Simulacija sigurne mreže korištenjem GNS3 programskog alata

Pešut, Neven

Sveučilište Jurja Dobrile u Puli

Fakultet informatike u Puli

Neven Pešut

Simulacija sigurne mreže korištenjem GNS3 alata

Diplomski rad

Pula, veljača, 2022. godine

Sveučilište Jurja Dobrile u Puli

Fakultet informatike u Puli

Neven Pešut

Simulacija sigurne mreže korištenjem GNS3 alata

Diplomski rad

JMBAG: Neven Pešut, 0303071157

Studijski smjer: Informatika

Predmet: Mrežne tehnologije

Znanstveno područje: Društvene znanosti

Znanstveno polje: Informacijske i komunikacijske znanosti

Znanstvena grana: Informacijski sustavi i informatologija

Mentor: Prof.dr.sc. Mario Radovan

Pula, veljača, 2022. godine

IZJAVA O AKADEMSKOJ ČESTITOSTI

Ja, dolje potpisani *Neven Pešut*, kandidat za magistra informatike ovime izjavljujem da je ovaj Diplomski rad rezultat isključivo mojega vlastitog rada, da se temelji na mojim istraživanjima te da se oslanja na objavljenu literaturu kao što to pokazuju korištene bilješke i bibliografija. Izjavljujem da niti jedan dio Diplomskog rada nije napisan na nedozvoljen način, odnosno da je prepisan iz kojega necitiranog rada, te da nikoji dio rada krši bilo čija autorska prava. Izjavljujem, također, da nijedan dio rada nije iskorišten za koji drugi rad pri bilo kojoj drugoj visokoškolskoj, znanstvenoj ili radnoj ustanovi.

Student

_____

U Puli, _____, _____ godine

IZJAVA

o korištenju autorskog djela

Ja, *Neven Pešut* dajem odobrenje Sveučilištu Jurja Dobrile u Puli, kao nositelju prava iskorištavanja, da moj diplomski rad pod nazivom *Simulacija sigurne mreže korištenjem GNS3* alata koristi na način da gore navedeno autorsko djelo, kao cjeloviti tekst trajno objavi u javnoj internetskoj bazi Sveučilišne knjižnice Sveučilišta Jurja Dobrile u Puli te kopira u javnu internetsku bazu završnih radova Nacionalne i sveučilišne knjižnice (stavljanje na raspolaganje javnosti), sve u skladu s Zakonom o autorskom pravu i drugim srodnim pravima i dobrom akademskom praksom, a radi promicanja otvorenoga, slobodnoga pristupa znanstvenim informacijama. Za korištenje autorskog djela na gore navedeni način ne potražujem naknadu.

U Puli, _____

Potpis

_____

Sadržaj:

1. UVOD

U ovom diplomskom radu biti će predstavljena mrežna arhitektura koja nam može prikazati „realnu sliku“ u današnjem mrežnom okruženju.

Svrha rada je simulacija sigurne mreže i njena analiza za utvrđivanje prednosti i nedostataka te kako bi se napravila pravilna implementacija u budućim mrežnim okruženjima.

Cilj je stvoriti simulaciju koja bi predstavljala relativno sigurnu mrežu i slične scenarije korištenjem grafičkog programskog alata za simulaciju zvanog GNS3.

Teoretski dio obuhvaća prvih šest poglavlja kao i sam cilj problematike ovog rada, dok praktični dio počinje od sedmog poglavlja pristupanjem GNS3 osnovama koje prelaze na naglasak simulaciju sigurne mreže.

Provedena je analiza osnovnih atributa i karakteristika mrežnih komponenta i sigurnosti. Kroz spomenuta poglavlja obrađeno je način i pristup rada računalnih mreža, uređaja te njihovi trendovi sigurnosti s naglaskom na vatrozide, objašnjena je njena konstrukcija i način uporabe. Predstavljeni su protokoli kako bi lakše razumjeli proces prijenosa paketa i njihov promet kako bi znali što i kako zaštiti. Spomenuli smo najčešće sigurnosne prijetnje i na što trebamo obratiti pozornost kako bi spriječili zlonamjerne faktore na našu organizaciju.

Na dalje u radu je obrađen i detaljno elaboriran pregled na program za simulaciju *Graphical Network Simulator* 3 (GNS3) i vatrozid *FortiGate*. Kroz ove pojmove smo proveli analizu radnog okruženja i njihovih performansi i funkcionalnosti koje ovi alati pružaju. Na temelju istraživačke analize dolazi se do zaključka kako je riječ o iznimno naprednim simulacijskim programima čija je optimizacija na visokoj razini te njihovo grafičko sučelje koje je jednostavno i intuitivno što omogućuje laku spoznaju i snalažljivost klijentima.

Provedenu emulaciju putem GNS3 simulacijskog alata odnosno praktični dio se može podijeliti na potpoglavlje kao što je konstrukcija LAN mreže odnosno njena

konfiguracija, sastavnice mrežnih uređaja i njihove karakteristike. Odrađen je detaljan uvid u svaku sastavnicu praktičnog dijela od same izrade mrežne topologije do njenog pokretanja i dodavanje uloga unutar same arhitekture mreže.

2. KLASIFIKACIJA RAČUNALNE MREŽE PREMA VELIČINI

Kada je riječ o klasifikaciji računalne mreže prema veličini tj. o samoj distanci pojedinih čvorišta mreže, možemo ih razvrstati na lokalnu (LAN), gradsku (MAN), mrežu širokog područja (WAN) i na kraju Internet, koji je isto WAN. Tablica 1. nam prikazuje odnos između tih pojmova.

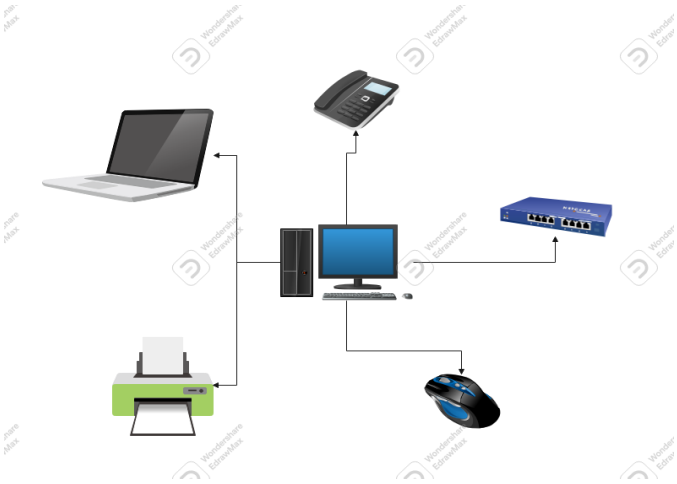
Tablica 1. Klasifikacija računalnih mreža

Vrsta mreže	Lokacija	Udaljenost izvora
Osobna mreža (PAN)	Naposredna blizina samog korisnika	Naposredna blizina samog korisnika
Lokalna mreža (LAN)	Manji prostor npr. soba Zgrada Niz objekata	10 m 100 m 1 km
Gradska rač. mreža (MAN)	Grad	10km
Globalna mreža (WAN)	Država Kontinent	100 km 1000 km
Internet mreža (isto kao i WAN)	Planet Zemlja	>10000 km

Izvor: https://electronicsguide4u.com/wide-area-networkwanlocal-area-networklan-metropolitan-area-networkman-personal-area-networkpan-campus-area-networkcan/, 2022.

2.1. Osobna mreža (PAN)

Osobna mreža odnosno PAN *(engl. Personal Area Network)* je mreža koja služi za povezivanja različitih uređaja na računalo čiji doseg nekoliko metara. Ovim tipom se omogućuje prijenos podataka na kratkim udaljenostima odnosno vezama, računalo sa računalom, računalo-printer, računalo-server, računalo-kamera i dr.[1] Primjer PAN mreže prikazan slikom 1.



Slika 1. Prikaz PAN mreže

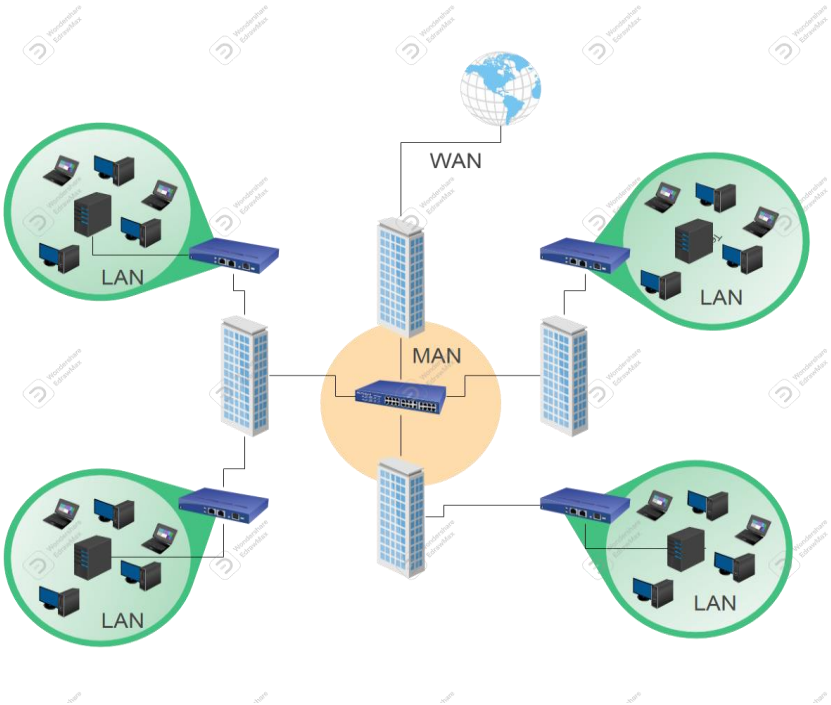
Izvor: samostalna izrada, 2022.

2.2. Gradska mreža (MAN)

Ovaj tip mreže pokriva teritoriji preko cijelog grada i zato se naziva gradska mreža ili MAN *(engl. Metropolitan Area Network)*. Ovakav tip mreže ima raspon povezanosti od nekoliko kilometara do par desetaka kilometara, čime možemo iskoristiti i povezati nekoliko LAN mreža. Često ovakav oblik je iskorišten u implementaciji sveučilišnih kampusa pa možemo se susresti s nazivom CAN *(engl. Campus Area Network).*[2]

Što se tiče brzine prijenosa podataka nešto je manja od brzine prijenosa u lokalnim mrežama. Osnovni primjer gradskih mreža su kabelske televizijske mreže koje se sve više zamjenjuju razvojem Internetom. Primjer MAN mreže prikazan slikom 2.

[1] Types of Network: LAN,WAN, WLAN; MAN, SAN, PAN, EPN & VPN [16]
[2] Types of Network: LAN,WAN, WLAN; MAN, SAN, PAN, EPN & VPN [16]



Slika 2. Prikaz MAN mreže

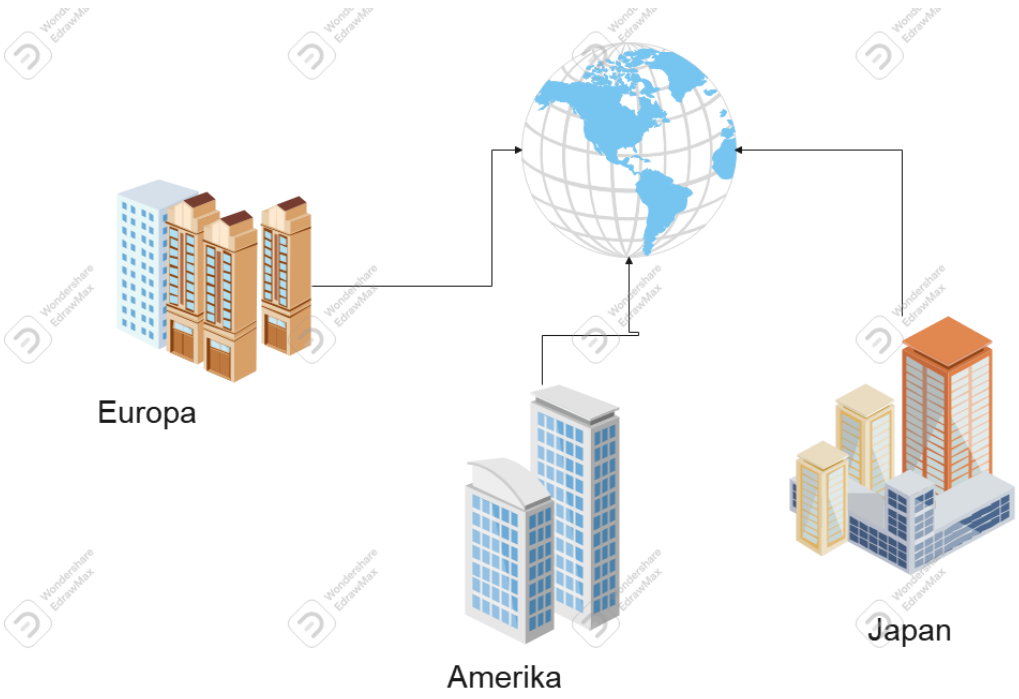
Izvor: samostalna izrada, 2022.

2.3. Mreže globalnog područja (WAN)

Regionalne mreže ili WAN *(engl. Wide Area Network)* raspolažu opsegom grada, regije ili cijele države. Za uspostavu povezanosti koriste se usmjerivači i javne komunikacijske veze. Brzina naspram LAN je ograničena. Karakteristika WAN mreže je ta da nije u vlasništvu jedne ili više osoba ili organizacije. Primjer javne WAN mreže je sami internet. [3]

Uz dosadašnje spomenute mreže tu su i mobilne mreže. Vrste mobilnih mrežnih tehnologija su, najnovija 5G, 4G(LTE), 3G(HSPDA), EDGE, HEDGE, Bluetooth, WI-FI, WI-FI 6, GPRS. Primjer WAN mreže prikazan slikom 3.

[3] Types of Network: LAN,WAN, WLAN; MAN, SAN, PAN, EPN & VPN [16]



Slika 3. Prikaz WAN mreže

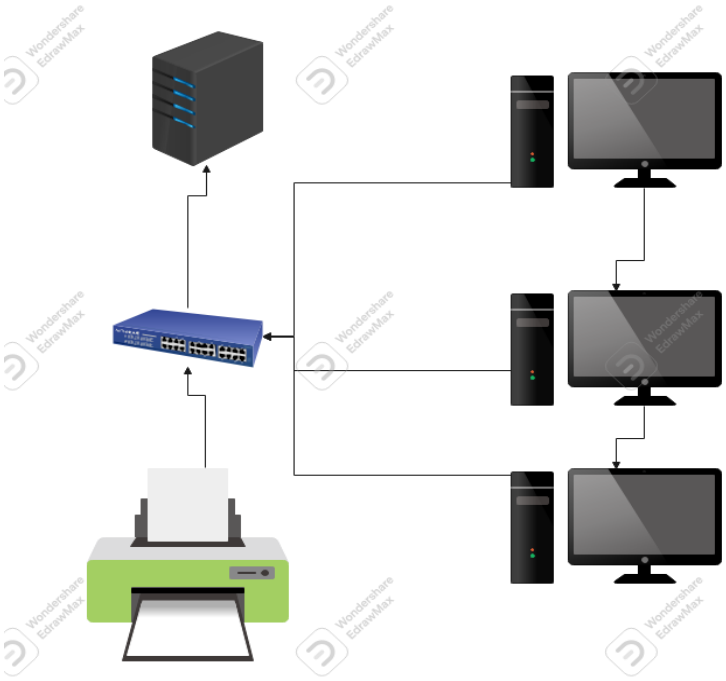
Izvor: vlastita izrada, 2022.

2.4. Lokalna mreža (LAN)

Lokalna mreža *(Local Area Network – LAN)* je mreža koja uspostavlja komunikaciju između razovrsnih uređaja unutar zacrtanog tj. ograničenog prostora. Obilježja LAN mreže su:

LAN mreža je često implementirana unutar jedne ili više objekata na određenom teritorijalnom prostoru. Odakle i sam pridjev lokalna. Broj krajnjih uređaja poput osobnog računala, printera i slično spojenih u LAN mrežu je ograničen, a njen raspon može biti od nekoliko desetaka do par stotina uređaja u samoj LAN mreži. LAN mrežu susrećemo najčešće unutar organizacije. Raspon brzine unutar LAN mreža su poprilično visoke gdje najviša brzina dostiže i do 1Gbit/s ili 1000 mps. U lokalnim mrežama moguća je uspostava veze od točke do točke *(Point to Point)* na višim

protokolnim slojevima. Uređaji u LAN mrežama međusobno komuniciraju na načelu ravnopravnosti *(peer to peer)*. To je koncept koji nam donosi umrežavanje uređaja bez poslužitelja odnosno da svaki krajnji uređaj u lokalnoj mreži može uspostaviti komunikaciju a da ne čeka na inicijativu ostalih krajnjih uređaja.[4] Primjer LAN mreže prikazan slikom 4.



Slika 4. Prikaz LAN mreže

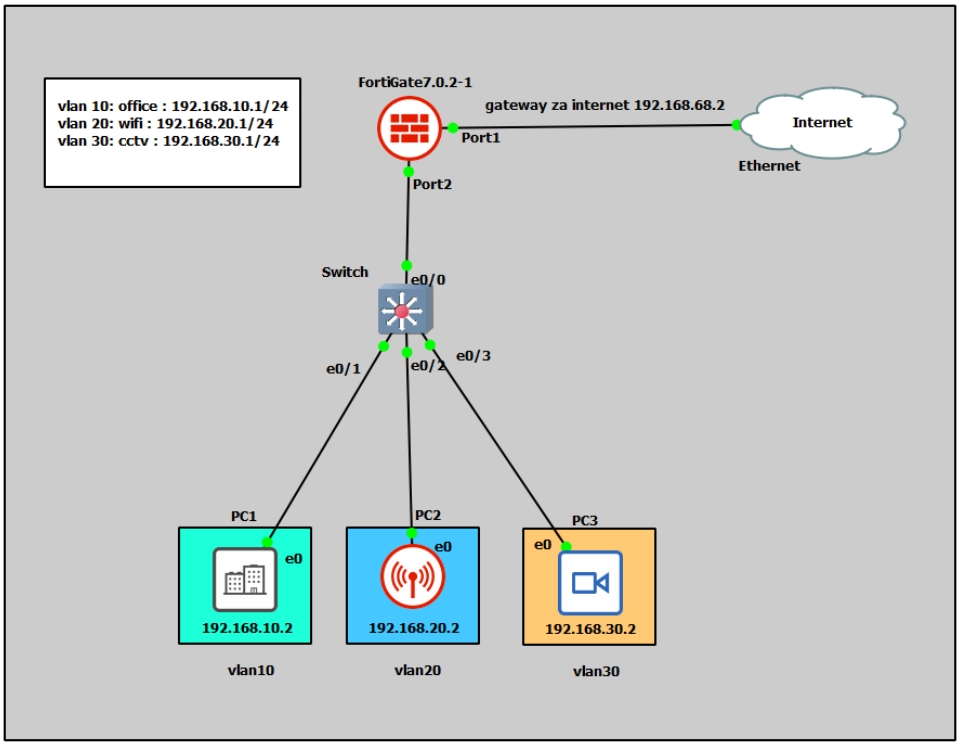
Izvor: samostalna izrada, 2022.

2.5. Virtualna lokalna mreža

VLAN *(engl. Virtual Local Area Network, Virtual LAN)* je verzija lokalne mreže gdje je podjela logička na domene *postiranja* i ona se ostvaruje neovisno o fizičkoj povezanosti mrežnih uređaja. Virtualne LAN-ove opisuje standard IEEE 802.1Q. IEEE 802.1Q, koji se često naziva Dot1q. Ovaj standard definira implementaciju za VLAN tj. za *Ethernet* okvire *(engl. Frames)* i opcije koje će se koristiti za mostove i preklopnike unutar tih okvira. Ujedno sadrži odredbu za određivanje prioriteta

[4] Types of Network: LAN,WAN, WLAN; MAN, SAN, PAN, EPN & VPN [16]

kvalitete usluge poznato kao IEEE 802.1p i definira generički protokol za registraciju atributskih podataka. Standard je razvio IEEE 802.1 odbor radne skupine IEEE 802 i konstantno se revidira. Jedna od značajnijih revizija je 802.1Q-2014 koja uključuje IEEE 802.1aq *(Shortest Path Bridging)* i veći dio standarda IEEE 802.1D.[5] Ovaj standard ćemo koristiti u implementaciji projektu jedan i projektu dva. Primjer VLAN mreže je prikazan sljedećom slikom 5.



Slika 5. Prikaz VLAN mreže
Izvor: samostalna izrada, 2022.

[5] VLAN Wikipedia [19]

3. MREŽNI UREĐAJI

Mrežni uređaji su uređaji koji sudjeluju u radnji prijenosa informacije putem računalnih mreža. Takve uređaje možemo klasificirati u krajnje uređaje i posredničke uređaje.

3.1. Krajnji uređaji

To su uređaji domaćini *(engl. Host)* koji predstavljaju izvorište ili odredište gdje se odvija obrada različitih signala u prilagođene informacije da se mogu prenositi nekakvih medijem. Krajnji uređaji mogu imati tri uloge, a to su klijent, poslužitelj i klijent-poslužitelj. Uređaji koji imaju ulogu klijenta koriste usluge drugog krajnjeg uređaja, a taj drugi uređaj je poslužitelj. Poslužitelj sadrži softver koji omogućuje pristup korisnicima i njihovim uslugama, podacima koji klijent zatraži. Danas sve više uređaja poprima ulogu klijent-poslužitelj i njima se konstantno raspolaže.[6] Odnos je jednostavnije ocrtan sljedećim slikovnim primjerom 6.

Slika 6. Veza između Klijent-Poslužitelj

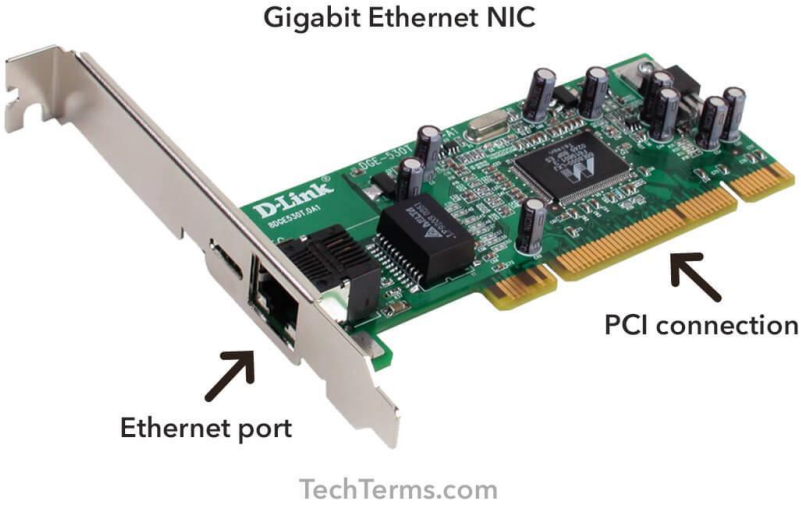
Izvor: samostalna izrada, 2022.

[6] Exploring the Modern Computer Network: Types, Functions, and Hardware [5]

U skupinu krajnjih uređaja možemo svrstati računala, laptope, servere, čitače kartica kreditnih, osobnih, debitnih, telefone, printere, CCTV kamere i dr. Svaki krajnji uređaj ima svoju unikatnu adresu koja se koristi u mreži pri samom prijenosu informacija. Kako bi se razmjena podataka tj. paketa ostvarila moramo poznavati adresu ishodišta i mjesto cilja od krajnjih uređaja. Proces adresiranja zahtjeva poznavanje razlike između logičkog i fizičkog adresiranja. Kod fizičkog je adresa unaprijed određena dok koga logičkog adresiranja sami mrežni administrator dodjeljuje adresu.

3.2. Posrednički uređaji

Jedan od posredničkih uređaja možemo svrstati i mrežnu karticu. Mrežna kartica *(engl. Network Interface Card, NIC*) (sl. 7) je komponenta u uređaju kao što je računalo i omogućava nam pristup mreži. Primarna zadaća mrežne kartice je konverzija podataka koji su bili u binarnom obliku koji je pogodan za prijenos putem određenog medija za prenošenje podataka. U samoj mrežnoj kartici je otisnut 48 bitni broj koji nam očitava jedinstvenu adresu koja je još poznatija pod nazivom MAC adresa *(engl. Media Access Control).*



Slika 7. Prikaz mrežne kartice

Izvor: https://techterms.com/, 2022.

Kako bi paket u nekakvoj mreži znao na koji se konkretni posrednički uređaj treba poslati u samom zaglavlju trenutnog paketa dodaje se fizička tj. MAC adresa. Kako bi dodali MAC adresu upotrebljavamo metodu fizičkog adresiranja.

Zatim dolazi preklopnik *(engl. switch)* (sl. 8) - posrednički uređaj koji sadrži nekoliko priključaka koji se svrstavaju po broju ulaza ili izlaza ovisno o samom modelu preklopnika. Preklopnik radi na način kada zaprimi informaciju odnosno podatak na određeni ulaz od pošiljatelja da direktno šalje na određeni izlaz zaprimljen podatak primatelju. Tako ćemo izbjeći gubitak i protok podataka će biti efikasniji i neće dolaziti do zastoja podatkovnog toka odnosno njihovog podatkovnog prometa.[7]

Slika 8. Prikaz preklopnika

Izvor: https://www.pngwing.com, 2022.

Jedan od najvažnijih posredničkih uređaja je usmjerenik ili pod poznatijim imenom usmjerivač *(engl. Router)*. Usmjerivač sadrži više funkcionalnosti nego preklopnik, on omogućava spajanje dva ili više mrežnih uređaja koji se sastoje od više usmjerivača na regionalnoj čak i na svjetskoj razini. Usmjeriač sadrži sve funkcionalnosti preklopnika. Bez usmjerenika implementacija regionalne mreže ne bi mogla biti uspostavljena. Osnovna zadaća je da odredi najbolju rutu kojom se šalje paket od

[7] Exploring the Modern Computer Network: Types, Functions, and Hardware [5]

ishodišta do odredišta putem algoritma za usmjeravanje. Kod takvog procesa postoje tri čimbenika kroz koje se vrši optimizacija a to su optimizacija pouzdanosti, vrijeme čekanja i vrijeme prijenosa.

Slika 9. Prikaz usmjerenika

Izvor: https://toppng.com/, 2022.

4. KARAKTERISTIKE I FUNKCIJE MREŽE

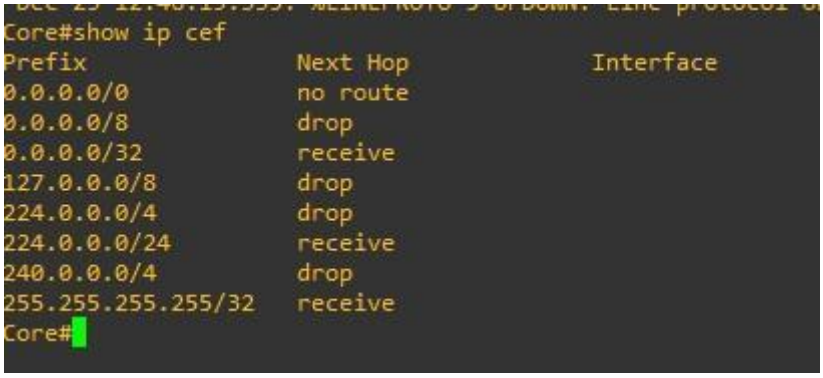
Ovo se poglavlje detaljno bavi MPLS-om (*Multi Protocol Label Switching)*, mrežnim prometnim inženjerstvom, MPLS VPN-om i osobinama mreža.

4.1. MPLS

Multi Protocol Label Switching akronim koji koristimo je MPLS je tehnologija koja se temelji na Cisco-u, koji su preuzeli od IP *switching scheme* koja definira kako se vrši spajanje IP paketa kroz ATM *(engl. Asynchronus Transfer Mode)*. Naspram ostalih protokola ta što ne ovisi ni o jednom protokolu za distribuciju oznaka, stoga možemo reći da MPLS koriste razne protokole za svoju distribuciju. Najpoznatiji protokoli MPLS-a su LDP *(engl. Label Distribution Protocol)* i RSVP-TE *(engl. Resource Reservation Protocol – Traffic Engineering).*

Osnovna ideja je ta da se stvori protokol koji će surađivati sa bilo kojim drugim protokolom mreže, npr. Ipv4, Ipv6, TP/IX, TUBA i dr. Ovaj protokol je razvijen kako bi se IP mreža što učinkovitije iskoristila. Naši usmjerivači odnosno usmjerivači se sastoje od podatkovnog i kontrolnog dijela. Kontrolni dio sadrži informacije koje nam govore o protokolima i njihovim usmjerenjima kao što su OSPF *(engl. Open Shortest Path First)*, BGP *(engl. Border Gateway Protocol)* i EIGRP *(engl. Enhanced Interior Gateway Routing Protocol).* Na ovoj razini se sporazumijevaju i prikazuju rute i njihova izmjena informacija, konkretnije postoji tablica koja sadrži informacije i prebacuju se u podatkovnu razinu zapravo u FIB *(engl. Forward Information Base)* tablicu (sl. 10). Na podatkovnoj razini usmjerivač odlučuje komunikaciju odnosno prosljeđivanje paketa uzimajući u obzir FIB tablicu. Kada promet dolazi do usmjerivača, on gleda IP rutu tj. adresu paketa i po tome se ravna u FIB tablici. Ovakav način izvođenja rada algoritma se naziva *longest prefix match algorithm*. [8]

[8] Campus Network for High Availability Design Guide [1]



Slika 10. Tablica FIB (engl. *Forward Information Base*)

Izvor: samostalna izrada, 2022.

