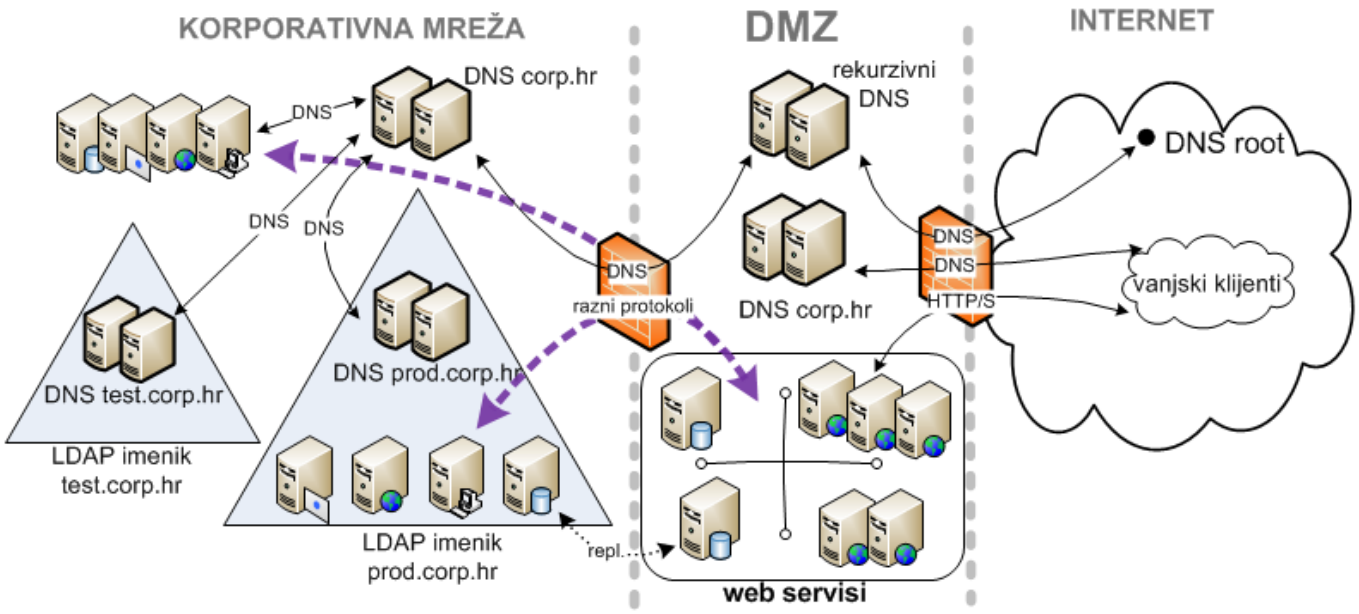
DNS – optimizacija "resolvinga" internih i eksternih imena

DNS servis je jedan od ključnih, običnom korisniku nevidljivih kotačića u očekivanom funkcioniranju Interneta. U članku pod nazivom "Arhitektura sigurnog DNS sustava" objašnjavali smo kako taj servis uspostaviti na siguran način, a u ovom nastavku dalje razrađujemo istu temu.

Uvod u problem

U članku pod linkom http://sistemac.carnet.hr/node/1380 [1] modelirali smo siguran DNS sustav za fiktivnu tvrtku corp.hr. Iz didaktičkih razloga tada smo zanemarili detalje o IT infrastrukturi tvrtke. Skica koja slijedi sugerira nam da je Corp u stvari poslovni subjekt sa povećim brojem raznovrsnih servisa, desktop i serverskih instalacija. U internoj mreži primjećujemo infrastrukturne servise i aplikacije za najrazličitije potrebe; u DMZ se naseliše HTTP(S) web farme dvoslojne i troslojne arhitekture, razdijeljene VLAN-ovima i access listama; mission critical servisi su redundantni jer to je poslovni imperativ.... ukratko, razgranata i složena računalno-komunikacijska infrastruktura.



Poput goleme većine dugovječnijih poduzeća, Corp se je svojevremeno opredijelio za primjenu tzv. „split DNS“ arhitekture, to nam govori postojanje unutarnje i vanjske corp.hr domene. U unutarnjem DNS ogranku – nešto u corp.hr, nešto u prod.corp.hr - su interni zapisi, sa privatnim IP adresama; u vanjskom corp.hr su zapisi za javne servise, sa Internet IP adresama. Taj model je svojevremeno, zbog tadašnjih značajki DNS servisa i objektivnih potreba poduzeća, bio uobičajeni način rješavanja resolvinga imena tipa FQDN. Naime, dugo je bilo dovoljno oglašavati svoju prisutnost na Mreži posredstvom jednog do dva web serverčića sa HTTP pristupom... ali ekspanzija Internet poslovanja uzrokovala je naglo „bubrenje“ servisa u DMZ-u, time i samog DMZ-a kao infrastrukturne osnovice.

