HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Razdvojeni DNS sustavi

CCERT-PUBDOC-2006-02-149

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

DNS (eng. *Domain Name System*) servis služi za prevođenje simboličkih imena računala u njihove IP adrese i obratno. Upotreba klasičnog DNS sustava podrazumijeva pohranu DNS informacija o vanjskoj i unutarnjoj domeni na istom poslužitelju koji je javno dostupan. Na ovaj način zlonamjernim korisnicima se olakšava pristup povjerljivim informacijama o unutarnjoj domeni. Upotrebom razdvojenog DNS sustava podaci o vanjskoj i unutarnjoj domeni su razdvojeni i nalaze se na različitim poslužiteljima smještenim u različitim sigurnosnim zonama. Podaci o javnoj domeni su javno dostupni svima, dok su podaci o unutarnjoj domeni pohranjeni na unutarnjem DNS poslužitelju i dostupni su isključivo korisnicima s unutarnje mreže. Na takav način otežan je pristup zlonamjernim korisnicima i podignut stupanj sigurnosti računalne mreže.

U radnim okolinama koje zahtijevaju veću razinu sigurnosti od one koju pruža klasični DNS sustav, potrebno je implementirati više DNS poslužitelja od kojih su neki javno vidljivi, dok drugi nisu. Mreže kod kojih se preporuča uporaba razdvojenog DNS sustava su one koje koriste različita domenska imena na unutarnjoj od onih na vanjskoj mreži (Internet) ili one koje posjeduju resurse u unutarnjoj mreži, a koji bi trebali biti dostupni i na vanjskoj mreži. Uobičajeni razlog postavljanja razdvojene DNS arhitekture je zaštita unutarnjih DNS informacija od vanjskih Internet korisnika.

Dokument opisuje razdvojeni DNS sustav, navodi glavne prednosti i nedostatke te daje primjer podešavanja razdvojenog DNS sustava.

2. DNS servis

Domain Name System (DNS) originalno je definiran RFC 882 [1] i RFC 883 dokumentima [2], koji su kasnije dopunjeni i objavljeni u dokumentima RFC 1034 [3] i RFC 1035 [4]. Osim tih dokumenata koji definiraju osnovnu funkcionalnost DNS servisa, postoje i drugi dokumenti koji dopunjavaju osnovnu definiciju DNS sustava.

DNS servis služi za prevođenje simboličkih imena računala u njihove IP adrese i obratno. DNS predstavlja set protokola i servisa na TCP/IP mreži koji omogućavaju korištenje hijerarhijski postavljenih simboličkih imena računala umjesto njihovih stvarnih IP adresa. Korištenjem DNS sustava svakom računalu dodijeljeno je jedinstveno FQDN (eng. *Fully Qualified Domain Name*) ime. DNS radi na 7 nivou OSI modela i može koristiti UDP i TCP protokole (standardni portovi: UDP 53 ili TCP 53). Sustav se sastoji od distribuirane baze podataka s imenima računala. Bez ovog servisa komunikacija među poslužiteljima bila bi moguća samo unošenjem njihovih IP adresa.

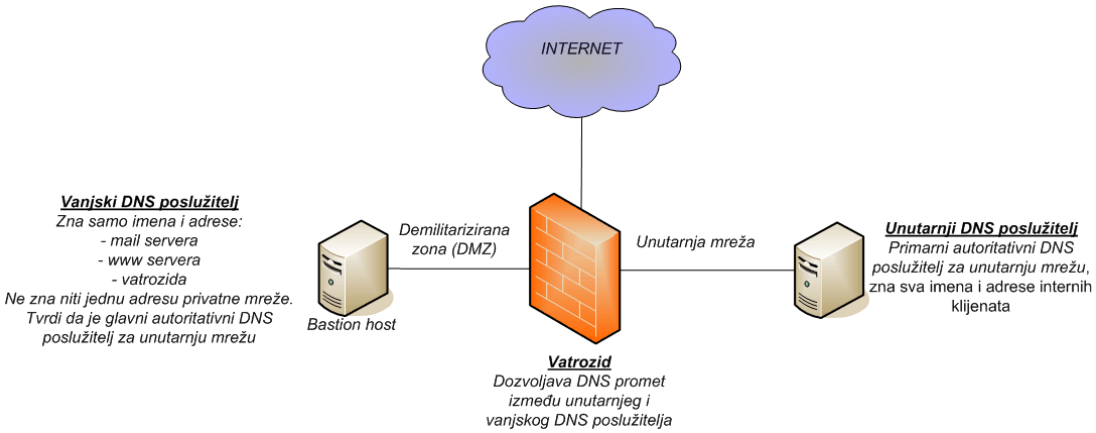
DNS se sastoji od tri osnovna elementa:

