HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Filtriranje prometa usmjerivačima

CCERT–PUBDOC–2008–02-220

CARNet CERT u suradnji s LS&S

Sigurnosni problemi u računalnim programima i operativnim sustavima područje je na kojem CARNet CERT kontinuirano radi.

Rezultat toga rada ovaj je dokument, koji je nastao suradnjom CARNet CERT–a i LS&S–a, a za koji se nadamo se da će Vam koristiti u poboljšanju sigurnosti Vašeg sustava.

CARNet CERT, www.cert.hr – nacionalno središte za **sigurnost računalnih mreža** i sustava.

LS&S, www.lss.hr – laboratorij za sustave i signale pri Zavodu za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu.

Sadržaj

1. Uvod

Usmjeravanje (eng. *routing*) je postupak odabira puta za slanje podataka računalnom mrežom, a provode ga takozvani algoritmi usmjeravanja koji izgrađuju tablice usmjeravanja, u njih pohranjuju dostupne podatke o topologiji mreže na kojoj djeluju i na temelju tih podataka određuju rute kojima se podaci prosljeđuju. Oni se izvode na specijaliziranim uređajima zajedničkog imena usmjerivači (eng. *router*).

Spomenuti uređaji, pored usmjeravanja podatkovnog prometa, omogućuju stvaranje lista za kontrolu pristupa (eng. *Access Control List - ACL*) pomoću kojih je moguće ograničiti ili potpuno onemogućiti pristup pojedinim uslugama te otežati izvođenje određenih vrsta mrežnih napada.

U ovom dokumentu dan je pregled osnovnih koncepata vezanih uz usmjeravanje, usmjerivače i liste usmjeravanja te je opisan koncept lista za kontrolu pristupa. Stvaranje i podešavanje različitih lista za kontrolu pristupa ilustrirano je na primjerima naredbi IOS (eng. *Internetwork Operating System*) operacijskog sustava tvrtke *Cisco*. Ovaj sustav izvodi se na velikoj većini usmjerivača spomenute tvrtke te na svim aktualnim mrežnim preklopnicima (eng. *switch*) iste tvrtke. Upravo zbog svoje popularnosti izabran je za demonstraciju mogućnosti i primjena ACL lista.

2. Osnove usmjeravanja i usmjerivača

2.1. Usmjeravanje

Usmjeravanjem se određuje način prosljeđivanja (eng. *forwarding*) logički adresiranih paketa od njihove izvorišne mreže do krajnjeg odredišta, a preko posrednih čvorova. Ovi čvorovi su najčešće posebno oblikovani sklopovski uređaji, tzv. usmjerivači. Usmjeravanje paketa provodi se na temelju tablica usmjeravanja u kojima su zabilježene najbolje rute medu pojedinim mrežnim odredištima. Zbog toga je za efikasno usmjeravanje presudan odgovarajući postupak stvaranja i održavanja tablica usmjeravanja. One su pohranjene u memoriji usmjerivača.

Usmjeravanje se razlikuje od premošćivanja (eng. *bridging*) po tome što se na temelju strukture adresa mrežnih odredišta pretpostavlja njihov raspored unutar mreže: odredišta sa sličnim adresama su međusobno bliža i obrnuto. Time je omogućeno pohranjivanje rute prema skupini adresa jednim unosom u tablici usmjeravanja. Kod većih mreža usmjeravanje pokazuje bolje performanse od premošćivanja i prevladavajući je način određivanja puta podataka na Internetu.

Unutar manjih mreža moguće je za usmjeravanje koristiti ručno podešene tablice usmjeravanja. Kod velikih mreža takvo podešavanje je otežano složenim topologijama i stalnim promjenama strukture. Unatoč tome PSTN (eng. *Public Switched Telephone Network*) telefonske mreže koriste prethodno proračunate tablice usmjeravanja, s pričuvnim rutama za slučaj da najkraće postanu nedostupne. Dinamičko usmjeravanje je pristup ovom problemu usmjeravanja kod kojega se tablice automatski proračunavaju na temelju podataka prenošenih prema protokolima usmjeravanja. Iako se tako postavljena mreža do određenog stupnja autonomno prilagođava sklopovskim kvarovima i zagušenjima, ipak je prilikom njenog postavljanja i tijekom održavanja nužno sudjelovanje stručnjaka.

Kod prospojnih mreža (eng. *packet switched*), kakva je Internet, podaci se prije slanja razlažu u pakete od kojih svaki nosi adresu odredišta i usmjeruje ih se pojedinačno. Spojne mreže (eng. *circuit switched*), npr. telefonska mreža, također provode usmjeravanje sa ciljem pronalaženja najbolje rute za uspostavljanje kruga, npr. telefonskog poziva, preko kojeg se šalju veće količine podataka bez ponovljenog prijenosa adresa odredišta.

