# Filtriranje saobraćaja – uvid u tehnologije i mesta njihove primene u AMRESu

Dokument najbolje prakse
(smernice i preporuke)

Izrađen u okviru AMRES tematske grupe za oblast Sigurnost
(AMRES BPD 102)

**Autori: Zoran Mihailović, Bojan Jakovljević, Mara Bukvić**

**Jul 2011.**

Dokument broj: GN3-NA3-T4-AMRES-BPD-102
Verzija / datum: Jul 2011.
Izvorni jezik : Srpski
Originalni naslov: “Preporuke za filtriranje saobraćaja u krajnjim institucijama”
Originalna verzija / datum: Revizija 1 (dela dokumenta iz maja 2010.) / 11. jul 2011.
Kontakt: helpdesk@rcub.bg.ac.rs

AMRES/RCUB snosi odgovornost za sadržaj ovog dokumenta. U izradi dokumenta učestvovala je tematska grupa za Sigurnost organizovana u AMRESu radi sprovođenja zajedničkih aktivnosti na razvoju i širenju dokumenata sa tehničkim smernicama i preporukama za mrežne servise u višokoškolskim obrazovnim i istraživačkim ustanovama u Srbiji.



Dokument je nastao kao rezultat istraživanja koja su finansirana sredstvima Sedmog okvirnog programa Evropske zajednice (FP7/2007-2013) po ugovoru br. 238875, koji se odnosi na projekat „Multi-Gigabit European Research and Education Network and Associated Services (GN3)”.

# Sadržaj

# Rezime

Cilj ovog dokumenta je da predstavi raspoložive tehnologije filtriranja saobraćaja, njihovu generalnu upotrebu, ali i da ukaže na načine i mesta njihove očekivane primene u hijerarijskoj strukturi AMRES mreže.

U želji da se smanje sigurnosne pretnje, u AMRESu se koriste različiti uređaji, tehnologije i tehnike za filtriranje saobraćaja. Svaka institucija/organizacija koja želi da poboljša efikasnost filtriranja i bezbednost u svojoj mreži treba da se, u skladu sa zahtevima i sopstvenim potrebama, opredeli za tehnologiju i pravila filtriranja saobraćaja koju će da implementira u svojoj lokalnoj mreži.

Bolje razumevanje načina na koji se saobraćaj filtrira na pojedinim mestima u AMRES mreži, trebalo bi da olakša definisanje pravila u pojedinačnim institucijama i postizanje bolje usklađenosti pravila svake institucije sa praksom u ostatku mreže.

Dokument je namenjen prvenstveno rukovodiocima i onim administratorima koji učestvuju u izradi pravila filtriranja i izboru tehnologije filtriranja za mrežu institucije za koju su odgovorni. Pored toga, dokument može posredno da pomogne mrežnim administratorima u krajnjim institucijama kod identifikacije i otklanjanja uzroka problema vezanih za filtriranje saobraćaja na nekim mestima u mreži.

# Uvod

Veliki broj radnih stanica, servera i drugih uređaja u AMRES mreži je svakodnevno izložen negativnim uticajima, kako unutar same AMRES mreže, tako i sa Interneta. Zbog toga se pred administratore u AMRESu postavlja zadatak da maksimalno onemoguće negativne uticaje na svoju mrežu, a pri tome omoguće normalno funkcionisanje mreže. Pored toga, potrebno je onemogućiti i širenje negativnih uticaja sa mreže za koju je odgovoran administrator, ka ostalim mrežama unutar AMRES mreže, kao i na Internet.

Da bi ispunili ove zadatke, administratori filtriraju saobraćaj na različitim mestima u AMRES mreži. Filtriranje saobraćaja se može izvesti pomoću pravila filtriranja implementiranih na ruterima i/ili firewall uređajima, kao i primenom drugih tehnologija opisanih u ovom dokumentu.

Dokument je pripremljen s ciljem da administratore koji upravljaju mrežama, bilo na lokalnom nivou, bilo na nivou servisnog centra ili na nivou AMRES-a, upozna sa osnovnim pravilima i praksom filtriranja paketa u AMRES-u, kao i o pozicijama na kojima su filtriranje saobraća implementira u hijerarhijskoj topologiji AMRES mreže.

Bolje razumevanje načina na koji se saobraćaj filtrira na pojedinim mestima u AMRESu, trebalo bi da olakša definisanje pravila u pojedinačnim institucijama i postizanje bolje usklađenosti pravila svake institucije sa praksom u ostatku mreže.

Postupak razvoja i primena paketskih filtara u krajnjim institucijama/organizacijama AMRESa definisani su u dokumentu AMRES BPD 110 „Filtriranje saobraćaja u krajnjim institucijama”.

Dokument može da doprinese razumevanju potrebe za definisanjem ili objavljivanjem već postojećih pravila u formi pravilnika, kao izradi i usvajanju pravilnika u različitim institucijama AMRESa.

# 1 Četiri polazne preporuke za filtriranje saobraćaja

Da bi se smanjile sigurnosne pretnje, u AMRESu se koriste različiti uređaji, tehnologije i tehnike za filtriranje saobraćaja. Svaka institucija/organizacija koja želi da poboljša efikasnost filtriranja i postigne veći nivo bezbednost u svojoj mreži, treba da primeni sledeće preporuke:

1. Da definiše pravila o filtriranju saobraćaja, kojima će biti određeno kako se reguliše protok dolaznog i odlaznog saobraćaja u mreži. Skup pravila o filtriranju saobraćaja se može usvojiti kao samostalan pravilnik (*packet filtering policy*) i kao deo pravilnika o bezbednost IKT u instituciji (*information security policy*).
2. Da se u skladu sa zahtevima i potrebama opredeli za tehnologiju filtriranja saobraćaja koju će da implementira.
3. Da na izabranoj tehnologiji, izvrši implemenatciju definisanih pravila i uskladi ih sa performansama uređaja.
4. Da održava sve komponente rešenja, što uključuje ne samo uređaje, već i pravilnik.

Važno je primetiti da se ove preporuke mogu primeniti u bilo kojoj organizaciji, pa i u AMRESu kao celini.

Dokument AMRES BPD 102 „Filtriranje saobraćaja – uvid u tehnologije i mesta njihove primene u AMRESu" je pripremljen da podrži implemenatciju preporuke broj 2, dok je AMRES BPD 110 „Filtriranje saobraćaja u krajnjim institucijama" pripremljen u vezi sa implementacijom preporuka 1 i 3 u krajnjim institucijama.

# 2 Pregled tehnologija za filtriranje saobraćaja

Tehnologije za filtiraranje saobraćaja, najčešće se dele na tehnologiju filtriranja paketa (*packet filtering – stateless firewall*) i *stateful firewall* tehnologije.

