Request for Information (RFI)

DNS caching sistem

Sadržaj

1 Uvod

1.1 Ciljevi

Cilj ovog dokumenta je prikupljanje informacija o potencijalnim rješenjima koja bi se mogla iskoristiti kao caching DNS sistem u BH Telecomu u naredne tri/pet godine.

Namjena postojećeg javnog cache-ing DNS sistema BH Telecoma je da procesom DNS rezolucije, opslužuje korisnike usluga Internet konekcije DNS servisom u okviru kojeg se izvršava prevođenje imena u Internet domenskom prostoru u IP adrese. U proces DNS rezolucije su uključeni svi broadband korisnici BH Telecoma sa dinamičkim i statičkim IP adresama, korisnici mobilne telefonije, korisnici hosting usluga itd.

1.2 Ciljana publika

Ovaj dokument je namijenjen kompanijama koje su vendori, integratori ili imeplementatori DNS caching sistema. Reference za rješenje trebaju zadovoljavati implementaciju u okruženjima sa 100.000 QPS-ova. Navedene implementacije se trebaju se nalaziti u Evropi ili Sjevernoj Americi i trebaju biti realizirane u protekle tri godine (jedna implementacija je dovoljna).

1.3 Terminologija

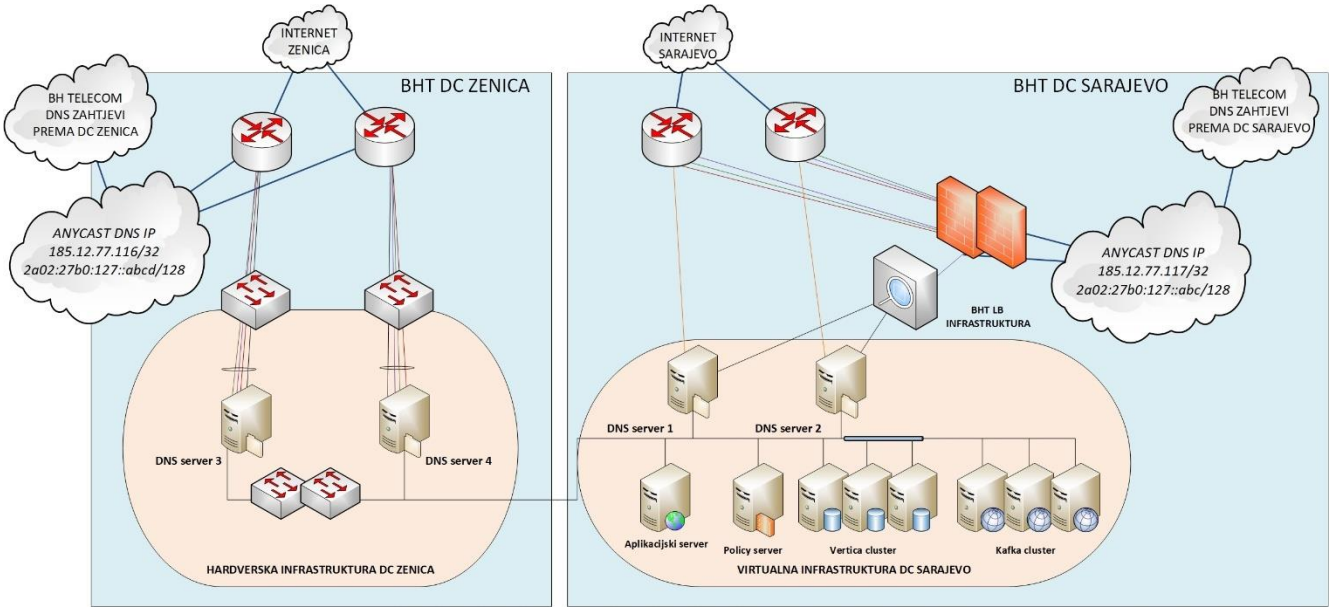
DNS – Domain Name System
QPS – Queries per second
CPE – Customer premises equipment
DDoS – Distributed Denial-of-Service
PRSD – Pseudo Random Subdomain
LB – Load balancer
CLI – Command-line interface
GUI – Graphical user interface

2 Arhitektura postojećeg rješenja

Trenutni javni cache-ing DNS sistem BH Telecoma se bazira na softverskom rješenju implementiranom od strane Akamai proizvođača, kao jednog od vodećih lidera u tržišnom segmentu sigurnosti i DNS softvera. Akamai softver, sa pripadajućim konfiguracijama, je instaliran na svakom DNS serveru (bilo da se radi o hardverskom uređaju ili virtualnoj mašini) te funkcioniše u *resolver* modu, bez *forwarding* ili *authority* funkcionalnosti.

Kompletan DNS sistem je implementiran kao visoko dostupno georedundantno rješenje sa 4 DNS serverske instance u dva Data centra, na dvije fizički odvojene lokacije, u Sarajevu i Zenici. Dva DNS servera su instalirana na hardverskim serverima, dok su druga dva instalirana na virtualnim mašinama VMware virtualizacijske platforme BH Telecoma.