4.2. Mrežno prometno inženjerstvo

Glavna misao je ta da se optimizira i što učinkovitije iskoriste mrežni resursi kako bi smanjili lošu protočnost među vezama. IP mreže su koristile rutanje na samu osnovu IP adrese, a prometno inženjerstvo se oslanja na topologiju mreže ili prema IGP *(engl. Interior Gateway Protocol)* protokolu gdje se događa daljnje modificiranje kao što je PBR *(engl. Policy Based Routing)*. Prometno inženjerstvo može unutar MPLS-a odrađivati usmjeravanje na osnovu odredišne adrese a postoji mogućnost da se odradi usmjeravanje pomoću proširenja postojećih protokola.[9] Jedne od osnovnih funkcija prometnog inženjerstva su:

- Distribucija informacija o mrežnoj arhitekturi;
- Izračunavanje najboljeg puta;
- Optimizacija mrežnog prometa i resursa;
- Tuneliranje i spajanje oznaka (koristi se kod MPLS VPN-a);
- Protekcijski mehanizmi (npr. *FastReroute*)

1. [9] SimulatorComputer Networks 2008: Volume 52, Dynamic traffic engineering for mixed traffic on international networks: Simulation and analysis on real network and traffic scenarios [3]

4.3. MPLS VPN

MPLS VPN je aplikacijska ekspanzija u MPLS mrežama te se često koristi kod firmi koje zahtijevaju različite privatne mreže različitih tipova. Virtualne mreže se nazivaju zbog korisničkih resursa gdje korisnik dijeli resurs s drugim korisnikom. Stoga korisnik nema vlastiti vod prema određenoj lokaciji jer je taj sami vod raščlanjen na nekoliko korisnika. Razlog zašto su privatne je taj što su međusobno mreže logički izolirane što rezultira tok prometa jednog klijenta ne može i ne smije se križati s prometnim tokom drugih korisnika. Virtualne mreže raščlanjujemo na bazirane mreže i terminale. MPLS VPN pripada baziranim mrežama u virtualnim mrežama. U našem projektu koristimo L3*(engl. Layer 3)* i L2 *(engl. Layer 2)* od Cisco-a koji su mrežno bazirani kao i MPLS VPN. L3 može biti virtualni usmjerivač dok L2 se dijeli na Ethernet, Point to Point VPWS *(engl. Virtual Private WireService)*.[10]

4.4. Osobine mreže

Osobine mreže opisuje značajke s kojima se susresti prilikom rada s mrežnim tehnologijama. Jedan od niz faktora je kvaliteta usluge koja objedinjuje faktore propusnosti, gubitak paketa, kašnjenje, treperenje. Ovo su najvažniji čimbenici koji donose prilagođavanje na zahtjeve poslovnih korisnika ujedno i privatnih koje se modificiraju prilikom integriranje usluge odnosno modificiranje kvalitete usluge i njenih parametara.

Kvaliteta usluge očitava se kao „skup performansi usluge koji određuju stupanj zadovoljstva korisnika s uslugom“. Kvaliteta usluge se sastoji od čimbenika koje smo

[10] Campus Network for High Availability Design Guide [1]
[10] Catal, F., Tcholtchev, N., Höfig, E., & Hoffmann, A. 2019. [1]

prije spomenuli a to su gubitak paketa, kašnjenje, treperenje i propusnost. Kako bismo zadovoljili kvalitetu usluge moramo obraditi svaki ovaj čimbenik.

Gubitak paketa (*engl. Packet loss*) se odnosi na paket koji ne dođe do odredišta a može biti povezan s čimbenikom propusnosti i kašnjenjem. Paketi koji se gube u mrežnom prometu namjerno se odbacuju putem mrežnih uređaja kako ne bi došlo do zastoja i gušenja. Gubitak nastaje prilikom zasićenosti spremnika u čvorovima podatkovne mreže, kojim rezultira kao čekanje paketa u redovima za usmjeravanje. Kada kod nekih aplikacija paket kasni uzastopno automatski taj paket se smatra izgubljenim. Za primjer se mogu spomenuti greške u mreži, zastoj u mreži i oštećeni paketi.

Kašnjenje paketa (engl. *Delay*) smatra se vremenom koje je potrebno jednoj bitnoj jedinici da prijeđe put kroz kanal mreže između ishodišta i odredišta. Svaki čimbenik implementiran u mrežnu topologiju pridonosi kašnjenje, to vrijedi za uključene usmjerivače, preklopnike i sl.

Treperenje (engl. *Jitter*) je varijacija kašnjenja paketa u mrežnom prometu između trenutka kada se signal prenosi i kada je primljen putem mreže. Mjerenje se izvodi u vremenskim jedinicama, najčešće se koriste milisekunde. Treperenje će nam biti važan pokazatelj prilikom upotrebe video usluga ili reprodukcije. [11]

[11] Catal, F., Tcholtchev, N., Höfig, E., & Hoffmann, A. 2019. [1]

5. KONSTRUKCIJA MREŽE

Konstrukcija mreže podrazumijeva adekvatnu konfiguraciju, arhitekturu, povezivanje njeno upravljanje te i njen nadzor. Ispravnost i zdravlje o mreži se brine administrator mreže. Administator se brine o komunikaciji u mreži, njenim krajnjim uređajima ili sistemima, procesima i aplikacijama koje se izvode i sveobuhvatno o njenim podacima i njenim korisnicima.

Komunikacijsku opremu možemo svesti na dva dijela, aktivni i pasivni dio. Jedan od njih ne traži konfiguraciju niti ikakvo upravljanje, već on postaje funkcionalan kada se priključi u mrežu. Aktivni dio sadržava elektronička oprema koja distribuira i prima promet u kanalu mreže tj. svi koji imaju memoriju i procesor, dok pasivni dio čini žični sustav zapravo kablovi npr. bakar i optika koji služe za povezivanje aktivnog dijela. Također se sastoji od konektora, preklopnika, razvodnog panela, sustav za hlađenje, komunikacijskog ormara, električno napajanje i dr.

Rasprostranjenost mreže i njena veličina ne utječe na pripadanje i prepoznavanje uređaja na mreži koji su definirani adresama. Protokol TCP/IP (*engl. Transmission Control Protocol/ Internet Protocol*) danas omogućuje komunikaciju putem povezanih mreža, a najzastupljeniji je u lokalnim mrežama, također ga možemo primijetiti u globalnoj mreži koju nazivamo Internet. Uređaji koji su povezani u mrežu njihovo adresiranje vršimo preko IP adrese i naziva. Mrežne usluge većinom su zasnovane na modelu klijent – poslužitelj. Poslužitelj možemo zamisliti kao nekakvu firmu koja nam omogućuje i ispunjava naše zahtjeve ili računalni program koji vrši svoje zadatke od strane drugih uređaja ili samog korisnika. Posao u računalnom modelu se raspoređuje po poslužiteljima koji pružaju usluge, resurse i po klijentu koje te stvari konzumira tj. zahtjeva. Njihova komunikacija se ostvaruje putem protokola kojeg sačinjavaju skupovi pravila koje se obje strane moraju pridržavati. Jedna od najpoznatijih protokola su: Telnet preko kojeg se omogućuje pristup računalu, FTP

(*File Transfer Protocol*) omogućuje prijenos podataka između dva ili više uređaja, SMTP te POP3 za slanje elektroničke pošte, HTTP ili sigurniji HTTPS koji omogućuje prijenos World Wide Web stranice i dr.[12]

5.1. Protokoli usmjeravanja

Usmjeravanje je proces koji obuhvaća selekciju kanala u mrežnom prometu za slanje podataka to je ujedno i funkcija usmjerivača. Koristeći bilo koju komutacijsku metodu uspostavlja se put od ishodišta do odredišta uz raspoloživosti mrežnih resursa. Te puteve definira mrežni administrator. Razne protokole koje upotrebljavamo za utvrđivanje puta možemo ih svrstati u dvije temeljne grupe a to su protokoli koji se temelje na vektoru udaljenosti i protokolu stanje veze.

Protokol vektora udaljenosti radi na način tako da svaki usmjerivač koristi tablicu usmjeravanja (*engl. Routing table*) kako bi se paketu uručila najkraći poznati put do svakog cilja i definira se ruta koje će paket koristiti.

Protokol usmjeravanja s vektorom puta je protokol mrežnog usmjeravanja koji sadrži informacije o putu koji se dinamički ažuriraju. Ažuriranja koja su prošla kroz mrežu i vratila se na isti čvor lako se otkrivaju i odbacuju. Ovakav se algoritam ponekad koristi za usmjeravanje *Bellman–Ford* kako bi se izbjegli problemi "Broj do beskonačnosti". Razlikuje se od protokola vektorom udaljenosti i protokola stanja veze. Svaki unos u tablicu usmjeravanja sadrži odredišnu mrežu, sljedeći usmjerenik i put do odredišta.

Border Gateway Protocol (BGP) je primjer za protokol vektor puta. U BGP-u usmjerivači nezavisnog sustava šalju poruke vektoru puta kako bi dobili odgovor koje su mreže dostupne. Svaki usmjerivač koji primi poruku oblika vektorske putanje mora verificirati svoj put u skladu sa pravilima. Ako je poruka u skladu sa pravilima autentifikacije, usmjerivač mijenja svoju tablicu usmjeravanja i poruku prije slanja poruke sljedećem krajnjem ili posredničkom uređaju. Modificira se tablica usmjeravanja kako bi zadržao nezavisne sustave kojima se prolazi kako bi se došlo do odredišta i njegovog sustava. Modificira se poruka kako bi dodao svoj AS broj i zamijenio sljedeći unos usmjerivača njegovom identifikacijom. AS broj (*engl.*

[12] Procedia Computer Science Volume 130, 2018. [2]

Autonomous System number) je grupa jedne ili više IP prefiksa odnosno lista IP adresa dostupne u mreži.

Protokol stanja veze njegov postulat da obradi komutaciju svakog čvora tj. oni čvorovi koji su spremni za prosljeđivanje paketa. Njegov temeljni zadatak da svaki čvor konstruira kartu povezanosti u obliku grafa kako bi se prikazala povezanosti između čvorova i tko je s kim povezan. Zatim svaki čvor računa najbolji logički put od njega do krajnjeg odredišta u mrežnom sustavu. Nakon računanja oformava se zbirka najboljih puteva i stvara se tablica usmjeravanja svakog čvora. Za izračunavanje najkraće udaljenosti do bilo kojeg čvora koristi se Dijkstrin algoritam. Reference za ovaj protokol su *Intermediate System to Intermediate System (IS-IS) i Open Shortest Path First (OSPF).*[13]

Ovo je suprotnost s protokolima vektorom udaljenosti, koji započinje tako da svaki čvor dijeli svoju tablicu usmjeravanja sa svojim susjedima, u protokolu stanja veze jedina informacija koja se prenosi između čvorova odnosi se na povezanost. Algoritmi stanja veze ponekad se neformalno okarakteriziraju kao usmjerivač koji komunicira sa svojim susjednim uređajima.

5.2. TCP protokol

TCP i IP protokol (*engl. Transmission Control Protocol, Internet Protocol)* (tab. 2) su glavni protokoli Interneta. Korištenjem ovog protokola razvijamo logičku vezu između klijenta i poslužitelja gdje se obavlja komunikacija i razmjena paketa. TCP spada u grupu spojnih protokola za razliku od bespojnih čiji je član UDP protokol. TCP nam garantira pouzdanu isporuku paketa u kontroliranom okruženju od pošiljatelja do primatelja. Ovaj protokol omogućava spajanje višestrukih povezivanja u realnom vremenu prema jednoj aplikaciji više klijenata na jednom poslužitelju, za primjer možemo spomenuti poslužitelj e-pošte. Obavlja se proces pakiranja pristiglih okteta

[13] [13] Procedia Computer Science Volume 130, 2018. [2]

u TCP segmente gdje dodjeljuje adrese izvorišnog i odredišnog priključka zatim slijedi sekvenca broja tih segmenata. Svaka strana TCP konekcije ima dodijeljenu 16-bitnu oznaku za obje strane aplikacije za slanje i primanje. Priključci su svrstani u tri kategorije: poznati priključci, registrirani priključci i dinamički/privatni priključci.[14]

Tablica 2. Struktura segmenta TCP-a

+	Bitovi 0-3	4-9	10-15	16-31
0	Izvorišni priključak			Odredišni priključak
32	Broj sekvence			
64	Broj potvrde			
96	Podatkovni ofset	Rezervirano	Zastavice	Prozor
128	Checksum			Hitni pokazivač
160	Opcionalno			
192	Opcije (ako ih ima)			Padding (do 32)
224	Korisnički podaci			

Izvor: https://hr.wikipedia.org/wiki/TCP, 2022.

Nakon slanja paketa se zaprima potvrda koja izvorištu govori da je paket stigao na svoje odredište. Osim takvog tipa potvrde može se dobiti da je paket izgubljen ili oštećen te povodom ovih potvrda isti se paket ponovno šalje zato možemo smatrati ovim protokolom pouzdanim i netolerantnim prema pogreškama. TCP protokol sadrži mogućnost kontrole toka prometa i veze no samo njeno modificiranje može biti obrnuto proporcionalno time što može izazvati kašnjenje.

[14] TCP Wikipedia [14]

5.3. UDP protokol

Kao već ranije spomenuto, UDP je beskonekcijski protokol i ponešto jednostavniji naspram TCP-a, a oba protokola su u transportnom segmentu OSI i TCP/IP modela. Koncept UDP protokola je jednostavniji prijenos i jednostavnija struktura paketa. Prisustvuje u mrežama temeljenim na grupi IP protokola kao prethodno spomenuti protokol. Pristignuti podaci slažu se u UDP segmente koje čine brojevi ishodišnog i odredišnog priključka za multipleksiranje i demultipleksiranje.

Tablica 3. Struktura segmenta UDP-a

+	Bit-ovi 0 - 15	16 - 31
0	Izvor priključka	Odredišni priključak
32	Duljina paketa	Kontrolni zbroj
64	Podatkovni zapis	

Izvor: https://hr.wikipedia.org/wiki/UDP, 2022.

Diferencijacija od TCP, protokol UDP ne prolazi kroz nikakav mehanizam kontrole toka, pogreške ili da nam pošalje potvrdu o zaprimljenosti paketa s postignutog mjesta. Ovakav protokol se ne iziskuje kod aplikacija kojima je potrebna sigurnost i pouzdanost i korektnost, već kod aplikacijskih programa kojima je razina kašnjenja mala. Za primjer se navode online računalne igre, video poziv, streaming medija.[15]

[15] Procedia Computer Science Volume 130, 2018. [2]

5.4. IP protokol

IP ili Internet Protokol je protokol mrežnog sloja TCP/IP i OSI modela, bez ovog protokola Internet ne bi bio Internet. Podaci koji se šalju u IP mrežu, šalju se u blokovima koje se nazivju paketi ili datagrami. Isti se naziva i *best effort* protokol koji nam govori da nema pouzdanosti hoće li paketi koji su poslani na odredište zaista doći. Kao i kod UDP, ovaj protokol se ne koristi u aplikacijama koje traže pouzdanost. Paket koji se šalje se može u procesu prijenosa promijeniti, odnosno promijeniti redoslijed paketa u naspram redoslijedu s kojeg je poslan, paket se može duplicirati ili krajnje izgubiti u prijenosu. S obzirom da paket ne prolazi kroz nikakvu kontrolu ili sličan mehanizam, proces usmjeravanja paketa je jednostavan i brz. IP protokol je standard na računalnoj mreži koju nazivamo Internet. Najraširenija verzija IP protokola na Internetu je IP inačica 4 a potom slijedi IP inačica 6 koja je i njegov nasljednik.[16]

IPv4 je najzastupljeniji protokol na mreži internet. Segmentu kod logičkog adresiranja dodaje se 32-bitna IP adresa cilja, 4 x 8 bit-a. Takva adresa sadrži dva identifikatora a to su identifikator mreže i krajnjeg uređaja (engl. NET ID i HOST ID). Identifikator mreže nam predstavlja mrežu gdje se smješteno mrežno sučelje. IP adresa se zapisuje decimalnom notacijom od 32-bitnog binarnog broja. 32-bitni broj se odvaja u četiri grupe po 8 bitova. Svaka se grupa zapisuje dekadski i onda se ti zapisi prikažu s odvojenim točkama. IP adrese se zapisuju binarno, dekadski i simbolički. IP adrese se svrstavaju u klase razine A,B,C,D i E. Pojedini spektar IP adresa nisu dostupne za korištenje na internetu, stoga imaju drugačiju ulogu. Identifikator od krajnjeg uređaja pokazuje na MAC adresu odnosno identifikacijski broj mrežnog sučelja. Tablicom 4 se prikazuju rasponi IPv4. U sklopu projekta su korištene IP adrese C klase.

[16] Procedia Computer Science Volume 130, 2018 [2]

Tablica 4. Rasponi IPv4 adresa

ADRESA	NAMJENA	KLASA	BROJ ADRESA
0.0.0.0 - 0.255.255.255	nul-adrese	A	16,777,216
10.0.0.0 - 10.255.255.255	Privatne adrese	A	16,777,216
127.0.0.0 - 127.255.255.255	Lokalni domaćin (*loopback* adresa)	A	16,777,216
169.254.0.0 - 169.254.255.255	Zeroconf	B	65,536
172.16.0.0 - 172.31.255.255	Privatne IP adrese	B	1,048,576
192.0.2.0 - 192.0.2.255	Dokumentacija i primjeri	C	256
192.88.99.0 - 192.88.99.255	IPv6 prema IPv4 *relay Anycast*	C	256
192.168.0.0 - 192.168.255.255	Privatne IP adrese	C	65,536
198.18.0.0 - 198.19.255.255	*Network Device Benchmark*	C	131,072
224.0.0.0 - 239.255.255.255	Multikast- raspoređivanje adresa	D	268,435,456
240.0.0.0 - 255.255.255.255	Rezervirano	E	268,435,456

Izvor: https://hr.wikipedia.org/wiki/IPv4, 2022.

Kada je završen proces logičkog adresiranja provjerava se paketna veličina IPv4 ili IPv4 datagram. Provjera je neophodna zato što iziskuje pregled okvira i njenih veličina tako zvani MTU (engl. *Maximum Transmission Unit*). Ako je paketni okvir veći od MTU dijeli ga se na fragmente kojim se šalju novim datagram-ima. U slučaju da se fragment zagubi, gubi se i cijeli datagram odnosno paket. Ovaj protokol ne prolazi kroz nikakav mehanizam kontrole, stoga se ne dobiva ni potvrda je li podatak stigao na svoje odredište.

Novija verzija protokola koji je IPv6 razlikuje se po načinu adresiranja koji omogućava 128 bit-no adresiranje, što znači da ima više raspoloživih adresa za razliku od IPv4 protokola. U IPv4 protokolu adresa se zapisuje u dekadskom dok u IPv6 adresu se zapisuje u heksadekadskom sustavu. Maksimalan broj adresa je približno 4,3 milijarde adresa.

Benefiti IPv6 protokola su da se ne trebaju koristiti NAT (engl. *Network Address Translation*). Poboljšana verzija *multicast* raspoređivanja adresa u usmjeravanju, lakša administracija što znači nema više DHCP-a (engl. *Dynamic Host Configuration Protocol)* s kojim dodjeljuje IP adrese i postavke koje obuhvaćaju za gateway, subnet masku, IP adrese DNS-a *(*engl. *Domain Name Server).* [17]

5.5. RIP protokol

Routing Information Protocol ili skraćeno RIP je najpopularniji i najstariji današnji protokol za usmjeravanje. RIP omogućava razmjenu informacija usmjerivačima i radnim stanicama koje im govore o usmjerivačkim rutama, smjerovima unutar računalne mreže. Zasniva se na algoritmu *Bellmann-Ford* za određivanje najbolje rute, odnosno odabire put s najmanjim brojem koraka. U sklopu RIP protokola obuhvaća *Split horizon, route poisoning i holddown mehanizme* kako bi spriječili širenje krivih informacija o usmjeravanju. Koncept RIP protokola kada nastupi promjena u mrežnoj arhitekturi, šalju se poruke svakom dijelu čvorišne mreže koje se vraćaju nazad izvorištu s ciljem postoji li promjena u mrežnoj topologiji. Uz pomoć

[17] Procedia Computer Science Volume 130, 2018 [2]

ovih funkcija ažurira se tablica usmjeravanja te potom se kreiraju novi putevi. U tablicu ulaze samo oni putevi koji omogućavaju paketu najmanju udaljenost do nekog odredišta.

Split horizon je mehanizam koji sprječava usmjerivačke petlje između dva usmjerivača. Ovaj mehanizam dolazi iz protokola usmjeravanja udaljenosti vektora. Split horizon zabranjuje usmjerivaču da pokazuje put natrag na izvorno sučelje.

Route poisoning je mehanizam koji sprječava usmjerivač da šalje pakete rutama koje su nevažeće unutar računalne mreže.

Holddown je mehanizam koji funkcionira na način da usmjerivač pokrene mjerač vremena kada prvi put zaprimi informaciju o mreži koja je nedostupna. Dok mjerač ne istekne, usmjerivač će odbaciti sve naknadne poruke rute koje ukazuju da je ona nedostupna. Može se riješiti slučaj kada je više usmjerenika povezano neizravno.[18]

Postoje tri inačice RIP protokola (tab. 5): RIP verzija jedan (RIPv1), RIP verzija dva (RIPv2) i RIP sljedeća generacija (engl. RIP next generation) RIPng.

[18] RIP Wikipedia [13]

Tablica 5. Vrste RIP protokola

RIPv1	RIPv2	RIPng
Šalje ažuriranje kao prijenos (broadcast)	Šalje ažuriranje kao multiprijenos (multicast)	Šalje ažuriranje kao multiprijenos
Prijenos je u rasponu 255.255.255.255	Multiprijenos na 224.0.0.9	Multi prijenos na FF02::9 jer može funkcionirati samo na IPv6
Ne podržava mehanizme autentifikacije za slanje poruka	Podržava mehanizme autentifikacije za slanje poruka	-
Klasni protokol usmjeravanja	besklasni protokol usmjeravanja ali podržava klasni protokol	Isti kao i RIPv2

Izvor: samostalna izrada, 2022.

RIPv1 je poznat kao i klasni protokol usmjeravanja jer ne šalje informacije o subnet masci u ažuriranju usmjeravanja.RIPv2 je besklasni protkol usmjeravanja za razliku od RIPv1 ovaj protokol šalje informacije o subnet masci.[19]

5.6. OSPF protokol

Open Shortest Path First ili OSPF protokol kao i prijašnji protokoli služe za usmjeravanje na računalnoj mreži odnosno mreže koje se temelje na IP protokolu kao što je internet. OSPF je protokol otvorene domene što rezultira da su njegove konfiguracije javne. Koristi Dijkstrin algoritam pošto dolazi iz grupe stanja veze (engl. Link State Routing, LSR) kojim se pronalazi najkraći put. Dodatak OSPF protokolu da šalje pozdrav pakete tj. *„hello“* pakete čiji je zadatak da se provjeri ima li kakvih promjena i postoje li nova saznanja o novim čvorištima.

OSPF prikuplja informacije o stanju veze raspoloživih usmjerivača koji čine arhitekturu mreže. Arhitektura je predstavljena kao tablica usmjeravanja na

[19] The Performance of IPv4 and IPv6 in Terms of Routing Protocols using GNS 3 [15]

internetski sloj za usmjeravanje paketa rutama. OSPF podržava IPv4 i IPv6 protokole te podržava model kao što je RIPv2 a to je model besklasnog među-domensko usmjeravanja adresa.[20]

Ovaj protokol se često koristi u računalnim mrežama velikih firmi i poduzeća.

Svaki usmjerivač ima arhiviranu bazu podataka stanja veze prema kojoj šalju LSA paketa (*link state advertisement*, informacije za otkrivanje susjednih čvorišta). OSPF je efikasniji od RIP protokola jer je puno brži sa slanjem informacija zato što u računalnoj mreži usmjerivači razmjenjuju podatke u obliku LSA paketa a ne distribuiraju pakete koje sadrže podatke o kompletnoj mreži kao RIP protokol.

OSPF dijeli mrežu na područja usmjeravanja kako bi se pojednostavila administracija i optimizirao promet i korištenje resursa. Područja su identificirana 32-bitnim brojevima, izraženim jednostavno u decimalnom obliku ili često u istom oktetu temeljenom na decimalnom zapisu koji se koristi za IPv4 adrese. Za multiprijenos (*engl. multicast)* putem IPv4 se koristi 224.0.0.5 adresa za normalnu komunikaciju, za ažuriranje nekog usmjerivača se koristi 224.0.0.6, a za IPv6 se koristi FF02::6. Ne koristi se transportni protokol kao na primjer UDP ili TCP protokol. On svoje podatke enkapsulira izravno u IP pakete sa brojem protokola 89, jedna od suprotnosti naspram ostalih protokola poput RIP i *Border Gateway Protocol* (BGP). OSPF implementira svoje vlastite mehanizme otkrivanja i ispravljanja pogrešaka u prijenosu.

5.7. EIGRP protokol

Enhanced Interior Gateway Routing Protocol ili EIGRP protokol je napredni protokol grupe usmjerivača vektora udaljenosti. Koristi se za automatizaciju odluka i usmjeravanju konfiguracija. Dizajniran je od strane *Cisco Systems*-a i dostupan je samo Cisco usmjerivačima. Osmišljen je kako bi iskoristio svu fleksibilnost protokola usmjeravanja uz puno bržom konvergencijom[21] svih usmjerivača. EIGRP koristimo

[20] RIP Wikipedia [13]
[21] Konvergencija (engl. convergence) predstavlja vrijeme potrebno usmjerniku da osvježi tablicu usmjeravanja

na usmjerivaču za dijeljenje ruta s drugim usmjerivačima unutar istog autonomnog sustava. Za razliku od RIP protokola, EIGRP šalje samo inkrementalna ažuriranja i time smanjuje opterećenje usmjerivača i količinu podataka u prijenosu. Naspram ostalih protokola za izračunavanje puta putem *Bellmann-Ford*-ovog algoritma, EIGRP koristi *Diffusing Update Algorithm* (DUAL) algoritam gdje se izračunavanje puteva vrši između dva usmjerivača. Usmjerivač šalje informaciju o korekciji rute kao vektor udaljenosti izravno povezanih ruta a ne ostalih ruta u mreži. Ako dođe do korekcije u arhitekturi mreže, usmjerivač javlja susjednom usmjerivaču samo ako je ta promjena imala učinak na te puteve.

EIGRP ne radi kontinuirana ažuriranja već inkrementalna, odnosno ažuriranje se vrši samo kada se promjeni udaljenost puta tj. promjena broja skokova. Propagacija ažuriranja se događa kod usmjerivača kod kojih je potrebna te rezultira puno manja pojasna širina EIGRP protokolu.

Da bi se izvele funkcije EIGRP-a, protokol mora stvoriti tri tablice, a to su:

- Tablica susjedstva
- Tablica topologije
- Tablica usmjeravanja

Tablica susjedstva sadrži informaciju puteva koju koriste usmjerivači EIGRP-a.

Tablica topologije sadrži rute koju se raspoložive za slanje paketa kroz mrežu. Pohranjuje optimalnu rutu od ishodišta prema odredištu.

Tablica usmjeravanja sadrži rute koje su trenutno aktivne kojom se šalju paketi putem mreže. Kao i tablica topologije sadrži optimalne rute za pošiljatelja.

Vrste paketa determinirano po nazivu paketa „Pozdrav, Ažuriranje, Upit, Odgovor i paket Potvrde.

Paket Pozdrav određuje susjedni usmjerivač koji također ima ulogu kao sistem za održavanje između usmjerivača. Ako je usmjernik A skopčan s usmjernikom B, a usmjernik A ne prima pozdravne pakete od usmjernika B, tada pretpostavlja se da usmjernik B nije dostupan i da je mreža prekinuta tj. nedostupna.

Paket Ažuriranja služi za slanje informacija o ruti svojim susjedima. Kada se pronađe novi usmjerivač, paketi ažuriranja se šalju susjedu kako bi se izgradila tablica topologije.

Paket Upita se upotrebljava naročito za traženje informacija o ruti. Djeluju kao dio paketa sve dok ne dostave primljene argumente koji su upiti njihovih odgovora. Poslat će upite samo kada je odredišno stanje aktivno.

Paket Odgovor odgovara na argument upita koji šalje informaciju da izvorni usmjerivač ne mora ići u aktivno stanje kao pouzdan nasljednik odredišne mreže. Argumenti se prosljeđuju kada odredište učestvuje u aktivnom stanju. Za paket argumenta mehanizam šalje odgovore o potvrdi.

I na kraju paket Potvrde biva poslan na EIGRP pakete upita, ažuriranja i odgovora. Dijeli se s unicast adresom koja se izravno šalje s jednog domaćina *(engl. Host)* na drugi, a samo dva domaćina komuniciraju preko utvrđene rute i također potvrdom koja se ne šalje na Hello pakete.

Temeljni čimbenici ovog protokola koje razlikuje naspram ostalih je ta da brzo prikuplja informacije o arhitekturi mreže, pruža šifriranje radi sigurnosti i može se upotrebljavati s iBGP-om za praćenje i usmjeravanje WAN mreže. Podržava IPv4 i IPv6 mreže, učinkovitije koristi vezu ECMP (*engl. Equal-Cost Multi-Path*) i njenu cijenu višestrukih puteva bez velikog opterećenja. EIGRP smanjuje mrežni promet korištenjem inkrementalnog ažuriranja. Ovaj protokol je dizajniran da se lako implementira te ojačava koheziju i smanjuje opseg tabele za usmjeravanje. EIGRP pohranjuje tablice usmjeravanja svojih bližnjih susjeda stoga možemo brzo prilagodit alternativnu rutu, ako primjeren put ne postoji protokol traži alternativan put.