- prostora imena (eng. *name space*) koji je hijerarhijski organiziran u stablastu strukturu i u kojoj svaka grana predstavlja domenu te sadrži informacije o njoj,
- poslužitelja (eng. *name servers*) koji sadrže informacije o strukturi pojedinih domena te autoritativne informacije o pojedinim dijelovima domena,
- klijenata (eng. *resolvers*) koji generiraju DNS upite te ih šalju poslužiteljima da bi nazad dobili odgovarajuće informacije.

DNS poslužitelji dijele se u dvije kategorije: primarni i sekundarni. U normalnim uvjetima rada sve upite prima primarni DNS poslužitelj. Uloga sekundarnih DNS poslužitelja je u primanju podataka s primarnih DNS poslužitelja i njihovom privremenom spremanju (eng. *cache*). U slučaju da primarni DNS poslužitelj ne radi, umjesto njega na upite odgovara sekundarni DNS poslužitelj.

3. Razdvojeni DNS sustav

Korištenje klasičnog DNS sustava podrazumijeva pohranu DNS informacija o vanjskoj i unutarnjoj domeni na istom poslužitelju koji je javno dostupan. Zlonamjernim korisnicima na ovaj se način omogućava da na relativno jednostavan način dođu do povjerljivih informacija o unutarnjoj domeni. Za sustave gdje se traži siguran ustroj DNS servisa uobičajeno je kombiniranje nekoliko DNS poslužitelja od kojih su neki javno vidljivi, dok drugi nisu. Najčešće korištena konfiguracija je ona kod koje skriveni DNS poslužitelji interno isporučuju unutarnjim korisnicima DNS informacije koje nisu vidljive na javnoj (vanjskoj) mreži. Vanjskim klijentima daje se dio informacija za koje se smatra da su im potrebne, a unutarnjim se daje drugi dio informacija za koje se smatra da su im dovoljne. Time se eliminira sigurnosni problem da "svi vide sve". Ovaj princip, uspostavljanje različitih pogleda ili “vidljivosti“ DNS imeničkog prostora na unutarnje i vanjske DNS poslužitelje, još se naziva sustavom razdvojenih poslužitelja (eng. *split name server*), odnosno razdvojeni DNS (eng. *split DNS*). Na slici *Slika 1* prikazana je logička shema razdvojenog DNS-a.



Slika 1: Logička shema razdvojenog DNS-a

3.1. Razlozi korištenja razdvojenog DNS sustava

Postoji nekoliko razloga zbog kojih se koriste DNS poslužitelji u konfiguraciji razdvojenog DNS sustava, i to kada se:

- koriste domenska imena na unutarnjoj mreži koja su različita od onih na vanjskoj mreži,
- želi sakriti interne DNS informacije od vanjskih Internet klijenata,
- omogućava unutarnjoj mreži, koja je obično iza različitih filtara i unutar raspona privatnih IP adresa definiranih dokumentom RFC 1918 [5], postavljanje DNS upita prema vanjskoj mreži (Internetu),
- dozvoljava ulazak elektroničke pošte poslane iz vanjske mreže u unutarnju mrežu.