Funkcijonalnost filtriranja paketa (*stateless firewall*) je ugrađena u većinu operativnih sistema i uređaja koji mogu da rutiraju saobraćaj. Najčešće je to ruter na kome su primenjene liste za kontrolu pristupa (*access control list* **–** ACL).

Paketski filtar implementiran na ruteru je najjednostavniji, i samo jedan od mogućih metoda za filtriranje saobraćaja. U okviru ovog poglavlja su opisane druge raspoložive *firewall* tehnologije i njihova generalna upotreba. Date su preporuke za njihovu primenu u okviru hijerarhijske strukture AMRES mreže.

## 2.1 Paketski filtar nasuprot *stateful firewall*-a

Funkcija filtriranja paketa je osnovno obeležje svih *firewall* uređaja. Rani *firewall* uređaji koji nisu imali ništa više od paket filtera su se nazivali i *stateless inspection firewalls*. Nasuprot tome, smatra da današnji *firewall* uređaji imaju daleko više mogućnosti u pogledu filtriranja paketa.

Paket filter omogućava implementaciju kontrole pristupa resursima, tako što na osnovu informacija u zaglavlju IP paketa donosi odluku, da li je dopušten prolaz tom paketu ili ne. Paket filter ne proverava sadržaj paketa (poput *content filtera*), niti na osnovu informacija iz TCP ili UPD zaglavlja paketa pokušava da ustanovi kojim sesijama pripadaju pojedinačni paketi, pa ne donosi ni dalje odluke u skladu sa tim. Zbog toga je opisani process poznat još pod nazivom ***stateless packet inspection***.

Zbog ovakvog načina rada, gde se ne prate informacije o stanju konekcija, prilikom konfiguracije *stateless firewall* uređaja potrebno je eksplicitno dozvoliti saobraćaj u oba smera veze.

*Stateless firewall* uređaji proveravaju svaki paket pojedinačno i filtriraju pakete na osnovu informacija na 3. i 4. sloju OSI referentnog modela.

Odluku o filtriranju donose na osnovu sledećih informacija:

- izvorišna IP adresa
- odredišna IP adresa
- protokol
- izvorišni broj porta
- odredišni broj porta

Najčešće su implementirani kao deo funkcionalnosti na samim ruterima (ACL, *firewall* filtri itd.), ali i na serverima.

Prednosti primene paketskih filtera:

- jednostavni za implementaciju;
- većina rutera ih podržava, te ne mora da se investira u novu opremu i softver;
- retko prouzrokuje usko grlo na mestu primene, čak i pri velikim brzinama u gigabitnim mrežama.

Nedostaci primene paketskih filtera:

- osetljivi su na IP *spoofing* napade;
- ranjivi su na napade koji koriste nedostatke u TCP/IP protokol steku i specifikaciji protokola;
- imaju problem sa filtriranjem fragmentiranih paketa (uzrok inkopatibilnosti i nefunkcionisanja VPN veza);
- ne podržavaju dinamičko fitriranje pojedinih servisa (takvih servisa koji zahtevaju dinamičko dogovaranje o portovima koji se koriste u komunikaciji – pasivni FTP)

**Mesto primene paketskih filtara u AMRES mreži:** Imajući u vidu hijerarhijsku strukturu AMRESa opisanu u poglavlju 3, paketski filtri se koriste na vezama AMRESa prema Internetu (pozicija/nivo 1), na vezama između pojedinih institucija/organizacija i regionalnog servisnog centra kome pripadaju (pozicija/nivo 3), na serverima posvećenim konkretnom servisu (*dedicated servers*). Mogu se naći, mada ređe, i u internim mrežama institucija/organizacija članica.

***Stateful packet inspection*** nastoji da unapredi proces filtriranja paketa, tako što prati stanje svake konekcije koja se uspostavlja kroz *firewall* uređaj.

Poznato je da TCP protokol podržava pouzdanu dvosmernu komunikaciju i da TCP saobraćaj opisuju tri glavna stanja - uspostavljanje konekcije, razmena podataka i terminacija konekcije. S*tateful packet inspection* pri uspostaljanju konekcije evidentira svaku vezu u tabeli stanja.

Tokom razmene podataka, uređaj prati određene parametre u zaglavlju L3 paketa i L4 segmenta i u zavisnosti od njihovih vrednosti i sadržaja tabele stanja donose odluku o filtriranju. U tabeli stanja se nalaze sve trenutno aktivne konekcije. Zbog ovakvog načina rada, eventualni napadač, koji pokuša da podmetne paket sa zaglavljem koje označava da je paket deo uspostavljene veze, može biti otkriven samo sa *stateful inspection firewall* uređajem, prilikom provere da li konekcija postoji zabeležena u tabeli stanja.

Tabela stanja sadrži sledeće informacije:

- izvorišna IP adresa
- odredišna IP adresa

- izvorišni broj porta
- odredišni broj porta
- TCP brojevi sekvence
- TCP vrednosti flag-ova

U okviru TCP zaglavlja, prati se stanje flag-ova *synchronize* (SYN), *reset* (RST), *acknowledgment* (ACK), *finish* (FIN) i na osnovu njih donosi zaključak o stanju pojedine konekcije.

UDP protokol nema formalni postupak za uspostavljanje i prekid konekcije. Međutim, uređaji sa *stateful* inspekcijom mogu da prate stanje pojedinačnih *flows*-ova[1] i mogu da upare različite *flows*-ove, kada logički odgovaraja jedni drugima. (npr. prolaz DNS odgovora sa spoljnog servera može biti dozvoljen samo ako je prethodno evidentiran odgovarajući DNS upit iz internog izvora ka tom serveru)

Prednosti primene *stateful firewall* uređaja:

- pružaju viši stepen zaštite u odnosu na *stateless firewall* uređaje (veća efikasnost i detaljnija analiza saobraćaja);
- otkrivaju IP *spoofing* i DoS napade;
- pružaju više *log* informacija u odnosu na paketske filtre.

Nedostaci primene *stateful firewall* uređaja:

- ne pružaju zaštitu od napada na aplikativnom sloju;
- degradiraju performanse rutera na kojima su pokrenuti (zavisi od veličine mreže i drugih servisa pokrenutih na ruteru);
- ne pružaju svi podršku za UDP, GRE i IPSec protokole, već ih tretiraju kao i *stateless firewall* uređaji;
- ne podržavaju autentifikaciju korisnika.

