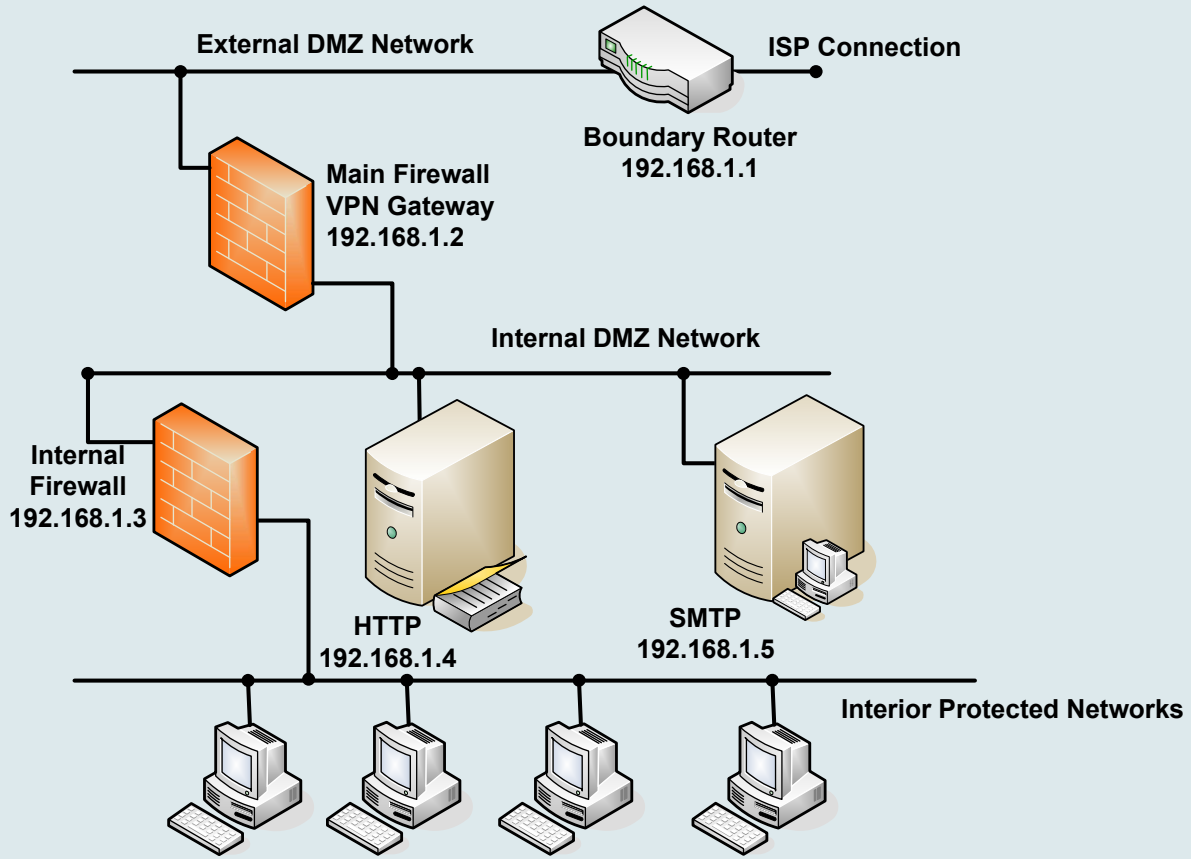
Primer razdvajanja DNS-a



Primer realnog okruženja



Primer okruženja sa graničnim ruterom



Uzorak skupa pravila za granični ruter

	Izvorišna adresa	Izvorišni port	Odredišna adresa	Odredišni port	Akcija	Opis
1	Bilo koja	Bilo koji	192.168.1.0	>1023	Dozvoli	Rule to allow return TCP connections to internal subnet
2	192.168.1.1	Bilo koji	Bilo koja	Bilo koji	Odbij	Spreči samu mrežnu barijeru da se direktno povezuja na bilo šta
3	Bilo koja	Bilo koji	192.168.1.2	VPN	Dozvoli	Dozvoli spoljnim korisnicima da se povezuju na VPN server
4	Bilo koja	Bilo koji	192.168.1.2	SMTP	Dozvoli	Dozvoli spoljnim korisnicima da pošalju e-mail proksiju
5	Bilo koja	Bilo koja	192.168.1.2	HTTP	Dozvoli	Pošalji unutrašnji HTTP saobraćaj ka proksiju
5	Bilo koja	Bilo koji	192.168.1.2	SMTP	Dozvoli	Dozvoli spoljnim korisnicima da šalju mail unutra
6	Bilo koja	Bilo koji	192.168.1.1	Bilo koji	Odbij	Spreči spoljne korisnike da direktno pristupaju mrežnoj barijeri
7	192.168.1.0	Bilo koji	Bilo koja	Bilo koji	Dozvoli	Unutrašnji korisnici mogu da pristupe spoljnim serverima
8	Bilo koja	Bilo koji	Bilo koja	Bilo koja	Odbij	„Uhvati sve” pravilo - sve što nije prethodno eksplicitno dovoljeno, zabranjeno je.