3.2. Opis razdvojenog DNS sustava

Razdvojeni DNS se realizira kombiniranjem minimalno dva DNS poslužitelja, koji trebaju biti smješteni u različitim sigurnosnim zonama. Ti poslužitelji razdvajaju se korištenjem vatrozida. Poslužitelji koji su namijenjeni korisnicima iz unutarnje mreže zovu se u unutarnji (interni) DNS poslužitelji, a oni koji su uobičajeno namijenjeni vanjskim Internet korisnicima zovu se vanjski (eksterni) DNS poslužitelji. Razdvojeni DNS dostavlja na isti upit različite odgovore, ovisno o IP adresi s koje je DNS upit poslan. Obično se koristi u velikim poslovnim okolinama gdje je potrebno davati različite odgovore postavljene s različitih strana vatrozida.

3.2.1. Unutarnji DNS poslužitelj

Unutarnji DNS poslužitelj sadrži distribuiranu bazu podataka svih DNS imena računala unutar unutarnje mreže. Korist se za prevođenje simboličkih imena računala u njihove stvarne IP adrese i obratno, pri čemu odgovara samo na upite unutarnjih klijenata, a upite za eksternim podacima prosljeđuje prema vanjskom DNS poslužitelju.
S unutarnjeg DNS poslužitelja nema grupnog prijenosa DNS informacija (eng. *zone transfer*), osim ako ne postoji više unutarnjih DNS poslužitelja.

3.2.2. Vanjski DNS poslužitelj

Vanjski DNS poslužitelj služi za prevođenje simboličkih imena računala u njihove stvarne IP adrese i obratno za vanjske Internet klijente. Izvršava samo rekurzivne upite za unutarnje klijente (obično za unutarnji DNS poslužitelj). Kod vanjskih DNS poslužitelja je dopušten grupni prijenos DNS informacija, ali samo do sekundarnih DNS poslužitelja. Vanjski DNS poslužitelj preslikava isključivo imena s vanjske mreže (mail, web poslužitelji, ftp…).

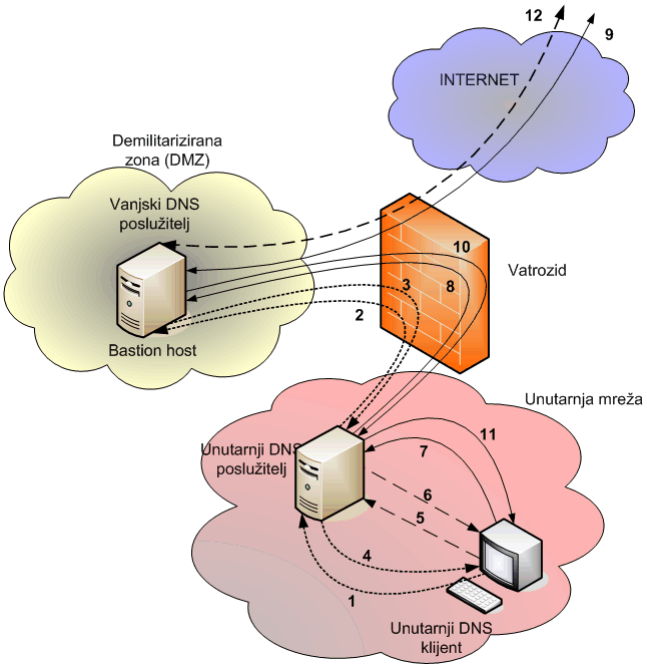
3.3. Prednosti i nedostaci razdvojenog DNS sustava

Osnovna prednost razdvojenog DNS sustava je da grupni prijenos DNS informacija nije dopušten između unutarnjeg i vanjskog DNS poslužitelja. Takva konfiguracija dopušta unutarnjem DNS poslužitelju da zaštiti informacije o imenima i adresama unutarnjih klijenata od vanjskih klijenata (Interneta) te se time podiže razina sigurnosti računalne mreže.
Međutim, upitno je koliko se korištenjem razdvojenih DNS sustava stvarno podiže razina sigurnosti. Naime, unutarnje DNS informacije mogu "curiti" na mnogo različitih načina, npr. kroz mail zaglavlja (eng. *mail headers*) te snalažljivi napadači mogu na druge načine doći do unutarnjih DNS podataka koji su im potrebni za njihove neovlaštene aktivnosti.

