DIZAJN I IMPLEMENTACIJA RJEŠENJA ZA OPORAVAK OD KATASTROFALNOG OTKAZA MREŽNIH KONEKCIJA

Šebalj, Danijel

VISOKO UČILIŠTE ALGEBRA

ZAVRŠNI RAD

DIZAJN I IMPLEMENTACIJA RJEŠENJA ZA OPORAVAK OD KATASTROFALNOG OTKAZA MREŽNIH KONEKCIJA

Danijel Šebalj

Zagreb, 21.veljače 2018.

Student vlastoručno potpisuje Završni rad na prvoj stranici ispred Predgovora s datumom i oznakom mjesta završetka rada te naznakom:

„Pod punom odgovornošću pismeno potvrđujem da je ovo moj autorski rad čiji niti jedan dio nije nastao kopiranjem ili plagiranjem tuđeg sadržaja. Prilikom izrade rada koristio sam tuđe materijale navedene u popisu literature, ali nisam kopirao niti jedan njihov dio, osim citata za koje sam naveo autora i izvor, te ih jasno označio znakovima navodnika. U slučaju da se u bilo kojem trenutku dokaže suprotno, spreman sam snositi sve posljedice uključivo i poništenje javne isprave stečene dijelom i na temelju ovoga rada“.

U Zagrebu, 21.velječe 2018.

Danijel Šebalj

Predgovor

Ova stranica treba sadržavati izjavu ili zahvalu kandidata…..

Prilikom uvezivanja rada, Umjesto ove stranice ne zaboravite umetnuti original potvrde o prihvaćanju teme završnog rada kojeg ste preuzeli u studentskoj referadi

Sažetak

Ovim radom se želi prikazati na koji je način moguće osigurati neometano odvijanje ključnih poslovnih procesa tvrtki koje se uvelike oslanjanju na upotrebu informacijskih tehnologija. U ovom radu će se prikazati način osiguravanja visoke dostupnosti usluga, koji su problemi i moguća rješenja prilikom dizajna i implementacije sustava za oporavak od katastrofe, te pružiti uvid u neke od dostupnih tehnologija za povezivanje primarne i sekundarne lokacije. Primarno će se obraditi korištenje mrežnih tehnologija, dok će cjelokupna serverska infrastruktura, pripadajuće tehnologije i rješenja biti obrađeni do razine potrebne za razumijevanje tematike.

Ključne riječi: raspodjela opterećenja, visoka dostupnost, mrežna povezanost, usmjeravanje prometa

Abstract

This thesis describes how to ensure continuity of key business processes of a company that heavily relies on use of information technologies. Specifically, the goal is to show how to achieve high availability of services, what are challenges and its possible solutions while designing and implementing disaster recovery solution as well as available technology for connecting primary and secondary location. The primary emphasis is put on use of network technologies while the overall server infrastructure as well as the related technologies and solutions will not be the focus of this thesis except up to the level needed to understand the theme.

Key words: load balance, high availability, network connectivity, traffic routing

Sadržaj

1. Uvod

Uspješnost i tržišna konkurentnost tvrtki u današnje vrijeme uvelike ovisi o neprekidnoj dostupnosti, tj. raspoloživosti usluga koje pružaju korisnicima. Kako bi postigli ranije spomenuto, tvrtke često imaju potrebu osigurati dostupnost svojih usluga putem sekundarne lokacije za oporavak od katastrofe (eng. *disaster recovery*). Osiguravanjem sekundarne lokacije tvrtka je u mogućnosti korisniku isporučiti uslugu u slučaju katastrofalnog ispada pojedinih elemenata sustava ili kompletnog prekida primarne lokacije uzrokovanog prirodnom katastrofom ili nekom drugom prijetnjom.

Kroz ovaj rad želi se prikazati jedan od mogućih načina implementacije i dizajna rješenja za oporavak od katastrofalnog ispada mrežne dostupnosti primarne lokacije. Ideje i način izvedbe se mogu iskoristiti kao metodologija za inženjere koji će raditi na dizajnu i implementaciji istih ili sličnih projekata.

Prilikom pisanja rada korištena je stručna literatura, informacije dostupne na internetu, te vlastita praktična iskustava i znanja autora. Sve slike i tablice korištene u ovome radu djelo su autora.

2. Uloga Disaster Recovery lokacije u kontekstu uspješnog poslovanja tvrtke

Većina korisnika se u prošlosti oslanjala na vlastitu infrastrukturu, te su bili uvjerenja kako neće doći do katastrofalnog događaja koji bi ugrozio poslovanje tvrtke. U današnje vrijeme taj trend se mijenja i korisnici osvještavaju vjerojatnost pojave događaja koji mogu ugroziti poslovanje tvrtke. Prirodna katastrofa, ljudska pogreška, kvar na određenoj komponenti sustava, te zloćudni programi samo su neki od događaja koji mogu ugroziti poslovanje.

Rastuća stopa kibernetičkog kriminala i njegove posljedice postaju sve veća opasnost za svaku organizaciju. Prema istraživanju organizacije Gemalto provedenom u prvoj polovici 2017. godine zabilježeni su sljedeći statistički podaci[1]:

- kompromitirano, ukradeno ili izgubljeno je 1.9 milijardi podataka, što čini ukupni porast od 164% u odnosu na posljednjih 6 mjeseci u 2016. godini
- vanjski zlonamjerni napadači uzrokovali su 74% napada povezanih s krađom podatka, što je porast od 23%
- 25% svih napada povezanih s krađom podataka pretrpjele su zdravstvene organizacije

Zabilježeni su slučajevi u kojima su neke od najpoznatijih svjetskih tvrtki u određenim trenucima imale poteškoća s dostupnošću svojih usluga ili otežanom isporukom u periodu od nekoliko sati pa sve do nekoliko dana. Neki od najpoznatijih slučajeva uključuju[2]:

Bank of America

Usluga Internet bankarstva ove banke je bila otežana ili u potpunosti nedostupna u vremenskom periodu od 6 dana za sve korisnike (kojih je u tom trenutku bilo 29 mil.). Problem je pripisan višegodišnjem projektu čiji je cilj bio nadogradnja sustava Internet bankarstva, a u konačnici je prouzročio tehničke probleme u kombinaciji s neočekivanim porastom *web* prometa.

---

[1] https://www.gemalto.com/press/pages/first-half-2017-breach-level-index-report-identity-theft-and-poor-internal-security-practices-take-a-toll.aspx, veljača. 2018.

[2] https://www.evolven.com/blog/2011-devastating-outages-major-brands.html, veljača. 2018.

Amazon EC2

Izmjene na mrežnim postavkama Amazonove usluge „*Amazon Elastic Compute Cloud"* prouzročile su nedostupnost usluge u periodu od 4 dana.

Google Gmail

Usluga elektroničke pošte koju pruža Google kroz svoju Gmail uslugu prouzrokovala je probleme za 120 000 korisnika.

Microsoft Windows Live Hotmail

Zahvaćenim korisnicima izbrisan je ulazni spremnik elektroničke pošte, te su neke od ulaznih poruka premještene u mapu koja služi za izbrisane poruke. Microsoft nije iznio detalje o događaju.

Netflix

Usluga za video *streaming* sadržaja pretrpjela je nedostupnost u periodu od 4 do 8 sati. Broj zahvaćenih korisnika iznosio je 20 mil., a Netflix nije iznio detalje o uzroku problema, samo pojašnjene da se radilo o „rijetkom tehničkom problemu".

Neovisno radi li se o kritičnoj usluzi ili usluzi koja ne utječe u velikoj mjeri na poslovanje, svaki ispad može prouzročiti lakše ili teže posljedice za organizaciju. Osim financijskog gubitka, mnogo veća može biti šteta koja će narušiti ugled organizacije, a samim time i narušiti povjerenje korisnika što direktno utječe na nastavak poslovanja. Upravo zbog tih rizika trebalo bi voditi računa o *disaster recovery* lokaciji.

2.1. Što je Disaster recovery

Disaster recovery uključuje niz politika, alata i procedura koje omogućavaju oporavak ili nastavak poslovanja uslijed katastrofalnog događaja kao što su: ljudska pogreška, požar, poplava, kvar vitalnih dijelova komunikacijske infrastrukture i sl.

Disaster recovery je dio, odnosno podskup plana koji se naziva kontinuitet poslovanja (eng. *Business Continuity).* Iako se ova dva naziva ponekad koriste zajedno, te se preklapaju u pojedinim elementima, oni nikako nisu isto. Kontinuitet poslovanja se odnosi na metodologiju koja podrazumijeva plan koji će omogućiti nastavak poslovanja prije, za vrijeme i nakon katastrofalnog događaja ili prekida, te validaciju istog, dok je zadaća *disaster recovery-a* u što kraćem vremenskom periodu zaustaviti posljedice katastrofe i omogućiti

nastavak poslovanja. Ukoliko dođe do katastrofalnog događaja, potrebno je slijediti plan koji će organizaciji pomoći da se što prije oporavi. Dokument u kojem se navodi takav plan naziva se *Disaster Recovery Plan* i može uključivati radnje kao što su isključivanje sustava iz pogona, identifikacija sustava zahvaćenih poplavom ili potresom, preusmjeravanje prometa na alternativnu lokaciju, zamjena oštećenih dijelova sustava i sl.

Implementacijom redundantnih uređaja unutar sustava štiti se sustav u slučaju otkaza jedne ili više komponenti sustava, a zajedno sa sustavom i usluge koji on isporučuje. Za razliku od visoke dostupnosti, *disaster recovery* podrazumijeva aktivnosti i resurse na alternativnoj lokaciji koji su potrebne za oporavak od katastrofe, a ne samo preuzimanje (eng. *failover)* funkcionalnosti štićenog uređaja, odnosno lokacije.

2.2. Prednosti za poslovanje

Tvrtka provodi politiku izrade sigurnosne kopije podataka kako bi se zaštitila od gubitka podataka. Izradom sigurnosnih kopija tvrtka štiti svoje podatke u slučajevima kvara na sustavima za pohranu podataka (eng. *storage*), nenamjerne ljudske pogreške, virusnih infekcija datoteka i sl. U slučajevima katastrofalnih događaja pri kojima je ugrožena fizička lokacija tvrtke i sva njena imovina (npr. potresi, poplave, požari i sl.), potrebno je rješenje koje će biti geografski dovoljno udaljeno kako ne bi bilo zahvaćeno istom katastrofom. Politiku izrade sigurnosnih kopija tvrtka nikako ne bi smjela zamijeniti *disaster recovery* lokacijom iz razloga što ju ne štiti od iste vrste rizika.

Komercijalne usluge koje tvrtka nudi krajnjim korisnicima predmet su Ugovora o razini usluge (eng. *Service Level Agreement*) kojim se garantira visoka dostupnost na razini od **99.9%** na mjesečnoj razini, što iznosi približno **43min 12sec**, odnosno **1min 26sec** nedostupnosti po danu u mjesecu[3]. U slučaju nepoštivanja Ugovora, tvrtka je dužna nadoknaditi štetu prema naručitelju usluge u iznosu ugovorenih penala. Tvrtka se odlučila za izgradnju *disaster recovery* rješenja, kako bi se osigurala od isplate velikih novčanih naknada zbog nepoštivanja Ugovora. Posjedujući *disaster recovery* rješenje, tvrtka također stječe sljedeće poslovne prednosti:

[3] http://www.slatools.com/sla-uptime-calculator, veljača. 2018

1. **Manji financijski gubici u poslovanju**

   Katastrofalni događaj ili otkaz pojedinog dijela sustava za organizaciju bi značio nemogućnost poslovanja. Ukoliko tvrtka nije u mogućnosti isporučivati svoje usluge, gubi novac. Obzirom na djelatnost tvrtke, generirani gubitak, kao izravna posljedica katastrofe može ujedno značiti i propast tvrtke, ukoliko potraje kroz dulji vremenski period. Posjedujući *disaster recovery* rješenje, tvrtka je u mogućnosti ubrzo nakon katastrofe uspostaviti vitalne dijelove sustava važne za poslovanje i nastaviti generirati prihod.

2. **Minimiziran negativan utjecaj na ugled tvrtke uslijed otkaza informacijskog sustava**

   Iako financijski gubici predstavljaju veliki problem za svaku tvrtku, mnogo veći mogu biti oni povezani s ugledom koji tvrtka uživa kod krajnjih korisnika i partnera. Ukoliko zbog nedostupnosti pojedine usluge tvrtka nije u mogućnosti ispuniti svoje obveze (prema korisnicima i/ili partnerima), njen ugled može biti značajno narušen. Jednom izgubljeni ugled teško je povratiti. Osim izgubljenog ugleda, postoji i mogućnost da se tvrtka suoči s predstojećim sudskim tužbama zbog neispunjenih ugovornih obveza.

3. **Položaj na tržištu**

   Tvrtka je uložila značajna sredstva u osiguravanje svog položaja na tržištu, obzirom da nema povlašteni položaj (monopol), a samim time je privukla i korisnike. Sigurno je da tvrtka svoje korisnike i dobit koju generiraju ne želi prepustiti konkurenciji, već želi zadržati njihovo povjerenje. Kako bi zadržala postojeće korisnike i stekla povjerenje novih, tvrtka mora osigurati visoko dostupne usluge i u slučajevima katastrofe. Jednom izgubljene korisnike puno je teže ponovno privući nego li zadržati postojeće.

4. **Zadovoljavanje kriterija nametnutih od strane regulatornih agencija**

   Pružajući komercijalno dostupne usluge, tvrtka podliježe specifičnim zakonskim regulativama prema kojima je obvezna osigurati dostupnost podataka u bilo kojem trenutku. Tvrtka je sigurna da je u skladu s zakonskim propisima te da joj u slučaju katastrofe ne prijete sudske tužbe i progon ukoliko ima implementirano adekvatno rješenje za oporavak od katastrofe.

3. Definiranje ključnih zahtjeva poslovanja prema IT sustavu

Odgovorna osoba tvrtke koja je predmet ovoga rada, potpisala je Ugovor o povjerljivosti (eng. *Non-disclosure agreement*), stoga je navođenje naziva tvrtke u ovom radu strogo zabranjeno. Glavna djelatnost tvrtke je pružanje komercijalno dostupnih usluga svojim korisnicima putem interneta. Tvrtka svojim korisnicima garantira 99.9% dostupnosti usluga na mjesečnoj razini. Kako bi se osigurala od isplate velikih novčanih naknada zbog nepoštivanja Ugovora, tvrtka se odlučila za izgradnju *disaster recovery* rješenja. Obzirom da informacijske tehnologije (eng. *information technologies*) čine okosnicu sustava kojom se isporučuju usluge, pred mrežne inženjere postavljen je niz informacijsko tehnoloških preduvjeta koje rješenje za oporavak od katastrofe mora ispunjavati:

1. Lokacija na kojoj će se nalaziti rješenje za oporavak od katastrofe mora posjedovati redundantnu vezu prema internetu.
2. Redundantna veza prema internetu mora biti omogućena putem dva različita pružatelja internet usluge. Rješenje mora biti implementirano pomoću *Single-multihomed* ili *Dual-multihomed* načina povezivanja prema internetu.
3. Promet se mora moći usmjeravati putem primarne veze cijelo vrijeme njezine dostupnosti. U slučaju ispada primarne veze, promet se treba preusmjeravati alternativnom vezom.
4. Sve usluge se moraju isporučivati putem primarne lokacije cijelo vrijeme njezine dostupnosti. U slučaju nedostupnosti usluge na primarnoj lokaciji, usluga se mora moći isporučiti putem sekundarne (*disaster recovery*) lokacije.
5. Za uspostavu veze prema primarnoj lokaciji mora se koristit sigurnosni, kriptirani tunel za uspostavu kojeg se mora se koristiti vatrozid nove generacije (eng. *Next-Generation Firewall*).
6. Mreža mora biti strogo segmentirana i zaštićena od malicioznih prijetnji s interneta korištenjem antivirusnog i IPS (eng. *Intrusion Prevention System*) sustava implementiranog na vatrozidu nove generacije.
7. Za objavu javno dostupnih usluga mora se koristiti balanser opterećenja (eng. *load balancer*) s *reverse proxy* funkcionalnošću.
8. Sva komunikacijska oprema mora podržavati neki oblik redundantnog načina rada.

4. Definiranje ključnih slabosti

Tvrtka svojim korisnicima garantira 99.9% dostupnost usluga na mjesečnoj razini. Tvrtka je imala problema s isporučivanjem usluga, obzirom da se radi o vrlo visokom postotku raspoloživosti koji pruža minimalan prostor za pogrešku. Da bi se osigurala od isplate penala zbog nepoštivanja ugovorenih obveza, tvrtka se odlučila za izgradnju *disaster recovery* rješenja. Kao ključni nedostaci trenutnog rješenja prepoznati su:

- **povezanost prema internetu**
- **nedostupnost pojedine usluge (aplikacije)**
- **katastrofalni događaj**

4.1. Povezanost prema internetu

Na lokaciji tvrtke nalaze se dva pružatelja internet usluge putem kojih je osigurana veza prema internetu. Obzirom da je usluga oba pružatelja realizirana putem iste fizičke veze (optičkog kabla), koji vodi do sjedišta tvrtke, u slučaju ispada fizičke veze tvrtka ostaje bez pristupa internetu, te samim time i mogućnosti isporučivanja usluge. Zbog tehničkih nedostataka, kojih su svjesni i sami pružatelji internet usluge, nemoguće je sklopiti odgovarajući SLA ugovor kojim bi se tvrtka osigurala u slučaju ispada veze prema internetu. Uzimajući u obzir navedeno, jedino prihvatljivo rješenje u slučaju ispada obje veze prema internetu tvrtka je pronašla u vidu *disaster recovery* lokacije.

