HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Filtriranje sadržaja web stranica korištenjem Squid poslužitelja

CCERT-PUBDOC-2007-05-193

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

Programski paketi za kontrolu sadržaja (eng. *content-control*), odnosno alati za filtriranje sadržaja web stranica (eng. *web filtering*), koriste se za onemogućavanje pristupa određenim web stranicama s pojedinih računala ili iz cijelih računalnih mreža. Ograničavanje pristupa pojedinim sadržajima često se provodi kako bi se spriječilo pregledavanje web stranica koje vlasnik računala ili vlasti smatraju spornima. Kada se provodi bez pristanka korisnika, kontrola sadržaja može predstavljati oblik cenzure. Uobičajene primjene su onemogućavanje pristupa neprikladnim sadržajima djeci od strane roditelja ili škole te onemogućavanje posjećivanja pojedinih web stranica zaposlenicima od strane tvrtke.

Squid programski paket je posredni poslužitelj (eng. *proxy server*) i pozadinska aplikacija za stvaranje privremenih kopija web stranica (eng. *web cache daemon*). Koristi se za ubrzavanje web poslužitelja pohranjivanjem opetovanih zahtjeva, web stranica, DNS (eng. *Domain Name System*) i drugih mrežnih zahtijeva te za podizanje razine sigurnosti filtriranjem prometa. Izvorno je namijenjen radu s HTTP (eng. *Hypertext Transfer Protocol*) i FTP (eng. *File Transfer Protocol*) protokolima, ali posjeduje i ograničenu podršku drugih protokola, kao što su TLS (eng. *Transport Layer Security*), SSL (eng. *Secure Socket Layer*), Internet Gopher i HTTPS (eng. *HTTP Secure*) protokoli. Radi se o programskom paketu otvorenog programskog koda distribuiranom pod GPL (eng. *GNU General Public License*) licencom.

SquidGuard programski paket predstavlja dodatak Squid poslužitelju i objedinjuje funkcionalnosti filtriranja, preusmjeravanja i kontrole pristupa web stranicama. Osnovne značajke su mu fleksibilnost, brzina, jednostavnost instalacije, prenosivost i činjenica da se radi o programskom paketu otvorenog programskog koda distribuiranom pod GPLv2 licencom.

2. Filtriranje sadržaja

Filtar sadržaja može biti implementiran kao:

- programski paket koji se izvodi lokalno na osobnom računalu ili
- poslužitelj koji omogućuje pristup Internetu.

Odabir pružatelja Internet usluga (eng. *Internet Service Provider - ISP*) koji provodi filtriranje sadržaja prije njihova prosljeđivanja korisnicima može pomoći roditeljima u zaštiti djece od neprikladnih te potencijalno štetnih i opasnih sadržaja.

Filtriranje sadržaja često se odnosi na stranice koje, prema stajalištu tvrtke, organizacije ili pojedinca koji provodi filtriranje:

- uključuju ilegalne sadržaje,
- promiču, omogućuju ili sadrže rasprave o:
  - napadima na računalne sustave,
  - neovlaštenoj distribuciji vlasničkih programskih paketa (eng. *software piracy*),
  - kriminalnim vještinama ili
  - drugim potencijalno ilegalnim radnjama,
- uključuju seksualno eksplicitne sadržaje kao što su pornografski i erotski sadržaji te neerotske rasprave o seksualnim temama,
- promiču, omogućuju ili sadrže rasprave o životnim stilovima koje se mogu smatrati nemoralnima kao što su promiskuitet, sve seksualne orijentacije osim heteroseksualne, seksualna aktivnost izvan braka te drugi alternativni životni stilovi,
- uključuju sadržaje vezane uz nasilje,
- promiču, omogućuju ili sadrže rasprave o predrasudama i o govoru mržnje,
- promiču, omogućuju ili sadrže rasprave o:
  - kockanju,
  - zloupotrebi droge i alkohola te
  - ostalim aktivnostima koje se smatraju porocima,
- vrlo vjerojatno ne uključuju sadržaje vezane uz školovanje pojedinog učenika, poslovne zadatke određenog zaposlenika ili druge zadatke kojima je računalo, na kojemu se filtriranje provodi, namijenjeno,
- u suprotnosti su s interesima tvrtke, organizacije ili pojedinca koji provodi filtriranje kao što su radničko udruživanje ili kritike određene tvrtke ili industrije,
- promiču ili sadrže rasprave o politici, religiji ili drugim neželjenim temama,
- uključuju mogućnosti socijalnog umrežavanja (eng. *social networking*) putem kojih bi djeca mogla biti izložena napasnicima.

Pored različitih oblika zaštite, filtriranje sadržaja pruža i brojne mogućnosti zlouporabe. Na primjer, filtriranje određenih stajališta i političkih pitanja može predstavljati oblik propagande. Upitna je i opravdanost filtriranja sadržaja na ISP poslužitelju, bilo po snazi zakona ili samovoljom davatelja usluge, ukoliko se korisniku ne ostavi mogućnost njegovog isključivanja za vlastitu vezu. Pojedini kritičari kontrole sadržaja ističu kako ona predstavlja ograničavanje građanskih prava i izravno narušavanje slobode govora.

