FIREWALL SISTEMI

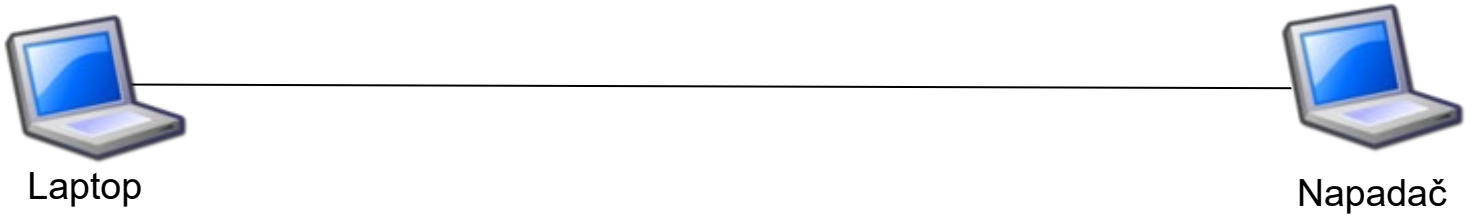
Predmet: Bezbednost Aplikacija

Predavač: dr Dušan Stefanović

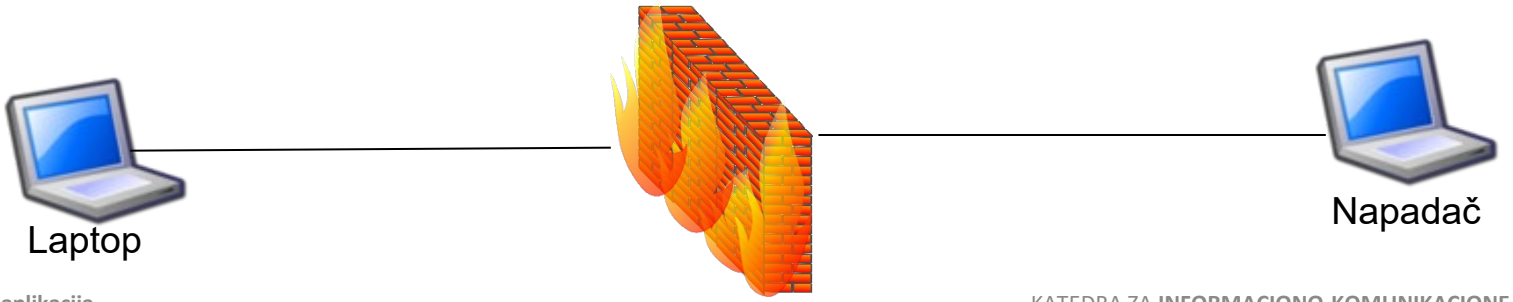
ULOGA FIREWALL-a

Uloga Firewall-a je kontrola saobraćaja (paketa) koji iz spoljne mreže dolaze do internog računara ili mreže, odnosno odlaze od internog računara ili mreže ka spoljnoj mreži.

Bez Firewall-a drugi računari će biti u mogućnosti da se povežu na računar i da pristupe servisima

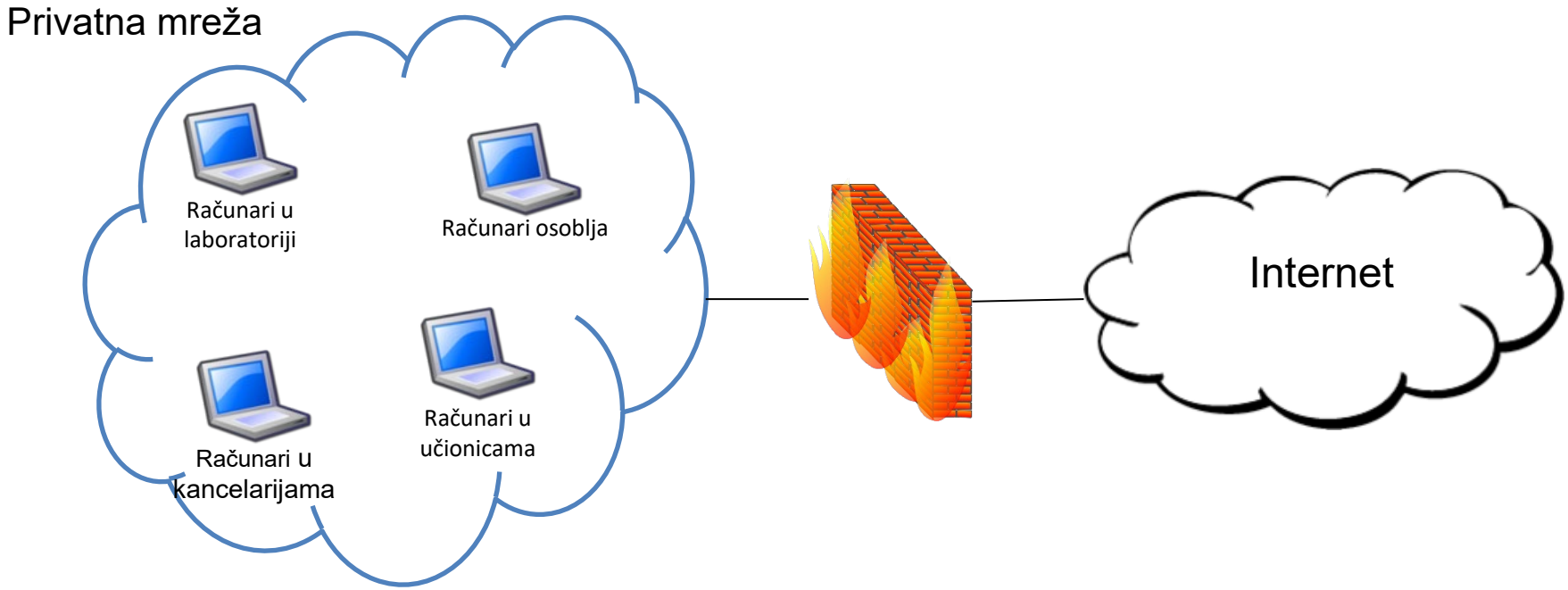


Firewall sprečava korisnike sa drugih računara da pristupe vašem računaru



ULOGA FIREWALL-a

Firewall sprečava korisnike koji se nalaze izvan privatne mreže da pristupe računarima unutar mreže, odnosno kontroliše ko izvan privatne mreže može da pristupi tim računarima



Firewall takođe sprečava korisnike iz privatne mreže da pristupe sadržajima van mreže kojima ne želimo da oni pristupe (npr. ne želimo da dozvolimo studentima da sa školskih računara pristupaju Facebook-u i ostalim društvenim mrežama)

- Internet konekcija je od suštinskog značaja za organizacije
  - Ovo dovodi do opasnosti po bezbednost mreže organizacije

- Firewall-ovi su efikasna sredstva za zaštitu lokalnih računarskih mreža
  - Zaštita na jednom mestu bolja je nego da se štiti svaki računar pojedinačno

- FW se umeće između interne i eksterne mreže kako bi uspostavio kontrolisani link

- Firewall se koristi kao *zonska* odbrana
  - Izoluje interni sistem od eksternih mreža

- Internet konekcija je od suštinskog značaja za organizacije
  - Ovo dovodi do opasnosti po bezbednost mreže organizacije

- Firewall-ovi su efikasna sredstva za zaštitu lokalnih računarskih mreža
  - Zaštita na jednom mestu bolja je nego da se štiti svaki računar pojedinačno

- FW se umeće između interne i eksterne mreže kako bi uspostavio kontrolisani link

- Firewall se koristi kao *zonska* odbrana
  - Izoluje interni sistem od eksternih mreža

- Internet konekcija je od suštinskog značaja za organizacije
  - Ovo dovodi do opasnosti po bezbednost mreže organizacije
- Firewall-ovi su efikasna sredstva za zaštitu lokalnih računarskih mreža
  - Zaštita na jednom mestu bolja je nego da se štiti svaki računar pojedinačno
- FW se umeće između interne i eksterne mreže kako bi uspostavio kontrolisani link
- Firewall se koristi kao *zonska* odbrana
  - Izoluje interni sistem od eksternih mreža

- Internet konekcija je od suštinskog značaja za organizacije
  - Ovo dovodi do opasnosti po bezbednost mreže organizacije
- Firewall-ovi su efikasna sredstva za zaštitu lokalnih računarskih mreža
  - Zaštita na jednom mestu bolja je nego da se štiti svaki računar pojedinačno
- FW se umeće između interne i eksterne mreže kako bi uspostavio kontrolisani link
- Firewall se koristi kao zonska odbrana
  - Izoluje interni sistem od eksternih mreža

INTERNET IZVOR NAPADA

Većini organizacija internet je ključni resurs i potreban im je za ostvarivanje ciljeva

Povezivanje mreže jedne organizacije na internet dovodi do raznih opasnosti

Maliciozni korisnici mogu da pokušaju da pristupe resursima organizacije, da izvedu DoS napade ili da instaliraju viruse na računare organizacije i time naprave još veću štetu

ŠTA JE FIREWALL

Hardver ili softver koji kontroliše šta može da uđe u zaštićenu mrežu, a ponekada i šta iz nje izlazi

U manjim organizacijama ili u kućnim uslovima firewall je najčešće softver instaliran na računaru

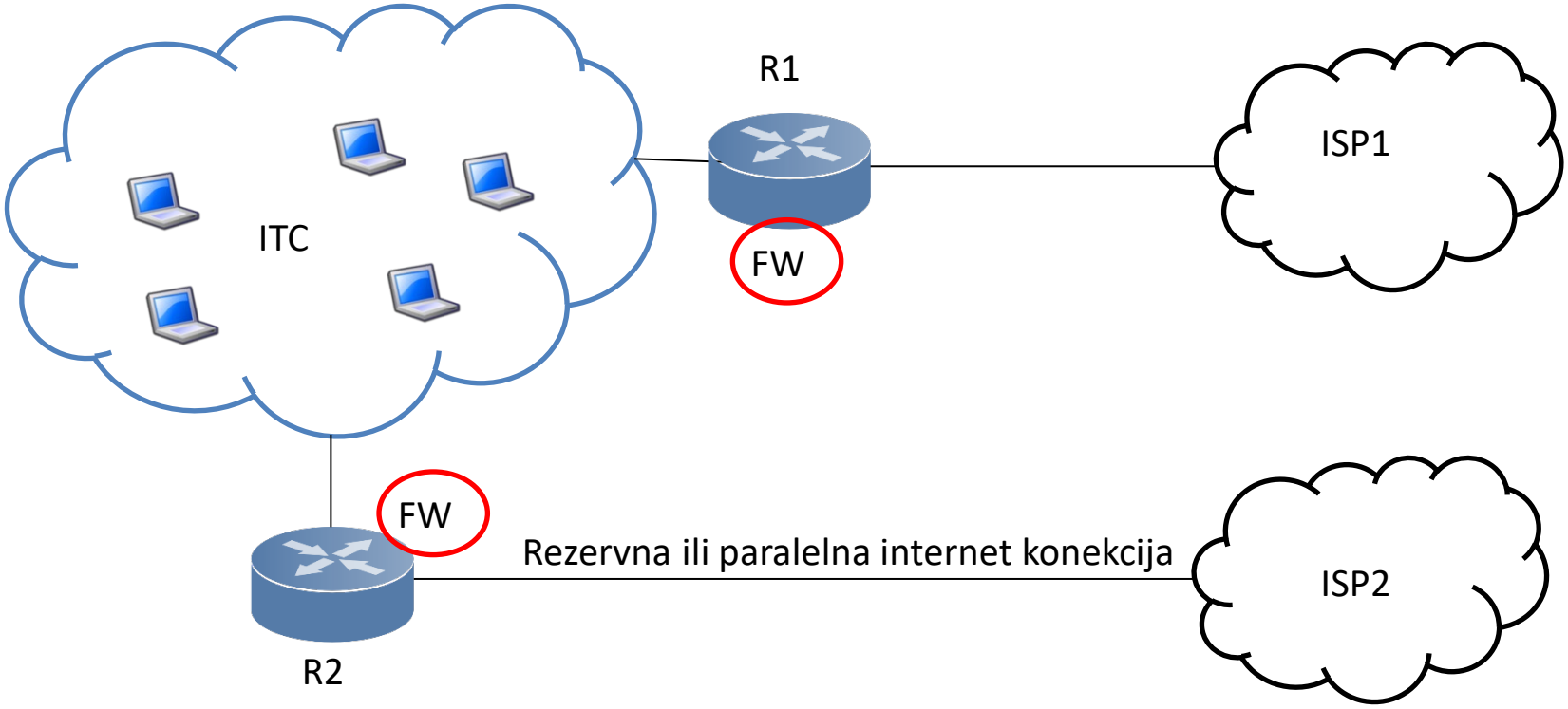
U velikim organizacijama firewall je zaseban uređaj sa specijalizovanim softverom koji kontroliše šta može da uđe u mrežu i šta iz nje izlazi

Na kom mrežnom uređaju je najbolje postaviti firewall?