4.2. Nedostupnost pojedine usluge (aplikacije)

Kako bi ispunila poslovne zahtjeve, tvrtka se čvrsto oslanja na korištenje informacijskih tehnologija. Redundancija infrastrukturnih komponenti informacijsko tehnološkog sustava svakako je preduvjet koji je potrebno ispuniti ukoliko se korisniku želi isporučiti visoko dostupna usluga. Informacijsko tehnološki sustav sastoji se od mnogo elemenata koji se mogu učiniti redundantnima i čiju dostupnost se može nadzirati, ali u ovom radu fokus se stavlja na aplikacije kao jedan od najvažnijih dijelova sustava čija je nedostupnost generator značajnih gubitaka[4].

[4] https://smallbiztrends.com/2013/08/amazon-down-custom-error-page.html, veljača. 2018

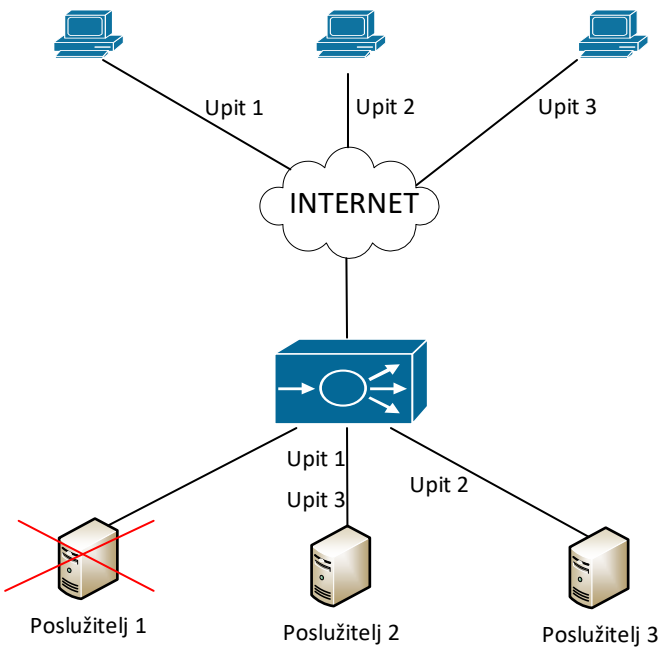
Kako bi se to osiguralo, potrebno je implementirati uređaj koji će posjedovati potrebnu logiku kojom bi ustanovio u kojem trenutku je određena usluga nedostupna na aplikativnoj razini. Uređaji koji su u stanju osigurati visoku dostupnost aplikacije nazivaju se **balanseri opterećenja.** Koristeći balanser opterećenja, klijentske upite moguće je usmjeravati prema određenim poslužiteljima, na temelju višestrukih kriterija, kao što su:

- **dostupnost aplikacije –** koristeći razne metode za provjeru zdravlja (eng. *health check*) određene aplikacije, klijentske upite moguće je usmjeriti na odgovarajuće poslužitelje ovisno o dostupnosti aplikacije koja se na istome izvršava. Neke od dostupnih opcija za provjeru zdravalja aplikacije uključuju: **ping, HTTP** (eng. *HyperText Transfer Protocol*) **konekciju, TCP** (eng. *Transmission Control Protocol*) ***konekciju,* DNS** (eng. *Domain Name System*) **upit, SMTP** (eng. *Simple Mail Transfer Protocol*) i sl. Prilikom odabira pojedine opcije važno je voditi računa o implementaciji iste i aplikaciji koja se provjerava. Npr. ukoliko se **ping** odabere kao opcija za provjeru zdravlja HTTP aplikacije, poslužitelj koji poslužuje HTTP aplikaciju može odgovarati na ICMP (engl. *Internet Control Message Protocol*) upite, dok sama aplikacija može biti nedostupna. S druge strane, ukoliko se uzme za primjer HTTP aplikacija i ovoga puta se za provjeru zdravlja postavi opcija HTTP konekcija, implementacija opcije može očekivati HTTP kod **„200 OK“** kako bi se aplikacija smatrala dostupnom, dok sama aplikacija na isti upit može odgovoriti nekim drugim HTTP kodom.
- **broj uspostavljenih konekcija –** klijentski zahtjevi usmjeravaju se ovisno o broju istovremeno uspostavljenih konekcija na određenom poslužitelju. Ovo je ujedno i najpopularnija metoda ukoliko se radi o DNS prometu ili aplikacijama temeljenim na *Web* tehnologijama. Uređaj mora pohranjivati informacije o broju aktivnih konekcija svakog poslužitelja unutar farme kako bi ova metoda bila uspješna,.
- **težinska (ponderirana) distribucija -** ovisno o performansama određenog poslužitelja, svakome se dodjeljuje težinska vrijednost te se na temelju nje klijentski zahtjevi usmjeravaju prema poslužitelju. Npr. ukoliko poslužitelj *x* ima 4x bolje performanse od poslužitelja *y,* poslužitelj *x* će posluživati 4x više zahtjeva naspram poslužitelja *y*.
- **vrijeme odgovora –** ovisno o vremenu koje je potrebno određenom poslužitelju da odgovori na upit, balanser opterećenja prosljeđuje zahtjeve prema poslužitelju s najboljim (najbržim) vremenom odgovora. Zbog kompleksnosti vezane uz proračun

vremena koji uvelike ovisi o vrsti aplikacije koja se poslužuje, ovo metoda se rijetko kad koristi.

- **geografska lokacija –** uređaji koji podržavaju tzv. GSLB (eng. *Global Server Load Balancing*) funkcionalnost u mogućnsti su proslijediti upit prema poslužitelju koji se nalazi na geografskom području koje je najbliže izvoru upita. Ova metoda uvelike se oslanja na imenički servis te u nekim specifičnim situacijama ne dovodi do očekivanih rezultata.

Aplikacija se uglavnom izvodi na dva ili više poslužitelja koji se još nazivaju i farma, a korisnički upiti se usmjeravaju na određene poslužitelje po unaprijed definiranom algoritmu. Dostupnost pojedine aplikacije moguće je ustanoviti generiranjem specifičnih upita prema istoj, te analizom povratnog odgovora. Ukoliko povratni odgovor izostane ili ne sadrži očekivane vrijednosti, poslužitelj se izbacuje iz farme te se daljnji upiti prosljeđuju na preostale poslužitelje. Nakon što se ustanovi da je izbačeni poslužitelj ponovno spreman posluživati klijente, isti se vraća u farmu te nastavlja s radom.



Slika 4.1 Usmjeravanje klijentskih upita prema poslužiteljima[5]

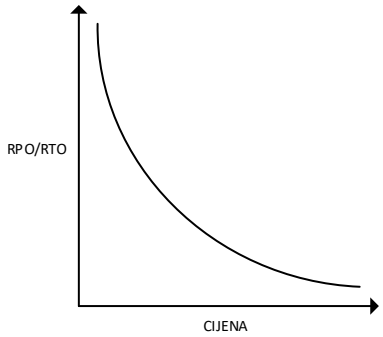
[5] Vlastiti rad autora

4.3. Katastrofalni događaj

Na primarnoj lokaciji tvrtke nalazi se redundantna veza prema internetu te su infrastrukturni elementi informacijsko tehnološkog sustava realizirani u visoko dostupnom načinu rada. Međutim, u slučaju katastrofalnog događaja poput potresa, poplave, požara i sl., kojim bi sustav mogao biti pogođen, tvrtka više nije u stanju isporučiti svoju uslugu korisnicima. Tvrtka se iz tog razloga odlučila za izgradnju *disaster recovery* rješenja koje će biti geografski dovoljno udaljeno od primarne lokacije kako ne bi bilo zahvaćeno istom katastrofom.

5. Disaster recovery rješenje

Prije donošenja odluke o *disaster recovery* rješenju, potrebno je provesti **analizu utjecanja na poslovanje** (eng. *business impact analysis*). Cilj analize utjecaja na poslovanje je ustanoviti koji su kritični poslovni procesi i koje su posljedice ukoliko poslovni procesi prestanu funkcionirati. Nakon prikupljenih informacija, potrebno je odrediti **maksimalno prihvatljivo vrijeme zastoja** (eng. *maximum tolerable downtime*). Maksimalno prihvatljivo vrijeme zastoja je suma **cilja vremena oporavka** (eng. *recovery time objective*) i **vrijeme rada oporavka** (eng. *work recovery time*). Što je vrijeme oporavka manje, to je cijena implementacije DR sustava veća.



Slika 5.1 Cijena sustava u odnosu na vrijeme oporavka[6]

Ovisno o prihvatljivom vremenu zastoja, potrebno je odabrati adekvatan tip lokacije za uspostavu DR rješenja. U slučaju katastrofe, različiti tipovi lokacija u mogućnosti su osigurati nastavak poslovanja u različitom vremenskom roku.

5.1. Općenito

Svako ozbiljnije planiranje koje uključuje upravljanje rizicima i planiranje nepredvidivih situacija (engl. *Contingency Planning)* mora uključivati plan kojim se pokriva katastrofalni događaj, unatoč činjenici da katastrofalni događaji nisu česta pojava. Obično taj plan podrazumijeva alternativnu lokaciju koja mora biti spremna posluživati korisnike na duži vremenski period u slučaju nedostupnosti primarne lokacije. *Disaster recovery* lokacija se može svrstati u jednu od sljedećih kategorija[7]:

[6] Vlastiti rad autora
[7] http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-34r1.pdf, veljača. 2018

- **dedicirana lokacija pod upravljanjem i u vlasništvu tvrtke**
- **uzajamni dogovor ili memorandum o suglasnosti s unutarnjim ili vanjskim entitetom**
- **iznajmljena lokacija**

Svaka od navedenih kategorija ima svoje prednosti i nedostatke. Međutim, za koju god opciju se tvrtka odluči, mora biti sigurna da će ispunjavati sve potrebne uvijete za funkcioniranje vitalnih procesa unutar tvrtke. Kategorije lokacija mogu se dodatno podijeliti ovisno o njihovoj spremnosti, vremenu potrebnom za realizaciju, složenosti implementacije i financijskom trošku. Uzevši u obzir spomenute faktore, lokacije se dodatno mogu svrstati u[8]:

- **Hladne** (engl. *Cold Sites*)
- **Tople** (engl. *Warm Sites*)
- **Vruće** (engl. *Hot Sites*)
- **Mobilne** (engl. *Mobile Sites*)
- **Zrcaljene** (engl. *Mirrored Sites*)

Hladna lokacija

Hladna lokacija je prazno postrojenje koje uključuje osnovne sadržaje kao što su: električne instalacije, povišeni podovi, odgovarajući klima uređaj, komunikacijske instalacije i sl. Obzirom da hladna lokacija najčešće ne sadrži potrebne uređaje ili oni nisu u funkciji, replikacija podataka s primarne lokacije nije moguća. U slučaju katastrofe tvrtka je dužna osigurati sve potrebne uređaje kako bi uspostavila razinu usluge jednaku ili približnu razini prije katastrofe. Prednost hladne lokacije je u minimalnim financijskim sredstvima koja je potrebno uložiti kako bi se realizirala.

Topla lokacija

Topla lokacija sadrži sve što je potrebno od električnih instalacija, uređaja, komunikacijskih instalacija i sl. kako bi se u slučaju katastrofe u što kraćem vremenskom razdoblju stavila u funkciju. U slučaju katastrofe najčešće postoji definirana procedura koju je potrebno slijediti za osposobljavanje lokacije. Procedura može sadržavati upute kao što su: osoba koju je potrebno kontaktirati u slučaju da je lokaciju potrebno aktivirati, potrebne korake za

[8] http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-34r1.pdf, veljača. 2018

uspostavljanje funkcionalnih komunikacijskih veza, procedura kojom se pokreću potrebne aplikacije i sl. Obzirom da je riječ o vrsti lokacije koja uglavnom nema uspostavljenu aktivnu komunikacijsku vezu s primarnom lokacijom, sigurnosne kopije podataka potrebno je ručno dostaviti na lokaciju. Koliko će podaci biti ažurirani ovisi o definiranom planu, tj. vremenu definiranom unutar **zadane točke oporavka** (eng. r*ecovery point objective*) kojom se definira prihvatljiva količina izgubljenih podataka.

Vruća lokacija

Vruća lokacija podrazumijeva prostor prikladne veličine koji je u slučaju katastrofe u mogućnosti podržati sve sistemske zahtjeve. Vruća lokacija sadrži svu potrebnu opremu za rad, infrastrukturu i pomoćno osoblje. Pomoćno osoblje je prisutno na lokaciji 24/7 i u slučaju aktivacije plana, započinje s potrebnim priprema.

Mobilna lokacija

Mobilna lokacija je samoodrživo postrojenje koje se nalazi unutar prikolice, pokretno je i u slučaju katastrofe može biti postavljeno na alternativnu lokaciju. Takvo postrojenje se obično iznajmljuje, te se oprema specifičnom opremom koja je prilagođena potrebama tvrtke. Oprema može uključivati: kuhinju, uredske prostore za određenu količinu ljudi, neprekidno napajanje, telekomunikacijsku i računalnu opremu i sl. Kako bi organizacija bila sigurna da je mobilna lokacija pouzdana i u slučaju katastrofe spremna za rad, potrebno je unaprijed dogovoriti sve detalje s proizvođačem vezane uz dizajn te potpisati SLA ugovor.

Zrcaljena lokacija

Zrcaljena lokacija podrazumijeva u potpunosti redundantno rješenje koje uključuje svu potrebnu opremu i replikaciju podataka u stvarnom vremenu (eng. *real-time*). Tvrtka je u mogućnosti nastaviti pružati uslugu s minimalnim ili zanemarivim zastojem u slučaju katastrofe. Iako s financijskog stajališta, zrcaljena lokacija zahtjeva najviše sredstava, za organizacije poput financijskih institucija, vladinih organizacija i pozivnih centara ne postoji pouzdanije rješenje zbog specifičnosti usluga koje pružaju svojim korisnicima.

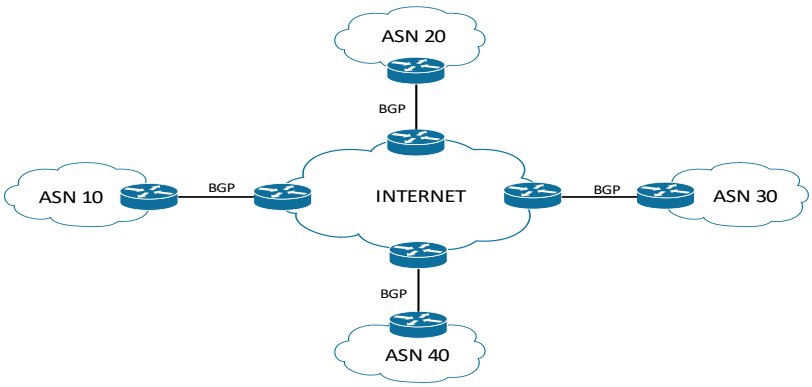
Zbog razlike u cijeni i spremnosti pojedinih lokacija, tvrtka bi trebala imati dobro razrađeni plan prije nego li se odluči za određenu opciju.

Potrebno je precizno definirati u kojem trenutku će se aktivirati sekundarna lokacija (ukoliko se ne radi o zrcaljenoj lokaciji). Obzirom na financijski trošak i resurse potrebne za aktivaciju sekundarne lokacije, tvrtka ne želi aktivirati sekundarnu lokaciju u slučaju manjeg zastoja.

Nameće se pitanje kojem trenutku bi trebalo aktivirati sekundarnu lokaciju? Ne postoji univerzalni odgovor na postavljeno pitanje već on ovisi o nekoliko faktora: maksimalnom vremenu prihvatljivog zastoja, prihodovnim gubicima koji će se generirati za vrijeme nedostupnosti usluge, te novčanom iznosu koji je potrebno izdvojiti za pokretanje sekundarne lokacije.

5.2. Dizajn i implementacija DR rješenja

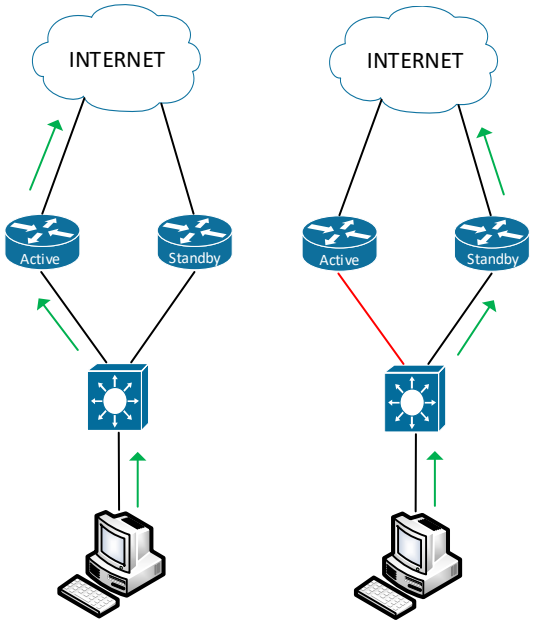
Primarna lokacija tvrtke obuhvaća usluge u vidu aplikacija koje se poslužuju krajnjim korisnicima putem interneta. Usluge su klasificirane kao kritični poslovni procesi čije je odvijanje potrebno osigurati i u slučaju katastrofe. Iz tog razloga potrebno je realizirati DR lokaciju koja će biti u mogućnosti osigurati podršku kritičnim poslovnim procesima za vrijeme nedostupnosti primarne lokacije. Za uspostavu DR rješenja, donesena je odluka o korištenju identičnog javnog raspon IP adresa, kako bi se izbjegli problemi s imeničkim servisom tj. pohranom (eng. *caching*) odgovara na klijentskoj strani. Ukoliko se želi omogućiti spomenuti dizajn potrebno je izvršiti određene manipulacije prilikom usmjeravanja prometa na internetu. Za tu svrhu potrebno je koristiti **BGP** (eng. *Border Gateway Protocol*) protokol obzirom da je jedini protokol koji se u vrijeme pisanja ovoga rada koristi za usmjeravanje prometa na internetu. Iako je u suradnji s pružateljem internet usluge moguće dogovoriti određene parametre usmjeravanja, u ovome slučaju to nije moguće iz razloga što tvrtka želi zadržati potpunu kontrolu nad svojim sustavom. Na DR lokaciji potrebno je uspostaviti BGP susjedski odnos s pružateljem internet usluge.



