Sigurna komunikacija unutar MPLS L3 VPN oblaka

Maloča, Josip

Undergraduate thesis / Završni rad

2018

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **Algebra University College / Visoko učilište Algebra**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:225:627314

Rights / Prava: In copyright / Zaštićeno autorskim pravom.

Download date / Datum preuzimanja: **2024-04-19**

Repository / Repozitorij:

Algebra Univerity College - Repository of Algebra Univerity College

VISOKO UČILIŠTE ALGEBRA

ZAVRŠNI RAD

SIGURNA KOMUNIKACIJA UNUTAR MPLS L3 VPN OBLAKA

Josip Maloča

Zagreb, Veljača 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, datum.

Josip Maloča

Predgovor

Ovom prilikom bih se htio zahvaliti prvenstveno svom mentoru dipl. ing. Silviju Papiću što je svojom voljom, predanošću te dobrim smjernicama omogućio pisanje ovog završnog rada.

Također bih htio iskoristiti priliku i zahvaliti se svim predavačima i asistentima Visokog učilišta Algebra koji su svojim pristupom prema tehnologijama omogućili usavršavanje znanja kako bih sa razumijevanjem opisao tehnologije u ovom radu.

Za kraj zahvaljujem se svojoj tvrtki King-ICT d.o.o. te njezinim djelatnicima što su mi pružili rad na tehnologijama koje sam opisivao u ovom radu.

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

Sažetak

Komunikacija između udaljenih lokacija uvijek je izazov u smislu sigurnosti, redundancije i pouzdanosti, a posebno ako se ta komunikacija odvija preko infrastrukture koja nije pod vlastitim nadzorom. WAN (eng. Wide Area Network) segment koji povezuje udaljene lokacije mora, uz sve navedeno, omogućiti kategorizaciju i određivanje prioriteta mrežnog prometa. U ovom će radu biti predstavljen jedan način kako se ovi zahtjevi mogu zadovoljiti, a to je napredna implementacija MPLS (eng. Multiprotocol Label Switching) tehnologije koja je danas temelj za komunikaciju u velikim mrežama, a između ostalog omogućava fleksibilnost i skalabilnost u bilo kojem trenutku. Rješenje je bazirano na implementaciji MPLS oblaka koji se koristi kroz cijelu jezgrenu mrežu pružatelja usluge (eng. Internet Service Provider-ISP) s ciljem povezivanja udaljenih lokacija na kojima se korisnik povezuje korištenjem varozida (eng. Firewall) za uspostavu sigurne komunikacije korištenjem IPSec protokola i usmjeravanja prometa kroz MPLS oblak pružatelja usluga. Odluka o usmjeravanju donosi se na temelju dinamičke kategorizacije prometa korištenjem naprednih politika usmjeravanja (eng. Policy Based Routing). Osim tehničko-tehnoloških elemenata kroz rad će se opravdati potreba za ovakvim rješenjem s aspekta poslovanja organizacije što je zapravo glavni pokretač za implementacijom ovako kompleksnog rješenja.

Ključne riječi: sigurnost, redundancija, pouzdanost, komunikacija.

Abstract

Communication between remote locations is always a challenge in terms of security, redundancy, and reliability, especially if communication takes place through infrastructure that is not under one's own control. The Wide Area Network (WAN) segment that links remote locations must, with all of the above, enable categorization and prioritization of network traffic. This work will present one way to meet these requirements, which is the advanced implementation of MPLS (Multiprotocol Label Switching) technology, which is today the foundation for communication in large networks, and among other things, it enables flexibility and scalability in any moment.The solution is based on the MPLS cloud implementation, which is used throughout the core ISP (Internet Service Provider) network to connect remote locations to which the user connects using Firewalls to establish secure communications and traffic routing through the MPLS cloud of the service providers network. The routing decision is made by the traffic priority by the implementation of the Policy Based Routing. In addition to technical-technological elements, work will be justified by the need for such a solution from an organization's point of view, which is actually the main driver for implementing such a complex solution.

Keywords: security, redundancy, reliability, communication.

Sadržaj

1. Uvod 1

2. Korisnik Državna uprava za zaštitu i spašavanje 2

2.1. Vizija i misija Državne uprave za zaštitu i spašavanje 3

3. Zatečeno stanje 4

4. Projekt unaprijeđena DUZS - IT sustava 112 8

4.1. Korisnički zahtjevi 8

4.2. Prijedlog mogućih rješenja 9

4.3. DMVPN 15

4.4. MPLS L3 VPN 17

4.5. Plan implementacije rješenja 20

4.6. Opis konačnog rješenja 22

5. Testiranje 29

5.1. Alati 29

5.2. Način testiranja 30

5.3. IPSec VPN test ostvarivanja IPSec VPN tunela 31

5.4. Test usmjeravanja *(routing)* 31

5.5. Test IP *unicast* prometa 32

5.6. Test propusnost i stabilnosti IP komunikacije 33

5.7. Test određivanja iznosa MTU 41

Zaključak 45

Popis slika 46

Popis tablica 47

Popis kratica 48

1. Uvod

Tema ovog završnog rada je implementacija tehnologije koja omogućuje visoku dostupnost, pouzdanost te sigurnost u komunikaciji preko nesigurne mreže tj. interneta. Internet kao resurs u poslovnim organizacijama je nužan za uspješno poslovanje, a posebno u slučaju kada je infrastruktura organizacije geografski razgranata, što zahtjeva poseban pristup u povezivanju putem Interneta. Kako tehnologije iz dana u dan idu naprijed, te se kompleksnost mreže povećava eksponencijalno u smislu broja konekcija ostvarenih putem interneta što od strane uređaja koji pristupaju internetu tako i svih aplikacija, te servisa. Osim očitog napretka u tehnologiji znatan napredak je vidljiv i u potrebnim razinama znanja koje moraju posjedovati ljudi koji upravljaju složenom mrežnom infrastrukturom u kojoj krucijalnu važnost zauzima sigurnost komunikacije putem nesigurne mreže odnosno interneta. Ključna tehnologija koja će biti opisana u radu je MPLS VPN (*MultiProtocol Label Switching Virtual Private Network*) koja u suradnji sa telekomunikacijskim operaterom pruža sve blagodati koji su potrebne za sigurnu komunikaciju, i visoku dostupnost. Dodatno na spomenutu tehnologiju, koja već sama po sebi pruža dovoljnu razinu privatnosti u opisanom slučaju implementiran je i IPSec *(Internet Protocol Security*) okvir sa protokolima koji jamče potpunu sigurnost komunikacije kroz kriptirane tunele preko interneta između svih lokacija opisane organizacije.

2. Korisnik Državna uprava za zaštitu i spašavanje

Državna uprava za zaštitu i spašavanje je samostalna, strukovna i upravna organizacija u Republici Hrvatskoj koja priprema, planira i rukovodi operativnim snagama te koordinira djelovanje svih sudionika zaštite i spašavanja koja je započela s radom 01. siječna 2005. godine. Sukladno zakonu o sustavu civilne zaštite u narodnim novinama članak 12. državna uprava nadležna je sljedeće poslove[1]:

- izrađuje procjenu rizika od nastanka i procjenu posljedica od nastale katastrofe i velike nesreće za Republiku Hrvatsku,
- izdaje obvezne upute za upravljanje rizikom svim sudionicima zaštite i spašavanja,
- izrađuje Plan zaštite i spašavanja Republike Hrvatske koji donosi Vlada Republike Hrvatske,
- koordinira unutarnje planove operatora za sprječavanje velikih nesreća s opasnim tvarima i vanjske planove koje izrađuju županije,
- donosi odluku o potrebi izrade vanjskog plana za svaki pogon,
- obavlja poslove promidžbe i nakladničke djelatnosti iz područja zaštite i spašavanja,
- u hitnim situacijama pri nesrećama provodi koordinaciju između sudionika akcije zaštite i spašavanja,
- vodi jedinstvenu informacijsku bazu podataka o svim vrstama nesreća te njihovim posljedicama.

Iz navedenog je vidljivo da je Državna uprava za zaštitu i spašavanje osnovana kao krovna organizacija sa zadaćom zaštite i spašavanja ugroženog i stradalog stanovništva u slučaju nastanka katastrofa i/ili velikih nesreća kao i obvezama u planiranju i provođenju preventivnih mjera zaštite te edukacije stanovništva.

[1] Izvor: https://narodne-novine.nn.hr/clanci/sluzbeni/2015_07_82_1567.html Datum: 23.11.2017.

2.1. Vizija i misija Državne uprave za zaštitu i spašavanje

Vizija[2]

Državna uprava za zaštitu i spašavanje je vodeća organizacija zaštite i spašavanja ljudi, dobara i okoliša u Republici Hrvatskoj, primjerena potrebama suvremenog društva

Misija

Ustrojiti i održavati moderan sustav zaštite i spašavanja u Republici Hrvatskoj koji će svim raspoloživim resursima biti sposoban odgovoriti potrebama u zaštiti ljudi, dobara i okoliša u ugrozama, stradanjima i drugim izazovima suvremenog društva, a prema potrebi pružiti pomoć drugim ili primiti pomoć drugih zemalja.

[2] Izvor: http://duzs.hr/o-nama/ Datum: 23.11.2017.

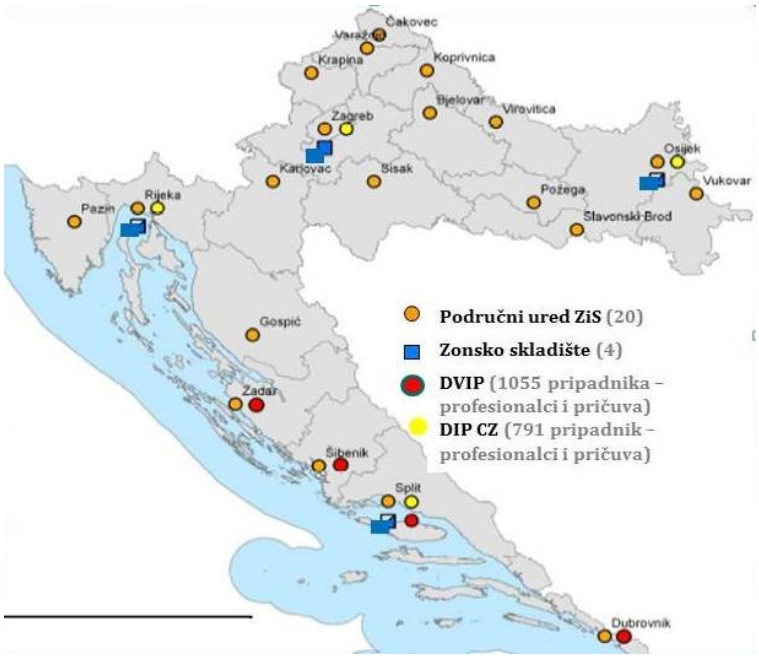
3. Zatečeno stanje

Infrastruktura DUZS-a u ovom radu je prikazana prije nadogradnje sustava odnosno zatečeno stanje koje je bilo namijenjeno za prilično ograničeno poslovanje.

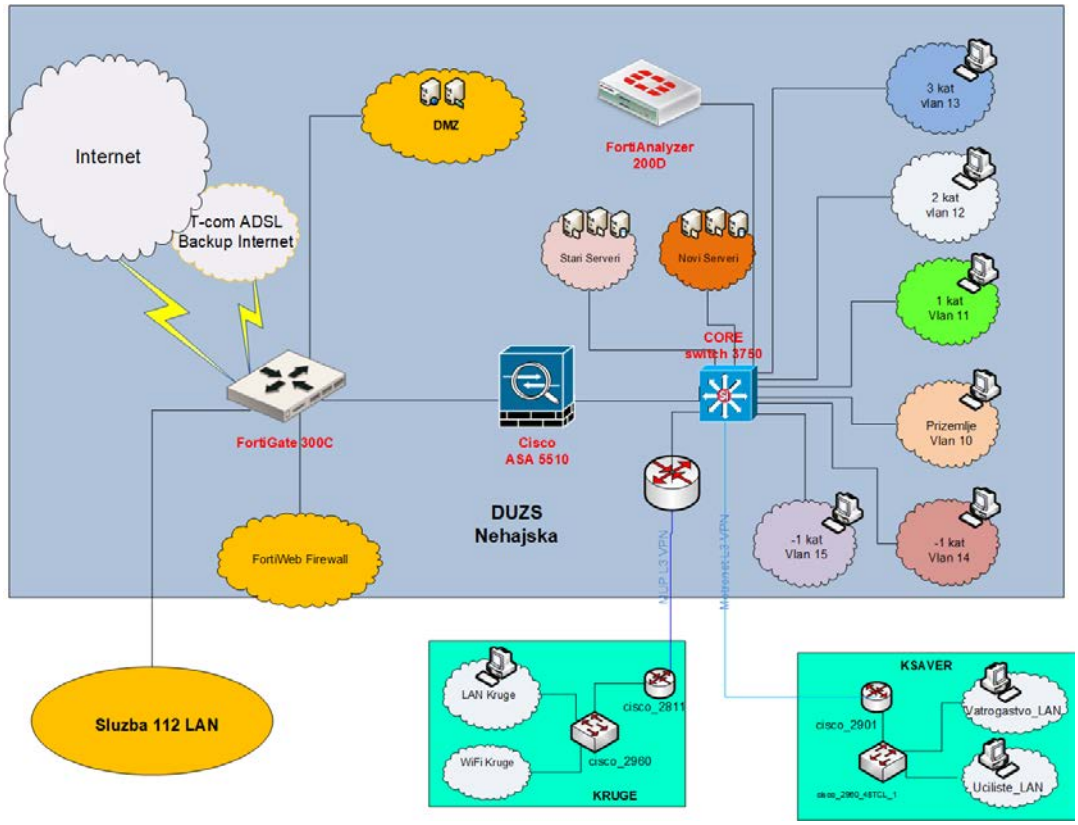
- Razmjena informacija, dokumenata isključivo putem e-maila ili putem prijenosnog medija
- Vlastiti pristup Internetu svake lokacije bez centralnog nadzora i kontrole

Danas ukoliko trebate angažirati jednog ili više djelatnika koji će obilaziti vaše podružnice ili koji će nazivati telefonskim putem druge djelatnike jer nedostaju neki dokumenti pa tražiti da se isti pošalju mailom odnosno skupljati na prijenosne medije važne informacije, da bi iste pohranili na centralnu lokaciju jasno je da takvo poslovanje nije profesionalno. Svaki područni ured koristi vlastiti pristup internetu, bez ikakvih ograničenja što se tiče sadržaja koji se pretražuju na internetu s tim se pristupom omogućava malicioznim programima da ozbiljno ugroze korisničko poslovanje. Uzevši u obzir ovako velike nedostatke u poslovanju pravo je čudo da se isto uopće uspjelo održati.