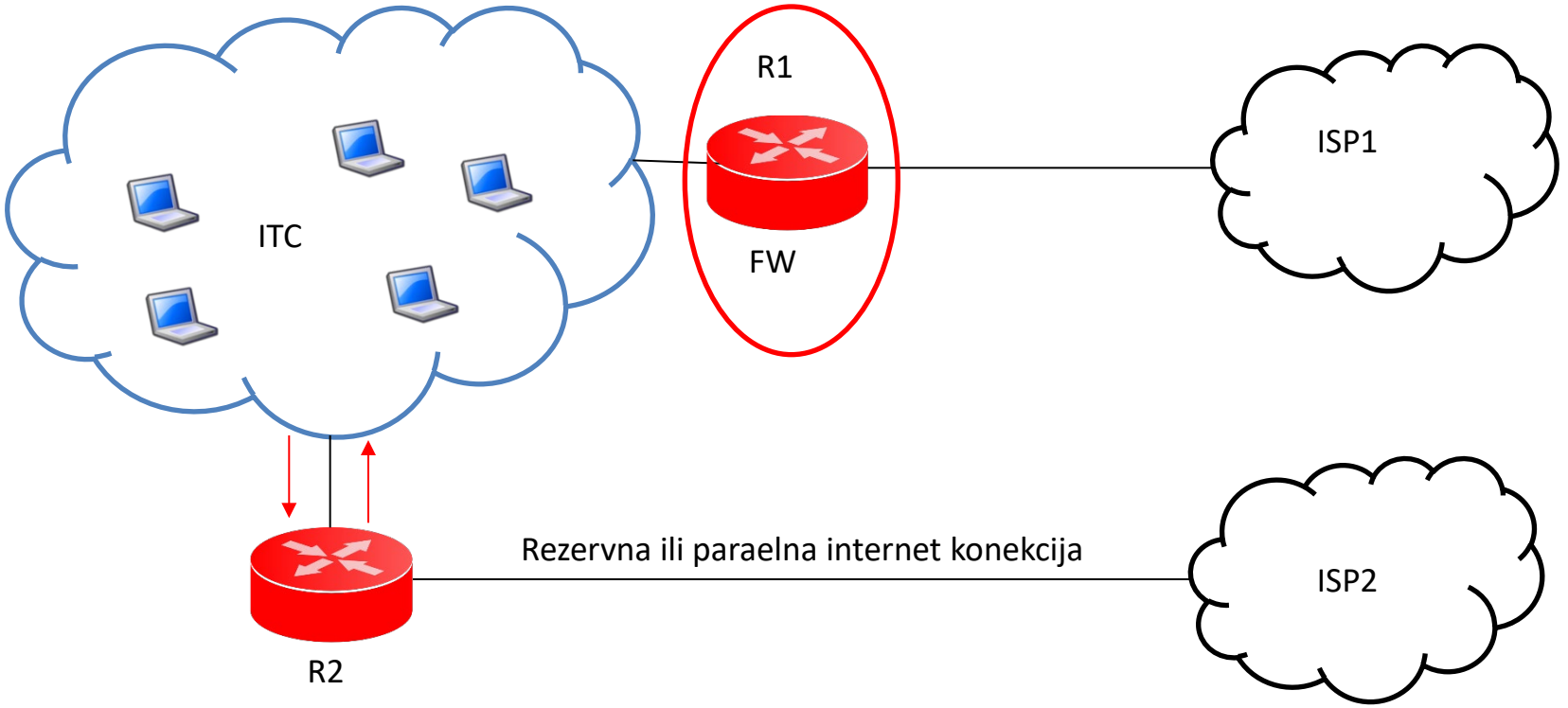
Najbolje rešenje je ruter ili firewall uređaj koji spaja internu i eksternu mrežu. Na taj način će biti zaštićeni svi uređaji unutar interne mreže.

- Ciljevi dizajna
  - Kompletan saobraćaj iz spoljašnje u unutrašnju mrežu i iz unutrašnje u spoljašnju mrežu mora da prođe kroz Firewall
  - Samo autorizovanom saobraćaju će biti dozvoljeno da prođe – unapred definisano lokalnom sigurnosnom politikom
  - Firewall sam po sebi mora da bude imun na proboje

- Opšte tehnike
  - Service control (kontrola servisa) - filter se zasniva na IP adresi, broju porta i td.
  - Direction control (kontrola smera) - ka internoj mreži, ka eksternoj mreži
  - User control (kontrola korisnika) – student ili profesor
  - Kontrola ponašanja – filtriranje elektronske pošte sa spam-om



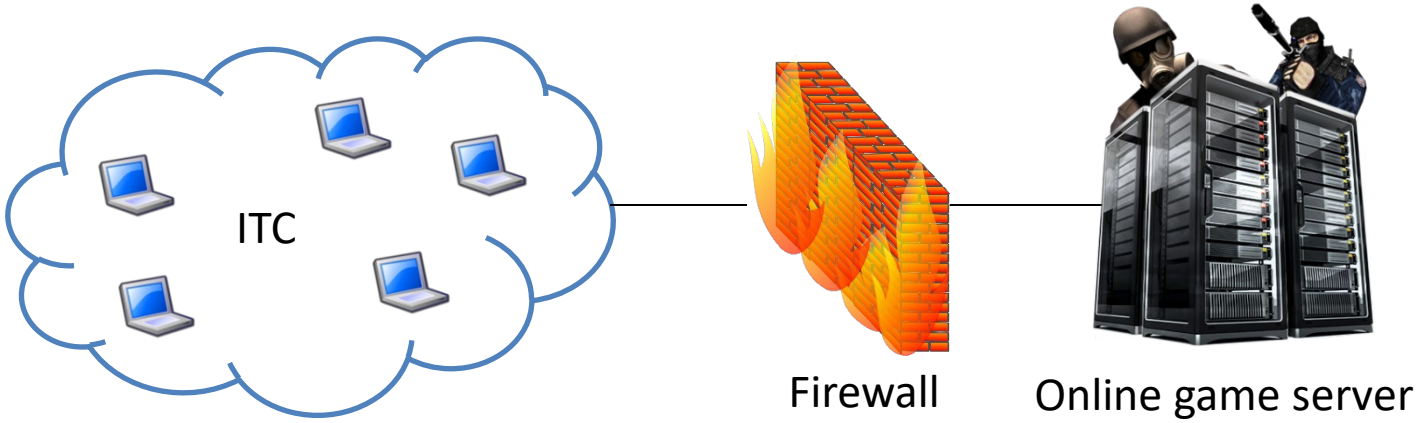
- Najbitnija stvar je da sav dolazni i odlazni saobraćaj prođe kroz firewall
- Očigledna pozicija firewall-a u ovom preimeru je na ruteru koji spaja mrežu ITC sa provajderom
- Problem je u tome što većina organizacija ima više konekcija ka spoljnoj mreži
- U koliko interna mreža ima više veza sa spoljašnjom mrežom, FW mora biti primenjen na svim ruterima koji spajaju unutrašnju i spoljašnju mrežu



- U koliko firewall primenimo samo na ruteru 1 a zatim podatke šaljemo preko drugog linka firewall na ruteru 1 taj saobraćaj ne može da kontroliše i kao rezultat toga u mrežu može da uđe neki malware.
- Ovo je veoma komplikovano kod velikih mreža zato što one imaju veliki broj ulaznih i izlaznih tačaka

- Ciljevi dizajna
  - Kompletan saobraćaj iz spoljašnje u unutrašnju mrežu i iz unutrašnje u spoljašnju mrežu mora da prođe kroz Firewall
  - Samo autorizovanom saobraćaju će biti dozvoljeno da prođe – unapred definisano lokalnom sigurnosnom politikom
  - Firewall sam po sebi mora da bude imun na proboje
- Opšte tehnike
  - Service control (kontrola servisa) - filter se zasniva na IP adresi, broju porta...
  - Direction control (kontrola smera) - ka internoj mreži, ka eksternoj mreži
  - User control (kontrola korisnika) – student ili profesor
  - Behaveour control (kontrola ponašanja) – filtriranje elektronske pošte sa spam-om

- Pravila šta može da uđe u mrežu i šta iz nje može da izađe
- Npr. želimo da zabranimo da se sa računara ITC mreže pristupa online igricama



- U firewall unosimo IP adrese poznatih online game servera i postavljamo pravilo da svi paketi iz ITC mreže upućeni ka ovim IP adresama budu odbačeni
- Rezultat je da se sa računara ITC mreže ne može pristupiti online igricama
- Određena pravila definišu šta želimo da postignemo pomoću firewall-a

Samo autorizovanom saobraćaju će biti dozvoljeno da prođe unapred definisanom lokalnom sigurnosnom politikom

- Ciljevi dizajna
  - Kompletan saobraćaj iz spoljašnje u unutrašnju mrežu i iz unutrašnje u spoljašnju mrežu mora da prođe kroz Firewall
  - Samo autorizovanom saobraćaju će biti dozvoljeno da prođe – unapred definisano lokalnom sigurnosnom politikom
  - Firewall sam po sebi mora da bude imun na proboje

- Opšte tehnike
  - Service control (kontrola servisa) - filter se zasniva na IP adresi, broju porta ...
  - Direction control (kontrola smera) - ka internoj mreži, ka eksternoj mreži
  - User control (kontrola korisnika) – student ili profesor
  - Behaveour control (kontrola ponašanja) – filtriranje elektronske pošte sa spam-om

- Veoma važna stvar je da firewall ne može da bude kompromitovan
- Firewall je bezbedonosni uređaj i on kontroliše šta može da uđe u mrežu i šta iz nje izlazi.
- Ako napadač kompromituje FW tada napadač ima punu kontrolu nad FW sistemom a samim tim i na saobraćaj koji može da prolazi kroz FW.

Firewall mora da bude imun na proboje

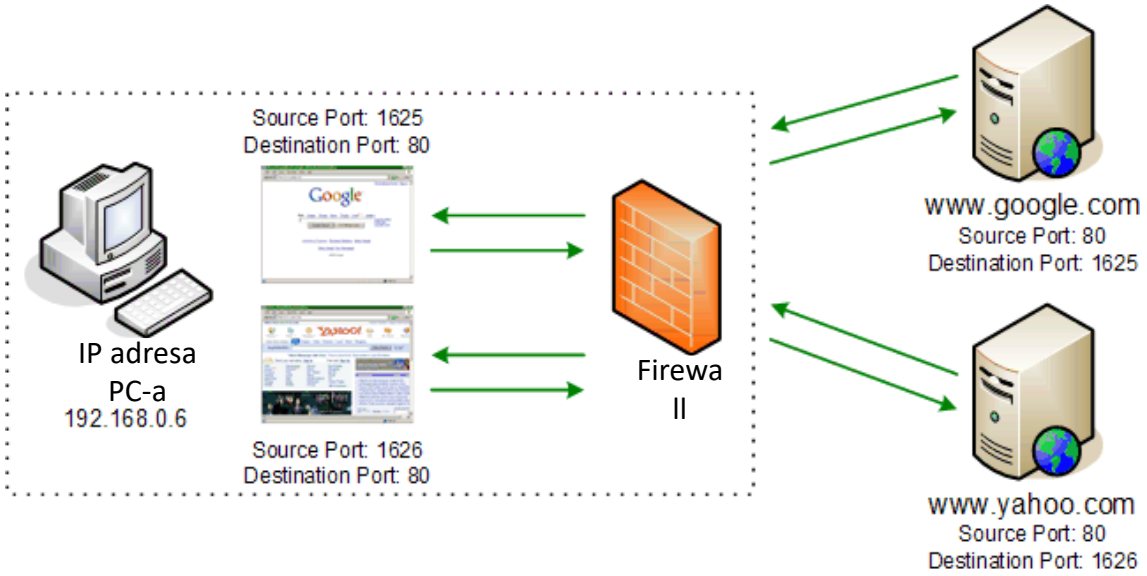
IMPLEMENTACIONA FIREWALL PRAVILA

Četiri opšte tehnike:

1) Kontrola servisa
   - filter se zasniva na IP adresi, broju porta ...
2) Kontrola smera
   - definiše smer saobraćaja ka internoj ili eksternoj mreži
3) Kontrola korisnika
   - nivo pristupa resursima
4) Kontrola ponašanja
   - filtriranje elektronske pošte koja dolazi kao spam