Iz navedenih razloga organizacije kao što je *Censorware Project* provode analizu (eng. *reverse engineering*) programskih paketa za filtriranje sadržaja i dekriptiranje crnih listi kako bi utvrdili koje web stranice oni blokiraju. Takvim analizama utvrđeno je učestalo blokiranje bezopasnih web stranica uz istovremeno omogućavanje pregledavanja zabranjenih sadržaja. Poznat primjer je blokiranje svih web stranica koje sadrže riječ *breast* (grudi) pod pretpostavkom da se ona koristi samo u seksualnom kontekstu. Ovo je rezultiralo onemogućavanjem pristupa stranicama koje se odnose na rak dojki, žensku odjeću pa čak i web stranice koje sadrže recepte za jela od piletine. Na sličan način pojedini alati, u pokušaju blokiranja stranica koje sadrže riječ *sex*, onemogućuju pristup stranicama s riječima kao što su *Essex* ili *Sussex*.

Pojedine programske pakete za kontrolu prometa moguće je zaobići na različite načine:

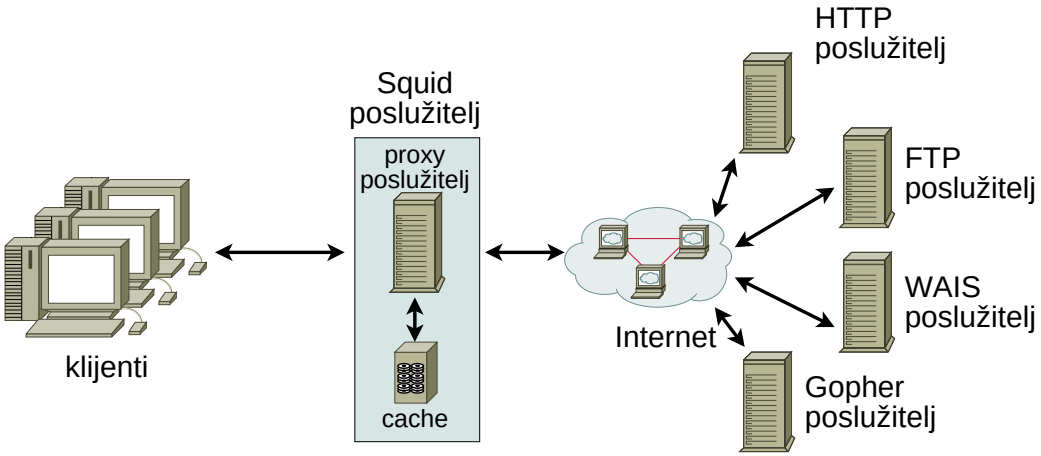
- korištenjem alternativnih protokola kao što su FTP (eng. *File Transfer Protocol*) ili *telnet* (eng. *TELetype NETwork*),

- pretraživanjem na nekom od jezika različitom od jezika za kojega je filtar postavljen,
- korištenjem *proxy* poslužitelja ili
- pomoću posebnih programskih paketa kao što je *Psiphon*.

U nekim slučajevima kopije web stranica (eng. *cached web page*) koje kao rezultat pretrage vraća *Google* ili neki drugi pretraživač mogu zaobići alate za filtriranje sadržaja. Isto je moguće i kada pojedine web stranice prikazuju dijelove drugih web stranica (eng. *web syndication*). Djelovanje lošijih programskih paketa za filtriranje sadržaja web stranica moguće je prekinuti gašenjem odgovarajućih procesa. Kod *Microsoft Windows* operacijskih sustava to je moguće učiniti korištenjem *Task Manager* alata, a kod *Mac OS X* sustava pomoću *Activity Monitor* alata.

3. Squid

Squid djeluje kao posredni poslužitelj koji preuzima zahtjeve od klijenata, na primjer web preglednika, i prosljeđuje ih odgovarajućim Internet poslužiteljima. Kopiju klijentu vraćenih podataka pohranjuje na lokalnom diskovnom prostoru namijenjenom privremenim kopijama (eng. *on-disk cache*). Prednosti Squid paketa do izražaja dolaze kod ponovljenih zahtjeva, zbog toga što se tada klijentu prosljeđuju prethodno pohranjene privremene kopije zatraženih podataka. Tako se ubrzava pristup podacima uz smanjeno opterećenje komunikacijskih kanala.



Slika 1: Princip djelovanja Squid poslužitelja

Brojni Internet vatrozidi također posjeduju posredne poslužitelje. Od njih se Squid se razlikuje po tome što:

- pohranjuje pričuvne kopije,
- podržava brojne protokole dok vatrozidi često imaju posebne poslužitelje namijenjene pojedinim protokolima čime se povećava mogućnost sigurnosnog propusta, te
- omogućuje stvaranje hijerarhija poslužitelja sa složenim međusobnom odnosima.

Kako bi se spriječilo prosljeđivanje zastarjelih podataka klijentima Squid omogućuje postavljanje vremena osvježivanja pričuvnih kopija.

Squid poslužitelj temelji se na HTTP/1.1 specifikaciji i zbog toga može posluživati samo aplikacije koje za pristup Internetu koriste istu specifikaciju, prije svega se to odnosi na web preglednike. Squid nije generički poslužitelj i podržava samo manji podskup Internet protokola među kojima nisu *News*, *RealAudio*, *Video Conferencing* i drugi protokoli. UDP (eng. *User Datagram Protocol*) protokol kod Squid poslužitelja koristi se samo za internu komunikaciju. Zbog toga on ne podržava klijentske aplikacije koje koriste UDP protokol. Program je namijenjen slijedećim operacijskim sustavima:

- AIX (eng. *Advanced Interactive eXecutive*),
- BSDi (eng. *Berkeley Software Design, Inc.*) poznat i pod nazivima BSD/OS i BSD/386,
- Tru64 UNIX prethodno poznat kao Digital Unix,
- FreeBSD,
- HP-UX (eng. *Hewlett Packard UniX*),
- IRIX,

- Linux,
- Mac OS X,
- NetBSD,
- NeXTStep,
- OpenBSD,
- SCO Unix,
- Solaris i
- Windows.