**Mesto primene *stateful firewall* uređaja u AMRES mreži:** Imajući u vidu hijerarhijsku strukturu AMRESa opisanu u poglavlju 3, *stateful firewall* uređaji se ne mogu očekivati iznad pozicije/nivoa 3. Mogu se naći i u internim mrežama institucija AMRES članica.

**Preporuka:** Uporediti zahteve i potrebe institucije za filtriranjem saobraćaja sa mogućnostima uređaja, koji se planira nabaviti. U skladu doneti i odluku o opravdanosti investicije u značajno skuplji *firewall* uređaj. Imati u vidu iskustvo mnogih administratora u AMRESu, koji smatraju da je paketski filter implementiran na ruteru dovoljno dobro rešenje za većinu potreba u manjim institucijama.

[1] *Flows* je definisan konkretnom izvorišnom i odredišnom IP adresom, parom portova (izvor, odredište), protokolom, TOS poljem i ulaznim interfejsom uređaja.

## 2.2 Opis drugih raspoloživih *firewall* tehnologija

U novije vreme, standardna *stateful packet inspection* tehnologija pokušava se unaprediti dodavanjem osnovnih rešenja iz *intrusion detection* tehnologije. Unapređena tehnologija se zove *stateful* protokol analiza, a neretko se korisi i naziv *DPI (deep packet inspection)* analiza podataka na aplikativnom sloju.

Uređaja nastali iz takvog pravca razvoja su *Application Firewall, Application Proxy Gateways* i *Proxy* serveri.

Za razliku od *stateful firewall* uređaja koji saobraćaj filtriraju na osnovu podataka na 3., 4. i 5. sloju OSI referentnog modela, ovi uređaji mogu da filtriraju saobraćaj i na osnovu informacija na aplikativnom (7) sloju OSI referentnog modela.

### 2.2.1 *Application Firewall*

*Application Firewall* (AF) uređaji vrše *stateful* protokol analizu protokola aplikativnog nivoa. Podržavaju dosta uobičajenih protokola, kao što su HTTP, SQL, email servis (SMTP, POP3 i IMAP), VoIP, XML itd.

*Stateful* protokol analiza se oslanja na predefinisane profile prihvatljivog rada odabranog protokola, na osnovu kojih se mogu identifikovati eventualna odstupanja i nepravilnosti u konkretnom toku poruka tog protokola kroz uređaj. Problemi se mogu pojaviti ukoliko postoji konflikt između profila rada određenog protokola, definisanog na AF uređaju, i načina implementacije protokola u verziji same aplikacije ili operativnih sistema koji se koriste u mreži.

*Stateful* protokol analiza može da:

- ustanovi da li *email* poruka sadrži tip *attachemta* koji nije dozvoljen (npr. *exec* fajlove);
- ustanovi da li se *instant messaging* koristi preko HTTP porta;
- da blokira konekciju preko koje se izvšava neželjena komanda (npr. FTP *put* komanda na FTP server);
- da blokira pristup stranici koja sadrži neželjeni aktivni sadržaj, npr. Java;
- identifikuje nepravilnu sekvencu komandi koje se razmenjuju u komunikaciji između 2 hosta (npr. neuobičajeno veliki broj ponavljanja iste komande ili upotrebljavanje neke komande pre komande od koje je zavisna i sl.);
- omogući proveru pojedinačnih komandi, minimalne i maksimalane dužina odgovarajućih argumenata komande (npr. broj karatera koji se koriste za *username* i sl.).

AF uređaj ne može da detektuju napade koji ne krše generalno prihvatljive procedure rada određenog protokola, poput DoS (*denial of service*) napada, izazvanog ponavljanjem velikog broja prihvatljivih sekvenci poruka u kratkom vremenskom intervalu.

Zbog kompleksnosti analize koju vrše, kao i zbog praćenja stanja velikog broja istovremenih sesija, glavni nedostatak metoda *stateful* protokol analize je intenzivno korišćenje resursa AF uređaja.

**Mesto primene AF uređaja u AMRES mreži:** Imajući u vidu hijerarhijsku strukturu AMRESa opisanu u poglavlju 3, upotreba AF uređaja nije česta, ali je uslovno opravdana u internim mrežama institucija AMRES članica. Primena AF uređaja se ne može očekivati iznad pozicije 3.

### 2.2.2 *Application Proxy Gateway*

*Application Proxy Gateway* (APG) uređaji, takođe vrše analizu toka saobraćaja na aplikativnom nivou. U odnosu na AF uređaje, APG uređaji pružaju veći stepen sigurnosti za pojedinačne aplikacije, jer onemogućavaju direktnu vezu između dva hosta, a mogu da vrše inspekciju sadržaja poruka aplikativnog sloja.

APG uređaji sadrže *proxy* agente, tzv. "posrednike" u komunikaciji između dva krajnja hosta. Na taj način ne dozvoljavaju direktnu komunikaciju između njih. Svaka uspešna konekcija između krajnjih hostova, sastoji se iz dve konekcije – prva je između klijenta i *proxy* servera, a druga između *proxy* servera i odredišnog uređaja. *Proxy* agenti, na osnovu pravila filtriranja definisanim na APG uređaju, donose odluku da li će mrežni saobraćaj biti dopušten ili ne. Odluke o filtriranju saobraćaja mogu donositi i na osnovu informacija u zaglavlju poruke aplikativnog sloja ili čak i na osnovu sadržaja koju ta poruka prenosi. Dodatno, *proxy* agenti mogu da zahtevaju autentifikaciju korisnika.

Postoje APG uređaji, koji imaju i mogućnost dekripcije paketa, njihovog ispitivanja i ponovnog enkriptovanja, pre nego što se paket prosledi odredišnom hostu. Paketi, koji se ne mogu dekriptovati, se jednostavno prosleđuju kroz uređaj.

U odnosu na paketske filtre i *stateful* uređaje, APG uređaji imaju niz nedostataka. Način rada APG uređaja uzrokuje znatno veći utrošak resursa, tj. zahtevaju više memorije i veći utrošak procesorskog vremena za ispitivanje i interpretaciju svakog paketa koji kroz uređaj prolazi. Zbog toga, APG uređaji nisu pogodni za filtriranje aplikacija zahtevnijih u pogledu propusnog opsega ili aplikacija koje su osetljive na vremensko kašnjenje (*real-time* aplikacije). Kao još jedan nedostatak, može se navesti i ograničenost u broju servisa koji se mogu filtrirati kroz ove uređaje. Svaki tip saobraćaja koji prolazi kroz uređaj, zahteva specifičan *proxy* agent, koji bi bio zadužen za posredovanje u komunikaciji. Zbog toga se može desiti da APG uređaji ne podržavaju filtriranje novih aplikacija ili protokola.