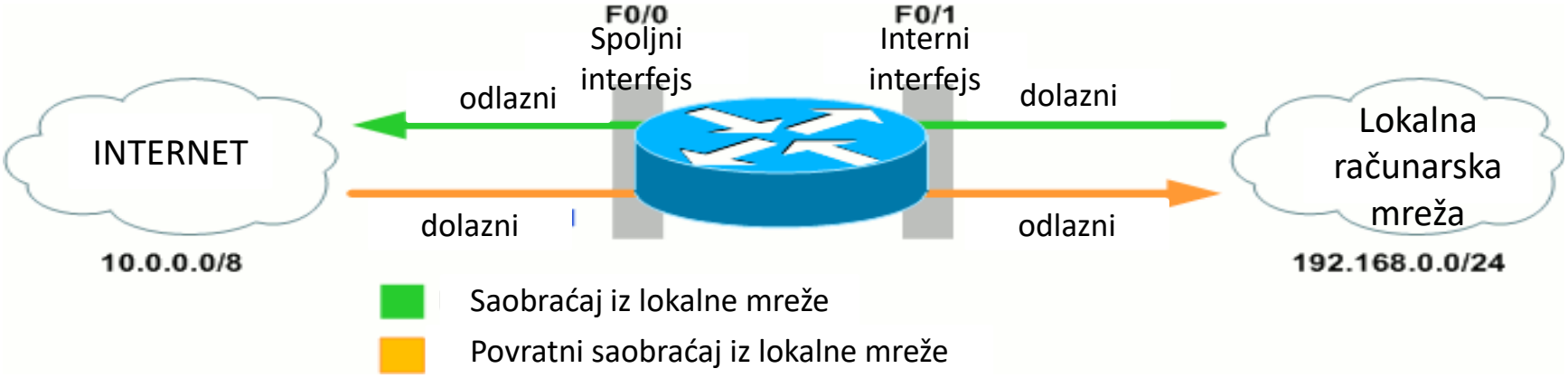
KONTROLA SERVISA

- Za identifikaciju različitih servisa najčešće se koriste adrese (IP i PORT)
- Na osnovu IP adrese i broja porta kontroliše se filtriranje paketa u zavisnosti od FW pravila
- Npr. ako znamo IP adrese najpopularnijih gejmerskih servera, postavićemo pravilo da ako bilo koj paket iz interne mreže ide na neku od tih IP adresa biće blokiran
- Ako neko iz spoljne mreže želi da pristupi SSH serverima u internoj mreži možemo da koristimo broj porta da to sprečimo



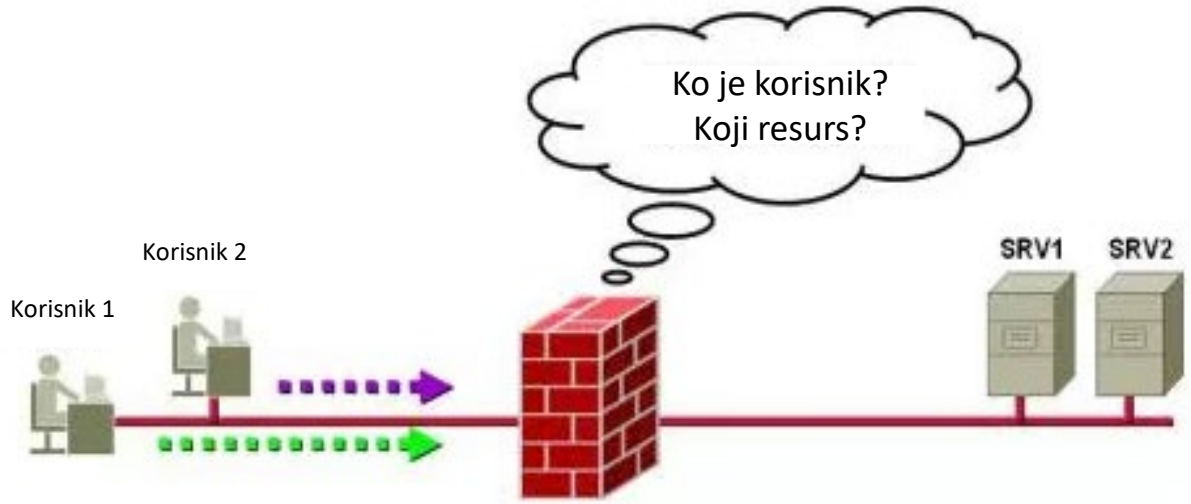
KONTROLA SMERA

- Kontrola smera – odluku o kontroli smera donosimo na osnovu odakle paket dolazi
- Ako paket dolazi iz spoljašnje mreže koristimo jedna pravila, a ako paket iz unutrašnje mreže odlazi u spoljašnju druga pravila
  - Ako studentima želimo da zabranimo da igraju online igrice, pravilo se primenjuje na saobraćaj koji iz interne mreže odlazi ka spoljnoj mreži
  - Ako želimo malware da zaustavimo da uđe u našu internu mrežu interesantan saobraćaj nam je dolazni saobraćaj
- Kreiraju se različita pravila u zavisnosti od toga da li je saobraćaj dolazni ili odlazni



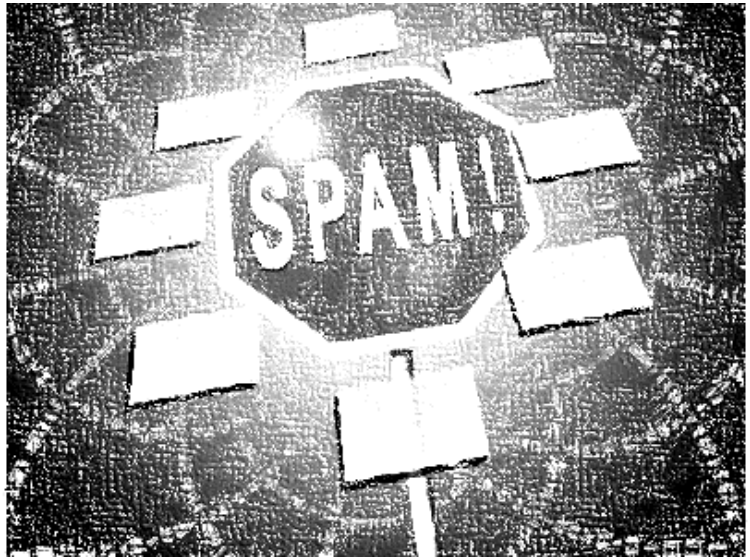
KONTROLA KORISNIKA

- Kontrola korisnika – zasniva se na tome ko generiše određene pakete
  - Zabrana studentima da igraju online igrice ali ne i osoblju ITC-a.
- Kreira se pravilo koje prepoznaje korisnike
- Firewall-a pored toga što gleda servise i smer kretanja paketa, proverava i to ko je generisao paket i na osnovu toga donosi odluke.



KONTROLA PONAŠANJA

- Firewall može da prati i sadržaj podataka
  - Npr. kontrola email-a koji kada stigne do internu mrežu FW odradi inspekciju tog mail-a na spam poruke i viruse
  - Ako FW otkrije spam poruku ili virus u mail-u ili ga blokira ili očisti mail pre prosleđivanja krajnjem korisniku.



MOGUĆNOSTI I OGRANIČENJA

- Mogućnosti
  - Obezbeđuje lokaciju za praćenje bezbedonosnih događaja
  - Pogodna platforma za neke funkcionalnosti koje nisu vezane za bezbednost
  - Može da posluži kao platforma za VPN i endpoint

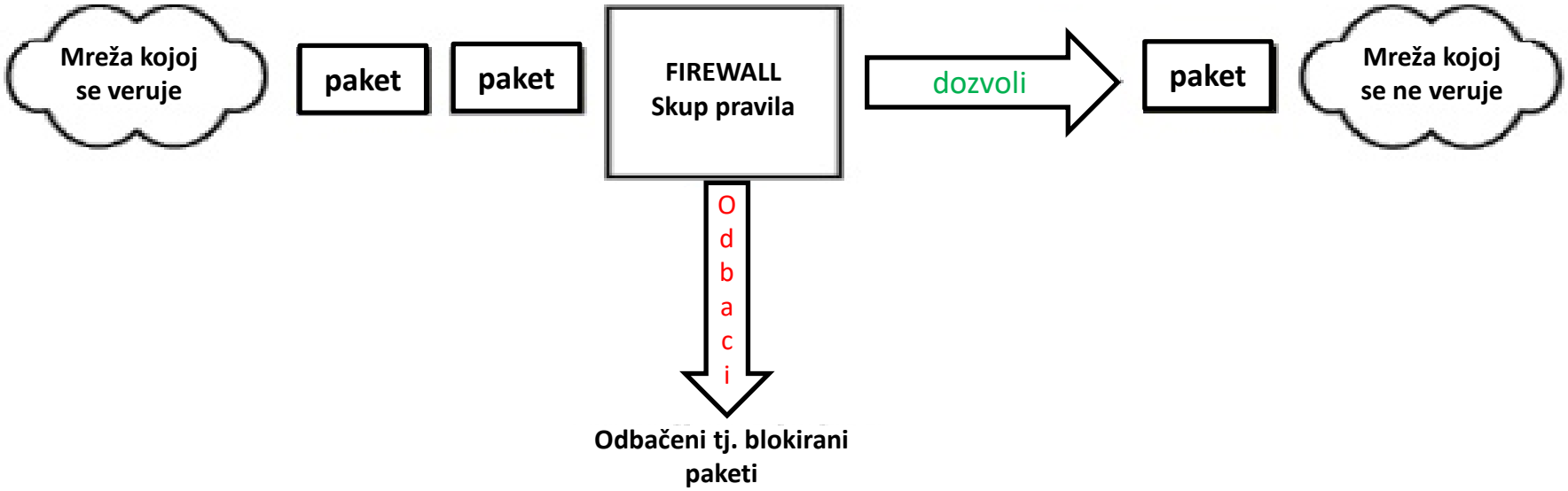
- Ograničenja
  - Ne može da štiti od napada koji zaobiđu FW
  - Ne može da štiti od opasnosti iz interne mreže
  - Nepravilno obezbeđenoj wireless LAN mreži može se pristupiti sa spoljne mreže
  - Laptop, telefon i USB mogu biti inficirani izvan zaštićene mreže. Kada se unesu u internu mrežu inficiraće i nju

VRSTE MREŽNIH BARIJERA (FIREWALL)

- Filtriranje paketa
- Stateful Packet Inspection
- Aplication Proxy

FILTRIRANJE PAKETA

- Sigurnosna politika se implementira skupom pravila
- Pravila definišu koji paketi mogu da prođu kroz firewall

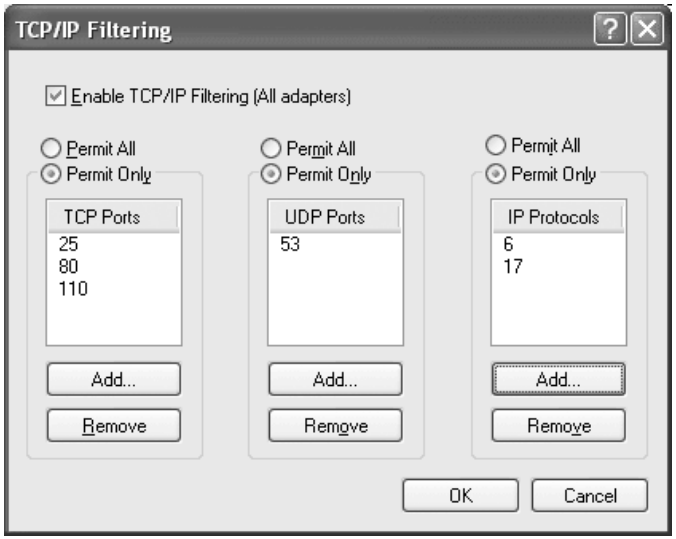


FILTRIRANJE PAKETA

- Firewall proverava svaki paket (dolazni ili odlazni), poredi ga sa setom pravila, i u zavisnosti od toga sa kojim se pravilom podudara preduzima određenu akciju

- Podrazumevana politika je ono što se radi u slučaju da se vrednosti paketa ne podudara ni sa jednim pravilom

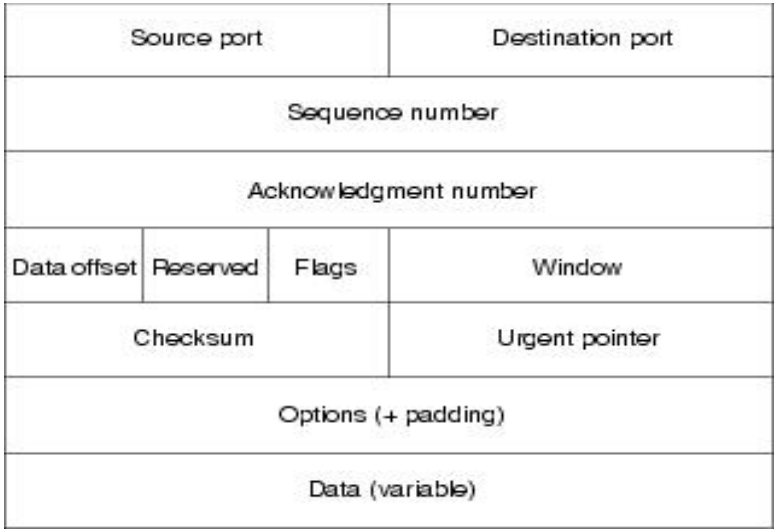
    - Accept – paket se prihvata - PROSLEĐUJE
    - Drop – paket se odbacuje - PREPORUČENO



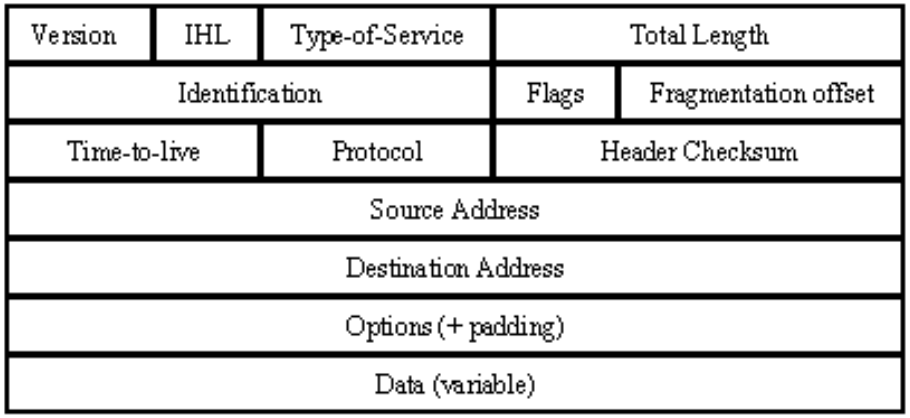
FILTRIRANJE PAKETA

- Filtriranje paketa – uprošćen koncept – na osnovu podataka iz zaglavlja paketa firewall donosi odluku da li paket prosleđuje ili odbacuje
- Zaglavlja paketa – TCP i IP zaglavlje