3.1. ICC protokoli

ICC (eng. *Inter-Cache Communication*) protokoli omogućuju umrežavanje spremnika privremenih kopija. Povezivanje više različitih spremnika olakšava pronalaženje pohranjenih sadržaja, a dodatno u slučaju velikih računalnih mreža, omogućuje smanjenje opterećenja poslužitelja dijeljenjem spremnika na odvojene poslužitelje.
Squid podržava sljedeće ICC protokole:

- HTTP – koristi se za dohvaćanje pričuvnih kopija iz drugih spremnika,
- ICP (eng. *Internet Cache Protocol*) – koristi se za utvrđivanje prisutnosti privremene kopije određenog sadržaja u pojedinom spremniku,
- Cache Digest – koristi se za dohvaćanje indeksa privremene kopije pojedinog sadržaja pohranjenog u udaljenom spremniku,
- SNMP (eng. *Simple Network Management Protocol*) – uobičajeni SNMP alati koriste se za dohvaćanje podataka o pojedinom spremniku,
- HTCP (eng. *Hyper Text Caching Protocol*) – predstavlja nasljednika ICP protokola.

3.2. Instalacija

3.2.1. Pripreme

Prije instalacije Squid poslužitelja na Linux/Unix operacijskim sustavima preporuča se prilagoda postavki korisnika pod čijim će se imenom izvoditi Squid pozadinska aplikacija kao i postavki njoj pridijeljene korisničke skupine. Osim toga, potreno je stvoriti odgovarajuću strukturu direktorija. Prema izvornim postavkama spomenutu pozadinsku aplikaciju pokreće *nobody* korisnik s pridijeljenom *nogroup* korisničkom grupom. Kako bi korisnici s tzv. root korisničkim ovlastima, kao i oni koji takve ovlasti nemaju, mogli po potrebi mijenjati postavke Squid poslužitelja preporučeno je stvoriti posebnog korisnika i korisničku grupu, npr. oboje naziva *squid*, i dodatnu administratorsku korisničku grupu, npr. *squidadm*. Ukoliko postoji više administratora potrebno ih je sve učiniti članovima *squidadm* grupe.
Uobičajena direktorijska struktura Squid paketa je:

```
/usr/local/squid/
  /bin/
  /cache/
  /etc/
  /src/squid-version/
```

Gdje je *version* broj koji označuje inačicu Squid poslužitelja, npr. 2.6.
Ako na računalu postoji više diskovnih particija na kojima su pohranjene privremene kopije preporuča se na svakoj stvoriti poddirektorij u *cache* direktoriju. Na primjer, ukoliko postoje dvije takve particije moguće ih postaviti (eng. *mount*) u poddirektorije */usr/local/squid/cache/1/* i */usr/local/squid/cache/2/*.

3.2.2. Preuzimanje

Squid je moguće instalirati na dva načina:

- preuzimanjem izvornog programskog koda kojega je potom potrebno prevesti (eng. *compile*) ili
- preuzimanjem već prevedene binarne inačice i njezinom instalacijom.

Kako bi se izbjeglo preuzimanje binarnih inačica programskog paketa iz nepouzdanih izvora i s ciljem prilagođavanja Squid poslužitelja operacijskom sustavu na koga se instalira, preporuča se preuzimanje izvornog koda s neke od službenih stranica i njegovo prevođenje. Za Linux operacijske sustave izvorni programski kod distribuira se unutar *tar.gz* arhiva, na primjer *squid-version.tar.gz*.
Na raspolaganju su brojne binarne inačice ovog programskog paketa namijenjene različitim operacijskim sustavima. Binarne inačice koje službeno distribuira proizvođač pojedinog operacijskog sustava smatraju se sigurnima i njihova instalacija je relativno jednostavna, a sam postupak ovisi o operacijskom sustavu i inačici poslužitelja. U daljnjem tekstu opisani su postupci raspakiravanja, prevođenja i instalacije inačice Squid programskog paketa namijenjene Linux operacijskim sustavima.

3.2.3. Raspakiravanje

Preuzetu arhivu potrebno je postaviti u prethodno stvoreni */usr/local/squid/src/* direktorij. Pojedine inačice *tar* programskog paketa komprimirane arhive (arhive sa ekstenzijom ".tgz" ili ".tar.gz") mogu raspakirati u jednom koraku, ali ovdje je naveden općenitiji postupak u dva koraka. Naredbom:

```
$ gzip -dv squid-version.tar.gz
```

komprimirana arhiva se dekomprimira u *squid-version.tar* datoteku. Pojedine datoteke izvornog koda se iz dobivene datoteke izdvajaju naredbom:

```
$ tar xvf squid-version.tar
```

Izvršavanjem naredbe datoteke s izvršnim programskim kodom postavljaju se u novostvoreni direktorij, npr. */usr/local/squid/src/squid-2.1.PRE2*. Nakon postavljanja u direktorij moguće je započeti postupak prevođenja.

3.2.4. Prevođenje

Prije samog prevođenja potrebno je prilagoditi njegove postavke stvaranjem *configure* programske skripte naredbom koja može izgledati poput:

```
$ ./configure --enble-err-language=Croatian --prefix=/usr/local
```

Postavke iz ove naredbe dane su kao primjer i ovisno o potrebama mogu izgledati drugačije.
Nakon ovog koraka prevođenje se provodi jednostavnim pokretanjem slijedeće naredbe:

```
$ make
```

Ona stvara binarne datoteke unutar */usr/local/squid/src/squid/* direktorija.