Navedena ograničenja tj. nedostaci predstavljaju ogroman problem u samom poslovanju DUZS-a prvenstveno zbog budućih aplikacija koje će biti implementirane na svim lokacijama uključujući i centralnu. DUZS sačinjava sedamnaest udaljenih lokacija Područni ureda (PUZS) rasprostranjenih po cijeloj hrvatskoj i jedna centralna lokacija u Zagrebu kao što je prikazano na slici 3.1.



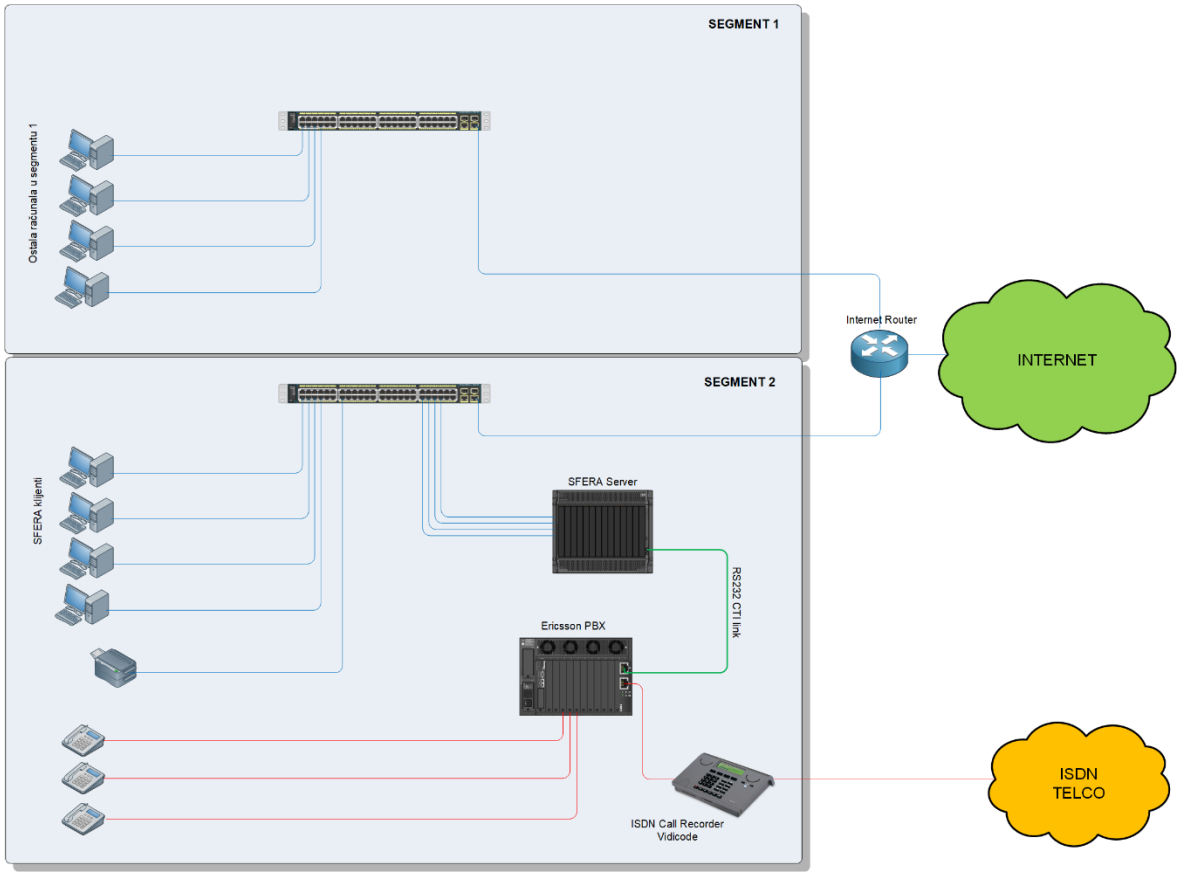
Slika 3.1 PUZS lokacije po hrvatskoj[3]



Slika 3.2 Logička topologija centralna lokacija prije nadogradnje[4]

[3] Izvor: Državna uprava za zaštitu i spašavanje 23.11.2017.
[4] Izvor: Vlastiti rad autora 23.11.2017.

Svaki područni ured ima identičnu *hardwaresku* infrastrukturu kao što prikazuje slika 3.2.



Slika 3.3 Fizička topologija centralne lokacije prije nadogradnje[5]

Na vrhu kao rubni uređaj je usmjerivač na kojem su priključena dva preklopnika koji su predstavljali dva odvojena mrežna segmenta. Segment 1 na slici 3.3 predstavlja korporacijski dio, i služi za gore navedeno kao ograničenja u poslovanju. Svi područni uredi koriste „svoj" Internet. Takvi primjeri povezivanja na Internet je ne moguće pratiti odnosno kontrolirati. Djelatnici nemaju nadzora pa se posjećuju stranice koji konzumiraju puno *bandwitha,* a kao rezultat toga su prijave ostalih djelatnika da je internetska veza spora ili je u prekidu. Segment 2 na slici 3.3 služi za kompletno zatvoren sustav odnosno komunikacija se odvija isključivo lokalno untar pojedine lokacije. U toj komunikaciji sudjeluju računala na kojima su instalirani klijenti, snimač poziva, poslužitelj te telekomunikacijska centrala. Obzirom da se svi 112 pozivi snimaju, tako glavnu ulogu predstavlja „Vidicode" odnosno snimač poziva.

Vidicode je dizajniran na način da bez nadzora odnosno bez ljudske interakcije kontinuirano snima pozive te ih pohranjuje na integrirani čvrsti disk velikog kapaciteta. Veliki kapaciteti

[5] Vlastiti rad autora 23.11.2017.

diska omogućavaju pohranu 20700 sati poziva, bez kompresije. Moguća je i komprimiranje diska pa kapacitet raste dvostruko 41400 sati za pohranu poziva. Jedna zanimljivost kod snimača poziva je, da integrirani diskovi nakon što potroše svoj kapacitet pohrane poziva, pozivi se i dalje pohranjuju samo najstariji poziv prebrisan je najnovijim. Pohranjenim pozivima je moguće pristupiti putem IP adrese, potrebna je samo instalacija klijenta na bilo koje računalo sa bilo kojim operacijskim sustavom koji se dobije prilikom kupnje Vidicoda.

Potreba za drugim segmentom se pojavila nakon što je pružatelj usluga omogućio geolokaciju prilikom poziva unesrećene osobe na broj 112. Prednost u takvom okruženju DUZS je odlučio dizajnirati programsko rješenje CTI *(Computer Telephone Integration)* nazvan „Sfera“.

Sfera ima mogućnost preusmjeravanja žurnih poziva iz bilo koje županije prema potrebnoj žurnoj službi (policija, vatrogasci, hitna pomoć) s zatečenog područja i k tome kreirati zapise o pozivima kao što su vrijeme poziva, te trajanje istog. Budući da je ovaj sustav implementiran na sve udaljenje lokacije uključujući centralnu lokaciju u Zagrebu, ideja o pohrani metapodatka od strane Sfere je da se isti pohranjuju na centralnoj lokaciji u Zagrebu. Metapodaci su vrijeme poziva, trajanje te geolokacija istog. Kao što je već navedeno, ova pohrana se radila na način da se prvo podaci spremaju lokalno na svaku od lokacija, te nakon nekom vremena dostavljaju u Zagreb putem kurirske službe te konačno pohranjuju na centralni poslužitelj. Ovaj način pohrane podataka nije adekvatan iz puno razloga, kao npr. oštećenje medija na kojem se isti prenose, gubitka istog itd.

Iz ovog opisa jasno je uvidjeti da postoji nedostatak u mrežnoj infrastrukturi koja bi zamijenila proces prijenosa podataka ljudskim faktorom sigurnim i pouzdanim komuniciranjem udaljenih lokacija sa centralnom lokacijom. Jer postoji mogućnost gubitka podataka, i još važnije podaci nisu aktualni.

4. Projekt unaprijeđena DUZS - IT sustava 112

4.1. Korisnički zahtjevi

Prilikom poslovanja nekog poduzeća kojem nije jezgra poslovanja IT, nego im je IT potreban u smislu olakšavanja poslovanja gotovo uvijek zahtjevi sa perspektive mrežne infrastrukture takvih poduzeća se zasnivaju na tri ključna elementa:

- Stabilnost
- Pouzdanost
- Sigurnost

Kako je opisano u infrastrukturi zatečenog stanja DUZS raspolaže sa sedamnaest PUZS lokacija i jednom centralnom lokacijom.

Korisnički zahtjevi bazirani su za sljedeće kriterije:

- **Povezivanje Geografski raširenih lokacija**
  - Svaka PUZS lokacija mora moći komunicirati sa centralnom lokacijom
  - Na svakoj PUZS lokaciji mora postojati dva odvojena mrežna segmenta
  - Sfera mrežnom sustavu ograničiti pristup internetu
- **Raspodjela resursa**
  - Propusnost (Ovisno o PUZS lokaciji)
- **Kvaliteta usluge**
  - SLA *(Service Level Agreement)*
  - Pouzdanost
  - Privatnost
  - Skalabilnost
  - Prioriteti za 112 VoIP mrežu
  - Ograničenja brzina
- **Sigurnost**
  - Promet između lokacija mora biti kriptiran

4.2. Prijedlog mogućih rješenja

Prijedlog mogućih rješenja opisanom u ovom poglavlju referenciran je na korisničke zahtjeve.

Sumarnim pregledom korisničkih zahtjeva dolazi se do zaključka da jedan dio zahtjeva se odnosi na konfiguraciju preklopnika. Razdvajanje segmenta na preklopnicima lako se izvodi na istima koji imaju mogućnost virtualizacije VLAN *(Virtual Local Area Network).*

Kako je opisano u zatečenom stanju na PUZS lokacijama prije nadogradnje sustava bila su dva preklopnika koja nisu imala mogućnost virtualizacije. Zamjenom tih preklopnika novim inteligentnim preklopnikom te implementacijom VLAN-ova mreža je segmentirana na svakoj od lokacija na VLAN1 koji je prozvan „nesigurna mreža“ i VLAN2 „sigurna mreža“. Sigurna mreža odnosila se mrežni segment sustava Sfere, dok nesigurna na ostala računala u PUZS centru.

U korisničkim zahtjevima je navedeno da mreža sustava Sfere mora imati određena ograničenja prilikom pristupa internetu što uključuje svega nekoliko web stranica, te da sve PUZS lokacije moraju moći komunicirati sa centralnom lokacijom na siguran način sa oba svoja mrežna segmenta. Promet sa svih PUZS lokacija prema centralnoj lokaciji mora biti kriptiran.

Također je navedeno da su potrebna ograničenja brzina na PUZS lokacijama, a odnosilo na sljedeće:

- 40Mbit/s za sve područne urede
- 2 Mbit/s prema Internet resursima s 112 mrežnog segmenta

Za navedene brzine kriteriji su bili najbolji omjer cijene i pružene usluge s obzirom na potrebe svake lokacije što je određeno kroz promatranje tijekom dugoročnog rada tih lokacija. Za sve područne urede je dozvoljen pristup svim resursima na internetu osim kategorija kao što stranice ne primjerenog sadržaja.

Kako je već navedeno da MPLS pruža jamstvo, to se odnosilo na zakupljene brzine. DUZS je zakupio od pružatelja usluga svojim svim područnim uredima 20Mbit/s za pristup internetu, te 100Mbit/s za centralnu lokaciju. Obzirom da sve lokacije prilikom pristupanja internetu prolaze kroz centralnu lokaciju, potrebno se zaštiti kako se ne bi resursi iscrpili, u ovom slučaju *bandwidth.* Stoga su za sve područne urede stavljena dijeljena brzina od

40Mbit/s, te jamčena brzina od 10Mbit/s. Ovo znači ukoliko vrlo malo lokacija odjednom pristupa prema internetu, te lokacije mogu imati do 40Mbit/s, no ukoliko sve lokacije odjednom pristupaju te se brzina znatno naruši, tu je jamčena brzina koja nikad neće pasti ispod 10Mbit/s kako je definirano na vatrozidu centralne lokacije. Dodatno svi 112 područni uredi za svojih nekoliko dozvoljenih resursa na internetu koriste brzinu od 2 Mbit/s, odnosno jamčenu brzinu od 1,4Mbit/s. Popis Internet stranica koje su dostupne za 112 su na slici 4.3. Brzina od 2Mbit/s je dovoljna za navedene stranice jer za otvaranja istih nije potrebno puno *bandwitha.*

Name	Type	Guaranteed Bandwidth	Max Bandwidth
F-Secure-Shaper	Shared		2500 Kbps
guarantee-100kbps	Shared	100 Kbps	1048576 Kbps
high-priority	Shared		1048576 Kbps
low-priority	Shared		1048576 Kbps
MAX-2Mbit-112	Per-IP		2000 Kbps
medium-priority	Shared		1048576 Kbps
MS-Update-Shaper	Shared		10000 Kbps
Shaper-2Mbit-112	Shared	1400 Kbps	2000 Kbps
Shaper-15Mbit-Udaljene-WSUS	Shared	2000 Kbps	15000 Kbps
Shaper-40Mbit-UdaljeneLokacije	Shared	10000 Kbps	40000 Kbps
shared-1M-pipe	Shared		1024 Kbps

Slika 4.1 Popis ograničenja za različite mrežne segmente[6]

[6] Vlastiti rad autora, 23.11.2017.