U nastavku je prikazana ilustracija toplogije sistema.

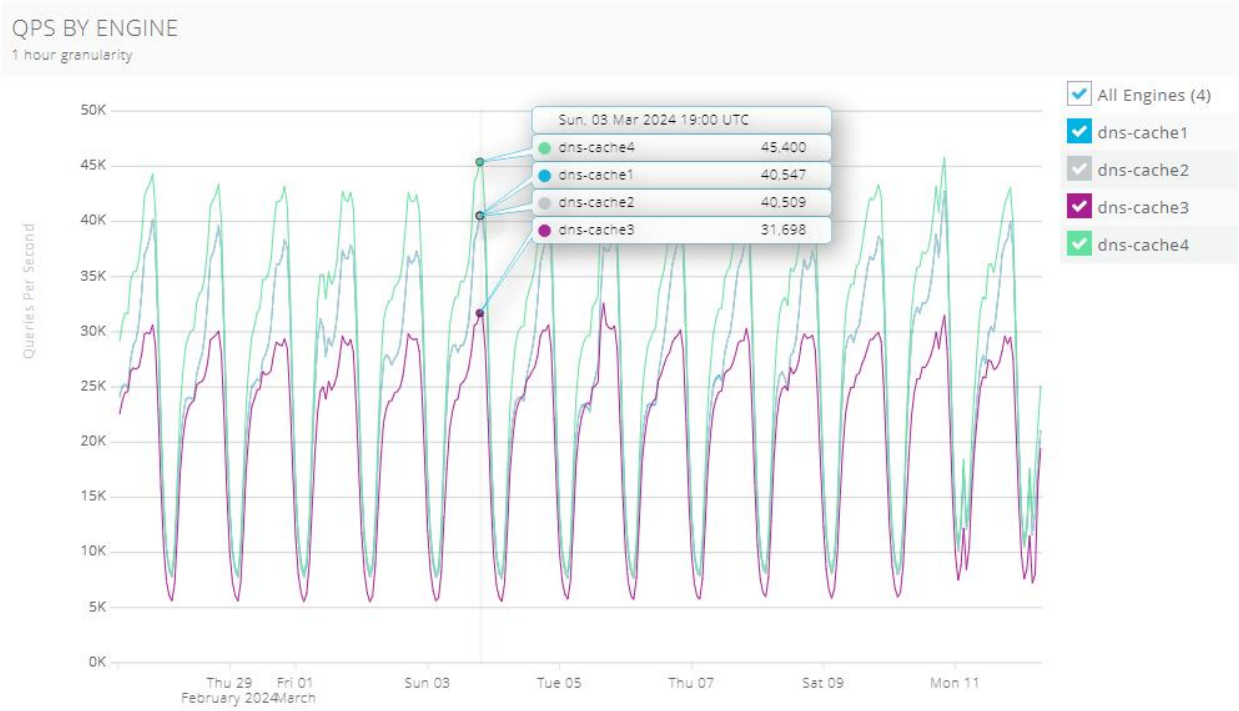


Topologija javnog cache-ing DNS sistema BH Telecoma

Postojeći javni cache-ing DNS sistem je konfigurisan na način da DNS rekurzijom opslužuje samo korisnike BH Telecoma (IP adrese koje pripadaju BH Telecomu). Na ovaj način se izbjegava *open resolver* postavka DNS sistema koja bi omogućila i korisnicima drugih *provider*-a da koriste DNS sistem BH Telecoma. Ukupan broj jedinstvenih DNS upita koji na cjelokupan sistem pristižu od strane korisnika, u periodima najvećeg dnevnog opterećenja iznosi oko 110k QPS (Query per Second), gdje se navedeni broj odnosi na jedinstvene klijentske DNS upite (30k QPS do 45k QPS po svakom DNS serveru).

U proteklom periodu uočen je konstantan porast broja upita, što je rezultat povećanog broja korisnika odnosno terminalnih uređaja (računari, laptopi, mobiteli, CPE uređaji itd.), kao i veći broj DNS zahtjeva uzrokovan specifičnim vremenskim intervalima (u nekim peak periodima – dva-tri puta godišnje) u kojima broj jedinstvenih upita dostiže vrijednost i do 160k QPS.