Neizbježno, u DMZ se pojavio problem *resolvinga* imena servera i servisa lociranih izvan te sigurnosne zone: neki serveri moraju moći resolvirati Internet imena, neki interna imena a neki, bome, i jedno i drugo. Svakako, računala u internoj mreži moraju moći resolvirati FQDN imena servera i servisa lociranih u DMZ. Ljubičaste dvokrake strelice na gornjoj skici simboliziraju tu

potrebu. Glede instalacija u DMZ, sve dok u tom segmentu imamo nekoliko servera, potpuno je opravdana uporaba lokalnih Hosts datoteka za resolviranje internih i eksternih imena. Ali upisivati tucet stavki u Hosts datoteke na tucet servera, sa svješću da će toga biti sve više... e, ta spoznaja će svakog agilnijeg informatičara motivirati da „mućne glavom“ kako posao reslovinga FQDN imena prebaciti na DNS servis. „Ta zato ga imamo, zar ne?!“ – reći će i oni iz interne mreže kojima treba resloviranje imena servera i servisa lociranih u DMZ.

Kad proanaliziramo situaciju, shvatit ćemo da je duplicirana corp.hr domena jedini stvarni problem. Konačno rješenje za optimizaciju resolvinga posredstvom DNS-a jako ovisi o tome možemo li „ubiti“ internu corp.hr domenu. Sudbinu ove domene, pak, određuje dosta faktora, npr.:

- brojnost i tipovi zapisa - lakše je analizirati i izmigrirati par stotina A zapisa nego par tisuća njih - A, CNAME, što živih, što mrtvih - a treba nešto učiniti i sa reverznom zonom zbog konsolidacije PTR zapisa;
- jesu li u internoj corp.hr domeni samo zapisi servera ili i stanica, ili oboje, zajedno sa imenima aktivne mrežne opreme – jer DNS treba čak i nama informatičarima, za naš nadzorni i upravljački softver;
- koji točno interni serveri, upisani u internu corp.hr, rabe SSL certifikate – trebat će im mijenjati certifikate, informirati klijente;
- koje interne aplikacije imaju hard coded imena internih servera / servisa sa sufiksom corp.hr – ako to ne korigiramo, riskiramo prekid radnog procesa;
- kojim su sve računalima DNS-ovi autoritativni za corp.hr postavljeni kao primarni i sekundarni DNS serveri;

... a sve to treba uskladiti sa internim politikama i procesima jer jedna jedina nekome-i-zbog-nečega-bitna norma može obezvrijediti i najsavršeniji tehnički rezon! :-)

Opis mogućeg rješenja

Ako ne možemo ukinuti internu corp.hr domenu, a u pravilu ne možemo, govore mi dosadašnja iskustva, možemo ovako „reprogramirati“ korporativni DNS resolving:

- Potrebu resolviranja imena svih servera i servisa lociranih u DMZ, a koji su konfigurirani sa sufiksom corp.hr, riješit ćemo tako da njihova imena i privatne IP adrese zapišemo u interni corp.hr i nadalje ih tu održavamo. Naši mrežari moraju omogućiti pristup tim serverima / servisima iz interne mreže.
- Na rekurzivnim DNS serverima postaviti Conditional Forwarding za interne domene corp.hr i prod.corp.hr. Ovdje je zgodno uočiti da za Conditional Forwarding ne moramo upisivati sve interne DNS-ove, dovoljna su po dva za svaku internu DNS domenu, tek da osiguramo visoku raspoloživost DNS servisa. Recimo, ako je naš imenični servis Active Directory, a taj sustav opslužuje desetak teritorijalno rasijanih Domain Controllera, kao Conditional Forwardere navesti ćemo dva najbliža.
- Na vatrozidu koji dijeli rekurzivne od internih DNS servera naši mrežari moraju propustiti TCP/UDP 53 i to tako da obje strane mogu inicirati konekcije. Nasuprot ovome, vatrozid kroz kojega rekurzivni serveri pričaju sa Internetom mora biti podešen tako da dopušta samo promet kojega su inicirali naši reverzni DNS-ovi.
- Svim serverima u DMZ postaviti rekurzivne DNS servere kao primarni i sekundarni. Ujedno, tim serverima onemogućiti resolving posredstvom Hosts datoteke (ili ih temeljito pročistiti).

Može li drugačije?

Kako to u praksi često biva, moguće su varijacije opisanog rješenja, ovisno o značajkama vaše ICT infrastrukture i aktualnim politikama.

Moguće je da se opredijelite i za neki drugačiji model. U čanku sam zradio koncept kojega ja preferiram, ali možemo, recimo, u DMZ postaviti par novih DNS servera koji će biti sekundarni za domene corp.hr i prod.corp.hr; njih usmjerimo na reverzni DNS a te sekundarne postavimo serverima u DMZ... Nema potrebe detaljizirati, jer čim „poslovnjak“ čuje da su za ovaj model potrebna dva dodatna servera - hop, eto nas opet na onom prvom rješenju! :-)

uto, 2014-05-13 19:38 - Ratko Žižek**Vote:** 0

No votes yet

Source URL: https://sysportal.carnet.hr/node/1395

Links
[1] https://sysportal.carnet.hr/node/1380