3.2.5. Instalacija

Izvođenje *make* naredbe stvara binarne datoteke, ali ih ne instalira. To se čini naredbom:

```
$ make install
```

koja stvara */usr/local/squid/bin* i */usr/local/squid/etc* direktorije i u njih kopira odgovarajuće binarne datoteke i datoteke s izvornim postavkama poslužitelja. Ako se ovom naredbom provodi nadogradnja ili reinstalacija paketa, binarne datoteke biti će prepisane novima dok će stare datoteke s postavkama ostati sačuvane kako bi ih se moglo usporediti s novostvorenima.

3.3. Kratak opis funkcionalnosti

Nakon uspješne instalacije potrebno je prilagoditi postavke Squid poslužitelja te postavke web preglednika. Datoteke koje sadrže postavke poslužitelja nalaze se unutar */usr/local/squid/etc* direktorija. Iako se ovdje nalazi više datoteka, većini administratora dovoljna će biti prilagodba postavki unutar *squid.conf* datoteke. Između svih postavki koje se u njoj nude, važno je prilagoditi slijedeće:

- **http_port** –određuje portove na kojima Squid očekuje zahtjeve. Portove ispod 1024 može koristiti samo administrator, a koriste ih i programski paketi koji pružaju osnovne Internet usluge, kao što su SMTP, POP, DNS i HTTP. Većina web poslužitelja očekuje zahtjeve na portu 80 i ako se on postavi kao Squid HTTP port, ovaj će programski paket morati pokretati tzv. *root* korisnik. Zbog toga se često koristi lako pamtljivi port 8080.
- **cache_dir** –određuje direktorij za pohranu privremenih kopija, njegovu najveću moguću veličinu, kao i način organiziranja pohranjenih podataka.
- **cache_mgr** –određuje adresu elektroničke pošte na koju Squid poslužitelj šalje obavijest u slučaju poteškoća u radu. Ista adresa ispisuje se na stranicama s obavijestima o pogrešci kojima se korisnike izvješćuje o nedostupnosti zatražene web stranice.
- **cache_effective_user** i **cache_effective_group** – ako je Squid postavljen tako da zahtjeve očekuje na „niskim" portovima (portovima ispod 1024) potrebno ga je pokrenuti s *root* korisničkim ovlastima. Budući da izvođenje paketa s povišenim korisničkim ovlastima nije preporučeno, Squid nakon inicijalizacije mijenja korisnika i grupu prema informacijama zapisanim u ovim postavkama.
- **ftp_user** – FTP protokol građen je za autoriziranu razmjenu podataka tako da zahtijeva korisničko ime i zaporku. Za javni pristup koristi se *anonymus* korisničko ime, a zaporka je najčešće adresa elektroničke pošte korisnika. Većina web preglednika kao zaporku automatski upisuje nevažeću adresu. Ponekad je korisno, a kod nekih FTP poslužitelja i nužno, koristiti važeću adresu pa ju je ovdje moguće definirati.

3.3.1. Liste kontrole pristupa

Squid poslužitelj nije preporučeno koristiti bez barem minimalne kontrole pristupa jer neovlašteni korisnici preusmjeravanjem prometa preko nezaštićenog poslužitelja mogu provoditi nezakonite aktivnosti ili ubrzavati svoj pristup Internetu.
Kontrola pristupa provodi se pojedinačno po protokolima. Primjerice ako Squid primi HTTP zahtjev provjerava se lista kontrole pristupa za HTTP protokol, a ako je zaprimljen ICP zahtjev provjerava se odgovarajuća ICP ACL (eng. *Access Control List*) lista. Jednostavnu definiciju kontrole pristupa na temelju IP (eng. *Internet Protocol*) adresa moguće je provesti odgovarajućim unosima u *squid.conf* datoteku. Na primjer, za omogućavanje pristupa pohranjenim privremenim kopijama s određenih IP adresa korištenjem HTTP i ICP protokola u spomenutoj datoteci potrebno je izmijeniti unose poput:

```
acl localnet src 192.168.1.0/255.255.255.0
..
http_access allow localnet
icp_access allow localnet
```

Squid poslužitelj nakon primitka zahtjeva započinje s pregledom ACL pravila vezanih uz protokol na kojega se zahtjev odnosi. Pravila se provjeravaju redom kojim su navedena, odozgo prema dolje. Prvo pravilo koje odgovara danom zahtjevu uzrokuje prekid pretraživanja. Ako niti jedno pravilo ne odgovara zahtjevu, primjenjuje se posljednje pravilo na ACL listi odgovarajućeg protokola. Zbog toga je poželjno ACL listu zaključiti pravilom koje obuhvaća sve moguće zahtjeve.
Opisana pravila su zbog svoje jednostavnosti prikladna za kontrolu pristupa unutar manjih organizacija. Kod većih organizacija praktičnije je definirati klase korisnika te zatim takvim klasama dozvoliti ili onemogućiti pristup pojedinim resursima.

3.3.2. Komunikacija s drugim poslužiteljima

Squid poslužitelj podržava koncept hijerarhije posrednih poslužitelja. Uobičajeni postupak poslužitelja, kada među pohranjenim privremenim kopijama nema zatraženu web stranicu, je njeno dohvaćanje s izvornog web poslužitelja. Ako su poslužitelji privremenih kopija hijerarhijski organizirani moguća je razmjena privremenih kopija među njima.
Poslužitelji su unutar hijerarhije podijeljeni na:

- ravnopravne (eng. *sibling*) poslužitelje – odgovaraju na zahtjeve drugih poslužitelja samo ako u spremniku posjeduju privremenu kopiju zatražene web stranice i
- nadređene (eng. *parent*) poslužitelje – u slučaju primitka zahtjeva za web stranicom koje nema u spremniku oni stranicu dohvaćaju s izvornog web poslužitelja.