2.2. Tablice usmjeravanja

Tablice usmjeravanja su baze podataka smještene na usmjerivačima unutar kojih su pohranjeni podaci o topologiji mreže. Koriste se prilikom prosljeđivanja podatkovnih paketa tako što se adresa odredišta povezuje s mrežnim rutama koje do njega vode. Izgradnja i održavanje ovih tablica osnovni je zadatak protokola usmjeravanja.

Kod najjednostavnijeg modela usmjeravanja, tzv. *hop-by-hop* modela, svaka tablica usmjeravanja sadrži adresu sljedećeg uređaja na ruti prema svakom dostupnom odredištu. U ovakvom slučaju, i pod pretpostavkom dosljednosti tablica usmjeravanja, jednostavan algoritam prosljeđivanja paketa prema sljedećem uređaju na ruti osigurava uspješno usmjeravanje podataka prema svim odredištima u mreži. U praksi se umjesto opisanog jednostavnog modela usmjeravanja češće koriste slojevite arhitekture, npr. MPLS (eng. *Multiprotocol Label Switching*), kod kojih je pomoću jednog zapisa iz tablice usmjeravanja moguće odrediti nekoliko sljedećih postaja na ruti prema odredištu. Na ovaj se način smanjuje broj potrebnih čitanja tablice te se poboljšavaju performanse usmjeravanja.

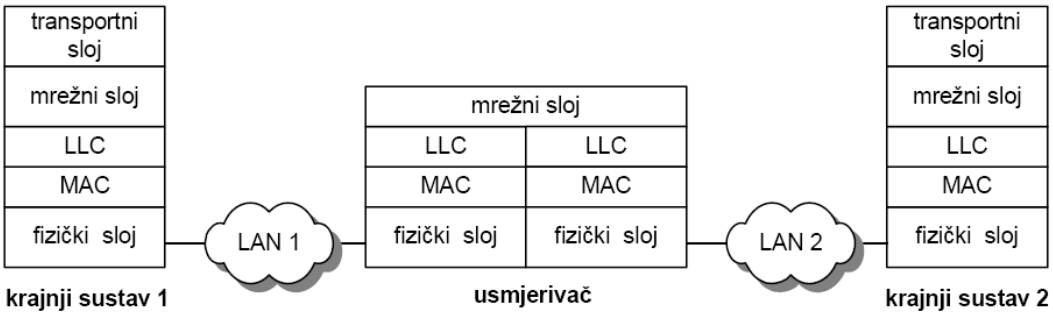
Osnovni problem u izgradnji tablica usmjeravanja je potreba za pohranjivanjem ruta prema velikom broju mrežnih odredišta unutar ograničenog memorijskog prostora. Pretpostavka na kojoj se temelji usmjeravanje je da se slične adrese odnose na uređaje blisko smještene unutar mreže, što su adrese sličnije to su uređaji bliže postavljeni. Ovime je omogućeno pohranjivanje rute prema većem broju odredišta jednim zapisom u tablici usmjeravanja. Grupiranje mrežnih odredišta aktivno je područje istraživanja, a trenutno na Internetu prevladava CIDR (eng. *Classless Inter_Domain Routing*) tehnologija interpretiranja IP adresa.

Tablice usmjeravanja među pojedinim elementima mreže moraju biti dosljedne, kako ne bi došlo do zatvaranja petlji usmjeravanja. Ovo je naročito važno kod *hop-by-hop* modela kod kojih nedosljedne tablice nekolicine usmjerivača mogu dovesti do prosljeđivanja paketa u beskonačnoj petlji.

Osiguravanje dosljednosti tablica i ograničavanje njihove veličine glavni su zadaci protokola usmjeravanja.

2.3. Usmjerivači

Usmjerivač je mrežni uređaj koji radi na mrežnom sloju protokolnog OSI (eng. *Open Systems Interconnection*) modela. *Slika 1* prikazuje mogući scenarij povezivanja dviju lokalnih mreža usmjerivačem. Ako obje lokalne mreže koriste iste protokole drugog sloja, tada usmjerivač djeluje isključivo na mrežnom sloju. Ako se na ovaj način povezuju dvije lokalne mreže koje koriste različite protokole sloja podatkovne veze, tada usmjerivač mora djelovati i na drugom sloju, tj. mora obavljati i pretvorbu formata MAC (eng. *Media Access Control*) okvira.



Slika 1: Prikaz protokolnog stoga usmjerivača koji povezuje dvije lokalne mreže

Osnovne operacije koje svaki usmjerivač mora obavljati su:

- prosljeđivanje paketa iz jedne u drugu mrežu (eng. *forwarding*), i
- određivanje smjerova prijenosa paketa kroz mrežu (eng. *routing*).

Kad usmjerivač po jednom od svojih priključaka primi paket, na temelju odredišne mrežne adrese (npr. IP adrese) upisane u zaglavlje paketa i tablice usmjeravanja donosi odluku na koji će priključak proslijediti paket. Paralelno s procesom prosljeđivanja paketa, svaki usmjerivač proračunava optimalne smjerove prijenosa paketa korištenjem odgovarajućih algoritama. Usmjerivači međusobno razmjenjuju informaciju o smjerovima prijenosa koristeći pritom usmjerivačke protokole, npr. RIP (eng. *Routing Information Protocol*), OSPF (eng. *Open Shortest Path First*) i druge.