Zbog svoje cene, APG uređaji se najčešće koristi za zaštitu date centara ili ostalih mreža koje sadrže javno dostupne servere, a koji su od većeg značaja za neku organizaciju.

Da bi se smanjilo opterećenje na APG uređaje i postigla veća efikasnost, u današnjim mrežama češće se koriste *proxy* serveri (*dedicated proxy* serveri) zaduženi za tačno određene servise, koji nisu toliko osetljivi na vremensko kašnjenje (npr. *email* ili *web proxy* serveri).

**Mesto primene APG uređaja u AMRES mreži:** Imajući u vidu hijerarhijsku strukturu AMRESa opisanu u poglavlju 3, upotreba APG uređaja nije česta, ali je uslovno opravdana u internim mrežama institucija AMRES članica. Primena APG uređaja se ne može očekivati iznad pozicije 3.

### 2.2.3 *Dedicated Proxy Server*

*Dedicated proxy* (DP) serveri, kao i APG uređaji, imaju ulogu "posrednika" u komunikaciji između 2 hosta, ali su njihove mogućnosti u filtriranju saobraćaja značajno manje. Ova vrsta uređaja, namanjena je analizi rada specifičnih servisa i protokola (npr. HTTP ili SMTP).

Zbog ograničenih mogućnosti u filtriranju saobraćaja, DP uređaji se u arhitekturi mreže, postavljaju iza *firewall* uređaja. Njihova glavna funkcija je da izvrše specijalizovano filtriranje određenog tipa saobraćaja (na osnovu ograničenog skupa parametara) i izvrše operaciju logovanja. Izvršavanjem ovih specifičnih aktivnosti, značajno se smanjuje opterećenje samog *firewall* uređaja, koji se nalazi ispred DPS uređaja.

Najpoznatiji primer, za ovakav tip uređaja, jesu *Web Proxy* serveri. Karakteristični primer primene je HTTP *proxy* server (upotrebljen iza *firewall* uređaja ili rutera), na koji se korisnici moraju povezati kada žele da pristupe eksternim *web* serverima. Kada institucija raspolaže izlaznom vezom (*uplink*-om) nižeg propusnog opsega preporučuje se da koristi funkciju keširanja (*caching*), da bi se smanjio nivo saobraćaja i poboljšalo vreme odziva.

Zbog, porasta dostupnih *Web* aplikacija i povećanog broja pretnji koje se prenose preko HTTP protokola, *Web Proxy* serveri dobijaju na značaju. Stoga danas imamo situaciju, da razni proizvođači opreme, klasičnim *Web Proxy* serverima dodaju funkcionalnosti raznih *firewall* tehnologija i na taj način povećavaju njihove mogućnosti u filtriranju saobraćaja.

**Mesto primene *dedicated proxy* servera u AMRES mreži:** Imajući u vidu hijerarhijsku strukturu AMRESa opisanu u poglavlju 3, *dedicated proxy* serveri u servisnim centrima AMRESa (pozicija/nivo 2) su konfigurisani tako da mogu da podrže opcionu upotrebu *proxy* servera u internim mrežama institucija AMRES članica (pozicija/nivo 4). Konfiguracije i upotreba *proxy* tehnologije na različitim mestima mora biti usklađena.

## 2.3 Rešenja u kojima se filtriranje saobraćaja kombinuje sa drugim tehnologijama

Pored svoje osnovne namene, da blokiraju neželjeni saobraćaj, *firewall* uređaji često funkciju filtriranja kombinuju i sa drugim tehnologijama, pre svega sa rutiranjem. Za rutere važi obrnuto. Otuda se NAT ponekad doživljava kao *firewall* tehnologija, mada je u suštini tehnika rutiranja.

Na *firewall* uređajima su često raspoložive i druge srodne funkcionalnosti poput VPN, IDP. U ovom poglavlju su, zbog kompletnosti pregleda i učestalosti njihove upotrebe, kratko opisane i ove tehnologije.

### 2.3.1 NAT (*Network Address Translation*)

**NAT (*Network Address Translation*)** je tehnologija koja omogućava uređajima koji koriste privatne IP adrese, da komuniciraju sa uređajima na Internetu. Ova tehnologija pruža servis translacije privatnih IP adresa, koje uređaji mogu da koriste u okviru LAN mreže, u javno dostupne Internet adrese.

Primenom NAT tehnologije može se (namerno ili slučajno) ograničiti broj dostupnih servisa, odnosno onemogućiti funkcionisanje servisa koji zahtevaju direktnu *end-to-end* komunikaciju (poput VoIP i dr.).

Postoje 3 tipa NAT translacija: dinamički, statički i PAT

**Dinamički NAT** koristi skup javno dostupnih IP adresa, koje sukcesivno dodeljuje hostovima sa privatnim IP adresama. Kada host sa privatnom IP adresom ima potrebu da komunicira sa uređajem na Internetu, dinamički NAT vrši translaciju njegove privatne IP adrese u javno dostupnu IP adresu, uzimanjem prve slobodne IP adrese iz definisanog skupa javno dostupnih IP adresa. Pogodan je za klijentske računare.

**Statički NAT** podrazumeva jednoznačno mapiranje između privatne IP adrese nekog hosta i njemu dodeljene javne IP adrese. Na ovaj način, host sa privatnom IP adresom se na Internetu pojavljuje uvek sa istom javnom IP adresom. Ovo je glavna razlika između statičke i dinamičke translacije. Pogodan je za servere.

Kod oba pomenuta tipa translacija, svaka privatna IP adresa se translira u posebnu javnu IP adresu. Da bi bio podržan zadovoljavajući broj istovremenih korisničkih sesija, organizacija koja koristi dinamički i/ili statički NAT, mora da poseduje dovoljan broj javnih IP adresa.

**PAT (Port Address Translation ili kako se još naziva NAT overload)** translacija vrši mapiranje između više privatnih IP adresa i jedne ili više javnih IP adresa. Mapiranje svake od privatnih IP adresa se vrši pomoću broja porta javne IP adrese. PAT translacija obezbeđuje da se svakom klijentu iz LAN mreže, koji uspostavlja konekciju sa uređajem na Internetu, dodeli različit broj porta javne IP adrese. Odgovor sa Interneta, koji stiže kao rezultat upućenog zahteva, se šalje na port sa kojeg je zahtev i upućen. Na ovaj način je omogućeno, da uređaj koji vrši translaciju (ruter, *firewall* ili server), zna ka kom hostu iz LAN mreže, treba da prosledi paket. Ova osobina PAT translacija, na neki način povećava nivo sigurnosti LAN mreže, jer onemogućava uspostavljanje konekcija sa Interneta, direktno ka hostovima u LAN mreži. Zbog ovakvog načina rada, PAT se ponekad pogrešno svrstava u sigurnosne tehnologije, iako je primarno tehnologija rutiranja.