URL Filter

Create | Edit | Delete

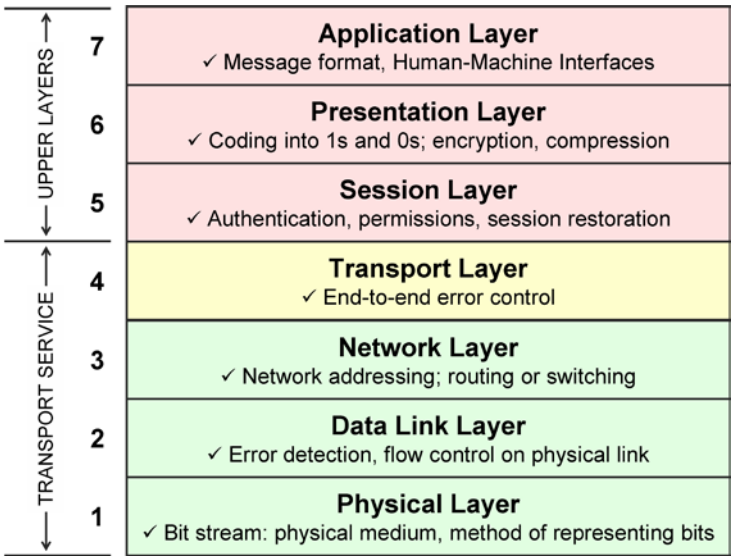
URL	Type	Action	Status
.duzs.hr	Wildcard	Monitor	Enable
.giscloud.com	Wildcard	Monitor	Enable
.alert.hvz.hr	Wildcard	Monitor	Enable
.vatrogasna-mreza.com	Wildcard	Monitor	Enable
.vatronet.hvz.hr	Wildcard	Monitor	Enable
.hvz.hr	Wildcard	Monitor	Enable
.vzzz.hr	Wildcard	Monitor	Enable
10.190.201.245	Simple	Monitor	Enable
.voda.hr	Wildcard	Exempt	Enable
.meteo.hr	Wildcard	Exempt	Enable
.dhmz.	Wildcard	Monitor	Enable
.google.com/earth/	Wildcard	Exempt	Enable
.google.com/maps/	Wildcard	Exempt	Enable
earth.google.com/	Wildcard	Exempt	Enable
.hak.hr	Wildcard	Exempt	Enable
.nn.hr	Wildcard	Exempt	Enable
.	Wildcard	Block	Enable
.hvz.giscloud.com	Wildcard	Monitor	Enable
.bing.com/mapspreview	Wildcard	Exempt	Enable
.pljusak.com	Wildcard	Monitor	Enable

Slika 4.2 Popis dozvoljenih stranica za 112 segment[7]

Navedene stranice prikazane na slici 4.3 su dopuštene isključivo zato jer djelatnici DUZS-a koji rade u službi 112 imaju na raspolaganju sve potrebne informacije u slučaju bilo kakvog upita. Sve ostale stranice su za ovaj segment zabranjene, te u ukoliko jedan od djelatnika želi pristupiti stranicama koje nisu na popisu dozvoljenih, za to se koriste ostala računala u centru.

Iz ovoga jasno je vidljivo da je potrebna implementacija NGFW *(Next Generation FireWall)* vatrozida. Implementacijom NGFW dobivamo na mogućnosti analize prometa svih sedam *OSI (Open System InterConnection)* slojeva. OSI Referentni model kojim se opisuje način komunikacije na mreži. Dijeli se na sedam slojeva[8] prikazanih na slici 4.3.

[7] Vlastiti rad autora, 24.11.2017.
[8] Izvor: http://www.freeccnastudyguide.com/study-guides/ccna/ch1/1-3-osi-reference-model/
Datum: 25.11.2017



Slika 4.3 Prikaz sedam OSI slojeva[9]

Kako slika 4.2 pokazuje dozvoljene stranice za Sfera mrežni segment, vatrozidi koji ne pripadaju skupiti NGFW imaju mogućnost filtracije prometa isključivo od L2 do L4 OSI referentnog modela. Obzirom da se u ovom slučaju radi o filtraciji na aplikativnom sloju, to potvrđuje nužnost implementacije NGFW-a. Uz mogućnost filtriranja prometa na aplikativnom sloju NGFW također imaju i mogućnost sljedećih funkcionalnosti:

- IPS *(Intrudion Prevetion System)*
- Kontrola aplikacija
- Antivirus
- Optimiziranje brzine
- DLP *(Data Lost Prevention)*
- Web Filter

Za sve lokacije uključujući i centralnu lokaciju odabran je proizvođač NGFW FortiNet. Ovisno o modelima te o zahtjevima lokacije implementirani su sljedeći uređaji:

- Zagreb centralna lokacija – FortiGate 400D
- Split DR site – FortiGate 300C
- Sve ostale PUZS lokacije FortiGate 30D

[9] Izvor:https://www.techpluto.com/osi-model-explanation/ , 25.11.2017.

	Cisco ASA 5525-x	FortiGate 400D
Integarted Antrivirus	✓	✓
Protocols Scanning	✗	HTTP,POP,IMAP
File Extension Type Scanning	✗	✓
Encrypted VPN Inspection	✓	✓
Encryption Protocols	AES, 3DES	DES, 3DES, AES128, AES192, **AES 256**
Firewall Throughput	650 Mbps	16 Gbps
IPS Throughput	600 Mbps	2.8 Gbps

Tablica 4.1 Usporedba dvaju NGFW za centralnu lokaciju[10]

Odgovor na pitanje zašto FortiGate dobiven je temeljem puno pozitivnog iskustva u radu s ovim uređajem od strane inženjera u IT industriji. Omjer cijene i performansi također ide u prilog ovom proizvođaču relativno na druge uređaje.

Slika 4.4 Gartner 2017 Magic Quadrant for Enterprise Network Firewalls

[10] Izvor: https://www.techpillar.com/comparison/network-security/fortigate-400d-VS-cisco-asa-5525-x
Datum: 27.12.2017

Gartner Magic Quadrant [11](MQ) predstavlja izvješće koje je rezultat istraživanja tržišta u svijetu relevantne IT konzultantske tvrtke Gartner, a koja se oslanjaju na vlastite kvalitativne metode analize podataka za pokazivanje tržišnih trendova. Njihove se analize provode za nekoliko specifičnih tehnoloških industrija i ažuriraju se svake 1-2 godine.

Za svaki od korisničkih zahtjeva puno jednostavnije je odabrati opremu odnosno proizvođača koji ima funkcionalnosti za ispunjavanje istih. Ono što predstavlja izazov se odnosi na odabir tehnologije koja će biti odgovorna za prijenos podataka sukladno korisničkim zahtjevima.

Kao moguća tehnička rješenja, njihove prednosti i nedostaci u ovom poglavlju će biti opisane dvije glavne tehnologije:

- **DMVPN** *(Dynamic Multipoint Virutal Private Network)*
- **MPLS L3 VPN** *(Multi Protocol Label Swtiching L3 VPN)*

Ovaj rad će se bazirati na ključnim razlikama ovih tehnologija, jer je to upravo ono presudno za svakog korisnika u odbiru rješenja za svoje poslovanje.

Počevši od toga što je zajedničko ovim tehnologijama je da bi iste radile ne moraju imati uključene mehanizme kriptiranja . Počevši od toga što je zajedničko ovim tehnologijama je da bi iste radile ne moraju imati uključene mehanizme kriptiranja. Česta pogreška kod većine korisnika je što akronim VPN *(Virtual Private Network)* povezuju s kriptiranjem zbog čestog korištenja VPN pristupa prema tvrtkama u kojima određeni korisnici rade. Svaki korisnik od IT osoblja u svojoj tvrtki dobije objašnjenje da VPN konekcija je kriptirana. Kao što je već navedeno kod ovih tehnologija ukoliko se želi promet između lokacija kriptirati, potrebno je

[11]Izvor:https://www.forcepoint.com/resources/industry-analyst-reports/gartner-2017-magic-quadrant-enterprise-network-firewalls
Datum: 01.12.2017

koristiti IPsec protokol uz jednu od odabranih tehnologija. Zajedničko im je i mogućnost povezivanja više lokacija sa jednom centralnom lokacijom.

Razlike ovih tehnologija koje su opisane u ovom poglavlju omogućit će nam jasniju sliku na temelju koje ćemo odabrati adekvatno rješenje za implementirati u sustav korisnika.

4.3. DMVPN

DMVPN protokol je u početcima dizajniran za *Hub-and-Spoke* mrežne dizajne. Ovaj tip dizajna je idealan ako imate jednu centralnu lokaciju i više udaljenih lokacija. Ako bolje pogledamo DUZS-ova mrežna infrastruktura upravo predstavlja takav dizajn. No, problem se javlja je postoje tri načine implementacije DMVPN protokola ovisno o korisničkih zahtjevima[12]. Dakle odmah u analizi korisničkih zahtjeva je potrebno odabrati način implementacije jer svaki od načina predstavlja promjene u funkcionalnosti.

U prvom načinu implementacije DMVPN-a moguća je direktna komunikacija isključivo između jednog područnog ureda i centralne lokacije. Ako neki područni ured želi komunicirati s drugim područnim uredom sva komunikacija mora proći kroz centralnu lokaciju.

U drugom načinu implementacije sličan scenarij s jedinom razlikom što na centralnoj lokaciji usmjerivač s protokolom NHRP *(Next Hoop Resolution Protocol)* može detektirati da se radi o komunikaciji između područnih ureda. Nakon detekcije, dolazi do automatske uspostave tunela između područnih ureda, te se komunikacija ostvaruje bez posredovanje centralne lokacije. Dinamički tuneli postoje određeno vrijeme, nakon isteka vremena tuneli između područnih ureda se zatvaraju. Bitno je za naglasiti da kompletna usmjerivačka tablica za sve područne urede se nalazi na centralnoj lokaciji.

Treći način implementacije je samo nadogradnja na drugi način. Nadogradnja se odnosila na jedini nedostatak drugog načina implementacije. Ukoliko s vremenom na jednom od područnih ureda dođe do implementacije više mrežnih segmenta, za svaki taj mrežni segment centralna lokacija mora poslati na sve druge područne urede specifičnu putanju kako bi se mogla ostvariti komunikacija s tim novim mrežnim segmentom. Jasno je vidljivo

[12] Izvor: https://learningnetwork.cisco.com/blogs/vip-perspectives/2017/02/15/dmvpn-the-phases-in-depth

Datum: 08.01.2018

da ovaj dio mora administrator konfigurirati na centralnoj lokaciji odnosno na svim područnim uredima. Ovaj način ima mogućnost slanja poruka sa centralne lokacije na sve područne urede, koja je davala do znanja usmjerivačima da postoji bolja putanja za novi mrežni segment odnosno da postoji „prečica“ do istog bez komunikacije sa centralnom lokacijom. Omogućavanje slanja poruka sa centralne lokacije prema svim područnim uredima potrebno je na centralnom usmjerivaču omogućiti *ip nhrp redirect,* te na usmjerivačima područnih ureda *ip nhrp shortcut.*

Važno je spomenuti da kompletna administracija ovog protokola je na korisničkoj strani odnosno inženjerima koji administriraju mrežu korisnika. Obzirom da su načini implementacije nastajali kako je vrijeme odmicalo od trenutka prve pojave ovog protokola implementacijom zadnjeg načina dobiva se na prostoru u smislu skalabilnosti korisničke mreže. Problem se javlja što je ovaj protokol skalabilan do jedne točke, odnosno obzirom da u komunikaciji između svih udaljenih lokacija sudjeluje i centralna lokacija, porastom broja udaljenih lokacija može narušiti performanse usmjerivača na centralnoj lokaciji. Ukoliko korisnik odluči proširiti mrežne segmente na područnim uredima pojavljivat će se problem kod usmjeravanja prometa prvenstveno ukoliko je potrebna komunikacija između područnih ureda što je objašnjeno gore u mogućnostima implementacije različitih načina ovog protokola. Sukladno tome, javljat će se problem sa kompleksnošću konfiguracije jer sve promjene radi administrator za korisnika ili sam korisnik.

Budući da je navedeno da promet mora biti kriptiran DMVPN ima mogućnost integracije IPsec protokola kako bi zaštitio promet. Što se tiče kvalitete usluge DMVPN nema nikakve mehanizme jamstva odnosno kako DMVPN povezuje lokacije preko interneta, čak i ako se zakupe velike brzine na krajevima tunela vaša latencija ovisi o drugim usmjerivačima preko kojih se vaša komunikacija ostvarila. Kako je poznato da je VoIP komunikacija jako osjetljiva na zagušenja u mreži, a DUZS koristi 112 pozive za unesrećene bitno je da se ova komunikacija ostvaruje besprijekorno. Također ne postoji nikakav SLA *(Service Level Agreement)* od strane pružatelja usluga u slučaju da se lokacije korisnika povezuju preko javne mreže interneta.

Ono što je vrlo bitna stavka DMVPN je u vlasništvu Cisco te ga je moguće implementirati isključivo na Cisco uređaje, što dodatno predstavlja trošak nabave Cisco uređaja. Čak i da

ne postoje financijska ograničenja problem se javlja što NGFW od Cisco nemaju mogućnost implementacije DMVPN-a.