3. Osnove ACL lista

Lista kontrole pristupa je uređeni skup podataka o ovlastima ili pravima pristupa svih korisnika ili aplikacija na računalnom sustavu. Svaki korisnik ili grupa korisnika ima određena prava pristupa i ovlasti nad pojedinim direktorijem ili datotekom, kao što su ovlasti čitanja, pisanja ili izvođenja. Kod uobičajenih lista kontrole pristupa svaki element liste određuje subjekt i operacije koje on smije obavljati nad određenim objektom. Na primjer unos *(Alice, delete)* u listi za neku datoteku daje korisniku Alice ovlasti brisanja te datoteke.

Kod računalnih mreža, ACL liste predstavljaju skupinu pravila koja određuju portove ili pozadinske aplikacije (eng. *deamon*) koje su raspoložive na uređaju mrežnog sloja OSI modela, a uz listu korisnika ili mreža kojima je dozvoljeno korištenje te usluge. Pojedini mrežni poslužitelji te usmjerivači mogu posjedovati ACL liste koje je moguće podesiti tako da kontroliraju dolazni i odlazni podatkovni promet. U tom smislu ACL liste slične su vatrozidima.

Osnovna podjela ACL lista je na standardne i proširene liste. Standardne liste omogućuju filtriranje prometa samo na temelju izvorišne adrese zapisane u zaglavlju IP (eng. *Internet Protocol*) podatkovnog paketa. Proširene ACL liste omogućuju filtriranje prometa i prema:

- izvorišnoj IP adresi,
- odredišnoj IP adresi,
- TCP/IP protokolu, kao što su IP, ICMP (eng. *Internet Control Message Protocol*), OSPF, TCP (eng. *Transmission Control Protocol*), UDP (eng. *User Datagram Protocol*) i drugi,
- podacima TCP/IP protokola kao što su brojevi TCP i UDP portova, TCP zastavice i ICMP poruke.

Iz navedene razlike između dvaju osnovnih tipova lista kontrole pristupa proizlaze i razlike u primjenama. Standardne ACL liste na usmjerivačima se koriste za:

- ograničavanje pristupa usmjerivaču putem VTY (eng. *Virtual Teletype Terminal*) linija korištenjem Telnet (eng. *Telecomunication Network*) ili SSH (eng. *Secure Shell*) protokola,
- ograničavanje pristupa usmjerivaču putem HTTP (eng. *Hypertekst Transfer Protocol*) ili HTTPS (eng. *HTTP Secure*) protokola,
- filtriranje poruka za osvježavanje postavki usmjerivača.

Proširene ACL liste uobičajeno se koriste za filtriranje prometa među sučeljima na samom usmjerivaču, prije svega zbog njihove prilagodljivosti koja proizlazi iz mogućnosti djelovanja na protokola drugog, trećeg i četvrtog sloja OSI mrežnog modela.

Prednosti filtriranja prometa na usmjerivačima pred vatrozidima su:

- usmjerivači mogu podatkovne pakete obrađivati vrlo velikom brzinom,
- djelovanje na 3. i 4. sloju OSI modela omogućuje veliku fleksibilnost implementiranja sigurnosne politike.

Prilikom postavljanja sustava zaštite računalne mreže potrebno je na umu imati ograničenja lista kontrole pristupa. One naime ne mogu spriječiti sve vrste napada, ali zato mogu ukloniti veliku količinu nepoželjnih i štetnih paketa smanjujući tako opterećenje sljedećih stupnjeva zaštite, npr. vatrozida.

3.1. Stvaranje ACL lista

Za svaki filtrirani protokol, na primjer za IP ili IPX (eng. *Internetworking Packet Exchange*) protokole, potrebno je stvoriti zasebnu ACL listu. Svaka lista predstavlja skupinu unosa koji definiraju pravila filtriranja, a unosi se grupiraju na temelju imena ili brojevne oznake. Kod brojevnog označivanja nije moguće pridjeljivanje nasumičnih brojeva, već su uz pojedine protokole vezani raspoloživi rasponi oznaka. Tako su, na primjer kod usmjerivača tvrtke *Cisco*, IP protokolu dodijeljeni rasponi brojevnih oznaka 1 do 99 i 1300 do 1999, AppleTalk protokolu brojevi od 600 do 699, a IPX protokolu 800 do 899.

Prilikom stvaranja lista za kontrolu pristupa preporuča se:

- poznavanje topologije računalne mreže i sigurnosnih politika koje je potrebno implementirati,
- implementacija sigurnosnih politika redom od najrestriktivnijih prema manje restriktivnima,
- kod ACL unosa iste razine savjetuje se njihovo raspoređivanje tako da češće korišteni unosi prethode rjeđe korištenima, kako bi se smanjilo opterećenje usmjerivača,
- korištenje komentara radi lakšeg razumijevanja i održavanja liste.