4. Primjer podešavanja razdvojenog DNS sustava

U ovom poglavlju dani su primjeri podešavanja razdvojenog DNS sustava. Pri tome je uzeta jedna izmišljena organizacija koja je nazvana "Kompanija d.d." (`kompanija.hr`), koja ima nekoliko lokacija sa zajedničkom unutarnjom mrežom baziranom na privatnim IP adresama i vanjsku demilitariziranu zonu (DMZ), tj. "vanjski" dio mreže koji je dostupan vanjskim klijentima.
Sigurnosna politika "Kompanija d.d." je takva da njeni unutarnji DNS klijenti mogu preslikati vanjska domenska imena i razmjenjivati elektroničku poštu s korisnicima koji se nalaze izvan unutarnje mreže. Dio sigurnosne politike je i da unutarnji DNS klijenti imaju pristup do određenih unutarnjih zona koje nisu vidljive i dohvatljive korisnicima izvan unutarnje mreže.

Da bi realizirala postavljene ciljeve, organizacija mora postaviti dva DNS poslužitelja. Prvi se pozicionira na unutarnjoj mreži, a drugi unutar demilitarizirane zone, na računalu s najvišim nivoom sigurnosti (eng. *bastion host*), koji je "*proxy*" poslužitelj i može razmjenjivati upite s obje mreže (unutarnjom i vanjskom).
Unutarnji DNS poslužitelj treba biti podešen da prosljeđuje sve upite (osim onih upita koji su namijenjeni `site1.internal`, `site2.internal`, `site1.kompanija.hr` i `site2.kompanija.hr`) prema vanjskom DNS poslužitelju koji se nalaze u demilitariziranoj zoni. Ti unutarnji DNS poslužitelji moraju imati kompletan set informacija za navedene domene.
Da bi se zaštitile `site1.internal` i `site2.internal` unutarnje domene, unutarnji DNS poslužitelji moraju biti podešeni da ne dozvoljavaju nikakve upite prema tim domenama od bilo kojeg vanjskog klijenta, uključujući i od *bastion hosta*.
Vanjski DNS poslužitelj, koji je na *bastion hostu*, u svojoj osnovnoj postavki dozvoljava pregledavanje vanjskih (javnih) inačica domena `site1.kompanija.hr` i `site2.kompanija.hr`. Na vanjskim DNS poslužiteljima bi se trebali nalaziti podaci kao što su klijentski zapisi za javne poslužitelje (`www.kompanija.hr` i `ftp.kompanija.hr`) i *mail exchange* (MX) zapisi (`a.mx.kompanija.hr` i `b.mx.kompanija.hr`).



Slika 2: Tijek upita za site1 domenama od unutarnjeg i vanjskog klijenta

Na slici *Slika 2* može se vidjeti tijek upita za `site1` domenom postavljen od unutarnjeg i vanjskog klijenta:

1. Unutarnji DNS klijent šalje upit za `site1.kompanija.hr` koji ide na unutarnji DNS poslužitelj.
2. Unutarnji DNS poslužitelj prosljeđuje upit za `site1.kompanija.hr` prema vanjskom DNS poslužitelju na *bastion host*-u.
3. Vanjski DNS poslužitelj odgovara na upit unutarnjeg DNS poslužitelja za `site1.kompanija.hr`.
4. Unutarnji DNS poslužitelj odgovara na upit unutarnjeg DNS klijenta za `site1.kompanija.hr`.
5. Unutarnji DNS klijent šalje upit za `site1.internal` koji ide na unutarnji DNS poslužitelj.
6. Unutarnji DNS poslužitelj odgovara na upit unutarnjeg DNS klijenta za `site1.internal`.
7. Unutarnji DNS klijent šalje upit za `www.carnet.hr` koji ide na unutarnji DNS poslužitelj

8. Unutarnji DNS poslužitelj prosljeđuje upit za www.carnet.hr prema vanjskom DNS poslužitelju.
9. Vanjski DNS poslužitelj šalje upit za www.carnet.hr na vanjsku mrežu (Internet) i dobiva traženi odgovor.
10. Vanjski DNS poslužitelj odgovara na upit unutarnjeg DNS poslužitelja za www.carnet.hr.
11. Unutarnji DNS poslužitelj odgovara na upit unutarnjeg DNS klijenta za www.carnet.hr.
12. Vanjski DNS klijent šalje upit za site1.kompanija.hr prema vanjskom DNS poslužitelju i dobiva traženi odgovor bez kontaktiranja unutarnjeg DNS poslužitelja.