### 2.3.2 VPN (*Virtual Private Networking*)

**VPN (*Virtual Private Networking*)** tehnologija se koristi za povećanje bezbednosti prenosa informacija, kroz mrežnu infrastrukturu koja ne pruža odgovarajući stepen bezbednosti podataka. Ona omogućava enkripciju i dekripciju mrežnog saobraćaja između spoljašnjih mreža i unutrašnje, zaštićene mreže.

VPN funkcionalnost, može biti raspoloživa na samim *firewall* uređajima ili implementirana na VPN serverima koji se u arhitekturi mreže, postavljaju iza *firewall* uređaja.

U mnogim slučajevima, implementacija VPN servisa na samom *firewall* uređaju je najoptimalnije rešenje. Smeštanje VPN servera iza *firewall* uređaja, zahteva da VPN saobraćaj prođe kroz *firewall* uređaj enkriptovan. Na taj način, *firewall* uređaj nije u mogućnosti da izvrši inspekciju, kontrolu pristupa ili logovanje mrežnog saobraćaja i izvrši skeniranje na određene sigurnosne pretnje.

Međutim, bez obzira na mesto implementacije, VPN servis zahteva, da odgovarajuća pravila filtriranja *firewall* uređaja omogućavaju njegovo nesmetano funksionisanje. U skladu sa tim, pri implementaciji bilo kog rešenja VPN arhitekture, posebnu pažnju treba obratiti na dopuštanje odgovarajućih protokola i TCP/UDP servisa, neophodnih za funkcionisanje izabranog VPN rešenja.

### 2.3.3 IDP (*Intrusion Detection and Prevention*)

**Detekcija mrežnih upada (*intrusion detection* - ID)** se bazirana na praćenju rada računarskih sistema ili mreža i analizi procesa koji se u njima odvijaju, a koji mogu da ukažu na pojavu određenih incidenata.

Incidenti su događaji koji predstavljaju pretnju ili kršenje definisanih sigurnosnih pravila, kršenje AUPa (*acceptable use policies*) pravila ili kršenje opšteprihvaćenih sigurnosnih normi. Pojavljuju se usled delovanja različitih *malware* programa (npr. crvi, spyware, virusi, trojanci itd.), pokušaja neautorizovanog pristupa sistemu kroz javnu infrastrukturu (Internet), usled delovanja autorizovanih korisnika sistema koji zloupotrebljavaju svoje privilegije itd.

**Prevencija mrežnih upada (intrusion prevention – IP)** obuhvata proces otkrivanja mrežnih upada, ali i proces sprečavanja i zaustavljanja uočenih ili verovatnih mrežnih incidenata.

**Sistemi za detekciju i prevenciju mrežnih upada (IDP)** se zasnivaju na procesu identifikovanja mogućih incidenata, logovanju informacija o njima, pokušaju da se oni spreče i alarmiranju administratora zaduženih za sigurnost. Takođe, pored ove svoje bazične funkcije, IDP sistemi se mogu koristiti i za identifikaciju problema sa usvojenim sigurnosnim pravilima, dokumentovanju postojećih sigurnosnih pretnji, kao i kod obeshrabrivanja pojedinaca u kršenju sigurnosnih pravila.

IDP sistemi koriste različite metodologije za otkrivanje incidenata.
Tri primarna klase u metodologiji detekcije su:

a. **Metod detekcije zasnovan na karakterističnom potpisu napada (*Signature-based detection*)**

Neke sigurnosne pretnje mogu biti prepoznate po svom karakterističnom načinu pojavljivanja. Oblik ponašanja neke od već otkrivenih sigurnosnih pretnji, opisan u formi koja se može iskoristiti za otkrivanje sledećih pojava iste pretnje, naziva se potpis (signature) napada.

Metod detekcije zasnovan na karakterističnom potpisu napada, predstavlja proces upoređivanja poznatih oblika pojavljivanja pretnje sa konkretnim mrežnim saobraćajem, kako bi se identifikovali pojedini incidenti.

Iako veoma efikasan u otkrivanje narednih pojava poznatih pretnji, ovaj metod detekcije je izrazito neefikasan u detekciji kako potpuno nepoznatih pretnji, tako i pretnji koje su prikrivene različitim tehnikama, kao i već poznatih sigurnosnih pretnji koje su na neki način u međuvremenu izmenjene. Smatra se najjednostavnijim metodom detekcije i ne može se koristiti u praćenju i analizi stanja nekih komleksnijih vidova komunikacije.

b. **Metod detekcije zasnovan na detekciji anomalija (*Anomaly-based detection*)**

Ovaj metod rada IDP sistema se zasniva na otkrivanju anomalija u konkretnom toku saobraćaja u mreži. Detekcija anomalija se vrši na osnovu definisanog profila prihvatljivog saobraćaja, njegovim poređenjem sa konkretnim saobraćajem u mreži.

Profili prihvatljivog saobraćaja formiraju se praćenjem tipičnih karakteristika saobraćaja u mreži (npr. broj *e-mail* poruka poslatih od strane nekog korisnika, broj pokušaja logovanja na neki host ili nivo korišćenja procesora u datom vremenskom intervalu) tokom određenog vremenskog intervala, pri čemu se smatra da su karakteristike ponašanja korisnika, hostova, konekcija ili aplikacija, u istom vremenskom intervalu, potpuno prihvatljive.

Međutim, profili prihvatljivog ponašanja, mogu nenamerno sadržati i pojedine sigurnosne pretnje, što dovodi do problema u njegovoj primeni. Takođe, neprecizno definisani profili prihvatljivog ponašanja, mogu uzrokovati i pojavu mnoštva alarma, a koje generiše sam sistem, kao reakciju na pojedine (čak prihvatljive) aktivnosti u mreži.

Najveća prednost ovog metoda detekcije je velika efikasnost u otkrivanju predhodno nepoznatih sigurnosnih pretnji.

c. **Metod detekcije zasnovan na stateful protokol analizi**

*Stateful* protokol analiza je proces upoređivanja predefinisanih profila rada nekog protokola sa konkretnim tokom podataka tog protokola u mreži. Predefinisane profile rada nekog protokola, definišu proizvođači IDP uređaja i u njima je identifikovano šta je prihvatljivo, a šta ne u razmeni poruka određenog protokola. Za razliku od metoda detekcije anomalija u saobraćaju, gde se profili kreiraju na osnovu hostova ili specifičnih aktivnosti u mreži, stateful protokol analiza koristi opšte profile generisane od strane proizvođača opreme.