TCP zaglavlje

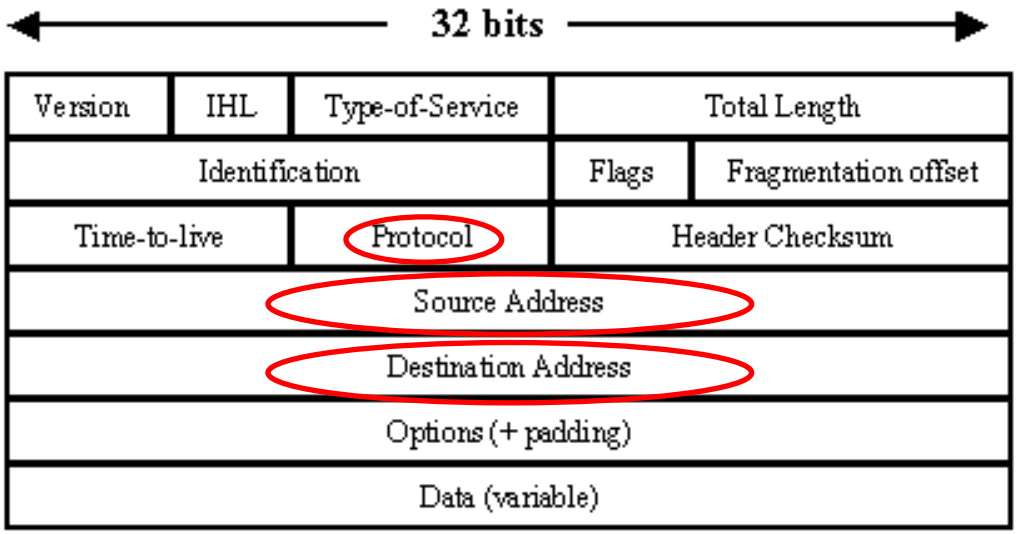


IP zaglavlje



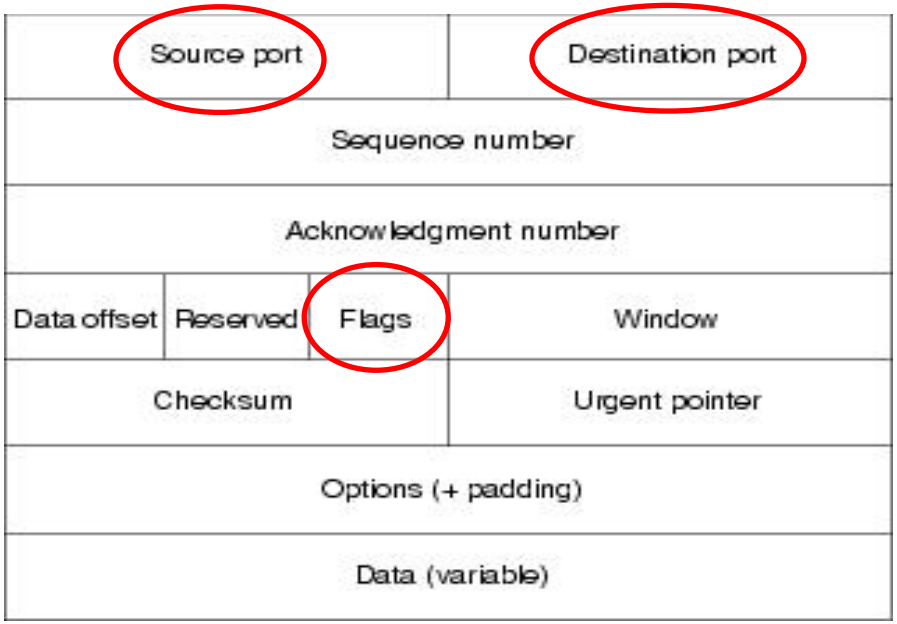
FILTRIRANJE PAKETA

- Polja u zaglavlju koja su značajna za firewall
- U IP zaglavlju važna su izvorišna i odredišna IP adresa – pomoću njih saznajemo koji uređaji komuniciraju.
- Polje Protocol – sadrži podatak o transportnom protokolu koji se koristi (6 ->TCP, 17->UDP)



FILTRIRANJE PAKETA

- U TCP zaglavlju polja koja su interesatna za FW su izvorišni i odredišni port – port definiše koja aplikacija se koristi i polje Flags koje opisuje stanje sesije



FILTRIRANJE PAKETA

- Filtriranja paketa se zasniva na praćenje sledećih polja

Izvorišna IP adresa

Odredišna IP adresa

Broj protokola

Izvorišni port

Odredišni port

- Kada podesimo FW i konfigurišemo pravila ona nam ukazuju da li paket sa tim vrednostima FW treba da propusti ili blokira

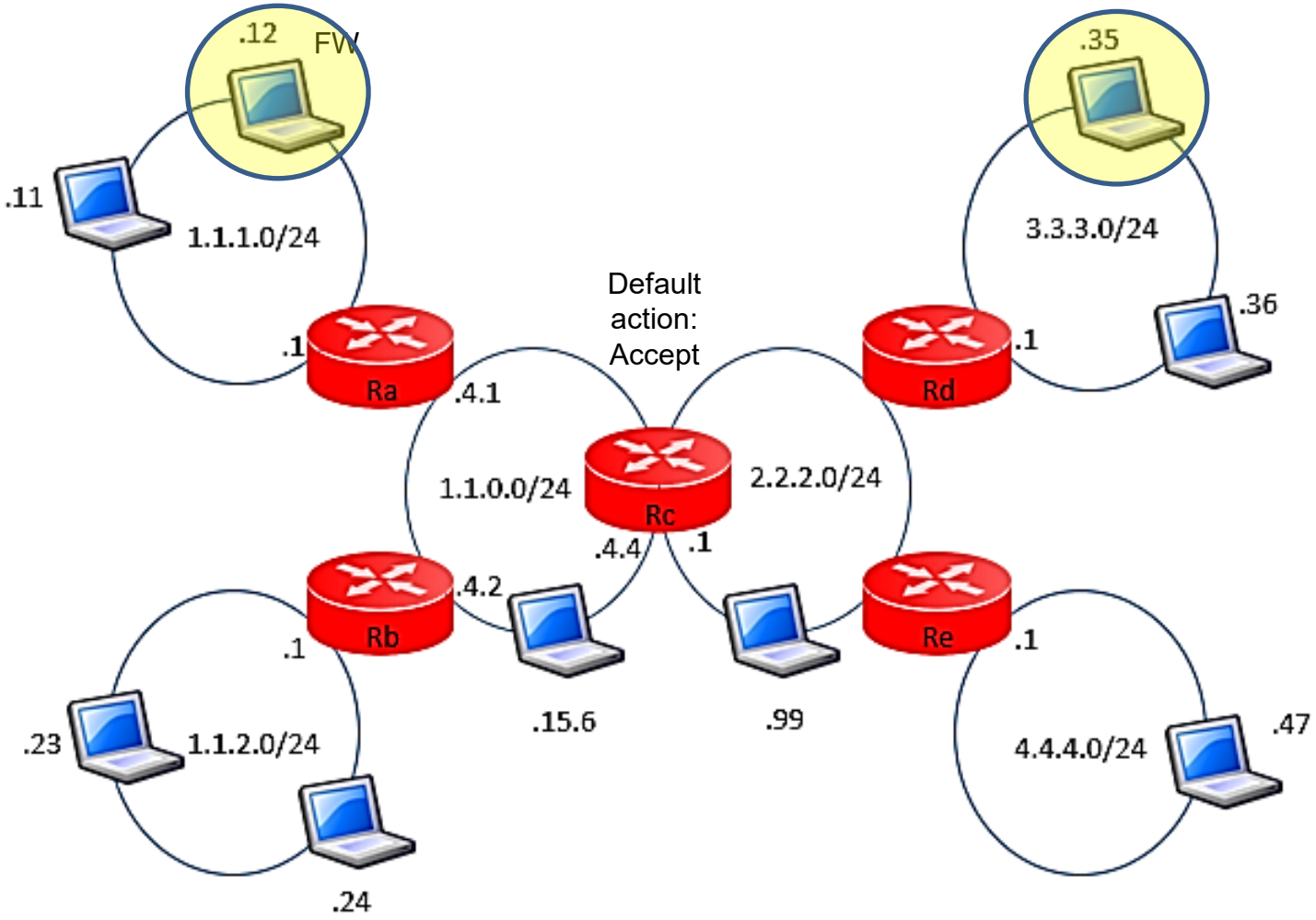
ACCEPT

ili

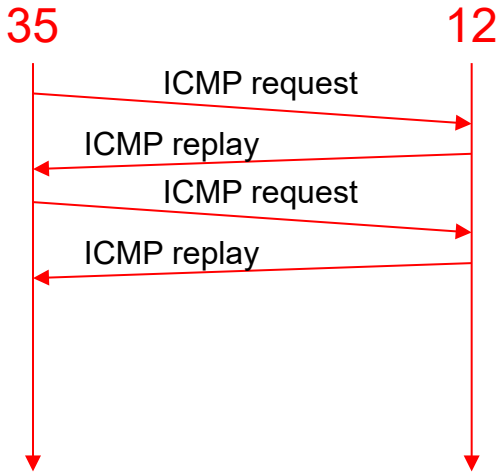
DROP

FW se nalazi na individualnom računaru – kao kod kuće (računar br. 12)

Zadatak je zaustaviti računar 35 da pinguje računar 12

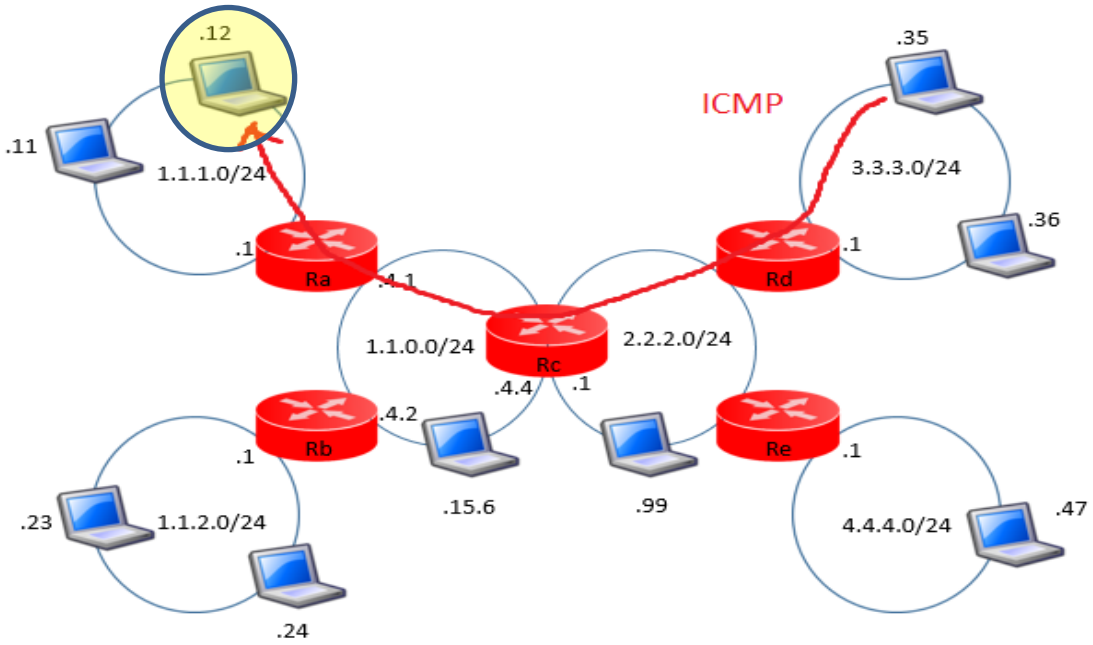


- Ping je alat koji koristi IP protokol a koji primaocu nalaže da odgovori na poruku i vrati pošiljaocu sadržaj koji je dobio u istom paketu. Koristi se za merenje brzine protoka i odziva internet veza. Transportni protokol koji ping koristi je ICMP
  - Uprošćen princip rada