Kantonalni sud Sarajevo **Br. UF/I-520/04** Identifikacioni broj: **4200211100005** Porezni broj: **0107880400** PDV broj: **200211100005**
Računi BH Telecoma d.d. Sarajevo
ASA Banka Naša i snažna d.d. Sarajevo, glavni račun BH Telecoma - KM: 1401010007090054; RAIFFEISEN BANK d.d. BiH, KM: 1610000030950092, IBAN: BA39 1611 0000 0124 8933, SWIFT: RZBABA2S; UNICREDIT BANK d.d. Mostar, KM: 3383202250226088, IBAN: BA39 3383 2048 9065 5134, SWIFT: UNCRBA22; NLB BANKA d.d. Sarajevo, KM: 1322600311707003; INTESA SANPAOLO BANKA d.d. BiH, KM: 1540012000318547; SPARKASSE BANK d.d. BiH, KM: 1990490005000203; UNION BANKA d.d. Sarajevo, KM: 1020500000020853; NOVA BANKA a.d. Banja Luka, KM: 5550050047194638; BOSNA BANK INTERNATIONAL d.d. Sarajevo, KM: 1410010000000941; ASA BANKA d.d. Sarajevo, KM: 1340100000160849; PRIVREDNA BANKA SARAJEVO d.d. Sarajevo, KM: 1010000050732105; ZIRAATBANK BH d.d. Sarajevo, KM: 1860001060841009;



Opterećenje servera sa QPS vrijednostima

3 Zahtjevi za buduće stanje

Ponuda koja uključuje DNS sistem treba biti bazirana na TCO konceptu sa garantnim periodom od tri godine i postgarantnom periodu od dvije godine. Sistem treba da zadovoljava sljedeće zahtijeve:

- Sistem mora biti postavljen *on-premise* na lokacijama BH Telecoma na kojima je postavljen i postojeći DNS caching sistem (dvije lokacije);
- Broj DNS caching servera po lokaciji mora biti minimalno dva;
- Za raspodijelu saobraćaja po site-u lokaciji mora biti podržan metod BGP *anycast*-a i mora biti podržan klasičan princip load-balancinga (HA Proxy, F5 i slično);
- Sistem mora moći podržavati minimalno 220.000 jedinstvenih upita;
- Moraju biti podržani IPv4, IPv6 i dual-stack;
- Cache hit radio mora biti u rasponu 95% - 99%;
- Sva infrastruktura, uključujući DNS servere i eventualno popratne dodatne sisteme (za kontrolu, monitoring itd) se mora moći deployati na vmware virtuelnoj infrastrukturi;
- Za operativni sistem/i na kojima je rješenje postavljeno ne smije biit najavljen EOL/EOS period u narednih 5 godina;
- Sa sigurnosnog aspekta treba biti podržana mogućnost mitigacije napada kao što su: DNS *amplification*, *cache-poisoning*, NXDOMAIN napadi, PRSD, DNS DDoS, DNS *tunneling* te *reflection-based* distribuirani napadi;
- Sistem mora podržavati mogućnost konfigurisanja access listi, brisanja unosa za domene i poddomene na caching serverima i konfigurisanje DNS view-a;
- DNS sistem treba da ima mogućnost centraliziranog upravljanja u smislu kreiranja sigurnosnih politika i apliciranja na svaki od servera putem *GUI-ja;*

- DNS treba da posjeduje pregled mogućnost konfiguracije i putem CLI-a;
- Sistem treba da ima mogućnost monitoringa DNS kroz GUI koji omogućava uvid u trenutnu opterećenost sistema i broj pristiglih upita u sekundi na svaki od pojedinih DNS servera;
- Sistem treba da ima mogućnost pružanja pregleda podataka o pojedinim komponentama sistema, sigurnosnim događajima i incidentima;
- Sistem treba da ima mogućnost generisanja izvještaj;a
- Sistem mora biti proširiv na način da se nudi *customer-based pojedinačan* DNS servis prema krajnjim korisnicima;

U sklopu odgovora na RFI, pored tehničkih detalja, potrebno je dostaviti i informativnu cijenu i vremenski okvir potreban za realizaciju implementacije ovog projekta.

Kantonalni sud Sarajevo **Br. UF/I-520/04** Identifikacioni broj: **4200211100005** Porezni broj: **0107880400** PDV broj: **200211100005**
Računi BH Telecoma d.d. Sarajevo
ASA Banka Naša i snažna d.d. Sarajevo, glavni račun BH Telecoma - KM: 1401010007090054; RAIFFEISEN BANK d.d. BiH, KM: 1610000030950092, IBAN: BA39 1611 0000 0124 8933, SWIFT: RZBABA2S; UNICREDIT BANK d.d. Mostar, KM: 3383202250226088, IBAN: BA39 3383 2048 9065 5134, SWIFT: UNCRBA22; NLB BANKA d.d. Sarajevo, KM: 1322600311707003; INTESA SANPAOLO BANKA d.d. BiH, KM: 1540012000318547; SPARKASSE BANK d.d. BiH, KM: 1990490005000203; UNION BANKA d.d. Sarajevo, KM: 1020500000020853; NOVA BANKA a.d. Banja Luka, KM: 5550050047194638; BOSNA BANK INTERNATIONAL d.d. Sarajevo, KM: 1410010000000941; ASA BANKA d.d. Sarajevo, KM: 1340100000160849; PRIVREDNA BANKA SARAJEVO d.d. Sarajevo, KM: 1010000050732105; ZIRAATBANK BH d.d. Sarajevo, KM: 1860001060841009;