Virtuelne privatne mreže

- Virtualne privatne mreže, poznate i kao šifrovani tuneli, omogućavaju zaštićeno povezivanje dve fizički odvojene mreže preko Interneta.
- Podaci koji se razmenjuju na ovaj način nevidljivi su za neovlašćene entitete.
- VPN može biti predmet raznih neugodnih napada, kao što su pokušaji redirekcije, inicijalizovanje lažne veze ili bilo koji drugi vid napada dok se uspostavlja tunel.

Šifrovana provera identiteta

- Šifrovana provera identiteta omogućava spoljnim korisnicima na Internetu da mrežnoj barijeri dokažu da su ovlašćeni i da tako otvore vezu kroz tu barijeru ka unutrašnjoj mreži.
- Za šifrovanu proveru identiteta može se koristiti bilo koji protokol za proveru identiteta.
- Kada je veza uspostavljena, ona može, a i ne mora, biti šifrovana, što zavisi od konkretnog prozvoda koji se koristi i od toga da li je na klijentu instaliran dodatni softver koji obezbeđuje podršku za tunelovanje.

Ograničenja mrežnih barijera

- Ne može zaštiti od napada koji ga “preskaču” (bypassing) npr. organizacije i servisi (recimo SSL/SSH) kojima se veruje
- Ne može zaštititi protiv internih pretnji npr. nezadovoljnog zaposlenog
- Ne može zaštiti od prenosa fajlova zaraženih virusima

Problemi koje mrežne barijere ne mogu rešiti

- Mrežna barijera neće zaštititi od napada koji se sprovode **oponašanjem legitimnog saobraćaja** na otvorenim portovima. Za sprečavanje takvih napada morate da koristite sisteme za sprečavanje upada u mreže (engl. *Intrusion Prevention System*, IPS).

- Ozbiljna pretnja bezbednosti vaše mreže – **skriveni prolazi** pomoću kojih se korisnici mogu povezati na Internet

Različiti pristupi filtriranju

- Usluge filtriranja paketa na nivou ISP-a
- Jedna mrežna barijera sa javnim serverima u privatnoj mreži
- Jedna mrežna barijera sa javnim serverima van privatne mreže
- Demilitarizovane zone
- Korporativna mrežna barijera
- Isključenje sa mreže

Najslabija karika

- Kada organizacija ima više spoljnih veza tada za svaku od njih mora da instalira mrežnu barijeru
- Potrebno je uskladiti sve mrežne barijere (koncept je jednostavan, ali detalji komplikuju izgradnju mrežnih barijera)
- Ranjivost mreže postoji ako se pristup ne ograniči na identičan način na svim mrežnim barijerama

5.3 iptables

- U jezgra Linux sistema, počev od verzije 2.4, ugrađen je sistem za filtriranje paketa poznat kao Netfilter.

- Netfilter lanci za filtriranje paketa rade u zaštićenom režimu rada (engl. *kernel mode*). U korisničkom režimu radi poseban alat – iptables, koji zahteva privilegije korisnika root i služi za konfigurisanje:
  - filterskih lanaca,
  - NAT tabela i
  - mangle tabele.

*Biće detaljnije obrađeno na vežbama.

5.4 Skeniranje portova - provera konfiguracije mrežne barijere

- 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.

Skeniranje portova...

- 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.

*Biće detaljnije obrađeno na vežbama.

nmap

- 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.

- Nmap je besplatan i isporučuje se uz većinu distribucija Linuxa. Ukoliko ga nema u distribuciji koju koristite, preuzmite ga sa adrese www.insecure.org/nmap. Nmap postoji i u verzijama za druge operativne sisteme. Verzija za Windows ne omogućava skeniranje portova računara sa kog je pokrenut nmap.