3.2. Aktiviranje ACL lista

Nakon stvaranja liste za kontrolu pristupa potrebno ju je aktivirati kako bi ona imala utjecaja na rad usmjerivača. Pri tome je potrebno odrediti na koji protokol će se lista primjenjivati te primjenjuje li se lista na dolazni ili odlazni promet.

3.3. Izmjena ACL lista

Kod pojedinih starijih usmjerivača, odnosno starijih inačica operacijskih sustava usmjerivača, postoje određena ograničenja u izmjenama ACL lista. Na primjer, nije moguće izbrisati unos, umetnuti unos na određeno mjesto u listi ili izmijeniti pojedini unos. Kod takvih usmjerivača postupak izmjene liste za kontrolu pristupa je složen i provodi se u više koraka. Noviji usmjerivači omogućuju jednostavne izmjene pojedinih unosa ACL lista.

3.4. Višeznačne maske

Primjenjivanje unosa ACL liste na veći broj IP adresa moguće je implementirati korištenjem višeznačne (eng. *wildcard*) maske. Ako je, na primjer, potrebno omogućiti pristup prema svim IP adresama iz raspona 192.168.1.0/254 moguće je u ACL listu upisati 254 unosa, po jedan za svaku

adresu iz navedenog raspona. Ovim pristupom otežava se izgradnja lista za kontrolu pristupa i degradiraju performanse usmjerivača. Drugi pristup je korištenje višeznačnih maski.
Višeznačne maske su, jednako kao i IP adrese, 32-bitne vrijednosti. Pojedini bitovi višeznačne maske određuju uzimaju li se odgovarajući bitovi IP adrese u obzir prilikom odluke o primjeni ACL unosa na promet s ili prema toj adresi. Tako se, na primjer, postavljanjem iznosa višeznačne maske na 0.0.0.255 pravila filtriranja ACL liste primjenjuju na sve adrese čijih se gornjih 24 bita (gornja tri okteta) poklapaju s adresama u ACL unosima. Vrijednost donjeg okteta nije bitan (eng. *don't care*).

4. Standardne ACL liste

Prvotno je postojala velika razlika u performansama standardnih i proširenih lista za kontrolu pristupa. Ova razlika proizlazila je iz činjenica kako je standardne ACL liste, za razliku od proširenih, bilo moguće pohranjivati u priručne memorije (eng. *cache*) usmjerivača. Administratori su tada, s ciljem maksimiziranjem performansi usmjerivača, izbjegavali upotrebu proširenih lista. Danas brojni usmjerivači omogućuju sklopovsku obradu ACL lista, na primjer usmjerivači koji podržavaju CEF (eng. *Cisco Express Forwarding*) tehnologiju, pa izbor između standardnih i proširenih lista ovisi u najvećoj mjeri o potrebama pojedine primjene.

4.1. Pobrojane standardne ACL liste

Prije svakog stvaranja ili podešavanja ACL listi IOS operacijski sustav potrebno je postaviti u način rada za podešavanje naredbom `config`:

```
Router# config
Router(config)#
```

Kao što je u primjeru vidljivo, nakon izvođenja naredbe ulazak u način rada za podešavanje prikazan je promjenom odzivnog znaka (eng. *prompt*). Nakon toga, pobrojanoj ACL listi unosi se dodaju naredbom:

```
Router(config)# access-list ACL_# {permit | deny}
    source_IP_address [wildcard_mask] [log]
```

Naredbi proslijeđeni parametri su:

- `ACL_#` - broj liste koji može biti iz raspona 1 do 99 ili 1300 do 1999,
- `{permit | deny}` - akcija koja se poduzima u slučaju zadovoljenja uvjeta (omogućavanje ili onemogućavanje zatražene radnje),
- `source_IP_address` - izvorišna IP adresa,
- `[wildcard_mask]` - višeznačna maska, ovaj parametar nije nužan,
- `[log]` - posljednji parametar određuje stvara li se u slučaju zadovoljenja uvjeta dnevnički zapis. Zapis se, ovisno o postavkama usmjerivačima, stvara na konzoli, unutrašnjem spremniku usmjerivača ili na tzv. *syslog* poslužitelju.

U slučaju izostavljanja `[wildcard_mask]` parametra primjenjuje se višeznačna maska 0.0.0.0, što znači da je za primjenu pravila potrebno poklapanje IP adrese s onom iz unosa u ACL listu. Ako se pravilo želi primjenjivati na promet sa svih IP adresa `source_IP_address` i `[wildcard_mask]` zamjenjuju se ključnom riječi `any`. U ovom kao i u daljnjim primjerima parametri koje je moguće izostaviti označeni su uglatim zagradama.
Nakon stvaranja ACL liste potrebno ju je aktivirati. To je moguće učiniti naredbama:

```
Router(config)# interface type [slot_#/]port_#
Router(config-if)# ip access-group ACL_#_or_ACL_name {in | out}
```

Naredbom `interface type` mijenja se način rada, što je opet prikazano promjenom odzivnog znaka. Nakon toga se naredbi `ip access-group` prosljeđuje ime ili broj ACL liste koju se želi

aktivirati te se određuje hoće li se promet obrađivati na ulasku u usmjerivač (`in`) ili na izlasku iz njega (`out`).