6. SIGURNOST

Najčešći razlozi ranjivosti mreže:

- Neispravno instaliran hardver ili softver
- Operativni sustavi ili firmver koji nisu ažurirani
- Zloupotreba hardvera ili softvera
- Slaba ili potpuni nedostatak fizičke sigurnosti
- Nesigurne lozinke
- Nedostaci dizajna u operativnom sustavu uređaja ili u mreži

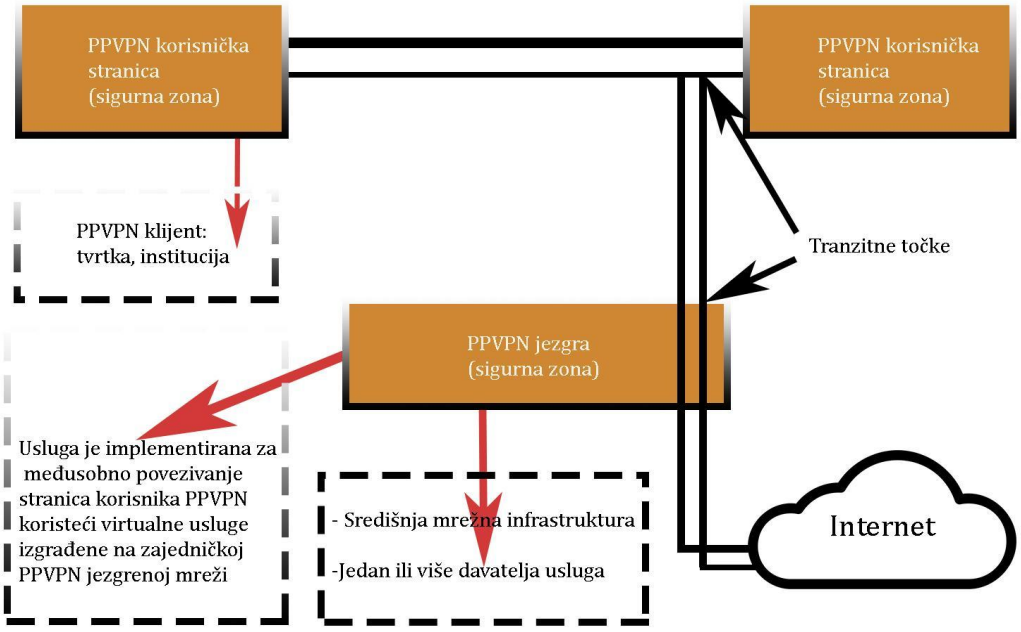
Sigurnost se odnosi na održavanje integriteta, povjerljivosti i pristupačnosti mreže i podataka. Razne prijetnje prema našoj sigurnosti PPVPN-u se mogu kategorizirati kao:

6.1. Napadi na podatke

Napadi koji uključuju prijetnju korisničkim podacima (s mjesta usluge pružatelja).

Njuškanje (*engl. Sniffing*): Njuškanje korisničkih podataka može se obaviti na dva načina

Prvi način je neovlašteno praćenje VPN paketa i analizu njihovog sadržaja. Time se ugrožava povjerljivost informacija. Podaci prikupljeni na ovaj način mogu se mijenjati i ponovno se mogu umetnuti u mrežu od strane napadača. Drugi način je neovlaštena analiza VPN paketa i inspekcija aspekata ili meta aspekta paketa tako da se mogu čak i interpretirati ako su paketi šifrirani. Mogu se dobiti korisne informacije na slici 11. - sigurne zone u PPVPN-ovim promatranjem tijeka prometa može se saznati veličina paketa te adresa izvora i odredišta. Takvi napadi su znatno manje zabrinjavajući u usporedbi s drugim napadima.



Slika 11. Sigurne zone

Izvor: samostalna izrada, 2022.

Prijevara i ponavljanje *(engl. Spoofing and Replay)*: lažiranje se odnosi na lažno predstavljanje od strane napadača kao ovlaštenog korisnika mreže. Koristeći ovaj identitet, napadač ubacuje neovlaštene podatkovne pakete u VPN, s ciljem da ovlašteni primatelj te pakete prihvati kao legitimne podatke. *Replay* tj. ponavljanje znači snimanje legitimnih podataka poslanih ranije, a zatim ponovno umetanje kopija istih podataka na mrežu.

Neovlaštena izmjena i brisanje podataka *(engl. Unauthorized modification and deletion of data)*: Ovo se odnosi na nelegitimnu promjenu sadržaja paketa ili ispuštanje podatkovnih paketa dok prolaze kroz tok mreže.

Napad uskraćivanja usluge *(engl. DoS, Denial of Service*): U DoS napadima napadač cilja prekinuti ili spriječiti izvornog korisnika u pristupu uslugama. DoS napadi se mogu izvesti preplavljivanjem mrežnih uređaja zahtjevima za razne usluge (iscrpljivanje resursa kroz kanale mreže), što rezultira povlačenje mrežnih uređaja iz upotrebe i njihovih usluga i promjenom konfiguracije samih uređaja. Iscrpljivanje resursa, cilja se na resurse kao što su propusnost, snaga CPU-a, usmjeravanje odnosno routing i kapacitet sesije. Na primjer, iscrpljivanje resursa može se provesti

na podatkovnoj razini određenog PPVPN-a pokušavajući lažirati ogromnu količinu podataka u VPN izvana. Takva aktivnost može iscrpiti dostupnu propusnost VPN-u ili preopteretiti kriptografski algoritam autentičnosti.

6.2. Napadi na kontrolnoj razini

Ovakvi napadi ciljaju na kontrolnu infrastrukturu kojima upravlja pružatelji VPN usluga.

- DoS napadi na mrežnu infrastrukturu: Jedna posebna vrsta DoS napada je kada jedan od grupe korisnika VPN-a troši prekomjerne mrežne resurse, što dovodi do uskraćivanja usluga VPN-a drugim korisnicima.
- Neovlašteni pristup mrežnoj opremi: u ovakvom napadu se konfigurira oprema od pružatelja usluga kako bi se dobila željena informacija.
- Tehnika društvenog napada: napad se održava od strane kompromitirane zaposlenog osoblja koje otkriva povjerljive informacije ili konfigurira samu mrežu.
- Promet kroz raskrižja veze: mogu se dogoditi pogrešne veze u VPN-u, a uzrok može biti od strane pružatelja usluge ili akcija od strane napadača. Posljedica može biti nepravilno spajanje dvije ili više veza VPN-a, podatkovni paketi se nepravilno isporučuju izvan same mreže. Prodor od napača može biti logički odnosno neispravna konfiguracija uređaja ili fizički gdje je usmjerivač na prostoru korisnika povezan s usmjerivačem od pružatelja usluga mreže IP/MPLS.
- Napad na protokol usmjeravanja: napad je u izravnoj liniji sa pružateljem usluga i njegovih protokola.

U VPLS-u koji se temelji na BGP-u, sve razmjene na kontrolnoj razini su izvršene korištenjem BGP poruka. Kako bi se poboljšala sigurnost na ovoj razini, uvedena je nova TCP opcija za prijenos *Message Digest5* (zvan još i MD5, koji je algoritam u kriptografiji). MD5 je definiran kao suštinski kontrolni zbroj koji se koristi za provjeru autentičnosti datoteke ili njeni niz. Za potrebe našeg projekta postavljen je vatrozid. Vatrozidovi su softverski programi, hardverski uređaj ili obje kombinacije koji blokiraju

neželjeni promet od ulaska u mrežu. Mogu se konfigurirati tako da blokiraju samo sumnjiv ili neovlašteni promet, dok i dalje dopuštaju pristup legitimnim i ovlaštenim zahtjevima.[22]

[22] *Current cyber-defense trends in industrial control systems [5]*

7. VATROZID

Firewall odnosno vatrozid je mrežni sigurnosni uređaj koji nadzire dolazni i odlazni mrežni tok prometa i na temelju unaprijed određenih parametara on odlučuje hoće li dopustiti ili blokirati određeni promet. Vatrozidi su prva crta obrane u mrežnoj sigurnosti više od 25 godina. Oni uspostavljaju barijeru između zaštićenih i kontroliranih unutarnjih mreža koje su pouzdane i mrežama kojima se ne može vjerovati u sigurnost, kao što je internetska mreža.

Vatrozid može biti hardverski, softverski ili oboje. Softverski vatrozid štiti jedno računalo osim ako nije opredijeljeno za zaštitu čitave mreže, dok hardverski vatrozid omogućuje zaštitu čitave mreže ili specifičan broj računala. Kako bi raspoznavali rad vatrozida potrebno je poznavati pojmove kao što su IP adresa, TCP i UDP protokoli koje smo prethodno spomenuli.

7.1. Tipovi vatrozida

Tipovi vatrozida s kojima se možemo susresti su, *Proxy firewall, Stateful inspection firewall, Unified threat management (UTM) firewall* i Virtualni vatrozid kojeg ćemo koristiti u našem projektu.

Proxy firewall najsigurniji je oblik vatrozida koji filtrira poruke na sloju aplikacije kako bi zaštitio mrežne resurse. Ograničava aplikacije koje mreža može podržavati, tako povećava razinu sigurnosti i s tim se može povećati brzina i funkcionalnost. Tradicionalni vatrozidi nisu dizajnirani za dešifriranje prometa ili provjeravanje protokolskog prometa. *Proxy firewall* određuje koji promet treba biti dopušten i odbijen te analizira dolazni promet kako bi otkrio znakove potencijalnog cyber napada ili zlonamjernog softvera. *Proxy firewall* predmemorira, filtrira, bilježi i kontrolira zahtjeve s uređaja kako bi zaštitio mreže i spriječio pristup neovlaštenim stranama i cyber napade.

*Stateful inspection firewal*l vrsta vatrozida koji prati stanje aktivnih mrežnih veza dok analizira dolazni promet i traži potencijalne prometne i podatkovne rizike. Ovaj

vatrozid nalazi se na slojevima 3 i 4 modela *Open Systems Interconnection* više poznatijom kraticom OSI model. Osnovne značajke ovog vatrozida uključuju blokiranje određenog prometa kao opasnog od ulaska u mrežu ili napuštanja mreže. Važno je pratiti stanje i kontekst mrežne komunikacije jer se te informacije mogu koristiti za prepoznavanje prijetnji - bilo na temelju odakle dolaze, kamo idu ili sadržaja njihovih paketa podataka. Vatrozidi s podacima o stanju mogu otkriti pokušaje neovlaštenih pojedinaca da pristupe mreži, kao i analizirati podatke unutar paketa kako bi vidjeli sadrže li zlonamjerni kod. Prikuplja podatke o svakoj vezi uspostavljenoj putem njega. Sve ove podatkovne točke profiliraju svojstva "sigurne" veze. Po potrebi ovaj vatrozid može implementirati dodatke kao što su enkripcija ili tuneliranje. Time se povećavaju performanse jer se blokiraju zlonamjerni akteri od čitanja i snifanja sadržaja u našoj komunikaciji.

Unified threat management je pristup informacijskoj sigurnosti gdje jedan hardver ili softver pružaju više sigurnosnih opcija. UTM pojednostavljuje upravljanje sigurnošću informacija pružajući jedno mjesto upravljanja i izvještavanja za sigurnosnog administratora umjesto upravljanja višestrukim proizvodima različitih dobavljača. UTM uređaji postaji popularniji do 2009. godine zato što su im opcije sve na jednom mjestu što pojednostavljuje konfiguraciju, instalaciju i održavanje što uveliko štedi novac i vrijeme. Ovakav pristup smanjuje broj uređaja s jednom funkcijom, mrežni administratori mogu raspolagati sa uređajima koje imaju više funkcija i potom centralno upravljati sa svojom zaštitom s jednog računalnog uređaja. Spomenut ćemo nekoliko UTM brendova a to su *Cisco, Fortinet, Netgear, Huawei, SonicWall* i na kraju *Fortigate* kojeg ćemo koristiti u našem projektu.[23]

Virtualni vatrozid također poznat kao vatrozid u oblaku, virtualni je uređaj dizajniran za pružanje istih sigurnosnih i inspekcijskih mogućnosti kao i fizički vatrozid. Virtualni vatrozid je rješenje za mrežnu sigurnost za okruženja gdje postavljanje fizičkih vatrozida je teško ili nemoguće, kao što su javna i privatna okruženja u oblaku. Poput hardverskih vatrozida, virtualni vatrozidi dopuštaju ili odbijaju pristup mreži tokovima prometa između nepouzdanih zona i pouzdanih zona. Za razliku od hardverskih vatrozida koji se fizički nalaze lokalno u podatkovnim centrima, virtualni vatrozidi su u suštini softver koji ih čini idealnim za zaštitu virtualnog okruženja. Kako inovacijama

[23] UTM Security with Fortinet Mastering FortiOS [4]

i smanjenju troškova računalne opreme i prelazak na virtualno okruženje tj. računalstvo u oblaku s tim dolaze i sigurnosni rizici. Dolaze nove vrste napada koje zaobilaze parametre standardne sigurnosti i sustavi koji imaju decentraliziranu strukturu gdje su aplikacije i podaci postavljaju na više krajnjih točaka a ne s jednog posvećenog izvora rezultira otežanu vidljivost i sigurnost imovine. Virtualni vatrozid se može instalirati kao tradicionalni softverski vatrozid na gostujućoj virtualnoj mašini koji već radi u virtualiziranom okruženju. Trenutni smjer u tehnologiji virtualnog vatrozida je kombinacija virtualnih prekidača koji imaju mogućnost zaštite i virtualnih sigurnosnih uređaja. Neki virtualni vatrozidi integriraju dodatne funkcije kao što su VPN *(engl. Virtual Private Network)* od mjesta do mjesta i udaljenog pristupa, QoS *(engl. Quality of Service)*, filtriranje URL-ova i još mnogo toga. Nije iznenađujuće da su se LAN menadžeri, stručnjaci za sigurnost i dobavljači mrežne sigurnosti počeli pitati je li možda učinkovitije zadržati promet u potpunosti unutar virtualiziranog okruženja i osigurati ga od tamo.

7.2. FortiGate

U sklopu ovog projekta koristi se vatrozid sljedeće generacije koji može biti i softverski i hardverski a to je *FortiGate.*

FortiGate je prvi proizvod firme *Fortinet* koja razvija i prodaje rješenja mrežne sigurnosti. Razvijen je kao fizički vatrozid koji je s vremenom se proširio i kao virtualna inačica koja se pokreće uz pomoć virtualnih platformi kao što je *VMware vSphere.*

Fortinet je s vremenom objedinio sigurnosne funkcije kao što je vatrozid, anti-spam i antivirusni softver u jedan proizvod. 2016. godine započeli su graditi platformu gdje može se može odvijati komunikacija između njihovih sigurnosnih proizvoda. Osim *FortiGate*-a postoji *FortiGuard* vođen umjetnom inteligencijom za bolje otkrivanje novih i nepoznatih prijetnji, *FortiOS* predstavlja sigurnosni operativni sustav, *Fortinet Manager* pruža uslugu centralnog upravljanja *Fortinet* uređajima s mjesta jednog uređaja. To omogućuje potpunu administraciju i lakšu vidljivost uređaja.

Vatrozid *FortiGate* radi tako što ispituje podatke koji ulaze u vašu mrežu i provjerava jesu li isti sigurni za proći kroz mrežu tvrtke. Niži sloj vatrozida će ispitati podatke i

tražiti informacije vezano za njihovu lokaciju i njen izvor. Dobivene informacije se uspoređuju sa popisom premise kako bi se procijenilo mogu li ti paketi biti pušteni ili ne.

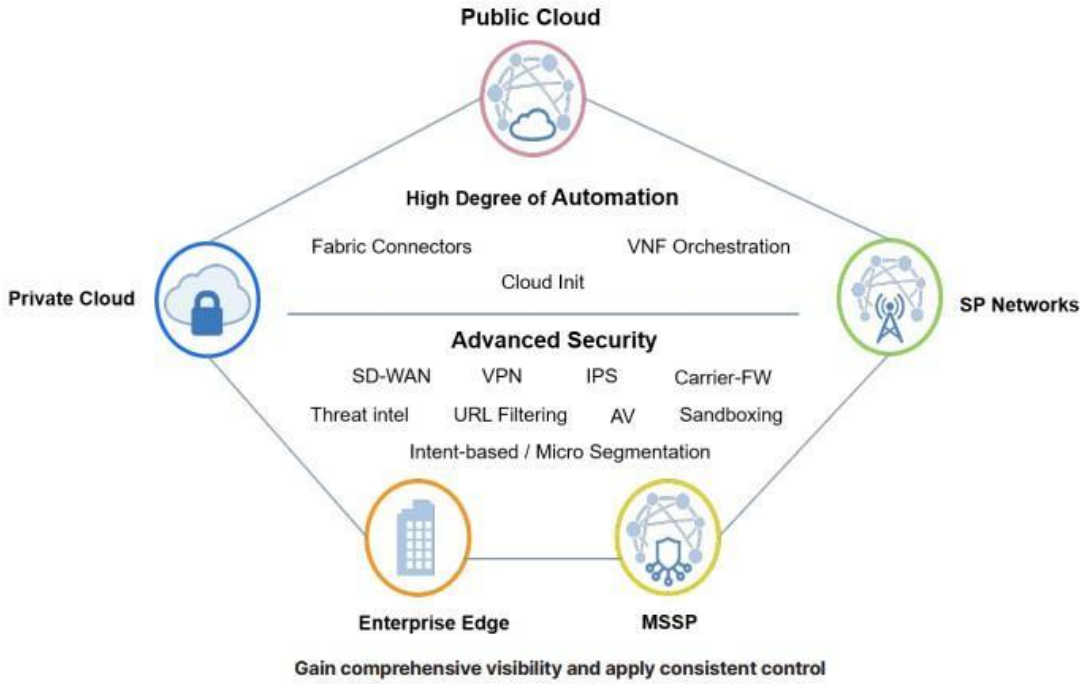
Jedna od glavnih značajki *FortiGate-a* je visoka performansa zaštite od prijetnji koja uključuju filtriranje *weba*, antivirusna i kontrola aplikacije osiguravaju protok informacija i nesmetano poslovanje. Faktor automatizacije procjene rizika koja automatizira tijek rada i značajno olakšava rad u sektoru IT. Konstantno nas obavještava o informacijama vezano za prijetnje i osigurava nas od poznatih i nepoznatih napada. Mogućnost raspolaganja i modificiranja zaštite nad imovinom neovisno gdje se nalazimo.[24]

Vatrozid FortiGate može zaštititi od brojnih prijetnji kao što su :

- Zlonamjerni softver *(engl. Malware)*
- Špijunski softver *(eng. Spyware / Grayware)*
- *Phishing / Sheme* društvenog inženjeringa *(engl. Social Engineering schemes)*
- Farming napadi *(engl. Phrming attacks)*
- Virusne instant poruke *(engl. Instant messaging viruses)*
- *Peer-to-Peer* mreže
- Kombinirani mrežni napadi *(engl. Blended network attacks)*
- E-mail
- Upadi u mrežu

[24] Product FortiGate [11]

Plan raspoređivanja (sl. 12)



Slika 12. Plan raspoređivanja Fortinet-a

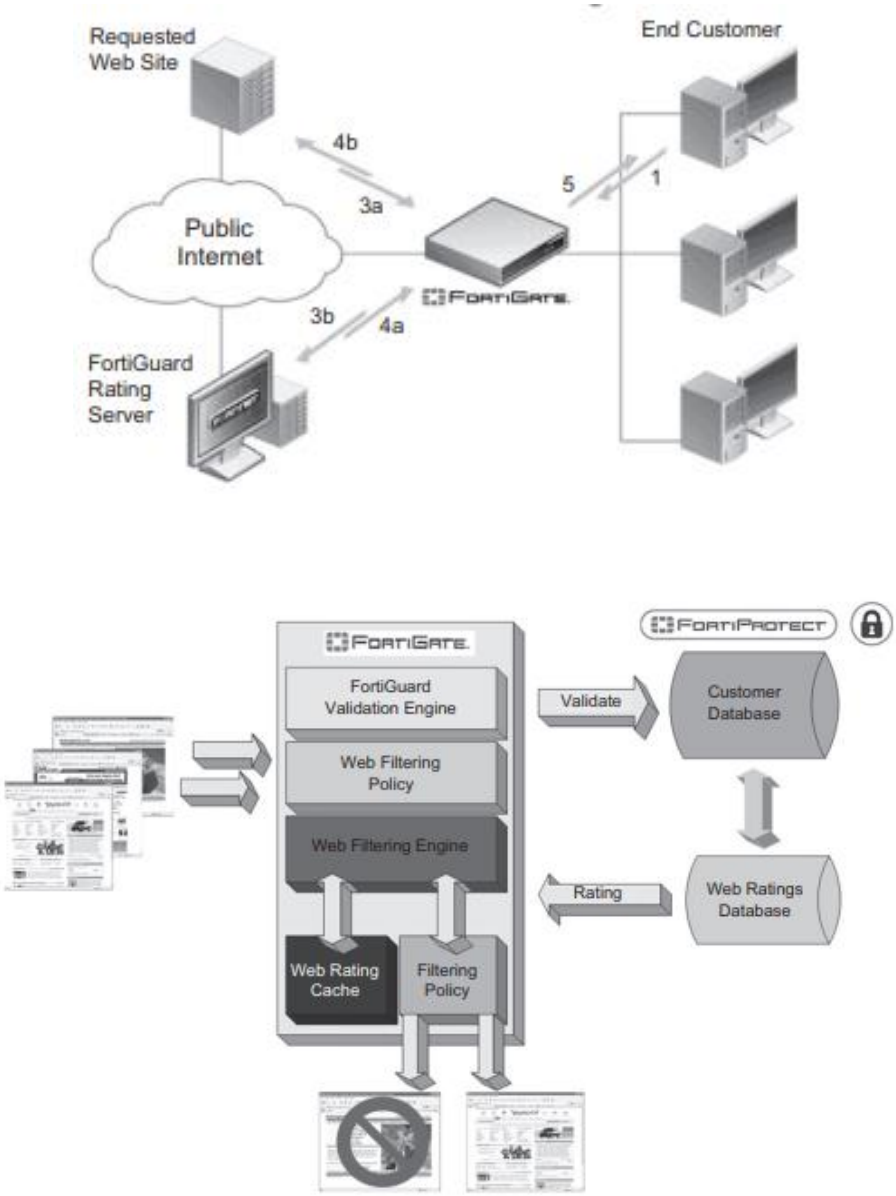
Izvor: https://www.fortinet.com/, 2022.

Virtualni vatrozid se implementira kao prva linija obrane ili zaštita u unutrašnjim zonama virtualnih okruženja. FortiOS je vodeći operativni sustav koji omogućava konvergenciju visoke razine umrežavanja i sigurnosti kroz platformu *Fortinet Security Fabric*. Platforma je dosljedna i konstantno aktivna kroz sve krajnje točke mreže u računalnom oblaku. Aktivni i jedinstven pristup omogućuje stvaranje novih vrsta zaštite i omogućuje organizacijama da vode svoje poslovanje nesmetano i bez ikakvih ugrožavanja performansi ili zaštite. Nude usluge kao što je *FortGuard i FortiCare*. *FortiGuard* nudi informacije o prijetnjama u realnom vremenu, te pritom daje opsežna sigurnosna rješenja diljem njihove platforme prilikom ažuriranja.[25]

[25] FortiGate virtual appliances [5]

FortiCare je tehnička podrška za njihove klijente. Fortinet surađuje s inženjerima, istraživačima sigurnosnih prijetnji, forenzičkim stručnjacima, organizacijama za provedbu zakona i ostalim pružateljima računalnih mreža.

Na sljedećim slikovnim primjerom 13. prikazujemo jedno mrežno čvorište i njen vatrozid. Unutrašnji dio FortiGate vatrozida prikazujemo tok sortiranja sadržaja njenu distribuciju i kategorizaciju.



Slika 13. Filtriranje sadržaja kroz FortiGate

Izvor: Computer and Information Security Handbook, Third Edition, poglavlje e87

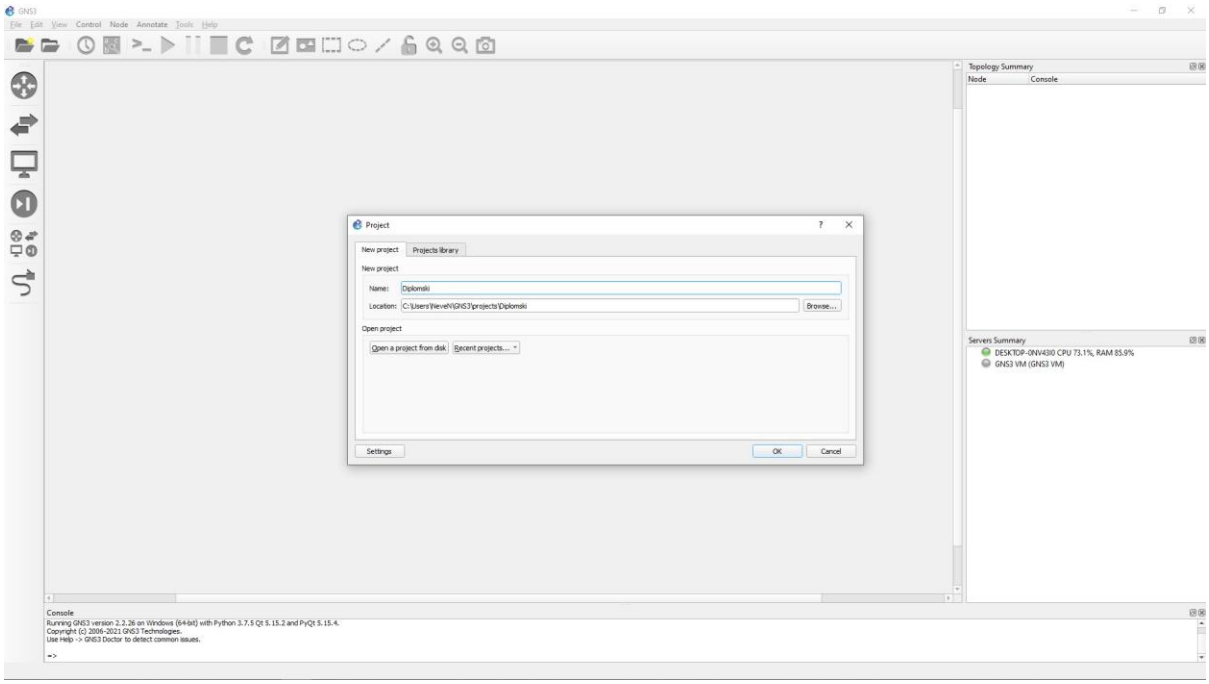
8. GNS3

Ovo poglavlje približava GNS3 *(engl. Graphical Network Simulator*) i konfiguraciju sigurnosti jednostavnih mreža. Naime, GNS3 je alat otvorenog koda i kao takav daje besplatnu licencu za rad. Može se koristiti na različitim platformama operacijskih sustava kao što su *Windows OS, Linux i MacOS X*.

8.1. Značajke GNS3-a

Jedna od osnovnih zadaća ovog programskog alata je testiranje i simulacija mrežnih uređaja. Jedna od posebnih značajki je ta da ima integriran Wireshark sučelje za snimanje odnosno praćenje mrežnog prometa na virtualnim poveznicama unutar laboratorijskih okolina. GNS3 je alat za simulaciju kompleksnih mrežnih okolina koje mogu poslužiti za pripremu polaganja različitih certifikata kao što su CCIP, CCNA, CCNP, JNCIE i drugi. Kroz ovaj alat moguće je eksperimentalno testirati značajke i inačice Cisco IOS-a i Juniper JunOS ili napraviti testnu topologiju koje će se kasnije moći iskoristiti u stvarnoj mrežnoj okolini.[26]

[26] Graphical Network Simulator (GNS) [7]



Slika 14. GNS3 UI/sučelje

Izvor: samostalna izrada, 2022.

Osim početnog prozora, izbornik se račva na dva dijela na lijevi, desni, gornji i donji dio. Gornja strana nam omogućuje izrada novog projekta, učitavanje postojećeg projekta, napraviti snimak trenutne situacije, otvaranje konzole, start-pauza-stop svih uređaja u mrežnoj okolini te njegovo ponovno osvježavanje do pisanja teksta i izrada oblika kako bi znali koji element kome pripada i na kraju snimak ekrana trenutnog projekta. Prikaz na sljedećoj slici.

Slika 15. Kontrolna ploča GNS3

Izvor: samostalna izrada, 2022.

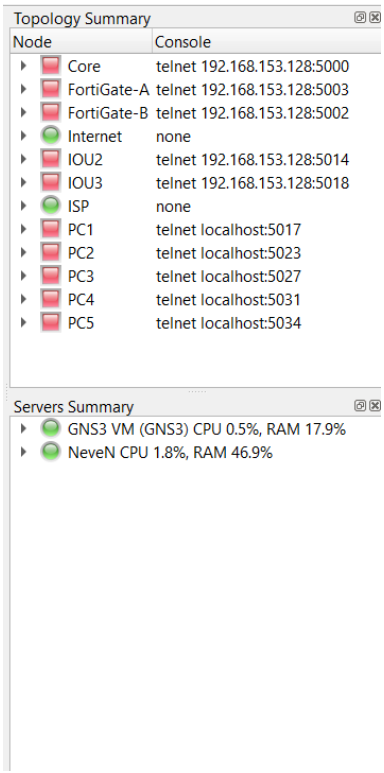
Lijevi dio se proteže od vrha silazno gdje vidimo opcije za mrežne uređaje, usmjernike, preklopnike, terminal, sigurnosne mrežne uređaje, izbornik svih učitanih

uređaja u sustavu i na kraju povezivanje mrežnih uređaja Ethernet kabelom. Prikaz na sljedećoj slici.

Slika 16. Kontrolna ploča GNS3

Izvor: samostalna izrada, 2022.

Desna strana nam predstavlja dva prozora u kojem gornji prikazuje listu uređaja koje imamo u našoj topologiji a drugi prozor prikazuje naše servere i njihovu potrošnju radne snage. Prikaz na sljedećoj slici 17.



Slika 17. Elementi topologije u GNS3

Izvor: samostalna izrada, 2022.