4.4. MPLS L3 VPN

MPLS L3 VPN je usluga koju pružaju davatelji usluga tako da korisnicima njihov mrežni promet implementiraju u vlastito okruženje. Na taj način skidaju odgovornost s korisnika, te isto preuzimaju iz čega u konačnici proizlazi pouzdana komunikacija. S aspekta korisnika ogromna prednost u odnosu na DMVPN je što korisnik nije svjestan tehnologije kojom raspolaže jer za kompletnu administraciju MPLS L3 VPN-a odgovoran je pružatelj usluga.

Velika prednost MPLS L3 VPN relativno na DMVPN se odnosi na to što komunikacija unutar MPLS L3 VPN se odvija unutar mrežne infrastrukture pružatelja usluga[13], dakle mrežni promet korisnika nije nikada izložen javnoj nesigurnoj mreži Internet.

Što se tiče kvalitete usluge, opet dajemo veliku prednost MPLS L3 VPN-u koji ima mehanizme kojima može jamčiti brzine i latenciju između udaljenih lokacija jer kao što je već spomenuto komunikacija se odvija pod jurisdikcijom pružatelja usluga, te isti imaju točno kontrolu kojim putem vaša komunikacija se ostvaruje.

Kako je već navedeno DUZS-ova usluga 112 je najbitniji i najosjetljiviji dio poslovanja, što znači da ova mreža mora biti uvijek dostupna i funkcionirati bez ikakvih smetnji prilikom poziva unesrećene osobe. Pružatelj usluga također ima opciju za implementacijom MPLS EF *(Expedited Forwarding)* odnosno jednog od QoS *(Quality of Service)* mehanizma gdje pružatelj usluga kroz svoju mrežu postavlja najveći prioritet za DUZS-ovu 112 mrežu, kojim jamči da, čak i u slučaju da u mreži davatelja usluga dođe do zagušenja, pozivi prema 112 imaju prednost u odnosu na bilo koji drugi mrežni promet.

U ovom poglavlju već je navedeno da MPLS L3 VPN usluga sama po sebi ima elemente privatnosti korisničkog prometa, moguće je promet dodatno kriptirati IPsec protokolom kao

[13]Izvor:http://www.ciscopress.com/store/ccie-routing-and-switching-v5.0-official-cert-guide-9781587144929
Datum: 17.01.2018

najvišu razinu sigurnosti. Kombinacijom MPLS L3 VPN usluge i IPSec protokola postižemo u potpunosti sigurnu komunikaciju između bilo koje dvije točke sustava.

MPLS L3 VPN uslugu je potrebno kupiti od pružatelja usluga, a budući da je MPLS L3 VPN usluga koja je u nadzoru od strane pružatelja usluga također je moguće ostvariti i vrlo visoke razine SLA.

Razlike	DMVPN	MPLS L3 VPN
SLA	✗	✓
Jamstvo	✗	✓
IPsec	✓	✓
Ograničenje na proizvođača	✓	✗
Skalabilnost	Ograničena	Neograničena
Administracija	Korisnik	Pružatelj usluga

Tablica 4.2 Prednosti i nedostaci mogućih rješenja[14]

SLA je dokument koji se sklapa između dvije tvrtke[15]. Danas je SLA standard u svijetu. Svaka tvrtka koja plaća uslugu drugoj tvrtki, potpisuje SLA sa definiranim vrijednostima ovisno o projektu. Dodatno vrlo često je u ponudi više mogućnosti SLA, pa sukladno cijeni korisnik može birati najpogodnije za svoje poslovanje.

Ovisno o razini ugovorene usluge između korisnika i pružatelja usluge odnosno o složenosti samog SLA ugovora cijena tog ugovora će biti različita.

Za kompleksne i zahtjevne ugovore po pitanju vremena reakcije, dolaska na lokaciju, uklanjanja kvara i slično cijene su daleko skuplje nego za jednostavne ugovore koji ne zahtijevaju veliki angažman resursa od strane pružatelja usluga. DUZS najviše zbog usluge 112 je odabrao „zlatni“ SLA. Naime, radi se o najvišem prioritetu te se pružatelj usluga obvezuje ukloniti sve eventualne poteškoće na bilo kojoj od područnih ureda i/ili centralnoj lokaciji u vremenskom roku od 60 minuta. Vrijeme reakcije davatelja usluga mora biti unutar

[14] Vlastiti rad autora, 28.01.2018.
[15] Izvor: http://www.snc-blog.com/2012/03/19/defining-and-differentiating-slas-using-service-levels-gold-silver-and-bronze/
Datum 28.01.2018.

svega nekoliko minuta, jer je korisniku na raspolaganju poseban pristup prijave kvara preko *weba* odnosno poseban kontakt broj gdje nema čekanja do javljanja operatera i sl. Za svaku od područnih ureda i centralne lokacija korisnik ima na raspolaganju identičnu zamjensku opremu kao i inicijalno postavljenu. Kako vrijeme ugovora odmiče korisnik ima pravo zamjene opreme boljih performansi za svako od lokacija bez dodatnih troškova.

Vrijedno je spomenuti da u ovom slučaju korisnik je imao pravu izbora paketa SLA. Kako je *gold* SLA objašnjen također je postojao izbor *silver* i *bronze* SLA.

Silver SLA je identične resurse s aspekta zamjenske opreme za sve lokacije. No, ključna razlika je bila u vremenu reakcije odnosno u slučaju prijave ispada sustava od strane korisnika. Vremena otklanja kvara su bila u roku od 12 sati, te odziv nakon prijave je bio 120 minuta.

Bronze SLA davao je korisniku na raspolaganje osam lokacija i centralnu lokaciju za koju je osigurana zamjenska oprema u slučaju ispada, što je ostavljalo korisniku izbora piratizacije područnih ureda. Obzirom da su svi područni uredi moraju biti dostupni za 112 pozive ovaj uvjet je bio neprihvatljiv. Također u ovom tipu SLA nije postojao poseban kontakt broj za prijavu kvara, što također korisniku ovakve važnosti nije imalo smisla.

Prezentacijom djelatnicima DUZS-a ovog prijedloga mogućeg rješenja, za komunikaciju između svih PUZS lokacija sa centralnom lokacijom odabran je **MPLS L3 VPN**.

4.5. Plan implementacije rješenja

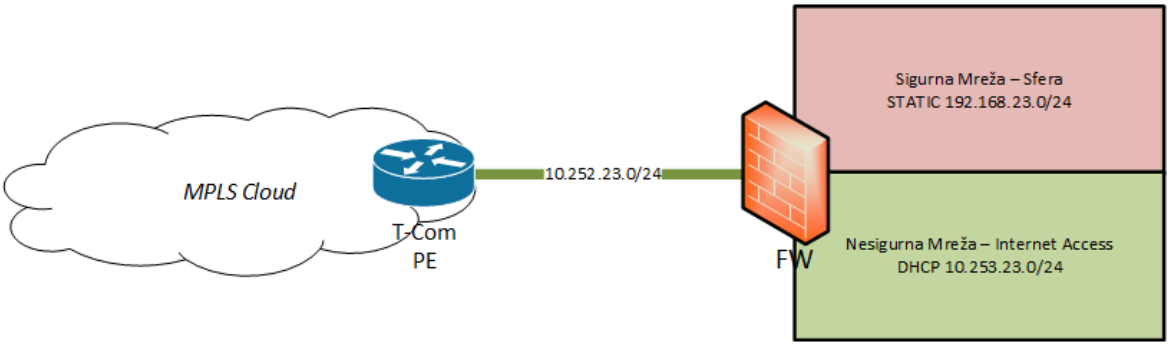
Poglavlje „Plan implementacije“ je opis koraka koji su potrebni prilikom cjelokupnog projekta. Nakon što se određuju resursi koji će biti dodani ovom projektu plan implementacije se može podijeliti u slijedeće cjeline:

- Sastanak s korisnikom
- Sastanak s pružateljem usluge
- Izrada dizajna – adresna shema
- Pružatelj usluga implementacija PE usmjerivača
- Implementacija NGFW-a
- Konfiguracija NGFW-a
- Testiranje rješenja

Sastanak s korisnikom kad je riječ o planiranju implementacije je dogovaranje u kojim vremenskim terminima je moguće implementirati ponuđeno rješenje. Naime, veliku ulogu u ovom koraku ima pružatelj usluga jer je prije implementacije NGFW-a potrebno implementirati MPLS L3 VPN na svim područnim uredima. Vremenski rok koji je potreban pružatelju usluga za navedenu implementaciju je 10 dana. Obzirom da pružatelj usluga također ima podružnicu na svakoj od lokacija gdje su i područni uredi DUZS-a vrijeme za implementaciju MPLS L3 VPN-a je više nego dovoljno.

Bitno je za spomenuti da inicijalni sastanak sa pružateljem usluga i administratora korisničke mreže se morao održati kako bi pružatelj usluga znao koje IP adrese po područnim uredima konfigurirati kako bi usluga bila aktivna.

Izrada dizajna je vrlo jednostavna, jer svaki područni ured ima već postavljen *hardware,* tako da se dizajn odnosio uglavnom na adresne sheme. Shema za svaku od područnih ureda mora biti jedinstvena kako bi MPLS L3 VPN usluga funkcionirala. Područni uredi imaju dva mrežna segmenta sa svega nekoliko *host* uređaja koji su trebali IP adresu. Zbog skalabilnosti mreže za „nesigurni“ segment odabrana je „A“ klasa, a za „sigurni“ segment u kojem se nalazi Sfera sustav „C“ klasa privatnih IP adresa. IP adrese su dogovorene logičkim slijedom. Slika područnog ureda Zadar prikazuje primjer konfiguracije.



Slika 4.4 Primjer adresiranja na područnom uredu Zadar[16]

Na slici 4.5 je su prikazane navedene IP adrese. U ovom odlomku će biti kratko objašnjena logika postavljana istih.

IP adresa 10.252.X.0/24 se odnosi na vezu između usmjerivača pružatelja usluge i vatrozida na lokaciji Zadar. 10.252. je zajedničko za sve područne urede dok „X“ označava pozivni broj grada u kojem se područni ured nalazi. U ovom primjeru je uzet grad Zadar, a pozivni broj za Zadar je „023“ tako treći oktet u IP adresi je upravo broj „23“. Istom logikom su dodijeljene IP adrese za Sfera sustav odnosno segment za pristup internetu. DHCP (*Dynamic Host Configuration Protocol)* je servis koji dinamički dodjeljuje IP adrese svim *hostovima* na mrežnom segmentu. U DHCP protokolu postoji vrijeme do kad pojedini uređaj smije držati dobivenu adresu. Nakon isteka tog vremena uređaj je ponovo zatraži od DHCP poslužitelja koji je u ovom slučaju NGFW FortiGate 30D. Razlog zadnjeg navedenog je što u nesigurnom segmentu nije bitno ako neko računalo koje nije dugo bilo na mreži, pa prilikom komuniciranja dobije različitu IP adresu od prethodne jer ovaj segment služi za manje bite stavke u poslovanju. Sfera sustav ima statički konfigurirane IP adrese te za iste ne vrijedi pravilo isteka što omogućuje nesmetanu komunikaciju između raznih servisa na Sfera sustavu. Zadnja stavka na IP adresi „/24“ označava koliki je broj mogućih IP adresa na određenom segmentu. U ovom slučaju ovaj broj označava 254 moguće adrese odnosno raspon od 10.252.23.1 – 254 koje određeni *host* može dobiti na određenom mrežnom segmentu.

Implementaciju PE *Provider edge* usmjerivača je dio posla u odgovornosti pružatelja usluga. Nakon njihove konfiguracije područnog ureda slijedi implementacija NGFW koja je u

[16] Vlastiti rad autora, 29.01.2018.

odgovornosti korisnika odnosno administratora korisničke mreže. Poglavlje „Opis konačnog rješenja“ opisuje detalje implementacije NGFW-a te konfiguracije istog.

4.6. Opis konačnog rješenja

Nakon što je DUZS prihvatio MPLS L3 VPN kao rješenje, pružatelj usluga je poslao svoje inženjere do svakog područnog ured kako bi postavili svoj konfiguriran usmjerivač prema korisničkim zahtjevima. Navedeni usmjerivač je zadnji uređaj u lancu sa perspektive centralne lokacije.

Budući da je cijeli rad baziran na komunikaciji između centralne lokacije u Zagrebu i ostalih sedamnaest područnih ureda uzet će se primjer jednog područnog ureda jer za ostalih šesnaest je identična konfiguracija. Razlike su samo u adresnoj shemi koja je objašnjena u poglavlju „Plan implementacije rješenja“.

Danas pružatelji usluga posluju sa stotinama tisuća korisnika, bilo oni privatne osobe ili poduzeća. Količina mrežne infrastrukture koja je potrebna kako bi komunikacija bila stabilna i pouzdana i naravno redundantna je vrlo velika, a same mreže vrlo kompleksne. Mreže pružatelja usluga moraju biti takve kako bi postigle adekvatnu razinu robusnosti i pouzdanosti, jer najam infrastrukture i osiguravanje pouzdane komunikacije korisnicima je glavni posao pružatelja usluga i mrežna infrastruktura je ono što im omogućava tržišnu prednost. Pošto pružatelji usluga povezuju veliki broj korisnika preko svoje infrastrukture potrebno je osigurati privatnost komunikacije za svakog pojedinog korisnika. Za tu namjenu koristi se danas nezamjenjiva MPLS L3 VPN usluga. MPLS L3 VPN pružateljima daje mogućnost privatizacije prometa na način da se na jedan usmjerivač virtualno kreiraju više usmjerivačkih instanci i svaka ta instanca može biti za zasebnog korisnika. Što je još zanimljivije moguća su i ponovna preklapanja adresnog prostora, a takvu funkcionalnost ne pruža niti jedna druga tehnologija. Virtualne usmjerivačke instance se zovu VRF *(Virtual Routind and Forwardning).* VRF radi tako da svaka IP adresa koja se doda na usmjerivaču postaje dio jedne zasebne usmjerničke tablice. Usmjerivači koriste ukupne resurse za sve radnje nad paketima za koje su konfigurirani, bilo to usmjeravanje, filtriranje i slično. Današnji usmjerivači imaju mogućnost razdvajanja memorijskog prostora te alociranja istih na određene procese. Kako je i usmjerivačka tablica alocirani dio memorijskog prostora, moguće je kreiranjem VRF-a, odvojiti jedan dio memorije usmjerivača te isti alocirati na

novu usmjerivačku tablicu u tom kreiranom VRF-u. Ono što je bitno za naglasiti jest da dva ili više odvojenih memorijskih prostora mogu nezavisno komunicirati. Ovo se događa se u pozadini, dok s perspektive administratora kreiranjem VRF-a dobiva se mogućnost više usmjerivačkih tablica na jednom usmjerivaču. Na kraju važno je spomenuti kako usmjerivači razlikuju koja od više usmjerivačkih tablica namijenjena za određenog korisnika. Za to se koristi jedinstvena RD *(Route Distinguisher) oznaka.* RD se definira unutar svakog korisničkog VRF-a i usmjerivači je koriste kako bi znali kojem korisniku je promet namijenjen.