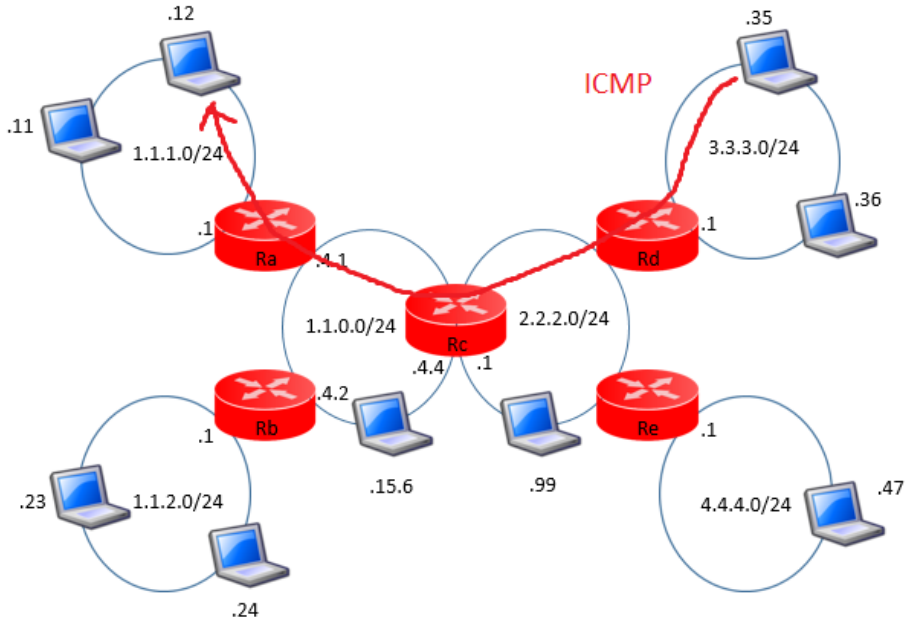


- Kada računar 35 pokuša da pinguje računar 12 on šalje *ICMP echo request* računaru 12.
- Kada računar 12 primi taj zahtev obrađuje ga i nazad šalje odgovor (*ICMP Replay*)
- Ping ponavlja ICMP zahteve svake sekunde, posle nekog vremena ponovo će uraditi isto

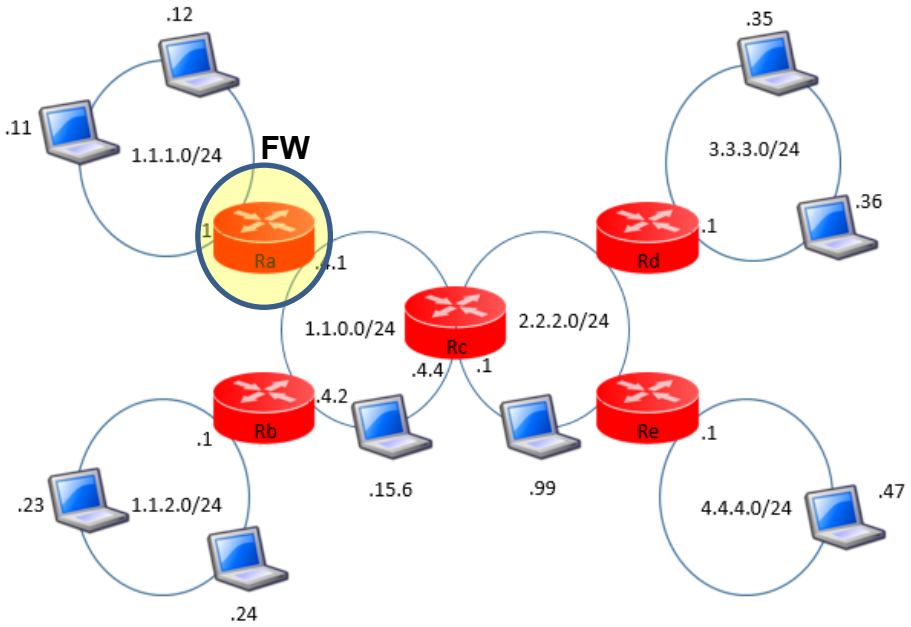
- Zadatak je da podesimo firewall na računaru 12 tako da ping ne radi.
- Računar 12 ne može da spreči računar 35 da pošalje zahtev već kada zahtev stigne, firewall treba da odbaci taj paket pre nego on dođe do ping softvera.
- Ključna polja u ovom slučaju su:
  - Izvorišna adresa = 3.3.3.35
  - Odredišna adresa = 1.1.1.12
  - Protocol = 1 (Ping koristi trasnportni protokol ICMP)
  - ICMP ne koristi brojeve porta



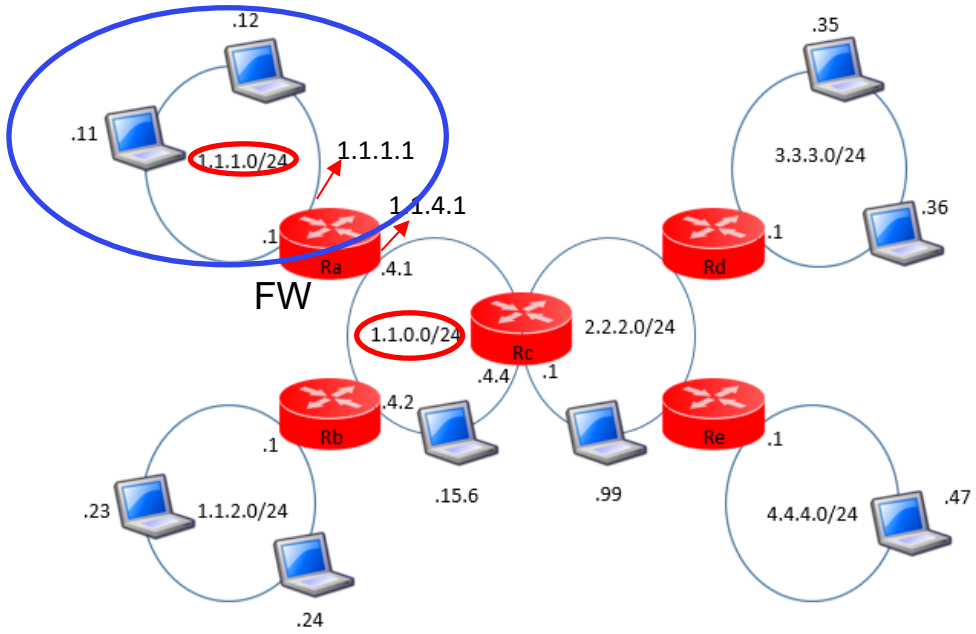
- U ovom slučaju naše pravilo sadrži samo tri parametra:
  - SrcIP = 3.3.3.35
  - DestIP = 1.1.1.12
  - Protocol= 1
- Rezultat je da ping softver na računaru 12 neće dobiti paket i neće biti odgovora na ping zahtev.
- Ping više ne funkcioniše.



- U primeru 1 je firewall softver instaliran na laptop-u.
- To je rešenje u koliko treba da se zaštiti samo jedan računar.
- U slučaju da treba da se zaštite računari kompanije, a njih je obično mnogo, na način iz primera 1 morali bi da instaliramo i konfigurišemo FW na svakom od tih računara.
- To je nepraktično i lako dolazi do greške u konfiguraciji računara.
- U slučaju mreže kompanije, pametnije je firewall postaviti mrežni uređaj poput rutera.
- Pravila se konfigurišu tako da štite sve računare te mreže.



- Firewall premeštamo sa laptopa na ruter R1.
- Ruter R1 je običan ruter sa firewall softverom u sebi.



- Ruter R1 povezuje mrežu 1.1.1.0/24 i 1.1.0.0/24.
- Ruter R1 ima dva interfejsa i kao rezultat toga 2 IP adrese (1.1.1.1 i 1.1.4.1)
- Mreža 1.1.1.0/24 je interna mreža, ona koju treba da zaštitimo
- Cilj je zaštititi mrežu 1.1.1.0/24 i sve računare te mreže.

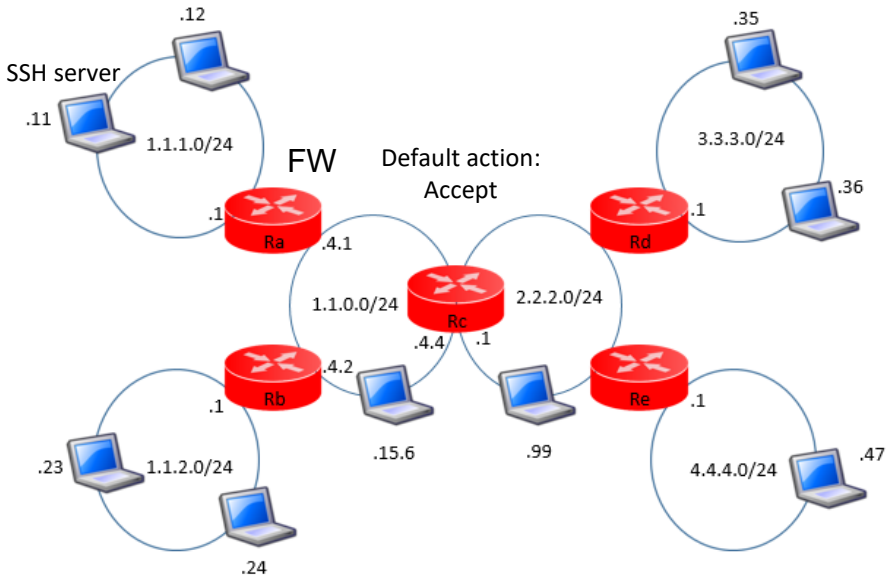
- Na računaru 11 u internoj mreži imamo SSH server.
- Cilj je zabraniti bilo kom računaru iz spoljne mreže pristup tom SSH serveru.
- FW pravilo treba da uključi 5 uslova:

Korak 1 – Definišu se sledeće 5 vrednosti

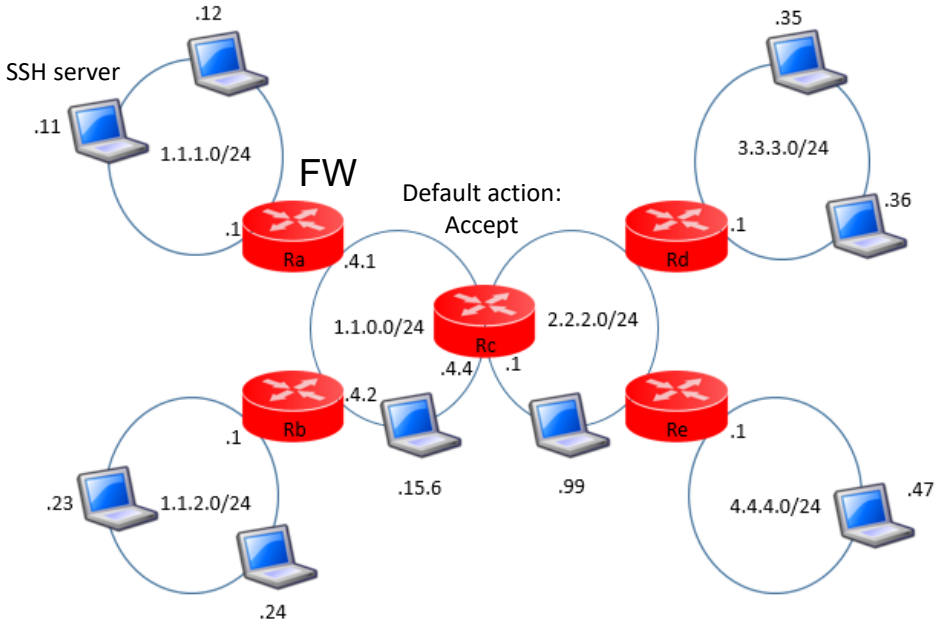
- SrcIP=?
- DestIP=?
- Protocol=?
- SrcPort=?
- DestPort=?

Korak 2 - Akcija koja će se izvršiti ukoliko se vrednosti paketa podudara sa ovih 5 vrednosti

- Action=?



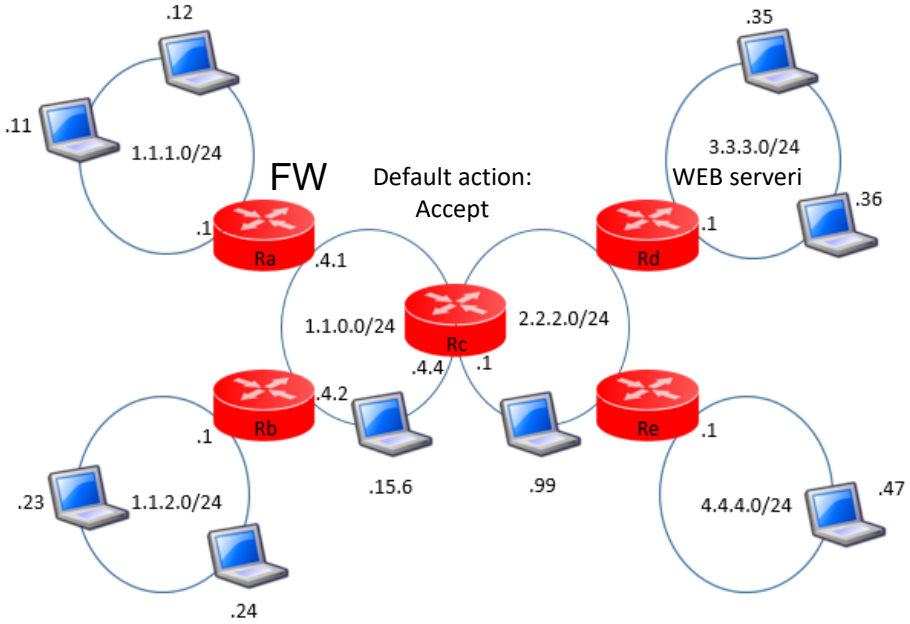
- Karakteristike koje ima paket u slučaju da neko pokuša da pristupi SSH serveru na računaru 11?