4.2. Imenovane standardne ACL liste

Imenovane ACL liste kod Cisco IOS sustava uvedene su s inačicom 11.2. Njihove glavne prednosti pred standardnim ACL listama su:

- omogućuju davanje opisnih imena listama za kontrolu pristupa te
- stvaranje slijednih (eng. *sequenced*) ACL lista.

Osim navedenih razlika, izbor između pobrojanih i imenovanih lista u većini slučajeva stvar je osobnog izbora.
Unos u imenovanu ACL listu dodaje se slijedom naredbi:

```
Router(config)# ip access-list standard name_of_ACL
Router(config-std-nacl)# deny {source [src_wildcard] | any} [log]
Router(config-std-nacl)# permit {source [src_wildcard] | any} [log]
Router(config-std-nacl)# exit
```

Naredbom `ip access-list` određuje se tip ACL liste (`standard`) te njezino ime. Navedeno ime može biti i broj, npr. moguće je stvoriti listu za kontrolu pristupa imena 50. Izvršavanjem ove naredbe prelazi se u novi način rada u kojemu se unose `deny` i `permit` naredbe koje imaju jednaku sintaksu kao opisana `access-list` naredba kod pobrojanih standardnih lista.
ACL lista se, nakon unosa, aktivira također navedenom, `ip access-group` naredbom.

5. Proširene ACL liste

Proširene liste za kontrolu pristupa mnogo su fleksibilnije od standardnih jer omogućuju stvaranje složenijih kriterija za omogućavanje ili onemogućavanje pristupa. Kao i kod standardnih lista, dijele se na standardne i proširene. Zbog toga što su osnovne razlike između pobrojanih i imenovanih lista za kontrolu pristupa opisane u odjeljku o standardnim ACL listama, u nastavku je dan samo pregled pobrojanih proširenih lista.

5.1. Pobrojane proširene ACL liste

Unos u pobrojanu proširenu listu stvara se naredbom:

```
Router(config)# access-list ACL_# {deny | permit}
    protocol_name_or_#
    source_IP_address source_wildcard_mask
    destination_IP_address destination_wildcard
    [protocol_options] [precedence precedence]
    [dscp value] [tos tos] [log | log-input] [fragments]
    [established]
```

Prvi parametar `access-list` naredbi je broj liste koji može biti iz raspona 100 do 199 ili 2000 do 2699. Nakon toga slijedi ime ili broj TCP/IP protokola. Cisco IOS podržava sljedeća imena protokola:

- **ahp** - eng. *Authentication Header Protocol*,
- **eigrp** - Cisco EIGRP (eng. *Enhanced Interior Gateway Routing Protocol*) protokol za usmjeravanje,
- **esp** - eng. *Encapsulation Security Payload*,
- **gre** - Cisco GRE (eng. *Generic Routing Encapsulation*) tuneliranje,
- **icmp** - eng. *Internet Control Message Protocol*,
- **igmp** - eng. *Internet Gateway Message Protocol*,
- **ip** - bilo koji IP protokol,
- **ipinip** - IP u IP tuneliranju,

- **nos** - KA9Q NOS kompatibilno IP u IP tuneliranje,
- **ospf** - OSPF protokol za usmjeravanje,
- **pcp** - eng. *Payload Compression Protocol*,
- **pim** - eng. *Protocol Independent Multicast*,
- **tcp** - eng. *Transmission Control Protocol*,
- **udp** - eng. *User Datagram Protocol*.

U slučaju filtriranja nekog od protokola čije ime nije podržano, potrebno je umjesto imena unijeti broj. Podržani su brojevi protokola od 0 do 255. Nakon oznake protokola potrebno je unijeti izvorišnu i odredišnu IP adresu te pripadne višeznačne maske.

Ostali parametri su neobavezni. Parametar `[protocol_options]` vezan je uz odabrani protokol, dok `precedence` omogućuje filtriranje na određenom stupnju prioriteta, od 0 do 7. Polje prioriteta kod IP paketa najčešće određuje QoS (eng. *Quality of Service*) razinu kvalitete usluge. Umjesto broja moguće je koristiti sljedeće oznake prioriteta:

- **critical** (0),
- **flash** (1),
- **flash-override** (2),
- **immediate** (3),
- **internet** (4),
- **network** (5),
- **priority** (6),
- **routine** (7).

Parametar `dscp` omogućuje filtriranje na temelju vrijednosti DSCP (eng. *Differentiated Services Code Point*) polja iz zaglavlja IP paketa. Ova vrijednost koristi se za implementiranje QoS prioritizarnog prometa, a naredbi je moguće proslijediti brojevnu vrijednost iz raspona 0 do 63 ili ime DSCP koda.