Slika 5.2 Prikaz BGP susjedskih odnosa na internetu[9]

[9] Vlastiti rad autora

Da bi se osigurala visoka dostupnost usluge, tj. veze prema internetu, potrebno je korištenje više uređaja i veza koje ih međusobno povezuju. Kako redundancija infrastrukturnih elemenata sustava ne bi postala problem, potrebno je korištenje protokola koji će nadzirati rad samih uređaja. Različiti uređaji, na različitim slojevima OSI (eng. *Open System Interconnection*) modela koriste različite protokole koji im omogućavaju redundantan način rada. Kako bi se osigurala redundancija *gatewaya* unutar sustava, potrebno je konfigurirati jedan od dostupnih FHRP (eng. *First Hop Redundancy Protocol*) protokola. Obzirom da se na primarnoj lokaciji tvrtke već koristi **HSRP** (eng. *Hot Standby Routing Protocol*) protokol, zbog unificirane konfiguracije i poslovnih zahtjeva, na DR lokaciji će se također konfigurirati HSRP protokol. U slučaju ispada aktivnog uređaja, uređaj u pripravnosti preuzima glavnu ulogu te nastavlja pružati izlaz prema internetu.



Slika 5.3 HSRP - prikaz toka prometa nakon ispada aktivnog usmjernika[10]

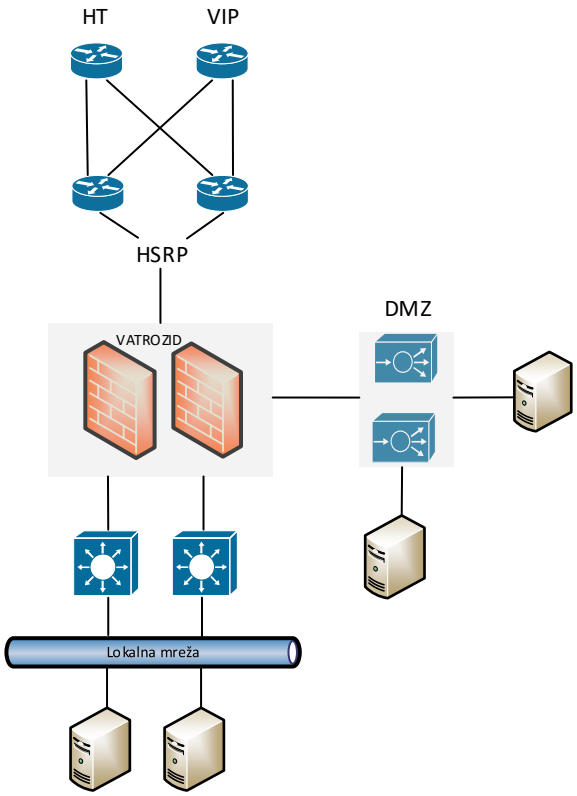
Da bi tvrtka bila u mogućnosti poštovati ugovorne obveze kojima garantira dostupnost svojih usluga na razini od 99.9%, potrebno je implementirati uređaj koji će moći nadgledati dostupnost pojedine aplikacije. Prilikom dizajna DR lokacije, potrebno je voditi računa o implementaciji **balansera opterećenja** kao jednom od ključnih elemenata sustava.

Obzirom da je riječ o uslugama koje tvrtka isporučuje svojim korisnicima putem interneta, visoka dostupnost javnog imeničkog poslužitelja mora biti osigurana, te je zbog toga na DR

[10] Vlastiti rad autora

lokaciji potrebno implementirati **sekundarni imenički poslužitelj**. Imenički poslužitelj sadržavat će kopiju primarne zone te ujedno biti autoritativan poslužitelj za zonu čiju kopiju posjeduje.

Obzirom da je sigurnost cjelokupnog sustava iznimno važna, za kontrolu vanjskog i unutarnjeg prometa na perimetru mreže potrebno je implementirati **vatrozid nove generacije**. Osim za kontrolu prometa, on će biti zadužen za zaštitu od malicioznih prijetnji s interneta koristeći antivirusnu te IPS (eng. *Intrusion Prevetion System*) zaštitu i za uspostavu sigurnosnog komunikacijskog kanala (tunela) putem kojeg će se odvijati komunikacija prema primarnoj lokaciji.



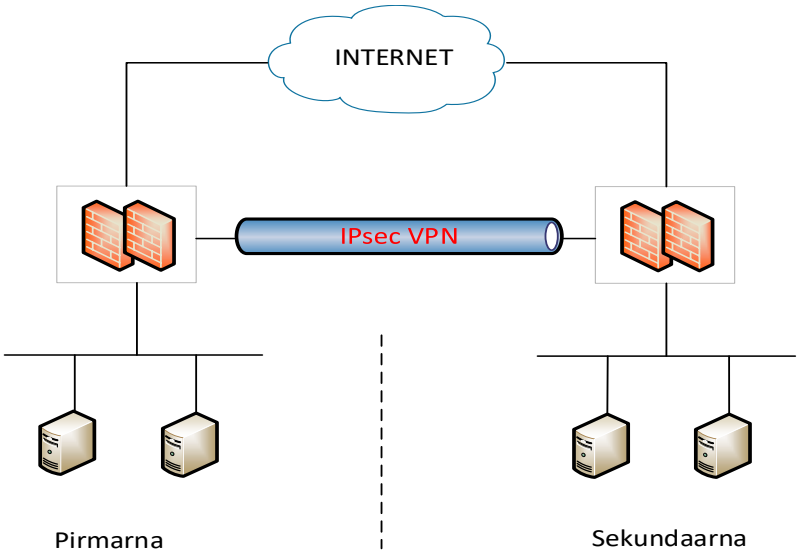
Slika 5.4 Shematski prikaz DR sustava[11]

5.3. Povezanost prema primarnoj lokaciji

Odabir tehnologije i/ili transportnog mehanizma za povezivanje primarne i sekundarne lokacije uvelike ovisi o raspoloživim sredstvima, potrebama organizacije, udaljenosti

[11] Vlastiti rad autora

između lokacija koje se povezuju, broju lokacija, infrastrukturi koja ih povezuje, karakteristikama uređaja i sl. Povezivanje primarne i sekundarne lokacije bit će ostvareno putem ćIPsec-a (eng. *Internet Protocol Security*) tehnologija.



Slika 5.5 Povezanost prema primarnoj lokaciji[12]

Uzevši u obzir udaljenost između dviju lokacija, IPsec tehnologija odabrana je kao pouzdan, siguran te cjenovno najprihvatljiviji način povezivanja. Obzirom da je virtualnu privatnu mrežu koja povezuje udaljene lokacije potrebno terminirati na određenom uređaju, za tu potrebu koristit će se vatrozid nove generacije.

[12] Vlastiti rad autora

6. Analiza trenutnog tržišta vatrozida i njihove komparativne prednosti

Današnje tržište preplavljeno je proizvodima različitih proizvođača, stoga često nije jednostavno donijeti ispravnu odluku prilikom odabira optimalnog rješenja. Renomirani svjetski proizvođači kao što su: **Cisco, Palo Alto, Check Point i Fortinet** prilagođavaju se potrebama tržišta te nastoje biti konkurentni što u konačnici dovodi do ponude uređaja vrlo sličnih ili gotovo istih funkcionalnosti. Kako bi tvrtkama, inženjerima i svim ostalim zainteresiranim skupinama pružili uvid u trenutno stanje tržišta, upoznali ih s kvalitetom pojedinih uređaja i olakšali im odabir adekvatnog rješenja, organizacije poput Gartnera i NSS Labsa redovito provode analizu tržišta i testiranje uređaja, te objavljuju rezultate svojih istraživanja.

Da bi smanjile svoje troškove, povećale profit i u što većoj mjeri iskoristile dostupne resurse na svojim poslužiteljima, organizacije se sve više okreću rješenjima koje nude virtualizacijske tehnologije. Kako cijene usluga u oblaku (eng. *cloud services*) postaju sve pristupačnije, sve veći broj organizacija se odlučuje na potpunu ili djelomičnu migraciju svojih usluga u oblak. Upravo iz tih razloga današnji proizvođači vatrozida, uz standardnu ponudu hardverskih uređaja (eng. *hardware appliance*), svakako bi trebali nuditi i virtualizacijsko rješenje koje je moguće implementirati na neke od najpoznatijih virtualizacijskih platformi, kao što su: **VMware, Hyper-V, KVM.**

Kroz svoju dugu povijest postojanja vatrozidi su proživjeli nekoliko faza razvoja. Prošla su vremena kada se od vatrozida očekivalo da besprijekorno obavlja svoju funkciju isključivo na nižim slojevima OSI modela, poput trećeg i četvrtog sloja. U današnje vrijeme kada se susrećemo sa sve većom stopom kibernetičkog kriminala, sve sofisticiranijim tehnikama napada na računalne sustave, sve većim brojem malicioznih programa i nizom ostalih prijetnji, potrebno je više nego ikada posjedovati kvalitetno sigurnosno rješenje. Kako bi pokušali odgovoriti na ranije spomenute prijetnje vatrozidi su morali evoluirati u današnje proizvode koji se nazivaju **vatrozidi nove generacije**. Vodeći računa o svemu ranije spomenutom, svaki ozbiljniji proizvođač vatrozid opreme morao bi nuditi proizvode koji uključuju sve funkcionalnosti vatrozida nove generacije. Konkretno, vatrozidi nove generacije svakako bi trebali uključivati sljedeći set funkcionalnosti:

- **Antivirusna zaštita –** sprječava prodor malicioznih aplikacija poput: virusa, crva, trojanskog konja, špijunskog softvera, ucjenjivačkog softvera i sl. u unutarnju mrežu.
- ***Web* zaštita –** kontrola pristupa Internet stranicama koje korisnici posjećuju. Ova funkcionalnost podrazumijeva filtriranje sadržaja na temelju određenih kategorija kao što su: pornografija, alkohol, droga, oružje, društvene mreže i sl.
- **Kontrola aplikacija –** uključuje prepoznavanje i kontrolu aplikacija na temelju poznatih, unaprijed definiranih potpisa (eng. *signatures*).
- **Zaštita od upada** (engl. *Intrusion protection*) – zaštita od vanjskih upada koristeći poznate propuste unutar aplikacija. Temeljem unaprijed definiranih potpisa, poseban modul unutar vatrozida pretražuje određene uzorke u prometu te u slučaju detekcije poznatih, malicioznih uzoraka, filtrira promet.
- **Sprječavanje curenja podataka** – sprječavanje curenja osjetljivih podataka van organizacije, pomoću ručno definiranih uzoraka podataka, unutar prometa koji se pretražuje.

Kako bi se osigurala što veća zaštita korisnika na internetu, sve više prometa biva kriptirano snažnim enkripcijskim algoritmima. Iako je u većini slučajeva ovakav, kriptirani način komunikacije poželjan, u nekim slučajevima promet je ipak potrebno dekriptirani na putu prema destinaciji. Npr., ukoliko tvrtka želi primijeniti sigurnosnu politiku, kojom će zabraniti pristup društvenim mrežama svim zaposlenicima unutar radnog vremena ili pak želi spriječiti pristup određenom sadržaju, ukoliko je promet kriptiran, vatrozid nije u mogućnosti primijeniti sigurnosna pravila. Da bi tvrtka bila u mogućnosti provoditi sigurnosnu politiku, vatrozid mora imati mogućnost presretanja kriptiranog prometa, njegove dekripcije, primjene sigurnosnih pravila te ponovne enkripcije i slanja prema destinaciji. Mogućnost presretanja prometa i njegove dekripcije se naziva još i **SSL inspekcija**. Ovisno o veličini organizacije, ista može imati potrebu za implementacijom više od jednog vatrozida. Npr., u slučajevima gdje tvrtka zbog potreba poslovanja vrši svoju djelatnost u više gradova, država ili kontinenata. Kako bi upravljanje uređajima bilo što jednostavnije, proizvođači vatrozida morali bi nuditi rješenje pomoću kojeg je omogućeno **centralizirano upravljanje** uređajima. Obzirom da je riječ o sigurnosnim uređajima, čija je namjena zaštiti unutarnji dio mreže od zlonamjernih korisnika i provoditi sigurnosne politike organizacije, često se javlja potreba za analizom prometa i uvidom u informacije o tome tko je radio što na mreži. Kako bi bili u stanju isporučiti takve informacije, poželjno je da vatrozidi imaju implementiran kvalitetan sustav **zapisivanja događaja** (eng. *log recording*).

Sustav zapisivanja događaja trebao bi nuditi detaljne opcije pretraživanja te po mogućnosti **izradu izvještaja**. U većini slučajeva proizvođači vatrozida ipak ne nude mogućnost izrade izvještaja na samom uređaju, već u ponudi imaju specijalizirane uređaje za takvu namjenu. Iako je često riječ o subjektivnom dojmu, sučelje kroz koje se vrši konfiguracija vatrozida trebalo bi biti jednostavno i intuitivno. Također, obzirom da je riječ o uređajima koji nude napredne mogućnosti i pregršt opcija, bilo bi poželjno da proizvođači izdaju što detaljniju dokumentaciju o radu svojih uređaja. Nakon provedene analize tržišta vatrozida, tablica niže sadrži popis dostupnih funkcionalnosti za pojedine modele uređaja.

NAZIV FUNKCIONALNOSTI	**UREĐAJ**			
	Fortigate 200E	**ASA 5545-X w/FirePOWER**	**Palo Alto PA-5020**	**Check Point 5100**
Virtualizacija	✓	✓	✓	✓
Next Generation Firewall	✓	✓	✓	✓
Antivirusna zaštita	✓	✓	✓	✓
Web zaštita	✓	✓	✓	✓
Kontrola aplikacija	✓	✓	✓	✓
Zaštita od upada	✓	✓	✓	✓
Sprječavanje curenja podataka	✓	✘[7]	✓	✓
SSL inspekcija	✓	✓	✓	✓
Centralizirano upravljanje	✘[13]	✓	✘[7]	✓
Izrada izvještaja	✘[7]	✓	✓	✓
Jednostavno upravljanje	✓	✘[14]	✓	✓

Tablica 6.1 Usporedba funkcionalnosti između pojedinih modela vatrozida

[13] Potreban dodatan uređaj
[14] Subjektivan dojam donesen na temelju iskustva u radu s konkurentnim proizvodima

6.1. Odabir vatrozida

Tvrtka bi trebala imati jasnu viziju o tome na koji način će koristiti vatrozid, prije nego li se odluči za njegovu nabavku. Iako vatrozidi nove generacije nude mnoštvo funkcionalnosti koje bi trebalo implementirati unutar tvrtke, omogućavanjem svih opcija drastično se narušavaju performanse uređaja. Obzirom da je vatrozid uređaj koji će tvrtka u većini slučajeva koristiti na rubu svoje mreže (prema internetu), svakako treba voditi računa o propusnosti internet veze i performansama samog uređaja. Drugim riječima, uređaj bi trebao imati dovoljnu propusnost, tj. trebao bi odgovarati propusnosti internet veze.

Također, valjalo bi obratiti pozornost na broj korisnika koji se štiti. Podaci kao što su broj istovremenih konekcija i broj novih konekcija, direktno su povezani s brojem korisnika koji se nalaze iza vatrozida. Osim zaštite samih korisnika, vatrozid se često koristi za uspostavljanje virtualne privatne mreže prema udaljenim lokacijama. Uz to, udaljenim korisnicima koji imaju potrebu pristupiti internim resursima, putem javne, nesigurne mreže, vatrozid će omogućiti uspostavu sigurnosnog - kriptiranog tunela. Imajući na umu sve ranije spomenuto, svakako bi trebalo odabrati rješenje koje nudi opciju redundantnog načina rada, te dodatnog izvora napajanja.

Za potrebe implementacije DR rješenja, tvrtka će koristiti vatrozid za uspostavu sigurnosnog tunela prema primarnoj lokaciji. Kako bi zaštitili poslužitelje od malicioznih prijetnji s interneta, promet koji putuje prema internom te demilitariziranom dijelu mrežu podliježe antivirusnoj i IPS inspekciji. Prilikom odabira vatrozid rješenja, posebnu pažnju treba obratiti na propusnost IPsec VPN prometa, te propusnost s konfiguriranom antivirusnom i IPS inspekcijom.

U tablici niže moguće je pronaći usporedne performanse između pojedinih modela vatrozida koji odgovaraju potrebama implementacije[15].