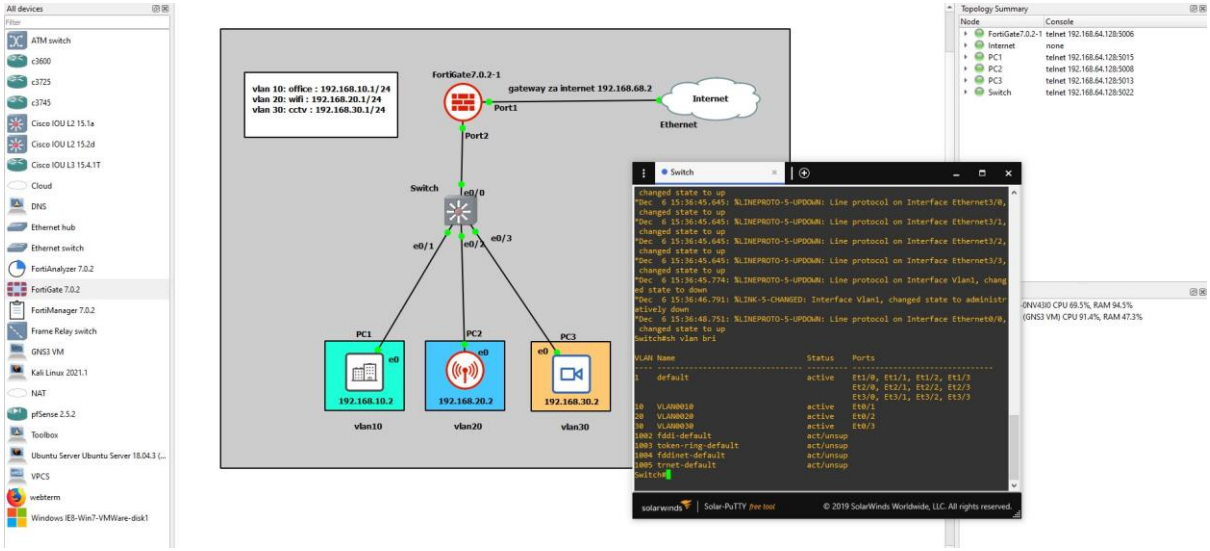
Donja strana prikazuje nam terminal konzolnog prozor koji je integriran sa jezikom Python koji nam javlja učinak, kontrolne greške, upozorenja vezane za pojedinačne uređaje ili cijelu topologiju projekta. Prikaz na sljedećoj slici.

Slika 18. Terminal konzole GNS3

Izvor: samostalna izrada, 2022.

Kako bi započeo rad u GNS3 treba imati inačicu konkretnog uređaja odnosno engleski *image* na kojem su sačuvani podaci gdje možemo obaviti instalaciju tj.

učitavanje samog uređaja u sučelje GNS3 programskog alata. Za izvođenje ovog rada koristiti ćemo preklopnik Cisco IOU L2 15.2d i vatrozid FortiGate 6.4.7 koji se prikazuju na slici 19, te njihov terminal za uspostavljanje povezanosti i određenih pravila.

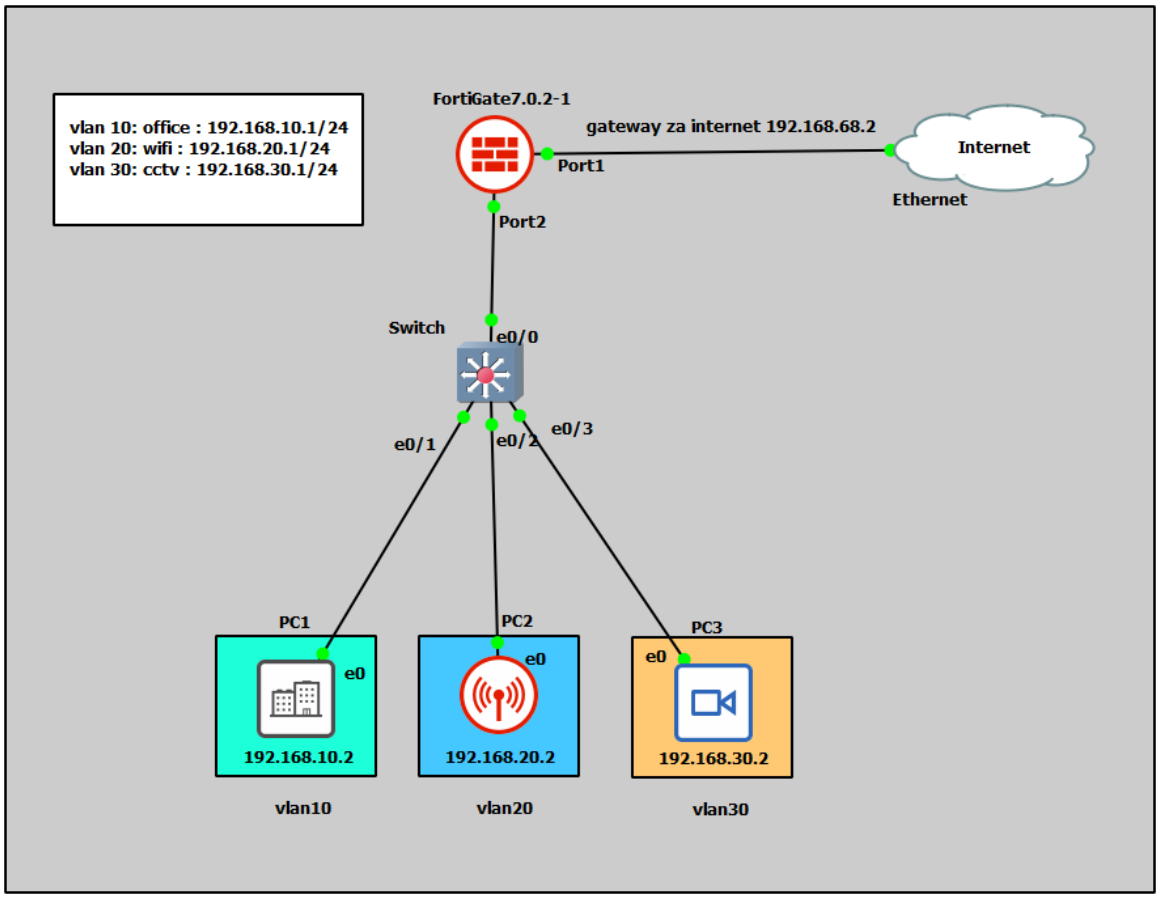


Slika 19. Topologija projekta 1

Izvor: samostalna izrada, 2022.

8.2. Konfiguracija sigurnosti jednostavne mreže

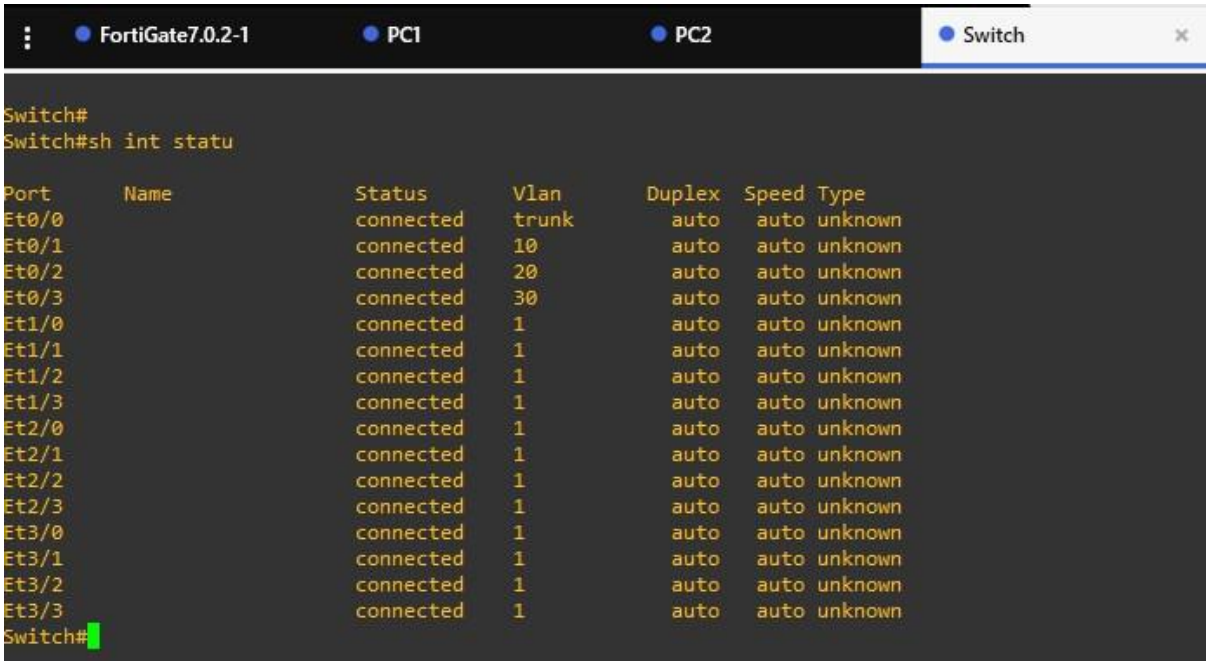
U prvom primjeru prikazati će se svrha i princip rada sigurnosne mreže. Prikazati će se upotreba ISP-a, VRF-a, VLAN, FortiGate-a, OSPF. Biti će simulirane različite VLAN mreže koje će korisnik dobiti svaku svoju IP adresu koje će biti povezane preko preklopnika na kojem je povezan vatrozid FortiGate. FortiGate omogućuje VRF, pristup mrežnim uređajima i njihovim pravilima ponašanja. Za upotrebu ove simulacije koristi se VPCS koje se preoblikuje u CE *(engl. Customer Edge)*, Cisco IOU L2 15.2d i posluži kao preklopnik i vatrozid FortiGate 6.4.7. Cijela topologija se vidi na slici 20.



Slika 20. Topologija prvog primjera

Izvor: samostalna izrada, 2022.

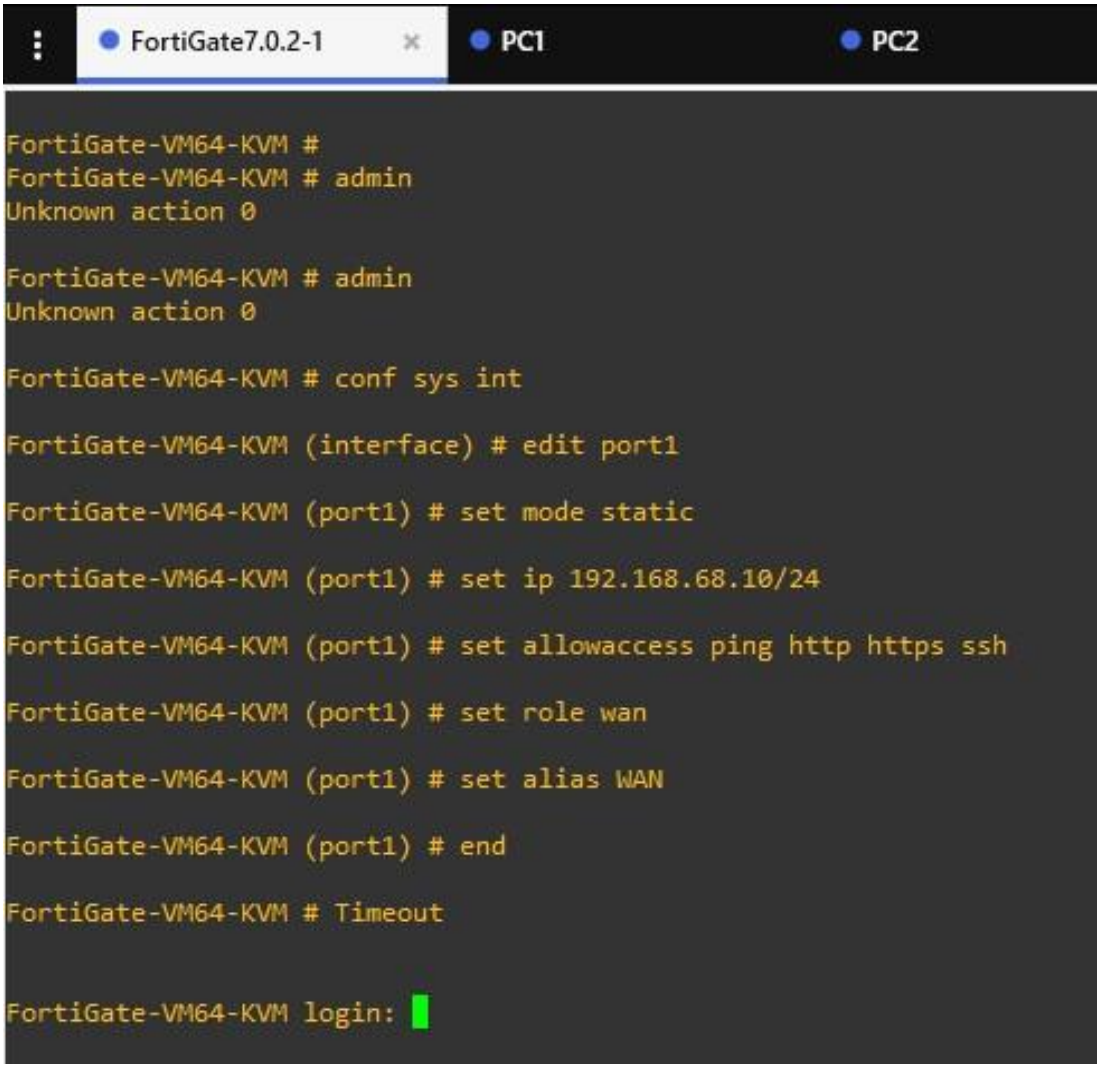
Postavljena su tri VPCS -a gdje PC1 ima ulogu Office-a odnosno ureda, PC2 ima ulogu WiFi mreže i PC3 ima ulogu CCTV kamere. Svaka VPCS ima domenu određene IP adrese koje su spojene preko preklopnika koji omogućava međusobnu komunikaciju. Kod preklopnika preko konzole možemo saznati u kojem se statusu nalaze naši priključci *(engl. port)* naredbom show interface status. Na slici 21 se može vidjeti koliko ima aktivnih priključaka i koji su to konkretni i njihove postavke.



Slika 21. Status priključka

Izvor: samostalna izrada, 2022.

1. Konfigurira se vatrozidov priključak kako bi imao grafičko sučelje koje je povezano sa internetom.
2. U FortiGate-u se konfigurira sučelje *(engl. interface)* za VLAN mreže. Kad se stvore sučelja, treba napraviti zonu kako bi VLAN mreže mogle komunicirati ili ne komunicirati jedni s drugima. Kreira se statička rutu za izlaz prema internetu, u ovom slučaju to je 192.168.68.2. I posljednje, treba napraviti policu vatrozida, odnosno *IPv4 Policy* gdje se omogućuje zoni pristup internetu.
3. Nakon toga treba postaviti preklopnik i povezati pravilne priključke (sl. 22).
4. Kada se pravilno dodjeli VLAN mreže može se prijeći do VPCS-a.
5. Nakon konfiguracije preklopnika se upale uređaji koji mogu biti stvarni operacijski sustavi poput *Ubunut, Linux, Windows,* no u ovom slučaju VPCS. Kada se uređaji pokrenu, oni automatski dobiju IP adresu zbog DHCP-a koji je uključen za sučelja preko FortGate-a (sl. 23).
6. Kad se sve poveže, naredbom *ping se* testira komunikacija između uređaja vatrozida i povezanosti s internetom (sl. 24).

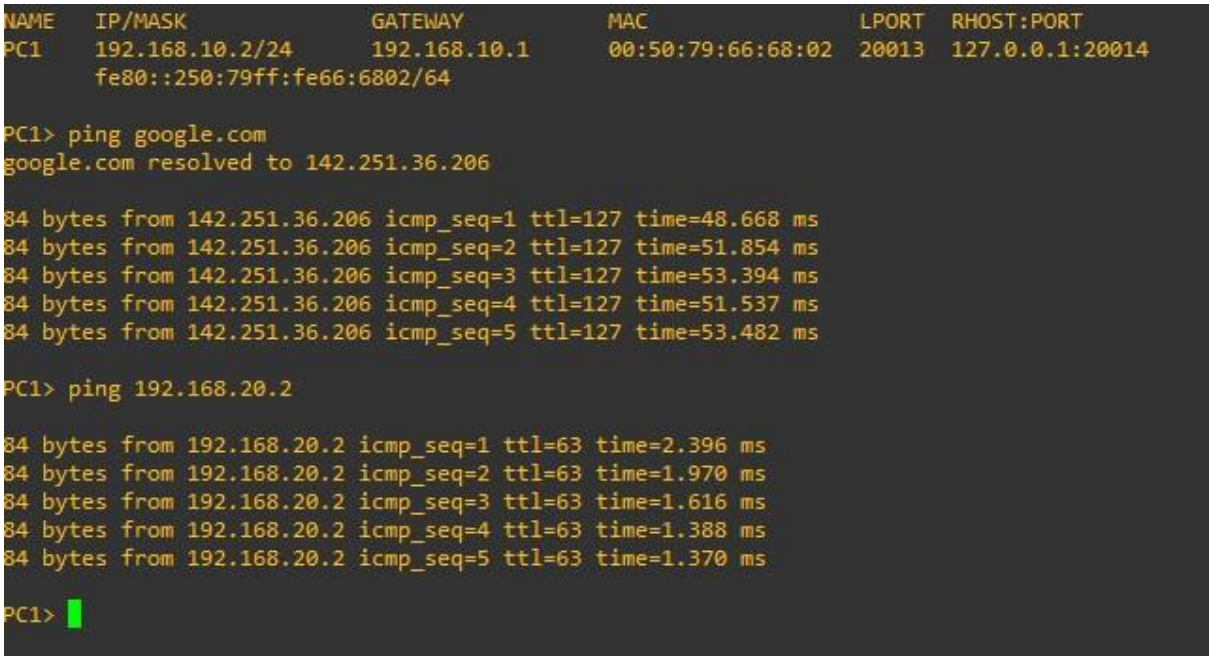


Slika 22. Konfiguracija FortiGate-a

Izvor: samostalna izrada, 2022.

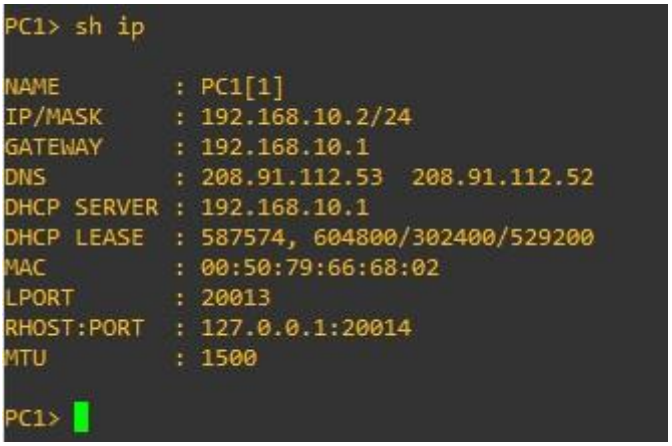
Slika 23. Lista VLAN mreža

Izvor: samostalna izrada, 2022.



Slika 24. Testiranje komunikacije između uređaja i pristup prema Internetu

Izvor: samostalna izrada, 2022.



Slika 25. IP informacije Office-a

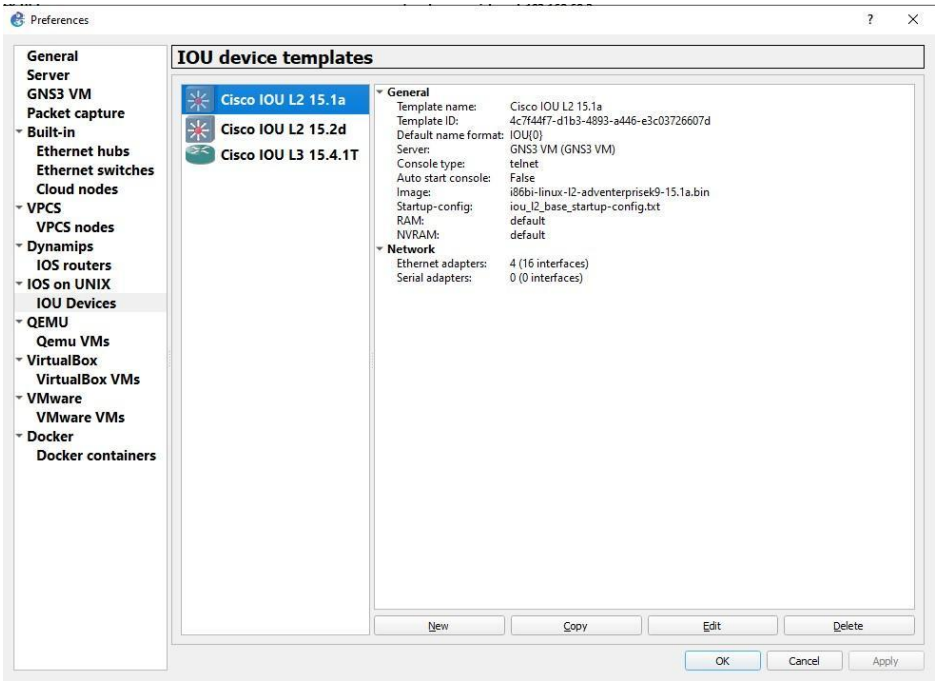
Izvor: samostalna izrada, 2022.

9. SIMULACIJA SIGURNE MREŽE PUTEM GNS3

U ovom dijelu poglavlja se predstavlja infrastruktura i topologija projekta. Opisuju se uređaji koji koriste njihovu konfiguraciju.

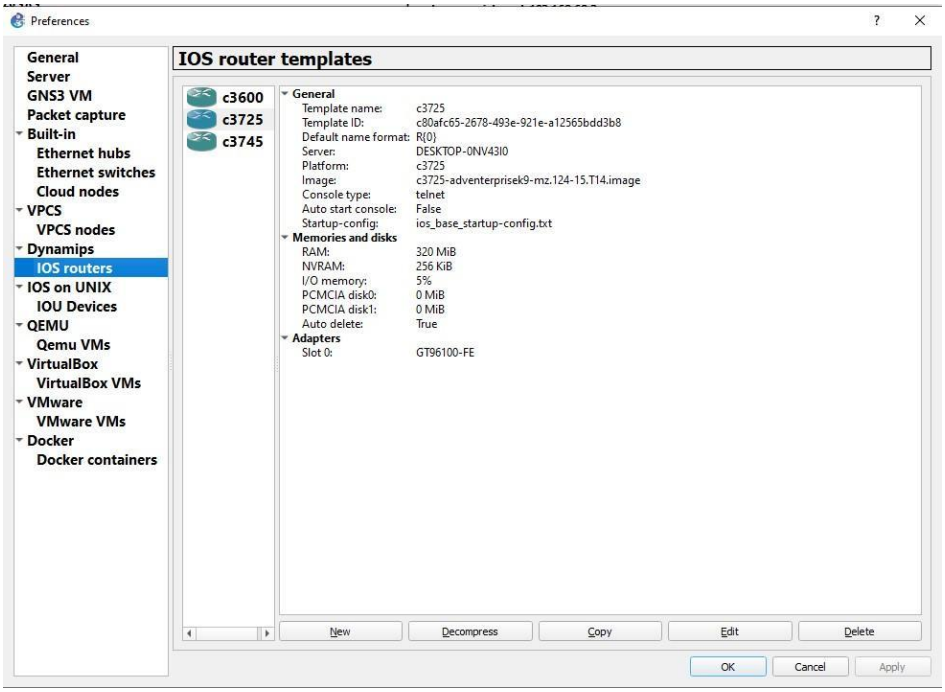
9.1. Sastavnice projekta

Za emulaciju ovog projektnog zadatka potreban je već spomenuti GNS3 verzija 2.2.26 koja se pokrenula na operativnom sustavu Windows 10. Također je potreban i virtualna mašina kako bi se pokrenuo Operativni sustav *Kali Linux, Ubuntu*, da bi se ostavarila internet veza. U sklopu projekta se koristila *Vmware Workstation 16 PRO* verzija 16.2.0, kao platforma za pokretanje virtualnih mašina. U programu GNS3 koristile su se inačice usmjerivača, preklopnika, vatrozida te ostalih virtualnih uređaja. Cijeli projekt je u sklopu virtualnog okruženja sa stvarnim inačicama proizvoda kao što je vatrozid FortiGate, preklopnik Cisco L2 ili L3. Sljedećim slikama su prikazani korišteni virtualni uređaji. Slika 26. prikazuje Cisco IOU *(engl. Cisco IOS on Unix)* L2 15.2a i njegove parametre. Slikovni primjer 27. prikazuje Cisco usmjernike, dok 28. prikazuje Qemu platformu za pokretanje virtualnih mašina na operativnom sustavu Linux. Na toj platformi se koristi FortiGate verzija 6.4.7, Kali Linux verzija 2021.1. Slikovni primjer broja 29. prikazuje *Toolbox i webterm* koji dolaze u sklopu Docker-a koji omogućuje jednostavnu uporabu i instalaciju ovih elemenata.



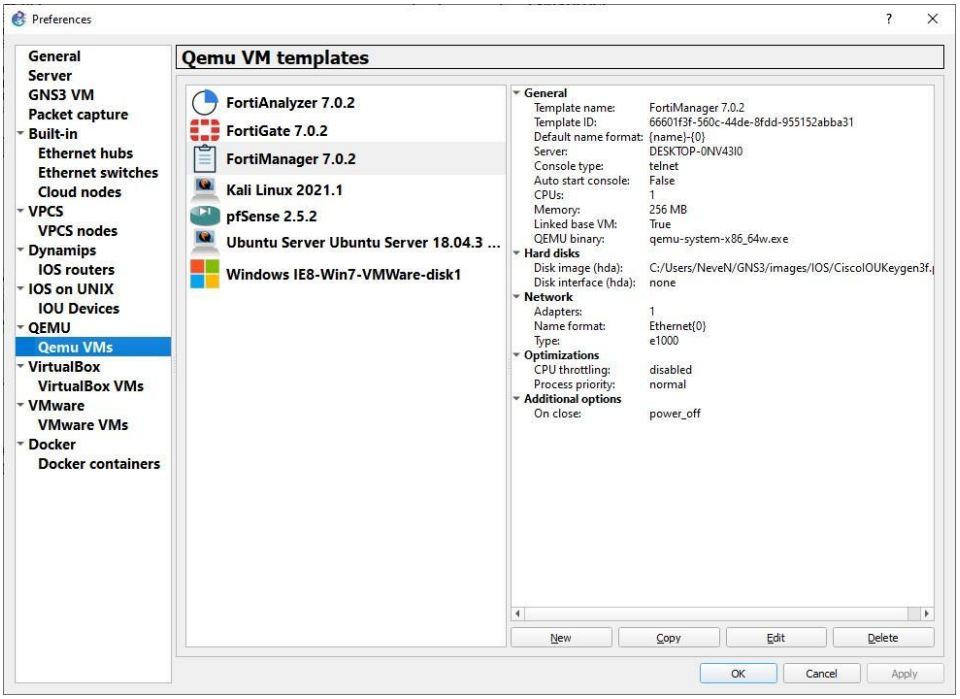
Slika 26. Prikaz preklopnika u GNS3

Izvor: samostalna izrada, 2022.



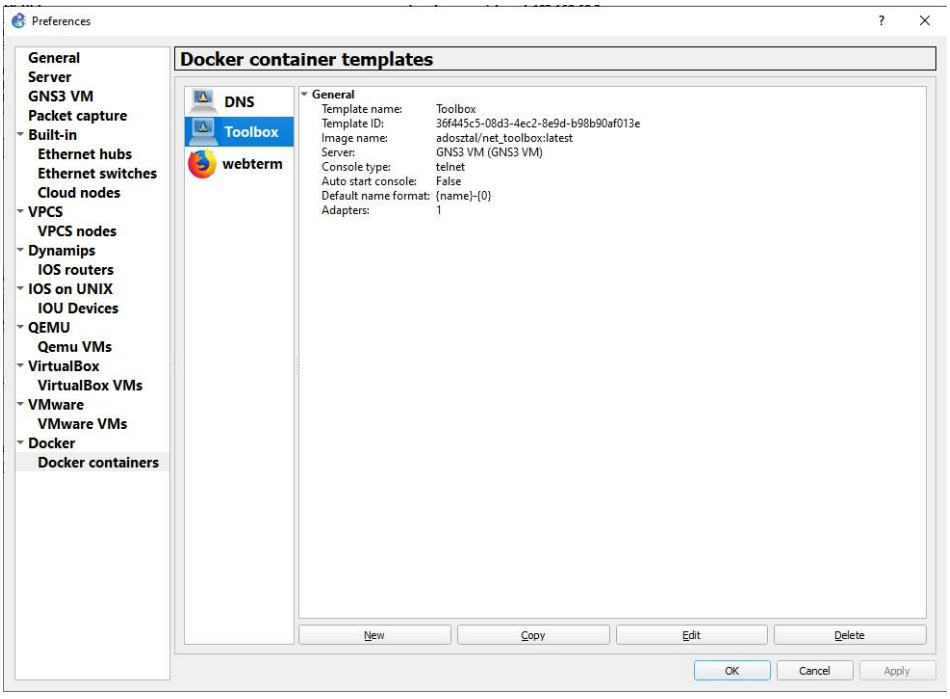
Slika 27. Prikaz usmjerivača u GNS3

Izvor: samostalna izrada, 2022.



Slika 28. Prikaz vatrozida, OS Kali Linux, pfSense i Fortinet proizvoda u GNS3

Izvor: samostalna izrada, 2022.



Slika 29. Prikaz elemenata koji dolaze u Docker kontejneru

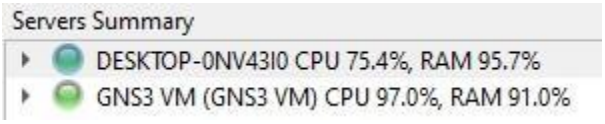
Izvor: samostalna izrada, 2022.

9.2. Konfiguracija

Kada se zna koje će se stavke koristiti, mora se odlučiti koji će se server upražnjavati. Postoje dvije opcije, primjer je predstavljen na slici 30.