- SrcIP=* (Ne želimo nikome iz spoljne mreže da dozvolimo da pristupi SSH serveru na računaru 11)
- DestIP=1.1.1.11
- Protocol=6 (TCP) – SSH koristi transportni protokol TCP. Potreban nam je broj porta
- SrcPort=* (Izvorišni port je dinamički i promeniće se svaki put kada klijent pošalje paket)
- DestPort=22 (SSH)

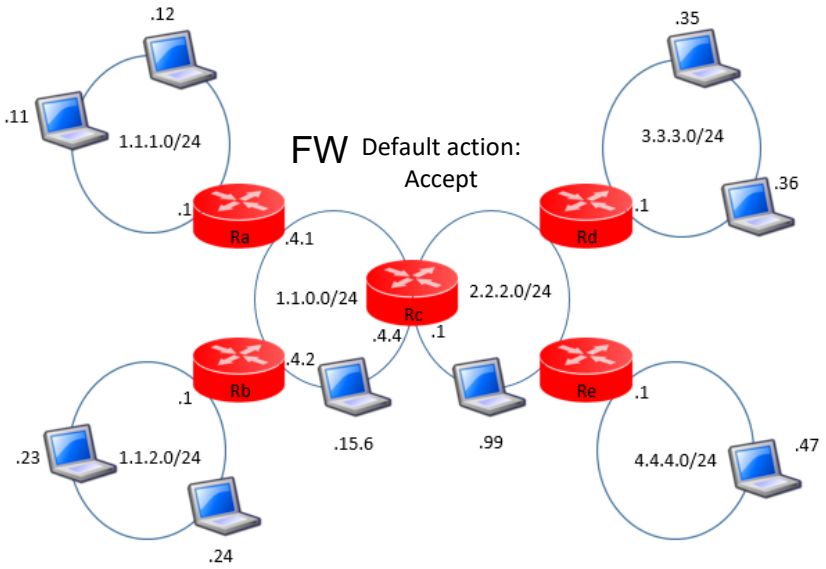
Zadatak:

- Zaustaviti računar 12 da pristupi web serverima koji se nalaze u mreži 3 (3.3.3.0/24). Podrazumevana akcija i dalje je Accept.



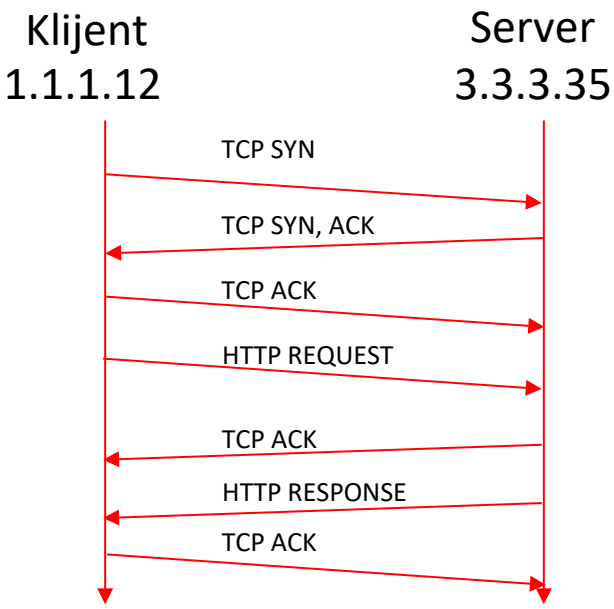
- U ovom slučaju se kreira pravilo u suprotnom smeru u odnosu na primer 2.
- Želimo da zabranimo računarima iz unutrašnje mreže da pristupe podacima u spoljašnjoj mreži.
- Podrazumevana akcija je Accept.

- Razmatramo 5 kriterijuma
  - SrcIP=1.1.1.12
  - DestIP=3.3.3.0/24
  - Protocol=6
  - SrcPort=*
  - DestPort=80
  - Action=DROP



- Ako u web browser na računaru 12 unesemo web adresu 3.3.3.35 paket kreće od računara 12 i stiže do rutera, firewall pregleda taj paket, mečuju se parametri – paket se odbacuje.
- Ovo pravilo može da se zaobiđe korišćenjem porta 443 koji koristi HTTPS.
- Isti paket će biti poslat samo preko porta 443 i firewall neće odbaciti paket.
- Prilikom pisanja pravila ako želimo da zabranimo pristup web serverima pored porta 80 treba da unesemo i port 443.
- Često se javlja potreba za specijalnim slučajevima koje moramo uzeti u obzir kako ih neko ne bi iskoristio da zaobiđe pravila.

Uspostavljanje TCP i HTTP konekcije

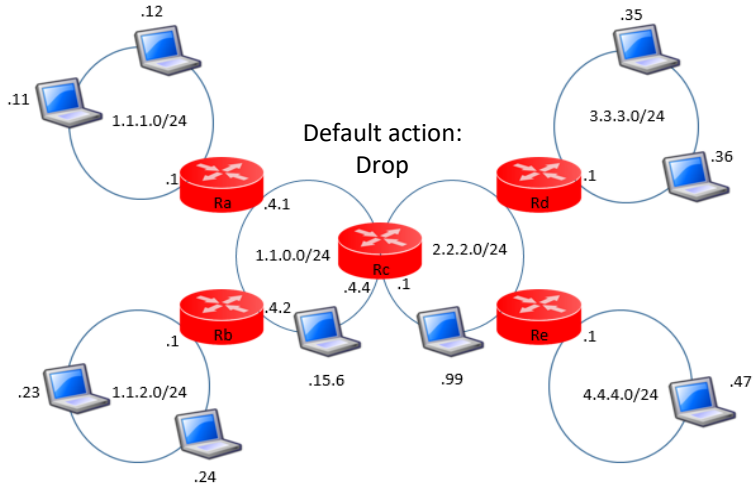


- Browser šalje SYN poruku u želji da se sinhronizuje sa serverom
- Server šalje odgovor – TCP poruku koja sadrži: OK, primio sam tvoju poruku za sinhronizovanje i želim da se sinhronizujem sa tobom
- Vraća se ACK paket od klijenta ka serveru i u tom trenutku konekcija je uspostavljena
- Sledi razmena podataka između klijenta i servera preko porotokola na aplikativnom sloju.

Cilj:

- Dozvoliti računaru 12 da pristupi web serveru na mreži 3.3.3.0/24.
- Podrazumevana akcija je Drop.

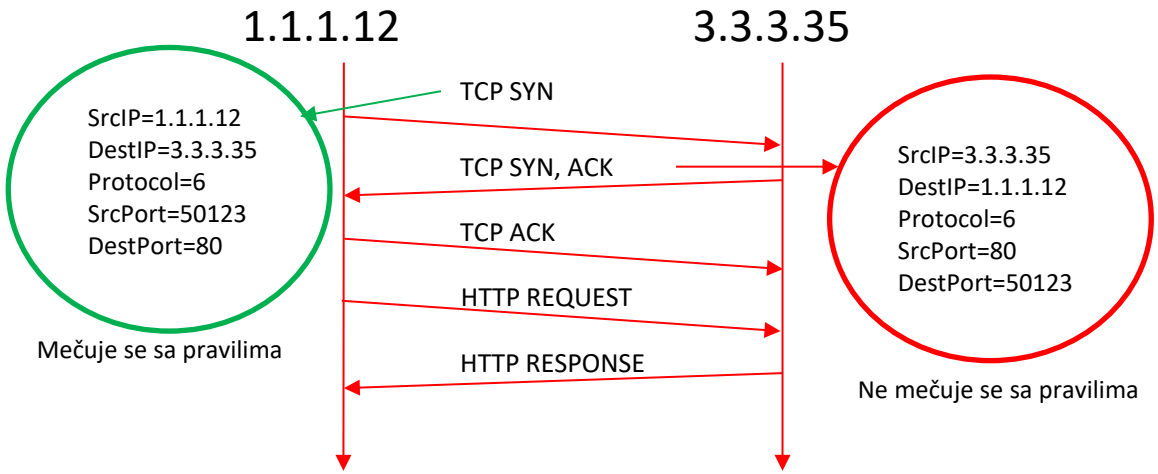
- SrcIP=1.1.1.12
- DestIP=3.3.3.0/24
- Protocol=6
- SrcPort=*
- DestPort=80
- Action=Accept



- Razlika u odnosu na prethodni primer je u akciji koju preduzimamo u slučaju da se parametri paketa ne podudaraju sa pravilima FW.
- Ideja ovde je da odbacujemo sve pakete sem onih čiji se parametri mečuju sa našim pravilima.

- Da li će sa gore navedenim pravilima naš cilj biti postignut?

- Parametri TCP SYN paketa se slažu sa pravilima firewall-a i ovaj paket će biti propušten dalje.
- TCP SYN paket dolazi do servera i server nazad šalje TCP SYN,ACK paket.
- Šta će da se desi sa ovim paketom kada dođe do firewall-a?



- Parametri TCP SYN,ACK paketa se ne podudaraju sa pravilima firewall-a zbog čega će firewall odbaciti ovaj paket, i neće biti komunikacije između klijenta i servera.
- Pravilo koje smo napisali ne omogućava nam komunikaciju između klijenta i servera.

- Rešenje ovog problema je novo pravilo koje će omogućiti prolazak povratnih paketa kroz firewall

SrcIP	DestIP	Protocol	SrcPort	DestPort	Action
1.1.1.12	3.3.3.0/24	6	*	80	Accept
3.3.3.0/24	1.1.1.12	6	80	*	Accept

- TCP SYN,ACK paket će biti propušten kroz firewall, a i svi sledeći paketi ove komunikacije će se podudarati sa jednim od ova dva pravila
- Bilo nam je potrebno jedno pravilo koje omogućava paketima da izađu iz mreže i drugo pravilo koje odgovorima omogućava da se vrate nazad.

- Kada ima više pravila u firewall-u obrađuju se redom.
- Poredimo parametre paketa sa prvim pravilom, ako se podudaraju izvršava se akcija a ako se ne podudaraju prelazi se na sledeće pravilo.
- Ako se parametri paketa ne podudaraju ni sa jednim pravilom vrši se podrazumevana akcija.

PODRAZUMEVANA AKCIJA ACCEPT VS DROP

- Kada se podešava FW nije to samo jedno ili dva pravila.
- U realnoj situaciji tih pravila je mnogo.

- Bitno je voditi računa o tome da prilikom podešavanja FW ne dođe do greške.
- Ako se napravi propust FW neće funkcionisati kako treba i to može da dovede ili do ugrožavanja bezbednosti ili do problema za korisnike prilikom korišćenja određenih aplikacija tj. servisa.

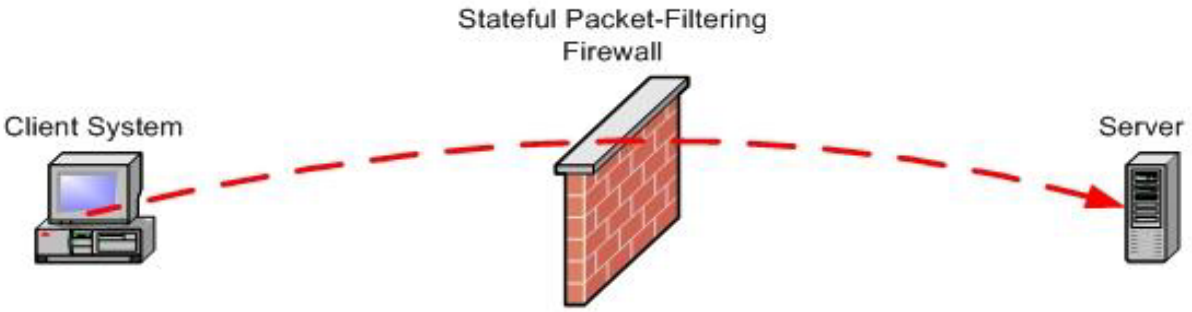
- U slučaju podrazumevane akcije Accept, u slučaju greške napadači iz spoljne mreže mogu lako da pristupe internoj mreži jer podrazumevana politika prihvata sve.
- To je osnovni problem sa Accept podrazumevanom politikom.

- U slučaju podrazumevane politike Drop, ako dođe do greške prilikom konfigurisanja pravila najčešće se ne ugožava bezbednost već korisnici imaju problem prilikom pokušaja da koriste određene aplikacije.

- FW ima dva pravila:
  - jedno da propušta pakete od klijenta ka serveu i
  - drugo da propusti pakete od servera ka klijentu.
- Potencijalni bezbedonosni problem?
  - Maliciozni korisnik može na nekom od računara u mreži 3.3.3.0/24 da kreira aplikaciju (posebnu aplikaciju samo za ovaj napad) koja koristi port 80 i da je pošalje računaru 1.1.1.12.
  - Ovaj paket će se mečovati sa drugim pravilom našeg FW i maliciozni korisnik će dobiti pristup internoj mreži
- Drugim pravilom nismo omogućili samo odgovorima web zahteva da uđu u internu mrežu već i svim ostalim paketima koji se mečuju sa pravilima.
- Rešenje je da se drugo pravilo odnosi samo na odgovore web servera.
- Rešenje je Stateful Packet Inspection

STATEFUL PACKET INSPECTION

- Tradicionalno filtriranje paketa donosi odluke za svaki paket pojedinačno i ne uzima u obzir prošle pakete
- Mnoge aplikacije moraju da uspostave prvo konekciju između klijenta i servera – toj konekciji pripada grupa paketa
- Često je lakše definisati pravilo za konekciju nego za individualne pakete
- Potrebno je sačuvati informacije o ranijem ponašanju
- SPI je proširenje tradicionalnog filtriranja paketa praćenjem svih TCP konekcija kreiranjem SPI tabele u kojoj se prati stanje konekcije
- Svaka TCP konekcija počinje procedurom rukovana(Syn, Syn-Ack i Ack) i završava se Fin paketom ili posle određenog perioda neaktivnosti.