Većina IDP sistema koristi istovremeno više metoda detekcije i na taj način omogućava sveobuhvatniji i precizniji način detekcije.

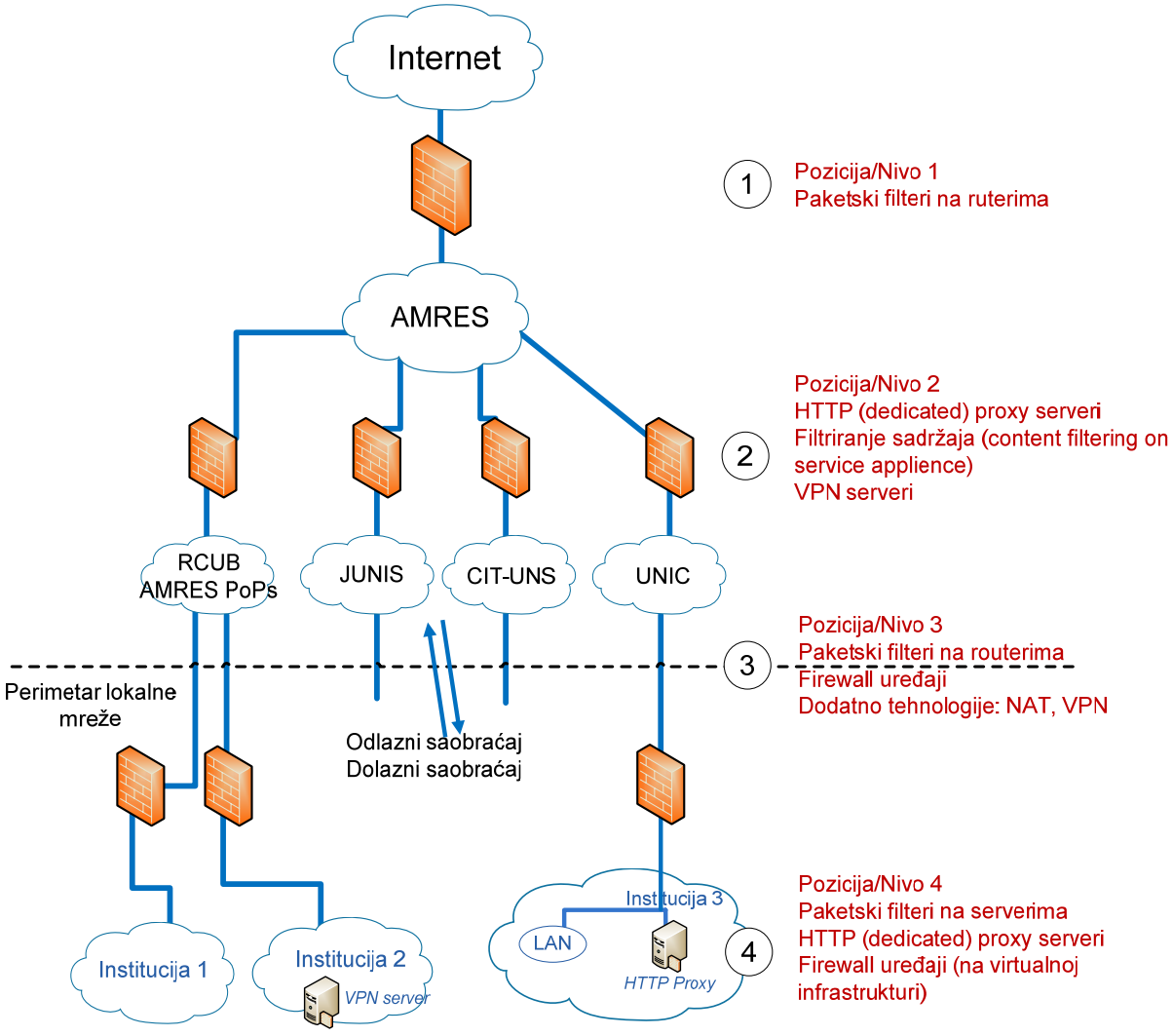
# 3 Primene tehnologija za filtriranje saobraćaja u hijerarijskoj strukturi AMRESa

Pravila o filtriranju saobraćaja mogu da se definišu i usvajaju na različitim mestima u mreži.

S obzirom na topologiju Akademske mreže Srbije (AMRES), može se identifikovati više mesta na kojima se vrši filtriranja saobraćaja:

- Pozicija/Nivo 1 – na vezama AMRES-a prema Internetu;
- Pozicija/Nivo 2 – u servisnim centrima AMRES-a (RCUB, CIT-UNS, JUNIS i UNIC);
- Pozicija/Nivo 3 – na vezama pojedinih institucija/organizacija i regionalnog servisnog centara kome pripadaju i na koji su povezane;
- Pozicija/Nivo 4 – u internoj mreži samih institucija/organizacija članica AMRESa.

U ovom poglavlju, opisana su konkretna rešenja, odnosno način na koji su tehnologije za filtriranja saobraćaja primenjene ili se može očekivati da budu primenjene na pojedinim hijerarhijskim pozicijama u AMRES mreži. Bolje razumevanje načina na koji se saobraćaj filtrira na pojedinim mestima u AMRES mreži, trebalo bi da koristi administratorima u krajnjim institucijama pri izradi pravila filtriranja u sopstvenim mrežama, kao i u postizanju bolje usklađenosti pravila u svakoj instituciji sa praksom u ostatku mreže.




Osnovna pravila i praksa na mestima filtriranja saobraćaja u AMRES-u:

- Na svim vezama AMRES mreže prema Internetu, primenjuje se paketsko filtriranje saobraćaja na ruterima, čija je primarna svrha da odbaci nedozvoljene protokole, odredišne servis portove i IP adrese, kao i nedozvoljene izvorišne IP adrese i servis portove.

  Dokument kojim bi trebalo da se reguliše filtriranje na ovom nivou je Pravilnik o filtriranju saobraćaja u AMRESu. Pravilnik o filtriranju saobraćaja se utvrđuje na nivou NREN-a, a usvaja ga upravljačko telo NREN-a. Izrađen je nacrt Pravilnika o filtriranju saobraćaja u AMRESu. U isčekivanju njegovog usvajanja, u AMRES-u se primenjuju pravila utvrđena kodeksom ustanovljenim u ranijim razvojnim fazama AMRES-a.