Kako je već spomenuto korisnik nema doticaja sa MPLS L3 VPN tehnologijom zato iako već privatnost na visokom nivou korisnik je zahtijevao da komunikacija unutar MPLS L3 VPN oblaka bude kriptirana. Budući da MPLS L3 VPN ima mogućnost integracije sa IPsec protokolom tako da isti je implementiran na svim PUZS lokacijama te centralnom lokacijom. Odabir algoritma za enkripciju podataka je AES256 *(Advanced Encryption Standard).* Broj 256 predstavlja 256 bitnu enkripciju, te ukoliko netko pokuša nasilno „razbiti“ ovaj algoritam slika opisuje koliko potrebnih kombinacija je potrebno za „razbijanje“ istog.

Key Size	Possible combinations
1-bit	2
2-bit	4
4-bit	16
8-bit	256
16-bit	65536
32-bit	4.2×10^{9}
56-bit (DES)	7.2×10^{16}
64-bit	1.8×10^{19}
128-bit (AES)	3.4×10^{38}
192-bit (AES)	6.2×10^{57}
256-bit (AES)	1.1×10^{77}

Slika 4.5 Prikaz mogućih kombinacija za AES256[17]

Enkripcija podatka je jamstvo korisniku, ako dođe do pogrešne konfiguracije unutar mrežne infrastrukture od strane pružatelja usluga te mrežni promet od DUZS-a završi u

[17] Izvor: https://blog.v-comply.com/256-bit-encryption/
Datum 01.02.2018

usmjerivačkoj tablici nekog drugog korisnika taj promet je nemoguće zloupotrijebiti jer je isti kriptiran.

Nakon što je pružatelj usluga implementirao MPLS odmah potom je rađena implementacije NGFW-a po PUZS lokacijama. Dolaskom na lokaciju sa postojeće mrežne infrastrukture se uklonilo dva stara preklopnika i implementirao se novi preklopnik. Iako implementacijom jednog preklopnika umjesto dva izgleda kao lošije rješenje, u ovom slučaju to nije jer je novo postavljeni preklopnik novije generacije te raspoloživi resursi istog zadovoljavaju puno veće zahtjeve od zahtjeva jednog područnog ureda. Novi preklopnih ima mogućnost virtualizacije odnosno logički razdvajanje mrežnih segmenta. Budući da je potrebno razdvajanje Sfera sustava od ostatka mreže, na preklopniku su kreirana dva VLAN-a za „sigurnu“ i „nesigurnu“ komunikaciju.

Obzirom da je Sfera sustav namijenjen za pohranu točnog vremena, trajanja i geolokaciju poziva koje prikuplja od telefonske centrale na svakom područnom uredu. Prikupljene podatke je potrebno sigurno poslati na centralnu lokaciju u Zagreb te prema tim politikama je omogućena komunikacija isključivo prema Sfera sustavu u Zagrebu. Nesigurni segment su bila ostala računala u područnom uredu koji su služili djelatnicima za neograničen pristup prema internetu uz jedino ograničenje, a to je brzina komunikacije koja je regulirana na spomenutih 2Mbit/s.

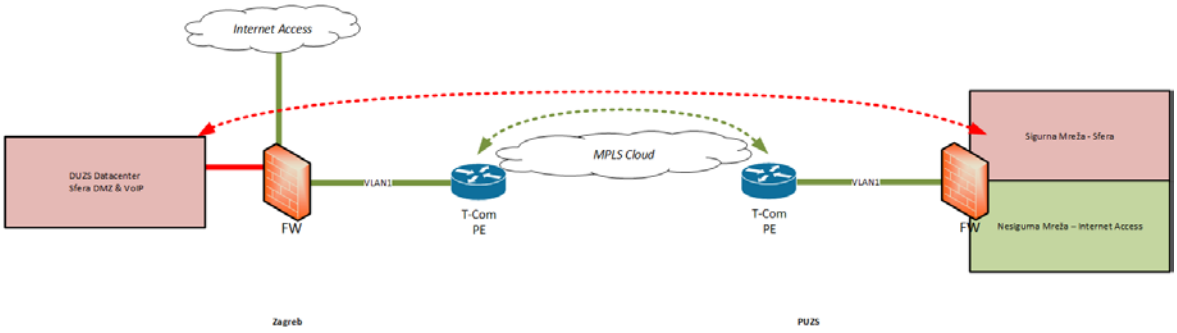
U poglavlju infrastruktura zatečenog stanja je opisano kako je svaki područni ured imao svoj Internet točnije svoj DSL *(Digital Subscriber Line)* usmjerivač. Navedeni usmjerivač je zamijenjen NGFW-om budući da isti ima sve mogućnosti konfiguracije koje je korisnik zahtijevao za svoje područne urede.

Fizička interakcija s opremom je završena, nakon čega slijedi dio same konfiguracije uređaja kako bi uređaji mogli obavljati funkciju za koju su zamišljeni. Potrebna konfiguracija obuhvaća slijedeće elemente:

- Konfiguracija IP adresa
- Kreiranje statičkih ruta
- Kreiranje statičkih tunela
- Kreiranje PBR-a *(Policy-based Routing)*

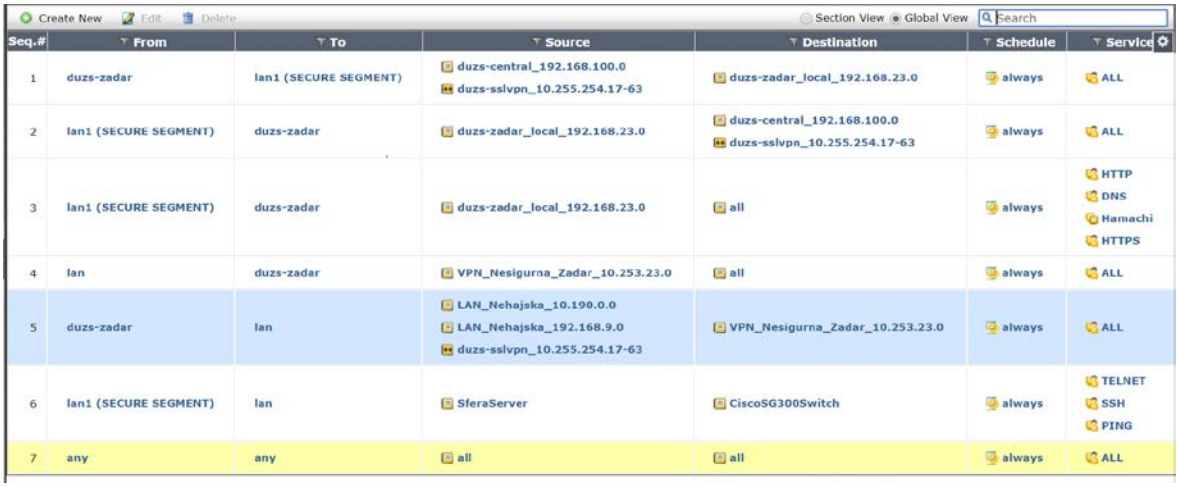
Konfiguracija IP adresa je dogovoreno sa pružateljem usluga budući da konekcija prolazi kroz mrežu pružatelja usluga. Statičke rute služe za usmjeravanje prometa prema željenim destinacijama. Budući da sva komunikacije ide prema centralnoj lokaciji, dovoljno je kreirati

jednu statičku s destinacijom centralne lokacije u Zagrebu s kojim se ujedno i zatvara IPsec tunel, te drugu zadanu rutu koja kompletan promet usmjerava u tunel također prema centralnoj lokaciji u Zagrebu.



Slika 4.6 Konfiguracija PUZS lokacije

PBR je također usmjeravanje prometa po posebnim politikama. Kako je već navedeno za sve lokacije je identična konfiguracija politika, stoga je dovoljno pokazati samo na jednom područnom uredu.


Create New Edit Delete Section View Global View Search

Seq.#	From	To	Source	Destination	Schedule	Service
1	duzs-zadar	lan1 (SECURE SEGMENT)	duzs-central_192.168.100.0 duzs-sslvpn_10.255.254.17-63	duzs-zadar_local_192.168.23.0	always	ALL
2	lan1 (SECURE SEGMENT)	duzs-zadar	duzs-zadar_local_192.168.23.0	duzs-central_192.168.100.0 duzs-sslvpn_10.255.254.17-63	always	ALL
3	lan1 (SECURE SEGMENT)	duzs-zadar	duzs-zadar_local_192.168.23.0	all	always	HTTP DNS Hamachi HTTPS
4	lan	duzs-zadar	VPN_Nesigurna_Zadar_10.253.23.0	all	always	ALL
5	duzs-zadar	lan	LAN_Nehajska_10.190.0.0 LAN_Nehajska_192.168.9.0 duzs-sslvpn_10.255.254.17-63	VPN_Nesigurna_Zadar_10.253.23.0	always	ALL
6	lan1 (SECURE SEGMENT)	lan	SferaServer	CiscoSG300Switch	always	TELNET SSH PING
7	any	any	all	all	always	ALL

Slika 4.7 Područni ured Zadar

Kao što je prikazano na slici vidljivo je da na NGFW-u se nalazi šest usmjerivačkih politika. Ono što je bitno za naglasiti su pojmovi kako bilo jasnije prepoznati pravila navedena na slici.

- duzs_zadar - naziv statičkog tunela
- lan1 - sigurna mreža Sfere sustava
- lan – nesigurna mreža (ostatak računala u PUZS)
- duzs_central – Sfera sustav u Zagrebu

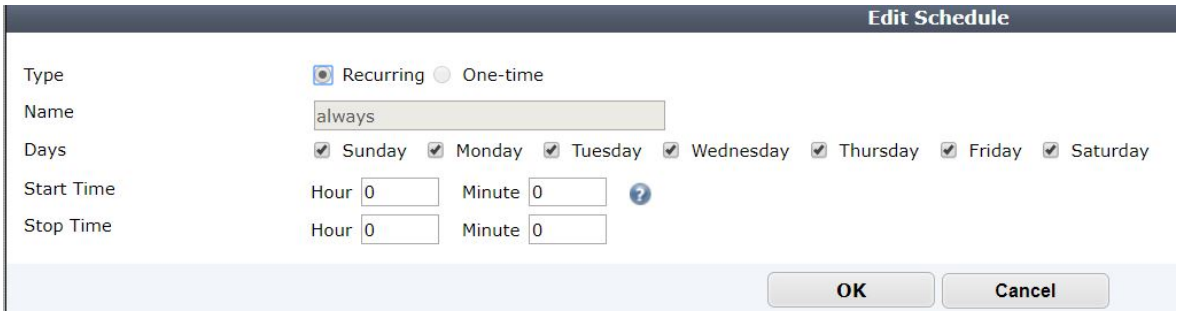
- duzs_sslvpn – VPN adresa

VPN adresa se koristi za siguran pristup korisničkoj mreži putem *web* sučelja. U ovom konkretnom slučaju administratori koriste VPN adresu za administraciju NGFW-a na lokacijama na kojima nisu fizički prisutni.

Polje *Seq* se odnosni na redni broj politike koja je primijenjena. Iako možda izgleda prilično intuitivno jako je bitan poredak ovih politika. Jednom kad vaš NGFW bude uspoređivao paketni promet sa politikama prva tvrdnja u poretku konfiguracije koje će odgovarati primljenim paketima sve ostale tvrdnje ispod ogovarajuće neće uopće biti uzete u obzir. Tako da je jako bitno navesti sve potrebno u odgovarajućoj tvrdnji.