[15] Polje koje sadrži vrijednost „-„ nije navedeno u dokumentaciji proizvođača ili je navedeno s različitom kombinacijom uključenih opcija od ostalih proizvoda u tablici

NAZIV FUNKCIONALNOSTI	**UREĐAJ**			
	Fortigate 200E[16]	**ASA 5545-X w/FirePOWER[17]**	**Palo Alto PA-5020[18]**	**Check Point 5100[19]**
Propusnost vatrozida	20 / 20 / 9 Gbps[20]	-	-	14.5 Mbps[21]
Propusnost s uključenom kontrolom aplikacija	-	1.5 Gbps	5 Gbps	-
Propusnost s uključenom kontrolom aplikacija i IPS zaštitom	-	1 Gbps	-	2.2 Gbps
Stateful propusnost (maksimalno)[22]	-	3 Gbps	-	-
Stateful propusnost (kombinacija protokola)[23]	-	1.5 Gbps	-	-
Broj istovremenih konekcija	2 miliona	750 000	1 milion	3.2/6.4 miliona[24]
Broj novih konekcija/s	135 000	30 000	120 000	110 000
IPsec VPN propusnost	9 Gbps[25]	400 Mbps[26]	2 Gbps	1.6 Gbps
IPS propusnost	6 / 2.2 Gbps[27]	-	-	2.45 Gbps
Propusnost SSL inspekcije	1 Gbps (IPS, HTTP)[28]	-	-	-

[16] https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiGate_200E_Series.pdf
[17] https://www.cisco.com/c/en/us/products/collateral/security/asa-5500-series-next-generation-firewalls/datasheet-c78-733916.html
[18] https://www.paloaltonetworks.com/products/secure-the-network/next-generation-firewall/pa-5000-series
[19] https://www.checkpoint.com/downloads/product-related/datasheets/ds-5100-appliance.pdf
[20] Paketi veličine 1512/512/64 bajtova UDP
[21] Maksimalna propusnost dobivena mjerenjem UDP veličine 1518 bajtova
[22] Maksimalna propusnost dobivena mjerenjem UDP prometa u idealnim uvjetima
[23] Uglavnom aplikacije koji koriste TCP protokol: HTTP, SMTP, FTP, IMAPv4, BitTorrent
[24] Maksimalne vrijednosti s osnovnom/maksimalnom memorijom
[25] Paketi veličine 512 bajtova
[26] 3DES/AES
[27] Optimalan promet/*Enterprise* mješoviti promet s uključenim NGFW funkcionalnostima i zapisivanjem događaja
[28] SSL VPN test propusnosti koristeći TLSv1.2 s AES128 – SHA256

NGFW propusnost	1.8 Gbps[29]	-	2 Gbps	1.34 Gbps[30]
Mogućnost uparivanja u klaster	✓	✓	✓	✓
Redundantno napajanje	✓[31]	✗	✓	✗

Tablica 6.2 Usporedba performansi vatrozida

Za potrebe ove implementacije, odabran je uređaj Fortigate 200E na temelju povoljnije cijene[32] u usporedbi s konkurencijom te na temelju iskustva u radu na navedenom proizvodom.

6.2. Funkcija vatrozida u kontekstu implementacije DR rješenja

Mreža će se segmentirati na javni i unutarnji dio mreže na DR lokaciji tvrtke. Dodatno, za objavu javno dostupnih usluga i DNS poslužitelja zaduženog za javni imenički prostor, implementirat će se demilitarizirana zona kao zaseban mrežni segment. Različiti dijelovi mreža (javni dio, DMZ te unutarnji dio) povezani su vatrozidom koji primjenom sigurnosnih pravila štiti DMZ i unutarnji dio mreže od malicioznih prijetnji s interneta.

Da bi komunikacija između primarne i sekundarne lokacije bila moguća, potrebno je uspostaviti virtualnu privatnu mrežu. Virtualna privatna mreža omogućava komunikaciju putem logičke veze (tunela). Koristeći snažne enkripcijske algoritme, vatrozid osigurava tajnovitost i integritet podataka koji se prenose unutar tunela putem javne, nesigurne mreže. U slučaju ispada usluge na primarnoj lokaciji, promet se preusmjerava putem tunela do poslužitelja koji se nalaze na DR lokaciji. Ukoliko primarna lokacija postane u potpunosti nedostupna te se usluga počne isporučivati isključivo putem DR lokacije, poslužiteljima koji se nalaze na DR lokaciji potrebno je osigurati pristup prema internetu. Omogućavanje

[29] NGFW funkcionalnost mjerena s uključenim vatrozidom, IPS te Kontrolom aplikacija
[30] Uključuje propusnost: Vatrozida, Kontrole aplikacija, filtriranje *Web* stranica, IPS, antivirus, A*nti-Bot, SandBlast*
[31] Opcionalno
[32] Dobivene projektne cijene uređaja od strane proizvođača opreme nije moguće javno iznijeti

pristupa internetu osigurat će vatrozid, koji za te potrebe obavlja funkciju prevođenja privatnih IP adresa u javne (eng. *Network Address Translation*).

7. Implementacija rješenja

7.1. Konfiguracija usmjernika

Usmjernici R2 i R5 koriste dva sučelja za povezivanje prema internetu. Jedno sučelje se koristi za vezu prema pružatelju usluga HT-u, dok se drugo koristi za vezu prema VIP-u. Na oba usmjernika podešene su javne IP adrese dodijeljene od strane pružatelja internet usluge i to na način da je svakom usmjerniku dodijeljena jedna, ali različita IP adresa. Različite IP adrese potrebno je koristiti kako bi svaki usmjernik bio u mogućnosti uspostaviti BGP susjedski odnos s HT-om, odnosno VIP-om. Ovo je iznimno važno iz razloga što BGP protokol za komunikaciju koristi TCP na portu 179. U slučaju ispada primarnog usmjernika, ukoliko ne postoji TCP konekcija s drugim usmjernikom, BGP susjedski odnos će se raskinuti.

BGP protokol koristi se za oglašavanja javnog raspona IP adresa prema internetu. Obzirom da postoje dvije veze prema internetu, kako bi se omogućila komunikacija isključivo putem primarne, HT veze, za cijelo vrijeme njezine dostupnosti, ali isto tako i spriječila sva komunikacija prema DR lokaciji za vrijeme dostupnosti primarne lokacije, potrebno je izvršiti određene konfiguracijske prilagodbe prilikom oglašavanja javnog raspona. Prema HT vezi pridodaje se AS_PATH prefiks, kako bi se promet prema javnom rasponu tvrtke uvijek usmjeravao prema primarnoj lokaciji, za cijelo vrijeme njezine dostupnosti. Isto tako, AS_PATH prefiks pridodaje se prema VIP vezi, ali s većim popisom prefiksa. Na taj način u slučaju ispada primarne lokacije, povratni promet će se usmjeravati na DR lokaciju, ali isključivo putem preferirane HT veze, za cijelo vrijeme njezine dostupnosti. Za usmjeravanje odlaznog prometa koriste se plutajuće (eng. *floating*) statičke putanje. Putanja prema HT vezi ima bolju administrativnu distancu (eng. *administrative distance*) za razliku od VIP veze, te se na taj način odlazni promet usmjerava preferiranom komunikacijskom vezom.

Prema unutarnjem dijelu mreže konfiguriran je HSRP protokol kako bi se osigurala redundancija *gatewaya*. Kako bi se osigurao pristup prema internetu u slučaju ispada pojedine veze na aktivnom ili pasivnom usmjerniku, potrebno je konfigurirati nadgledanje sučelja. Sučelja koja se nadgledaju su ona prema internetu, ali isto tako i ono prema unutarnjem dijelu mreže. U slučaju ispada pojedinog sučelja, aktivni usmjernik spušta svoj prioritet za 20, što je dovoljno da pasivni usmjernik preuzme glavnu ulogu. Primarni

usmjernik ima konfiguriran prioritet u iznosu od 110 za razliku od pasivnog čija vrijednost iznosi 100.

Za uspostavu IPsec tunela s primarnom lokacijom koriste se javne IP adrese dodijeljene od strane pružatelja internet usluge. Kako bi se IPsec tunel uspostavio, na usmjernicima je potrebno konfigurirati prevođenje IP adresa (eng. *Network Address Translation*) za promet namijenjen prema vatrozidu. Potrebno je koristiti statičko prevođenje (eng. *Static Network Address Translation*) IP adresa da bi udaljeni uređaj bio u mogućnosti uspostaviti komunikaciju prema vatrozidu,. Nakon što se konfigurira statičko prevođenje, usmjernik podatke o prevođenju sprema u translacijsku tablicu (eng. *Network Address Translation table*) te na taj način omogućava uspostavu dolaznih konekcija. Ovakvo prevođenje se razlikuje u odnosu na dinamičko prevođenje IP adresa pri kojem je komunikaciju moguće inicirati isključivo iz unutarnjeg dijela mreže.

Nakon što se konfigurira statičko prevođenje na usmjernicima R2 i R5, oba usmjernika se ponašaju na način kao da im je adresa korištena za prevođenje dodijeljena na vanjskom sučelju. Iako je ovakav način ponašanja nužan kako bi se omogućila uspostava konekcije na vanjskom sučelju prema unutarnjem dijelu mreže, u slučaju kada postoje redundantni uređaji i kada su priključeni na isti mrežni segment, dolazi do konflikta. Naime, prilikom ARP (eng. *Address Resolution Protocol*) rezolucije, oba usmjernika će odgovarati na ARP upite, te na taj način narušiti normalno funkcioniranje sustava. Da bi se spriječili neželjeni efekti, a omogućila redundancija usmjernika, potrebno je konfigurirati prevođenje IP adresa u suradnji s HSRP protokolom. Nakon što se konfiguriraju potrebni parametri, usmjernik će koristiti nešto drukčiju logiku te će na ARP upite za prevedenim IP adresama odgovarati samo aktivni usmjernik.

Kako bi se osigurala visoka dostupnost usluge u slučaju ispada pojedinih veza na primarnoj i sekundarnoj lokaciji, potrebno je omogućiti uspostavu IPsec tunela između HT → HT te VIP → VIP veze na primarnoj i sekundarnoj lokaciji, ali isto tako između HT → VIP te VIP VIP → HT veze. U tu svrhu su korištene dodatne IP adrese na HT, odnosno VIP sučeljima koje služe isključivo za uspostavu IPsec tunela između različitih veza na primarnoj i sekundarnoj lokaciji. Međutim, prilikom prevođenja IP adresa potrebno je konfigurirati dodatnu logiku kako se promet u slučaju ispada pojedine veze ne bi na putu prema destinaciji preveo u pogrešnu IP adresu. Stoga, na usmjernicima R2 i R5 konfigurirane su pristupne liste (eng. *access-list*) kojima se određuje izvor i destinacija prometa, te se korištenjem *route-map-a* određuje izlazno sučelje prilikom prevođenja IP adresa.

7.2. Konfiguracija balansera opterećenja

Na DR lokaciji tvrtke nalaze se dva balansera opterećenja konfigurirana za visoko dostupan način rada. U slučaju ispada aktivnog balansera opterećenja, pasivni preuzima glavnu ulogu. Uređaji su smješteni u demilitariziranom segmentu mreže te se nalaze iza vatrozida koji im ujedno služi kao izlaz prema ostalim mrežama i internetu. Konfigurirani su virtualni servisi s pripadajućim adresama i portovima koji služe za prihvat dolaznih upita. Svakom virtualnom servisu dodijeljene su odgovarajuće postavke za provjeru zdravlja poslužitelja, odnosno aplikacija i dodijeljeni su im odgovarajući pravi poslužitelji (eng. *real server*) koji su dio farme.

Za provjeru zdravlja imeničkog poslužitelja koristi se upit za rezolucijom *www.visokadostupnost.hr* zapisa, a kao algoritam za prosljeđivanje novih upita koristi se broj uspostavljenih konekcija. Za usluge koje se nude u vidu HTTP aplikacija, konfiguriran je mehanizam provjere zdravalja u vidu HTTP HEAD upita, a kao algoritam za prosljeđivanje novih upita koristi se *round-robin*.

Jedno od osnovnih pravila prilikom korištenja balansera opterećenja je da se svi upiti proslijeđeni prema balanseru opterećenja moraju vratiti prema balanseru opterećenja prije nego li se odgovor isporuči pošiljatelju, stoga je na balanseru opterećenja konfigurirana opcija prevođenja izvorne IP adrese (eng. *Source Network Address Translation*), te isključena opcija transparentnosti na razini virtualnog servisa. Takvom konfiguracijom dolazni upiti na strani poslužitelja biti će vidljivi kao da im je izvor balanser opterećenja, te će odgovor biti proslijeđen prema balanseru opterećenja čime je zadovoljeno ranije spomenuto pravilo.

7.3. Konfiguracija vatrozida

Dva vatrozida konfigurirana su u visoko dostupnom načinu rada. Vatrozid je postavljen između vanjske mreže, unutarnje te demilitarizirane zone. Na vanjskom sučelju vatrozida postavljena je javna IP adresa koja je dodijeljena tvrtki na korištenje te se preklapa s adresom na primarnoj lokaciji. Osim provođenja sigurnosnih politika kojima se štiti unutarnja mreža, jedna od glavnih zadaća vatrozida je uspostava sigurnosnog tunela prema primarnoj lokaciji.

Za uspostavljanje kriptiranog tunela s primarnom lokacijom, potrebno je konfigurirati IP adresu uređaja koji će se koristiti za terminiranje tunela. Uzevši u obzir da primarna lokacija

ne može uspostaviti vezu sa sekundarnom lokacijom zbog ranije opisanih problema s korištenjem javnog raspona IP adresa, te utjecaja na povratni promet prema javnom rasponu tvrtke, potrebno je uspostaviti tunel prema dodatnim, javnim IP adresama dodijeljenima od strane pružatelja internet usluge. Obzirom da se uređaji zaduženi za terminiranje tunela nalaze iza usmjernika kojem su dodijeljene javne IP adrese na HT, odnosno VIP sučelju i koji je zadužen za prevođenje IP adresa prema primarnoj destinaciji, potrebno je koristiti opciju zaobilaženja translacije, odnosno NAT-T (eng. *NAT traversal*).

Kako bi se osigurala visoka dostupnost sustava u slučaju ispada bilo koje veze na primarnoj ili sekundarnoj lokaciji, na svakom vatrozidu potrebno je podesiti 4 tunela (ukupno 8). S druge strane, da bi se tunel mogao uspostaviti, potrebno je koristiti dvije javno dostupne adrese na svakom sučelju (prema HT i prema VIP) koje će biti rezervirane samo za vatrozid. Za ovu potrebu, na svakom usmjerniku su konfigurirana statička mapiranja potrebnih adresa, te pravilo kojim se definira u kojem trenutku i za koji promet se mapiranje izvodi. U sljedećoj tablici prikazan je rezultat prevođenja IP adresa u odnosu na destinacijsku adresu s kojom se pokušava uspostaviti tunel.

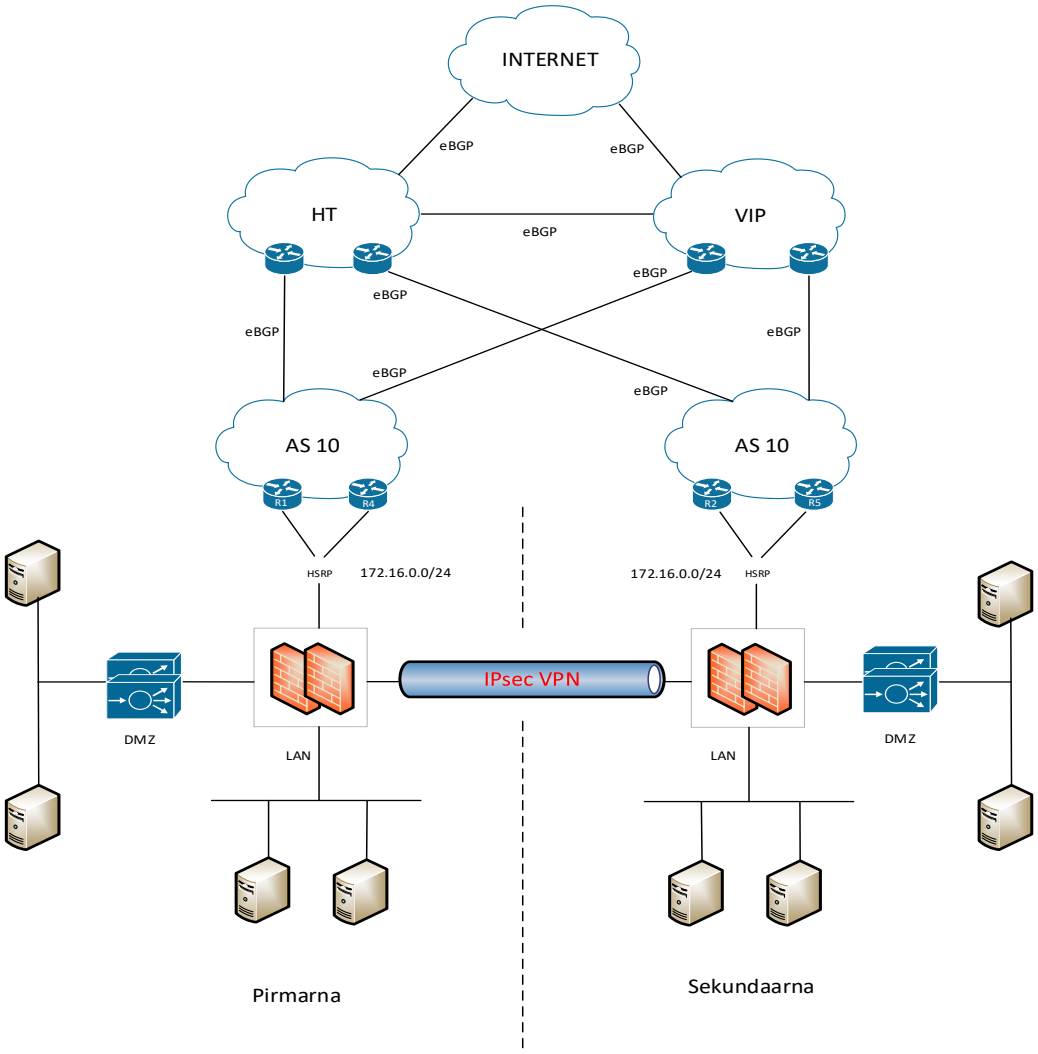
ID	Izvor	Destinacija	Veza
1	192.168.30.100	192.168.10.100	HT → HT
2	192.168.40.100	192.168.20.100	VIP → VIP
3	192.168.30.101	192.168.20.101	HT → VIP
4	192.168.40.101	192.168.10.101	VIP → HT

Tablica 7.1 Prikaz IP adresa za uspostavu IPsec tunela

U trenutku dostupnosti svih veza, moguće je uspostaviti 2 tunela istovremeno zbog postavki i pravila koji se primjenjuju za prevođenje IP adresa. Prilikom ispada pojedine veze (HT ili VIP), moguće je ostvariti komunikaciju putem HT → VIP ili VIP → HT veze. Kako bi se omogućila komunikacija putem preferirane putanje, na vatrozidu je konfigurirana usmjernička tablica kojom se daje prednost putanji putem HT veze. U slučaju nedostupnosti tunela putem HT veze, promet se preusmjerava na alternativni tunel koji je podignut putem VIP veze. Da bi se osigurala što veća dostupnost putem tunela, dodatno su modificirana

vremena detekcije nedostupnog susjeda. Izostankom potrebnog paketa (poruke) u vremenskom intervalu od 5 sekundi, susjed se smatra nedostupnim te se onemogućava komunikacija putem dotičnog tunela. Adrese javno dostupnih usluga objavljene su na vatrozidu, te se nakon dolaznog upita prosljeđuju prema uređaju zaduženom za balansiranje opterećenja. Kako bi se sustav zaštitio od malicioznih napada, promet prema DMZ poslužiteljima i prema internetu podliježe antivirusnom i IPS skeniranju. Kako bi se poslužiteljima osigurao pristup prema internetu, na vatrozidu su podešena pravila za prevođenje IP adresa.