Squid ne šalje zahtjeve ostalim poslužiteljima pojedinačno, već se svi ICP paketi šalju istovremeno. Klijentov zahtjev tada se stavlja na čekanje do primitka prvog pozitivnog odgovora od jednog od prozvanih poslužitelja te s njega dohvaća zatražena web stranica, neovisno o tome radi li se o ravnopravnom ili nadređenom poslužitelju.
Squid se s ostalim poslužiteljima povezuje odgovarajućim unosima u *squid.conf* datoteci. Na primjer, za povezivanje s *cache.myparent.example* nadređenim i *cache.sibling.example* poslužiteljima potrebno je u datoteku unijeti slijedeće:

```
cache_peer cache.myparent.example parent 3128 3130
cache_peer cache.sibling.example sibling 8080 3130
```

U navedenom primjeru Squid s nadređenim poslužiteljem komunicira na HTTP portu 3128 i ICP portu 3130, a s ravnopravnim poslužiteljem na HTTP portu 8080 i istom ICP portu.

3.3.3. Squid kao web poslužitelj

Pojedini poslužitelji privremenih kopija mogu djelovati kao web poslužitelji (i obrnuto) što znači da prihvaćaju web zahtjeve, koji sadrže ime datoteke i put do nje, kao i zahtjeve oblikovane za posredne poslužitelje (eng. *proxy-specific*), koji sadrže URL (eng. *Uniform Resource Locator*) oznaku. Squid poslužitelj nije tako oblikovan kako bi se pojednostavio izvoran programski kod i time poslužitelj učinilo stabilnijim. Squid je dakle poslužitelj privremenih kopija web stranica i ne može djelovati kao web poslužitelj.
Ipak, zahvaljujući sloju prevođenja, Squid može prihvaćati i posluživati web zahtjeve. Spomenuti sloj prilagođava pristigle web zahtjeve mijenjajući oznake odredišnog poslužitelja i porta. Squid s tako prevedenim zahtjevima rukuje kao s normalnim zahtjevima: zatraženi podaci dohvaćaju se s udaljenog poslužitelja, prosljeđuju klijentu i pohranjuju za eventualnu kasniju uporabu.
Ovu funkcionalnost preporučeno je koristiti za:

- ubrzavanje sporijeg poslužitelja – ako se Squid nalazi ispred sporijeg web poslužitelja može ubrzati posluživanje klijenata pohranjivanjem privremenih kopija,
- postavljanje poslužitelja koji objedinjuje funkcije web poslužitelja i poslužitelja privremenih kopija,
- transparentno posluživanje (eng. *transparent caching/proxy*) i
- osiguranje web poslužitelja – postavljanjem Squid poslužitelja između Interneta i nesigurnog web poslužitelja moguće je spriječiti posluživanje neželjenih klijenata i onemogućiti iskorištavanja sigurnosnih propusta.

4. SquidGuard

SquidGuard je dodatak Squid poslužitelju koji, među ostalim, može biti korišten za:

- ograničavanje ili onemogućavanje pristupa određenim web poslužiteljima i/ili URL adresama pojedinim korisnicima,
- onemogućavanje pristupa URL adresama koje odgovaraju određenim predlošcima ili sadrže određene riječi,
- zabranu korištenja IP adresa u URL oznakama,

- preusmjeravanje onemogućenih URL zahtjeva na stranice temeljene na CGI (eng. *Common Gateway Interface*) sučelju,
- preusmjeravanje neregistriranih korisnika na formular za registraciju,
- preusmjeravanje zahtjeva za dohvaćanjem popularnih datoteka na lokalne kopije,
- postavljanje različitih pravila pristupa ovisno o dobu dana, danu u tjednu itd.,
- postavljanje različitih pravila za različite skupine korisnika …

SquidGuard, kao ni Squid, ne može:

- filtrirati, cenzurirati ili mijenjati tekst unutar dokumenata,
- filtrirati, cenzurirati ili mijenjati programski kod pisan skriptnim programskim jezicima (npr. JavaScript ili VBscript), a koji je ugrađen u HTML programski kod.

4.1. Filtriranje prometa

Filtriranje prometa pomoću SquidGuard programskog paketa moguće je zadati prema različitim kriterijima:

1. **Vremenski intervali** se mogu sastojati od bilo koje kombinacije:
   - vremena u danu, npr. *00:00–08:00*, *17:00–24:00*,
   - dana u tjednu, npr. *sa* za subotu,
   - datuma, npr. *2007-07-07*,
   - raspona datuma, npr. *2007-01-01-2007-07-07* i
   - datumskih višeznačnika (eng. *wildcard*), npr. **-01-01*.
2. **Grupiranje klijenata** u kategorije kao što su *menadžeri*, *zaposlenici*, *profesori*, *učenici*, *kupci*, *gosti* itd. na temelju:
   - raspona IP adresa označenih:
     - prefiksima, npr. *172.16.0.0/12*,
     - oznakom podmreže (eng. *netmask*), npr. *172.160.0.0/255.240.0.0*,
     - prvom i zadnjom IP adresom u nizu, npr. *172.160.0.11-172.160.0.35*,
   - liste IP adresa,
   - liste domena,
   - liste korisničkih identifikacijskih oznaka,