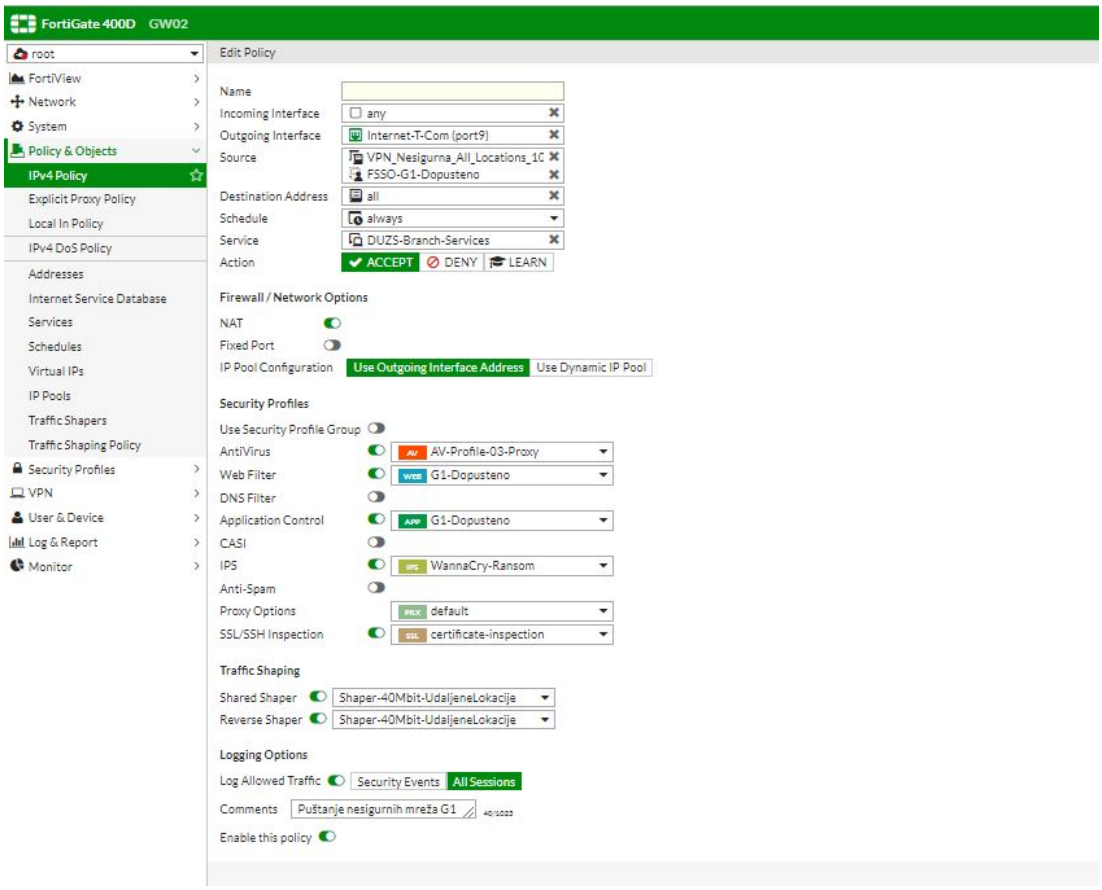
Polje *From* se odnosni sa kojeg sučelja promet odlazi dok polje To se odnosi na sučelje na koji promet dolazi. *Source* je samo izvorišna IP adresa, a *Destination* destinacijska IP adresa.

Također je moguće je u polju *Schedule* odrediti vrijeme kad da se vaša politika primjenjuje. U ovom slučaju *Always* znači uvijek.



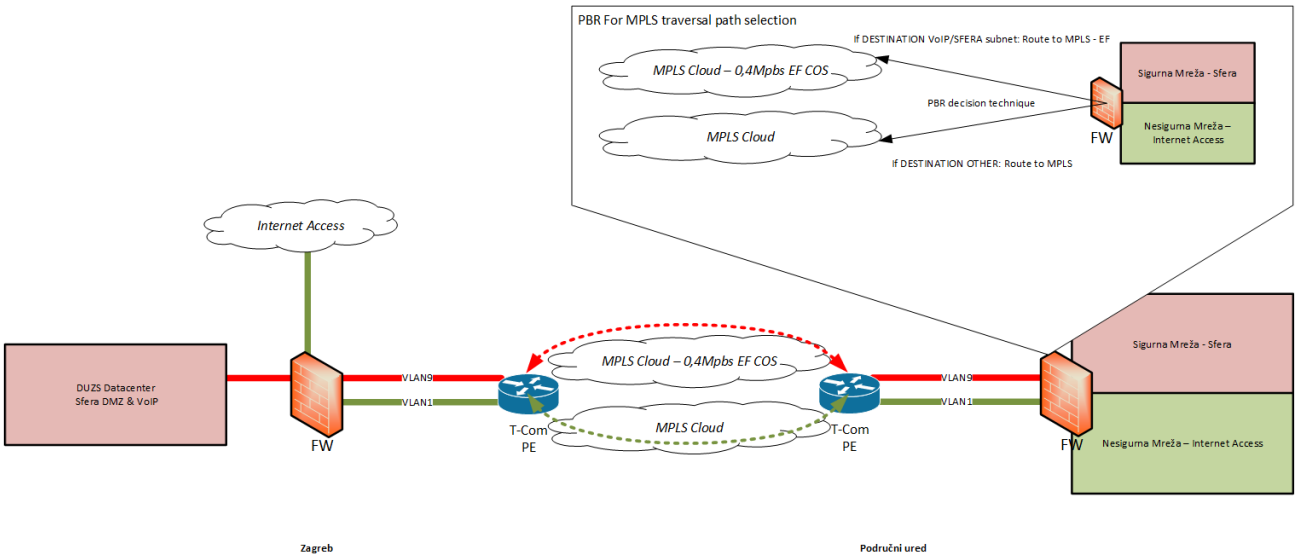
Slika 4.8 Određivanje vremena primjene politike

U polju *Service* je moguće odabrati na koje se IP servise odnosi politika. Ako se označi All svi postojeći servisi će biti propušteni sa navedenih ishodišnih adresa. Budući da postoji jako velik broj servisa u ovom radu neće biti opisa istih. Ipak, svi navedeni servisi moraju biti propušteni na centralnoj lokaciji u Zagrebu.



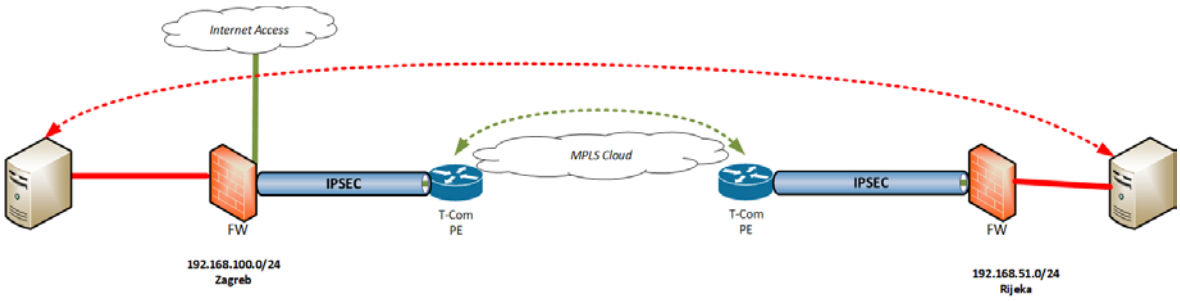
Slika 4.9 Puštanje PUZS nesigurne mreže na Internet

U ovom radu MPLS L3 VPN tehnologija je tzv. „Pouzdan prijenos“ korisničkih paketa iz tog razloga nisu svi tehnički detalji opisani jer je usluga dana korisniku kao konačno rješenje. Najveća prednost MPLS L3 VPN-a u ovom konkretnom slučaju je jamstvo koje pružatelj usluga daje DUZS-u za njihovu 112 mrežu. Naime, riječ je o MPLS EF QoS rješenju za koju pružatelj usluga daje maksimalan prioritet. Na vatrozidu svakog područnom ureda je konfiguriran PBR politika koja usmjerava promet po destinacijskoj adresi. Ukoliko je promet namijenjen za bilo koji „sigurni“ VoIP Sfera segment, taj promet se vraća prema MPLS oblaku pružatelju usluga, gdje isti označava taj promet kao MPLS EF, te ga se odmah prosljeđuje za odgovarajuću adresu. Primjer i logiku konfiguracije MPLS EF se vidi na slici 5.6.



Slika 4.10 PBR politika za MPLS EF

5. Testiranje



Slika 5.1 Instalirana dva D-ITG poslužitelja na udaljenim lokacijama

Testiranje se izvodi nakon implementacije pojedine udaljene lokacije kako bi dokazali funkcionalnost implementiranih tehnologija te korisniku isporučili izvješće sa detaljima o propusnosti, stabilnosti i općenito o eventualnim IP komunikacijskim ograničenjima na pojedinoj lokaciji. Testiranje će se bazirati prema slici 6.1.

5.1. Alati

CentOS računalo na lokaciji koristi se za iniciranje mrežnog testa IP komunikacije UDP probama na svakoj pojedinoj implementiranoj udaljenoj lokaciji prema centralnoj lokaciji u Zagrebu kako bi dokazali funkcionalnost i zadovoljavajuću propusnost implementirane usluge. Što se tiče alata za testiranje, isti će se pokretati na Cent OS 6.8 računalu na udaljenoj lokaciji kao i na Virtualnim Serverima virtualiziranima na VMware hypervisoru na centralnoj lokaciji. VMware je odabran kao jedina platforma za podizanje dodatnih servera/servisa dostupna na svim lokacijama korisnika. Kao software za testiranje IP komunikacije odabran je, u znanstvenoj i tehničkog zajednici posebno dokumentiran i kvalitetom dokazan software D-ITG kojeg i inače koristimo kod sličnih zadataka u projektima KING-ICT.

CeonOS operativni sustav je odabran kao najpouzdanija verzija OS-a na kojoj D-ITG, software za testiranje i generiranje mrežnog prometa, radi najpouzdanije te dostiže najbolje performanse ukoliko je OS virtualiziran.

ICMP

Standardni PING test IP dosega do određene destinacije. *Stateless* proba dokazuje prolazak komunikacije inicirane sa obje strane.

D-ITG 2.8.1

Open Source testni softver za simuliranje i testiranje *unicast* IP komunikacije kojim će se dokazivati funkcionalnost IP komunikacije na implementiranim lokacijama te će se korisniku isporučili izvješće sa detaljima o propusnosti, stabilnosti i općenito o IP komunikaciji pojedine lokacije.

5.2. Način testiranja

Primjer u nastavku prikazati će testove izvedene prilikom implementacije udaljene DUZS lokacije Rijeka. Istovjetni testovi su napravljeni za sve implementirane udaljene lokacije kako bi se prije odlaska inženjera sa lokacije dokazalo da je implementacija prošla uspješno te da se servisi koji ovise o toj novoj komunikaciji mogu osloniti na novu funkciju. Plan izvođenja testiranja

Svaki od planiranih testova je specifičan te mu je namjera da prikaže određenu funkcionalnost sustava ili međudjelovanje više funkcija sustava. Detalji oko izvođenja svakog od testova mogu se naći na sljedećim stranicama te lista u sljedećoj tablici.

Popis izvođenja testova		
1.1	IPSec VPN test ostvarivanja IPSec VPN tunela	PASS: ☐ FAIL: ☐
1.2	Test usmjeravanja (ruting)	PASS: ☐ FAIL: ☐
1.3	Test IP *unicast* prometa	PASS: ☐ FAIL: ☐
1.4	Test propusnost i stabilnosti IP komunikacije	PASS: ☐ FAIL: ☐
1.5	Test određivanja iznosa MTU	PASS: ☐ FAIL: ☐

Slika 2 Plan izvođenja testiranja[18]

[18] Vlastiti rad autora, 15.02.108.

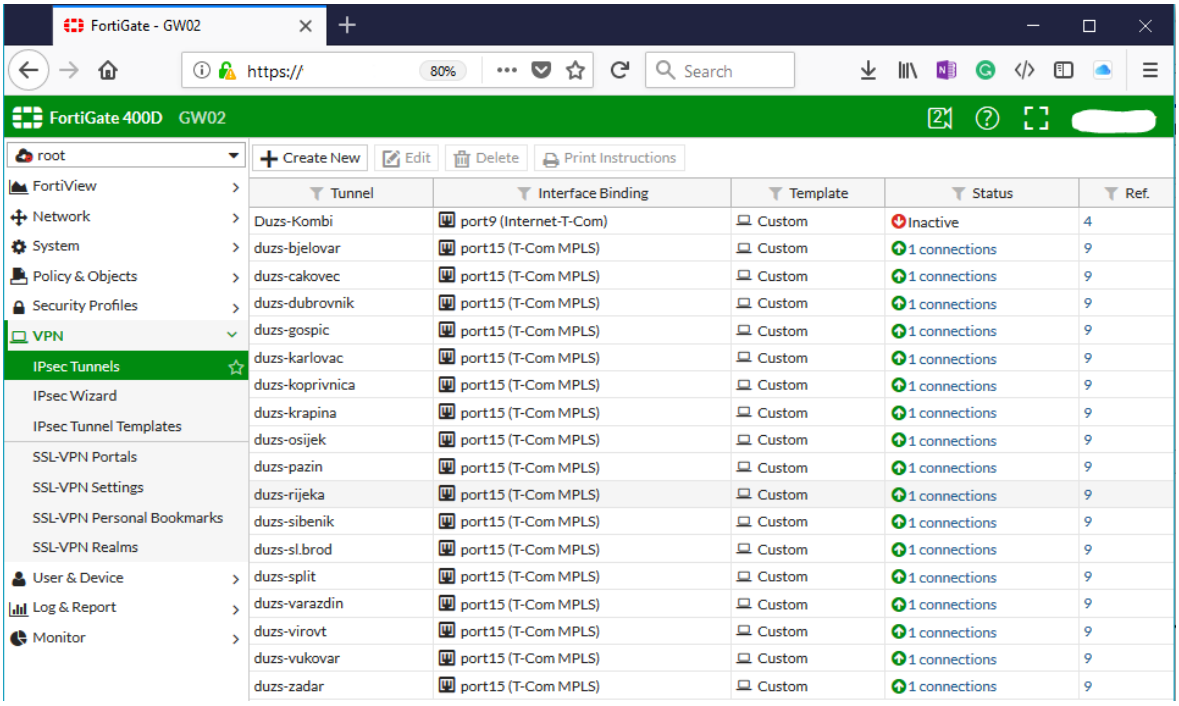
5.3. IPSec VPN test ostvarivanja IPSec VPN tunela

Namjena testa

Test pregledom stanja centralnog vatrozida potvrđuje uspješno podignute IPSec VPN tunele između lokacije Zagreb i trenutno implementiranih lokacija te prikazuje ispis detalja oko ostvarivanja IPSec VPN tunela.