- Na poziciji 2 sa slike, primenjuju se tehnike filtriranja saobraćaja na aplikativnom nivou. Koriste se namenski *proxy* serveri i povremeno drugi uređaji specijalne namene (kao što su uređaji za filtriranje sadržaja). Rešenja i tehike, koje se u kontinuitetu koriste, implementirane su isključivo u servisnim centrima AMRES-a: RCUB-u, JUNIS-u, CIT-UNS i UNIC-u. Uređaji specijalne namene, druga rešenja i tehnike, koje mogu da se primenjuju i povremeno nad delovima mreže ili mrežom u celini, mogu da se po potrebi implementiraju ne samo u servisnim centrima AMRES-a, već i u svim ostalim većim čvorištima AMRES-a (PoP AMRES).

Na poziciji 2, kao najznačanije, izdvaja se filtriranje HTTP saobraćaja upotrebom *proxy* servera. Prema *on-line* statistikama, udeo HTTP saobraćaja u ukupnom saobraćaju je oko 80%. Tradicionalni razlozi upotrebe, radi ublažavanja nedostatka resursa i potrebe očuvanja propusnog opsega, nisu više primarni razlozi korišćenja *proxy* servera u AMRESu. Trenutni razlozi su, pre svega, vezani za ispunjavanje obaveze evidencije saobraćaja u AMRES-u, zaštiti od različitih sigurnosnih pretnji i kontrolisanoj podršci servisu KOBSON.

Od drugih tehnologija, na nivou dva, može biti primenjeno filtriranje sadržaja (*content filetring*).

Dokument kojim bi trebalo da se reguliše filtriranje saobraćaja na drugom nivou je Pravilnik o filtriranju saobraćaja u AMRES mreži, isto kao i za predhodni nivo (poziciju 1).

- Pristup stranim stručnim časopisima i literaturi, obezbeđen preko servisa za objedinjenu nabavku časopisa KOBSON, može se ostvariti **isključivo** korišćenjem namenskih HTTP *proxy* servera na poziciji 2. Prema zahtevu Narodne biblioteke i resornog ministarstva, servis KOBSON mora biti ograničen i raspoloživ jedino za korisnike iz institucija članica AMRES mreže. Rešenje sa autentifikacijom svakog pojedinačnog korisnika pri pristupu KOBSON servisu je izbegnuto, a ispunjavanje postavljenog zahteva je podržano kroz tzv. *proxy* servis AMRESa i prati se na *proxy* serverima u servisnim centrima AMRES-a. Svi HTTP *proxy* serveri na poziciji 2 se koriste u netransparetnom modu. To znači da se računari krajnjih korisnika, u institucijama članicama AMRES mreže, moraju konfigurisati za prolaz kroz *proxy* servis AMRESa.

- Prema priloženoj slici, pozicija 3 se nalazi između čvorišta servisnog centra/PoP AMRES-a i pojedinačnih institucija koje pristupaju *backbone*-u preko tog servisnog centra/PoP AMRES-a. U dokumentu AMRES BPD 110 „Filtriranje saobraćaja u krajnjim institucijama" nalaze se preporuke za institucije članice AMRESa o izradi i upotrebi pravila filtriranja saobraćaja na poziciji 3.

  Postoji praksa da servisni centri filtriraju saobraćaj u ime svih svojih fakulteta/instituta na jednom mestu - mestu isporuke saobraćaja prema/od AMRES PoP-u. Bez obzira što se takvo rešenje fizički implementira u AMRES servisnom centru, ono logički pripada poziciji 3 sa slike, pa se mogu primeniti iste preporuke kao i za svaku drugu pojedinačnu instituciju.

- Na poziciji 3 se mogu primeniti gotovo sve tehnologije filtriranja saobraćaja pobrojane u predhodnim poglavljima ili njihove kombinacije. Načešće se koriste paketski filteri na ruterima/L3 svičevima, samostalni ili kombinovani sa NAT tehnologijom. Druga popularna opcija je upotreba *firewall* uređaja, na kome je ponekad podignut i VPN server.

- Preporuka za AMRES servisne centre je da na interfejsu ka svakoj instituciji članici, primene paketski filter čija je svrha da brani ostatak mreže od nedozvoljenog saobraćaja koji potiče iz mreže institucije članice AMRES-a (IP *spoofing*, i sl.). Obratite pažnju na činjenicu da je ovo preporuka o primeni tzv. ***skupa generalnih pravila filtriranja u AMRESu*** na saobraćaj institucije u samo jednom smeru (na odlazni saobraćaj sa mreža AMRES članica).

  Skup generalnih pravila filtriranja u AMRESu sadrži pravila za *antispoofing*, anti *spam*, ograničavanje upotrebe privatnog i adresnog prostora, ograničavanje ICMP protokola (na računare koje koristi osoblje zaduženo za administraciju mreže), ograničavanje upotrebe protokola koji se pretežno koriste u LAN mrežama (tipa NetBIOS, SQL i sl.). Više o skupu generalnih pravila filtriranja potražite u dokumentu AMRES BPD 110 „Filtriranje saobraćaja u krajnjim institucijama". Skup generalnih pravila filtriranja je uključen u nacrt Pravilnika o filtriranju saobraćaja u AMRESu.

- Nivo 3 ujedno je i perimetar mreže institucije članice AMRES mreže. U odnosu na tu poziciju se definiše termin odlazni i dolazni saobraćaj. Odlazni saobraćaj je saobraćaj koji generiše resurs iz interne mreže AMRES članice u pokušaju pristupa eksternoj usluzi. Alternativni termini za odlazni saobraćaj su izlazni ili *egress* saobraćaj. Dolazni saobraćaj je saobraćaj koji generiše eksterni resurs u pokušaju pristupa usluzi (servisu) u internom delu AMRES članice. Alternativni termini za dolazni saobraćaj su ulazni ili *ingress* saobraćaj.

  Svaka institucija članica AMRES mreže bi trebalo da, na perimetru svoje mreže, samostalno kontroliše dolazni i odlazni saobraćaj po važećim pravilima u AMRESu, koja mogu biti proširenja definisanjem sopstvenih pravila i upotrebom tehnologije po sopstvenom izboru. To, od institucija/organizacija članica AMRESa, zahteva izvesno angažovanje na ovim aktivnostima, naročito na početku. AMRES BPD 110 dokument o filtriranju saobraćaja u krajnjim institucijama sadrži preporuke i predloge (uključujući komande za konfiguraciju paketskih filtara na IOS operativom sistemu). Mišljenja smo da ove preporuke mogu pomoći institucijama članicama u postupku preuzimanja filtriranja u svoju naležost, ali ne obavezuje pojedinačne institucije/organizacije da ih primene. U krajnjem, primena preporuka iz ovog dokumenta, treba da podigne nivo bezbednosti i efikasnost filtriranja saobraćaja u celom AMRESu.