Lokalni server pokrenut na računalu

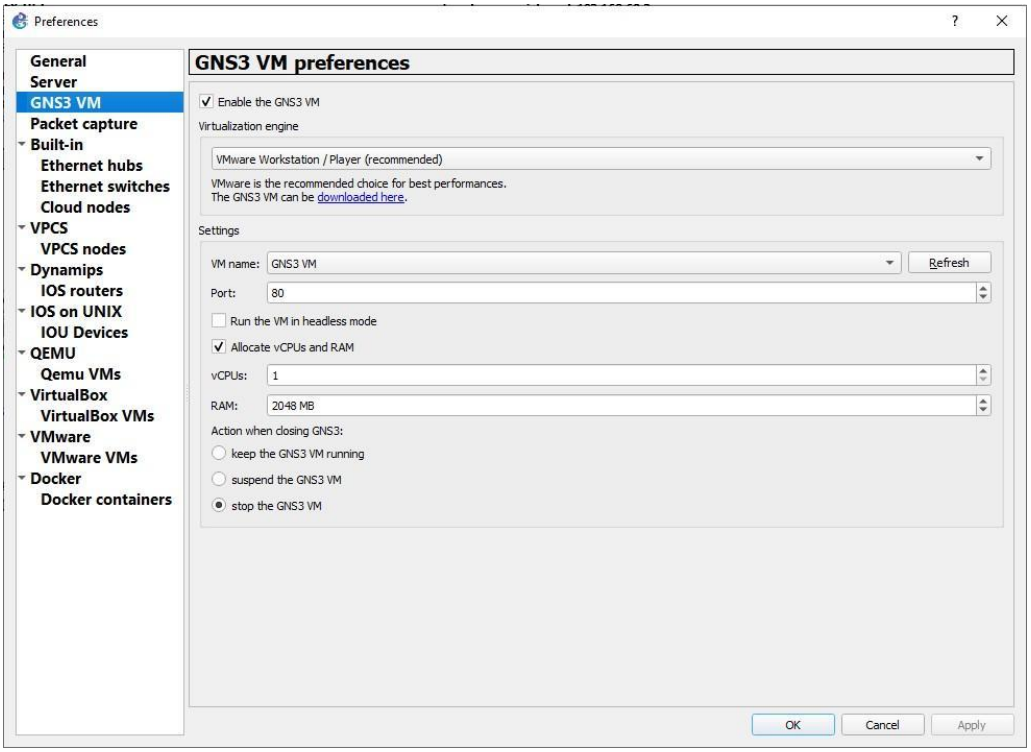
Virtualni server pokrenut na VMware-u



Slika 30. Prikaz servera unutar GNS3

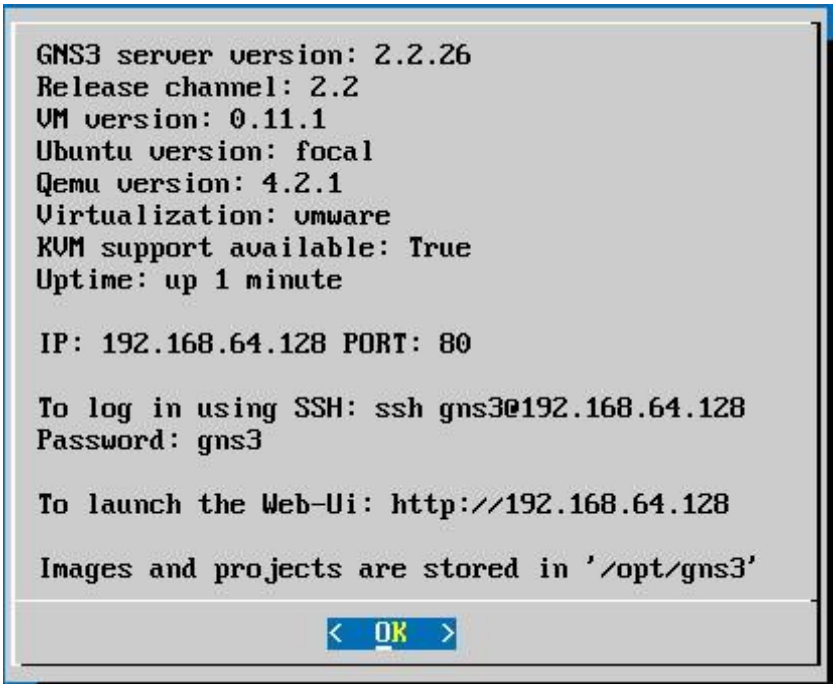
Izvor: samostalna izrada, 2022.

Prilikom konfiguracije projekta izabran je virtualni server, a da bi server radio treba imati određenu konfiguraciju koja je prikazana na slikama 31. i 32.



Slika 31. Prikaz parametara u GNS3

Izvor: samostalna izrada, 2022.

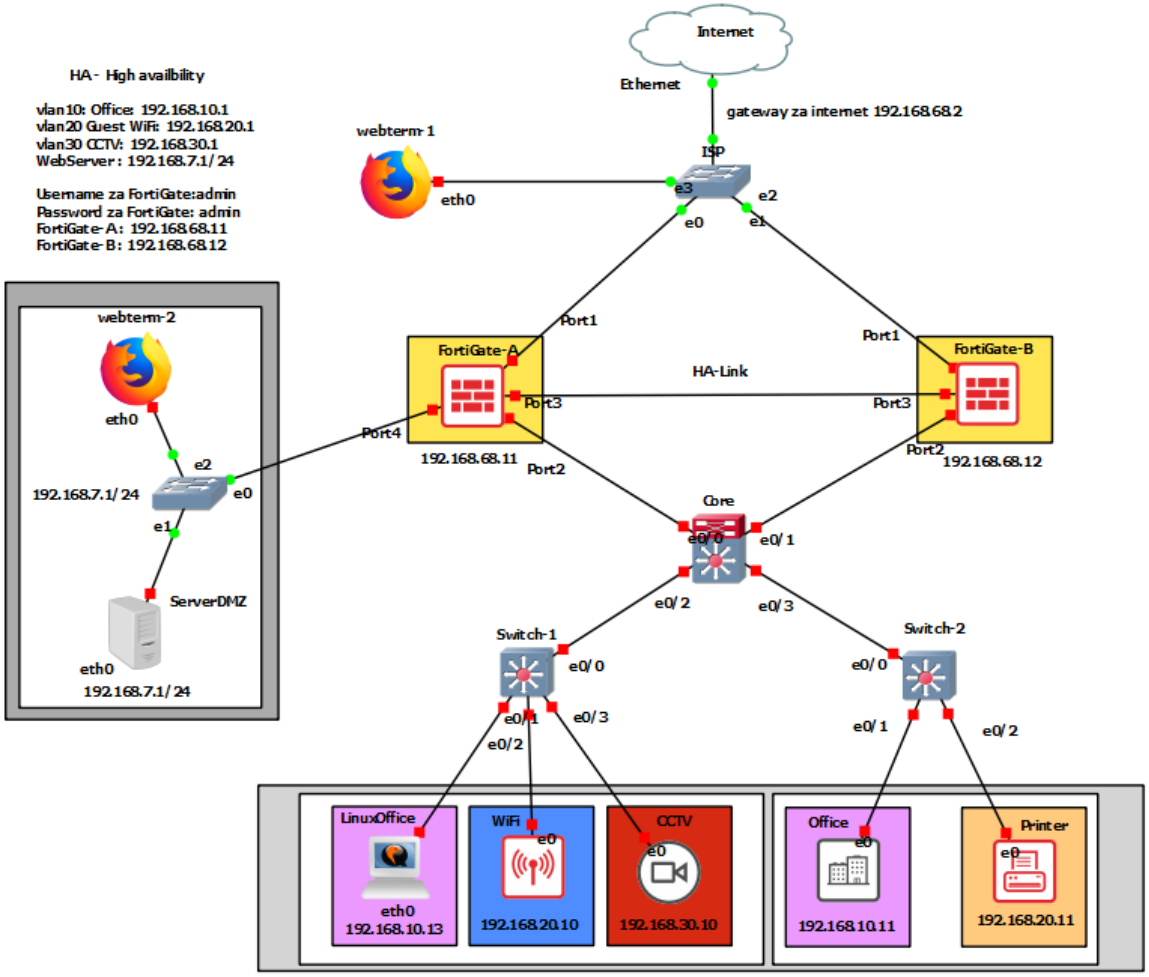


Slika 32. Prikaz parametara u VM Workstation 16 PRO

Izvor: samostalna izrada, 2022.

9.3. Oblikovanje LAN mreže

Nakon što je konfiguracija provedena za server, može se dizajnirati LAN mreža. U sklopu projekta se koriste Virtualna računala koji se nazivaju VPCS, preklopnik Cisco IOU L2 15.2d, vatrozid FortiGate verzije 6.4.7, toolbox kao DMZ i webterm koji se kasnije koristi kao preglednik i terminal. Prikaz mreže predstavljen je slikom 33.

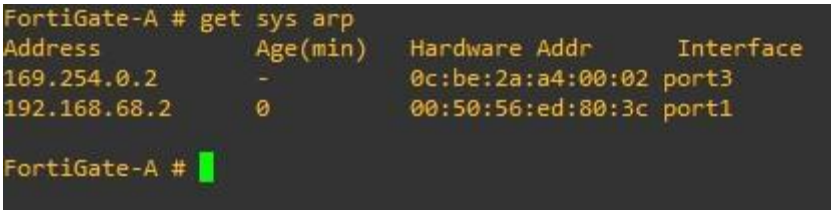


Slika 33. Prikaz LAN mreže

Izvor: samostalna izrada, 2022.

9.3.1. Konfiguriranje FortiGate-a

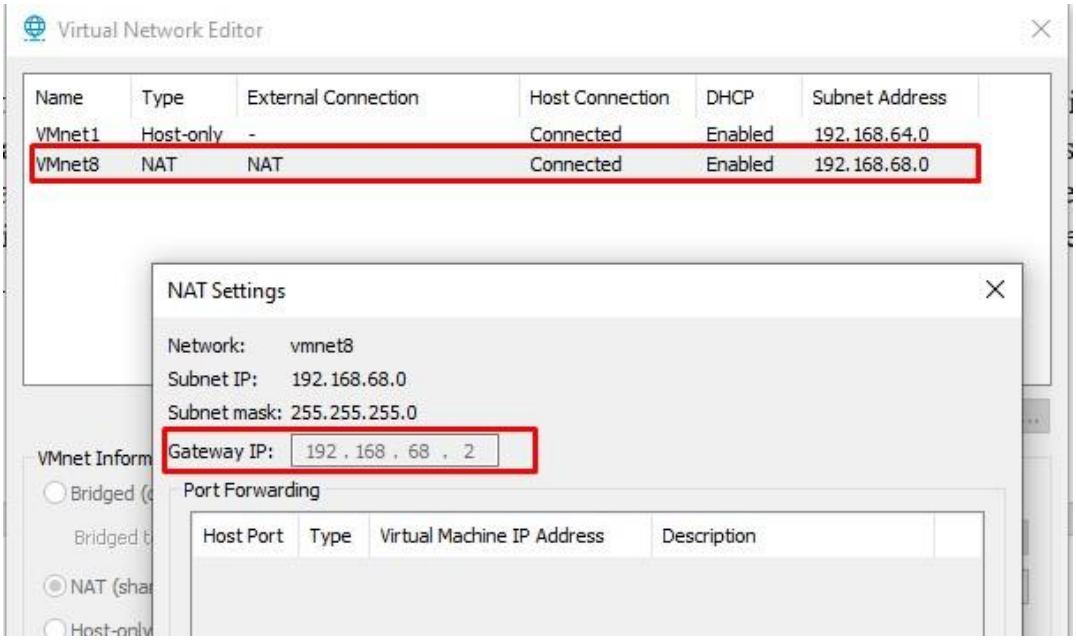
Nakon što su se svi uređaji spojili s Ethernet kabelom, uključivanje svih uređaja prije konfiguracije nije dobra ideja, zato što program opterećuje računalo i treba se pridržavati nekakvog redoslijeda prilikom osposobljavanja uređaja. Prvi uređaj koji je konfiguriran je FortiGate-A. Nakon prijavljivanja u uređaj, provjerava se ima li vezu s internetom. Kako bi to saznali upisuje se naredba „*get sys arp*“.



Slika 34. Prikaz izlaza na Internet putem VMware-a

Izvor: samostalna izrada, 2022.

Također, to se može saznati i preko *VMware Workstation*-a klikom na opciju *Virtual Network editor* i dobiju se informacije o pristupu *(engl. Gateway)* odnosno izlazu na internet vezu (sl. 35).

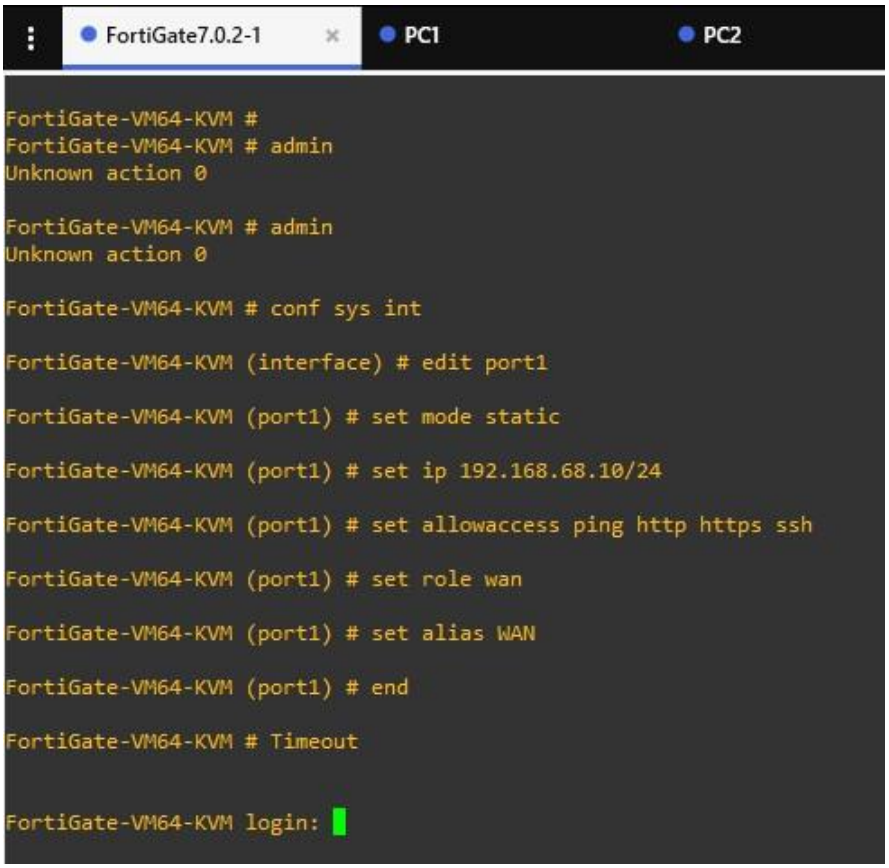


Slika 35. Prikaz pristupa na Internet putem VMware-a

Izvor: samostalna izrada, 2022.

Kada se sazna pristup internetu, namješta se port koji je spojen direktno na internet i dodjeljuje se vatrozidu IP adresu u sklopu Gateway-a (pristupa), u ovom slučaju to je 192.168.68.2/24, stoga adresa za sučelje FortiGate-a je 192.168.68.10/24. Dopušta se ping koji služi za provjeru dostupnosti, http, https i ssh. Uloga je WAN jer je to pristup internet vezi. Kako bi se lakše prepoznao port ili priključak stavlja mu se

alias WAN. Na sljedećoj slici broja 36. se vidi red naredbi. Nakon dodjeljenje adrese drektno se pristupa grafičkom sučelju preko preglednika upisujući zadanu adresu koja je zadana, u ovom slučaju 192.168.68.10/24.

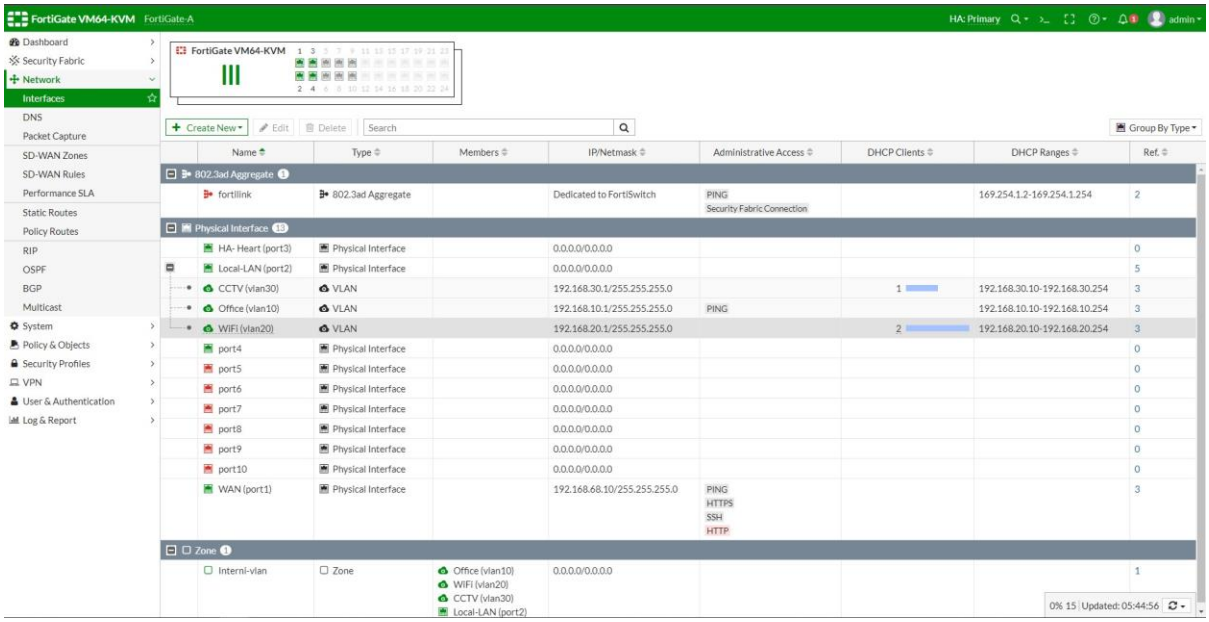


Slika 36. Kreiranje grafičkog sučelja i dodjeljivanje adrese FireGate-u

Izvor: samostalna izrada, 2022.

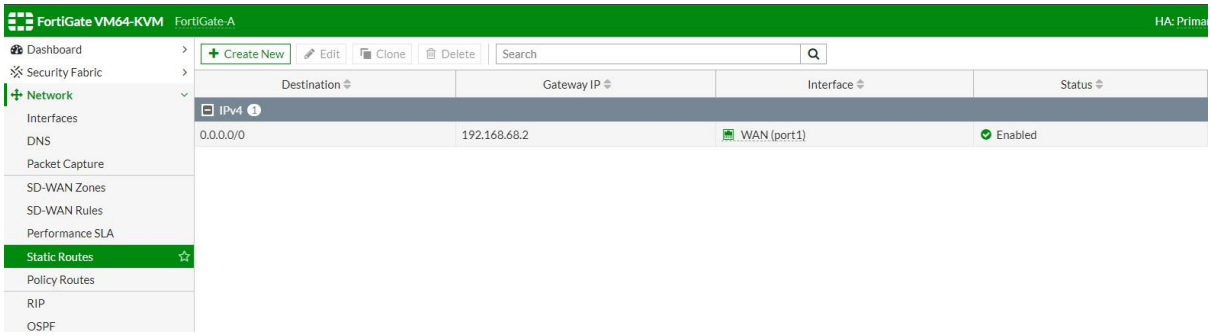
9.3.2. Konfiguriranje VLAN-a

Grafičko sučelje FortiGate-a jako je intuitivno i jednostavno postavljeno (sl. 37). Ideja je da se sve stavke centraliziraju. Na lijevoj strani smještena je kontrolna ploča, *Security Fabric* koja je dio platforme povezivajući proizvod Fortinet-a. Sekcija *Network* je ta gdje se mogu pregledati stanja portova, kontrolnih zona, sučelja, statičnih ruta i drugo. Na slici broj 37. prikazano je sučelje za isti.



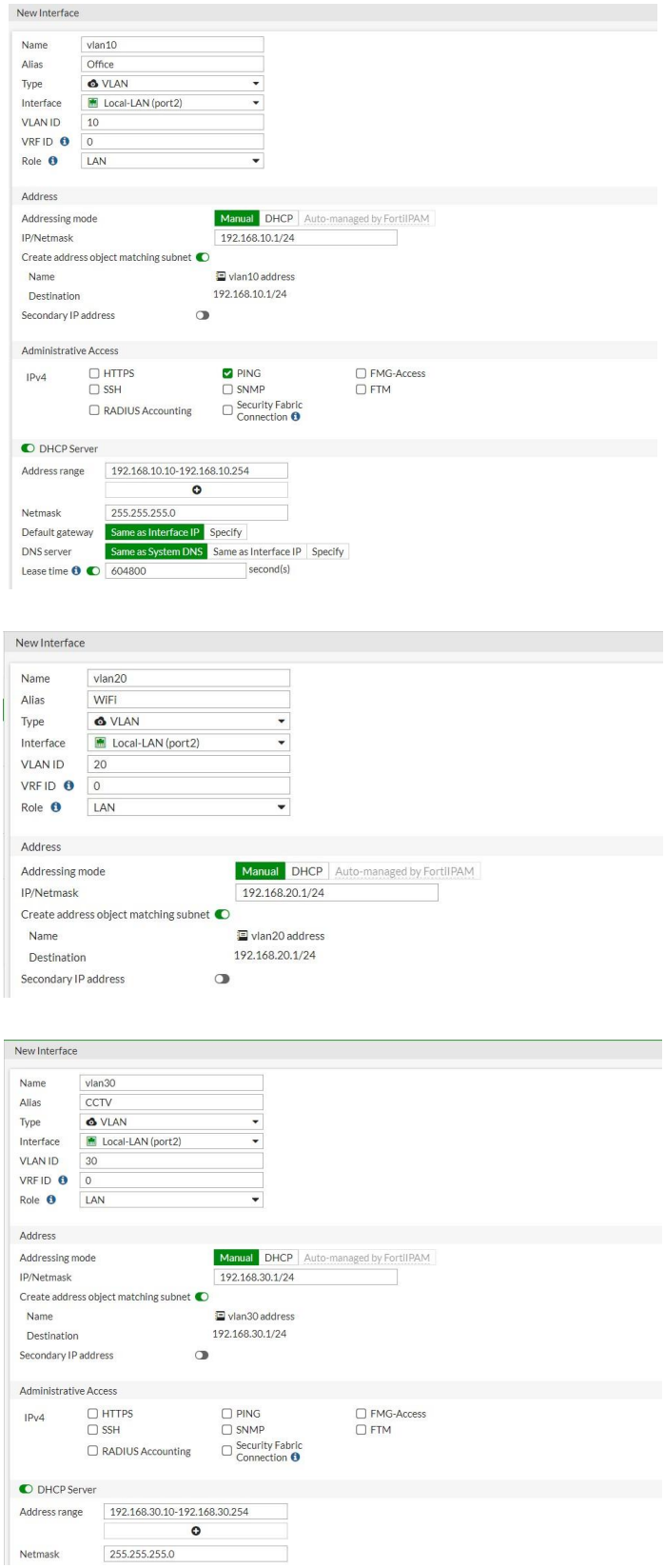
Slika 37. Prikaz sučelja skecije Network u FortiGate-u
Izvor: samostalna izrada, 2022.

Po zadanom, svi portovi su blokirani, kako bi bili povezani s internetom, dolazi do konfiguracije vatrozida i njegovih portova kako bi ostali uređaji imali pristup internetu i internoj komunikaciji, što rezultira uspostavljanje statične rute, prikazano na slici 38.



Slika 38. Prikaz statičke rute prema Internet vezi
Izvor: samostalna izrada, 2022.

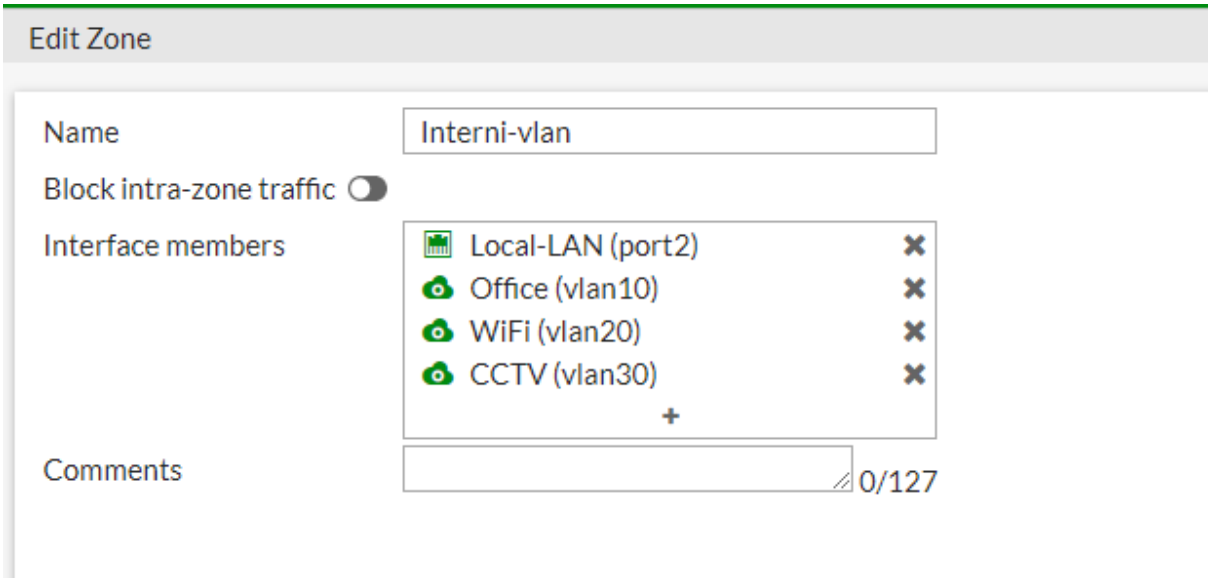
Zatim slijedi konfiguriranje sučelja za virtualne mreže odnosno VLAN. Modificiranje se obavlja preko sučelja FortiGate-a tako što se otiđe u sekciju *Network* i kreira novo sučelje. VLAN se podijeliti u dijelove koje svako imaju svoju ulogu. VLAN 10 je određen za Office, VLAN 20 predodređen je za WiFi i na kraju VLAN 30 zadan je za CCTV kamere. Njihova konfiguracija se vidi na sljedećim slikama.



Slika 39. Prikaz konfiguracije sučelja za VLAN

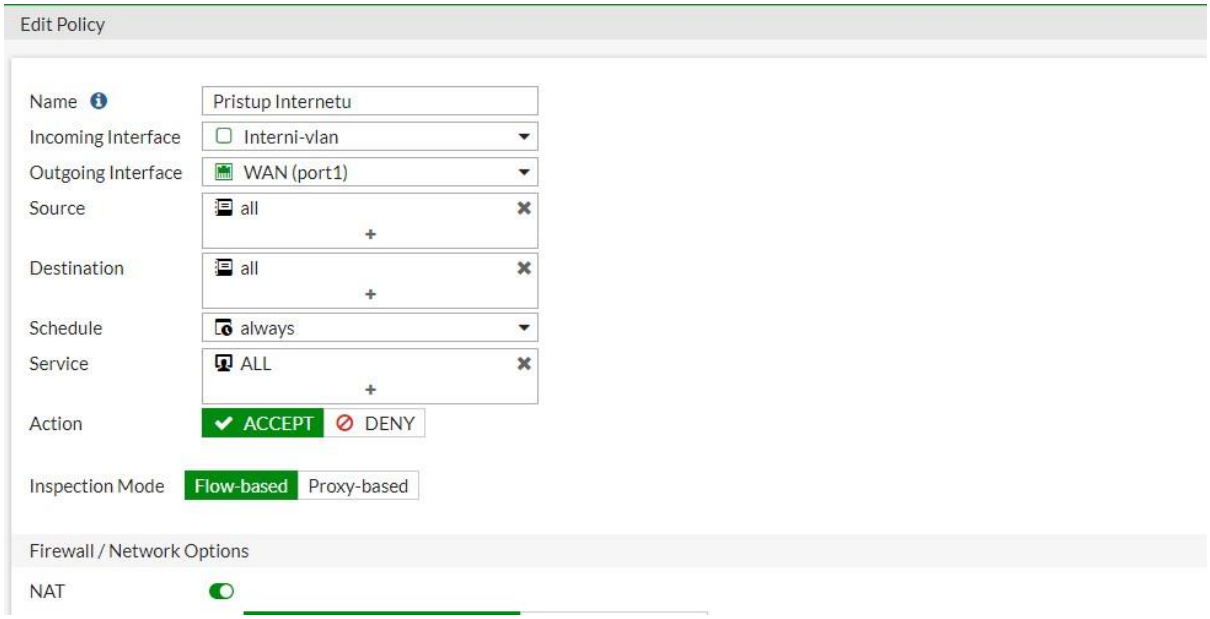
Izvor: samostalna izrada, 2022.

Nakon kreiranja sučelja, kreira se i zona kojem portu pripadaju VLAN sučelja. Kako bi VLAN sučelja neometano komunicirala i razmjenjivala podatke, iisključuje se opcija *Block intra-zone traffic* unutar zone. Predstavljeni pojmovi su na sljedećem slikovnom primjeru.



Slika 40. Prikaz Zone
Izvor: samostalna izrada, 2022.