Vanjske (javne) inačice domena site1.kompanija.hr i site2.kompanija.hr trebaju imati posebne MX zapise koji sadrže *wildcard* (´*´) zapise koji upućuju na *bastion host*. To je potrebno kako vanjski mail poslužitelji ne bi imali niti jedan drugi način dostave elektroničke pošte unutarnjim klijentima osim ovog. S takvim *wildcard* zapisima elektronička pošta će se dostavljati *bastion host*-u koji ih onda može proslijediti unutarnjim klijentima.
Jedan od primjera *wildcard* zapisa:

```
*    IN MX 10 externall.kompanija.hr
```

Nakon što se podesi tako da može primati elektroničku poštu za bilo kojeg klijenta u unutarnjoj mreži, *bastion host* treba znati kako da proslijedi elektroničku poštu unutarnjim klijentima, stoga klijent na *bastion host*-u treba podesiti da sve upite prosljeđuje na unutarnji DNS poslužitelj koji treba provesti DNS raščlanjivanje (eng. *DNS resolution*).
Upiti upućeni za dobivanje unutarnjih naziva računala bit će odgovoreni od unutarnjih DNS poslužitelja, a upiti za vanjskim nazivima računala bit će proslijeđeni natrag na vanjski DNS poslužitelj koji se nalazi u demilitariziranoj zoni na *bastion hostu*.
Da bi prosljeđivanje radilo pravilno, unutarnji klijenti moraju biti tako podešeni da DNS upite šalju **samo** prema unutarnjim DNS poslužiteljima, a to se postiže preko selektivnog filtriranja mreže.
Uz pravilnu konfiguraciju, unutarnji klijenti zamišljene organizacije mogu:

- potražiti bilo koji naziv računala na site1.kompanija.hr i site2.kompanija.hr,
- potražiti bilo koji naziv računala na site1.internal i site2.internal,
- potražiti bilo koji naziv računala na Internetu,
- razmjenjivati mail poruke s unutarnjim i vanjskim klijentima.

Vanjski klijenti mogu:

- potražiti bilo koji naziv računala na site1.kompanija.hr i site2.kompanija.hr,
- razmjenjivati mail poruke s bilo kojim računalom na site1.kompanija.hr i site2.kompanija.hr.

4.1. Podešavanje unutarnjeg DNS poslužitelja

Primjer *named.conf* skripte unutarnjeg DNS poslužitelja [6]:

```
// definiranje pristupnih lista
acl internals { 172.16.10.0/24; 192.168.1.0/24; };

acl externals { 1.2.3.4 };

// definiranje parametara rada
options {
  directory "/etc/bind";        // radni direktorij
  forward only;                 // isključivo prosljeđivanje upita
  forwarders {                  // definiranje liste poslužitelja na
                                // koju se prosljeđuju upiti
      1.2.3.4;
       };
  allow-transfer { none; };          // zabrana transfera zone
```

```
                    // svim računalima
  allow-query { internals; externals; };    // ograničavanje upita
                                            // na unutarnju i
                                            // vanjsku domenu
  allow-recursion { internals; };   // ograničavanje obavljanja
                                    // rekurzivnih upita na
                                    // računala u unutarnjoj
                                    // mreži
};
// definiranje primarne zone za kompanija.hr domenu
// kompletan pogled na zonu
zone "site1.kompanija.hr" {

  type master;
  file "m/site1.kompanija.hr";
forwarders { }; // dozvoljavanje iterativnih upita svim računalima
                // (niti jednom poslužitelju se ne prosljeđuju
                // upiti)
  allow-query { internals; externals; };
  allow-transfer { internals; };
};

// definiranje sekundarne zone za kompanija.hr domenu
// kompletan pogled na zonu
zone "site2.kompanija.hr" {

  type slave;
  file "s/site2.kompanija.hr";
  masters { 172.16.10.3; };
  forwarders { };
  allow-query { internals; externals; };
  allow-transfer { internals; };
};

// definiranje primarne zone za internal domenu
// kompletan pogled na zonu
zone "site1.internal" {
  type master;
  file "m/site1.internal";
  forwarders { };
  allow-query { internals; };
  allow-transfer { internals; }
};

// definiranje primarne zone za internal domenu
// kompletan pogled na zonu
zone "site2.internal" {
  type slave;
  file "s/site2.internal";
  masters { 172.16.10.3; };
  forwarders { };
  allow-query { internals };
  allow-transfer { internals; }
};
```