Parametar `tos` omogućuje filtriranje na temelju vrijednosti ToS (eng. *Type of Service*) polja u zaglavlju IP paketa, koje se također ponekad koristi za implementaciju QoS mehanizama. Parametar može poprimiti vrijednosti od 1 do 15 ili se naredbi prosljeđuje ime usluge:

- **max-reliability**,
- **max-throughput**,
- **min-delay**,
- **min-monetary-cost**,
- **normal**.

Parametrom `log` podešava se stvaranje dnevničkog zapisa u slučaju ostvarenja uvjeta iz ACL unosa. Medij na koji se vrši upis može se, jednako kao kod standardnih lista, podesiti postavkama usmjerivača. Među ostalim, u dnevnički zapis se upisuje:

- izvedena akcija: omogućavanje ili onemogućavanje prometa,
- protokol, kao što su TCP, UDP ili ICMP,
- izvorišna i odredišna adresa,
- kod TCP i UDP protokola zapisuju se i brojevi izvorišnih i odredišnih portova,
- za ICMP protokol upisuje se tip poruke.

Dnevnički zapis stvara se kod prvog paketa koji zadovoljava postavljene uvjete, te se nakon toga 5 minuta ne stvaraju zapisi. Nakon isteka ovog perioda postupak se ponavlja. Ovime se usmjerivač osigurava od napada uskraćivanjem usluga (eng. *Denial of Service - DoS*). Izvorno postavljeni interval od 5 min moguće je u slučaju potrebe podesiti `ip access-list log-update` naredbom.

Omogućavanjem dnevničkih zapisa onemogućuje se CEF (eng. *Cisco Express Forwarding*) tehnika brzog usmjeravanja paketa pa se performanse usmjerivača time znatno degradiraju. Zbog toga je dnevničke zapise preporučeno koristiti samo za otkrivanje počinitelja mrežnog napada, nakon čega se savjetuje isključivanje ove mogućnosti.

Varijanta `log-input` parametra za omogućavanje stvaranja dnevničkih zapisa pruža mogućnost određivanja dolaznog sučelja primljenih paketa koji se zapisuju te njihovih adresa iz drugog sloja OSI modela, kao što su Ethernet MAC adrese, relejni DLCI (eng. *Data Link Connection Identifier*) broj okvira ili ATM (eng. *Asynchronous Transfer Mode*) VC (eng. *Virtual Channel*) broj.

Parametrom `fragments` moguće je onemogućiti prolazak fragmentiranih IP paketa usmjerivačem. Ovime se postiže dodatni stupanj sigurnosti jer se pojedini udaljeni napadi temelje na zaobilaženju zaštitnih mehanizama razbijanjem zlonamjerno oblikovanih podatkovnih paketa u fragmente.
Kod TCP protokola `established` parametar omogućuje propuštanje povratnih TCP paketa s postavljenom nekom od sljedećih zastavica:

- ACK (eng. *ACKnowledge*),
- FIN (eng. *FINished*),
- PSH (eng. *PuSH*),
- RST (eng. *ReSeT*),
- SYN (eng. *SYNchronize*),
- URG (eng. *URGent*).

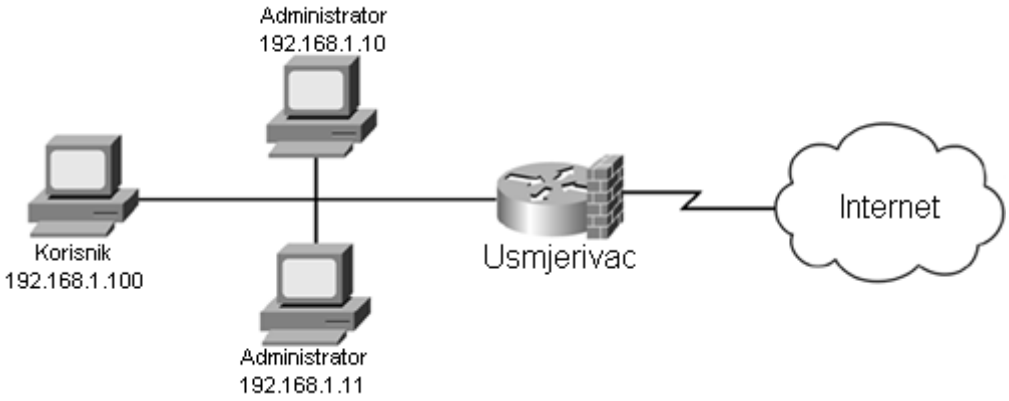
6. Primjeri

6.1. Ograničavanje VTY pristupa standardnom ACL listom

VTY pristup na mreži prikazanoj slikom *Slika 2* moguće je ograničiti pobrojanom standardnom ACL listom na sljedeći način:

```
Router(config)# access-list 1 permit 192.168.1.10
Router(config)# access-list 1 permit 192.168.1.11
Router(config)# line vty 0 4
Router(config-line)# access-class 1 in
```

Navedenim naredbama VTY pristup omogućen je dvama administratorskim računalima, dok je korisniku onemogućen.