   Moguće je povezivanje pojedine grupe s vremenskim intervalom:
   - pozitivno, npr. unutar radnog vremena ili
   - negativno, npr. izvan radnog vremena.
3. **Grupiranje odredišta** (poslužitelja ili URL adresa) na temelju:
   - domena, uključujući poddomene, npr. *foo.bar.com*,
   - poslužitelja, npr. *host. foo.bar.com*,
   - URL adresa koje sadrže direktorije, uključujući poddirektorije, npr. *foo.bar.com/some/dir*,
   - URL adresa datoteka, npr. *foo.bar.com/somedirs/file.html*,
   - predložaka (eng. *regular expression*), npr. *(expr1|expr2|expr3…)*,

   Moguće je povezivanje pojedine grupe s vremenskim intervalom, jednako kao kod grupa klijenata.
4. **Prepisivanje/preusmjeravanje URL oznaka:**
   - izmjenom znakovnih nizova,
   - zamjenom URL adresa, koja može biti korisniku vidljiva ili od njega skrivena.
5. **Liste kontrole pristupa** koje omogućuju
   - pridjeljivanje:
     - lista prihvatljivih i nedopuštenih odredišta te liste zabranjenih URL adresa i
     - skupova pravila preusmjeravanja za pojedine klijente,
   - pozitivno i negativno povezivanje ACL liste s vremenskim intervalom,
   - definiranje izvornih (eng. *fallback/default*) pravila
6. **Selektivno stvaranje dnevničkih zapisa**
   - dnevnički zapisi vezani uz grupu klijenata,
   - dnevnički zapisi vezani uz grupu odredišta,

- dnevnički zapisi vezani uz skup pravila.

4.2. Crne liste

Crne liste (eng. *blacklist*) predstavljaju liste domena te IP i URL adresa odredišta s nepoželjnim sadržajem. Korisnici SquidGuard paketa mogu kreirati vlastite crne liste ili preuzeti gotove lista te ih eventualno prilagoditi vlastitim potrebama. Dostupna su tri besplatna paketa crnih listi:

- MESD blacklists,
- Shalla's Blacklists te
- Université Toulouse blacklist collection,

kao i jedan komercijalan paket naziva URLBlacklist.com.
Crne liste su unutar navedenih paketa podijeljene u skupine prema sadržajima na koje se odnose. Tako su liste unutar MESD paketa podijeljene na sljedeće kategorije:

- *ads* – reklamni sadržaji,
- *aggressive* – sadržaji koji promiču mržnju,
- *audio-video* – zvučni i vizualni sadržaji,
- *drugs* – sadržaji vezani uz zloupotrebu droga,
- *gambling* – sadržaji vezani uz igre na sreću,
- *hacking* – sadržaji vezani uz računalni kriminal,
- *mail* – webmail poslužitelji,
- *porn* – pornografski sadržaji,
- *proxy* – posredni poslužitelji,
- *redirector* – preusmjeravanje URL zahtjeva,
- *spyware* – sadržaji vezani uz neovlašteno prikupljanje podataka o korisnicima,
- *suspect* – sumnjiva odredišta za koja nije sigurno utvrđeno da pripadaju nekoj od ostalih kategorija,
- *violence* – nasilni sadržaji, te
- *warez* – sadržaji vezani uz ilegalnu distribuciju komercijalnih programskih paketa.

Unutar svake kategorije definira se lista zabranjenih domena te lista zabranjenih URL adresa.
Primjer sadržaja crne liste iz *warez* kategorije:

```
209.196.24.84
207.192.95.95
crack.am
bittorent.biz
2bcalvi.com
crazyhack.abclan.com
astalavista.com
```

Odgovarajuće crne liste, bile one preuzete ili novostvorene, potrebno je postaviti u direktorij određen postavkama SquidGuard paketa (izvorno je to */usr/local/squidGuard/db* direktorij) i inicijalizirati ih. Postupci postavljanja i inicijalizacije crnih listi opisani su u nastavku teksta.

4.3. Instalacija

Postupak instalacije započinje raspakiravanjem izvornog programskog koda:

```
$ tar xvzf squidGuard-1.2.1.tar.gr
```

nakon čega je potrebno ući u novostvoreni *squidGuard-1.2.1* direktorij, prilagoditi postavke prevođenja i provesti samo prevođenje izvornog programskog koda:

```
$ cd squidGuard-1.2.1
$ ./configure
$ make
```

Gornjim nizom naredbi stvorene su binarne datoteke koje je potom potrebno instalirati naredbom:

```
$ make install
```

Nakon instalacije SquidGuard programskog paketa potrebno je instalirati crne liste. Postupak se sastoji od njihova kopiranja u željeni direktorij (izvorno je to */usr/local/squidGuard/db* direktorij), raspakiravanja i izdvajanja iz *.tar* datoteke.

```
$ cp /put/do/crneliste.tar.gz /usr/local/squidGuard/db
$ cd /usr/local/squidGuard/db
$ gzip -d crneliste.tar.gz
$ tar xfv crneliste.tar
```

4.4. Izmjena postavki filtriranja

4.4.1. Osnovno filtriranje

Filtriranje se zadaje unosima u *squidGuard.conf* konfiguracijskoj datoteci koja se nalazi u direktoriju u kojemu je paket instaliran, npr. */usr/local/squidGuard*. Slijedi primjer jednostavne konfiguracijske datoteke:

```
dbhome /usr/local/squidGuard/db
logdir /usr/local/squidGuard/logs

dest porn {
       domainlist porn/domains
       urllist porn/urls
}

acl {
       default {
              pass !porn all
              redirect http://localhost/block.html
       }
}
```

Navedeni unosi označuju:

- **dbhome** – direktorij u kojem se nalaze crne liste,
- **logdir** – direktorij u kojega se pohranjuju dnevnički zapisi,
- **dest** – odredišta koja je potrebno onemogućiti,
- **acl** – pravila blokiranja. U primjeru se skupina odredišta definirana *dest* naredbom onemogućuje *pass !porn all* naredbom, te se svi onemogućeni zahtjevi preusmjeravaju na *http://localhost/block.html*.