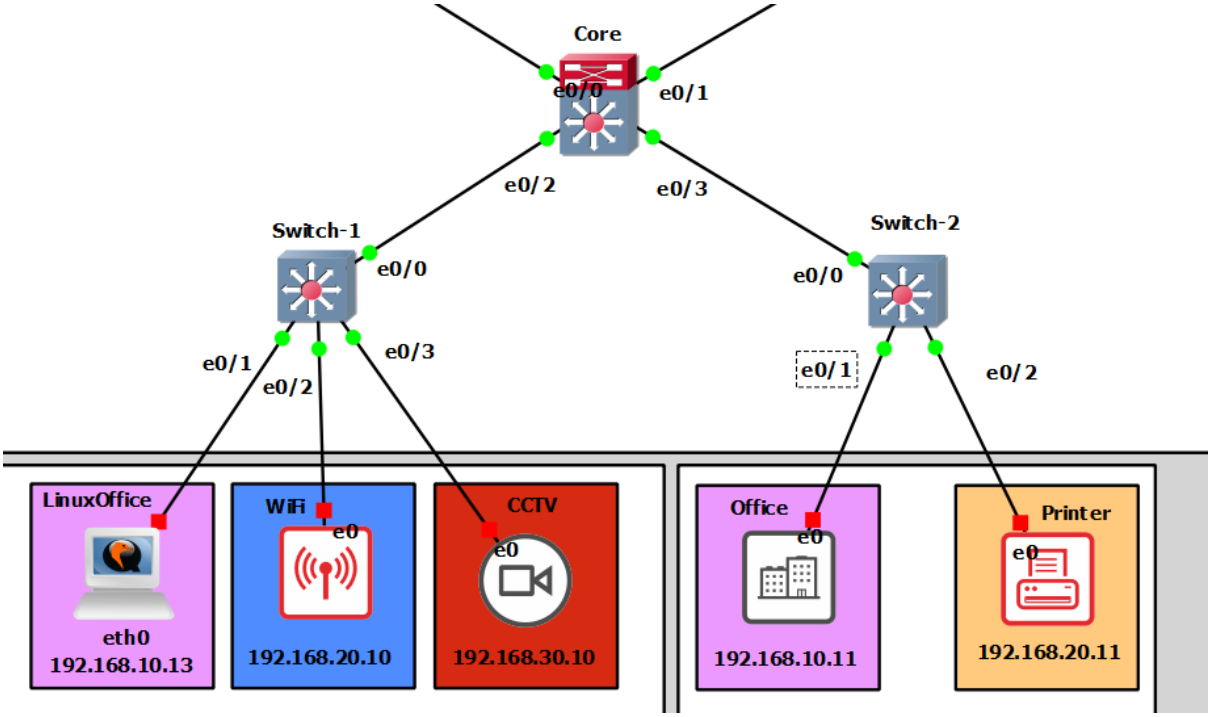
Nakon kreirane zone, ta zona se mora spojiti s internetom tako što se narede postavke u FortiGate-u. U parametrima se spajaju zone koja se nalaze na portu 2 sa zonom 1 koja ima direktnu vezu s internetom te obavezno NAT opcija mora biti uključena. Ovim opcijama se pristupa sekciji Firewall u FortiGate grafičkom sučelju. Parametri su na slici 41 .



Slika 41. Prikaz pristup Internet vezi od strane Zone
Izvor: samostalna izrada, 2022.

9.3.4. Konfiguracija preklopnika

Da bi krajnji uređaji bili povezani s vatrozidom i imali pristup internetu treba modificirati preklopnike. U svaki preklopnik treba kreirati VLAN tranking *(engl. VLAN trunk)* koji omogućuje kretanje prometa na različite dijelove VLAN mreže. Trank je *point-to-point* veza između dva mrežna uređaja koji nose jedan ili više VLAN-ova. S VLAN trankingom se može proširiti konfigurirani VLAN na cijelu mrežu. Pažljivo se odabiru ciljani portovi i kroz njih treba provesti trank i odrediti koji port će imati čije VLAN sučelje. Slika 42. nam predstavlja preklopnike i ime veza njihovih portova.



Slika 42. Prikaz preklopnika i krajnjih uređaja
Izvor: samostalna izrada, 2022.

Slika 43. prikazuje programiranje preklopnika naziva Switch-2. Port e0/0 ima trank konekciju koja je spojena s glavnim preklopnikom Core. Portu e0/1 se dodjeljuje VLAN 10, a portu e0/2 se dodjeljuje VLAN 20.

```
Switch-2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch-2(config)#int e0/0
Switch-2(config-if)#sw
Switch-2(config-if)#switchport trunk en
Switch-2(config-if)#switchport trunk encapsulation d
Switch-2(config-if)#switchport trunk encapsulation dot1q
Switch-2(config-if)#sw
Switch-2(config-if)#switchport mod tru
Switch-2(config-if)#int e0/1
Switch-2(config-if)#sw
Switch-2(config-if)#switchport mod acc
Switch-2(config-if)#ssw
Switch-2(config-if)#sw
Switch-2(config-if)#switchport acc vlan 10
% Access VLAN does not exist. Creating vlan 10
Switch-2(config-if)#int e0/2
Switch-2(config-if)#sw
Switch-2(config-if)#switchport mod acc
Switch-2(config-if)#s
Switch-2(config-if)#sw
Switch-2(config-if)#switchport acc vlan 20
% Access VLAN does not exist. Creating vlan 20
Switch-2(config-if)#end
Switch-2#wr
*Jan  4 14:18:34.462: %SYS-5-CONFIG_I: Configured from console by console
Switch-2#wr
Warning: Attempting to overwrite an NVRAM configuration previously written
by a different version of the system image.
Overwrite the previous NVRAM configuration?[confirm]
Building configuration...
Compressed configuration from 1527 bytes to 913 bytes[OK]
Switch-2#
```

Slika 43. Prikaz uspostavljanje funkcije portova
Izvor: samostalna izrada, 2022.

Slična procedura je za preklopnik Switch-1 i preklopnik Core, jedina razlika naspram preklopnika Switch-2 je ta da Switch-1 ima jedan VLAN više, a preklopnik Core na svojim portovima ima trunk konekciju i tri VLAN sučelja (sl.44).

```
Core#sh vlan bri

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Et1/0, Et1/1, Et1/2, Et1/3
                                                Et2/0, Et2/1, Et2/2, Et2/3
                                                Et3/0, Et3/1, Et3/2, Et3/3
10   VLAN0010                         active
20   VLAN0020                         active
30   VLAN0030                         active
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
Core#
```

Slika 44. Prikaz VLAN sučelja u preklopniku Core
Izvor: samostalna izrada, 2022.

Kako bi se provjerilo jesu li portovi spojeni i aktivirani, obavi se naredba u konzoli *show interface status* ili kraće - *sh int statu*. Tako se izlistaju informacije status portova.

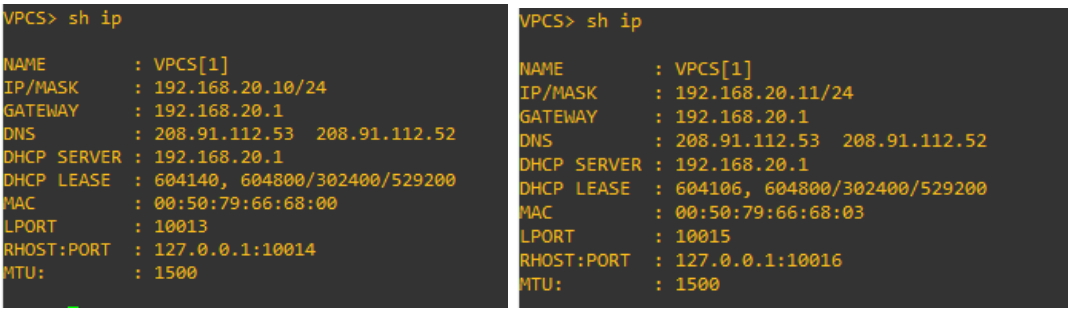
FortiGate7.0.2-1 | PC1 | PC2 | Switch

```
Switch#
Switch#sh int statu

Port      Name               Status       Vlan       Duplex  Speed Type
Et0/0                        connected    trunk        auto   auto unknown
Et0/1                        connected    10           auto   auto unknown
Et0/2                        connected    20           auto   auto unknown
Et0/3                        connected    30           auto   auto unknown
Et1/0                        connected    1            auto   auto unknown
Et1/1                        connected    1            auto   auto unknown
Et1/2                        connected    1            auto   auto unknown
Et1/3                        connected    1            auto   auto unknown
Et2/0                        connected    1            auto   auto unknown
Et2/1                        connected    1            auto   auto unknown
Et2/2                        connected    1            auto   auto unknown
Et2/3                        connected    1            auto   auto unknown
Et3/0                        connected    1            auto   auto unknown
Et3/1                        connected    1            auto   auto unknown
Et3/2                        connected    1            auto   auto unknown
Et3/3                        connected    1            auto   auto unknown
Switch#
```

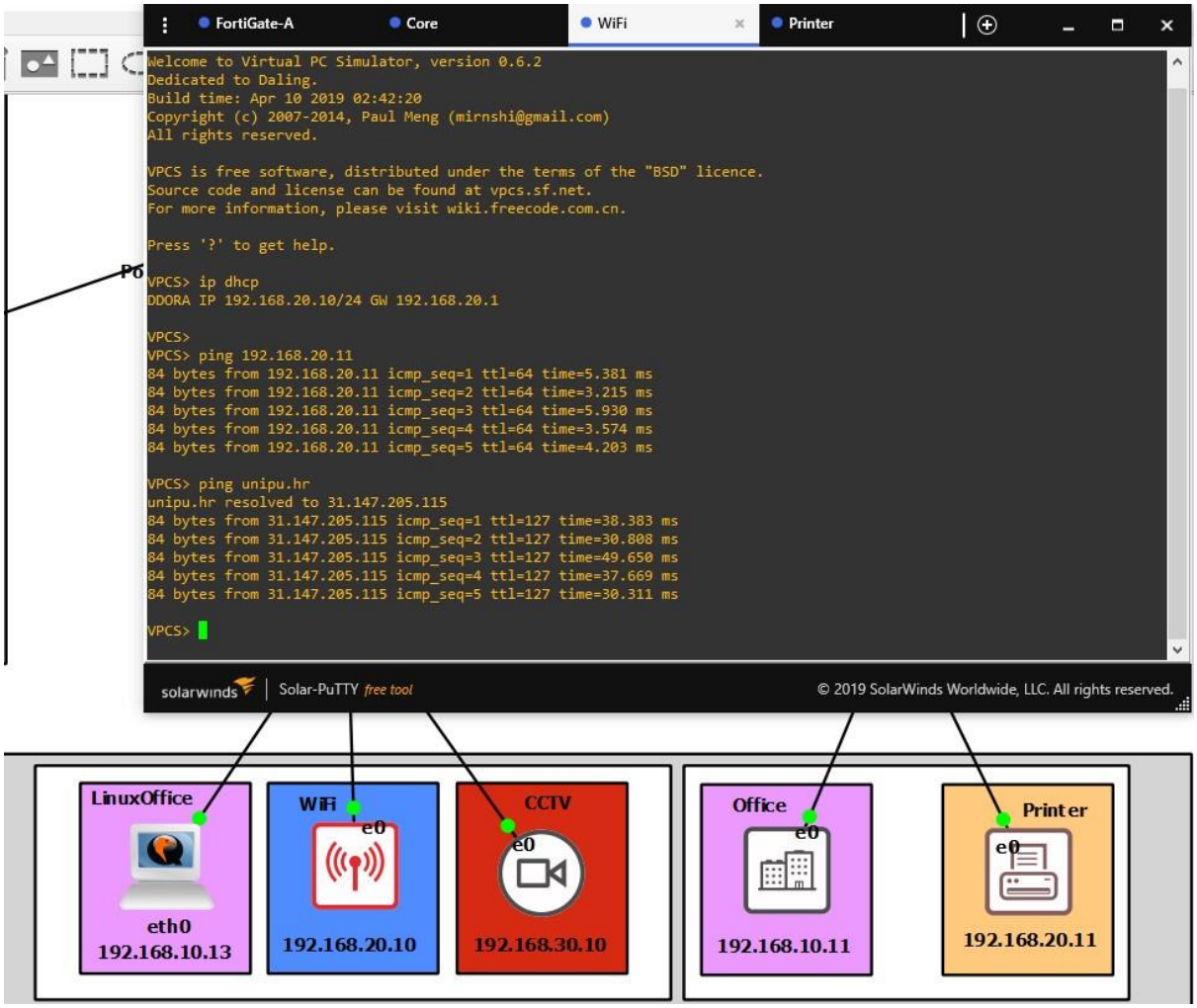
Slika 45. Prikaz status portova u preklopniku
Izvor: samostalna izrada, 2022.

9.4. Pokretanje LAN mreže s krajnjim uređajima

Ako je sve pravilno spojeno, naredbom ping se provjerava uspostava komunikacije uređaja i interneta. Zatim se pokrene VPCS koji služi kao WiFi te ima VLAN 20 (sl.46) kao sučelje. Da bi se dodijelila adresa, koristi se DHCP. Naredba *"ip dhcp"* služi za dodjeljivanje zadane adrese krajnjim uređajima. U ovom slučaju se dobije adresa 192.168.20.10/24 za WiFi i 192.168.20.11/24 za printer (sl. 47).



Slika 46. IP adrese VLAN 20
Izvor: samostalna izrada, 2022.

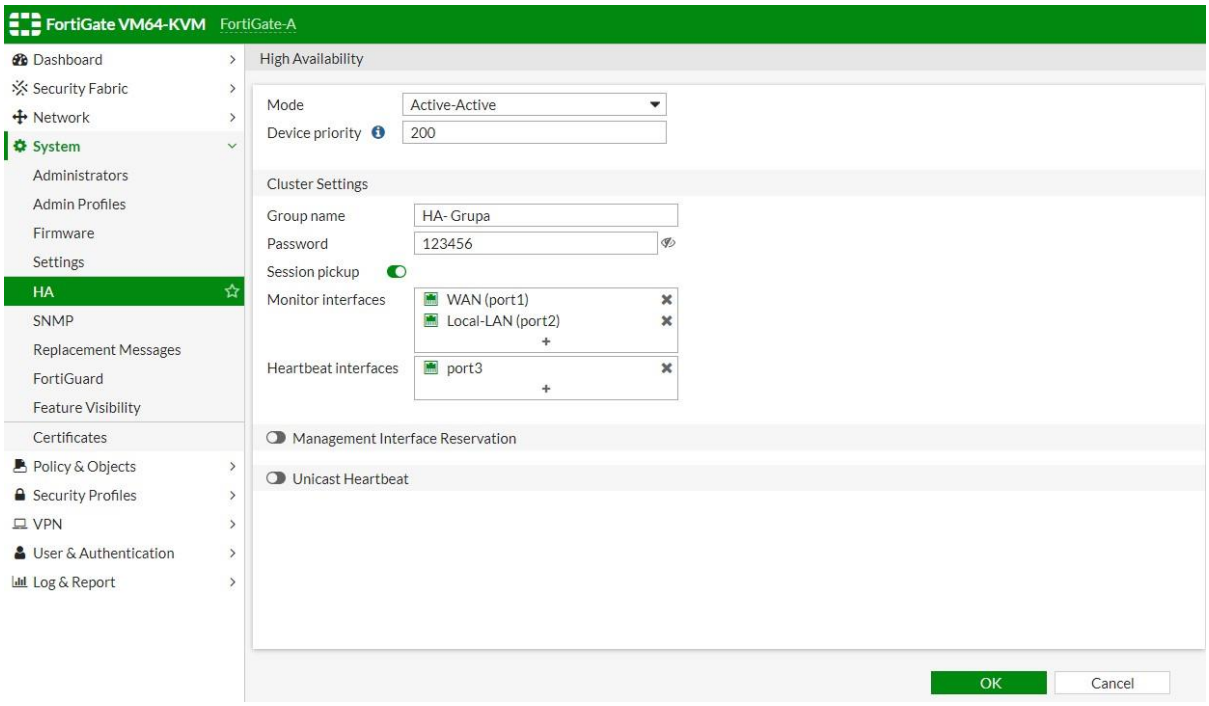


Slika 47. Prikaz komunikacije između Wifi-ja i printera
Izvor: samostalna izrada, 2022.

Na slici se vidi kako je veza između WiFi-ja i printera uspostavljena, te da je WiFi spojen na internet vezu.

Nakon uspješne uspostave komunikacije slijedi vraćanje na vatrozid FortiGate-B koji služi kao rezervni u slučaju pada, popravka, ili nepravilnog rada Master vatrozida da bi nam *Slave* (engl. sluga) vatrozid bio u pripremi da ga zamjeni. Kako se ne bi trebalo namještati sve iz početka, bitno je da konfigurirati *Heartbeat Link* - vezu između dva *FortiGate-a.* Pojam koji je konfiguriran zove se *High Availabiltiy* (HA) čija je svrha osigurati određenu razinu performansi za razdoblje duže od normalnog. Modernizacija je rezultirala povećanje oslanjanja na takve sustave (npr. bolnice). Podatkovni centri zahtijevaju visoku dostupnost tj. HA za obavljanje rutinskih aktivnosti koji se odvijaju svakodnevno i neprekidno. HA se nalazi u sekciji *System* na *FortiGate* sučelju. Mod se stavlja A-A odnosno *active-active* gdje dva ili više

uređaja rade kao tim. Prioritet uređaja se stavlja na 200 (jer je standardni broj 128) tako da *FortiGate-A* ima veći prioritet nego *FortiGate-B.* Monitoriranje se postavlja na portove koji žele biti praćeni, u ovom slučaju - port 1 i port 2. Port 3 je veza između dva vatrozida koja se naziva *Heartbeat*. Odabire se naziv grupe i određuje lozinka. Na slici 48. i 49. su jasno prikazane opcije i podešavanja.



Slika 48. Prikaz konfiguracije HA
Izvor: samostalna izrada, 2022.

```
FortiGate-A # sh sys ha
config system ha
    set group-name "HA- Grupa"
    set mode a-a
    set password ENC 51I4+ihWUDE7hQFUOH1AylIDcoy7ic2nV4GS3PAq+B/Gm32Vc3+AefOpj4JFg7CI6RBZe0DzLzcrnf6PZN8pm86qk2l6QqHcONkF19S
UFwk2bJ92e4bjCm2a7fgkey+cQz+q8SJCzwWvXJObBOR1Oz33Q0Xz26CSFtt0TlJ4OKyW3vBQVx1qsTZE7XRlN+Mh8mbEGg==
    set hbdev "port3" 0
    set session-pickup enable
    set override disable
    set priority 200
    set monitor "port1" "port2"
end
```

Slika 49. Parametri HA
Izvor: samostalna izrada, 2022.

Uspostavom HA se prelazi na konfiguraciju FortiGate-B-a. Kako ne bi morali sve svaku opciju naređivati zasebno, omogučujemo opciju *session-pickup* kako bi sinkronizirali parametre iz Master vatrozida (sl. 50).

```
FortiGate-VM64-KVM # con sys global

FortiGate-VM64-KVM (global) # set hostname FortiGate-B

FortiGate-VM64-KVM (global) # end

FortiGate-B # conf sys ha

FortiGate-B (ha) # set mode a-a

FortiGate-B (ha) # set group-name HA-Grupa

FortiGate-B (ha) # set password 123456

FortiGate-B (ha) # set session-pickup enable

FortiGate-B (ha) # set hbdev port3 0

FortiGate-B (ha) # end
```

Slika 50. Prikaz konfiguracija FortiGate-B
Izvor: samostalna izrada, 2022.

Slika 51. prikazuje informaciju da je sinkronizacija između FortiGate-A i B uspješno sinkronizirana, a slikovnim primjerom 52. je to potvrđeno.

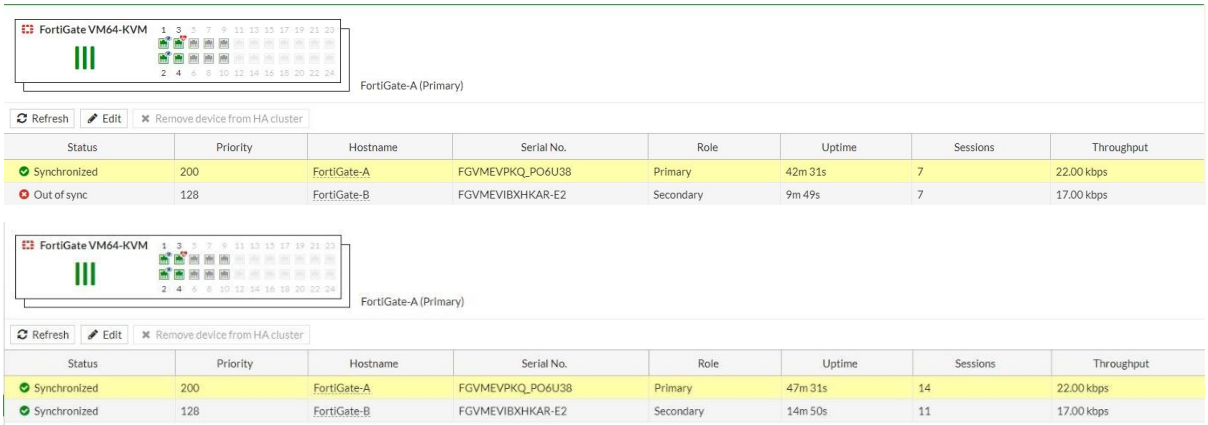
```
FortiGate-B # conf sys ha

FortiGate-B (ha) # set mode a-a

FortiGate-B (ha) # set group-name HA-Grupa

FortiGate-B (ha) # set password 123456

FortiGate-B (ha) # set session-pickup enable

FortiGate-B (ha) # set hbdev port3 0

FortiGate-B (ha) # end

FortiGate-B # secondary's external files are not in sync with the primary's, sequence:0. (type CERT_LOCAL)
secondary's external files are not in sync with the primary's, sequence:1. (type CERT_LOCAL)
secondary's external files are not in sync with the primary's, sequence:2. (type CERT_LOCAL)
secondary's external files are not in sync with the primary's, sequence:3. (type CERT_LOCAL)
secondary's external files are not in sync with the primary's, sequence:4. (type CERT_LOCAL)
secondary succeeded to sync external files with primary
secondary's configuration is not in sync with the primary's, sequence:0
secondary's configuration is not in sync with the primary's, sequence:1
secondary's configuration is not in sync with the primary's, sequence:2
secondary's configuration is not in sync with the primary's, sequence:3
secondary's configuration is not in sync with the primary's, sequence:4
secondary starts to sync with primary
logout all admin users

FortiGate-B #

FortiGate-B login: secondary's external files are not in sync with the primary's, sequence:0. (type CERT_LOCAL)
secondary's external files are not in sync with the primary's, sequence:1. (type CERT_LOCAL)
secondary's external files are not in sync with the primary's, sequence:2. (type CERT_LOCAL)
secondary's external files are not in sync with the primary's, sequence:3. (type CERT_LOCAL)
secondary's external files are not in sync with the primary's, sequence:4. (type CERT_LOCAL)
secondary succeeded to sync external files with primary
```

Slika 51. Prikaz uspješnog sinkroniziranja
Izvor: samostalna izrada, 2022.

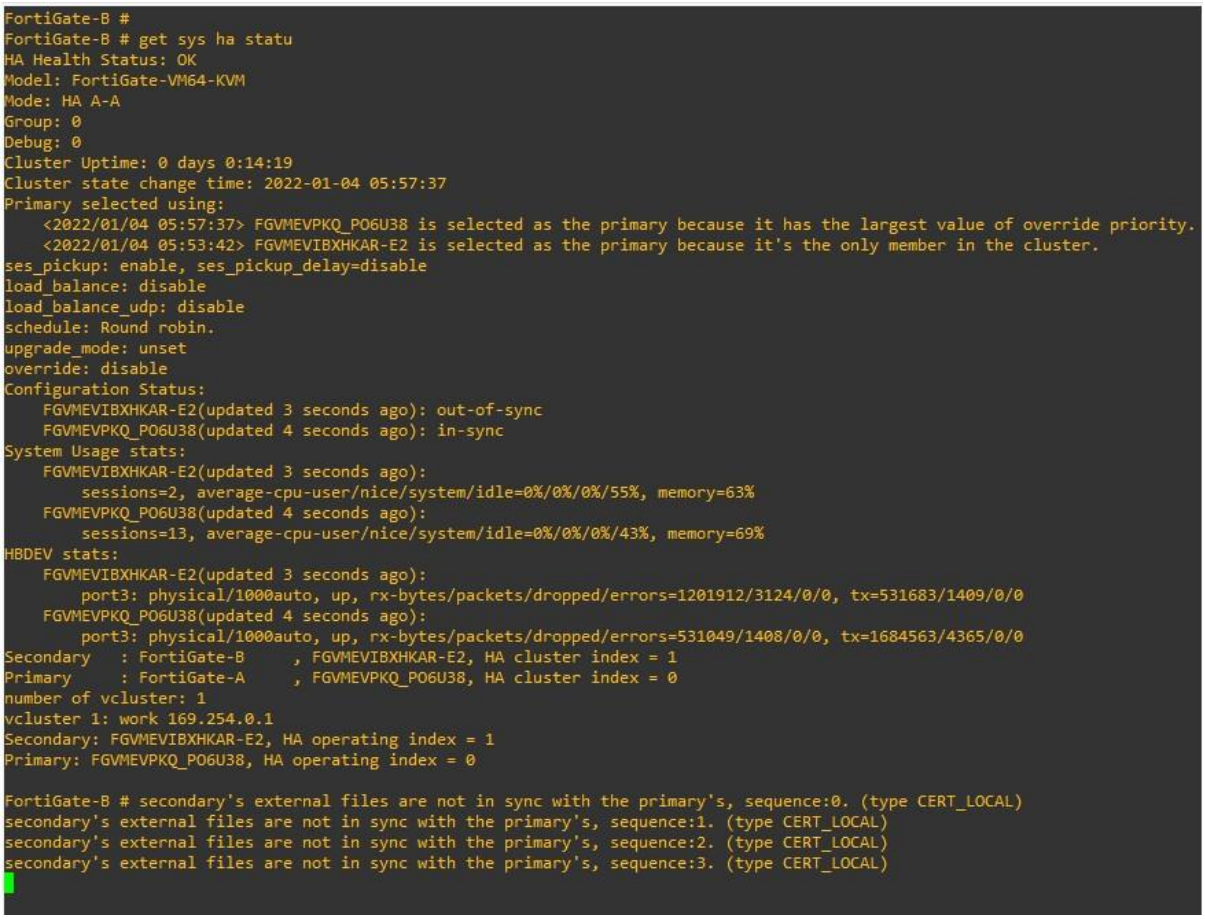
```
FortiGate-B # sh sys int
config system interface
    edit "port1"
        set vdom "root"
        set ip 192.168.68.10 255.255.255.0
        set allowaccess ping https ssh http
        set type physical
        set alias "WAN"
        set lldp-reception enable
        set role wan
        set snmp-index 1
    next
    edit "port2"
        set vdom "root"
        set type physical
        set alias "Local-LAN"
        set device-identification enable
        set lldp-transmission enable
        set role lan
        set snmp-index 2
    next
    edit "port3"
        set vdom "root"
        set type physical
        set alias "HA- Heart"
        set snmp-index 3
    next
    edit "port4"
        set vdom "root"
        set type physical
        set snmp-index 4
    next
    edit "port5"
        set vdom "root"
        set type physical
        set snmp-index 5
    next
    edit "port6"
        set vdom "root"
        set type physical
        set snmp-index 6
```

Slika 52. FortiGate-B nakon sinkronizacije
Izvor: samostalna izrada, 2022.

Slika 53. prikazuje prije i poslije sinkronizacije vatrozida i njihovu validnost za upotrebu. Slika 54. prikazuje status FortiGate-B i njegovu poziciju. Jasno se vidi da je sekundaran, njegovo aktivno vrijeme, vrijeme ažuriranja. Da bi dobili tu informaciju, koristi se naredba *„get sys ha statu“.*



Slika 53. Prikaz prije i poslije sinkronizacije vatrozida
Izvor: samostalna izrada, 2022.



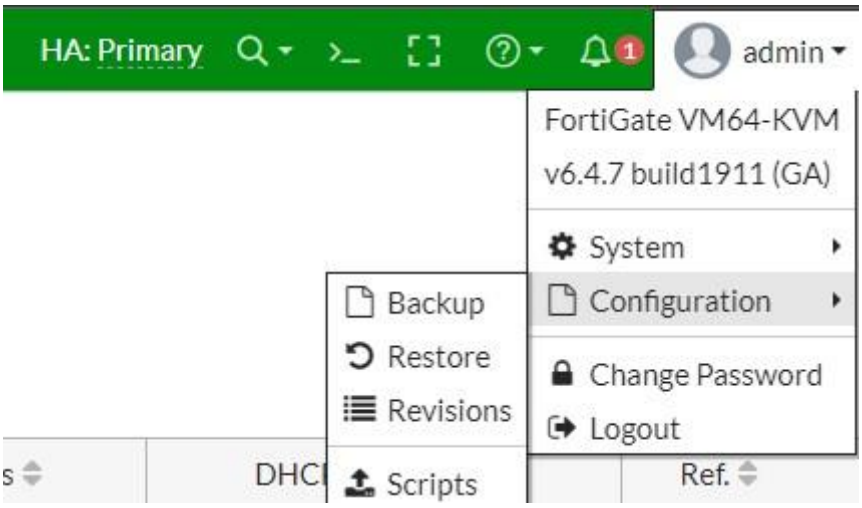
Slika 54. Prikaz parametara i statusa FortiGate-B
Izvor: samostalna izrada, 2022.

Kako dva uređaja rade kao tim oni dijele istu IP adresu. Da bi pristupiti određenom FortiGate vatrozidu treba kreirati njihove IP adrese. Opet se mora konfigurirati port 1 i dodati adresa za menadžment naredbom „*set managment-ip 192.168.68.11/24*“ za *FortiGate-A*. Za FG-B IP adresa bi bila 192.168.68.12/24.

```
FortiGate-A # conf sys int

FortiGate-A (interface) # edit port1

FortiGate-A (port1) # set management-ip 192.168.68.11/24

FortiGate-A (port1) # sh
config system interface
    edit "port1"
        set vdom "root"
        set management-ip 192.168.68.11 255.255.255.0
        set ip 192.168.68.10 255.255.255.0
        set allowaccess ping https ssh http
        set type physical
        set alias "WAN"
        set lldp-reception enable
        set role wan
        set snmp-index 1
    next
end
```

Slika 55. Dodavanje posebne IP adrese za menadžment FG-a
Izvor: samostalna izrada, 2022.