8. Analiza izvedenog stanja



Slika 8.1 Shematski prikaz sustava[33]

Dva neovisna pružatelja internet usluge osiguravaju pristup internetu na DR lokaciji tvrtke. Zadaća dva postavljena usmjernika je oglašavanje javnog raspona adresa tvrtke i uspostava dvostrukog BGP susjedskog odnosa prema oba pružatelja internet usluge. Isti, javni raspon IP adresa koji je dodijeljen tvrtki koristi se na primarnoj i sekundarnoj lokaciji. Takav dizajn

[33] Vlastiti rad autora

ima prednosti, ali isto tako predstavlja i niz izazova. Primjerice, ukoliko primarna i sekundarna lokacija koriste različite raspone javnih IP adresa, te se usluga krajnjim korisnicima želi isporučivati isključivo putem primarne lokacije, imenički servis će vrlo vjerojatno predstavljati izazov. Uzmemo li za primjer korisnika koji pristupa sadržaju putem https://www.visokadostupnost.hr adrese, te za istu dobije odgovor da se nalazi na IP adresi 172.16.0.111 (primarna lokacija), klijent će rezultat pohraniti u internu memoriju. Jednako tako, svi imenički poslužitelji koji su dobili takav upit također će pohraniti rezultat kako bi brže odgovarali na buduće upite.

Ukoliko poslužitelj na navedenoj IP adresi u nekom trenutku postane nedostupan, a DNS zapis još uvijek nije istekao na klijentskom računalu ili na nekom od imeničkih poslužitelja, usluga će postati nedostupna. Dakako, postoji mogućnost da se imenički poslužitelj konfigurira na način da na željene upite prosljeđuje više odgovora. Situacija u kojoj se korisnik želi posluživati isključivo putem primarne lokacije, može predstavljati problem zbog načina na koji rade razni DNS *resolveri*. Druga opcija bi bila postaviti nižu vrijednost za zapis koji će klijenti ili imenički poslužitelji dobivati kao odgovor, no u slučaju postavljanja niskih vrijednosti dodatno se opterećuje imenički poslužitelj. S druge strane, ukoliko se koristi isti raspon javnih IP adresa na obje lokacije, usmjeravanje putem interneta može postati izazovno. Jedan od zahtjeva prilikom implementacije DR rješenja jest da obje lokacije budu povezane sigurnosnim – kriptiranim tunelom. U slučaju ispada pojedinog aplikativnog poslužitelja na primarnoj lokaciji, klijentski upiti i dalje će se posluživati putem primarne lokacije, međutim, potrebni podaci će se dohvaćati putem kriptiranog tunela s udaljene (DR) lokacije. Također, razni servisi zbog replikacijskih zahtjeva imaju potrebu komunicirati s primarnom lokacijom.

Kako bi se osigurala visoka dostupnost *gatewaya* (u ovom slučaju usmjernika) i omogućio pristup internetu, na usmjernicima je konfiguriran HSRP protokol. HSRP protokol je konfiguriran prema vatrozidu, te se nalazi na javnom segmentu mreže[34] kao što je prikazano na Slika 8.1 Shematski prikaz sustava. U slučaju ispada pojedinog usmjernika, drugi usmjernik preuzima aktivnu ulogu (eng. *active*) i nastavlja pružati izlaz prema internetu. Iako je svaki usmjernik povezan vezom i prema alternativnoj putanji (VIP), u slučaju ispada sučelja prema HT-u, aktivni usmjernik spušta svoj prioritet kako bi omogućio tok prometa

[34] Iako je riječ o privatnom rasponu IP adresa, koji je opisan RFC 1918 - https://tools.ietf.org/html/rfc1918 dokumentom, za potrebe ovoga rada, pretpostavit će se da je riječ o javno dostupnim IP adresama

putem preferirane putanje. Uloga usmjernika u ovom slučaju je i prevođenje IP adresa, stoga je na oba usmjernika potrebno konfigurirati identične postavke. Obzirom da se dva usmjernika nalaze na istom segmentu mreže, korištene su postavke koje omogućavaju prevođenje IP adresa u visoko dostupnom načinu rada prilikom korištenja HSRP protokola.

Prilikom uspostave BGP susjedstva, dogovorene su standardne vrijednosti brojača (eng. *timers*) u iznosu od 180, odnosno 60 sekundi. Ukoliko BGP susjed u zadanom vremenskom intervalu ne zaprimi kontrolni paket, pokreće se brojač (eng. *timer*). Nakon isteka vremena u kojem se susjed smatra dostupnim, sve putanje naučene putem nedostupnog susjeda brišu se iz usmjerničke tablice.

Balanser opterećenja koristi se i za objavu javno dostupnih usluga i na njemu su konfigurirane objave *Web* aplikacija te javno dostupnog imeničkog servisa. U slučaju ispada pojedinog poslužitelja na primarnoj lokaciji, promet se putem tunela preusmjerava prema poslužiteljima koji se nalaze na DR lokaciji i vrši se balansiranje prometa prema više poslužitelja koji se nalaze u farmi. Balanseri opterećenja konfigurirani su u visoko dostupnom načinu rada kako bi se sustav zaštitio od ispada pojedinog. Pasivni uređaj u slučaju ispada primarnog preuzima glavnu ulogu i nastavlja posluživati korisnike. Iako visoko dostupni, klaster u kojem su podešeni balanseri opterećenja štiti sustav od ispada pojedinog uređaja. Kako bi se osigurala maksimalna dostupnost u svim slučajevima, potrebno je implementirati mehanizam zaštite od ispada oba balansera opterećenja. Obično se ovakav način zaštite implementira koristeći GSLB (*Global Server Load Balancing*), međutim, zbog načina na koji je dizajniran sustav kojim se ovaj rad bavi, takva opcija nije moguća[35].

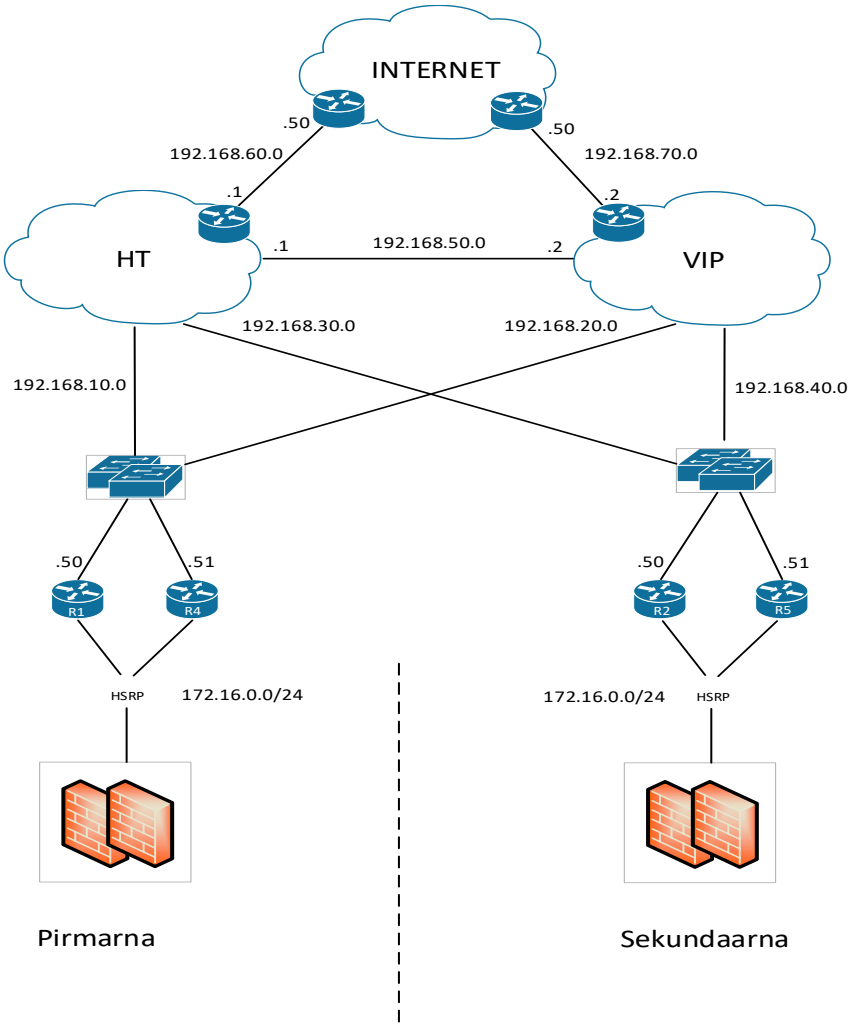
Prilikom korištenja ponešto drukčijeg dizajna, GSLB uređaj bi se instalirao na visoko dostupnu lokaciju (u ovom slučaju ne govorimo o sekundarnoj – DR lokaciji, već o lokaciji kao što je podatkovni centar) te bi nakon ispada pojedine aplikacije, na razini lokacije, promet preusmjeravao na alternativnu – DR lokaciju. Kako su za usmjeravanje prometa u ovome radu zaduženi usmjernici koji se nalaze na lokaciji tvrtke, te se na primarnoj i sekundarnoj lokaciji nalazi isti raspon javnih IP adresa, spomenuta metoda korištenja GSLB uređaja nije moguća.

[35] Iako je tehnički izvedivo, potrebni mehanizmi uključuju napredne opcije usmjeravanja prometa te provjere određenih parametara na usmjernicima koje za potrebe ove implementacije nisu korištene

Autoritativni imenički poslužitelj za javni imenički prostor tvrtke, nalazi se na primarnoj lokaciji. Dodatni, sekundarni poslužitelj postavljen je na DR lokaciju i sadrži kopiju primarne zone. Na autoritativnom poslužitelju za **.hr** javni imenički prostor, dodan je novi NS (*Name Server*) zapis koji pokazuje na poslužitelj koji se nalazi na DR lokaciji. Za sinkronizaciju primarne zone (eng. *Primary zone*) koristi ste kriptirani tunel.

9. Simulacija ispada primarne lokacije

Nakon završetka faze planiranja i implementacije sustava koji će se nalaziti na DR lokaciji, potrebno je izvršiti sva potrebna testiranja kako bi se utvrdilo da je novi sustav spreman za upotrebu u slučaju katastrofe. Završetak potrebnih testiranja i utvrđivanje da je sustav spreman za rad nikako ne bi trebao značiti da u budućnosti sustav nije potrebno podvrgnuti novim testovima. Pouzdan sustav može biti jedino onaj sustav čiji rezultati redovnog testiranja zadovoljavaju postavljene kriterije.



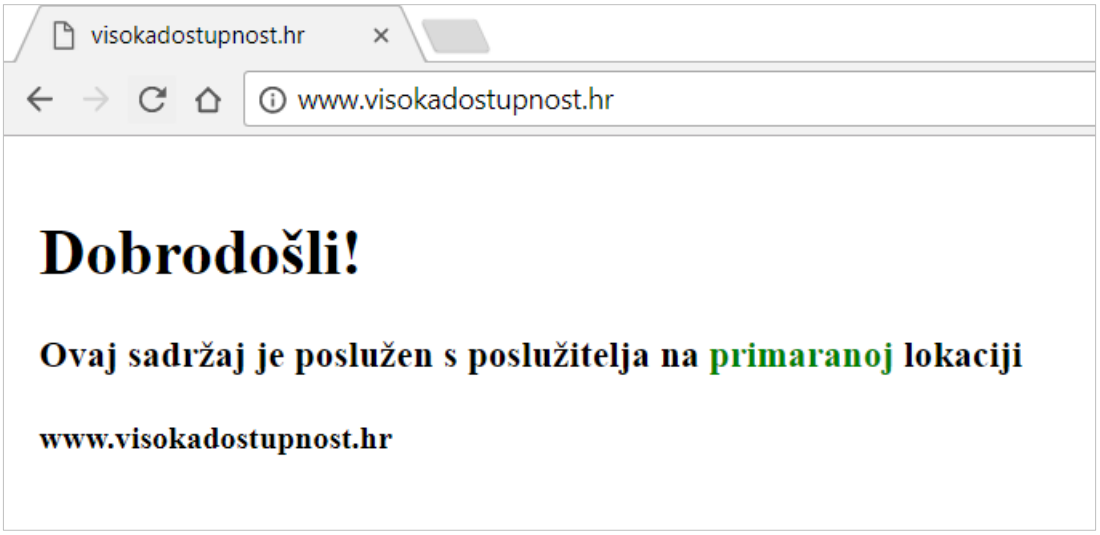
Slika 9.1 Shematski prikaz javne mreže[36]

[36] Vlastiti rad autora

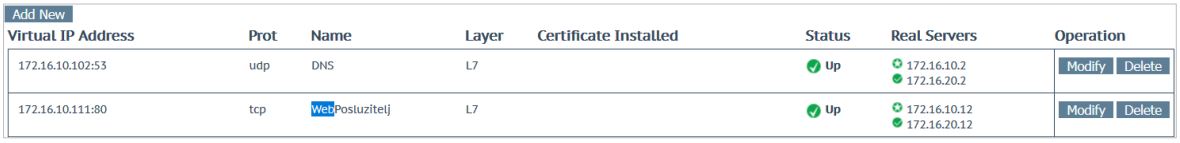
9.1. Ispad HT veze na primarnoj lokaciji

Cilj ovog testa je potvrditi funkcioniranje sustava u slučaju ispada HT veze na pojedinom usmjerniku te ispada HT veze na razini cijele lokacije. Simulacije će se obaviti jednostavnim isključivanjem sučelja, koje povezuje HT opremu s usmjernicima R1 i R4, kao što je prikazano na Slika 9.1 Shematski prikaz javne mreže.

Prikaz ponašanja sustava prije provedbe simulacije



Slika 9.2 Prikaz *Web* stranice prije ispada HT veze[37]



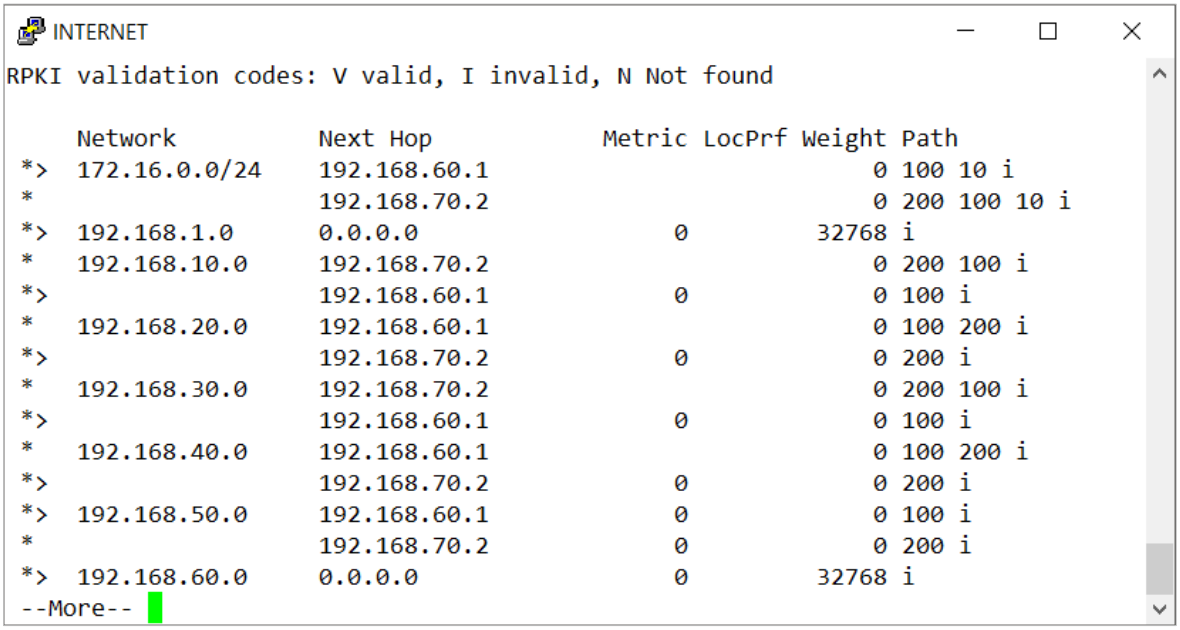
Slika 9.3 Prikaz virtualnih servisa na balanseru opterećenja prije ispada HT veze[38]

[37] Vlastiti rad autora
[38] Vlastiti rad autora

```
Tracing route to 172.16.0.111 over a maximum of 30 hops

  1    23 ms     9 ms     6 ms  192.168.1.3
  2   107 ms    19 ms    18 ms  192.168.60.1
  3    27 ms    28 ms    27 ms  192.168.10.51
  4    35 ms    37 ms    37 ms  172.16.0.100
  5    33 ms    50 ms    37 ms  172.16.0.111
```