Procedura tijeka testiranja

Administrator se na uređaje spaja HTTPS protokolom s testnog računala te otvara konzolu monitoring VPN tunela gdje dokazuje uspješno uspostavljen IPSec za traženu lokaciju:



Slika 5.3 Statični tuneli svih PUZS lokacija[19]

5.4. Test usmjeravanja *(routing)*

Namjena Testa

Test pregledom stanja centralnog vatrozida prikazujemo uredan ispis usmjerivačke (routing) tablice na centralnoj lokaciji te potvrđuje kako su mreže udaljenih lokacija unutar routing

[19] Vlastiti rad autora, 15.02.2018.

tablice što će omogućiti uredno prosljeđivanje paketa unutar IPSec VPN tunela prema udaljenim lokacijama.

Dodatno se spajanjem sa ZGSRV testnog poslužitelja prema serveru na udaljenoj lokaciji dokazuje da osim konfiguracije usmjeravanja prometa radi i sam IP Unicast prosljeđivanje paketa na temelju unesenih ruta. Razlika između usmjeravanja i prosljeđivanja u ovom slučaju usmjeravanje se bazira na pakete s kojeg *interfacea* je isti ušao, te na koji *interface* paket mora izaći. Usmjeravanje s druge strane se bazira cijeloj putanji, odnosno na parametrima koji određuju najbolju putanju do odredišta.

Postupak testiranja

Administrator se na uređaje spaja HTTPS protokolom s testnog računala te otvara konzolu monitoring IP ruta gdje dokazuje uspješno postavljeno usmjeravanje.

5.5. Test IP *unicast* prometa

Namjena Testa

Test ICMP ping probe prema udaljenoj lokaciji sa centralnog Fortigate vatrozida dokazuje rad IP forwardinga.

Postupak testiranja

Administrator izvodi ICMP ping test prema udaljenoj lokaciji sa centralnog Fortigate vatrozida:

```
GW02 # config vdom

GW02 (vdom) # edit root
current vf=root:0

GW02 (root) # execute ping 10.253.22.1
PING 10.253.22.1 (10.253.22.1): 56 data bytes
64 bytes from 10.253.22.1: icmp_seq=0 ttl=58 time=6.3 ms
64 bytes from 10.253.22.1: icmp_seq=1 ttl=58 time=6.3 ms
64 bytes from 10.253.22.1: icmp_seq=2 ttl=58 time=6.3 ms
64 bytes from 10.253.22.1: icmp_seq=3 ttl=58 time=6.3 ms
64 bytes from 10.253.22.1: icmp_seq=4 ttl=58 time=6.3 ms
```

5.6. Test propusnost i stabilnosti IP komunikacije

Namjena testa

Ujedno i najvažniji te najopširniji test, slanjem UDP proba prikazuje kako je omogućena normalna IP unicast mrežna komunikacija između računala ZGSRV i RISRV koja su smještena u LAN segment centralne lokacije Zagreb (ZGSRV) i udaljene lokacije Rijeka (RISRV). Također, svrha ovoga testa je pokazati da su mrežni parametri (gubitak paketa, kašnjenje i *jitter*[20]) u skladu s očekivanim vrijednostima kako bi korisniku prikazali kako je implementirano rješenje odgovarajuće za buduću implementaciju VoIP telefonije putem ove WAN mreže.

Jitter je razlika kašnjenje *(delay)* paketa prilikom određene komunikacije. Obzirom da VoIP promet je jako osjetljiv na kašnjenja jer nastaju smetnje kao što su isprekidan govor itd. Također jitter prilikom video komunikacije (IPTV) je jako bitan jer ako je isti velik nastaju smetnje na ekranima kao što se „kockice“ po TV prijemnicima i slično.

Naime kod UDP prometa ne postoji mehanizam ponovnog slanja izgubljenih paketa te je vrlo bitno, posebice za VoIP promet, da se gubitak UDP paketa pokuša potpuno izbjeći ili pak smanjiti na najmanju moguću razinu.

Razlika u razmaku između primanja paketa iste IP komunikacije (jitter), uzrokuje probleme kod VoIP prometa zbog povećane mogućnosti stvaranja jeke, šumova te nesinkroniziranog prijenosa razgovora obaju ili više sugovornika što smanjuje kvalitetu razgovora ili ga u najgorim slučajevima potpuno onemogućava.

Planirano generiranje prometa u ovome je testu definirano na način da kroz pola minute dokaže da komunikacija može osigurati najmanje potrebne vrijednosti spomenutih parametara i time dokazati gore navedeno.

Procedura tijeka testiranja

Administrator pokreće UDP probu (test_prema_ri) s testnog poslužitelja ZGSRV na lokaciji u Zagrebu prema IP adresi LAN sučelja testnog poslužitelja na lokaciji u Rijeci RISRV 192.168.51.100.

[20] Izvor: https://howdoesinternetwork.com/2013/jitter
Datum 15.02.2018.

Nakon odvijanja prvog testa (test_prema_ri), administrator pokreće UDP probu (test_prema_zg) s testnog poslužitelja RISRV na lokaciji u Rijeci prema IP adresi LAN sučelja testnog poslužitelja na lokaciji u Zagrebu ZGSRV 192.168.100.100. Kako će se VoIP promet odvijati obostrano, potrebno je osigurati rezultate testova iniciranih sa obje strane kako bi se izbjegle poteškoće u prijenosu u oba slučaja.

Planirano generiranje prometa

- Unicast (UDP) promet
    - *One-way delay meter* opcija mjeri kašnjenje paketa (*delay*) u jednom smjeru
    - Vrijeme trajanja *streama*: 30 sec = 30000ms
    - Učestalost slanja paketa: 200 pps (-C 200)
    - Veličina paketa: 800 (-c 800 bytes)

Popis komunikacijskih tokova

- Unicast UDP promet protocol ZGSRV <-> RISRV: 192.168.100.100 <-> 192.168.51.100:8999
- Unicast UDP promet protocol RISRV <-> ZGSRV: 192.168.51.100 <-> 10.10.13.99:8999

Komunikacijski tok 1, Zagreb -> Rijeka

Isključujemo privremeno vatrozid na testnom računalu RISRV jer će nam u protivnom testna IP komunikacija biti odbačena od strane lokalnog ip tables vatrozida na OS-u

```
service iptables stop
```

Opcionalno permanentno gašenje vatrozida na testnom računalu RISRV također kako ne ni lokalni poslužitelj zaustavljao testni promet.

```
chkconfig iptables off
```

Pokretanje D-ITG primatelja (poslužitelja) na destinaciji RISRV u Rijeci

```
./ITGRecv
```

Sinkroniziramo sat na svim testnim poslužiteljima radi preciznosti D-ITG statistika

```
date 012715482017

hwclock --systohc
```

Pokretanje probe s testnog servera u Zagrebu ZGSRV 192.168.100.100 prema testnom serveru u Rijeci RISRV 192.168.51.100

```
./ITGSend -a 192.168.51.100 -t 30000 -T UDP -C 200 -c 800 -l test_prema_ri.log -x test_prema_ri.log
```

Provjera ispisa UDP proba na računalu u Zagrebu.

```
./ITGDec test_prema_ri.log
```

Provjera ispisa UDP proba na računalu u Rijeci.

```
./ITGDec test_prema_ri.log
```

Komunikacijski tok 2, Rijeka -> Zagreb

Isključuje se privremeno vatrozid na testnom računalu ZGSRV

```
service iptables stop
```

Opcionalno permanentno gašenje vatrozida na testnom računalu ZGSRV

```
chkconfig iptables off
```

Pokretanje D-ITG primatelja (poslužitelja) na destinaciji ZGSRV u Zagrebu

```
./ITGRecv
```

Pokretanje probe s testnog servera u Rijeci RISRV 192.168.51.100 prema testnom serveru u Zagrebu ZGSRV 192.168.100.100

```
./ITGSend -a 192.168.100.100 -t 30000 -T UDP -C 200 -c 800 -l test_prema_zg.log -x test_prema_zg.log
```

Provjera ispisa UDP proba na računalu u Rijeci.

```
./ITGDec test_prema_zg.log
```

Provjera ispisa UDP proba na računalu u Zagrebu.

```
./ITGDec test_prema_zg.log
```

Primjer prikaza ispisa rezultata generatora prometa sa statusom pošiljatelja u Zagreb (gore) Rijeka (dole)

Test name	test_prema_zg.log
Test location	Zagreb
Total time	29.998756 s
Total packets	5908
Minimum delay	0.000000 s
Maximum delay	0.000000 s
Average delay	0.000000 s
Average jitter	0.000000 s
Delay standard deviation	0.000000 s
Bytes received	4726400
Average bitrate	1260.425599 Kbit/s
Average packet rate	196.941500 pkt/s
Packets dropped	0 (0.00 %)
Average loss-burst size	0.000000 pkt

Slika 5.4 Ispis rezultata s testnog računala Zagreb – Rijeka[21]

[21] Vlastiti rad autora, 18.02.2018.

Test name	test_prema_zg.log
Test location	Rijeka
Total time	29.998604 s
Total packets	5908
Minimum delay	0.001495 s
Maximum delay	0.004391 s
Average delay	0.001544 s
Average jitter	0.000030 s
Delay standard deviation	0.000104 s
Bytes received	4726400
Average bitrate	1260.431985 Kbit/s
Average packet rate	196.942498 pkt/s
Packets dropped	0 (0.00 %)
Average loss-burst size	0.000000 pkt

Slika 5.5 Ispis rezultata s testnog računala Rijeka – Zagreb

Očekivani rezultati testova

Očekivano je da se nakon izvođenja testa **test_prema_ri** pokaže kako je UDP promet odaslan sa poslužitelja u Zagrebu ZGSRV prema LAN adresi poslužitelja u Rijeci RISRV primljen što dokazuje funkcionalnost IP Unicast usmjeravanja (routing).

Očekivano je i da se promet u suprotnom smjeru, testiran dodatnim komunikacijskim tokom u testu **test_prema_zg** pokaže kako je UDP promet odaslan s poslužitelja u Rijeci RISRV prema LAN adresi poslužitelja u Zagrebu ZGSRV primljen, što dodatno dokazuje funkcionalnost IP Unicast usmjeravanja (routing).

Očekivani rezultati testiranja za testni tok podataka

Kako je generirani promet u slučaju obaju testova unutar maksimalne dopuštene propusnosti nad svakim pojedinim IPSec VPN tunelom, očekivani rezultati iščitani s ispisa rezultata generatora prometa u nastavku trebaju pokazati zadovoljavanje uvjeta o prosječnom kašnjenju, prosječnom *jitteru* te pokazati minimalni gubitak paketa (po mogućnosti od 0 paketa za svaki komunikacijski tok):

- Prosječno kašnjenje: <= 100 msec
- Prosječni jitter: <= 50ms
- Maksimalni gubitak paketa: <= 0,5%

Ispis u nastavku prikazuje izvođenje i rezultate testa **test_prema_ri** s izvorišne strane na lokaciji Zagreb sa servera ZGSRV rezultate istog testa sa destinacijske strane na lokaciji Rijeka sa servera RISRV.

Test name	test_prema_zg.log
Test location	Zagreb
Total time	29.998756 s
Total packets	5908
Minimum delay	0.000000 s
Maximum delay	0.000000 s
Average delay	0.000000 s
Average jitter	0.000000 s
Delay standard deviation	0.000000 s
Bytes received	4726400
Average bitrate	1260.425599 Kbit/s
Average packet rate	196.941500 pkt/s
Packets dropped	0 (0.00 %)
Average loss-burst size	0.000000 pkt

Slika 5.6 Rezultati kašnjenja i gubitka paketa Zagreb - Rijeka

Test name	test_prema_zg.log
Test location	Rijeka
Total time	29.998604 s
Total packets	5908
Minimum delay	0.001495 s
Maximum delay	0.004391 s
Average delay	0.001544 s
Average jitter	0.000030 s
Delay standard deviation	0.000104 s
Bytes received	4726400
Average bitrate	1260.431985 Kbit/s
Average packet rate	196.942498 pkt/s
Packets dropped	0 (0.00 %)
Average loss-burst size	0.000000 pkt

Slika 5.7 Rezultati kašnjenja i gubitka paketa Rijeka - Zagreb

Prilikom analize rezultata testiranja prosječno kašnjenje je u ispisu definirano kao *Average Delay*, prosječne varijacije u kašnjenju kao *Average Jitter*[22], a maksimalni gubitak paketa kao *Packets dropped*.

Test name	test_prema_zg.log
Test location	Zagreb
Total time	29.998756 s
Total packets	5908
Minimum delay	0.000000 s
Maximum delay	0.000000 s
Average delay	0.000000 s
Average jitter	0.000000 s
Delay standard deviation	0.000000 s
Bytes received	4726400
Average bitrate	1260.425599 Kbit/s
Average packet rate	196.941500 pkt/s
Packets dropped	0 (0.00 %)
Average loss-burst size	0.000000 pkt

Slika 5.8 Rezultati kašnjenja i gubitka paketa Zagreb – Rijeka

Test name	test_prema_zg.log
Test location	Rijeka
Total time	29.998604 s
Total packets	5908
Minimum delay	0.001495 s
Maximum delay	0.004391 s
Average delay	0.001544 s
Average jitter	0.000030 s
Delay standard deviation	0.000104 s
Bytes received	4726400
Average bitrate	1260.431985 Kbit/s
Average packet rate	196.942498 pkt/s
Packets dropped	0 (0.00 %)
Average loss-burst size	0.000000 pkt

Slika 5.9 Rezultati kašnjenja i gubitka paketa Rijeka - Zagreb

Ispis u nastavku prikazuje izvođenje i rezultate testa **test_prema_zg** s izvorišne strane na lokaciji Rijeka sa servera RISRV te rezultate istog testa sa destinacijske strane na lokaciji Zagreb sa servera ZGSRV.