  Dokument kojim bi institucija članica AMRES mreže trebalo, ukoliko to želi, da reguliše filtriranje na trećem, četvrtom i svim sledećim nivoima je Pravilnik o filtriranju saobraćaja te institucije (ukoliko se donosi kao samostalni dokument). Filtriranje može biti regulisano i kao deo Pravilnika o bezbednost IKT u toj instituciji (*information security policy*), ukoliko takav Pravilnik postoji.

- Trenutno se u AMRESu na više mesta koristi tehničko rešenje, koje za posledicu ima, da se perimetar mreže krajnje institucije nalazi „unutar" jednog uređaju (najčešće L3 svič pod administrativnom kontrolom AMRES servisnog centra), a ne na vezi između dva uređaja, kao što je prikazano na priloženoj slici. Svi takvi slučajevi, zbog pitanja nadležnosti, zahtevaju više koordinacije između servisnog centra i krajnje institucije, pri implementaciji i održavanju pristupnih listi. Pitanje prenosa nadležnosti se rešava upotrebom neke od metoda autorizacije raspoložive na mrežnom uređaju. Za Cisco uređaje (koji se koriste u najvećem broju situacija) testirana su dva rešenje kojima se korisniku prava proširuju na skup komandi potrebnih za implementaciju pristupnih listi. Autorizacija se ostvaruju pomoću *rola* u *Role-based CLI* okruženju ili definisanjem različitih nivoa privilegija za enable *password*.

- Nivo 4 je uključen, da bi objasnili različite potrebe i načine primene tehnologija filtriranja saobraćaja, unutar mreže pojedinih institucija članica AMRES-a. Posebno važno mesto je upotreba *proxy* servisa.

  Kao što je pomenuto, iza paketskog filtra na poziciji 3, može se implementirati HTTP proxy server institucije (na poziciji 4 u internoj mreži institucija članica AMRES-a). Pri tome se mora uzeti u obzir činjenica, da se pristup KOBSON servisu, može ostvariti isključivo upotrebnom proxy servera u AMRES servisnim centrima (nivo dva). Preporuka za institucija članice AMRES mreže, koje koriste sopstvene *proxy* servere je da ih konfigurišu u *parent* modu u odnosu na HTTP *proxy* servere u servisnim cetrima AMRES-a (na poziciji 2).

  Postoji mogućnost da se samostalni *proxy* server u instituciji članici AMRES mreže podesi tako, da direktno pristupa HTTP ili HTTPS serverima izvan AMRES-a, sem za servise KOBSON, koji se odvijaju preko *proxy* servera u AMRES servisnim centrima. Ovakvo rešenje zahteva više veštine pri podešavanju i više truda pri održavanju.

  Svi servisni centri AMRES-a, kao i sve članice AMRES-a, moraju koristiti standard (*X-Forwarded-For*) za identifikaciju originalne IP adrese klijenta koji je inicirao saobraćaj, pri prolasku kroz *proxy* server. Datoteke sa logovima se moraju čuvati minimalno 3 meseca.

- Institucije članice AMRESa, mogu da koriste *firewall* na poziciji 4 sa slike, da bi obezbedile dodatni nivo bezbednosti u lokalnoj mreži. Time se najčešće želi sprečiti neovlašćen pristup onim delovima mreže, na kojima se nalaze posebno važni resursi ili se vrše posebno osetljive funkcije poput računovodstva, studentske službe i sl.

- Preporuka je svim institucijama da koriste paketske filtere ili različita *firewall* rešenja, raspoloživa na serverima, i da putem njih omoguće pristup samo ka servisima tog servera, a da onemoguće svi druge portove na serveru.

# 4 Reference


[1] Karen Scarfone, Paul Hoffman, Guidelines on Firewalls and Firewall Policy, Recommendations of the NIST, September 2009.

[2] Eizabet D. Zwicky, Simon Cooper & D. Brent Chapman, *Buidling Internet Firewalls*, O'Reilly Media, Second Edition, June 2000.

[3] Brian Morgan, Neil Lovering, CCNP ISCW Official Exam Ceerification Guide, Cisco Press, July 2007.

[4] NIST SP 800-95, Guide to Secure Web Services, http://csrc.nist.gov/publications/PubsSPs.html.

[5] NIST SP 800-94, Guide to Intrusion Detection and Prevention Systems (IDPS) http://csrc.nist.gov/publications/PubsSPs.html.

[6] JNCIA-Junos Study Guide—Part 2, https://learningportal.juniper.net

# 5 Rečnik

| | |
|---|---|
| **ACL** | Access Control List |
| **AF** | Application Firewall |
| **AMRES** | Akademska mreža Srbije |
| **APG** | Application Proxy Gateway |
| **AUP** | Acceptable Use Policy |
| **CIT-UNS** | Centar za informacione tehnologije Univerziteta u Novom Sadu |
| **DP** | Dedicated Proxy |
| **DPI** | Deep Packet Inspection |
| **DNS** | Domain Name System |
| **DoS** | Denial of Service |
| **FTP** | File Transfer Protocol |
| **GRE** | Generic Routing Encapsulation |
| **HTTP** | HyperText Transfer Protocol |
| **HTTPS** | HyperText Transfer Protocol Secure |
| **ICMP** | Internet Control Message Protocol |
| **IDP** | Intrusion Detection and Prevention |
| **ID** | Intrusion Detection |
| **IMAP** | Internet Message Access Protocol |
| **IP** | Internet Protocol |
| **IP** | Intrusion Prevention |
| **IPSec** | Internet Protocol Security |
| **JUNIS** | Jedinstveni naučno-nastavni informacioni sistem Univerziteta u Nišu |
| **KOBSON** | Konzorcijum biblioteka Srbije za objedinjenu nabavku naučnih časopisa |
| **LAN** | Local Area Network |
| **L3** | OSI layer 3 – Network layer |
| **L4** | OSI Layer 4 – Transport layer |
| **NAT** | Network Address Translation |
| **NetBIOS** | Network Basic Input/Output Sistem |
| **NREN** | Nacional Research and Education Network |
| **OSI** | Open Systems Interconnection |
| **PAT** | Port Address Translation |
| **POP3** | Post Office Protocol Version 3 |
| **RCUB** | Računarski centar Univerziteta u Beogradu |
| **SMTP** | Simple Mail Transfer Protocol |
| **SQL** | Structured Query Language |
| **TCP** | Transmission Control Protocol |

| | |
|---|---|
| **UNIC** | Računarski Centar Univerziteta u Kragujevcu |
| **VoIP** | Voice over Internet Protocol |
| **VPN** | Virtual Private Network |
| **XML** | Extensible Markup Language |