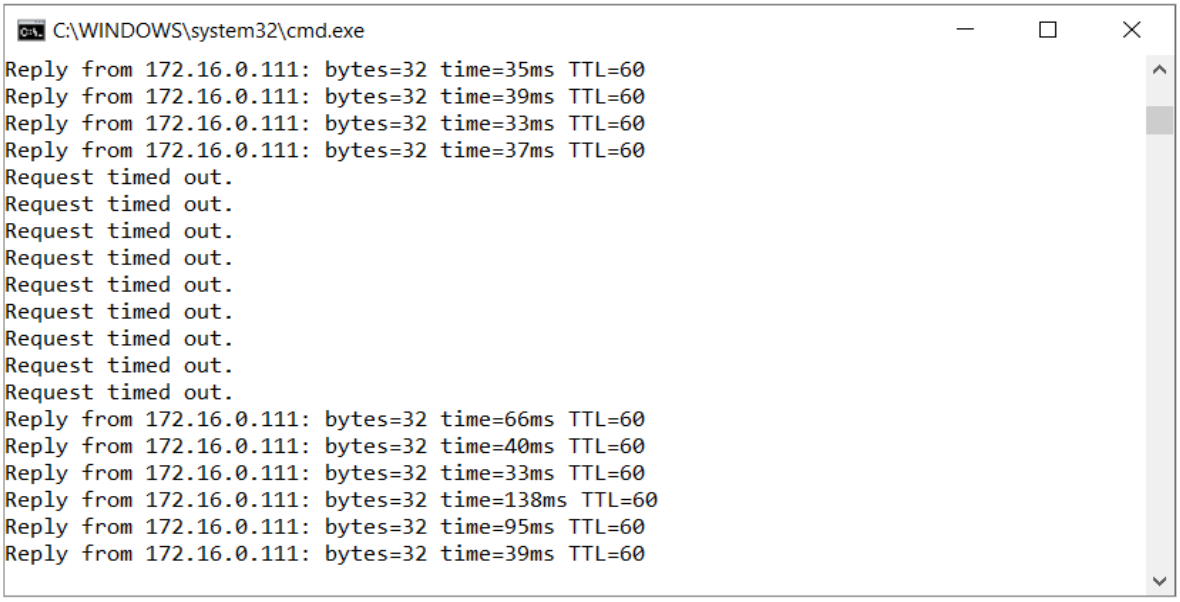
Slika 9.4 Ispis tracert -d naredbe prije ispada HT veze[39]



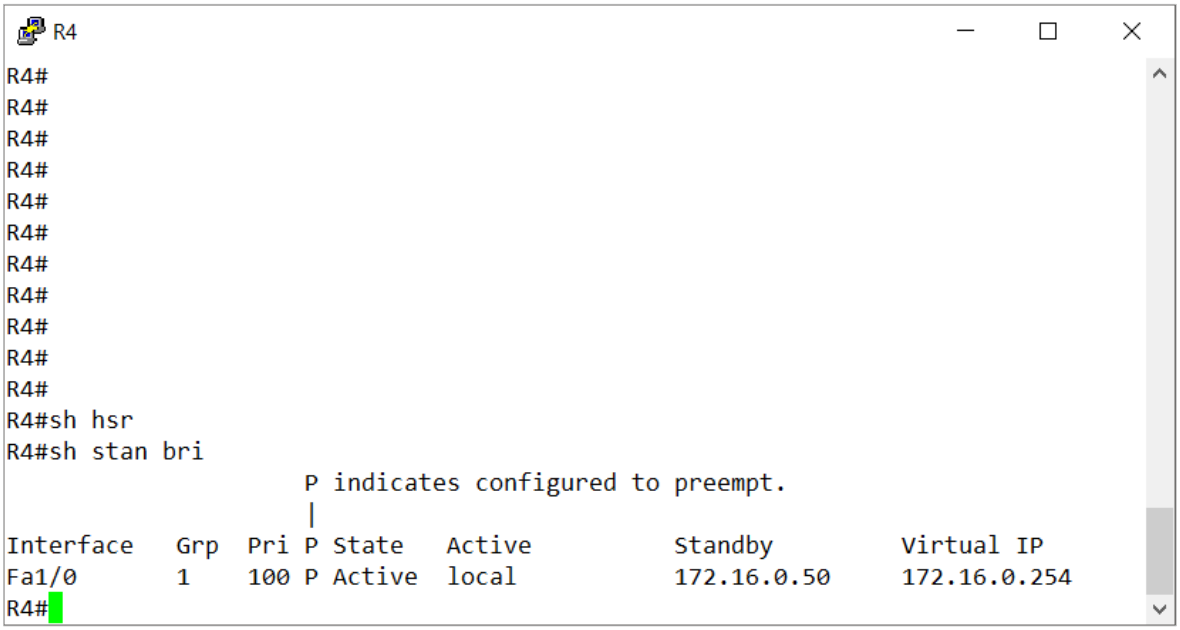
Slika 9.5 Prikaz usmjerničke tablice na Internet usmjerniku prije ispada HT veze[40]

[39] Vlastiti rad autora
[40] Vlastiti rad autora

Prikaz ponašanja sustava nakon ispada HT veze na usmjerniku R1[41]

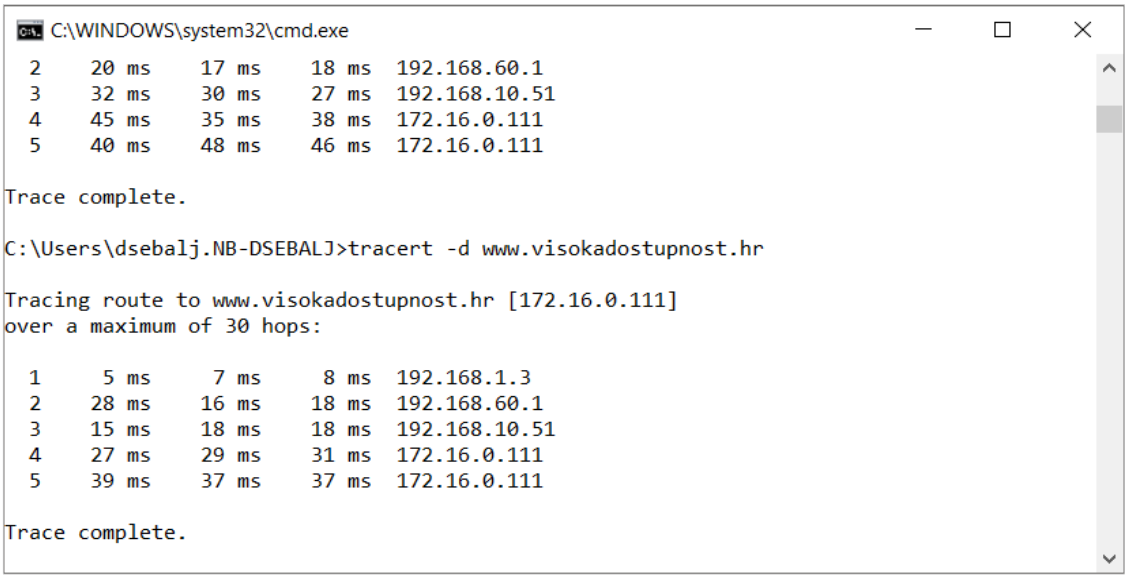


Slika 9.6 Ispis ping naredbe nakon ispada HT veze na usmjerniku R1[42]



Slika 9.7 Prikaz HSRP aktivnog usmjernika nakon ispada HT veze na R1 usmjerniku[43]

[41] Prikaz samo relevantnih informacija vezanih uz usmjeravanje prometa
[42] Vlastiti rad autora
[43] Vlastiti rad autora

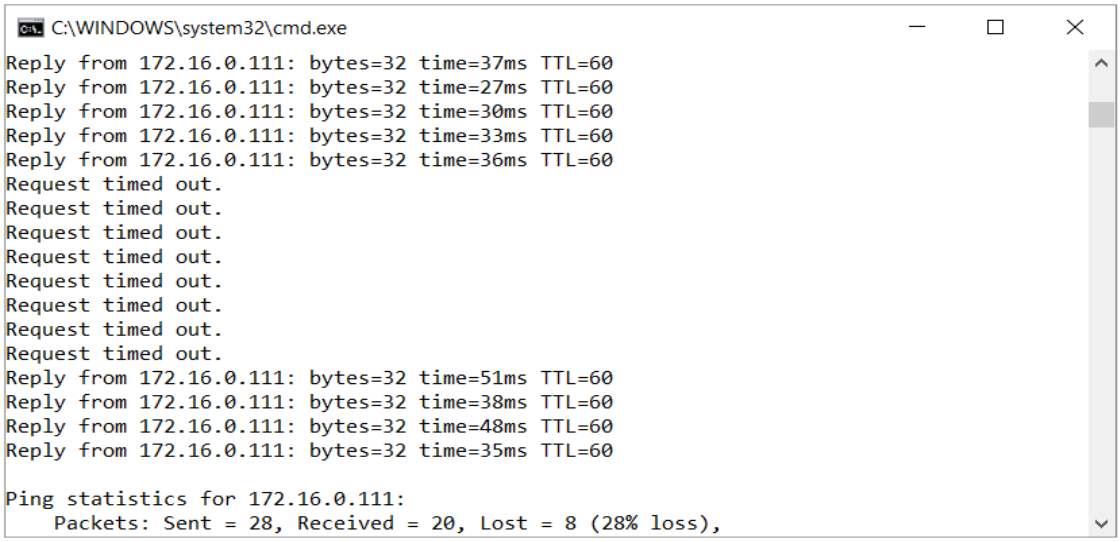


Slika 9.8 Ispis tracert -d naredbe nakon ispada HT veze na usmjerniku R1[44]

Name	Type	Remote Gateway	User Name	Status	Incoming Data	Outgoing Data	Phase 1
IPsecHT_2	Custom	192.168.10.101		Down			IPsecHT_2
IPsecPR_2	Custom	192.168.20.100		Up			IPsecPR_2
IPsecVIP_2	Custom	192.168.20.101		Down			IPsecVIP_2
IPsecPR	Custom	192.168.10.100		Up	76.94 kB	56.41 kB	IPsecPR

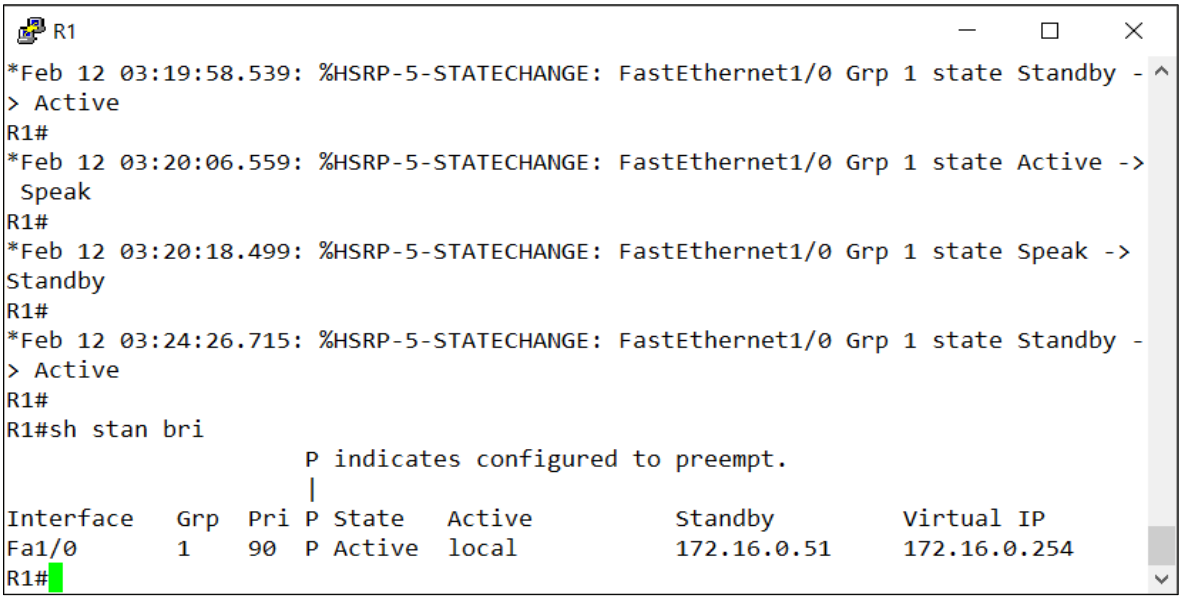
Slika 9.9 Prikaz stanja IPsec tunela nakon ispada HT veze na usmjerniku R1[45]

Prikaz ponašanja sustava nakon ispada HT veze na razini lokacije



Slika 9.10 Ispis ping naredbe nakon ispada HT veze na razini lokacije[46]

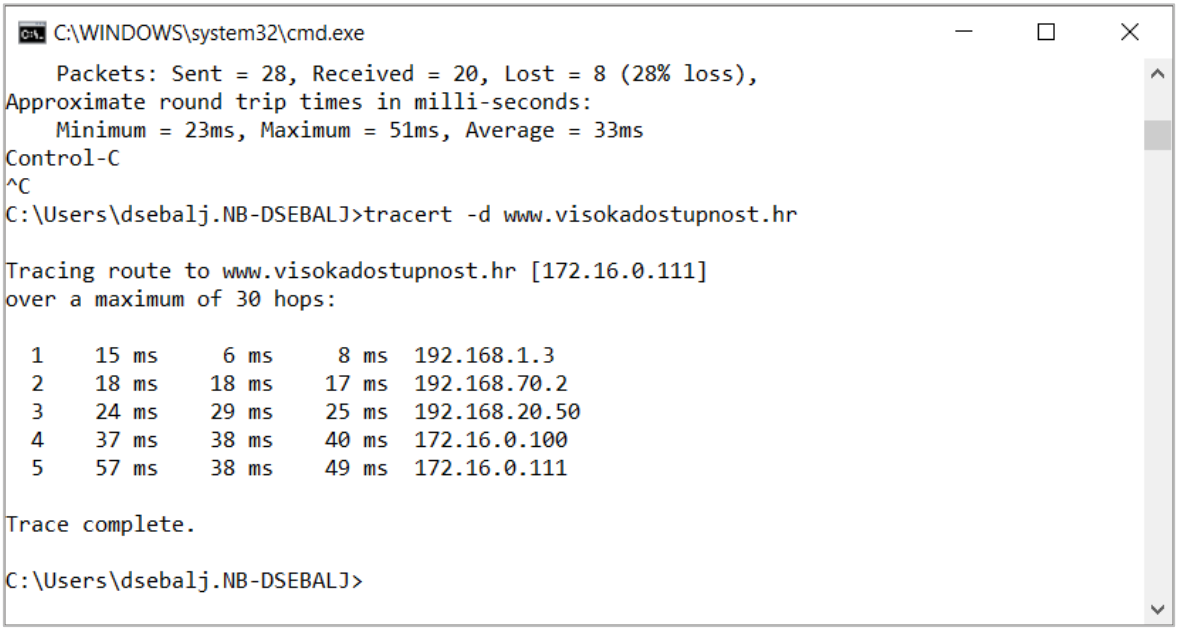
[44] Vlastiti rad autora
[45] Vlastiti rad autora
[46] Vlastiti rad autora



Slika 9.11 Prikaz aktivnog HSRP usmjernika nakon ispada HT veze na razini lokacije[47]

Name	Type	Remote Gateway	User Name	Status	Incoming Data	Outgoing Data	Phase 1
IPsecHT_2	Custom	192.168.10.101		Down			IPsecHT_2
IPsecPR_2	Custom	192.168.20.100		Up	32.46 kB	23.66 kB	IPsecPR_2
IPsecVIP_2	Custom	192.168.20.101		Up			IPsecVIP_2
IPsecPR	Custom	192.168.10.100		Down			IPsecPR

Slika 9.12 Prikaz stanja IPsec tunela nakon ispada HT veze na razini lokacije[48]

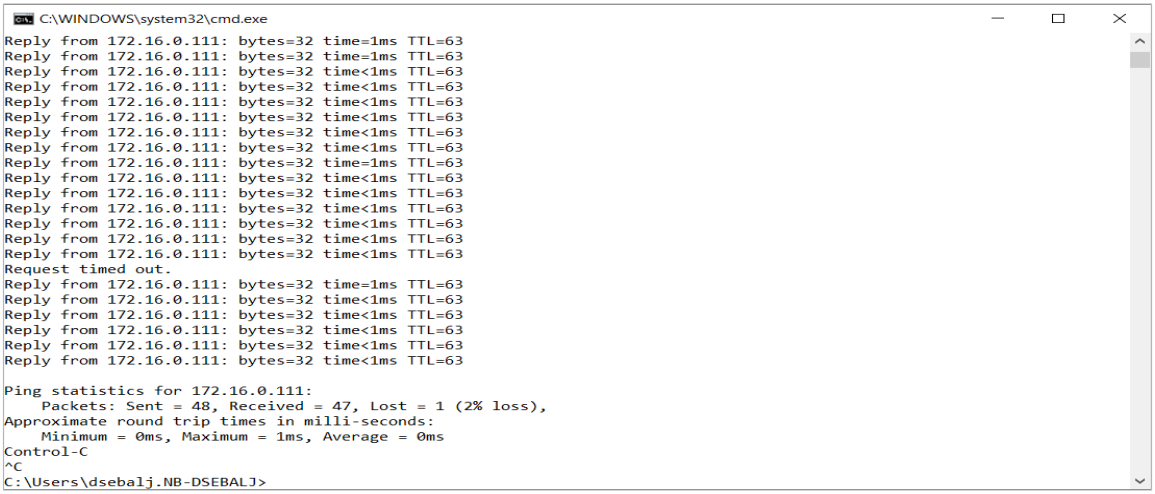


Slika 9.13 Ispis tracert – d naredbe nakon ispada HT veze na razini lokacije[49]

[47] Vlastiti rad autora
[48] Vlastiti rad autora
[49] Vlastiti rad autora

9.2. Ispad primarnog balansera opterećenja

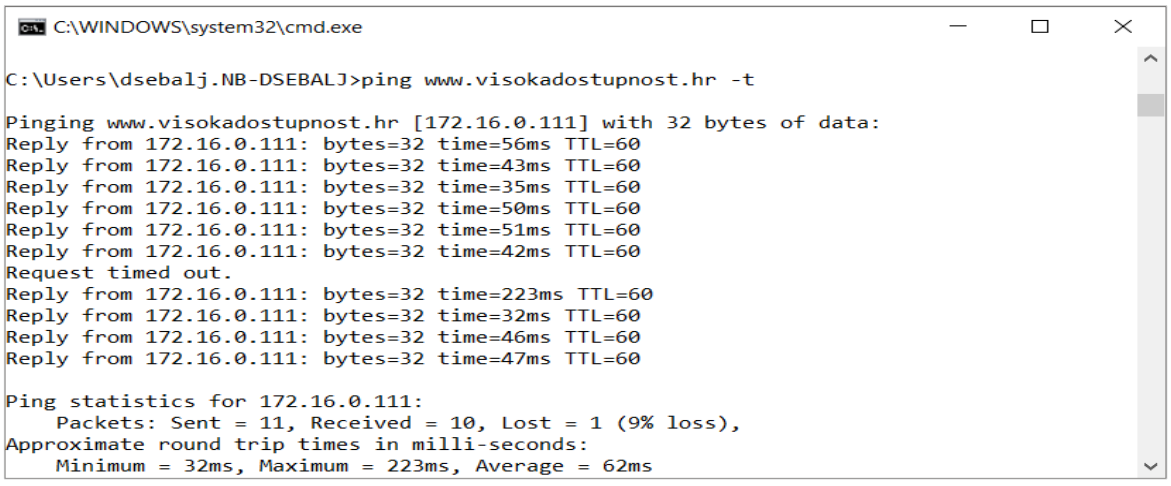
U slučaju ispada primarnog balansera opterećenja, uređaj koji se nalazi u pripravnosti preuzima ulogu primarnog te se zahtjevi i dalje nastavljaju posluživati klijentima.