Slika 2: Primjer jednostavne mreže s usmjerivačem

Jednak učinak moguće je postići standardnom imenovanom ACL listom:

```
Router(config)# ip access-list standard restrict_VTY
Router(config-std-nacl)# permit 192.168.1.10
Router(config-std-nacl)# permit 192.168.1.11
Router(config-std-nacl)# exit
Router(config)# line vty 0 4
Router(config-line)# access-class restrict_VTY in
```

6.2. Filtriranje TCP prometa pobrojanom proširenom ACL listom

TCP promet moguće je filtrirati pobrojanom proširenom ACL listom korištenjem naredbe:

```
Router(config)# access-list ACL_# {deny | permit} tcp
    source_IP_address source_wildcard_mask
    [operator src_port_name_or_number]
    destination_IP_address destination_wildcard
    [operator dest_port_name_or_number]
    [log | log-input] [precedence precedence] [dscp value]
    [tos tos] [fragments]
    [established] [ack] [fin] [psh] [rst] [syn] [urg]
```

Jedna od specifičnosti navedenog primjera vezanih uz TCP protokol je [*operator dest_port_name_or_number*] izraz koji omogućuje filtriranje po brojevima izvorišnih i odredišnih portova. Pri tome je potrebno navesti operator te ime ili broj porta. Podržani su operatori:

- **eq** - broj porta mora odgovarati navedenom,
- **lt** - broj porta mora biti niži od navedenog,
- **gt** - broj porta mora biti viši od navedenog,
- **neq** - broj porta mora biti različit navedenom,
- **range** - broj porta mora biti iz raspona s graničnim vrijednostima koje se navode s razmakom, na primjer: `range 22 33`.

Osim brojem, port je moguće navesti i imenom ukoliko je specifično ime podržano. U suprotnom je nužno navesti broj porta.
Ostali parametri navedeni u primjeru opisani su u odjeljku o pobrojanim proširenim ACL listama.

6.3. Blokiranje prometa s nepridijeljenih IP adresa

Pojedine IP adrese nisu alocirane od strane IANA (eng. *Internet Assigned Numbers Authority*) organizacije te se one često koriste za izvođenje DoS te DDoS (eng. *Distributed DoS*) napada. Zbog toga ih je preporučeno blokirati, kao u primjeru:

```
Router(config)# ip access-list extended ingress-filter
Router(config-ext-nacl)# remark Unassigned IANA addresses
Router(config-ext-nacl)# deny ip 1.0.0.0 0.255.255.255 any
Router(config-ext-nacl)# deny ip 2.0.0.0 0.255.255.255 any
…
Router(config-ext-nacl)# remark RFC 1918 private addresses
Router(config-ext-nacl)# deny ip 10.0.0.0 0.255.255.255 any
Router(config-ext-nacl)# deny ip 172.16.0.0 0.15.255.255 any
…

Router(config-ext-nacl)# remark Other bogons
Router(config-ext-nacl)# deny ip 224.0.0.0 15.255.255.255 any
Router(config-ext-nacl)# deny ip 240.0.0.0 15.255.255.255 any
…
```

Navedenim primjerom filtrira se dolazni promet s nepridijeljenih adresa, ali kako brojne sigurnosne prijetnje nastaju unutar štićene mreže potrebno je ograničiti i odlazni promet. To je moguće učiniti nabrajanjem nedozvoljenih izvorišnih i odredišnih adresa, kao u prethodnom primjeru, ali jednostavnije je omogućiti promet samo s ispravnih IP adresa, npr.:

```
Router(config)# ip access-list extended egress-filter
Router(config-ext-nacl)# permit ip 200.1.1.0 0.0.0.255 any
Router(config-ext-nacl)# deny ip any any
Router(config-ext-nacl)# exit
Router(config)# interface ethernet1
Router(config-if)# ip access-group egress-filter out
```

6.4. Onemogućavanje DoS napada

Napadi uskraćivanjem usluga za cilj imaju zagušivanje ili čak rušenje usmjerivača, a moguće ih je izvoditi korištenjem različitih protokola, npr. ICMP, TCP i UDP protokola. Različite oblike ovakvih napada potrebno je onemogućiti specifičnim listama za kontrolu pristupa. Tako se tzv. *TCP SYN flood* napad, čiji cilj je zagušiti usmjerivač zahtjevima za uspostavom TCP veze, onemogućuje unosom:

```
Router(config)# ip access-list extended tcp-syn-flood
Router(config-ext-nacl)# permit tcp any 200.1.1.0 0.0.0.255
    established
Router(config-ext-nacl)# permit tcp any host 200.1.1.11 eq 25
Router(config-ext-nacl)# deny ip any any
Router(config-ext-nacl)# exit
Router(config)# interface ethernet1
Router(config-if)# ip access-group tcp-syn-flood in
```

Prvom `permit` naredbom omogućuju se povratne poruke kao odgovor na odlazne zahtjeve za uspostavom TCP veze, dok se drugom instancom iste naredbe u mrežu puštaju TCP SYN paketi s poslužitelja elektroničke pošte, kako bi se korisnicima omogućilo korištenje te usluge. Ova dva izraza predstavljaju slabost prikazane liste jer napadač može zlonamjerni paket oblikovati tako da mu postavi neku od zastavica koje označuju povratne pakete ili može za izvođenje napada iskoristiti kompromitirani poslužitelj elektroničke pošte. Zbog toga je za potpuniju zaštitu potrebo implementirati složeniju ACL listu.