Da bi se mijenjali uređaji ili da ih se nadograđuje, često bi morali konfiguraciju započinjati od nule. No, Svaki *FortiGate* ima opciju za sigurnosnu kopiju koja se može zaključati. Prilikom isteka licence ili uspostave novog uređaja može se učitati prethodno zadana konfiguracija.



Slika 56. Prikaz spremanje sigurnosne kopije FortiGate-a
Izvor: samostalna izrada, 2022.

Podatke, usluge, FTP informacije se spremaju na siguran server tako da i u slučaju prestanka rada interneta se može pristupiti tim podacima te da se komunikacija unutar organizacije nastavlja.

9.5. DMZ

DMZ *(engl. demilitarized zone)* ili Delimitirizirana zona je perimetarska mreža koja štiti i dodaje dodatni sloj sigurnosti unutar LAN mreže od nepouzdanog prometa. DMZ je podmreža između internet mreže i privatne.

Cilj DMZ-a je omogućiti pristup organizaciji nepouzdanim mrežama kao što je Internet a istovremeno štiteći privatne mreže odnosno LAN. Organizacije obično pohranjuju vanjske usluge, resurse, web poslužitelje, FTP, DNS u DMZ. Pristup DMZ-u od strane napadača otežava izravan pristup podacima.

DMZ mreža pruža međuspremnik između interneta i privatne mreže organizacije. DMZ je izoliran sigurnosnim pristupom, kao što je vatrozid, koji filtrira promet između DMZ-a i LAN-a. Zadani DMZ poslužitelj zaštićen je drugim sigurnosnim pristupom koji filtrira promet koji dolazi s vanjskih mreža. Idealno je smješten između dva vatrozida, a postavljanje DMZ vatrozida osigurava da vatrozid ili drugi sigurnosni alati promatraju dolazne mrežne pakete prije nego što dođu do poslužitelja smještenih u DMZ-u. To znači da čak i ako sofisticirani napadač uspije proći prvi vatrozid, mora također pristupiti ojačanim uslugama u DMZ-u prije nego što može nanijeti štetu tvrtki.

9.5.1 Prednosti DMZ-a

Glavna prednost DMZ-a je osigurati internu mrežu s naprednim sigurnosnim slojem ograničavanjem pristupa osjetljivim podacima i poslužiteljima. Omogućavanje kontrole pristupa, tvrtke mogu korisnicima omogućiti pristup uslugama izvan perimetra svoje mreže putem javnog interneta. DMZ također može uključivati proxy poslužitelj, koji centralizira unutarnji protok prometa i pojednostavljuje praćenje i snimanje tog prometa.

Sprječavanje izviđanja mreže:

Pružajući međuspremnik između interneta i privatne mreže, DMZ sprječava napadače da obavljaju izviđački rad koji provode u potrazi za potencijalnim ciljevima.

Poslužitelji unutar DMZ-a javno su izloženi, ali im vatrozid nudi još jedan sloj zaštite koji sprječava napadaču da vidi unutarnju mrežu. Čak i ako DMZ sustav bude ugrožen, unutarnji vatrozid odvaja privatnu mrežu od DMZ-a kako bi bio siguran i otežavao vanjsko izviđanje.

Blokiranje lažnog internetskog protokola (IP):

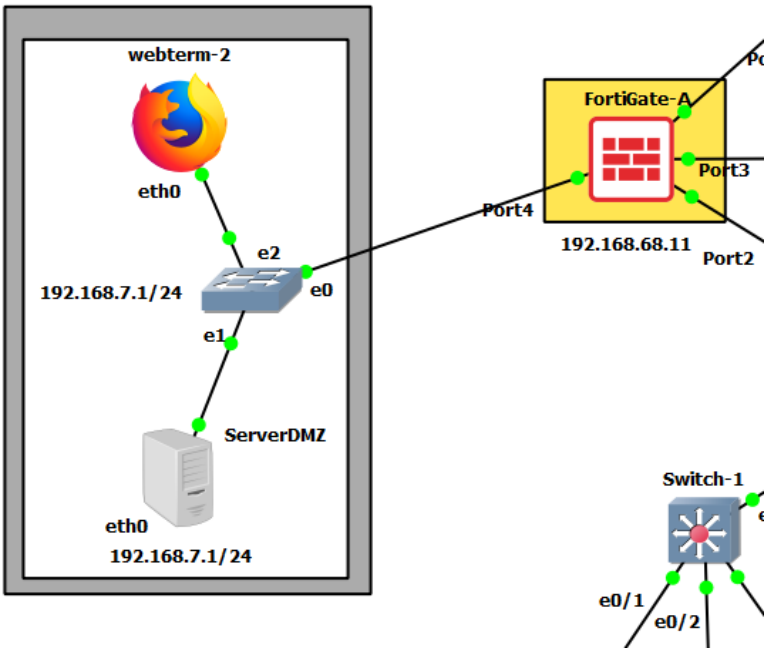
Napadači pokušavaju pronaći načine za pristup sustavima lažiranjem IP adrese i lažnim predstavljanjem od strane uređaja koji je odobren i prijavljen na mrežu. DMZ može otkriti i zaustaviti takve pokušaje lažiranja dok druga usluga provjerava legitimnost IP adrese.

Usluge DMZ-a uključuju:

- DNS poslužitelji
- FTP poslužitelji
- Poslužitelji pošte
- Proxy poslužitelji
- Web poslužitelji

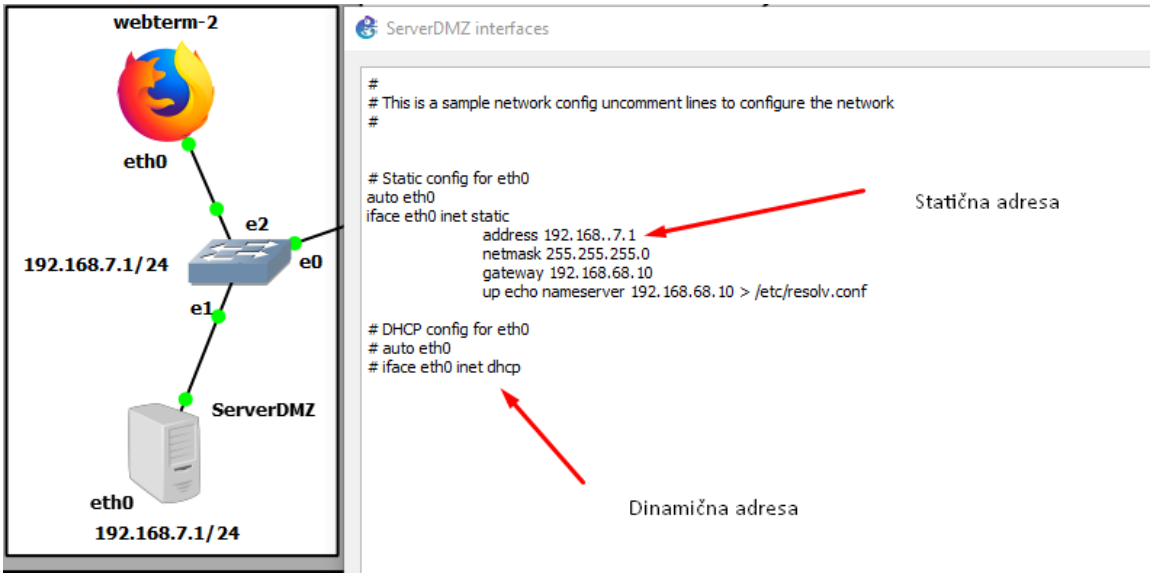
9.5.2. Kreiranje DMZ-a

Za kreiranje DMZ servera korišten je Docker-ov uređaj *Network Toolbox* koji podržava FTP, DHCP, SNMP server i drugo.



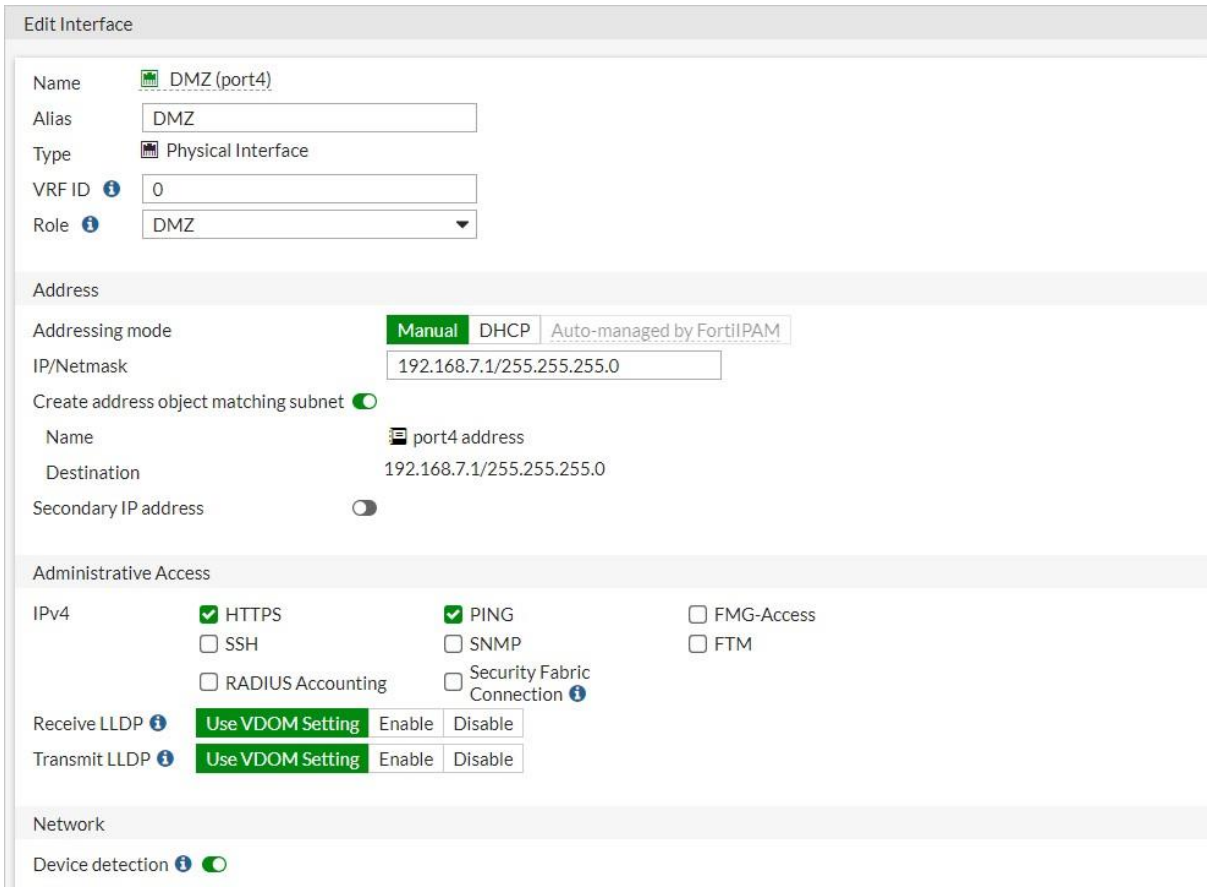
Slika 57. Prikaz DMZ zone
Izvor: samostalna izrada, 2022.

Za početak *Toolbox* se konfigurira tako što mu se zadaje statična IP adresa, podmaska, a za pristup se koristila adresa 192.168.68.10 koja je sučelje od *FortiGate-A*. Kako bi uređaj dobio automatsku adresu, trebaju se zakomentirati stavke za statičnu adresu a izbrisati # (ljestve) za zadnja tri reda koji su prikazani na slici 58.



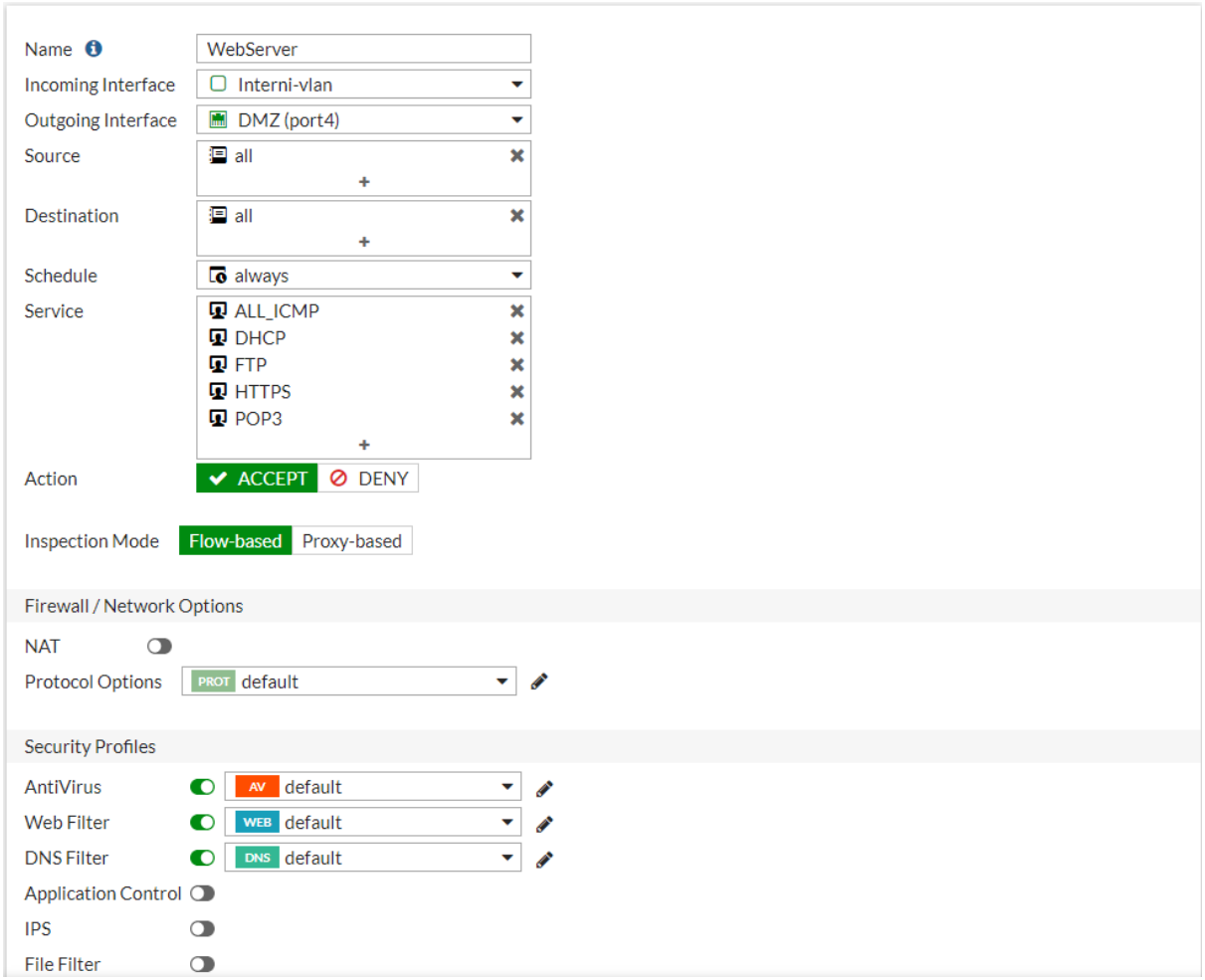
Slika 58. Prikaz konfiguracije Toolbox-a
Izvor: samostalna izrada, 2022.

Napravljena konfiguracija se sačuva i onda se odlazi na sučelje vatrozida *FortiGate-A* gdje se postavljaju zaštitna pravila i način komuniciranja i protok prometa. Za početak se konfigurirao port 4. Uloga priključka stavljena je DMZ, i zadana mu je pristupna IP adresu. Omogućena mu je funkcija ping radi provjere dostupnosti uređaja i pristup preko HTTPS-a (sl. 59).



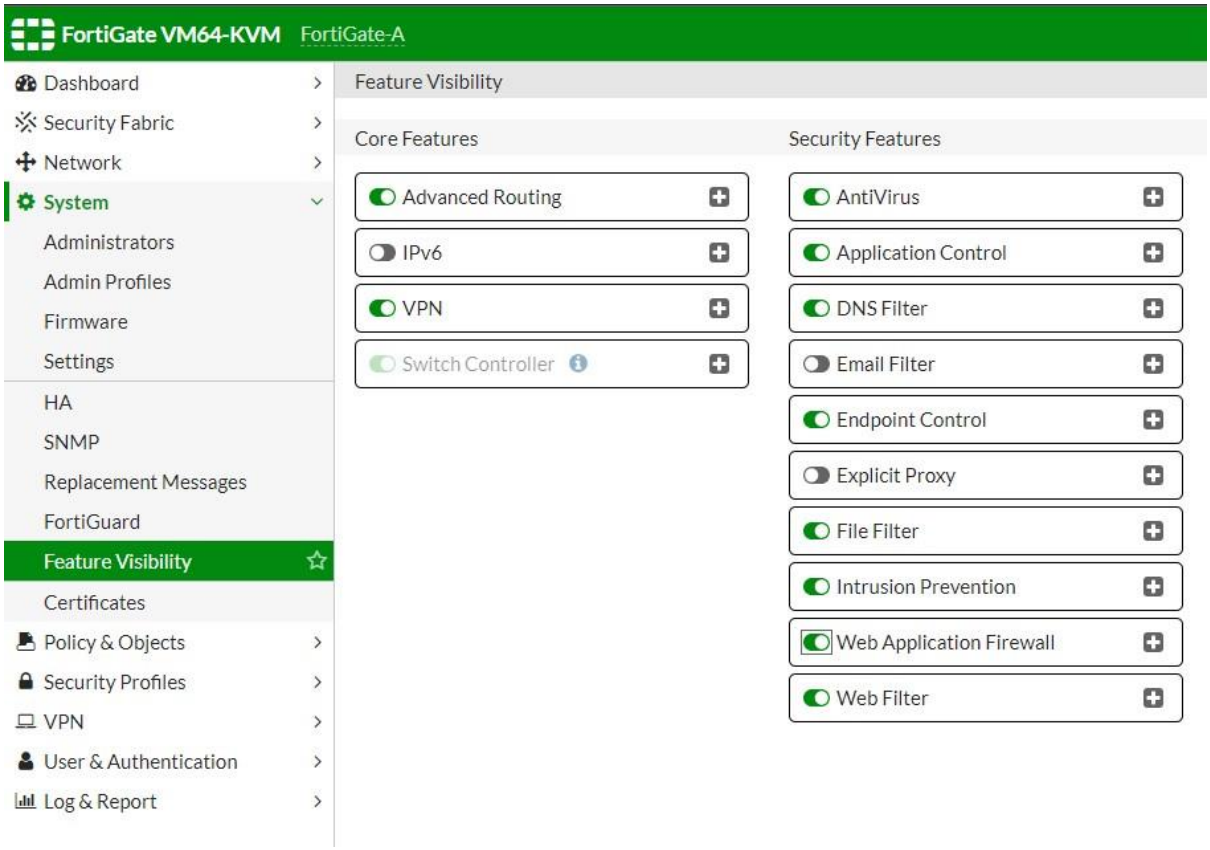
Slika 59. Prikaz konfiguriranje port 4 za DMZ
Izvor: samostalna izrada, 2022.

Slika 60. prikazuje pravila unutar tog vatrozida. Da se lakše raspoznaje pravilo, za ime se stavilo WebServer. Mjesto s kojeg se šalju upiti za informacije je stavljeno „Interni-vlan“ - koji je kreiran kada su se razvijala sučelja VLAN mreža. DMZ je nazvano odredište, port 4. Pod izvor je stavljen pristup adresi čiju autentifikaciju vrše preko e-mail adresa. Isto tako i za destinaciju, za usluge je stavljeno ALL_ICMP tako da se mogu vršiti sve ICMP poruke, HTTPS, FTP, POP3 za email i drugo. Opciju NAT je isključena zbog sigurnosnih razloga (kako ne bi imali pristup od strane internet veze). Uključene su funkcije za Antivirus, filtriranje web prometa (Web filter, DNS filter). Sav promet koji je dopušten se zapisuje u listu preko opcije *Log Allowed Traffic.*



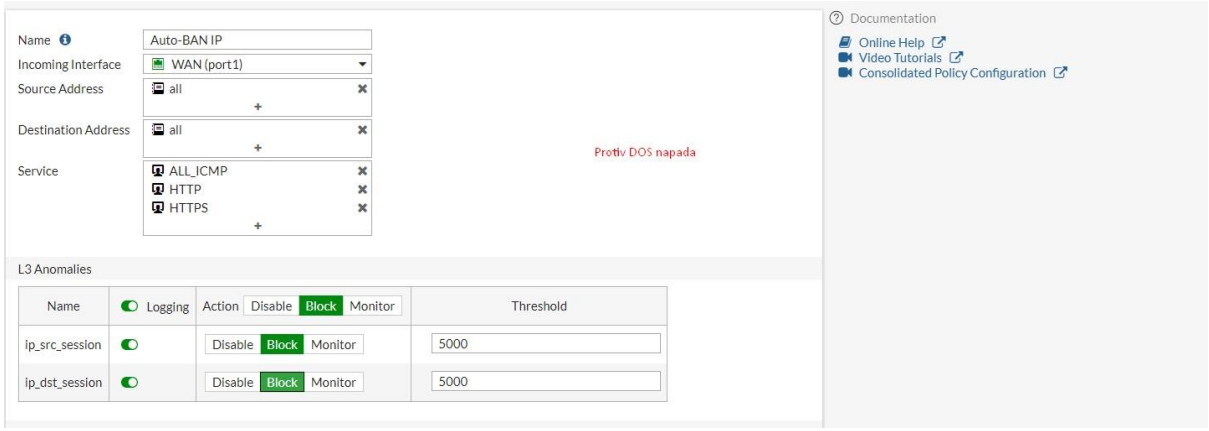
Slika 60. Konfiguracija parametara za DMZ u FortiGate-u
Izvor: samostalna izrada, 2022.

Kako bi podigli zaštitu treba uključiti opciju *Web Application Firewall* da bi se mogla kreirati i modificirati pravila sigurnosti odnosno rad samog vatrozida (sl.61)



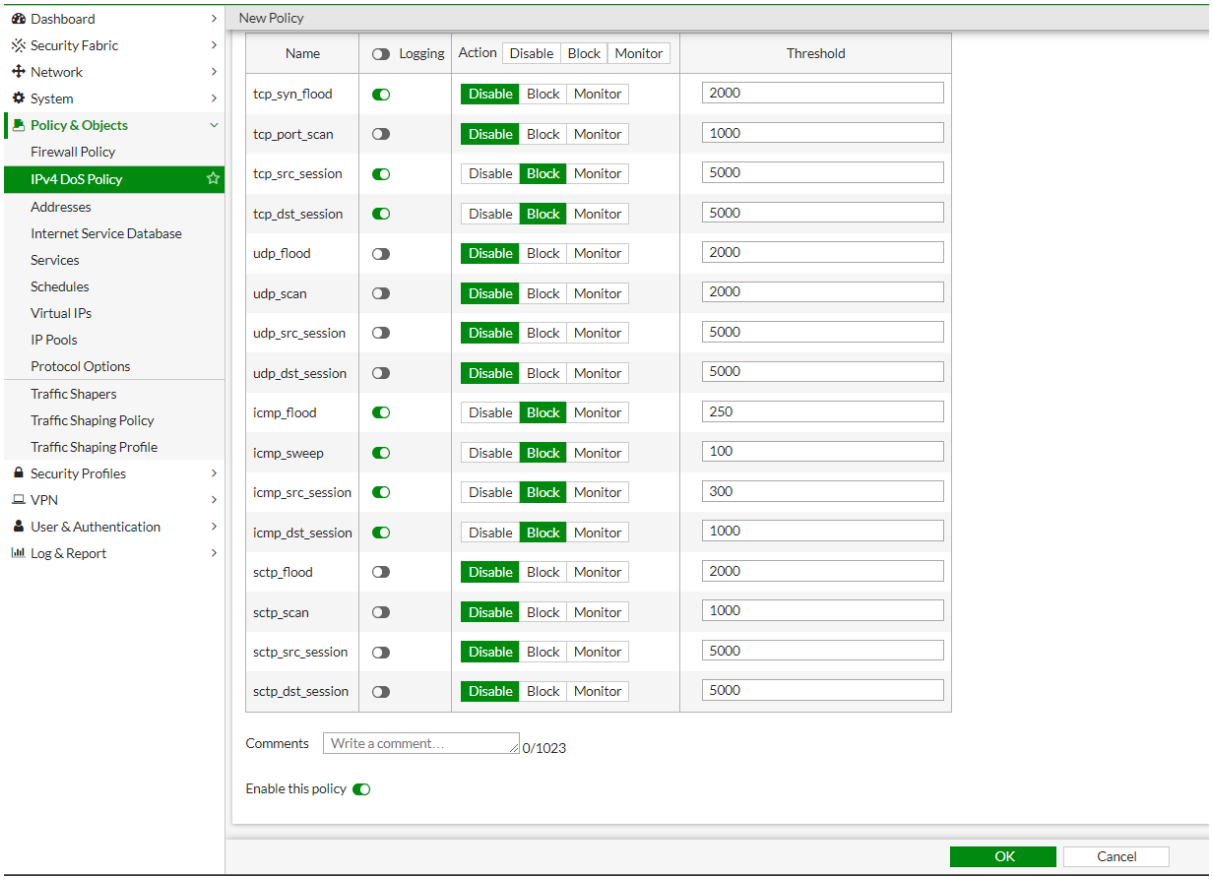
Slika 61. Dodatne sigurnosne opcije FortiGate
Izvor: samostalna izrada, 2022.

Protiv DOS *(engl. Denial of Service)* - postave se parametri i monitoriranje od strane porta 1. Ako previše sesija dolaze od strane izvora, treba ih blokirati. Isto tako ako ima previše nadolazećih izvora na server (sl. 62).



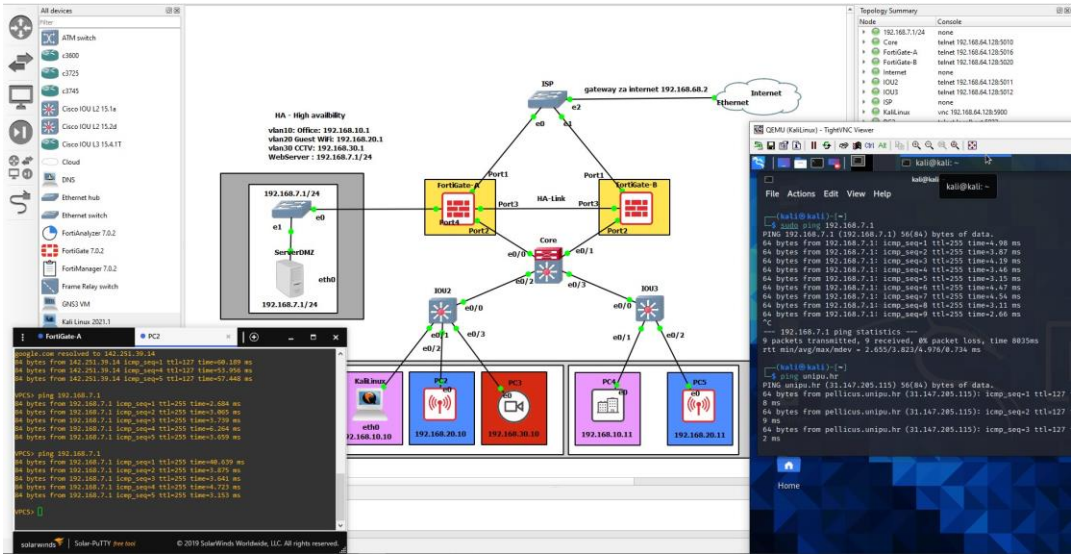
Slika 62. DoS pravila
Izvor: samostalna izrada, 2022.

Slika 63. prikazuje nastavak opcija koje se mogu monitorirati, blokirati ili isključiti. Kada bude abnormalno puno sesija preko ICMP ili TCP-a - treba ih blokirati.

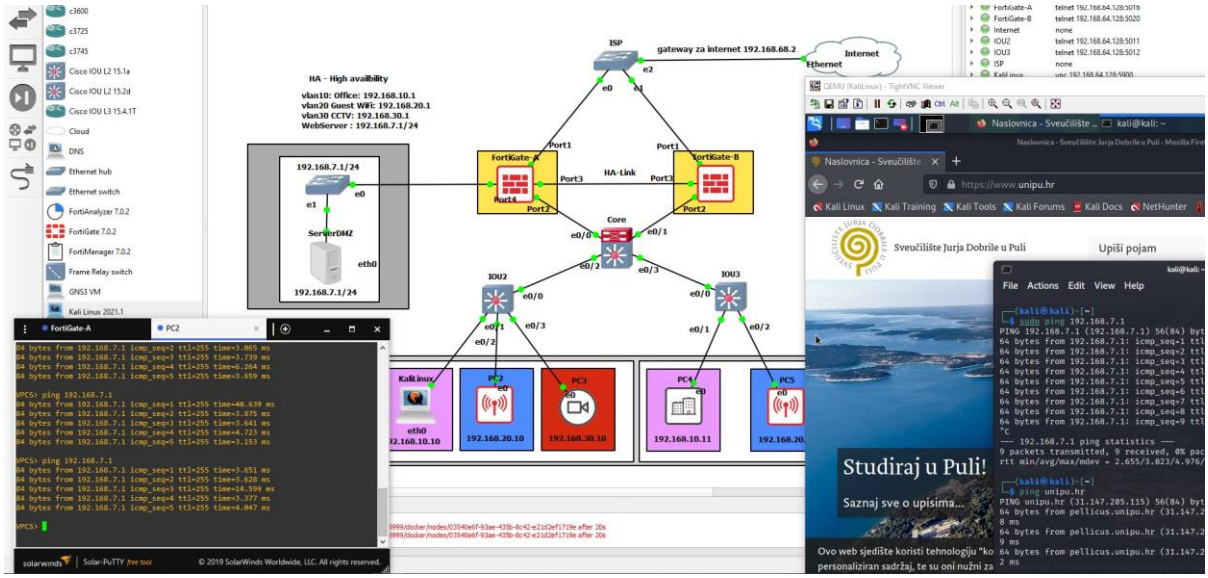


Slika 63. DoS pravila
Izvor: samostalna izrada, 2022.