Slika 9.14 Ispis ping naredbe nakon ispada primarnog balansera opterećenja[50]

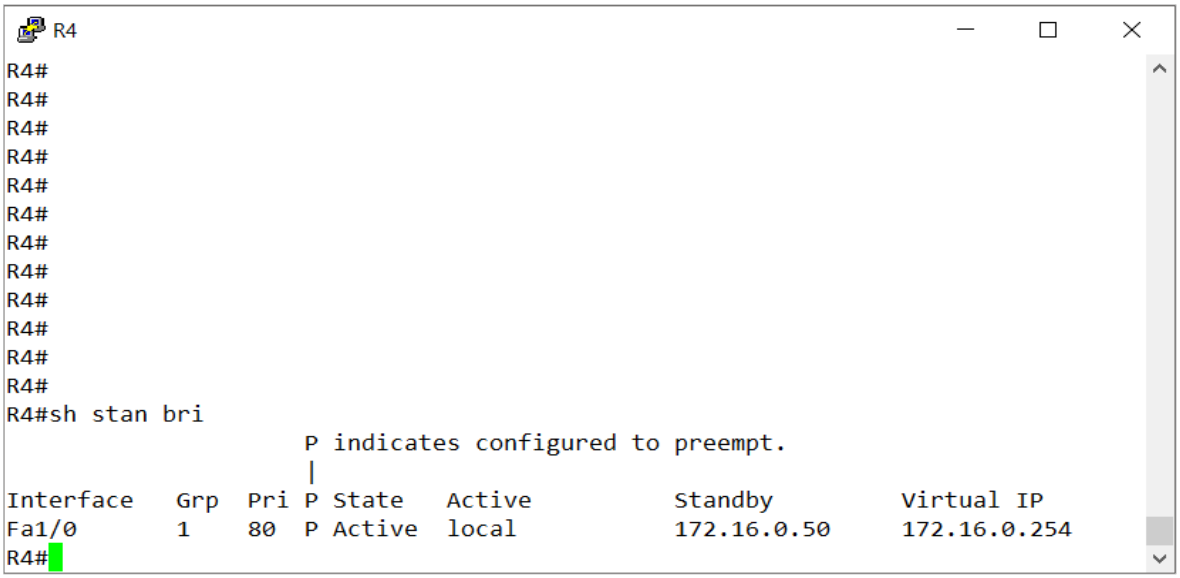
9.3. Ispad obje veze na primarnoj lokaciji

Prikaz ponašanja sustava nakon ispada obje veze na R1 usmjerniku

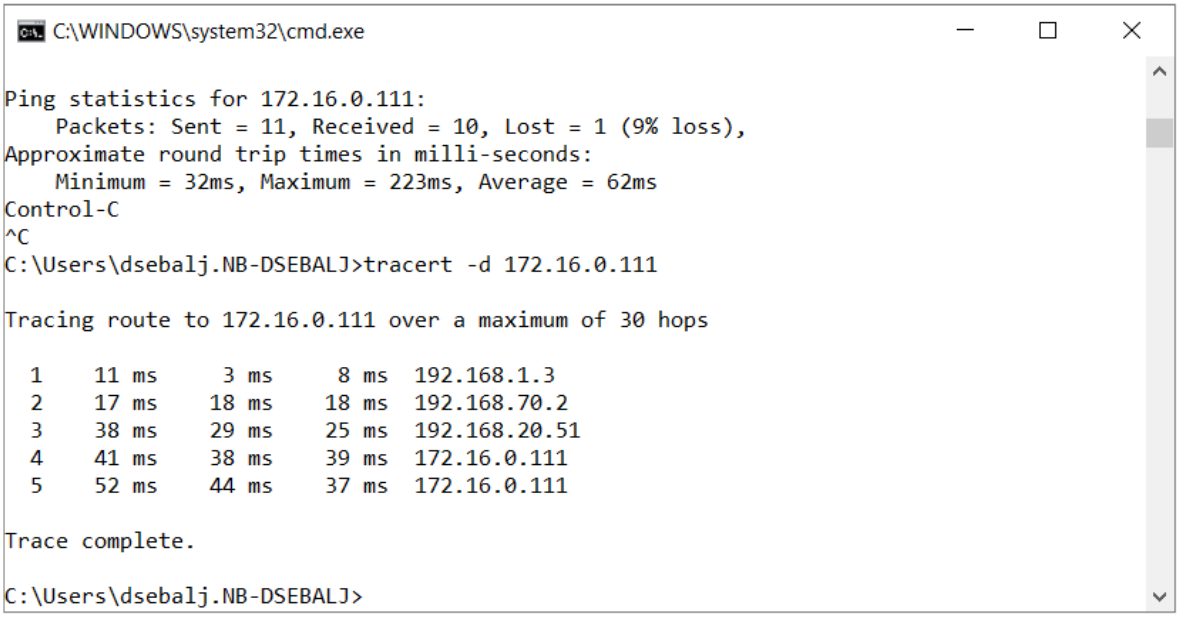


Slika 9.15 Ispis ping naredbe nakon ispada obje veze na R1 usmjerniku[51]

[50] Vlastiti rad autora
[51] Vlastiti rad autora



Slika 9.16 Prikaz aktivnog HSRP usmjernika nakon ispada obje veze na R1 usmjerniku[52]



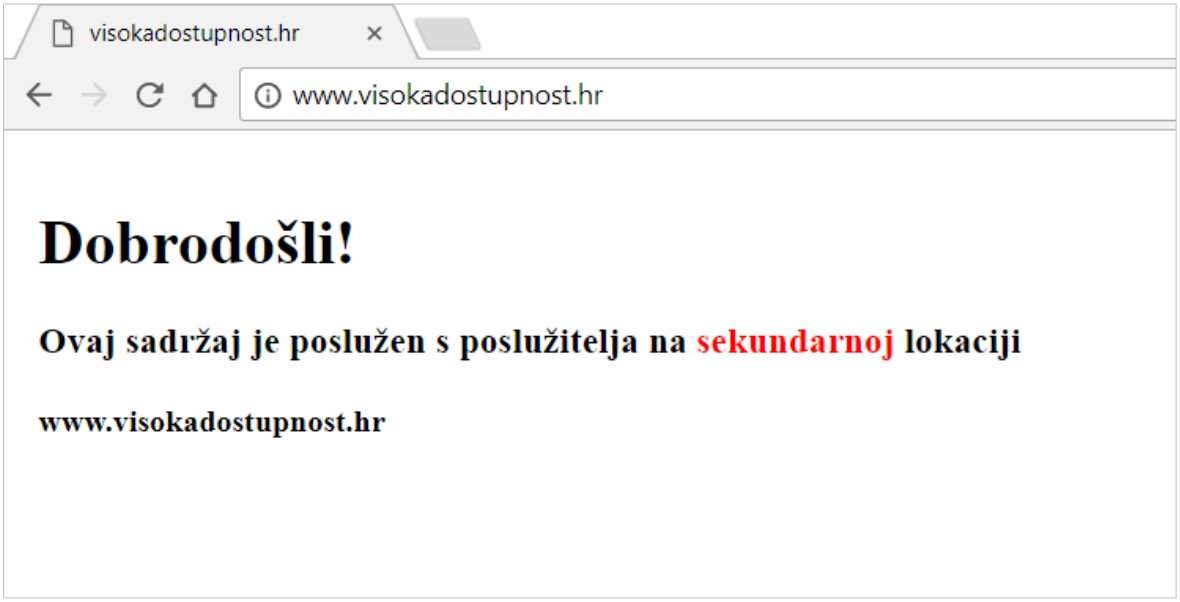
Slika 9.17 Ispis tracert -d naredbe nakon ispada obje veze na R1 usmjerniku[53]

Name	Type	Remote Gateway	User Name	Status	Incoming Data	Outgoing Data	Phase 1
IPsecHT_2	Custom	192.168.10.101		Down			IPsecHT_2
IPsecPR_2	Custom	192.168.20.100		Up	17.31 kB	12.45 kB	IPsecPR_2
IPsecVIP_2	Custom	192.168.20.101		Up			IPsecVIP_2
IPsecPR	Custom	192.168.10.100		Down			IPsecPR

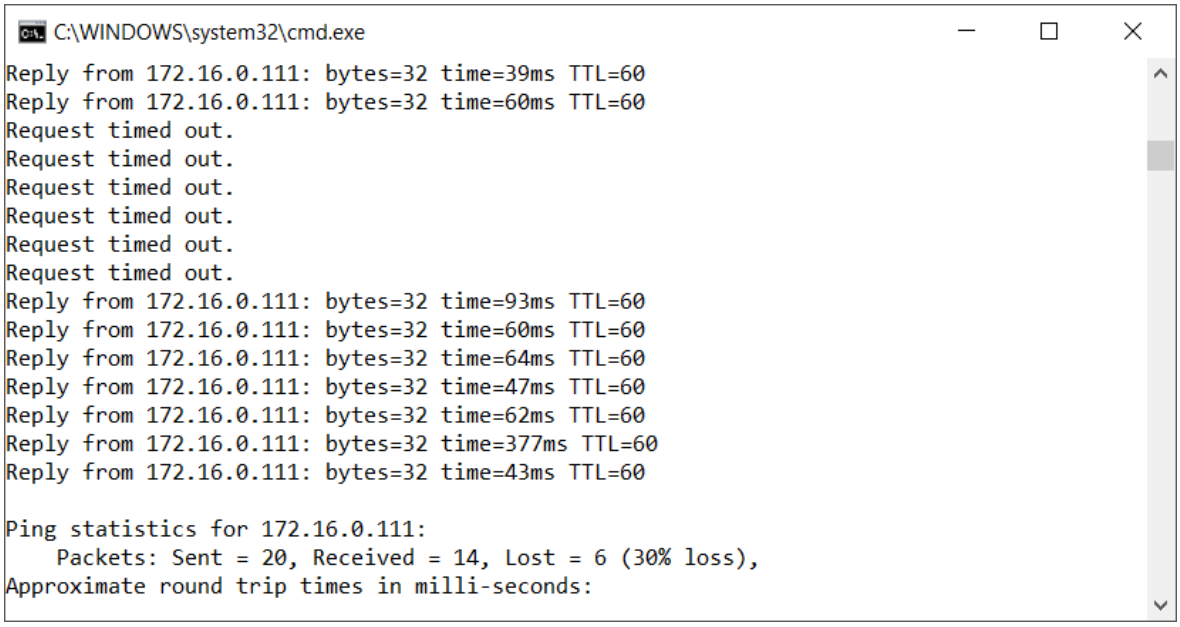
Slika 9.18 Prikaz stanja IPsec tunela nakon ispada obje veze na R1 usmjerniku[54]

[52] Vlastiti rad autora
[53] Vlastiti rad autora
[54] Vlastiti rad autora

Prikaz ponašanja sustava nakon ispada primarne lokacije

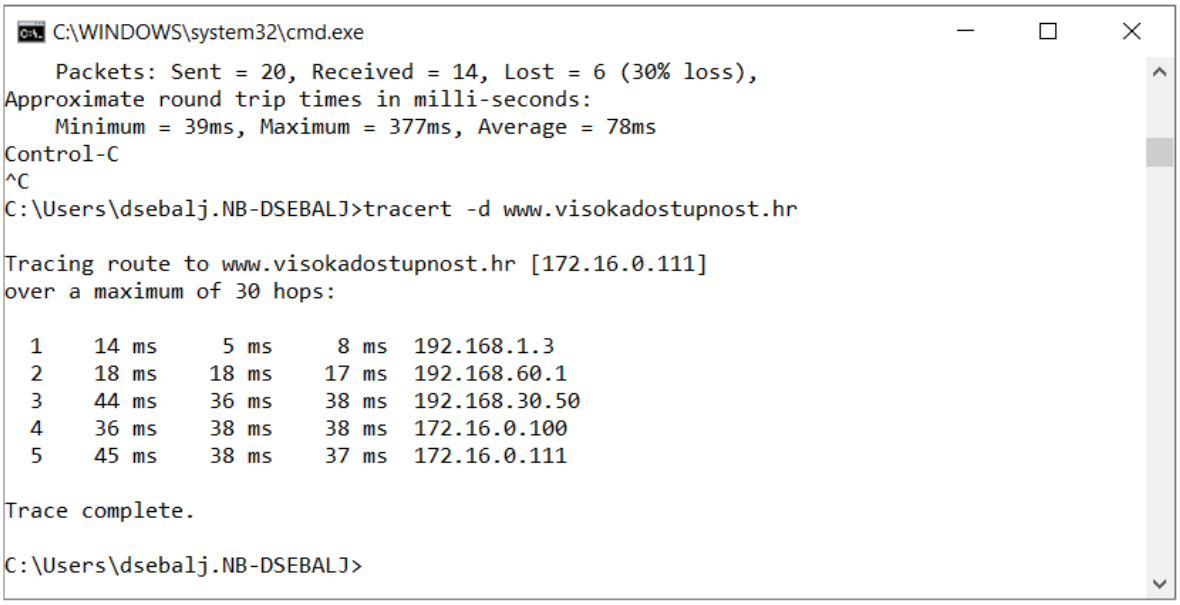


Slika 9.19 Prikaz *Web* stranice nakon ispada primarne lokacije[55]

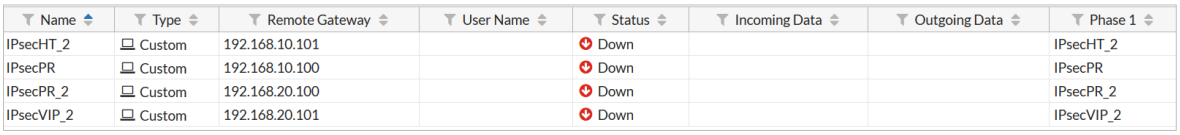


Slika 9.20 Ispis ping naredbe nakon ispada primarne lokacije[56]

[55] Vlastiti rad autora
[56] Vlastiti rad autora

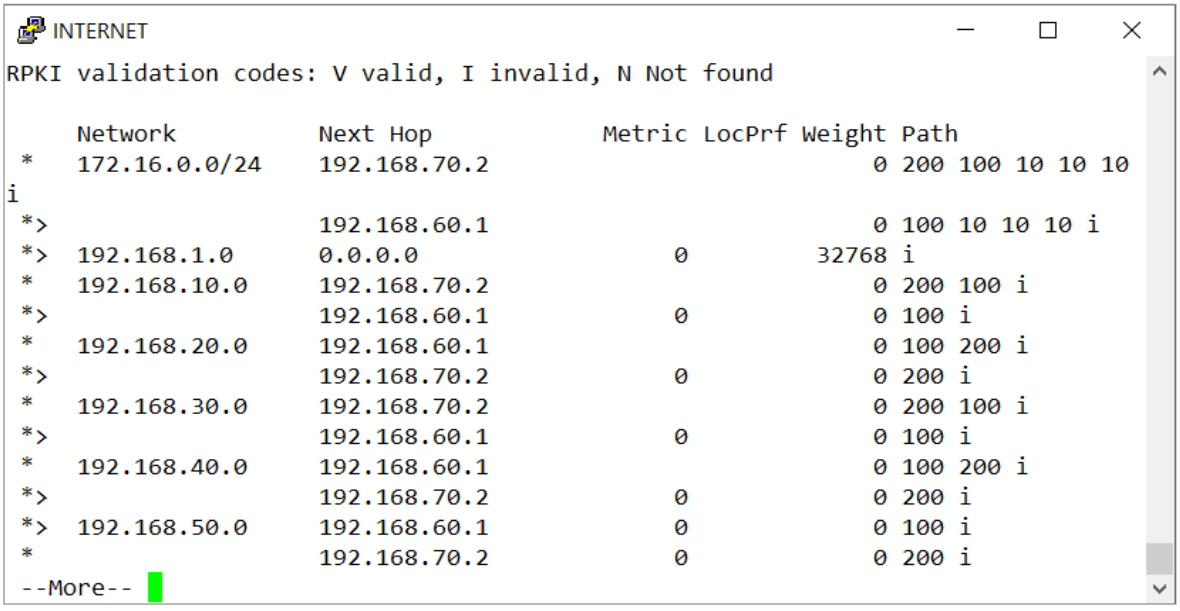


Slika 9.21 Ispis tracert -d naredbe nakon ispada primarne lokacije[57]



Name	Type	Remote Gateway	User Name	Status	Incoming Data	Outgoing Data	Phase 1
IPsecHT_2	Custom	192.168.10.101		Down			IPsecHT_2
IPsecPR	Custom	192.168.10.100		Down			IPsecPR
IPsecPR_2	Custom	192.168.20.100		Down			IPsecPR_2
IPsecVIP_2	Custom	192.168.20.101		Down			IPsecVIP_2

Slika 9.22 Prikaz stanja IPsec tunela nakon ispada primarne lokacije[58]



Slika 9.23 Prikaz usmjerničke tablice na Internet usmjerniku nakon ispada primarne lokacije[59]

[57] Vlastiti rad autora
[58] Vlastiti rad autora
[59] Vlastiti rad autora

9.4. Ispad oba balansera opterećenja

Uslugu nije moguće isporučiti bez potrebe za ljudskom intervencijom slučaju ispada oba balansera opterećenja,.