Traceroute alat za skeniranje portova

- Može se koristiti za pronalaženje mrežnih barijera na mreži
- UNIX: traceroute
- NT: tracert.exe
- Linux: traceroute
- Vrlo je verovatno da IP adresa neposredno pre ciljne adrese predstavlja IP adresu mrežne barijere

Zaštita od skeniranja TCP portova korišćenjem traceroute alata

- Konfigurisati rutere da ne odgovaraju na TTL EXPIRED poruke kada prime paket čiji je TTL 0 ili 1
- Konfigurisati mrežne barijere i granične rutere da ne odgovaraju na TTL istekle pakete

5.5 Squid proksi server

- Proksi server je, u najširem smislu, sloj između lokalne i spoljašnje mreže koji omogućava većem broju računara da dele jednu vezu ka Internetu i skladišti, tj. kešira podatke kako bi se ubrzao pristup tim podacima sa lokalne mreže.
- Proksi serveri rade na aplikacionom sloju OSI modela, što znači da svaki klijent mora biti pojedinačno konfigurisan (moraju se navesti adresa proksi servera i port na kome proksi server pruža usluge).

Squid

- Squid je nastao na osnovu projekta Harvest koji se, između ostalog, bavio i keširanjem pristupa objektima na mreži.
- Licenciran je opštom javnom licencom GNU, što znači da je besplatan. Podržava FTP, gopher i HTTP protokole, SSL, kontrolu pristupa i praćenje događaja, tj. vođenje evidencije o zahtevima.

*Biće detaljnije obrađeno na vežbama.

5.6 Kućna rešenja – mrežne barijere za Windows XP / Vista / W7

- Windows Vista Firewall
  - prikaz
- Sunbelt Kerio Personal Firewall
- Zone Alarm (Pro)
  - prikaz

*Biće detaljnije obrađeno na vežbama.

5.7 Filtriranje paketa pomoću Cisco rutera

- Konfigurisanje osnovnih parametara
  - Postavljanje lozinki
  - Dodela IP adrese mrežnom interfejsu
  - Konfigurisanje protokola za rutiranje

- Liste kontrole pristupa (za IP protokol)
  - Standardne ACL liste
  - Proširene ACL liste
  - Imenovane ACL liste

*Biće detaljnije obrađeno na vežbama.

Šifrovali ste podatke i postavili mrežnu barijeru. Šta dalje?

- Mrežne barijere su samo deo skupa celovitih sigurnosnih mera, a njihova funkcija zavisi od drugih elemenata odbrane kao što su:
  - Antivirusni alati i alati za odbranu od špijunskih i drugih zlonamernih programa
  - Alati za zaštitu privatnosti
  - Sistemi za detekciju i prevenciju upada
  - Alati za nadzor u upravljanje računarskim mrežama
  - Brojne druge mere o kojima će biti reči na narednim predavanjima

Literatura

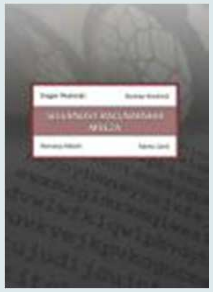
- D. Pleskonjić, N. Maček, B. Đorđević, M. Carić: **"Sigurnost računarskih sistema i mreža"**, Mikro knjiga, Beograd, 2007., ISBN: 978-86-7555-305-2, knjiga – udžbenik
- www.conwex.info/draganp/books_SRSiM.html
- www.mikroknjiga.rs/store/prikaz.php?ref=978-86-7555-305-2

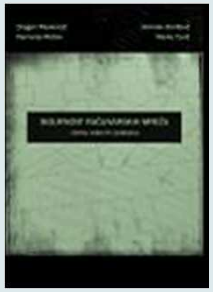
- Za predavanje 5:
  - Poglavlje 5: Kontrola pristupa i mrežne barijere

Literatura - nastavak

- D. Pleskonjić, B. Đorđević, N. Maček, Marko Carić: **"Sigurnost računarskih mreža"**, Viša elektrotehnička škola, Beograd, 2006., ISBN 86-85081-16-5, knjiga - udžbenik
- D. Pleskonjić, B. Đorđević, N. Maček, Marko Carić: **"Sigurnost računarskih mreža - priručnik za laboratorijske vežbe"**, Viša elektrotehnička škola, Beograd, 2006., ISBN 86-85081-49-1
- D. Pleskonjić, B. Đorđević, N. Maček, Marko Carić: **"Sigurnost računarskih mreža - zbirka rešenih zadataka"**, Viša elektrotehnička škola, Beograd, 2006., ISBN 86-85081-55-6

www.conwex.info/draganp/books.html





Dodatna literatura

- **Applied Cryptography**
  Bruce Schneier
  John Wiley & Sons, 1995

- **Cryptography and Network Security**
  William Stallings
  Prentice Hall, 1998

- **The CISSP Prep Guide – Mastering the Ten Domains of Computer Security**
  Ronald L. Krutz, Russell Dean Vines
  John Wiley & Sons, 2001

  Druge knjige i razni *online* resursi

- ***Napomena:*** tokom predavanja će biti naglašena dodatna literatura, po potrebi.

Pitanja

?