Nakon postavljanja i konfiguriranje DMZ zone provjerava se funkcijom *ping* ima li dostupnost uređaja od strane drugih krajnjih uređaja. Slike 64 i 65. pokazuju uspješnu konekciju od strane operativnog sustava *Kali Linux i Windows 7.*



Slika 64. Komunikacija između Kali Linux-a i DMZ-a
Izvor: samostalna izrada, 2022.



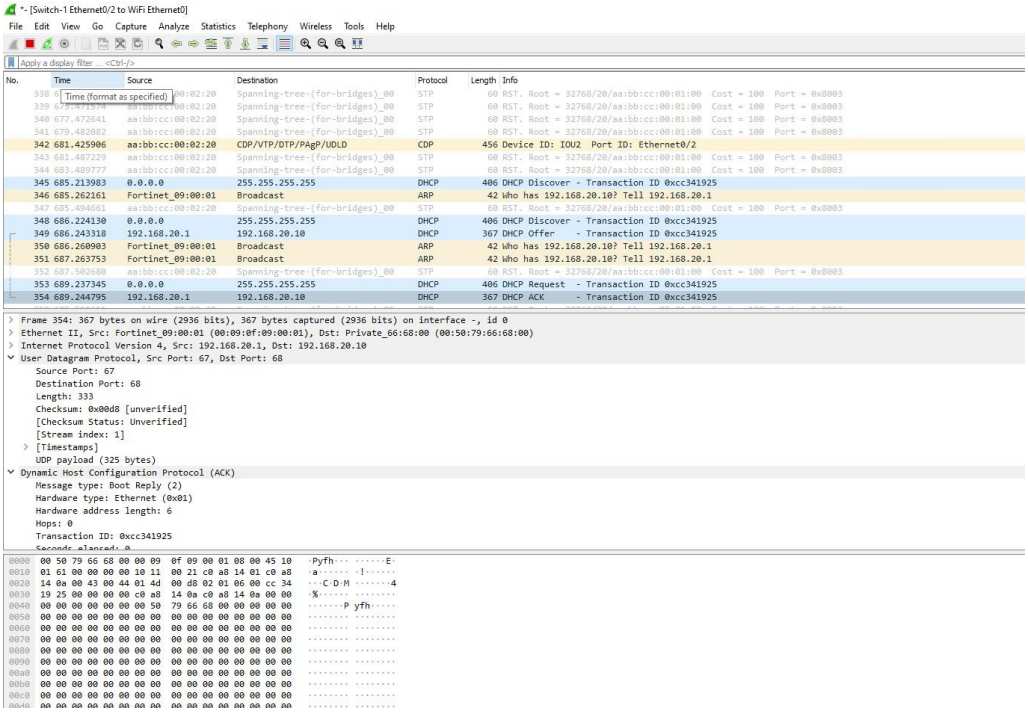
Slika 65. Komunikacija između Windows-a i DMZ-a
Izvor: samostalna izrada, 2022.

9.6. Wireshark

Da se dodatno analizira mrežni promet može se koristiti *Wireshark. Wireshark* je alat kojim se direktno prati i analizira paket unutar naših protokola. Uz pomoć ovog alata koji monitorira pakete mogu se riješiti mrežni problemi. On podatke iz paketa dekodira kako bi ih lakše razumio tako što „skine“ slojeve koji su enkapsulirani kako bi identificirao ili dopustio korištenje u mreži. *Wireshark* svoju analizu mreže razbija na tri panela:

- Sažetak; prikazuje sažetak u jednom retku protokola najvišeg sloja sadržanog u okviru, kao i vrijeme snimanja te izvorne i odredišne adrese.
- Detalj; pruža detalje o svim slojevima unutar okvira.
- Heksadecimalni; prikazuje neobrađene snimljene podatke u heksadecimalnom formatu

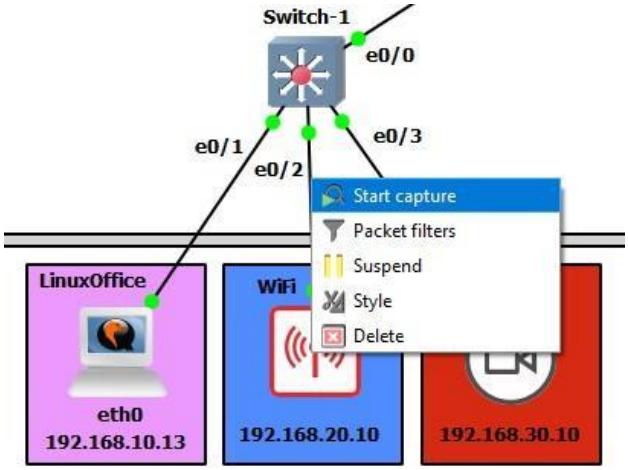
Slika 66. prikazuje sučelje tj. tri panela kroz koje se vidi filtriranje informacija o razmjeni paketa.



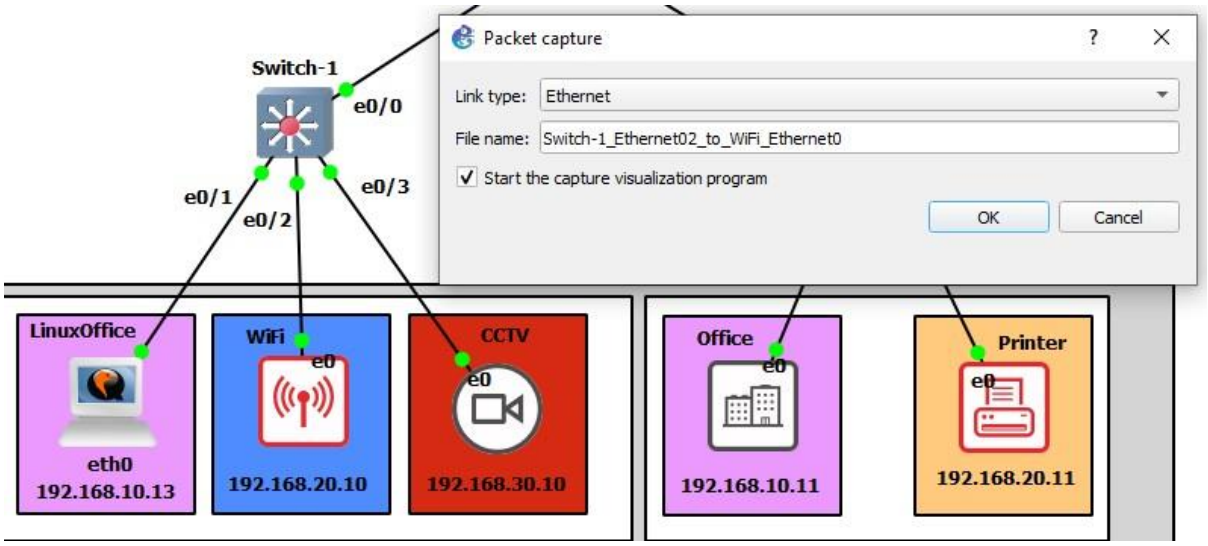
Slika 66. Prikaz sučelje Wireshark-a
Izvor: samostalna izrada, 2022.

Uz pomoć *Wireshark-a* se mogu dekodirati podatci u mreži, analizirati aktivnost mreže putem određenog protokola, generirati statistiku o aktivnosti mreže i proizvesti uzorke analize određene mreže. Slični programi kao što je *Wireshark* koji se mogu susresti su *WinPcap* ali on se mora koristit uz *Wireshark i Riverbed*, uz ove programe *Wireshark* može biti nadograđen i obrađivati i pružati analizu mreže na višoj razini.

Da bi se krenulo sa monitoriranjem treba odabrati koju rutu ili koji kanal treba analizirati. Desnim klikom na određen kanal se dobije opcija za analiziranje. Slika 67. i 68. prikazuju spomenute korake.Slika 68. Prikazuje komunikaciju prema uređaju WiFi koji je na VLAN 20 mreži.

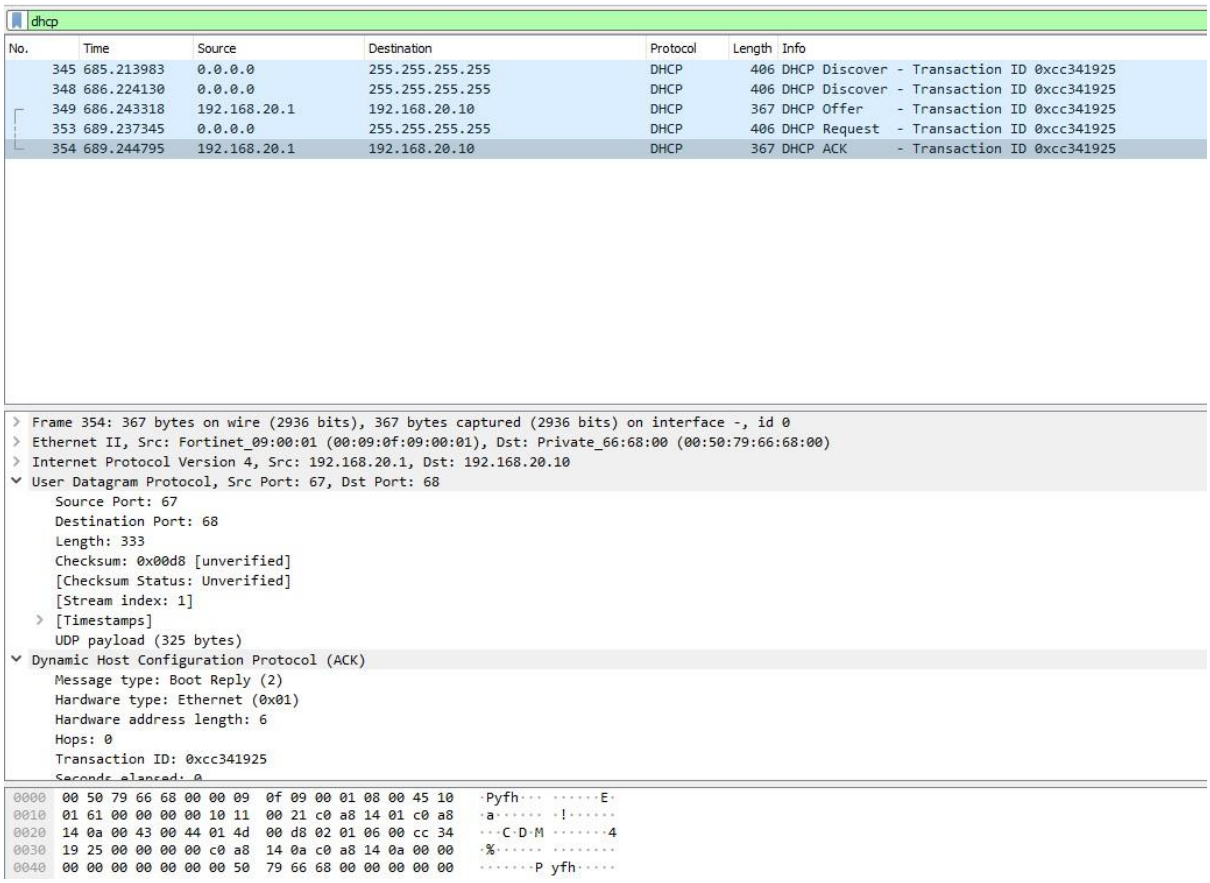


Slika 67. Opcija za analizu mreže putem Wireshark-a
Izvor: samostalna izrada, 2022.



Slika 68. Opcija za analizu mreže
Izvor: samostalna izrada, 2022.

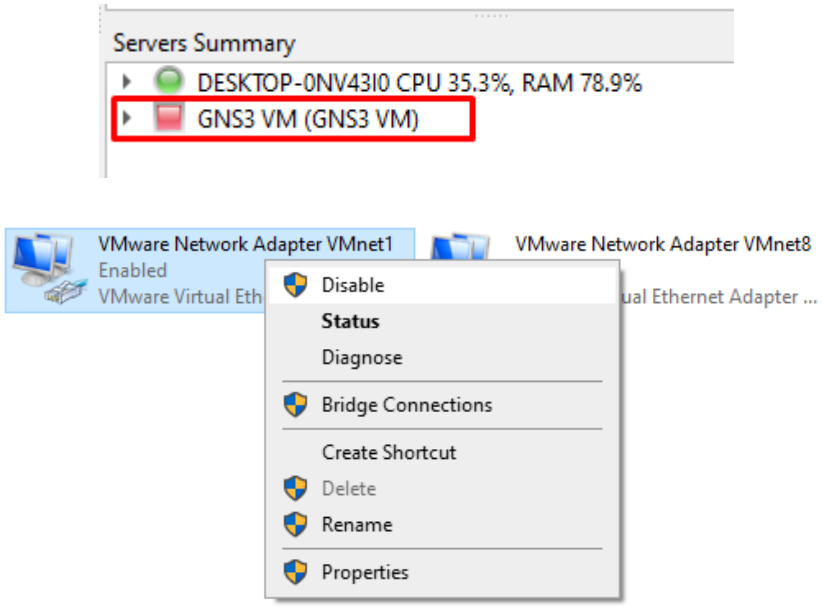
Sljedećim slikovnim primjerom 69. prikazano je vrijeme razmjene paketa, destinacija i izvorište portova, dužina trajanja komunikacije, veličina paketa, koji je protokol korišten i naziv ID transakcije i puno drugih informacija.



Slika 69. Prikaz analize VLAN 20 mreže
Izvor: samostalna izrada, 2022.

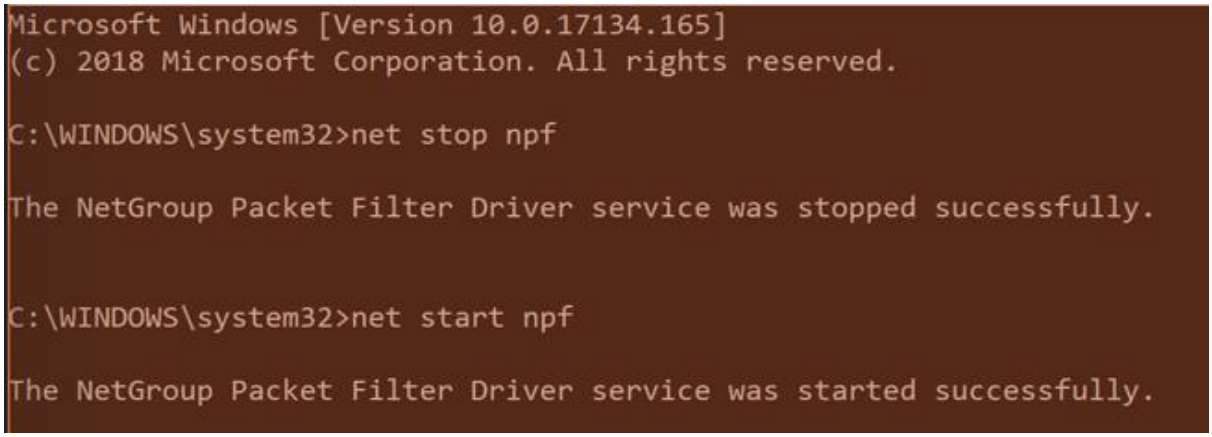
10. ČESTE POGREŠKE

a) Kada se prilikom pokretanja GNS3 programa ne želi pokrenuti virtualni server na *VMware-u*, treba isključiti mrežne adaptere *VMnet1i VMnet8* i ponovno ih uključiti (sl. 70).



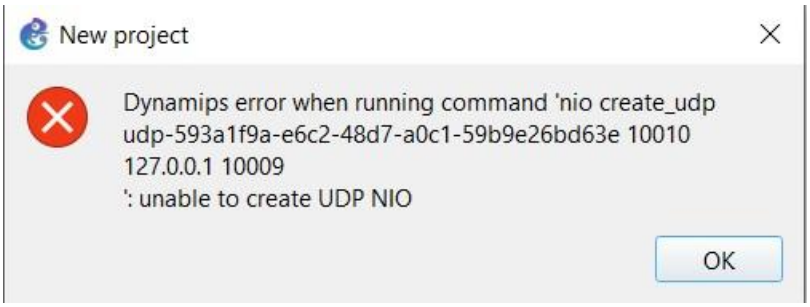
Slika 70. Restart VM servera
Izvor: samostalna izrada, 2022.

b) Ako i dalje server se ne može pokrenuti, niti NAT ne reagira, onda se u terminal upisuju sljedeće naredbe (sl. 71):



Slika 71. Restart VM servera
Izvor: samostalna izrada, 2022.

c) Ukoliko se pojavi greška *„unable to create UDP NIO“* prilikom otvaranja projekta, treba deinstalirati *Nvidia Geforce Experience* ili promijeniti UDP-ov port na kojem se GNS3 koristi.



Slika 72. Greška prilikom otvaranja projekta
Izvor: samostalna izrada, 2022.

11. ZAKLJUČAK

Promet koji putuje mrežnim sustavima putuje u obliku optičkog ili elektroničkog impulsa koji se naziva signal. U početku slanja informacija signal je čist i promatrački prepoznatljiv, prilikom na duže relacije on postepeno slabi. Kako ne bi izgubili trag signalu, potrebno ga je osvježiti. Za takvo nešto potrebni su mrežni uređaji koji će konstantno osvježavati signale i slati dalje u mrežnu infrastrukturu.

Šifrirani tekstovi i tajni ključevi se prenose preko mreže i mogu se naći pod nečijim povećalom za analizu podataka odnosno sami promet mreže. Kada se dokopaju takvih podataka mogu oponašati njihov izvor ili u gorem slučaju prouzročiti uskraćivanje usluge. Dakle kako bi pomogli enkripciji i složenim metodama distribucije, mreža mora biti sigurna i elegantna. Mreža treba imati primjenjive uređaje koji nadziru i otkrivaju napade, te da posjeduju određenu strategiju za nadmašivanje napadača. Mrežna sigurnost je drugačija tema od sigurnosti podataka, međutim odabrani uređaji moraju nadopunjavati cjelinu za infrastrukturu. Akumulacija u ključnim tehnologijama tvrtkama je omogućila da mogu predvidjeti cijelu infrastrukturu bez prepreka. Napredak u procesiranju signala koji koriste elektroničke sklopove i software za pretvaranje informacije u signale i signali koji nose informacije pogodne na određene udaljenosti ili pogodne za pohranu na određenu stanicu i ta obrada se događa munjevitom brzinom. Sveobuhvatna mrežna infrastruktura zahtjeva pristup koji omogućuje učinkovito upravljanje cijelom topologijom. Veliki su troškovi povezani za ugradnju i izgradnju same infrastrukture u objektima. Mreže moraju biti skalabilne i podržavati više vrsta medija kao što je optika ili bežični sustavi koji zahtijevaju različitu kvalitetu usluge te različite propusnosti podataka.

Sigurnost se odnosi na održavanje integriteta, povjerljivosti i pristupačnosti mreže i podataka. Sigurnosne mjere djeluju kao obrambeni mehanizam od vanjskih i unutarnjih zlonamjernih korisnika i ublažavaju sigurnosne napade. Narušavanje sigurnosti u PPVPN-u može rezultirati ponavljanjem, promatranjem, izmjenom ili brisanjem korisničkih podataka, ubacivanjem zlonamjernih podataka u mrežu, analizom uzorka prometa, degradacijom kvalitete usluge (QoS) PPVPN-a ili prekidom usluge. PPVPN omogućuje ograničenu i kontroliranu komunikaciju između pouzdanih zona kroz precizno definirane tranzitne točke.

Tijekom praktičnog dijela se dobiva u uvid široka lepeza kontrolem, odnosno spektar korištenja uređaja te višu implementaciju simulacijskih funkcionalnosti.

Primjena vatrozida *FortiGat*e-a koji može biti fizički, virtualan ili oba tipa, možemo spriječiti upade stranih i zlonamjernih faktora. Uz pomoć GNS3 se mogu simulirati okruženja i zaštiti ga virtualnim uređajima poput FortiGate ili pfSense. Otkriva se putem jednostavnog i centraliziranog sučelja raspon radnji i operacija za našu zaštitu te kontroliranje, monitoriranje, blokiranje različitih ruta, prometa i njihovih komunikacija između mrežnih uređaja. Obradia se DMZ zona koja je nužna svakoj organizaciji ili firmi za pravilno i sigurno odvijanje poslovanja.

Nesumnjivo u budućnosti kako bude rasla populacija ljudskog stanovništva i širenje mrežnih područja kao što je internet, te samim time rasti će broj klijenata i broj firmi koje će zahtijevati precizno i koncizno mrežno rješenje i različite topologije mrežnih tehnologija. Kako bi napredovali i održavali konstantu moramo obratiti na kvalitetu usluge ili dobra koje pružamo, te potreba za inovacijama i držanje korak za svjetskim trendovima. To je jedini način da se bude dominantan naspram ostalih. Kako bi izbjegli nepotrebno gubljenje vremena i novaca za kreiranje nekakvog mrežnog sklopa napamet, uz pomoć GNS3 možemo pronaći, iskoristiti adekvatne uređaje prema našim željama i proračunima i s vremenom ih nadograditi. Digitalna rješenja možemo iskorištavat u budućnosti i oblikovati ih prema potrebi drugih firmi i organizacija. Proizvodi se mogu isprobati bez kupnje uz njihovu licencu, te tako ubrzati proces istraživanja. Licenca za *FortiGate* virtualne uređaje je četrnaest dana gdje se besplatno može konfigurirati proizvod unutar probnog razdoblja. Kao zaključak tijekom analize istraživanja i montaža simulacije dolazi se do upoznavanja čimbenika mrežne tehnologije, njihov način rada kako bi prevenirali negativne utjecaje i poboljšali performanse unutar same mreže. Shodno tome mrežne emulacije imaju ključnu ulogu danas i u budućnosti u svijetu informacijske komunikacijske tehnologije (IKT). Svakodnevno stižu inovacije te samim time i njihove osjetljive točke koje je potrebno zaštiti. Današnji svijet sve više ide prema računarstvu u oblaku te samim time dolaze nove prijetnje koje zaobilaze standardne zaštite i mi moramo biti spremni i educirani o njima.

POPIS LITERATURE

Knjige i članci:

1. Catal, F., Tcholtchev, N., Höfig, E., & Hoffmann, A. 2019: *Visualization of Traffic Flows in a Simulated Network Environment to investigate abnormal Network Behavior in complex Network Infrastructures.* Procedia Computer Science

2. Procedia Computer Science Volume 130, 2018: *The Performance of IPv4 and IPv6 in Terms of Routing Protocols using GNS 3*

3. SimulatorComputer *Networks* 2008: *Volume 52, Dynamic traffic engineering for mixed traffic on international networks: Simulation and analysis on real network and traffic scenarios*

4. *UTM Security with Fortinet Mastering FortiOS,* 2013.

5. Juan Enrique Rubio, Cristina Alcaraz, Rodrigo Roman, Javier Lopez, 2019: *Current cyber-defense trends in industrial control systems,* Volume 87

Internet:

1. Campus Network for High Availability Design Guide Campus Network for High Availability Design Guide - Cisco, pristupljeno 2. rujna 2021.
2. Cisco Systems Products, Solutions, and Services - Cisco, pristupljeno 5. rujna 2021.
3. Computer and Information Security Handbook, Third Edition, 2017, poglavlje e87, pristupljeno 18. siječnja 2022.
4. Distributed network security framework of energy internet based on internet of things, pristupljeno 3. listopad 2021.
5. DMZ https://en.wikipedia.org/wiki/DMZ_(computing), pristupljeno 5. rujna 2021.
6. Exploring the Modern Computer Network: Types, Functions, and Hardware https://www.ciscopress.com/articles/article.asp?p=2158215&seqNum=6, pristupljeno 5. rujna 2021.
7. FortiGate virtual appliances https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-vm.pdf, pristupljeno 18. siječanj 2022.
8. King of Networking Different Types of Computer Networks - King Of Networking (weebly.com), pristupljeno 23. studenog 2021
9. Graphical Network Simulator (GNS) https://www.gns3.com/, pristupljeno 10. listopad 2021.
10. https://www.computernetworkingnotes.com/networking-tutorials/network-cable-types-and-specifications.html, pristupljeno 11. listopad 2021.
11. Internet Society http://www.internetsociety.org/articles/problems-low-delay-internet communication-congestion-management (srpanj 2016.) , pristupljeno 5. rujna 2021.
12. IPv4 https://hr.wikipedia.org/wiki/IPv4, pristupljeno 7. studenis 2021.
13. Product FortiGate https://www.fortinet.com/products/private-cloud-security/fortigate-virtual-appliances, pristupljeno 13. svibanj 2021.
14. Radlovački L.: Računarske mreže i komunikacije, Vršac, 2008. v02.Upredena.Parica.pdf (sbb.rs), pristupljeno 6. listopad 2021.

15. RIP https://hr.wikipedia.org/wiki/Routing_Information_Protocol, pristupljeno 5. rujna 2021.
16. TCP https://hr.wikipedia.org/wiki/TCP, pristupljeno 29. rujna 2021.
17. The Performance of IPv4 and IPv6 in Terms of Routing Protocols using GNS 3 Simulatorhttps://www.sciencedirect.com/science/article/pii/S187705091830509X, pristupljeno 13. rujna 2021.
18. Types of Network: LAN,WAN, WLAN; MAN, SAN, PAN, EPN & VPN Types of Networks: LAN, WAN, WLAN, MAN, SAN, PAN, EPN & VPN - Video & Lesson Transcript | Study.com
19. UDP https://hr.wikipedia.org/wiki/UDP, pristupljeno 12. studenog 2021.
20. VLAN https://hr.wikipedia.org/wiki/VLAN, pristup 12.studenog 2021.

Slike:

1. Mrežna kartica https://techterms.com/definition/nic, pristupljeno 15. siječnja 2022.
2. Preklopnik https://www.pngwing.com/en/search?q=Network+switch, pristupljeno 15. siječnja 2022.
3. Usmjernik https://toppng.com/router-PNG-free-PNG-Images_5055, pristupljeno 15. siječnja 2022.
4. Distribucija sigurnosti https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-vm.pdf, pristupljeno 15. siječnja 2022.

POPIS SLIKA

POPIS TABLICA

Tablica Akronima

Akronim – Definicija akronima

ACL - Access Control List

BGP - Border Gateway Protocol

CE - Customer Edge device

CPVPN - Customer Provisioned Virtual Private Network

DDoS - Distributed Denial of Service

DE - Domain Edge

DHCP – Dynamic Host Configuration Protocol

DNS – Domain Name System

DoS - Denial of Service

EIGRP – Enhanced Interior Gateway Routing Protocol

EVPN - Ethernet Virtual Private Network

FIB - Forward Information Base

FTP – File Transfer Protocol GNS – Graphical Network Simulator

HA – High Availability

I-BGP - Internal Border Gateway Protocol

ICMP - Internet Control Message Protocol

IoT - Internet of Things IP Internet Protocol

IPsec - Internet Protocol security

ISP – Internet Service Provider IS-IS – Intermediate System to Intermediate System

L2 - Layer two

L3 - Layer three

LSP/LSA – Link State Packet/Link State Advertisement

LSR - Label Switching Routers

MAC – Media Access Control

IEEE – Institute of Electrical and Electronics Engineers

MD-5 - Message Digest five

MPLS - Multiprotocol Label Switching

MTU - Maximum Transmission Unit

NIC – Network Interface Controller

OS - Operating System

PPVPN - Provider Provisioned Virtual Private Network

QoS - Quality of Service

RIP – Routing Information Protocol

S-BGP - Secure Border Gateway Protocol

SSL - Secure Socket Layer

TCP - Transmission Control Protocol

TCP – Transmission Control Protocol TCP/IP – Transmission Control Protocol/Internet Protocol

TLS - Transport Layer Security

UDP – User Datagram Protocol

VLAN - Virtual Local Area Network

VoIP - Voice over Internet Protocol

VPCS – Virtual PCs

VPLS - Virtual Private LAN Service

VPN - Virtual Private Network

WAN - Wireless Area Network

WLAN - Wireless Local Area Network

SAŽETAK

U diplomskom radu opisani su trendovi sigurnosti na mrežama uz koje ćemo prikazati pomoću simulacije. Razvojem informacijsko-komunikacijskih tehnologija javlja se potreba za novim načinom zaštite i njena konfiguracija. Svakodnevno raste broj firmi i organizacija što rezultira eksponencijalnim rastom i potraga za sigurnosna rješenja i konfiguracije.

Za potrebu izrade simulacije napraviti će se virtualna konfiguracija mrežnog sklopa u emulatoru GNS3. Potrebno je provesti istraživanje o samoj sigurnosti, mrežnim elementima i način konfiguracije tih elemenata u mrežnoj topologiji. U završnoj fazi rada očekuje se zaštita mrežnog prometa pomoću mrežnog vatrozida FortiGate.

KLJUČNE RIJEČI: GNS3, HA, FortiGate, Heartbeat-Link, DMZ; Mrežna arhitektura; Protokoli; IP; Računalne mreže; Simulacija;

SUMMARY

The thesis will describe the security trends in networks, which will be presented using a simulation. With the development of information and communication technologies, there is a need for a new way of protection and its configuration. The number of companies and organizations is growing every day, resulting in exponential growth and also the search for security solutions and configurations.

For the purpose of creating the simulation, a virtual configuration of the network assembly in the GNS3 emulator will be created. It is necessary to conduct research on the security itself, network elements and how to configure these elements in the network topology. In the final phase of work is protection of network traffic using the network firewall FortiGate.

KEY WORDS: GNS3, HA, FortiGate, Heartbeat-Link, DMZ; Network Architecture; Protocols; IP; Computer Networks; Simulation;