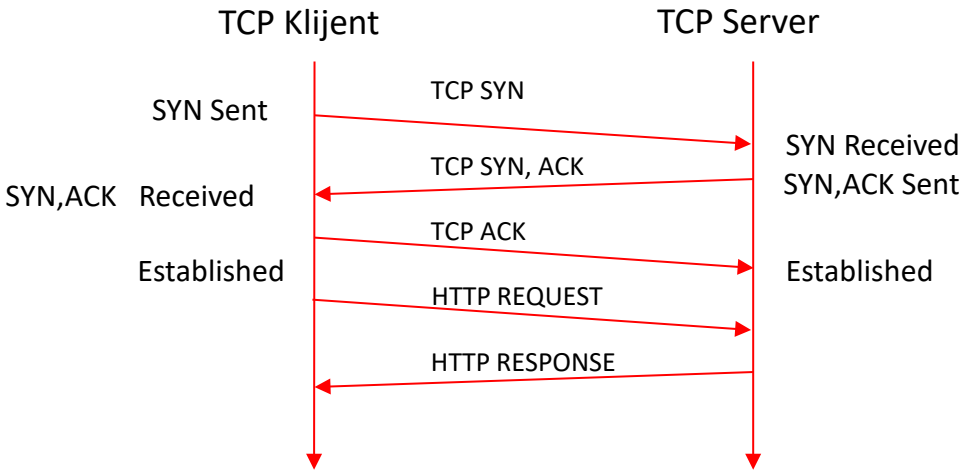


STATEFUL PACKET INSPECTION - KONCEPT

- U cilju zaobilaženja ovih problema koristimo *Stateful Packet Inspection*.
  - Koncept SPI je da kreira pravilo koje će paketu dozvoliti da izadje iz mreže ili da prvi paket razmene bude prihvaćen.
  - Kada se to dogodi FW čuva informacije koje omogućavaju da svi naredni paketi povezani sa ovim prvim paketom budu automatski prihvaćeni.
  - SPI je ključno svojstvo za većinu FW. Čini stvari mnogo jednostavnijim zato što nam je potrebno samo pravilo za propuštanje inicijalnog paketa. Svi ostali paketi koji pripadaju toj komunikaciji biće automatski propušteni kroz FW bez prethodne provere FW pravila.

STATEFUL PACKET INSPECTION – PRAĆENJE KONEKCIJE

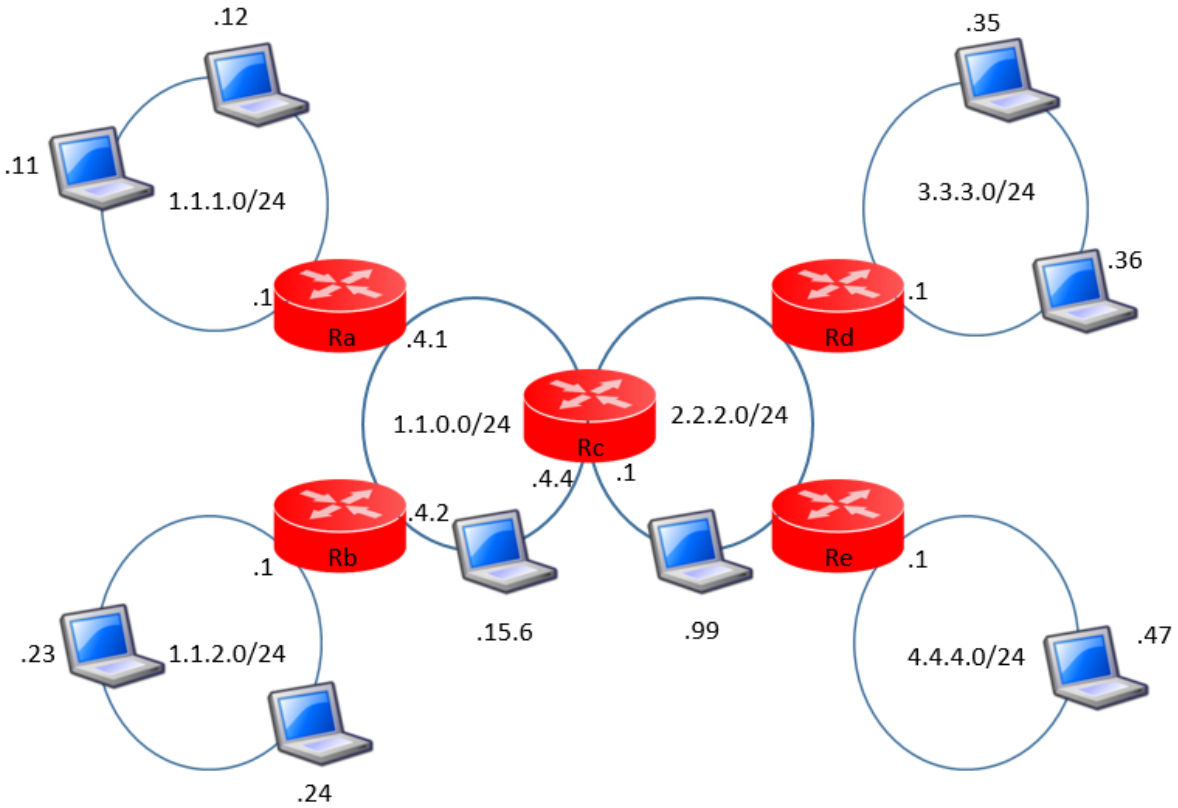
- SPI čini podešavanje FW mnogo lakšim
- SPI prati stanje konekcije koja je uspostavljena.
- TCP konekcija je na početku zatvorena, nakon slanja SYN, SYN+ACK i ACK paketa ona je uspostavljena, i nakon završetka slanja paketa konekcija se zatvara.
- Konekcija prolazi kroz više stanja a SPI prati ta stanja.
- Stanja kroz koja ona prolazi



Kada želimo da zatvorimo konekciju možemo da pošaljemo paket koji će stanje konekcije promeniti u TIME_WAIT (čeka se zatvaranje konekcije). Nakon zatvaranja konekcije stanje je CLOSED.

STATEFUL PACKET INSPECTION - PRIMER

Zadatak:
Omogućiti računaru 12 da pristupi web serveru na računaru 3.3.3.35 korišćenjem SPI



- Želimo da dozvolimo računaru 12 da pristupi web serveru na računaru 3.3.3.35.
- Potrebno nam je pravilo koje će prvom paketu (TCP SYN) da omogući da izađe iz mreže i dođe do servera.

FW Table Default action: Drop

Src	Dest	Protocol	Action
1.1.1.12:*	3.3.3.0/24:80	6	Accept

- Pored FW tabele kreira se i SPI tabela koja je na samom početku prazna
- Prilikom komunikacije između računara 12 i računara 35 šalje se paket:

SrcIP=1.1.1.12
DestIP=3.3.3.35
Protocol=6

SrcPort=48037
DestPort=80
Flag=SYN

Šta se dešava kada SYN paket dođe do FW?

- FW prvo proverava SPI tabelu ali u njoj još uvek nema unosa
- Sledeći korak je upoređivanje sa FW pravilima.
- Obzirom da postoji podudaranje FW prosleđuje paket dalje.
- Pored toga što prosleđuje paket FW unosi podatke u SPI tabelu

SPI tabela

Src	Dest	Protocol	State
1.1.1.12:48037	3.3.3.35:80	6	SYN Received

- U sledećem koraku server prima SYN paket i šalje odgovor – TCP SYN,ACK paket

IP	TCP
SrcIP=3.3.3.35	SrcPort=80
DestIP=1.1.1.12	DestPort=48037
Protocol=6	Flag=SYN,ACK

- Server 35 šalje paket računaru 12.
- Paket stiže do FW.
- FW prvo proverava SPI tabelu i na osnovu izvorišne, odredišne adrese i protokola zaključuje da ovaj paket pripada komunikaciji između uređaja 35 i 12.
- Prethodni flag bilo je SYN sad je SYN,ACK što za FW ima smisla i on će ovaj paket automatski prihvatiti.
- State u SPI tabeli se sada menja na SYN,ACK Received

SPI tabela

Src	Dest	Protocol	State
1.1.1.12:48037	3.3.3.35:80	6	SYN,ACK Received

- Treći paket, ACK, se vraća ka serveru.
- Parametri paketa su isti kao kod prvog paketa samo flag nije SYN nego je ACK

IP	TCP

SrcIP=1.1.1.12 SrcPort=48037

DestIP=3.3.3.35 DestPort=80

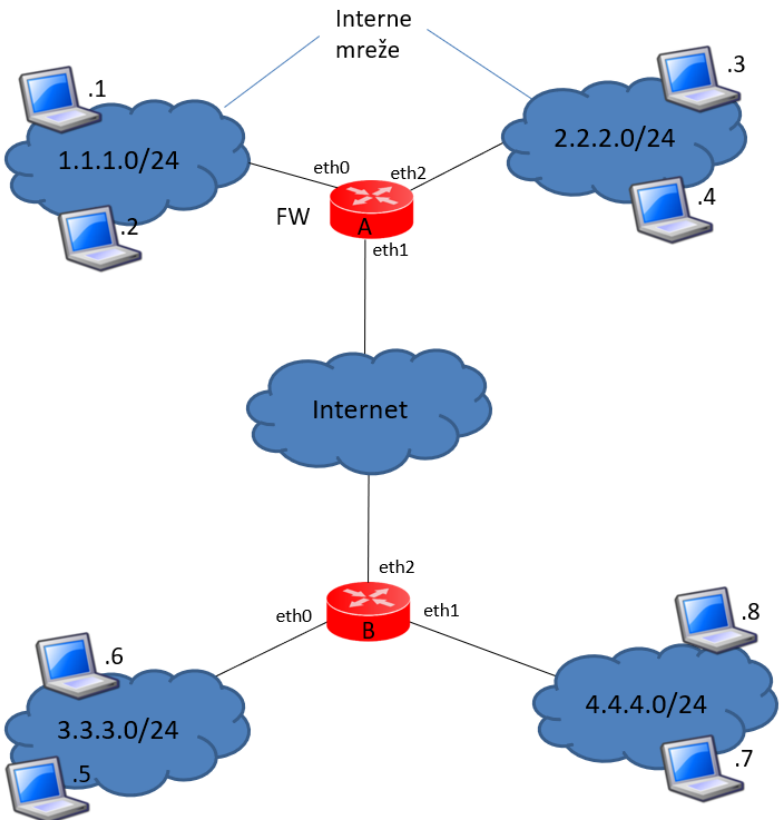
Protocol=6 Flag=ACK

- FW proverava SPI tabelu, zaključuje da je paket postojeće komunikacije i automatski ga propušta dalje.
- State u SPI tabeli menja se na Established.

SPI tabela

Src	Dest	Protocol	State
1.1.1.12:48037	3.3.3.35:80	6	Established

- Računar 12 šalje podatke serveru 35, i server 35 šalje podatke računaru 12.
- Kada FW vidi da ovi paket pripadaju uspostavljenoj konekciji on će ih automatski propuštati dalje.
- Nema potrebe za proverom FW pravila.
- Konačno stanje konekcije je Closed, prvo je Intermediate Closed, čeka se par minuta, a zatim se konekcija potpuna zatvara.
  - Kada se konekcija zatvori briše se unos iz SPI tabele.
  - Administrator kreira samo pravilo za prvi paket i sve ostalo se prihvata automatski.
  - Administrator ne mora da vodi računa o stanju konekcije, FW to radi umesto njega



FW tabela

Rule	SrcIP	SrcPort	DestIP	DestPort	Protocol	Action
1	3.3.3.6	ANY	1.1.1.2	22	TCP	ACCEPT
2	4.4.4.8	ANY	1.1.1.1	25	TCP	ACCEPT
3	2.2.2.0/24	ANY	2.2.2.0/24	ANY	TCP	ACCEPT
4	2.2.2.0/24	ANY	4.4.4.7	80	TCP	ACCEPT
5	4.4.4.0/24	ANY	2.2.2.3	80	TCP	ACCEPT

SPI tabela

SPI	SrcIP	SrcPort	DestIP	DestPort
1	3.3.3.6	44981	1.1.1.2	22
2	3.3.3.6	47231	1.1.1.2	22
3	3.3.3.6	47231	1.1.1.2	22
4	4.4.4.7	40327	2.2.2.3	80
5	4.4.4.7	47231	2.2.2.3	80
6	2.2.2.3	22	4.4.4.7	80
7	2.2.2.4	44981	2.2.2.4	40327
8	4.4.4.8		1.1.1.1	25

- FW prima paket sa sledećim karakteristikama:

SrcIP=1.1.1.12 SrcPort=23

DestIP=3.3.3.5 DestPort=44981

- Proveriće tabele i uporediti vrednosti paketa sa vrednostima iz tabela.
  - Prvo se proverava SPI tabela.
  - Nema podudaranja ni sa jednim unosom SPI tabele.
  - Ovo znači da paket nije povezan ni sa jednom konekcijom koja je u toku.
  - Ako je ovo novi paket proveravaju se vrednosti paketa sa vrednostima FW tabele.
  - Ni ovde nema podudaranja.
  - Paket će biti ODBAČEN (DEFAULT DROP).