4.2. Podešavanje vanjskog DNS poslužitelja

Primjer *named.conf* skripte vanjskog DNS poslužitelja [6]:

```
acl internals { 172.16.10.0/24; 192.168.1.0/24; };

acl externals { 1.2.3.4; };

options {
  directory "/etc/bind";            // radni direktorij
  allow-transfer { none; };         // zabrana transfera zone
                                    // svim računalima
  allow-query { internals; externals; };    // ograničavanje upita
                                            // na unutarnju i
                                            // vanjsku domenu
  allow-recursion { internals; externals; };       // ograničavanje
                                                   // rekurzivnih
                                                   // upita
};
// definiranje primarne zone za kompanija.hr domenu
// kompletan pogled na zonu
zone "site1.kompanija.hr" {
  type master;
  file "m/site1.kompanija.hr";
  allow-query { any; };
  allow-transfer { internals; externals; };
};
// definiranje sekundarne zone za kompanija.hr domenu
// kompletan pogled na zonu
zone "site2.kompanija.hr" {
  type slave;
  file "s/site2.kompanija.hr";
  masters { another_bastion_host_maybe; };
  allow-query { any; };
  allow-transfer { internals; externals; }
};
```

Unutar `resolv.conf` na *bastion host*-u treba upisati:

```
search  { internal; kompanija.hr }     // određivanje domena koje
                                       // se pretražuju za neko
                                       // računalo na koje se
                                       // želi spojiti
nameserver 172.16.10.2    // lista adresa postojećih
nameserver 172.16.10.3    // unutarnjih poslužitelja
nameserver 172.16.10.4    //
```

5. Zaključak

Razdvojeni DNS se može primijeniti u situacijama kada se koriste različita domenska imena na unutarnjoj mreži od onih koja se koriste na vanjskoj mreži. Kod uporabe klasičnog DNS-a u takvoj situaciji ne bi bilo moguće postavljanje DNS upita prema vanjskoj mreži jer odgovori ne bi stizali na ispravnu adresu. Uporabom razdvojenog DNS-a podiže se stupanj sigurnosti računalne mreže i pomaže se u skrivanju internih DNS informacija od zlonamjernih korisnika.
Samo podešavanje razdvojenog DNS-a iziskuje napredno poznavanje DNS-a i oduzima dosta vremena. Uz to, ovime se ne ostvaruje potpuna zaštita unutarnjih DNS informacija, budući da postoje i drugi načini "curenja" ovih podataka.

6. Reference

[1] RFC 882 - Domain names: Concepts and facilities, http://www.faqs.org/rfcs/rfc882.html
[2] RFC 883 - Domain names: Implementation specification, http://www.faqs.org/rfcs/rfc883.html
[3] RFC 1034 - Domain names - concepts and facilities, http://www.faqs.org/rfcs/rfc1034.html
[4] RFC 1035 - Domain names - implementation and specification, http://www.faqs.org/rfcs/rfc1035.html
[5] RFC 1918 - Address Allocation for Private Internets, http://www.faqs.org/rfcs/rfc1918.html
[6] BIND 9 Administrator Reference Manual, http://www.isc.org/sw/bind/arm93/Bv9ARM.html