9.5. Ispad pojedine aplikacije

Balanser opterećenja zahtjev preusmjerava putem IPsec tunela na poslužitelje koji se nalaze na DR lokaciji u slučaju ispada pojedine aplikacije,.

10. Analiza rezultata

Dovršetkom implementacije i provedenim testiranjima, te pogledom na dizajn cjelokupnog sustava, postoji nekoliko ključnih odluka koje su uvelike utjecale na konačno rješenje. Odlukom da se na primarnoj i sekundarnoj lokaciji koristi isti raspon javnih IP adresa dodijeljenih tvrtki eliminiraju se problemi s pohranom DNS upita na klijentskoj strani, ali se pojavljuju problemi povezani s usmjeravanjem prometa između dviju lokacija. Spomenutom problemu pridonosi i odluka koja je direktna posljedica nametnutih poslovnih zahtjeva tvrtke, kojom se preferira usmjeravanje prometa putem HT veze za vrijeme dostupnosti iste. Kako bi se riješio problem povezan s usmjeravanjem, potrebno je izvršiti određene manipulacije prilikom oglašavanja javno dostupnih IP adresa putem BGP protokola. Iako s tehničkog stajališta ne postoji prepreka zbog koje ne bi bilo moguće udovoljiti poslovnom zahtjevu tvrtke, često ovakve odluke vode do nezgrapnih implementacijskih rješenja koja kasnije predstavljaju problem inženjerima prilikom održavanja takvih sustava ili u situacijama kada je potrebno odraditi određene preinake ili dijagnosticirati kvar na sustavu. Za potrebe ove implementacije na usmjernicima R2 i R5 prema vezi HT Slika 8.1 Shematski prikaz sustava dodaje se niz BGP AS_PATH prefiksa kako se veza ne bi usmjeravala na DR lokaciju za vrijeme dostupnosti primarne lokacije. Da bi se HT putanja preferirala u odnosu na putanju dostupnu putem VIP veze, na VIP vezi se pridodaje dulji niz BGP AS_PATH prefiksa u odnosu na HT vezu. Konačni rezultat je prikazan na Slika 9.23 Prikaz usmjerničke tablice na Internet usmjerniku nakon ispada primarne lokacije iz koje je vidljivo kako internet usmjernik za javni raspon IP adresa 172.16.0.0/24 preferira putanju putem HT veze.

Kako bi se udovoljilo potrebama poslovanja i omogućila visoka dostupnost usluga koje se isporučuju korisnicima, na DR lokaciju postavljen je balanser opterećenja koji radi u visoko dostupnom načinu rada. Rješenje koje bi uključivalo uporabu balansera opterećenja u oblaku nije predstavljalo prihvatljivu opciju zbog poslovne politike koju tvrtka provodi[60].

Da bi se udovoljilo zahtjevima koji su postavljeni pred inženjere, na DR lokaciji postavljena su dva usmjernika koja se nalaze ispred vatrozida i dodijeljene su im javne IP adrese koje se koriste za povezivanje na opremu pružatelja internet usluge. Obzirom da je vatrozid postavljen iza usmjernika i koristi javni raspon IP adresa koji je dodijeljen tvrtki na korištenje

[60] https://cloud.google.com/load-balancing

Slika 9.1 Shematski prikaz javne mreže, da bi se uspostavio IPsec tunel između primarne i DR lokacije, potrebno je koristiti i NAT-T tehnologiju. Iako je NAT-T tehnologija osmišljena kako bi omogućila uređajima koji se nalaze iza prevedene IP adrese uspostavu IPsec tunela, NAT-T tehnologija nije po dizajnu implementiran unutar IKEv1 (eng. *Internet Key Exchange*) protokola, već je dodana naknadno. Temeljem vlastitog iskustva smatram kako korištenje NAT-T tehnologije ne pridonosi stabilnosti sustava. Implementacije NAT-T tehnologije mogu varirati između uređaja različitih proizvođača što može dovesti do nestabilnosti IPsec veze. Korištenjem NAT-T tehnologije smanjuje se količina prometa koju je moguće prenijeti unutar jednog paket zbog dodatne enkapsulacije prometa koju je potrebno izvršiti. Iz tog razloga, smatra se kako bi IPsec tunele trebalo uvijek terminirati na uređajima koji se nalaze na javno dostupnim IP adresama.

Javni raspon IP adresa na primarnoj i sekundarnoj lokaciji ima svoje prednosti, ali isto tako predstavlja problem prilikom usmjeravanja prometa, kako je već ranije spomenuto. U slučaju korištenja različitog javnog raspona IP adresa, na autoritativnim imeničkim poslužiteljima tvrtke mogla bi se postaviti maksimalna dopuštena vrijednost pohrane odgovora kojim bi se sustav zaštitio od dužeg vremenskog perioda nedostupnosti u slučaju ispada usluge na primarnoj lokaciji. Dodatno opterećenje na imeničke poslužitelje moglo bi se umanjiti balansiranjem prometa između većeg broja imeničkih poslužitelja. Međutim, u konkretnom slučaju koji se obrađuje u ovom radu, u slučaju ispada primarne lokacije rješenje se oslanja na BGP protokol.

Korištenje BGP protokola ne bi predstavljalo problem prilikom implementacija koje zahtijevaju brzi odgovor na promjene unutar mreže da BGP protokol nije inherentno spor po dizajnu. Zadane vrijednosti BGP brojača na usmjernicima R2 i R5 iznose 60 sekundi za pakete koji služe za održavanje veze, odnosno 180 sekundi kako bi se susjed smatrao nedostupnim u slučaju izostanka paketa kojim se održava veza. Nakon što usmjernik ustanovi da je određeni susjed nedostupan, ažurirat će usmjerničku tablicu i obavijest o novim putanjama proslijediti svim BGP susjedima. Iako je zadane vrijednosti moguće modificirati i time osigurati bržu reakciju na promijene unutar mreže, pružatelji internet usluga često se štite od preniskih vrijednosti kako se ne bi narušila stabilnost interneta. Ukoliko s pružateljem internet usluge nije moguće postići dogovor o manjim vrijednostima brojača, u slučaju nedostupnosti primarne lokacije vrijeme potrebno za ažuriranje usmjerničkih tablica na BGP usmjernicima može biti znatno dulje od vremena koje bi bilo potrebno za istek pohranjenog DNS odgovora. Iz tog razloga smatra se kako bi korištenje

DNS protokola u kombinaciji s balansiranjem prometa prema većem broju imeničkih poslužitelja bilo kvalitetnije rješenje.

Kako bi se osigurala komunikacija putem IPsec tunela u slučaju ispada pojedinih veza na primarnoj i/ili sekundarnoj lokaciji, potrebno je korištenje dodatnih javnih IP adresa na HT, odnosno VIP vezi. Npr. u slučaju ispada HT veze na primarnoj lokaciji, potrebno je osigurati uspostavu „pomoćnog“ IPsec tunela koji će se uspostaviti putem VIP → HT veze. Kako bi isto bilo moguće, potrebno je implementirati dodatnu logiku prilikom prevođenja IP adresa na usmjernicima R2 i R5. U suprotnom, u slučaju ispada različitih veza na primarnoj, tj. sekundarnoj lokaciji, pomoćni tunel se neće moći uspostaviti i vatrozid će ispisati sljedeću poruku:

```
ike 0:IPsecPR:24: out D4F91D15F4D5C4D5CC1CAE11F46C17C5041002000000000000000DC0A0000849488AA991D38991829CD0C77
967542087DE1319FD40309E019DFC5D0140CE5FD1CD36928F2A3AA8FE1394275A4C635F30C05BFB0C510D8DCCEED5B41B8FB4411D953DA
9F5A140000142EB936B69728AC02EEC11310CB793C6400000014AF80B386E0C585008F3DC0EC0653AE4B
ike 0:IPsecPR:24: sent IKE msg (ident_r2send): 172.16.1.100:500->192.168.10.100:500, len=220, id=d4f91d15f4d5c
ike 0:IPsecPR:24: ISAKMP SA d4f91d15f4d5c4d5/cc1cae11f46c17c5 key 8:0FE90EBDFBCF2996
iike 0: comes 192.168.20.100:4500->172.16.1.100:4500,ifindex=3....
ike 0: IKEv1 exchange=Identity Protection id=d4f91d15f4d5c4d5/cc1cae11f46c17c5 len=92
ike 0: in D4F91D15F4D5C4D5CC1CAE11F46C17C505100201000000000000005CF0AC7EBC87D6ABCD6FC4810F24D5AEBFB767E803BA88
908E9
ike 0:IPsecPR:24: remote address 192.168.20.100 does not match configuration address 192.168.10.100, drop
```

Slika 10.1 Udaljena adresa ne odgovara postavljenoj adresi[61]

Implementacijom dodatne logike za prevođenje IP adresa na usmjernicima R2 i R5 dodatno se komplicira konfiguracija usmjernika što kasnije dovodi do otežane administracije, narušavanja stabilnost sustava i otežane dijagnostike u slučaju kvara.

Korištenje vatrozida ispred usmjernika R2 i R5, ili izostavljanje usmjernika R2 i R5 u potpunosti iz dizajna nije bilo moguće zbog sigurnosne politike koju tvrtka provodi. Ukoliko bi dizajn koristio samo vatrozid, on bi morao provoditi sigurnosne politike tvrtke te ujedno imati konfiguriran BGP protokol. Sigurnosna politika tvrtke brani ovakav način implementacije, kojim bi jedan uređaj obavljao funkciju za koju nije primarno namijenjen. Zaključuje se da bi BGP funkcionalnosti implementirane unutar vatrozida, a vezane uz osnovnu mogućnost manipulacije prefiksima ipak bile dostatne za potrebe ove implementacije. Također, činjenica je da određene funkcionalnosti implementirane

[61] Vlastiti rad autora

prvenstveno na uređajima, čija je namjena obavljati specifičnu ulogu, nisu dostupne na ostalim uređajima koji određene tehnologije mogu podržavati, ali na rudimentarnoj razini.

11. Metodologija implementacije

Potrebno je razraditi niz detalja od trenutka kada tvrtka spozna da joj je potrebno rješenje za oporavak od katastrofe, pa sve do implementacije konkretnog rješenja. Detaljnom razradom plana koji će uključivati sve potrebne korake do konačnog rješenja, smanjuje se mogućnost pogreške i osigurava se nesmetano odvijanje ključnih poslovnih procesa za vrijeme trajanja implementacije. Potrebni koraci za uspješnu implementaciju rješenja uključuju:

1. Provesti analizu poslovnih procesa organizacije i odrediti ključne procese za nastavak poslovanja u slučaju katastrofalnih otkaza.
2. Jasno i precizno definirati što se sve smatra katastrofalnim otkazom.
3. Odrediti maksimalno prihvatljivo vrijeme nedostupnosti za poslovne procese utvrđene točkom 1.
4. Definirati ključne slabosti trenutnog rješenja koji mogu dovesti do situacije utvrđene točkom 2.
5. Ovisno o rezultatima točke 3, donijeti odluku o tipu DR lokacije koju je potrebno implementirati.
6. Odrediti način rada DR lokacije, želi li se implementirati aktivno/aktivno ili aktivno/pasivno rješenje.
7. Odrediti na koji način će se izvršiti odabir primarne ili sekundarne lokacije za korisnike koji pristupaju određenim uslugama, da li će se koristiti GSLB rješenje, imenički poslužitelj, preusmjeravanje (eng. *redirect*) ukoliko je riječ o HTTP prometu ili neko drugo rješenje.
8. Ovisno o točki 5 i 6, donijeti odluku o korištenju javnih IP adresa, da li će se za potrebe DR rješenja koristiti isti raspon javnih IP adresa kao i na primarnoj lokaciji ili je potrebno zakupiti nove IP adrese.
9. Ovisno o točki 7, odrediti na koji način će se vršiti usmjeravanje prometa na internetu, da li je potrebno vršiti određene modifikacije prilikom objave javnog raspona IP adresa, da li je potrebno konfigurirati BGP protokol ili je moguće postići željene rezultate u dogovoru s pružateljem internet usluge.
10. Odrediti načina povezivanja primarne i sekundarne lokacije ukoliko je potrebno ostvariti komunikaciju između istih.
11. Odrediti željeni nivo redundancije unutar sustava. Utvrditi da li je moguće ugovoriti odgovarajući SLA ugovor te se na taj način osigurati u slučaju ispada pojedinog

elementa sustava, da li je potrebno koristiti jednu ili više veza prema internetu. Ukoliko će se koristiti uređaji konfigurirani u visoko dostupnom načinu rada, koji su to uređaji čiju je visoku dostupnost potrebno osigurati.

12. Izraditi detaljan plan kojim će se jasno i precizno navesti svi koraci potrebni za uspješnu implementaciju rješenja.
13. Provesti implementaciju.
14. Nakon implementacije sustava provesti opsežno testiranje.
15. Temeljem provedenog testiranja, izvršiti analizu prikupljenih podataka kako bi se utvrdilo da li sustav udovoljava svim zahtjevima te ostvaruje očekivane rezultate.
16. Izrada detaljne dokumentacije sustava.
17. Podnošenje detaljnog izvještaja upravi o implementaciji rješenja te rezultatima provedenih testiranja.
18. Temeljem točke 15 iznijeti konstruktivne prijedloge o eventualnom poboljšanju sustava.

12. Zaključak

Tvrtkama je često vrlo teško izdvojiti potrebna financijska sredstva za izgradnju pouzdanih informacijsko tehnoloških sustava. Međutim, suočene s prijetnjama koje mogu trajno naštetiti njihovu poslovanju, pristaju na potrebna ulaganja kako bi se zaštitile od katastrofalnih ispada sustava. Prilikom izgradnje sustava pristalo se na određene kompromise kako bi potrebe poslovanja koje su postavljene pred sustav bile zadovoljene, a kako bi sustav istovremeno bio u skladu sa sigurnosnom politikom tvrtke. Provedena testiranja nakon implementacije ipak su u konačnici pokazala zadovoljavajuće rezultate. Nakon ispada pojedinih veza i/ili određenih elemenata informacijsko tehnološkog sustava na primarnoj lokaciji, sustav je sposoban preuzeti zadaću na sebe i osigurati tvrtki nastavak poslovanja u slučaju katastrofe. Prilikom implementacije sustava svakako treba obratiti pozornost prati li postojeće rješenje razvoj tvrtke i da li je u mogućnosti odgovoriti na eventualne buduće izazove koji se stave pred njega.

Popis kratica

ARP	*Address Resolution Protocol*	protokol za rezoluciju IP adrese u hardversku adresu mrežne kartice
BGP	*Border Gateway Protocol*	protokol koji se koristi za usmjeravanje prometa na internetu
DMZ	*Demilitarized zone*	fizička ili logička mreža u kojoj su smješteni poslužitelji na kojima su objavljene javno dostupne usluge
DNS	*Domain Name System*	protokol za prevođenje imena u IP adresu
DR	*Disaster Recovery*	oporavak od katastrofe
FHRP	*First Hop Redundancy Protocol*	skup protokola za redundanciju uređaja koji služi za izlaz iz mreže
GSLB	*Global Server Load Balancing*	balansiranje opterećenja na globalnoj razini
HSRP	*Hot Standby Redundancy Protocol*	protokol za redundanciju uređaja koji služi za izlaz iz mreže
HT	Hrvatski Telekom	pružatelj internet usluge
HTTP	*HyperText Transfer Protocol*	protokol za razmjenu sadržaja na internetu
ICMP	*Internet Control Message Protocol*	dijagnostički protokol
IP	*Internet Protocol*	protokol koji omogućava dostavu paketa na mreži
IPS	*Intrusion Prevention System*	sustav za zaštitu od malicioznih napada
IPsec	*Internet Protocol Security*	skup protokola za sigurnosnu razmjenu informacija putem nesigurnog kanala
NAT-T	*Network Address Translation – Traversal*	protokol kojim se omogućava IPsec komunikacija uz prevođenje IP adresa
NS	*Name Server*	zapis unutar zone DNS poslužitelja
OSI	*Open System Interconnection*	referentni model kojim se opisuju različiti slojevi arhitekture mreže
SLA	*Service Level Agreement*	ugovor o razini isporučene usluge
SMTP	*Simple Mail Transfer Protocol*	protokol za razmjenu elektroničke

		pošte
SSL	*Secure Socket Layer*	protokol za uspostavu sigurnosnog komunikacijskog kanala između klijenta i poslužitelja
TCP	*Transmission Control Protocol*	protokol za kontrolu prijenosa podataka

Popis slika

Popis tablica

Literatura

[1] SUSAN SNEDAKER, Business Continuity and Disaster Recovery Planning for IT Professionals, 2nd Edition, Syngress, Elsevir, 2010

[2] CHANDRA KOPPARAPHU, Load Balancing Servers, Firewalls, and Caches, Wiley, 2002

[3] NARBIK KOCHARIANS, PETER PALUCH, CCIE Routing and Switching v5.0 Official Cert Guide, Volume 1, 5th Edition, Cisco Press, 2014

[4] NARBIK KOCHARIANS, TERRY VINSON, CCIE Routing and Switching v5.0 Official Cert Guide, Volume 2, 5th Edition, Cisco Press, 2014

[5] http://www.loadbalancer.org/blog/multiple-sites-or-data-centres-what-are-my-options-im-confused/, veljača. 2018

[6] Vlastiti rad autora