6.5. Filtriranje neželjenih usluga

Neželjene usluge, kao što su sustavi trenutnih poruka (eng. *Instant Messaging - IM*) ili P2P (eng. *Peer to Peer*) sustavi za razmjenu datoteka, također je moguće filtrirati ACL listama. Na primjer MSN IM sustav tvrtke Microsoft moguće je filtrirati ACL unosima:

```
Router(config)# ip access-list extended MSN-messenger
Router(config-ext-nacl)# deny tcp any any eq 1503
Router(config-ext-nacl)# deny tcp any any eq 1863
Router(config-ext-nacl)# deny tcp any any eq 6891
Router(config-ext-nacl)# deny udp any any eq 1863
Router(config-ext-nacl)# deny udp any any range 13324 13325
Router(config-ext-nacl)# deny tcp any any eq 569
Router(config-ext-nacl)# deny udp any any eq 569
Router(config-ext-nacl)# deny ip any 64.4.13.0 0.0.0.255
Router(config-ext-nacl)# deny ip any host 207.46.104.20
Router(config-ext-nacl)# deny ip any 207.46.96.0 0.0.0.255
Router(config-ext-nacl)# exit
Router(config)# interface ethernet1
Router(config-if)# ip access-group MSN-messenger out
```

Gnutella je sustav za razmjenu datoteka kojega koriste Bearshare, LimeWare, Gnucleus, ToadNode i drugi servisi. Vrlo je fleksibilan u tome što može koristiti brojne portove. Slijedi primjer ACL liste koja uvelike ograničava razmjenu datoteka Gnutella sustavom:

```
Router(config)# ip access-list extended gnutella
Router(config-ext-nacl)# deny tcp any any range 6345-6349
Router(config-ext-nacl)# deny udp any any range 6345-6349
Router(config-ext-nacl)# exit
Router(config)# interface ethernet1
Router(config-if)# ip access-group gnutella in
Router(config-if)# ip access-group gnutella out
```

Većina Gnutella klijenata koristi TCP port 6346, ali poznati su i slučajevi korištenja ostalih TCP i UDP portova iz raspona 6345 do 6349.

7. Zaključak

ACL liste dijele se na standardne i proširene, a osnovna razlika među njima je u tome što standardne liste omogućuju filtriranje prometa samo na temelju izvorišne adrese dok proširene liste promet mogu filtrirati prema brojnim drugim kriterijima, kao što su izvorišna i odredišna adresa, protokol, te različiti, uz protokol vezani, podaci. Oba tipa dalje se dijele na pobrojane i imenovane ACL liste, ali razlike među ovim podvrstama lista za kontrolu pristupa su u većini primjena zanemarive te izbor uglavnom ovisi o osobnim preferencijama administratora.

Liste za kontrolu pristupa moćan su alat za filtriranje neželjenog podatkovnog prometa unutar računalne mreže te za otkrivanje i sprječavanje udaljenih napada. Ipak, na umu treba imati ograničenja proširenih lista kao što su nemogućnost filtriranja nekih P2P i IM veza te njihova neprikladnost za implementiranje filtriranja u ovisnosti o stanju mreže (eng. *stateful filtering*). Zbog toga je standardne i proširene ACL liste potrebno koristiti u kombinaciji s drugim sigurnosnim alatima kako bi se postigla optimalna razina zaštite.

8. Reference

[1] *Types of ACLs*, http://etutorials.org/Networking/Router+firewall+security/Part+III+Nonstateful+Filtering+Technologies/Chapter+7.+Basic+Access+Lists/Types+of+ACLs/, veljača 2008.

[2] *Protection Against Attacks*, http://etutorials.org/Networking/Router+firewall+security/Part+III+Nonstateful+Filtering+Technologies/Chapter+7.+Basic+Access+Lists/Protection+Against+Attacks/, veljača 2008.

[3] *Blocking Unecessary Services*, http://etutorials.org/Networking/Router+firewall+security/Part+III+Nonstateful+Filtering+Technologies/Chapter+7.+Basic+Access+Lists/Blocking+Unnecessary+Services/, veljača 2008.

[4] Alen Bažant: *Lokalne mreže*, www.tel.fer.hr/files/peta/LiP/LAN.pdf, veljača 2008.

[5] *Access control list*, http://en.wikipedia.org/wiki/Access_control_list, veljača 2008.