Moguće je definirati i onemogućiti više skupina odredišta:

```
dest adv {
       domainlist adv/domains
       urllist adv/urls
}

dest porn {
       domainlist porn/domains
       urllist porn/urls
}

dest warez {
       domainlist warez/domains
```

```
        urllist warez/urls
}

acl {
        default {
                pass !adv !porn !warez all
                redirect http://localhost/block.html
        }
}
```

Ponekad je potrebno privremeno omogućiti pojedina odredišta koja se nalaze u crnim listama. Ovaj se postupak naziva postavljanjem odredišta na bijelu listu (eng. *whitelisting*), na primjer:

```
dest white {
        domainlist white/domains
        urllist white/urls
}

acl {
        default {
                pass white !adv !porn !warez all
                redirect http://localhost/block.html
        }
}
```

Ovdje je pretpostavljeno da se liste odredišta koje je potrebno omogućiti nalaze u /white direktoriju unutar direktorija s crnim listama određenog *dbhome* izrazom, npr. */usr/local/squidGuard/db/white*, te da su u datoteci s postavkama prethodno definirane *adv*, *porn* i *warez* skupine odredišta. Skupinu odredišta koju se omogućuje potrebno je postaviti na prvo mjesto iza *pass* naredbe, bez uskličnika.

4.4.2. Napredno filtriranje

Zaobilaženje URL filtra unošenjem IP adrese umjesto punog imena domene moguće je spriječiti *!in-addr* oznakom kod *acl* pravila filtriranja unutar *squidGuard.conf* datoteke.

```
acl {
        default {
                pass !in-addr all
                redirect http://localhost/block.html
        }
}
```

Dva su načina postavljanja vremenski ovisnog filtriranja prometa. Oznakom *weekly* podešavaju se ponavljajuća vremenska razdoblja, dok se oznakom *date* postavlja filtriranje za pojedine datume. Dozvoljena je upotreba vremenskih višeznačnika.

```
time afterwork {
        weekly   * 17:00-24:00        # nakon radnog vremena
        weekly   fridays 16:00-17:00  # petkom kraće radno vrijeme
        weekly   saturdays sundays    # vikend
        date     *.01.01              # Nova godina
        date     *.12.24 12:00-24:00  # Badnjak
        date     *.01.01              # Nova godina
        date     2007.04.08           # Uskrs 2007. godine
}
```

Navedene vremenske oznake se kod *acl* pravila filtriranja koriste uz *within* i *outside* naredbe.

```
acl {
```

```
        all within afterwork {
                pass all
        }
        else {
                pass !adv !porn !warez all
        }
        default {
                pass none
                redirect http://localhost/block.html
        }
}
```

Kod prikazanog primjera svim korisnicima dopušten je slobodan pristup svim web stranicama nakon radnog vremena, dok je tijekom radnog vremena onemogućen pristup *adv*, *porn* i *warez* skupinama odredišta.
Različite razine dozvola pristupa web stranicama s pojedinih računala moguće je postaviti navođenjem njihovih IP adresa. Raspone IP adresa moguće je definirati početnom i krajnjim adresom, oznakom podmreže ili prefiksom.

```
src admins {
        ip 192.168.2.0-192.168.2.255
        ip 172.16.12.0/255.255.255.0
        ip 10.5.3.1/28
        }
}
```

Listu IP adresa moguće je postaviti u zasebnu datoteku unutar direktorija zadanog *dbhome* naredbom. Takva lista unutar *squidGuard.conf* datoteke inicijalizira se *iplist* naredbom iza koje slijedi naziv datoteke.

```
src admins {
        iplist adminlist
        }
}
```

Ako se datoteku koja sadrži listu IP adresa želi postaviti izvan *dbhome* direktorija u *squidGuard.conf* datoteci potrebno je navesti njezin položaj. Sadržaj ove datoteke potrebno je oblikovati kao:

```
192.168.2.0-192.168.2.255
172.16.12.0/255.255.255.0
10.5.3.1/28
```

SquidGuard omogućuje zapisivanje onemogućenih pokušaja pristupa zabranjenim odredištima unutar dnevničkih datoteka. Ova mogućnost definira se *log* naredbom unutar definicije skupina korisnika ili skupina odredišta. Uz navedenu naredbu potrebno je odrediti ime dnevničke datoteke. Ako uz ime datoteke nije naveden njezin položaj SquidGuard ju stvara unutar direktorija zadanog *logdir* naredbom.

```
dest porn {
        domainlist porn/domains
        urllist porn/urls
        log pornaccesses
}
```

4.4.3. Inicijalizacija crnih listi

Prije pokretanja SquidGuard programskog paketa potrebno je inicijalizirani crne liste, odnosno pretvoriti tekstualne datoteke u *.db* format čime se ubrzava njihovo pretraživanje. Inicijalizacija se provodi naredbama:

```
$ squidGuard -C all
$ chown -R <squiduser> /usr/local/squidGuard/db/*
```

Druga naredba, promjenom vlasnika *.db* datoteka, osigurava Squid paketu pristup crnim listama. Trajanje opisanog postupka varira ovisno o veličini crnih lista i brzini računala. Ako je uspješno proveden u */domains* i */urls* direktorijima stvorene su nove datoteke s nastavkom *.db*.

5. Prednosti i nedostaci implementiranog rješenja

Squid i SquidGuard su besplatni programski paketi izvrsnih performansi koje im pružaju veliku prednost. U usporedbi s komercijalnim filtrima sadržaja, filtri otvorenog programskog koda zahtijevaju znatno višu razinu znanja i angažmana tijekom instalacije, prilagodbe i nadogradnje.