Prilikom analize rezultata testiranja prosječno kašnjenje je u ispisu definirano kao *Average Delay*, prosječni jitter kao *Average Jitter*, a maksimalni gubitak paketa kao *Packets dropped*.

[22] Izvor: https://voipstudio.com/voip-how-much-jitter-is-acceptable/
Datum: 20.02.2018.

Test name	test_prema_zg.log
Test location	Zagreb
Total time	29.998756 s
Total packets	5908
Minimum delay	0.000000 s
Maximum delay	0.000000 s
Average delay	0.000000 s
Average jitter	0.000000 s
Delay standard deviation	0.000000 s
Bytes received	4726400
Average bitrate	1260.425599 K bit/s
Average packet rate	196.941500 pkt/s
Packets dropped	0 (0.00 %)
Average loss-burst size	0.000000 pkt

Slika 5.10 Rezultati kašnjenja i gubitka paketa Zagreb - Rijeka

Test name	test_prema_zg.log
Test location	Rijeka
Total time	29.998604 s
Total packets	5908
Minimum delay	0.001495 s
Maximum delay	0.004391 s
Average delay	0.001544 s
Average jitter	0.000030 s
Delay standard deviation	0.000104 s
Bytes received	4726400
Average bitrate	1260.431985 Kbit/s
Average packet rate	196.942498 pkt/s
Packets dropped	0 (0.00 %)
Average loss-burst size	0.000000 pkt

Slika 5.11 Rezultati kašnjenja i gubitka paketa Rijeka - Zagreb

5.7. Test određivanja iznosa MTU

Svrha testa

Test prikazuje određivanje maksimalne veličine paketa kojem je omogućen prolazak sa testnog poslužitelja centralne lokacije prema udaljenoj lokaciji bez potrebe za fragmentiranjem kod zadane konfiguracije sučelja.

Procedura tijeka testiranja

Administrator pokreće ICMP probu sa testnog servera ZGSRV na lokaciji u Zagrebu prema IP adresi testnog servera RISRV na lokaciji Rijeka s definiranim DF (don't fragment) bitom unutar ICMP zaglavlja. Na ovaj način uređajima na putu prema destinaciji naređujemo zabranu fragmentiranja poslanog paketa.

Administrator šalje ICMP probe sa definiranim DF bitom te sa različitim veličinama paketa kako bi odredio do koje maksimalne veličine paket uspije proći do destinacije. Kad se veličina paketa poveća na iznos veći od iznosa MTUa na sučeljima prema destinaciji, probi je onemogućen prolazak jer joj je zabranjeno fragmentiranje.

Na CentOS operativnom sustavu, ICMP ping naredba ima opciju (-s) definicije veličine ICMP paketa koja se definira bez veličine ICMP i IP zaglavlja. Kod prvog komunikacijskog toka, kako bi se odaslao ICMP paket veličine 1490 bajta, potrebno je definirati opciju „-s 1462“ (1490 bytes – 28 ICMP and IP header)

Planirano generiranje prometa

- Unicast (ICMP) proba 1
  - Vrijeme trajanja *streama*: 5 sec
  - Učestalost slanja paketa: 1 pps
  - Veličina paketa: 1500 bytes
- Unicast (ICMP) proba 2
  - Vrijeme trajanja *streama*: 5 sec
  - Učestalost slanja paketa: 1 pps
  - Veličina paketa: 1501 bytes

Popis komunikacijskih tokova

- Unicast ICMP protocol ZGSRV <-> RISRV: 192.168.100.100 <-> 192.168.51.100
- Unicast ICMP protocol ZGSRV <-> RISRV: 192.168.100.100 <-> 192.168.51.100

Isključujemo privremeno firewall na testnom poslužitelju kako ne bi poslužitelj lokalno zaustavljao testni promet.

RISRV:

```
service iptables stop
```

Opcionalno permanentno isključivanje vatrozida na testnom poslaužitelju RISRV:

```
chkconfig iptables off
```

Pokretanje ICMP probe 1 sa testnog poslužitelja ZGSRV prema RISRV veličine 1500 bajta sa definiranim DF tagom u ICMP zaglavlju:

```
ping -c 5 -i 1 -M do -s 1472 192.168.51.100
```

Objašnjenje naredbe[23]: ping –c *(count) –i (interval) –M (hint) (do no fragment DF) –s (packet size)* odnosno pingaj 5 puta, sa DF bitom u veličini *headera* 1472+28.

Provjera ispisa ICMP probe 1 sa testnog poslužitelja ZGSRV prema RISRV kako bi se provjerilo da li je proba prošla uspješno.

[23] Izvor: http://www.tutorialspoint.com/unix_commands/ping.htm
Datum: 23.02.2018.

Ukoliko je prethodna proba (1) prošla uspješno pokreće se sljedeća ICMP proba 2 sa testnog poslužitelja ZGSRV prema RISRV sa povećanom veličinom paketa od 1501 bajta sa definiranim DF tagom u ICMP zaglavlju:

```
ping -c 5 -i 1 -M do -s 1473 192.168.51.100
```

Provjera ispisa ICMP probe 2 sa testnog poslužitelja ZGSRV prema RISRV kako bi se provjerilo da li je proba prošla uspješno.

Ukoliko je prethodna proba (2) prošla neuspješno pokreće se sljedeća ICMP proba 2 sa testnog poslužitelja ZGSRV prema RISRV sa smanjenom veličinom paketa od 1501 bajta sa definiranim DF tagom u ICMP zaglavlju:

```
ping -c 5 -i 1 -M do -s 1473 192.168.51.100
```

Provjera ispisa ICMP probe 2 sa testnog poslužitelja ZGSRV prema RISRV

Očekivani rezultati testova

Očekivano je da se u slučaju ICMP probe, odaslane prema RISRV, proba bude uspješna sve dok se veličina paketa na poveća iznad veličine MTU-a.

Test prikazuje kako se postupnim povećanjem veličine paketa u koracima može odrediti točan iznos veličine MTUa na određenim komunikacijskim putem.

Za primjer je uzeta komunikacije ZGSRV testnog poslužitelja na lokaciji u Zagrebu koji šalje ICMP probe različitih veličina prema RISRV testnom poslužitelju na lokaciji Rijeka.

Očekivani ispis probe sa testnog poslužitelja ZGSRV prema RISRV:

Test 1: Prvi test je uspješan te dokazuje da je MTU veći ili jednak 1500 bajta

```
PING 192.168.51.100 (192.168.51.100) 1472(1500) bytes of data.
1480 bytes from 192.168.51.100: icmp_seq=1 ttl=63 time=1.07 ms
1480 bytes from 192.168.51.100: icmp_seq=2 ttl=63 time=1.07 ms
1480 bytes from 192.168.51.100: icmp_seq=3 ttl=63 time=1.09 ms
1480 bytes from 192.168.51.100: icmp_seq=4 ttl=63 time=1.04 ms
1480 bytes from 192.168.51.100: icmp_seq=5 ttl=63 time=1.04 ms

--- 192.168.51.100 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4005ms
rtt min/avg/max/mdev = 1.044/1.066/1.091/0.039 ms
```

Test 2: Drugi test je neuspješan te dokazuje da je MTU manji od 1501 bajta

```
[root@ZG bin]# ping -c 5 -i 1 -M do -s 1473 192.168.51.100
PING 192.168.51.100 (192.168.51.100) 1473(1501) bytes of data.
ping: local error: Message too long, mtu=1500
ping: local error: Message too long, mtu=1500
ping: local error: Message too long, mtu=1500
ping: local error: Message too long, mtu=1500
ping: local error: Message too long, mtu=1500

--- 192.168.51.100 ping statistics ---
5 packets transmitted, 0 received, +5 errors, 100% packet loss, time 4999ms
```

Kako nam peti test određuje da je MTU manji od 1501 bajta, a drugi test određuje da je MTU veći ili jednak 1500 bajta, dobivamo rezultat da je MTU 1500 bajta.

Korisno je znati kako CentOS, za razliku od nekih drugih operativnih sustava unutar ispisa ICMP testa (PING) u svakom slučaju ispisuje MTU veze kroz koje je test poslan, te se na ispisu u primjerima u prethodnom dijelu testa vidi da je CentOS ICMP test ispisala MTU od 1500 što dodatno potvrđuje točnost testa.

Zaključak

U ovom radu opisano je kako implementacijom MPLS L3 VPN-a u kombinaciji s IPSec protokolom osigurati pouzdanost i sigurnost u komunikaciji više udaljenih lokacije unutar infrastrukture pružatelja usluga. Korisnik Državna Uprava za zaštitu i spašavanje samo je jedan od korisnika koji se odlučili za implementaciju navedenog rješenja u svoje okruženje kako bi povezali svojih sedamnaest područnih ureda s glavnom centralnom lokacijom.

Prednosti ovog rješenja ne leži samo u tome što trenutno na tržištu ne postoji niti jedno rješenje koje ima opciju implementacije u infrastrukturu pružatelja usluga, ovo rješenje također održava pružatelj usluga. Rezultat navedenog je da korisnik u konačnici nije svjestan tehnologije koja mu je pružena od strane pružatelja usluga s aspekta konfiguracije. Uz sve prednosti objašnjene u ovom radu ovo rješenje također pruža korisniku kvalitetu usluge na način da korisnik može odrediti prioritet u poslovanju te sukladno tome pružatelj usluga jamči korisniku da navedeni zahtjevi biti će ispunjeni. Obzirom da 112 pozivi služe za pomoć unesrećenima, a k tome glavna su djelatnost državne uprave za zaštitu i spašavanje implementacijom QoS mehanizma u MPLS dobiva se mrežni promet sa najvišim prioritetom (MPLS EF) koje pružatelji usluga u svojoj infrastrukturi trenutno prosljeđuje na zadane adrese.

Ovaj rad objašnjava detalje vezano za SLA ugovor s kojima se pružatelj usluga obvezuje prema korisniku u ispunjavanju vremenskih rokova u slučaju nedostupnosti nekog od servisa te koje su uvjeti koji moraju biti zadovoljeni kako korisnikova mreža bila uvijek visoko dostupna i redundantna.

Popis slika

Slika 3.1 PUZS lokacije po hrvatskoj

Slika 3.2 Logička topologija centralna lokacija prije nadogradnje

Slika 4.1 Popis ograničenja za različite mrežne segmente

Slika 4.2 Popis dozvoljenih stranica za 112 segment

Slika 4.3 Prikaz sedam OSI slojeva

Slika 4.4 Primjer adresiranja na područnom uredu Zadar

Slika 4.5 Prikaz mogućih kombinacija za AES256

Slika 4.6 Konfiguracija PUZS lokacije

Slika 4.7 Područni ured Zadar

Slika 4.8 Određivanje vremena primjene politike

Slika 4.9 Puštanje PUZS nesigurne mreže na Internet

Slika 4.10 PBR politika za MPLS EF

Slika 5.3 Statični tuneli svih PUZS lokacija

Slika 5.4 Ispis rezultata s testnog računala Zagreb – Rijeka

Slika 5.5 Ispis rezultata s testnog računala Rijeka – Zagreb

Slika 5.6 Rezultati kašnjenja i gubitka paketa Zagreb - Rijeka

Slika 5.7 Rezultati kašnjenja i gubitka paketa Rijeka - Zagreb

Slika 5.8 Rezultati kašnjenja i gubitka paketa Zagreb – Rijeka

Slika 5.9 Rezultati kašnjenja i gubitka paketa Rijeka - Zagreb

Slika 5.10 Rezultati kašnjenja i gubitka paketa Zagreb - Rijeka

Slika 5.11 Rezultati kašnjenja i gubitka paketa Rijeka - Zagreb

Popis tablica

Tablica 4.1 Usporedba dvaju NGFW za centralnu lokaciju

Tablica 4.2 Prednosti i nedostaci mogućih rješenja

Slika 15 Plan izvođenja testiranja

Popis kratica

SLA – *Service-Level Agreement*

MPLS – *Multi Protocol Label Switching*

VPN – *Virtual Private Network*

EF – *Expedited Forwarding*

DMVPN – *Dynamaic Multipoint VPN*

PBR – *Policy-Based routing*

QoS – *Quality of Service*

MTU – *Maximum Transmission Unit*

ICMP – *Internet Control mesasge Protocol*

DF – *Do not Fragment bit*

DHCP – *Dynamic Host Configuration Protocol*

VRF – *Virtual Routing and Forwarding*

PE – *Provider Edge*

VLAN – *Virtual Local Area Network*

BGP – *Border Gateway Protocol*

UDP – *User Datagram Protocol*

TCP – *Transmission Control Protocol*

IPsec – *Intenet Protocol Security*

NHRP – *Next Hoop Resolution Protocol*

D-ITG - *Distributed Internet Traffic Generator*

VoIP – *Voice over Inernet Protocol*

DMZ - *Demilitarized Zone*

Literatura

[1] DMVPN Concepts and Configuration https://learningnetwork.cisco.com/docs/DOC-25970

[2] Microsoft Technet https://technet.microsoft.com/en-us/library/cc780760(v=ws.10).aspx

[3] Multiprotocol BGP MPLS VPN https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/mp_l3_vpns/configuration/15-mt/mp-l3-vpns-15-mt-book/mp-bgp-mpls-vpn.html

[4] The QoS Expedited Forwarding (EF) Model https://www.networkworld.com/article/2234016/cisco-subnet/the-qos-expedited-forwarding--ef--model.html

[5] Policy-based routing on Fortigate with VPN https://www.ispcolohost.com/2015/06/25/policy-based-routing-on-fortigate-with-vpn/

[6] QoS: Latency and Jitter Configuration Guide https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/qos_latjit/configuration/xe-16/qos-latjit-xe-16-book.html

Algebra
visoka škola za
primijenjeno računarstvo

NASLOV DIPLOMSKOG RADA

Pristupnik: Josip Maloča, 0135161223

Mentor: dipl. ing. Silvio Papić