➢ FW tabela

Rule	SrcIP	SrcPort	DestIP	DestPort	Protocol	Action
1	3.3.3.6	ANY	1.1.1.2	22	TCP	ACCEPT
2	4.4.4.8	ANY	1.1.1.1	25	TCP	ACCEPT
3	2.2.2.0/24	ANY	2.2.2.0/24	ANY	TCP	ACCEPT
4	2.2.2.0/24	ANY	4.4.4.7	80	TCP	ACCEPT
5	4.4.4.0/24	ANY	2.2.2.3	80	TCP	ACCEPT

➢ SPI tabela

SPI	SrcIP	SrcPort	DestIP	DestPort
1	3.3.3.6	44981	1.1.1.2	22
2	3.3.3.6	47231	1.1.1.2	22
3	3.3.3.6	47231	1.1.1.2	22
4	4.4.4.7	40327	2.2.2.3	80
5	4.4.4.7	47231	2.2.2.3	80
6	2.2.2.3	22	4.4.4.7	80
7	2.2.2.4	44981	2.2.2.4	40327
8	4.4.4.8		1.1.1.1	25

STATEFUL PACKET INSPECTION – PRIMER 2

- Stiže drugi paket sa sledećim parametrima:

SrcIP=4.4.4.7 SrcPort=44981

DestIP=2.2.2.3 DestPort=80

- Prvo se proverava SPI tabela da li ima podudaranja?
- Podudaranje postoji sa šestim pravilom.
- Paket će automatski biti prihvaćen bez provere FW pravila.

➢ FW tabela

Rule	SrcIP	SrcPort	DestIP	DestPort	Protocol	Action
1	3.3.3.6	ANY	1.1.1.2	22	TCP	ACCEPT
2	4.4.4.8	ANY	1.1.1.1	25	TCP	ACCEPT
3	2.2.2.0/24	ANY	2.2.2.0/24	ANY	TCP	ACCEPT
4	2.2.2.0/24	ANY	4.4.4.7	80	TCP	ACCEPT
5	4.4.4.0/24	ANY	2.2.2.3	80	TCP	ACCEPT

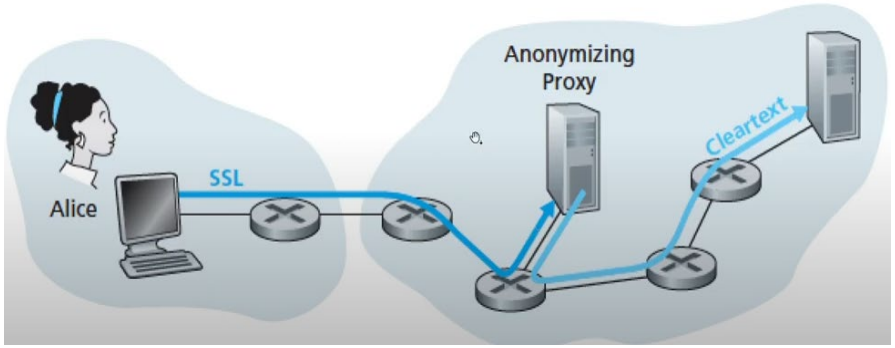
➢ SPI tabela

SPI	SrcIP	SrcPort	DestIP	DestPort
1	3.3.3.6	44981	1.1.1.2	22
2	3.3.3.6	47231	1.1.1.2	22
3	3.3.3.6	47231	1.1.1.2	22
4	4.4.4.7	40327	2.2.2.3	80
5	4.4.4.7	47231	2.2.2.3	80
6	2.2.2.3	22	4.4.4.7	80
7	2.2.2.4	44981	2.2.2.4	40327
8	4.4.4.8		1.1.1.1	25

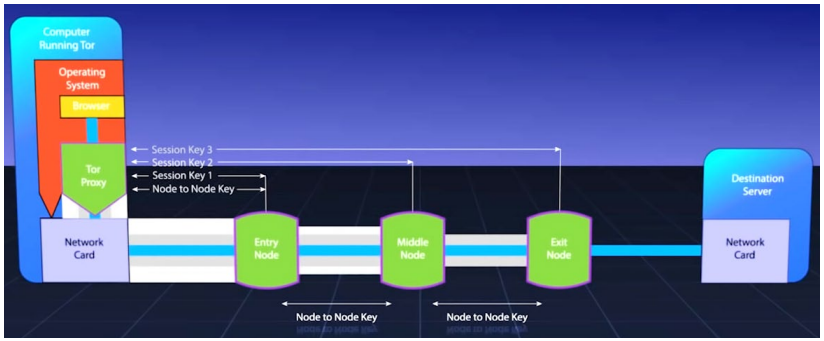
PROXY SERVER

- Proxy server ima ulogu prolaza na nivou aplikacije (Application Gateway)
- Štiti privatnost korisnika koji pristupa servisima na Internetu
- Važno je da se Proxy serveru bude kredibilan i da ima uključenu SSL konekciju.
  - Proxy server loguje sve zapise korisnika koji koristi njegovu uslugu za pristup drugim servisima (originalna i pozajmljena IP adresa i sadržaj kojem pristupa)
  - TOR je anonimni privatni proxy servis koji korisnički saobraćaj rutira kroz grupu proxy servera obezbeđujući da poslednji proxy server koji šalje zahtev web serveru nama informaciju o IP adresi kreatora zahteva.

TRADICIONALNA PROXY SERVER ARHITEKTURA

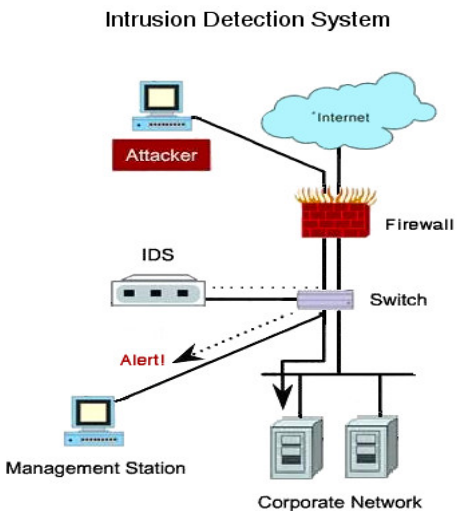


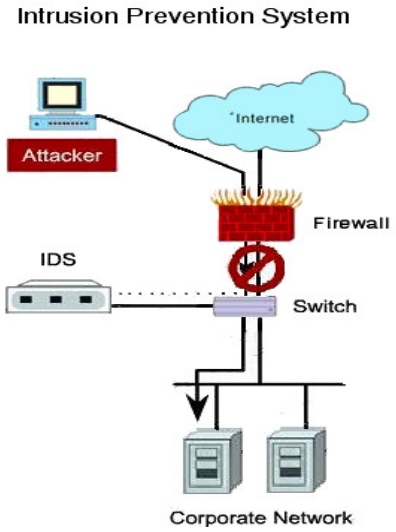
TOR ARHITEKTURA



INTRUSION DETECTION SISTEMI

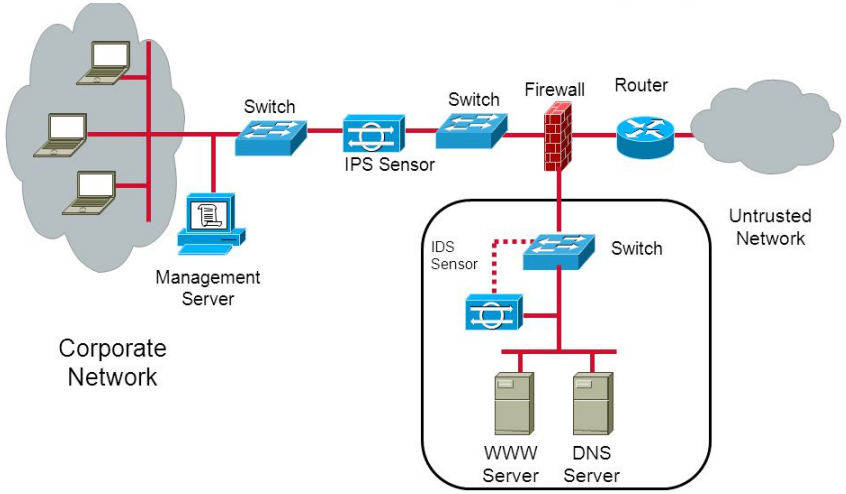
- Firewall – inspekcija paketa zasnovana na poljima u zaglavljima TCP-IP protokolskog steka
- Deep Packet Inspection – inspekcija pakete na aplikativnom sloju
- Intrusion Detection System – sistem koji generiše upozorenje (alerts) kada detektuje prisustvo malicioznog saobraćaja.
- Intrusion Prevention System – sistem koji uklanja (filtrira) sumnjiv saobraćaj.
- Koristi se za prepoznavanje
  - Skeniranje portova (Port scan)
  - Dos napada
  - Virusa i crva
  - Napad na OS ili aplikaciju
- Najveći izazov je prepoznavanje sumnjivog saobraćaja





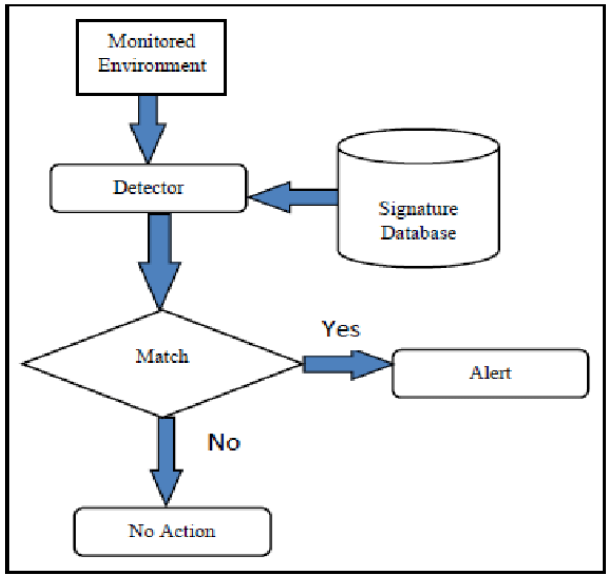
INTRUSION DETECTION SYSTEM - ARHITEKTURA

- Dva regiona u mreži
  - High secure region koji se štiti filtriranjem paketa, aplikativnim prolazom i IDS senzorima
  - Low security region (demilitarizovana zona) koja se štiti filtriranjem paketa i nadgleda se IDS senzorima
- Vrste IDS sistema
  - Zasnovana na signaturama
    - Baza podataka sa signaturama napada
  - Zasovana na anomalijama
    - Kreira se profil saobraćaja a zatim se posmatra saobraćaj i upoređuje sa kreiranim profilom.



IDS ZASNOVAN NA SIGNATURAMA

- Koncept se zasniva na signaturi (šablonu) samog napada slično antivirusnom programu
  - Karakteristike samog paketa - izvorišni/odredišni port, određen bit stringova u zaglavlju paketa,...
  - Karakteristike serije paketa
- Svaki paket se upoređuje sa sinaturama koje se nalaze u bazi napada u IDS sistemu.
- U slučaju podudaranja, alarm se generiše
- Efikasan je sa pretnjama koje su dobro poznate.
- Nedostaci su:
  - Ne reaguje na tzv (zero day attack) tj. na ranjivost za koju sistem nije upoznat tj. promenom načina napada u odnosu na signaturu napada,
  - Što je naprednija baza sa signaturama više CPU vremena je potrebno za analizu signatura



IDS ZASNOVAN NA ANOMALIJAMA

- Koncept se zasniva na praćenju saobraćaja i kreiranju profila za regularan saobraćaj
  - Zasniva se na pravilima a ne na šablonima ili signaturama
  - Može da se kreira profil na osnovu veštačke inteligencije i matematičkim modelima
  - Najveći nedostatak je definisanje pravila jer svaki protokol koji se analizira mora da se definiše, implementira i testira.
  - Koncept je još uvek u razvoju

IDS ZASNOVAN NA SIGNATURAMA vs IDS ZASNOVAN NA ANOMALIJAMA

- Efiksanost sistema se zasniva na odnosu uspešnih i pogrešna procena.
- False Positive – Pogrešno pozitivna procena je detekcija bezopasnog kao malicioznog saobraćaja
- False Negative – Pogrešno negativna procena je detekcija malicioznog saobraćaja kao bezopasnog saobraćaja.
- IDS zasnovan na signaturama ima nisku stopu pogrešno pozitivnih procena ali visoku stopu pogrešno negativnih procena
- IDS zasnovan na anomalijama ima visoku stopu pogrešno pozitivnih procena dok malu ili srednju stopu pogrešno negativnih procena.