5.1. Usporedba sa Squid filtriranjem

U usporedbi s ostalim varijantama filtriranja sadržaja temeljenim na programskim paketima otvorenog programskog koda implementirano rješenje ima svojih prednosti, ali i nedostataka. Na primjer, sam Squid programski paket omogućuje filtriranje sadržaja web stranica, a prednosti i nedostaci ovakvog rješenja u usporedbi sa SquidGuard paketom dani su u tablici *Tablica 1*.

<table>
<tr><th></th><th>Squid</th><th>SquidGuard (+ Squid)</th></tr>
<tr><td rowspan="3">PREDNOSTI</td><td>jednostavna instalacija i konfiguracija</td><td>velika fleksibilnost – moguće je kategorizirati domene i URL adrese</td></tr>
<tr><td>brz – ne zahtjeva druge aplikacije</td><td rowspan="2">jednostavno održavanje – moguće je zadati proizvoljno mnogo listi kontrole pristupa</td></tr>
<tr><td>jednostavno otkrivanje pogrešaka</td></tr>
<tr><td rowspan="3">NEDOSTACI</td><td>nefleksibilan – nije moguće kategorizirati odredišta</td><td>složenija instalacija i konfiguracija</td></tr>
<tr><td rowspan="2">složeno zadavanje višestrukih ACL listi</td><td>sporiji – poziva se iz Squid paketa</td></tr>
<tr><td>otežano pronalaženje pogrešaka</td></tr>
</table>

Tablica 1: Usporedba filtriranja pomoću Squid i SquidGuard programskih paketa

5.2. Usporedba s Squirm dodatkom Squid paketu

Squirm je dodatak Squid programskom paketu koji onemogućavanje pristupa pojedinim odredištima provodi preusmjeravanjem URL zahtjeva. U usporedbi sa SquidGuard paketom Squirm je znatno sporiji: za filtriranje dvije tisuće URL adresa uz crnu listu s jedanaest tisuća unosa na Pentium 233 računalu potrebne su mu dvije minute i dvadesetpet sekundi, dok je SquidGuard filtru potrebno samo devet sekundi. Za isti zadatak s crnom listom veličine sto adresa SquidGuard paketu potrebno je šest sekundi iz čega proizlazi kako kod filtriranja tim paketom malu ulogu ima veličina i broj korištenih crnih listi.

5.3. Usporedba s DansGuardian dodatkom Squid paketu

DansGuardian također je dodatak Squid programskom paketu namijenjen filtriranju sadržaja web stranica na temelju ključnih riječi. Ovakvo filtriranje je sveobuhvatno, ali povećava mogućnost blokiranja web stranica koje ne uključuju zabranjene sadržaje.
SquidGuard, s druge strane, filtriranje provodi na temelju domena i URL oznaka odredišta pa omogućuje preciznu kontrolu nad web stranicama kojima se pristup onemogućuje, a bez zahtjevne

obrade njihovog sadržaja. Nedostatak ovog pristupa posljedica je svakodnevnog nastajanja velikog broja novih web stranica zbog kojih je neprekidno potrebno osvježavati crne liste.

6. Zaključak

Squid posredni poslužitelj preuzima zahtjeve od klijenata i prosljeđuje ih odgovarajućim Internet poslužiteljima. Kopiju klijentu vraćenih podataka pohranjuje kako bi ih proslijedio u slučaju ponovljenih zahtjeva. Omogućuje kontrolu pristupa, korištenjem odgovarajućih ACL listi za svaki podržani komunikacijski protokol, te umrežavanje s drugim posrednim poslužiteljima i razmjenu privremenih kopija među njima. Zahvaljujući sloju prevođenja zahtjeva Squid može djelovati i kao web poslužitelj koji objedinjuje funkcije web poslužitelja i poslužitelja privremenih kopija, te nudi mogućnosti osiguranja i ubrzavanja postupka posluživanja.

SquidGuard, dodatak Squid poslužitelju, koristi se za ograničavanje ili onemogućavanje pristupa određenim web poslužiteljima i/ili URL adresama, onemogućavanje pristupa URL adresama koje odgovaraju određenim predlošcima ili sadrže određene riječi, zabranu korištenja IP adresa u URL oznakama, preusmjeravanje onemogućenih zahtjeva, preusmjeravanje zahtjeva za dohvaćanjem popularnih datoteka na lokalne kopije, zadavanje različitih pravila pristupa ovisno o dobu dana, danu u tjednu ili datumu te različitih pravila za različite skupine korisnika.

Filtriranje sadržaja web stranica korištenjem Squid poslužitelja brže je od filtiriranja sa SquidGuard filtrom, ali je manje prilagodljivo i složenije u slučaju korištenja višestrukih ACL listi. U usporedbi s drugim dodacima Squid poslužitelju koji su namijenjeni kontroli sadržaja, SquidGuard je brži, robusniji te omogućuje veću kontrolu nad onemogućenim sadržajima.

7. Reference

[1] Content-control software, http://en.wikipedia.org/wiki/Content-control_software, svibanj 2007.
[2] Squid: Optimising Web Delivery, http://www.squid-cache.org/, svibanj 2007.
[3] Oskar Pearson: The Squid Guide, http://www.deckle.co.za/squid-users-guide/Main_Page, svibanj 2007.
[4] SquidGuard, http://www.squidguard.org/, svibanj 2007.
[5] SquidGuard, http://cri.univ-tlse1.fr/documentations/cache/squidguard_en.html, svibanj 2007.